『推動 IPv4/IPv6 雙軌普行方案』

附錄六
『IPv6 寬頻分享器互通測試項目研究及 IASP 實際測試平台建置』

108 年委託研究報告

『IPv6 寬頻分享器互通測試項目研究及 IASP 實際測試平台建置』
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

IPv6 寬頻分享器互通測試項目研究及 IASP 實際測試平台建置

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、邱楷程、吳嘉偉、賴文彬

研究期程：中華民國 108 年 04 月至 108 年 12 月

研究經費：新臺幣 80 萬元

本報告不必然代表台灣網路資訊中心意見

中華民國 108 年 10 月

目　　次

表　　次 …… III

圖　　次 …… V

提　　要 …… VII

第一章 計畫執行狀況與檢討 1

第一節 計畫執行內容說明 1

第二節 與計畫符合情形 24

第三節 資源運用檢討 26

第二章 成果說明 28

第一節 IPv6 寬頻分享器製造商開發規範 28

第二節 IPv6 寬頻分享器製造商測試規範 37

第三節 IASP 實測平台建置與實機測試 49

第四節 政府採購共同供應契約設備參考規範 69

第三章 結論與建議 77

第一節 結論說明 77

第二節 建議事項 79

第四章 參考資料來源 81

附件一、 寬頻分享器相關 RFC 規範 1

附件二、 IPv6 Ready Logo 互連測試.....1

附件三、 寬頻分享器製造商訪談摘要.....1

附件四、 IPv6 寬頻分享器實機測試.....1

附件五、 政府採購共同供應契約設備參考規範.....1

表　次

表 1、IPv6 RA 封包上的 M/O/L/A 控制位元影響 4
表 2、IPv6 PPPoE 寬頻分享器測試項目 14
表 3、連接 Cable Modem 之 IPv6 寬頻分享器測試項目 . 15
表 4、各項工作執行進度 24
表 5、各項查核進度表 25
表 6、執行人力表 26
表 7、總經費運用情形統計表 27
表 8、總經費運用情形預估表 27
表 9、IPv6 寬頻分享器必須規範建議 29
表 10、IPv6 寬頻分享器選項規範建議 35
表 11、PPPoE 測試規範建議 38
表 12、IPoE 測試規範建議 40
表 13、SLAAC + stateless DHCPv6 搭配 RDNSS 配置測試規範建議 42
表 14、SLAAC + stateful DHCPv6 配置測試規範建議 .. 43
表 15、IPv6 PPPoE 斷線重撥測試規範建議 44

表 16、IPv6 MTU 測試規範建議 45
表 17、ICMPv6 封包過濾測試規範建議–DESTINATION UNRESEACHABLE 46
表 18、ICMPv6 封包過濾測試規範建議 – PACKET TOO BIG 46
表 19、IPv6 寬頻分享器 PPPOE 測試項目成果 I..... 51
表 20、IPv6 寬頻分享器 PPPOE 測試項目成果 II 53
表 21、IPv6 寬頻分享器 CABLE IPOE 測試項目成果 I..... 55
表 22、IPv6 寬頻分享器 IPOE 測試項目成果 II..... 56
表 23、IPv6 寬頻分享器之 LAN 端位址配置模式支援能力 58
表 24、IPv6 寬頻分享器之通訊界面支援能力 59
表 25、用戶連網終端作業系統 IPv6 支援評估 66
表 26、共同供應契約規範建議 71
表 27、既有共同供應契約 IPv6 相關規範 74

圖　次

圖 1、全球 GOOGLE IPV6 ENABLED USER 比例與預測.....1
圖 2、台灣 IPV6 發展趨勢與 ISP 支援 IPV6 比例.....3
圖 3、STATELESS 與 STATEFUL 位址配置流程.....5
圖 4、IPV4/IPV6 DS 網路位址配發方式..... 6
圖 5、IPV4/IPV6 固網寬頻相關 RFC 參考標準.....7
圖 6、模式一 RS/RA + DHCPV6 (STATELESS)..... 8
圖 7、模式二 RS/RA (RDNSS OPTION)..... 9
圖 8、模式三 RS /RA + DHCPV6 STATEFUL.....10
圖 9、模式四 RS/RA + DHCPV6-PD.....11
圖 10、計畫執行架構.....18
圖 11、HINET 光世代非固定制用戶 IPV6 連線架構.....19
圖 12、HINET 光世代 IPV6 寬頻分享器連線範例.....20
圖 13、CABLE 網路 IPV6 連網架構.....22
圖 14、CABLE 網路 IPV6 寬頻分享器連線範例.....23
圖 15、寬頻分享開發規範 IPV6 RFC 關聯圖.....28
圖 16、IPV6 PPPOE 連線測試架構.....38

圖 17、IPv6 over Ethernet 連線測試架構.....40
圖 18、寬頻分享器 IPv6 位址配置模式測試.....42
圖 19、IPv6 PPPoE 斷線重撥測試.....44
圖 20、IPv6 MTU 測試架構.....45
圖 21、寬頻分享器 IPv6 防火牆功能測試.....46
圖 22、IPv6 Ready LogoProgram 測試項目.....48
圖 23、IASP IPv6 實測平台.....49
圖 24、HiNet 光世代寬頻上網 IPv6 線路資訊.....50
圖 25、TBC 台灣寬頻 IPv6 線路資訊.....50
圖 26、寬頻分享器長時間 IPv6 連網測試 batch 腳本.....62
圖 27、PPPoE 長時間連網測試結果(1).....63
圖 28、PPPoE 長時間連網測試結果(2).....64
圖 29、Cable IPoE 長時間連網測試結果.....65
圖 30、政府採購共同供應契約之設備參考規範項目與來源
.....69
圖 31、各設備之 IPv6 參考規範內容.....70

提　要

關鍵詞：寬頻分享器、CPE、IPv6、PPPoE、Cable

一、研究緣起

鑑於 IPv4 位址資源逐漸耗盡，網路演進至 IPv6 已是國際共識,經過多年的發展,IPv6在技術能力上已經逐漸成熟，各國主要電信業者已陸續啟動 IPv6 商用運轉。由於 IPv6 技術已逐漸成熟，為協助 ISP 業者與網通設備業者驗證最後一哩IPv6商業部署所需的CPE網路設備功能,並了解國內IPv6寬頻分享器(CPE, Customer Premise Equipment)開發及實際連線使用情況，需研析 IPv6 寬頻分享器開發/測試與採購規範，並建立實際網路的測試環境，以確保廠商產品支援之 IPv6 功能符合我國固網環境之需求。為此，本計畫將建立IASP實測平台實際測試市售之IPv6寬頻分享器IPv6功能，並參考國際IPv6互連標準以及 Ready Logo 測試項目提出適合我國固網環境IPv6寬頻分享器之開發、測試以及共同供應契約參考規範，提供國內固網業者與設備廠商參考。

二、研究方法及過程

用戶寬頻分享器 CPE 是否支援 IPv6 功能是固網寬頻 CPE 的 IPv6 普及率的關鍵因素，CPE 裝置支援 IPv6 能力不一，除了讓用戶端終端裝置 IPv6 連線狀態不易檢測外，也會增加供裝營維運管理的複雜度。為此本計畫希望透過整理寬頻分享器 IPv6 互通測項以提供協助寬頻分享器製造業者開發 IPv6 寬頻分享器，並建置 IASP 實測平台以了解國內 IPv6 寬頻分享器開發及實際連線使用情況。

本計畫將依據我國固網寬頻環境 IPv6 的功能需求，針對 CPE 開發/測試/採購規範以及市售產品實際支援 IPv6 現況等四個議題進行探討。

(一) IPv6 寬頻分享器製造商開發規範：參考國際 RFC 標準，整理適合台灣固網環境連線中華電信 IPv6 PPPoE 及有線電視 Cable 業者之 IPv6 連線功能項目，並整理歸類哪些功能項目為必須，哪些功能項目為選項。

(二) IPv6 寬頻分享器製造商開發規範：參考 IPv6 Ready Logo 國際測試標準，提出 IPv6 寬頻分享器製造商開發規範並於 5 月前與至少兩家廠商完成訪談。

(三) 建立 IPv6 IASP 實測平台與實機測試：建置具 IPv6 PPPoE 及 IPv6 Cable Modem 之 IASP 連線實測平台，並於實測平台上測試製造日期為 2018 年（含）之後之 IPv6 寬頻分享器至少 10 款，需包含友訊、華碩、TP-Link 以及 TOTOLINK 等至少四家寬頻分享器製造商，每家至少二款，並整理測試報告。

(四) 政府採購共同供應契約設備參考規範:提出主機、伺服器、路由器以及網路保護裝置之共同供應契約之建議規範書以供參考。

為有效達成本計畫規劃之工作項目任務，開發/測試與採購規範建議方面的研究方法主要是以 RFC 國際標準以及 IPv6 Ready Logo 測項為主要參考依據，透過廠商面訪討論之方式，研擬適合我國固網環境的 IPv6 CPE 規範建議。在 IASP 實測平台與實機測試方面的研究方法則以申請國內固網業者 IPv6 測試電路以及購買市售寬頻分享器實際測試方式進行。

三、重要發現

(一) 根據廠商訪談的結果(附件三)發現，廠商對於新上市以及單價較高(高階)之產品型號啟動 IPv6 的意願較高，主要原因是廠商投入開發與測試的資源成本考量。

(二) IPv6 相關 RFC 標準規範條目數量眾多且涵蓋範圍廣泛，不過如廠商採 Linux-Based 的核心來實作，對於 IPv6 基本的功能如 DAD、ND 以及 SLAAC 自動配置機制、DHCPv6 等功能，作業系統本身已多能預設支援,實作設計上應可直接透過 GUI 介面將必須之 IPv6 功能整合即可支援。

(三) IPv6 CE Ready logo 互連測試規範是驗證 CPE IPv6 功能的國際標準，唯目前對於 PPPoE 以及 IPv6 安全檢測的項目仍略有不足。

四、主要建議事項

寬頻分享器的開發與測試多以 IETF RFC 國際標準為參考依據，本計畫已依據國際標準提出適合我國固網寬頻之開發與測試建議規範，為有效提昇我國固網寬頻網路 IPv6 使用率，以下針對寬頻分享器的 IPv6 推廣提出建議。

(一) 立即可行之建議

1. 網通廠商新上市之寬頻分享器 CPE 設備出廠即預設啟動 IPv4/IPv6 雙協定服務模式；
2. 網通商品需支援 IPv6 必須規格及測試項目，並建議政府納入共同供應契約，確保新採購之設備均能支援 IPv6；
3. 網通業者可提供支援 IPv6 合規的型錄清單，提供消費者採購相關商品的參考依據；
4. 主管機關提供設備廠商研發支援 IPv6 之相關獎勵、補助與減稅措施，以增加推動誘因；

(二) 中長期性建議

1. 鼓勵國內 Cable 業者應順勢逐步完善各級網路 IPv6 的佈署準備，與國際接軌，增加競爭力；

2. 建議電信業者可於網站主動公告寬頻網路 IPv6 連線設備須具備的 IPv6 必須功能，讓不同設備廠商能依據固網環境開發 IPv6 必備之功能選項；

3. 鼓勵電信業者與設備廠商採服務綁定之合作方式，提供客製化應用的服務模式。

4. CPE IPv6 網路安全議題重要性不可輕忽，由於涵蓋範圍廣泛且複雜性高，建議可另立專案研究，確保 IPv6 網路之安全。

Abstract

IPv4 address resources are gradually exhausted, and network evolution to IPv6 is an international consensus. After years of development, IPv6 has gradually matured in technical capabilities, and major telecommunications operators in various countries have started IPv6 commercial operations. As IPv6 technology has matured, in order to help ISPs and Network equipment manufacturers to verify the CPE network equipment functions required for the IPv6 commercial deployment, and to understand the development and actual connection of IPv6 CPE devices in Taiwan, it is necessary to study IPv6. CPE development/testing and procurement specifications, and establish a test environment for the telecom network to ensure that the IPv6 functionality supported by the vendor's products meets the requirements of Taiwan's fixed-line environment. The project will establish an IASP platform to test the commercially available IPv6 CPE functions, and refer to the international IPv6 interconnection standard and the Ready Logo program to propose the development, testing and joint supply contract for the IPv6 CPE in Taiwan's fixed-line environment. Refer to the specification to provide reference for

domestic fixed network operators and equipment manufacturers.

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，經過多年的發展，IPv6 在技術能力上已經逐漸成熟，各國主要電信業者已陸續啟動 IPv6 商用運轉。根據 Google 的統計[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 28.52%，較去年同期 18.3 成長約 8 個百分點，預計 2021 年將超過 40%。其中比利時 53.63%連線 Google 使用 IPv6 的比例為全球第一。上述資料為 2019 年 10 月 6 日的統計結果。

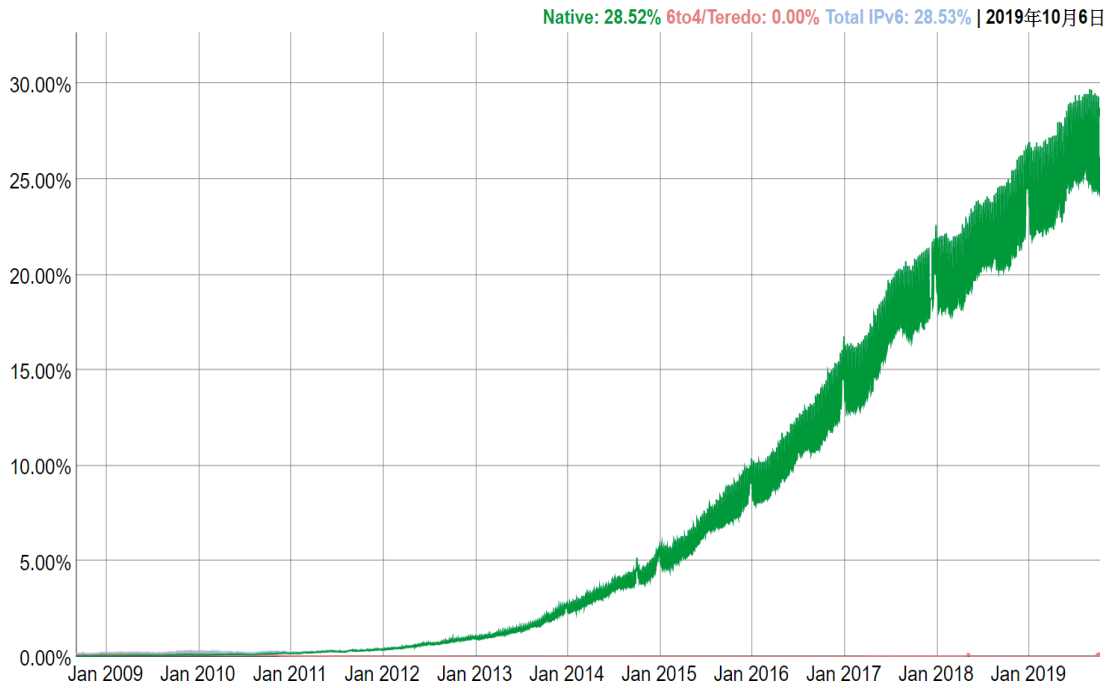


圖 1、全球 Google IPv6 Enabled User 比例與預測

在台灣的部份，依據台灣網路資訊中心 IPv6 全球排序網站公開資訊[2]，如圖 2 所示。2017 年 12 月台灣 IPv6 比例僅 0.38%，排名全球第 67。但自國內中華電信 2018 年年初 4G 行動上網 IPv6 開始商用服務，5 月 HiNet 光世代及公眾 Wi-Fi 逐步啟用 IPv6，台灣大哥大 4G 行動上網亦逐步啟用 IPv6，使台灣 IPv6 比例快速竄升，截至 2019 年 10 月，台灣 IPv6 全球排名已躍升至第 5 名。國內主要電信業者皆已啟動雙協定 IPv4/IPv6，國內前五大支援 IPv6 之 ISP 分別為：中華電信行動 LTE 網路 IPv6 比例為 81.03 %；遠傳 FETNet 為 62.74 %；台灣大哥大 Taiwan Mobile 45.85 %；亞太 AMBIT 32.07%以及中華電信固網光世代 23.02%。上述資料為 2019 年 10 月 6 日的統計結果。從支援 IPv6 的 ISP 來觀察，顯示行動網路的 IPv6 普及率較固網來得更高，主要原因如下：

- 4G LTE 與 VoLTE 屬於新建網路，順勢導入 IPv6 包袱較少，除可減緩整個行網對 IP 位址的消耗與需求，亦能提供電信業者長期發展演進的網路基礎，確保網路服務不中斷。
- 固網 CPE 設備支援 IPv6 程度不一，且固網 CPE 設備汰舊換新的過程複雜且費時，特別是用戶自備之寬頻分享器、SOHO Router、Wi-Fi AP 等，未能有一致的 IPv6 功能規範，是影響固網 IPv6 普及率的發展關鍵。

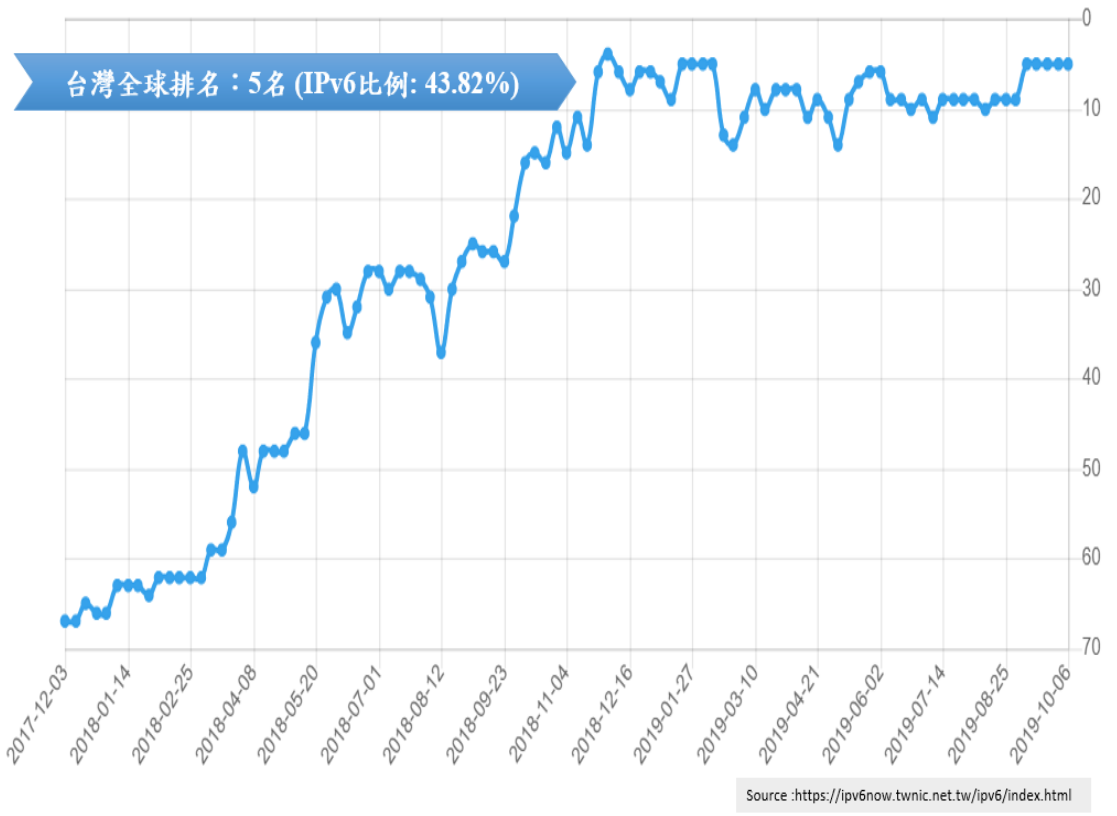


圖 2、台灣 IPv6 發展趨勢與 ISP 支援 IPv6 比例

二、IPv6 位址配置模式

在 IPv6 的網路環境中，用戶端設備 IPv6 位址的取得是連網服務的必須條件，以下將就 IPv6 位址自動配置的程序與位址配發模式說明。

(一) IPv6 自動配置程序

以位址配發方式來說，IPv6 具備隨插即用(Plug & Play)的特性，也就是用戶設備主機具備自動定址(Auto-configuration)的機制，終端設備可以在沒有額外輔助的情況下自動地從網路上收集資訊來進行設定，自動配置的資訊最主要是包含 IP 位址，預設路由閘道器位址(Default Gateway Address)以及 DNS 伺服器位址參數等三項基本的連網要素，其配置程序如圖 3 所示。依據網路路由廣播 RA 配置參數的不同，用戶端設備進行 IPv6 的自動定址的程序也有些許不同，其主要取決於 RA 封包上的 M/O/L/A 控制位元的影響，其影響如下表所示。

表 1、IPv6 RA 封包上的 M/O/L/A 控制位元影響

控制位元	影響
M	➢ 1-bit "Managed address configuration" flag. ➢ 主要用來確認用戶端設備是否採用 Dynamic Host Configuration Protocol [DHCPv6]的方式進行配置 ➢ 若 M Flag 設定為 1 表示採用 DHCPv6 進行配置，且 O Flag 就無需再確認
O	➢ 1-bit "Other configuration" flag. ➢ 主要是確認用戶端設備是否有其他參數配置的需求，例如 DNS 位址資訊
L	➢ 1-bit "on-link" flag. (default = 1) ➢ 主要是用來確認用戶端設備是否可有效配置該網段的 Prefix 參數
A	➢ 1-bit "autonomous address-configuration" flag. (default

	= 1) ➢ 主要是用來確認用戶端設備是否採用 Stateless Address Auto Configuration (SLAAC) 的方式進行自動配置

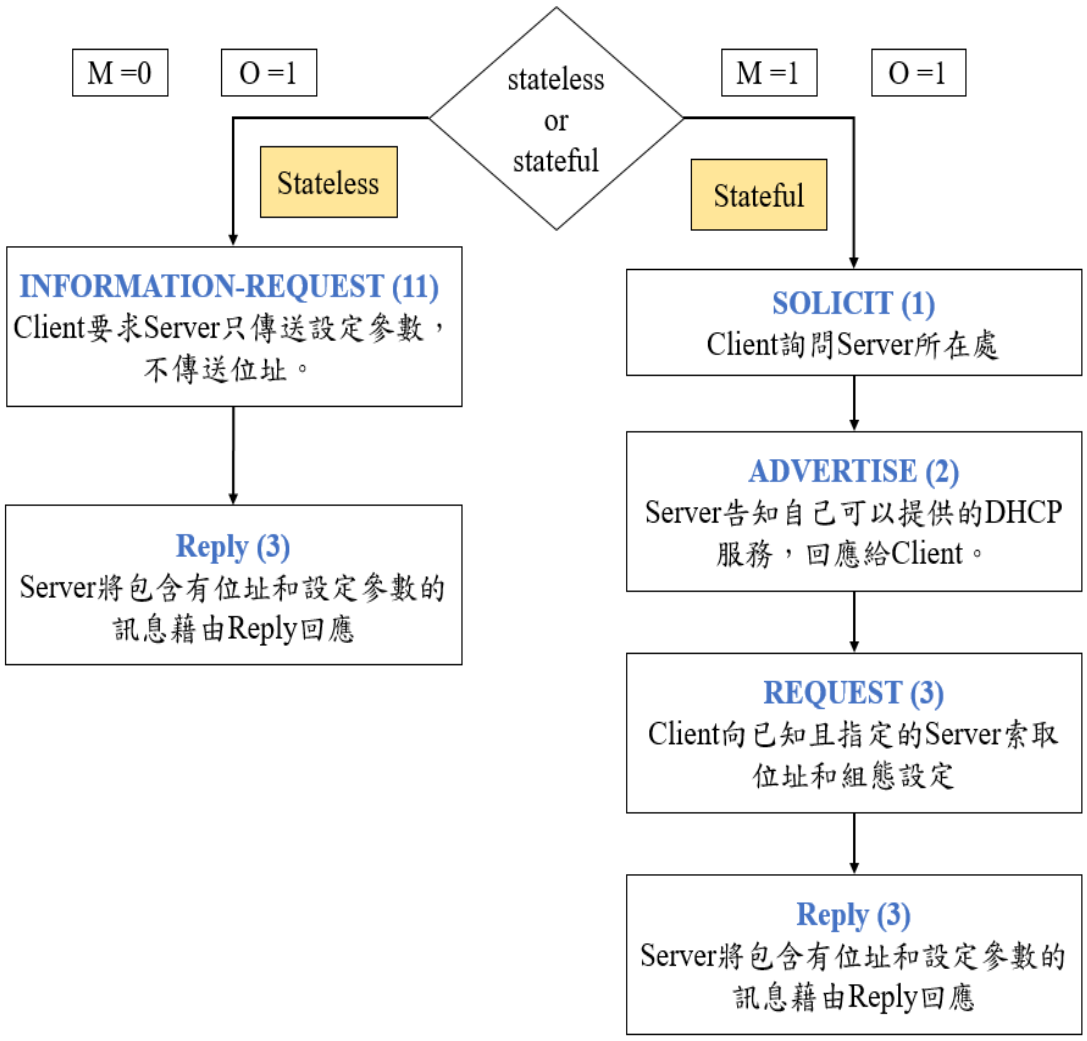


圖 3、Stateless 與 Stateful 位址配置流程

如圖 3 所示，用戶端設備會依據路由廣播訊息內含的 M/O Flag 來執行對應的自動配置模式(stateless 或 statefull)，當用戶完成自動配置程序後，會利用 ND 來執行重複位址偵測以驗證該自動配置位址的唯一性，以完成用戶端設備位址自動配置的程序。

(二) IPv6 位址配置模式

自動定址機制主要是用來簡化使用者連網參數的設定，在實務上依據配發方式的差異，可區分成底下四種模式，如圖 4 所示，以下主要將針對這四種模式進行說明與探討。圖 5 是 IPv4/IPv6 位址配發相關的 IETF RFC 參考標準[3]。除了位址配置相關的 RFC 外，尚有點對點通訊協定(Point-to-Point Protocol, PPP)、Dual Stack 環境的核心協定以及安全性相關的標準[4]~[10].

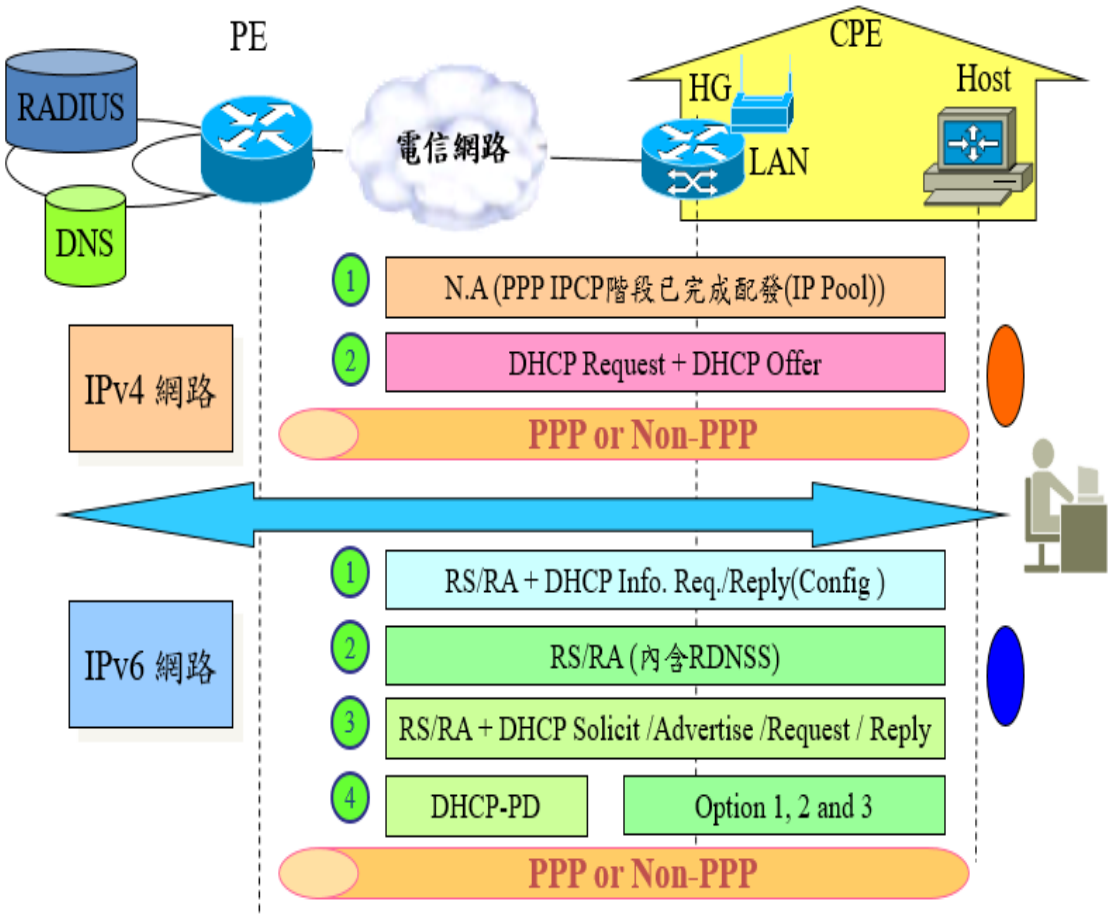


圖 4、IPv4/IPv6 DS 網路位址配發方式

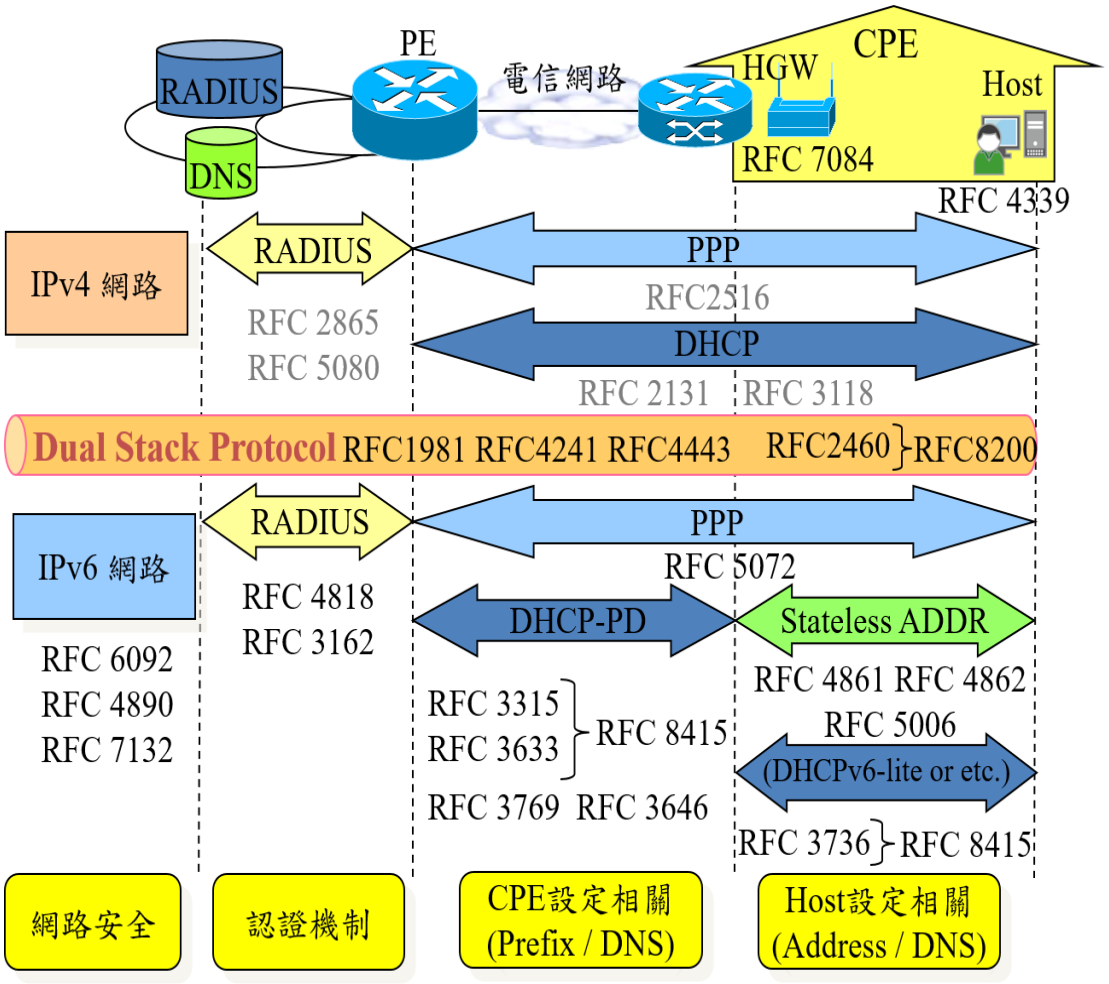


圖 5、IPv4/IPv6 固網寬頻相關 RFC 參考標準

1. 模式一 RS/RA + DHCPv6 (Stateless)

模式一採用 RS/RA 與 DHCPv6 stateless 混用的方式，又稱為無狀態自動設定(Stateless Address Auto-configuration, SLAAC)模式，IPv6 網路設備可以利用自動定址的技術得到 IPv6 位址，網域名稱服務(Domain Name Service, DNS)伺服器參數則透過 DHCPv6 stateless 方式配置，如圖 6 所示：

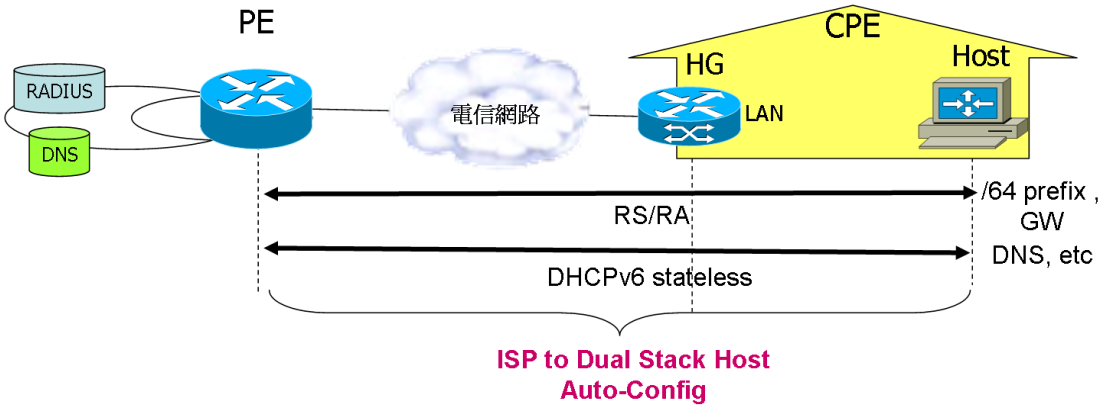


圖 6、模式一 RS/RA + DHCPv6 (Stateless)

IPv6 中的無狀態自動設定主要是依據 RFC 4862[11]的標準，利用鄰居發現協定(Neighbor Discovery Protocol, ND)來達成。在模式一無狀態自動配置過程中，用戶端設備首先啟動 IPv6 協定，透過 IEEE 所訂的 EUI-64 編碼方式，產生一個 Link-local IPv6 位址。接著用戶端設備會開始利用 ND 機制來取得全域的 IP 位址[12]。為了取得 IP 位址的網路前置碼(Network Prefix)，需向該網域之路由設備取得網路前置碼相關資訊，而此資訊包裝在路由器定時發出之路由廣播 Router Advertisement (RA)中，RA 除了定時發送外，在收到其他主機設備的 Router Solicitation (RS)後也會發出相應的 RA 封包。當 IPv6 用戶端設備接收到 RA 的時候，首先會判斷 RA 的格式是否正確，接著檢查封包內容是否有 Prefix Option；Prefix Option 內部 A Flag 參數，若值設定為 1，則代表路由器允許 IPv6 設備啟動位址自動配置程序，取出包含前 64 位元的 Prefix，加上自己的 Interface ID，就可以自動配置 IPv6 位址，與 Internet

中的其它主機設備進行網路層的通訊。而模式一除了自動配置 IPv6 位址外，為使用戶端設備能連結網路上的應用服務伺服器，其亦需配置 DNS 伺服器參數才行，這部份則是依據 RFC 3736[13]的規範(已由 RFC 8415 更新)，用戶端設備必須靠 RA 封包 Prefix Option 內部 O Flag 參數來觸發 DHCPv6 Stateless 的動作，然後完成整個用戶端設備自動配置的程序。

2. 模式二 RS/RA (RDNSS)

模式二採用 RA Option 的方式，依據 RFC 5006[14] 所提出的 IPv6 RDNSS (Router Advertisement Option for DNS Configuration)自動配置方式，如圖 7 所示。主要是新定義了一個包含 DNS 主機位址參數的路由廣播選項 RDNSS (Router Advertisement Option for DNS Configuration)，當用戶端設備透過 ND 機制接收到 RA 後，會檢視 RA 訊息中的 Prefix 選項與 RDNSS 選項，即可自動取得 IPv6 位址、預設閘道與 DNS 主機位址等參數，連結到網際網路。

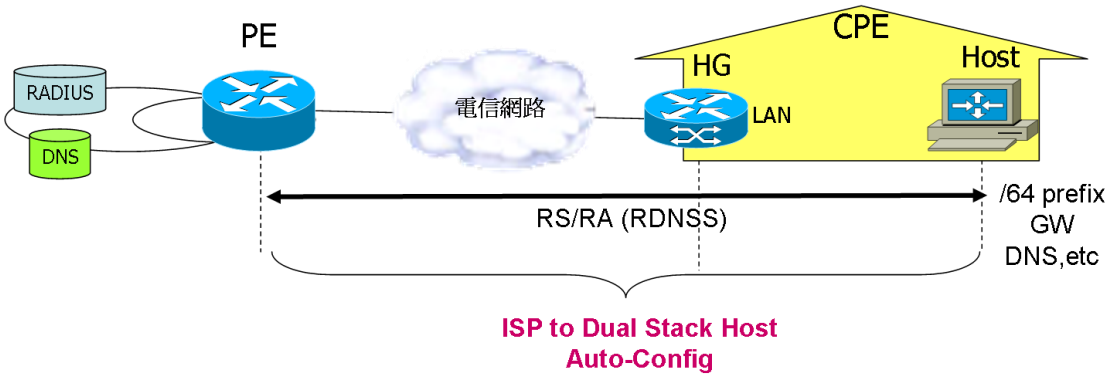


圖 7、模式二 RS/RA (RDNSS Option)

3. 模式三 DHCPv6 (Stateful)

模式三採用 RS/RA+DHCPv6 Stateful 的方式，又稱為全狀態自動設定(Stateful Auto-configuration)模式，路由廣播 RA 除了用來配置 IPv6 網路主機的預設閘道位址外，也用來觸發用戶端設備 DHCPv6 的動作，本模式使用現有的 ND 協定和 DHCPv6 交換機制，使 IPv6 網路設備可以利用 DHCPv6 自動定址的技術同時得到 IPv6 位址與 DNS 參數，如圖 8 所示：

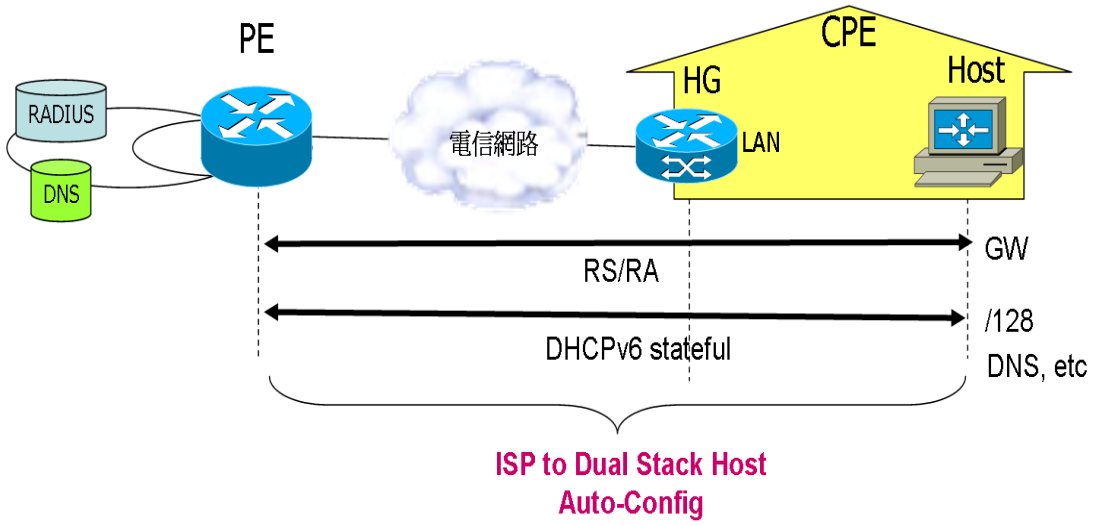


圖 8、模式三 RS /RA + DHCPv6 Stateful

RFC 3315[15](已由 RFC 8415 更新)中提出 RS/RA + DHCPv6 Stateful 自動設定的方式。在模式三全狀態自動配置過程中，對於用戶端設備來說，路由廣播 RA 中的 M Flag 會決定用戶端採用自動配置的模式，當 IPv6 主機接收到 RA 封包，如果 M Flag 為 1，則無需確認 O 位元是否設定，IPv6 主機就會自動啟動 DHCPv6 Client 的動作，

主動的向網路上的 DHCPv6 伺服器索取 IPv6 位址與 DNS 配置參數[16]，若該網路上的 DHCPv6 伺服器運作正常的話就可以直接自動配置用戶主機，讓 IPv6 的主機設備具備連結網路的能力。

4. 模式四 DHCPv6-PD

與上述三種配置方式不同，模式四的自動配置方式主要是針對用戶端的 HG 裝置為主，並非直接配發給用戶主機本身，結合 DHCPv6 Prefix delegation 與模式一或模式二的自動配置技術，來達到 IPv6 網路位址自動配置目的，如圖 9 所示。

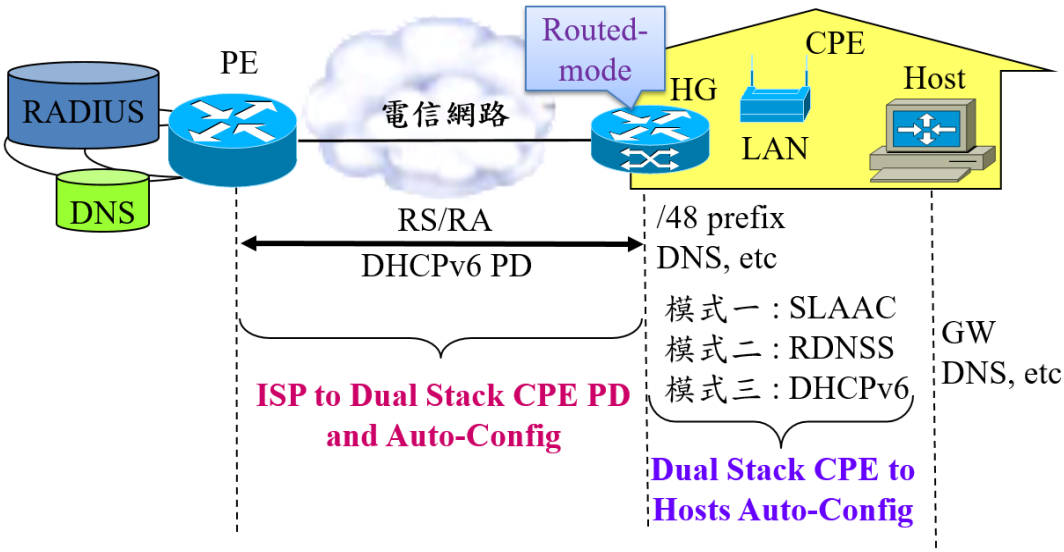


圖 9、模式四 RS/RA + DHCPv6-PD

RFC 3633[17](已由 RFC 8415 更新)中提出 DHCPv6 Prefix Delegation 自動設定的方式。這個模式主要是透過 Home gateway (HG)裝置進行位址轉發的自動配置模式，HG 裝

置本身需提供 WAN 與 LAN 介面，支持 IPv6 的 HG 裝置可以從服務供應商 ISP 獲得/48 或/64 的 Prefix 資訊，如果 HG 本身可以提供多個 LAN 的連接介面的話，則 HG 可以用 Subnet 的方式為每個納管的 LAN 介面配置/64 的 Prefix 資訊，而與該 LAN 介面相連的用戶端設備就可以利用 HG 裝置所配發的/64 進行自動配置，而這部分的配置方式可採用模式一或模式二皆可[18]。

三、工作項目

本計畫主要是透過整理寬頻分享器 IPv6 互通測項以提供協助寬頻分享器製造業者開發 IPv6 寬頻分享器，並建置 IASP 實測平台以了解國內 IPv6 寬頻分享器開發及實際連線使用情況。工作項目說明如下：

(一) 研究整理 IPv6 寬頻分享器製造商開發規範

主要參考以下 RFC 標準，並整理適合台灣固網環境連線中華電信 IPv6 PPPoE 及有線電視 Cable 業者之 IPv6 連線功能項目，並整理歸類哪些功能項目為必須，哪些功能項目為選項。

IPv6 核心及通訊功能：

- RFC 7084 Basic Requirements for IPv6 Customer Edge Routers
- RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 3646 DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 3736 Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6

- RFC 3633 IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6
- RFC 8415 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 2460 Internet Protocol, Version 6 (IPv6) Specification
- RFC 8200 Internet Protocol, Version 6 (IPv6) Specification
- RFC 4861 Neighbor Discovery for IP version 6 (IPv6)
- RFC 4862 IPv6 Stateless Address Autoconfiguration
- RFC 1981 Path MTU Discovery for IP version 6
- RFC 4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification

IPv6 接取撥接功能：

- RFC 5072 IP Version 6 over PPP

IPv6 安全防護功能：

- RFC 4890 Recommendations for Filtering ICMPv6 Messages in Firewalls
- RFC 6092 Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service
- RFC 7123 Security Implications of IPv6 on IPv4 Networks

(二) 研究整理 IPv6 寬頻分享器製造商測試規範

- 以 IPv6 Ready Logo 符合性測試以及互連性測試項目為參考依據，提出 IPv6 寬頻分享器製造商開發規範。
- 於 5 月前與友訊、華碩等至少兩家製造商訪談並確認以上測試項目符合製作商測試項目需求。
- 與國內設備廠商之訪談，請 TWNIC 協助提供聯繫管道。

(三) 建置 IPv6 IASP 實測平台與實機測試

- 建置具 IPv6 PPPoE 及 IPv6 Cable Modem 之 IASP 連線實測平台，並於實測平台上測試製造日期為 2018 年（含）之後之 IPv6 寬頻分享器至少 10 款，需包含友訊、華碩、TP-Link 以及 TOTOLINK 等至少四家寬頻分享器製造商，每家至少二款，並整理測試報告。
- 測試標的之寬頻分享器以該廠牌國內通路販售之設備型號為主，如可支援 IPv6 功能之型號未達二款，則以該廠牌市售現有之設備型號為主。

IPv6 PPPoE 寬頻分享器測試項目以及連接 Cable Modem 之 IPv6 寬頻分享器測試項目如下表所示。

表 2、IPv6 PPPoE 寬頻分享器測試項目

測試項目	測試方法
1 驗證分享器 PPPoE 撥接是否正常?	連結至分享器 Web 介面，確認 PPPoE 已連線
2 驗證分享器 IPv6、IPv6 PD、DNSv6 取得是否正常?	連結至分享器 Web 介面，確認取得 IPv6、IPv6 PD、DNSv6
3 驗證用戶 IPv6、DNSv6 取得是否正常?	使用 ipconfig 指令，確認取得用戶 IPv6、DNSv6
4 驗證用戶至 HiNet 路由是否正常?	使用 Ping 與 trace route 指令確認用戶路由正常
5 驗證用戶 IPv6 上網是否正常?	連結至 IPv6 測試網頁，確認 IPv6 上網正常 網址：http://test-ipv6.com/ 網址：http://ipv6-test.com/
6 驗證用戶熱門網頁開啟是否正常?	連結至 Google、Youtube、HiNet、Microsoft、Yahoo 等網站，確認開

	啟正常
7 驗證用戶上網速率是否正常?	使用 Dr. Speed 確認上下行速率正常
8 驗證分享器重撥，用戶 IPv6 更新是否正常?	用戶終端取得 IPv6 後，分享器重新撥 PPPoE，驗證用戶終端是否正常更新 IPv6
9 驗證用戶使用 IPv6 之 MTU 是否正常?	使用 netsh 指令確認用戶電腦的網路介面(區域連線)MTU 是否為 1492
10 驗證用戶連接 Wi-Fi 上網 IPv6、DNSv6 是否正常?	用戶終端使用 Wi-Fi 連接分享器，確認用戶取得之 IPv6、DNSv6 與上網是否正常
11 驗證用戶連接 Wi-Fi IPv6 上網是否正常?	連結至 IPv6 測試網頁，確認 IPv6 上網正常 網址：http://test-ipv6.com/ 網址：http://ipv6-test.com/
12 IPv6 PPPoE (或是 PPPoEv6)是否隨著 IPv4 PPPoE 啟用而自動啟用?	測試 IPv6 PPPoE (或是 PPPoEv6)是否隨著 IPv4 PPPoE 啟用而自動啟用，且正常連線
13 IPv6 PPPoE (或是 PPPoEv6)連線之 PPPoE Session 是「Share with IPv4」或是「Create a new Session」?	測試 IPv6 PPPoE (或是 PPPoEv6)連線之 PPPoE Session 是「Share with IPv4」或是「Create a new Session」
14 IPv6 寬頻分享器 IPv6 ACL 功能是否正常?	測試寬頻分享器 IPv6 ACL 功能是否能限制用戶終端 IPv6 連線

表 3、連接 Cable Modem 之 IPv6 寬頻分享器測試項目

測試項目	測試方法
1 驗證分享器連接 Cable Modem 是否正常?	連結至分享器 Web 介面，確認 IPv6 Cable Modem 已連線
2 驗證分享器 IPv6、IPv6 PD、DNSv6 取得是否正常?	連結至分享器 Web 介面，確認取得 IPv6、IPv6 PD、DNSv6
3 驗證用戶 IPv6、DNSv6 取得是否正常?	使用 ipconfig 指令，確認取得用戶 IPv6、DNSv6
4 驗證用戶至 Cable 業者路由是否	使用 Ping 與 trace route 指令確認

正常?	用戶路由正常
5 驗證用戶 IPv6 上網是否正常?	連結至 IPv6 測試網頁，確認 IPv6 上網正常 網址：http://test-ipv6.com/ 網址：http://ipv6-test.com/
6 驗證用戶熱門網頁開啟是否正常?	連結至 Google、Youtube、HiNet、Microsoft、Yahoo 等網站，確認開啟正常
7 驗證用戶上網速率是否正常?	使用 Dr. Speed 確認上下行速率正常
8 驗證分享器重撥 Cable Modem，用戶 IPv6 更新是否正常?	用戶終端取得 IPv6 後，分享器重新連接 Cable Modem，驗證用戶終端是否正常更新 IPv6
9 驗證用戶使用 IPv6 之 MTU 是否正常?	使用 netsh 指令確認用戶電腦的網路介面(區域連線)MTU 是否為 1492
10 驗證用戶連接 Wi-Fi 上網 IPv6、DNSv6 是否正常?	用戶終端使用 Wi-Fi 連接分享器，確認用戶取得之 IPv6、DNSv6 與上網是否正常
11 驗證用戶連接 Wi-Fi IPv6 上網是否正常?	連結至 IPv6 測試網頁，確認 IPv6 上網正常 網址：http://test-ipv6.com/ 網址：http://ipv6-test.com/
12 IPv6 連線功能是否隨著 IPv4 啟用而自動啟用?	測試 IPv6 連線功能是否隨著 IPv4 啟用而自動啟用，且正常連線
13 IPv6 寬頻分享器 IPv6 ACL 功能是否正常?	測試寬頻分享器 IPv6 ACL 功能是否能限制用戶終端 IPv6 連線

(四) 研擬政府採購共同供應契約設備參考規範

提出主機、伺服器、路由器以及網路保護裝置之共同供應契約之建議規範書以供參考。

四、預期成果

本計畫主要針對國內寬頻分享器的 IPv6 開發以及測試規範進行研究，並針對市售主要廠牌型號進行 IASP 實網 IPv6 功能的驗證，本計畫之執行將提出適合台灣固網 IPv6 環境之開發、測試以及共同供應契約參考規範,可提供台灣 ISP 固網以及網通業者開發與測試寬頻分享器 IPv6 功能之參考，進而提升我國相關產業之競爭優勢。本計畫預期成果或效益如下：

(一) 完成 IPv6 寬頻分享器製造商開發規範，可提供國內寬頻分享器製造商研發與設計 IPv6 產品之參考。

(二) 完成 IPv6 寬頻分享器製造商測試規範，可作為寬頻分享器製造商測試產品 IPv6 功能之參考。

(三) 完成 IPv6 IASP 實測平台建立並完成市售 IPv6 寬頻分享器實機測試，可作為固網 ISP 以及 Cable 業者驗證產品 IPv6 功能之測試環境。

(四) 完成政府採購共同供應契約設備參考規範，作為採購規範參考之依據。

五、研究方法

本計畫之執行架構如圖 10 所示,主要可分為技術報告以及 IASP 實測平台的建立。在技術報告方面,本計畫以 IETF RFC 標準以及 IPv6 Forum 的符合性與互通性測試規範作為主要的參考依據，進行 IPv6 寬頻分享器相關開發與測試的技術規範研究。IETF 會議為全世界 Internet 通訊協定的標準會議，而全球 IPv6 產業聯盟(IPv6 Forum)於

2003 年成立 IPv6 Ready Logo 委員會[21]，則是依據 IETF IPv6 標準規範，制訂全球性 IPv6 Ready Logo 認證標章，讓產業界研發之 IPv6 產品有遵循的測試標準。

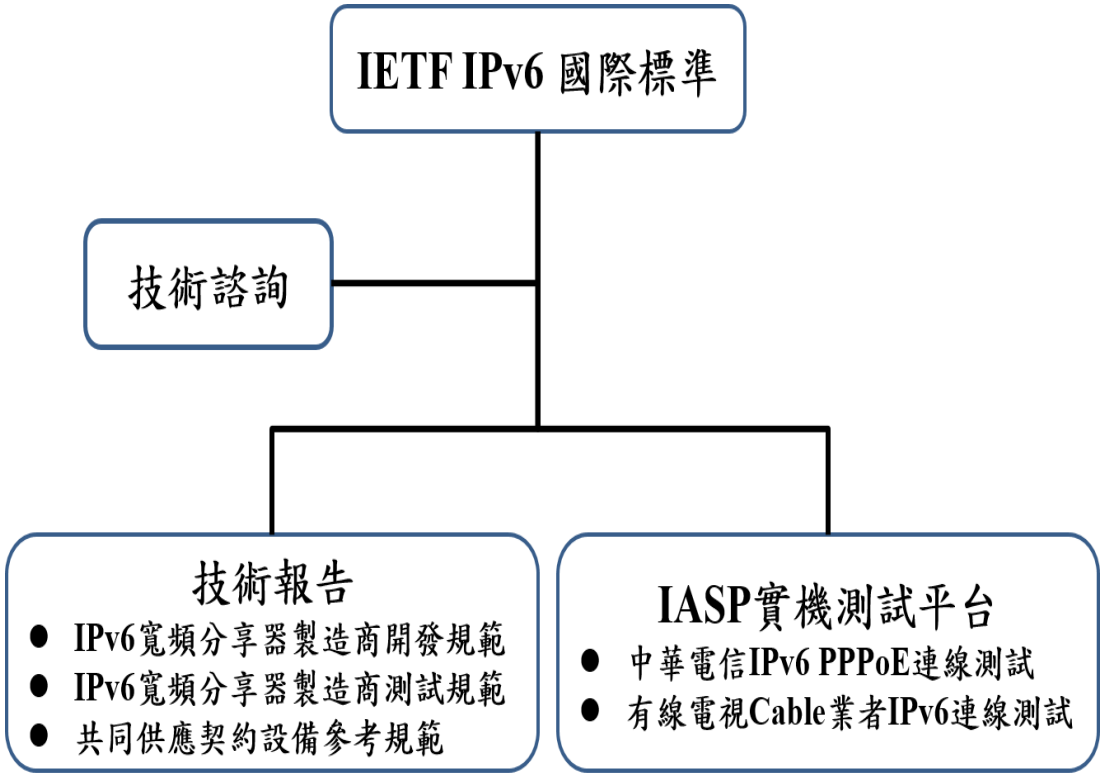


圖 10、計畫執行架構

在 IASP 實測平台部分，本計畫 IASP 實際測試平台架構將包含中華電信 HiNet 光世代 IPv6 PPPoE 及有線電視 Cable 業者 IPv6 連線測試環境。各連線測試環境內容說明如後。

六、施行方式與進行步驟

(一) 中華電信 HiNet 光世代 IPv6 PPPoE 連網測試

HiNet 光世代非固定制雙協定(Dual Stack, IPv4/IPv6)上網服務之用戶，用戶端網路可使用連網終端設備或是寬頻分享器設備，利用 PPPoE 方式連接 HiNet 寬頻網路接取公眾 Internet 網路。用戶連網架構如圖 11 所示。

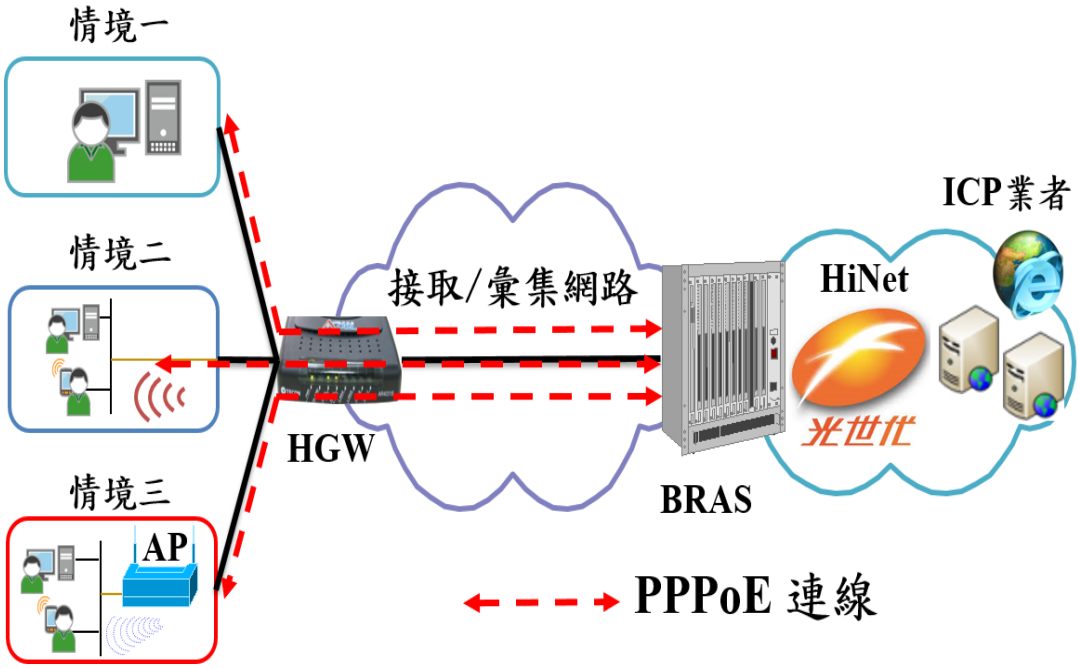


圖 11、HiNet 光世代非固定制用戶 IPv6 連線架構

非固定制用戶可透過建立 PPPoE 方式自動取得連網參數，目前該公司所提供之光世代非固定制雙協定上網服務可同時支援三種 PPPoE 上網情境：

1. 情境一：用戶連網終端設備直接建立 PPPoE 連線連接至網際網路。
2. 情境二：用戶連網終端設備透過局供 Home Gateway (HGW)的 PPPoE 連線間接連接網際網路。

3. 情境三：用戶連網終端設備透過自備寬頻分享器的 PPPoE 連線間接連接網際網路。

本計畫之測試規劃主要是針對情境三，用戶透過自備寬頻分享器配置用戶連網參數，除需搭配 CPE 裝置本身可支援的 IPv6 功能外，用戶連網終端的作業系統也必須支援 IPv6。

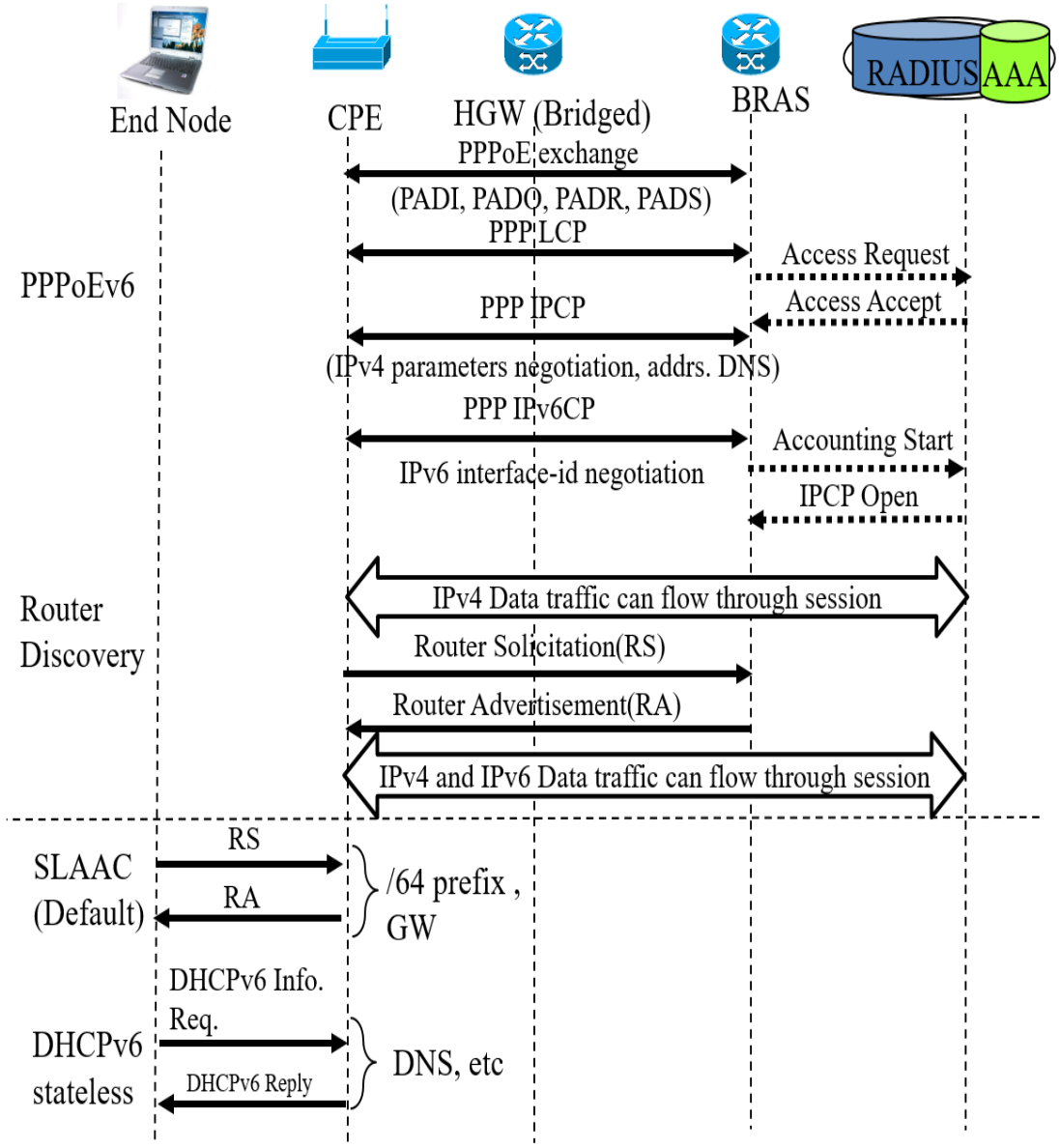


圖 12、HiNet 光世代 IPv6 寬頻分享器連線範例

圖 12 為 IPv6 寬頻分享器 PPPoE 連線範例。驗證測試步驟如下:

1. CPE WAN 端首先經由 PPPoE 取得 Interface ID，並根據收到的 RA 可得知預設閘道並自動產生 WAN 介面的 IPv6 位址；
2. CPE 於 WAN 介面啟動 DHCPv6 client 向局端 DHCPv6 伺服器要求 DHCPv6 PD、DNS 伺服器位址等資訊；
3. CPE 於取得 DHCPv6 PD 後自動產生 LAN 介面的 IPv6 位址，再將此 LAN 位址的 prefix 放入 RA 告知 LAN 底下的終端設備。

LAN 底下的終端設備可根據 CPE LAN 發送的 RA 產生預設閘道與 IPv6 位址。DNS 伺服器位址與 Domain Name Search List 可透過 RA 或經由 Stateless DHCPv6 方式得知。

(二) 有線電視 Cable 業者 IPv6 連網測試

CM(Cable Modem)主要是以現在有線電視的光纖同軸混合線路 HFC（Hybrid Fiber/Coax）來當作資料傳送的線路。用戶端網路可使用連網終端設備或是自備的寬頻分享器設備，利用 IPv6 over Etherent 方式連接 CMTS(Cable Modem Termination System)寬頻網路接取公眾 Internet 網路。Cable 用戶 IPv6 連網架構如圖 13 所示。

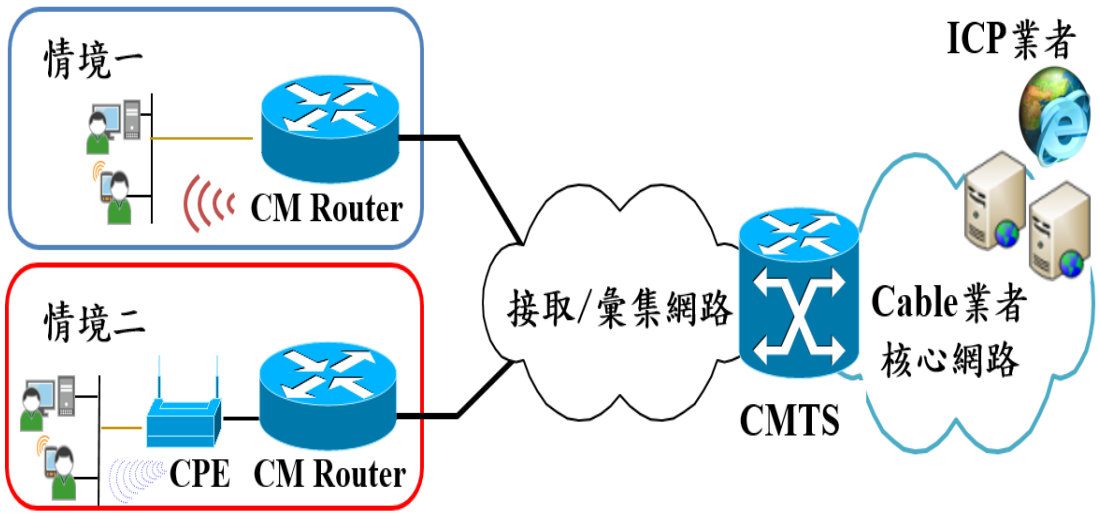


圖 13、Cable 網路 IPv6 連網架構

Cable 用戶終端裝置透過 DHCPv6 的方式自動取得連網參數，目前 Cable 業者所提供之雙協定上網服務可同時支援兩種上網情境：

1. 情境一：用戶連網終端設備透過 Cable Modem 連接至網際網路。
2. 情境二：用戶連網終端設備透過自備寬頻分享器連接連結 Cable Modem 間接連接至網際網路。

本計畫之 IPv6 寬頻分享器實機測試規劃主要是針對情境二，用戶可透過自備寬頻分享器裝置連接 Cable 業者的 IPv4/IPv6 雙協定測試網路。

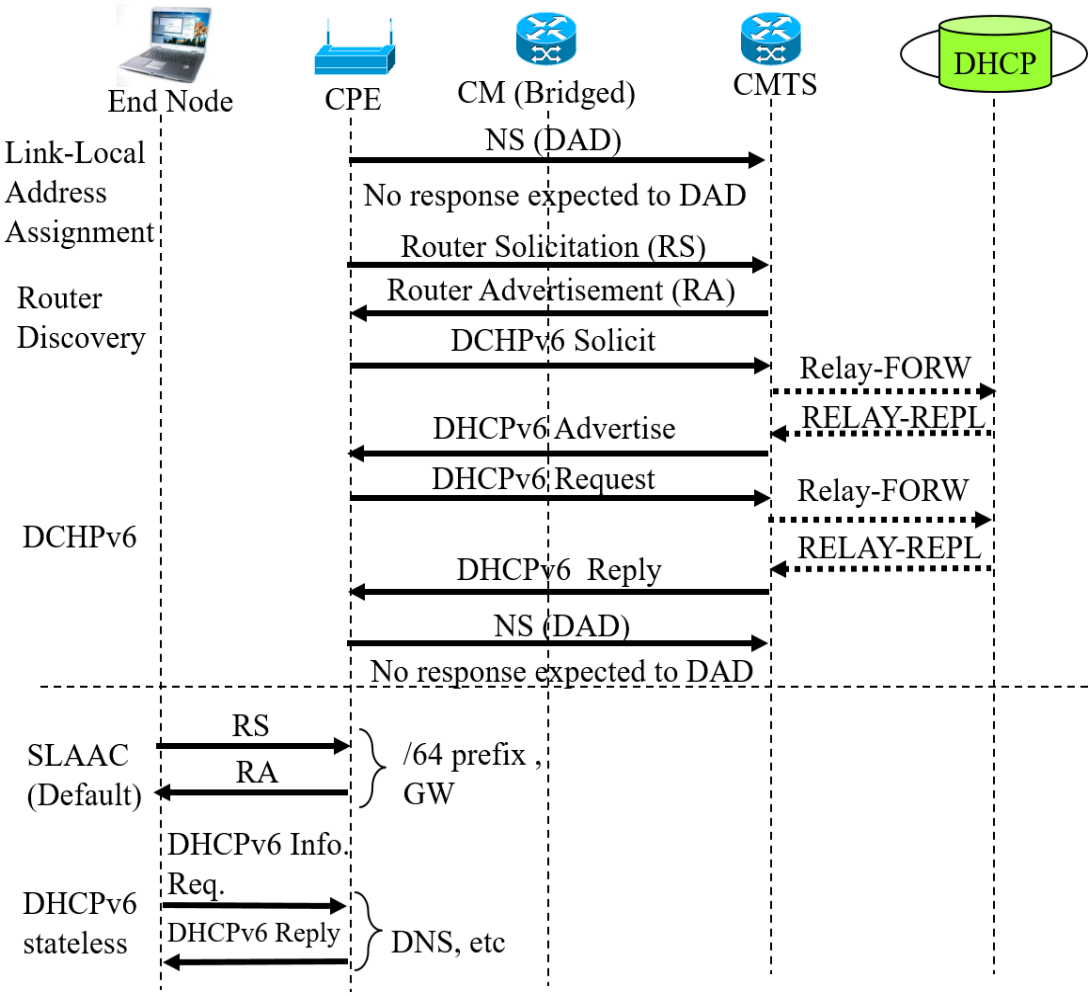


圖 14、Cable 網路 IPv6 寬頻分享器連線範例

圖 14 為 Cable 網路 IPv6 寬頻分享器 DHCPv6 連線範例。驗證測試步驟如下:

1. CPE WAN 端首先進行 Link-local address assignment 啟動 duplicate address detection (DAD)重複位址檢測的過程。
2. 當 CPE 檢測到 RA 會用來設置預設的路由資訊，如指定時間內沒收到 RA，CPE 裝置也可透過 RS 請求向 CMTS 請求路由通告的資訊。
3. LAN 底下的終端設備可透過預設 SLAAC 的機制由 CPE 取得連網的必須參數。

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 4、各項工作執行進度

月次 / 工作項目	1	2	3	4	5	6	7	8	9	10	11	12
1. 研究整理IPv6寬頻分享器製造商開發規範												
2. 研究整理IPv6寬頻分享器製造商測試規範												
期中報告												
3. 建置IPv6 IASP實測平台並使用IPv6寬頻分享器進行實機測試												
4. 研擬政府採購共同供應契約設備參考規範												
期末報告												
預定進度（累積數）				10%	30%	55%	60%	70%	85%	100%		

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 5、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	
IPv6 寬頻分享器製造商開發規範		V		
IPv6 寬頻分享器製造商測試規範		V		
IASP 實測平台建立與實機測試		V		
政府採購共同供應契約規範		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 6、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	研究與整理 IPv6 政府採購共同供應契約參考建議
協同研究人員	賴文彬	研究助理	碩班生	研析 IPv6 寬頻分享器相關 RFC 標準規範，提出製造商開發規範
協同研究人員	邱楷程	研究助理	碩班生	研析 IPv6 Ready Logo 符合性與互連性測試方法，提出製造商測試規範
協同研究人員	吳嘉偉	研究助理	碩班生	規劃 IPv6 IASP 實測平台與建立 IPv6 寬頻分享器 PPPoE 以及 Cable 連線測試報告範本

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，各項經費使用以及至年底的總經費使用情形預估如下表所示：

表 7、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	279,868	49.57%	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	143,000	54,783	38.31%	流入數: 0 流出數: 0
旅運費	19,716	4,218	21.39%	流入數: 0 流出數: 0
行政管理費	72,727	0	0.00%	流入數: 0 流出數: 0
合　計	**800,000**	**338,869**	**42.36%**	

表 8、總經費運用情形預估表

項　目	預算金額	使用金額	使用率	備　註
人事費用	564,557	564,557	100%	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	143,000	143,000	100%	流入數: 0 流出數: 0
旅運費	19,716	19,716	100%	流入數: 0 流出數: 0
行政管理費	72,727	72,727	100%	流入數: 0 流出數: 0
合　計	**800,000**	**800,000**	**100%**	

第二章成果說明

第一節 IPv6 寬頻分享器製造商開發規範

針對 IPv6 寬頻分享器製造商開發規範部分，本研究主要參考下圖之 RFC 相關標準，研析 IPv6 寬頻分享器的開發規範需求，由於各個 RFC 所描述的 IPv6 功能需求規範涵蓋內容廣泛，故本節僅摘要本計畫建議之 IPv6 規範選項，其餘細部的 IPv6 功能規範需求請參閱附件一。

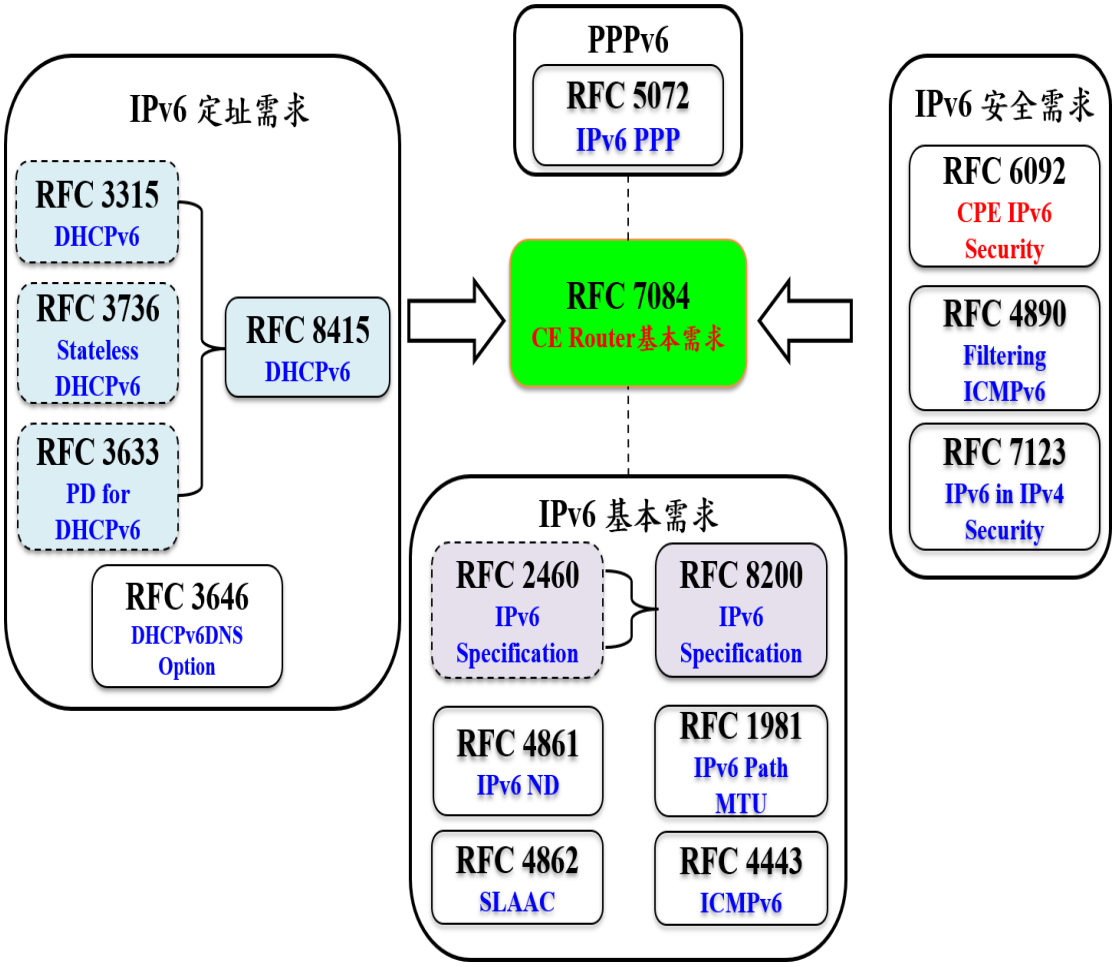


圖 15、寬頻分享開發規範 IPv6 RFC 關聯圖

由於 RFC 7084 是 IPv6 寬頻分享器的基本需求，因此本計畫以 RFC 7084 為主，列出建議之 IPv6 寬頻分享器的必須與選項規範如以下表說明。

表 9、IPv6 寬頻分享器必須規範建議

IPv6 寬頻分享器之 IPv6 基本需求必須規範建議	
RFC 7084 WAN 介面	1. IPv6 CE router 必須實作 ICMPv6 2. IPv6 CE router 必須實作 stateless 或 stateful 位址分配機制 3. IPv6 CE router 必須產生 link-local 位址，並於其網路介面完成 DAD 以及發送 RS 4. IPv6 CE Router 必須支援 DHCPv6 prefix delegation 5. IPv6 CE Router 必須支援 DHCPv6 規範之客戶端行為 6. IPv6 CE Router 必須支援 Ethernet 以及 PPP encapsulation 7. CE Router 必須支援 SOL_MAX_RT Option 8. IPv6 CE Router 必須支援 DHCPv6 options： ➢ Identity Association for Non-temporary Address (IA_NA) ➢ Reconfigure Accept ➢ DNS_SERVERS 9. 如 WAN 端連線中斷，必須透過 RA 機制通告 LAN 端用戶 10. 如收到的 RA 訊息中的 M or O flags 設置為 1 時，IPv6 CE Router 必須啟動 DHCPv6 prefix delegation 11. 如 IPv6 CE Router 沒有從 SLAAC 或 DHCPv6 獲取 Global IPv6 位址，則必須從其 delegated prefix 創建一個 Global IPv6 位址 12. IPv6 CE Router DHCPv6 同時請求 IA_NA 和 IA_PD 選項，其必須接受 DHCPv6 Advertise/Reply 訊息中的 IA_PD 選項，即使該訊息不包含任何位址
RFC 7084 LAN 介面	1. IPv6 CE Router 必須作為 site border router ，並可依 IPv6 來源或目的位址過濾 IPv6 封包 2. IPv6 CE Router 必須支援 Neighbor Discovery for IPv6

	3. IPv6 CE Router 必須為其每個 LAN Interface 分配一個單獨的/ 64 (由其被委託的 delegated prefix(es)) 4. IPv6 CE Router 必須透過 Route Information Option 通告其為 delegated prefix 配置的 Router 5. IPv6 CE Router 的每個 LAN Interface 都必須發送 RA 6. IPv6 CE Router 必須支援 IPv6 位址分配的 DHCPv6 server 或 stateless DHCPv6 server 功能 7. IPv6 CE Router 必須支援在 DHCPv6 DNS_SERVERS 以及和 DOMAIN_LIST options 中提供 DNS 資訊 8. IPv6 CE Router 必須支援可在 RA 中提供 DNS 資訊（Recursive DNS Server RDNSS 和 DNS Search List options） 9. 如 delegated prefix 發生變化，則 IPv6 CE Router 必須立即通告舊的 prefix 其 Preferred Lifetime 為零
RFC 8200 (取代 RFC 2460)	1. Extension 標頭必須依序處理 2. 所有 node 必須檢驗和處理 Hop-by-Hop Options header 3. 如果 Segments Left 為零，則節點必須忽略 Routing 標頭並繼續處理封包中的下一個標頭，其類型由 Routing 標頭中的 Next Header 欄位標識 4. 如果 Segments Left 不為零，則節點必須丟棄該封包並向封包的來源地址發送 ICMP Parameter Problem, Code 0 訊息 5. 如在接收到封包的第一個到達分段的 60 秒內收到不足的分段，則必須放棄該封包的重組，並且必須丟棄已經為該封包接收的所有分段 6. 必須適當選擇分段的長度，使得分段封包適合到達封包目的地的路徑上的 MTU 7. 在任何無法傳輸 1280 字節封包的鏈路上，必須在低於 IPv6 網路層提供特定於鏈路的分段和重組 8. 具有可配置 MTU 的鏈路（例如，PPP 鏈路[RFC-1661]）必須配置為具有至少 1280 個八位字節的 MTU 9. 節點必須能夠接受分段的封包，在重組後，該封包的大小為 1500 個八位字節
RFC 1981	1. 當節點收到 Packet Too Big 消息時，它必須根據消息中 MTU 欄位的值減少其對相關路徑的 PMTU 的估計 2. 節點不能將路徑 MTU 的估計值降低到 IPv6 最小鏈結 MTU 以下

RFC 4443	1. IPv6 網路節點必須支援 ICMPv6 2. 如收到未知類型的 ICMPv6 訊息，則必須以靜默方式丟棄
RFC 4861	1. RA/NA 來源 address 必須是傳送該訊息 interface 上的 link-local address 2. MTU option 用於 RA，且其他 ND 訊息必須將其忽略 3. Host 必須丟棄任何收到的 RS 訊息，且任何時候都不能傳送 RA 4. Router 必須丟棄任何不完全符合以下檢驗的的 RS 訊息: ➢ IP Hop Limit 欄位為 255，意即封包沒辦法讓 router 傳送 ➢ ICMP Checksum 是合法的 ➢ ICMP Code 是 0 ➢ ICMP length 是 8，或更多 octet ➢ 所有 option 都有大於 0 的 length ➢ 若來源 IP 位址為 unspecified address，則訊息中沒有 source link-layer option 5. RS/RA/NS/NA Reserved 欄位和任何無法辨認的 option，都必須被忽略 6. Router 必須丟棄任何沒有滿足以下所有檢驗的 RA 訊息: ➢ 來源 IP address 是 link-local address。 ➢ IP Hop Limit 欄位為 255，意即封包沒辦法讓 router 傳送 ➢ ICMP Checksum 是合法的 ➢ ICMP Code 是 0 ➢ ICMP length 是 16，或更多 octet ➢ 所有 option 都有大於 0 的 length 7. 一個 node 必須丟棄任何沒有滿足以下全部正當性檢查的 NS： ➢ Hop Limit 欄位的值為 255，也就是說該封包沒辦法透過 router forward ➢ ICMP Checksum 是合法的 ➢ ICMP Code 是 0 ➢ ICMP 長度大於 24 個 octets ➢ 目標 Address 不是 multicast address

	➢ 其中所有 option 的長度都大於 0 ➢ 若來源 IP address 沒有被標註，則目標 IP address 就是一個 solicited-node multicast address ➢ 若來源 IP address 是未被標註的，則訊息中不會有 link-layer address option 8. 一個 node 必須丟棄任何沒有滿足以下全部正當性檢查的 NA： ➢ Hop Limit 欄位的值為 255，也就是說該封包沒辦法透過 router forward ➢ ICMP Checksum 是正當的 ➢ ICMP Code 是 0 ➢ ICMP 長度大於 24 個 octets ➢ 目標 Address 不是 multicast address ➢ 若目標 address 是一個 multicast address，則 Solicited flag 為 0 ➢ 其中所有 option 的長度都大於 0
RFC 4862	1. 在將所有單播位址分配給 Interface 之前，必須對所有單播地址執行重複位址檢測 2. 節點必須以靜默方式丟棄任何未通過[RFC4861]中指定的有效性檢查的 NS 或 NA 3. 無效位址不得用作傳出通信中的來源位址，不得將其識別為接收 Interface 上的目標
IPv6 寬頻分享器之 IPv6 安全需求必須規範建議	
RFC 6092	1. 當封包從內部轉送到外部時，必須刷新 flows 的狀態記錄，並且當封包以反向方向轉送時，可以更新狀態記錄 2. 在預設的情況下，Gateway 必須回應 ICMPv6 Destination Unreachable 錯誤代碼 1 給以下封包（等待至少 6 秒） ➢ unsolicited inbound SYN packet ➢ Destination Unreachable 3. 如果 Gateway 無法確定 TCP flow 或 DCCP 端點是否處於活動狀態，則其可放棄該狀態記錄。在這種情況下： ➢ established flow idle-timeout 的值不得少於兩小時四分鐘

	➢ transitory flow idle- timeout 的值不得少於四分鐘 ➢ idle-timeouts 的值可以由網路管理員配置 4. IPv6 簡化安全功能的 Internet gateways 必須提供一個易於選擇的配置選項 transparent mode(可預先配置) 5. IPv4/IPv6 共存且採用 IPv4/IPv6 協定轉換(Translation)架構，位址轉換設備應提供 IPv4 與 IPv6 轉換日誌紀錄資訊並傳送給日誌伺服器
RFC 4890、RFC 7123	1. 網路管理不允許 IPv6 隧道時，需可阻擋 IPv4 header 中 Type 欄位值為 41 的 IPv4 封包 2. 可過濾 ICMPv6 封包，並制定封包過濾規則 3. 可過濾內含 Extension Header 的 IPv6 封包，並制定封包過濾規則
IPv6 寬頻分享器之 IPv6 定址需求必須規範建議	
RFC 3646	1. DNS Recursive Name Server option 不能出現在以下訊息中：Solicit，Advertise，Request，Renew，Rebind，Information-Request 和 Reply 2. Domain Search List option 不能出現在以下消息中：Solicit，Advertise，Request，Renew，Rebind，Information-Request 和 Reply
RFC 8415 (取代 RFC 3315、3736、3633)	1. 每個 DHCP client 或 DHCP server 都要必須有一個固定且唯一的 DUID 2. Client 配置請求 delegated prefixes 應該要生成至少一個不同的 IA_PD 3. Client 的每個網路 interface 必須至少關聯一個 IA 4. 如 DHCP client 從 server 沒有接收到應該要收到的回應，client 必須重送請求 5. Client 在重送的訊息中必須讓 transaction ID 維持不變 6. Client 或 server 必須丟棄任何收到含有未知訊息形式的 DHCP 訊息 7. Client 必須使用該 interface 上的 link-local address 作為 IP 封包 header 中的 source address 8. Client 必須丟棄任何以下接收到的訊息：: request, confirm, renew, rebind, decline, release, information request, relay-forward, relay-reply 9. Server 必須丟棄以下接收到的訊息 ➢ 任何接收到的訊息: advertise, reply, reconfigure, relay-reply

	➢ 任何目標位址是 unicast address 的 solicit、confirm、rebind 或 Information-request ➢ 沒有包含 client 和 Server Identifier option 的 solicit, confirm, rebind 10. Relay agent 必須丟棄任何以下接收到的訊息，任何接收到的訊息: advertise, reply, reconfigure 11. Servers 必須丟棄任何符合以下任一條件的 request message: ➢ 沒有包含 Server Identifier option ➢ Server Identifier option 中的內容跟 server 的 DUID 不匹配 ➢ 不包含 Client Identifier option 12. Server 必須丟棄任何符合以下任一條件的 renew message: ➢ 不包含 Server Identifier option ➢ Server Identifier option 中的內容和 server 識別碼不匹配 ➢ 不包含 Client Identifier option 13. Servers 必須丟棄符合以下任一條件的 decline message: ➢ 不包含 server 識別選項 ➢ 在 Server Identifier option 中的內容與 server 的識別碼不匹配 ➢ 不包含 Client Identifier option 14. Server 必須丟棄任何符合以下任一條件的 release message: ➢ 不包含 Server Identifier option ➢ Server Identifier option 中的內容和 server 識別碼不匹配 ➢ 不包含 Client Identifier option 15. Servers 必須丟棄任何符合以下條件的 Information-request message: ➢ Server Identifier option 中的 DUID 和 server 的 DUID 不匹配 ➢ 包含 IA 選項 16. Client 必須丟棄任何符合以下任一條件的 advertise message: ➢ 沒有包含 Server Identifier option

	➢ 沒有包含 Client Identifier option ➢ Client 的識別碼選項跟 client 的 DUID 不匹配 ➢ Transaction-id 欄位的值和 client 在 solicit message 所用的值不匹配 17. Clients 必須丟棄任何符合以下任一條件的 reply message: ➢ 不包含 Server Identifier option ➢ “transaction-id”欄位中的值和原來訊息中的值不匹配 18. Clients 必須丟棄任何符合以下任一條件的 Reconfigure message: ➢ 不是以 unicast 傳給 client ➢ 沒有包含 Server Identifier option ➢ 沒有包含 client 的 DUID 在 Client Identifier option 中 ➢ 沒有包含 Reconfigure Message 選項且 msg-type 要是正確的 ➢ 包含 IA 選項和 msg-type 是 INFORMATION-REQUSET ➢ 沒有包含 DHCP 驗證
IPv6 寬頻分享器之 PPPv6 需求必須規範建議	
RFC 5072	1. PPP 連結的本地端需使用協商的介面識別碼來自動配置 PPP 介面的 IPv6 連結本地單播地址

表 10、IPv6 寬頻分享器選項規範建議

IPv6 寬頻分享器選項規範建議	
RFC 7084 WAN 介面	1. IPv6 CE Router 應支援 DNS Search List (DNSSL) 2. IPv6 CE Router 應實作 Network Time Protocol (NTP) 3. IPv6 CE Router 應實作 Information Refresh Time option 相關客戶端行為 4. 如 delegated prefix 太小無法配置其所有 Interface 時，IPv6 CE Router 應該記錄系統管理錯誤 5. 如 IPv6 CE Router 收到的任何封包目的為 CE Router delegated prefix(es)但不屬於 CE Router LAN 端 prefix 包含的子集時，必須丟棄該封包

	6. IPv6 CE Router 應支援 Prefix Exclude option
RFC 7084 LAN 介面	1. IPv6 CE Router 應可產生 ULA prefix 且該 ULA Prefix 的值是可配置的，重新啟動後仍維持此 Prefix 2. A and L flags 應可由用戶自行配置(預設情況皆應設定為 1) 3. RA 通告訊息應將 M flag 設置為 0 並將 O flag 設置為 1 4. IPv6 CE Router 應可於 WAN Interface 上的 DHCPv6 客戶端接收到其配置給 LAN 端的 DHCPv6 options
RFC 7084 其它	1. IPv6 CE Router 應支援 6rd 與 DS-Lite 轉移技術 2. IPv6 CE Router 應支援 RFC6092 針對 CPE 設備訂定之安全能力 3. IPv6 CE Router 應支援 BCP 38 ingress filtering 的規範建議 4. 如 IPv6 CE Router 防火牆配置為可過濾 tunnel 技術封裝之資料，則防火牆應提供過濾來自 tunnel 解封裝封包的功能

第二節 IPv6 寬頻分享器製造商測試規範

針對 IPv6 寬頻分享器製造商開發規範部分，本節提出主要建議測試項目規範以及 IPv6 Ready Logo 測試選項建議，細部的 IPv6 測試規範需求請參閱附件二。附件三為寬頻分享器製造商(友訊、華碩)訪談紀錄。

一、主要建議測試項目規範

(一) IPv4/IPv6 PPPoE 與 IPoE 連線功能測試

測試目的：檢測寬頻分享器預設 PPPoE 與 IPoE 功能是否可支援 IPv6。PPPoE 與 IPoE 連線功能測試說明如下：

1. PPPoE 連線功能測試

   Point-to-Point Protocol (PPP)通常用在兩個網路節點間建立直接的通訊管道。主要是用於利用點對點的 Tunnel 來連接兩台網路設備，也適合用在寬頻網路設備的通訊連接。PPP 模式主要是提供一種資料鏈結層網路認證連線的機制，ISP 端的網路設備 BRAS 必須向 RADIUS 伺服器轉發用戶訊息，由 RADIUS 伺服器進行用戶身份認證，如果認證通過，用戶才可以繼續進行配置 IP 位址的程序。PPPoE 測試架構如圖 16 所示。

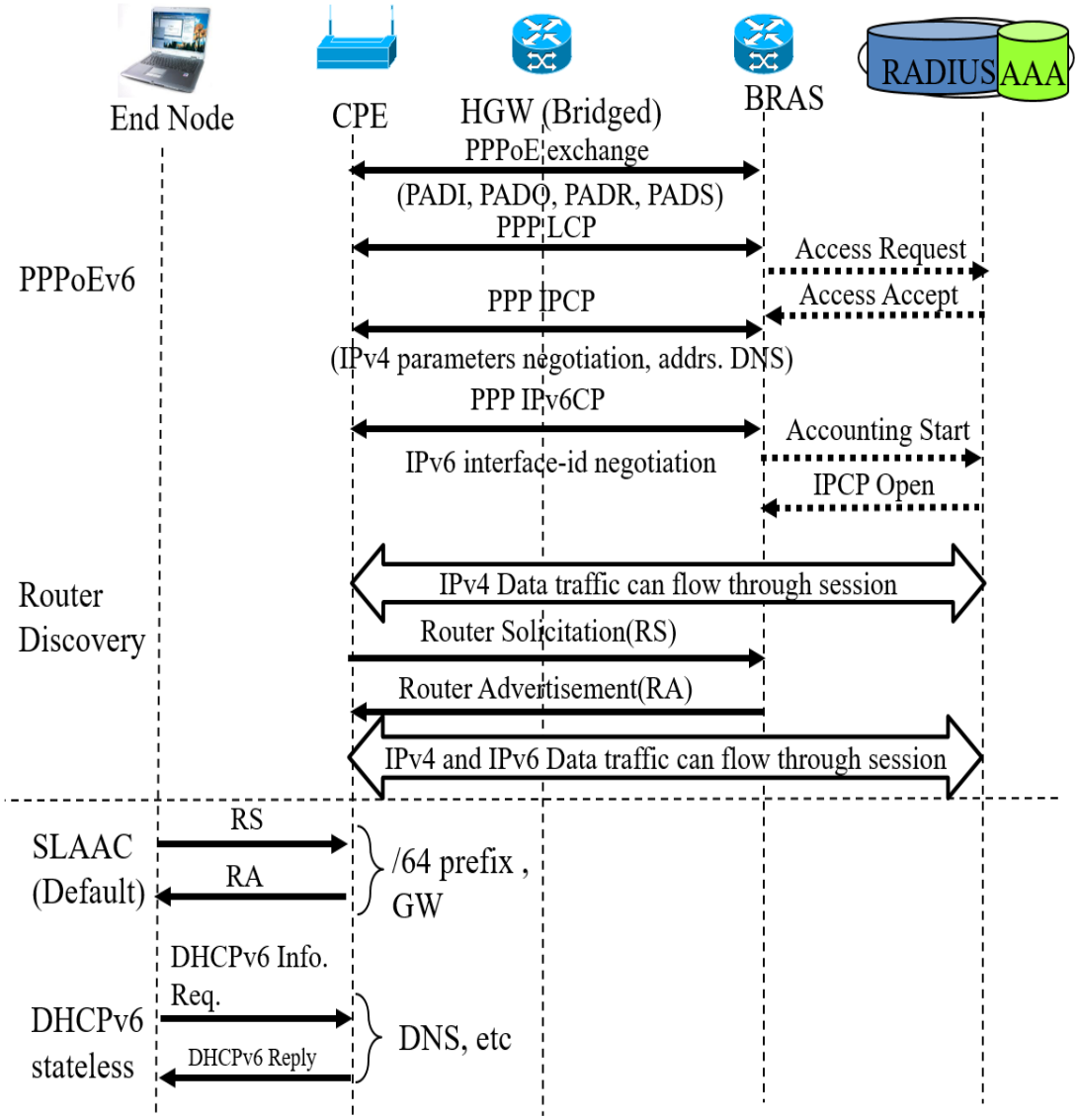


圖 16、IPv6 PPPoE 連線測試架構

PPPoE 測試規範建議流程如下：

表 11、PPPoE 測試規範建議

步驟	測試內容
1	動作：發起 PPPoE exchange 進行 PADI、PADO、PADR 及 PADS 檢驗：是否收到對方的 MAC address 及此對話的 session ID

2	動作：發起 PPP LCP 檢驗：收到每部裝置檢視的資料大小、壓縮及認證
3	動作：發起 PPP IPCP 檢驗：是否順利完成 IPCP 訊息交換
4	動作：發起 PPP IPv6CP 檢驗：是否順利完成 IPv6CP 訊息交換
5	動作：同時以 IPv4 及 IPv6 進行連線測試，檢查是否在同一 PPP session ID 裡 檢驗：是否同一 PPP session ID 的連線同時包含 IPv4 與 IPv6 連線成功收到 RA 封包
6	動作：寬頻分享器向使用者終端裝置配置連網參數 檢驗：用戶終端設備是否能成功連線 IPv4 與 IPv6 網際網路

2. IPoE 連線功能測試

IPoE 通常用在區域網路內，用戶端設備本身無需建立點對點的網路連線，而是由業者端網路設備直接配連網參數給終端裝置方式進行。IPoE 連線測試架構如圖 17 所示。

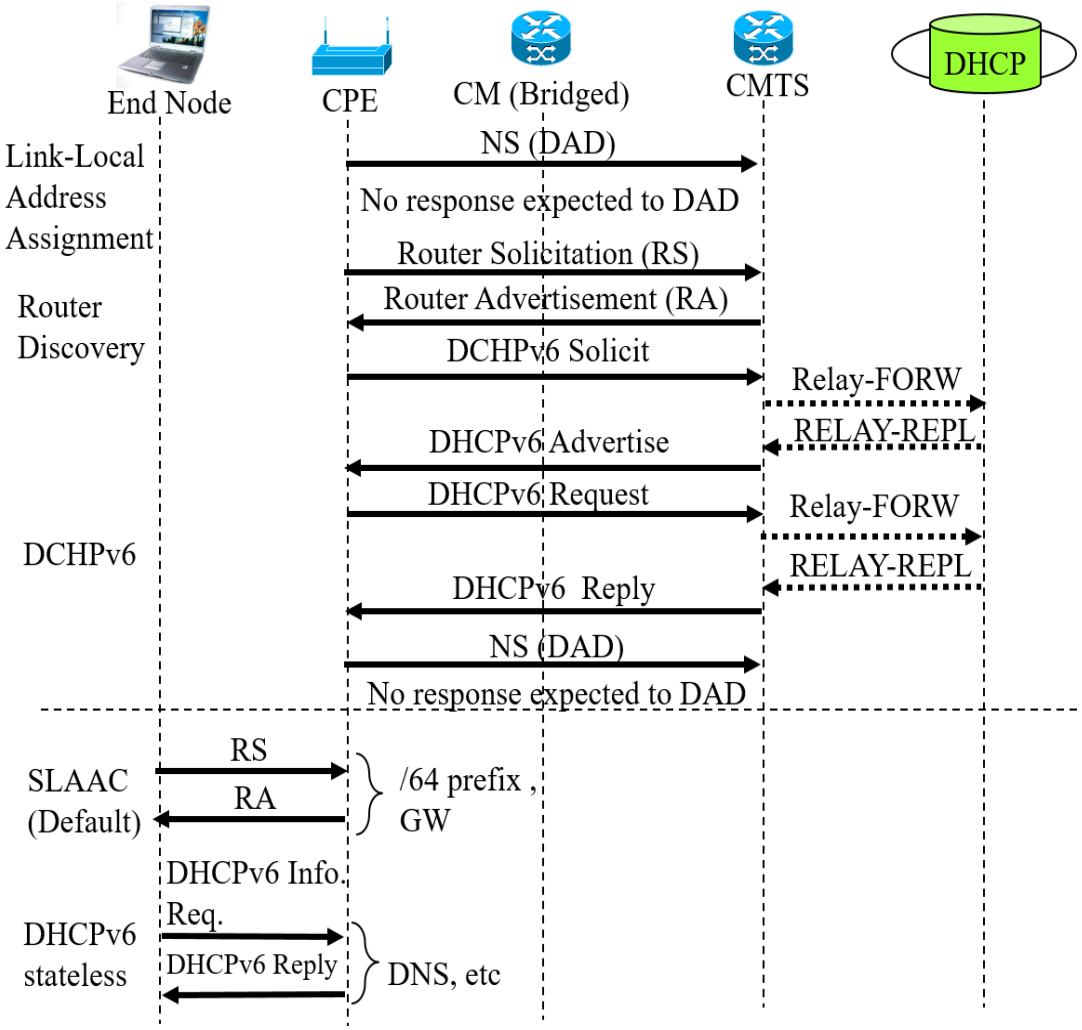


圖 17、IPv6 over Ethernet 連線測試架構

IPoE 測試規範建議流程如下：

表 12、IPoE 測試規範建議

步驟	測試內容
1	動作：CE-Router WAN 端 interface 傳送 Neighbor Solicitation (即進行 DAD) 檢驗：不會收到相對應的 Solicited Neighbor Advertisement
2	動作：CE Router 向 FF02::2 (所有 router 的 multicast address)發送 Router Solicitation

	檢驗:CE Router 收到 M bit 和 O bit 皆為 1 的 Solicited Router Advertisement，內容告知 CE Router 需要透過 DHCP 取得資訊
3	動作：CE Router 向 ff02::1:2 (所有 DHCP server 和 relay agent 的 multicast address) 傳送 DHCP Solicit 訊息 檢驗：CE Router 收到 DHCP Advertisement，並從這個封包中的來源 IP address 得知 DHCP server 的 link-local address
4	動作：CE Router 向在步驟 3 所得知的 DHCP server 的 link-local address 傳送 DHCP Request 訊息 檢驗：CE Router 收到 DHCP Reply 訊息，取得 prefix 和 DNS Server 等資訊
5	動作：使用者終端設備向 CE Router 發送 Router Solicitation (即進行 SLAAC) 檢驗：CE Router 向終端設備回傳 Router Advertisement，告知終端設備 prefix 和 gateway 位址資訊
6	動作：使用者終端設備向 CE Router 發送 DHCP Request 檢驗：CE Router 向終端設備發送 DHCP Reply，讓終端設備取得 DNS Server 等資訊
7	動作：寬頻分享器向使用者終端裝置配置連網參數 檢驗：用戶終端設備是否能成功連線 IPv4 與 IPv6 網際網路

(二) 寬頻分享器 IPv6 位址配置模式測試

測試目的：檢測寬頻分享器是否預設支援 SLAAC、RDNSS 以及 DHCPv6 三種 IPv6 位址配置功能。三種 IPv6 位址配置模式之說明請參閱第一章第一節第二小節之 IPv6 位址配置模式。

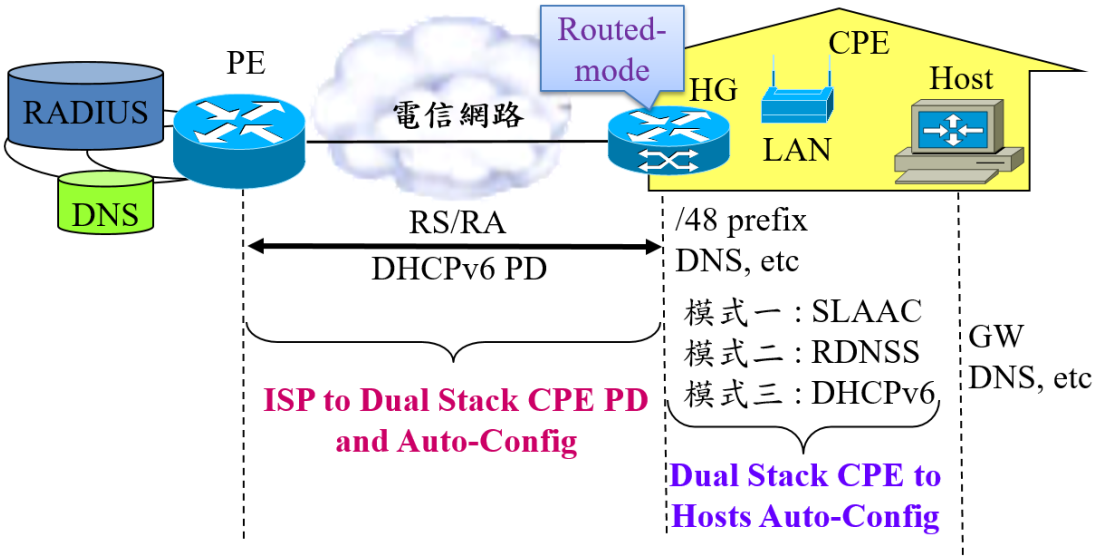


圖 18、寬頻分享器 IPv6 位址配置模式測試

本項測試規範建議如下：

表 13、SLAAC + stateless DHCPv6 搭配 RDNSS 配置測試規範建議

步驟	測試內容
1	動作:CE-Router 從 WAN 端取得 Prefix 和 DNS Server 位址資訊
2	動作：CE-Router 設定啟動 SLAAC 和 RDNSS 功能
3	動作：CE-Router 啟動 LAN 介面 檢驗：CE-Router 會定期發送 RA 訊息，其中 M、O 旗標都設定為 0，RA 訊息中 Option 欄位帶有 DNS Server 位址資訊。
4	動作：Host 介面設定為自動指派 IPv6 位址
5	動作：Host 啟動介面並連線至 CE-Router 的 LAN 介面 檢驗：Host 發送 RS 訊息到網域中，CE-Router 收到後會立刻發送 RA 訊息。Host 收到 RA 訊息後，根據其 Prefix 使用 EUI-64 或是 Privacy Extension 組成位址，此外 Host 會解析 RA 的 Option 欄位得到 DNS Server 資訊。

表 14、SLAAC + stateful DHCPv6 配置測試規範建議

步驟	測試內容
1	動作:CE-Router 從 WAN 端取得 Prefix 和 DNS Server 位址資訊
2	動作：CE-Router 設定啟動 SLAAC 和 DHCPv6 功能
3	動作：CE-Router 啟動 LAN 介面 檢驗：CE-Router 需定期發送 RA 訊息，其中 M 旗標設定為 0 而 O 旗標設定為 1。
4	動作：Host 介面設定為自動指派 IPv6 位址
5	動作：Host 啟動介面並連線至 CE-Router 的 LAN 介面 檢驗：Host 發送 RS，CE-Router 收到後會立刻發送 RA。Host 收到 RA 訊息後，根據其 Prefix 使用 EUI-64 或是 Privacy Extension 組成位址。Host 向 DHCPv6 伺服器請求 DNS 伺服器位址，CE-Router 收到請求後傳送回覆訊息給 Host，Host 解析回覆訊息得到 DNS 資訊。

(三) IPv6 PPPoE 斷線重撥測試

測試目的：檢測寬頻分享器 IPv6 PPPoE 是否支援斷線自動重播的功能。

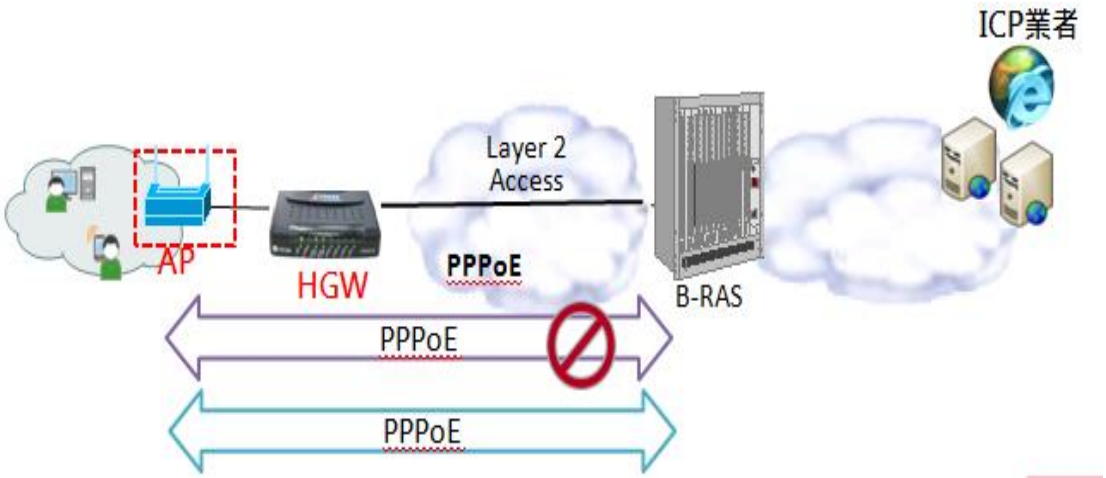


圖 19、IPv6 PPPoE 斷線重撥測試

本項測試規範建議如下：

表 15、IPv6 PPPoE 斷線重撥測試規範建議

步驟	測試內容
1	動作：第一次撥接成功後，將 WAN 端斷線 檢驗：如果沒有其他路由資訊，IPv6 CE Router 必須使用[RFC4861]中規定的 Router Discovery 來尋找 default router(s)，將發現的 Router 位址作為 next hop，並更新路由表預設路由

(四) MTU 測試

測試目的：檢測寬頻分享器是否支援 MTU Size 設定之功能以及對大封包的處置回應是否符合規範。

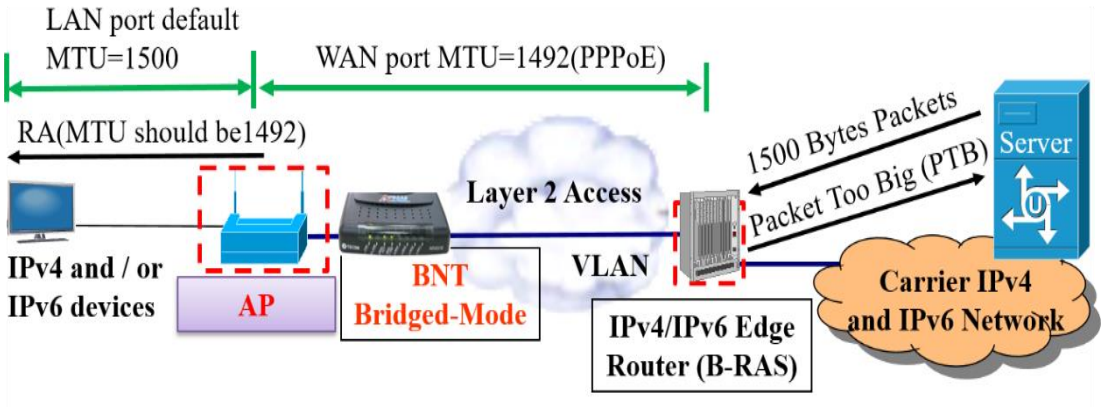


圖 20、IPv6 MTU 測試架構

IPv6 MTU 測試規範建議流程如下：

表 16、IPv6 MTU 測試規範建議

步驟	測試內容
1	動作：將 CE-Router WAN 端 interface 的 MTU 設為 1492
2	動作：LAN 端使用者設備向 2001:4860:4860::8888 (Google Public DNS for IPv6)發送 payload 為 1444 bytes 的 ICMPv6 Echo Request (ICMPv6 的 header 長度為 48，加上 payload 剛好為 1492) 檢驗：2001:4860:4860::8888 回傳 ICMPv6 Echo Reply 給使用者設備
3	動作：LAN 端使用者設備向 2001:4860:4860::8888 發送 payload 為 1445 bytes 的 ICMPv6 Echo Request (ICMPv6 的 header 長度為 48，加上 payload 為 1493) 檢驗：CE-Router 要向 LAN 端使用者設備發出 ICMPv6 Packet Too Big

(五) 寬頻分享器 IPv6 防火牆功能測試

測試目的：檢測寬頻分享器是否可設定 IPv6 防火牆規則以及確認防火牆能有效過濾並限制用戶 IPv6 的連線。



圖 21、寬頻分享器 IPv6 防火牆功能測試

本項測試規範建議如下：

表 17、ICMPv6 封包過濾測試規範建議–Destination Unreseachable

步驟	測試內容
1	動作：勾選開啟防火牆功能
2	動作：加入防火牆規則，allow ingress ICMPv6 Unreachable
3	動作：加入防火牆規則，deny Ingress ICMPv6
4	動作：內部客戶端對外 ping 不存在的 ip 位址 檢驗：內部客戶端會接收到 ICMPv6 Unreachable 的訊息
5	動作：內部客戶端對外 ping 存在的 ip 位址 檢驗：內部客戶端不會接收到 ICMP Echo Rely 的訊息

表 18、ICMPv6 封包過濾測試規範建議 – Packet Too Big

步驟	測試內容
1	動作：勾選開啟防火牆功能
2	動作：加入防火牆規則，allow Ingress ICMPv6 Packet Too Big
3	動作：加入防火牆規則，deny Ingress Extension Header

4	動作：外部客戶端對內部客戶端傳送加入 Extension Header 的封包(例如設定帶有 fragment Header) 檢驗:內部客戶端不會接收到外部客戶端傳送的封包
5	動作：內部客戶端對外傳送超過支援 MTU 大小的封包，並不加入 fragment Header 檢驗：內部客戶端會接收到 ICMPv6 Packet Too Big 訊息

二、IPv6 Ready Logo 建議測試項目選項規範

IPv6 CE Ready Logo 的測試可區分為四類共 23 項測試項目如圖 22（細部說明請參附件二）。WAN 與 LAN 兩類均為建議選測項目，General Requirement 以及 ULA 部分測項則建議可視際廠商實際需求評估是否納入建議測項。D-Link 廠商建議重點測試項目為 WAN Side Test 之第 2, 3, 4, 5, 7 項；LAN Side Test 之第 1, 2, 3, 4, 5, 7, 8, 9 項；General Requirement Test 之第 1, 3 項等。

WAN Side Test:
1. DUPLICATE ADDRESS DETECTION
2. ROUTER DISCOVERY
3. ADDRESS LIFETIME
4. DHCPV6
5. DHCPV6 PREFIX DELEGATION
6. UNNUMBERED WAN
7. DHCPV6 SOL_MAX_RT
8. L FLAG PROCESSING

General Requirement Test:
1. ICMPV6
2. IPV6 FORWARDING BEFORE ADDRESS ACQUISITION
3. NO DEFAULT ROUTE
4. FORWARDING LOOPS

LAN Side Test:
1. DUPLICATE ADDRESS DETECTION AND NEIGHBOR DISCOVERY
2. ASSIGNING PREFIXES TO LAN INTERFACES
3. ROUTER ADVERTISEMENT
4. STATELESS DHCP SERVER
5. DHCP SERVER
6. PREFIX CHANGE
7. LINK MTU
8. DNS INFORMATION IN ROUTER ADVERTISEMENT
9. INGRESS FILTERING

Unique Local Address Test:
1. ULA PREFIX GENERATION
2. ULA SITE BORDER

圖 22、IPv6 Ready LogoProgram 測試項目

第三節 IASP 實測平台建置與實機測試

本計畫規劃的測試平台主要由中華電信 HiNet 非固定制電路以及南桃園大寬頻 Cable 電路所組成。實測平台架構如圖 23 所示。用戶連網的三種情境之說明請參閱第一章第一節第六小節之中華電信 HiNet 光世代 IPv6 PPPoE 連網測試。

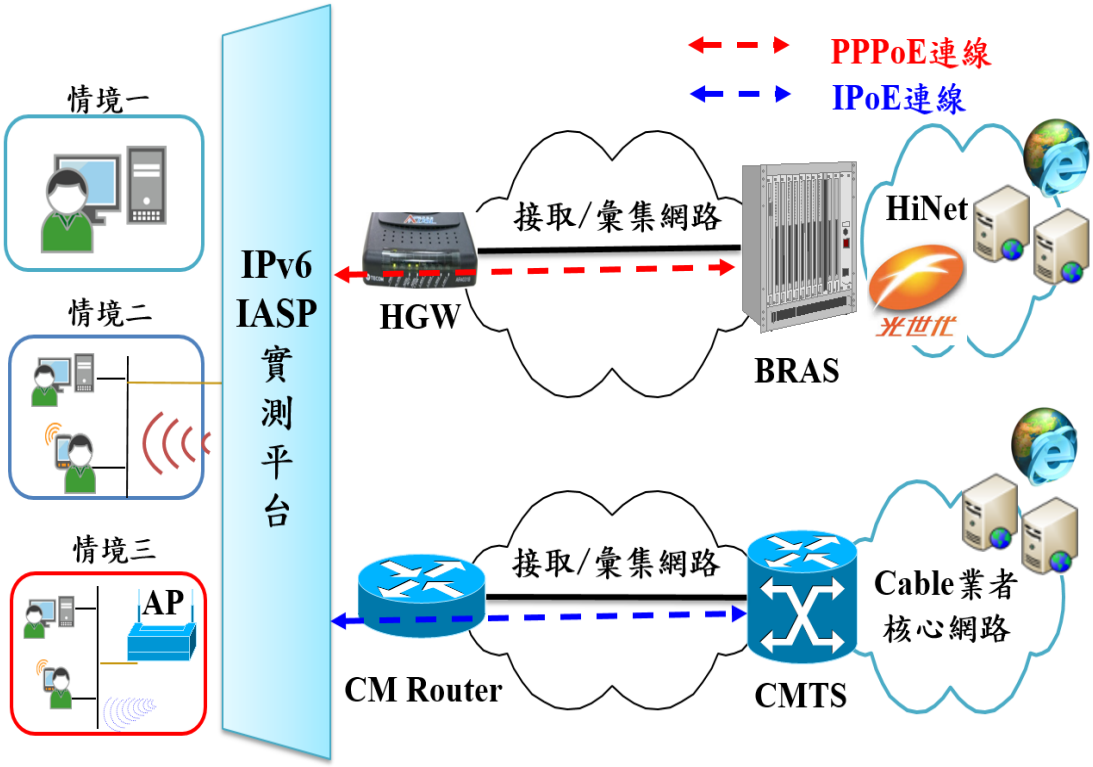


圖 23、IASP IPv6 實測平台

一、IASP 實測平台建置

針對 PPPoE 上網測試環境，本計畫主要以中華電信 HiNet 光世代非固定制為主，HiNet 非固定制電路建置資訊如圖 24 所示。針對 IPoE 上網測試環境，本計畫主要以 TBC 台灣寬頻通訊為主，電路建置資訊如圖 25 所示。

- HG為D-Link DSL-7740C





GENERAL

System Up Time : 21:37:29
F/W Code : DSL7740C.V6.TR069.20180723
DSL Code : A2pvbF038m.d24k
Wifi Code : 5.100.138.2008.cpe4.12L06B.4

韌體版本

INTERNET STATUS

IPv4連線資訊

Connect | Disconnect

Status : connected
Uptime : 13M:34S
MAC Address : 40:9B:CD:02:2E:53
Connection Type : PPPOE
IP Address : 114.37.86.78
Subnet Mask : 255.255.255.255
Default Gateway : 168.95.98.254
DNS Server : 168.95.192.1 168.95.1.1

IPV6 CONNECTION INFORMATION

IPv6連線資訊

IPv6 Connection Type : PPPDHCPv6PD
Network Status : connected
WAN IPv6 Address : 2001:b011:6cc0:2db:429b:cdff:fe03:2e53/64
IPv6 Default Gateway : fe80::d2f0:dbff:fe53:800
Primary DNS Server : 2001:b000:168::2
Secondary DNS Server : 2001:b000:168::1
DHCPv6 PD : 2001:b011:6cc0:3615::/64
LAN IPv6 Address : 2001:b011:6cc0:3615:429b:cdff:fe00:2e53/64
LAN IPv6 Link-Local Address : fe80::429b:cdff:fe00:2e53/64

圖 24、HiNet 光世代寬頻上網 IPv6 線路資訊

- HG為仲琦科技CGNF-TWN II









圖 25、TBC 台灣寬頻 IPv6 線路資訊

由於透過寬頻分享器裝置配置用戶 IPv6 連網參數的方法較為複雜，會因為配置方式的不同而有不同的模式，除需搭配 CPE 本身可支援的 IPv6 功能外，用戶主機的作業系統也必須支援，如用戶採用 CPE 上網方式，預設建議採用 SLAAC + Stateless DHCPv6 方式配置。

二、市售 IPv6 寬頻分享器實機測試成果

針對市售 IPv6 寬頻分享器實機測試需求，本節提出 D-Link、ASUS、TP-Link 以及 TOTOLINK 等四個廠牌共十個不同型號的寬頻分享器之測試成果摘要，依據固網寬頻 PPPoE 以及 Cable IPoE 的測試項目進行測試，摘要紀錄說明如下，個別廠牌型號設備細部測試結果請參閱附件四。

(一) 市售 IPv6 寬頻分享器之 PPPoE 測試項目成果如下表所示。

表 19、IPv6 寬頻分享器 PPPoE 測試項目成果 I

廠牌型號 / 測試項目	D-Link				ASUS
	DIR-853	DIR-2680	DIR-1960	DIR-1760	RT-AC66U
分享器 PPPoE 撥接是否正常?	O	O	O	O	O
分享器 IPv6、IPv6 PD、DNSv6 取得是否正常?	O	O	O	O	O
用戶 IPv6、DNSv6 取得是否正常?	O	O	O	O	O
用戶至 HiNet	O	O	O	O	O

路由是否正常?					
用戶 IPv6 上網是否正常?	O	O	O	O	O
用戶熱門網頁開啟是否正常?	O	O	O	O	O
用戶上網速率是否正常?	O	O	O	O	O
分享器重撥，用戶 IPv6 更新是否正常?	O	O	O	O	O
用戶使用 IPv6 之 MTU 是否正常?	1500	1492	1500	1500	1492
用戶連接 Wi-Fi 上網 IPv6、DNSv6 是否正常?	O	O	O	O	O
用戶連接 Wi-Fi IPv6 上網是否正常?	O	O	O	O	O
IPv6 PPPoE (或是 PPPoEv6)是否隨著 IPv4 PPPoE 啟用而自動啟用?	O	O	O	X	X

IPv6 PPPoE (或是 PPPoEv6)連線之 PPPoE Session 是『Share with IPv4』或是『Create a new Session』?	可設定兩種模式『New Session』WAN 端為斷線	可設定兩種模式	可設定兩種模式『New Session』WAN 端為斷線	可設定兩種模式『New Session』WAN 端為斷線	無提供此項設定
IPv6 ACL 功能是否正常？	O	O	O	O	O

表 20、IPv6 寬頻分享器 PPPoE 測試項目成果 II

廠牌型號 / 測試項目	ASUS	TP-Link		TOTOLINK	
	RT-AC1300UHP	Archer C1200	Archer A9	A7000R	A950RG
分享器 PPPoE 撥接是否正常?	O	O	O	O	O
分享器 IPv6、IPv6 PD、DNSv6 取得是否正常?	O	O	O	O	O
用戶 IPv6、DNSv6 取得是否正常?	O	O	O	O	O
用戶至 HiNet 路由是否正常?	O	O	O	O	O
用戶 IPv6 上網是否正常?	O	O	O	O	O

用戶熱門網頁開啟是否正常?	O	O	O	O	O
用戶上網速率是否正常?	O	O	O	O	O
分享器重撥，用戶 IPv6 更新是否正常?	O	O	O	O	O
用戶使用 IPv6 之 MTU 是否正常?	1492	1492	1492	1484	1500
用戶連接 Wi-Fi 上網 IPv6、DNSv6 是否正常?	O	O	O	O	O
用戶連接 Wi-Fi IPv6 上網是否正常?	O	O	O	O	O
IPv6 PPPoE (或是 PPPoEv6)是否隨著 IPv4 PPPoE 啟用而自動啟用?	X	X	X	O	X
IPv6 PPPoE (或是 PPPoEv6)連線之 PPPoE Session 是『Share with IPv4』或是『Create a new Session』?	無提供此項設定	可設定兩種模式	可設定兩種模式	無提供此項設定	無提供此項設定
IPv6 ACL 功能是否正常？	O	無支援 IPv6 ACL 功能	無支援 IPv6 ACL 功能	無支援 IPv6 ACL 功能	無支援 IPv6 ACL 功能

(二) 市售 IPv6 寬頻分享器之 Cable IPoE 測試項目成果如下表所示。

表 21、IPv6 寬頻分享器 Cable IPoE 測試項目成果 I

廠牌型號 / 測試項目	D-Link				ASUS
	DIR-853	DIR-2680	DIR-1960	DIR-1760	RT-AC66U
分享器連接 Cable Modem 是否正常?	O	O	O	O	O
分享器 IPv6、IPv6 PD、DNSv6 取得是否正常?	O	O	O	O	O
用戶 IPv6、DNSv6 取得是否正常?	O	O	O	O	O
用戶至 Cable 業者路由是否正常?	O	O	O	O	O
用戶 IPv6 上網是否正常?	O	O	O	O	O
用戶熱門網頁開啟是否正常?	O	O	O	O	O
用戶上網	O	O	O	O	O

速率是否正常?					
分享器重撥 Cable Modem，用戶 IPv6 更新是否正常?	O	O	O	O	O
用戶使用 IPv6 之 MTU 是否正常?	1500	1500	1500	1500	1500
用戶連接 Wi-Fi 上網 IPv6、DNSv6 是否正常?	O	O	O	O	O
用戶連接 Wi-Fi IPv6 上網是否正常?	O	O	O	O	O
IPv6 連線功能是否隨著 IPv4 啟用而自動啟用?	O	O	O	X	X
IPv6 ACL 功能是否正常？	O	O	O	O	O

表 22、IPv6 寬頻分享器 IPoE 測試項目成果 II

廠牌型號	ASUS	TP-Link		TOTOLINK	
	RT-AC13	Archer	Archer	A7000R	A950RG

測試項目	00UHP	C1200	A9		
分享器連接 Cable Modem 是否正常?	O	O	O	O	O
分享器 IPv6、IPv6 PD、DNSv6 取得是否正常?	O	O	O	O	O
用戶 IPv6、DNSv6 取得是否正常?	O	O	O	O	O
用戶至 Cable 業者路由是否正常?	O	O	O	O	O
用戶 IPv6 上網是否正常?	O	O	O	O	O
用戶熱門網頁開啟是否正常?	O	O	O	O	O
用戶上網速率是否正常?	O	O	O	O	O
分享器重撥 Cable Modem，用戶 IPv6 更新是否正常?	O	O	O	O	O
用戶使用 IPv6 之 MTU 是否	1500	1492	1500	1480	1500

正常?					
用戶連接 Wi-Fi 上網 IPv6、DNSv6 是否正常?	O	O	O	O	O
用戶連接 Wi-Fi IPv6 上網是否正常?	O	O	O	O	O
IPv6 連線功能是否隨著 IPv4 啟用而自動啟用?	X	X	X	X	X
IPv6 ACL 功能是否正常?	O	無支援 IPv6 ACL 功能	無支援 IPv6 ACL 功能	無支援 IPv6 ACL 功能	無支援 IPv6 ACL 功能

(三) IPv6 寬頻分享器之 LAN 端位址配置模式統整，下表列出分享器對於 SLAAC + stateless DHCPv6、SLAAC + stateful DHCPv6、SLAAC + RDNSS 三種位址配置模式之選項設定支援狀況。

表 23、IPv6 寬頻分享器之 LAN 端位址配置模式支援能力

廠牌	測試型號	IPv6 位址配置功能支援模式		
		SLAAC + DHCPv6 stateless	SLAAC + DHCPv6 stateful	SLAAC + RDNSS
D-Link	DIR-853	O	O	O

D-Link	DIR-2680	O	O	O
D-Link	DIR-1960	O	O	O
D-Link	DIR-1760	O	O	O
ASUS	RT-AC66U	O	O	—
ASUS	RT-AC1300 UHP	O	O	—
TP-Link	Archer C1200	O	O	O
TP-Link	Archer A9	O	O	O
TOTOLINK	A7000R	僅支援 RADVD + SLAAC		
TOTOLINK	A950RG	僅支援 RADVD + DHCPv6		

(四) IPv6 寬頻分享器通訊界面支援能力統整，下表列出分享器對於 Wi-Fi (LAN)、IPoE (WAN)、PPPoE (WAN)之三種通訊界面支援能力。

表 24、IPv6 寬頻分享器之通訊界面支援能力

廠牌	測試型號	寬頻分享器通訊界面 IPv6 支援能力		
		WiFi	IPoE	PPPoE

D-Link	DIR-853	O	O	O
D-Link	DIR-2680	O	O	O
D-Link	DIR-1960	O	O	O
D-Link	DIR-1760	O	O	O
ASUS	RT-AC66U	O	O	O
ASUS	RT-AC1300UHP	O	O	O
TP-Link	Archer C1200	O	O	O
TP-Link	Archer A9	O	O	O
TOTOLINK	A7000R	O	O	O
TOTOLINK	A950RG	O	O	O

(五) 市售寬頻分享器測試成果觀察與建議

1. MTU Size 的設定

觀察結果：

- 使用 PPPoE 連線時 MTU 必須為 1492(或更低)。
- 實測各廠牌型號結果顯示其 MTU 預設略有不同。

建議：

- 建議設備廠商 MTU 大小可由 CPE 網頁管理介面設定。

2. IPv6 預設啟用支援

觀察結果：

- 部分廠牌型號測試結果顯示其無法在使用 IPv4 快速設定介面(設定精靈)後，直接取得 IPv6 連線。

建議：

- 建議在快速設定完成後，自動啟用「IPv6 與 IPv4 共享 Session」的選項；或是將 IPv6 之啟用設定納入快速設定選項中。

3. IPv6 LAN 端位址配置模式

觀察結果：

- CPE IPv6 LAN 端位址配置模式主要有三種，各廠牌支援之模式設定略有差異。

建議：

- 建議 CPE 設備廠商應支援表 22 所列三種 IPv6 LAN 端位址配置模式。

(六) 寬頻分享器長時間 IPv6 連網測試

除以上所述之測試項目外，為驗證 CPE 設備長時間 IPv6 連網之狀態能力，本計畫於 PPPoE 以 84 小時、Cable IPoE 以 18 小時進行測試，摘要如下：

1. 測試方法：

自行撰寫的 windows batch 檔，每一小時下載一個檔案大小為 72 KB 的 html 檔及一個檔案大小為 49 MB 的 MP4 檔，詳細 batch 腳本如圖 26 所示。

(1) 以開源專案 youtube-dl 下載 49MB 的 MP4 影片

(2) 以開源軟體 wget 下載 72KB 的 RFC 7084 網頁

(3) 以上指令皆以「-6」的參數強制透過 IPv6 下載

(4) 下載取得之檔案將以下載時間命名，如 date.mp4、date.html

```
@ECHO OFF
set INTERVAL=3600

:DOWNLOADINTERVAL
echo. >> log.txt
echo %date%%time% >> log.txt
echo ----------------------------------------^
----------------------------------------^
----------------------------------------^
---------------------------------------- >> log.txt

For /f "tokens=1-4 delims=/ " %%a ^
in ('date /t') do (set mydate=%%a-%%b-%%c)
For /f "tokens=1-2 delims=/:" %%a ^
in ("%TIME%") do (set mytime=%%a%%b)

echo. >> log.txt
echo "[Youtube Download]" >> log.txt
youtube-dl.exe "https://www.youtube.com/watch?v=YbJOTdZBX1g" ^
-6 --verbose -o "[%mydate%_%mytime%] Rewind.mp4" >> log.txt 2>&1

echo. >> log.txt
echo "[RFC7084 Download]" >> log.txt
wget.exe -6 -v --no-check-certificate ^
https://tools.ietf.org/html/rfc7084 ^
-O "[%mydate%_%mytime%] RFC7084.html" >> log.txt 2>&1 || del ^
"[%mydate%_%mytime%] RFC7084.html"

timeout %INTERVAL%
GOTO DOWNLOADINTERVAL
```

將輸出檔名設為目前的時間

限制youtube-dl.exe透過IPv6方式下載

限制wget.exe透過IPv6方式下載

間隔3600秒後再次執行

圖 26、寬頻分享器長時間 IPv6 連網測試 batch 腳本

2. 測試結果

以 D-Link DIR-853 為例，PPPoE 長時間連網測試結果如圖 27 和圖 28 所示，開始的下載時間為 9/23 14:37，最後下載的時間為 9/27 13:29，連網時間超過 84 小時並且期間內每一小時皆有成功下載檔案；Cable IPoE 長時間連網測試結果如圖 29 所示，開始的下載時間為 9/03 14:16，最後下載的時間為 9/04 13:22，連網時間超過 18 小時並且期間內每一小時皆有成功下載檔案。

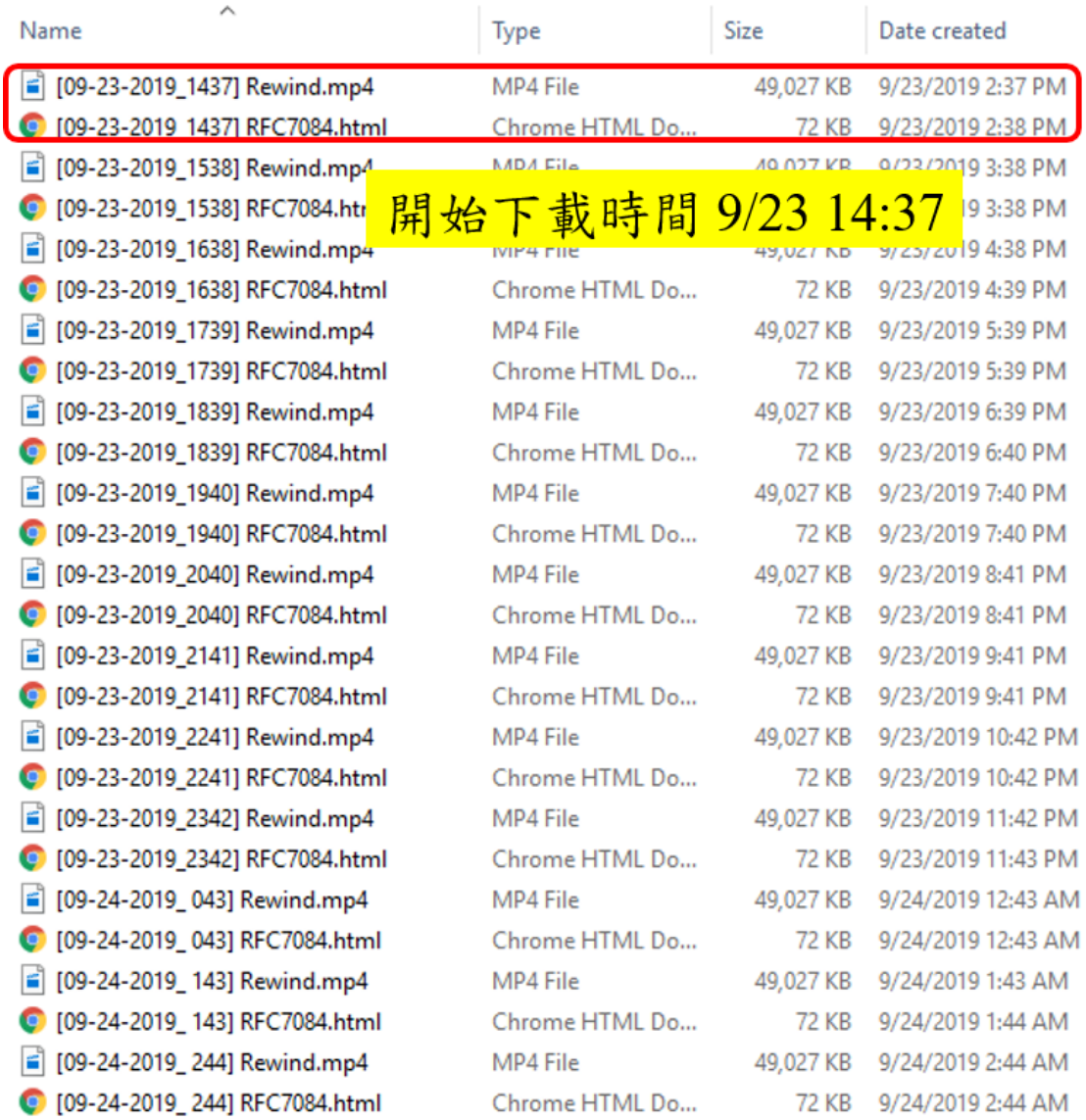


圖 27、PPPoE 長時間連網測試結果(1)



圖 28、PPPoE 長時間連網測試結果(2)



圖 29、Cable IPoE 長時間連網測試結果

(1) PPPoE 長時間連網測試

接在 CPE LAN 端之設備，透過 IPv6 每小時下載測試持續 84 小時，完成所有檔案下載之型號如下：

- ASUS RT-AC66U

- D-Link DIR-853
- D-Link DIR-2680
- D-Link DIR-1760
- TP-Link Archer C1200
- TP-Link Archer A9

(2) Cable IPoE 長時間連網測試

接在 CPE LAN 端之設備，透過 IPv6 每小時下載測試持續 18 小時，完成所有檔案下載之型號如下：

- ASUS RT-AC66U
- D-Link DIR-853
- D-Link DIR-2680
- D-Link DIR-1960
- D-Link DIR-1760
- TP-Link Archer C1200
- TP-Link Archer A9
- TOTOLINK A7000R

三、用戶連網終端設備 IPv6 支援評估

用戶連網終端設備支援 IPv6 能力評估資料如下表，用戶端需選用以下可支援 IPv6 之作業系統，如用戶電腦作業系統 Windows 7 以上、Linux Ver. 2.4 以上、MAC OS X Ver. 4.2 以上；行動裝置作業系統 iOS Ver. 4.2 以上及 Android Ver 2.1 以上。

表 25、用戶連網終端作業系統 IPv6 支援評估

類別	作業系統	版本功能	備註
腦 電 人 個	Windows 8	支援(Enabled by default)	支援 SLAAC 位址配置 支援 DHCPv6 client.模

			式 支援 IPv6 DNS 配置
	Windows 7	支援(Enabled by default)	支援 SLAAC 位址配置 支援 DHCPv6 client.模式 支援 IPv6 DNS 配置
	Windows 2008	支援(Enabled by default)	支援 SLAAC 位址配置 支援 DHCPv6 client.模式 支援 IPv6 DNS 配置
	Windows Vista	支援(Enabled by default)	支援 SLAAC 位址配置 支援 DHCPv6 client.模式 支援 IPv6 DNS 配置
	Windows 2003	支援(run netsh install ipv6)	支援 SLAAC 位址配置
	Windows XP	SP1 及 SP2 均支援	支援 SLAAC 位址配置
	FreeBSD	Ver. 4.0 以上	Based on the KAME project
	Linux	Ver. 2.4 以上, Ver 2.6.15 佳	多數的版本已支援
	NetBSD	Ver. 1.5 以上	Based on the KAME project
	OpenBSD	Ver. 3.9 以上	Based on the KAME project
	Sun Solaris	Ver. 8 以上	Ver. 8 以上
	Ubuntu	Ver 12.04 以上	支援 SLAAC 位址配置 支援 IPv6 DNS 配置
	MAC OS X	Ver. 10.7 以上	支援 SLAAC 位址配置 支援 RDNSS 位址配置 支援 IPv6 DNS 配置
手機	iOS	Ver. 11 以上	支援 SLAAC 位址配置 支援 IPv6 DNS 配置
	Android	Ver. 7 以上	支援 SLAAC 位址配置 支援 IPv6 DNS 配置

第四節 政府採購共同供應契約設備參考規範

本計畫針對主機、伺服器、路由器以及網路保護裝置等四種網路設備歸納其共同供應契約之規範建議書以供參考。參考規範的來源包含： (1)美國政府 IPv6 技術規畫 - USG IPv6 Profile [21] (2)國際 IPv6 測試計畫 - Ready Logo Program [22] (3)歐洲網路資訊中心 – RIPE 554, Requirements for IPv6 in ICT Equipment [23] (4)中華民國交通部 – IPv6 資通認證設備與軟體採購規範建議書[24]。其中的規範囊括 IPv6 的基本規格、路由、位址、安全性與管理。參考來源與規範內容如下圖所示：

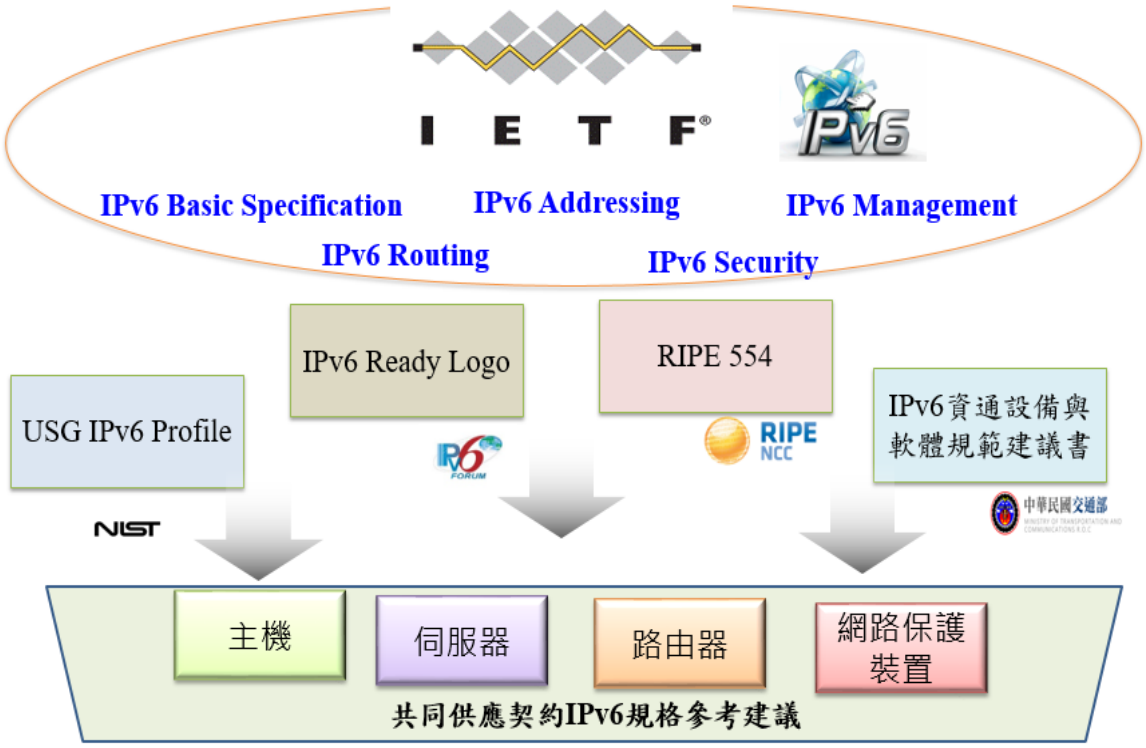


圖 30、政府採購共同供應契約之設備參考規範項目與來源

下圖為設備對 IPv6 之功能需求規範，其中主機的規範內容包含大部分的 IPv6 基本功能，而其他設備則基於主機之規範，再加上針對該類設備額外的功能需求。

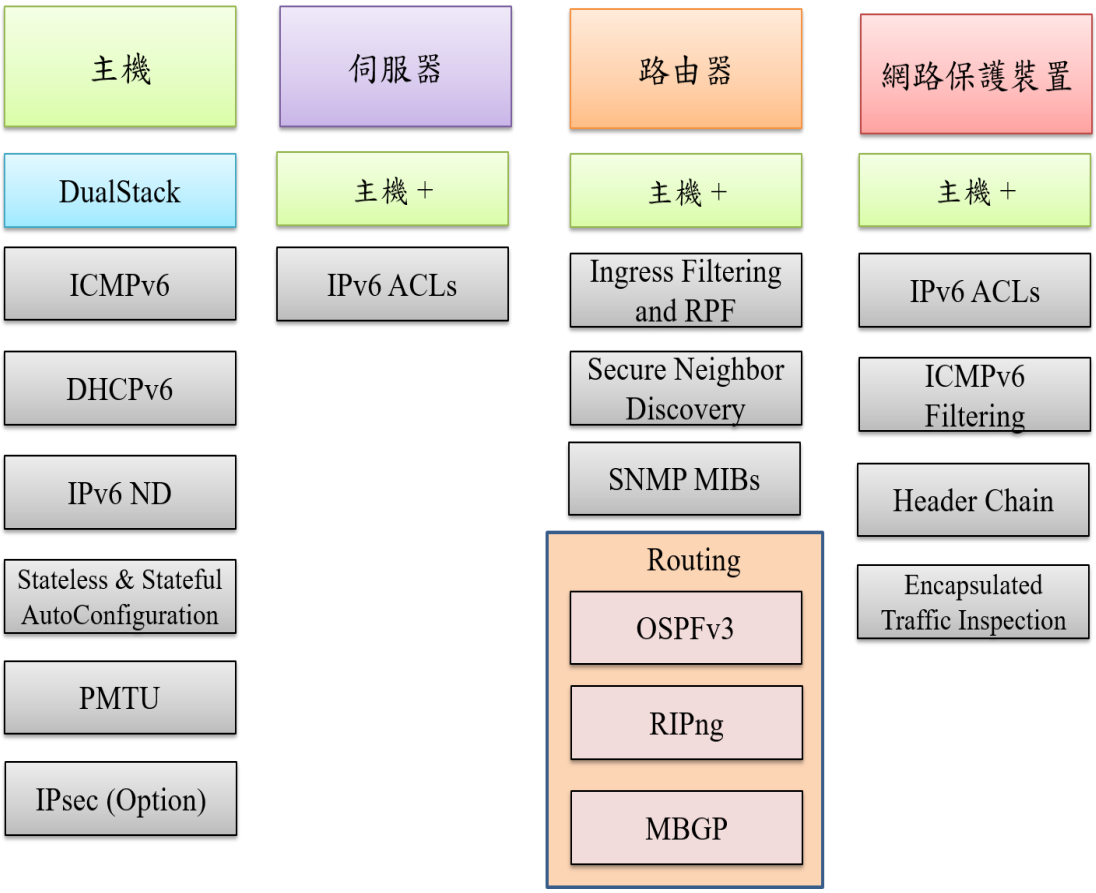


圖 31、各設備之 IPv6 參考規範內容

各設備之共同供應契約細節，分別針對主機、伺服器、路由器、網路保護裝置之參考項目，表列各參考規範如下表所示：

表 26、共同供應契約規範建議

設備	規範條列
主機	1. 必須支援 IPv6 Addressing Architecture 定義之位址格式規範 2. 必須支援 IPv6 Default Address Selection 功能 3. 必須支援 Unique Local IPv6 Unicast Addresses (ULA)位址格式 4. 必須支援 ICMPv6 通訊協定 5. 必須支援 DHCPv6 規範之 Client 行為 6. 必須支援 Stateless 或 Stateful 位址分配機制 7. 必須支援 Path MTU Discovery 功能 8. 必須支援 Neighbor Discovery 功能 9. 必須支援 IPv6 DNS 資源記錄以及 Extension DNS 功能 10. 如須支援 Tunneling 以及 Dual Stack 環境，則主機必須支援基本 IPv6 轉移機制 11. 如須支援 Mobile IPv6 環境，則主機必須支援 MIPv6 機制 12. 必須棄用 IPv6 Type 0 Routing Headers
伺服器	1. 必須支援 IPv6 Addressing Architecture 定義之位址格式規範 2. 必須支援 IPv6 Default Address Selection 功能 3. 必須支援 Unique Local IPv6 Unicast Addresses (ULA)位址格式 4. 必須支援 ICMPv6 通訊協定 5. 必須支援 DHCPv6 規範之 Client 行為 6. 必須支援 Stateless 或 Stateful 位址分配機制 7. 必須支援 Path MTU Discovery 功能 8. 必須支援 Neighbor Discovery 功能 9. 必須支援 IPv6 DNS 資源記錄以及 Extension DNS 功能 10. 如須支援 Tunneling 以及 Dual Stack 環境，則主機必須支援基本 IPv6 轉移機制 11. 如須支援 Mobile IPv6 環境，則主機必須支援 MIPv6 機制

	12.必須棄用 IPv6 Type 0 Routing Headers
路由器	1. 必須支援 IPv6 Addressing Architecture 定義之位址格式規範 2. 必須支援 IPv6 Default Address Selection 功能 3. 必須支援 Unique Local IPv6 Unicast Addresses (ULA)位址格式 4. 必須支援 ICMPv6 通訊協定 5. 必須支援 SLAAC 功能 6. 應支援 Multicast Listener Discovery version 2 (MLDv2)以及 MLDv2 snooping 功能 7. 必須支援 Router-Alert option 功能 8. 必須支援 Path MTU Discovery 功能 9. 必須支援 Neighbor Discovery 功能 10.必須支援 IPv6 QoS 功能 11.必須棄用 IPv6 Type 0 Routing Headers 12.如須支援 Interior Gateway Protocol (IGP) ，則 Router 路由器必須支援 RIPng 以及 OSPFv3 13.如須使用 OSPFv3，則 Router 路由器必須支援 Authentication/Confidentiality for OSPFv3 14.如須支援 Exterior Gateway Protocol (EGP)，則 Router 路由器必須支援 MBGP 功能 15.如須支援 Tunneling 以及 Dual Stack，則 Router 路由器必須支援基本 IPv6 轉移機制 16.如須支援 Mobile IPv6 ，則 Router 路由器必須支援 MIPv6 機制以及 Mobile IPv6 Operation With IKEv2 的行為模式 17.如須支援 MPLS，則 Router 路由器必須支援 MPLS Traffic Engineer(TE)以及 MPLS Fast Reroute(FRR) 功能 18.如須支援 L3 VPN，則 Router 路由器必須支援 BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN

網路保護裝置設備	1. 必須支援 IPv6 Addressing Architecture 定義之位址格式規範 2. 必須支援 IPv6 Default Address Selection 功能 3. 必須支援 ICMPv6 功能 4. 必須支援 IPv6 StateLess Address AutoConfiguration 功能 (FW, IPS) 5. 必須支援 Router-Alert option 功能 (FW, IPS) 6. 必須支援 Path MTU Discovery 功能 7. 必須支援 Neighbor Discovery 功能 8. 必須支援 IPv6 QoS 功能(FW, APFW) 9. 如須支援 Interior Gateway Protocol (IGP) ，則裝置必須支援 RIPng 以及 OSPFv3 10. 如須支援 Exterior Gateway Protocol (EGP)，則裝置必須支援 MBGP 11. 如須使用 OSPFv3，則裝置必須支援 Authentication/Confidentiality for OSPFv3 12. 如須支援 Tunneling，則裝置必須支援基本 IPv6 轉移機制 (FW) 13. 必須棄用 IPv6 Type 0 Routing Headers 14. 網路管理不允許 IPv6 隧道時，需可檢查/阻擋 IPv4 header 中 Type 欄位值為 41 的 IPv4 封包(IPS/FW) 15. 可過濾 ICMPv6 封包，並制定封包過濾規則(FW) 16. 可過濾內含 Extension Header 的 IPv6 封包，並制定封包過濾規則(FW)

針對共同採購契約 IPv6 規範驗收可操作性部分需求，建議可參考本計畫提出之寬頻分享器測試規範建議進行 IPv6 基礎與必須功能驗證。對於本計畫提出的共同供應契約規範建議和既有的共同供應契約規範的比較請參考附件五。下表為既有的共同供應契約中主機、伺服器、路由器及網路保護裝置等設備的 IPv6 相關規範。主機規範參考台灣銀行共同供應契約 LP5-108019 [25]第 1 組；伺服器規範參考台灣銀行共同供應契約 LP5-107003 [26]第 1 組；路由器規範參考台

灣銀行共同供應契約 LP5-101018 [27]第 1 組；網路保護裝置規範參考台灣銀行共同供應契約 LP5-101018 第 3 組。

表 27、既有共同供應契約 IPv6 相關規範

設備	既有共同供應契約 IPv6 相關規範
主機	2-1. Windows 10(含)以上 Professional 64bit 中文專業版作業系統【作業系統提供原廠合法系統還原功能內含完整作業系統及相關驅動程式】
伺服器	14-1. Windows Server 2016(含)以上 Standard(標準版) 16 Core 中文版最新版作業系統含 10 個 Users(1+10 存取授權，僅提供 10 台機器或 10 個用戶端連線使用權利，若超過 10 台機器，或用戶端超過 10 人連線，請加購 Windows Server 用戶端存取授權最新授權版(User or Device CAL)) 14-2. Windows 10 Pro for Workstations 中文最新版作業系統 14-3. Red Hat Enterprise Linux 最新版或 SUSE Linux Enterprise Server 最新版或 Oracle Enterprise Linux 14-4. Enterprise Linux for Workstation 最新版或 SUSE Linux Enterprise Desktop 最新版或 Ubuntu Desktop LTS 最新版
路由器	17-1-14.符合下列任一 IPv6 功能說明或證明文件 17-1-14-1. 通過 IPv6 組織驗證測試，具備 IPv6 Ready Logo Phase2 認證文件 17-1-14-2. 符合 IETF(Internet Engineering Task Force)(網際網路專案任務小組)發展 規範 Request for Comments 之 RFC 2460 Internet Protocol, Version 6(IPv6) Specification、RFC 4861 Neighbor Discovery for IP Version 6(IPv6)、RFC 4862 IPv6 Stateless Address Autoconfiguration、RFC 4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification、RFC5095 Deprecation of Type 0 Routing

	Headers in IPv6 及 RFC1981 Path MTU Discovery for IP version 6 等規範標準 17-1-14-3. 經由 IPv6 組織網站(https://www.ipv6ready.org/db/index.php/public)驗證 查詢，取得相關該產品名稱或系列名稱等文件證明(須為通過IPv6 Ready Logo Phase2 產品)
網路保護裝置設備(入侵偵測系統)	1-1-18. 符合下列任一 IPv6 功能說明或證明文件 1-1-18-1. 通過 IPv6 組織驗證測試，具備 IPv6 Ready Logo Phase2 認證文件 1-1-18-2. 符合 IETF(Internet Engineering Task Force)(網際網路專案任務小組)發展規範 Request for Comments 之 RFC 2460 Internet Protocol, Version 6(IPv6) Specification 、RFC 4861 Neighbor Discovery for IP Version 6(IPv6)、RFC 4862 IPv6 Stateless Address Autoconfiguration、RFC 4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification 、RFC5095 Deprecation of Type 0 Routing Headers in IPv6 及 RFC1981 Path MTU Discovery for IP version 6 等規範標準 1-1-18-3. 經由 IPv6 組織網站(https://www.ipv6ready.org/db/index.php/public)驗證查詢，取得相關該產品名稱或系列名稱等文件證明(須為通過 IPv6 Ready Logo Phase2 產品) 1-1-18-4. 具備單獨偵測 IPv4(Native IPv4)與 IPv6(Native IPv6)網路 封包，並在 IPv4 及 IPv6 雙軌(Dual Stack)運行之網路環境 同時偵測 IPv4 與 IPv6 網路封包

網路保護裝置設備(防火牆)	2-1-11. 符合下列任一 IPv6 功能說明或證明文件 2-1-11-11. 通過 IPv6 組織驗證測試，具備 IPv6 Ready Logo Phase2 認證文件 2-1-11-12. 符合 IETF(Internet Engineering Task Force)(網際網路專案任務小組)發展規範 Request for Comments 之 RFC 2460 Internet Protocol, Version 6(IPv6) Specification 、RFC 4861 Neighbor Discovery for IP Version 6(IPv6)、RFC 4862 IPv6 Stateless Address Autoconfiguration、RFC 4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification 、RFC5095 Deprecation of Type 0 Routing Headers in IPv6 及 RFC1981 Path MTU Discovery for IP version 6 等規範標準 2-1-11-13. 經由 IPv6 組織網站(https://www.ipv6ready.org/db/index.php/public)驗證查詢，取得相關該產品名稱或系列名稱等文件證明(須為通過 IPv6 Ready Logo Phase2 產品) 2-1-11-14. 具備狀態檢視(stateful packet inspection (SPI) or stateful inspection)過濾 IPv4(Native IPv4)與 IPv6(Native IPv6)網路封包，並在 IPv4 及 IPv6 雙軌(Dual Stack)運行之網路環境同時過濾 IPv4 與 IPv6 網路封包，另提供 IPv6 路由協定(Static route)功能

第三章結論與建議

第一節 結論說明

有鑒於國內電信業者已陸續開放 IPv6，用戶自備寬頻分享器乃普及固網 IPv6 最後一哩環境之關鍵設備，唯目前市售寬頻分享器未能有一致的 IPv6 功能規範，為此本計畫乃參考國際 IPv6 RFC 標準以及 Ready Logo 測試項目，提出適合我國固網環境 IPv6 寬頻分享器之開發與測試規範，可提供網通設備業者參考。此外，為驗證市售寬頻分享器實際支援 IPv6 的功能狀態，本計畫也建立 IASP 實測平台實際測試市售之 IPv6 寬頻分享器 IPv6 功能，本計畫執行之測試結果可提供國內固網寬頻業者以及寬頻設備廠商提昇或改善 IPv6 功能。另針對政府採購共同供應契約的設備參考規範部分，本計畫亦將主機、伺服器、路由器以及網路保護裝置之採購規範建議以獨立規格項次方式將 IPv6 相容規格要求加入契約規範。本計畫結論摘要重點如下：

一、寬頻分享器 IPv6 開發規範

完成 16 個寬頻分享器相關 IPv6 RFC 標準開發規範研究，分列必須(Must), 應該(Should)以及可能(MAY)三種規範說明，重點摘要影響固網寬頻用戶連線的必須與選項建議規範，可提供國內寬頻分享器製造商研發與設計 IPv6 產品之參考。

二、寬頻分享器 IPv6 測試規範

研擬 5 種適合我國寬頻網路 IPv4/IPv6 雙協定網路的測試建議規範，可作為電信業者以及網通廠商測試 IPv6 上網服務的參考依據；此外，本計畫也依據 IPv6 Ready Logo 互連測試的標準，提出 23 項

共 133 個 IPv6 參考測項，可作為寬頻分享器製造商測試產品 IPv6 功能之參考。

三、IASP 實測平台與實機測試

完成 PPPoE 與 IPoE IASP IPv6 連網環境建置與上網功能測試，提供寬頻分享器 IPv6 連網功能的測試場域；此外，本案亦完成四家廠商共 10 款市售寬頻分享器 IPv6 功能實際驗證測試，測試結果可提供國內固網寬頻業者以及寬頻設備廠商提昇或改善 IPv6 功能的參考。

四、共同供應契約 IPv6 採購規範

研擬 12 個主機 Host IPv6 規範以及 12 個伺服器 Server IPv6 規範，並提出 18 個路由器 Router IPv6 規範以及 13 個網路保護裝置設備 (FW/IPS/) IPv6 規範，可作為政府採購共同供應契約 IPv6 規範的參考依據。

第二節 建議事項

隨著 IPv6 網路的逐漸普及，國內主要的寬頻業者如中華電信與台灣寬頻也已宣布啟動 IPv6，使得我國固網寬頻的 IPv6 環境逐步完善，也為未來以 IPv6 為主的創新應用需求建立良好的基礎。要進一步普及與優化用戶 IPv6 連網涵蓋率，用戶自備寬頻分享器 CPE 是不可或缺的關鍵，然而因 IPv6 規格可設定參數眾多，不同 IASP 亦有不同的供裝配置模式，也讓網通設備廠商對於是否預設啟動 IPv6 採取不一樣的策略。本計畫已針對我國固網環境提出寬頻分享器 IPv6 開發與測試規範，期能協助國內廠商與寬頻業者提昇預設啟動 CPE IPv6 功能的意願，藉此普及我國 IPv6 的使用環境。相關建議事項如下：

一、網通廠商新上市之寬頻分享器 CPE 設備出廠即預設啟動 IPv4/IPv6 雙協定服務模式。

二、網通商品需支援 IPv6 必須規格及測試項目，並建議政府納入共同供應契約，確保新採購之設備均能支援 IPv6。

三、建置支援 IPv6 合規的網通商品型錄資料庫及建置推廣網站，提供消費者採購相關商品的參考依據。

四、提供設備廠商研發支援 IPv6 之相關獎勵、補助與減稅措施，以增加推動誘因。

五、透過規管政策限制寬頻業者與網通廠商之服務與產品需支援 IPv6。

此外，在 IPv6 網路安全部分重要性亦不可輕忽，由於相關議題涵蓋範圍廣泛且複雜性高，建議可另立專案研究，確保 IPv6 網路之安全，以下僅針對 IPv6 網路安全防護提出基本建議如下：

一、IPv6 不建議採用 NAT，因此防火牆在 IPv6 資安上更顯重要。CPE 防火牆功能必須支援 IPv6，並確認 IPv6 功能之完整性及效能。

二、IPv4 的最佳實作建議仍適用於 IPv6，但必須確認 IPv6 資安設備可提供對等的 IPv6 防護機制 (L3 Spoofing、NDP Spoofing…等)。

三、IPv6 相關協定及產品實作可能因安全議題陸續修定，須定期追蹤設備/軟體商、CVE 等發佈之弱點公告，即時修補可能的安全弱點或漏洞。

第四章參考資料來源

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

[2] IPv6 全球排序網站，https://ipv6now.twnic.net.tw/ipv6/index.html

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

[4] RFC 2460 Internet Protocol, Version 6 (IPv6) Specification

[5] RFC 1981 Path MTU Discovery for IP version 6

[6] RFC 4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification

[7] RFC 5072 IP Version 6 over PPP

[8] RFC 4890 Recommendations for Filtering ICMPv6 Messages in Firewalls

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

[10] RFC 7123 Security Implications of IPv6 on IPv4 Networks

[11] RFC 4862 IPv6 Stateless Address Autoconfiguration

[12] RFC 4861 Neighbor Discovery for IP version 6 (IPv6)

[13] RFC 3736 Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6

[14] RFC 5006 IPv6 Router Advertisement Option for DNS Configuration

[15] RFC 3646 DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

[16] RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

[17] RFC 3633 IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6

[18] RFC 7084 Basic Requirements for IPv6 Customer Edge Routers

[19] RFC 8200 Internet Protocol, Version 6 (IPv6) Specification

[20] RFC 8415 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

[21] USG IPv6 Profile，https://www.nist.gov/document-16884

[22] IPv6 Ready Logo Program, https://www.ipv6ready.org

[23] RIPE554，https://www.nist.gov/document-16884

[24] 政府採購 IPv6 資通設備與軟體規範建議書，http://interop.ipv6.org.tw/pdf/TaiwanIPv6ProfileV301201202.pdf

[25] 台灣銀行共同供應契約 LP-108019，https://www.bot.com.tw/Procurement/Procure_supply/Supply_index/Documents/108/LP5-108019/procure_Cmsup_Spec_pc108019_001.htm

[26] 台灣銀行共同供應契約 LP-107003，https://www.bot.com.tw/Procurement/Procure_supply/Supply_index/Documents/107/LP5-107003/procure_Cmsup_Spec_pc107003_001.htm

[27] 台灣銀行共同供應契約 LP-107003，https://www.bot.com.tw/Procurement/Procure_supply/Supply_index/Documents/101/LP5-101018/LP5_101018_1011201_002.htm

中英專有名詞對照

C

CPE 用戶終端設備(Customer Premise Equipment)

D

DAD 重複位址檢測(Duplicate Address Detection)

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

DNS 網域名稱伺服器(Domain Name System, DNS)

Dual Stack IPv4/ IPv6 雙協定 (Dual Stack)

F

FTTx 光世代網(Fiber To The x, FTTx)

G

Gateway 閘道器(Gateway)

H

HG 家庭網路閘道器 (Home Gateway)

I

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

IoT 物聯網 Internet of Things, IoT)

IP 網際網路協議(Internet Protocol, IP)

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

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

IPv4/v6 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)

IPv6 Ready Logo 網際網路通訊協定第六版認證獎章(IPv6 Ready Logo)

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

L

LAN 區域網路(Local Area Network)

N

NAT 網路位址轉譯(Network Address Translation, NAT)

P

PPPoE 網路對等協定 (Point-to-Point Protocol Over Ethernet)

R

RDNSS 路由廣播帶 DNS 資訊 (Router Advertisement Option for DNS Configuration)

Router 路由器(Router)

S

SLAAC 無狀態位址自動設定(Stateless Auto-configuration)

T

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

W

WAN 廣域網路(Wide Area Network)

附件一、寬頻分享器相關 RFC 規範

國立中央大學 National Central University

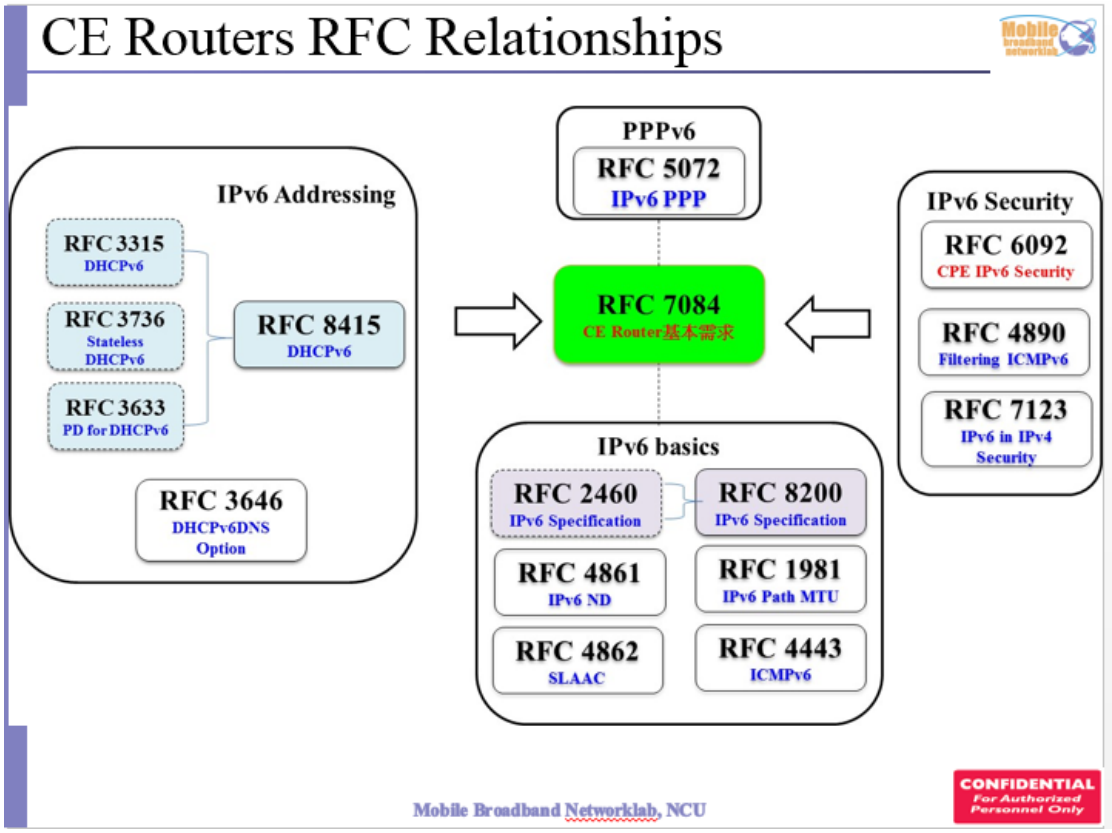
IPv6寬頻分享器互通測試項目研究及IASP實際測試平台建置

IPv6寬頻分享器製造商開發規範

周立德

國立中央大學主任秘書

國立中央大學資訊工程學系特聘教授



RFC 7084
Basic Requirements for IPv6 Customer Edge Routers

周立德

國立中央大學主任秘書

國立中央大學資訊工程學系特聘教授

2019

3

General Requirements

General Requirements		
ID	Requirements	需求
G-1	An IPv6 CE router is an IPv6 node according to the IPv6 Node Requirements specification [RFC6434].	根據[RFC6434]定義，IPv6 CE Router亦是IPv6節點
G-2	The IPv6 CE router MUST implement ICMPv6 according to [RFC4443]. In particular, point-to-point links MUST be handled as described in Section 3.1 of [RFC4443]	IPv6 CE router必須根據[RFC4443]實作ICMPv6
G-3	The IPv6 CE router MUST NOT forward any IPv6 traffic between its LAN interface(s) and its WAN interface until the router has successfully completed the IPv6 address and the delegated prefix acquisition process	IPv6 CE Router不可在LAN及WAN介面之間轉送任何IPv6流量，直到Router完成IPv6位址與Prefix delegation程序
G-4	By default, an IPv6 CE router that has no default router(s) on its WAN interface MUST NOT advertise itself as an IPv6 default router on its LAN interfaces. That is, the "Router Lifetime" field is set to zero in all Router Advertisement messages it originates [RFC4861].	預設情況下，IPv6 CE Router WAN介面沒有預設路由的情況下，不可在其LAN介面發送RA封包 ➢ RA的Router Lifetime必須設定為0
G-5	By default, if the IPv6 CE router is an advertising router and loses its IPv6 default router(s) and/or detects loss of connectivity on the WAN interface, it MUST explicitly invalidate itself as an IPv6 default router on each of its advertising interfaces by immediately transmitting one or more Router Advertisement messages with the "Router Lifetime" field set to zero [RFC4861].	當IPv6 CE Router是advertising router且WAN端路由連線中斷時，必須透過RA機制通告其LAN端的用戶 ➢ RA的Router Lifetime必須設定為0

CONFIDENTIAL For Authorized Personnel Only

WAN-Side Configuration

WAN-Side Configuration- WAN-Side requirements

ID	Requirements	需求
W-1	When the router is attached to the WAN interface link, it MUST act as an IPv6 host for the purposes of stateless [RFC4862] or stateful [RFC3315] interface address assignment.	當Router連接到WAN Interface鏈路時，它必須充當IPv6主機，以實現stateless [RFC4862]或stateful [RFC3315] Interface位址分配
W-2	The IPv6 CE router MUST generate a link-local address and finish Duplicate Address Detection according to [RFC4862] prior to sending any Router Solicitations on the interface. The source address used in the subsequent Router Solicitation MUST be the link-local address on the WAN interface.	➢ IPv6 CE Router必須生成link-local位址，並根據[RFC4862]在Interface完成重複位址檢測以及Router Solicitations ➢ Router Solicitation中使用的來源位址必須是WAN Interface上的link-local位址
W-3	Absent other routing information, the IPv6 CE router MUST use Router Discovery as specified in [RFC4861] to discover a default router(s) and install a default route(s) in its routing table with the discovered router's address as the next hop.	如果沒有其他路由資訊，IPv6 CE Router必須使用[RFC4861]中規定的Router Discovery來尋找default router(s) ➢ 將發現的Router位址作為next hop，並更新路由表預設路由
W-4	The router MUST act as a requesting router for the purposes of DHCPv6 prefix delegation ([RFC3633]).	Router必須充當requesting router以實現DHCPv6 Prefix委派（[RFC3633]）
W-5	The IPv6 CE router MUST use a persistent DHCP Unique Identifier (DUID) for DHCPv6 messages. The DUID MUST NOT change between network-interface resets or IPv6 CE router reboots.	➢ IPv6 CE Router必須支援persistent DHCP Unique Identifier (DUID) ➢ DUID不得在網路介面重置或IPv6 CE Router重啟之間切換

For Authorized Personnel Only

WAN-Side Configuration

WAN-Side Configuration- WAN-Side requirements

ID	Requirements	需求
W-6	W-6: The WAN interface of the CE router SHOULD support a Port Control Protocol (PCP) client as specified in [RFC6887] for use by applications on the CE router. The PCP client SHOULD follow the procedure specified in Section 8.1 of [RFC6887] to discover its PCP server. This document takes no position on whether such functionality is enabled by default or mechanisms by which users would configure the functionality. Handling PCP requests from PCP clients in the LAN side of the CE router is out of scope.	CE Router的WAN Interface應該支持[RFC6887]中規定的Port Control Protocol (PCP)客戶端協議

CONFIDENTIAL For Authorized Personnel Only

WAN-Side Configuration

WAN-Side Configuration- Link-layer requirements		
ID	Requirements	需求
WLL-1	WLL-1: If the WAN interface supports Ethernet encapsulation, then the IPv6 CE router MUST support IPv6 over Ethernet [RFC2464].	如WAN Interface支援Ethernet encapsulation，則IPv6 CE Router必須符合[RFC2464]規範
WLL-2	WLL-2: If the WAN interface supports PPP encapsulation, the IPv6 CE router MUST support IPv6 over PPP [RFC5072].	如WAN Interface支援PPP encapsulation，則IPv6 CE Router必須符合[RFC5072]規範
WLL-3	WLL-3: If the WAN interface supports PPP encapsulation, in a dual-stack environment with IPCP and IPV6CP running over one PPP logical channel, the Network Control Protocols (NCPs) MUST be treated as independent of each other and start and terminate independently	如WAN Interface支援PPP encapsulation，在dual-stack環境中，IPCP和IPV6CP必須視為獨立的Network Control Protocols (NCPs)

CONFIDENTIAL For Authorized Personnel Only

WAN-Side Configuration

WAN-Side Configuration- Address assignment requirements		
ID	Requirements	需求
WAA-1	The IPv6 CE router MUST support Stateless Address Autoconfiguration (SLAAC) [RFC4862]	IPv6 CE router必須支援Stateless Address Autoconfiguration (SLAAC) [RFC4862]
WAA-2	The IPv6 CE router MUST follow the recommendations in Section 4 of [RFC5942], and in particular the handling of the L flag in the Router Advertisement Prefix Information option	IPv6 CE router必須遵循[RFC5942]規定，特別是針對RA Option L flag的處理
WAA-3	The IPv6 CE router MUST support DHCPv6 [RFC3315] client behavior	IPv6 CE router必須支援DHCPv6規範之客戶端行為[RFC3315]
WAA-4	The IPv6 CE router MUST be able to support the following DHCPv6 options: Identity Association for Non-temporary Address (IA_NA), Reconfigure Accept [RFC3315], and DNS_SERVERS [RFC3646]. The IPv6 CE router SHOULD be able to support the DNS Search List (DNSSL) option as specified in [RFC3646]	IPv6 CE Router必須支援DHCPv6 options： ➢ Identity Association for Non-temporary Address (IA_NA) ➢ Reconfigure Accept [RFC3315] ➢ DNS_SERVERS [RFC3646] IPv6 CE Router應支援DNS Search List (DNSSL) [RFC3646]

CONFIDENTIAL For Authorized Personnel Only

WAN-Side Configuration

WAN-Side Configuration- Address assignment requirements

ID	Requirements	需求
WAA-5	WAA-5: The IPv6 CE router SHOULD implement the Network Time Protocol (NTP) as specified in [RFC5905] to provide a time reference common to the service provider for other protocols, such as DHCPv6, to use. If the CE router implements NTP, it requests the NTP Server DHCPv6 option [RFC5908] and uses the received list of servers as primary time reference, unless explicitly configured otherwise. LAN side support of NTP is out of scope for this document.	IPv6 CE Router應實作[RFC5905]中規定的網路時間協議（NTP），以便為服務提供商提供其他協議（如DHCPv6）使用的時間參考。
WAA-6	WAA-6: If the IPv6 CE router receives a Router Advertisement message (described in [RFC4861]) with the M flag set to 1, the IPv6 CE router MUST do DHCPv6 address assignment (request an IA_NA option).	如果IPv6 CE Router收到 RA通告且M flag設置為1，則IPv6 CE Router必須執行DHCPv6位址分配
WAA-7	WAA-7: If the IPv6 CE router does not acquire a global IPv6 address(es) from either SLAAC or DHCPv6, then it MUST create a global IPv6 address(es) from its delegated prefix(es) and configure those on one of its internal virtual network interfaces, unless configured to require a global IPv6 address on the WAN interface.	如IPv6 CE Router沒有從SLAAC或DHCPv6獲取Global IPv6位址，則其必須從其delegated prefix(es創建一個Global IPv6位址，並在其中一個內部虛擬網路Interface配置，除非Global IPv6位址已配置在WAN Interface上

CONFIDENTIAL For Authorized Personnel Only

WAN-Side Configuration

WAN-Side Configuration- Address assignment requirements

ID	Requirements	需求
WAA-8	The CE router MUST support the SOL_MAX_RT option [RFC7083] and request the SOL_MAX_RT option in an Option Request Option (ORO).	CE Router必須支援SOL_MAX_RT Option [RFC7083]
WAA-9	As a router, the IPv6 CE router MUST follow the weak host (Weak End System) model [RFC1122]. When originating packets from an interface, it will use a source address from another one of its interfaces if the outgoing interface does not have an address of suitable scope	根據[RFC 1122]，IPv6 CE Router必須遵循弱點主機（弱端系統）模型[RFC1122]。當從 Interface發起封包時，如該 Interface沒有合適範圍的位址，則CE Router可使用另一個 Interface的來源位址
WAA-10	The IPv6 CE router SHOULD implement the Information Refresh Time option and associated client behavior as specified in [RFC4242].	IPv6 CE Router應該實現信息刷新時間選項和[RFC4242]中指定的相關客戶端行為

CONFIDENTIAL For Authorized Personnel Only

WAN-Side Configuration

WAN-Side Configuration- Prefix delegation requirements

ID	Requirements	需求
WPD-1	The IPv6 CE router MUST support DHCPv6 prefix delegation requesting router behavior as specified in [RFC3633] (Identity Association for Prefix Delegation (IA_PD) option).	根據[RFC3633]，IPv6 CE Router必須支援DHCPv6 prefix delegation（IA_PD option中指定的Router行為
WPD-2	The IPv6 CE router MAY indicate as a hint to the delegating router the size of the prefix it requires. If so, it MUST ask for a prefix large enough to assign one /64 for each of its interfaces, rounded up to the nearest nibble, and SHOULD be configurable to ask for more	IPv6 CE Router可向delegating router指示其所需的prefix大小。如果可行，則其必須要求一個足夠大的prefix，可為每個Interface分配一個/64
WPD-3	The IPv6 CE router MUST be prepared to accept a delegated prefix size different from what is given in the hint. If the delegated prefix is too small to address all of its interfaces, the IPv6 CE router SHOULD log a system management error. [RFC6177] covers the recommendations for service providers for prefix allocation sizes	IPv6 CE Router必須準備好接受大小不同的delegated prefix大小。如delegated prefix太小無法配置其所有Interface時，IPv6 CE Router應該記錄系統管理錯誤 ➢ [RFC6177]提供服務提供商對prefix分配大小的建議
WPD-4	By default, the IPv6 CE router MUST initiate DHCPv6 prefix delegation when either the M or O flags are set to 1 in a received Router Advertisement (RA) message. Behavior of the CE router to use DHCPv6 prefix delegation when the CE router has not received any RA or received an RA with the M and the O bits set to zero is out of scope for this document.	預設情況下，當收到的RA訊息中的M or O flags設置為1時，IPv6 CE Router必須啟動DHCPv6 prefix delegation

Personnel Only

WAN-Side Configuration

WAN-Side Configuration- Prefix delegation requirements

ID	Requirements	需求
WPD-5	Any packet received by the CE router with a destination address in the prefix(es) delegated to the CE router but not in the set of prefixes assigned by the CE router to the LAN must be dropped. In other words, the next hop for the prefix(es) delegated to the CE router should be the null destination. This is necessary to prevent forwarding loops when some addresses covered by the aggregate are not reachable [RFC4632]. (a) The IPv6 CE router SHOULD send an ICMPv6 Destination Unreachable message in accordance with Section 3.1 of [RFC4443] back to the source of the packet, if the packet is to be dropped due to this rule.	根據[RFC4632]，CE Router收到的任何封包目的為CE Router delegated prefix(es)但不屬於CE Router LAN端prefix包含的子集時，必須丟棄該封包 （a）根據[RFC4443] Section 3.1，如果由於封包因此規則必須丟棄，則IPv6 CE Router應發送ICMPv6 Destination Unreachable訊息給封包的來源位址
WPD-6	If the IPv6 CE router requests both an IA_NA and an IA_PD option in DHCPv6, it MUST accept an IA_PD option in DHCPv6 Advertise/Reply messages, even if the message does not contain any addresses, unless configured to only obtain its WAN IPv6 address via DHCPv6; see [DHCPv6-STATEFUL-ISSUES].	如IPv6 CE Router在DHCPv6同時請求IA_NA和IA_PD選項，它必須接受DHCPv6 Advertise/Reply訊息中的IA_PD選項，即使該訊息不包含任何位址

CONFIDENTIAL For Authorized Personnel Only

WAN-Side Configuration

WAN-Side Configuration- Prefix delegation requirements		
ID	Requirements	需求
WPD-7	By default, an IPv6 CE router MUST NOT initiate any dynamic routing protocol on its WAN interface.	預設情況下，IPv6 CE Router不可在其WAN Interface上啟動任何動態路由協議
WPD-8	The IPv6 CE router SHOULD support the [RFC6603] Prefix Exclude option.	根據[RFC6603]，IPv6 CE Router應支援Prefix Exclude option

CONFIDENTIAL For Authorized Personnel Only

LAN-Side Configuration

LAN-Side Configuration- ULA requirements		
ID	Requirements	需求
ULA-1	The IPv6 CE router SHOULD be capable of generating a ULA prefix [RFC4193]	根據[RFC4193]，IPv6 CE Router應可產生ULA prefix
ULA-2	An IPv6 CE router with a ULA prefix MUST maintain this prefix consistently across reboots	具有ULA prefix的IPv6 CE Router必須在重新啟動後仍維持此prefix
ULA-3	The value of the ULA prefix SHOULD be configurable	ULA Prefix的值應該是可配置的
ULA-4	By default, the IPv6 CE router MUST act as a site border router according to Section 4.3 of [RFC4193] and filter packets with local IPv6 source or destination addresses accordingly	根據[RFC4193] Section 4.3，在預設情況下，IPv6 CE Router必須充當site border router，並依IPv6來源或目的位址過濾IPv6封包
ULA-5	An IPv6 CE router MUST NOT advertise itself as a default router with a Router Lifetime greater than zero whenever all of its configured and delegated prefixes are ULA prefixes	如IPv6 CE Router配置和delegated prefixes都是ULA prefix，則IPv6 CE Router不可其自身default router（Router Lifetime大於零）

CONFIDENTIAL For Authorized Personnel Only

LAN-Side Configuration

LAN-Side Configuration- LAN requirements		
ID	Requirements	需求
L-1	The IPv6 CE router MUST support router behavior according to Neighbor Discovery for IPv6 [RFC4861].	根據[RFC4861]，IPv6 CE Router必須支援 Neighbor Discovery for IPv6
L-2	The IPv6 CE router MUST assign a separate /64 from its delegated prefix(es) (and ULA prefix if configured to provide ULA addressing) for each of its LAN interfaces	IPv6 CE Router必須為其每個LAN Interface分配一個單獨的/64由其被委託的delegated prefix(es)
L-3	An IPv6 CE router MUST advertise itself as a router for the delegated prefix(es) (and ULA prefix if configured to provide ULA addressing) using the "Route Information Option" specified in Section 2.3 of [RFC4191]. This advertisement is independent of having or not having IPv6 connectivity on the WAN interface	根據[RFC4191] Section 2.3，IPv6 CE Router必須透過Route Information Option通告其為delegated prefix 配置的 Router
L-4	An IPv6 CE router MUST NOT advertise itself as a default router with a Router Lifetime [RFC4861] greater than zero if it has no prefixes configured or delegated to it	如IPv6 CE Router沒有配置prefix或被委託，則其不可將自身通告為default router
L-5	The IPv6 CE router MUST make each LAN interface an advertising interface according to [RFC4861].	根據[RFC4861]，IPv6 CE Router的每個LAN Interface都必須發送RA

CONFIDENTIAL For Authorized Personnel Only

LAN-Side Configuration

LAN-Side Configuration- LAN requirements		
ID	Requirements	需求
L-6	In Router Advertisement messages ([RFC4861]), the Prefix Information option's A and L flags MUST be set to 1 by default	預設情況下，RA通告訊息中的A and L flags必須設為1
L-7	The A and L flags' ([RFC4861]) settings SHOULD be user configurable.	A and L flags（[RFC4861]）應可由用戶自行配置
L-8	The IPv6 CE router MUST support a DHCPv6 server capable of IPv6 address assignment according to [RFC3315] OR a stateless DHCPv6 server according to [RFC3736] on its LAN interfaces.	IPv6 CE Router必須根據[RFC3315]規範支援IPv6位址分配的DHCPv6 server，或根據[RFC3736]規範支援LAN Interface上的[stateless DHCPv6 server功能。
L-9	Unless the IPv6 CE router is configured to support the DHCPv6 IA_NA option, it SHOULD set the M flag to zero and the O flag to 1 in its Router Advertisement messages [RFC4861].	除非IPv6 CE Router配置為支援DHCPv6 IA_NA option，否則應在其RA通告訊息[RFC4861]中將M flag設置為零並將O flag設置為1
L-10	The IPv6 CE router MUST support providing DNS information in the DHCPv6 DNS_SERVERS and DOMAIN_LIST options [RFC3646].	IPv6 CE Router必須支援在DHCPv6 DNS_SERVERS以及和DOMAIN_LIST options中提供DNS資訊 如[RFC3646]規範建議

CONFIDENTIAL For Authorized Personnel Only

LAN-Side Configuration

LAN-Side Configuration- LAN requirements

ID	Requirements	需求
L-11	The IPv6 CE router MUST support providing DNS information in the Router Advertisement Recursive DNS Server RDNSS and DNS Search List options. Both options are specified in [RFC6106]	IPv6 CE Router必須支援可在RA中提供DNS資訊（Recursive DNS Server RDNSS和DNS Search List options）如[RFC6106]規範建議
L-12	The IPv6 CE router SHOULD make available a subset of DHCPv6 options (as listed in Section 5.3 of [RFC3736]) received from the DHCPv6 client on its WAN interface to its LAN-side DHCPv6 server	IPv6 CE Router應可於WAN Interface上的DHCPv6客戶端接收到其配置給LAN端的DHCPv6 options（如[RFC3736] Section 5.3規範）
L-13	If the delegated prefix changes, i.e., the current prefix is replaced with a new prefix without any overlapping time period, then the IPv6 CE router MUST immediately advertise the old prefix with a Preferred Lifetime of zero and a Valid Lifetime of either a) zero or b) the lower of the current Valid Lifetime and two hours (which must be decremented in real time) in a Router Advertisement message as described in Section 5.5.3, (e) of [RFC4862]	如delegated prefix發生變化，則IPv6 CE Router必須立即通告舊的prefix其Preferred Lifetime為零，以及Valid Lifetime為a）零或b）當前Valid Lifetime和兩小時內接收到RA訊息中的較低者
L-14	The IPv6 CE router MUST send an ICMPv6 Destination Unreachable message, code 5 (Source address failed ingress/egress policy) for packets forwarded to it that use an address from a prefix that has been invalidated	IPv6 CE Router必須傳送ICMPv6 Destination Unreachable message, code 5 (Source address failed ingress/egress policy轉發給其封包使用來自已無效的prefix。

CONFIDENTIAL For Authorized Personnel Only

Transition Technologies Support

Transition Technologies Support – 6rd

ID	Requirements	需求
6RD-1	The IPv6 CE router MUST support 6rd configuration via the 6rd DHCPv4 Option 212. If the CE router has obtained an IPv4 network address through some other means such as PPP, it SHOULD use the DHCPINFORM request message [RFC2131] to request the 6rd DHCPv4 Option. The IPv6 CE router MAY use other mechanisms to configure 6rd parameters. Such mechanisms are outside the scope of this document.	IPv6 CE Router必須透過6rd DHCPv4 Option 212來配置6rd，如CE Router透過PPP等其他方式獲得IPv4網路位址，則其應使用DHCPINFORM請求訊息[RFC2131]來獲得6rd DHCPv4 Option
6RD-2	If the IPv6 CE router is capable of automated configuration of IPv4 through IPCP (i.e., over a PPP connection), it MUST support user-entered configuration of 6rd.	如IPv6 CE Router能夠透過IPCP自動配置IPv4（例如PPP連接），則其必須支援user-entered的6rd配置
6RD-3	If the CE router supports configuration mechanisms other than the 6rd DHCPv4 Option 212 (user-entered, TR-069 [TR-069], etc.), the CE router MUST support 6rd in "hub and spoke" mode. 6rd in "hub and spoke" requires all IPv6 traffic to go to the 6rd Border Relay. In effect, this requirement removes the "direct connect to 6rd" route defined in Section 7.1.1 of [RFC5969].	如CE Router支援6rd DHCPv4 Option 212以外的選項（user-entered, TR-069 [TR-069], etc.），則CE Router必須支持 “hub and spoke”模式

CONFIDENTIAL For Authorized Personnel Only

Transition Technologies Support

Transition Technologies Support – 6rd		
ID	Requirements	需求
6RD-4	A CE router MUST allow 6rd and native IPv6 WAN interfaces to be active alone as well as simultaneously in order to support coexistence of the two technologies during an incremental migration period such as a migration from 6rd to native IPv6	CE Router必須允許單獨和同時啟懂6rd或native IPv6 WAN Interface
6RD-5	Each packet sent on a 6rd or native WAN interface MUST be directed such that its source IP address is derived from the delegated prefix associated with the particular interface from which the packet is being sent (Section 4.3 of [RFC3704])	在6rd或native IPv6 WAN Interface上發送的每個封包，其來源IP位址需由發送封包的特定Interface相關聯的delegated prefix來配置的（[RFC3704]的第4.3節）
6RD-6	The CE router MUST allow different as well as identical delegated prefixes to be configured via each (6rd or native) WAN interface	CE Router必須允許每個（6rd或native IPv6）WAN Interface配置不同的以及相同的delegated prefixes
6RD-7	In the event that forwarding rules produce a tie between 6rd and native IPv6, by default, the IPv6 CE router MUST prefer native IPv6	如同時有6rd和native IPv6轉發規則，則預設情況下IPv6 CE Router必須優先選擇native IPv6

CONFIDENTIAL For Authorized Personnel Only

Transition Technologies Support

Transition Technologies Support – Dual-Stack Lite (DS-Lite)		
ID	Requirements	需求
DLW-1	DLW-1: The CE router MUST support configuration of DS-Lite via the DS-Lite DHCPv6 option [RFC6334]. The IPv6 CE router MAY use other mechanisms to configure DS-Lite parameters. Such mechanisms are outside the scope of this document.	CE Router必須支援[RFC6334]規範之DS-Lite DHCPv6選項。IPv6 CE Router亦可以使用其他機制來配置DS-Lite參數
DLW-2	DLW-2: The IPv6 CE router MUST NOT perform IPv4 Network Address Translation (NAT) on IPv4 traffic encapsulated using DS-Lite	IPv6 CE Router不可使用DS-Lite技術針對IPv4訊務進行IPv4網路位址轉換（NAT）
DLW-3	DLW-3: If the IPv6 CE router is configured with an IPv4 address on its WAN interface, then the IPv6 CE router SHOULD disable the DS-Lite Basic Bridging BroadBand (B4) element	如IPv6 CE Router的WAN Interface配置IPv4位址，則IPv6 CE Router應該禁用DS-Lite Basic Bridging BroadBand（B4）element

CONFIDENTIAL For Authorized Personnel Only

Security requirements

Security requirements		
ID	Requirements	需求
S-1	S-1: The IPv6 CE router SHOULD support [RFC6092]. In particular, the IPv6 CE router SHOULD support functionality sufficient for implementing the set of recommendations in [RFC6092], Section 4. This document takes no position on whether such functionality is enabled by default or mechanisms by which users would configure it.	IPv6 CE Router應支援[RFC6092]。特別是[RFC6092] Section 4 規範建議 第4節中實現建議集的功能。該文檔沒有對默認情況下是否啟用此類功能或用戶配置它的機制採取任何立場。
S-2	The IPv6 CE router SHOULD support ingress filtering in accordance with BCP 38 [RFC2827]. Note that this requirement was downgraded from a MUST from RFC 6204 due to the difficulty of implementation in the CE router and the feature's redundancy with upstream router ingress filtering.	IPv6 CE Router應支援BCP38 [RFC2827] ingress filtering的規範建議
S-3	If the IPv6 CE router firewall is configured to filter incoming tunneled data, the firewall SHOULD provide the capability to filter decapsulated packets from a tunnel	如IPv6 CE Router防火牆配置為可過濾tunnel技術封裝之資料，則防火牆應提供過濾來自tunnel解封裝封包的功能

21

CONFIDENTIAL
For Authorized Personnel Only



22

國立中央大學 National Central University

RFC 5072
IP Version 6 over PPP

周立德
國立中央大學主任秘書
國立中央大學資訊工程學系特聘教授
2019

23

Introduction (介紹)

Introduction（介紹）	
In order to establish communications over a point-to-point link, each end of the PPP link must first send LCP packets to configure and test the data link.	為了通過點對點連結建立通訊，PPP連結的每一端必須首先發送LCP封包以配置和測試資料連結。
After the link has been established and optional facilities have been negotiated as needed by the LCP, PPP must send NCP packets to choose and configure one or more network-layer protocols.	在建立連結且LCP協商optional facilities後PPP必須發送NCP封包，以選擇和配置一個或多個網絡層協議。
Only Codes 1 through 7 (Configure-Request, Configure-Ack, Configure-Nak, Configure-Reject, Terminate-Request, Terminate-Ack and Code-Reject) are used for the IPv6 Control Protocol. Other Codes should be treated as unrecognized and should result in Code-Rejects.	只有Code 1到7（Configure-Request，Configure-Ack，Configure-Nak，Configure-Reject，Terminate-Request，Terminate-Ack和Code-Reject）用於IPv6控制協議。其他代碼應該被視為未識別，並應該導致Code-Rejects。

CONFIDENTIAL For Authorized Personnel Only

Sending IPv6 Datagrams

Sending IPv6 Datagrams	
Before any IPv6 packets may be communicated, PPP MUST reach the network-layer protocol phase, and the IPv6 Control Protocol MUST reach the Opened state.	在傳送IPv6封包之前，PPP必須達到網絡層協議階段，並且IPv6控制協議必須為Opened狀態。
PPP links supporting IPv6 MUST allow the information field to be at least as large as the minimum link MTU size required for IPv6.	支援IPv6的PPP連結的資訊欄位必須至少與IPv6最小的連結MTU大小一樣。

CONFIDENTIAL For Authorized Personnel Only

Interface Identifier (介面識別)

Interface Identifier (介面識別)	
A Configure-Request MUST contain exactly one instance of the interface-identifier option.	Configure-Request必須包含僅一個interface-identifier選項的實例。
The interface identifier MUST be unique within the PPP link. i.e., upon completion of the negotiation, different interface-identifier values are to be selected for the ends of the PPP link	介面識別必須在PPP連結中是唯一的，例如在完成協談(negotiation)後，將會為PPP連結的端點選擇不同的介面識別碼。
If an IEEE global identifier is not available, a different source of uniqueness should be used. Suggested sources of uniqueness include link-layer addresses, machine serial numbers, et cetera. In this case, the "u" bit of the interface identifier MUST be set to zero (0).	如果IEEE全域識別不可用，則應該使用不同辨別唯一性的方式。建議的方式包括使用連結層地址，機器序列號等。在此情況下，介面識別的“u”位元必須設置為零（0）。

CONFIDENTIAL For Authorized Personnel Only

Interface Identifier (介面識別)

Interface Identifier (介面識別)	
If a good source of uniqueness cannot be found, it is recommended that a random number be generated. In this case, the "u" bit of the interface identifier MUST be set to zero (0).	如果找不到良好的識別唯一性方式，建議生成隨機亂數。在這種情況下，介面識別的“u”位元必須設置為零（0）。
If the two interface identifiers are different and the received interface identifier is not zero, the interface identifier MUST be acknowledged, i.e., a Configure-Ack is sent with the requested interface identifier, meaning that the responding peer agrees with the interface identifier requested.	如果兩個介面識別不同且接收的介面識別不為零，則介面識別碼必須被確認，即發送帶有請求的介面識別的Configure-Ack，代表同意對方所請求的介面識別。
If the two interface identifiers are equal and are not zero, Configure-Nak MUST be sent specifying a different non-zero interface-identifier value suggested for use by the remote peer.	如果兩個介面識別相同且不為零，則必須發送Configure-Nak，以提供對方使用不同非零的介面識別值。

CONFIDENTIAL For Authorized Personnel Only

Interface Identifier (介面識別)

Interface Identifier (介面識別)	
If the two interface identifiers are equal to zero, the interface identifier's negotiation MUST be terminated by transmitting the Configure-Reject with the interface-identifier value set to zero.	如果兩個介面識別碼等於零，則必須發送Configure-Reject並將介面識別碼設置為零來結束介面識別的協商。
A new Configure-Request MUST NOT contain the interface-identifier option if a valid Interface-Identifier Configure-Reject is received.	如果收到有效的介面識別 Configure-Reject 則新的 Configure-Request 不能包含 interface-identifie選項。
When Reception of a Configure-Nak with a suggested interface identifier is different from that of the last Configure-Nak sent to the peer, a new Configure-Request MUST be sent with the identifier value suggested in the last Configure-Nak from the peer.	當建議的介面識別碼接收到的Configure-Nak與發送給對方最後一個Configure-Nak不同時，必須發送新的Configure-Request其含有來自對方最後一個Configure-Nak中建議的識別碼。

CONFIDENTIAL For Authorized Personnel Only

Interface Identifier (介面識別)

Interface Identifier (介面識別)	
If an IEEE global identifier (EUI-48 or EUI-64) is available anywhere on the node, it should be used to construct the tentative interface identifier due to its uniqueness properties. When extracting an IEEE global identifier from another device on the node, care should be taken that the extracted identifier is presented in canonical ordering.	如果節點上任何地方都可以使用IEEE全局識別（EUI-48或EUI-64），則應該使用它來構造臨時介面識別碼，因為它具有唯一性性。當從節點上的另一設備提取IEEE全局介面識別碼時，應該注意提取的identifier以規範順序呈現。
If an IEEE global identifier is not available, a different source of uniqueness should be used. Suggested sources of uniqueness include link-layer addresses, machine serial numbers, et cetera.	如果IEEE全局識別不可用，則應該使用不同的識別唯一性方法。建議的方法包括連結層地址，機器序列號等。

CONFIDENTIAL For Authorized Personnel Only

Interface Identifier (介面識別)

Interface Identifier (介面識別)	
A new Configure-Request SHOULD NOT be sent to the peer until a Configure-Nak is received or the Restart timer runs out.	新的配置請求不應該發送到對方，直到接收到Configure-Nak或者重新啟動計時器用完為止。
If the received interface identifier is equal to the one sent in the last Configure-Nak, a new interface identifier MUST be chosen. In this case, a new Configure- Request SHOULD be sent with the new tentative interface identifier.	如果接收到的介面識別碼等於最後一個Configure-Nak中發送的介面識別碼，則必須選擇新的介面識別碼。在這種情況下，應該使用新的臨時介面識別碼發送新的Configure-Request。

CONFIDENTIAL For Authorized Personnel Only

Interface Identifier (介面識別)

Interface Identifier (介面識別)	
If negotiation of the interface identifier is required, and the peer did not provide the option in its Configure-Request, the option SHOULD be appended to a Configure-Nak. The tentative value of the interface identifier given must be acceptable as the remote interface identifier; i.e., it should be different from the identifier value selected for the local end of the PPP link. The next Configure- Request from the peer may include this option. If the next Configure-Request does not include this option, the peer MUST NOT send another Configure-Nak with this option included. It should assume that the peer's implementation does not support this option.	如果需要協商介面識別碼，並且對方未在其Configure-Request中提供該選項，則該選項應該附加到Configure-Nak。給定的介面識別暫定值必須是可接受的遠程接介面識別碼;即，其應該與PPP連結的本地端選擇的介面識別值不同。來自對方的下一個配置請求可以包括該選項。如果下一個Configure-Request不包含此選項，則對方不能發送包含此選項的另一個Configure-Nak，應該假設對方的實現不支持此選項

CONFIDENTIAL For Authorized Personnel Only

Stateless Autoconfiguration and Link-Local Addresses (無狀態自動配置和鏈路本地地址)

Stateless Autoconfiguration and Link-Local Addresses(無狀態自動配置和鏈路本地地址)	
The negotiated interface identifier is used by the local end of the PPP link to autoconfigure an IPv6 link-local unicast address for the PPP interface. However, it SHOULD NOT be assumed that the same interface identifier is used in configuring global unicast addresses for the PPP interface using IPv6 stateless address autoconfiguration。	PPP連結的本地端使用協商的介面識別碼來自動配置PPP介面的IPv6連結本地單播地址。但是，不應該假設使用相同的介面識別碼來配置使用IPv6無狀態地址自動配置PPP介面的全域單播地址。

CONFIDENTIAL For Authorized Personnel Only



33

國立中央大學
National Central University

Mobile
broadband
networklab

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

周立德

國立中央大學主任秘書

國立中央大學資訊工程學系特聘教授

2019

34

Stateless Filters

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

CONFIDENTIAL For Authorized Personnel Only

Stateless Filters

Connection-Free Filters - Stateless Filters		
ID	Requirements	需求
REC-4	REC-4: Packets bearing deprecated extension headers prior to their first upper-layer-protocol header SHOULD NOT be forwarded or transmitted on any interface. In particular, all packets with routing extension header type 0 [RFC2460] preceding the first upper- layer-protocol header MUST NOT be forwarded. See [RFC5095] for additional background.	在第一個上層協議頭之前帶有已棄用的擴展標頭的封包不應該在任何介面上轉送或傳輸。 routing extension header type 0不可轉送
REC-5	REC-5: Outbound packets MUST NOT be forwarded if the source address in their outer IPv6 header does not have a unicast prefix configured for use by globally reachable nodes on the interior network.	如外部IPv6標頭中的來源位址沒有配置為由內部網路上的globally reachable nodes使用的unicast prefix，則不可轉送outbound封包。
REC-6	REC-6: Inbound packets MUST NOT be forwarded if the source address in their outer IPv6 header has a global unicast prefix assigned for use by globally reachable nodes on the interior network.	如外部IPv6標頭中的來源位址具有分配給內部網路上的global unicast prefix，則不可轉送inbound封包。
RFC-7	REC-7: By DEFAULT, packets with unique local source and/or destination addresses [RFC4193] SHOULD NOT be forwarded to or from the exterior network.	在預設的情況下，具有unique local source和/或destination addresses [RFC4193]的封包不應轉送到外部網路或從外部網路轉送
RFC-8	REC-8: By DEFAULT, inbound DNS queries received on exterior interfaces MUST NOT be processed by any integrated DNS resolving server.	在預設的情況下，外部介面上收到的inbound DNS查詢不可由任何integrated DNS 解析服務器處理。
REC-9	REC-9: Inbound DHCPv6 discovery packets [RFC3315] received on exterior interfaces MUST NOT be processed by any integrated DHCPv6 server or relay agent.	在外部介面上接收的inbound DHCPv6發現封包[RFC3315]不可由任何integrated DHCPv6 server 或 relay agent處理。

Connection-Free Filters

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

37

Mobile Broadband Networklab, NCU

CONFIDENTIAL For Authorized Personnel Only

Connection-Free Filters

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

38

Connection-Free Filters

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

CONFIDENTIAL For Authorized Personnel Only

Connection-Free Filters

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

For Authorized Personnel Only

Connection-Free Filters

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

CONFIDENTIAL For Authorized Personnel Only

Connection-Free Filters

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

CONFIDENTIAL For Authorized Personnel Only

Connection-Free Filters

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

CONFIDENTIAL For Authorized Personnel Only

Connection-Free Filters

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

CONFIDENTIAL For Authorized Personnel Only

Connection-Oriented Filters

Connection-Oriented Filters - TCP Filters

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

For Authorized Personnel Only

Connection-Oriented Filters

Connection-Oriented Filters - TCP Filters

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

For Authorized Personnel Only

Connection-Oriented Filters

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

For Authorized Personnel Only

Connection-Oriented Filters

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

CONFIDENTIAL For Authorized Personnel Only

Connection-Oriented Filters

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

CONFIDENTIAL For Authorized Personnel Only

Connection-Oriented Filters

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

CONFIDENTIAL For Authorized Personnel Only

Passive Listeners

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

CONFIDENTIAL For Authorized Personnel Only

Management Applications

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

CONFIDENTIAL For Authorized Personnel Only



53

國立中央大學
National Central University

Mobile
broadband
networklab

RFC 4890
Recommendations for Filtering ICMPv6 Messages in Firewalls

周立德

國立中央大學主任秘書

國立中央大學資訊工程學系特聘教授

2019

54

Recommendations for ICMPv6 Transit Traffic

Traffic That Must Not Be Dropped		
ID	Requirements	需求
	Error messages that are essential to the establishment and maintenance of communications: ➢ Destination Unreachable (Type 1) - All codes ➢ Packet Too Big (Type 2) ➢ Time Exceeded (Type 3) - Code 0 only o Parameter Problem (Type 4) - Codes 1 and 2 only	對通信建立和維護至關重要的錯誤消息 ➢ Destination Unreachable (Type 1) - All codes ➢ Packet Too Big (Type 2) ➢ Time Exceeded (Type 3) - Code 0 only o Parameter Problem (Type 4) - Codes 1 and 2 only
	Connectivity checking messages: ➢ Echo Request (Type 128) ➢ Echo Response (Type 129)	連通性的檢查訊息 ➢ Echo Request (Type 128) ➢ Echo Response (Type 129)

CONFIDENTIAL For Authorized Personnel Only

Recommendations for ICMPv6 Transit Traffic

Traffic That Normally Should Not Be Dropped		
ID	Requirements	需求
	Error messages ➢ Time Exceeded (Type 3) - Code 1 ➢ Parameter Problem (Type 4) - Code 0	錯誤訊息 ➢ Time Exceeded (Type 3) - Code 1 ➢ Parameter Problem (Type 4) - Code 0
	Mobile IPv6 messages that are needed to assist mobility: ➢ Home Agent Address Discovery Request (Type 144) ➢ Home Agent Address Discovery Reply (Type 145) ➢ Mobile Prefix Solicitation (Type 146) ➢ Mobile Prefix Advertisement (Type 147)	協助移動性所需的移動IPv6訊息： ➢ Home Agent Address Discovery Request (Type 144) ➢ Home Agent Address Discovery Reply (Type 145) ➢ Mobile Prefix Solicitation (Type 146) ➢ Mobile Prefix Advertisement (Type 147)

CONFIDENTIAL For Authorized Personnel Only

Recommendations for ICMPv6 Transit Traffic

Traffic That Will Be Dropped Anyway -- No Special Attention Needed		
ID	Requirements	需求
	Address Configuration and Router Selection messages (must be received with hop limit = 255): ➢ Router Solicitation (Type 133) ➢ Router Advertisement (Type 134) ➢ Neighbor Solicitation (Type 135) ➢ Neighbor Advertisement (Type 136) ➢ Redirect (Type 137) ➢ Inverse Neighbor Discovery Solicitation (Type 141) ➢ Inverse Neighbor Discovery Advertisement (Type 142)	位址配置和路由器選擇訊息(hop limit = 255): ➢ Router Solicitation (Type 133) ➢ Router Advertisement (Type 134) ➢ Neighbor Solicitation (Type 135) ➢ Neighbor Advertisement (Type 136) ➢ Redirect (Type 137) ➢ Inverse Neighbor Discovery Solicitation (Type 141) ➢ Inverse Neighbor Discovery Advertisement (Type 142)
	Link-local multicast receiver notification messages (must have link- local source address): ➢ Listener Query (Type 130) ➢ Listener Report (Type 131) ➢ Listener Done (Type 132) ➢ Listener Report v2 (Type 143)	Link-local multicast receiver通知訊息（必須具有link- local source address） ➢ Listener Query (Type 130) ➢ Listener Report (Type 131) ➢ Listener Done (Type 132) ➢ Listener Report v2 (Type 143)
	SEND Certificate Path notification messages (must be received with hop limit = 255): ➢ Certificate Path Solicitation (Type 148) ➢ Certificate Path Advertisement (Type 149)	SEND Certificate Path通知訊息(hop limit = 255) ➢ Certificate Path Solicitation (Type 148) ➢ Certificate Path Advertisement (Type 149)

CONFIDENTIAL For Authorized Personnel Only

Recommendations for ICMPv6 Transit Traffic

Traffic That Will Be Dropped Anyway -- No Special Attention Needed		
ID	Requirements	需求
	Multicast Router Discovery messages (must have link-local source address and hop limit = 1): ➢ Multicast Router Advertisement (Type 151) ➢ Multicast Router Solicitation (Type 152) ➢ Multicast Router Termination (Type 153)	群播路由發現訊息(必須具備link-local source address 以及hop limit = 1) ➢ Multicast Router Advertisement (Type 151) ➢ Multicast Router Solicitation (Type 152) ➢ Multicast Router Termination (Type 153)

CONFIDENTIAL For Authorized Personnel Only

Recommendations for ICMPv6 Transit Traffic

Traffic for Which a Policy Should Be Defined		
ID	Requirements	需求
	End site administrators should determine if they need to support these experiments and otherwise messages of this type should be dropped: ➢ Seamoby Experimental (Type 150)	網站管理必須確認此類訊息是否需阻擋
	Error messages not currently defined by IANA: ➢ Unallocated Error messages (Types 5-99 inclusive and 102-126 inclusive)	IANA當前未定義的錯誤消息 ➢ Unallocated Error messages (Types 5-99 inclusive and 102-126 inclusive)
	All informational messages with types not explicitly assigned by IANA, currently: ➢ Unallocated Informational messages (Types 154-199 inclusive and 202-254 inclusive).	目前IANA未明確指定類型的所有訊息 ➢ Unallocated Informational messages (Types 154-199 inclusive and 202-254 inclusive).

CONFIDENTIAL For Authorized Personnel Only

Recommendations for ICMPv6 Transit Traffic

Traffic That Should Be Dropped Unless a Good Case Can Be Made		
ID	Requirements	需求
	Some of these messages will be using non- link-local unicast addresses so that they will not necessarily be dropped by address scope limiting rules: ➢ Node Information Query (Type 139) ➢ Node Information Response (Type 140)	某些訊息使用non- link-local unicast addresses，因此不一定會被位址範圍限制規則刪除： ➢ Node Information Query (Type 139) ➢ Node Information Response (Type 140)
	Messages with types in the experimental allocations: ➢ Types 100, 101, 200, and 201	實驗分配的訊息類型 ➢ Types 100, 101, 200, and 201
	Messages using the extension type numbers until such time as ICMPv6 needs to use such extensions: ➢ Types 127 and 255	使用擴展類型的訊息 ➢ Types 127 and 255

CONFIDENTIAL For Authorized Personnel Only

Recommendations for ICMPv6 Local Configuration Traffic

Traffic That Must Not Be Dropped

ID	Requirements	需求
	Error messages that are essential to the establishment and maintenance of communications: ➢ Destination Unreachable (Type 1) - All codes ➢ Packet Too Big (Type 2) ➢ Time Exceeded (Type 3) - Code 0 only ➢ Parameter Problem (Type 4) - Codes 1 and 2 only	對建立和維護通信至關重要的錯誤消息 ➢ Destination Unreachable (Type 1) - All codes ➢ Packet Too Big (Type 2) ➢ Time Exceeded (Type 3) - Code 0 only ➢ Parameter Problem (Type 4) - Codes 1 and 2 only
	Connectivity checking messages: ➢ Echo Request (Type 128) ➢ Echo Response (Type 129)	確認的連通性的訊息 ➢ Echo Request (Type 128) ➢ Echo Response (Type 129)
	Address Configuration and Router Selection messages: ➢ Router Solicitation (Type 133) ➢ Router Advertisement (Type 134) ➢ Neighbor Solicitation (Type 135) ➢ Neighbor Advertisement (Type 136) ➢ Inverse Neighbor Discovery Solicitation (Type 141) ➢ Inverse Neighbor Discovery Advertisement (Type 142)	位址配置和路由器選擇訊息： ➢ Router Solicitation (Type 133) ➢ Router Advertisement (Type 134) ➢ Neighbor Solicitation (Type 135) ➢ Neighbor Advertisement (Type 136) ➢ Inverse Neighbor Discovery Solicitation (Type 141) ➢ Inverse Neighbor Discovery Advertisement (Type 142)

CONFIDENTIAL For Authorized Personnel Only

Recommendations for ICMPv6 Local Configuration Traffic

Traffic That Must Not Be Dropped

ID	Requirements	需求
	Link-Local Multicast Receiver Notification messages: ➢ Listener Query (Type 130) ➢ Listener Report (Type 131) ➢ Listener Done (Type 132) ➢ Listener Report v2 (Type 143)	Link-Local Multicast Receiver通知訊息 ➢ Listener Query (Type 130) ➢ Listener Report (Type 131) ➢ Listener Done (Type 132) ➢ Listener Report v2 (Type 143)
	SEND Certificate Path Notification messages: ➢ Certificate Path Solicitation (Type 148) ➢ Certificate Path Advertisement (Type 149)	SEND Certificate Path通知訊息 ➢ Certificate Path Solicitation (Type 148) ➢ Certificate Path Advertisement (Type 149)
	Multicast Router Discovery messages: ➢ Multicast Router Advertisement (Type 151) ➢ Multicast Router Solicitation (Type 152) ➢ Multicast Router Termination (Type 153)	Multicast Router Discovery messages ➢ Multicast Router Advertisement (Type 151) ➢ Multicast Router Solicitation (Type 152) ➢ Multicast Router Termination (Type 153)

CONFIDENTIAL For Authorized Personnel Only

Recommendations for ICMPv6 Local Configuration Traffic

Traffic That Normally Should Not Be Dropped

ID	Requirements	需求
	Error messages ➢ Time Exceeded (Type 3) - Code 1 ➢ Parameter Problem (Type 4) - Code 0	錯誤訊息 ➢ Time Exceeded (Type 3) - Code 1 ➢ Parameter Problem (Type 4) - Code 0

CONFIDENTIAL For Authorized Personnel Only

Recommendations for ICMPv6 Local Configuration Traffic

Traffic That Will Be Dropped Anyway -- No Special Attention Needed

ID	Requirements	需求
	Router Renumbering messages must be authenticated using IPsec, so it is not essential to filter these messages even if they are not allowed at the firewall/router: ➢ Router Renumbering (Type 138)	路由器重新編號消息必須使用IPsec進行身份驗證，因此即使防火牆/路由器不允許這些消息也不必過濾 ➢ Router Renumbering (Type 138)
	Mobile IPv6 messages that are needed to assist mobility: ➢ Home Agent Address Discovery Request (Type 144) ➢ Home Agent Address Discovery Reply (Type 145) ➢ Mobile Prefix Solicitation (Type 146) ➢ Mobile Prefix Advertisement (Type 147)	協助移動性所需的mobile IPv6訊息： ➢ Home Agent Address Discovery Request (Type 144) ➢ Home Agent Address Discovery Reply (Type 145) ➢ Mobile Prefix Solicitation (Type 146) ➢ Mobile Prefix Advertisement (Type 147)
	The message used by the experimental Seamoby protocols may be dropped but will be ignored if the service is not implemented: ➢ Seamoby Experimental (Type 150)	實驗性Seamoby協議使用的訊息 ➢ Seamoby Experimental (Type 150)

CONFIDENTIAL For Authorized Personnel Only

Recommendations for ICMPv6 Local Configuration Traffic

Traffic for Which a Policy Should Be Defined

ID	Requirements	需求
	Redirect messages provide a significant security risk, and administrators should take a case-by-case approach to whether firewalls, routers in general, and other nodes should accept these messages: ➢ Redirect (Type 137)	管理員應該根據具體情況採取措施，確定防火牆，路由器和其他節點是否應接受這些訊息 ➢ Redirect (Type 137)
	If a node implements the experimental Node Information service, the administrator needs to make an explicit decision as to whether the node should respond to or accept Node Information messages on each interface: ➢ Node Information Query (Type 139) ➢ Node Information Response (Type 140)	管理員需要明確決定節點是否應回應或接受每個interface上的節點訊息 ➢ Node Information Query (Type 139) ➢ Node Information Response (Type 140)
	Error messages not currently defined by IANA: ➢ Unallocated Error messages (Types 5-99 inclusive and 102-126 inclusive)	IANA當前未定義的錯誤消息 ➢ Unallocated Error messages (Types 5-99 inclusive and 102-126 inclusive)

CONFIDENTIAL For Authorized Personnel Only

Recommendations for ICMPv6 Local Configuration Traffic

Traffic That Should Be Dropped Unless a Good Case Can Be Made

ID	Requirements	需求
	Messages with types in the experimental allocations: ➢ Types 100, 101, 200, and 201	實驗分配類型的訊息 ➢ Types 100, 101, 200, and 201
	Messages using the extension type numbers until such time as ICMPv6 needs to use such extensions: ➢ Types 127 and 255.	使用擴展類型的訊息 ➢ Types 127 and 255
	All informational messages with types not explicitly assigned by IANA, currently: ➢ Types 154-199 inclusive and 202-254 inclusive.	目前IANA未明確指定類型的所有訊息 ➢ Unallocated Informational messages (Types 154-199 inclusive and 202-254 inclusive)

CONFIDENTIAL For Authorized Personnel Only

RFC 4890 規範建議

		Must Not Drop		Should Not Drop	
類型	Message(Type)	Transit	Local	Transit	Local
通訊維護	Destination Unreachable (1) – All codes	V	V		
	Packet Too Big (2)	V	V		
	Time Exceeded (3) – Code 0 only	V	V		
	Parameter Problem (4) – Codes 1 and 2 only	V	V		
連通性	Echo Request (128)	V	V		
	Echo Response (129)	V	V		
位址配置與路由選擇	Router Solicitation (133)		V		
	Router Advertisement (134)		V		
	Neighbor Solicitation (135)		V		
	Neighbor Advertisement (136)		V		
	Inverse Neighbor Discovery Solicitation (141)		V		
	Inverse Neighbor Discovery Advertisement (142)		V		

CONFIDENTIAL
For Authorized Personnel Only

RFC 4890 規範建議

		Must Not Drop		Should Not Drop	
類型	Message(Type)	Transit	Local	Transit	Local
Link-local 群播通知	Listener Query (130)		V		
	Listener Report (131)		V		
	Listener Done (132)		V		
	Listener Report v2 (143)		V		
SEND Certification 路徑通知	Certification Path Solicitation (148)		V		
	Certification Path Advertisement (149)		V		
群播路由發現	Multicast Router Advertisement (151)		V		
	Multicast Router Solicitation (152)		V		
	Multicast Router Termination (153)		V		
錯誤訊息	Time Exceeded (3) – Code 1			V	V
	Parameter Problem (4) – Code 0			V	V
Mobile IPv6	Home Agent Address Discovery Request (144)			V	
	Home Agent Address Discovery Reply (145)			V	
	Mobile Prefix Solicitation (146)			V	
	Mobile Prefix Advertisement (147)			V	



69

國立中央大學
National Central University

Mobile
broadband
networklab

RFC 7123
Security Implications of IPv6 on IPv4 Networks

周立德
國立中央大學主任秘書
國立中央大學資訊工程學系特聘教授

2019

70

Security Implications of Tunneling Mechanisms

Security Implications of Tunneling Mechanisms

ID	Requirements	需求
1	➢ 6in4 tunnels can be blocked by blocking IPv4 packets with a Protocol field of 41. ➢ 6over4 encapsulates IPv6 packets in IPv4 packets with their Protocol field set to 41. ➢ 6rd can be blocked by blocking IPv4 packets with the Protocol field set to 41. ➢ ISATAP can be easily blocked by blocking IPv4 packets with a Protocol field of 41. ➢ Tunnel Broker data channel can be blocked by blocking UDP packets originated from the local network and destined to UDP port 3653, and IPv4 packets with a Protocol field set to 41 ➢ AYIYA can be blocked by blocking TCP and UDP packets originating from the local network and destined to UDP port 5072 or TCP port 5072.	➢ 限制Protocol field 41的IPv6封包可以限制6in4, 6over4, 6rd, ISATAP, Tunnel Broker等tunnel機制 ➢ 限制UDP port 3653可以限制Tunnel Broker ➢ 可以透過限制UDP port 5072或TCP port 5072的封包來限制AYIYA

CONFIDENTIAL For Authorized Personnel Only

Security Implications of Tunneling Mechanisms

Filtering 6to4

ID	Requirements	需求
1	If 6to4 traffic is meant to be filtered while other IPv6-in-IPv4 traffic is allowed, then more finer-grained filtering rules could be applied. For example, 6to4 traffic could be filtered by applying filtering rules such as: ➢ Filter outgoing IPv4 packets that have the Destination Address set to an address that belongs to the prefix 192.88.99.0/24. ➢ Filter incoming IPv4 packets that have the Source Address set to an address that belongs to the prefix 192.88.99.0/24. ➢ Filter outgoing IPv4 packets that have the Destination Address set to the IPv4 address of well-known 6to4 relays. ➢ Filter incoming IPv4 packets that have the Source Address set to the IPv4 address of well-known 6to4 relays.	如要在其他IPv6-in-IPv4流量允許的情況下過濾6to4流量，則可應用更細部的過濾規則 ➢ 過濾將目標位址設置為屬於prefix192.88.99.0/24的位址的外傳IPv4封包。 ➢ 過濾內送的IPv4封包，其來源位址設置為屬於prefix192.88.99.0/24的位址 ➢ 過濾將目標位址設置為已知的6to4中繼的IPv4位址的外傳IPv4封包 ➢ 過濾內送的IPv4封包，其來源位址設置為已知的6to4中繼的IPv4位址
2	If the filtering device has capabilities to inspect the payload of IPv4 packets, then the following filtering rules could be enforced: ➢ Filter outgoing IPv4 packets that have their Protocol field set to 41, and that have an IPv6 Source Address (embedded in the IPv4 payload) that belongs to the prefix 2002::/16. ➢ Filter incoming IPv4 packets that have their Protocol field set to 41, and that have an IPv6 Destination address (embedded in the IPv4 payload) that belongs to the prefix 2002::/16.	如過濾設備具有檢查IPv4封包payload的能力，則可以強制執行以下過濾規則： ➢ 過濾其Protocol field設置為41且具有屬於prefix 2002 :: / 16的IPv6源位址（嵌入在IPv4有效負載中）的外送IPv4封包 ➢ 過濾內送的IPv4封包，其Protocol field設置為41，並且具有屬於prefix 2002 :: / 16的IPv6目標位址（嵌入在IPv4有效負載中）

CONFIDENTIAL For Authorized Personnel Only

Security Implications of Tunneling Mechanisms

Filtering Teredo

ID	Requirements	需求
3	If the filtering device has capabilities to inspect the payload of IPv4 packets, the following (additional) filtering policy could be enforced: ➢ Filter outgoing IPv4/UDP packets that embed an IPv6 packet with the "Version" field set to 6, and an IPv6 Source Address that belongs to the prefix 2001::/32. ➢ Filter incoming IPv4/UDP packets that embed an IPv6 packet with the "Version" field set to 6, and an IPv6 Destination Address that belongs to the prefix 2001::/32.	如果過濾設備具有檢查IPv4封包payload的能力，則可以強制執行以下（附加）過濾策略： ➢ 過濾掉嵌入IPv6封包的IPv4 / UDP封包，其中Version欄位設置為6，IPv6來源地址屬於prefix 2001 :: / 32。 ➢ 過濾傳入的IPv4 / UDP封包，其中嵌入Version欄位設置為6的IPv6封包，以及屬於prefix 2001 :: / 32的IPv6目標地址。

73

CONFIDENTIAL
For Authorized Personnel Only



74

國立中央大學 National Central University

RFC 3315
Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

周立德

國立中央大學主任秘書

國立中央大學資訊工程學系特聘教授

2019

75

RFC 3315

- 目的
  - 說明DHCPv6的基本規範與功能，讓DHCP server傳送設定參數給網路節點，達到自動IP位址分配的效果。
- IPv6 名詞(1/2)
  - address：interface上IP layer的識別碼
  - host：不是router的node
  - IP：在本文中專指IPv6
  - interface：一個node與一個link的連接處
  - link：不同node間在link layer的通訊媒介
  - link-layer identifier：interface上link layer的識別碼
  - link-local address：在同個link中讓node可以互相通訊的address
  - multicast address：代表一個interface集合的識別碼。
  - neighbor：在同一個link上的node
  - node：實作IP的裝置

CONFIDENTIAL For Authorized Personnel Only

RFC 3315

- IPv6 名詞(2/2)
  - packet：IP的header加上payload
  - prefix：一個address的起始bits
  - prefix length：prefix中的bit數量
  - router：轉送沒有指明給自己的IP packet
  - unicast address：單一interface的識別碼
- DHCP名詞(1/2)
  - appropriate to the link：一個address符合server對網路拓樸認知
  - binding：一組包含Identity Association的address，或指派給client設定的server資料紀錄
  - Configuration parameter：server上設定資訊中的元素，並透過DHCP傳送給client
  - DHCP：DHCPv6
  - (DHCP) client：為了得到configuration parameter在link上發起請求的node
  - (DHCP) server：回應來自client的請求

CONFIDENTIAL For Authorized Personnel Only

RFC 3315

- DHCP名詞(2/2)
  - DHCP domain：一群由DHCP管理的link，由administrative entity操作
  - DHCP realm：用以識別administrative entity的名字
  - (DHCP) relay agent：在client和server中負責中繼傳輸DHCP訊息的node
  - DUID：DHCP Unique Identifier，每個DHCP中的node都要有的識別碼
  - Identity association (IA)：指派給一個client的address集合，每個IA都有一個IAID
  - identity association identifier (IAID)：由client選擇的唯一識別碼
  - identity association for non-temporary addresses (IA_NA)：夾帶要指派的address不是temporary address的IA
  - identity association for temporary addresses (IA_TA)：夾帶temporary address的IA
  - message：以UDP payload的方式被傳送的資料
  - reconfigure key：由server提供給client的key，用於提供reconfigure message的安全性
  - relaying：DHCP relay agent中繼傳輸DHCP訊息
  - transaction ID：用於匹配回應的數值

CONFIDENTIAL For Authorized Personnel Only

5. DHCP 基本名詞

Multicast Addresses	
All_DHCP_Relay_Agents_and_Servers (FF02::1:2) • A link-scoped multicast address used by a client to communicate with neighboring (i.e., on-link) relay agents and servers.	All_DHCP_Relay_Agents_and_Servers (FF02::1:2) • Client會透過此multicast address來和relay agents和server溝通
All_DHCP_Servers (FF05::1:3) • A site-scoped multicast address used by a relay agent to communicate with servers. • In order for a relay agent to use this address, it must have an address of sufficient scope to be reachable by the servers.	All_DHCP_Servers (FF05::1:3) • Relay Agent透過此multicast address和server溝通，因此Relay Agent必須在一定的scope內與server溝通

Mobile Broadband Networklab, NCU
CONFIDENTIAL For Authorized Personnel Only

7. Relay Agent/Server Message格式

兩種Relay Message	
Relay-forward Message: MUST include a "Relay Message option" (see Section 22.10).	Replay-forward Message: 必須加入"Relay Message option" (參考 section 22.10)
Relay-reply Message: MUST include a "Relay Message option" (see Section 22.10).	必須加入"Relay Message option" (參考 section 22.10)

Mobile Broadband Networklab, NCU
CONFIDENTIAL For Authorized Personnel Only

8. Domain Names 的表示與使用

Domain Names 的表示與使用	
Domain names may be encoded uniformly, a domain name or a list of domain names is encoded using the technique described in section 3.1 of [RFC1035].	可能會透過section 3.1中所提到的技術將domain names加密
A domain name, or list of domain names, in DHCP MUST NOT be stored in compressed form, as described in Section 4.1.4 of [RFC1035].	在DHCP中不能壓縮domain name，如section 4.14所述)

CONFIDENTIAL For Authorized Personnel Only

9. DHCP Unique Identifier (1/6)

DHCP Unique Identifier (DUID)	
Each DHCP client and server has a DUID.	每個DHCP client或DHCP server都要有個DUID
DHCP servers use DUIDs to identify clients for the selection of configuration parameters and in the association of IAs with clients.	DHCP server透過DUID來辨認client，以選擇設定參數，和IA與client的關聯
DHCP clients use DUIDs to identify a server in messages where a server needs to be identified.	DHCP client透過訊息中的DUID辨認server
Clients and servers MUST treat DUIDs as opaque values and MUST only compare DUIDs for equality.	clients和servers必須將DUID視為opaque value，且必須只將DUID用於比較異同
Clients and servers MUST NOT in any other way interpret DUIDs.	Clients和servers不能以其他形式解析DUID

CONFIDENTIAL For Authorized Personnel Only

9. DHCP Unique Identifier (2/6)

DHCP Unique Identifier (DUID)	
Clients and servers MUST NOT restrict DUIDs to the types defined in this document, as additional DUID types may be defined in the future.	Clients和server不能只將DUID限制於這份文件中所定義的型別，未來可能還會定義新的DUID型別
The DUID is carried in an option because it may be variable length and because it is not required in all DHCP messages.	DUID會放在option欄位，因為它的長度可能會變動，且不一定要出現在所有的DHCP訊息中
The DUID used by a client or server SHOULD NOT change over time.	clients和servers所使用的DUID不應該隨著時間變換
The DUID must be globally unique, and must also be easy to generate.	DUID必須是唯一的，且必須容易產生
Some devices may not contain any persistent storage, so the DUID scheme must accommodate such devices.	有些裝置可能沒有永久性的儲存空間，因此DUID的方案必須適應這些裝置

CONFIDENTIAL For Authorized Personnel Only

9. DHCP Unique Identifier (3/6)

DUID Based on Link-layer Address Plus Time (DUID-LLT)	
The hardware type MUST be a valid hardware type assigned by the IANA as described in [RFC826].	硬體型別必須是IANA規定在[RFC826]中的正當型別
The same DUID-LLT SHOULD be used in configuring all network interfaces connected to the device.	一樣的DUID-LLT應該用於設定該裝置上所有的網路interface
Clients and servers using this type of DUID MUST store the DUID-LLT in stable storage, and MUST continue to use this DUID-LLT even if the network interface used to generate the DUID-LLT is removed.	clients和servers必須將DUID-LLT存在穩定的儲存裝置中，且即使用於生產此DUID-TTL的interface已經從裝置上一除了，也必須持續使用該DUID-LLT
Clients and servers that do not have any stable storage MUST NOT use this type of DUID.	clients和servers若沒有穩定的儲存裝置，則不能使用這種類型的DUID

CONFIDENTIAL For Authorized Personnel Only

9. DHCP Unique Identifier (4/6)

DUID Based on Link-layer Address Plus Time (DUID-LLT)	
Clients and servers that use this DUID SHOULD attempt to configure the time prior to generating the DUID.	使用這種DUID的clients或servers應該在產生DUID前設定好時間
MUST use some sort of time source (for example, a real-time clock) in generating the DUID.	必須使用某種時間來源方式 (如現實時間) 來產生DUID
A DHCP client that generates a DUID-LLT using this mechanism MUST provide an administrative interface that replaces the existing DUID with a newly-generated DUID-LLT.	使用這種方式產生DUID的DHCP client必須提供一個管理介面，讓新的DUID-TTL可以取代現有的DUID

CONFIDENTIAL For Authorized Personnel Only

9. DHCP Unique Identifier (5/6)

DUID Assigned by Vendor Based on Enterprise Number (DUID-EN)	
Each identifier part of each DUID-EN MUST be unique to the device that is using it, and MUST be assigned to the device at the time it is manufactured and stored in some form of non-volatile storage.	每個DUID-EN中的identifier part必須在使用它的的裝置中是唯一的，且必須在裝置被製造時被指定，並存在穩定的儲存裝置中
The generated DUID SHOULD be recorded in non-erasable storage.	所產生的DUID應該被記錄在非揮發性的儲存裝置

CONFIDENTIAL For Authorized Personnel Only

9. DHCP Unique Identifier (6/6)

DUID Based on Link-layer Address (DUID-LL)	
The hardware type MUST be a valid hardware type assigned by the IANA, as described in [RFC826].	硬體型別必須是IANA規定在[RFC826]中的正當型別
The same DUID-LL SHOULD be used in configuring all network interfaces connected to the device.	一樣的DUID-LLT應該用於設定該裝置上所有的網路interface
DUID-LL MUST NOT be used by DHCP clients or servers that cannot tell whether or not a network interface is permanently attached to the device on which the DHCP client is running.	DHCP client或DHCP server若無法判別一個網路interface是否會永久在該裝置上，則不能使用DUID-LL

CONFIDENTIAL For Authorized Personnel Only

10. Identity Association (1/2)

Identity Association (IA)	
A construct through which a server and a client can identify, group, and manage a set of related IPv6 addresses.	IA是server和client可以透過一組互相關聯的IPv6 address識別、群組、和管理的結構
Each IA consists of an IAID and associated configuration information.	每個IA由IAID和相關的設定資訊組成
A client must associate at least one distinct IA with each of its network interfaces.	一個client的每個網路interface必須至少關聯一個IA
Each IA must be associated with exactly one interface.	每個IA必須剛好關聯一個interface

CONFIDENTIAL For Authorized Personnel Only

10. Identity Association (2/2)

Identity Association (IA)	
The IAID uniquely identifies the IA and must be chosen to be unique among the IAIDs on the client.	一個IAID可以代表一個IA且必須在client上的所有IAIDs中是唯一的
For any given use of an IA by the client, the IAID for that IA MUST be consistent across restarts of the DHCP client.	給client所使用的IA，其IAID必須在client重啟時仍保持一致
The client may maintain consistency either by storing the IAID in non-volatile storage or by using an algorithm that will consistently produce the same IAID.	Client可能會透過將IAID儲存在非揮發裝置中或是使用一套演算法可以產生相同的IAID

Mobile Broadband Networklab, NCU
CONFIDENTIAL For Authorized Personnel Only

11. 選擇給IA的位址

選擇給IA的位址	
Any address assigned by a server that is based on an EUI-64 identifier MUST include an interface identifier with the “u” (universal/local) and “g” (individual/group) bits of the interface identifier set appropriately, as indicated in Section 2.5.1 of [RFC 2373].	任何從server根據EUI-64識別碼所產生的address必須包含interface的識別碼，並由此設置u bit和g bit ([RFC2373] section 2.5.1)
A server MUST NOT assign an address that is otherwise reserved for some other purpose.	server不能指派為了其他目的保留的address
A server MUST NOT assign reserved anycast addresses, as defined in [RFC2526], from any subnet.	server不能指派從任何subnet保留的anycast address ([RFC2526])

Mobile Broadband Networklab, NCU
CONFIDENTIAL For Authorized Personnel Only

14. 由Client發起的訊息交換可信度 (1/2)

RT	Retransmission timeout
IRT	Initial retransmission time
MRC	Maximum retransmission count
MRT	Maximum retransmission time
MRD	Maximum retransmission duration
RAND	Randomization factor

Mobile Broadband Networklab, NCU
CONFIDENTIAL For Authorized Personnel Only

14. 由Client發起的訊息交換可信度 (2/2)

由Client發起的訊息交換可信度	
If a DHCP client fails to receive an expected response from a server, the client must retransmit its message.	若DHCP client從server沒有接收到應該要收到的回應，client必須重送請求
If RT expires before the message exchange terminates, the client recomputes RT and retransmits the message.	若在訊息交換結束前RT就過期，client會重新計算RT並重送訊息
Each of the computations of a new RT include a randomization factor (RAND), which is a random number chosen with a uniform distribution between -0.1 and +0.1.	每次新RT的計算會包含一個介於-0.1與+0.1常態分佈的亂數
The algorithm SHOULD produce a different sequence of random numbers from each invocation of the DHCP client.	演算法應該從每個DHCP client的調用產生亂數的不同序號

Mobile Broadband Networklab, NCU
CONFIDENTIAL For Authorized Personnel Only

15. 訊息驗證(1/14)

訊息驗證	
Clients and servers SHOULD discard any messages that contain options that are not allowed to appear in the received message.	client和server應該丟棄包含了不允許出現在訊息中的選項
A server MUST discard any Solicit, Confirm, Rebind or Information-request messages it receives with a unicast destination address.	server必須丟棄任何目標位址是unicast address的solicit、confirm、rebind或Information-request message
If a server receives a message that contains options it should not contain, is missing options that it should contain, or is otherwise not valid, it MAY send out a Reply.	若server收到包含了在一則訊息中不該有的選項或不該少的選項，抑或是不正當的選項，則可能會送出Reply訊息

CONFIDENTIAL For Authorized Personnel Only

15. 訊息驗證(2/14)

Transaction IDs 的用途	
The "transaction-id" field holds a value used by clients and servers to synchronize server responses to client messages.	“transcation-id”的欄位放置了clients和servers所使用的值來同步server對client的回覆訊息
A client SHOULD generate a random number that cannot easily be guessed or predicted to use as the transaction ID for each new message it sends	client應該為每個其新產的訊息生一個不會被輕易猜到的亂數作為transaction ID
A client MUST leave the transaction ID unchanged in retransmissions of a message.	client在重送的訊息中必須讓transaction ID維持不變

CONFIDENTIAL For Authorized Personnel Only

15. 訊息驗證(3/14)

Solicit Message	
Clients MUST discard any received Solicit messages.	client必須丟棄任何接收到的solicit message
Servers MUST discard any Solicit messages that do not include a Client Identifier option or that do include a Server Identifier option.	server必須丟棄任何沒有包含client和Server Identifier option的solicit message

CONFIDENTIAL For Authorized Personnel Only

15. 訊息驗證(4/14)

Advertise Message	
Clients MUST discard any received Advertise messages that meet any of the following conditions: • The message does not include a Server Identifier option. • The message does not include a Client Identifier option. • The contents of the Client Identifier option does not match the client's DUID. • The "transaction-id" field value does not match the value the client used in its Solicit message.	client必須丟棄任何符合以下任一條件的advertise message: • 沒有包含Server Identifier option • 沒有包含Client Identifier option • client的識別碼選項跟client的DUID不匹配 • “transaction-id”欄位的值和clien在solicit message所用的值不匹配
Servers and relay agents MUST discard any received Advertise messages.	server和relay agent必須丟棄任何advertise message

CONFIDENTIAL For Authorized Personnel Only

15. 訊息驗證(5/14)

Request Message	
Clients MUST discard any received Request messages.	clients必須丟棄任何request message
Servers MUST discard any received Request message that meet any of the following conditions: • The message does not include a Server Identifier option. • The contents of the Server Identifier option do not match the server's DUID. • The message does not include a Client Identifier option.	Servers必須丟棄任何符合以下任一條件的request message: • 沒有包含Server Identifier option • Server Identifier option中的內容跟server的DUID不匹配 • 不包含Client Identifier option

CONFIDENTIAL For Authorized Personnel Only

15. 訊息驗證(6/14)

Confirm Message	
Clients MUST discard any received Confirm messages.	clients必須丟棄任何confirm message
Servers MUST discard any received Confirm messages that do not include a Client Identifier option or that do include a Server Identifier option.	server必須丟棄任何不包含server和client是別選項的confirm message

CONFIDENTIAL For Authorized Personnel Only

15. 訊息驗證(7/14)

Renew Message	
Clients MUST discard any received Renew messages.	clients必須丟棄任何renew message
Servers MUST discard any received Renew message that meets any of the following conditions: • The message does not include a Server Identifier option. • The contents of the Server Identifier option does not match the server's identifier. • The message does not include a Client Identifier option.	server必須丟棄任何符合以下任一條件的renew message: • 不包含Server Identifier option • Server Identifier option中的內容和server識別碼不匹配 • 不包含Client Identifier option

CONFIDENTIAL For Authorized Personnel Only

15. 訊息驗證(8/14)

Rebind Message	
Clients MUST discard any received Rebind messages.	clients必須丟棄任何rebind message
Servers MUST discard any received Rebind messages that do not include a Client Identifier option or that do include a Server Identifier option.	server必須丟棄任何沒有包含client和Server Identifier option的rebind message

CONFIDENTIAL For Authorized Personnel Only

15. 訊息驗證(9/14)

Decline Message	
Clients MUST discard any received Decline messages.	clients必須丟棄任何decline message
Servers MUST discard any received Decline message that meets any of the following conditions: • The message does not include a Server Identifier option. • The contents of the Server Identifier option does not match the server's identifier. • The message does not include a Client Identifier option.	servers必須丟棄符合以下任一條件的decline message: • 不包含server是別選項 • 在Server Identifier option中的內容與server的識別碼不匹配 • 不包含Client Identifier option

CONFIDENTIAL For Authorized Personnel Only

15. 訊息驗證(10/14)

Release Message	
Clients MUST discard any received Release messages.	clients必須丟棄任何release message
Servers MUST discard any received Release message that meets any of the following conditions: • The message does not include a Server Identifier option. • The contents of the Server Identifier option does not match the server's identifier. • The message does not include a Client Identifier option.	Server必須丟棄任何符合以下任一條件的release message: • 不包含Server Identifier option • Server Identifier option中的內容和server識別碼不匹配 • 不包含Client Identifier option

CONFIDENTIAL For Authorized Personnel Only

15. 訊息驗證(11/14)

Reply Message	
Clients MUST discard any received Reply message that meets any of the following conditions: • The message does not include a Server Identifier option. • The "transaction-id" field in the message does not match the value used in the original message.	clients必須丟棄任何符合以下任一條件的reply message: • 不包含Server Identifier option • “transaction-id”欄位中的值和原來訊息中的值不匹配
If the client included a Client Identifier option in the original message, the Reply message MUST include a Client Identifier option.	若client在原本的訊息中包含Client Identifier option，reply message必須包含Client Identifier option

Mobile Broadband Networklab, NCU
CONFIDENTIAL For Authorized Personnel Only

15. 訊息驗證(12/14)

Reply Message	
And the contents of the Client Identifier option MUST match the DUID of the client	Client Identifier option中的內容必須和client的DUID匹配
If the client did not include a Client Identifier option in the original message, the Reply message MUST NOT include a Client Identifier option	若client沒有在原本的訊息物中包含Client Identifier option，則reply message不能包含Client Identifier option
Servers and relay agents MUST discard any received Reply messages.	servers和relay agents必須丟棄任何reply message

Mobile Broadband Networklab, NCU
CONFIDENTIAL For Authorized Personnel Only

15. 訊息驗證(13/14)

Reconfigure Message	
Servers and relay agents MUST discard any received Reconfigure messages.	server和relay agents必須丟棄任何Reconfigure message
Clients MUST discard any Reconfigure messages that meets any of the following conditions: • The message was not unicast to the client. • The message does not include a Server Identifier option. • The message does not include a Client Identifier option that contains the client's DUID. • The message does not contain a Reconfigure Message option and the msg-type must be a valid value. • The message includes any IA options and the msg-type in the Reconfigure Message option is INFORMATION-REQUEST. • The message does not include DHCP authentication	clients必須丟棄任何符合以下任一條件 的Reconfigure message: • 不是以unicast傳給client • 沒有包含Server Identifier option • 沒有包含client的DUID在Client Identifier option中 • 沒有包含Reconfigure Message選項且msg-type要是正確的 • 包含IA選項和msg-type是INFORMATION-REQUSET • 沒有包含DHCP驗證

CONFIDENTIAL For Authorized Personnel Only

15. 訊息驗證(14/14)

Information-request	
Clients MUST discard any received Information-request messages.	clients必須丟棄任何Information-request message
Servers MUST discard any received Information-request message that meets any of the following conditions: • The message includes a Server Identifier option and the DUID in the option does not match the server's DUID. • The message includes an IA option.	servers必須丟棄任何符合以下條件的Information-request message: • Server Identifier option中的DUID和server的DUID不匹配 • 包含了IA選項
Relay-forward Message	
Clients MUST discard any received Relay-forward messages.	Clients必須丟棄任何Relay-forward message
Relay-reply Message	
Clients and servers MUST discard any received Relay-reply messages.	Clients和servers都必須丟棄任何Relay-reply message

CONFIDENTIAL For Authorized Personnel Only

16. Client的來源Address和Interface選擇

Client的來源Address和Interface選擇	
When a client sends a DHCP message to the All_DHCP_Relay_Agents_and_Servers address, it SHOULD send the message through the interface for which configuration information is being requested.	當client傳送DHCP訊息給All_DHCP_Relay_Agents_and_Servers的address時，應該要透過需要被資訊設定的interface發送
The client MUST use a link-local address assigned to the interface for which it is requesting configuration information as the source address in the header of the IP datagram	該client必須使用該interface上的link-local address作為IP封包header中的source address
When a client sends a DHCP message directly to a server using unicast the source address in the header of the IP datagram MUST be an address assigned to the interface.	當client透過unicast直接傳送一個DHCP訊息給server時，IP封包header中的source address必須是interface被指派的address

CONFIDENTIAL For Authorized Personnel Only

17. DHCP Server Solicitation (1/6)

Client Behavior	
Creation of Solicit Message • The client MUST include a Client Identifier option to identify itself to the server. • The client MUST NOT include any other options in the Solicit message, except as specifically allowed in the definition of individual options. • The client SHOULD include an Option Request option (see section 22.7) to indicate the options the client is interested in receiving.	Solicit Message的產生： • client必須包含一個Client Identifier option • client不能包含任何其它option，除非有私人特別允許 • Client應該包含一個Option Request option來表示client有興趣接收到的option

CONFIDENTIAL For Authorized Personnel Only

17. DHCP Server Solicitation (2/6)

Client Behavior	
Transmission of Solicit Messages • The first Solicit message from the client on the interface MUST be delayed by a random amount of time between 0 and SOL_MAX_DELAY. • The message exchange is not terminated by the receipt of an Advertise before the first RT has elapsed. Rather, the client collects Advertise messages until the first RT has elapsed. Also, the first RT MUST be selected to be strictly greater than IRT by choosing RAND to be strictly greater than 0. • A client MUST collect Advertise messages for the first RT seconds, unless it receives an Advertise message with a preference value of 255	Solicit Message的傳送： • client上某個interface的第一個solicit message必須有從0到SOL_MAX_DELAY中的隨機時間延遲 • 在RT到期前收到Advertise，訊息交換都還不會結束。相反，client蒐集advertise message直到第一個RT到期。因此第一個RT必須大於IRT，透過選擇RAND大於0達成 • 一個client必須蒐集Advertise message直到第一次RT到期，除非它收到了performance value是255的Advertise message

CONFIDENTIAL For Authorized Personnel Only

17. DHCP Server Solicitation (3/6)

Client Behavior	
Transmission of Solicit Messages • If the first RT elapses and the client has received an Advertise message, the client SHOULD continue with a client-initiated message exchange by sending a Request message. • A DHCP client SHOULD choose MRC and MRD to be 0. • If the DHCP client is configured with either MRC or MRD set to a value other than 0, it MUST stop trying to configure the interface if the message exchange fails. • After the DHCP client stops trying to configure the interface, it SHOULD restart the reconfiguration process after some external event.	Solicit Message的傳送： • 當第一次RT到期且client收到了Advertise message，則client應該繼續發送Request message • client應該將MRC和MRD設為0 • 如果MRC和MRD不是被設為0，client必須在訊息交換失敗後停止設定interface • 在client停止設定interface之後，client應該在其他外部事件發生後重新開始設定

CONFIDENTIAL For Authorized Personnel Only

17. DHCP Server Solicitation (4/6)

Client Behavior	
Receipt of Advertise Messages • The client MUST ignore any Advertise message that includes a Status Code option containing the value NoAddrsAvail.	Advertise Message的接收: • Client應該忽略任何包含了Status Code option有NoAddrsAvail的Advertise message
Server Behavior	
Creation and Transmission of Advertise Messages • The server implementation SHOULD allow the setting of a server preference value by the administrator. • The server preference value MUST default to zero unless otherwise configured by the server administrator.	Advertise Message的創造與傳送: • server應該允許server管理者的偏好設定 • Server偏好值必須預設為0，除非管理者有額外設定

CONFIDENTIAL For Authorized Personnel Only

17. DHCP Server Solicitation (5/6)

Server Behavior	
Creation and Transmission of Advertise Messages • If the Solicit message from the client included one or more IA options, the server MUST include IA options in the Advertise message containing any addresses that would be assigned to IAs. • If the server will not assign any addresses to any IAs in a subsequent Request from the client, the server MUST send an Advertise message to the client that includes only a Status Code option with code NoAddrsAvail and a status message for the user	Advertise Message的創造與傳送: • 若client發出的Solicit message中包含了IA option，server必須在Advertise message中包含任何被指派於這些IA的address • 若server接下來不會指派任何address給IA，server必須傳送包含了status code為NoAddrsAvail的Advertise message和status message給使用者

CONFIDENTIAL For Authorized Personnel Only

17. DHCP Server Solicitation (6/6)

Server Behavior	
Creation and Transmission of Advertise Messages • If the Solicit message was received directly by the server, the server unicasts the Advertise message directly to the client using the address in the source address field from the IP datagram in which the Solicit message was received. The Advertise message MUST be unicast on the link from which the Solicit message was received.	Advertise Message的創造與傳送: • 若server直接收到Solicit message，server直接將Advertise message透過unicast回傳給client，且Advertise message必須在收到Solicit message的link上是unicast
Creation and Transmission of Reply Messages • The server MUST commit the assignment of any addresses or other configuration information message before sending a Reply message to a client in response to a Solicit message.	• Server在傳送Reply message回應Solicit message前必須確認address的指派以及其它設定資訊的訊息

Mobile Broadband Networklab, NCU
CONFIDENTIAL For Authorized Personnel Only

18. Client發起的DHCP設定交換 (1/14)

Client Behavior	
If the client has a source address of sufficient scope that can be used by the server as a return address, and the client has received a Server Unicast option (section 22.12) from the server, the client SHOULD unicast any Request, Renew, Release and Decline messages to the server.	若client有可以被server傳送訊息的address，且client接收到Server Unicast option，client就應該透過unicast傳送任何Request, Renew, Release, Decline message給server
Creation and Transmission of Request Messages • The client MUST include a Client Identifier option to identify itself to the server. • The client MUST include an Option Request option (see section 22.7) to indicate the options the client is interested in receiving.	Request Message的產生與傳送： • client必須包含一個Client Identifier option • Client必須包含一個Option Request option表明client想要收到什麼樣的option

Mobile Broadband Networklab, NCU
CONFIDENTIAL For Authorized Personnel Only

18. Client發起的DHCP設定交換 (2/14)

Client Behavior	
Creation and Transmission of Confirm Messages • When a client have moved to a new link, the client MUST initiate a Confirm/Reply message exchange. • The client MUST include a Client Identifier option • The client SHOULD set the T1 and T2 fields in any IA_NA options, and the preferred-lifetime and valid-lifetime fields in the IA Address options to 0. • The first Confirm message from the client on the interface MUST be delayed by a random amount of time between 0 and CNF_MAX_DELAY.	Confirm Message的產生與傳送： • 當client移到新的link上時，必須發起一個Confirm或Reply的訊息交換 • Client必須包含一個Client Identifier option • Client應該設置T1和T2欄位為任何IA_NA option，且設置preferred-lifetime和valid-lifetime欄位為0 • client上的一個interface的第一次Confirm message必須有從0到CNF_MAX_DELAY中的隨機時間延遲

CONFIDENTIAL For Authorized Personnel Only

18. Client發起的DHCP設定交換 (3/14)

Client Behavior	
Creation and Transmission of Confirm Messages • If the client receives no responses before the message transmission process terminates, as described in section 14, the client SHOULD continue to use any IP addresses, using the last known lifetimes for those addresses, and SHOULD continue to use any other previously obtained configuration parameters.	Confirm Message的產生與傳送： • 若client在傳送程序結束前沒有收到回應，如section 14所述，client應該繼續使用任何IP address，並使用最後所得到的lifetime，且應該繼續使用先前所得到的參數

CONFIDENTIAL For Authorized Personnel Only

18. Client發起的DHCP設定交換 (4/14)

Client Behavior	
Creation and Transmission of Renew Messages • The client MUST include a Client Identifier option to identify itself to the server. • The client MUST include the list of addresses the client currently has associated with the IAs in the Renew message. • The client MUST include an Option Request option	Renew Message的產生與傳送： • client必須加入一個Client Identifier option • client必須加入其目前跟Renew message中的IA有關的address清單 • client必須加入一個Option Request option
Creation and Transmission of Rebind Messages • The client MUST include a Client Identifier option. • The client MUST include the list of addresses the client currently has associated with the IAs in the Rebind message. • The client MUST include an Option Request option.	Rebind Message的生產與傳送： • client必須加入一個Client Identifier option • client必須加入其目前跟Renew message中的IA有關的address清單 • client必須加入一個Option Request option

CONFIDENTIAL For Authorized Personnel Only

18. Client發起的DHCP設定交換 (5/14)

Client Behavior	
Creation and Transmission of Information-request Messages • The client SHOULD include a Client Identifier option • The client MUST include a Client Identifier option if the Information-Request message will be authenticated. • The client MUST include an Option Request option • The first Information-request message from the client on the interface MUST be delayed by a random amount of time between 0 and INF_MAX_DELAY.	Information-request Message的產生與傳送： • client應該加入一個Client Identifier option • 若該Information-request message會被驗證，則必須加入一個Client Identifier option • client必須加入一個Option Request option • client上的一個interface的第一次Confirm message必須有從0到INF_MAX_DELAY中的隨機時間延遲

CONFIDENTIAL For Authorized Personnel Only

18. Client發起的DHCP設定交換 (6/14)

Client Behavior	
Creation and Transmission of Release Messages • The client MUST include a Client Identifier option. • The addresses to be released MUST be included in the IAs. • Any addresses for the IAs the client wishes to continue to use MUST NOT be added to the IAs • The client MUST NOT use any of the addresses it is releasing as the source address in the Release message or in any subsequently transmitted message.	Information-request Message的產生與傳送： • client必須加入一個Client Identifier option • 要被釋出的address必須加入在IA中 • 任何需要繼續使用於IA的address不能被加入到IA中 • client不能在Release message或接下來傳送的訊息中使用任何正在被釋出的address作為source address

CONFIDENTIAL For Authorized Personnel Only

18. Client發起的DHCP設定交換 (7/14)

Client Behavior	
Creation and Transmission of Release Messages • Because Release messages may be lost, the client should retransmit the Release if no Reply is received. Implementations SHOULD retransmit one or more times, but MAY choose to terminate the retransmission procedure early. • The client MUST stop using all of the addresses being released as soon as the client begins the Release message exchange process.	Release Message的產生與傳送： • 因為Release message可能遺失，client在沒有收到Reply時應該重送。因此實際上應該要重送多次，但也可能選擇提早終止重送 • 在Release message交換開始前client必須停止所有要被釋出的address

CONFIDENTIAL For Authorized Personnel Only

18. Client發起的DHCP設定交換 (8/14)

Client Behavior	
Creation and Transmission of Decline Messages • The client MUST include a Client Identifier option • The addresses to be declined MUST be included in the IAs. • Any addresses for the IAs the client wishes to continue to use should not be in added to the IAs. • The client MUST NOT use any of the addresses it is declining as the source address in the Decline message or in any subsequently transmitted message.	Decline Message的產生與傳送： • client必須加入一個Client Identifier option • 要被拒絕的address必須加入在IA中 • 任何需要繼續使用於IA的address不應該被加入到IA中 • client不能在Decline message或接下來傳送的訊息中使用任何正在被拒絕的address作為source address

Mobile Broadband Networklab, NCU
CONFIDENTIAL For Authorized Personnel Only

18. Client發起的DHCP設定交換 (9/14)

Client Behavior	
Receipt of Reply Messages • The client SHOULD perform duplicate address detection [17] on each of the addresses in any IAs it receives in the Reply message before using that address for traffic. • If the client receives a Reply message with a Status Code containing UnspecFail, the server is indicating that it was unable to process the message due to an unspecified failure condition. If the client retransmits the original message to the same server to retry the desired operation, the client MUST limit the rate at which it retransmits the message and limit the duration of the time during which it retransmits the message	Reply Message的接收： • Client在使用IA中的address傳送流量前應該執行duplicate address detection (DAD) • 若client收到一個Status Code為UnspecFail的Reply message，則代表server由於未知錯誤無法處理訊息。若client想要重送訊息以取得需要的操作，則client必須限制其重送訊息的頻率和持續時間。

Mobile Broadband Networklab, NCU
CONFIDENTIAL For Authorized Personnel Only

18. Client發起的DHCP設定交換 (10/14)

Server Behavior	
• This Reply message MUST always contain the Server Identifier option containing the server's DUID and the Client Identifier option from the client message if one was present. • The server must be aware of the recommendations on packet sizes and the use of fragmentation in section 5 of [RFC2460].	• 這個Reply message必須包含有著server DUID的Server Identifier option，以及從client訊息中來的Client Identifier option • Server必須注意在[RFC2460 section 5]中的封包大小

Mobile Broadband Networklab, NCU
CONFIDENTIAL For Authorized Personnel Only

18. Client發起的DHCP設定交換 (11/14)

Server Behavior	
Receipt of Request Messages • The server MUST include a Server Identifier option containing the server's DUID and the Client Identifier option from the Request message in the Reply message. • If the server finds that the prefix on one or more IP addresses in any IA in the message from the client is not appropriate for the link to which the client is connected, the server MUST return the IA to the client with a Status Code option with the value NotOnLink • If the server cannot assign any addresses to an IA in the message from the client, the server MUST include the IA in the Reply message with no addresses in the IA and a Status Code option in the IA containing status code NoAddrsAvail.	Request Message的接收 • Server必須加入包含server DUID的Server Identifier option，以及在Request message中的Client Identifier option • 若server發現IA中的address prefix不適合這個link，server必須回傳Status Code option為NotOnLink的IA給client • 若serve無法指派任何address給client訊息中的IA，server必須在IA中不加入任何address，並加入NoAddrsAvail在Status Code option中

Mobile Broadband Networklab, NCU
CONFIDENTIAL For Authorized Personnel Only

18. Client發起的DHCP設定交換 (12/14)

Server Behavior	
Receipt of Confirm Messages • If the server is unable to perform this test, or there were no addresses in any of the IAs sent by the client, the server MUST NOT send a reply to the client. • The server MUST include a Server Identifier option containing the server's DUID and the Client Identifier option from the Confirm message in the Reply message.	Confirm Message的接收 • 若server無法執行測試，或client並沒有在IA中傳送address，server則不能傳送reply給client • Server必須在Reply Message中加入包含server DUID的Server Identifier option，以及在Confirm message中的Client Identifier option
Receipt of Renew Messages • The server MUST include a Server Identifier option containing the server's DUID and the Client Identifier option from the Renew message in the Reply message.	Renew Message的接收 • Server必須在Reply Message中加入包含server DUID的Server Identifier option，以及在Renew message中的Client Identifier option

CONFIDENTIAL For Authorized Personnel Only

18. Client發起的DHCP設定交換 (13/14)

Server Behavior	
Receipt of Rebind Messages • If the server finds the addresses in the IA for the client then the server SHOULD send back the IA to the client with new lifetimes and T1/T2 times • The server MUST include a Server Identifier option containing the server's DUID and the Client Identifier option from the Rebind message in the Reply message.	Rebind Message的接收 • 若server在IA中找到給client的address，則server應該用新的lifetim和T1/T2 time 回傳IA給client • Server必須在Reply Message中加入包含server DUID的Server Identifier option，以及在Rebind message中的Client Identifier option

CONFIDENTIAL For Authorized Personnel Only

18. Client發起的DHCP設定交換(14/14)

Server Behavior	
Receipt of Information-request Messages • The server MUST include a Server Identifier option containing the server's DUID in the Reply message. • If the Information-request message received from the client did not include a Client Identifier option, the server SHOULD respond with a Reply message containing any configuration parameters that are not determined by the client's identity.	Information-request Message的接收： • Server必須在Reply Message中加入包含server DUID的Server Identifier option • 若從client收到的Information-request message不包含Client Identifier option，server應該回覆一個尚未決定任何設定參數的Reply message
Receipt of Decline Messages • The client has found any addresses in the Decline messages to be already in use on its link. Therefore, the server SHOULD mark the addresses declined by the client.	Decline Message的接收： • Client已經找到其link中已經被使用，在Decline message中的address，因此server應該標註被client拒絕的address
Transmission of Reply Messages • The Reply message MUST be unicast through the interface on which the original message was received.	Reply Message的傳送： • Reply message必須由原本的接收到訊息的介面卡透過unicast傳送

CONFIDENTIAL For Authorized Personnel Only

19. DHCPserver啟動的配置交換

伺服器行為	
If the server identifies the IA option in the Option Request option, the server MUST include an IA option that contains no other sub-options to identify each IA that is to be reconfigured on the client.	如果server在Option Request選項中識別IA選項，則server必須包含IA選項，該選項不包含其他子選項以標識要在客戶端上重新配置的每個IA。
The server MUST include a Reconfigure Message option (defined in section 22.19) to select whether the client responds with a Renew message or an Information-Request message.	Server必須包括Reconfigure Message選項（在第22.19節中定義），以選擇客戶端是以Renew message還是Information-Request message進行響應。
The server MUST NOT include any other options in the Reconfigure except as specifically allowed in the definition of individual options.	除非在各個選項的定義中明確允許，否則server不得在Reconfigure中包含任何其他選項。
The server continues this process until REC_MAX_RC unsuccessful attempts have been made, at which point the server SHOULD abort the reconfigure process for that client.	Server繼續此過程，直到REC_MAX_RC嘗試失敗，此時server應該中止該客戶端的重新配置過程。

TIAL For Authorized Personnel Only

用戶行為	
Since the results of a reconfiguration event may affect application layer programs, the client SHOULD log these events, and MAY notify these programs of the change through an implementation-specific interface.	由於重新配置事件的結果可能會影響應用程序層程序，因此客戶端應該記錄這些事件，並通過特定於實現的接口通知這些程序。

CONFIDENTIAL For Authorized Personnel Only

20.Relay Agent行為(1/2)

中繼代理行為	
If the relay agent has not been explicitly configured, it MUST use the All_DHCP_Servers multicast address as the default.	如果尚未明確配置中繼代理，則必須使用All_DHCP_Servers多播地址作為默認值。

CONFIDENTIAL For Authorized Personnel Only

20. Relay Agent行為(1/2)

中繼Client Message或Relay-forward Message	
If the relay agent received the message to be relayed from a client, the relay agent places a global or site-scoped address with a prefix assigned to the link on which the client should be assigned an address in the link-address field.	如果中繼代理接收到要從客戶端中繼的消息，則中繼代理放置全局或站點範圍的地址，該地址具有分配給鏈路的前綴，在該鏈路上應該在鏈路地址字段中為客戶端分配地址。
This address will be used by the server to determine the link from which the client should be assigned an address and other configuration information.	Server將使用此地址來確定應該從中為客戶端分配地址和其他配置信息的鏈接。
If the relay agent cannot use the address in the link-address field to identify the interface through which the response to the client will be relayed, the relay agent MUST include an Interface-id option (see section 22.18) in the Relay-forward message.	如果中繼代理不能使用鏈路地址字段中的地址來識別通過其中繼對客戶端的響應的接口，則中繼代理必須在中繼轉發消息中包含Interface-id選項（參見第22.18節）。

CONFIDENTIAL For Authorized Personnel Only

20. 中繼代理行為(2/2)

構建中繼回復消息	
A response to the client MUST be relayed through the same relay agents as the original client message.	對客戶端的響應必須通過與原始客戶端消息相同的中繼代理進行中繼。
The server must record the contents of the peer-address fields in the received message so it can construct the appropriate Relay-reply message carrying the response from the server.	Server必須在接收的消息中記錄對等地址字段的內容，以便它可以建構攜帶來自server的響應的適當的中繼回復消息。

CONFIDENTIAL For Authorized Personnel Only

21.DHCP訊息驗證 (1/5)

server和中繼代理之間發送的消息的安全性	
If a client message is relayed through multiple relay agents, each of the relay agents must have established independent, pairwise trust relationships.	如果通過多個中繼代理中繼客戶端消息，則每個中繼代理必須已建立獨立的成對信任關係。
If messages from client C will be relayed by relay agent A to relay agent B and then to the server, relay agents A and B must be configured to use IPSec for the messages they exchange, and relay agent B and the server must be configured to use IPSec for the messages they exchange.	如果來自客戶端C的消息將由中繼代理A中繼到中繼代理B然後再中繼到server，則中繼代理A和B必須配置為使用IPSec用於它們交換的消息，並且中繼代理B和server必須配置為 將IPSec用於他們交換的消息。

CONFIDENTIAL For Authorized Personnel Only

21.DHCP訊息驗證 (1/5)

server和中繼代理之間發送的消息的安全性	
Relay agents are manually configured with the addresses of the relay agent or server to which DHCP messages are to be forwarded. Each relay agent and server that will be using IPsec for securing DHCP messages must also be configured with a list of the relay agents to which messages will be returned. The selectors for the relay agents and servers will be the pairs of addresses defining relay agents and servers that exchange DHCP messages on the DHCPv6 UDP ports 546 and 547.	手動配置中繼代理，使用要轉發DHCP消息的中繼代理或server的地址。 每個將使用IPsec保護DHCP消息的中繼代理和server還必須配置一個將返回消息的中繼代理列表。 中繼代理和server的選擇器將是定義中繼代理的server對和在DHCPv6 UDP端口546和547上交換DHCP消息的server。

CONFIDENTIAL For Authorized Personnel Only

21. DHCP訊息驗證 (2/5)

server和中繼代理之間發送的消息的安全性	
Because the relay agents and servers are used an organization, public key schemes are not necessary. Because the relay agents and servers must be manually configured, manually configured key management may suffice, but does not provide defense against replayed messages.	由於relay agent和server是組織使用的，因此不需要公鑰方案。 由於必須手動配置中繼代理和server，因此手動配置的密鑰管理可能就足夠了，但不能防止重放的消息。
Accordingly, IKE with preshared secrets SHOULD be supported.	應該支持具有預共享秘密的IKE
IKE with public keys MAY be supported.	可以支持使用公鑰的IKE
DHCP messages between relay agents and servers should only be accepted from DHCP peers as identified in the local configuration.	中繼代理和server之間的DHCP消息應該只能從本地配置中標識的DHCP對等方接受。
DHCP認證摘要	
Any DHCP message MUST NOT include more than one Authentication option.	任何DHCP消息都不得包含多個身份驗證選項。

CONFIDENTIAL For Authorized Personnel Only

21. DHCP訊息驗證 (3/5)

重播檢測	
If the RDM field contains 0x00, the replay detection field MUST be set to the value of a monotonically increasing counter.	如果RDM字段包含0x00，則重放檢測字段必須設置為單調遞增計數器的值。
Using a counter value, such as the current time of day (for example, an NTP-format timestamp [9]), can reduce the danger of replay attacks. This method MUST be supported by all protocols.	使用計數器值（例如當前時間（例如，NTP格式時間戳[9]））可以降低重放攻擊的危險。 所有協議都必須支持此方法。

CONFIDENTIAL For Authorized Personnel Only

21. DHCP訊息驗證 (3/5)

延遲認證協議	
Any DHCP message that includes more than one authentication option MUST be discarded.	必須丟棄包含多個身份驗證選項的任何DHCP消息。
If the MAC computed by the receiver does not match the MAC contained in the authentication option, the receiver MUST discard the DHCP message.	如果接收方計算的MAC與認證選項中包含的MAC不匹配，則接收方必須丟棄DHCP消息。
The decision to set local policy to accept unauthenticated messages should be made with care.	設置本地策略以接受未經身份驗證的消息的決定應該謹慎進行。
A client MUST be configurable to discard unauthenticated messages, and SHOULD be configured by default to discard unauthenticated messages if the client has been configured with an authentication key or other authentication information.	客戶端必須可配置為丟棄未經身份驗證的消息，如果客戶端已配置了身份驗證密鑰或其他身份驗證信息，則應該默認配置為丟棄未經身份驗證的消息。
If a client does accept an unauthenticated message, the client SHOULD inform any local users and SHOULD log the event.	如果客戶端確實接受了未經身份驗證的消息，則客戶端應該通知任何本地用戶，並且應該記錄該事件。

CONFIDENTIAL For Authorized Personnel Only

21. DHCP訊息驗證 (4/5)

延遲認證協議	
If the client authenticated the Advertise message through which the client selected the server, the client MUST generate authentication information for subsequent Request, Confirm, Renew, Rebind or Release messages sent to the server.	如果客戶端驗證了客戶端通過其選擇server的Advertise消息，則客戶端必須為發送到server的後續Request，Confirm Renew，Rebind或Release消息生成認證信息。
When the client sends a subsequent message, it MUST use the same key used by the server to generate the authentication information.	當客戶端發送後續消息時，它必須使用server使用的相同密鑰來生成認證信息。
If the server has selected a key for the client in a previous message exchange (see section 21.4.5.1), the client MUST use the same key to generate the authentication information throughout the session.	如果server在先前的消息交換中為客戶端選擇了密鑰（請參閱第21.4.5.1節），則客戶端必須使用相同的密鑰在整個會話期間生成身份驗證信息。

CONFIDENTIAL For Authorized Personnel Only

21. DHCP訊息驗證 (5/5)

延遲認證協議	
If the client authenticated the Advertise it accepted, the client MUST validate the associated Reply message from the server.	如果客戶端對接受的廣告進行了身份驗證，則客戶端必須從server驗證關聯的Reply消息。
The client MUST discard the Reply if the message fails to pass the validation test and MAY log the validation failure.	如果消息未能通過驗證測試並且可能記錄驗證失敗，則客戶端必須丟棄Reply。
If the Reply fails to pass the validation test, the client MUST restart the DHCP configuration process by sending a Solicit message.	如果Reply無法通過驗證測試，客戶端必須通過發送Solicit消息重新啟動DHCP配置過程。
The client MUST discard the Reconfigure if the message fails to pass the validation test and MAY log the validation failure.	如果消息未通過驗證測試並且可能記錄驗證失敗，客戶端必須丟棄重新配置。
The server MUST record the identifier of the key selected for the client and use that same key for validating subsequent messages with the client.	Server必須記錄為客戶端選擇的密鑰的標識符，並使用相同的密鑰來驗證與客戶端的後續消息。
If the message fails to pass the validation test or the server does not know the key identified by the 'key ID' field, the server MUST discard the message and MAY choose to log the validation failure.	如果消息未通過驗證測試或server不知道“密鑰ID”字段標識的密鑰，則server必須丟棄該消息並且可以選擇記錄驗證失敗。

CONFIDENTIAL For Authorized Personnel Only

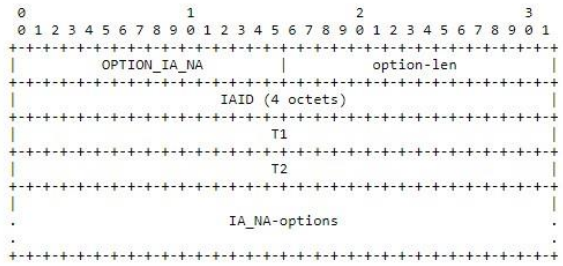
22. DHCP選項

DHCP選項	
Unless otherwise noted, each option may appear only in the options area of a DHCP message and may appear only once. If an option does appear multiple times, each instance is considered separate and the data areas of the options MUST NOT be concatenated or otherwise combined.	除非另有說明，否則每個選項可能僅出現在DHCP消息的選項區域中，並且可能只出現一次。 如果選項確實出現多次，則每個實例都被視為獨立的，並且選項的數據區域不得連接或以其他方式組合。

CONFIDENTIAL For Authorized Personnel Only

22. DHCP選項

The format of the IA_NA option is:

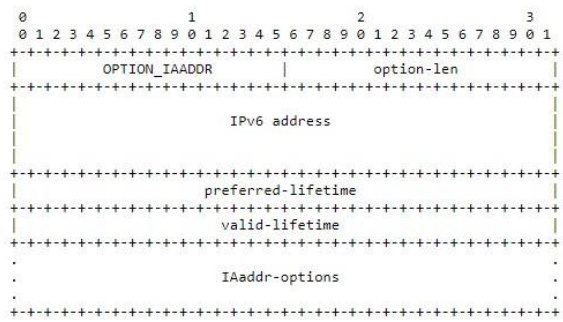


非臨時地址選項的身份關聯	
In a message sent by a server to a client, the client MUST use the values in the T1 and T2 fields for the T1 and T2 parameters, unless those values in those fields are 0.	在server發送給客戶端的消息中，客戶端必須使用T1和T2字段中的值作為T1和T2參數，除非這些字段中的值為0。

CONFIDENTIAL For Authorized Personnel Only

22. DHCP選項

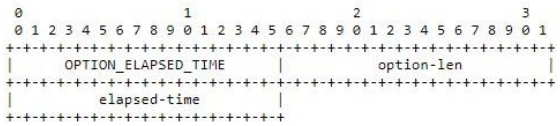
The format of the IA Address option is:



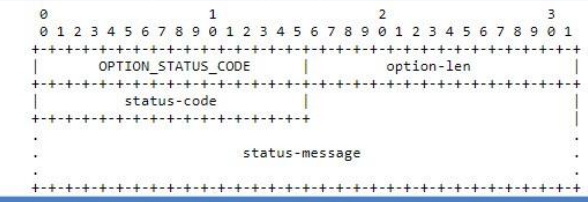
IA地址選項	
In a message sent by a server to a client, the client MUST use the values in the preferred and valid lifetime fields for the preferred and valid lifetimes.	在server發送到客戶端的消息中，客戶端必須使用首選和有效生命週期字段中的值來獲取首選和有效生命週期。

CONFIDENTIAL For Authorized Personnel Only

22. DHCP選項



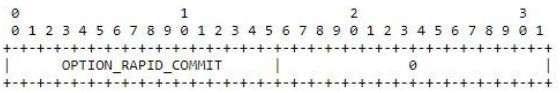
IA地址選項	
A client MUST include an Elapsed Time option in messages to indicate how long the client has been trying to complete a DHCP message exchange.	客戶端必須在消息中包含Elapsed Time選項，以指示客戶端嘗試完成DHCP消息交換的時間。



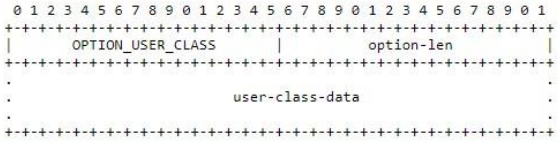
狀態代碼選項	
A UTF-8 encoded text string suitable for display to an end user, which MUST NOT be null-terminated.	UTF-8編碼的文本字符串，適合顯示給最終用戶，不得以空值終止。

CONFIDENTIAL For Authorized Personnel Only

22. DHCP選項



快速提交選項	
A server MUST include this option in a Reply message sent in response to a Solicit message when completing the Solicit-Reply message exchange.	Server必須在完成Solicit-Reply消息交換時響應Solicit消息而發送的Reply消息中包含此選項。

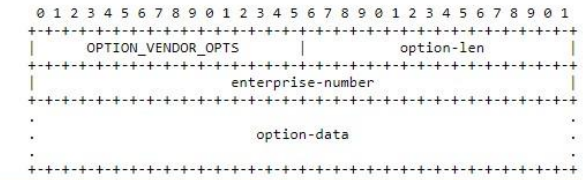


用戶類選項	
The user class information carried in this option MUST be configurable on the client.	此選項中攜帶的用戶類信息必須可在客戶端上配置。
The data area of the user class option MUST contain one or more instances of user class data.	用戶類選項的數據區域必須包含一個或多個用戶類數據實例。

TIAL For Authorized Personnel Only

22. DHCP選項

The format of the Vendor-specific Information option is:

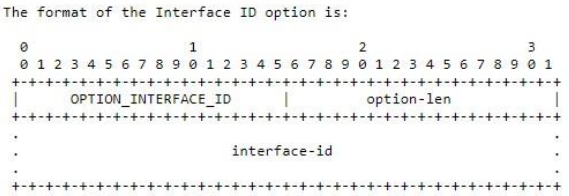


供應商特定信息選項	
The encapsulated vendor-specific options field MUST be encoded as a sequence of code/length/value fields of identical format to the DHCP options field.	封裝的供應商特定選項字段必須編碼為與DHCP選項字段格式相同的一系列代碼/長度/值字段。

CONFIDENTIAL For Authorized Personnel Only

22. DHCP選項

The format of the Interface ID option is:



Interface-Id選項	
The server MUST copy the Interface-Id option from the Relay-Forward message into the Relay-Reply message the server sends to the relay agent in response to the Relay-Forward message.	Server必須將Interface-Id選項從Relay-Forward消息複製到server發送給中繼代理的Relay-Reply消息中，以響應Relay-Forward消息。
This option MUST NOT appear in any message except a Relay-Forward or Relay-Reply message.	除了Relay-Forward或Relay-Reply消息之外，該選項不得出現在任何消息中。
Servers MAY use the Interface-ID for parameter assignment policies.	server可以使用Interface-ID進行參數分配策略。

CONFIDENTIAL For Authorized Personnel Only

22. DHCP選項

Interface-Id選項	
The Interface-ID SHOULD be considered an opaque value, with policies based on exact match only.	Interface-ID應該被視為不透明值，策略僅基於完全匹配。
The Interface-ID SHOULD NOT be internally parsed by the server.	Interface-ID不應該由server在內部解析。
The Interface-ID value for an interface SHOULD be stable and remain unchanged.	接口的Interface-ID值應該穩定並保持不變。

CONFIDENTIAL For Authorized Personnel Only

23.安全考慮因素

安全考慮因素	
DHCP is not used to exchange authentication or configuration information that must be kept secret from other networks nodes.	DHCP不用於交換必須對其他網絡節點保密的身份驗證或配置信息。
Because of the opportunity for attack through the Reconfigure message, a DHCP client MUST discard any Reconfigure message that does not include authentication or that does not pass the validation process for the authentication protocol.	由於通過重新配置消息進行攻擊的機會，DHCP客戶端必須丟棄任何不包含身份驗證或未通過身份驗證協議驗證過程的重新配置消息。

CONFIDENTIAL For Authorized Personnel Only



149

國立中央大學
National Central University

Mobile
broadband
networklab

RFC 3633
IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6

周立德

國立中央大學主任秘書

國立中央大學資訊工程學系特聘教授

2019

150

RFC 3633 Terminology

- 名詞參照RFC 3315和 RFC 2460
- requesting router: The router that acts as a DHCP client and is requesting prefix(es) to be assigned.
- 請求路由器：充當DHCP客戶端並請求分配前綴的路由器。
- delegating router: The router that acts as a DHCP server, and is responding to the prefix request.
- 委派路由器：充當DHCP服務器並回應前綴請求的路由器。
- Identity Association for Prefix Delegation (IA_PD): A collection of prefixes assigned to the requesting router. Each IA_PD has an associated IAID. A requesting router may have more than one IA_PD assigned to it; for example, one for each of its interfaces.
- 前綴委派身份關聯（IA_PD）：分配給請求路由器的前綴集合。每個IA_PD都有一個關聯的IAID。請求路由器可能分配了多個IA_PD；例如，每個接口一個。

CONFIDENTIAL For Authorized Personnel Only

Example network architecture

- Figure 1 illustrates a network architecture in which prefix delegation could be used.

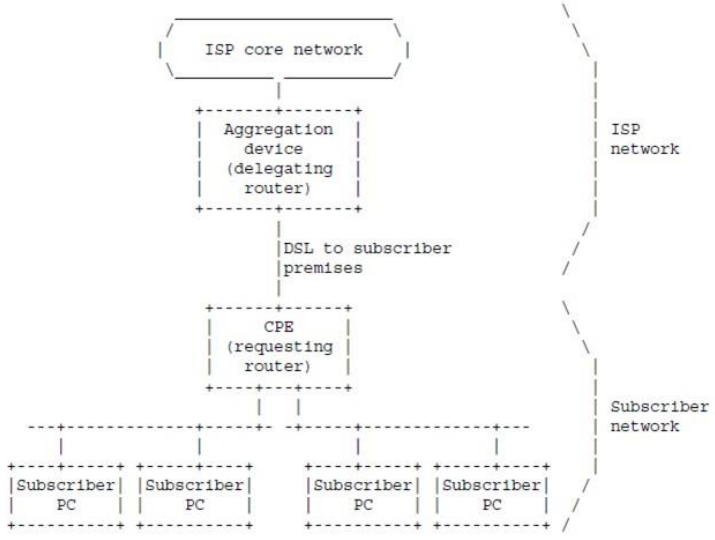


Figure 1: An example of prefix delegation.

CONFIDENTIAL For Authorized Personnel Only

Identity Association for Prefix Delegation (前綴委派身份關聯)	
A requesting router must create at least one distinct IA_PD.	請求路由器必須至少創建一個不同的IA_PD。
The IAID uniquely identifies the IA_PD and must be chosen to be unique among the IA_PD IAIDs on the requesting router.	IAID唯一標識IA_PD，並且必須在請求路由器上的IA_PD IAID中選擇唯一的IAID。
The IAID is chosen by the requesting router. For any given use of an IA_PD by the requesting router, the IAID for that IA_PD MUST be consistent across restarts of the requesting router.	IAID由請求路由器選擇。對於請求路由器對IA_PD的任何給定使用，該IA_PD的IAID必須在請求路由器的重新啟動之間保持一致。

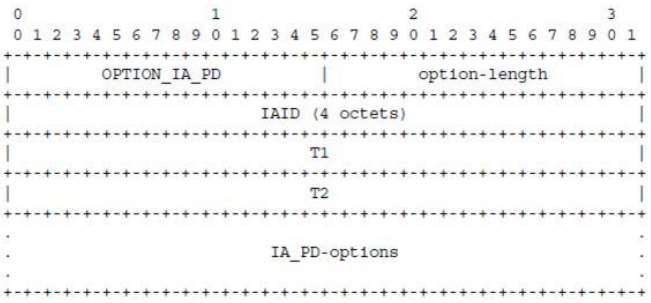
CONFIDENTIAL For Authorized Personnel Only

Interface Selection (介面選擇)

Interface Selection（介面選擇）	
When a requesting router sends a DHCP message, it SHOULD be sent on the interface associated with the upstream router (ISP network).	當請求路由器發送DHCP消息時，它應該在與上游路由器（ISP網絡）相關的接口上發送。
When a requesting router sends a DHCP message directly to a delegating router using unicast (after receiving the Server Unicast option from that delegating router), the source address SHOULD be an address from the upstream interface and which is suitable for use by the delegating router in responding to the requesting router.	當請求路由器使用單播直接向委派路由器發送DHCP消息時（在從該委派路由器接收到服務器單播選項之後），來源地址應該是來自上游接口的地址，並且適合委派路由器使用回應請求路由器。

CONFIDENTIAL For Authorized Personnel Only

Identity Association for Prefix Delegation Option（前綴委派選項的身份關聯）	
IAID: The unique identifier for this IA_PD; the IAID must be unique among the identifiers for all of this requesting router's IA_PDs.	IAID：此IA_PD的唯一標識符; IAID在所有請求路由器的IA_PD的標識符中必須是唯一的。



CONFIDENTIAL For Authorized Personnel Only

Identity Association for Prefix Delegation Option（前綴委派選項的身份關聯）	
T1: The time at which the requesting router should contact the delegating router from which the prefixes in the IA_PD were obtained to extend the lifetimes of the prefixes delegated to the IA_PD; T1 is a time duration relative to the current time expressed in units of seconds.	T1：請求路由器應該從獲得IA_PD中的前綴的委派路由器聯繫的時間，以延長委託給IA_PD的前綴的生存期; T1是相對於當前時間的持續時間，以秒為單位表示。
T2: The time at which the requesting router should contact any available delegating router to extend the lifetimes of the prefixes assigned to the IA_PD; T2 is a time duration relative to the current time expressed in units of seconds.	T2：請求路由器應該聯繫任何可用的委派路由器以延長分配給IA_PD的前綴的生存期的時間; T2是相對於當前時間的持續時間，以秒為單位表示。

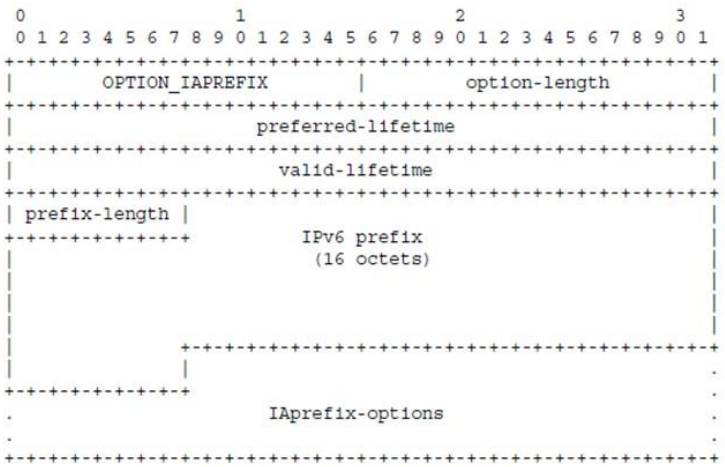
CONFIDENTIAL For Authorized Personnel Only

Identity Association for Prefix Delegation Option（前綴委派選項的身份關聯）	
When the valid lifetimes of all of the prefixes in a IA_PD have expired, the IA_PD can be considered as having expired. T1 and T2 are included to give delegating routers explicit control over when a requesting router should contact the delegating router about a specific IA_PD.	當IA_PD中所有前綴的有效生命週期到期時，IA_PD可被視為已過期。包括T1和T2以便委派路由器明確控制請求路由器何時應該與委派路由器聯繫關於特定IA_PD。
In a message sent by a delegating router to a requesting router, the requesting router MUST use the values in the T1 and T2 fields for the T1 and T2 parameters.	在委派路由器發送到請求路由器的消息中請求路由器必須使用T1和T2欄位中的值作為T1和T2參數。

Mobile Broadband Networklab, NCU
CONFIDENTIAL For Authorized Personnel Only

IA_PD Prefix option (IA_PD前綴選項)

IA_PD Prefix option（IA_PD前綴選項）	
The IA_PD Prefix option is used to specify IPv6 address prefixes associated with an IA_PD. The IA_PD Prefix option must be encapsulated in the IA_PD-options field of an IA_PD option.	IA_PD Prefix選項用於指定與IA_PD關聯的IPv6地址前綴。必須將IA_PD Prefix選項封裝在IA_PD選項的IA_PD-options欄位中。



Mobile Broadband Networklab, NCU
CONFIDENTIAL For Authorized Personnel Only

IA_PD Prefix option (IA_PD前綴選項)

IA_PD Prefix option (IA_PD前綴選項)	
In a message sent by a delegating router the preferred and valid lifetimes should be set to the values of AdvPreferredLifetime and AdvValidLifetime as specified in section 6.2.1, "Router Configuration Variables" of RFC 2461 [4], unless administratively configured.	在委派路由器發送的消息中，首選和有效生命週期應該設置為AdvPreferredLifetime和AdvValidLifetime的值，如RFC 2461 [4]的第6.2.1節“路由器配置變量”中所述，除非進行管理配置。

CONFIDENTIAL For Authorized Personnel Only

Requesting router behavior (請求路由器行為)

Requesting router behavior (請求路由器行為)	
The requesting router creates and transmits a Solicit message as described in sections 17.1.1, "Creation of Solicit Messages" and 17.1.2, "Transmission of Solicit Messages" of RFC 3315. The requesting router creates an IA_PD and assigns it an IAID. The requesting router MUST include the IA_PD option in the Solicit message.	請求路由器創建並發送Solicit消息，如RFC 3315的第17.1.1節“創建請求消息”和17.1.2“請求消息的傳輸”中所述。請求路由器創建IA_PD並為其分配IAID。 請求路由器必須在Solicit消息中包含IA_PD選項。
The requesting router MUST ignore any Advertise message that includes a Status Code option containing the value NoPrefixAvail, with the exception that the requesting router MAY display the associated status message to the user.	請求路由器必須忽略包含值NoPrefixAvail的狀態代碼選項的任何Advertise消息，除了請求路由器可以向用戶顯示相關的狀態消息。

CONFIDENTIAL For Authorized Personnel Only

Delegating router behavior (委派路由器行為)

Delegating router behavior（委派路由器行為）	
The delegating router sends an Advertise message to the requesting router in the same way as described in section, "Creation and transmission of Advertise messages" of RFC 3315. The delegating router MUST include an IA_PD option, identifying any prefix(es) that the delegating router will delegate to the requesting router.	委派路由器以與RFC 3315中“廣告消息的創建和傳輸”一節中描述的相同方式向請求路由器發送Advertise消息。委派路由器必須包含IA_PD選項，標識委派路由器將委託給請求路由器的任何前綴。
If the delegating router will not assign any prefixes to any IA_PDs in a subsequent Request from the requesting router, the delegating router MUST send an Advertise message to the requesting router that includes the IA_PD with no prefixes in the IA_PD and a Status Code option in the IA_PD containing status code NoPrefixAvail and a status message for the user, a Server Identifier option with the delegating router's DUID and a Client Identifier option with the requesting router's DUID.	如果委派路由器不會在請求路由器的後續請求中為任何IA_PD分配任何前綴，則委派路由器必須向請求路由器發送一條Advertise消息，該消息包含IA_PD中沒有前綴的IA_PD和一個狀態代碼選項。IA_PD包含狀態代碼NoPrefixAvail和用戶的狀態消息，服務器標識符選項包含委派路由器的DUID，客戶端標識符選項包含請求路由器的DUID。

CONFIDENTIAL For Authorized Personnel Only

Requesting router behavior (請求路由器行為)

Requesting router behavior (請求路由器行為)	
If such verification is needed the requesting router MUST initiate a Rebind/Reply message exchange as described in section 18.1.4, "Creation and Transmission of Rebind Messages" of RFC 3315, with the exception that the retransmission parameters should be set as for the Confirm message, described in section 18.1.2, "Creation and Transmission of Confirm Messages" of RFC 3315. The requesting router includes any IA_PDs, along with prefixes associated with those IA_PDs in its Rebind message.	如果需要這樣的驗證，請求路由器必須發起重新綁定/回覆消息交換，如RFC 3315的第18.1.4節“重新綁定消息的創建和傳輸”中所述，但重傳參數應該設置為確認消息，在RFC 3315的第18.1.2節“確認消息的創建和傳輸”中描述。請求路由器包括任何IA_PD，以及在其重新綁定消息中與這些IA_PD相關聯的前綴。

CONFIDENTIAL For Authorized Personnel Only

Requesting router behavior (請求路由器行為)

Requesting router behavior (請求路由器行為)	
The requesting router uses a Release message to return a delegated prefix to a delegating router. The prefixes to be released MUST be included in the IA_PDs.	請求路由器使用Release消息將委派的前綴返回給委派路由器。 要釋放的前綴必須包含在IA_PD中。
Upon the receipt of a valid Reply message, for each IA_PD the requesting router assigns a subnet from each of the delegated prefixes to each of the links to which the associated interfaces are attached, with the following exception: the requesting router MUST NOT assign any delegated prefixes or subnets from the delegated prefix(es) to the link through which it received the DHCP message from the delegating router.	在收到有效的Reply消息後，對於每個IA_PD，請求路由器將每個委託前綴的子網分配給相關接口所連接的每個鏈路，但有以下例外：請求路由器不能分配任何委託的 從委派前綴到從委派路由器接收DHCP消息的鏈接的前綴或子網。
When a requesting router subnets a delegated prefix, it must assign additional bits to the prefix to generate unique, longer prefixes.	當請求路由器子網委託前綴時，它必須為前綴分配額外的位以生成唯一的，更長的前綴。

CONFIDENTIAL For Authorized Personnel Only

Requesting router behavior (請求路由器行為)

Requesting router behavior (請求路由器行為)	
If the requesting router assigns a delegated prefix to a link to which the router is attached, and begins to send router advertisements for the prefix on the link, the requesting router MUST set the valid lifetime in those advertisements to be no later than the valid lifetime specified in the IA_PD Prefix option. A requesting router MAY use the preferred lifetime specified in the IA_PD Prefix option.	如果請求路由器將指定的前綴分配給路由器所連接的鏈路，並開始在鏈路上發送前綴的路由器通告，則請求路由器必須將這些通告中的有效生存期設置為不晚於有效生命週期 在IA_PD前綴選項中指定。請求路由器可以使用IA_PD前綴選項中指定的首選生命週期。

CONFIDENTIAL For Authorized Personnel Only

Delegating router behavior (委派路由器行為)

Delegating router behavior (委派路由器行為)	
The delegating router MUST include an IA_PD Prefix option or options (in an IA_PD option) in Reply messages sent to a requesting router.	委派路由器必須在發送給請求路由器的Reply消息中包含IA_PD Prefix選項或選項（在IA_PD選項中）。

CONFIDENTIAL For Authorized Personnel Only

Requesting router behavior (請求路由器行為)

Requesting router behavior (請求路由器行為)	
The requesting router responds to a Reconfigure message, acting as a DHCP client, received from a delegating router as described in section 19.4, "Client Behavior" of RFC 3315. The requesting router MUST include the IA_PD Prefix option(s) (in an IA_PD option) for prefix(es) that have been delegated to the requesting router by the delegating router from which the Reconfigure message was received.	請求路由器響應作為DHCP客戶端的重新配置消息，如第19.4節“RFC 3315的客戶端行為”中所述從委派路由器接收。請求路由器必須包含IA_PD前綴選項（在一個IA_PD選項中）用於已從接收重新配置消息的委派路由器委派給請求路由器的前綴。

CONFIDENTIAL For Authorized Personnel Only

Security Considerations

Security Considerations	
To guard against attacks through prefix delegation, requesting routers and delegating routers SHOULD use DHCP authentication as described in section 21, "Authentication of DHCP messages" of RFC 3315.	為了防止通過前綴委派進行攻擊，請求路由器和委派路由器應該使用DHCP認證，如RFC 3315的第21節 “DHCP消息認證”中所述。
Because a requesting router and delegating routers must each have at least one assigned IPv6 address, the routers may be able to use IPsec for authentication of DHCPv6 messages.	因為請求路由器和委派路由器必須各自具有至少一個分配的IPv6地址，所以路由器可能能夠使用IPsec來驗證DHCPv6消息。
Networks configured with delegated prefixes should be configured to preclude intentional or inadvertent inappropriate advertisement of these prefixes.	配置有委託前綴的網絡應該配置為排除對這些前綴的故意或無意的不適當廣告。

167

CONFIDENTIAL
For Authorized Personnel Only



168

RFC 3646
DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

周立德

國立中央大學主任秘書

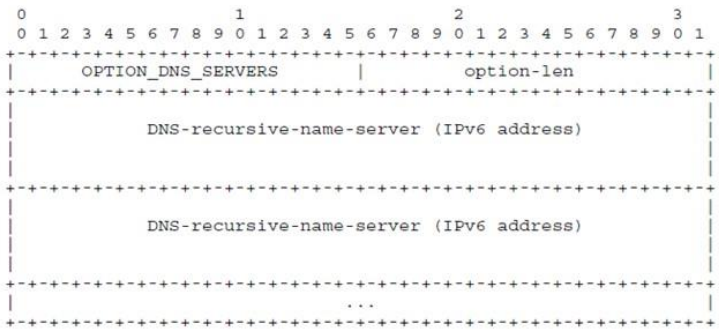
國立中央大學資訊工程學系特聘教授

2019

169

DNS Recursive Name Server option

DNS Recursive Name Server option (DNS 遞迴名稱伺服器選項)	
option-len: Length of the list of DNS recursive name servers in octets; must be a multiple of 16	option-len：八位字節中DNS遞迴名稱伺服器列表的長度; 必須是16的倍數

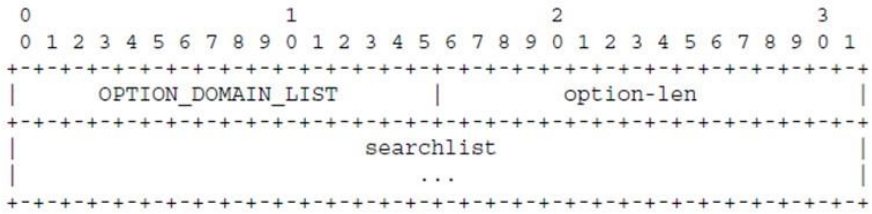


Format of the DNS Recursive Name Server option

CONFIDENTIAL
For Authorized Personnel Only

Domain Search List option (域名搜索列表選項)

Domain Search List option (域名搜索列表選項)	
The list of domain names in the 'searchlist' MUST be encoded as specified in section "Representation and use of domain names" of RFC 3315.	"搜索列表"中的域名列表必須按照RFC 3315的"域名的表示和使用"部分中的規定進行編碼。



Format of the Domain Search List option

CONFIDENTIAL For Authorized Personnel Only

Appearance of these options

Appearance of these options	
The DNS Recursive Name Server option MUST NOT appear in any other than the following messages: Solicit, Advertise, Request, Renew, Rebind, Information-Request, and Reply.	DNS遞歸名稱服務器選項不能出現在以下訊息中：Solicit，Advertise，Request，Renew，Rebind，Information-Request和Reply。
The Domain Search List option MUST NOT appear in any other than the following messages: Solicit, Advertise, Request, Renew, Rebind, Information-Request, and Reply.	域搜索列表選項不能出現在以下消息中：Solicit，Advertise，Request，Renew，Rebind，Information-Request和Reply。

CONFIDENTIAL For Authorized Personnel Only

Security Considerations (安全性考量)

Security Considerations (安全性考量)	
Use searchlists only when explicitly specified; no implicit searchlists should be used.	僅在明確指定時使用搜索列表；不應該使用隱式搜索列表。
Resolve a name containing no dots by appending with the searchlist right away, but once again, no implicit searchlists should be used.	通過立即附加搜索列表來解析不包含點的名稱，但是再一次，不應該使用隱式搜索列表。

CONFIDENTIAL For Authorized Personnel Only

Security Considerations (安全性考量)

Security Considerations (安全性考量)	
Hosts implementing the domain search option SHOULD also implement the searchlist recommendations of RFC1536, section 6.	實現域搜索選項的主機也應該實現RFC1536第6節的搜索列表建議。
Where DNS parameters such as the domain searchlist or DNS servers have been manually configured, these parameters SHOULD NOT be overridden by DHCP.	在手動配置域名搜索列表或DNS服務器等DNS參數的情況下，DHCP不應該覆蓋這些參數。
A host SHOULD require the use of DHCP authentication (see section "Authentication of DHCP messages" in RFC 3315) prior to accepting a domain search option.	在接受域搜索選項之前，主機應該要求使用DHCP身份驗證（請參閱RFC 3315中的"DHCP消息身份驗證"一節）。

CONFIDENTIAL For Authorized Personnel Only



175

國立中央大學
National Central University

Mobile
broadband
networklab

RFC 3736
Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6

周立德

國立中央大學主任秘書

國立中央大學資訊工程學系特聘教授

2019

176

Abstact (摘要)

Abstract (摘要)	
A node that uses stateless DHCP must have obtained its IPv6 addresses through some other mechanism, typically stateless address autoconfiguration.	使用無狀態DHCP的節點必須通過其他一些機制（通常是無狀態地址自動配置）獲取其IPv6地址。
This document explains which parts of RFC 3315 must be implemented in each of the different kinds of DHCP agents so that agent can support stateless DHCP.	本文檔說明了必須在每種不同類型的DHCP代理中實現RFC 3315的哪些部分，以便代理可以支持無狀態DHCP。

CONFIDENTIAL For Authorized Personnel Only

Introduction (介紹)

Introduction (介紹)	
Section 4 of this document lists the sections of the DHCP document that an implementor should read for an overview of the DHCP specification and the basic requirements of a DHCP service.	本文檔的第4部分列出了DHCP文檔的各個部分，實現者應該閱讀這些部分，以了解DHCP規範的概述和DHCP服務的基本要求。

CONFIDENTIAL For Authorized Personnel Only

4. Basic Requirements for Implementation of DHCP

- Several sections of the DHCP specification provide background information or define parts of the specification that are common to all implementations:
- 1-4: give an introduction to DHCP and an overview of DHCP message flows
- 5: defines constants used throughout the protocol specification
- 6, 7: illustrate the format of DHCP messages
- 8: describes the representation of Domain Names
- 9: defines the "DHCP unique identifier" (DUID)
- 13-16: describe DHCP message transmission, retransmission, and validation
- 21: describes authentication for DHCP

179

CONFIDENTIAL
For Authorized Personnel Only



180

國立中央大學 National Central University

RFC 2460
Internet Protocol, Version 6 (IPv6) Specification

周立德

國立中央大學主任秘書

國立中央大學資訊工程學系特聘教授

2019

181

RFC 2460

- 目的
  - 定義 IPv6 封包的基本標頭格式
  - 初步規劃 IPv6 封包中的 extension 和 options 欄位
- 名詞
  - node：使用 IPv6 的裝置
  - router：轉發未明確尋址到自身的 IPv6 packet 的 node
  - host：任何不是 router 的 node
  - upper layer：緊接在 IPv6 之上的 protocol layer
  - link：nodes 之間可以在 link layer 通信的設備或介質
  - neighbors：**附加 (attach)** 在同一 link 上的 nodes
  - interface：node 對 link 的 **附件 (attachment)**
  - address：一個或多個 IPv6 interfaces 的 IPv6-layer 識別碼
  - packet：一個 IPv6 標頭加上 payload
  - link MTU：最大的傳輸單位
  - path MTU：來源端和接收端之間所有 links 中的最小 link MTU

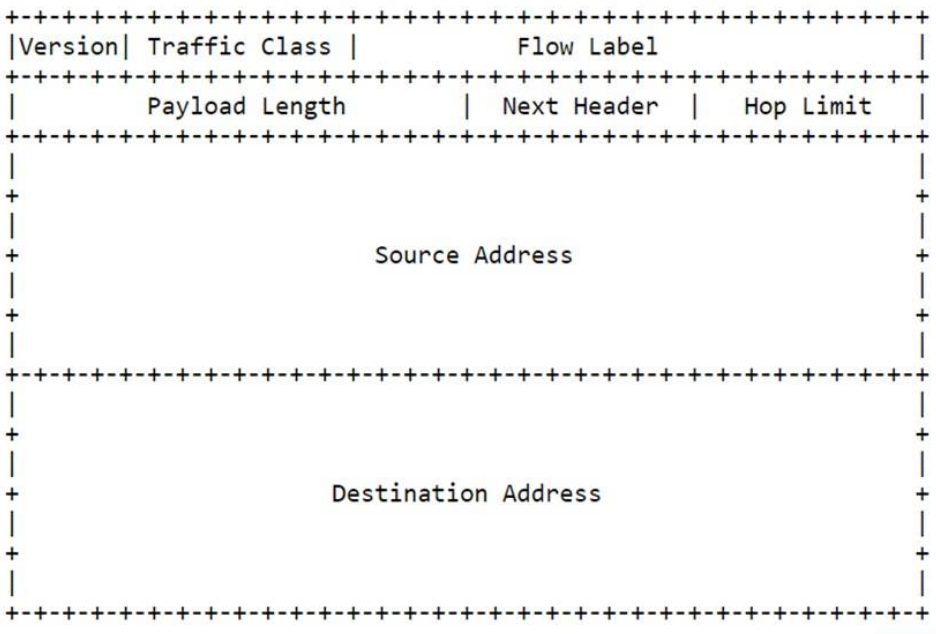
CONFIDENTIAL For Authorized Personnel Only

IPv6 封包格式

- Version：4-bit Internet Protocol 版本號 = 6
- Traffic Class：8-bit 訊務類別 (traffic class) 欄位
- Flow Label：20-bit 訊務流 (flow) 標記
- Payload Length：16-bit 封包標頭 payload 長度，octets格式
  - Octets 以 8 bits 代表一個數字
- Next Header：8-bit 代表下一個標頭的類型，功能同 IPv4
- Hop Limit：8-bit 經過每一節點數值減一，撿到零就丟棄
- Source Address：128-bit 來源端位址
- Destination Address：128-bit 接收端位址
  - 若有 Routing 標頭則可能不為接收端
  - Routing 目的為列出封包會經過的節點

CONFIDENTIAL For Authorized Personnel Only

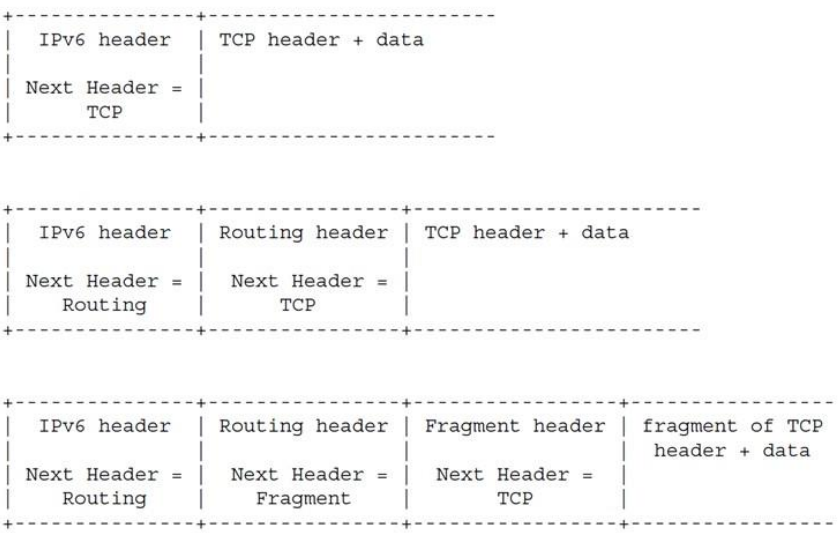
IPv6 封包標頭的格式



CONFIDENTIAL For Authorized Personnel Only

IPv6 Extension Headers

- As illustrated in these examples, an IPv6 packet may carry zero, one, or more extension headers, each identified by the Next Header field of the preceding header:



CONFIDENTIAL For Authorized Personnel Only

IPv6 Extension Headers (擴展標頭)

IPv6 Extension Headers (擴展標頭)	
Extension headers must be processed strictly in the order they appear in the packet.	必須嚴格按照Extension標頭在封包中出現的順序處理它們。
A receiver must not, for example, scan through a packet looking for a particular kind of extension header and process that header prior to processing all preceding ones.	接收方不能掃描尋找特定類型擴展標頭的封包，並在處理所有前面的標頭之前處理該標頭。
The exception referred to in the preceding paragraph is the Hop-by-Hop Options header, which carries information that must be examined and processed by every node along a packet's delivery path, including the source and destination nodes.	前一段中提到的例外是Hop-by-Hop Options標頭，它包含必須由封包傳送路徑上的每個節點檢查和處理的信息，包括來源節點和目的節點。
The Hop-by-Hop Options header, when present, must immediately follow the IPv6 header.	Hop-by-Hop Options標頭（如果存在）必須緊跟IPv6標頭。

CONFIDENTIAL For Authorized Personnel Only

IPv6 Extension Headers (IPv6擴展標頭)

IPv6 Extension Headers (IPv6擴展標頭)	
If, as a result of processing a header, a node is required to proceed to the next header but the Next Header value in the current header is unrecognized by the node, it should discard the packet and send an ICMP Parameter Problem message to the source of the packet, with an ICMP Code value of 1 ("unrecognized Next Header type encountered") and the ICMP Pointer field containing the offset of the unrecognized value within the original packet.	如果由於處理標頭而需要節點繼續進行下一個標頭但節點無法識別當前標頭中的Next Header值，則應該丟棄該封包並向來源端發送ICMP Parameter Problem消息，封包的ICMP代碼值為1（遇到“無法識別的Next Header類型”）和ICMP Pointer欄位包含原始封包中無法識別的值的偏移量。
The same action should be taken if a node encounters a Next Header value of zero in any header other than an IPv6 header.	如果節點在除IPv6標頭之外的任何標頭中遇到Next Header值為零，則應該採取相同的操作。

CONFIDENTIAL For Authorized Personnel Only

Extension Header Order (擴展標頭排序)

Extension Header Order (擴展標頭排序)	
Each extension header should occur at most once, except for the Destination Options header which should occur at most twice (once before a Routing header and once before the upper-layer header).	每個擴展標頭最多應該出現一次，但Destination Options標頭除外，該標頭最多應該出現兩次（一次在Routing標頭之前，一次在高層標頭之前）。
If and when other extension headers are defined, their ordering constraints relative to the above listed headers must be specified.	如果定義了其他擴展標頭，則必須指定它們相對於上面列出的標頭的排序約束。
IPv6 nodes must accept and attempt to process extension headers in any order and occurring any number of times in the same packet, except for the Hop-by-Hop Options header which is restricted to appear immediately after an IPv6 header only.	IPv6節點必須接受並嘗試以任何順序處理擴展標頭，並在同一封包中發生任意次數但Hop-by-Hop Options標頭除外，該標頭僅限於僅在IPv6標頭之後出現。

CONFIDENTIAL For Authorized Personnel Only

Options

- Two of the currently-defined extension headers -- the Hop-by-Hop Options header and the Destination Options header -- carry a variable number of type-length-value (TLV) encoded "options", of the following format:

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+- - - - - - - - -
|  Option Type  |  Opt Data Len |  Option Data
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+- - - - - - - - -
```

Option Type	8-bit identifier of the type of option.
Opt Data Len	8-bit unsigned integer. Length of the Option Data field of this option, in octets.
Option Data	Variable-length field. Option-Type-specific data.

CONFIDENTIAL For Authorized Personnel Only

Options (選項)

Options (選項)	
The sequence of options within a header must be processed strictly in the order they appear in the header; a receiver must not, for example, scan through the header looking for a particular kind of option and process that option prior to processing all preceding ones.	標頭中的選項序列必須嚴格按照它們在標頭中出現的順序進行處理; 例如，接收方不能掃描標題，尋找特定類型的選項，並在處理所有前面的選項之前處理該選項。
The Option Type identifiers are internally encoded such that their highest-order two bits specify the action that must be taken if the processing IPv6 node does not recognize the Option Type.	Option Type標識符是在內部編碼，它們的最高位2位元指定在處理IPv6節點不識別Option Type時必須採取的操作。
When an Authentication header is present in the packet, for any option whose data may change en-route, its entire Option Data field must be treated as zero-valued octets when computing or verifying the packet's authenticating value.	當封包中存在Authentication標頭時，對於其資料可能在途中發生變化的任何選項，在計算或驗證封包的驗證值時，必須將其整個Option Data欄位視為零值八位字節。

CONFIDENTIAL For Authorized Personnel Only

Options (選項)

Options (選項)	
The alignment requirement of an option is specified using the notation xn+y, meaning the Option Type must appear at an integer multiple of x octets from the start of the header, plus y octets.	使用符號xn + y指定選項的對齊要求，這意味著Option Type必須出現在從頭開始加x個八位字節的x個八位字節的整數倍處。
There are two padding options which are used when necessary to align subsequent options and to pad out the containing header to a multiple of 8 octets in length. These padding options must be recognized by all IPv6 implementations.	有兩個填充選項，在必要時用於對齊後續選項並將包含的標題填充到長度為8個八位字節的倍數。 所有IPv6實現都必須識別這些填充選項。
The Pad1 option is used to insert one octet of padding into the Options area of a header. If more than one octet of padding is required, the PadN option, described next, should be used, rather than multiple Pad1 options.	Pad1選項用於將一個八位字節的填充插入標頭的“Option”區域。 如果需要多個填充八位字節，則應該使用下面描述的PadN選項，而不是多個Pad1選項。

CONFIDENTIAL For Authorized Personnel Only

Options

- Pad1 and PadN option

```
Pad1 option  (alignment requirement: none)

   +-+-+-+-+-+-+-+-+
   |       0       |
   +-+-+-+-+-+-+-+-+

   NOTE! the format of the Pad1 option is a special case -- it does
         not have length and value fields.

   The Pad1 option is used to insert one octet of padding into the
   Options area of a header.  If more than one octet of padding is
   required, the PadN option, described next, should be used, rather
   than multiple Pad1 options.

PadN option  (alignment requirement: none)

   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+- - - - - - - - -
   |       1       |  Opt Data Len |  Option Data
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+- - - - - - - - -

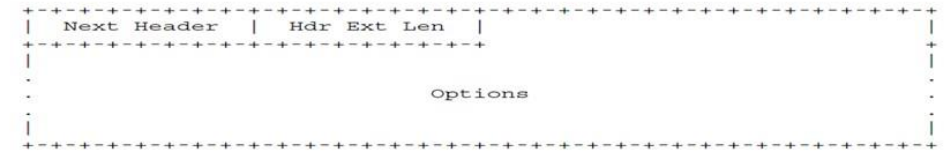
   The PadN option is used to insert two or more octets of padding
   into the Options area of a header.  For N octets of padding, the
   Opt Data Len field contains the value N-2, and the Option Data
   consists of N-2 zero-valued octets.

Appendix B contains formatting guidelines for designing new options.
```


CONFIDENTIAL For Authorized Personnel Only

Hop-by-Hop Options Header (逐跳選項標頭)

Hop-by-Hop Options Header (逐跳選項標頭)	
The Hop-by-Hop Options header is used to carry optional information that must be examined by every node along a packet's delivery path.	Hop-by-Hop Options標頭是用於攜帶必須由封包傳送路徑上的每個節點檢查的可選信息。

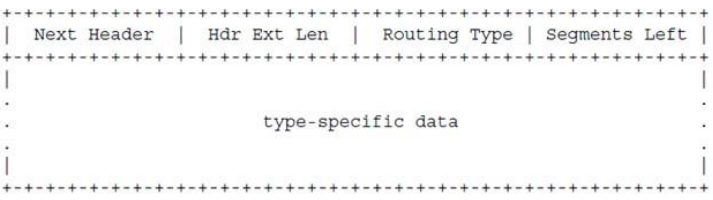


Next Header	8-bit selector. Identifies the type of header immediately following the Hop-by-Hop Options header. Uses the same values as the IPv4 Protocol field [RFC-1700 et seq.].
Hdr Ext Len	8-bit unsigned integer. Length of the Hop-by-Hop Options header in 8-octet units, not including the first 8 octets.
Options	Variable-length field, of length such that the complete Hop-by-Hop Options header is an integer multiple of 8 octets long. Contains one or more TLV-encoded options, as described in section 4.2.

Hop-by-Hop Options Header

CONFIDENTIAL For Authorized Personnel Only

Routing Header

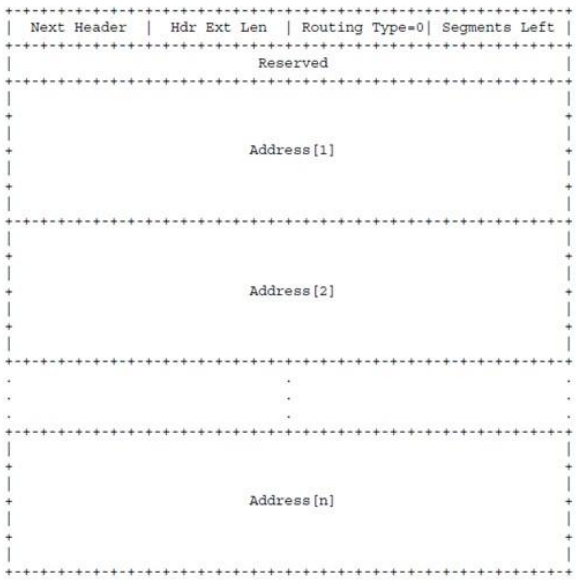


Next Header	8-bit selector. Identifies the type of header immediately following the Routing header. Uses the same values as the IPv4 Protocol field [RFC-1700 et seq.].
Hdr Ext Len	8-bit unsigned integer. Length of the Routing header in 8-octet units, not including the first 8 octets.
Routing Type	8-bit identifier of a particular Routing header variant.
Segments Left	8-bit unsigned integer. Number of route segments remaining, i.e., number of explicitly listed intermediate nodes still to be visited before reaching the final destination.
type-specific data	Variable-length field, of format determined by the Routing Type, and of length such that the complete Routing header is an integer multiple of 8 octets long.

CONFIDENTIAL For Authorized Personnel Only

Routing Header

- The Type 0 Routing header has the following format:



CONFIDENTIAL For Authorized Personnel Only

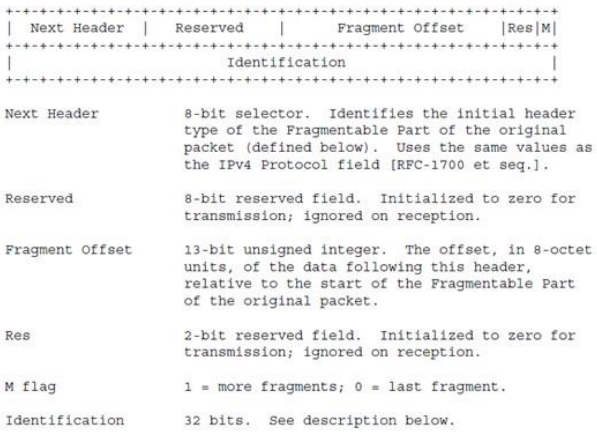
Routing Header (路由標頭)

Routing Header (路由標頭)	
If Segments Left is zero, the node must ignore the Routing header and proceed to process the next header in the packet, whose type is identified by the Next Header field in the Routing header.	如果Segments Left為零，則節點必須忽略Routing標頭並繼續處理封包中的下一個標頭，其類型由Routing標頭中的Next Header欄位標識。
If Segments Left is non-zero, the node must discard the packet and send an ICMP Parameter Problem, Code 0, message to the packet's Source Address, pointing to the unrecognized Routing Type.	如果Segments Left不為零，則節點必須丟棄該封包並向封包的來源地址發送ICMP Parameter Problem, Code 0訊息，指向無法識別的Routing Type。
If, after processing a Routing header of a received packet, an intermediate node determines that the packet is to be forwarded onto a link whose link MTU is less than the size of the packet, the node must discard the packet and send an ICMP Packet Too Big message to the packet's Source Address.	如果在處理接收到的封包的Routing標頭之後，中間節點確定該封包將被轉發到鏈路MTU小於封包大小的鏈路上，則該節點必須丟棄該封包並發送ICMP Packet Too Big到該封包的來源地址。
Multicast addresses must not appear in a Routing header of Type 0, or in the IPv6 Destination Address field of a packet carrying a Routing header of Type 0.	多播地址不能出現在Type 0的Routing標頭中，或出現在攜帶Type 0的Routing標頭的封包的IPv6目標地址欄位中。

CONFIDENTIAL For Authorized Personnel Only

Fragment Header

- The Fragment header is identified by a Next Header value of 44 in the immediately preceding header, and has the following format:

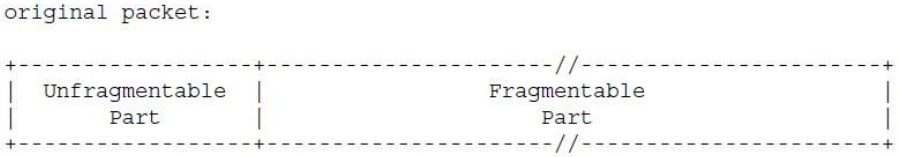


- In order to send a packet that is too large to fit in the MTU of the path to its destination, a source node may divide the packet into fragments and send each fragment as a separate packet, to be reassembled at the receiver.

CONFIDENTIAL For Authorized Personnel Only

Fragment Header

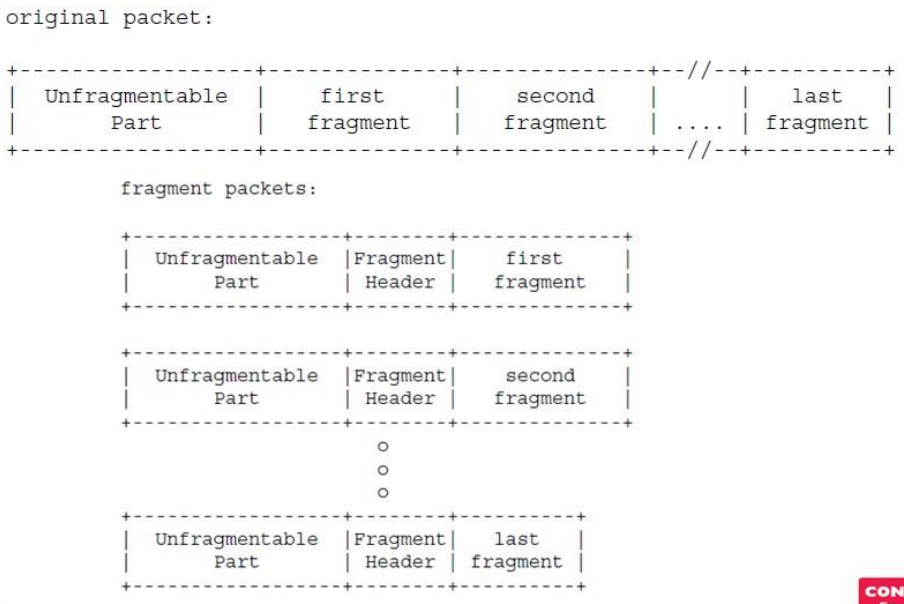
- The initial, large, unfragmented packet is referred to as the "original packet", and it is considered to consist of two parts, as illustrated:



CONFIDENTIAL For Authorized Personnel Only

Fragment Header

- The Fragmentable Part of the original packet is divided into fragments, each, except possibly the last ("rightmost") one, being an integer multiple of 8 octets long. The fragments are transmitted in separate "fragment packets" as illustrated:



CONFIDENTIAL For Authorized Personnel Only

Fragment Header (分段標頭)

Fragment Header (分段標頭)	
The Identification must be different than that of any other fragmented packet sent recently* with the same Source Address and Destination Address.	Identification必須與最近*發送的具有相同來源地址和目標地址的任何其他被分段的封包不同。
The Unfragmentable Part consists of the IPv6 header plus any extension headers that must be processed by nodes en-route to the destination, that is, all headers up to and including the Routing header if present, else the Hop-by-Hop Options header if present, else no extension headers.	Unfragmentable Part由IPv6標頭和任何必須由到達目的地的節點處理的擴展標頭組成即所有標頭，包括Routing標頭（如果存在），否則是Hop-by-Hop Options標頭。目前，否則沒有擴展標頭。

CONFIDENTIAL For Authorized Personnel Only

Fragment Header (分段標頭)

Fragment Header (分段標頭)	
"recently" means within the maximum likely lifetime of a packet, including transit time from source to destination and time spent awaiting reassembly with other fragments of the same packet. However, it is not required that a source node know the maximum packet lifetime. Rather, it is assumed that the requirement can be met by maintaining the Identification value as a simple, 32-bit, "wrap-round" counter, incremented each time a packet must be fragmented. It is an implementation choice whether to maintain a single counter for the node or multiple counters, e.g., one for each of the node's possible source addresses, or one for each active (source address, destination address) combination.	"最近"表示在封包的最大可能生命週期內，包括從來源到目的地的傳輸時間以及等待與同一封包的其他分段重組的時間。但是，來源節點不需要知道最大封包生存期。相反，假設可以通過將Identification值保持為簡單的32位元"wrap-round"計數器來滿足要求，每次必須對封包進行分段時遞增。無論是為節點還是多個計數器維護單個計數器，例如，每個節點的可能源地址一個，或者每個活動（來源地址，目的地址）組合一個計數器，都是一種實現選擇。

CONFIDENTIAL For Authorized Personnel Only

Fragment Header (分段標頭)

Fragment Header (分段標頭)	
The lengths of the fragments must be chosen such that the resulting fragment packets fit within the MTU of the path to the packets' destination(s).	必須適當選擇分段的長度，使得分段封包適合到達封包目的地的路徑上的MTU。
If insufficient fragments are received to complete reassembly of a packet within 60 seconds of the reception of the first-arriving fragment of that packet, reassembly of that packet must be abandoned and all the fragments that have been received for that packet must be discarded.	如果在接收到封包的第一個到達分段的60秒內收到不足的分段以完成該封包的重組則必須放棄該封包的重組，並且必須丟棄已經為該封包接收的所有分段。
If the first fragment (i.e., the one with a Fragment Offset of zero) has been received, an ICMP Time Exceeded -- Fragment Reassembly Time Exceeded message should be sent to the source of that fragment.	如果已收到第一個分段（即Fragment Offset為零的分段），則應該將ICMP Time Exceed – Fragment Reassembly Time Exceeded訊息發送到該分段的來源。

CONFIDENTIAL For Authorized Personnel Only

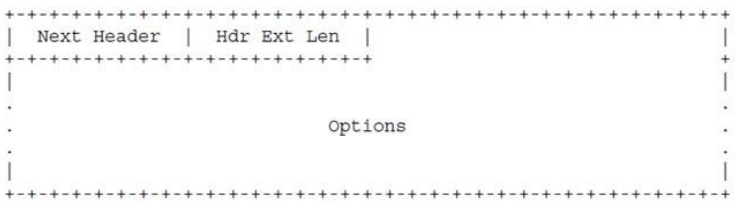
Fragment Header (分段標頭)

Fragment Header (分段標頭)	
If the length of a fragment, as derived from the fragment packet's Payload Length field, is not a multiple of 8 octets and the M flag of that fragment is 1, then that fragment must be discarded and an ICMP Parameter Problem, Code 0, message should be sent to the source of the fragment, pointing to the Payload Length field of the fragment packet.	如果從分段封包的Payload Length欄位導出的分段長度不是8個八位字節的倍數並且該分段的M標誌是1，則必須丟棄該分段並且應該將一個ICMP Parameter Problem, Code 0, 訊息發送到分段的來源，指向分段封包的Payload Length欄位。
If the length and offset of a fragment are such that the Payload Length of the packet reassembled from that fragment would exceed 65,535 octets, then that fragment must be discarded and an ICMP Parameter Problem, Code 0, message should be sent to the source of the fragment, pointing to the Fragment Offset field of the fragment packet.	如果分段的長度和偏移量使得從該分段重新組裝的封包的Payload Length將超過65,535個八位字節，那麼必須丟棄該分段並且應該將一個ICMP Parameter Problem, Code 0, 訊息發送到分段的來源，指向分段封包的Fragment Offset欄位。

Mobile Broadband Networklab, NCU
CONFIDENTIAL For Authorized Personnel Only

Destination Options Header

- The Destination Options header is used to carry optional information that need be examined only by a packet's destination node(s). The Destination Options header is identified by a Next Header value of 60 in the immediately preceding header, and has the following format:



Next Header	8-bit selector. Identifies the type of header immediately following the Destination Options header. Uses the same values as the IPv4 Protocol field [RFC-1700 et seq.].
Hdr Ext Len	8-bit unsigned integer. Length of the Destination Options header in 8-octet units, not including the first 8 octets.
Options	Variable-length field, of length such that the complete Destination Options header is an integer multiple of 8 octets long. Contains one or more TLV-encoded options, as described in section 4.2.

Mobile Broadband Networklab, NCU
CONFIDENTIAL For Authorized Personnel Only

Destination Options Header

- If any other action is desired, the information must be encoded as an option in the Destination Options header whose Option Type has the value 00, 01, or 10 in its highest-order two bits, specifying the desired action.

CONFIDENTIAL For Authorized Personnel Only

Destination Options Header (目的選項標頭)

Destination Options Header (目的選項標頭)	
If any other action is desired, the information must be encoded as an option in the Destination Options header whose Option Type has the value 00, 01, or 10 in its highest-order two bits, specifying the desired action.	如果需要任何其他操作，則必須將信息編碼為Destination Options標頭中的選項，其Option Type的最高位為2位，值為00,01或10，指定所需的操作。

CONFIDENTIAL For Authorized Personnel Only

No Next Header (沒有下一個標頭)

No Next Header (沒有下一個標頭)	
The value 59 in the Next Header field of an IPv6 header or any extension header indicates that there is nothing following that header. If the Payload Length field of the IPv6 header indicates the presence of octets past the end of a header whose Next Header field contains 59, those octets must be ignored, and passed on unchanged if the packet is forwarded.	IPv6標頭或任何擴展標頭的Next Header欄位中的值59表示該標頭後面沒有任何內容。如果IPv6標頭的Payload Length欄位指示在Next Header字段包含59的標頭的末尾之後存在八位字節，則必須忽略這些八位字節並且如果轉發該封包則不改變地傳遞。

CONFIDENTIAL For Authorized Personnel Only

Packet Size Issues (封包大小問題)

Packet Size Issues (封包大小問題)	
On any link that cannot convey a 1280-octet packet in one piece, link-specific fragmentation and reassembly must be provided at a layer below IPv6.	在任何無法傳輸1280字節封包的鏈路上，必須在低於IPv6的層提供特定於鏈路的分段和重組。
Links that have a configurable MTU (for example, PPP links [RFC-1661]) must be configured to have an MTU of at least 1280 octets.	具有可配置MTU的鏈路（例如，PPP鏈路[RFC-1661]）必須配置為具有至少1280個八位字節的MTU。
From each link to which a node is directly attached, the node must be able to accept packets as large as that link's MTU.	從直接連接節點的每個鏈路，節點必須能夠接受與該鏈路的MTU一樣大的封包。
A node must be able to accept a fragmented packet that, after reassembly, is as large as 1500 octets.	節點必須能夠接受分段的封包，在重組後該封包的大小為1500個八位字節。

CONFIDENTIAL For Authorized Personnel Only

Packet Size Issues (封包大小問題)

Packet Size Issues (封包大小問題)	
An upper-layer protocol or application that depends on IPv6 fragmentation to send packets larger than the MTU of a path should not send packets larger than 1500 octets unless it has assurance that the destination is capable of reassembling packets of that larger size.	依賴於IPv6分段來發送大於路徑MTU的數據包的上層協議或應用程序不應該發送大於1500個八位字節的數據包，除非它確保目標能夠重新組合更大的數據包。
In that case, the IPv6 node is not required to reduce the size of subsequent packets to less than 1280, but must include a Fragment header in those packets so that the IPv6-to-IPv4 translating router can obtain a suitable Identification value to use in resulting IPv4 fragments.	在這種情況下，IPv6節點不需要將後續封包的大小減小到小於1280，但必須在這些封包中包含Fragment標頭，以便IPv6到IPv4轉換路由器可以獲得合適的Identification以用於產生IPv4分段。

CONFIDENTIAL For Authorized Personnel Only

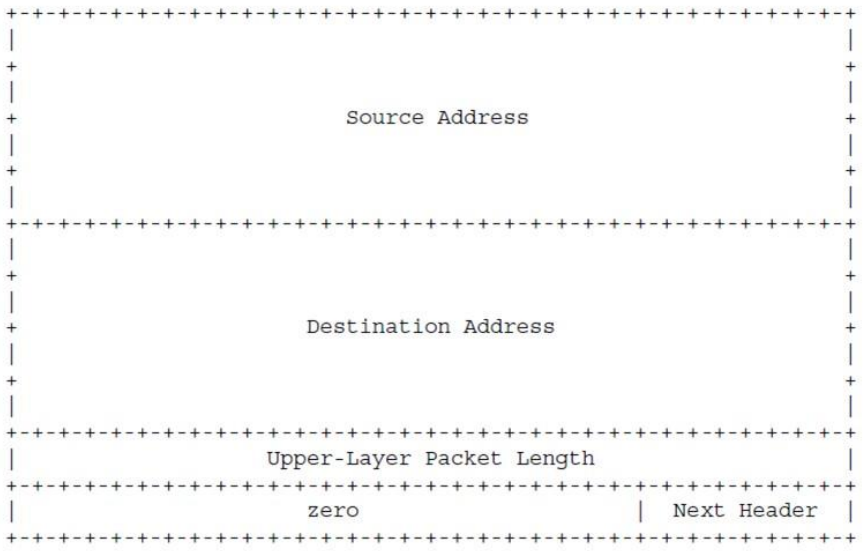
Traffic Classes (訊務類別)

Traffic Classes (訊務類別)	
The service interface to the IPv6 service within a node must provide a means for an upper-layer protocol to supply the value of the Traffic Class bits in packets originated by that upperlayer protocol. The default value must be zero for all 8 bits.	節點內IPv6服務的服務接口必須為上層協議提供一種手段，以便提供由該上層協議發起的封包中的Traffic Class位元的值。 所有8位元的默認值必須為零。
Nodes that support a specific (experimental or eventual standard) use of some or all of the Traffic Class bits are permitted to change the value of those bits in packets that they originate, forward, or receive, as required for that specific use. Nodes should ignore and leave unchanged any bits of the Traffic Class field for which they do not support a specific use.	支持某些或所有Traffic Class位元的特定（實驗或最終標準）使用的節點被允許根據特定用途的需要改變它們發起，轉發或接收的封包中的那些位元的值。 節點應該忽略並保持不支持特定用途的Traffic Class欄位的任何位元。
An upper-layer protocol must not assume that the value of the Traffic Class bits in a received packet are the same as the value sent by the packet's source.	上層協議不能假設接收封包包中的Traffic Class位元的值與封包來源發送的值相同。

CONFIDENTIAL For Authorized Personnel Only

Upper-Layer Checksums

- the following illustration shows the TCP and UDP "pseudo-header" for IPv6:



CONFIDENTIAL For Authorized Personnel Only

Upper-Layer Checksums (上層核對和)

Upper-Layer Checksums (上層核對和)	
Any transport or other upper-layer protocol that includes the addresses from the IP header in its checksum computation must be modified for use over IPv6, to include the 128-bit IPv6 addresses instead of 32-bit IPv4 addresses.	必須修改在其核對和計算中包含來自IP標頭的地址的任何傳輸或其他上層協議，以便在IPv6上使用，以包括128位元IPv6地址而不是32位元IPv4地址。
Whenever originating a UDP packet, an IPv6 node must compute a UDP checksum over the packet and the pseudo-header, and, if that computation yields a result of zero, it must be changed to hex FFFF for placement in the UDP header. IPv6 receivers must discard UDP packets containing a zero checksum, and should log the error.	無論何時發起UDP封包，IPv6節點都必須計算封包和虛擬標頭的UDP核對和，如果該計算結果為零，則必須將其更改為十六進制FFFF以放置在UDP標頭中。IPv6接收器必須丟棄包含零核對和的UDP封包，並應該記錄錯誤。

CONFIDENTIAL For Authorized Personnel Only

Maximum Upper-Layer Payload Size (最大上層有效負載大小)	
When computing the maximum payload size available for upper-layer data, an upper-layer protocol must take into account the larger size of the IPv6 header relative to the IPv4 header.	在計算可用於上層數據的最大有效載荷大小時，上層協議必須考慮相對於IPv4標頭IPv6標頭較大。
When using TCP over IPv6, the MSS must be computed as the maximum packet size minus 60 octets, because the minimum-length IPv6 header (i.e., an IPv6 header with no extension headers) is 20 octets longer than a minimum-length IPv4 header.	當使用基於IPv6的TCP時，必須將MSS計算為最大封包大小減去60個八位字節，因為最小長度IPv6標頭（即，沒有擴展標頭的IPv6報頭）比最小長度IPv4標頭長20個八位字節。

CONFIDENTIAL For Authorized Personnel Only

Responding to Packets Carrying Routing Headers (回應攜帶路由標頭的封包)	
When an upper-layer protocol sends one or more packets in response to a received packet that included a Routing header, the response packet(s) must not include a Routing header that was automatically derived by "reversing" the received Routing header UNLESS the integrity and authenticity of the received Source Address and Routing header have been verified (e.g., via the use of an Authentication header in the received packet).	當上層協議為了回應它所收到的一個包含Routing標頭的封包而發出一個或多個封包時，回應封包不能包括通過“反轉”接收的Routing標頭自動導出的Routing標頭，除非完整性已經驗證了所接收的來源地址和Routing標頭的真實性（例如，通過在所接收的封包中使用認證標頭）。

CONFIDENTIAL For Authorized Personnel Only

Semantics and Usage of the Flow Label Field (流量標籤的語意和用法)	
New flow labels must be chosen (pseudo-)randomly and uniformly from the range 1 to FFFFF hex.	必須從1到FFFFF十六進制範圍內隨機均勻地選擇新流量標籤。
All packets belonging to the same flow must be sent with the same source address, destination address, and flow label.	屬於同一流量的所有封包必須使用相同的來源地址，目標地址和流量標籤發送。
If any of those packets includes a Hop-by-Hop Options header, then they all must be originated with the same Hop-by-Hop Options header contents (excluding the Next Header field of the Hop-by-Hop Options header).	如果這些封包中的任何一個包括Hop-by-Hop Options標頭，那麼它們都必須具有相同的Hop-by-Hop Options標頭內容（不包括Hop-by-Hop Options標頭的Next Header欄位）。
If any of those packets includes a Routing header, then they all must be originated with the same contents in all extension headers up to and including the Routing header (excluding the Next Header field in the Routing header).	如果這些封包中的任何一個包含Routing標頭，那麼它們都必須在所有擴展標頭中包含相同的內容，包括Routing標頭（不包括Routing標頭中的Next Header欄位）。

CONFIDENTIAL For Authorized Personnel Only

Semantics and Usage of the Flow Label Field (流量標籤的語意和用法)	
The routers or destinations are permitted, but not required, to verify that these conditions are satisfied. If a violation is detected, it should be reported to the source by an ICMP Parameter Problem message, Code 0, pointing to the high-order octet of the Flow Label field (i.e., offset 1 within the IPv6 packet).	允許但不要求路由器或目的地驗證是否滿足這些條件。如果檢測到違規，則應該通過將ICMP Parameter Problem消息, Code 0, 回報告給來源，該消息指向流量標籤欄位的高階八位字節（即，IPv6封包內的偏移1）。
The maximum lifetime of any flow-handling state established along a flow's path must be specified as part of the description of the state-establishment mechanism, e.g., the resource reservation protocol or the flow-setup hop-by-hop option.	沿著流量的路徑建立的任何流量處理狀態的最大壽命必須被指定為狀態建立機制的描述的一部分，例如資源預留協議或流量設置逐跳選項。

CONFIDENTIAL For Authorized Personnel Only

Semantics and Usage of the Flow Label Field (流量標籤的語意和用法)	
A source must not reuse a flow label for a new flow within the maximum lifetime of any flow-handling state that might have been established for the prior use of that flow label.	在任何流量處理狀態的最大生命週期內，來源不能為新流量重新用流量標籤，該流程標籤可是能為先前使用而建立的。
When a node stops and restarts (e.g., as a result of a "crash"), it must be careful not to use a flow label that it might have used for an earlier flow whose lifetime may not have expired yet.	當節點停止並重新啟動時（例如，由於“崩潰”），必須小心不要使用它可能已用於其生命週期可能尚未到期的流量的流量標籤。

CONFIDENTIAL For Authorized Personnel Only

Formatting Guidelines for Options (選項格式化指南)	
One desirable feature is that any multi-octet fields within the Option Data area of an option be aligned on their natural boundaries, i.e., fields of width n octets should be placed at an integer multiple of n octets from the start of the Hop-by-Hop or Destination Options header, for n = 1, 2, 4, or 8.	一個理想的特徵是選項的Option Data區域內的任何多八位字節字段在其自然邊界上對齊，即，寬度為n個八位字節的字段應放置在從Hop-by-Hop或Destination Options標頭開始的n個八位字節的整數倍處。適用於n = 1,2,4或8。

CONFIDENTIAL For Authorized Personnel Only



219

國立中央大學
National Central University

Mobile
broadband
networklab

RFC 1981
Path MTU Discovery for IP version 6

周立德
國立中央大學主任秘書
國立中央大學資訊工程學系特聘教授

2019

220

Terminology

- node (節點)：一個實現IPv6的設備
- router (路由器)：轉發未明確尋址到自身的IPv6封包的節點
- host (主機)：任何不是路由器的節點
- upper layer (上層)：緊接在IPv6之上的協定層
- link (鏈結)：節點可以通過的通信設施或介質在鏈結層進行通信
- interface (介面)：節點對鏈結的附件 (attachment)
- address (地址)：介面或一組介面的IPv6層標識符。
- packet (封包)：IPv6標頭加有效負載 (payload)
- link MTU (鏈結MTU)：最大傳輸單元，即可以通過一個鏈結傳送的八位字節的最大封包大小。

CONFIDENTIAL For Authorized Personnel Only

Terminology

- path (路徑)：來源節點和目標節點之間封包遍歷的鏈結集
- path MTU (路徑MTU)：來源節點和目標節點之間路徑中所有鏈結的最小鏈結MTU。
- PMTU (PMTU)：路徑MTU
- Path MTU Discovery (鏈結MTU發現)：節點學習一個路徑的PMTU的過程
- flow (流量)：從特定來源發送到特定（單播或多播）目的地的封包序列，來源要求中間路由器進行特殊處理。
- flow id ()：來源地址和非零流量標籤的組合。

CONFIDENTIAL For Authorized Personnel Only

Introduction (介紹)

Introduction（介紹）	
IPv6 nodes SHOULD implement Path MTU Discovery in order to discover and take advantage of paths with PMTU greater than the IPv6 minimum link MTU [IPv6-SPEC].	IPv6節點應該實現路徑MTU發現，以便發現並利用PMTU大於IPv6最小鏈結MTU [IPv6-SPEC]的路徑。

CONFIDENTIAL For Authorized Personnel Only

Protocol overview (協定概觀)

Protocol overview (協定概觀)	
To detect increases in a path's PMTU, a node periodically increases its assumed PMTU. This will almost always result in packets being discarded and Packet Too Big messages being generated, because in most cases the PMTU of the path will not have changed. Therefore, attempts to detect increases in a path's PMTU should be done infrequently.	為了檢測路徑的PMTU的增加，節點週期性地增加其假設的PMTU。這幾乎總是會導致丟棄封包並生成Packet Too Big消息，因為在大多數情況下，路徑的PMTU不會發生變化。因此，應該不經常嘗試檢測路徑的PMTU中的增加。
Note that Path MTU Discovery must be performed even in cases where a node "thinks" a destination is attached to the same link as itself.	請注意，即使在節點“認為”目標附加到與其自身相同的鏈結的情況下，也必須執行路徑MTU發現。

CONFIDENTIAL For Authorized Personnel Only

Protocol Requirements (協定需求)

Protocol Requirements (協定需求)	
When a node receives a Packet Too Big message, it MUST reduce its estimate of the PMTU for the relevant path, based on the value of the MTU field in the message.	當節點收到Packet Too Big消息時，它必須根據消息中MTU欄位的值減少其對相關路徑的PMTU的估計。
After receiving a Packet Too Big message, a node MUST attempt to avoid eliciting more such messages in the near future. The node MUST reduce the size of the packets it is sending along the path.	在收到Packet Too Big消息後，節點必須嘗試避免在不久的將來引出更多此類消息。節點必須減小它沿路徑發送的封包的大小。
Using a PMTU estimate larger than the IPv6 minimum link MTU may continue to elicit Packet Too Big messages. Since each of these messages (and the dropped packets they respond to) consume network resources, the node MUST force the Path MTU Discovery process to end.	使用大於IPv6最小鏈結MTU的PMTU估計可以繼續引出封包太大消息。由於這些消息中的每一個（以及它們回應的丟棄封包）都消耗網絡資源，因此節點必須強制路徑MTU發現過程結束。
Nodes using Path MTU Discovery MUST detect decreases in PMTU as fast as possible.	使用路徑MTU發現的節點必須盡可能快地檢測PMTU的減少。

Personnel Only

Protocol Requirements (協定需求)

Protocol Requirements (協定需求)	
Nodes MAY detect increases in PMTU, but because doing so requires sending packets larger than the current estimated PMTU, and because the likelihood is that the PMTU will not have increased, this MUST be done at infrequent intervals.	節點可以檢測PMTU的增加，但是因為這樣做需要發送大於當前估計的PMTU的封包，並且因為可能是PMTU不會增加，所以必須在不頻繁的時間間隔完成。
An attempt to detect an increase (by sending a packet larger than the current estimate) MUST NOT be done less than 5 minutes after a Packet Too Big message has been received for the given path.	嘗試檢測增加（通過發送大於當前估計的封包）不能在收到給定路徑的Packet Too Big消息後不到5分鐘內完成。
A node MUST NOT reduce its estimate of the Path MTU below the IPv6 minimum link MTU.	節點不能將路徑MTU的估計值降低到IPv6最小鏈結MTU以下。
A node MUST NOT increase its estimate of the Path MTU in response to the contents of a Packet Too Big message.	節點不能回應Packet Too Big消息的內容而增加其對Path MTU的估計。

CONFIDENTIAL For Authorized Personnel Only

Storing PMTU information (儲存PMTU資訊)

Storing PMTU information (儲存PMTU資訊)	
Ideally, a PMTU value should be associated with a specific path traversed by packets exchanged between the source and destination nodes.	理想情況下，PMTU值應該與來源節點和目標節點之間交換的封包所遍歷的特定路徑相關聯。
However, in most cases a node will not have enough information to completely and accurately identify such a path. Rather, a node must associate a PMTU value with some local representation of a path.	然而，在大多數情況下，節點將沒有足夠的信息來完全準確地識別這樣的路徑。 相反，節點必須將PMTU值與路徑的某個本地表示相關聯。
The local representation of the "path" to a multicast destination must in fact represent a potentially large set of paths.	到多播目的地的“路徑”的本地表示實際上必須表示可能大的路徑集。

CONFIDENTIAL For Authorized Personnel Only

Storing PMTU information (儲存PMTU資訊)

Storing PMTU information (儲存PMTU資訊)	
The packetization layers must be notified about decreases in the PMTU. Any packetization layer instance (for example, a TCP connection) that is actively using the path must be notified if the PMTU estimate is decreased.	必須通知封包包裝層關於PMTU的減少。 如果PMTU估計值降低，則必須通知正在使用該路徑的任何封包包裝層實例（例如TCP連接）。
Also, the instance that sent the packet that elicited the Packet Too Big message should be notified that its packet has been dropped, even if the PMTU estimate has not changed, so that it may retransmit the dropped data.	此外，即使PMTU估計沒有改變，也應該通知發送引發封包太大消息的封包的實例其封包已被丟棄，以便它可以重傳丟棄的資料。

CONFIDENTIAL For Authorized Personnel Only

Storing PMTU information (儲存PMTU資訊)

Storing PMTU information (儲存PMTU資訊)	
It is important to understand that the notification of the packetization layer instances using the path about the change in the PMTU is distinct from the notification of a specific instance that a packet has been dropped. The latter should be done as soon as practical (i.e., asynchronously from the point of view of the packetization layer instance), while the former may be delayed until a packetization layer instance wants to create a packet.	重要的是要理解使用關於PMTU中的改變的路徑的封包包裝層實例的通知不同於已丟棄封包的特定實例的通知。後者應該盡快完成（即，從封包包裝層實例的角度來看是異步的），而前者可以被延遲直到封包包裝層實例想要創建封包。
Retransmission should be done for only for those packets that are known to be dropped, as indicated by a Packet Too Big message.	應該僅針對已知丟棄的那些封包進行重傳，如封包太大消息所示。

CONFIDENTIAL For Authorized Personnel Only

Purging stale PMTU information (清除陳舊的PMTU資訊)

Purging stale PMTU information (清除陳舊的PMTU資訊)	
If the stale PMTU value is too large, this will be discovered almost immediately once a large enough packet is sent on the path. No such mechanism exists for realizing that a stale PMTU value is too small, so an implementation should "age" cached values. When a PMTU value has not been decreased for a while (on the order of 10 minutes), the PMTU estimate should be set to the MTU of the first-hop link, and the packetization layers should be notified of the change. This will cause the complete Path MTU Discovery process to take place again.	如果過時的PMTU值太大，一旦在路徑上發送足夠大的封包，就會立即發現這一點。沒有這樣的機制來實現過時的PMTU值太小，因此實現應該“老化”緩存的值。當PMTU值暫時沒有減少（大約10分鐘）時，應該將PMTU估計設置為第一跳鏈結的MTU，並且應該通知封包包裝層改變。這將導致完整的Path MTU Discovery過程再次發生。
An upper layer must not retransmit data in response to an increase in the PMTU estimate, since this increase never comes in response to an indication of a dropped packet.	上層不能回應於PMTU估計的增加而重新發送資料，因為這種增加永遠不會回應於丟棄封包的指示而來。

CONFIDENTIAL For Authorized Personnel Only

TCP layer actions (TCP階層行為)

TCP layer actions (TCP階層行為)	
The TCP layer must track the PMTU for the path(s) in use by a connection; it should not send segments that would result in packets larger than the PMTU.	TCP層必須跟踪連接使用的路徑的PMTU;它不應該發送會導致封包大於PMTU的段。
A TCP implementation must also store the MSS value received from its peer, and must not send any segment larger than this MSS, regardless of the PMTU.	TCP實現還必須存儲從其對等方接收的MSS值，並且不管PMTU如何，都不能發送大於該MSS的任何段。
The packet size used in the retransmission should be no larger than the new PMTU.	重傳中使用的封包大小應該不大於新PMTU。

CONFIDENTIAL For Authorized Personnel Only

TCP layer actions (TCP階層行為)

TCP layer actions (TCP階層行為)	
Unlike a retransmission caused by a TCP retransmission timeout, a retransmission caused by a Packet Too Big message should not change the congestion window. It should, however, trigger the slow-start mechanism (i.e., only one segment should be retransmitted until acknowledgements begin to arrive again).	與TCP重傳超時引起的重傳不同，由封包太大消息引起的重傳不應該改變擁塞窗口。然而，它應該觸發慢啟動機制（即，只有一個段應該被重傳，直到確認開始再次到達）。
The maximum window size should be set to the greatest multiple of the segment size that is less than or equal to the sender's buffer space size.	最大窗口大小應該設置為小於或等於發送方緩衝區空間大小的段大小的最大倍數。

CONFIDENTIAL For Authorized Personnel Only

Issues for other transport protocols (其他傳輸協定的問題)

Issues for other transport protocols (其他傳輸協定的問題)	
Subsequent segments, when transmitted for the first time, should be no larger than allowed by the Path MTU.	當第一次傳輸時，後續段應該不大於路徑MTU允許的段。
The Sun Network File System (NFS) uses a Remote Procedure Call (RPC) protocol [RPC] that, when used over UDP, in many cases will generate payloads that must be fragmented even for the first-hop link.	Sun網絡文件系統（NFS）使用遠程過程調用（RPC）協議[RPC]，當通過UDP使用時，在許多情況下將生成有效負載，即使對於第一跳鏈結也必須進行分段。
NFS implementations should not reduce the payload size below this threshold, even if Path MTU Discovery suggests a lower value.	即使Path MTU Discovery建議較低的值，NFS實現也不應該將有效負載大小減小到此閾值以下。

CONFIDENTIAL For Authorized Personnel Only

Management interface (管理介面)

Management interface (管理介面)	
The implementation should also provide a way to change the timeout period for aging stale PMTU information.	實現還應該提供一種方法來更改老化的過時PMTU信息的超時時間。

CONFIDENTIAL For Authorized Personnel Only

Security Considerations (安全考量)

Security Considerations (安全考量)	
This Path MTU Discovery mechanism makes possible two denial-of service attacks, both based on a malicious party sending false Packet Too Big messages to a node. In the first attack, the false message indicates a PMTU much smaller than reality. This should not entirely stop data flow, since the victim node should never set its PMTU estimate below the IPv6 minimum link MTU. It will, however, result in suboptimal performance.	此路徑MTU發現機制使兩種拒絕服務攻擊成為可能，這兩種攻擊都基於惡意方向節點發送錯誤的封包太大消息。在第一次攻擊中，虛假消息表明PMTU遠小於現實。這不應該完全停止資料流，因為受害節點不應該將其PMTU估計值設置為低於IPv6最小鏈結MTU。但是，它會導致性能欠佳。

CONFIDENTIAL For Authorized Personnel Only

Security Considerations (安全考量)

Security Considerations (安全考量)	
In the second attack, the false message indicates a PMTU larger than reality. If believed, this could cause temporary blockage as the victim sends packets that will be dropped by some router. Within one round-trip time, the node would discover its mistake (receiving Packet Too Big messages from that router), but frequent repetition of this attack could cause lots of packets to be dropped. A node, however, should never raise its estimate of the PMTU based on a Packet Too Big message, so should not be vulnerable to this attack.	在第二次攻擊中，虛假消息表明PMTU大於現實。如果相信，這可能會導致臨時阻塞，因為受害者會發送一些路由器丟棄的封包。在一個往返時間內，節點將發現其錯誤（從該路由器接收Packet Too Big消息），但頻繁重複此攻擊可能導致丟棄大量封包。但是，節點不應該根據Packet Too Big消息提高其對PMTU的估計，因此不應該容易受到此攻擊。

CONFIDENTIAL For Authorized Personnel Only



237

國立中央大學
National Central University

Mobile
broadband
networklab

RFC 8200
Internet Protocol, Version 6 (IPv6) Specification

周立德
國立中央大學主任秘書
國立中央大學資訊工程學系特聘教授

2019

238

RFC 8200

- 目的
  - 定義 IPv6 封包的基本標頭格式
  - 初步規劃 IPv6 封包中的 extension 和 options 欄位
- 名詞
  - node：使用 IPv6 的裝置
  - router：轉發未明確尋址到自身的 IPv6 packet 的 node
  - host：任何不是 router 的 node
  - upper layer：緊接在 IPv6 之上的 protocol layer
  - link：nodes 之間可以在 link layer 通信的設備或介質
  - neighbors：**附加 (attach)** 在同一 link 上的 nodes
  - interface：node 對 link 的**附件 (attachment)**
  - address：一個或多個 IPv6 interfaces 的 IPv6-layer 識別碼
  - packet：一個 IPv6 標頭加上 payload
  - link MTU：最大的傳輸單位
  - path MTU：來源端和接收端之間所有 links 中的最小 link MTU

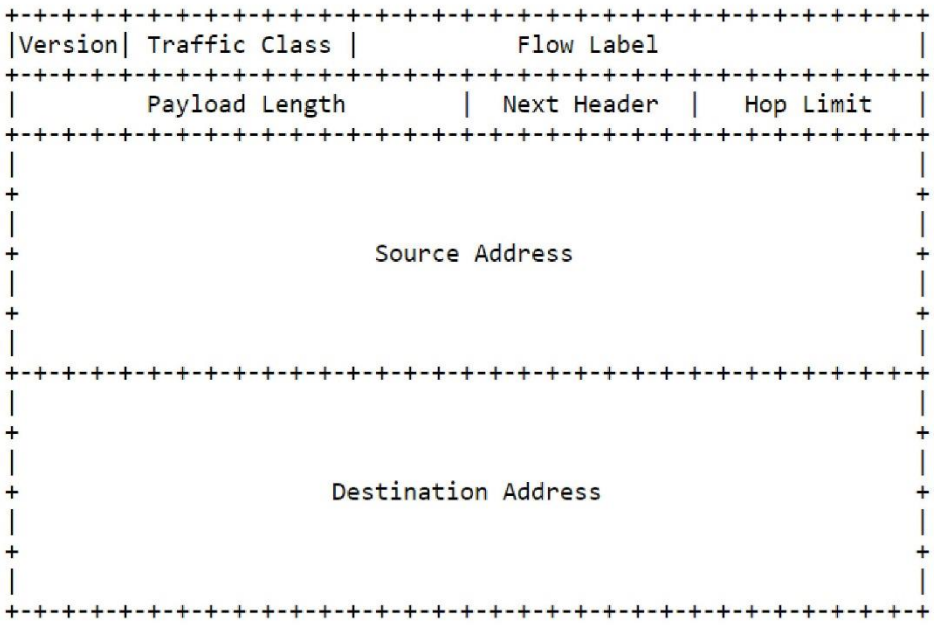
CONFIDENTIAL For Authorized Personnel Only

IPv6 封包格式

- Version：4-bit Internet Protocol 版本號 = 6
- Traffic Class：8-bit 訊務類別 (traffic class) 欄位
- Flow Label：20-bit 訊務流 (flow) 標記
- Payload Length：16-bit 封包標頭 payload 長度，octets格式
  - Octets 以 8 bits 代表一個數字
- Next Header：8-bit 代表下一個標頭的類型，功能同 IPv4
- Hop Limit：8-bit 經過每一節點數值減一，撿到零就丟棄
- Source Address：128-bit 來源端位址
- Destination Address：128-bit 接收端位址
  - 若有 Routing 標頭則可能不為接收端
  - Routing 目的為列出封包會經過的節點

CONFIDENTIAL For Authorized Personnel Only

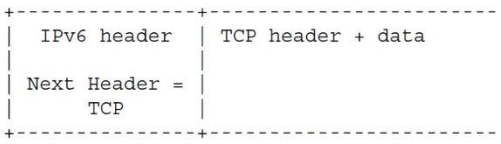
IPv6 封包標頭的格式

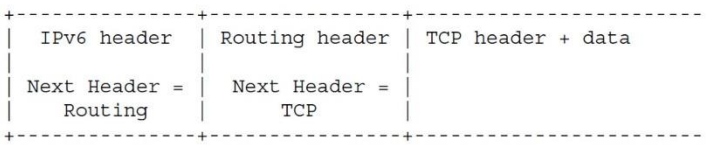


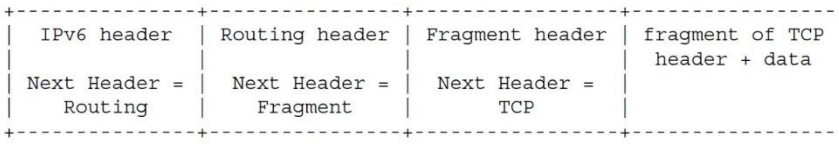
CONFIDENTIAL For Authorized Personnel Only

IPv6 Extension Headers

- As illustrated in these examples, an IPv6 packet may carry zero, one, or more extension headers, each identified by the Next Header field of the preceding header:







CONFIDENTIAL For Authorized Personnel Only

IPv6 Extension Headers (擴展標頭)

IPv6 Extension Headers (擴展標頭)	
The Hop-by-Hop Options header, when present, must immediately follow the IPv6 header.	Hop-by-Hop Options標頭（如果存在）必須緊跟IPv6標頭。
Extension headers must be processed strictly in the order they appear in the packet.	必須嚴格按照Extension標頭在封包中出現的順序處理它們。
A receiver must not, for example, scan through a packet looking for a particular kind of extension header and process that header prior to processing all preceding ones.	接收方不能掃描尋找特定類型擴展標頭的封包，並在處理所有前面的標頭之前處理該標頭。
While [RFC2460] required that all nodes must examine and process the Hop-by-Hop Options header, it is now expected that nodes along a packet's delivery path only examine and process the Hop-by-Hop Options header if explicitly configured to do so.	在[RFC2460]要求所有node必須檢驗和處裡Hop-by-Hop Options header，現在只要求封包傳遞方向備明確要求處裡那個header的處理Hop-by-Hop Options

CONFIDENTIAL For Authorized Personnel Only

Extension Header Order (擴展標頭排序)

Extension Header Order (擴展標頭排序)	
If and when other extension headers are defined, their ordering constraints relative to the above listed headers must be specified.	如果定義了其他擴展標頭，則必須指定它們相對於上面列出的標頭的排序約束。
IPv6 nodes must accept and attempt to process extension headers in any order and occurring any number of times in the same packet, except for the Hop-by-Hop Options header which is restricted to appear immediately after an IPv6 header only.	IPv6節點必須接受並嘗試以任何順序處理擴展標頭，並在同一封包中發生任意次數但Hop-by-Hop Options標頭除外，該標頭僅限於僅在IPv6標頭之後出現。

CONFIDENTIAL For Authorized Personnel Only

Options

- Two of the currently-defined extension headers -- the Hop-by-Hop Options header and the Destination Options header -- carry a variable number of type-length-value (TLV) encoded "options", of the following format:

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+- - - - - - - -
|  Option Type  |  Opt Data Len |  Option Data
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+- - - - - - - -
```

Option Type	8-bit identifier of the type of option.
Opt Data Len	8-bit unsigned integer. Length of the Option Data field of this option, in octets.
Option Data	Variable-length field. Option-Type-specific data.

CONFIDENTIAL For Authorized Personnel Only

Options (選項)

Options (選項)	
The sequence of options within a header must be processed strictly in the order they appear in the header; a receiver must not, for example, scan through the header looking for a particular kind of option and process that option prior to processing all preceding ones.	標頭中的選項序列必須嚴格按照它們在標頭中出現的順序進行處理; 例如，接收方不能掃描標題，尋找特定類型的選項，並在處理所有前面的選項之前處理該選項。
The Option Type identifiers are internally encoded such that their highest-order two bits specify the action that must be taken if the processing IPv6 node does not recognize the Option Type.	Option Type標識符是在內部編碼，它們的最高位2位元指定在處理IPv6節點不識別Option Type時必須採取的操作。
When an Authentication header is present in the packet, for any option whose data may change en-route, its entire Option Data field must be treated as zero-valued octets when computing or verifying the packet's authenticating value.	當封包中存在Authentication標頭時，對於其資料可能在途中發生變化的任何選項，在計算或驗證封包的驗證值時，必須將其整個Option Data欄位視為零值八位字節。

CONFIDENTIAL For Authorized Personnel Only

Options (選項)

Options (選項)	
The alignment requirement of an option is specified using the notation xn+y, meaning the Option Type must appear at an integer multiple of x octets from the start of the header, plus y octets.	使用符號xn + y指定選項的對齊要求，這意味著Option Type必須出現在從頭開始加x個八位字節的x個八位字節的整數倍處。
There are two padding options which are used when necessary to align subsequent options and to pad out the containing header to a multiple of 8 octets in length. These padding options must be recognized by all IPv6 implementations.	有兩個填充選項，在必要時用於對齊後續選項並將包含的標題填充到長度為8個八位字節的倍數。 所有IPv6實現都必須識別這些填充選項。

Mobile Broadband Networklab, NCU
CONFIDENTIAL For Authorized Personnel Only

Options

- Pad1 and PadN option

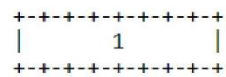
Pad1 option (alignment requirement: none)



NOTE! the format of the Pad1 option is a special case -- it does not have length and value fields.

The Pad1 option is used to insert one octet of padding into the Options area of a header. If more than one octet of padding is required, the PadN option, described next, should be used, rather than multiple Pad1 options.

PadN option (alignment requirement: none)

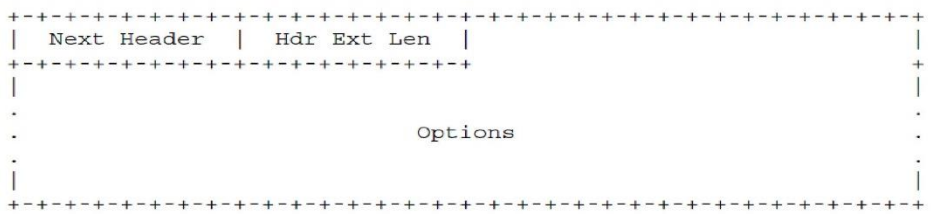


The PadN option is used to insert two or more octets of padding into the Options area of a header. For N octets of padding, the Opt Data Len field contains the value N-2, and the Option Data consists of N-2 zero-valued octets.

Appendix B contains formatting guidelines for designing new options.

Mobile Broadband Networklab, NCU
CONFIDENTIAL For Authorized Personnel Only

Hop-by-Hop Options Header (逐跳選項標頭)

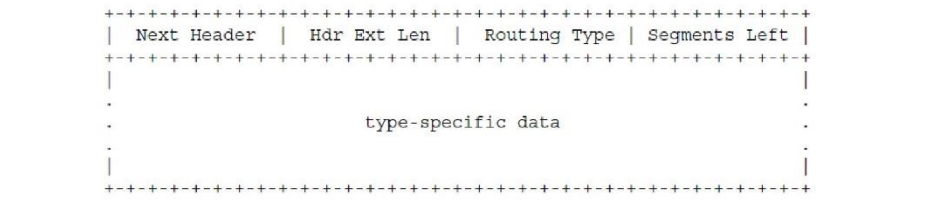


Next Header	8-bit selector. Identifies the type of header immediately following the Hop-by-Hop Options header. Uses the same values as the IPv4 Protocol field [RFC-1700 et seq.].
Hdr Ext Len	8-bit unsigned integer. Length of the Hop-by-Hop Options header in 8-octet units, not including the first 8 octets.
Options	Variable-length field, of length such that the complete Hop-by-Hop Options header is an integer multiple of 8 octets long. Contains one or more TLV-encoded options, as described in section 4.2.

Hop-by-Hop Options Header

CONFIDENTIAL For Authorized Personnel Only

Routing Header

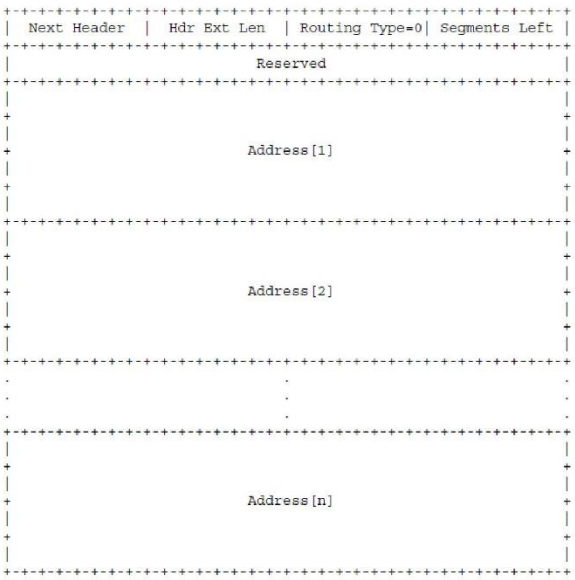


Next Header	8-bit selector. Identifies the type of header immediately following the Routing header. Uses the same values as the IPv4 Protocol field [RFC-1700 et seq.].
Hdr Ext Len	8-bit unsigned integer. Length of the Routing header in 8-octet units, not including the first 8 octets.
Routing Type	8-bit identifier of a particular Routing header variant.
Segments Left	8-bit unsigned integer. Number of route segments remaining, i.e., number of explicitly listed intermediate nodes still to be visited before reaching the final destination.
type-specific data	Variable-length field, of format determined by the Routing Type, and of length such that the complete Routing header is an integer multiple of 8 octets long.

CONFIDENTIAL For Authorized Personnel Only

Routing Header

- The Type 0 Routing header has the following format:



CONFIDENTIAL For Authorized Personnel Only

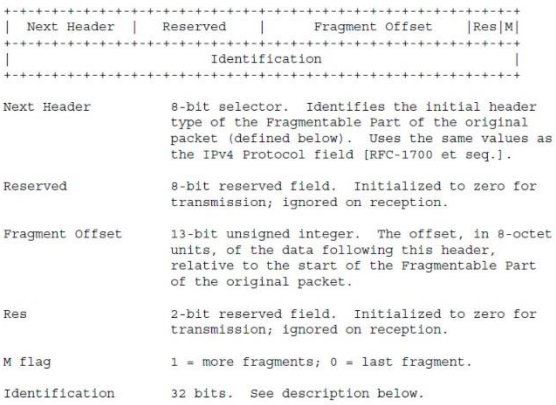
Routing Header (路由標頭)

Routing Header (路由標頭)	
If Segments Left is zero, the node must ignore the Routing header and proceed to process the next header in the packet, whose type is identified by the Next Header field in the Routing header.	如果Segments Left為零，則節點必須忽略Routing標頭並繼續處理封包中的下一個標頭，其類型由Routing標頭中的Next Header欄位標識。
If Segments Left is non-zero, the node must discard the packet and send an ICMP Parameter Problem, Code 0, message to the packet's Source Address, pointing to the unrecognized Routing Type.	如果Segments Left不為零，則節點必須丟棄該封包並向封包的來源地址發送ICMP Parameter Problem, Code 0訊息，指向無法識別的Routing Type。
If, after processing a Routing header of a received packet, an intermediate node determines that the packet is to be forwarded onto a link whose link MTU is less than the size of the packet, the node must discard the packet and send an ICMP Packet Too Big message to the packet's Source Address.	如果在處理接收到的封包的Routing標頭之後，中間節點確定該封包將被轉發到鏈路MTU小於封包大小的鏈路上，則該節點必須丟棄該封包並發送ICMP Packet Too Big到該封包的來源地址。

CONFIDENTIAL For Authorized Personnel Only

Fragment Header

- The Fragment header is identified by a Next Header value of 44 in the immediately preceding header, and has the following format:



- In order to send a packet that is too large to fit in the MTU of the path to its destination, a source node may divide the packet into fragments and send each fragment as a separate packet, to be reassembled at the receiver.

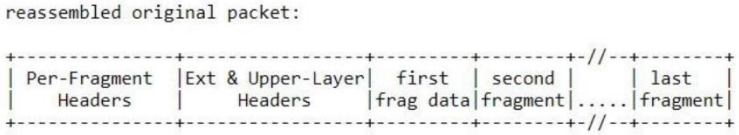
CONFIDENTIAL For Authorized Personnel Only

Fragment Header

- The initial, large, unfragmented packet is referred to as the "original packet", and it is considered to consist of three parts, as illustrated:



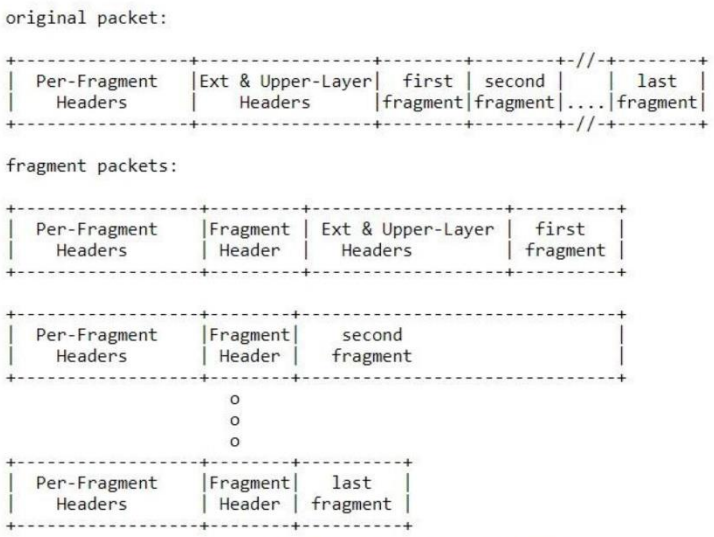
- At the destination, fragment packets are reassembled into their original, unfragmented form, as illustrated:



CONFIDENTIAL For Authorized Personnel Only

Fragment Header

- The Fragmentable Part of the original packet is divided into fragments. The lengths of the fragments must be chosen such that the resulting fragment packets fit within the MTU of the path to the packet's destination(s). Each complete fragment, except possibly the last ("rightmost") one, is an integer multiple of 8 octets long.
- The fragments are transmitted in separate "fragment packets" as illustrated:



CONFIDENTIAL For Authorized Personnel Only

Fragment Header (分段標頭)

Fragment Header (分段標頭)	
The Identification must be different than that of any other fragmented packet sent recently* with the same Source Address and Destination Address.	Identification必須與最近*發送的具有相同來源地址和目標地址的任何其他被分段的封包不同。
The Per-Fragment headers must consists of the IPv6 header plus any extension headers that must be processed by nodes en-route to the destination, that is, all headers up to and including the Routing header if present, else the Hop-by-Hop Options header if present, else no extension headers.	Per-Fragment headers必須由IPv6標頭和任何必須由到達目的地的節點處理的擴展標頭組成，即所有標頭，包括Routing標頭（如果存在），否則是Hop-by-Hop Options標頭。 目前，否則沒有擴展標頭

CONFIDENTIAL For Authorized Personnel Only

Fragment Header (分段標頭)

Fragment Header (分段標頭)	
The lengths of the fragments must be chosen such that the resulting fragment packets fit within the MTU of the path to the packets' destination(s).	必須適當選擇分段的長度，使得分段封包適合到達封包目的地的路徑上的MTU。
The first fragment packet is composed of: Extension headers, if any, and the Upper-Layer header. These headers must be in the first fragment.	第一個分段由Extension headers和如果有Upper-Layer header組成，這些header必須被放在低一個分段
Fragments must not be created that overlap with any other fragments created from the original packet.	被產生的分段不能覆蓋其他被original packet產生的分段
If insufficient fragments are received to complete reassembly of a packet within 60 seconds of the reception of the first-arriving fragment of that packet, reassembly of that packet must be abandoned and all the fragments that have been received for that packet must be discarded.	如果在接收到封包的第一個到達分段的60秒內收到不足的分段以完成該封包的重組則必須放棄該封包的重組，並且必須丟棄已經為該封包接收的所有分段。

CONFIDENTIAL For Authorized Personnel Only

Fragment Header (分段標頭)

Fragment Header (分段標頭)	
If the length of a fragment, as derived from the fragment packet's Payload Length field, is not a multiple of 8 octets and the M flag of that fragment is 1, then that fragment must be discarded and an ICMP Parameter Problem, Code 0, message should be sent to the source of the fragment, pointing to the Payload Length field of the fragment packet.	如果從分段封包的Payload Length欄位導出的分段長度不是8個八位字節的倍數並且該分段的M標誌是1，則必須丟棄該分段並且應該將一個ICMP Parameter Problem, Code 0, 訊息發送到分段的來源，指向分段封包的Payload Length欄位。
If the length and offset of a fragment are such that the Payload Length of the packet reassembled from that fragment would exceed 65,535 octets, then that fragment must be discarded and an ICMP Parameter Problem, Code 0, message should be sent to the source of the fragment, pointing to the Fragment Offset field of the fragment packet.	如果分段的長度和偏移量使得從該分段重新組裝的封包的Payload Length將超過65,535個八位字節，那麼必須丟棄該分段並且應該將一個ICMP Parameter Problem, Code 0, 訊息發送到分段的來源，指向分段封包的Fragment Offset欄位。

CONFIDENTIAL For Authorized Personnel Only

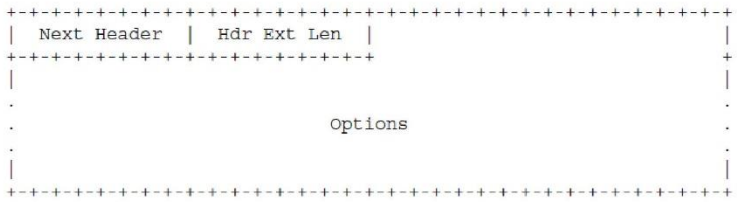
Fragment Header (分段標頭)

Fragment Header (分段標頭)	
If any of the fragments being reassembled overlap with any other fragments being reassembled for the same packet, reassembly of that packet must be abandoned and all the fragments that have been received for that packet must be discarded, and no ICMP error messages should be sent.	如果任何重組分段交疊其他同一個封包的重組分段，那個封包必須被丟棄所有收到的分段也必須被丟棄且沒有ICMP error應該被發送

CONFIDENTIAL For Authorized Personnel Only

Destination Options Header

- The Destination Options header is used to carry optional information that need be examined only by a packet's destination node(s). The Destination Options header is identified by a Next Header value of 60 in the immediately preceding header, and has the following format:



Next Header	8-bit selector. Identifies the type of header immediately following the Destination Options header. Uses the same values as the IPv4 Protocol field [RFC-1700 et seq.].
Hdr Ext Len	8-bit unsigned integer. Length of the Destination Options header in 8-octet units, not including the first 8 octets.
Options	Variable-length field, of length such that the complete Destination Options header is an integer multiple of 8 octets long. Contains one or more TLV-encoded options, as described in section 4.2.

CONFIDENTIAL For Authorized Personnel Only

Destination Options Header (目的選項標頭)

Destination Options Header (目的選項標頭)	
If any other action is desired, the information must be encoded as an option in the Destination Options header whose Option Type has the value 00, 01, or 10 in its highest-order two bits, specifying the desired action.	如果需要任何其他操作，則必須將信息編碼為Destination Options標頭中的選項，其Option Type的最高位為2位，值為00,01或10，指定所需的操作。

CONFIDENTIAL For Authorized Personnel Only

No Next Header (沒有下一個標頭)

No Next Header (沒有下一個標頭)	
The value 59 in the Next Header field of an IPv6 header or any extension header indicates that there is nothing following that header. If the Payload Length field of the IPv6 header indicates the presence of octets past the end of a header whose Next Header field contains 59, those octets must be ignored, and passed on unchanged if the packet is forwarded.	IPv6標頭或任何擴展標頭的Next Header欄位中的值59表示該標頭後面沒有任何內容如果IPv6標頭的Payload Length欄位指示在Next Header字段包含59的標頭的末尾之後存在八位字節，則必須忽略這些八位字節並且如果轉發該封包則不改變地傳遞。

CONFIDENTIAL For Authorized Personnel Only

Defining New Extension Headers and Options

Defining New Extension Headers and Options	
A proposal to specify a new IPv6 extension header must include a detailed technical explanation of why an existing IPv6 extension header can not be used for the desired new function.	提議要建立一個新的IPv6額外的header必須解釋為何現存的IPv6 header不能完成新功能想達到的目的
New extension headers that require hop-by-hop behavior must not be defined because, as specified in Section 4 of this document, the only extension header that has hop-by-hop behavior is the Hop-by-Hop Options header.	不能新增額外需要hop-by-hop behavior的Header，因為文件定義唯一有hop-by-hop行為的extension header只能是Hop-by-Hop Options header
Instead of defining new extension headers, it is recommended that the Destination Options header is used to carry optional information that must be examined only by a packet's destination node(s), because they provide better handling and backward compatibility.	相對於定義一個新的extension header，建議使用只必須被封包的目的地檢查的Destination Options header來攜帶選擇性的資訊，因為它提供更好的維護和後續的相容性

CONFIDENTIAL For Authorized Personnel Only

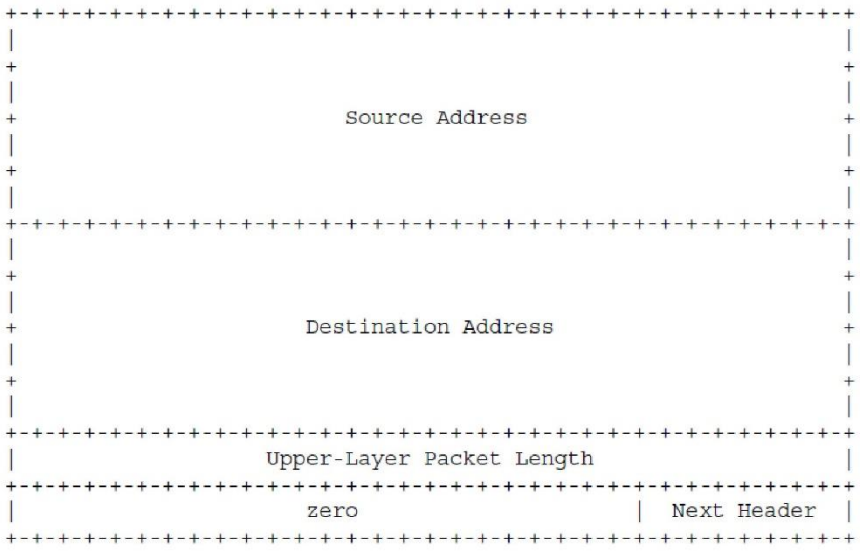
Packet Size Issues (封包大小問題)

Packet Size Issues (封包大小問題)	
On any link that cannot convey a 1280-octet packet in one piece, link-specific fragmentation and reassembly must be provided at a layer below IPv6.	在任何無法傳輸1280字節封包的鏈路上，必須在低於IPv6的層提供特定於鏈路的分段和重組。
Links that have a configurable MTU (for example, PPP links [RFC-1661]) must be configured to have an MTU of at least 1280 octets.	具有可配置MTU的鏈路（例如，PPP鏈路[RFC-1661]）必須配置為具有至少1280個八位字節的MTU。
From each link to which a node is directly attached, the node must be able to accept packets as large as that link's MTU.	從直接連接節點的每個鏈路，節點必須能夠接受與該鏈路的MTU一樣大的封包。
A node must be able to accept a fragmented packet that, after reassembly, is as large as 1500 octets.	節點必須能夠接受分段的封包，在重組後該封包的大小為1500個八位字節。

CONFIDENTIAL For Authorized Personnel Only

Upper-Layer Checksums

- the following illustration shows the TCP and UDP "pseudo-header" for IPv6:



CONFIDENTIAL For Authorized Personnel Only

Upper-Layer Checksums (上層核對和)

Upper-Layer Checksums (上層核對和)	
Any transport or other upper-layer protocol that includes the addresses from the IP header in its checksum computation must be modified for use over IPv6, to include the 128-bit IPv6 addresses instead of 32-bit IPv4 addresses.	必須修改在其核對和計算中包含來自IP標頭的地址的任何傳輸或其他上層協議，以便在IPv6上使用，以包括128位元IPv6地址而不是32位元IPv4地址。
Whenever originating a UDP packet, an IPv6 node must compute a UDP checksum over the packet and the pseudo-header, and, if that computation yields a result of zero, it must be changed to hex FFFF for placement in the UDP header. IPv6 receivers must discard UDP packets containing a zero checksum, and should log the error.	無論何時發起UDP封包，IPv6節點都必須計算封包和虛擬標頭的UDP核對和，如果該計算結果為零，則必須將其更改為十六進制FFFF以放置在UDP標頭中。IPv6接收器必須丟棄包含零核對和的UDP封包，並應該記錄錯誤。
Any node implementing zero-checksum mode must follow the requirements specified in "Applicability Statement for the Use of IPv6 UDP Datagrams with Zero Checksums"	任何node安裝zero-checksum mode必須遵守"Applicability Statement for the Use of IPv6 UDP Datagrams with Zero Checksums"的要求

CONFIDENTIAL For Authorized Personnel Only

Maximum Upper-Layer Payload Size (最大上層有效負載大小)

Maximum Upper-Layer Payload Size (最大上層有效負載大小)	
When computing the maximum payload size available for upper-layer data, an upper-layer protocol must take into account the larger size of the IPv6 header relative to the IPv4 header.	在計算可用於上層數據的最大有效載荷大小時，上層協議必須考慮相對於IPv4標頭IPv6標頭較大。
When using TCP over IPv6, the MSS must be computed as the maximum packet size minus 60 octets, because the minimum-length IPv6 header (i.e., an IPv6 header with no extension headers) is 20 octets longer than a minimum-length IPv4 header.	當使用基於IPv6的TCP時，必須將MSS計算為最大封包大小減去60個八位字節，因為最小長度IPv6標頭（即，沒有擴展標頭的IPv6報頭）比最小長度IPv4標頭長20個八位字節。

CONFIDENTIAL For Authorized Personnel Only

Security Consideration

Security Consideration	
Changed the text to require that IPv6 nodes must not create overlapping fragments.	轉換要求IPv6節點的文字不能產生重疊分段
when reassembling an IPv6 datagram, if one or more of its constituent fragments is determined to be an overlapping fragment, the entire datagram (and any constituent fragments) must be silently discarded.	當重組一個IPv6的datagram，若一個或多個組成的組成的分段被定義為一個重疊的分段整個datagram必須被丟棄

CONFIDENTIAL For Authorized Personnel Only



269

國立中央大學
National Central University

Mobile
broadband
networklab

RFC 8415
Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

周立德
國立中央大學主任秘書
國立中央大學資訊工程學系特聘教授

2019

270

RFC 8415

- 目的
  - 說明DHCPv6的基本規範與功能，讓DHCP server傳送設定參數給網路節點，達到自動IP位址分配的效果。
- IPv6 名詞(1/2)
  - address：interface上IP layer的識別碼
  - GUA : Global unicast address
  - host：不是router的node
  - IP：在本文中專指IPv6
  - interface：一個node與一個link的連接處
  - link：不同node間在link layer的通訊媒介
  - link-layer identifier：interface上link layer的識別碼
  - link-local address：在同個link中讓node可以互相通訊的address
  - multicast address：代表一個interface集合的識別碼。
  - neighbor：在同一個link上的node
  - node：實作IP的裝置

CONFIDENTIAL For Authorized Personnel Only

RFC 8415

- IPv6 名詞(2/2)
  - packet：IP的header加上payload
  - prefix：一個address的起始bits
  - prefix length：prefix中的bit數量
  - router：轉送沒有指明給自己的IP packet
  - ULA : Unique local address
  - unicast address：單一interface的識別碼
- DHCP名詞(1/3)
  - appropriate to the link：一個address符合server對網路拓樸認知
  - binding：一組包含Identity Association的address，或指派給client設定的server資料紀錄
  - Configuration parameter：server上設定資訊中的元素，並透過DHCP傳送給client
  - container option : 一個包裝其他 option 的 option
  - delegating router : 作為 DHCP server ，回應 delegated prefixes 的請求
  - DHCP：DHCPv6
  - (DHCP) client：為了得到configuration parameter在link上發起請求的node
  - (DHCP) server：回應來自client的請求

CONFIDENTIAL For Authorized Personnel Only

RFC 8415

- DHCP名詞(2/3)
  - DHCP domain：一群由DHCP管理的link，由administrative entity操作
  - (DHCP) relay agent：在client和server中負責中繼傳輸DHCP訊息的node
  - DUID：DHCP Unique Identifier，每個DHCP中的node都要有的識別碼
  - encapsulated option : 一個通常只被另一個 option 包含的 DHCP option
  - identity association (IA)：指派給一個client的address集合，每個IA都有一個IAID
  - IA option(s) : 一個或多個 IA_NA, IA_TA, IA_PD options
  - identity association for Prefix Delegation (IA_PD) : 夾帶 delegated prefixes 的IA
  - identity association identifier (IAID)：由client選擇的唯一識別碼
  - identity association for non-temporary addresses (IA_NA)：夾帶要指派的address不是temporary address的IA
  - identity association for temporary addresses (IA_TA)：夾帶temporary address的IA
  - lease : server 發放 address 或 delegated prefix 給特定client 一段時間的合約
  - message：以UDP payload的方式被傳送的資料

CONFIDENTIAL For Authorized Personnel Only

RFC 8415

- DHCP名詞(3/3)
  - reconfigure key：由server提供給client的key，用於提供reconfigure message的安全性
  - relaying：DHCP relay agent中繼傳輸DHCP訊息
  - requesting router : 當作 DHCP client 請求分配 prefixes
  - retransmission : 嘗試從同樣的 client 或 sever 再次發送一樣的 DHCP message
  - RKAP : The Reconfiguration Key Authentication Protocol
  - Singleton option : 一個只被允許出現一次當作一個 top-level option 或當作任何 encapsulation level option
  - T1 : client 應該要聯絡 Sever 使其延長(更新) 位置分配的生命週期或 prefixed delegated 給 client 之後的時間區間
  - T2 : client 應該要聯絡 任何允許的 Sever 使其延長(重新裝訂) 位置分配的生命週期或 prefixed delegated 給 client 的之後時間區間
  - top-level option : 由 DHCP message 直接傳送的 option
  - transaction ID：用於匹配回應的數值

CONFIDENTIAL For Authorized Personnel Only

5.DHCP for prefix Delegation(1/2)

Figure 1 illustrates a network architecture in which prefix delegation could be used.

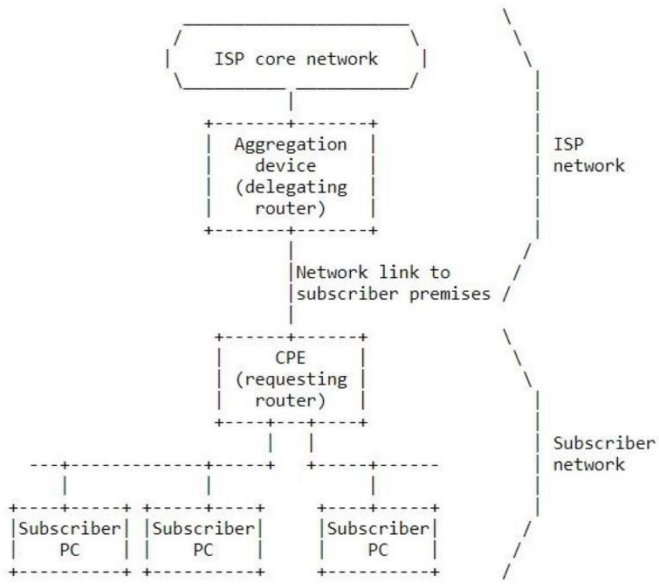


Figure 1: Prefix Delegation Network

CONFIDENTIAL For Authorized Personnel Only

5.DHCP for prefix Delegation(1/2)

DHCP for prefix Delegation	
If the client uses a delegated prefix to configure addresses on interfaces on itself or other nodes behind it, the preferred and valid lifetimes of those addresses MUST be no longer than the remaining preferred and valid lifetimes, respectively, for the delegated prefix at any time	如果client使用delegated prefix來配置在自己或其他在後面的節點的接口上的位置，那些位址的有效和優先的生命週期在任何時候必須分別比剩餘的lifetime短
if the delegated prefix or a prefix derived from it is advertised for stateless address autoconfiguration , the advertised preferred and valid lifetimes MUST NOT exceed the corresponding remaining lifetimes of the delegated prefix.	如果delegated prefix或是prefix是被拿來廣告無狀態的位置配置，那須廣告的優先和有效生命週期不應該超過相對應delegated prefix的剩餘lifetime

CONFIDENTIAL For Authorized Personnel Only

7.Multicast Addresses

Multicast Addresses	
All_DHCP_Relay_Agents_and_Servers (FF02::1:2) • A link-scoped multicast address used by a client to communicate with neighboring (i.e., on-link) relay agents and servers.	All_DHCP_Relay_Agents_and_Servers (FF02::1:2) • Client會透過此multicast address來和relay agents和server溝通
All_DHCP_Servers (FF05::1:3) • A site-scoped multicast address used by a relay agent to communicate with servers. • In order for a relay agent to use this address, it must have an address of sufficient scope to be reachable by the servers.	All_DHCP_Servers (FF05::1:3) • Relay Agent透過此multicast address和server溝通，因此Relay Agent必須在一定的scope內與server溝通

CONFIDENTIAL For Authorized Personnel Only

9. Relay Agent/Server Message格式

兩種Relay Message	
Relay-forward Message: MUST include a "Relay Message option" (see Section 22.10).	Replay-forward Message: 必須加入"Relay Message option" (參考section 22.10)
Relay-reply Message: MUST include a "Relay Message option" (see Section 22.10).	必須加入"Relay Message option" (參考section 22.10)

CONFIDENTIAL For Authorized Personnel Only

10. Domain Names 的表示與使用

Domain Names 的表示與使用	
Domain names may be encoded uniformly, a domain name or a list of domain names is encoded using the technique described in section 3.1 of [RFC1035].	可能會透過section 3.1中所提到的技術將domain names加密
A domain name, or list of domain names, in DHCP MUST NOT be stored in compressed form, as described in Section 4.1.4 of [RFC1035].	在DHCP中不能壓縮domain name，如section 4.14所述)

CONFIDENTIAL For Authorized Personnel Only

11. DHCP Unique Identifier (1/6)

DHCP Unique Identifier (DUID)	
Each DHCP client and server has a DUID.	每個DHCP client或DHCP server都要有個DUID
DHCP servers use DUIDs to identify clients for the selection of configuration parameters and in the association of IAs with clients.	DHCP server透過DUID來辨認client，以選擇設定參數，和IA與client的關聯
DHCP clients use DUIDs to identify a server in messages where a server needs to be identified.	DHCP client透過訊息中的DUID辨認server
Clients and servers MUST treat DUIDs as opaque values and MUST only compare DUIDs for equality.	clients和servers必須將DUID視為opaque value，且必須只將DUID用於比較異同
Clients and servers MUST NOT in any other way interpret DUIDs.	Clients和servers不能以其他形式解析DUID

CONFIDENTIAL For Authorized Personnel Only

11. DHCP Unique Identifier (2/6)

DHCP Unique Identifier (DUID)	
Clients and servers MUST NOT restrict DUIDs to the types defined in this document, as additional DUID types may be defined in the future.	Clients和server不能只將DUID限制於這份文件中所定義的型別，未來可能還會定義新的DUID型別
The DUID is carried in an option because it may be variable length and because it is not required in all DHCP messages.	DUID會放在option欄位，因為它的長度可能會變動，且不一定要出現在所有的DHCP訊息中
The DUID used by a client or server SHOULD NOT change over time.	clients和servers所使用的DUID不應該隨著時間變換
The DUID must be globally unique, and must also be easy to generate.	DUID必須是唯一的，且必須容易產生
Some devices may not contain any persistent storage, so the DUID scheme must accommodate such devices.	有些裝置可能沒有永久性的儲存空間，因此DUID的方案必須適應這些裝置

CONFIDENTIAL For Authorized Personnel Only

11. DHCP Unique Identifier (3/6)

DUID Based on Link-layer Address Plus Time (DUID-LLT)	
The hardware type MUST be a valid hardware type assigned by the IANA as described in [RFC826].	硬體型別必須是IANA規定在[RFC826]中的正當型別
The same DUID-LLT SHOULD be used in configuring all network interfaces connected to the device.	一樣的DUID-LLT應該用於設定該裝置上所有的網路interface
Clients and servers using this type of DUID MUST store the DUID-LLT in stable storage, and MUST continue to use this DUID-LLT even if the network interface used to generate the DUID-LLT is removed.	clients和servers必須將DUID-LLT存在穩定的儲存裝置中，且即使用於生產此DUID-TTL的interface已經從裝置上一除了，也必須持續使用該DUID-LLT
Clients and servers that do not have any stable storage MUST NOT use this type of DUID.	clients和servers若沒有穩定的儲存裝置，則不能使用這種類型的DUID

CONFIDENTIAL For Authorized Personnel Only

11. DHCP Unique Identifier (4/6)

DUID Based on Link-layer Address Plus Time (DUID-LLT)	
Clients and servers that use this DUID SHOULD attempt to configure the time prior to generating the DUID.	使用這種DUID的clients或servers應該在產生DUID前設定好時間
MUST use some sort of time source (for example, a real-time clock) in generating the DUID.	必須使用某種時間來源方式 (如現實時間) 來產生DUID
A DHCP client that generates a DUID-LLT using this mechanism MUST provide an administrative interface that replaces the existing DUID with a newly-generated DUID-LLT.	使用這種方式產生DUID的DHCP client必須提供一個管理介面，讓新的DUID-TTL可以取代現有的DUID

CONFIDENTIAL For Authorized Personnel Only

11. DHCP Unique Identifier (5/6)

DUID Assigned by Vendor Based on Enterprise Number (DUID-EN)	
Each identifier part of each DUID-EN MUST be unique to the device that is using it, and MUST be assigned to the device at the time it is manufactured and stored in some form of non-volatile storage.	每個DUID-EN中的identifier part必須在使用它的的裝置中是唯一的，且必須在裝置被製造時被指定，並存在穩定的儲存裝置中
The generated DUID SHOULD be recorded in non-erasable storage.	所產生的DUID應該被記錄在非揮發性的儲存裝置

CONFIDENTIAL For Authorized Personnel Only

11. DHCP Unique Identifier (6/6)

DUID Based on Link-layer Address (DUID-LL)	
The hardware type MUST be a valid hardware type assigned by the IANA, as described in [RFC826].	硬體型別必須是IANA規定在[RFC826]中的正當型別
The same DUID-LL SHOULD be used in configuring all network interfaces connected to the device.	一樣的DUID-LLT應該用於設定該裝置上所有的網路interface
DUID-LL MUST NOT be used by DHCP clients or servers that cannot tell whether or not a network interface is permanently attached to the device on which the DHCP client is running.	DHCP client或DHCP server若無法判別一個網路interface是否會永久在該裝置上，則不能使用DUID-LL

CONFIDENTIAL For Authorized Personnel Only

12. Identity Association (1/3)

Identity Association (IA)	
A construct through which a server and a client can identify, group, and manage a set of related IPv6 addresses.	IA是server和client可以透過一組互相關聯的IPv6 address識別、群組、和管理的結構
Each IA consists of an IAID and associated configuration information.	每個IA由IAID和相關的設定資訊組成

CONFIDENTIAL For Authorized Personnel Only

12. Identity Association (2/3)

Identity Association (IA)	
The IAID uniquely identifies the IA and must be chosen to be unique among the IAIDs on the client.	一個IAID可以代表一個IA且必須在client上的所有IAIDs中是唯一的
For any given use of an IA by the client, the IAID for that IA MUST be consistent across restarts of the DHCP client.	給client所使用的IA，其IAID必須在client重啟時仍保持一致
A client must associate at least one distinct IA with each of its network interfaces.	一個client的每個網路interface必須至少關聯一個IA
Each IA must be associated with exactly one interface.	每個IA必須剛好關聯一個interface
The client may maintain consistency either by storing the IAID in non-volatile storage or by using an algorithm that will consistently produce the same IAID.	Client可能會透過將IAID儲存在非揮發裝置中或是使用一套演算法可以產生相同的IAID

CONFIDENTIAL For Authorized Personnel Only

12. Identity Association (3/3)

Identity Associations for Prefix Delegation	
A client configured to request delegated prefixes must create at least one distinct IA_PD	Client 配置請求 delegated prefixes 應該要生成至少一個不同的 IA_PD

CONFIDENTIAL For Authorized Personnel Only

13. 選擇給IA的位址

選擇給IA的位址	
According to [RFC6221], the server MUST ignore any link-address field whose value is zero	根據RFC6221，server必須忽視任何質零的 link-address field
A server MUST NOT assign an address that is otherwise reserved for some other purpose.	server不能指派為了其他目的保留的 address
A server MUST NOT assign reserved anycast addresses, as defined in [RFC2526], from any subnet.	server不能指派從任何subnet保留的 anycast address ([RFC2526])

CONFIDENTIAL For Authorized Personnel Only

14. Rate Limiting(1/2)

Rate Limiting	
In order to avoid prolonged message bursts that may be caused by possible logic loops, a DHCP client MUST limit the rate of DHCP messages it transmits or retransmits.	為了避免因為可能的邏輯迴圈而造成的過長的訊息突然過多出現，DHCP client必須限制DHCP 訊息的傳送率或重傳率
a client must not initiate transmissions too frequently.	Client 不應該初始化傳送太頻繁
For a device that has multiple interfaces, the limit MUST be enforced on a per-interface basis.	若 device 有多個介面，限制應該基於每個介面

CONFIDENTIAL For Authorized Personnel Only

14. Rate Limiting(2/2)

Client Behavior when T1 and/or T2 Are 0	
When T1 and/or T2 values are set to 0, the client MUST choose a time to avoid packet storms.	當T1或T2 其一之質或皆為零，client 必須選擇一個時間來避免packet storm
it MUST NOT transmit immediately.	不該立即被傳送
The client MUST choose renew and rebind times to not violate rate-limiting restrictions as defined in Section 14.1.	Client 應該選擇更新和重新綁定時間

CONFIDENTIAL For Authorized Personnel Only

15. 由Client發起的訊息交換可信度 (1/2)

RT	Retransmission timeout
IRT	Initial retransmission time
MRC	Maximum retransmission count
MRT	Maximum retransmission time
MRD	Maximum retransmission duration
RAND	Randomization factor

CONFIDENTIAL For Authorized Personnel Only

15. 由Client發起的訊息交換可信度 (2/2)

由Client發起的訊息交換可信度	
If a DHCP client fails to receive an expected response from a server, the client must retransmit its message.	若DHCP client從server沒有接收到應該要收到的回應，client必須重送請求
The client MUST update an "elapsed-time" value within an Elapsed Time option in the retransmitted message.	Client 必須在重傳訊息中透過Elapsed Time option更新經過時間
If RT expires before the message exchange terminates, the client recomputes RT and retransmits the message.	若在訊息交換結束前RT就過期，client會重新計算RT並重送訊息

CONFIDENTIAL For Authorized Personnel Only

15. 由Client發起的訊息交換可信度 (3/3)

由Client發起的訊息交換可信度	
Each of the computations of a new RT include a randomization factor (RAND), which is a random number chosen with a uniform distribution between -0.1 and +0.1.	每次新RT的計算會包含一個介於-0.1與+0.1常態分佈的亂數
The algorithm SHOULD produce a different sequence of random numbers from each invocation of the DHCP client.	演算法應該從每個DHCP client的調用產生亂數的不同序號
a client MUST listen for a Reconfigure if it has negotiated for its use with the server.	Client如果已經和server溝噌過她的使用方式則client應該要聆聽重新配置

CONFIDENTIAL For Authorized Personnel Only

16. 訊息驗證(1/14)

訊息驗證	
Clients, relay agents, and servers MUST NOT discard messages that contain unknown options (or instances of vendor options with unknown enterprise-number values).	Clients和relay agents 和servers 不能拋棄包含未知option的message(或具有未知企業編號值的vendor option的例子)
A server MUST discard any Solicit, Confirm, Rebind or Information-request messages it receives with a unicast destination address.	server必須丟棄任何目標位址是unicast address的solicit、confirm、rebind或Information-request message
A client or server MUST discard any received DHCP messages with an unknown message type.	Client或 server 必須丟棄任何收到含有未知訊息形式的DHCP訊息

CONFIDENTIAL For Authorized Personnel Only

16. 訊息驗證(2/14)

Transaction IDs 的用途	
The "transaction-id" field holds a value used by clients and servers to synchronize server responses to client messages.	“transcation-id”的欄位放置了clients和servers所使用的值來同步server對client的回覆訊息
A client SHOULD generate a random number that cannot easily be guessed or predicted to use as the transaction ID for each new message it sends	client應該為每個其新產的訊息生一個不會被輕易猜到的亂數作為transaction ID
A client MUST leave the transaction ID unchanged in retransmissions of a message.	client在重送的訊息中必須讓transaction ID維持不變

CONFIDENTIAL For Authorized Personnel Only

16. 訊息驗證(3/14)

Solicit Message	
Clients MUST discard any received Solicit messages.	client必須丟棄任何接收到的solicit message
Servers MUST discard any Solicit messages that do not include a Client Identifier option or that do include a Server Identifier option.	server必須丟棄任何沒有包含client和Server Identifier option的solicit message

CONFIDENTIAL For Authorized Personnel Only

16. 訊息驗證(4/14)

Advertise Message	
Clients MUST discard any received Advertise messages that meet any of the following conditions: • The message does not include a Server Identifier option. • The message does not include a Client Identifier option. • The contents of the Client Identifier option does not match the client's DUID. • The "transaction-id" field value does not match the value the client used in its Solicit message.	client必須丟棄任何符合以下任一條件的advertise message: • 沒有包含Server Identifier option • 沒有包含Client Identifier option • client的識別碼選項跟client的DUID不匹配 • “transaction-id”欄位的值和clien在solicit message所用的值不匹配
Servers and relay agents MUST discard any received Advertise messages.	server和relay agent必須丟棄任何advertise message

CONFIDENTIAL For Authorized Personnel Only

16. 訊息驗證(5/14)

Request Message	
Clients MUST discard any received Request messages.	clients必須丟棄任何request message
Servers MUST discard any received Request message that meet any of the following conditions: • The message does not include a Server Identifier option. • The contents of the Server Identifier option do not match the server's DUID. • The message does not include a Client Identifier option.	Servers必須丟棄任何符合以下任一條件的request message: • 沒有包含Server Identifier option • Server Identifier option中的內容跟server的DUID不匹配 • 不包含Client Identifier option

CONFIDENTIAL For Authorized Personnel Only

16. 訊息驗證(6/14)

Confirm Message	
Clients MUST discard any received Confirm messages.	clients必須丟棄任何confirm message
Servers MUST discard any received Confirm messages that do not include a Client Identifier option or that do include a Server Identifier option.	server必須丟棄任何不包含server和client是別選項的confirm message

CONFIDENTIAL For Authorized Personnel Only

16. 訊息驗證(7/14)

Renew Message	
Clients MUST discard any received Renew messages.	clients必須丟棄任何renew message
Servers MUST discard any received Renew message that meets any of the following conditions: • The message does not include a Server Identifier option. • The contents of the Server Identifier option does not match the server's identifier. • The message does not include a Client Identifier option.	server必須丟棄任何符合以下任一條件的renew message: • 不包含Server Identifier option • Server Identifier option中的內容和server識別碼不匹配 • 不包含Client Identifier option

CONFIDENTIAL For Authorized Personnel Only

16. 訊息驗證(8/14)

Rebind Message	
Clients MUST discard any received Rebind messages.	clients必須丟棄任何rebind message
Servers MUST discard any received Rebind messages that do not include a Client Identifier option or that do include a Server Identifier option.	server必須丟棄任何沒有包含client和Server Identifier option的rebind message

CONFIDENTIAL For Authorized Personnel Only

16. 訊息驗證(9/14)

Decline Message	
Clients MUST discard any received Decline messages.	clients必須丟棄任何decline message
Servers MUST discard any received Decline message that meets any of the following conditions: • The message does not include a Server Identifier option. • The contents of the Server Identifier option does not match the server's identifier. • The message does not include a Client Identifier option.	servers必須丟棄符合以下任一條件的decline message: • 不包含server是別選項 • 在Server Identifier option中的內容與server的識別碼不匹配 • 不包含Client Identifier option

CONFIDENTIAL For Authorized Personnel Only

16. 訊息驗證(10/14)

Release Message	
Clients MUST discard any received Release messages.	clients必須丟棄任何release message
Servers MUST discard any received Release message that meets any of the following conditions: • The message does not include a Server Identifier option. • The contents of the Server Identifier option does not match the server's identifier. • The message does not include a Client Identifier option.	Server必須丟棄任何符合以下任一條件的release message: • 不包含Server Identifier option • Server Identifier option中的內容和server識別碼不匹配 • 不包含Client Identifier option

CONFIDENTIAL For Authorized Personnel Only

16. 訊息驗證(11/14)

Reply Message	
Clients MUST discard any received Reply message that meets any of the following conditions: • The message does not include a Server Identifier option. • The "transaction-id" field in the message does not match the value used in the original message.	clients必須丟棄任何符合以下任一條件的reply message: • 不包含Server Identifier option • “transaction-id”欄位中的值和原來訊息中的值不匹配
If the client included a Client Identifier option in the original message, the Reply message MUST include a Client Identifier option.	若client在原本的訊息中包含Client Identifier option，reply message必須包含Client Identifier option

CONFIDENTIAL For Authorized Personnel Only

16. 訊息驗證(12/14)

Reply Message	
And the contents of the Client Identifier option MUST match the DUID of the client	Client Identifier option中的內容必須和client的DUID匹配
If the client did not include a Client Identifier option in the original message, the Reply message MUST NOT include a Client Identifier option	若client沒有在原本的訊息物中包含Client Identifier option，則reply message不能包含Client Identifier option
Servers and relay agents MUST discard any received Reply messages.	servers和relay agents必須丟棄任何reply message

CONFIDENTIAL For Authorized Personnel Only

16. 訊息驗證(13/14)

Reconfigure Message	
Servers and relay agents MUST discard any received Reconfigure messages.	server和relay agents必須丟棄任何Reconfigure message
Clients MUST discard any Reconfigure messages that meets any of the following conditions: • The message was not unicast to the client. • The message does not include a Server Identifier option. • The message does not include a Client Identifier option that contains the client's DUID. • The message does not contain a Reconfigure Message option and the msg-type must be a valid value. • The message includes any IA options and the msg-type in the Reconfigure Message option is INFORMATION-REQUEST. • The message does not include DHCP authentication	clients必須丟棄任何符合以下任一條件 的Reconfigure message: • 不是以unicast傳給client • 沒有包含Server Identifier option • 沒有包含client的DUID在Client Identifier option中 • 沒有包含Reconfigure Message選項且msg-type要是正確的 • 包含IA選項和msg-type是INFORMATION-REQUSET • 沒有包含DHCP驗證

CONFIDENTIAL For Authorized Personnel Only

16. 訊息驗證(14/14)

Information-request	
Clients MUST discard any received Information-request messages.	clients必須丟棄任何Information-request message
Servers MUST discard any received Information-request message that meets any of the following conditions: • The message includes a Server Identifier option and the DUID in the option does not match the server's DUID. • The message includes an IA option.	servers必須丟棄任何符合以下條件的Information-request message: • Server Identifier option中的DUID和server的DUID不匹配 • 包含了IA選項
Relay-forward Message	
Clients MUST discard any received Relay-forward messages.	Clients必須丟棄任何Relay-forward message
Relay-reply Message	
Clients and servers MUST discard any received Relay-reply messages.	Clients和servers都必須丟棄任何Relay-reply message

CONFIDENTIAL For Authorized Personnel Only

17. Client的來源Address和Interface選擇

Client的來源Address和Interface選擇	
When a client sends a DHCP message to the All_DHCP_Relay_Agents_and_Servers address, it SHOULD send the message through the interface for which configuration information is being requested.	當client傳送DHCP訊息給All_DHCP_Relay_Agents_and_Servers的address時，應該要透過需要被資訊設定的interface發送
When a client sends a DHCP message directly to a server using unicast, the source address in the header of the IP datagram MUST be an address assigned to the interface.	當client透過unicast直接傳送一個DHCP訊息給server時，IP封包header中的source address必須是interface被指派的address

CONFIDENTIAL For Authorized Personnel Only

18.DHCP 配置交換(1/29)

DHCP 配置交換	
The client MUST NOT be using any of the addresses or delegated prefixes for which it tries to obtain the bindings by sending the Solicit message.	Client不能使用任何client試圖透過傳送solicit message來獲得binding的address或delegated prefixes
if the client had some valid bindings and has chosen to start the server discovery process to obtain the same bindings from a different server, the client MUST stop using the addresses and delegated prefixes for the bindings that it had obtained from the previous server and that it is now trying to obtain from a new server.	如果client擁有一些有效的binding且被選為開始尋找sever程序用來從其他的sever獲得一樣得binding時，client必須停止使用從前一個server獲得和正在嘗試從新sever獲得的的addresses和delegated prefixes

CONFIDENTIAL For Authorized Personnel Only

18.DHCP 配置交換 Client(2/29)

適用於多IA Options的簡單交換	
To facilitate a client's use of a single transaction for all IA options, servers MUST return the same T1/T2 values for all IA options in a Reply so that the client will generate a single transaction when renewing or rebinding its leases.	為了促使 client利用單一交換來符合所有IA options，server必須在一個Reply中的所有IA option回傳相同的 T1/T2值使得client 將會再renewing或rebinding client的租用時產生一個單一交換當
because some servers may not yet conform to this requirement, a client MUST be prepared to select appropriate T1/T2 times.	因為有些server 可能還沒符合這個要求，client必須準備好選擇適當的T1/T2時間
Client behavior	
The client SHOULD be suspicious of the Reconfigure message (they may be faked), and it MUST NOT abandon any resources it might have already obtained.	Client應該懷疑重新配置的message是否為真，而且client不能放棄任何已經取得的資源

CONFIDENTIAL For Authorized Personnel Only

18.DHCP 配置交換 Client(3/29)

Creation and Transmission of Solicit Messages	
Creation of Solicit Message • The client MUST include a Client Identifier option to identify itself to the server. • The client MUST NOT include any other options in the Solicit message, except as specifically allowed in the definition of individual options. • The client MUST include an Option Request option (see section 21.7) to request the SOL_MAXRT option and any other options the client is interested in receiving. • The client MUST NOT include any other options in the Solicit message, except as specifically allowed in the definition of individual options.	Solicit Message的產生： • client必須包含一個Client Identifier option • client不能包含任何其它option，除非有私人特別允許 • Client必須包含一個Option Request option來請求SOL_MAXRT option和任何client有興趣收到的option • Client不能在Solicit message內包含任何其他option，除了特別允許的單一option

CONFIDENTIAL For Authorized Personnel Only

18.DHCP 配置交換 Client(4/29)

Creation and Transmission of Solicit Messages

Transmission of Solicit Messages

- The message exchange is not terminated by the receipt of an Advertise before the first RT has elapsed. Rather, the client collects Advertise messages until the first RT has elapsed. Also, the first RT MUST be selected to be strictly greater than IRT by choosing RAND to be strictly greater than 0.
- A client MUST collect Advertise messages for the first RT seconds, unless it receives an Advertise message with a preference value of 255
- If the DHCP client is configured with either MRC or MRD set to a value other than 0, it MUST stop trying to configure the interface if the message exchange fails.

Solicit Message的傳送：

- 在RT到期前收到Advertise，訊息交換都還不會結束。相反，client蒐集advertise message直到第一個RT到期。因此第一個RT必須大於IRT，透過選擇RAND大於0達成
- 一個client必須蒐集Advertise message直到第一次RT到期，除非它收到了performance value是255的Advertise message
- 當DHCP client的MRC或MRD被設為非零的值，如果message交換失敗client必須停止嘗試配置那個interface

CONFIDENTIAL For Authorized Personnel Only

18.DHCP 配置交換 Client(5/29)

Creation and Transmission of Request Messages

- The client MUST include the identifier of the destination server in a Server Identifier option
- The client MUST include a Client Identifier option (see Section 21.2) to identify itself to the server.
- The client MUST include an Elapsed Time option (see Section 21.9) to indicate how long the client has been trying to complete the current DHCP message exchange.
- The client MUST include an Option Request option (see Section 21.7) to request the SOL_MAX_RT option (see Section 21.24) and any other options the client is interested in receiving.

- Client必須包含在Server identifier option裡的destination server的身分識別
- Client 必須包含一個client identifier option，用來表明自己身分告訴server.
- Client 必須包含一個經過時間option用來指示client已經花多少時間在完成現在的DHCP message交換
- Client 必須包含一個 Option Request option用來要求SOL_MAX_RT option和其他client 有興趣收到的option

CONFIDENTIAL For Authorized Personnel Only

18.DHCP 配置交換 Client(6/29)

Creation and Transmission of Confirm Messages

- The client MUST include a Client Identifier option (see Section 21.2) to identify itself to the server.
- The client MUST include an Elapsed Time option (see Section 21.9) to indicate how long the client has been trying to complete the current DHCP message exchange.
- The first Confirm message from the client on the interface MUST be delayed by a random amount of time between 0 and CNF_MAX_DELAY.

- Client 必須包含一個client identifier option，用來表明自己身分告訴server.
- Client 必須包含一個經過時間option用來指示client已經花多少時間在完成現在的DHCP message交換
- 第一個在interface上從client來的Confirm message必須延遲隨機時間從0到CNF_MAX_DELAY

Mobile Broadband Networklab, NCU
CONFIDENTIAL For Authorized Personnel Only

18.DHCP 配置交換 Client(7/29)

Creation and Transmission of Renew Messages

- As the client SHOULD renew/rebind all IAs from the server at the same time, the client MUST select T1 and T2 times from all IA options that will guarantee that the client initiates transmissions of Renew/Rebind messages not later than at the T1/T2 times associated with any of the client's bindings
- A client MUST also initiate a Renew/Reply message exchange before time T1 if the client's link-local address used in previous interactions with the server is no longer valid and it is willing to receive Reconfigure messages.
- As the client SHOULD renew/rebind all IAs from the server at the same time, the client MUST select T1 and T2 times from all IA options that will guarantee that the client initiates transmissions of Renew/Rebind messages not later than at the T1/T2 times associated with any of the client's bindings

- 當client應該同時renew或rebind所有從Server來的IAs，client必須從所有IA option中選擇T1及T2時間確保client最初始的Renew/Rebind傳送訊息沒有比和其他有關連的client的binding的T1/T2時間還晚
- 如果client之前用來和server互動的link-local address已失效且client願意收到重新配置message，Client 必須在T1時間前初始化Renew/Reply message exchange
- 當client應該同時renew或rebind所有從Server來的IAs，client必須從所有IA option中選擇T1及T2時間確保client最初始的Renew/Rebind傳送訊息沒有比和其他有

18.DHCP 配置交換 Client(8/29)

Creation and Transmission of Renew Messages

- A client MUST also initiate a Renew/Reply message exchange before time T1 if the client's link-local address used in previous interactions with the server is no longer valid and it is willing to receive Reconfigure messages.
- If T1 or T2 had been set to 0 by the server (for an IA_NA or IA_PD) or there are no T1 or T2 times (for an IA_TA) in a previous Reply, the client may, at its discretion, send a Renew or Rebind message, respectively. The client MUST follow the rules defined in Section 14.2.
- The client MUST include a Server Identifier option (see Section 21.3) in the Renew message, identifying the server with which the client most recently communicated.

- 關連的client的binding的T1/T2時間還晚
- 如果client之前用來和server互動的link-local address已失效且client願意收到重新配置message，Client 必須在T1時間前初始化Renew/Reply message exchange
- 如果T1或T2在前一個reply已經透過Server被設為0，或沒有T1/T2時間，client可能考慮分別傳送一個Renew或Rebind message，client必須遵守定義在Section 14.2的規則
- Client必須在Renew message內包含一個Serve Identifier message，識別最近害clien聯絡過的server

CONFIDENTIAL For Authorized Personnel Only

18.DHCP 配置交換 Client(9/29)

Creation and Transmission of Renew Messages

- The client MUST include a Client Identifier option (see Section 21.2) to identify itself to the server.
- The client MUST include an Elapsed Time option (see Section 21.9) to indicate how long the client has been trying to complete the current DHCP message exchange
- The client MUST NOT include addresses and prefixes in any IA option that the client did not obtain from the server or that are no longer valid (that have a valid lifetime of 0).

- Client 必須包含一個client identifier option，用來表明自己身分告訴server.
- Client 必須包含一個經過時間option用來指示client已經花多少時間在完成現在的DHCP message交換
- client不能包含不是從sever或已經無效在IA option的任何address和prefix

CONFIDENTIAL For Authorized Personnel Only

18.DHCP 配置交換 Client(10/29)

Creation and Transmission of Information-request Messages

- The client MUST include an Elapsed Time option (see Section 21.9) to indicate how long the client has been trying to complete the current DHCP message exchange.
- The client MUST include an Option Request option (see Section 21.7) to request the INF_MAX_RT option (see Section 21.25), the Information Refresh Time option (see Section 21.23), and any other options the client is interested in receiving.
- The first Information-request message from the client on the interface MUST be delayed by a random amount of time between 0 and INF_MAX_DELAY.

- Client 必須包含一個經過時間option用來指示client已經花多少時間在完成現在的DHCP message交換
- Client 必須包含一個 Option Request option 用來要求INF_MAX_RT option和the Information Refresh Time option和其他client 有興趣收到的option
- 第一個在interface上從client來的Information-request message必須延遲隨機時間從0到INF_MAX_DELAY

Mobile Broadband Networklab, NCU
CONFIDENTIAL For Authorized Personnel Only

18.DHCP 配置交換 Client(11/29)

Creation and Transmission of Release Messages

- The client MUST include a Client Identifier option (see Section 21.2) to identify itself to the server.
- The client MUST include an Elapsed Time option (see Section 21.9) to indicate how long the client has been trying to complete the current DHCP message exchange.
- The leases to be released MUST be included in the IAs.
- Any leases for the IAs the client wishes to continue to use MUST NOT be added to the IAs.
- The client MUST stop using all of the leases being released before the client begins the Release message exchange process.

- Client 必須包含一個client identifier option，用來表明自己身分告訴server.
- Client 必須包含一個經過時間option用來指示client已經花多少時間在完成現在的DHCP message交換
- 被釋放的租用必須被包含在IA裡面
- 任何client希望繼續使用的IA租用不能被加進IA裡面

Mobile Broadband Networklab, NCU
CONFIDENTIAL For Authorized Personnel Only

18.DHCP 配置交換 Client(12/29)

Creation and Transmission of Release Messages

- The client MUST stop using all of the leases being released before the client begins the Release message exchange process.
- For an address, this means the address MUST have been removed from the interface.
- For a delegated prefix, this means the prefix MUST have been advertised with a Preferred Lifetime and a Valid Lifetime of 0 in a Router Advertisement message
- The client MUST NOT use any of the addresses it is releasing as the source address in the Release message or in any subsequently transmitted message.

- Client在開始Release message交換前必須停止使用所有被釋放的租用
- 上述意思表示，address必須已經從interface中被移除
- 上述意思表示，prefix必須已經透過Router advertisement message被廣告告知一個preferred lifetime跟valid time為0
- Client不能使用任何在release message或subsequently transmitted message被釋放出來當作source address的address

Mobile Broadband Networklab, NCU
CONFIDENTIAL For Authorized Personnel Only

18.DHCP 配置交換 Client(13/29)

Creation and Transmission of Decline Messages

- The Decline message is not used in prefix delegation; thus, the client MUST NOT include IA_PD options (see Section 21.21) in the Decline message.
- The client MUST include a Client Identifier option (see Section 21.2) to identify itself to the server
- The client MUST include an Elapsed Time option (see Section 21.9) to indicate how long the client has been trying to complete the current DHCP message exchange.
- The addresses to be declined MUST be included in the IAs.
- The client MUST NOT use any of the addresses it is declining as the source address in the Decline message or in any subsequently transmitted message.

- Decline message 不被用在prefix delegation，因此client不能包含IA_PD option在Decline message裡
- Client 必須包含一個client identifier option，用來表明自己身分告訴server
- Client 必須包含一個經過時間option用來指示client已經花多少時間在完成現在的DHCP message交換
- 要被decline的address必須被包含在IAs裡
- Client不能使用任何在decline message或subsequently transmitted message被decline來當作source address的address

Mobile Broadband Networklab, NCU
CONFIDENTIAL For Authorized Personnel Only

18.DHCP 配置交換 Client(14/29)

Receipt of Advertise Messages	
• The client MUST process any SOL_MAX_RT option and INF_MAX_RT option present in an Advertise message, even if the message contains a Status Code option indicating a failure, and the Advertise message will be discarded by the client. • The client MUST ignore any Advertise message that contains no addresses, with the exception that the client: - MUST process an included SOL_MAX_RT option and - MUST process an included INF_MAX_RT option.	• Client必須處理呈現在Advertise message的任何SOL_MAX_RT option和INF_MAX_RT option，即便message包含的Status code option指示為失敗且此Advertise message將被client捨棄 • Client必須忽略任何不包含address的Advertise message但必須處理包含SOL_MAX_RT option和SOL_MAX_RT option的message
The client ignoring an Advertise message MUST NOT restart the Solicit retransmission timer.	• Client忽略一個Advertise message不能重新開始Solicit retransmission timer

CONFIDENTIAL For Authorized Personnel Only

18.DHCP 配置交換 Client(15/29)

Receipt of Reply Messages	
• The client MUST process any SOL_MAX_RT option and INF_MAX_RT option present in an Reply message, even if the message contains a Status Code option indicating a failure, and the Advertise message will be discarded by the client. • If the client retransmits the original message to the same server to retry the desired operation, the client MUST limit the rate at which it retransmits the message and limit the duration of the time during which it retransmits the message.	• Client必須處理呈現在Reply message的任何SOL_MAX_RT option和INF_MAX_RT option，即便message包含的Status code option指示為失敗且此Advertise message將被client捨棄 • 如果client重傳原始的message給同一個server來重新嘗試她想要的動作，client必須限制重新傳送的速率和限制重新傳送訊息的經過時間
a client that previously received an NTP server address from the DHCP server and does not receive it anymore MUST stop using the configured NTP server address.	• 先前從DHCP Server拿到NTP Server address的但再也沒拿到過了的Client必須停止使用配置的NTP Server address

CONFIDENTIAL For Authorized Personnel Only

18.DHCP 配置交換 Client(16/29)

Reply for Solicit, Request, Renew, or Rebind	
The client MUST perform duplicate address detection [17] on each of the addresses in any IAs it receives in the Reply message before using that address for traffic.	Client在使用IA中的address傳送流量前必須執行duplicate address detection (DAD)
For each assigned address that does not have any associated reachability information, in order to avoid the problems described in [RFC4943], the client MUST NOT assume that any addresses are reachable on-link as a result of receiving an IA_NA or IA_TA.	對那些被指派不包含任何associated reachability information的address，為了避免在[RFC4943]的問題，client不能假設任何收到 IA_NA或IA_TA的address是reachable on-link
Addresses obtained from an IA_NA or IA_TA MUST NOT be used to form an implicit prefix with a length other than 128.	那些從IA_NA或IA_TA獲得的address不能被用來形成一個不明確長度不是128的prefix

CONFIDENTIAL For Authorized Personnel Only

18.DHCP 配置交換 Client(17/29)

Reply for Solicit, Request, Renew, or Rebind	
When a client subnets a delegated prefix, it must assign additional bits to the prefix to generate unique, longer prefixes.	當client遮住一個delegated prefix，他必須指派額外的bit給prefix用來產稱獨特且更長的prefix
• If the client uses a delegated prefix to configure addresses on interfaces on itself or other nodes behind it, the preferred and valid lifetimes of those addresses MUST be no longer than the remaining preferred and valid lifetimes, respectively, for the delegated prefix at any time. • if the delegated prefix or a prefix derived from it is advertised for stateless address autoconfiguration, the advertised preferred and valid lifetimes MUST NOT exceed the corresponding remaining lifetimes of the delegated prefix.	• 如果client用delegated prefix來配置在自己或其他在他後面的節點的介面時，那些address的preferred跟valid的lifetime必須比剩餘的preferred跟valid的lifetime短，對於任何時間的delegated prefix • 如果delegated prefix或從他取得的是用來廣告無狀態address的autoconfiguration，廣告的preferred跟valid的lifetime不能超過對應的delegated prefix的剩餘lifetime
The client MUST rate-limit its transmissions and MAY just wait for the normal retransmission time.	Client必須rate-limit他的傳送且等待一般的重傳時間

CONFIDENTIAL For Authorized Personnel Only

18.DHCP 配置交換 Client(18/29)

Receipt of Reconfigure Messages	
Once the client has received a Reconfigure, the client proceeds with the message exchange; the client MUST ignore any additional Reconfigure messages until the exchange is complete.	一旦client收到重新配置client繼續進行message交換，client必須忽視任何額外的重新配置message直到交換完成
Refreshing Configuration Information	
If the client has any valid delegated prefixes obtained from the DHCP server, the client MUST initiate a Rebind/Reply message exchange as described in Section 18.2.5, with the exception that the retransmission parameters should be set as for the Confirm message.	如果client有任何有效從DHCP serve獲得的的delegated prefix，client必須初始化Rebind/Reply message exchange，且retransmission parameter應該設為符合confirm message
If the client has only obtained network information using Information-request/Reply message exchanges, the client MUST initiate an Information-request/Reply message exchange as described in Section 18.2.6.	如果Client只利用Information-request/Reply message exchanges獲得網路資訊，client必須初始化Information-request/Reply message 交換
a client MUST rate-limit such attempts to avoid flooding a server with requests when there are link issues	當出現連線問題時Client必須rate-limit試圖避免用request flooding server

TIAL For Authorized Personnel Only

18.DHCP 配置交換 Server(19/29)

Server Behavior	
• This Reply message MUST always contain the Server Identifier option containing the server's DUID and the Client Identifier option from the client message if one was present. • The server must be aware of the recommendations on packet sizes and the use of fragmentation in section 5 of [RFC2460]. • The server MUST use the received message to construct the proper Relay-reply message to allow the response to the received message to be relayed through the same relay agents (in reverse order) as the original client message.	• 這個Reply message必須包含有著server DUID的Server Identifier option，以及從client訊息中來的Client Identifier option • Server必須注意在[RFC2460 section 5]中的封包大小 • Server必須使用received message來建立適當的Relay-reply message來允許回應給received message可以使用相同的relay agent

CONFIDENTIAL For Authorized Personnel Only

18.DHCP 配置交換 Server(20/29)

Receipt of Solicit Messages	
• The server MUST commit the assignment of any addresses and delegated prefixes or other configuration information before sending a Reply message to a client.	• Server必須在傳送reply訊息給client前保證任何address和delegated prefix 或其他配置資訊

CONFIDENTIAL For Authorized Personnel Only

18.DHCP 配置交換 Server(21/29)

Receipt of Request Messages	
Receipt of Request Messages • The server MUST include a Server Identifier option containing the server's DUID and the Client Identifier option from the Request message in the Reply message. • If any of the prefixes of the included addresses are not appropriate for the link to which the client is connected, the server MUST return the IA to the client with a Status Code option with the value NotOnLink • If the server does not send the NotOnLink status code but it cannot assign any IP addresses to an IA, the server MUST return the IA option in the Reply message with no addresses in the IA and a Status Code option containing status code NoAddrsAvail in the IA.	Request Message的接收 • Server必須加入包含server DUID的Server Identifier option，以及在Request message中的Client Identifier option • 若server發現IA中的任何prefix不適合這個link，server必須回傳Status Code option為NotOnLink的IA給client • 若server沒有傳送NotOnLink status code但serve不能分配任何IP address給IA，server必須在reply message中回傳沒有address 在IA裡在IA option中且包含NoAddrsAvail在IA裡在Status Code option中

CONFIDENTIAL For Authorized Personnel Only

18.DHCP 配置交換 Server(22/29)

Receipt of Request Messages

Receipt of Request Messages
- For any IA_PD option in the Request message to which the server cannot assign any delegated prefixes, the server MUST return the IA_PD option in the Reply message with no prefixes in the IA_PD and with a Status Code option containing status code NoPrefixAvail in the IA_PD.
- The server MUST NOT include any addresses or delegated prefixes in the IA that the server does not assign to the client.
- The T1/T2 times set in each applicable IA option for a Reply MUST be the same values across all IAs.
- The server MUST determine the T1/T2 times across all of the applicable client's bindings in the Reply.
- The server MUST NOT cache its responses.

Request Message的接收
- 對任何Server不能分配任何delegated prefixes的Request message裡的IA_PD option，server必須在Reply message裡的IA_PD option表示IA_PD沒有prefix和 Status Code option裡表示在IA_PD中NoPrefixAvail
- Server不能在Server沒分配給client的IA包含任何addresses或delegated prefixes
- 被設定在可適用於reply的IA option裡的T1/T2時間必須和所有IA一樣
- Sever必須決定所有綁在reply裡可適用的client的T1/T2時間
- Server不能cache他的回應

CONFIDENTIAL For Authorized Personnel Only

18.DHCP 配置交換 Server(23/29)

Receipt of Confirm Messages

Receipt of Confirm Messages
- If the server is unable to perform this test, or there were no addresses in any of the IAs sent by the client, the server MUST NOT send a reply to the client.
- The server MUST include a Server Identifier option containing the server's DUID and the Client Identifier option from the Confirm message in the Reply message.

Confirm Message的接收
- 若server無法執行測試，或client並沒有在IA中傳送address，server則不能傳送reply給client
- Server必須在Reply Message中加入包含server DUID的Server Identifier option，以及在Confirm message中的Client Identifier option

CONFIDENTIAL For Authorized Personnel Only

18.DHCP 配置交換 Server(24/29)

Receipt of Renew Messages

Receipt of Renew Messages
- The server MUST include in the Reply message a Server Identifier option containing the server's DUID and the Client Identifier option from the Renew message.
- The T1/T2 values set in each applicable IA option for a Reply MUST be the same across all IAs.
- The server MUST determine the T1/T2 values across all of the applicable client's bindings in the Reply.

Renew Message的接收
- Server必須在Reply Message中加入包含server DUID的Server Identifier option，以及在Renew message中的Client Identifier option
- 被設定在可適用於reply的IA option裡的T1/T2時間必須和所有IA一樣
- Sever必須決定所有綁在reply裡可適用的client的T1/T2時間

CONFIDENTIAL For Authorized Personnel Only

18.DHCP 配置交換 Server(25/29)

Receipt of Rebind Messages

Receipt of Rebind Messages
- The Reply with lifetimes of 0 constitutes an explicit notification to the client that the specific addresses and delegated prefixes are no longer valid and MUST NOT be used by the client.
- The server MUST NOT return any addresses or delegated prefixes in the IA that the server does not assign to the client.
- The server MUST include in the Reply message a Server Identifier option containing the server's DUID and the Client Identifier option from the Rebind message.
- The T1 or T2 values set in each applicable IA option for a Reply MUST be the same values across all IAs.
- The server MUST determine the T1 or T2 values across all of the applicable client's bindings in the Reply.

Rebind Message的接收
- lifetime為零的reply形成一個明確提醒client specific addresses和 delegated prefixes已無效不能再被使用
- Server不能回傳任何address 或 delegated prefixes 在server沒分配給client的IA裡
- Server必須在Reply Message中加入包含server DUID的Server Identifier option，以及在Rebind message中的Client Identifier option
- 被設定在可適用於reply的IA option裡的T1/T2時間必須和所有IA一樣
- Sever必須決定所有綁在reply裡可適用的client的T1/T2時間

CONFIDENTIAL For Authorized Personnel Only

18.DHCP 配置交換 Server(26/29)

Receipt of Information-request Messages	
Receipt of Information-request Messages • The server MUST include a Server Identifier option containing the server's DUID in the Reply message.	Information-request Message的接收： • Server必須在Reply Message中加入包含server DUID的Server Identifier option
Receipt of Decline Messages • The client has found any addresses in the Decline messages to be already in use on its link. Therefore, the server SHOULD mark the addresses declined by the client.	Decline Message的接收： • Client已經找到其link中已經被使用，在Decline message中的address，因此server應該標註被client拒絕的address

CONFIDENTIAL For Authorized Personnel Only

18.DHCP 配置交換 Server(27/29)

Creation of Advertise Messages	
• The server preference value MUST default to 0 unless otherwise configured by the server administrator. • The server MUST include options in the Advertise message containing configuration parameters for all of the options identified in the Option Request option (see Section 21.7) in the Solicit message that the server has been configured to return to the client. • If the Option Request option includes a container option, the server MUST include all the options that are eligible to be encapsulated in the container. • The server MUST include IA options in the Advertise message containing any addresses and/or delegated prefixes that would be assigned to IAs contained in the Solicit message from the client.	• Server的preference value應該被設為零除非另有Server管理者配置 • Server必須包含在Advertise message含有給所有Server已經配置返還給client的Solicit message裡Option Request Option option的配置參數options • 如果Option Request option包含一個Container option，server必須包含所有能夠被包裝在container的option • Server必須在包含任何會被分派給從client傳來的solicit message的address或delegated prefix的Advertise message中包含IA option

CONFIDENTIAL For Authorized Personnel Only

18.DHCP 配置交換 Server(28/29)

Creation of Advertise Messages

- If the server is not going to assign an address or delegated prefix received as a hint in the Solicit message, the server MUST NOT include this address or delegated prefix in the Advertise message.
- the server MUST include the IA option in the Advertise message with no addresses in that IA and a Status Code option encapsulated in the IA option containing status code NoAddrsAvail.
- If the server will not assign any prefixes to an IA_PD in subsequent Request messages from the client, the server MUST include the IA_PD option in the Advertise message with no prefixes in the IA_PD option and a Status Code option encapsulated in the IA_PD containing status code NoPrefixAvail.

- 如果server不再分配在solicit message收到當作hint的address或delegated prefix，server不能在Advertise message中包含這個address或delegated prefix
- Server必須在advertise message中包含IA option，IA option內沒有IA且被包裝在IA option裡的Status Code option包含status code NoAddrsAvail
- 如果server不再分配任何prefix給從client來的subsequence request message，server必須在advertise message包含沒有prefix在裡面的IA_PD option，且包裝在IA_PD option裡的Status Code option包含status code NoPrefixAvail

CONFIDENTIAL For Authorized Personnel Only

18.DHCP 配置交換 Server(29/29)

Transmission of Advertise and Reply Messages

- The Advertise or Reply message MUST be unicast through the interface on which the original message was received.

- Advertise或Reply message必須由原本的接收到訊息的介面卡透過unicast傳送

Creation and Transmission of Reconfigure Messages

- The server MUST use DHCP authentication in the Reconfigure message
- The server MUST include a Reconfigure Message option (see Section 21.19) to select whether the client responds with a Renew message, a Rebind message, or an Information-request message.
- The server MUST NOT include any other options in the Reconfigure message, except as specifically allowed in the definition of individual options.

- Server必須在reconfigure message中使用DHCP驗證
- Server必須包括Reconfigure Message選項（在第22.19節中定義），以選擇客戶端是以Renew message還是Information-Request message進行響應。
- Server必須包括Reconfigure Message選項（在第22.19節中定義），以選擇客戶端是以Renew message還是Information-Request message進行響應

CONFIDENTIAL For Authorized Personnel Only

19.Relay Agent行為(1/5)

中繼代理行為	
• If the relay agent has not been explicitly configured, it MUST use the All_DHCP_Servers multicast address as the default. • If the relay agent receives a message other than Relay-forward and Relay-reply and the relay agent does not recognize its message type, it MUST forward the message as described in Section 19.1.1.	• 如果尚未明確配置中繼代理，則必須使用All_DHCP_Servers多播地址作為默認值。 • 如果relay agent收到message非Relay-forward或Relay-reply且relay agent無法辨認message type，relay agent必須照Section 19.1.1的方式傳送

CONFIDENTIAL For Authorized Personnel Only

19.Relay Agent行為(2/5)

中繼Client Message或Relay-forward Message	
If the relay agent cannot use the address in the link-address field to identify the interface through which the response to the client will be relayed, the relay agent MUST include an Interface-id option (see section 22.18) in the Relay-forward message.	如果中繼代理不能使用鏈路地址字段中的地址來識別通過其中繼對客戶端的響應的接口，則中繼代理必須在中繼轉發消息中包含Interface-id選項（參見第22.18節）。

CONFIDENTIAL For Authorized Personnel Only

19.Relay Agent行為(3/5)

Relaying a Relay-reply Message	
• Relay agents MUST NOT modify the message. • If the relay agent receives a Relay-reply message, it MUST process the message as defined above, regardless of the type of message encapsulated in the Relay Message option.	• Relay agent不能修改message • 如果relay agent收到一個Relay-reply message，他必須依照上述定義的方式處理message無論被包含在relay message option的message是什麼type

CONFIDENTIAL For Authorized Personnel Only

19.Relay Agent行為(4/5)

構建中繼回复消息	
A response to the client MUST be relayed through the same relay agents as the original client message.	對客戶端的響應必須通過與原始客戶端消息相同的中繼代理進行中繼。
The server must record the contents of the peer-address fields in the received message so it can construct the appropriate Relay-reply message carrying the response from the server.	Server必須在接收的消息中記錄對等地址字段的內容，以便它可以建構攜帶來自server的響應的適當的中繼回复消息。

CONFIDENTIAL For Authorized Personnel Only

19.Relay Agent行為(5/5)

Interaction between Relay Agents and Servers	
Each relay is allowed to insert additional options on the encapsulation level it added but MUST NOT change anything in the packet being encapsulated.	每個relay被允許插入附加的option在relay封裝的level但不能改變任何被封裝的packet

CONFIDENTIAL For Authorized Personnel Only

20.DHCP訊息驗證(1/4)

DHCP認證摘要	
Any DHCP message MUST NOT include more than one Authentication option.	任何DHCP消息都不能包含多個身份驗證選項。

CONFIDENTIAL For Authorized Personnel Only

20.DHCP訊息驗證(2/4)

重播檢測	
If the RDM field contains 0x00, the replay detection field MUST be set to the value of a monotonically increasing counter.	如果RDM字段包含0x00，則重放檢測字段必須設置為單調遞增計數器的值。
Using a counter value, such as the current time of day (for example, an NTP-format timestamp [9]), can reduce the danger of replay attacks. This method MUST be supported by all protocols.	使用計數器值（例如當前時間（例如，NTP格式時間戳[9]））可以降低重放攻擊的危險。 所有協議都必須支持此方法。
A client that receives a message with the RDM field set to 0x00 MUST compare its replay detection field with the previous value sent by that same server and only accept the message if the received value is greater and record this as the new value.	收到RDM字段被設為0x00訊息的client必須和前一個Server發送的比較它的replay偵測字段比較值，且只接受更高的值且記錄他為新的值

CONFIDENTIAL For Authorized Personnel Only

20.DHCP訊息驗證(3/4)

重播檢測	
If this is the first time a client processes an Authentication option sent by a server, the client MUST record the replay detection value and skip the replay detection check.	如果這是第一次client處理被server傳來的Authentication option，client必須記錄replay detection值且忽略the replay detection檢測
Servers that support the reconfigure mechanism MUST ensure that the replay detection value is retained between restarts.	支持重新配置機制的server必須確保replay detection值在每次重新開始時被保留

CONFIDENTIAL For Authorized Personnel Only

20.DHCP訊息驗證(4/4)

Server Considerations for RKAP	
The reconfigure key is 128 bits long and MUST be a cryptographically strong random or pseudorandom number that cannot easily be predicted.	重新配置的key為128bit長且必須為不容易被預測的加密強隨機或偽隨基數

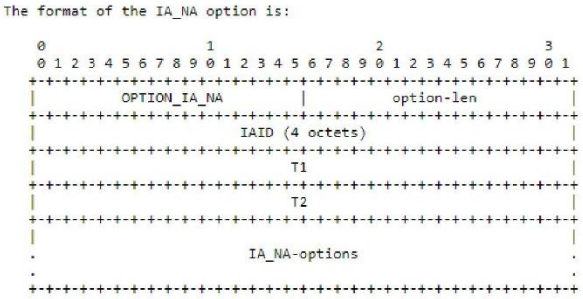
CONFIDENTIAL For Authorized Personnel Only

21. DHCP選項(1/19)

DHCP選項	
Unless otherwise noted, each option may appear only in the options area of a DHCP message and may appear only once. If an option does appear multiple times, each instance is considered separate and the data areas of the options MUST NOT be concatenated or otherwise combined.	除非另有說明，否則每個選項可能僅出現在DHCP消息的選項區域中，並且可能只出現一次。 如果選項確實出現多次，則每個實例都被視為獨立的，並且選項的數據區域不能連接或以其他方式組合。

CONFIDENTIAL For Authorized Personnel Only

21. DHCP選項(2/19)



非臨時地址選項的身份關聯	
In a message sent by a client to a server, the T1 and T2 fields SHOULD be set to 0. The server MUST ignore any values in these fields in messages received from a client.	Client發送給server的message，T1和T2字段應該被設為0。Server必須忽視任何從client收到的message在這兩個區段的值

CONFIDENTIAL For Authorized Personnel Only

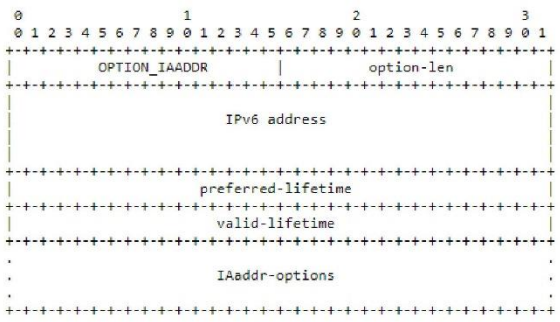
21. DHCP選項(3/19)

非臨時地址選項的身份關聯	
In a message sent by a server to a client, the client MUST use the values in the T1 and T2 fields for the T1 and T2 parameters, unless those values in those fields are 0.	在server發送給客戶端的消息中，客戶端必須使用T1和T2字段中的值作為T1和T2參數，除非這些字段中的值為0。
The client MUST follow the rules defined in Section 14.2.	Client必須遵守定義在Section 14.2的規則
臨時地址選項的身份關聯	
A server MUST return the same set of temporary addresses for the same IA_TA (as identified by the IAID) as long as those addresses are still valid.	Server必須返還同一組temporary addresses給相同的IA_TA只要那些address仍然有效

CONFIDENTIAL For Authorized Personnel Only

21. DHCP選項(4/19)

The format of the IA Address option is:



IA地址選項	
In a message sent by a server to a client, the client MUST use the values in the preferred and valid lifetime fields for the preferred and valid lifetimes.	在server發送到客戶端的消息中，客戶端必須使用首選和有效生命週期字段中的值來獲取首選和有效生命週期。

CONFIDENTIAL For Authorized Personnel Only

21. DHCP選項(5/19)

IA地址選項	
A client MUST NOT form an implicit prefix with a length other than 128 for this address.	Client不能形成一個不明確長度不為128的prefix給這個address
In a message sent by a client to a server, the preferred-lifetime and valid-lifetime fields SHOULD be set to 0. The server MUST ignore any values in these fields in messages received from a client.	Client發送給server的message，preferred-lifetime和valid-lifetime字段應該被設為0。Server必須忽視任何從client收到的message在這兩個區段的值
In a message sent by a server to a client, the client MUST use the values in the preferred-lifetime and valid-lifetime fields for the preferred and valid lifetimes.	在server發送給客戶端的消息中，客戶端必須使用preferred-lifetime和valid-lifetime字段中的值作為preferred-lifetime和 valid-lifetime參數，除非這些字段中的值為0。
The client MUST discard any addresses for which the preferred lifetime is greater than the valid lifetime.	Client必須捨棄任何preferred lifetime大於valid time的address

CONFIDENTIAL For Authorized Personnel Only

21. DHCP選項(6/19)

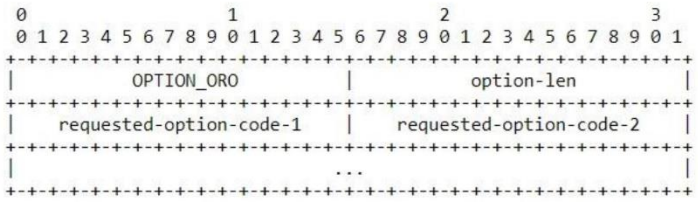


Figure 18: Option Request Option Format

Option Request Option	
A client MUST include an Option Request option in a Solicit, Request, Renew, Rebind, or Information-request message to inform the server about options the client wants the server to send to the client.	client必須在Solicit, Request, Renew, Rebind,和Information-request message包含一個Option Request option來告知server，client想要server傳送給clien的option

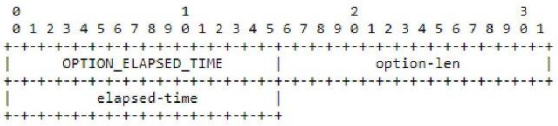
CONFIDENTIAL For Authorized Personnel Only

21. DHCP選項(7/19)

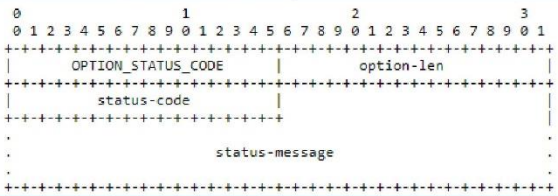
Option Request Option	
For certain message types, some option codes MUST be included in the Option Request option; see Table 4 for details.	對於某幾個message形式，某些option code必須被包含在Option Request option細節如表4
The Option Request option MUST NOT include the following options: - Client Identifier - Server Identifier - IA_NA - IA_TA - IA_PD - IA Address - IA Prefix - Option Request - Elapsed Time - Preference - Relay - Authentication - Server Unicast - Status Code - Rapid Commit - User Class - Vendor Class - Interface-Id - Reconfigure Message - Reconfigure Accept	Option Request option不能包含下列選項: - Client Identifier - Server Identifier - IA_NA - IA_TA - IA_PD - IA Address - IA Prefix - Option Request - Elapsed Time - Preference - Relay - Authentication - Server Unicast - Status Code - Rapid Commit - User Class - Vendor Class - Interface-Id - Reconfigure Message - Reconfigure Accept
Other top-level options MUST appear in the Option Request option or they will not be sent by the server.	其他top-level option必須出現在Option Request option 否則他不會被server傳送

CONFIDENTIAL For Authorized Personnel Only

21. DHCP選項(8/19)



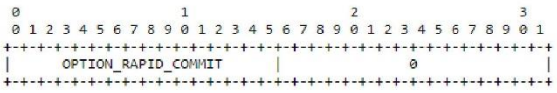
經過時間選項	
A client MUST include an Elapsed Time option in messages to indicate how long the client has been trying to complete a DHCP message exchange.	客戶端必須在消息中包含Elapsed Time選項，以指示客戶端嘗試完成DHCP消息交換的時間。



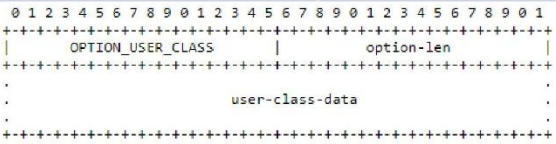
狀態代碼選項	
A UTF-8 encoded text string suitable for display to an end user, which MUST NOT be null-terminated.	UTF-8編碼的文本字符串，適合顯示給最終用戶，不能以空值終止。

CONFIDENTIAL For Authorized Personnel Only

21. DHCP選項(9/19)



快速提交選項	
A server MUST include this option in a Reply message sent in response to a Solicit message when completing the Solicit-Reply message exchange.	Server必須在完成Solicit-Reply消息交換時響應Solicit消息而發送的Reply消息中包含此選項。



用戶類選項	
The user class information carried in this option MUST be configurable on the client.	此選項中攜帶的用戶類信息必須可在客戶端上配置。
The data area of the user class option MUST contain one or more instances of user class data.	用戶類選項的數據區域必須包含一個或多個用戶類數據實例。

21. DHCP選項(10/19)

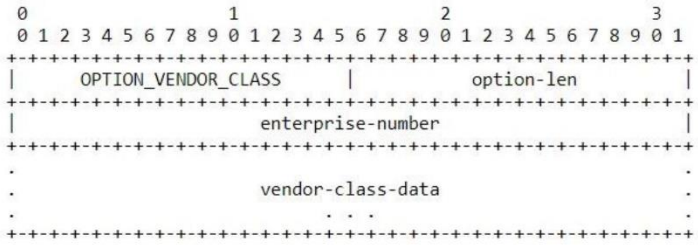


Figure 28: Vendor Class Option Format

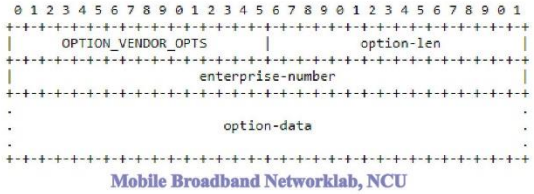
供應商類別選項	
Servers and clients MUST NOT include more than one instance of OPTION_VENDOR_CLASS with the same Enterprise Number.	Server和client不能包含多於一個的OPTION_VENDOR_CLASS有相同的企業代碼

Mobile Broadband Networklab, NCU
CONFIDENTIAL For Authorized Personnel Only

21. DHCP選項(11/19)

供應商特定信息選項	
The encapsulated vendor-specific options field MUST be encoded as a sequence of code/length/value fields of identical format to the DHCP options field.	封裝的供應商特定選項字段必須編碼為與DHCP選項字段格式相同的一系列代碼/長度/值字段。
Servers and clients MUST NOT send more than one instance of the Vendor-specific Information option with the same Enterprise Number.	Server和client不能包含多於一個的Vendor-specific Information option有相同的企業代碼
A client that is interested in receiving a Vendor-specific Information option MUST specify the Vendor-specific Information option in an Option Request option.	client有興趣收到Vendor-specific Information option必須在Option Request option明確要求Vendor-specific Information option

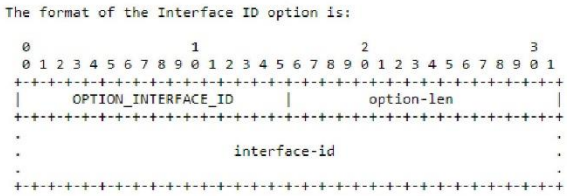
The format of the Vendor-specific Information option is:



Mobile Broadband Networklab, NCU
CONFIDENTIAL For Authorized Personnel Only

21. DHCP選項(12/19)

The format of the Interface ID option is:

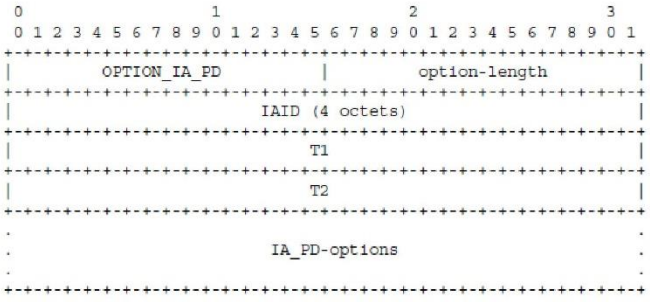


Interface-Id選項	
The server MUST copy the Interface-Id option from the Relay-Forward message into the Relay-Reply message the server sends to the relay agent in response to the Relay-Forward message.	Server必須將Interface-Id選項從Relay-Forward消息複製到server發送給中繼代理的Relay-Reply消息中，以響應Relay-Forward消息。
This option MUST NOT appear in any message except a Relay-Forward or Relay-Reply message.	除了Relay-Forward或Relay-Reply消息之外，該選項不能出現在任何消息中。
Servers MAY use the Interface-ID for parameter assignment policies.	server可以使用Interface-ID進行參數分配策略。

CONFIDENTIAL For Authorized Personnel Only

21. DHCP選項(13/19)

Identity Association for Prefix Delegation Option（前綴委派選項的身份關聯）	
IAID: The unique identifier for this IA_PD; the IAID must be unique among the identifiers for all of this requesting router's IA_PDs.	IAID：此IA_PD的唯一標識符; IAID在所有請求路由器的IA_PD的標識符中必須是唯一的。



CONFIDENTIAL For Authorized Personnel Only

21. DHCP選項(14/19)

Identity Association for Prefix Delegation Option（前綴委派選項的身份關聯）	
In a message sent by a client to a server, the T1 and T2 fields SHOULD be set to 0. The server MUST ignore any values in these fields in messages received from a client.	Client發送給server的message，T1和T2字段應該被設為0。Server必須忽視任何從client收到的message在這兩個區段的值
In a message sent by a server to a client, the client MUST use the values in the T1 and T2 fields for the T1 and T2 timers, unless values in those fields are 0.	在server發送給客戶端的消息中，客戶端必須使用T1和T2字段中的值作為T1和T2參數，除非這些字段中的值為0。
The client MUST follow the rules defined in Section 14.2.	Client必須遵守定義在Section 14.2的規則

CONFIDENTIAL For Authorized Personnel Only

21. DHCP選項(15/19)

IA Prefix Option	
The IA Prefix option must be encapsulated in the IA_PD-options field of an IA_PD option	IA prefix option必須被包裝在IA_PD option的IA_PD-options 字段
In a message sent by a server to a client, the client MUST use the values in the preferred-lifetime and valid-lifetime fields for the preferred and valid lifetimes.	在server發送給客戶端的消息中，客戶端必須使用preferred-lifetime和valid-lifetime字段中的值作為preferred-lifetime和 valid-lifetime參數，除非這些字段中的值為0。
The client MUST discard any prefixes for which the preferred lifetime is greater than the valid lifetime.	Client必須捨棄任何preferred lifetime大於valid time的address

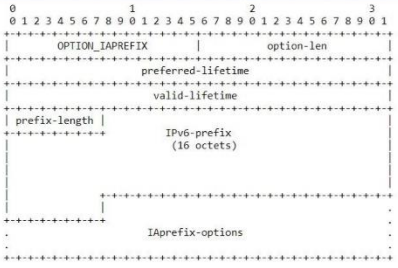


Figure 36: IA Prefix Option Format

CONFIDENTIAL For Authorized Personnel Only

21. DHCP選項(16/19)

Information Refresh Time Option	
A DHCP client MUST request this option in the Option Request option (see Section 21.7) when sending Information-request messages.	DHCP client必須在option request option裡請求這個option當發送Information-request messages
A client MUST NOT request this option in the Option Request option in any other messages.	client不能在其他messag的option request option請求這個option
The option value MUST NOT be smaller than IRT_MINIMUM.	Option的值不能比IRT_MINIMUM還小
This option MUST only appear in the top-level options area of Reply messages	這個option必須只能出現在reply message的top-level option區

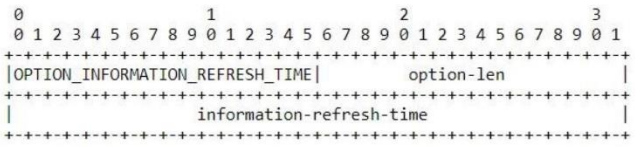


Figure 37: Information Refresh Time Option Format

CONFIDENTIAL For Authorized Personnel Only

21. DHCP選項(17/19)

Information Refresh Time Option	
If the Reply to an Information-request message does not contain this option, the client MUST behave as if the option with the value IRT_DEFAULT was provided.	如果Information-request message的回應沒有包含這個option，client必須預設option的值為IRT_DEFAULT
A client MUST use the refresh time IRT_MINIMUM if it receives the option with a value less than IRT_MINIMUM.	如果收到的option值比IRT_MINIMUM小，Client必須設refresh time為IRT_MINIMUM
the client MUST delay sending the first Information-request by a random amount of time between 0 and INF_MAX_DELAY.	client必須延遲發送第一個Information-request，延遲時間介於零到INF_MAX_DELAY.

CONFIDENTIAL For Authorized Personnel Only

21. DHCP選項(18/19)

SOL_MAX_RT Option	
A DHCP client MUST include the SOL_MAX_RT option code in any Option Request option (see Section 21.7) it sends in a Solicit message.	DHCP client必須在任何在Solicit message的Option Request option包含SOL_MAX_RT option code
A DHCP client MUST ignore any SOL_MAX_RT option values that are less than 60 or more than 86400.	DHCP client必須忽略任何SOL_MAX_RT option值小於60或大於86400
If a DHCP client receives a message containing a SOL_MAX_RT option that has a valid value for SOL_MAX_RT, the client MUST set its internal SOL_MAX_RT parameter to the value contained in the SOL_MAX_RT option.	如果DHCP client收到包含有效值的SOL_MAX_RT option，client必須設置它的內部SOL_MAX_RT參數為SOL_MAX_RT option裡的值

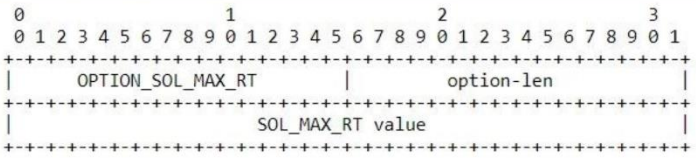


Figure 38: SOL_MAX_RT Option Format

365

CONFIDENTIAL For Authorized Personnel Only

21. DHCP選項(19/19)

INF_MAX_RT Option	
A DHCP client MUST include the INF_MAX_RT option code in any Option Request option (see Section 21.7) it sends in a Solicit message.	DHCP client必須在任何在Information-requestmessage的Option Request option包含SOL_MAX_RT option code
A DHCP client MUST ignore any INF_MAX_RT option values that are less than 60 or more than 86400.	DHCP client必須忽略任何INF_MAX_RT option值小於60或大於86400
If a DHCP client receives a message containing a INF_MAX_RT option that has a valid value for INF_MAX_RT, the client MUST set its internal INF_MAX_RT parameter to the value contained in the INF_MAX_RT option.	如果DHCP client收到包含有效值的INF_MAX_RT option，client必須設置它的內部INF_MAX_RT參數為INF_MAX_RT option裡的值

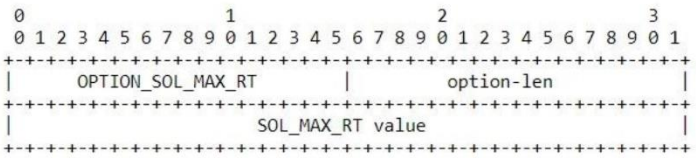


Figure 38: SOL_MAX_RT Option Format

366

CONFIDENTIAL For Authorized Personnel Only

22.安全考慮因素

安全考慮因素	
Because of the opportunity for attack through the Reconfigure message, a DHCP client MUST discard any Reconfigure message that does not include authentication or that does not pass the validation process for the authentication protocol.	由於通過重新配置消息進行攻擊的機會，DHCP客戶端必須丟棄任何不包含身份驗證或未通過身份驗證協議驗證過程的重新配置消息。

Mobile Broadband Networklab, NCU

CONFIDENTIAL
For Authorized Personnel Only



附件二、IPv6 Ready Logo 互連測試

IPv6寬頻分享器互通測試項目研究及IASP實際測試平台建置

IPv6寬頻分享器製造商測試規範

周立德

國立中央大學主任秘書

國立中央大學資訊工程學系特聘教授

1

IPv6 ready logo互連性測試項目

- IPv6 ready logo互連性測試項目

WAN Side Test:
1. DUPLICATE ADDRESS DETECTION
2. ROUTER DISCOVERY
3. ADDRESS LIFETIME
4. DHCPV6
5. DHCPV6 PREFIX DELEGATION
6. UNNUMBERED WAN
7. DHCPV6 SOL_MAX_RT
8. L FLAG PROCESSING

LAN Side Test:
1. DUPLICATE ADDRESS DETECTION AND NEIGHBOR DISCOVERY
2. ASSIGNING PREFIXES TO LAN INTERFACES
3. ROUTER ADVERTISEMENT
4. STATELESS DHCP SERVER
5. DHCP SERVER
6. PREFIX CHANGE
7. LINK MTU
8. DNS INFORMATION IN ROUTER ADVERTISEMENT
9. INGRESS FILTERING

General Requirement Test:
1. ICMPV6
2. IPV6 FORWARDING BEFORE ADDRESS ACQUISITION
3. NO DEFAULT ROUTE
4. FORWARDING LOOPS

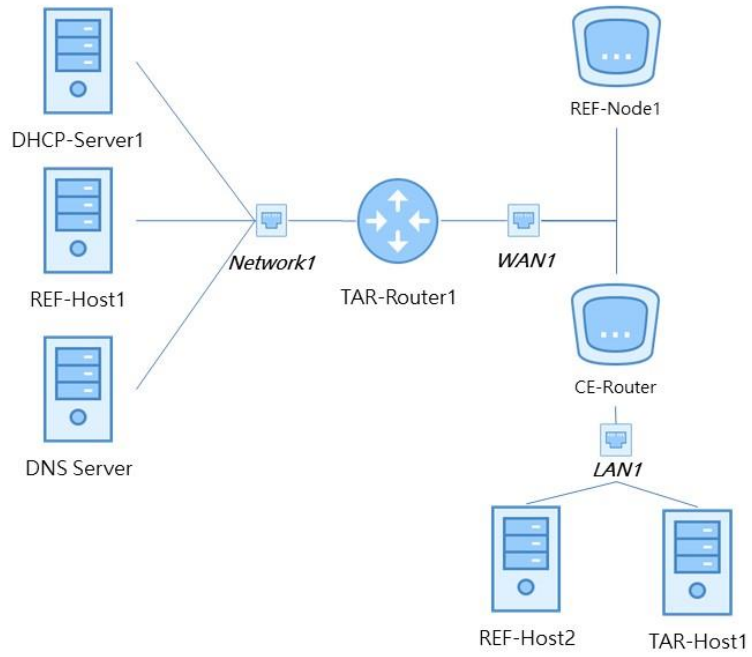
Unique Local Address Test:
1. ULA PREFIX GENERATION
2. ULA SITE BORDER

2

Mobile Broadband Networklab, NCU

CONFIDENTIAL For Authorized Personnel Only

Common Topology

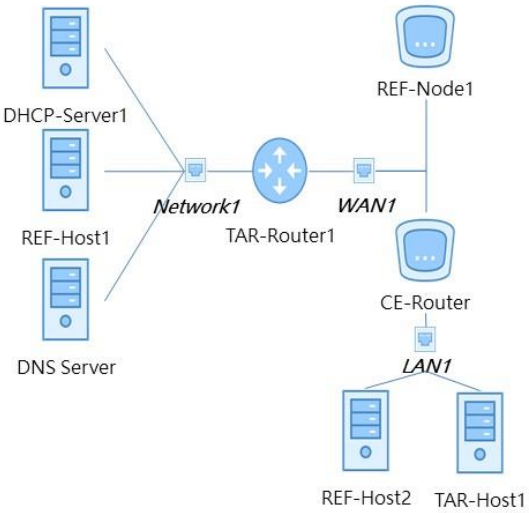


CONFIDENTIAL For Authorized Personnel Only

Common Test Setup

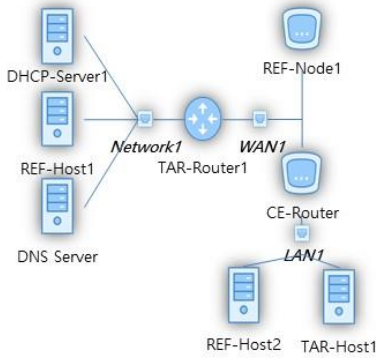
建置步驟：

- TAR-Router1 分配global address給Network1上的node，讓DNS-Server和REF-Host1可以有基本的routing
- TAR-Router是一個DHCPv6的Relay Agent
- TAR-Router透過DHCPv6指派global address給CE-Router，或是CE-Router透過SLAAC獲得global address
- TAR-Router1 傳送Router Advertisement (RA)到WAN端的介面卡，並將RA的O和M flag設成1



CONFIDENTIAL For Authorized Personnel Only

WAN Side Configuration



CONFIDENTIAL For Authorized Personnel Only

Duplicate Address Detection

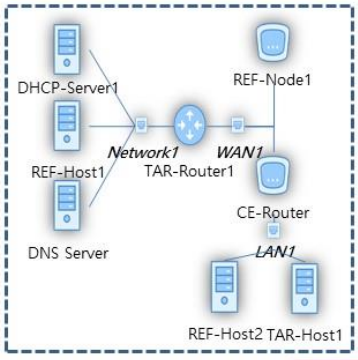
- Part A: Duplicate Address Detection – Tentative Address Unique (Link-Local)

測試1

1. 關閉所有連線至WAN1的介面
2. 再開啟WAN1上的介面，開啟TAR-Router1 後開啟CE-Router
3. 等待一段時間使WAN1上的裝置在裝置的link-local address執行Duplicate Address Detection
4. 並開啟REF-Node1後確保已經清除neighbor cache
5. 從REF-Node1傳送ICMPv6 Echo Request到CE-Router WAN介面的link-local address

成果1

1. CE-Router回應ICMPv6 Echo Replies給所有從REF-Node1傳來的ICMPv6 Echo Request



CONFIDENTIAL For Authorized Personnel Only

Duplicate Address Detection

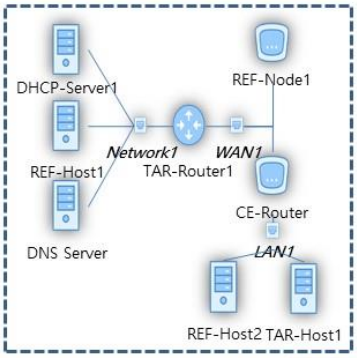
- Part A: Duplicate Address Detection – Tentative Address Unique (Link-Local)

測試2

1. 重複測試1步驟，並將步驟2的順序更改為，先開啟CE-Router後開啟TAR-Router1

成果2

1. CE-Router回應ICMPv6 Echo Replies給所有從REF-Node1傳來的ICMPv6 Echo Request



CONFIDENTIAL For Authorized Personnel Only

Duplicate Address Detection

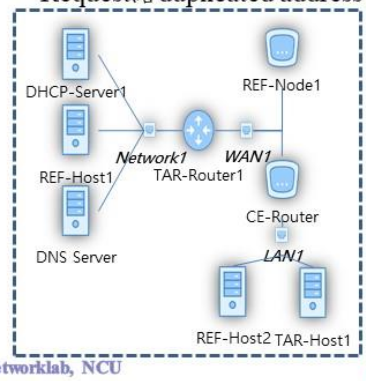
- Part B: Duplicate Address Detection – Tentative Address Duplicated. (Link-Local)

測試3

1. 關閉所有連線至WAN1的介面
2. 配置TAR-Router1的link-local address和CE-Router的WAN1介面一樣
3. 開啟所有在WAN1上的介面，開啟TAR-Router1 後開啟CE-Router
4. 等待一段時間使WAN1上的裝置在裝置的link-local address執行Duplicate Address Detection
5. 並開啟REF-Node1 後確保已經清除neighbor cache
6. 從REF-Node1傳送ICMPv6 Echo Request到CE-Router WAN介面的link-local address

成果3

1. TAR-Router1回應ICMPv6 Echo Replies給所有從REF-Node1傳來的ICMPv6 Echo Request，CE-Router不會回應任何neighbor solicitations或ICMPv6 Echo Request給duplicated address



CONFIDENTIAL For Authorized Personnel Only

Duplicate Address Detection

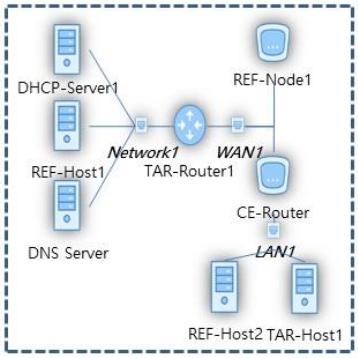
- Part B: Duplicate Address Detection – Tentative Address Duplicated. (Link-Local)

測試4

1. 重複測試3步驟，並將步驟2的順序更改為，先開啟CE-Router後開啟TAR-Router1

成果4

1. CE-Router回應ICMPv6 Echo Replies給所有從REF-Node1傳來的ICMPv6 Echo Request



CONFIDENTIAL For Authorized Personnel Only

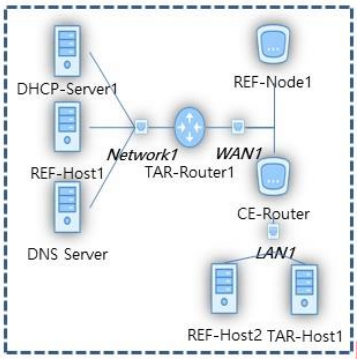
Router Discovery

測試1

1. 重啟CE-Router

成果1

1. CE-Router在傳送Router Solicitation之前，在link-local address上完成DAD
2. Router Solicitation包含一個link-local source address 跟所有router的多播地址



CONFIDENTIAL For Authorized Personnel Only

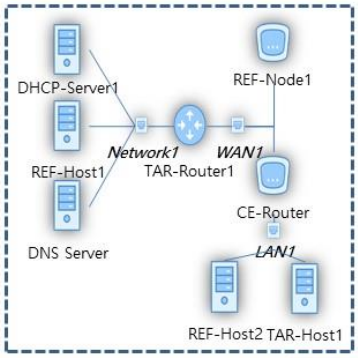
Router Discovery

測試2

1. 等待CE-Router透過每個DHCP執行DAD得到global address
2. REF-Host1 傳送一個ICMPv6 Echo Request給 CE-Router在WAN介面的DHCPv6 global address

成果2

1. CE-Router使用global source address回應ICMPv6 Echo Replies給所有從REF-Node1傳來的ICMPv6 Echo Request



CONFIDENTIAL For Authorized Personnel Only

Address Lifetime

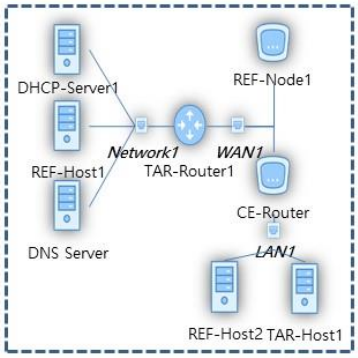
- Part A: Lifetime expires

測試1

1. 建置TAR-Router1 在WAN1上傳送一個有效期30秒的address的one prefix Router Advertisement並等待CE-Router執行Duplicate Address Detection
2. 從REF-Host1傳送一個ICMPv6 Echo Request給CE-Router的global address

成果1

1. CE-Router應該回應ICMPv6 Echo Replies給所有從REF-Host1傳來的ICMPv6 Echo Request



CONFIDENTIAL For Authorized Personnel Only

Address Lifetime

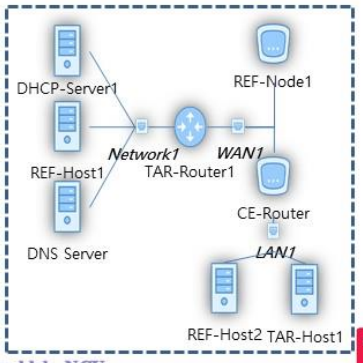
- Part A: Lifetime expires

測試2

1. TAR-Router1 不發送Router Advertisement，並等待35秒
2. REF-Host1傳送一個ICMPv6 Echo Request給CE-Router透過在WAN介面上的Router Advertisement獲得的global address

成果2

1. CE-Router應該timeout Prefix1
2. CE-Router 應該不回應任何從REF-Host1發送含有跟Prefix1有關連的address的ICMPv6 Echo Requests 或 Neighbor Solicitations



CONFIDENTIAL For Authorized Personnel Only

Address Lifetime

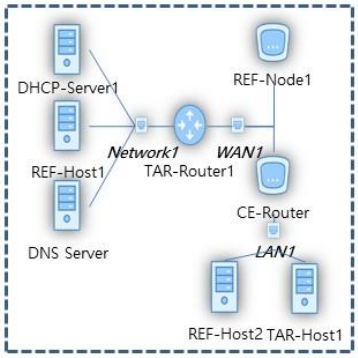
- Part B: Multiple Prefix Discovery

測試3

1. 建置TAR-Router1 在WAN1上傳送一個two prefixes的Router Advertisement: Prefix X, Prefix Y並等待CE-Router執行Duplicate Address Detection
2. 從REF-Host1傳送一個ICMPv6 Echo Request給CE-Router在WAN1上跟Prefix X有關聯的global address

成果3

1. CE-Router應該回應ICMPv6 Echo Replies給所有從REF-Host1傳來跟Prefix 有關聯的ICMPv6 Echo Request



CONFIDENTIAL For Authorized Personnel Only

Address Lifetime

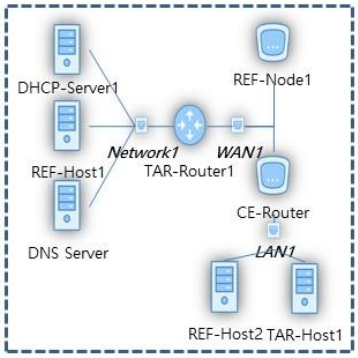
- Part B: Multiple Prefix Discovery

測試4

1. 從REF-Host1傳送一個ICMPv6 Echo Request給CE-Router在WAN1上跟Prefix Y有關聯的global address

成果4

1. CE-Router應該回應ICMPv6 Echo Replies給所有從REF-Host1傳來跟Prefix 有關聯的ICMPv6 Echo Request



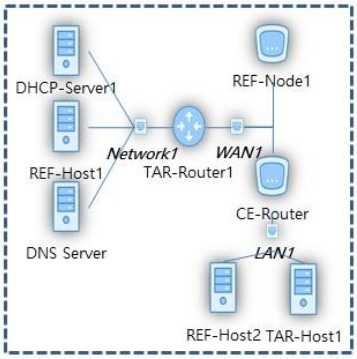
CONFIDENTIAL For Authorized Personnel Only

DHCPv6

- Part A: Initialization

測試1

1. 在WAN1上開啟CE-Router



成果1

1. CE-Router應該要傳送一個包含Reconfigure Accept Option, IA_NA Option, 和Option Request Option的DHCPv6 Solicit message
2. Option request option須包含一個含有DNS_SERVERS Option的Requested option code
3. DHCP-Server1傳送一個含有IPv6 address information的DHCPv6 Advertisement message
4. CE-Router傳送一個DHCPv6 Request messages用來確認IPv6 address和詢問額外資訊
5. 5DHCP-Server1回應一個包含確定的地址的DHCPv6 Reply message

CONFIDENTIAL For Authorized Personnel Only

DHCPv6

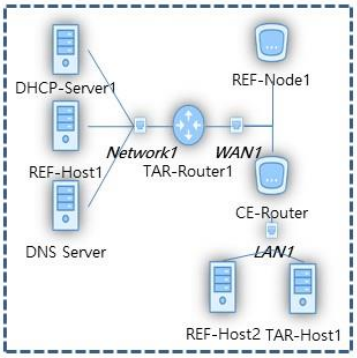
- Part A: Initialization

測試2

1. REF-Host1傳送ICMPv6 Echo Request給CE-Router DHCPv6 global address

成果2

1. CE-Router應該要回應ICMPv6 Echo Replies給所有從REF-Host1來的ICMPv6 Echo Requests



Mobile Broadband Networklab, NCU
CONFIDENTIAL For Authorized Personnel Only

DHCPv6

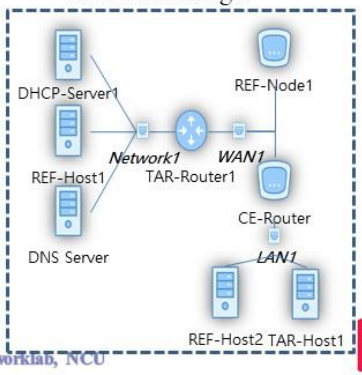
- Part B: Renew message

測試3

1. 在WAN1上開啟CE-Router
2. CE-Router 應該已經收到從DHCP-Server1傳來的IPv6 address information
   DHCP-Server1分配T1和T2 參數給CE-Router IA (DHCP-Server1 設定 T1 為 50s T2為80s)
3. 等待T1時間觀察在WAN1上傳送的訊息

成果3

1. CE-Router在收到DHCP-Server1傳來的DHCPv6 Reply message的回應後，經過T1(50)秒傳送第一個 DHCPv6 Renew message
2. DHCP-Server1 傳送一個適當格式化的 Reply message回應給DHCP Renew message



Mobile Broadband Networklab, NCU
CONFIDENTIAL For Authorized Personnel Only

DHCPv6

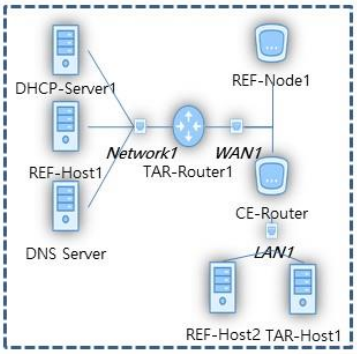
- Part B: Renew message

測試4

1. CE-Router 應該回應ICMPv6 Echo Replies給從REF-Host1所有傳來的ICMPv6 Echo Requests

成果4

1. CE-Router 應該回應ICMPv6 Echo Replies給從REF-Host1所有傳來的ICMPv6 Echo Requests



CONFIDENTIAL For Authorized Personnel Only

DHCPv6

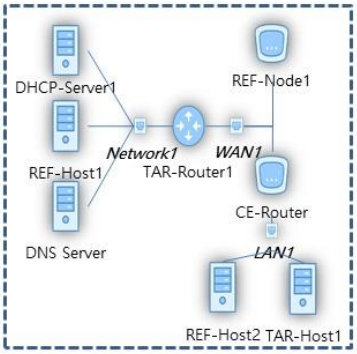
- Part C: Rebind message

測試5

1. 在WAN1上開啟CE-Router
2. 等待足夠時間讓CE-Router收到從DHCP-Server1傳來的IPv6 address information
3. DHCP-Server1 分配T1跟T2 參數給CE-Router IA_NA (TAR-Router1 設定T1 為 50秒T2為80秒)
4. 關閉DHCP-Server1
5. 等待T2時間後觀察在WAN1上傳送的message

成果5

1. CE-Router傳送一個DHCPv6 Rebind Message



CONFIDENTIAL For Authorized Personnel Only

DHCPv6

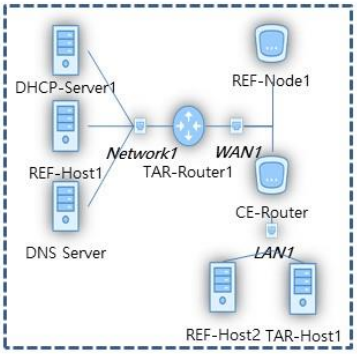
- Part C: Rebind message

測試6

1. 開啟 DHCP-Server1 並確認CE-Router 地址被更新為下一個rebind
2. REF-Host1傳送一個 ICMPv6 Echo Request 給 CE-Router DHCPv6 global address

成果6

1. CE-Router應該要回應ICMPv6 Echo Replies給所有從REF-Host1來的ICMPv6 Echo Requests



CONFIDENTIAL For Authorized Personnel Only

DHCPv6

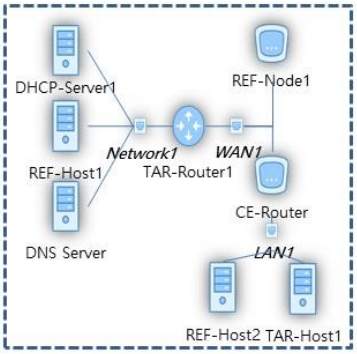
- Part D: Release Message

測試7

1. 在WAN1上開啟CE-Router
2. 等待足夠時間讓CE-Router收到從DHCP-Server1傳來的IPv6 address information
3. TAR-Router1 傳送一個an ICMPv6 Echo Request 給 CE-Router DHCPv6 global address.

成果7

1. CE-Router應該要回應ICMPv6 Echo Replies給所有從TAR-Router1來的ICMPv6 Echo Requests



CONFIDENTIAL For Authorized Personnel Only

DHCPv6

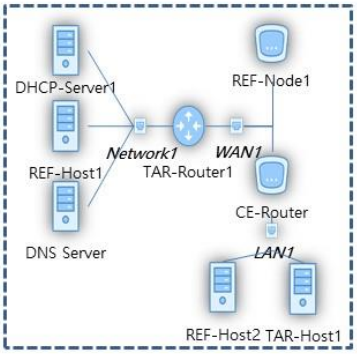
- Part D: Release Message

測試8

1. 配置 CE-Router 釋放IPv6 global address

成果8

1. CE-Router 傳送一個DHCPv6 Release Message



CONFIDENTIAL For Authorized Personnel Only

DHCPv6

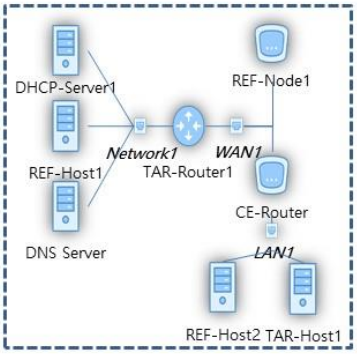
- Part D: Release Message

測試9

1. TAR-Router1 傳送一個 ICMPv6 Echo Request給CE-Router DHCPv6 global address

成果9

1. CE-Router應該要timeout Prefix1
2. CE-Router 不該回應從TAR-Router1傳來和Prefix1有關聯的地址的ICMPv6 Echo Requests 或 Neighbor Solicitations



CONFIDENTIAL For Authorized Personnel Only

DHCPv6

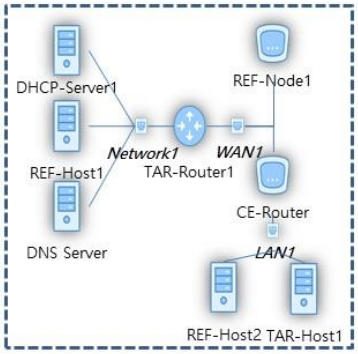
- Part E: Confirm messages

測試10

1. 在WAN1上開啟CE-Router

成果10

1. 對來自TAR-Router1的DHCPv6 Reply message中接收到的IA中的每個地址上執行duplicate address detection



CONFIDENTIAL For Authorized Personnel Only

DHCPv6

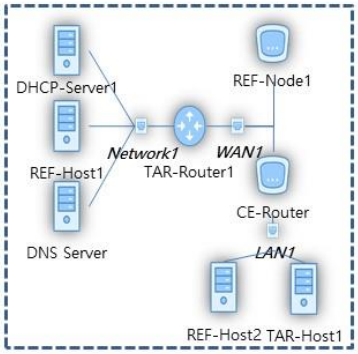
- Part E: Confirm messages

測試11

1. REF-Host1 傳送 ICMPv6 Echo Request 給CE-Router 的DHCPv6 global address

成果11

1. CE-Router 應該回應ICMPv6 Echo Replies 給所有從REF-Host1 來的 ICMPv6 Echo Requests



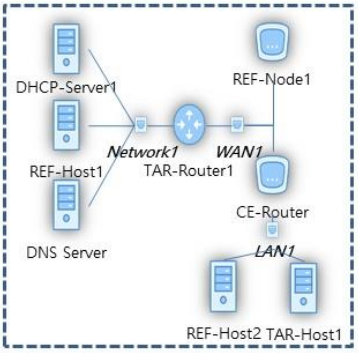
CONFIDENTIAL For Authorized Personnel Only

DHCPv6

- Part E: Confirm messages

測試12

1. 重新插拔 WAN 介面



成果12

1. CE-Router 傳送一個DHCPv6 Confirm message 給TAR-Router1
2. TAR-Router1 回應一個沒有status code option 或有status code option 但status code為0的DHCPv6 Reply message表示address是適合link的
3. DHCPv6 Reply message 不包含 IA_NA Option或IA_PD Option.

CONFIDENTIAL For Authorized Personnel Only

DHCPv6

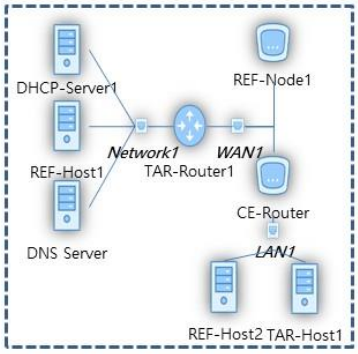
- Part E: Confirm messages

測試13

1. REF-Host1 傳送ICMPv6 Echo Request 給CE-Router的 DHCPv6 global address

成果13

1. CE-Router 應該回應ICMPv6 Echo Replies.從REF-Host1來的給全部 ICMPv6 Echo Requests



CONFIDENTIAL For Authorized Personnel Only

DHCPv6

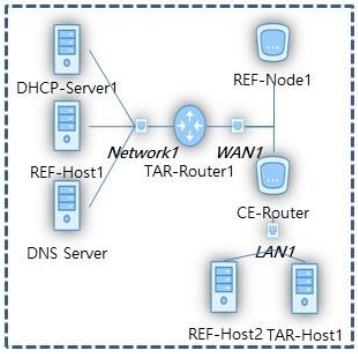
- Part F: Decline Message

測試14

1. 建置 REF-Node1使他有跟DHCP-Server1 分配給 CE-Router一樣的 address
2. 開啟在WAN1上的 CE-Router等待足夠時間讓CE-Router收到從REF-Node1傳來的IPv6 address information

成果14

1. CE-Router 應該回應ICMPv6 Echo Replies.從REF-Host1來的給全部 ICMPv6 Echo Requests



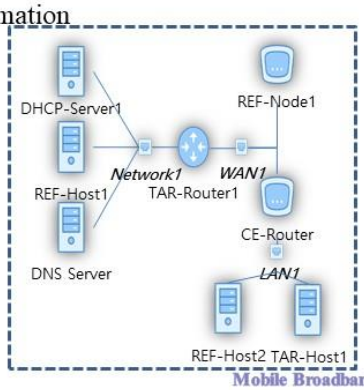
CONFIDENTIAL For Authorized Personnel Only

DHCPv6

- Part F: Decline Message

測試14

1. 建置 REF-Node1使他有跟DHCP-Server1 分配給 CE-Router一樣的 address
2. 開啟在WAN1上的 CE-Router等待足夠時間讓CE-Router收到從REF-Node1傳來的IPv6 address information



成果14

1. CE-Router為他的global address傳送一個DAD NS
2. REF-Node1 傳送一個solicited NA回應non-unique tentative address給DAD NS
3. CE-Router傳送一個DHCPv6 Decline message
4. DHCP-Server 傳送一個DHCPv6 Reply message

CONFIDENTIAL For Authorized Personnel Only

DHCPv6

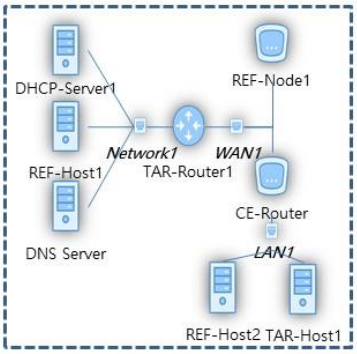
- Part G: DNS Recursive Name Server Option

測試15

1. 建置DHCP-Server1 包含一個有包含DNSServer global IPv6 address的DNS Recursive Name Server option
2. 開啟在WAN1上的CE-Router 等待足夠時間讓CE-Router收到從DHCP-Server1傳來的IPv6 address information
3. CE-Router傳送一個 ICMPv6 Echo Request 到 “dhcpv6.test.example.com”

成果15

1. CE-Router 應該傳送一個有效的DNS request給DNS-Server1
2. DNS-Server1 應該傳送一個有效的DNS response



CONFIDENTIAL For Authorized Personnel Only

DHCPv6

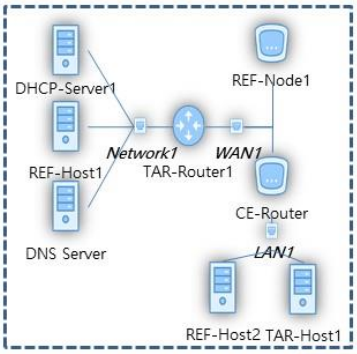
- Part H: Domain Search List Option

測試16

1. 建置 DHCP-Server1 包含一個含有DNSServer global IPv6 address 當作name server 的DNS Recursive Name Server option和包含一個含有 “test.example.com” 的Domain Search List option
2. 開啟在WAN1上的CE-Router 等待足夠時間讓CE-Router收到從DHCP-Server1傳來的IPv6 address information
3. CE-Router傳送一個ICMPv6 Echo Request 給 “dhcpv6”

成果16

1. CE-Router 應該傳送一個有效的DNS request給DNS-Server1
2. DNS-Server1 應該傳送一個有效的DNS response



CONFIDENTIAL For Authorized Personnel Only

DHCPv6

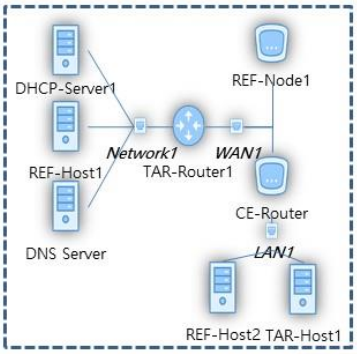
- Part I: Timeout

測試17

1. 開啟WAN1上的CE-Router
2. 等待足夠時間讓CE-Router 透過DHCP收到IPv6 address information
3. 關閉DHCP-Server1
4. TAR-Router1 傳送一個ICMPv6 Echo Request 給CE-Router的DHCPv6 global address

成果17

1. CE-Router 應該回復ICMPv6 Echo Replies 給所有從TAR-Router1 來的ICMPv6 Echo Requests



CONFIDENTIAL For Authorized Personnel Only

DHCPv6

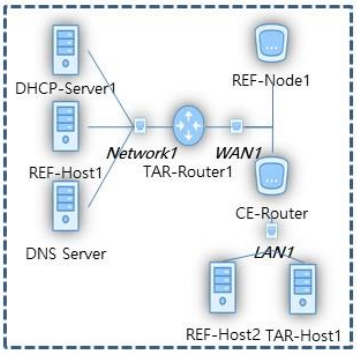
- Part I: Timeout

測試18

1. 等待來自DHCP IA_NA(測試17步驟2)提供的有效lifetime
2. TAR-Router1傳送一個ICMPv6 Echo Request給CE-Router的 global address

成果18

1. CE-Router應該要timeout Prefix1. CE-Router不該回應從TAR-Router1來和Prefix1有關的address任何ICMPv6 Echo Requests或Neighbor Solicitations



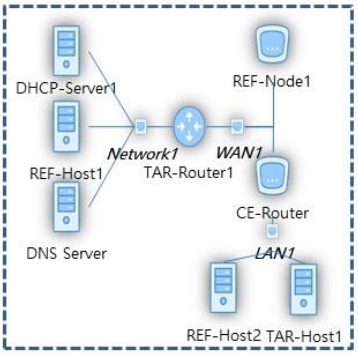
CONFIDENTIAL For Authorized Personnel Only

DHCPv6 Prefix Delegation

- Part A: Prefix Delegation

測試1

1. 建置一個CE-Router以開啟DHCPv6-PD



成果1

1. CE-Router傳送一個有效的DHCPv6 Solicit Message
2. DHCP-Server1傳送一個有效的DHCPv6 Advertise Message給CE-Router
3. CE-Router 傳送一個有效的DHCPv6 Request Message
4. DHCP-Server1傳送一個有效的DHCPv6 Reply message給CE-Router

CONFIDENTIAL For Authorized Personnel Only

DHCPv6 Prefix Delegation

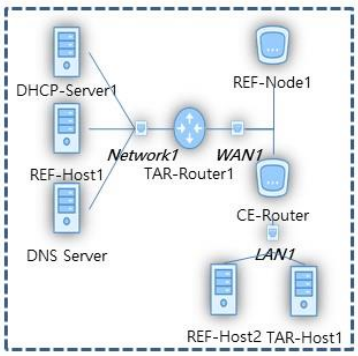
- Part A: Prefix Delegation

測試2

1. 等待T1時間 (50s)過期

成果2

1. CE-Router傳送一個有效且包含IA_PD option跟 IA_PD Prefix option 且兩者數值跟成果1一樣的DHCPv6 Renew Message



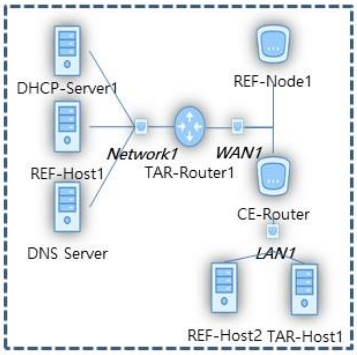
CONFIDENTIAL For Authorized Personnel Only

DHCPv6 Prefix Delegation

- Part B: Renew Message

測試3

1. 建置一個CE-Router以開啟DHCPv6-PD



成果3

1. CE-Router傳送一個有效的DHCPv6 Solicit Message
2. DHCP-Server1傳送一個有效的DHCPv6 Advertise Message給CE-Router
3. CE-Router 傳送一個有效的DHCPv6 Request Message
4. DHCP-Server1傳送一個有效的DHCPv6 Reply message給CE-Router

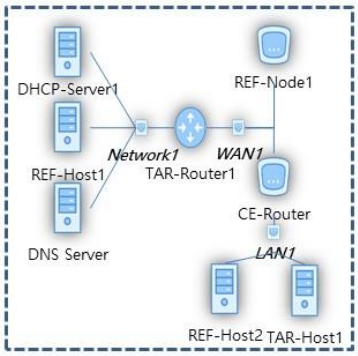
CONFIDENTIAL For Authorized Personnel Only

DHCPv6 Prefix Delegation

- Part B: Renew Message

測試4

1. CE-Router從DHCP-Server1.收到IPv6 prefix information
2. DHCP-Server1指派T1 跟T2 參數給CE-Router 的IA_PD (TAR-Router1 設定T1 為50sT2為80s)
3. 等待T1時間 (50s)過期



成果4

1. CE-Router傳送一個有效的且和成果3的DHCPv6 Reply Message有相同prefix
2. 的DHCPv6 Renew message
3. DHCP-Server1傳送一個有效的且狀態為”成功”的 DHCP Reply message

CONFIDENTIAL For Authorized Personnel Only

DHCPv6 Prefix Delegation

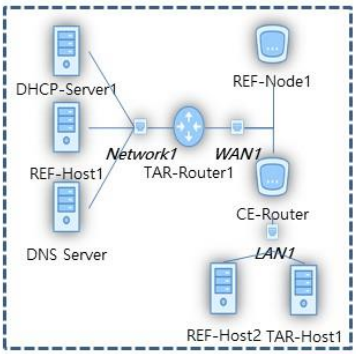
- Part B: Renew Message

測試5

1. 等待T1時間 (50s)過期

成果5

1. CE-Router傳送一個有效且包含IA_PD option跟 IA_PD Prefix option 且兩者數值跟成果3成果4一樣的DHCPv6 Renew Message



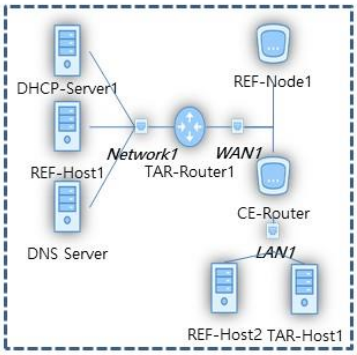
CONFIDENTIAL For Authorized Personnel Only

DHCPv6 Prefix Delegation

- Part C: Rebind Message

測試6

1. 建置一個CE-Router以開啟DHCPv6-PD



成果6

1. CE-Router傳送一個有效的DHCPv6 Solicit Message
2. DHCP-Server1傳送一個有效的DHCPv6 Advertise Message給CE-Router
3. CE-Router 傳送一個有效的DHCPv6 Request Message
4. DHCP-Server1傳送一個有效的DHCPv6 Reply message給CE-Router

CONFIDENTIAL For Authorized Personnel Only

DHCPv6 Prefix Delegation

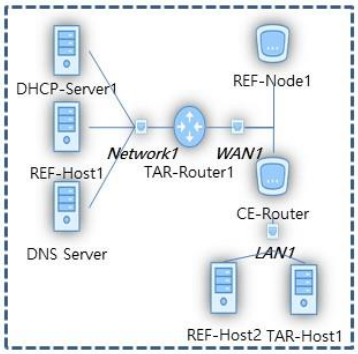
- Part C: Rebind Message

測試7

1. CE-Router收到從DHCP-Server1傳來的IPv6 prefix information
2. DHCP-Server1指派T1 跟T2 參數給CE-Router 的IA_PD (TAR-Router1 設定T1 為50s T2為80s)
3. 關閉DHCP-Server1
4. 等待T2時間 (Reply message後80s)

成果7

1. CE-Router傳送一個有效且包含IA_PD option跟 IA_PD Prefix option 且兩者數值跟成果6一樣的DHCPv6 Renew Message



CONFIDENTIAL For Authorized Personnel Only

DHCPv6 Prefix Delegation

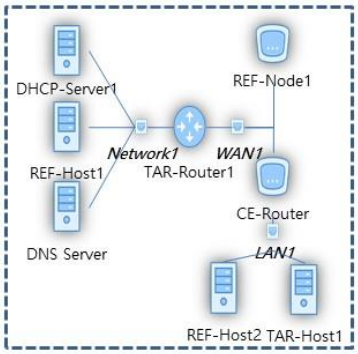
- Part C: Rebind Message

測試8

1. 開啟DHCP-Server1並確認CE-Router address在下一個綁定後被更新
2. 等待T1時間 (50s)過期

成果8

1. CE-Router傳送一個有效的且和成果6的DHCPv6 Reply Message有相同prefix的DHCPv6 Renew message



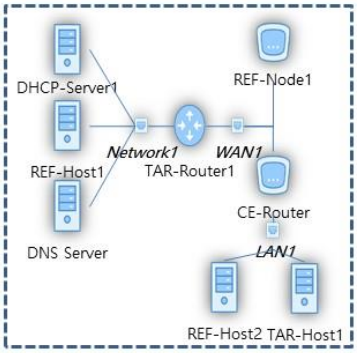
CONFIDENTIAL For Authorized Personnel Only

DHCPv6 Prefix Delegation

- Part D: Release Message

測試9

1. 建置一個CE-Router以開啟DHCPv6-PD



成果9

1. CE-Router傳送一個有效的DHCPv6 Solicit Message
2. DHCP-Server1傳送一個有效的DHCPv6 Advertise Message給CE-Router
3. CE-Router 傳送一個有效的DHCPv6 Request Message
4. TAR-Router1傳送一個有效的DHCPv6 Reply message給CE-Router

CONFIDENTIAL For Authorized Personnel Only

DHCPv6 Prefix Delegation

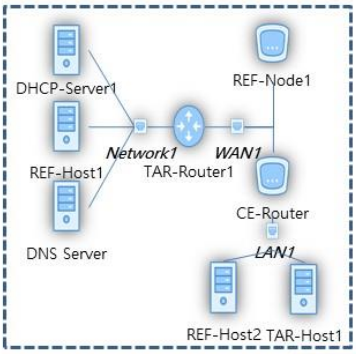
- Part D: Release Message

測試10

1. CE-Router收到從DHCP-Server1傳來的IPv6 prefix information
2. DHCP-Server1指派T1 跟T2 參數給CE-Router 的IA_PD (TAR-Router1 設定T1 為50s T2為80s)
3. 建置 CE-Router釋放IPv6 Prefix.

成果10

1. CE-Router傳送一個有效且包含IA_PD option跟 IA_PD Prefix option 且兩者數值跟成果9一樣的DHCPv6 Renew Message



CONFIDENTIAL For Authorized Personnel Only

DHCPv6 Prefix Delegation

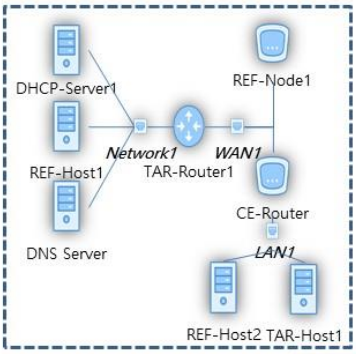
- Part D: Release Message

測試11

1. 等待T1時間 (50s)過期

成果11

1. CE-Router不傳任何 Client-Initiated Configuration messages 給被釋放的IA_PD



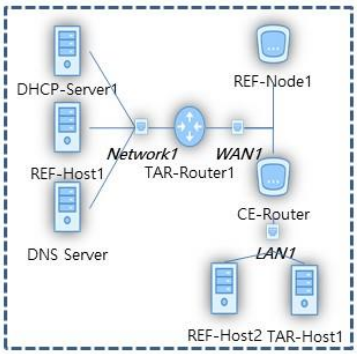
CONFIDENTIAL For Authorized Personnel Only

DHCPv6 Prefix Delegation

- Part E: Hint

測試12

1. 設定CE-Router開啟DHCPv6-PD



成果12

1. CE-Router傳送一個有效的 DHCPv6 Solicit Message
2. DHCP-Server1傳送一個有效的 DHCPv6 Advertise Message給CE-Router
3. CE-Router 傳送一個有效的 DHCPv6 Request Message

CONFIDENTIAL For Authorized Personnel Only

DHCPv6 Prefix Delegation

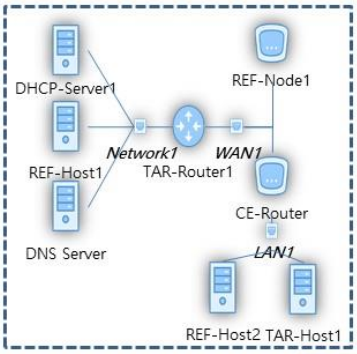
- Part E: Hint

測試13

1. 配置DHCP-Server1 分配不同prefix長度然後從CE-Router傳來的DHCPv6 Solicit message 提供prefix hint
2. 等待T1時間 (50s)過期

成果13

1. CE-Router傳送一個有效且包含IA_PD option跟 IA_PD Prefix option 且兩者數值跟成果12一樣的DHCPv6 Renew Message



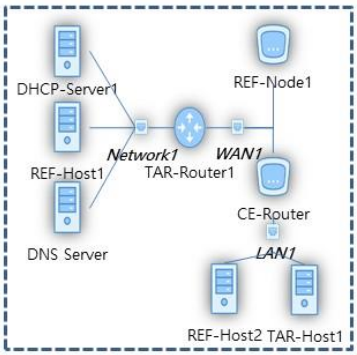
CONFIDENTIAL For Authorized Personnel Only

DHCPv6 Prefix Delegation

- Part F: M Flag

測試14

1. 配置TAR-Router1傳送M flag設為1且O flag 設為0的Router Advertisement
2. 建置一個CE-Router以開啟DHCPv6-PD



成果14

1. CE-Router傳送一個有效的DHCPv6 Solicit Message
2. DHCP-Server1傳送一個有效的DHCPv6 Advertise Message給CE-Router
3. CE-Router 傳送一個有效的DHCPv6 Request Message
4. DHCP-Server1傳送一個有效的DHCPv6 Reply message給CE-Router

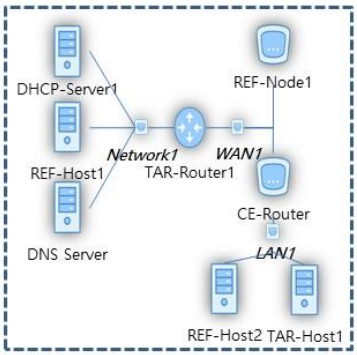
CONFIDENTIAL For Authorized Personnel Only

DHCPv6 Prefix Delegation

- Part G: O Flag

測試15

1. 配置TAR-Router1傳送M flag設為0且O flag 設為1的Router Advertisement
2. 建置一個CE-Router以開啟DHCPv6-PD



成果15

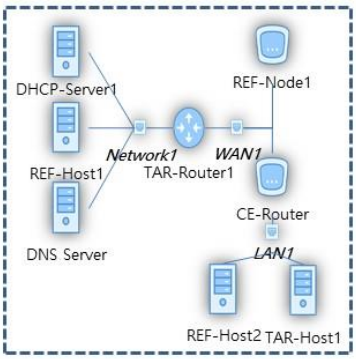
1. CE-Router傳送一個有效的DHCPv6 Solicit Message
2. DHCP-Server1傳送一個有效的DHCPv6 Advertise Message給CE-Router
3. CE-Router 傳送一個有效的DHCPv6 Request Message
4. DHCP-Server1傳送一個有效的DHCPv6 Reply message給CE-Router

CONFIDENTIAL For Authorized Personnel Only

Unnumbered WAN

測試1

1. 設定TAR-Router1傳送一個M flag設為0且O flag設為1的Router Advertisement



成果1

1. CE-Router傳送一個有效的DHCPv6 Solicit Message
2. DHCP-Server1傳送一個有效的DHCPv6 Advertise Message給CE-Router
3. CE-Router傳送一個有效的DHCPv6 Request

CONFIDENTIAL For Authorized Personnel Only

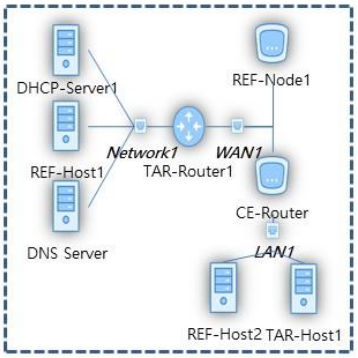
Unnumbered WAN

測試2

1. 使用一個應用程式例如traceroute6使REF-Host1傳送一個hop-limit為2的IPv6封包給TAR-Host1

成果2

1. CE-Router應該用LAN interface 上取得的global source address傳送一個ICMPv6 Time Exceeded message給 REF-Host1



CONFIDENTIAL For Authorized Personnel Only

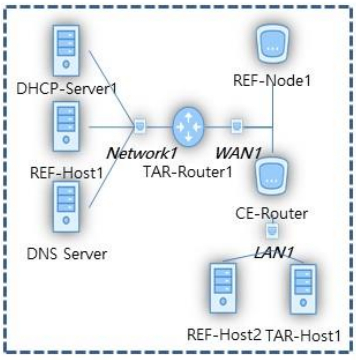
DHCPv6 SOL_MAX_RT

測試1

1. 配置DHCP-Server1回應包含SOL_MAX_RT option 的DHCPv6 Advertise message
2. 設定MAX_SOL_RT 為180 秒
3. 配置DHCP server不指派IPv6 addresses或prefixes
4. 開啟CE-Router

成果1

1. DHCP-Server1傳送一個包含所有從CE-Router傳來SOL_MAX_RT option設為180的有效的Solicit Message 的DHCPv6 Advertise Message
2. CE-Router不應該發送 Request messages給DHCP-Server1



CONFIDENTIAL For Authorized Personnel Only

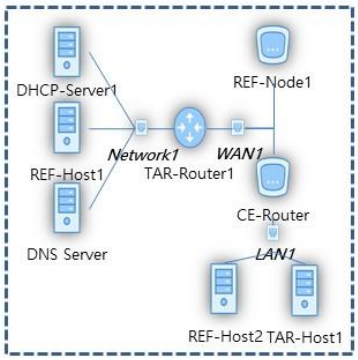
DHCPv6 SOL_MAX_RT

測試2

1. 等待600秒

成果2

1. 最後兩個被CE-Router傳送的DHCPv6 Solicit Messages 應該分別是162和198秒



CONFIDENTIAL For Authorized Personnel Only

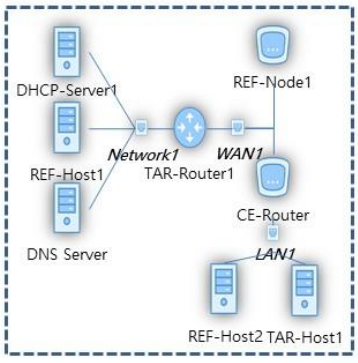
L Flag Processing

測試1

1. 配置TAR-Router1在WAN1上傳送one prefix的Router Advertisements (valid lifetime = 30秒) 並且清除L-flag . Prefix 應該和正在為WAN介面服務的DHCP Server的prefix一樣
2. 等待足夠時間讓CE-Router透過DHCPv6獲得一個IPv6 address
3. 從REF-Node1傳送一個ICMPv6 Echo Request 給CERouter 的DHCPv6 global address

成果1

1. CE-Router應該會將TAR-Router1作為下一個hop回應所有從REF-Node1傳來的ICMPv6 Echo Requests



CONFIDENTIAL For Authorized Personnel Only

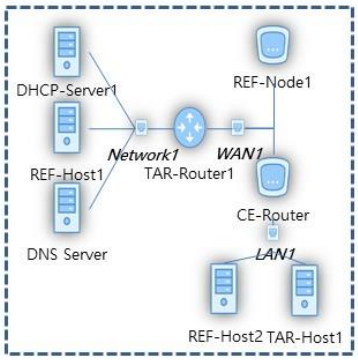
L Flag Processing

測試1

1. 配置TAR-Router1在WAN1上傳送one prefix的Router Advertisements (valid lifetime = 30秒) 並且清除L-flag . Prefix 應該和正在為WAN介面服務的DHCP Server的prefix一樣
2. 等待足夠時間讓CE-Router透過DHCPv6獲得一個IPv6 address
3. 從REF-Node1傳送一個ICMPv6 Echo Request 給CERouter 的DHCPv6 global address

成果1

1. CE-Router應該會將TAR-Router1作為下一個hop回應所有從REF-Node1傳來的ICMPv6 Echo Requests



CONFIDENTIAL
For Authorized Personnel Only

Mobile broadband networklab

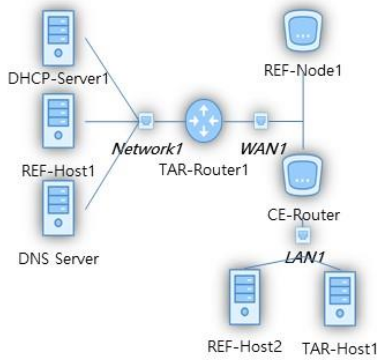


Q & A





LAN Side Configuration



CONFIDENTIAL
For Authorized Personnel Only

Duplicate Address Detection and Neighbor Discovery

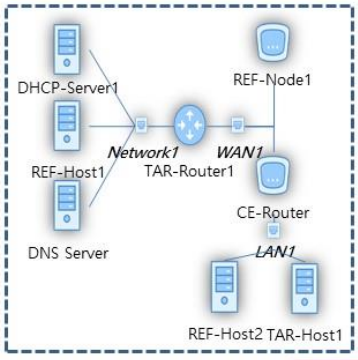
- Part A: Duplicate Address Detection – Tentative Address Unique (Link-Local)

測試1

1. 關閉所有連線至LAN1的介面
2. 開啟所有在LAN1上的介面，開啟CE-Router後開啟TAR-Host1
3. 等待所有在LAN1 上的裝置在他們的link-local addresses上執行 Duplicate Address Detection
4. 開啟REF-Host2確保他已經清除 neighbor cache
5. 從REF-Host2傳送ICMPv6 Echo Request給CE-Router的LAN1介面的link-local address

成果1

1. CE-Router應該回應ICMPv6 Echo Replies給所有從REF-Host2來的ICMPv6 Echo Requests



CONFIDENTIAL
For Authorized Personnel Only

Duplicate Address Detection and Neighbor Discovery

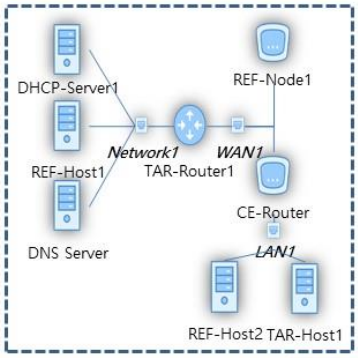
- Part A: Duplicate Address Detection – Tentative Address Unique (Link-Local)

測試2

1. 重複執行測試1步驟但在步驟2時先開啟TAR-Host1後開啟CE-Router

成果2

1. CE-Router應該回應ICMPv6 Echo Replies給所有從REF-Host2來的ICMPv6 Echo Requests



CONFIDENTIAL For Authorized Personnel Only

Duplicate Address Detection and Neighbor Discovery

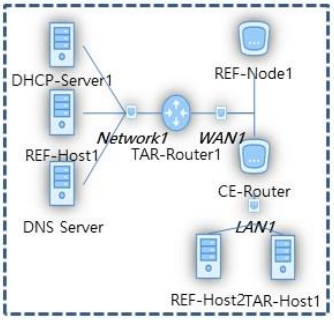
- Part B: Duplicate Address Detection – Tentative Address Duplicated. (Link-Local)

測試3

1. 關閉所有連線至LAN1的介面
2. 配置TAR-Host1 和CE-Router有同樣的link-local address
3. 開啟所有在LAN1上的介面，開啟TAR-Host1後開啟CE-Router
4. 等待所有在LAN1 上的裝置在他們的link-local addresses上執行Duplicate Address Detection
5. 開啟REF-Host2確保他已經清除neighbor cache
6. 從REF-Host2傳送ICMPv6 Echo Request給CE-Router的LAN1介面的link-local address

成果3

1. TAR-Host1應該回應ICMPv6 Echo Replies給所有從REF-Host2來的ICMPv6 Echo Requests
2. CE-Router不該因為duplicated address回應任何 neighbor solicitations 或ICMPv6 Echo Request



CONFIDENTIAL For Authorized Personnel Only

Duplicate Address Detection and Neighbor Discovery

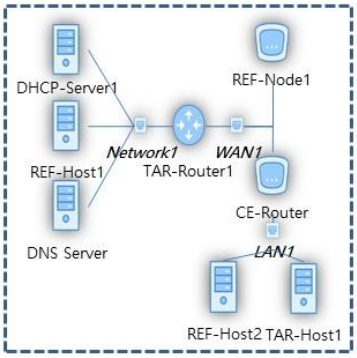
- Part B: Duplicate Address Detection – Tentative Address Duplicated. (Link-Local)

測試4

1. 關閉所有連線至LAN1的介面
2. 開啟所有在LAN1上的介面，開啟CE-Router後開啟TAR-Host1
3. 等待所有在LAN1 上的裝置在他們的link-local addresses上執行Duplicate Address Detection
4. 從REF-Host2傳送ICMPv6 Echo Request給CE-Router的LAN1介面的link-local address

成果4

1. CE-Router應該回應ICMPv6 Echo Replies給所有從REF-Host2來的ICMPv6 Echo Requests



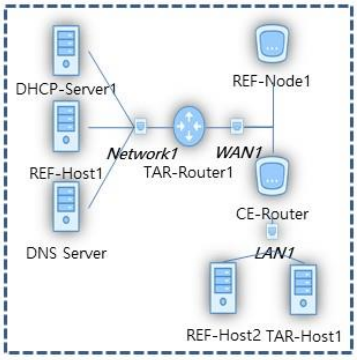
CONFIDENTIAL For Authorized Personnel Only

Assigning Prefixes to LAN Interfaces

- Part A: Prefix Length of /64

測試1

1. 配置DHCP-Server1 透過Prefix Delegation分配一個/64 prefix
2. CE-Router開啟DHCPv6-PD



成果1

1. CE-Router傳送一個有效的DHCPv6 Solicit Message
2. DHCP-Server1傳送一個有效的DHCPv6 Advertise Message給CE-Router
3. CE-Router傳送一個有效的DHCPv6 Request Message
4. DHCP-Server1傳送一個有效的DHCP Reply message給CE-Router

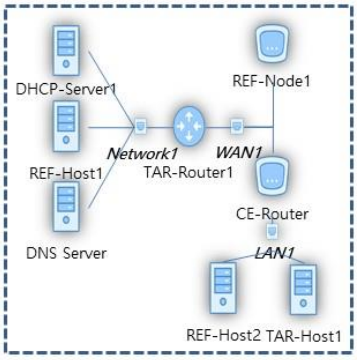
CONFIDENTIAL For Authorized Personnel Only

Assigning Prefixes to LAN Interfaces

- Part A: Prefix Length of /64

測試2

1. 等待在LAN1上的address configuration和Router Advertisements的傳送



成果2

1. CE-Router應該執行Duplicate Address Detection為了將addresses分配給他的介面
2. CE-Router應該傳送一個Prefix Information Option 為測試1分配的/64 prefix 的Router Advertisements
3. 在Prefix Information Option內期待的和有效的lifetimes應該比在IA_PD內的短

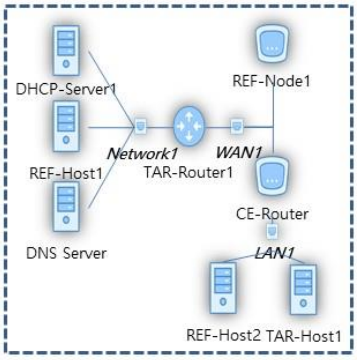
CONFIDENTIAL For Authorized Personnel Only

Assigning Prefixes to LAN Interfaces

- Part A: Prefix Length of /64

測試3

1. TAR-Host1傳送ICMPv6 Echo Request 給在LAN1上的CE-Router 的 global address



成果3

1. CE-Router應該回應ICMPv6 Echo Replies給所有從TAR-Host1來的ICMPv6 Echo Requests

CONFIDENTIAL For Authorized Personnel Only

Assigning Prefixes to LAN Interfaces

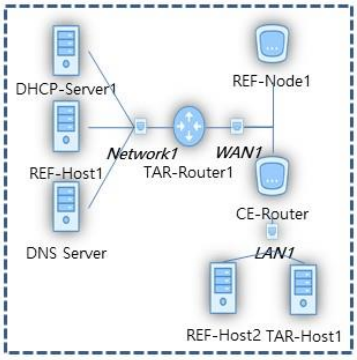
- Part A: Prefix Length of /64

測試4

1. TAR-Host1傳送ICMPv6 Echo Request給REF-Host1

成果4

1. REF-Host1應該回應ICMPv6 Echo Replies給所有從TAR-Host1來的ICMPv6 Echo Requests



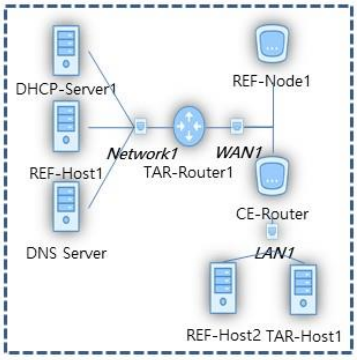
CONFIDENTIAL For Authorized Personnel Only

Assigning Prefixes to LAN Interfaces

- Part B: Prefix Length of /60

測試5

1. 配置DHCP-Server1 透過Prefix Delegation分配一個/60 prefix
2. CE-Router開啟DHCPv6-PD



成果5

1. CE-Router傳送一個有效的DHCPv6 Solicit Message
2. DHCP-Server1傳送一個有效的DHCPv6 Advertise Message給CE-Router
3. CE-Router傳送一個有效的DHCPv6 Request Message
4. DHCP-Server1傳送一個有效的DHCP Reply message給CE-Router

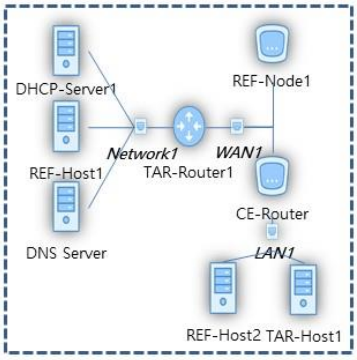
CONFIDENTIAL For Authorized Personnel Only

Assigning Prefixes to LAN Interfaces

- Part B: Prefix Length of /60

測試6

1. 等待在LAN1上的address configuration和Router Advertisements的傳送



成果6

1. CE-Router應該執行Duplicate Address Detection為了將addresses分配給他的介面
2. CE-Router應該傳送一個包含/64 prefix的Prefix Information Option為測試6分配的/56prefix 的Router Advertisements
3. 在Prefix Information Option內期待的和有效的lifetimes應該比在IA_PD內的短

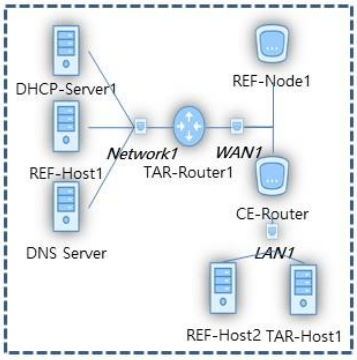
CONFIDENTIAL For Authorized Personnel Only

Assigning Prefixes to LAN Interfaces

- Part B: Prefix Length of /60

測試7

1. TAR-Host1傳送ICMPv6 Echo Request 給在LAN1上的CE-Router的 global address



成果7

1. CE-Router應該回應ICMPv6 Echo Replies給所有從TAR-Host1來的ICMPv6 Echo Requests

CONFIDENTIAL For Authorized Personnel Only

Assigning Prefixes to LAN Interfaces

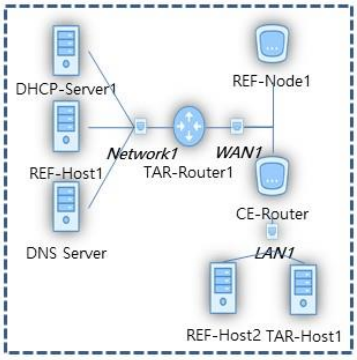
- Part B: Prefix Length of /60

測試8

1. TAR-Host1傳送ICMPv6 Echo Request給REF-Host1

成果8

1. REF-Host1應該回應ICMPv6 Echo Replies給所有從TAR-Host1來的ICMPv6 Echo Requests



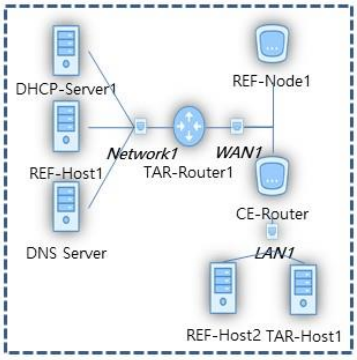
CONFIDENTIAL For Authorized Personnel Only

Assigning Prefixes to LAN Interfaces

- Part C: Prefix Length of /56

測試9

1. 配置DHCP-Server1 透過Prefix Delegation分配一個/56 prefix
2. CE-Router開啟DHCPv6-PD



成果9

1. CE-Router傳送一個有效的DHCPv6 Solicit Message
2. DHCP-Server1傳送一個有效的DHCPv6 Advertise Message給CE-Router
3. CE-Router傳送一個有效的DHCPv6 Request Message
4. DHCP-Server1傳送一個有效的DHCP Reply message給CE-Router

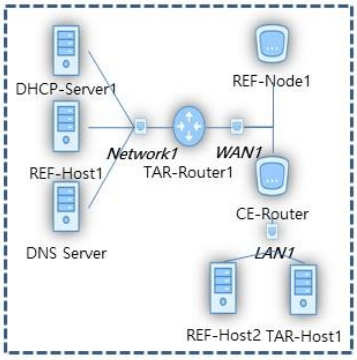
CONFIDENTIAL For Authorized Personnel Only

Assigning Prefixes to LAN Interfaces

- Part C: Prefix Length of /56

測試10

1. 等待在LAN1上的address configuration和Router Advertisements的傳送



成果10

1. 為了將addresses分配給介面卡，CE-Router應該執行Duplicate Address Detection
2. CE-Router應該傳送一個包含/64 prefix的Prefix Information Option為測試9分配的/56 prefix 的Router Advertisements
3. 在Prefix Information Option內期待的和有效的lifetimes應該比在IA_PD內的短

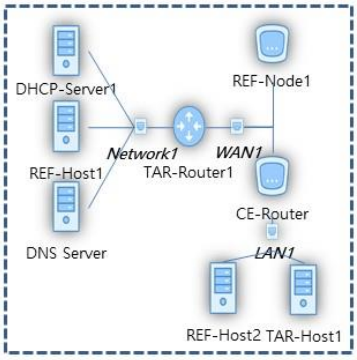
CONFIDENTIAL For Authorized Personnel Only

Assigning Prefixes to LAN Interfaces

- Part C: Prefix Length of /56

測試11

1. TAR-Host1傳送ICMPv6 Echo Request 給在LAN1上的CE-Router的 global address



成果11

1. CE-Router應該回應ICMPv6 Echo Replies給所有從TAR-Host1來的ICMPv6 Echo Requests

CONFIDENTIAL For Authorized Personnel Only

Assigning Prefixes to LAN Interfaces

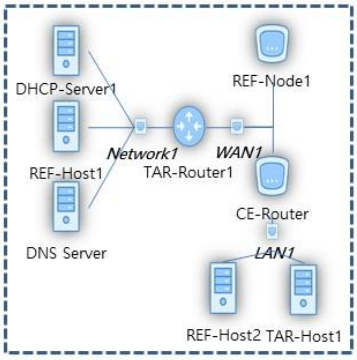
- Part C: Prefix Length of /56

測試12

1. TAR-Host1傳送ICMPv6 Echo Request給REF-Host1

成果12

1. REF-Host1應該回應ICMPv6 Echo Replies給所有從TAR-Host1來的ICMPv6 Echo Requests



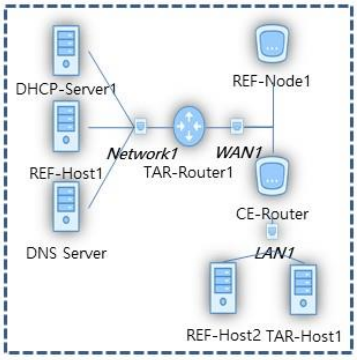
CONFIDENTIAL For Authorized Personnel Only

Router Advertisement

- Part A: Route Information Option

測試1

1. 配置DHCP-Server1 透過Prefix Delegation分配一個/60 prefix
2. CE-Router開啟DHCPv6-PD



成果1

(WAN1)

1. CE-Router傳送一個有效的DHCP Solicit Message
2. DHCP-Server1傳送一個有效的DHCP Advertise Message給CE-Router.
3. CE-Router傳送一個有效的DHCP Request Message
4. DHCP-Server1傳送一個有效的DHCP Reply message給CE-Router

(LAN1)

1. CE-Router傳送一個包含Route Information Option包含delegated prefix的Router Advertisement
2. Prefix Length 和Route Lifetime應該符合DHCPv6 Prefix Delegation提供的資訊

CONFIDENTIAL For Authorized Personnel Only

Router Advertisement

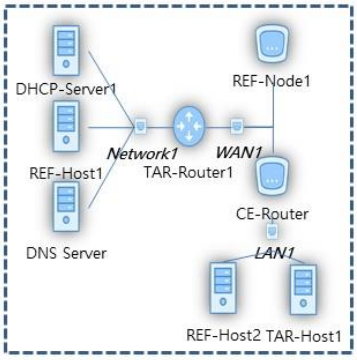
- Part A: Route Information Option

測試2

1. REF-Host1傳送一個ICMPv6 Echo Request給TAR-Host1的global address

成果2

1. TAR-Host1 應該回應ICMPv6 Echo Replies給所有從REF-Host1傳來的ICMPv6 Echo Requests



CONFIDENTIAL For Authorized Personnel Only

Router Advertisement

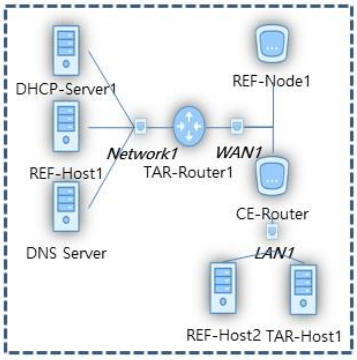
- Part B: No Prefixes

測試3

1. 關閉在WAN1上的CE-Router
2. 配置DHCP-Server不指派IA_PD
3. 開啟在WAN1上的CE-Router

成果3

1. CE-Router不會在LAN上傳輸lifetime大於0的Router Advertisements



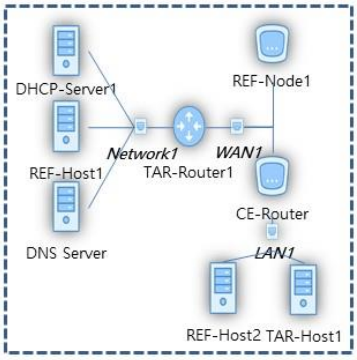
CONFIDENTIAL For Authorized Personnel Only

Router Advertisement

- Part C: Advertising Interface

測試4

1. 關閉在WAN1上的TAR-Host1
2. 開啟在WAN1上的TAR-Host1



成果4

1. TAR-Host傳送一個Router Solicitation
2. CE-Router傳送Router Advertisements
3. Prefix Information Option A和L flags應該被設為1

CONFIDENTIAL For Authorized Personnel Only

Stateless DHCP Server

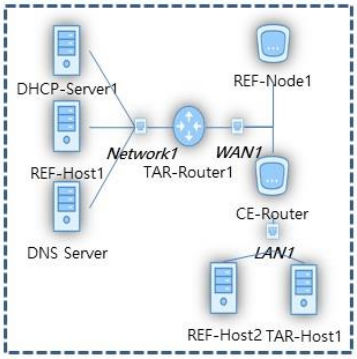
- Part A: DNS Recursive Name Server Option

測試1

1. 配置DHCP-Server 1，包含一個遞迴的DNS服務器選項，該選項包括DNS Server的 global IPv6位址作為name server。
2. CE-Router從DHCP-Server1獲取位址和DNS的資訊
3. 配置CE-Router和TAR-Host1以啟用無狀態的DHCPv6
4. 觀察LAN1上傳輸的封包情況

成果1

1. TAR-Host1必須發送DHCPv6的請求訊息
2. CE-Router從步驟1開始發送帶有DNS Recursive Name Server Option的DHCPv6 Reply message



CONFIDENTIAL For Authorized Personnel Only

Stateless DHCP Server

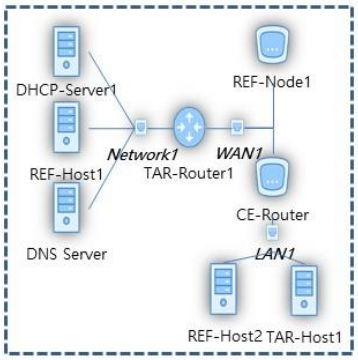
- Part A: DNS Recursive Name Server Option

測試2

1. 配置TAR-Host1來將ICMPv6 Echo Request發送到 “dhcpv6.test.example.com”
2. 觀察LAN1上傳輸的封包

成果2

1. TAR-Host1必須向DNS-Server1發送有效的DNS Request。 DNS-Server1必須傳輸有效的DNS Reply



CONFIDENTIAL For Authorized Personnel Only

Stateless DHCP Server

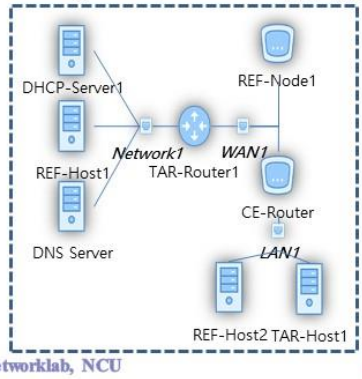
- Part B: Domain Search List Option

測試3

1. 將DHCP-Server1配置為包括一個DNS Recursive Name Server option，該option包括DNS Server global IPv6地址作為name server及包含 “test.example.com”的Domain Search List
2. CE-Router從DHCP-Server1獲取尋址和DNS信息。
3. 配置TAR-Host1以啟用DHCPv6無狀態DHCPv6
4. Configure TAR-Host1 to enable DHCPv6 stateless DHCPv6.

成果3

1. TAR-Host1必須發送一個DHCPv6 Information Request message
2. CE-Router從步驟1開始發送帶有DNS Recursive Name Server Option和Domain Search List Option的DHCPv6回應消息



CONFIDENTIAL For Authorized Personnel Only

Stateless DHCP Server

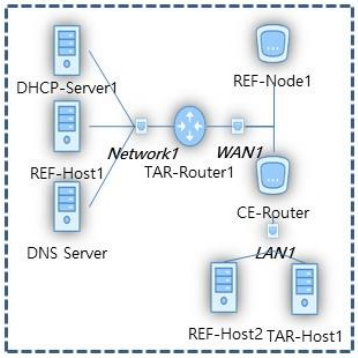
- Part B: Domain Search List Option

測試4

1. 配置TAR-Host1以將ICMPv6 Echo Request發送到 “dhcpv6”

成果4

1. TAR-Host1必須向DNS-Server1發送有效的DNS請求
2. DNS-Server1必須傳輸有效的DNS回應



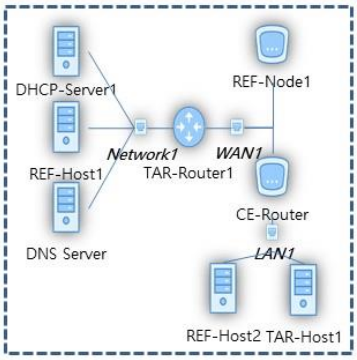
CONFIDENTIAL For Authorized Personnel Only

DHCP Server

- Part A: Initialization

測試1

1. 在LAN1上啟用TAR-Host1



成果1

1. TAR-Host1必須發送DHCPv6 Solicit message
2. CE-Router發送包含IPv6位址信息的DHCPv6 Advertisement message
3. TAR-Host1發送DHCPv6請求信息以確認IPv6地址並請求其他信息
4. CE-Router回應一個包含確認地址的DHCPv6 Reply message

CONFIDENTIAL For Authorized Personnel Only

DHCP Server

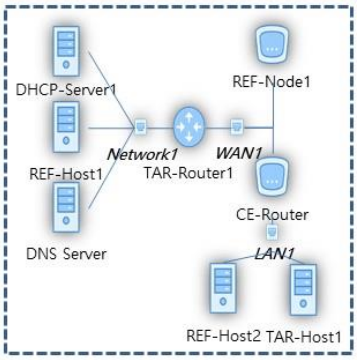
- Part A: Initialization

測試2

1. REF-Host1將ICMPv6 Echo的請求發送到TAR-Host1的DHCPv6位址

成果2

1. TAR-Host1必須使用ICMPv6 Echo Replies來回應來自REF-Host1的所有ICMPv6 Echo Request。



CONFIDENTIAL For Authorized Personnel Only

DHCP Server

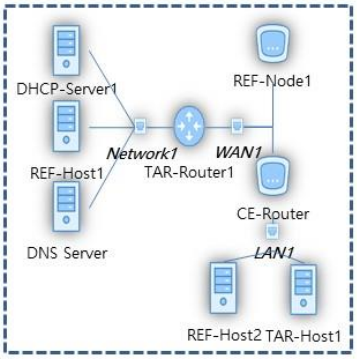
- Part B: Renew message

測試3

1. 在LAN1上啟用TAR-Host1
2. TAR-Host1應從CE-Router收到IPv6地址信息
3. 等待T1時間

成果3

1. TAR-Host1在從CE-Router接收到DHCPv6 Reply message後T1秒發送其第一個DHCPv6 Renew message
2. CE-Router傳送格式正確的DHCP Reply message作為對DHCPv6 Renew message的回應發送格式正確的DHCP Reply message



CONFIDENTIAL For Authorized Personnel Only

DHCP Server

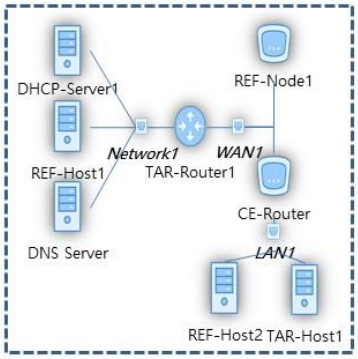
- Part B: Renew message

測試4

1. REF-Host1將ICMPv6 Echo request發送到TAR-Host1 DHCPv6的位址

成果4

1. TAR-Host1必須使用ICMPv6 Echo Replies回應來自REF-Host1的所有ICMPv6 Echo Request



CONFIDENTIAL For Authorized Personnel Only

DHCP Server

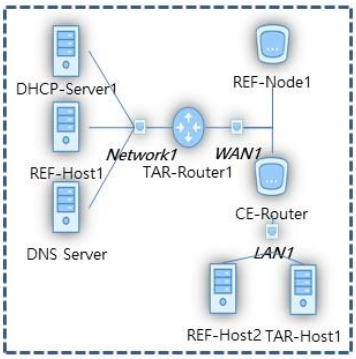
- Part C: Rebind message

測試5

1. 在LAN1上啟用TAR-Host1
2. 留出足夠的時間讓TAR-Host1從CE-Router接收IPv6位址信息。CERouter將T1和T2參數分配給TAR-Host1
3. 在CE-Router上禁用LAN1接口
4. 等待T2時間

成果5

1. AR-Host1發送DHCPv6 Rebind message



CONFIDENTIAL For Authorized Personnel Only

DHCP Server

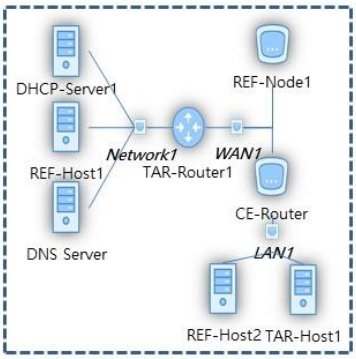
- Part C: Rebind message

測試6

1. 在CE-Router啟用LAN接口，並確認在下一次重新綁定時更新TAR-Host1位址
2. REF-Host1將Echo Request發送到TAR-Host1 DHCPv6位址

成果6

1. TAR-Host1必須使用ICMPv6 Echo Replies回應來自REF-Host1的所有ICMPv6 Echo Request。



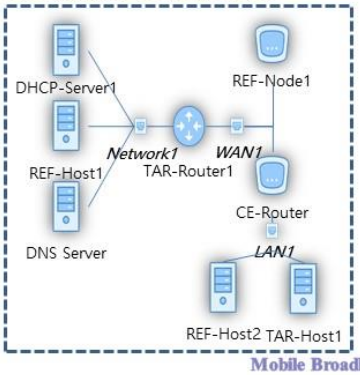
CONFIDENTIAL For Authorized Personnel Only

HCP Server

- Part D: Decline Message

測試7

1. 將REF-Host2配置為與CE-Router分配給TARHost1的global address相同
2. 在LAN1上啟用TAR-Host1，留足夠的時間讓TAR-Host1從CE-Router接收IPv6地址信息



成果7

1. TAR-Host1為其global address發送DAD NS
2. REF-Host2發送請求的NA來回應具有non-unique tentative address的DAD NS
3. TAR-Host1發送DHCP Decline Message
4. CE-Router發送DHCP Reply Message

CONFIDENTIAL For Authorized Personnel Only

DHCP Server

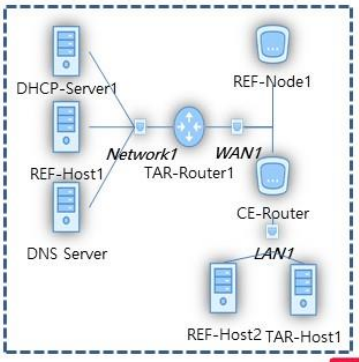
- Part E: DNS Recursive Name Server Option

測試8

1. 配置CE-Router以包括一個具有DNS-Server global IPv6 address option的DNS Recursive Name Server option
2. 在LAN1上啟用TAR-Host1，留出足夠的時間讓TAR-Host1從CE-Router接收IPv6地址信息
3. TAR-Host1將ICMPv6 Echo Request發送到“dhcpv6.test.example.com”

成果8

1. TAR-Host1必須向DNS-Server1發送有效的DNS請求
2. DNS-Server1必須傳輸有效的DNS回應



CONFIDENTIAL For Authorized Personnel Only

DHCP Server

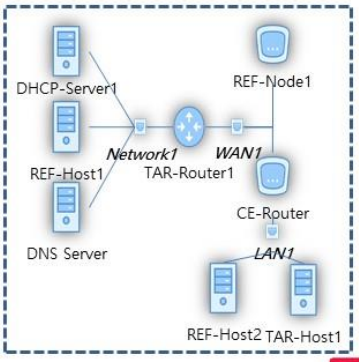
- Part F: Domain Search List Option

測試9

1. 配置CE-Router以包括一個具有DNS-Server global IPv6 address option和包含“test.example.com”的Domain Search List option的DNS Recursive Name Server option
2. 在LAN1上啟用TAR-Host1
3. 允許CE-Router有足夠的時間從CE-Router接收IPv6地址信息
4. TAR-Host1將Echo Request發送到“dhcpv6”

成果9

1. TAR-Host1必須向DNS-Server1發送有效的DNS請求
2. DNS-Server1必須傳輸有效的DNS回應



CONFIDENTIAL For Authorized Personnel Only

Prefix Change

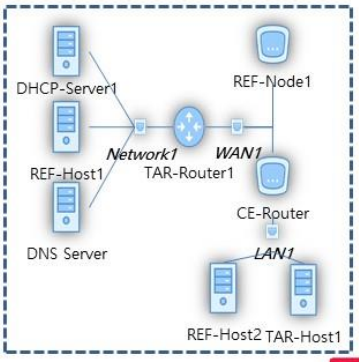
- Part A: Prefix Timeout

測試1

1. 將DHCP-Server1配置為指定的Prefix X，其首選及有效生命週期為1分鐘
2. CE-Router啟用DHCPv6-PD，留時間讓CE-Router在LAN接口上分配Prefix X
3. REF-Host1將ICMPv6 Echo Request發送到TAR-Host1的Prefix X global address

成果1

1. TAR-Host1必須使用ICMPv6 Echo Replies回應來自REF-Host1的所有ICMPv6 Echo Request



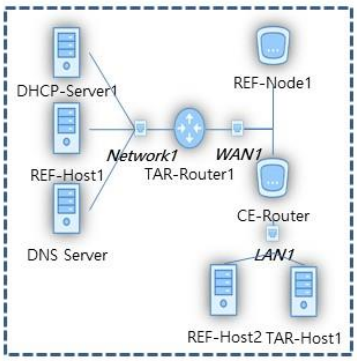
CONFIDENTIAL For Authorized Personnel Only

Prefix Change

- Part A: Prefix Timeout

測試2

1. 配置DHCP-Server1以從可用的prefixes中刪除Prefix X
2. 配置Prefix Y為可用於CE-Router
3. 等待CE-Router為Prefix X發送DHCPv6更新



成果2

1. CE-Router發送有效的DHCPv6 Renew message
2. DHCP-Server1在WAN1上從測試2步驟1發送帶有新IPv6 prefix的有效DHCP Reply message
3. CE-Router必須使用Prefix Information Option發送Router Advertisement，該option包含以前在LAN1上委派的所有preferred lifetime為零的prefix
4. prefix選項的有效生命週期不得大於IA_PD中公佈的值
5. 未來來自CE-Router的DHCPv6 Renew message不得包含舊的IPv6 prefix

CONFIDENTIAL For Authorized Personnel Only

Prefix Change

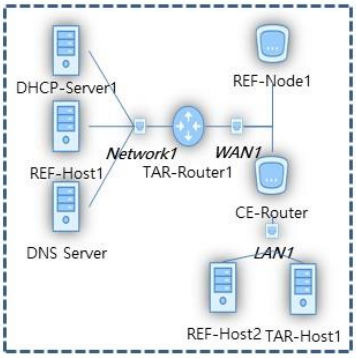
- Part A: Prefix Timeout

測試3

1. 等待Prefix X的有效生命週期超時
2. 使用測試1第二步驟中的Prefix X來分配一個global address 給REF-Host2
3. REF-Host1將ICMPv6 Echo request發送到TAR-Host1的prefix Y global address

成果3

1. TAR-Host1必須使用ICMPv6 Echo Replies回應來自REF-Host1的所有ICMPv6 Echo Request



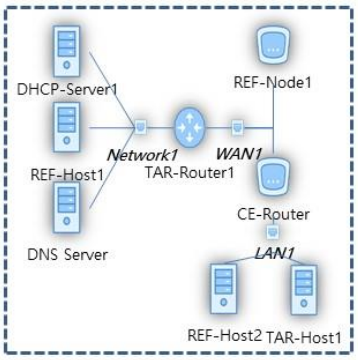
CONFIDENTIAL For Authorized Personnel Only

Prefix Change

- Part A: Prefix Timeout

測試4

1. REF-Host2將來自prefix X global address的ICMPv6 Echo Request發送到TAR-Host1 prefix X global address



成果4

1. TAR-Host1必須將Prefix1設為timeout，TAR -Host1不得回應來自REF-Host2的ICMPv6 Echo Request或Neighbor Solicitations，且REF-Host2的位址與Prefix X相關聯

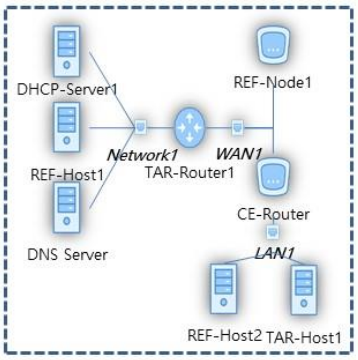
CONFIDENTIAL For Authorized Personnel Only

Prefix Change

- Part A: Prefix Timeout

測試5

1. REF-Host2將來自測試3步驟2的prefix X global address的ICMPv6 Echo Request發送到REF-Host1



成果5

1. CE-Router不得轉發來自REF-Host2的ICMPv6 Echo Request
2. CE-Router必須向REF-Host2發送帶有code為5的ICMPv6 Destination Unreachable message

CONFIDENTIAL For Authorized Personnel Only

Prefix Change

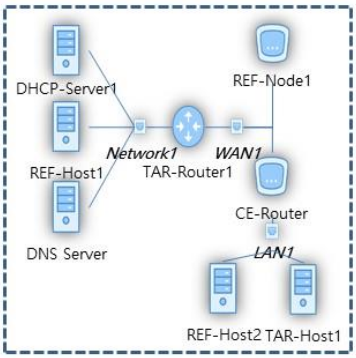
- Part B: Reconfigure

測試6

1. CE-Router啟用DHCPv6-PD
2. 允許CE-Router在LAN接口上分配prefix X，preferred和valid的lifetime期為1分鐘
3. REF-Host1將ICMPv6 Echo Request發送到TAR-Host1的Prefix X global address

成果6

1. TAR-Host1必須使用ICMPv6 Echo Replies回應來自REF-Host1的所有ICMPv6 Echo Request



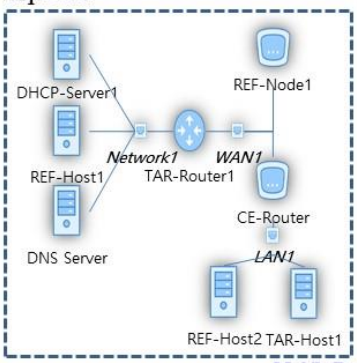
CONFIDENTIAL For Authorized Personnel Only

Prefix Change

- Part B: Reconfigure

測試7

1. 配置DHCP-Server1以使用DHCPv6重新配置將新的Prefix Y委派給CE-Router
2. 允許CE-Router timeout Prefix X的valid lifetime並在LAN接口上分配prefix



成果7

1. DHCP-Server1向WAN1上的CE-Router發送DHCPv6 Reconfigure
2. CE-Router將DHCPv6 Renew Message發送到DHCP-Server1
3. DHCP-Server1發送preferred lifetime為0的Prefix X的DHCPv6 Reply和具有valid preferred lifetime的Prefix Y
4. CE-Router必須使用Prefix Information Option發送Router Advertisements，該option包含以前在LAN1上委派的所有preferred lifetime為零的prefix
5. Prefix Option的valid lifetime不得大於IA_PD中公佈的值
6. 來自CE-Router的未來的DHCPv6 Renew messages不得包含舊的IPv6 prefix

Mobile Broadband Networklab, NCU
CONFIDENTIAL For Authorized Personnel Only

Prefix Change

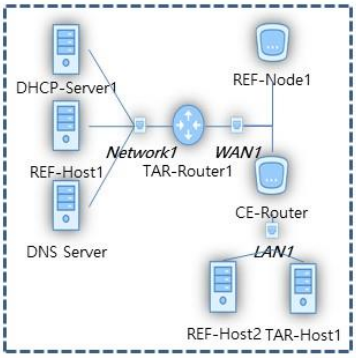
- Part B: Reconfigure

測試8

1. 使用測試1步驟1中的prefix X為REF-Host2 global address
2. REF-Host1將ICMPv6 Echo Request發送到TAR-Host1的Prefix Y global address

成果8

1. TAR-Host1必須使用ICMPv6 Echo Replies回應來自REF-Host1的所有ICMPv6 Echo Request



Mobile Broadband Networklab, NCU
CONFIDENTIAL For Authorized Personnel Only

Prefix Change

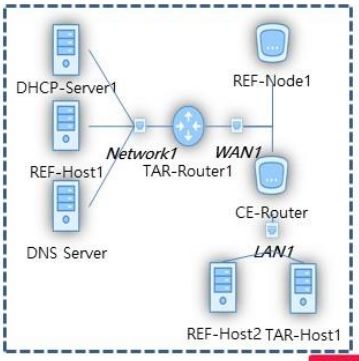
- Part B: Reconfigure

測試9

1. 1REF-Host2將來自Prefix X global address的ICMPv6 Echo Request發送到TAR-Host1 Prefix X global address

成果9

1. TAR-Host1必須timeout Prefix1
2. TAR-Host1不得使用與prefix X關聯的位址來回應來自REF-Host2的ICMPv6 Echo Request或Neighbor Solicitation



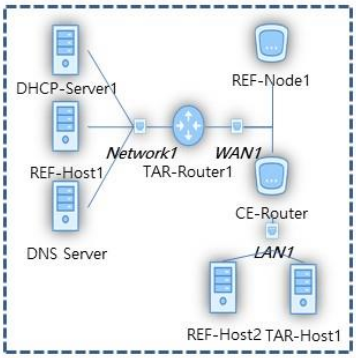
CONFIDENTIAL For Authorized Personnel Only

Prefix Change

- Part B: Reconfigure

測試10

1. REF-Host2將來自測試3步驟1的Prefix X global address的ICMPv6 Echo Request發送到REFHost1



成果10

1. CE-Router不得轉發來自REF-Host2的ICMPv6 Echo Request
2. CE-Router必須向REF-Host2發送帶有code為5的ICMPv6 Destination Unreachable message

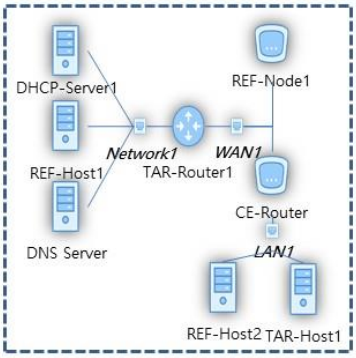
CONFIDENTIAL For Authorized Personnel Only

Link MTU

- Part A: Sending Packet Too Big

測試1

1. 配置CE-Router的WAN1為1280的MTU
2. TAR-Host1向REF-Host1發送1500的ICMPv6 Echo Request



成果1

1. CE-Router必須向TAR-Host1發送有效的ICMPv6 Packet Too Big message
2. 收到Packet Too Big message後，TAR-Host1應分割ICMPv6 Echo Request給REF-Host1

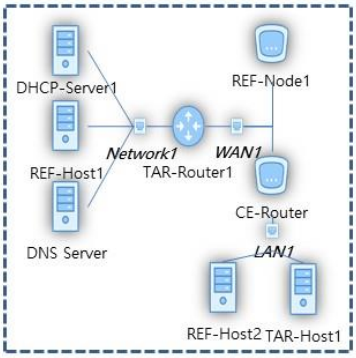
Mobile Broadband Networklab, NCU
CONFIDENTIAL For Authorized Personnel Only

Link MTU

- Part B: Forwarding Fragmented Packets

測試2

1. 將Network1MTU配置為1280
2. REF-Host1將大小為1500的ICMPv6 Echo Request發送到TAR-Host1



成果2

1. CE-Router應將被fragment的ICMPv6 Echo Request封包從WAN1網絡轉發到LAN1網絡

Mobile Broadband Networklab, NCU
CONFIDENTIAL For Authorized Personnel Only

DNS Information in Router Advertisement

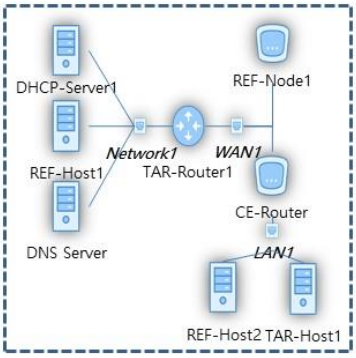
- Part A: Recursive DNS Server

測試1

1. 在TAR-Host1上禁用DHCPv6 Client
2. 將CE-Router配置為DNS Recursive Name Server option，包括DNS-Server global IPv6 address作為name server

成果1

1. CE-Router必須發送包含Recursive DNS Server Option的Router Advertisement



CONFIDENTIAL For Authorized Personnel Only

DNS Information in Router Advertisement

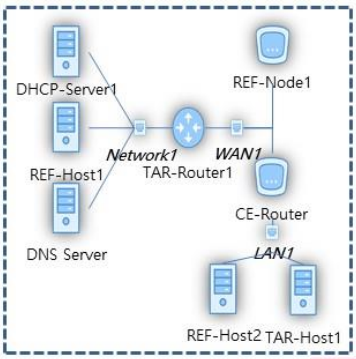
- Part A: Recursive DNS Server

測試2

1. 配置TAR-Host1以將ICMPv6 Echo Request發送到 “dhcpv6.test.example.com”

成果2

1. TAR-Host1必須向DNS-Server1發送有效的DNS request
2. DNS-Server1必須傳輸有效的DNS response



CONFIDENTIAL For Authorized Personnel Only

DNS Information in Router Advertisement

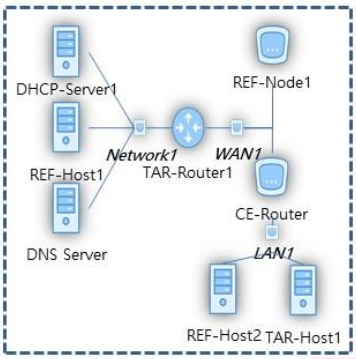
- Part B: DNS Search List

測試3

1. 在TAR-Host1上禁用DHCPv6用戶端
2. 將CE-Router配置為DNS Recursive Name Server option，包括DNS-Server global IPv6 address作為name server及包含“dhcpv6”的Domain Search List option
3. 在LAN1上啟用TAR-Host1。

成果3

1. CE-Router必須發送包含Recursive DNS Server Option和DNS Search List Option的Router Advertisement



CONFIDENTIAL For Authorized Personnel Only

DNS Information in Router Advertisement

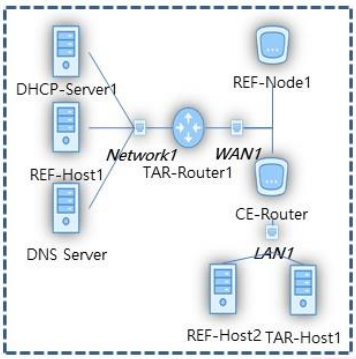
- Part B: DNS Search List

測試4

1. 配置TAR-Host1以將ICMPv6 Echo Request發送到“dhcpv6”

成果4

1. TAR-Host1必須向DNS-Server1發送有效的DNS request
2. DNS-Server1必須傳輸有效的DNS response



CONFIDENTIAL For Authorized Personnel Only

Ingress Filtering

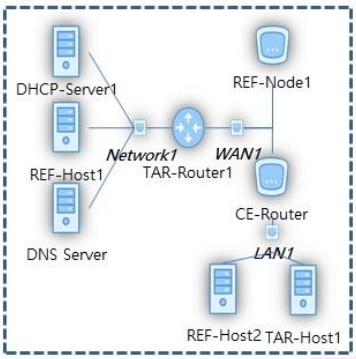
- Part A: Manually configured address

測試1

1. 使用未委託給CE-Router的prefix的global IPv6 address配置TAR-Host1
2. TAR-Host1使用步驟1中配置的位址向REF-Host1發送ICMPv6 Echo Request

成果1

1. CE-Router不得將ICARv6 Echo Request從TAR-Host1轉發到REF-Host1，而必須向TAR-Host1發送code為5的ICMPv6 Destination Unreachable message



CONFIDENTIAL For Authorized Personnel Only

Ingress Filtering

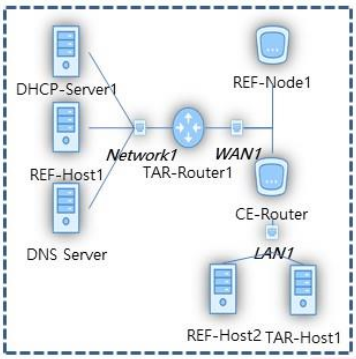
- Part B: Previous Address

測試2

1. 配置DHCP-Server1使用address lifetime 讓prefix X在整個測試持續有效
2. TAR-Host1將ICMPv6 Echo Request發送到REF-Host1

成果2

1. REF-Host1必須使用ICMPv6 Echo Replies回應來自TAR-Host1的所有ICMPv6 Echo Request



CONFIDENTIAL For Authorized Personnel Only

Ingress Filtering

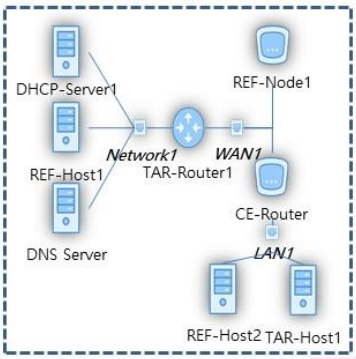
- Part B: Previous Address

測試3

1. 關閉CE-Router
2. 配置DHCP-Server1以將新的prefix Y委派給CE-Router
3. 打開CE-Router的電源，允許TAR-Host1獲取prefix Y
4. 配置TAR-Host1使用prefix X到REF-Host1的地址發送ICMPv6 Echo Request

成果3

1. CE-Router不得將ICMPv6 Echo Request從TAR-Host1轉發到REF-Host1，而必須向TAR-Host1發送code為5的ICMPv6 Destination Unreachable message



CONFIDENTIAL
For Authorized Personnel Only

Mobile broadband networklab

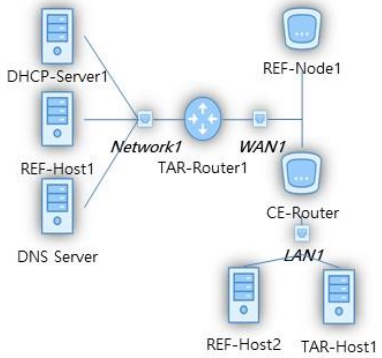


Q & A





General Requirement Test



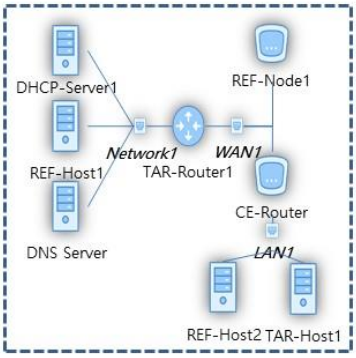
CONFIDENTIAL For Authorized Personnel Only

ICMPv6

- Part A: Link-Local Address (LAN)

測試1

1. 將TAR-Host1的ICMPv6 Echo Request發送到CE-Router的link-local address



成果1

1. CE-Router必須接收從TAR-Host1發送的所有ICMPv6 Echo Request，並使用ICMPv6 Echo Replies進行回應
2. Echo Reply的來源位址必須等於Echo Request中的目標位址，Echo Reply的目標位址必須等於Echo Request中的來源位址。

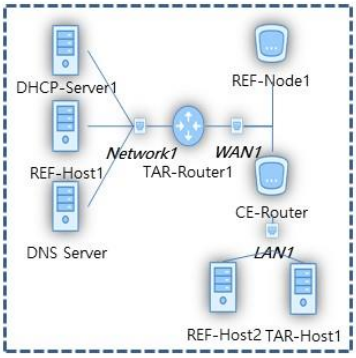
CONFIDENTIAL For Authorized Personnel Only

ICMPv6

- Part A: Link-Local Address (LAN)

測試2

1. 將CE-Router的ICMPv6 Echo Request發送到TAR-Host1的link-local address



成果2

1. TAR-Host1必須接收從CE-Router發送的所有ICMPv6 Echo Request，並使用ICMPv6 Echo Replies進行回應
2. Echo Reply的來源位址必須等於Echo Request中的目標位址，Echo Reply的目標位址必須等於Echo Request中的來源位址。

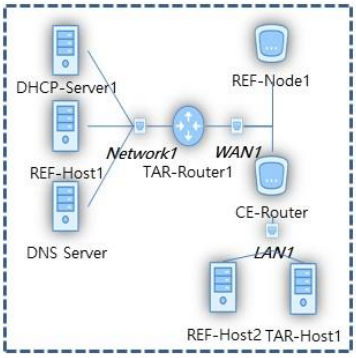
CONFIDENTIAL For Authorized Personnel Only

ICMPv6

- Part B: Global Unicast Address (LAN)

測試3

1. 將TAR-Host1的ICMPv6 Echo Request發送到CE-Router LAN接口的global address



成果3

1. CE-Router必須接收從TAR-Host1發送的所有ICMPv6 Echo Request，並使用ICMPv6 Echo Replies進行回應
2. Echo Reply的來源位址必須等於Echo Request中的目標位址，Echo Reply的目標位址必須等於Echo Request中的來源位址

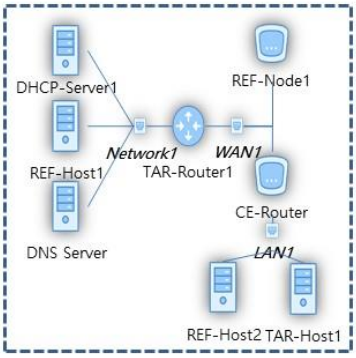
CONFIDENTIAL For Authorized Personnel Only

ICMPv6

- Part B: Global Unicast Address (LAN)

測試4

1. 將CE-Router的ICMPv6 Echo Request發送到TAR-Host1的global address



成果4

1. TAR-Host1必須接收從CE-Router發送的所有ICMPv6 Echo Request，並使用ICMPv6 Echo Replies進行回應
2. Echo Reply的來源位址必須等於Echo Request中的目標位址，Echo Reply的目標位址必須等於Echo Request中的來源位址

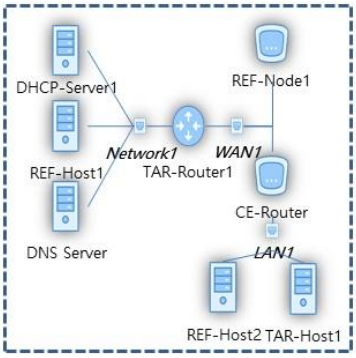
CONFIDENTIAL For Authorized Personnel Only

ICMPv6

- Part C: Link-Local Address (WAN)

測試5

1. 將TAR-Router1的ICMPv6 Echo Request傳送到CE-Router的link-local address



成果5

1. CE-Router必須接收從TAR-Router1發送的所有ICMPv6 Echo Request，並使用ICMPv6 Echo Replies進行回應
2. Echo Reply的來源位址必須等於Echo Request中的目標位址，Echo Reply的目標位址必須等於Echo Request中的來源位址

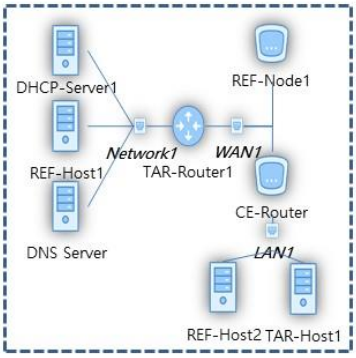
CONFIDENTIAL For Authorized Personnel Only

ICMPv6

- Part C: Link-Local Address (WAN)

測試6

1. 將CE-Router的ICMPv6 Echo Request發送到TAR-Router1的link-local address



成果6

1. TAR-Router1必須接收CE-Router發送的所有ICMPv6 Echo Request，並使用ICMPv6 Echo Replies進行回應
2. Echo Reply的來源位址必須等於Echo Request中的目標位址，Echo Reply的目標位址必須等於Echo Request中的來源位址

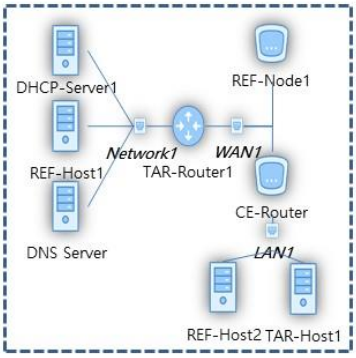
CONFIDENTIAL For Authorized Personnel Only

ICMPv6

- Part D: Global Unicast Address (WAN)

測試7

1. 將TAR-Router1的ICMPv6 Echo Request發送到CE-Router的DHCPv6 global address



成果7

1. CE-Router必須接收從TAR-Router1發送的所有ICMPv6 Echo Request，並使用ICMPv6 Echo Replies進行回應
2. Echo Reply的來源地址必須等於Echo Request中的目標地址，Echo Reply的目標地址必須等於Echo Request中的來源地址

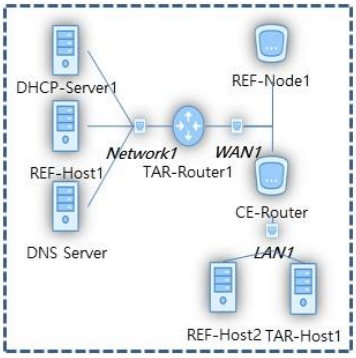
CONFIDENTIAL For Authorized Personnel Only

ICMPv6

- Part D: Global Unicast Address (WAN)

測試8

1. 將CE-Router的ICMPv6 Echo Request發送到TAR-Router1的global address



成果8

1. TAR-Router1必須接收CE-Router發送的所有ICMPv6 Echo Request，並使用ICMPv6 Echo Replies進行回應
2. Echo Reply的來源位址必須等於Echo Request中的目標位址，Echo Reply的目標位址必須等於Echo Request中的來源位址

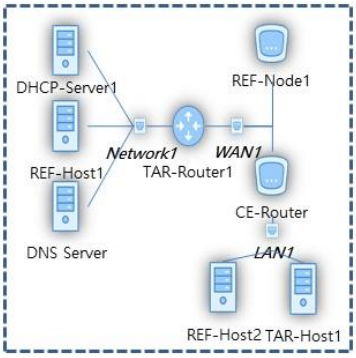
CONFIDENTIAL For Authorized Personnel Only

ICMPv6

- Part E: Router Forwarding (Off-link)

測試9

1. 將TAR-Host1的ICMPv6 Echo Request發送到REF-Host1的global address



成果9

1. CE-Router必須接收從TAR-Host1發送的ICMPv6 Echo Request，並透過過將其發送到WAN接口將ICMP Echo Request轉發給TAR-Router1，且不得更改Echo Request的來源和目標位址
2. TAR-Router1將Echo Reply從REF-Host1轉發到CE-Router
3. CE-Router必須將ICMPv6 Echo Reply轉發給TAR-Host1
4. 不得更改Echo Reply的來源和目標位址。

CONFIDENTIAL For Authorized Personnel Only

IPv6 Forwarding before Address Acquisition

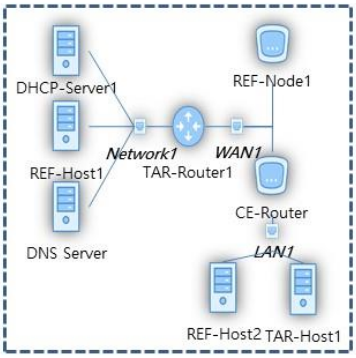
- Part A: LAN to WAN

測試1

1. 透過SLAAC或DHCP在TAR-Host1上配置global address
2. TAR-Host1連續向REF-Host1發送ICMPv6 Echo Request
3. 重啟CE-Router

成果1

1. 在CE-Router獲取位址和prefix之前，CE-Router不得將ICMPv6 Echo Request轉發到TAR-Router1



CONFIDENTIAL For Authorized Personnel Only

IPv6 Forwarding before Address Acquisition

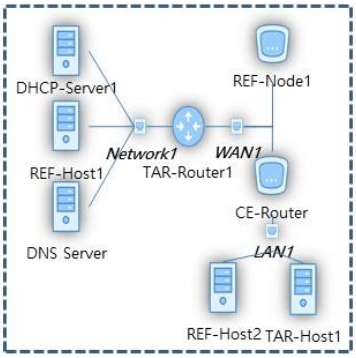
- Part B: WAN to LAN

測試2

1. 通過SLAAC或DHCP在TAR-Host1上配置global address
2. REF-Host1連續向TAR-Host1發送ICMPv6 Echo Request
3. 重啟CE-Router

成果2

1. 在CE-Router獲取位址和prefix之前，CE-Router不得將ICMPv6 Echo Request轉發到TAR-Router1



CONFIDENTIAL For Authorized Personnel Only

No Default Route

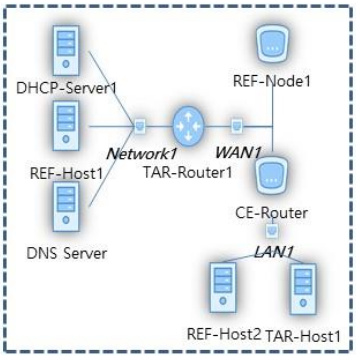
- Part A: No Default Route

測試1

1. 配置TAR-Router1發送Router Lifetime為0的Router Advertisement

成果1

1. CE-Router不得傳輸Router Lifetime大於零的Router Advertisement



CONFIDENTIAL For Authorized Personnel Only

No Default Route

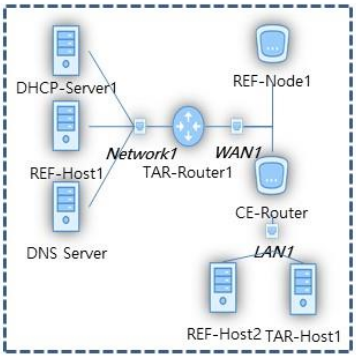
- Part A: No Default Route

測試2

1. REF-Host1向CE-Router發送ICMPv6 Echo Request

成果2

1. CE-Router不得向REF-Host1發送ICMPv6 Echo Reply



CONFIDENTIAL For Authorized Personnel Only

No Default Route

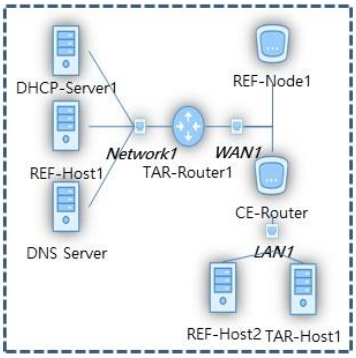
- Part A: No Default Route

測試3

1. TAR-Router1將ICMPv6 Echo Request發送到TAR-Host1

成果3

1. TAR-Host1不得向TAR-Router1發送ICMPv6 Echo Reply



CONFIDENTIAL For Authorized Personnel Only

No Default Route

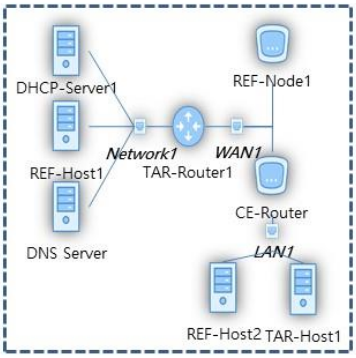
- Part B: Loses Default Route

測試4

1. 配置TAR-Router1傳輸Router Lifetime為600的Router Advertisement

成果4

1. CE-Router必須傳輸Router Lifetime大於零的Router Advertisement



CONFIDENTIAL For Authorized Personnel Only

No Default Route

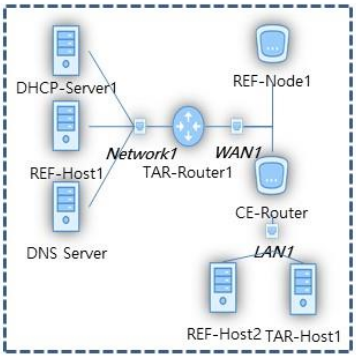
- Part B: Loses Default Route

測試5

1. 1REF-Host1將ICMPv6 Echo Request發送到TAR-Host1

成果5

1. AR-Host1必須向REF-Host1發送ICMPv6 Echo Replies



CONFIDENTIAL For Authorized Personnel Only

No Default Route

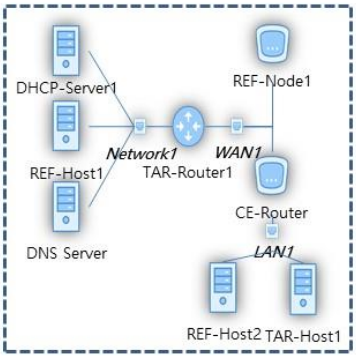
- Part B: Loses Default Route

測試6

1. 配置TAR-Router1傳輸Router Lifetime為0的Router Advertisement

成果6

1. CE-Router必須立即使用發送Router Lifetime為零的Router Advertisement



CONFIDENTIAL For Authorized Personnel Only

No Default Route

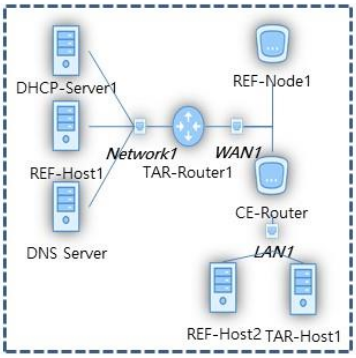
- Part B: Loses Default Route

測試7

1. REF-Host1向CE路由器發送ICMPv6 Echo Request

成果7

1. CE-Router不得向REF-Host1發送ICMPv6 Echo Reply



CONFIDENTIAL For Authorized Personnel Only

No Default Route

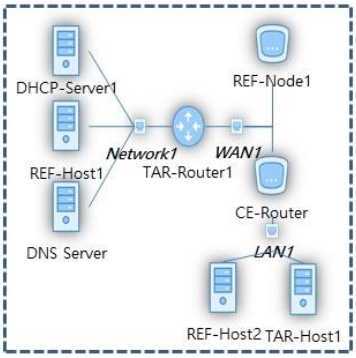
- Part B: Loses Default Route

測試8

1. TAR-Router1將ICMPv6 Echo Request發送到TAR-Host1

成果8

1. TAR-Host1不得向TAR-Router1發送ICMPv6 Echo Reply

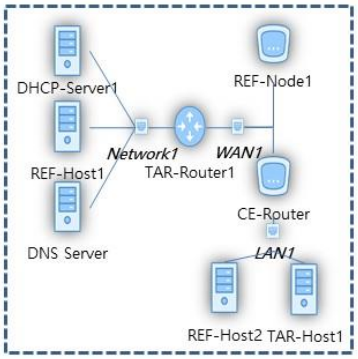


CONFIDENTIAL For Authorized Personnel Only

Forwarding Loops

測試1

1. 配置DHCP-Server1並發送大於CE-Router可以發送的prefix
2. 配置CE-Router使DHCPv6-PD能啟用



成果1

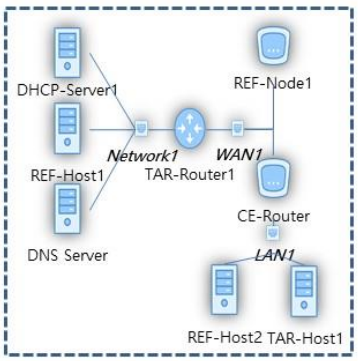
1. CE-Router發送有效的DHCPv6 Request message
2. DHCP-Server1向CE-Router發送有效的DHCPv6 Advertise message
3. CE-Router發送有效的DHCPv6 Request message
4. DHCP-Server向CE-Router發送有效的DHCPv6 Reply message

CONFIDENTIAL For Authorized Personnel Only

Forwarding Loops

測試2

1. TAR-Host1將ICMPv6 Echo Request發送到未分配給CE-Router上LAN接口的位址



成果2

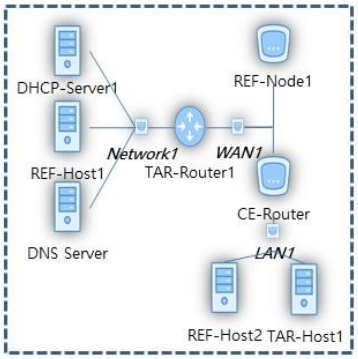
1. CE-Router不應向TAR-Router1發送任何ICMPv6 Echo Request
2. CE-Router應該向TAR-Host1發送ICMPv6 Destination Unreachable message

CONFIDENTIAL For Authorized Personnel Only

Forwarding Loops

測試3

1. TAR-Router1將ICMPv6 Echo Request發送到未分配給CE-Router上LAN接口的位址



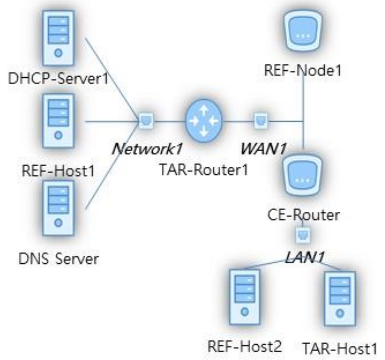
成果3

1. CE-Router不應向LAN1發送任何ICMPv6 Echo Request
2. CE-Router應該向TAR-Router1發送ICMPv6 Destination Unreachable message

CONFIDENTIAL
For Authorized Personnel Only



Unique Local Address



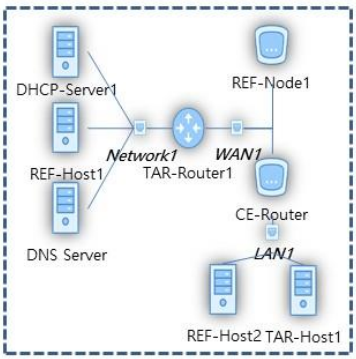
CONFIDENTIAL For Authorized Personnel Only

ULA Prefix Generation

- Part A: Prefix Generation

測試1

1. 配置CE-Router生成ULA prefix



成果1

1. CE-Router必須使用帶有有效ULA prefix的Prefix Information Option發送Router Advertisement
2. Router Advertisement必須包含被advertised的prefix的Router Information Option

CONFIDENTIAL For Authorized Personnel Only

ULA Prefix Generation

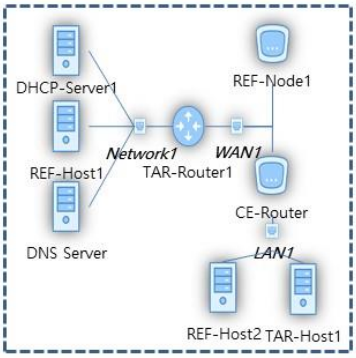
- Part A: Prefix Generation

測試2

1. 為LAN1上的所有設備留出時間，以便在其ULA address上執行Duplicate Address Detection
2. REF-Host2將ICMPv6 Echo Request發送到TAR-Host1的ULA address

成果2

1. R-Host1必須接收從REF-Host2發送的所有ICMPv6 Echo Request，並使用ICMPv6 Echo Replies進行回應



CONFIDENTIAL For Authorized Personnel Only

ULA Prefix Generation

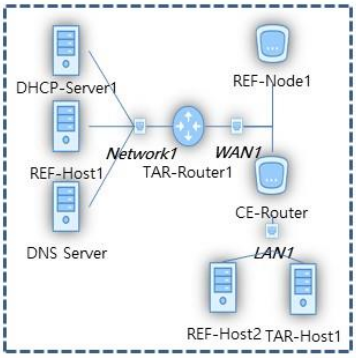
- Part B: Reboot

測試3

1. 配置CE-Router生成ULA prefix

成果3

1. CE-Router必須使用帶有有效ULA prefix的Prefix Information Option發送Router Advertisement



CONFIDENTIAL For Authorized Personnel Only

ULA Prefix Generation

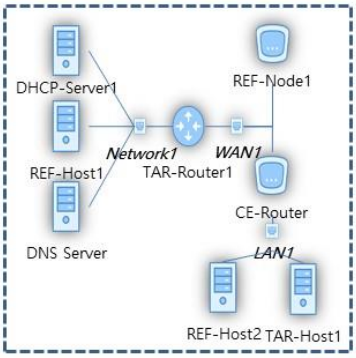
- Part B: Reboot

測試4

1. 為LAN1上的所有設備留出時間，以便在其ULA address上執行Duplicate Address Detection
2. REF-Host2將ICMPv6 Echo Request發送到TAR-Host1的ULA address

成果4

1. AR-Host1必須接收從REF-Host2發送的所有ICMPv6 Echo Request，並使用ICMPv6 Echo Replies進行回應



CONFIDENTIAL For Authorized Personnel Only

ULA Prefix Generation

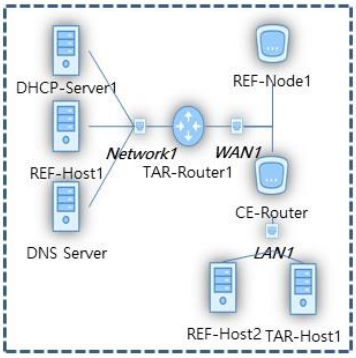
- Part B: Reboot

測試5

1. 重啟CE-Router

成果5

1. CE-Router必須發送和Part B測試1步驟2中被advertised 的相同prefix的Router Advertisements



CONFIDENTIAL For Authorized Personnel Only

ULA Prefix Generation

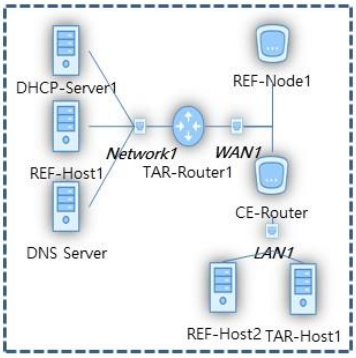
- Part B: Reboot

測試6

1. 為LAN1上的所有設備留時間，以便在其ULA address上執行Duplicate Address Detection
2. REF-Host2將ICMPv6 Echo Request發送到TAR-Host1的ULA address

成果6

1. TAR-Host1必須接收從REF-Host2發送的所有ICMPv6 Echo Request，並使用ICMPv6 Echo Replies進行回應



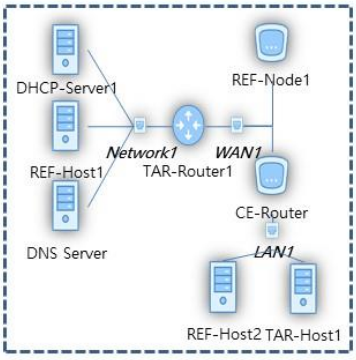
CONFIDENTIAL For Authorized Personnel Only

ULA Prefix Generation

- Part C: User Configuration

測試7

1. 使用有效的ULA address進行advertise來配置CE-Router



成果7

1. CE路由器必須使用在Part C測試1步驟1中配置的ULA prefix的Prefix Information Option發送Router Advertisement
2. Router Advertisement必須包含被advertised的prefix的Router Information Option

CONFIDENTIAL For Authorized Personnel Only

ULA Prefix Generation

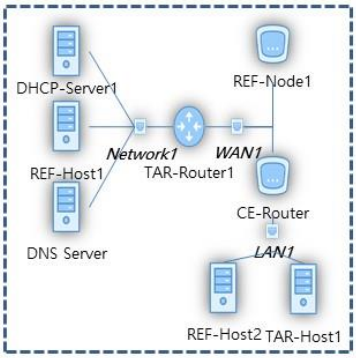
- Part C: User Configuration

測試8

1. 為LAN1上的所有設備留時間，以便在其ULA address上執行Duplicate Address Detection
2. REF-Host2將ICMPv6 Echo Request發送到TAR-Host1的ULA address

成果8

1. TAR-Host1必須接收從REF-Host2發送的所有ICMPv6 Echo Request，並使用ICMPv6 Echo Replies進行回應



CONFIDENTIAL For Authorized Personnel Only

ULA Prefix Generation

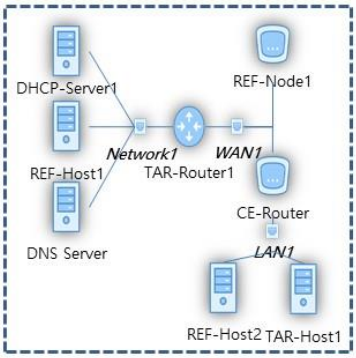
- Part D: Only Advertise Unique Local Address

測試9

1. 配置CE-Router後只發布Router Advertisements中的Unique Local Prefix

成果9

1. CE-Router必須在LAN1上傳輸router lifetime為零的Router Advertisements



CONFIDENTIAL For Authorized Personnel Only

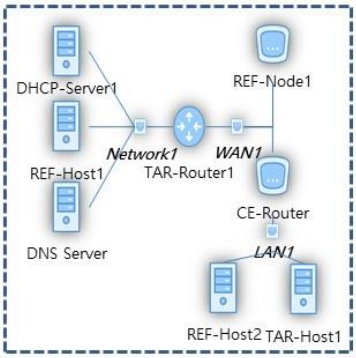
ULA Site Border

測試1

1. 配置CE-Router生成ULA prefix

成果1

1. CE-Router必須使用帶有有效ULA prefix的Prefix Information Option發送Router Advertisement



CONFIDENTIAL For Authorized Personnel Only

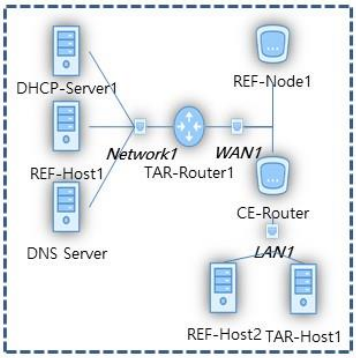
ULA Site Border

測試2

1. 為LAN1上的所有設備留時間，以便在其ULA address上執行重Duplicate Address Detection
2. TAR-Host1使用ULA來源位址向REF-Host1發送ICMPv6 Echo Request

成果2

1. AR-Host1使用ULA作為來源位址向REF-Host1的global address發送ICMPv6 Echo Request
2. CE-Router不得將Echo Request轉發給WAN1



CONFIDENTIAL For Authorized Personnel Only


Mobile
broadband
networklab
Q & A

附件三、寬頻分享器製造商訪談摘要

寬頻分享器製造商訪談摘要

1

廠商訪談會議資料

- 華碩廠商訪談
  - 時間：108.05.27
  - 地點：竹北市光明六路東一段245號13樓ASUS網通部門
  - 與會人員：
    - TWNIC：蔡更達、許淑芳
    - 中央大學：周立德、邱楷程、涂軒豪
    - 華碩廠商：邱青泉、沈長敦、吳政哲、黃宗仁、周家浩
- D-Link廠商訪談
  - 時間：108.05.31
  - 地點：台北市內湖區新湖三路289號D-Link營運總部
  - 與會人員：
    - TWNIC：顧靜恆、蔡更達、許淑芳
    - 中央大學：周立德、吳嘉偉、賴文彬
    - D-Link廠商：劉庭瑋、林聖傑

2 Mobile Broadband Networklab, NCU

CONFIDENTIAL For Authorized Personnel Only

廠商訪談簽到記錄

IPv6 寬頻分享器互通測試項目研究及 IASP 實際測試平台建置

108/05/27 訪談名單

單位	姓名
華碩	平晉泉
華碩	水春記
TWNIC	蔡更達
TWNIC	許淑芳
中央大學	周立德
中央大學	
中央大學	邱楷翔
中央大學	陳輝豪
華碩	吳政穆
華碩	黃宗仁
華碩	周承岱

IPv6 寬頻分享器互通測試項目研究及 IASP 實測平台建置

108/05/31 訪談名單

單位	姓名
友訊	劉庭瑋
友訊	林俊傑
NCC	
NCC	
NCC	
TWNIC	顧靜恒
TWNIC	蔡更達
TWNIC	許淑芳
中央大學	周立德
中央大學	吳嘉隆
中央大學	賴文彬
中央大學	

3

華碩訪談摘要

- Q1：RFC所摘要的開發規範是否包含中華與Cable業者服務模式涵蓋範圍?
  - 中央：RFC所制定的規範是通用的標準並未特別區分Cable或Non-Cable，例如RFC 7084即涵蓋中華與Cable業者服務模式
- Q2 ：RFC是否建議IPv4與IPv6使用同一個PPP session? 建議是使用同一個還是不同?
  - 中央：RFC並未建議IPv4與IPv6使用同一個PPP session，不過RFC7084有提到，如WAN Interface支援PPP encapsulation，則在Dual-Stack環境中，IPCP和IPV6CP必須視為獨立的Network Control Protocols
- Q3：若同時有IPv6與IPv4，用戶的流量會以什麼協定為主？
  - 中央：DS的情況下預設IPv6優先
- Q4：若分享器開發商預設使用IPv6的PPP，而ISP卻沒有提供IPv6的服務，是否會影響到用戶IPv4的上網?
  - 中央：若分享器開發商預設使用IPv6的PPP，而ISP卻沒有提供IPv6的服務，則IPv6連線無法建立；若分享器使用DualStack撥接，預設的情況應不影響到用戶IPv4上網
- Q5：華碩目前新出的分享器是否都會支援IPv6?是否有放OpenVPN功能?
  - 華碩：考量研發資源成本，以新上市或高階型號之產品為優先
- Q6：部分RFC有更新版本，有新版的RFC建議應以更新版本為主
  - 中央：RFC有更新部分後續會再註記

CONFIDENTIAL
For Authorized Personnel Only

D-Link廠商訪談摘要-開發規範

- LAN端位址分配模式
  - 中央：中華用/64為主，對LAN的 HOST 一定是64，分享器可搭配(SLAAC、RDNSS、DHCPv6方式配置
  - D-Link：家用路由器使用者通常不懂得怎麼做設定，D-Link支援SLAAC、RDNSS、DHCPv6三種模式，但是 Android 不支援 DHCPv6不管M/O bit怎麼設都會來問RDNSS，所以建議RDNSS是可與其他模式共用
- 開發規範安全性需求
  - 中央：安全性在7084列為"選項"參考其他RFC，如RFC 6092
  - D-Link：安全在D-Link的產品上是有做的，消費者都花錢了會希望有安全機制可以開，IPv6從有NAT到沒有NAT的世代轉換，安全性確實重要
  - D-Link：高階機種指的是DIR 850/ DIR 1300 以上，通常是4000台幣以上
- 6rd & DS-Lite
  - 中央：RFC內規範IPv6 CE Router必須支援6rd以及DS-Lite轉移機制，但是台灣應該不太需要
  - D-Link：這兩項應該在歐洲才有，NCC也沒有建立這兩項的環境

CONFIDENTIAL For Authorized Personnel Only

D-Link廠商訪談摘要-開發規範 (續)

- PCP (Port Control Protocol)
  - D-Link：PCP在台灣似乎沒有需要。實作方面，非常少用戶需要，到現在也沒有用戶抱怨這件事，所以不是MUST
  - 中央：這項在RFC標示為SHOULD
- WAN介面Reconfigure Accept
  - D-Link：Reconfigure Accept是指DHCPv6斷線重連取得不同的Prefix然後要求client或CPE重新取得刷新Prefix的資料，我們在新加坡機器有報BUG過，這個很重要，因為中華電信每兩天DHCP會重撥，對我們來說這個是必測項目
  - 中央：斷線重播的部分建議納入必須測試項目

CONFIDENTIAL For Authorized Personnel Only

D-Link廠商訪談摘要-測試規範

- MTU問題
  - D-Link：IPv6的MTU是跟著IPv4，因為PPP的設定是在IPv4(以自家產品來說)，但是IPv4的MTU修改後IPv6也需要跟著修改(在1280~1500之間)，中華電信是統一是1492
  - 中央：CPE的LAN端的MTU應該要設為1492給下面的Host，至少在上行時加上PPPoE的8剛好是1500，就不會做packet too big的動作
- IPv6 位址配置模式
  - D-Link：目前我們只發現到客戶的設備只有android會有這個問題(android不支援DHCPv6)，建議預設以模式一二一起(SLAAC+RDNSS)
  - 中央：建議CPE要提供三個模式(SLAAC、RDNSS、DHCPv6)讓客戶可以彈性選擇
- IPv6安全問題
  - 中央：安全本身是選項，但有些基本功能可列為必要。有些是列為transparent(封包可以透通)，像是packet too big和destination unreachable，這部分必須把provider的訊息能夠收回來，這部分transparent模式在7084內是列為選項，但實作上應該要考慮
  - D-Link：有些路由器要求更安全是連看都看不到，因為IPv4絕大多數廠商是做連看都看不到，不會回任何WAN端的ICMPv4，避免駭客掃描到這邊有一台電腦，但是IPv6位址滿多的，等駭客掃到可能已經更換IP了

CONFIDENTIAL For Authorized Personnel Only

D-Link廠商訪談摘要-測試規範 (續)

- Unique Local Address Test (ULA)問題
  - 中央：ULA在RFC上建議的，但台灣採用ULA的案例似乎不多
  - D-Link：ULA部分我們的產品預設是關閉的，因為有些client會以為ULA可以用，但是ULA不能到internet，雖然我們都支援但預設是關閉的
- IPv6互連性測項
  - D-Link：建議WAN3 LAN6,8列為必要的測試項目。8是因為有些國外的網路只給DNSv4，導致android用戶使用DNSv6查詢時花費數秒才回到DNSv4
- IPv6 pass through
  - TWNIC：分享器有想要支援v6 pass through 功能嗎，因為對學校很有用。
  - D-Link：目前沒收到這個需求，原因是因為家用沒有這個需求
- 用戶測項
  - D-Link：報告很豐富，建議做成檢查表
  - D-Link：製造商不希望看到以RFC當作分類的規格，希望以WAN/LAN分開，以security分開，整理時建議區隔比較好檢查

CONFIDENTIAL For Authorized Personnel Only

D-Link廠商訪談摘要-測試規範 (續)

- 下表為固網寬頻CE選測項目建議，建議選測項目可以IPv6 Ready Logo互聯性測式項目為主
- 粗體底線記號的項目為D-Link廠商建議列為重點測試項目

WAN Side Test:
1. DUPLICATE ADDRESS DETECTION
2. ROUTER DISCOVERY
3. ADDRESS LIFETIME
4. DHCPV6
5. DHCPV6 PREFIX DELEGATION
6. UNNUMBERED WAN
7. DHCPV6 SOL_MAX_RT
8. L FLAG PROCESSING

LAN Side Test:
1. DUPLICATE ADDRESS DETECTION AND NEIGHBOR DISCOVERY
2. ASSIGNING PREFIXES TO LAN INTERFACES
3. ROUTER ADVERTISEMENT
4. STATELESS DHCP SERVER
5. DHCP SERVER
6. PREFIX CHANGE
7. LINK MTU
8. DNS INFORMATION IN ROUTER ADVERTISEMENT
9. INGRESS FILTERING

General Requirement Test:
1. ICMPV6
2. IPV6 FORWARDING BEFORE ADDRESS ACQUISITION
3. NO DEFAULT ROUTE
4. FORWARDING LOOPS

Unique Local Address Test:
1. ULA PREFIX GENERATION
2. ULA SITE BORDER

CONFIDENTIAL
For Authorized Personnel Only

附件四、IPv6 寬頻分享器實機測試

D-Link DIR-853

分享器測試成果

1

測試設備與環境

分享器產品設備資訊	
產品型號	DIR-853
產品名稱	Wireless AC1300 MU-MIMO雙頻Gigabit無線路由器
硬體版本	A2
韌體版本	1.02B02
製造年份	2018



測試環境資訊	
測試環境	1.HiNet光世代 PPPoE
	2.Cable IPoE
測試終端	Windows 10
終端瀏覽器	Chrome
測試時間	2019-08~2019-10



Mobile Broadband Networklab, NCU

測試紀錄摘要

HiNet 光世代PPPoE測試		
	測試項目	DIR-853
1	分享器PPPoE撥接是否正常?	O
2	分享器IPv6、IPv6 PD、DNSv6取得是否正常?	O
3	用戶IPv6、DNSv6取得是否正常?	O
4	用戶至HiNet路由是否正常?	O
5	用戶IPv6上網是否正常?	O
6	用戶熱門網頁開啟是否正常?	O
7	用戶上網速率是否正常?	O
8	分享器重撥，用戶IPv6更新是否正常?	O
9	用戶使用IPv6之MTU是否正常?	1500
10	用戶連接Wi-Fi上網IPv6、DNSv6是否正常?	O
11	用戶連接Wi-Fi IPv6上網是否正常?	O
12	IPv6 PPPoE（或是PPPoEv6)是否隨著IPv4 PPPoE啟用而自動啟用?	O
13	IPv6 PPPoE（或是PPPoEv6)連線之PPPoE Session是『Share with IPv4』或是『Create a new Session』?	可設定兩種模式『New Session』WAN端為斷線
14	IPv6寬頻分享器IPv6 ACL功能是否正常?	O

Cable IPoE測試		
	測試項目	DIR-853
1	分享器連接Cable Modem是否正常?	O
2	分享器IPv6、IPv6 PD、DNSv6取得是否正常?	O
3	用戶IPv6、DNSv6取得是否正常?	O
4	用戶至Cable業者路由是否正常?	O
5	用戶IPv6上網是否正常?	O
6	用戶熱門網頁開啟是否正常?	O
7	用戶上網速率是否正常?	O
8	分享器重撥Cable Modem，用戶IPv6更新是否正常?	O
9	用戶使用IPv6之MTU是否正常?	1500
10	用戶連接Wi-Fi上網IPv6、DNSv6是否正常?	O
11	用戶連接Wi-Fi IPv6上網是否正常?	O
12	IPv6連線功能是否隨著IPv4啟用而自動啟用?	O
13	IPv6寬頻分享器IPv6 ACL功能是否正常?	O

測試紀錄摘要說明

- ✓ HiNet PPPoE環境 (Pass測項:12/14)
  - 測項9:RA ICMP option MTU1500，PPPoE環境可能導致用戶端packet too big須重傳
  - 測項13: 可選用兩種模式，但設定『Create a new session』則WAN端為斷線
- ✓ Cable IPoE環境(Pass測項:13/13)
  - 測試結果符合預期

分享器測試紀錄
HiNet 光世代 PPPoE環境



5

D-Link DIR-853 PPPoE 測項1

✓ 確認分享器PPPoE撥接正常

網際網路

IPv4 / IPv6

網路線連接狀態:	已連線
網路連線類型:	動態 PPPoE
網際網路狀態:	已連線
連線時間:	0 天 0 時 15 分 12 秒

MAC 位址:	0C:B6:D2:68:86:13
IP 位址:	118.168.145.62
子網域遮罩:	255.255.255.255
預設閘道器:	168.95.98.254
主要 DNS 伺服器:	168.95.192.1
輔助 DNS 伺服器:	168.95.1.1

前往設定頁面

Mobile Broadband Networklab, NCU

D-Link DIR-853 PPPoE 測項2

✓ 確認分享器IPv6、IPv6 PD、DNSv6取得正常

IPv6 網路　　LAN端位址資訊

Link-Local 位址: FE80::EB6:D2FF:FE68:8610

路由器 IPv6 位址: 2001:B011:6CC0:1C31:EB6:D2FF:FE68:8610

DHCP-PD: 啟用

配置的網段: 2001:B011:6CC0:1C31::/64

網際網路　　WAN端位址資訊

網路連線類型: PPPoE

網際網路狀態: CONNECTED

連線時間: 0 天 0 時 18 分 32 秒

IPv4 / **IPv6**

廣域網路 IPv6 位址: 2001:B011:6CC0:486C:F194:3869:CF81:31E9/64

預設閘道器: FE80::D2F0:DBFF:FE53:800

主要 DNS 伺服器: 2001:B000:168::2

輔助 DNS 伺服器: 2001:B000:168::1

前往設定頁面

D-Link DIR-853 PPPoE 測項3

✓ 確認用戶IPv6、DNSv6取得正常

```
乙太網路卡 乙太網路:

   連線特定 DNS 尾碼 . . . . . . . . :
   描述 . . . . . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   實體位址 . . . . . . . . . . . . . : 84-A9-3E-04-A8-BB
   DHCP 已啟用 . . . . . . . . . . . : 是
   自動設定啟用 . . . . . . . . . . . : 是
   IPv6 位址. . . . . . . . . . . . . : 2001:b011:6cc0:1c31:4d13:49bf:8df1:4fc8(偏好選項)
   臨時 IPv6 位址. . . . . . . . . . . : 2001:b011:6cc0:1c31:28e0:3169:c6d5:9319(偏好選項)
   連結-本機 IPv6 位址 . . . . . . . . : fe80::4d13:49bf:8df1:4fc8%14(偏好選項)
   IPv4 位址 . . . . . . . . . . . . . : 192.168.10.101(偏好選項)
   子網路遮罩 . . . . . . . . . . . . : 255.255.255.0
   租用取得 . . . . . . . . . . . . . : 2019年7月20日 下午 09:30:52
   租用到期 . . . . . . . . . . . . . : 2019年7月27日 下午 09:30:51
   預設閘道 . . . . . . . . . . . . . : fe80::eb6:d2ff:fe68:8610%14
                                        192.168.10.1
   DHCP 伺服器 . . . . . . . . . . . : 192.168.10.1
   DHCPv6 IAID . . . . . . . . . . . : 226797886
   DHCPv6 用戶端 DUID. . . . . . . . : 00-01-00-01-24-35-E6-77-84-A9-3E-04-A8-BB
   DNS 伺服器 . . . . . . . . . . . . : 192.168.10.1
                                        2001:b000:168::2
                                        2001:b000:168::1
   NetBIOS over Tcpip . . . . . . . . : 啟用
```

Mobile Broadband Networklab, NCU

D-Link DIR-853 PPPoE 測項4

✓ 確認用戶至HiNet路由正常

```
C:\Users\wenpi>ping dns.hinet.net

Ping dns.hinet.net [2001:b000:168::2] (使用 32 位元組的資料):
回覆自 2001:b000:168::2: 時間=12ms
回覆自 2001:b000:168::2: 時間=12ms
回覆自 2001:b000:168::2: 時間=12ms
回覆自 2001:b000:168::2: 時間=11ms

2001:b000:168::2 的 Ping 統計資料:
    封包: 已傳送 = 4，已收到 = 4，已遺失 = 0 (0% 遺失)，
大約的來回時間 (毫秒):
    最小值 = 11ms，最大值 = 12ms，平均 = 11ms

C:\Users\wenpi>tracert dns.hinet.net

在上限 30 個躍點上
追蹤 dns.hinet.net [2001:b000:168::2] 的路由:

  1    <1 ms    <1 ms    <1 ms  2001-b011-6cc0-1c31-0eb6-d2ff-fe68-8610.dynamic-ip6.hinet.net [2001:b011:6cc0:1c31:eb6:d2ff
:fe68:8610]
  2    12 ms    11 ms    10 ms  2001:b010:ffff::1
  3     9 ms    11 ms    11 ms  2001-b000-0089-0005-0022-2222-0002-0002.hinet-ip6.hinet.net [2001:b000:89:5:22:2222:2:2]
  4    13 ms     *        *     2001-b000-0080-0003-0080-0089-0022-000a.hinet-ip6.hinet.net [2001:b000:80:3:80:89:22:a]
  5    12 ms    15 ms    16 ms  2001-b000-0080-0004-3022-3012-0001-000b.hinet-ip6.hinet.net [2001:b000:80:4:3022:3012:1:b]

  6    14 ms    16 ms    16 ms  2001-b000-0080-0004-3022-3012-0001-000b.hinet-ip6.hinet.net [2001:b000:80:4:3022:3012:1:b]

  7    11 ms    13 ms    11 ms  2001-b000-0080-0004-3012-3312-0012-000b.hinet-ip6.hinet.net [2001:b000:80:4:3012:3312:12:b]

  8     *        *        *     要求等候逾時。
  9    10 ms    10 ms    12 ms  dns.hinet.net [2001:b000:168::2]

追蹤完成。
```

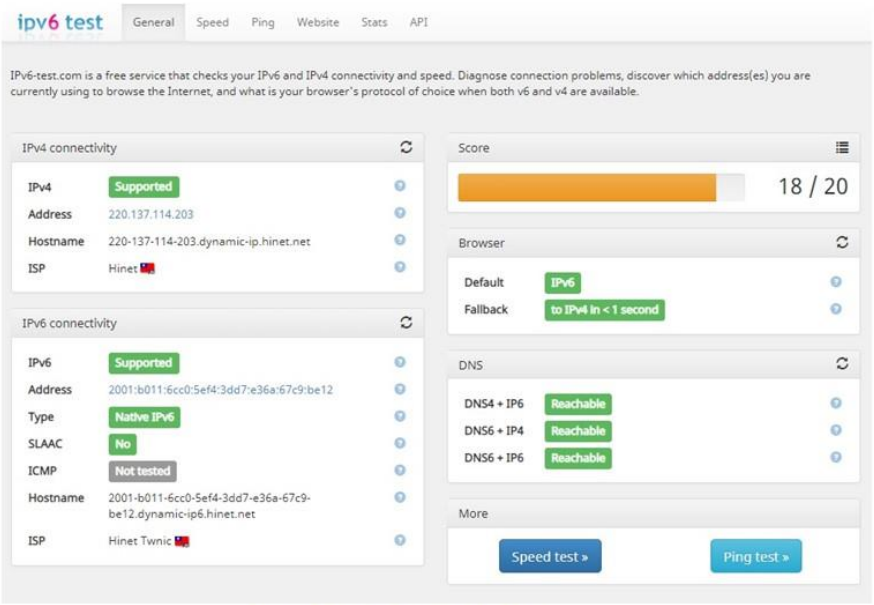

D-Link DIR-853 PPPoE 測項5

✓ 確認用戶IPv6上網正常(test-ipv6.com)



D-Link DIR-853 PPPoE 測項5(續)

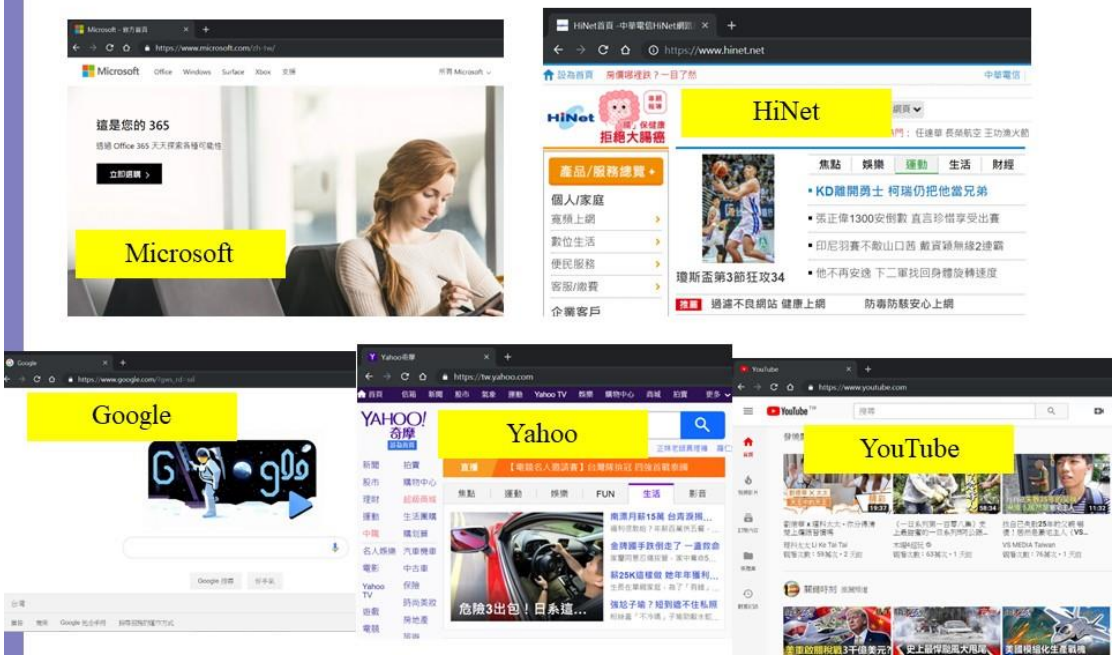
✓ 確認用戶IPv6上網正常(ipv6-test.com)



Mobile Broadband Networklab, NCU

D-Link DIR-853 PPPoE 測項6

✓ 確認用戶熱門網頁開啟正常



D-Link DIR-853 PPPoE 測項7

✓ 確認用戶上網速率正常



D-Link DIR-853 PPPoE 測項8

✓ 確認分享器重撥，用戶IPv6更新正常

測試你的 IPv6 連線。 分享器重撥之前



測試你的 IPv6 連線。 分享器重撥之後



D-Link DIR-853 PPPoE 測項9

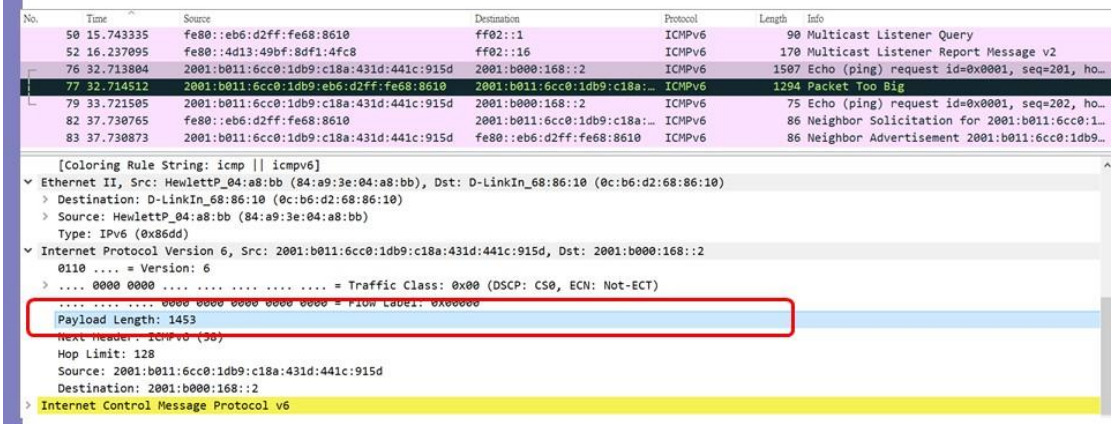
- ✓ 確認用戶使用IPv6之MTU不正常
  - 乙太網路介面之MTU為1500非1492

```
C:\Users\wenpi>netsh interface ipv6 show subinterface

   MTU  MediaSenseState   接收的位元組 傳送的位元組 介面
------  ---------------  ---------  ---------  -------------
4294967295                1          0     361800  Loopback Pseudo-Interface 1
  1500                2   59528194     942607  Wi-Fi
  1500                1   94686997   12718672  乙太網路
  1500                5          0       2540  區域連線* 1
  1500                5          0       4612  區域連線* 2
  1500                1          0     244380  Npcap Loopback Adapter
```


D-Link DIR-853 PPPoE 測項9 (續)

- ✓ 確認用戶使用IPv6之MTU不正常
  - 傳送Payload大小為1453之IPv6封包即收到Packet Too Big
  - 封包大小為IPv6 header 40 bytes plus payload size 1453



D-Link DIR-853 PPPoE 測項9 (續)

- ✓ 確認用戶使用IPv6之MTU不正常
  - 乙太網路介面之MTU為1500非1492

分享器的RA封包

```
Internet Protocol Version 6, Src: fe80::eb6:d2ff:fe68:8610, Dst: ff02::1
  0110 .... = Version: 6
> .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
  .... .... .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
  Payload Length: 128
  Next Header: ICMPv6 (58)
  Hop Limit: 255
  Source: fe80::eb6:d2ff:fe68:8610
  Destination: ff02::1
  [Source SA MAC: D-LinkIn_68:86:10 (0c:b6:d2:68:86:10)]
Internet Control Message Protocol v6
  Type: Router Advertisement (134)
  Code: 0
  Checksum: 0x5293 [correct]
  [Checksum Status: Good]
  Cur hop limit: 64
> Flags: 0x40, Other configuration, Prf (Default Router Preference): Medium
  Router lifetime (s): 1800
  Reachable time (ms): 0
  Retrans timer (ms): 0
> ICMPv6 Option (Prefix information : 2001:b011:6cc0:1db9::/64)
> ICMPv6 Option (Route Information : High 2001:b011:6cc0:1db9::/64)
> ICMPv6 Option (Recursive DNS Server 2001:b000:168::2 2001:b000:168::1)
> ICMPv6 Option (MTU : 1500)
> ICMPv6 Option (Source link-layer address : 0c:b6:d2:68:86:10)
```

分享器的位址

IPv6 網路

Link-Local 位址:	FE80::EB6:D2FF:FE68:8610
路由器 IPv6 位址:	2001:B011:6CC0:1DB9:EB6:D2FF:FE68:861 0
DHCP-PD:	啟用
配置的網段:	2001:B011:6CC0:1DB9::/64

D-Link DIR-853 PPPoE 測項10

- ✓ 確認用戶連接Wi-Fi上網IPv6、DNSv6正常

```
無線區域網路介面卡 Wi-Fi:

   連線特定 DNS 尾碼 . . . . . . . . :
   描述 . . . . . . . . . . . . . . : Intel(R) Wireless-AC 9461
   實體位址 . . . . . . . . . . . . : 38-BA-F8-FC-E8-6A
   DHCP 已啟用 . . . . . . . . . . . : 是
   自動設定啟用 . . . . . . . . . . . : 是
   IPv6 位址. . . . . . . . . . . . : 2001:b011:6cc0:1c31:852d:59eb:5e77:d3ff(偏好選項)
   臨時 IPv6 位址. . . . . . . . . . : 2001:b011:6cc0:1c31:852e:7afe:bc87:4c3e(偏好選項)
   連結-本機 IPv6 位址 . . . . . . . : fe80::852d:59eb:5e77:d3ff%19(偏好選項)
   IPv4 位址 . . . . . . . . . . . . : 192.168.10.97(偏好選項)
   子網路遮罩 . . . . . . . . . . . : 255.255.255.0
   租用取得 . . . . . . . . . . . . : 2019年7月20日 下午 10:58:29
   租用到期 . . . . . . . . . . . . : 2019年7月27日 下午 10:58:29
   預設閘道 . . . . . . . . . . . . : fe80::eb6:d2ff:fe68:8610%19
                                      192.168.10.1
   DHCP 伺服器 . . . . . . . . . . . : 192.168.10.1
   DHCPv6 IAID . . . . . . . . . . . : 154712824
   DHCPv6 用戶端 DUID. . . . . . . . : 00-01-00-01-24-35-E6-77-84-A9-3E-04-A8-BB
   DNS 伺服器 . . . . . . . . . . . : 2001:b000:168::2
                                      2001:b000:168::1
                                      192.168.10.1
                                      2001:b000:168::2
                                      2001:b000:168::1
   NetBIOS over Tcpip . . . . . . . : 啟用
```

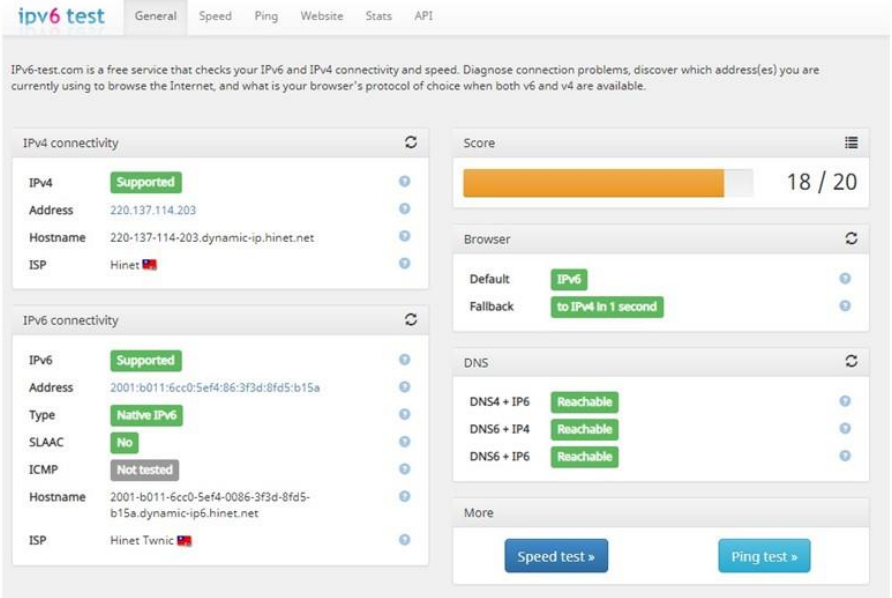
D-Link DIR-853 PPPoE 測項11

✓ 確認用戶連接Wi-Fi IPv6上網正常(test-ipv6.com)



D-Link DIR-853 PPPoE 測項11(續)

✓ 確認用戶連接Wi-Fi IPv6上網正常(ipv6-test.com)



Mobile Broadband Networklab, NCU

D-Link DIR-853 PPPoE 測項12

✓ IPv6 PPPoE (或是PPPoEv6)是否隨著IPv4 PPPoE啟用而自動啟用

- 重設分享器，依照介面指示設定後，IPv4啟用後IPv6即自動啟用

測試你的 IPv6 連線。

IPv6可正常連線



DIR-853 LAN



網際網路 IPv4 WAN



網際網路 IPv6 WAN



D-Link DIR-853 PPPoE 測項13

✓ IPv6 PPPoE (或是PPPoEv6)連線之PPPoE Session是『Share with IPv4』或是『Create a new Session』?

基本設定>>網際網路>>IPv6 VLAN IPv4

將PPPoEv6工作階段設定為與IPv4共享

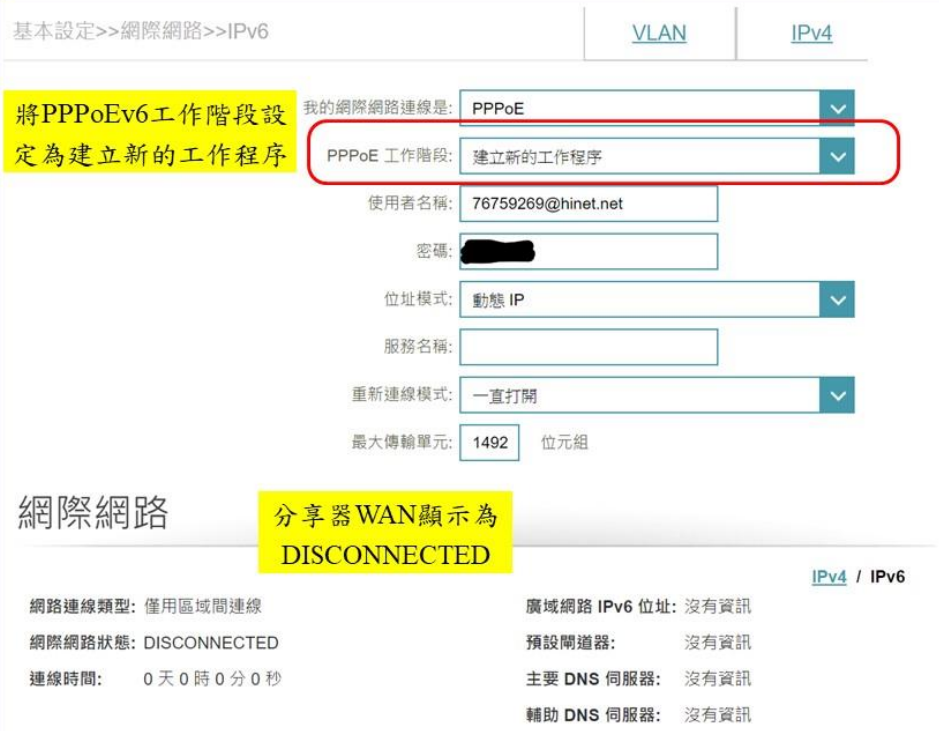


網際網路

分享器WAN顯示為PPPoE連線



D-Link DIR-853 PPPoE 測項13 (續)



D-Link DIR-853 PPPoE 測項14

- ✓ IPv6寬頻分享器IPv6 ACL功能是否正常?
  - □ 測試寬頻分享器 IPv6 ACL功能是否能限制用戶終端IPv6連線



D-Link DIR-853 PPPoE 測項14(續)

✓ 將ACL功能開啟



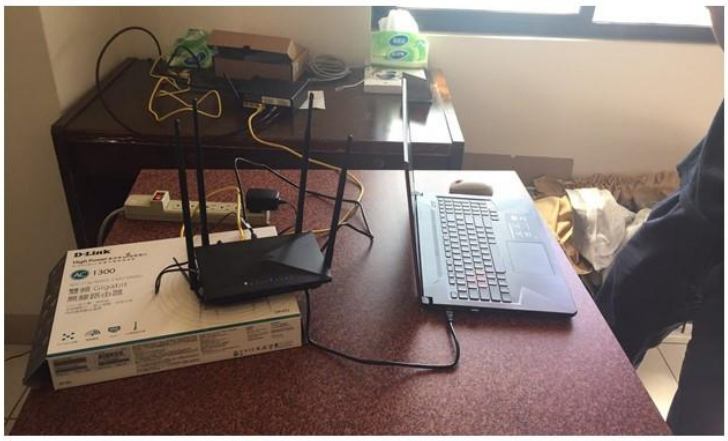
D-Link DIR-853 PPPoE 測項14(續)

✓ 啟用ACL功能後，被設定阻擋的主機無法取得IPv6位址



Mobile Broadband Networklab, NCU

分享器測試紀錄
Cable 寬頻 IPoE環境



27

D-Link DIR-853 CM 測項1

✓ 確認連接cable modem正常

網際網路

網路連線類型: 自動設定 (SLAAC/DHCPv6)
網際網路狀態: CONNECTED
連線時間: 0 天 0 時 2 分 17 秒
釋放

IPv4 / IPv6
廣域網路 IPv6 位址: 2405:9200:1125::C/128
預設閘道器: FE80::201:5CFF:FEA1:1646
主要 DNS 伺服器: 2404::1
輔助 DNS 伺服器: 2001:4860:4860::8888
前往設定頁面

Mobile Broadband Networklab, NCU

D-Link DIR-853 CM 測項2

✓ 確認取得IPv6、IPv6 PD、DNSv6

LAN端位址資訊

IPv6 網路

Link-Local 位址: FE80::EB6:D2FF:FE68:8610

路由器 IPv6 位址: 2405:9200:1110:0:EB6:D2FF:FE68:8610

DHCP-PD: 啟用

配置的網段: 2405:9200:1110::/64

網際網路

WAN端位址資訊

IPv4 / IPv6

網路連線類型: 自動設定 (SLAAC/DHCPv6)

網際網路狀態: CONNECTED

連線時間: 0 天 0 時 2 分 17 秒

釋放

廣域網路 IPv6 位址: 2405:9200:1125::C/128

預設閘道器: FE80::201:5CFF:FEA1:1646

主要 DNS 伺服器: 2404::1

輔助 DNS 伺服器: 2001:4860:4860::8888

前往設定頁面

D-Link DIR-853 CM 測項3

✓ 確認用戶IPv6、DNSv6取得正常

```
乙太網路卡 乙太網路:

   連線特定 DNS 尾碼 . . . . . . . . :
   描述 . . . . . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   實體位址 . . . . . . . . . . . . . : 84-A9-3E-04-A8-BB
   DHCP 已啟用 . . . . . . . . . . . : 是
   自動設定啟用 . . . . . . . . . . . : 是
   IPv6 位址. . . . . . . . . . . . . : 2405:9200:1110:0:4d13:49bf:8df1:4fc8(偏好選項)
   臨時 IPv6 位址. . . . . . . . . . . : 2405:9200:1110:0:55d7:e070:ce53:b80d(偏好選項)
   連結-本機 IPv6 位址 . . . . . . . . : fe80::4d13:49bf:8df1:4fc8%14(偏好選項)
   IPv4 位址 . . . . . . . . . . . . . : 192.168.10.101(偏好選項)
   子網路遮罩 . . . . . . . . . . . . : 255.255.255.0
   租用取得 . . . . . . . . . . . . . : 2019年7月24日 上午 10:27:43
   租用到期 . . . . . . . . . . . . . : 2019年7月31日 上午 10:27:43
   預設閘道 . . . . . . . . . . . . . : fe80::eb6:d2ff:fe68:8610%14
                                        192.168.10.1
   DHCP 伺服器 . . . . . . . . . . . : 192.168.10.1
   DHCPv6 IAID . . . . . . . . . . . : 226797886
   DHCPv6 用戶端 DUID. . . . . . . . : 00-01-00-01-24-35-E6-77-84-A9-3E-04-A8-BB
   DNS 伺服器 . . . . . . . . . . . . : 192.168.10.1
                                        2404::1
                                        2001:4860:4860::8888
                                        2001:b000:168::1
   NetBIOS over Tcpip . . . . . . . . : 啟用
```

D-Link DIR-853 CM 測項4

✓ 確認用戶至google ipv6路由正常

```
C:\Users\wenpi>tracert ipv6.google.com

在上限 30 個躍點上
追蹤 ipv6.l.google.com [2404:6800:4012:1::200e] 的路由:

  1    <1 ms    <1 ms    <1 ms  2405:9200:1110:0:eb6:d2ff:fe68:8610
  2     *        *        *     要求等候逾時。
  3     7 ms     9 ms     9 ms  2405:9200:1:0:172:16:28:169a
  4    12 ms    10 ms    10 ms  2405:9200:1:0:172:16:31:22a
  5    11 ms    11 ms    10 ms  2404:0:10ff:1:7709:13:1596:1212
  6    10 ms     9 ms    10 ms  2404:0:10ff::4:166
  7    12 ms    11 ms    11 ms  2404:0:10ff:1:7709:1:5169:61
  8    12 ms    12 ms    11 ms  2001:4860:0:1014::1
  9    16 ms    12 ms    12 ms  2001:4860:0:1::2e0b
 10    11 ms    11 ms    11 ms  tsa03s06-in-x0e.1e100.net [2404:6800:4012:1::200e]

追蹤完成。

C:\Users\wenpi>ping ipv6.google.com

Ping ipv6.l.google.com [2404:6800:4012:1::200e] (使用 32 位元組的資料):
回覆自 2404:6800:4012:1::200e: 時間=10ms
回覆自 2404:6800:4012:1::200e: 時間=12ms
回覆自 2404:6800:4012:1::200e: 時間=17ms
回覆自 2404:6800:4012:1::200e: 時間=11ms

2404:6800:4012:1::200e 的 Ping 統計資料:
    封包: 已傳送 = 4，已收到 = 4，已遺失 = 0 (0% 遺失)，
大約的來回時間 (毫秒):
    最小值 = 10ms，最大值 = 17ms，平均 = 12ms
```

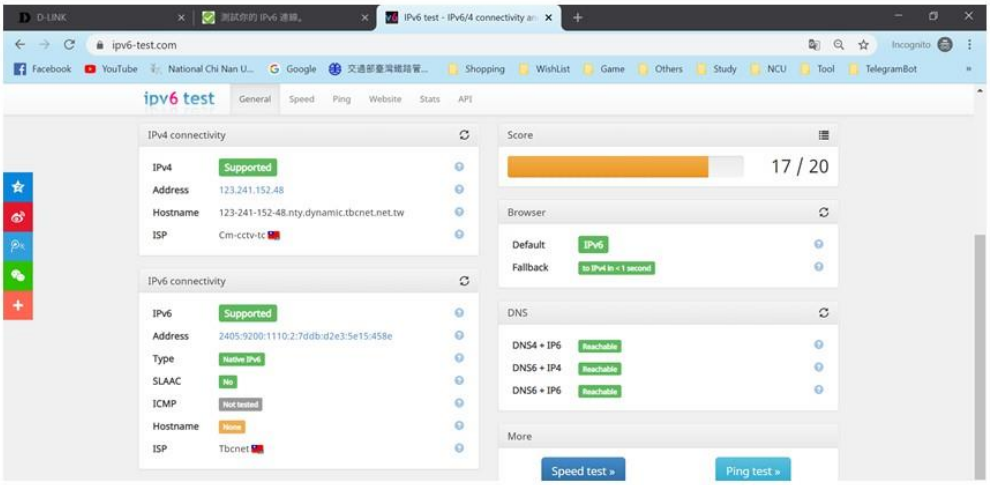

D-Link DIR-853 CM 測項5

✓ 確認用戶IPv6上網正常(test-ipv6.com)



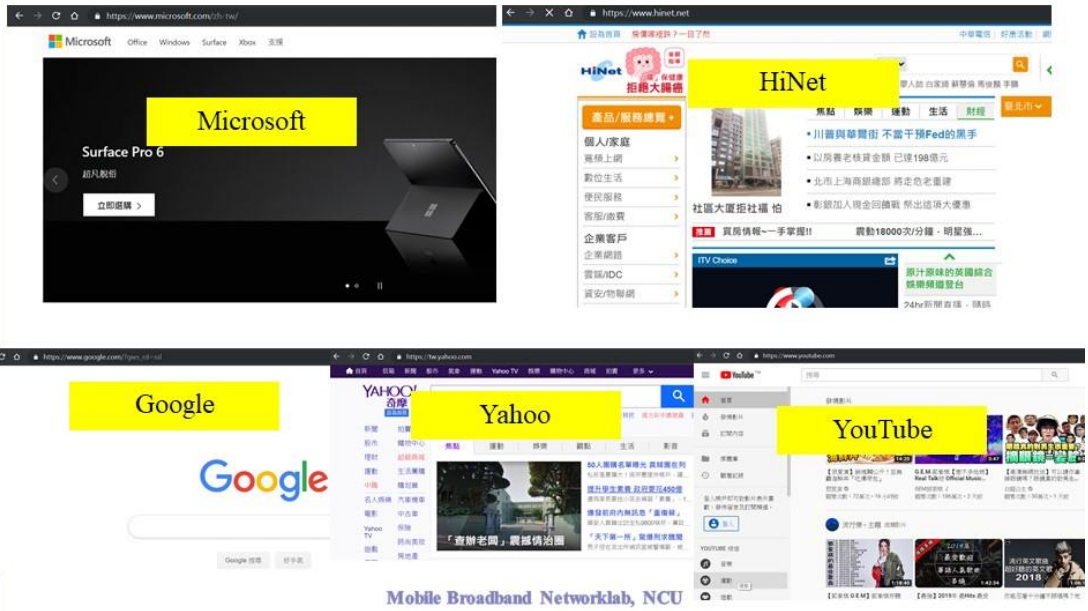
D-Link DIR-853 CM 測項5(續)

✓ 確認用戶IPv6上網正常(ipv6-test.com)



D-Link DIR-853 CM 測項6

✓ 確認用戶熱門網頁開啟正常



D-Link DIR-853 CM 測項7

✓ 確認用戶上網速率正常



D-Link DIR-853 CM 測項8

✓ 確認分享器重新連接cable modem之後，用戶ipv6相同，且連線正常

測試你的 IPv6 連線。

分享器重接CM前



測試你的 IPv6 連線。

分享器重接CM後



D-Link DIR-853 CM 測項9

✓ 確認用戶使用IPv6乙太網路介面之MTU為1500非1492

```
C:\Users\wenpi>netsh interface ipv6 show subinterface

   MTU  MediaSenseState   接收的位元組 傳送的位元組 介面
------  ---------------  --------- --------- -------------
4294967295                1         0       1292  Loopback Pseudo-Interface 1
  1500                2  43281287   1548848  Wi-Fi
  1500                1 295388003  75622631  乙太網路
  1500                5         0       152  區域連線* 1
  1500                5         0       152  區域連線* 2
  1500                1         0     88188  Npcap Loopback Adapter
```


D-Link DIR-853 CM 測項10

✓ 確認用戶連接Wi-Fi上網IPv6、DNSv6正常

```
無線區域網路介面卡 Wi-Fi:

   連線特定 DNS 尾碼 . . . . . . . . :
   描述 . . . . . . . . . . . . . . : Intel(R) Wireless-AC 9461
   實體位址 . . . . . . . . . . . . : 38-BA-F8-FC-E8-6A
   DHCP 已啟用 . . . . . . . . . . . : 是
   自動設定啟用 . . . . . . . . . . . : 是
   IPv6 位址. . . . . . . . . . . . : 2405:9200:1110:0:852d:59eb:5e77:d3ff(偏好選項)
   臨時 IPv6 位址. . . . . . . . . . : 2405:9200:1110:0:9d63:a8ac:3575:16ae(偏好選項)
   連結-本機 IPv6 位址 . . . . . . . . : fe80::852d:59eb:5e77:d3ff%19(偏好選項)
   IPv4 位址 . . . . . . . . . . . . : 192.168.10.97(偏好選項)
   子網路遮罩 . . . . . . . . . . . . : 255.255.255.0
   租用取得 . . . . . . . . . . . . : 2019年7月24日 上午 11:20:31
   租用到期 . . . . . . . . . . . . : 2019年7月31日 上午 11:20:31
   預設閘道 . . . . . . . . . . . . : fe80::eb6:d2ff:fe68:8610%19
                                       192.168.10.1
   DHCP 伺服器 . . . . . . . . . . . : 192.168.10.1
   DHCPv6 IAID . . . . . . . . . . . : 154712824
   DHCPv6 用戶端 DUID. . . . . . . . : 00-01-00-01-24-35-E6-77-84-A9-3E-04-A8-BB
   DNS 伺服器 . . . . . . . . . . . : 2404::1
                                       2001:4860:4860::8888
                                       2001:b000:168::1
                                       192.168.10.1
                                       2404::1
                                       2001:4860:4860::8888
                                       2001:b000:168::1
   NetBIOS over Tcpip . . . . . . . : 啟用
```

D-Link DIR-853 CM 測項11

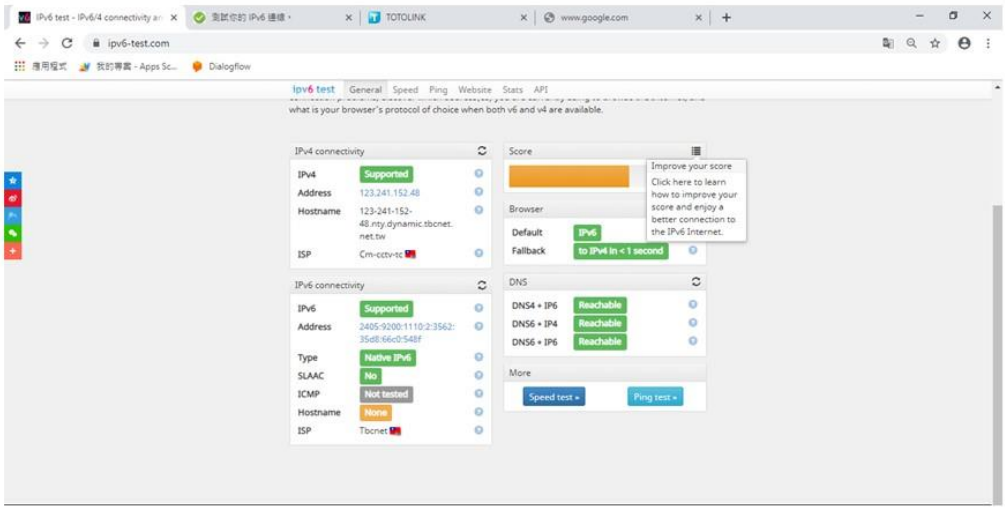
✓ 確認用戶連接Wi-Fi IPv6上網正常(test-ipv6.com)

測試你的 IPv6 連線。



D-Link DIR-853 CM 測項11(續)

✓ 確認用戶連接Wi-Fi IPv6上網正常(ipv6-test.com)



D-Link DIR-853 CM 測項12

- ✓ 確認IPv6 連線功能隨著IPv4啟用而自動啟用正常
  - 重設分享器，依照介面指示設定後，IPv4啟用後IPv6即自動啟用



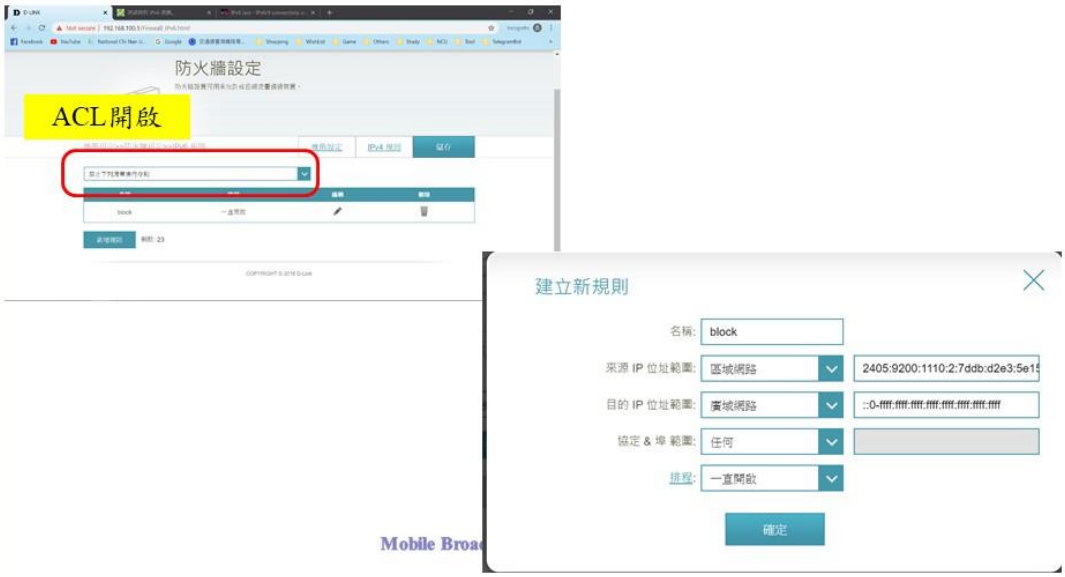
D-Link DIR-853 CM 測項13

- ✓ IPv6寬頻分享器IPv6 ACL功能是否正常?
  - 測試寬頻分享器 IPv6 ACL功能是否能限制用戶終端IPv6連線



D-Link DIR-853 CM 測項13(續)

- ✓ IPv6寬頻分享器IPv6 ACL功能是否正常?
  - 測試寬頻分享器 IPv6 ACL功能是否能限制用戶終端IPv6連線



D-Link DIR-853 CM 測項13(續)

- ✓ IPv6寬頻分享器IPv6 ACL功能是否正常?
  - 測試寬頻分享器 IPv6 ACL功能是否能限制用戶終端IPv6連線



D-Link DIR-1760

分享器測試成果

1

測試設備與環境

分享器產品設備資訊	
產品型號	DIR-1760
產品名稱	AC1750 Mesh無線路由器
硬體版本	A1
韌體版本	1.00
製造年份	2019

測試環境資訊	
測試環境	1.HiNet光世代 PPPoE
	2.Cable IPoE
測試終端	Windows 10
終端瀏覽器	Chrome
測試時間	2019-08~2019-10

硬體基本資料



Mobile Broadband Networklab, NCU

測試紀錄摘要

HiNet 光世代PPPoE測試		
	測試項目	DIR-1760
1	分享器PPPoE撥接是否正常?	O
2	分享器IPv6、IPv6 PD、DNSv6取得是否正常?	O
3	用戶IPv6、DNSv6取得是否正常?	O
4	用戶至HiNet路由是否正常?	O
5	用戶IPv6上網是否正常?	O
6	用戶熱門網頁開啟是否正常?	O
7	用戶上網速率是否正常?	O
8	分享器重撥，用戶IPv6更新是否正常?	O
9	用戶使用IPv6之MTU是否正常?	1500
10	用戶連接Wi-Fi上網IPv6、DNSv6是否正常?	O
11	用戶連接Wi-Fi IPv6上網是否正常?	O
12	IPv6 PPPoE（或是PPPoEv6)是否隨著IPv4 PPPoE啟用而自動啟用?	X
13	IPv6 PPPoE（或是PPPoEv6)連線之PPPoE Session是『Share with IPv4』或是『Create a new Session』?	可設定兩種模式『New Session』WAN端為斷線
14	IPv6寬頻分享器IPv6 ACL功能是否正常?	O

Cable IPoE測試		
	測試項目	DIR-1760
1	分享器連接Cable Modem是否正常?	O
2	分享器IPv6、IPv6 PD、DNSv6取得是否正常?	O
3	用戶IPv6、DNSv6取得是否正常?	O
4	用戶至Cable業者路由是否正常?	O
5	用戶IPv6上網是否正常?	O
6	用戶熱門網頁開啟是否正常?	O
7	用戶上網速率是否正常?	O
8	分享器重撥Cable Modem，用戶IPv6更新是否正常?	O
9	用戶使用IPv6之MTU是否正常?	1500
10	用戶連接Wi-Fi上網IPv6、DNSv6是否正常?	O
11	用戶連接Wi-Fi IPv6上網是否正常?	O
12	IPv6連線功能是否隨著IPv4啟用而自動啟用?	X
13	IPv6寬頻分享器IPv6 ACL功能是否正常?	O

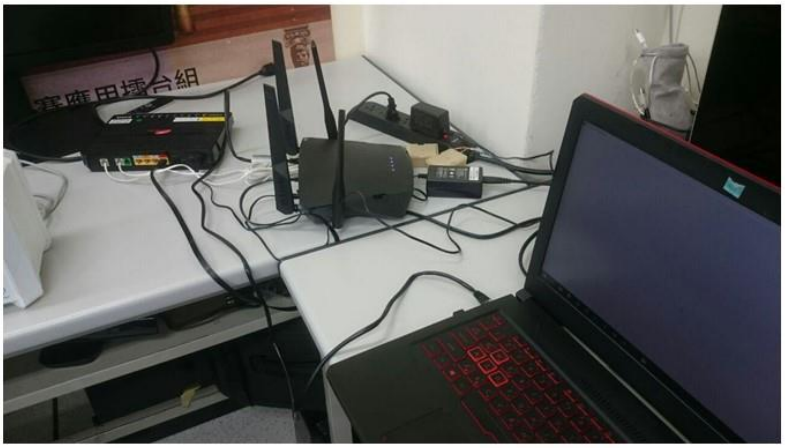
Mobile Broadband Networklab, NCU

測試紀錄摘要說明

- ✓ HiNet PPPoE環境 (Pass測項:11/14)
  - 測項9:RA ICMP option MTU1500，PPPoE環境可能導致用戶端packet too big須重傳
  - 測項12: 需要手動啟用IPv6
  - 測項13: 可選用兩種模式，但設定『Create a new session』則WAN端為斷線
- ✓ Cable IPoE環境(Pass測項:12/13)
  - 測項12: 需要手動啟用IPv6

Mobile Broadband Networklab, NCU

分享器測試紀錄
HiNet 光世代PPPoE環境



5

D-Link DIR-1760 PPPoE 測項1

✓ 確認分享器PPPoE撥接正常

網際網路

WAN端位址資訊

網路連線類型: PPPoE
網際網路狀態: 已連線
連線時間: 0 天 0 時 1 分 22 秒

IPv4 / IPv6
廣域網路 IPv6 位址: 2001:B011:6CC0:2DE4:F8AC:2E1A:F039:2AD6/64
預設閘道器: FE80::D2F0:DBFF:FE53:800
主要 DNS 伺服器: 2001:B000:168::2
輔助 DNS 伺服器: 2001:B000:168::1

Mobile Broadband Networklab, NCU

D-Link DIR-1760 PPPoE 測項2

✓ 確認分享器IPv6、IPv6 PD、DNSv6取得正常

網際網路

WAN端位址資訊

IPv4 / IPv6

網路連線類型: PPPoE

網際網路狀態: 已連線

連線時間: 0 天 0 時 1 分 22 秒

廣域網路 IPv6 位址: 2001:B011:6CC0:2DE4:F8AC:2E1A:F039:2AD6/64

預設閘道器: FE80::D2F0:DBFF:FE53:800

主要 DNS 伺服器: 2001:B000:168::2

輔助 DNS 伺服器: 2001:B000:168::1

IPv6 網路

LAN端位址資訊

Link-Local 位址: FE80::EEAD:E0FF:FE2E:667F

路由器 IPv6 位址: 2001:B011:6CC0:12FC:EEAD:E0FF:FE2E:667F

DHCP-PD: 啟用

配置的網段: 2001:B011:6CC0:12FC::/64

D-Link DIR-1760 PPPoE 測項3

✓ 確認用戶IPv6、DNSv6取得正常

乙太網路卡 乙太網路:

```
連線特定 DNS 尾碼 . . . . . :
描述 . . . . . : Realtek PCIe GBE Family Controller
實體位址 . . . . . : 1C-B7-2C-1E-CB-0E
DHCP 已啟用 . . . . . : 是
自動設定啟用 . . . . . : 是
IPv6 位址. . . . . : 2001:b011:6cc0:12fc:a032:c63b:766e:c8d4(偏好選項)
臨時 IPv6 位址. . . . . : 2001:b011:6cc0:12fc:98c0:db5c:d19a:b7bb(偏好選項)
連結-本機 IPv6 位址 . . . . . : fe80::a032:c63b:766e:c8d4%11(偏好選項)
IPv4 位址 . . . . . : 192.168.0.108(偏好選項)
子網路遮罩 . . . . . : 255.255.255.0
租用取得 . . . . . : 2019年8月22日 下午 02:55:11
租用到期 . . . . . : 2019年8月29日 下午 02:55:11
預設閘道 . . . . . : fe80::eead:e0ff:fe2e:667f%11
                     192.168.0.1
DHCP 伺服器 . . . . . : 192.168.0.1
DHCPv6 IAID . . . . . : 52213548
DHCPv6 用戶端 DUID. . . . . : 00-01-00-01-1C-CC-BE-EF-1C-B7-2C-1E-CB-0E
DNS 伺服器 . . . . . : 2404::1
                     2001:4860:4860::8888
                     2001:b000:168::1
                     192.168.0.1
                     2001:b000:168::2
                     2001:b000:168::1
                     2404::1
NetBIOS over Tcpip . . . . . : 啟用
```

D-Link DIR-1760 PPPoE 測項4

✓ 確認用戶至HiNet路由正常

```
C:\Users\ASUS>ping dns.hinet.net

Ping dns.hinet.net [2001:b000:168::2] (使用 32 位元組的資料):
回覆自 2001:b000:168::2: 時間=12ms
回覆自 2001:b000:168::2: 時間=11ms
回覆自 2001:b000:168::2: 時間=11ms
回覆自 2001:b000:168::2: 時間=10ms

2001:b000:168::2 的 Ping 統計資料:
    封包: 已傳送 = 4，已收到 = 4，已遺失 = 0 (0% 遺失)，
大約的來回時間 (毫秒):
    最小值 = 10ms，最大值 = 12ms，平均 = 11ms

C:\Users\ASUS>tracert dns.hinet.net

在上限 30 個躍點上
追蹤 dns.hinet.net [2001:b000:168::2] 的路由:

  1    <1 ms    <1 ms    <1 ms  2001-b011-6cc0-12fc-eead-e0ff-fe2e-667f.dynamic-ip6.hinet.net [2001:b011:6cc0:12fc:eead:e0ff:fe2e:667f]
  2    10 ms    10 ms     8 ms  2001:b010:ffff::1
  3     9 ms    10 ms    11 ms  2001-b000-0089-0005-0022-2222-0002-0002.hinet-ip6.hinet.net [2001:b000:89:5:22:2222:2:2]
  4    10 ms     *        *     2001-b000-0080-0003-0080-0089-0022-000a.hinet-ip6.hinet.net [2001:b000:80:3:80:89:22:a]
  5    13 ms     9 ms    11 ms  2001-b000-0080-0004-3022-3012-0003-000b.hinet-ip6.hinet.net [2001:b000:80:4:3022:3012:3:b]
  6    15 ms    14 ms    14 ms  2001-b000-0080-0004-3022-3012-0003-000b.hinet-ip6.hinet.net [2001:b000:80:4:3022:3012:3:b]
  7    11 ms    10 ms    10 ms  2001-b000-0080-0004-3012-3312-0012-000b.hinet-ip6.hinet.net [2001:b000:80:4:3012:3312:12:b]
  8    12 ms    10 ms    10 ms  2001-b000-0080-0006-3312-0000-0002-0001.hinet-ip6.hinet.net [2001:b000:80:6:3312:0:2:1]
  9    12 ms    11 ms    12 ms  dns.hinet.net [2001:b000:168::2]

追蹤完成。
```

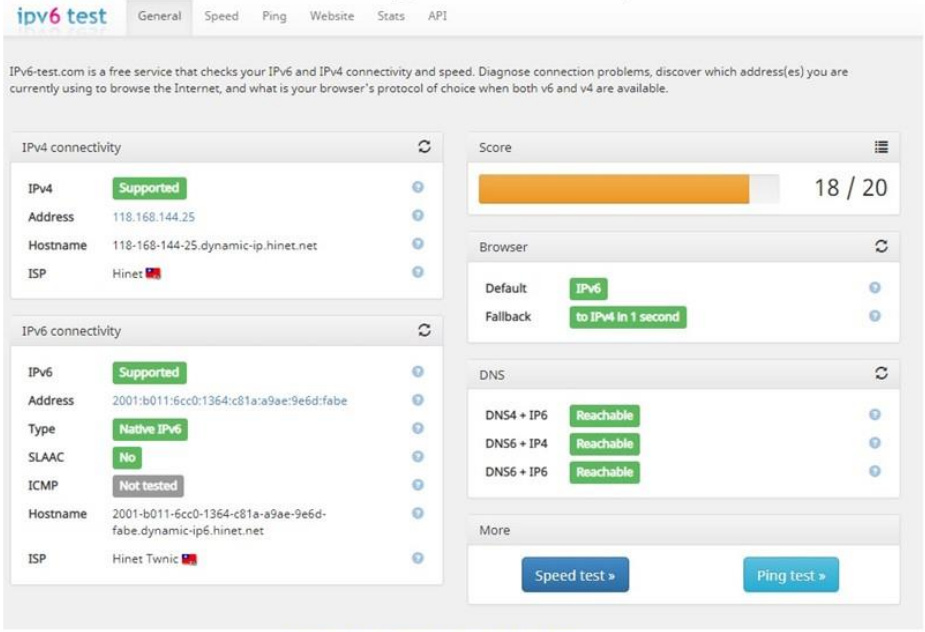

D-Link DIR-1760 PPPoE 測項5

✓ 確認用戶IPv6上網正常(test-ipv6.com)



D-Link DIR-1760 PPPoE 測項5(續)

✓ 確認用戶IPv6上網正常(ipv6-test.com)



D-Link DIR-1760 PPPoE 測項6

✓ 確認用戶熱門網頁開啟正常



D-Link DIR-1760 PPPoE 測項7

✓ 確認用戶上網速率正常



D-Link DIR-1760 PPPoE 測項8

✓ 確認分享器重撥，用戶IPv6更新正常



D-Link DIR-1760 PPPoE 測項9

✓ 確認用戶使用IPv6之MTU為**1500**非1492

```
C:\Users\ASUS>netsh interface ipv6 show subinterface

   MTU  MediaSenseState   接收的位元組  傳送的位元組  介面
------  ---------------  ---------  ---------  -------------
  1500                1   54544158    9222773  乙太網路
4294967295                1          0    3621277  Loopback Pseudo-Interface 1
  1500                2   73508197    5664034  Wi-Fi
  1500                5          0       2574  區域連線* 2
  1500                5          0       5538  區域連線* 4
  1500                5          0        228  Bluetooth 網路連線
```


D-Link DIR-1760 PPPoE 測項10

✓ 確認用戶連接Wi-Fi上網IPv6、DNSv6正常

```
無線區域網路介面卡 Wi-Fi:

   連線特定 DNS 尾碼 . . . . . . . . :
   描述 . . . . . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 7265
   實體位址 . . . . . . . . . . . . . : 34-02-86-63-18-11
   DHCP 已啟用 . . . . . . . . . . . : 是
   自動設定啟用 . . . . . . . . . . . : 是
   IPv6 位址. . . . . . . . . . . . . : 2001:b011:6cc0:12fc:80c3:57d2:60e7:e27a(偏好選項)
   臨時 IPv6 位址. . . . . . . . . . . : 2001:b011:6cc0:12fc:99f5:eb0c:4384:b905(偏好選項)
   連結-本機 IPv6 位址 . . . . . . . . : fe80::80c3:57d2:60e7:e27a%8(偏好選項)
   IPv4 位址 . . . . . . . . . . . . . : 192.168.0.160(偏好選項)
   子網路遮罩 . . . . . . . . . . . . : 255.255.255.0
   租用取得 . . . . . . . . . . . . . : 2019年8月22日 下午 03:30:04
   租用到期 . . . . . . . . . . . . . : 2019年8月29日 下午 03:30:04
   預設閘道 . . . . . . . . . . . . . : fe80::eead:e0ff:fe2e:667f%8
                                        192.168.0.1
   DHCP 伺服器 . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 120849030
   DHCPv6 用戶端 DUID. . . . . . . . : 00-01-00-01-1C-CC-BE-EF-1C-B7-2C-1E-CB-0E
   DNS 伺服器 . . . . . . . . . . . . : 2001:b000:168::2
                                        2001:b000:168::1
                                        192.168.0.1
   NetBIOS over Tcpip . . . . . . . . : 啟用
```

D-Link DIR-1760 PPPoE 測項11

✓ 確認用戶連接Wi-Fi IPv6上網正常(test-ipv6.com)

測試你的 IPv6 連線。

總結 | 測試結果 | 分享結果 / 聯繫我們 | 其他 IPv6 網站

你在網際網路上的IPv4位址 61.228.143.117

你在網際網路上的IPv6位址 2001:b011:6cc0:12fc:99f5:eb0c:4384:b905

你的網路服務提供者 (ISP) 是 HINET Data Communication Business Group

Since you have IPv6, we are including a tab that shows how well you can reach other IPv6 sites. [詳細資訊]

HTTPS 支援現已在本網站上提供。 [詳細資訊]

你的 DNS 伺服器 （可能由你的ISP維護）似乎支援 IPv6 的網際網路通訊協定。

你對於 IPv6 準備的分數

當網站陸續只使用 IPv6，請提早為您的 IPv6 做準備和設定

10/10

點擊查看 測試資料

D-Link DIR-1760 PPPoE 測項11(續)

✓ 確認用戶連接Wi-Fi IPv6上網正常(ipv6-test.com)

ipv6 test | General | Speed | Ping | Website | Stats | API

IPv6-test.com is a free service that checks your IPv6 and IPv4 connectivity and speed. Diagnose connection problems, discover which address(es) you are currently using to browse the Internet, and what is your browser's protocol of choice when both v6 and v4 are available.

IPv4 connectivity

IPv4	Supported
Address	118.168.144.25
Hostname	118-168-144-25.dynamic-ip.hinet.net
ISP	Hinet

IPv6 connectivity

IPv6	Supported
Address	2001:b011:6cc0:1364:d34:1e52:2071:c038
Type	Native IPv6
SLAAC	No
ICMP	Not tested
Hostname	2001-b011-6cc0-1364-0d34-1e52-2071-c038.dynamic-ip6.hinet.net
ISP	Hinet Twnic

Score

18 / 20

Browser

Default	IPv6
Fallback	to IPv4 in 1 second

DNS

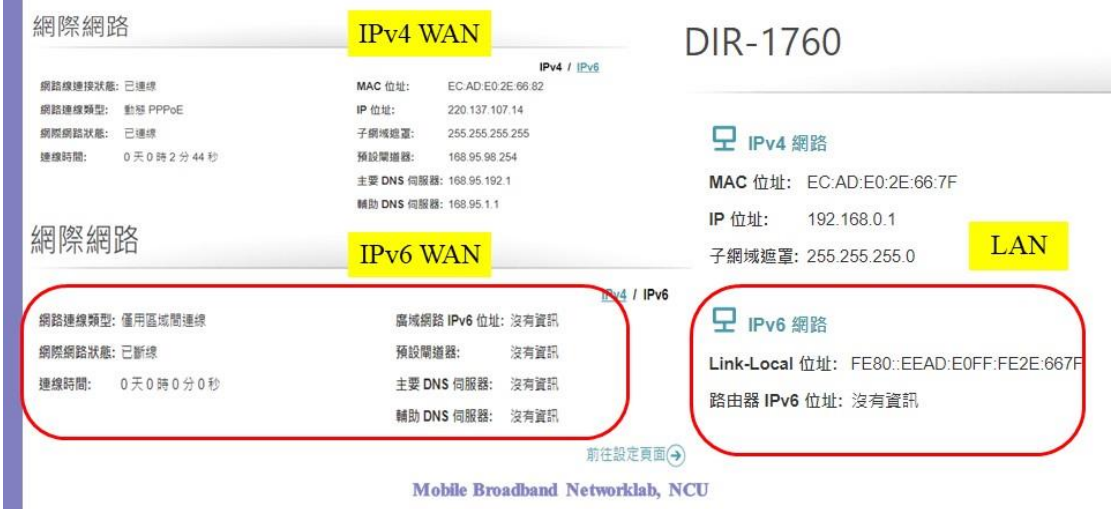
DNS4 + IP6	Reachable
DNS6 + IP4	Reachable
DNS6 + IP6	Reachable

More

Speed test » | Ping test »

D-Link DIR-1760 PPPoE 測項12

- ✓ IPv6 PPPoE (或是PPPoEv6)是否隨著IPv4 PPPoE啟用而自動啟用
  - 重設分享器後，經快速精靈設定，IPv4啟用後IPv6不會自動啟用



D-Link DIR-1760 PPPoE 測項12(續)

- ✓ IPv6 PPPoE (或是PPPoEv6)是否隨著IPv4 PPPoE啟用而自動啟用
  - 更改IPv6設定



D-Link DIR-1760 PPPoE 測項12(續)

- ✓ IPv6 PPPoE (或是PPPoEv6)是否隨著IPv4 PPPoE啟用而自動啟用
  - 更改IPv6設定



Mobile Broadband Networklab, NCU

D-Link DIR-1760 PPPoE 測項12(續)

- ✓ IPv6 PPPoE (或是PPPoEv6)是否隨著IPv4 PPPoE啟用而自動啟用
  - 更改IPv6設定後，IPv6成功啟用



D-Link DIR-1760 PPPoE 測項13

✓ IPv6 PPPoE (或是PPPoEv6)連線之PPPoE Session是『Share with IPv4』或是『Create a new Session』?



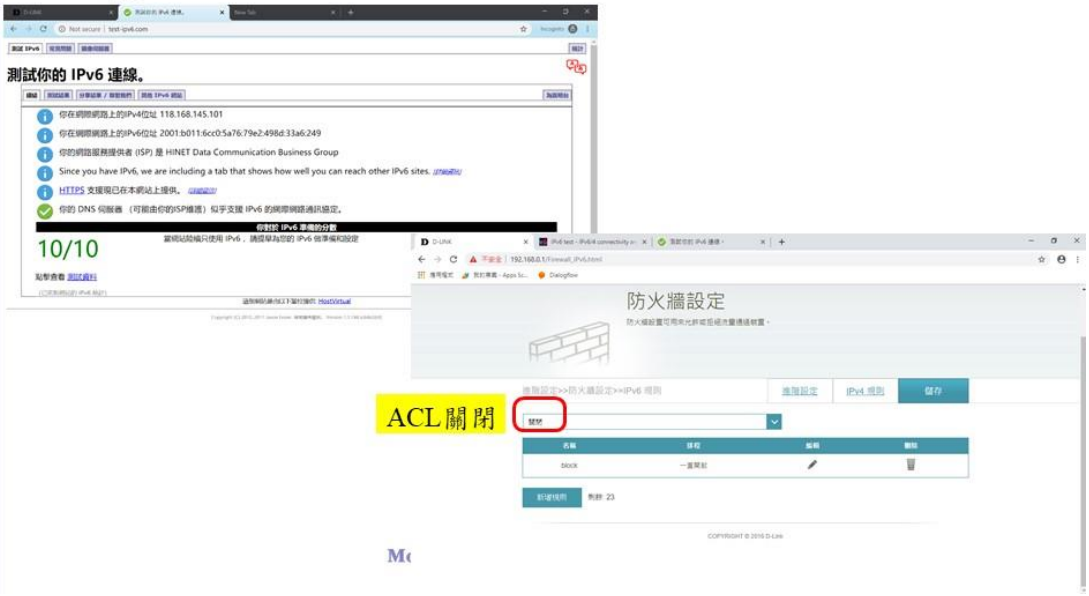
D-Link DIR-1760 PPPoE 測項13 (續)

✓ IPv6 PPPoE (或是PPPoEv6)連線之PPPoE Session是『Share with IPv4』或是『Create a new Session』?



D-Link DIR-1760 PPPoE 測項14

- ✓ IPv6寬頻分享器IPv6 ACL功能是否正常?
  - 測試寬頻分享器 IPv6 ACL功能是否能限制用戶終端IPv6連線



D-Link DIR-1760 PPPoE 測項14 (續)

- ✓ IPv6寬頻分享器IPv6 ACL功能是否正常?
  - 測試寬頻分享器 IPv6 ACL功能是否能限制用戶終端IPv6連線



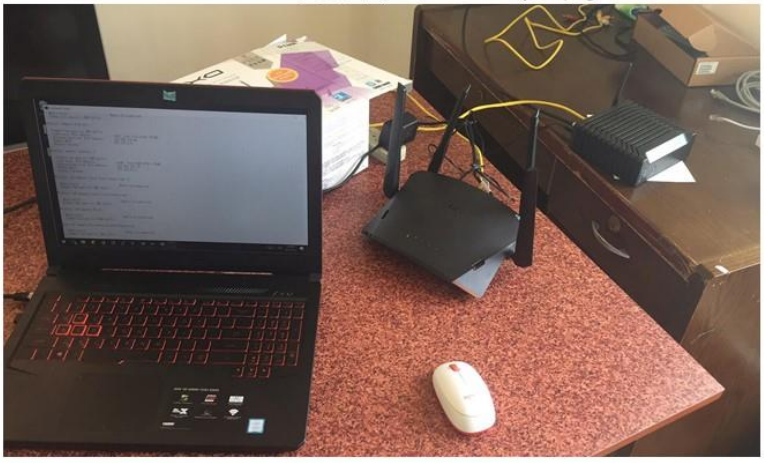
D-Link DIR-1760 PPPoE 測項14 (續)

- ✓ IPv6寬頻分享器IPv6 ACL功能是否正常?
  - 測試寬頻分享器 IPv6 ACL功能是否能限制用戶終端IPv6連線



分享器測試紀錄

Cable 寬頻 IPoE環境



D-Link DIR-1760 CM 測項1

✓ 確認連接cable modem正常



D-Link DIR-1760 CM 測項2

✓ 確認取得IPv6、IPv6 PD、DNSv6



D-Link DIR-1760 CM 測項3

✓ 確認用戶IPv6、DNSv6取得正常

乙太網路卡 乙太網路:

```
連線特定 DNS 尾碼 . . . . . :
描述 . . . . . : Realtek PCIe GBE Family Controller
實體位址 . . . . . : 1C-B7-2C-1E-CB-0E
DHCP 已啟用 . . . . . : 是
自動設定啟用 . . . . . : 是
IPv6 位址. . . . . : 2405:9200:1110:1c:a032:c63b:766e:c8d4(偏好選項)
臨時 IPv6 位址. . . . . : 2405:9200:1110:1c:d936:ccc4:1bed:100(偏好選項)
連結-本機 IPv6 位址 . . . . . : fe80::a032:c63b:766e:c8d4%11(偏好選項)
IPv4 位址 . . . . . : 192.168.0.108(偏好選項)
子網路遮罩 . . . . . : 255.255.255.0
租用取得 . . . . . : 2019年8月20日 下午 02:20:15
租用到期 . . . . . : 2019年8月27日 下午 02:20:15
預設閘道 . . . . . : fe80::eead:e0ff:fe2e:667f%11
                     192.168.0.1
DHCP 伺服器 . . . . . : 192.168.0.1
DHCPv6 IAID . . . . . : 52213548
DHCPv6 用戶端 DUID. . . . . : 00-01-00-01-1C-CC-BE-EF-1C-B7-2C-1E-CB-0E
DNS 伺服器 . . . . . : 192.168.0.1
NetBIOS over Tcpip . . . . . : 啟用
```


D-Link DIR-1760 CM 測項4

✓ 確認用戶至google ipv6路由正常

```
C:\Users\ASUS>ping ipv6.google.com

Ping ipv6.l.google.com [2404:6800:4008:803::200e] (使用 32 位元組的資料):
回覆自 2404:6800:4008:803::200e: 時間=12ms
回覆自 2404:6800:4008:803::200e: 時間=21ms
回覆自 2404:6800:4008:803::200e: 時間=12ms
回覆自 2404:6800:4008:803::200e: 時間=13ms

2404:6800:4008:803::200e 的 Ping 統計資料:
    封包: 已傳送 = 4，已收到 = 4，已遺失 = 0 (0% 遺失)，
大約的來回時間 (毫秒):
    最小值 = 12ms，最大值 = 21ms，平均 = 14ms

C:\Users\ASUS>tracert ipv6.google.com

在上限 30 個躍點上
追蹤 ipv6.l.google.com [2404:6800:4008:803::200e] 的路由:

  1    <1 ms    <1 ms    <1 ms  2405:9200:1110:1c:eead:e0ff:fe2e:667f
  2     *        *        *     要求等候逾時。
  3    11 ms    11 ms     8 ms  2405:9200:1:0:172:16:28:165a
  4    12 ms    11 ms    10 ms  2405:9200:1:0:172:16:31:6a
  5    11 ms    11 ms    10 ms  2404:0:10ff:1:7709:13:1596:1210
  6    12 ms    11 ms    11 ms  2404:0:10ff::4:166
  7    13 ms    12 ms    11 ms  2404:0:10ff:1:7709:1:5169:61
  8    13 ms    11 ms    11 ms  2001:4860:0:1014::1
  9    15 ms    11 ms    11 ms  2001:4860:0:1::8d7
 10    13 ms    12 ms    13 ms  tsa03s02-in-x0e.1e100.net [2404:6800:4008:803::200e]

追蹤完成。
```

D-Link DIR-1760 CM 測項5

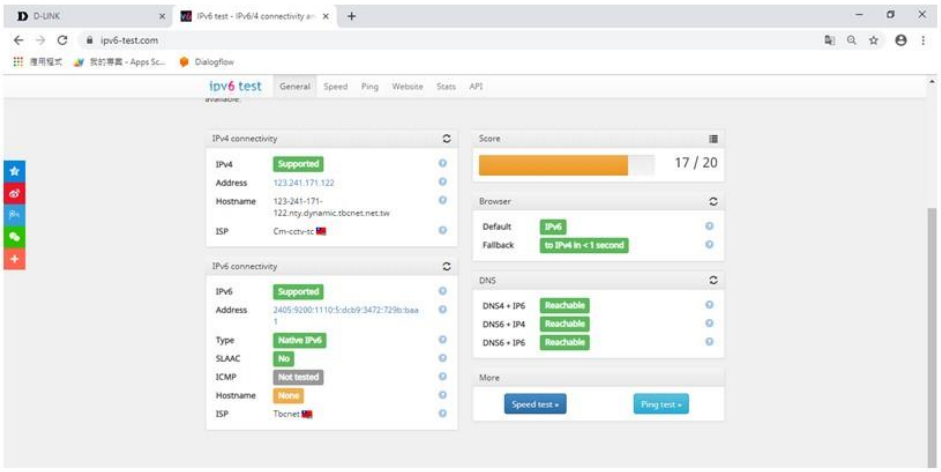
✓ 確認用戶IPv6上網正常(test-ipv6.com)

測試你的 IPv6 連線。



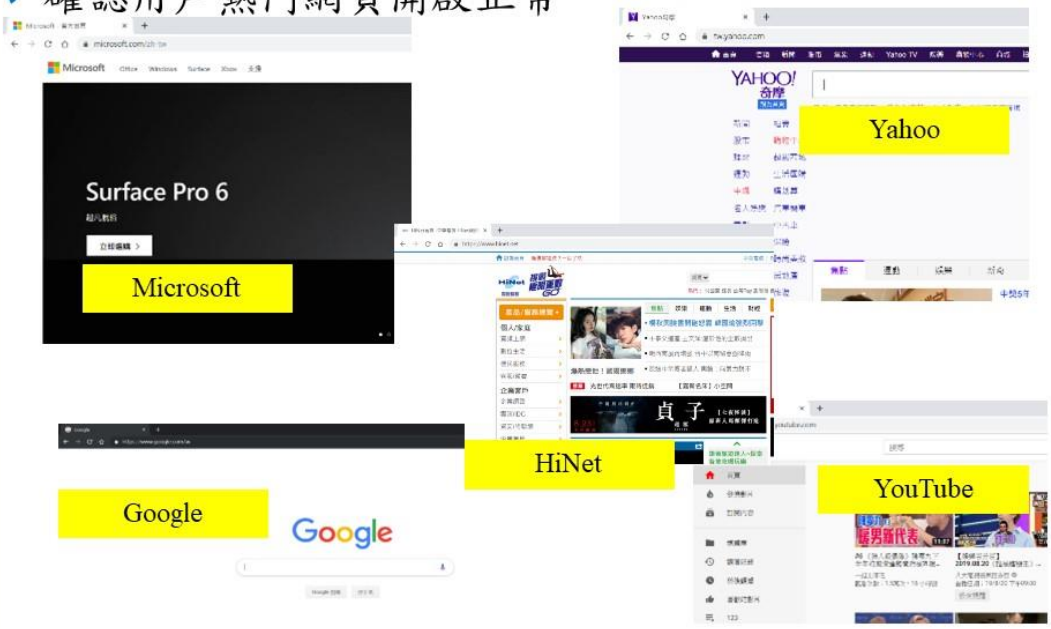
D-Link DIR-1760 CM 測項5(續)

✓ 確認用戶IPv6上網正常(ipv6-test.com)



D-Link DIR-1760 CM 測項6

✓確認用戶熱門網頁開啟正常



D-Link DIR-1760 CM 測項7

✓確認用戶上網速率正常



D-Link DIR-1760 CM 測項8

✓ 確認分享器重新連接cable modem之後，用戶ipv6相同，且連線正常

分享器重接CM前



分享器重接CM後



D-Link DIR-1760 CM 測項9

✓ 確認用戶使用IPv6乙太網路介面之MTU為1500

```
C:\Users\ASUS>netsh interface ipv6 show subinterface

   MTU  MediaSenseState   接收的位元組 傳送的位元組  介面
------  ---------------  ---------  ---------  -------------
  1500                1   70051092   49656188  乙太網路
4294967295                1          0    1286709  Loopback Pseudo-Interface 1
  1500                2    9111959     279209  Wi-Fi
  1500                5          0       1604  區域連線* 2
  1500                5          0       1604  區域連線* 4
  1500                5          0       1604  Bluetooth 網路連線
```

D-Link DIR-1760 CM 測項10

✓ 確認用戶連接Wi-Fi上網IPv6、DNSv6正常

無線區域網路介面卡 Wi-Fi:

```
   連線特定 DNS 尾碼 . . . . . . . . :
   描述 . . . . . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 7265
   實體位址 . . . . . . . . . . . . . : 34-02-86-63-18-11
   DHCP 已啟用 . . . . . . . . . . . : 是
   自動設定啟用 . . . . . . . . . . . : 是
   IPv6 位址. . . . . . . . . . . . . : 2405:9200:1110:1c:80c3:57d2:60e7:e27a(偏好選項)
   臨時 IPv6 位址. . . . . . . . . . . : 2405:9200:1110:1c:f468:b21:97d5:dcba(偏好選項)
   連結-本機 IPv6 位址 . . . . . . . . : fe80::80c3:57d2:60e7:e27a%8(偏好選項)
   IPv4 位址 . . . . . . . . . . . . . : 192.168.0.160(偏好選項)
   子網路遮罩 . . . . . . . . . . . . : 255.255.255.0
   租用取得 . . . . . . . . . . . . . : 2019年8月20日 下午 03:06:47
   租用到期 . . . . . . . . . . . . . : 2019年8月27日 下午 03:06:47
   預設閘道 . . . . . . . . . . . . . : fe80::eead:e0ff:fe2e:667f%8
                                        192.168.0.1
   DHCP 伺服器 . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 120849030
   DHCPv6 用戶端 DUID. . . . . . . . : 00-01-00-01-1C-CC-BE-EF-1C-B7-2C-1E-CB-0E
   DNS 伺服器 . . . . . . . . . . . . : 2404::1
                                        2001:4860:4860::8888
                                        2001:b000:168::1
                                        192.168.0.1
   NetBIOS over Tcpip . . . . . . . . : 啟用
```


D-Link DIR-1760 CM 測項11

✓ 確認用戶連接Wi-Fi IPv6上網正常(test-ipv6.com)

測試你的 IPv6 連線。

總結 | 測試結果 | 分享結果 / 聯繫我們 | 其他 IPv6 網站

- 你在網際網路上的IPv4位址 123.241.153.112
- 你在網際網路上的IPv6位址 2405:9200:1110:1c:f468:b21:97d5:dcba
- 你的網路服務提供者 (ISP) 是 TBCOM-NET TBC
- Since you have IPv6, we are including a tab that shows how well you can reach other IPv6 sites. [詳細資訊]
- HTTPS 支援現已在本網站上提供。 [詳細資訊]
- 你的 DNS 伺服器 （可能由你的ISP維護）似乎支援 IPv6 的網際網路通訊協定。

你對於 IPv6 準備的分數

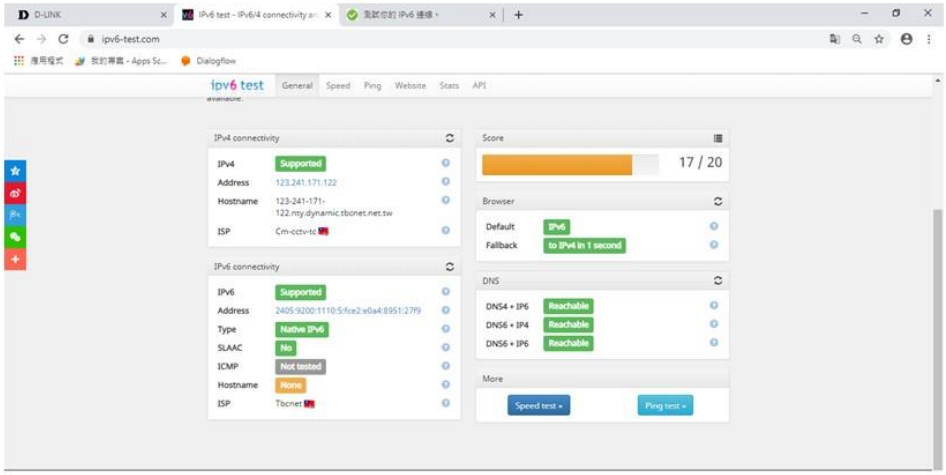
10/10

當網站陸續只使用 IPv6，請提早為您的 IPv6 做準備和設定

點擊查看 測試資料

D-Link DIR-1760 CM 測項11(續)

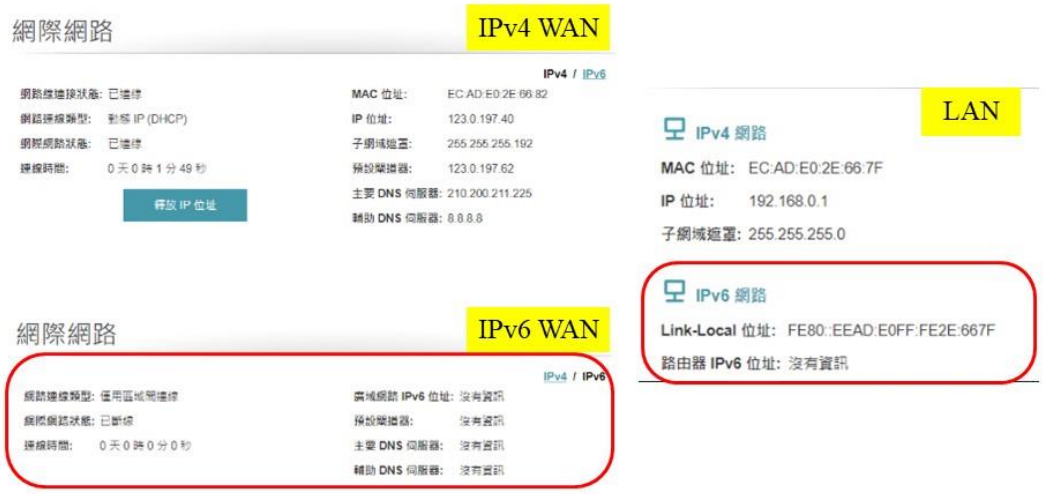
✓ 確認用戶連接Wi-Fi IPv6上網正常(ipv6-test.com)



D-Link DIR-1760 CM 測項12

✓ 確認IPv6 連線功能隨著IPv4啟用而自動啟用

- 重設分享器後，經快速精靈設定，IPv4啟用後IPv6不會自動啟用



D-Link DIR-1760 CM 測項12 (續)

- ✓ 確認IPv6 連線功能隨著IPv4啟用而自動啟用
  - 更改IPv6設定



D-Link DIR-1760 CM 測項12 (續)

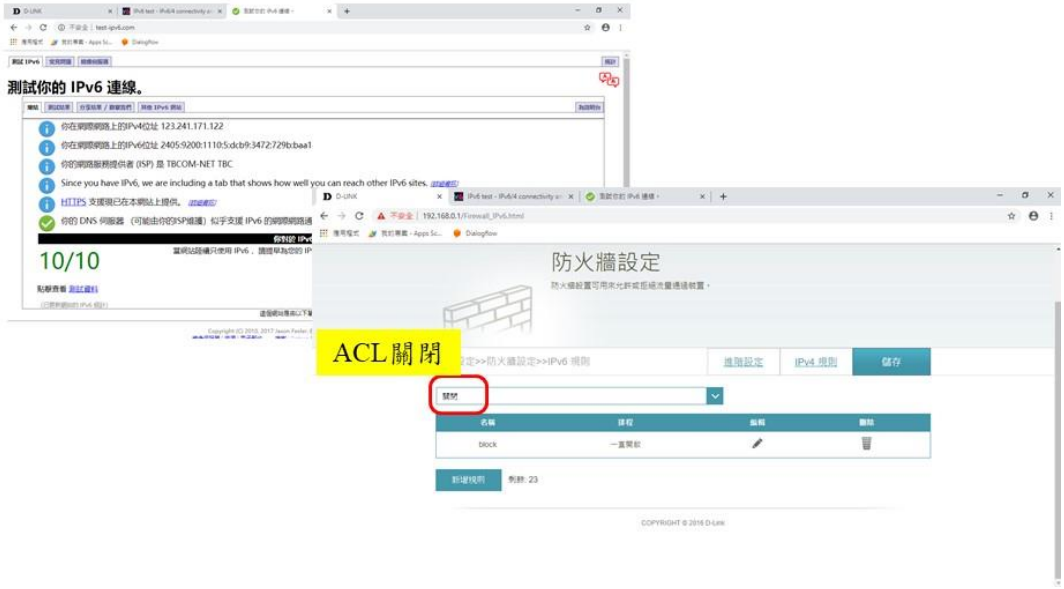
- ✓ 確認IPv6 連線功能隨著IPv4啟用而自動啟用
  - 更改IPv6設定後，IPv6成功啟用



Mobile Broadband Networklab, NCU

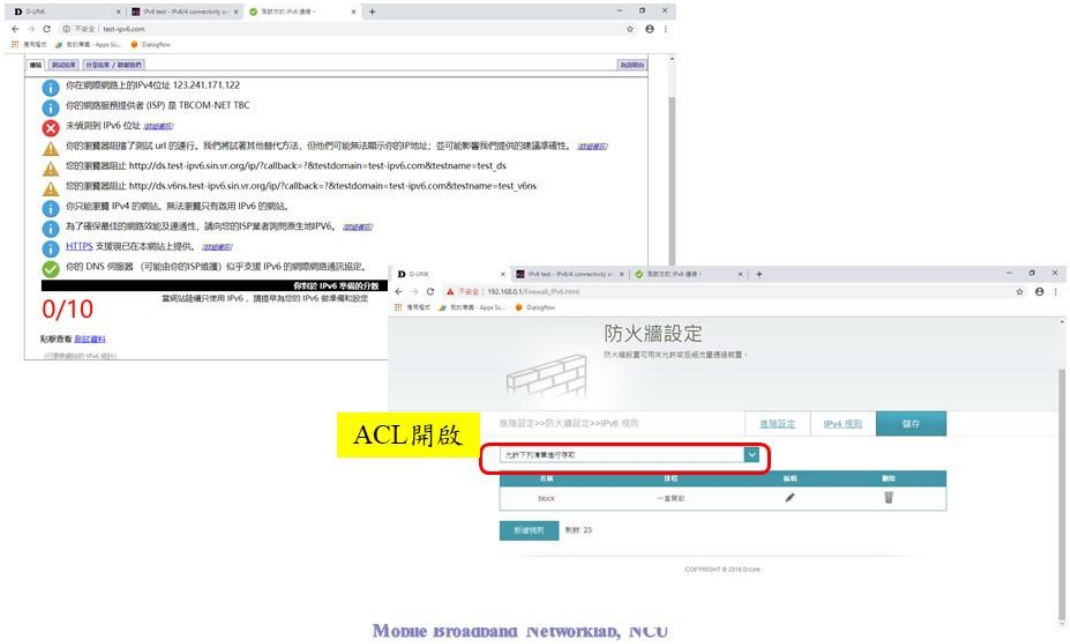
D-Link DIR-1760 CM 測項13

- ✓ IPv6寬頻分享器IPv6 ACL功能是否正常?
  - 測試寬頻分享器 IPv6 ACL功能是否能限制用戶終端IPv6連線



D-Link DIR-1760 CM 測項13(續)

啟用ACL功能後，被設定阻擋的主機無法取得IPv6位址



D-Link DIR-1960

分享器測試成果

1

測試設備與環境

分享器產品設備資訊	
產品型號	DIR-1960
產品名稱	AC1900 Mesh無線路由器
硬體版本	A1
韌體版本	1.00
製造年份	2019

測試環境資訊	
測試環境	1.HiNet光世代 PPPoE
	2.Cable IPoE
測試終端	Windows 10
終端瀏覽器	Chrome
測試時間	2019-08~2019-10



Mobile Broadband Networklab, NCU

測試紀錄摘要

HiNet 光世代PPPoE測試		
	測試項目	DIR-1960
1	分享器PPPoE撥接是否正常?	O
2	分享器IPv6、IPv6 PD、DNSv6取得是否正常?	O
3	用戶IPv6、DNSv6取得是否正常?	O
4	用戶至HiNet路由是否正常?	O
5	用戶IPv6上網是否正常?	O
6	用戶熱門網頁開啟是否正常?	O
7	用戶上網速率是否正常?	O
8	分享器重撥，用戶IPv6更新是否正常?	O
9	用戶使用IPv6之MTU是否正常?	1500
10	用戶連接Wi-Fi上網IPv6、DNSv6是否正常?	O
11	用戶連接Wi-Fi IPv6上網是否正常?	O
12	IPv6 PPPoE（或是PPPoEv6)是否隨著IPv4 PPPoE啟用而自動啟用?	O
13	IPv6 PPPoE（或是PPPoEv6)連線之PPPoE Session是『Share with IPv4』或是『Create a new Session』?	可設定兩種模式『New Session』WAN端為斷線
14	IPv6寬頻分享器IPv6 ACL功能是否正常?	O

Cable IPoE測試		
	測試項目	DIR-1960
1	分享器連接Cable Modem是否正常?	O
2	分享器IPv6、IPv6 PD、DNSv6取得是否正常?	O
3	用戶IPv6、DNSv6取得是否正常?	O
4	用戶至Cable業者路由是否正常?	O
5	用戶IPv6上網是否正常?	O
6	用戶熱門網頁開啟是否正常?	O
7	用戶上網速率是否正常?	O
8	分享器重撥Cable Modem，用戶IPv6更新是否正常?	O
9	用戶使用IPv6之MTU是否正常?	1500
10	用戶連接Wi-Fi上網IPv6、DNSv6是否正常?	O
11	用戶連接Wi-Fi IPv6上網是否正常?	O
12	IPv6連線功能是否隨著IPv4啟用而自動啟用?	O
13	IPv6寬頻分享器IPv6 ACL功能是否正常?	O

Mobile Broadband Networklab, NCU

測試紀錄摘要說明

- ✓ HiNet PPPoE環境 (Pass測項:12/14)
  - 測項9:RA ICMP option MTU1500，PPPoE環境可能導致用戶端packet too big須重傳
  - 測項13: 可選用兩種模式，但設定『Create a new session』則WAN端為斷線

- ✓ Cable IPoE環境(Pass測項:13/13)
  - 測試結果符合預期

Mobile Broadband Networklab, NCU

分享器測試紀錄
HiNet 光世代 PPPoE環境



5

D-Link DIR-1960 PPPoE 測項1

✓ 確認分享器PPPoE撥接正常

網際網路

網路連線類型: PPPoE
網際網路狀態: CONNECTED
連線時間: 0 天 0 時 0 分 33 秒

IPv4 / IPv6
廣域網路 IPv6 位址: 2001:B011:6CC0:BAD:9549:E251:A3C3:EE30/64
預設閘道器: FE80::D2F0:DBFF:FE53:800
主要 DNS 伺服器: 2001:B000:168::2
輔助 DNS 伺服器: 2001:B000:168::1

前往設定頁面

Mobile Broadband Networklab, NCU

D-Link DIR-1960 PPPoE 測項2

✓ 確認分享器IPv6、IPv6 PD、DNSv6取得正常



D-Link DIR-1960 PPPoE 測項3

✓ 確認用戶IPv6、DNSv6取得正常

```
乙太網路卡 乙太網路:

   連線特定 DNS 尾碼 . . . . . . . . :
   描述 . . . . . . . . . . . . . . : Realtek PCIe FE Family Controller
   實體位址 . . . . . . . . . . . . : 6C-2B-59-56-E5-DB
   DHCP 已啟用 . . . . . . . . . . . : 是
   自動設定啟用 . . . . . . . . . . . : 是
   IPv6 位址. . . . . . . . . . . . : 2001:b011:6cc0:1649:1089:df90:502:6cf9(偏好選項)
   IPv6 位址. . . . . . . . . . . . : 2001:b011:6cc0:3752:1089:df90:502:6cf9(偏好選項)
   臨時 IPv6 位址. . . . . . . . . . : 2001:b011:6cc0:1649:d814:4103:cd41:df1f(偏好選項)
   臨時 IPv6 位址. . . . . . . . . . : 2001:b011:6cc0:3752:d814:4103:cd41:df1f(偏好選項)
   連結-本機 IPv6 位址 . . . . . . . : fe80::1089:df90:502:6cf9%8(偏好選項)
   IPv4 位址 . . . . . . . . . . . . : 192.168.0.154(偏好選項)
   子網路遮罩 . . . . . . . . . . . : 255.255.255.0
   租用取得 . . . . . . . . . . . . : 2019年8月22日 下午 02:54:06
   租用到期 . . . . . . . . . . . . : 2019年8月29日 下午 02:54:06
   預設閘道 . . . . . . . . . . . . : fe80::eead:e0ff:fe2e:86e6%8
                                       192.168.0.1
   DHCP 伺服器 . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 72632336
   DHCPv6 用戶端 DUID. . . . . . . . : 00-01-00-01-24-92-58-57-6C-2B-59-56-E5-DB
   DNS 伺服器 . . . . . . . . . . . : 192.168.0.1
                                       2001:b000:168::2
                                       2001:b000:168::1
   NetBIOS over Tcpip . . . . . . . . 啟用
```

D-Link DIR-1960 PPPoE 測項4

✓ 確認用戶至HiNet路由正常

```
C:\Users\User>ping dns.hinet.net

Ping dns.hinet.net [2001:b000:168::2] (使用 32 位元組的資料):
回覆自 2001:b000:168::2: 時間=11ms
回覆自 2001:b000:168::2: 時間=11ms
回覆自 2001:b000:168::2: 時間=10ms
回覆自 2001:b000:168::2: 時間=10ms

2001:b000:168::2 的 Ping 統計資料:
    封包: 已傳送 = 4，已收到 = 4，已遺失 = 0 (0% 遺失)，
大約的來回時間 (毫秒):
    最小值 = 10ms，最大值 = 11ms，平均 = 10ms

C:\Users\User>tracert dns.hinet.net

在上限 30 個躍點上
追蹤 dns.hinet.net [2001:b000:168::2] 的路由:

  1    <1 ms    <1 ms    <1 ms  2001-b011-6cc0-1649-eead-e0ff-fe2e-86e6.dynamic-ip6.hinet.net [2001:b011:6cc0:1649:eead:e0ff:fe2e:86e6]
  2    11 ms    10 ms    11 ms  2001:b010:ffff::1
  3    11 ms    11 ms     9 ms  2001-b000-0089-0005-0021-2222-0002-0002.hinet-ip6.hinet.net [2001:b000:89:5:21:2222:2:2]
  4     *        *        *     要求等候逾時。
  5    13 ms    14 ms    13 ms  2001-b000-0080-0004-3021-3011-0001-000b.hinet-ip6.hinet.net [2001:b000:80:4:3021:3011:1:b]
  6    15 ms    15 ms    17 ms  2001-b000-0080-0004-3021-3011-0001-000b.hinet-ip6.hinet.net [2001:b000:80:4:3021:3011:1:b]
  7    10 ms    11 ms    11 ms  2001-b000-0080-0004-3011-3312-0012-000b.hinet-ip6.hinet.net [2001:b000:80:4:3011:3312:12:b]
  8    11 ms    10 ms    11 ms  2001-b000-0080-0006-3312-0000-0003-0001.hinet-ip6.hinet.net [2001:b000:80:6:3312:0:3:1]
  9    11 ms    11 ms    11 ms  dns.hinet.net [2001:b000:168::2]

追蹤完成。
```

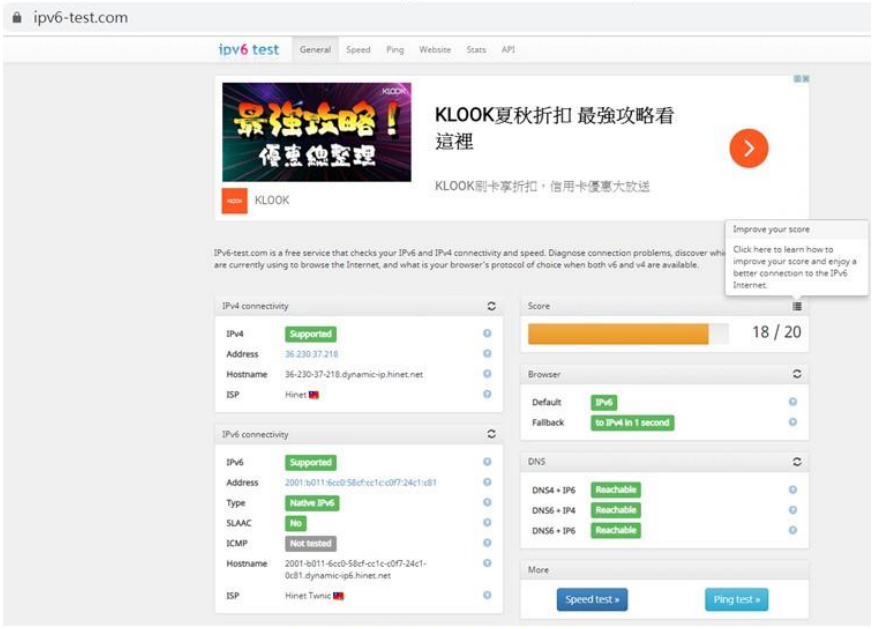

D-Link DIR-1960 PPPoE 測項5

✓ 確認用戶IPv6上網正常(test-ipv6.com)



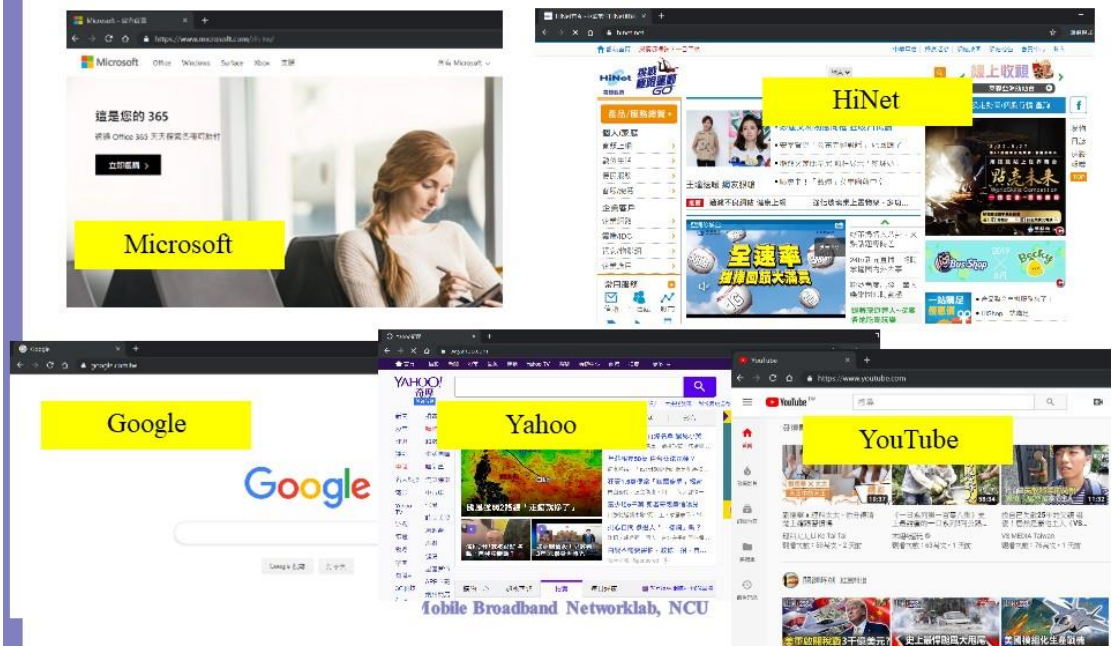
D-Link DIR-1960 PPPoE 測項5(續)

✓ 確認用戶IPv6上網正常(ipv6-test.com)



D-Link DIR-1960 PPPoE 測項6

✓ 確認用戶熱門網頁開啟正常



D-Link DIR-1960 PPPoE 測項7

✓ 確認用戶上網速率正常



D-Link DIR-1960 PPPoE 測項8

✓ 確認分享器重撥，用戶IPv6更新正常

測試你的 IPv6 連線。 分享器重撥之前



測試你的 IPv6 連線。 分享器重撥之後



D-Link DIR-1960 PPPoE 測項9

- ✓ 確認用戶使用IPv6之MTU
  - 乙太網路介面之MTU為1500非1492

```
C:\Users\User>netsh interface ipv6 show subinterface

   MTU  MediaSenseState   接收的位元組 傳送的位元組 介面
------  ---------------  --------- ---------  -------------
4294967295                1         0     329145  Loopback Pseudo-Interface 1
  1500                2   1220727     347728  Wi-Fi
  1500                1   6316735     667336  乙太網路
  1500                5         0        152  區域連線* 1
  1500                5         0        152  藍牙網路連線
  1500                5         0        152  區域連線* 2
  1500                1         0     150526  VirtualBox Host-Only Network
  1500                1         0      65912  Npcap Loopback Adapter
```


D-Link DIR-1960 PPPoE 測項10

- ✓ 確認用戶連接Wi-Fi上網IPv6、DNSv6正常

```
無線區域網路介面卡 Wi-Fi:

   連線特定 DNS 尾碼 . . . . . . . . :
   描述 . . . . . . . . . . . . . . : Intel(R) Wireless-AC 9462
   實體位址 . . . . . . . . . . . . : D8-F2-CA-70-16-24
   DHCP 已啟用 . . . . . . . . . . . : 是
   自動設定啟用 . . . . . . . . . . . : 是
   IPv6 位址. . . . . . . . . . . . : 2001:b011:6cc0:14f6:9d13:fcbc:8da3:a687(偏好選項)
   臨時 IPv6 位址. . . . . . . . . . : 2001:b011:6cc0:14f6:f4f1:ad1f:dfb1:80d1(偏好選項)
   連結-本機 IPv6 位址 . . . . . . . : fe80::9d13:fcbc:8da3:a687%9(偏好選項)
   IPv4 位址 . . . . . . . . . . . . : 192.168.0.182(偏好選項)
   子網路遮罩 . . . . . . . . . . . : 255.255.255.0
   租用取得 . . . . . . . . . . . . : 2019年8月22日 下午 03:45:14
   租用到期 . . . . . . . . . . . . : 2019年8月29日 下午 03:45:14
   預設閘道 . . . . . . . . . . . . : fe80::eead:e0ff:fe2e:86e6%9
                                      192.168.0.1
   DHCP 伺服器 . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 114881226
   DHCPv6 用戶端 DUID. . . . . . . . : 00-01-00-01-24-92-58-57-6C-2B-59-56-E5-DB
   DNS 伺服器 . . . . . . . . . . . : 2001:b000:168::2
                                      2001:b000:168::1
                                      192.168.0.1
   NetBIOS over Tcpip . . . . . . . : 啟用
```

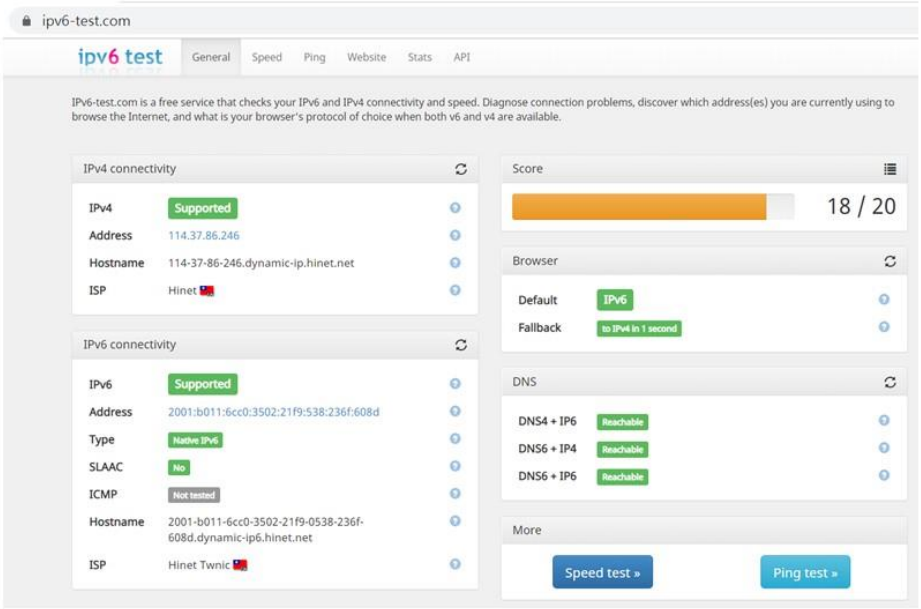
D-Link DIR-1960 PPPoE 測項11

✓ 確認用戶連接Wi-Fi IPv6上網正常(test-ipv6.com)



D-Link DIR-1960 PPPoE 測項11(續)

✓ 確認用戶連接Wi-Fi IPv6上網正常(ipv6-test.com)



D-Link DIR-1960 PPPoE 測項12

- ✓ IPv6 PPPoE (或是PPPoEv6)是否隨著IPv4 PPPoE啟用而自動啟用
  - IPv6 連線功能隨著IPv4啟用而自動啟用



D-Link DIR-1960 PPPoE 測項13

- ✓ IPv6 PPPoE (或是PPPoEv6)連線之PPPoE Session是『Share with IPv4』或是『Create a new Session』?



D-Link DIR-1960 PPPoE 測項13 (續)



D-Link DIR-1960 PPPoE 測項14

- ✓ IPv6寬頻分享器IPv6 ACL功能是否正常?
  - □ 測試寬頻分享器 IPv6 ACL功能是否能限制用戶終端IPv6連線



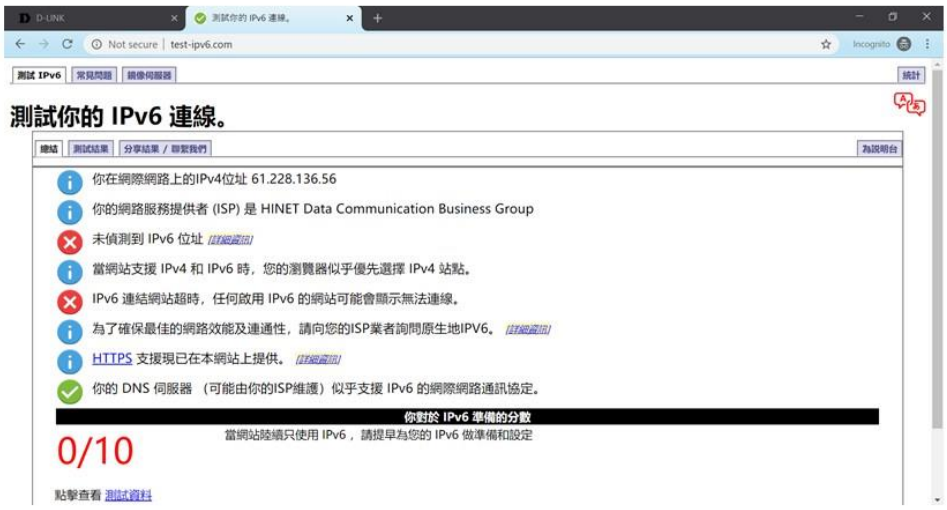
D-Link DIR-1960 PPPoE 測項14 (續)

- ✓ IPv6寬頻分享器IPv6 ACL功能是否正常?
  - 測試寬頻分享器 IPv6 ACL功能是否能限制用戶終端IPv6連線



D-Link DIR-1960 PPPoE 測項14 (續)

- ✓ IPv6寬頻分享器IPv6 ACL功能是否正常?
  - 測試寬頻分享器 IPv6 ACL功能是否能限制用戶終端IPv6連線



分享器測試紀錄
Cable 寬頻 IPoE環境



D-Link DIR-1960 CM 測項1

✓ 確認連接cable modem正常

網際網路

IPv4 / IPv6

網路連線類型: 自動設定 (SLAAC/DHCPv6)

網際網路狀態: CONNECTED

連線時間: 0 天 0 時 1 分 34 秒

釋放

廣域網路 IPv6 位址: 2405:9200:1125::B/128

預設閘道器: FE80::201:5CFF:FEA1:1646

主要 DNS 伺服器: 2404::1

輔助 DNS 伺服器: 2001:4860:4860::8888

前往設定頁面

Mobile Broadband Networklab, NCU

D-Link DIR-1960 CM 測項2

✓ 確認取得IPv6、IPv6 PD、DNSv6

LAN端位址資訊

IPv6 網路

Link-Local 位址: FE80::EEAD:E0FF:FE2E:86E6

路由器 IPv6 位址: 2405:9200:1110:17:EEAD:E0FF:FE2E:86E6

DHCP-PD: 啟用

配置的網段: 2405:9200:1110:17::/64

前往設定頁面

網際網路

WAN端位址資訊

IPv4 / IPv6

網路連線類型: 自動設定 (SLAAC/DHCPv6)

網際網路狀態: CONNECTED

連線時間: 0 天 0 時 1 分 34 秒

釋放

廣域網路 IPv6 位址: 2405:9200:1125::B/128

預設閘道器: FE80::201:5CFF:FEA1:1646

主要 DNS 伺服器: 2404::1

輔助 DNS 伺服器: 2001:4860:4860::8888

前往設定頁面

D-Link DIR-1960 CM 測項3

✓ 確認用戶IPv6、DNSv6取得正常

```
乙太網路卡 乙太網路:

   連線特定 DNS 尾碼 . . . . . . . . :
   描述 . . . . . . . . . . . . . . . : Realtek PCIe FE Family Controller
   實體位址 . . . . . . . . . . . . . : 6C-2B-59-56-E5-DB
   DHCP 已啟用 . . . . . . . . . . . : 是
   自動設定啟用 . . . . . . . . . . . : 是
   IPv6 位址. . . . . . . . . . . . . : 2405:9200:1110:17:1089:df90:502:6cf9(偏好選項)
   臨時 IPv6 位址. . . . . . . . . . . : 2405:9200:1110:17:544f:f70a:41e3:277b(偏好選項)
   連結-本機 IPv6 位址 . . . . . . . . : fe80::1089:df90:502:6cf9%6(偏好選項)
   IPv4 位址 . . . . . . . . . . . . . : 192.168.0.154(偏好選項)
   子網路遮罩 . . . . . . . . . . . . : 255.255.255.0
   租用取得 . . . . . . . . . . . . . : 2019年8月19日 下午 02:14:51
   租用到期 . . . . . . . . . . . . . : 2019年8月26日 下午 02:20:35
   預設閘道 . . . . . . . . . . . . . : fe80::eead:e0ff:fe2e:86e6%6
                                        192.168.0.1
   DHCP 伺服器 . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 72632336
   DHCPv6 用戶端 DUID. . . . . . . . : 00-01-00-01-24-92-58-57-6C-2B-59-56-E5-DB
   DNS 伺服器 . . . . . . . . . . . . : 2404::1
                                        2001:4860:4860::8888
                                        2001:b000:168::1
                                        192.168.0.1
   NetBIOS over Tcpip . . . . . . . . : 啟用
```

D-Link DIR-1960 CM 測項4

✓ 確認用戶至google ipv6路由正常

```
C:\Users\User>tracert ipv6.google.com

在上限 30 個躍點上
追蹤 ipv6.l.google.com [2404:6800:4008:801::200e] 的路由:

  1     1 ms     1 ms     1 ms  2405:9200:1110:17:eead:e0ff:fe2e:86e6
  2     *        *        *     要求等候逾時。
  3     9 ms     8 ms     8 ms  2405:9200:1:0:172:16:28:177a
  4    14 ms     9 ms    10 ms  2405:9200:1:0:172:16:31:18a
  5    11 ms    11 ms     9 ms  2404:0:10ff:1:7709:13:1596:712
  6    10 ms     9 ms    11 ms  2404:0:10ff::5:66
  7    10 ms    11 ms    10 ms  2404:0:10ff:1:7709:1:5169:61
  8    10 ms    11 ms    10 ms  2001:4860:0:1011::1
  9    11 ms    11 ms    10 ms  2001:4860:0:1::1e9f
 10    10 ms    10 ms    19 ms  tsa01s08-in-x0e.1e100.net [2404:6800:4008:801::200e]

追蹤完成。

C:\Users\User>ping ipv6.google.com

Ping ipv6.l.google.com [2404:6800:4008:801::200e] (使用 32 位元組的資料):
回覆自 2404:6800:4008:801::200e: 時間=10ms
回覆自 2404:6800:4008:801::200e: 時間=10ms
回覆自 2404:6800:4008:801::200e: 時間=10ms
回覆自 2404:6800:4008:801::200e: 時間=12ms

2404:6800:4008:801::200e 的 Ping 統計資料:
    封包: 已傳送 = 4，已收到 = 4，已遺失 = 0 (0% 遺失)，
大約的來回時間 (毫秒):
    最小值 = 10ms，最大值 = 12ms，平均 = 10ms
```

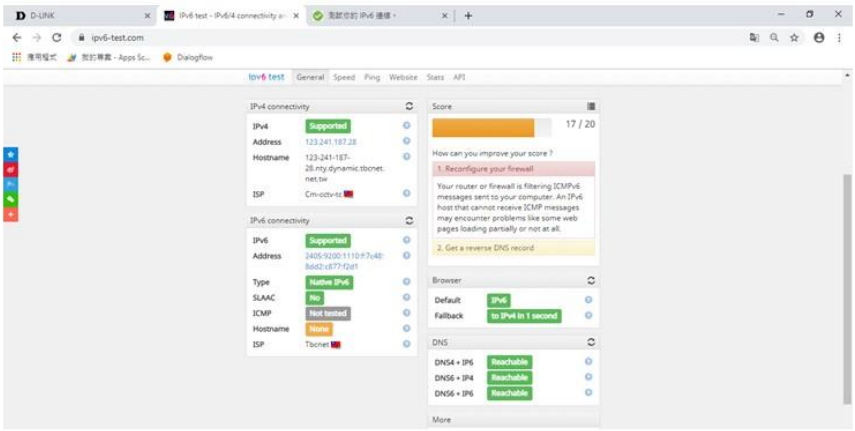

D-Link DIR-1960 CM 測項5

✓ 確認用戶IPv6上網正常(test-ipv6.com)



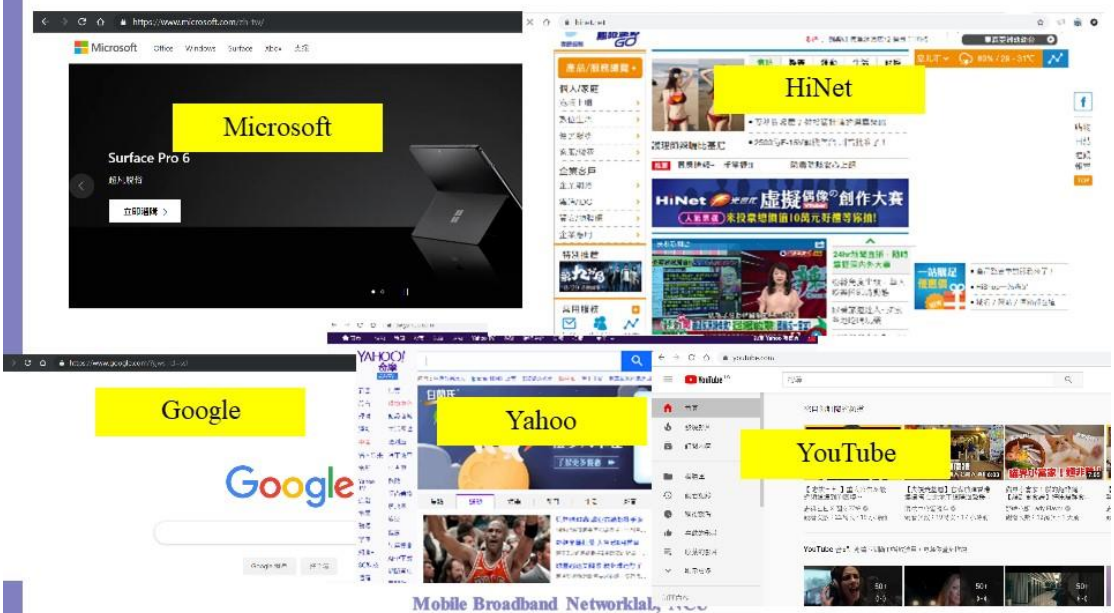
D-Link DIR-1960 CM 測項5(續)

✓ 確認用戶IPv6上網正常(ipv6-test.com)



D-Link DIR-1960 CM 測項6

✓ 確認用戶熱門網頁開啟正常



D-Link DIR-1960 CM 測項7

✓ 確認用戶上網速率正常



D-Link DIR-1960 CM 測項8

✓ 確認分享器重新連接cable modem之後，用戶ipv6相同，且連線正常

測試你的 IPv6 連線。

分享器重接CM前



測試你的 IPv6 連線。

分享器重接CM後



D-Link DIR-1960 CM 測項9

✓ 確認用戶使用IPv6乙太網路介面之MTU為1500

```
C:\Users\User>netsh interface ipv6 show subinterface

   MTU  MediaSenseState   接收的位元組 傳送的位元組 介面
------  ---------------  --------- --------- -------------
4294967295                1         0      25595  Loopback Pseudo-Interface 1
  1500                2     14362      65607  Wi-Fi
  1500                1  28471570    1700560  乙太網路
  1500                5         0        152  區域連線* 1
  1500                5         0        587  藍牙網路連線
  1500                5         0        152  區域連線* 2
  1500                1         0     133974  VirtualBox Host-Only Network
  1500                1         0      79723  Npcap Loopback Adapter
```


D-Link DIR-1960 CM 測項10

✓ 確認用戶連接Wi-Fi上網IPv6、DNSv6正常

```
無線區域網路介面卡 Wi-Fi:

   連線特定 DNS 尾碼 . . . . . . . . :
   描述 . . . . . . . . . . . . . . : Intel(R) Wireless-AC 9462
   實體位址 . . . . . . . . . . . . : D8-F2-CA-70-16-24
   DHCP 已啟用 . . . . . . . . . . . : 是
   自動設定啟用 . . . . . . . . . . . : 是
   IPv6 位址. . . . . . . . . . . . : 2405:9200:1110:17:9d13:fcbc:8da3:a687(偏好選項)
   臨時 IPv6 位址. . . . . . . . . . : 2405:9200:1110:17:564:ecaa:2c14:a497(偏好選項)
   連結-本機 IPv6 位址 . . . . . . . : fe80::9d13:fcbc:8da3:a687%7(偏好選項)
   IPv4 位址 . . . . . . . . . . . . : 192.168.0.182(偏好選項)
   子網路遮罩 . . . . . . . . . . . : 255.255.255.0
   租用取得 . . . . . . . . . . . . : 2019年8月19日 下午 02:44:36
   租用到期 . . . . . . . . . . . . : 2019年8月26日 下午 02:44:36
   預設閘道 . . . . . . . . . . . . : fe80::eead:e0ff:fe2e:86e6%7
                                       192.168.0.1
   DHCP 伺服器 . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 114881226
   DHCPv6 用戶端 DUID. . . . . . . . : 00-01-00-01-24-92-58-57-6C-2B-59-56-E5-DB
   DNS 伺服器 . . . . . . . . . . . : 2404::1
                                       2001:4860:4860::8888
                                       2001:b000:168::1
                                       192.168.0.1
   NetBIOS over Tcpip . . . . . . . : 啟用
```

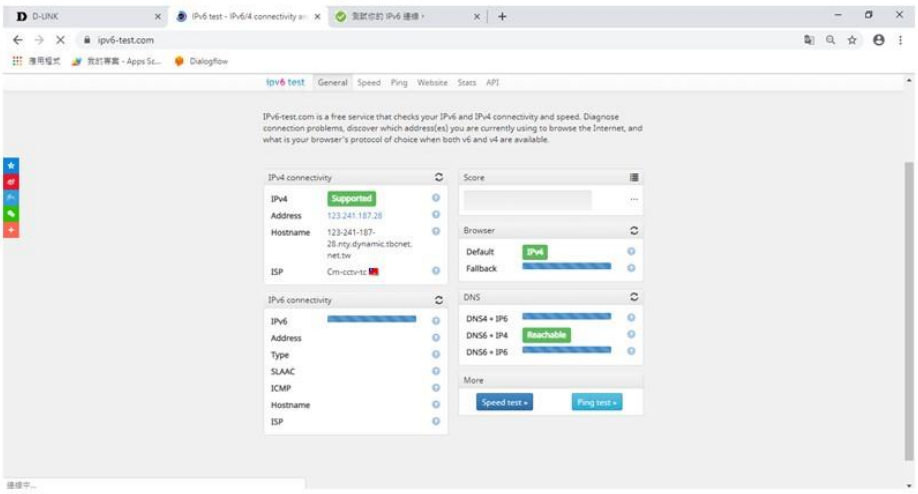
D-Link DIR-1960 CM 測項11

✓ 確認用戶連接Wi-Fi IPv6上網正常(test-ipv6.com)



D-Link DIR-1960 CM 測項11(續)

✓ 確認用戶連接Wi-Fi IPv6上網正常(ipv6-test.com)



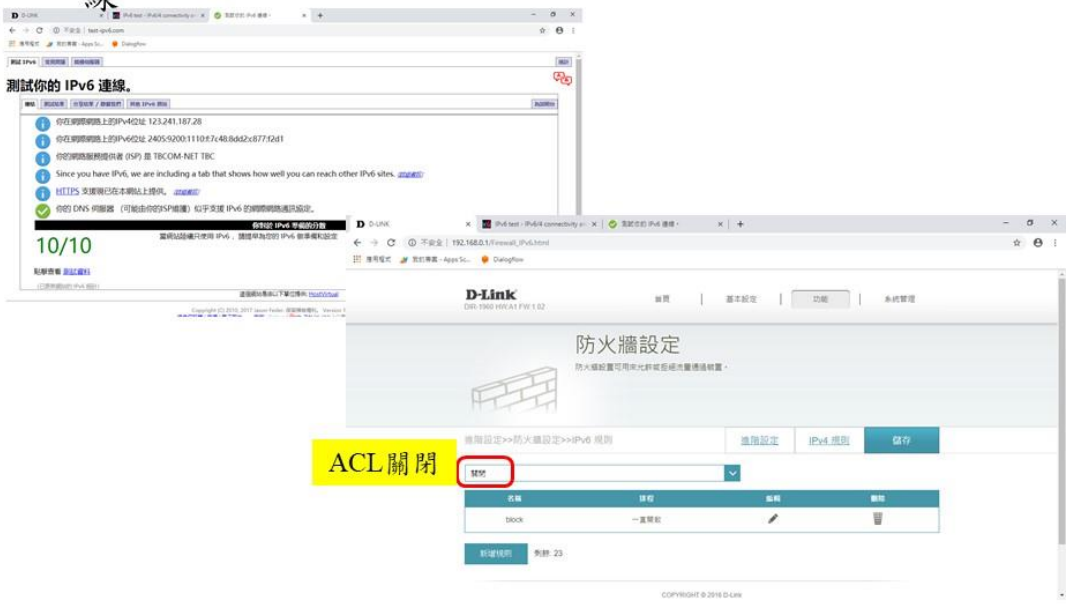
D-Link DIR-1960 CM 測項12

- ✓ 確認IPv6 連線功能隨著IPv4啟用而自動啟用
  - ✓ 重設分享器後，經快速精靈設定，IPv6會自動啟用



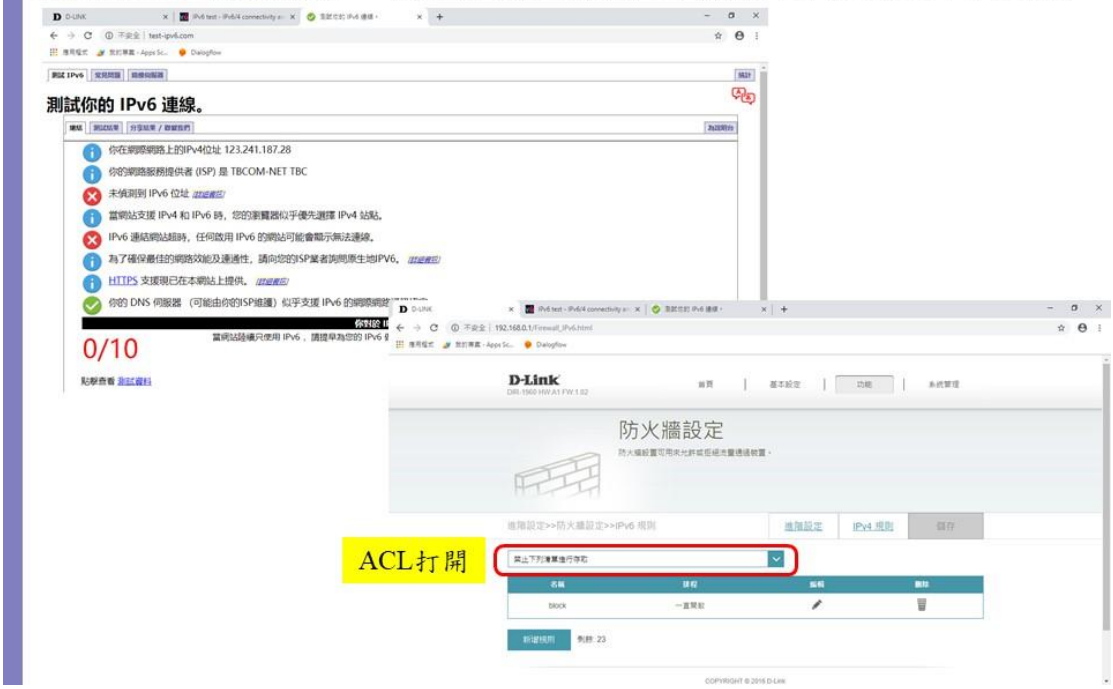
D-Link DIR-1960 CM 測項13

- ✓ IPv6寬頻分享器IPv6 ACL功能是否正常?
  - □ 測試寬頻分享器 IPv6 ACL功能是否能限制用戶終端IPv6連線



D-Link DIR-1960 CM 測項13(續)

啟用ACL功能後，被設定阻擋的主機無法取得IPv6位址



D-Link DIR-2680

分享器測試成果

測試設備與環境

分享器產品設備資訊	
產品型號	DIR-2680
產品名稱	D-Fend防禦型AC2600無線路由器
硬體版本	A1
韌體版本	1.00
製造年份	2018

測試環境資訊	
測試環境	1.HiNet光世代 PPPoE
	2.Cable IPoE
測試終端	Windows 10
終端瀏覽器	Chrome
測試時間	2019-08~2019-10



測試紀錄摘要

HiNet 光世代PPPoE測試		
	測試項目	DIR-2680
1	分享器PPPoE撥接是否正常?	O
2	分享器IPv6、IPv6 PD、DNSv6取得是否正常?	O
3	用戶IPv6、DNSv6取得是否正常?	O
4	用戶至HiNet路由是否正常?	O
5	用戶IPv6上網是否正常?	O
6	用戶熱門網頁開啟是否正常?	O
7	用戶上網速率是否正常?	O
8	分享器重撥，用戶IPv6更新是否正常?	O
9	用戶使用IPv6之MTU是否正常?	1492
10	用戶連接Wi-Fi上網IPv6、DNSv6是否正常?	O
11	用戶連接Wi-Fi IPv6上網是否正常?	O
12	IPv6 PPPoE（或是PPPoEv6)是否隨著IPv4 PPPoE啟用而自動啟用?	O
13	IPv6 PPPoE（或是PPPoEv6)連線之PPPoE Session是『Share with IPv4』或是『Create a new Session』?	可設定兩種模式
14	IPv6寬頻分享器IPv6 ACL功能是否正常?	O

Cable IPoE測試		
	測試項目	DIR-2680
1	分享器連接Cable Modem是否正常?	O
2	分享器IPv6、IPv6 PD、DNSv6取得是否正常?	O
3	用戶IPv6、DNSv6取得是否正常?	O
4	用戶至Cable業者路由是否正常?	O
5	用戶IPv6上網是否正常?	O
6	用戶熱門網頁開啟是否正常?	O
7	用戶上網速率是否正常?	O
8	分享器重撥Cable Modem，用戶IPv6更新是否正常?	O
9	用戶使用IPv6之MTU是否正常?	1500
10	用戶連接Wi-Fi上網IPv6、DNSv6是否正常?	O
11	用戶連接Wi-Fi IPv6上網是否正常?	O
12	IPv6連線功能是否隨著IPv4啟用而自動啟用?	O
13	IPv6寬頻分享器IPv6 ACL功能是否正常?	O

測試紀錄摘要說明

- ✓ HiNet PPPoE環境 (Pass測項:14/14)
  - 測試結果符合預期

- ✓ Cable IPoE環境(Pass測項:13/13)
  - 測試結果符合預期

分享器測試紀錄
HiNet 光世代 PPPoE環境



D-Link DIR-2680 PPPoE 測項1

✓ 確認分享器PPPoE撥接正常

網際網路

網路連線類型: PPPoE
網際網路狀態: 已連線
連線時間: 0 天 8 時 42 分 6 秒

IPv4 / IPv6
廣域網路 IPv6 位址: 2001:B011:6CC0:29FA:79D0:6490:F971:C2D6
預設閘道器: FE80::D2F0:DBFF:FE53:800
主要 DNS 伺服器: 2001:B000:168::2
輔助 DNS 伺服器: 2001:B000:168::1

前往設定頁面

Mobile Broadband Networklab, NCU

D-Link DIR-2680 PPPoE 測項2

✓ 確認分享器IPv6、IPv6 PD、DNSv6取得正常

IPv6 網路 LAN端位址資訊

Link-Local 位址: FE80::2AD:24FF:FE3F:1E3C
路由器 IPv6 位址: 2001:B011:6CC0:1844:02AD:24FF:FE3F:1E3C
DHCP-PD: 啟用
配置的網段: 2001:B011:6CC0:1844:0000:0000:0000:0000/64

網際網路 WAN端位址資訊

網路連線類型: PPPoE
網際網路狀態: 已連線
連線時間: 0 天 8 時 42 分 6 秒

IPv4 / IPv6
廣域網路 IPv6 位址: 2001:B011:6CC0:29FA:79D0:6490:F971:C2D6
預設閘道器: FE80::D2F0:DBFF:FE53:800
主要 DNS 伺服器: 2001:B000:168::2
輔助 DNS 伺服器: 2001:B000:168::1

前往設定頁面

Mobile Broadband Networklab, NCU

D-Link DIR-2680 PPPoE 測項3

✓ 確認用戶IPv6、DNSv6取得正常

乙太網路卡 乙太網路:

```
   連線特定 DNS 尾碼 . . . . . . . . : tbc.net.tw
   描述 . . . . . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   實體位址 . . . . . . . . . . . . . : 1C-B7-2C-1E-CB-0E
   DHCP 已啟用 . . . . . . . . . . . : 是
   自動設定啟用 . . . . . . . . . . . : 是
   IPv6 位址. . . . . . . . . . . . . : 2001:b011:6cc0:1844:a032:c63b:766e:c8d4(偏好選項)
   臨時 IPv6 位址. . . . . . . . . . . : 2001:b011:6cc0:1844:2ca6:e8b8:e4cb:59b3(偏好選項)
   連結-本機 IPv6 位址 . . . . . . . . : fe80::a032:c63b:766e:c8d4%11(偏好選項)
   IPv4 位址 . . . . . . . . . . . . . : 192.168.0.108(偏好選項)
   子網路遮罩 . . . . . . . . . . . . : 255.255.255.0
   租用取得 . . . . . . . . . . . . . : 2019年8月26日 下午 12:59:44
   租用到期 . . . . . . . . . . . . . : 2019年9月2日 下午 12:59:49
   預設閘道 . . . . . . . . . . . . . : fe80::2ad:24ff:fe3f:1e3c%11
                                        192.168.0.1
   DHCP 伺服器 . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 52213548
   DHCPv6 用戶端 DUID. . . . . . . . : 00-01-00-01-1C-CC-BE-EF-1C-B7-2C-1E-CB-0E
   DNS 伺服器 . . . . . . . . . . . . : fe80::2ad:24ff:fe3f:1e3c%11
                                        192.168.0.1
                                        fe80::2ad:24ff:fe3f:1e3c%11
   NetBIOS over Tcpip . . . . . . . . : 啟用
```


D-Link DIR-2680 PPPoE 測項4

✓ 確認用戶至HiNet路由正常

```
C:\Users\ASUS>ping dns.hinet.net

Ping dns.hinet.net [2001:b000:168::2] (使用 32 位元組的資料):
回覆自 2001:b000:168::2: 時間=11ms
回覆自 2001:b000:168::2: 時間=11ms
回覆自 2001:b000:168::2: 時間=11ms
回覆自 2001:b000:168::2: 時間=10ms

2001:b000:168::2 的 Ping 統計資料:
    封包: 已傳送 = 4，已收到 = 4，已遺失 = 0 (0% 遺失)，
大約的來回時間 (毫秒):
    最小值 = 10ms，最大值 = 11ms，平均 = 10ms

C:\Users\ASUS>tracert dns.hinet.net

在上限 30 個躍點上
追蹤 dns.hinet.net [2001:b000:168::2] 的路由:

  1    <1 ms    <1 ms    <1 ms  2001-b011-6cc0-1844-02ad-24ff-fe3f-1e3c.dynamic-ip6.hinet.net [2001:b011:6cc0:1844:2ad:24ff:fe3f:1e3c]
  2     9 ms    11 ms    10 ms  2001:b010:ffff::1
  3     9 ms     9 ms    10 ms  2001-b000-0089-0005-0021-2222-0002-0002.hinet-ip6.hinet.net [2001:b000:89:5:21:2222:2:2]
  4     *        *       11 ms  2001-b000-0080-0003-0080-0089-0021-000a.hinet-ip6.hinet.net [2001:b000:80:3:80:89:21:a]
  5    14 ms    14 ms    14 ms  2001-b000-0080-0004-3021-3011-0002-000b.hinet-ip6.hinet.net [2001:b000:80:4:3021:3011:2:b]
  6    13 ms    14 ms    14 ms  2001-b000-0080-0004-3021-3011-0002-000b.hinet-ip6.hinet.net [2001:b000:80:4:3021:3011:2:b]
  7    16 ms    11 ms    11 ms  2001-b000-0080-0004-3011-3312-0011-000b.hinet-ip6.hinet.net [2001:b000:80:4:3011:3312:11:b]
  8    11 ms    10 ms    11 ms  2001-b000-0080-0006-3312-0000-0003-0001.hinet-ip6.hinet.net [2001:b000:80:6:3312:0:3:1]
  9    12 ms    11 ms    10 ms  dns.hinet.net [2001:b000:168::2]

追蹤完成。
```

D-Link DIR-2680 PPPoE 測項5

✓ 確認用戶IPv6上網正常(test-ipv6.com)

測試你的 IPv6 連線。

總結 | 測試結果 | 分享結果 / 聯繫我們 | 其他 IPv6 網站

你在網際網路上的IPv4位址 220.137.131.98

你在網際網路上的IPv6位址 2001:b011:6cc0:1844:2ca6:e8b8:e4cb:59b3

你的網路服務提供者 (ISP) 是 HINET Data Communication Business Group

Since you have IPv6, we are including a tab that shows how well you can reach other IPv6 sites. [詳細資訊]

HTTPS 支援現已在本網站上提供。 [詳細資訊]

你的 DNS 伺服器 （可能由你的ISP維護）似乎支援 IPv6 的網際網路通訊協定。

你對於 IPv6 準備的分數

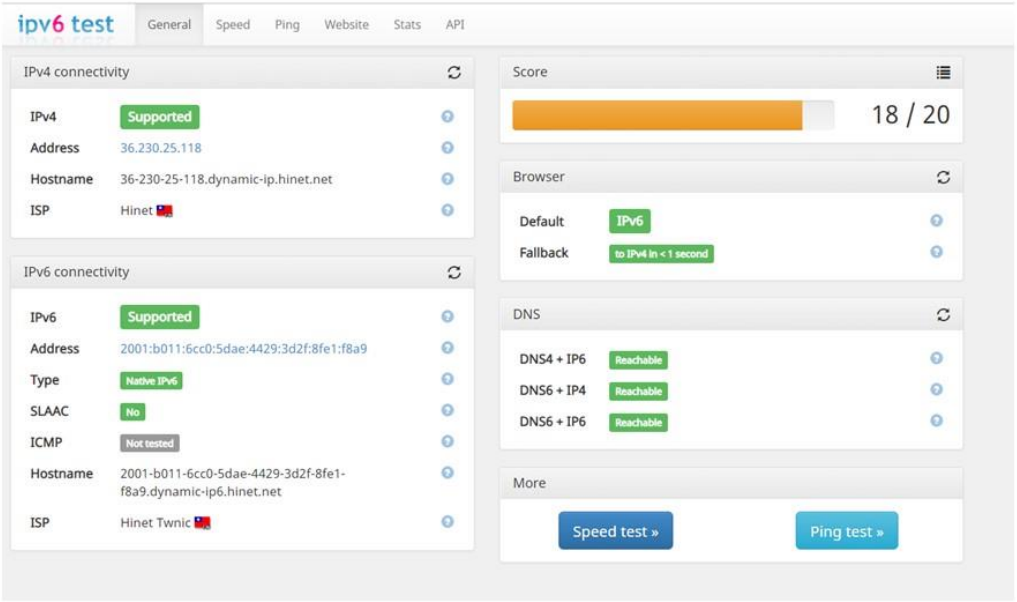
當網站陸續只使用 IPv6， 請提早為您的 IPv6 做準備和設定

10/10

點擊查看 測試資料

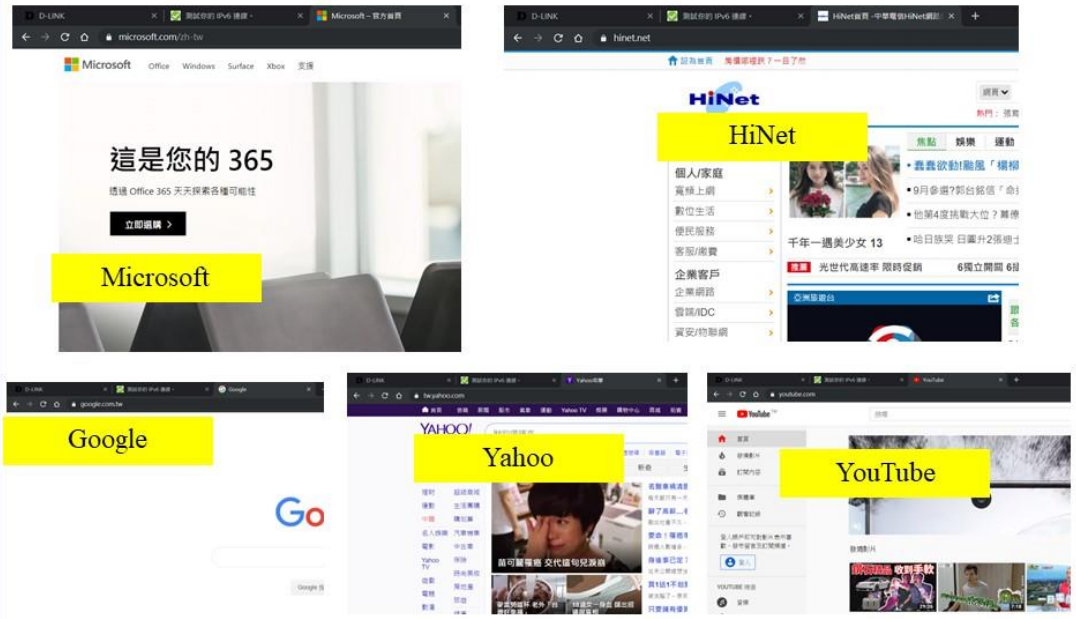
D-Link DIR-2680 PPPoE 測項5(續)

✓ 確認用戶IPv6上網正常(ipv6-test.com)



D-Link DIR-2680 PPPoE 測項6

✓確認用戶熱門網頁開啟正常



D-Link DIR-2680 PPPoE 測項7

✓確認用戶上網速率正常



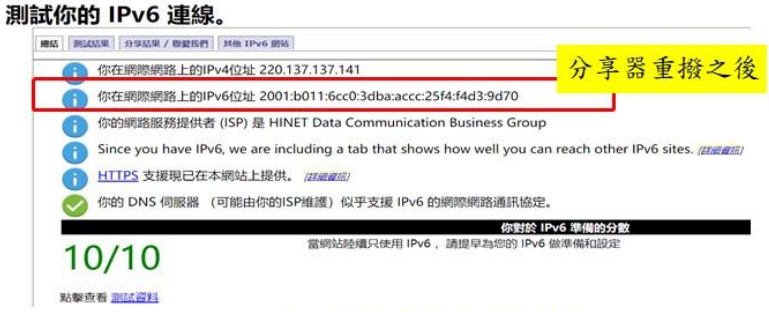
D-Link DIR-2680 PPPoE 測項8

✓ 確認分享器重撥，用戶IPv6更新正常

分享器重撥之前



分享器重撥之後



D-Link DIR-2680 PPPoE 測項9

✓ 確認用戶使用IPv6之乙太網路介面之MTU為1492

```
C:\Users\ASUS>netsh interface ipv6 show subinterface

   MTU  MediaSenseState   接收的位元組  傳送的位元組  介面
------  ---------------  ---------  ---------  -------------
  1492                1   66433076    9223732  乙太網路
4294967295                1          0     386769  Loopback Pseudo-Interface 1
  1500                2   45107764    2083724  Wi-Fi
  1500                5          0        152  區域連線* 2
  1500                5          0        152  區域連線* 4
  1500                5          0        152  Bluetooth 網路連線
```

D-Link DIR-2680 PPPoE 測項10

✓ 確認用戶連接Wi-Fi上網IPv6、DNSv6正常

無線區域網路介面卡 Wi-Fi:

```
   連線特定 DNS 尾碼 . . . . . . . . : tbc.net.tw
   描述 . . . . . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 7265
   實體位址 . . . . . . . . . . . . . : 34-02-86-63-18-11
   DHCP 已啟用 . . . . . . . . . . . : 是
   自動設定啟用 . . . . . . . . . . . : 是
   IPv6 位址. . . . . . . . . . . . . : 2001:b011:6cc0:3dba:80c3:57d2:60e7:e27a(偏好選項)
   臨時 IPv6 位址. . . . . . . . . . . : 2001:b011:6cc0:3dba:fc5f:b7e1:a1eb:c300(偏好選項)
   連結-本機 IPv6 位址 . . . . . . . . : fe80::80c3:57d2:60e7:e27a%8(偏好選項)
   IPv4 位址 . . . . . . . . . . . . . : 192.168.0.109(偏好選項)
   子網路遮罩 . . . . . . . . . . . . : 255.255.255.0
   租用取得 . . . . . . . . . . . . . : 2019年8月26日 下午 01:47:19
   租用到期 . . . . . . . . . . . . . : 2019年9月2日 下午 01:47:16
   預設閘道 . . . . . . . . . . . . . : fe80::2ad:24ff:fe3f:1e3c%8
                                        192.168.0.1
   DHCP 伺服器 . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 120849030
   DHCPv6 用戶端 DUID. . . . . . . . : 00-01-00-01-1C-CC-BE-EF-1C-B7-2C-1E-CB-0E
   DNS 伺服器 . . . . . . . . . . . . : fe80::2ad:24ff:fe3f:1e3c%8
                                        192.168.0.1
   NetBIOS over Tcpip . . . . . . . . : 啟用
```


D-Link DIR-2680 PPPoE 測項11

✓ 確認用戶連接Wi-Fi IPv6上網正常(test-ipv6.com)

測試你的 IPv6 連線。

總結 | 測試結果 | 分享結果 / 聯繫我們 | 其他 IPv6 網站

- 你在網際網路上的IPv4位址 220.137.143.170
- 你在網際網路上的IPv6位址 2001:b011:6cc0:3dba:fc5f:b7e1:a1eb:c300
- 你的網路服務提供者 (ISP) 是 HINET Data Communication Business Group
- Since you have IPv6, we are including a tab that shows how well you can reach other IPv6 sites. [詳細資訊]
- HTTPS 支援現已在本網站上提供。 [詳細資訊]
- 你的 DNS 伺服器 （可能由你的ISP維護）似乎支援 IPv6 的網際網路通訊協定。

你對於 IPv6 準備的分數

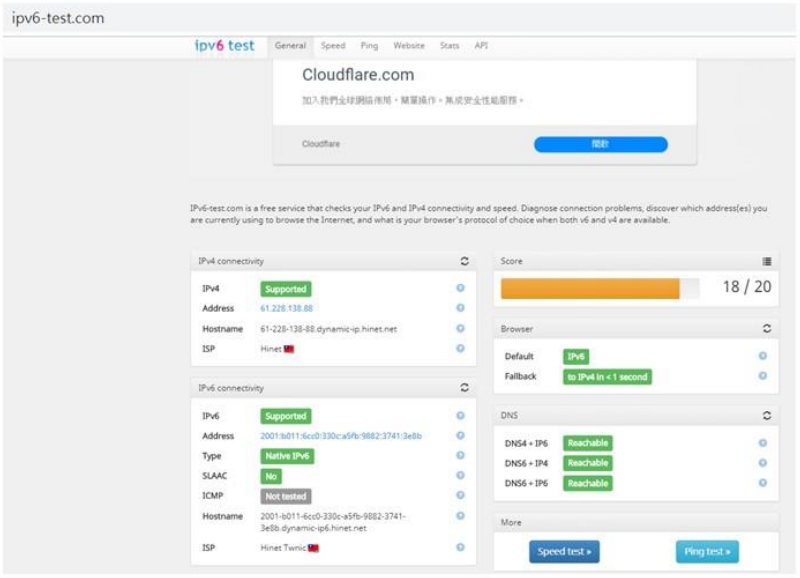
當網站陸續只使用 IPv6，請提早為您的 IPv6 做準備和設定

10/10

點擊查看 測試資料

D-Link DIR-2680 PPPoE 測項11(續)

✓ 確認用戶連接Wi-Fi IPv6上網正常(ipv6-test.com)



D-Link DIR-2680 PPPoE 測項12

✓ IPv6 PPPoE (或是PPPoEv6)是否隨著IPv4 PPPoE啟用而自動啟用

- IPv6 連線功能隨著IPv4啟用而自動啟用



D-Link DIR-2680 PPPoE 測項13

✓ IPv6 PPPoE (或是PPPoEv6)連線之PPPoE Session是『Share with IPv4』或是『Create a new Session』?



D-Link DIR-2680 PPPoE 測項13 (續)



D-Link DIR-2680 PPPoE 測項14

- ✓ IPv6寬頻分享器IPv6 ACL功能是否正常?
  - 測試寬頻分享器 IPv6 ACL功能是否能限制用戶終端IPv6連線



D-Link DIR-2680 PPPoE 測項14(續)

- ✓ 將ACL功能開啟



D-Link DIR-2680 PPPoE 測項14(續)

✓ 啟用ACL功能後，被設定阻擋的主機無法取得IPv6位址

測試你的 IPv6 連線。

總結 | 測試結果 | 分享結果 / 聯繫我們

- 你在網際網路上的IPv4位址 61.228.136.163
- 你的網路服務提供者 (ISP) 是 HINET Data Communication Business Group
- 未偵測到 IPv6 位址 [詳細資訊]
- 當網站支援 IPv4 和 IPv6 時，您的瀏覽器似乎優先選擇 IPv4 站點。
- IPv6 連結網站超時，任何啟用 IPv6 的網站可能會顯示無法連線。
- 為了確保最佳的網路效能及連通性，請向您的ISP業者詢問原生地IPV6。 [詳細資訊]
- HTTPS 支援現已在本網站上提供。 [詳細資訊]
- 你的 DNS 伺服器 （可能由你的ISP維護）似乎支援 IPv6 的網際網路通訊協定。

你對於 IPv6 準備的分數

0/10

當網站陸續只使用 IPv6，請提早為您的 IPv6 做準備和設定

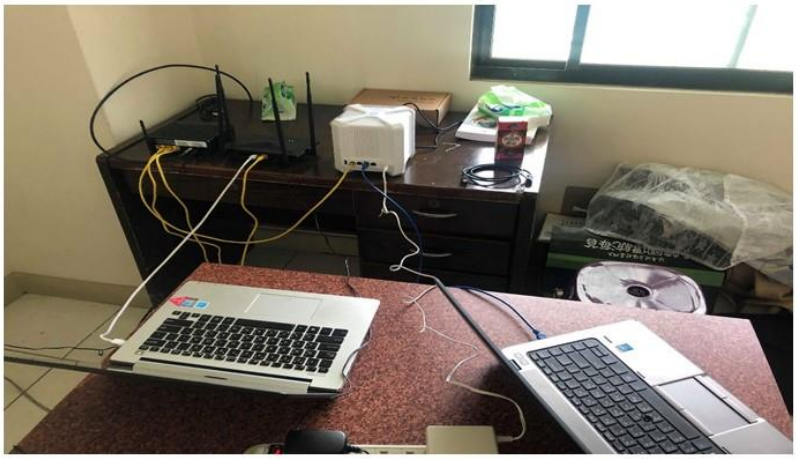
點擊查看 測試資料

(已更新網站的 IPv6 統計)

這個網站是由以下單位提供: HostVirtual

Mobile Broadband Networklab, NCU

分享器測試紀錄
Cable 寬頻 IPoE環境



25

D-Link DIR-2680 CM 測項1

✓ 確認連接cable modem正常



D-Link DIR-2680 CM 測項2

✓ 確認取得IPv6、IPv6 PD、DNSv6



D-Link DIR-2680 CM 測項3

✓ 確認用戶IPv6、DNSv6取得正常

```
乙太網路卡 乙太網路:

   連線特定 DNS 尾碼 . . . . . . . . : tbc.net.tw
   描述 . . . . . . . . . . . . . . . : Realtek PCIe FE Family Controller
   實體位址 . . . . . . . . . . . . . : 6C-2B-59-56-E5-DB
   DHCP 已啟用 . . . . . . . . . . . : 是
   自動設定啟用 . . . . . . . . . . . : 是
   IPv6 位址. . . . . . . . . . . . . : 2405:9200:1110:1b:1089:df90:502:6cf9(偏好選項)
   臨時 IPv6 位址. . . . . . . . . . . : 2405:9200:1110:1b:a920:6d06:52b9:e318(偏好選項)
   連結-本機 IPv6 位址 . . . . . . . . : fe80::1089:df90:502:6cf9%8(偏好選項)
   IPv4 位址 . . . . . . . . . . . . . : 192.168.0.120(偏好選項)
   子網路遮罩 . . . . . . . . . . . . : 255.255.255.0
   租用取得 . . . . . . . . . . . . . : 2019年8月20日 下午 02:19:01
   租用到期 . . . . . . . . . . . . . : 2019年8月27日 下午 02:19:00
   預設閘道 . . . . . . . . . . . . . : fe80::2ad:24ff:fe3f:1e3c%8
                                        192.168.0.1
   DHCP 伺服器 . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 72632336
   DHCPv6 用戶端 DUID. . . . . . . . : 00-01-00-01-24-92-58-57-6C-2B-59-56-E5-DB
   DNS 伺服器 . . . . . . . . . . . . : fe80::2ad:24ff:fe3f:1e3c%8
                                        192.168.0.1
   NetBIOS over Tcpip . . . . . . . . : 啟用
   連線特定 DNS 尾碼搜尋清單 :
                                        tbc.net.tw
```

D-Link DIR-2680 CM 測項4

✓ 確認用戶至google ipv6路由正常

```
C:\Users\User>tracert ipv6.google.com

在上限 30 個躍點上
追蹤 ipv6.l.google.com [2404:6800:4008:801::200e] 的路由:

  1     2 ms     1 ms     1 ms  2405:9200:1110:1b:2ad:24ff:fe3f:1e3c
  2     *        *        *     要求等候逾時。
  3    12 ms     9 ms    10 ms  2405:9200:1:0:172:16:28:165a
  4    15 ms    11 ms    13 ms  2405:9200:1:0:172:16:31:6a
  5    12 ms    10 ms    20 ms  2404:0:10ff:1:7709:13:1596:1110
  6    12 ms    11 ms    12 ms  2404:0:10ff::4:166
  7    29 ms    18 ms    10 ms  2404:0:10ff:1:7709:1:5169:61
  8    15 ms    14 ms    16 ms  2001:4860:0:1012::1
  9    14 ms    13 ms    12 ms  2001:4860:0:1::1e9d
 10    13 ms    14 ms    13 ms  tsa01s08-in-x0e.1e100.net [2404:6800:4008:801::200e]

追蹤完成。

C:\Users\User>ping ipv6.google.com

Ping ipv6.l.google.com [2404:6800:4008:801::200e] (使用 32 位元組的資料):
回覆自 2404:6800:4008:801::200e: 時間=11ms
回覆自 2404:6800:4008:801::200e: 時間=12ms
回覆自 2404:6800:4008:801::200e: 時間=13ms
回覆自 2404:6800:4008:801::200e: 時間=15ms

2404:6800:4008:801::200e 的 Ping 統計資料:
    封包: 已傳送 = 4，已收到 = 4, 已遺失 = 0 (0% 遺失)，
大約的來回時間 (毫秒):
    最小值 = 11ms，最大值 = 15ms，平均 = 12ms
```

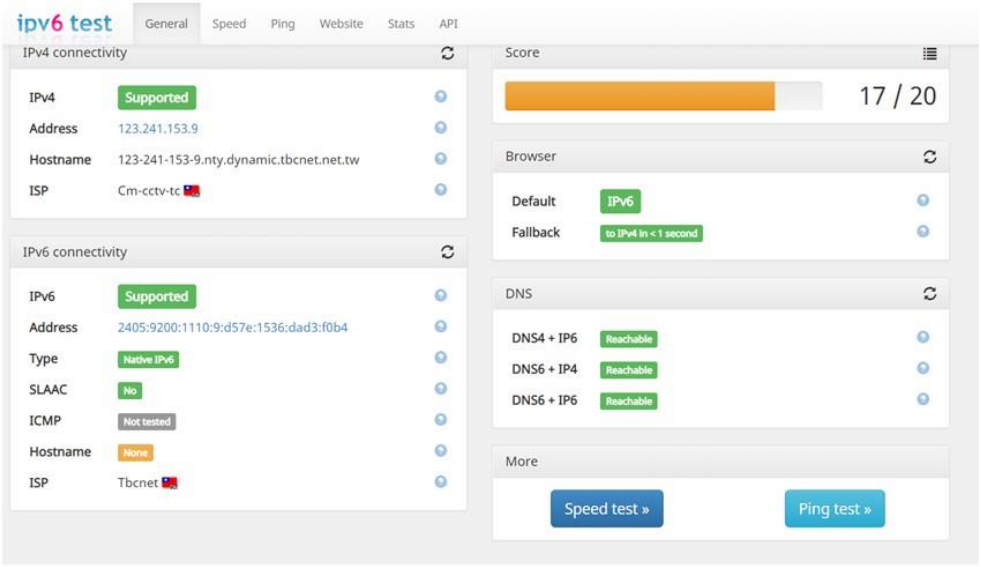
D-Link DIR-2680 CM 測項5

✓ 確認用戶IPv6上網正常(test-ipv6.com)



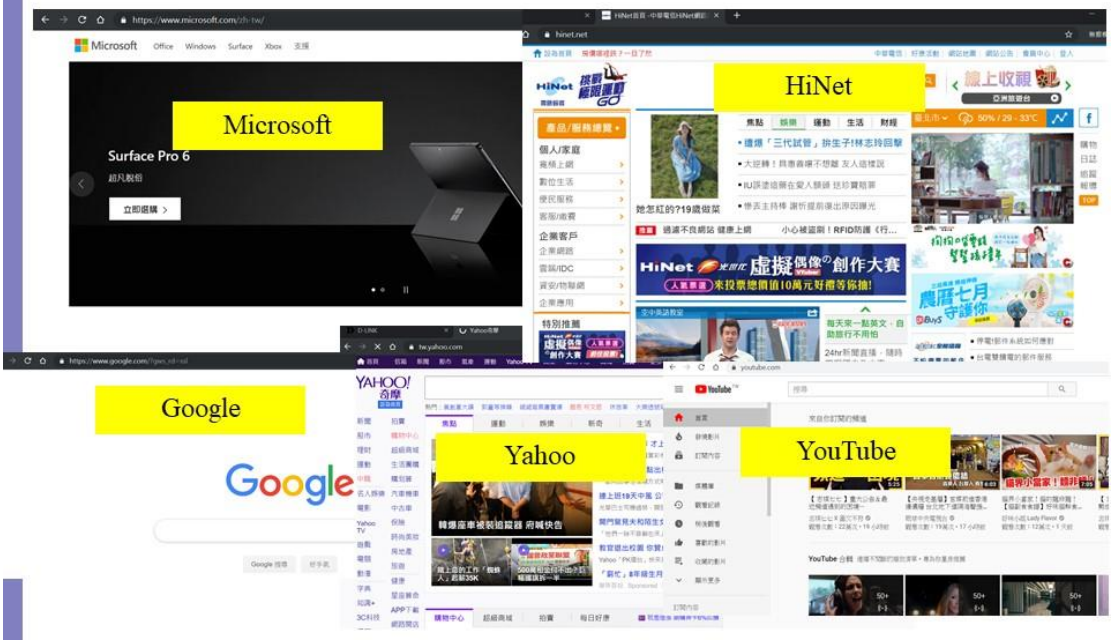
D-Link DIR-2680 CM 測項5(續)

✓ 確認用戶IPv6上網正常(ipv6-test.com)



D-Link DIR-2680 CM 測項6

✓確認用戶熱門網頁開啟正常



D-Link DIR-2680 CM 測項7

✓確認用戶上網速率正常



Mobile Broadband Networklab, NCU

D-Link DIR-2680 CM 測項8

✓ 確認分享器重新連接cable modem之後，用戶ipv6相同，且連線正常

測試你的 IPv6 連線。

分享器重接CM前



測試你的 IPv6 連線。

分享器重接CM後



D-Link DIR-2680 CM 測項9

✓ 確認用戶使用IPv6乙太網路介面之MTU為1500

```
C:\Users\User>netsh interface ipv6 show subinterface

   MTU  MediaSenseState   接收的位元組  傳送的位元組  介面
------  ---------------  ---------  ---------  -------------
4294967295                1          0     400518  Loopback Pseudo-Interface 1
  1500                2   18245222    1906716  Wi-Fi
  1500                1    2601633     608504  乙太網路
  1500                5          0        152  區域連線* 1
  1500                5          0        326  藍牙網路連線
  1500                5          0        152  區域連線* 2
  1500                1       1016     271884  VirtualBox Host-Only Network
  1500                1          0      35742  Npcap Loopback Adapter
```

D-Link DIR-2680 CM 測項10

✓ 確認用戶連接Wi-Fi上網IPv6、DNSv6正常

無線區域網路介面卡 Wi-Fi:

```
   連線特定 DNS 尾碼 . . . . . . . . : tbc.net.tw
   描述 . . . . . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 7265
   實體位址 . . . . . . . . . . . . . : 34-02-86-63-18-11
   DHCP 已啟用 . . . . . . . . . . . : 是
   自動設定啟用 . . . . . . . . . . . : 是
   IPv6 位址. . . . . . . . . . . . . : 2405:9200:1110:1b:80c3:57d2:60e7:e27a(偏好選項)
   臨時 IPv6 位址. . . . . . . . . . . : 2405:9200:1110:1b:d4ad:bd3b:8135:b5f9(偏好選項)
   連結-本機 IPv6 位址 . . . . . . . . : fe80::80c3:57d2:60e7:e27a%8(偏好選項)
   IPv4 位址 . . . . . . . . . . . . . : 192.168.0.173(偏好選項)
   子網路遮罩 . . . . . . . . . . . . : 255.255.255.0
   租用取得 . . . . . . . . . . . . . : 2019年8月20日 下午 03:17:45
   租用到期 . . . . . . . . . . . . . : 2019年8月27日 下午 03:17:45
   預設閘道 . . . . . . . . . . . . . : fe80::2ad:24ff:fe3f:1e3c%8
                                        192.168.0.1
   DHCP 伺服器 . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 120849030
   DHCPv6 用戶端 DUID. . . . . . . . : 00-01-00-01-1C-CC-BE-EF-1C-B7-2C-1E-CB-0E
   DNS 伺服器 . . . . . . . . . . . . : fe80::2ad:24ff:fe3f:1e3c%8
                                        192.168.0.1
   NetBIOS over Tcpip . . . . . . . . : 啟用
   連線特定 DNS 尾碼搜尋清單 :
                                        tbc.net.tw
```

D-Link DIR-2680 CM 測項11

✓ 確認用戶連接Wi-Fi IPv6上網正常(test-ipv6.com)

測試你的 IPv6 連線。

總結 | 測試結果 | 分享結果 / 聯繫我們 | 其他 IPv6 網站

- 你在網際網路上的IPv4位址 123.241.152.22
- 你在網際網路上的IPv6位址 2405:9200:1110:1b:d4ad:bd3b:8135:b5f9
- 你的網路服務提供者 (ISP) 是 TBCOM-NET TBC
- Since you have IPv6, we are including a tab that shows how well you can reach other IPv6 sites. [詳細資訊]
- HTTPS 支援現已在本網站上提供。 [詳細資訊]
- 你的 DNS 伺服器 （可能由你的ISP維護）似乎支援 IPv6 的網際網路通訊協定。

你對於 IPv6 準備的分數

10/10

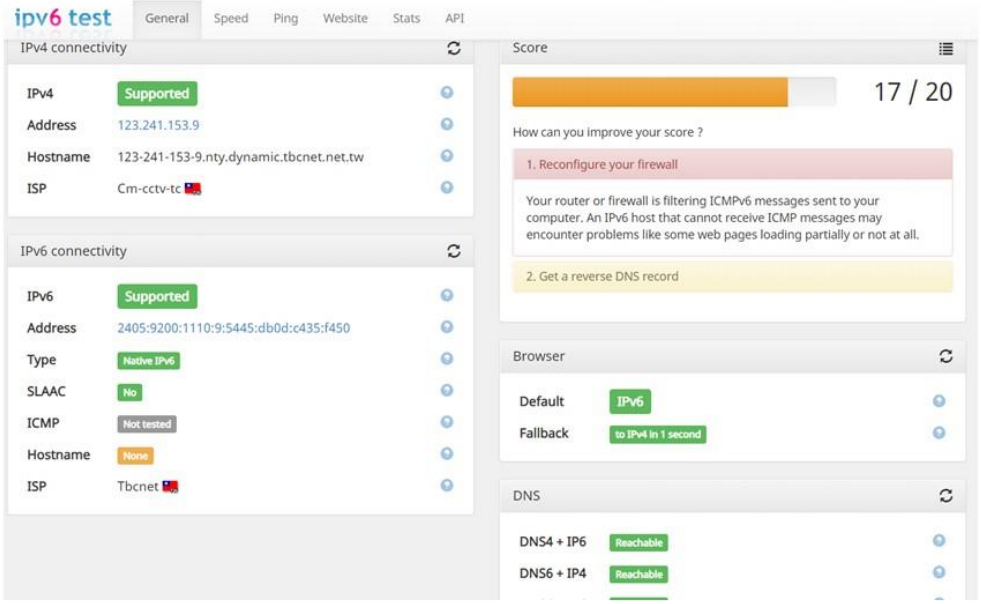
當網站陸續只使用 IPv6， 請提早為您的 IPv6 做準備和設定

點擊查看 測試資料

Mobile Broadband Networklab, NCU

D-Link DIR-2680 CM 測項11(續)

✓ 確認用戶連接Wi-Fi IPv6上網正常(ipv6-test.com)



D-Link DIR-2680 CM 測項12

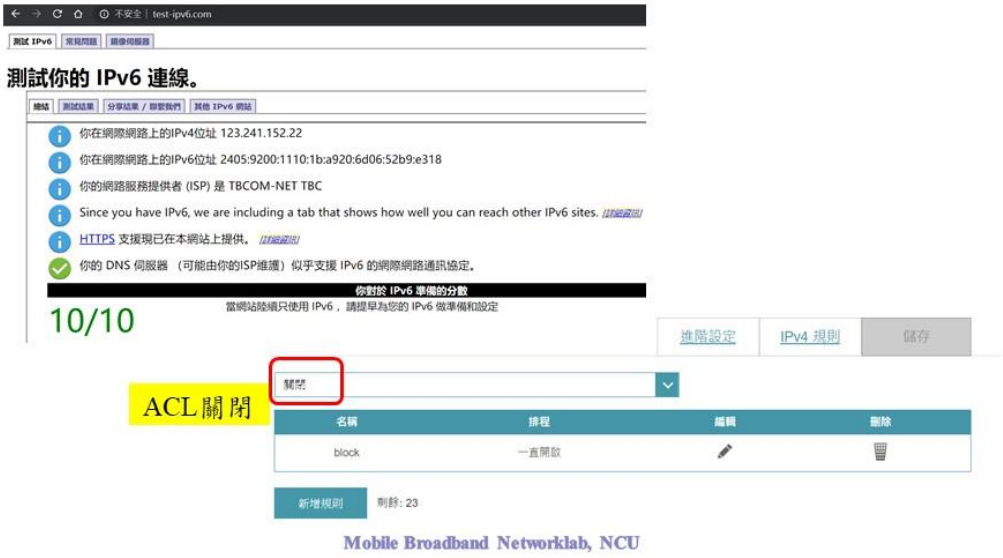
✓ 確認IPv6 連線功能隨著IPv4啟用而自動啟用正常

- 重設分享器後，經快速精靈設定，IPv4啟用後IPv6即自動啟用



D-Link DIR-2680 CM 測項13

- ✓ IPv6寬頻分享器IPv6 ACL功能是否正常?
  - 測試寬頻分享器 IPv6 ACL功能是否能限制用戶終端IPv6連線



D-Link DIR-2680 CM 測項13(續)

- ✓ 啟用ACL功能後，被設定阻擋的主機無法取得IPv6位址



國立中央大學 National Central University

Mobile broadband networklab

ASUS RT-AC66U

分享器測試成果

1

測試設備與環境

分享器產品設備資訊	
產品型號	RT-AC66U
產品名稱	Wireless-AC1750同步雙頻無線分享器
硬體版本	B2
韌體版本	3.0.0.4.384_32738
製造年份	2019

測試環境資訊	
測試環境	1.HiNet光世代 PPPoE
	2.Cable IPoE
測試終端	Windows 10
終端瀏覽器	Chrome
測試時間	2019-08~2019-10



硬體基本資料 出廠年份: 2019年

Mobile Broadband Networklab, NCU

測試紀錄摘要

HiNet 光世代PPPoE測試		
	測試項目	RT-AC66U
1	分享器PPPoE撥接是否正常?	O
2	分享器IPv6、IPv6 PD、DNSv6取得是否正常?	O
3	用戶IPv6、DNSv6取得是否正常?	O
4	用戶至HiNet路由是否正常?	O
5	用戶IPv6上網是否正常?	O
6	用戶熱門網頁開啟是否正常?	O
7	用戶上網速率是否正常?	O
8	分享器重撥，用戶IPv6更新是否正常?	O
9	用戶使用IPv6之MTU是否正常?	1492
10	用戶連接Wi-Fi上網IPv6、DNSv6是否正常?	O
11	用戶連接Wi-Fi IPv6上網是否正常?	O
12	IPv6 PPPoE（或是PPPoEv6)是否隨著IPv4 PPPoE啟用而自動啟用?	X
13	IPv6 PPPoE（或是PPPoEv6)連線之PPPoE Session是『Share with IPv4』或是『Create a new Session』?	無提供此項設定
14	IPv6寬頻分享器IPv6 ACL功能是否正常?	O

Cable IPoE測試		
	測試項目	RT-AC66U
1	分享器連接Cable Modem是否正常?	O
2	分享器IPv6、IPv6 PD、DNSv6取得是否正常?	O
3	用戶IPv6、DNSv6取得是否正常?	O
4	用戶至Cable業者路由是否正常?	O
5	用戶IPv6上網是否正常?	O
6	用戶熱門網頁開啟是否正常?	O
7	用戶上網速率是否正常?	O
8	分享器重撥Cable Modem，用戶IPv6更新是否正常?	O
9	用戶使用IPv6之MTU是否正常?	1500
10	用戶連接Wi-Fi上網IPv6、DNSv6是否正常?	O
11	用戶連接Wi-Fi IPv6上網是否正常?	O
12	IPv6連線功能是否隨著IPv4啟用而自動啟用?	X
14	IPv6寬頻分享器IPv6 ACL功能是否正常?	O

Mobile Broadband Networklab, NCU

測試紀錄摘要說明

- ✓ HiNet PPPoE環境 (Pass測項:12/14)
  - 測項12: 需要手動啟用IPv6
  - 測項13: 無提供此項設定

- ✓ Cable IPoE環境(Pass測項:12/13)
  - 測項12: 需要手動啟用IPv6

Mobile Broadband Networklab, NCU

分享器測試紀錄
HiNet 光世代 PPPoE環境

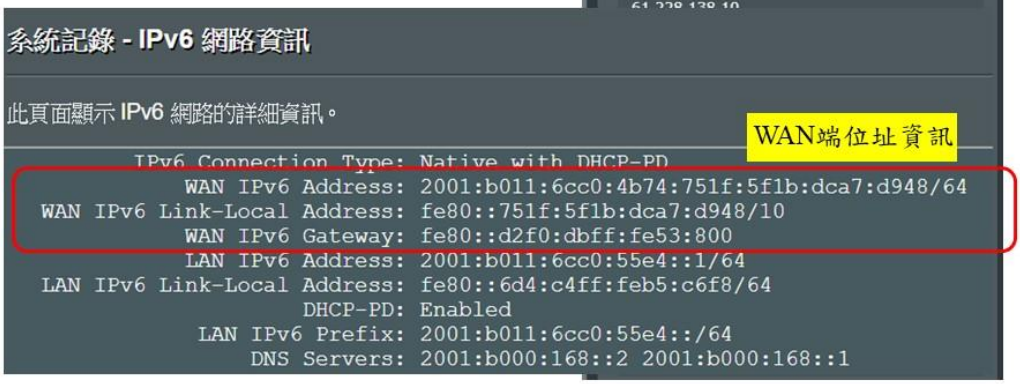


5

ASUS RT-AC66U PPPoE 測項1

✓ 確認分享器PPPoE撥接正常





ASUS RT-AC66U PPPoE 測項2

✓ 確認分享器IPv6、IPv6 PD、DNSv6取得正常

系統記錄 - IPv6 網路資訊

此頁面顯示 IPv6 網路的詳細資訊。

WAN端位址資訊

LAN端位址資訊

```
         IPv6 Connection Type: Native with DHCP-PD
              WAN IPv6 Address: 2001:b011:6cc0:4b74:751f:5f1b:dca7:d948/64
 WAN IPv6 Link-Local Address: fe80::751f:5f1b:dca7:d948/10
              WAN IPv6 Gateway: fe80::d2f0:dbff:fe53:800
              LAN IPv6 Address: 2001:b011:6cc0:55e4::1/64
 LAN IPv6 Link-Local Address: fe80::6d4:c4ff:feb5:c6f8/64
                     DHCP-PD: Enabled
               LAN IPv6 Prefix: 2001:b011:6cc0:55e4::/64
                   DNS Servers: 2001:b000:168::2 2001:b000:168::1
```


ASUS RT-AC66U PPPoE 測項3

✓ 確認用戶IPv6、DNSv6取得正常

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Physical Address. . . . . . . . . : 04-92-26-6E-D1-F8
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:b011:6cc0:55e4:1ce7:3c77:5218:7258(Preferred)
   Temporary IPv6 Address. . . . . . : 2001:b011:6cc0:55e4:a1cf:cb1b:20b8:6738(Preferred)
   Link-local IPv6 Address . . . . . : fe80::1ce7:3c77:5218:7258%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.50.116(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, July 31, 2019 10:13:26 AM
   Lease Expires . . . . . . . . . . : Thursday, August 1, 2019 10:35:07 AM
   Default Gateway . . . . . . . . . : fe80::6d4:c4ff:feb5:c6f8%3
                                       192.168.50.1
   DHCP Server . . . . . . . . . . . : 192.168.50.1
   DHCPv6 IAID . . . . . . . . . . . : 33853990
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-47-2F-7E-04-92-26-6E-D1-F8
   DNS Servers . . . . . . . . . . . : 2001:b011:6cc0:55e4::1
                                       192.168.50.1
                                       2001:b011:6cc0:55e4::1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

ASUS RT-AC66U PPPoE 測項4

✓ 確認用戶至HiNet路由正常

```
C:\Users\Hestia>ping dns.hinet.net

Pinging dns.hinet.net [2001:b000:168::2] with 32 bytes of data:
Reply from 2001:b000:168::2: time=10ms
Reply from 2001:b000:168::2: time=10ms
Reply from 2001:b000:168::2: time=10ms
Reply from 2001:b000:168::2: time=10ms

Ping statistics for 2001:b000:168::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 10ms, Average = 10ms

C:\Users\Hestia>tracert dns.hinet.net

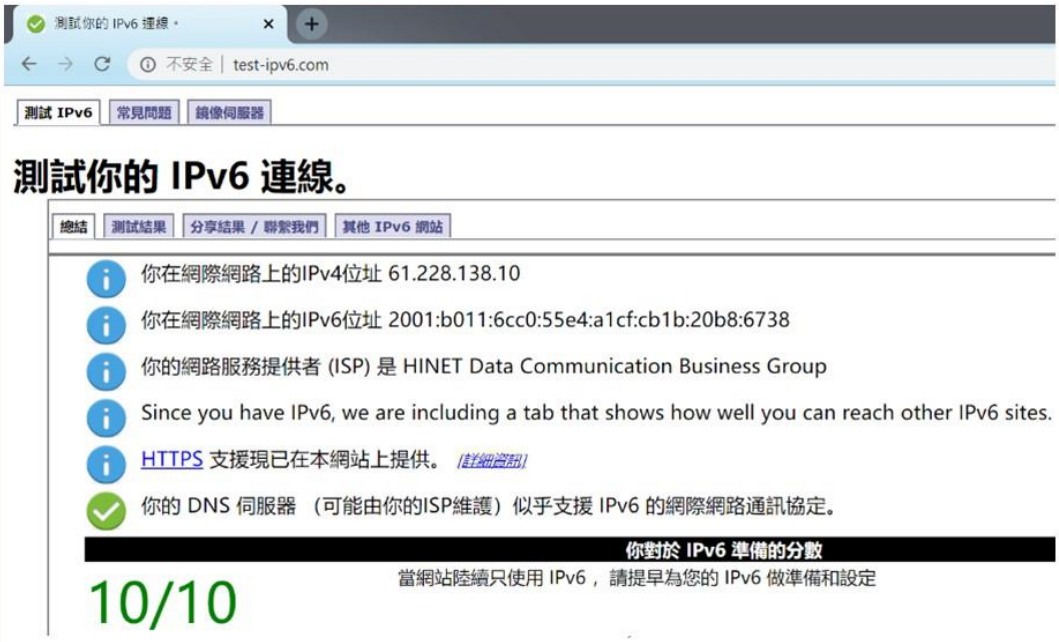
Tracing route to dns.hinet.net [2001:b000:168::2]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  2001-b011-6cc0-55e4-0000-0000-0000-0001.dynamic-ip6.hinet.net [2001:b011:6cc0:55e4::1]
  2    10 ms    10 ms    10 ms  2001:b010:ffff::1
  3    30 ms    10 ms    10 ms  2001-b000-0089-0005-0022-2222-0002-0002.hinet-ip6.hinet.net [2001:b000:89:5:22:2222:2:2]
  4    11 ms     *        *     2001-b000-0080-0003-0080-0089-0022-000a.hinet-ip6.hinet.net [2001:b000:80:3:80:89:22:a]
  5    14 ms    12 ms    10 ms  2001-b000-0080-0004-3022-3012-0005-000b.hinet-ip6.hinet.net [2001:b000:80:4:3022:3012:5:b]
  6    13 ms    10 ms    12 ms  2001-b000-0080-0004-3022-3012-0005-000b.hinet-ip6.hinet.net [2001:b000:80:4:3022:3012:5:b]
  7    10 ms    11 ms    11 ms  2001-b000-0080-0004-3012-3312-0012-000b.hinet-ip6.hinet.net [2001:b000:80:4:3012:3312:12:b]
  8     *        *        *     Request timed out.
  9    10 ms    10 ms    11 ms  dns.hinet.net [2001:b000:168::2]

Trace complete.
```

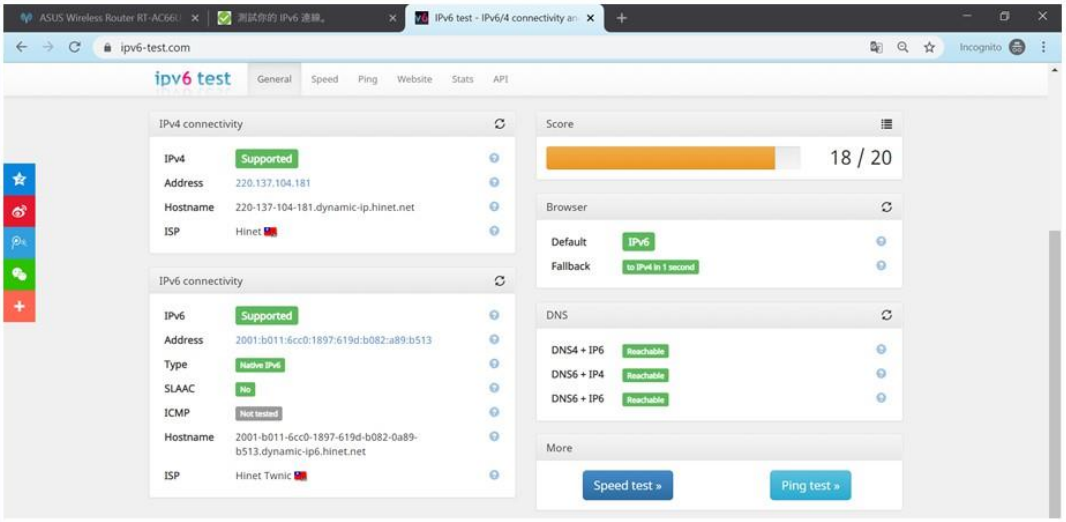

ASUS RT-AC66U PPPoE 測項5

✓ 確認用戶IPv6上網正常(test-ipv6.com)



ASUS RT-AC66U PPPoE 測項5 (續)

✓ 確認用戶IPv6上網正常(ipv6-test.com)



ASUS RT-AC66U PPPoE 測項6

✓ 確認用戶熱門網頁開啟正常



ASUS RT-AC66U PPPoE 測項7

✓ 確認用戶上網速率正常



ASUS RT-AC66U PPPoE 測項8

✓ 確認分享器重撥，用戶IPv6更新正常

測試你的 IPv6 連線。 分享器重撥之前

你在網際網路上的IPv4位址 36.230.24.77

你在網際網路上的IPv6位址 2001:b011:6cc0:564d:5c9d:4c0e:b92c:7e16

你的網路服務提供者 (ISP) 是 HINET Data Communication Business Group

Since you have IPv6, we are including a tab that shows how well you can reach other IPv6 sites.

HTTPS 支援現已在本網站上提供。

你的 DNS 伺服器 （可能由你的ISP維護）似乎支援 IPv6 的網際網路通訊協定。

你對於 IPv6 準備的分數

當網站陸續只使用 IPv6，請提早為您的 IPv6 做準備和設定

10/10

測試你的 IPv6 連線。 分享器重撥之後

你在網際網路上的IPv4位址 220.141.88.237

你在網際網路上的IPv6位址 2001:b011:6cc0:104c:1de0:5d0f:ad1d:316c

你的網路服務提供者 (ISP) 是 HINET Data Communication Business Group

Since you have IPv6, we are including a tab that shows how well you can reach other IPv6 sites.

HTTPS 支援現已在本網站上提供。

你的 DNS 伺服器 （可能由你的ISP維護）似乎支援 IPv6 的網際網路通訊協定。

你對於 IPv6 準備的分數

當網站陸續只使用 IPv6，請提早為您的 IPv6 做準備和設定

10/10

ASUS RT-AC66U PPPoE 測項9

✓ 確認用戶使用IPv6之MTU正常

```
C:\Users\Hestia>netsh interface ipv6 show subinterface

   MTU  MediaSenseState   Bytes In  Bytes Out  Interface
------  ---------------  ---------  ---------  -------------
4294967295                1          0     147661  Loopback Pseudo-Interface 1
  1500                2   11135371     637299  Wi-Fi
  1492                1   63448255   10896949  Ethernet
  1500                5          0       7053  Local Area Connection* 2
  1500                5          0       8306  Bluetooth Network Connection
  1500                5          0       8117  Local Area Connection* 3
  1400                5          0      17085  Local Area Connection* 1
 65536                1          0     160636  Ethernet 2
```


ASUS RT-AC66U PPPoE 測項10

✓ 確認用戶連接Wi-Fi上網IPv6、DNSv6正常

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wireless-AC 9560
   Physical Address. . . . . . . . . : 48-A4-72-42-63-96
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:b011:6cc0:564d:f115:d539:9dc9:ab66(Preferred)
   Temporary IPv6 Address. . . . . . : 2001:b011:6cc0:564d:5c9d:4c0e:b92c:7e16(Preferred)
   Link-local IPv6 Address . . . . . : fe80::f115:d539:9dc9:ab66%13(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.50.49(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, July 31, 2019 11:32:56 AM
   Lease Expires . . . . . . . . . . : Thursday, August 1, 2019 11:33:06 AM
   Default Gateway . . . . . . . . . : fe80::6d4:c4ff:feb5:c6f8%13
                                       192.168.50.1
   DHCP Server . . . . . . . . . . . : 192.168.50.1
   DHCPv6 IAID . . . . . . . . . . . : 222864498
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-47-2F-7E-04-92-26-6E-D1-F8
   DNS Servers . . . . . . . . . . . : 2001:b011:6cc0:564d::1
                                       192.168.50.1
                                       2001:b011:6cc0:564d::1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

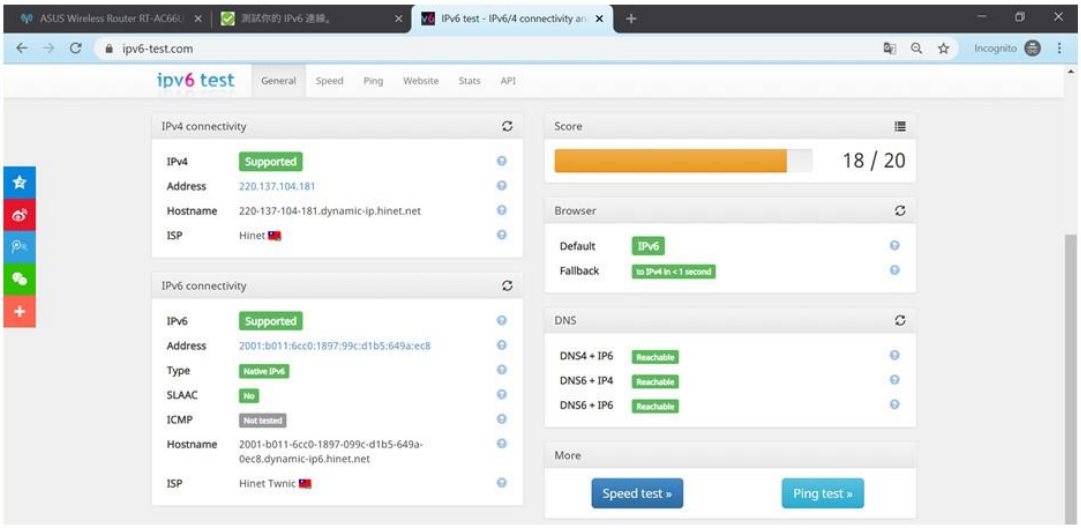
ASUS RT-AC66U PPPoE 測項11

✓ 確認用戶連接Wi-Fi IPv6上網正常(test-ipv6.com)



ASUS RT-AC66U PPPoE 測項11(續)

✓ 確認用戶連接Wi-Fi IPv6上網正常(ipv6-test.com)



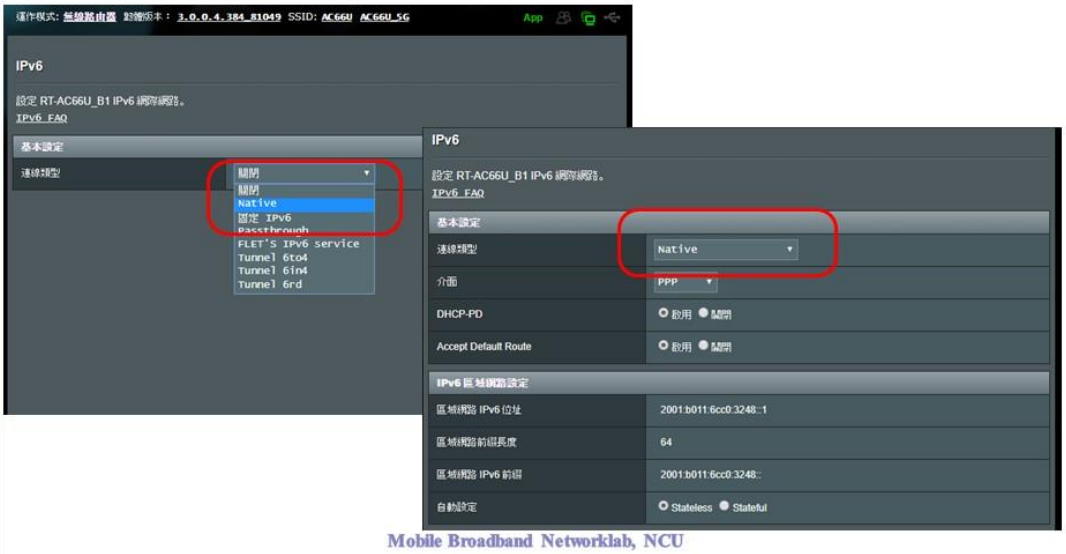
ASUS RT-AC66U PPPoE 測項12

- ✓ IPv6 PPPoE (或是PPPoEv6)是否隨著IPv4 PPPoE啟用而自動啟用
  - 重新Reset分享器後，依照"網路設定精靈操作"，無法直接取得IPv6位址



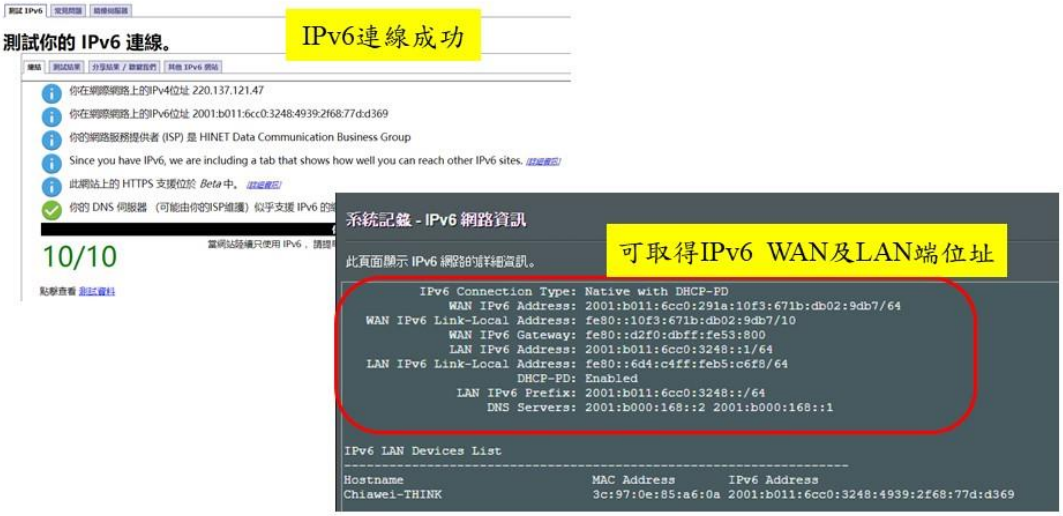
ASUS RT-AC66U PPPoE 測項12(續)

- ✓ IPv6 PPPoE (或是PPPoEv6)是否隨著IPv4 PPPoE啟用而自動啟用
  - 在IPv6設定中開啟IPv6功能，並設定連線類型Native



ASUS RT-AC66U PPPoE 測項12(續)

- ✓ IPv6 PPPoE (或是PPPoEv6)是否隨著IPv4 PPPoE啟用而自動啟用
  - ◻ 設定完啟用IPv6後即可正常連線



ASUS RT-AC66U PPPoE 測項13

- ✓ IPv6 PPPoE (或是PPPoEv6)連線之PPPoE Session是『Share with IPv4』或是『Create a new Session』?

華碩分享器並無提供此項設定

ASUS RT-AC66U PPPoE 測項14

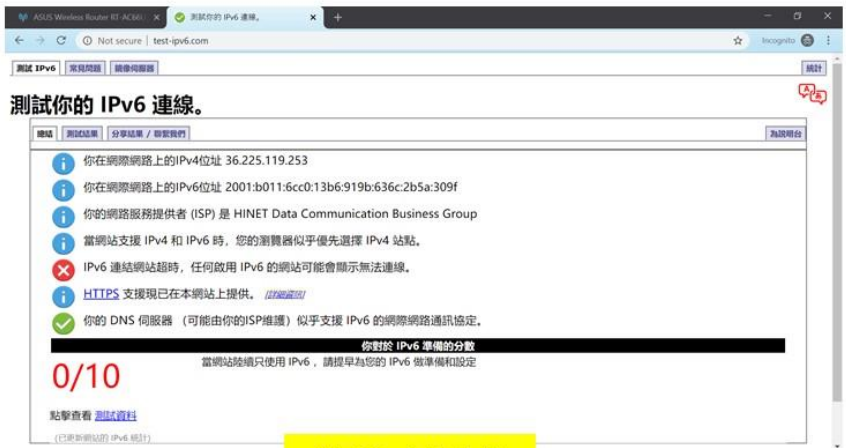
- ✓ IPv6寬頻分享器IPv6 ACL功能是否正常?
  - 測試寬頻分享器 IPv6 ACL功能是否能限制用戶終端IPv6連線





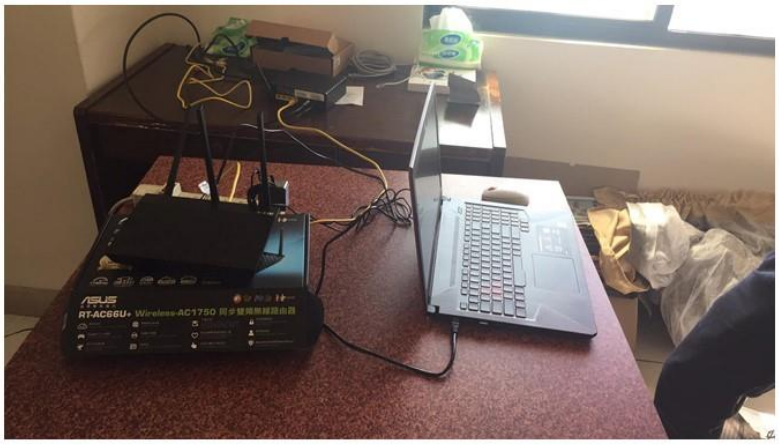
ASUS RT-AC66U PPPoE 測項14(續)

- ✓ IPv6寬頻分享器IPv6 ACL功能是否正常?
  - 測試寬頻分享器 IPv6 ACL功能是否能限制用戶終端IPv6連線





分享器測試紀錄
Cable 寬頻 IPoE環境



ASUS RT-AC66U CM 測項1

✓ 確認連接cable modem正常

系統記錄 - IPv6 網路資訊

此頁面顯示 IPv6 網路的詳細資訊。

```
        IPv6 Connection Type: Native with DHCP-PD
            WAN IPv6 Address: 2405:9200:1125::5
 WAN IPv6 Link-Local Address: fe80::6d4:c4ff:feb5:c6f8/64
            WAN IPv6 Gateway: fe80::201:5cff:fea1:1646
            LAN IPv6 Address: 2405:9200:1110:2::1/64
 LAN IPv6 Link-Local Address: fe80::6d4:c4ff:feb5:c6f8/64
                   DHCP-PD: Enabled
             LAN IPv6 Prefix: 2405:9200:1110:2::/64
                 DNS Servers: 2404::1 2001:4860:4860::8888 2001:b000:168::1
```

ASUS RT-AC66U CM 測項2

✓ 確認取得IPv6、IPv6 PD、DNSv6



ASUS RT-AC66U CM 測項3

✓ 確認用戶IPv6、DNSv6取得正常

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Physical Address. . . . . . . . . : 04-92-26-6E-D1-F8
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2405:9200:1110:2:1ce7:3c77:5218:7258(Preferred)
   Temporary IPv6 Address. . . . . . : 2405:9200:1110:2:8d2b:b5ee:7f6d:9dec(Preferred)
   Link-local IPv6 Address . . . . . : fe80::1ce7:3c77:5218:7258%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.50.116(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, July 31, 2019 3:09:25 PM
   Lease Expires . . . . . . . . . . : Thursday, August 1, 2019 3:09:23 PM
   Default Gateway . . . . . . . . . : fe80::6d4:c4ff:feb5:c6f8%3
                                       192.168.50.1
   DHCP Server . . . . . . . . . . . : 192.168.50.1
   DHCPv6 IAID . . . . . . . . . . . : 33853990
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-47-2F-7E-04-92-26-6E-D1-F8
   DNS Servers . . . . . . . . . . . : 192.168.50.1
                                       2405:9200:1110:2::1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

ASUS RT-AC66U CM 測項4

✓ 確認用戶至google ipv6路由正常

```
C:\Users\Hestia>ping ipv6.google.com

Pinging ipv6.l.google.com [2404:6800:4008:800::200e] with 32 bytes of data:
Reply from 2404:6800:4008:800::200e: time=13ms
Reply from 2404:6800:4008:800::200e: time=12ms
Reply from 2404:6800:4008:800::200e: time=14ms
Reply from 2404:6800:4008:800::200e: time=12ms

Ping statistics for 2404:6800:4008:800::200e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 14ms, Average = 12ms

C:\Users\Hestia>tracert ipv6.google.com

Tracing route to ipv6.l.google.com [2404:6800:4008:800::200e]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  2405:9200:1110:2::1
  2     *        *        *     Request timed out.
  3     8 ms     9 ms     9 ms  2405:9200:1:0:172:16:28:165a
  4    10 ms    11 ms    10 ms  2405:9200:1:0:172:16:31:2a
  5    11 ms    13 ms    18 ms  2404:0:10ff:1:7709:13:1596:710
  6    11 ms     9 ms    15 ms  2404:0:10ff::4:166
  7    12 ms    11 ms    11 ms  2404:0:10ff:1:7709:1:5169:61
  8    11 ms    10 ms    11 ms  2001:4860:0:1011::1
  9    12 ms    11 ms    11 ms  2001:4860:0:1::17c3
 10    11 ms    12 ms    11 ms  tsa01s07-in-x0e.1e100.net [2404:6800:4008:800::200e]

Trace complete.
```

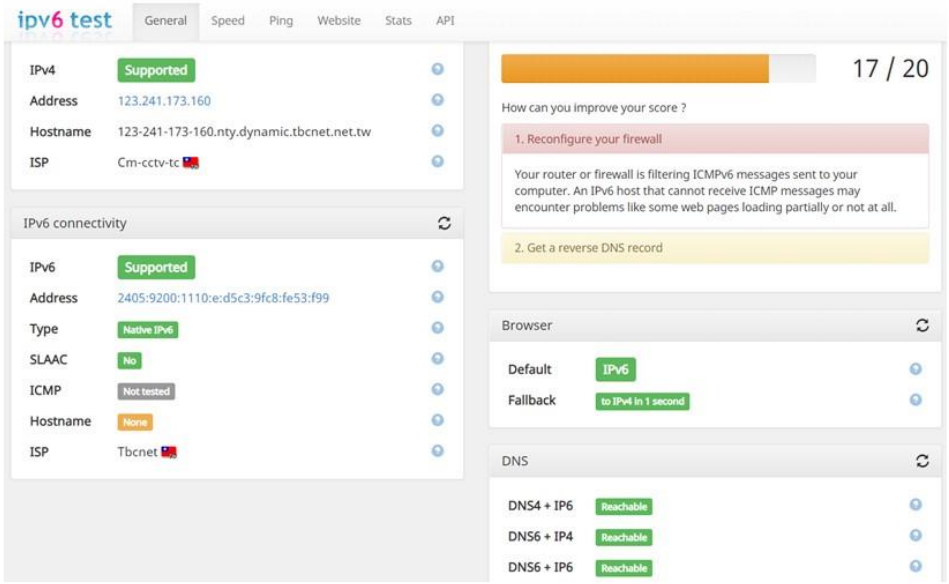
ASUS RT-AC66U CM 測項5

✓ 確認用戶IPv6上網正常(test-ipv6.com)



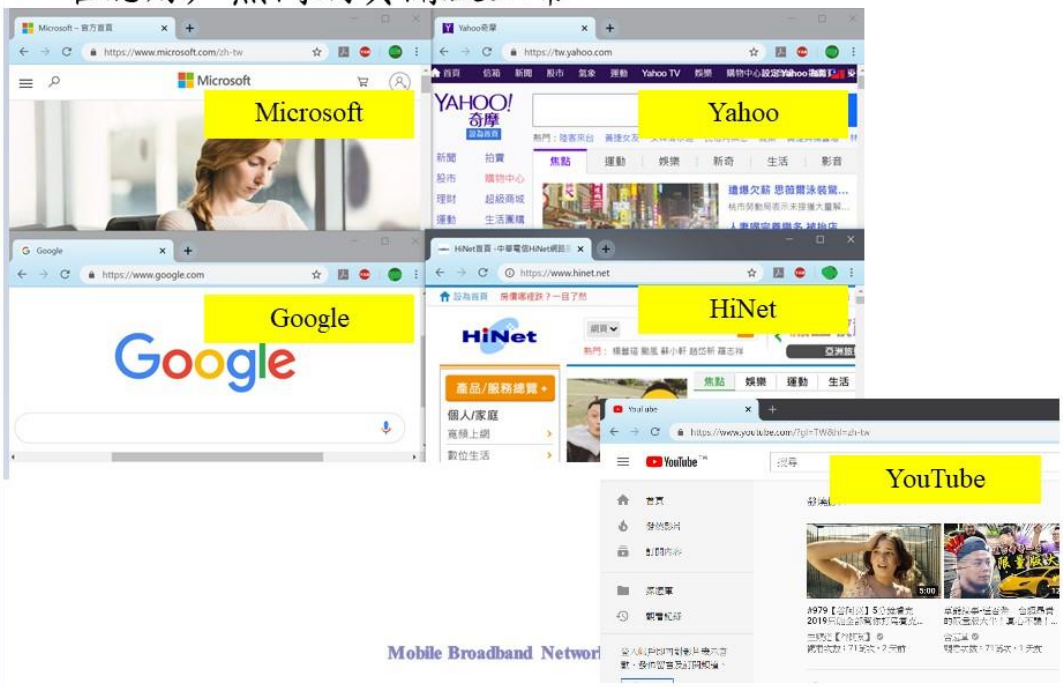
ASUS RT-AC66U CM 測項5(續)

✓ 確認用戶IPv6上網正常(ipv6-test.com)



ASUS RT-AC66U CM 測項6

✓ 確認用戶熱門網頁開啟正常



ASUS RT-AC66U CM 測項7

✓ 確認用戶上網速率正常



ASUS RT-AC66U CM 測項8

✓ 確認分享器重新連接cable modem之後，用戶ipv6相同，且連線正常

測試你的 IPv6 連線。 分享器重接CM前



測試你的 IPv6 連線。 分享器重接CM後



ASUS RT-AC66U CM 測項9

✓ 確認用戶使用IPv6乙太網路介面之MTU為1500非1492

```
C:\Users\Hestia>netsh interface ipv6 show subinterface

   MTU  MediaSenseState   Bytes In  Bytes Out  Interface
------  ---------------  ---------  ---------  -------------
4294967295                1          0     294405  Loopback Pseudo-Interface 1
  1492                2   13995157    1383555  Wi-Fi
  1500                1  375435498   76627769  Ethernet
  1500                5          0       7753  Local Area Connection* 2
  1500                5          0      10786  Bluetooth Network Connection
  1500                5          0       8817  Local Area Connection* 3
  1400                5          0      20021  Local Area Connection* 1
 65536                1          0      63480  Ethernet 2
```


ASUS RT-AC66U CM 測項10

✓ 確認用戶連接Wi-Fi上網IPv6、DNSv6正常

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wireless-AC 9560
   Physical Address. . . . . . . . . : 48-A4-72-42-63-96
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2405:9200:1110:2:f115:d539:9dc9:ab66(Preferred)
   Temporary IPv6 Address. . . . . . : 2405:9200:1110:2:348c:d59c:6734:10aa(Preferred)
   Link-local IPv6 Address . . . . . : fe80::f115:d539:9dc9:ab66%13(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.50.49(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, July 31, 2019 11:32:55 AM
   Lease Expires . . . . . . . . . . : Thursday, August 1, 2019 3:47:50 PM
   Default Gateway . . . . . . . . . : fe80::6d4:c4ff:feb5:c6f8%13
                                       192.168.50.1
   DHCP Server . . . . . . . . . . . : 192.168.50.1
   DHCPv6 IAID . . . . . . . . . . . : 222864498
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-47-2F-7E-04-92-26-6E-D1-F8
   DNS Servers . . . . . . . . . . . : 2405:9200:1110:2::1
                                       192.168.50.1
                                       2405:9200:1110:2::1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

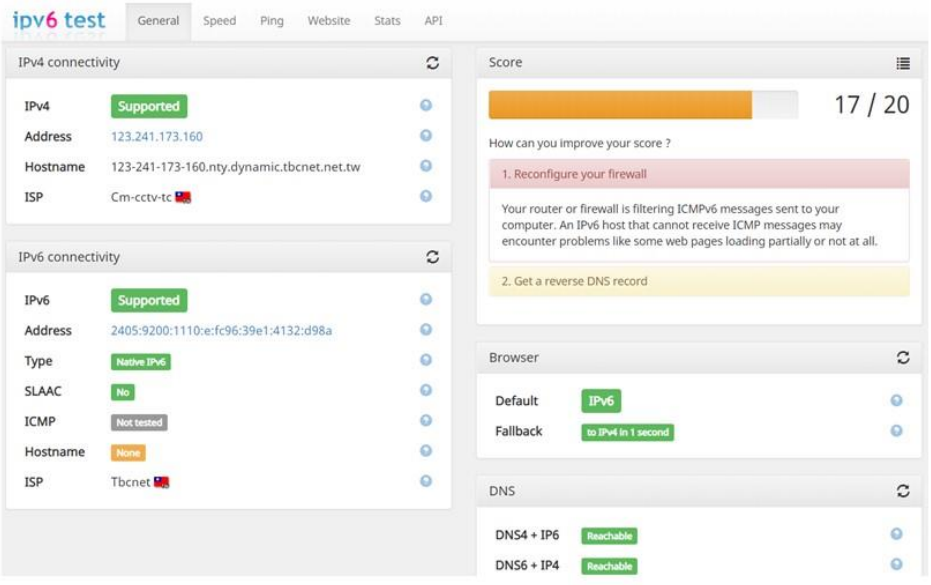
ASUS RT-AC66U CM 測項11

✓ 確認用戶連接Wi-Fi IPv6上網正常(test-ipv6.com)



ASUS RT-AC66U CM 測項11(續)

✓ 確認用戶連接Wi-Fi IPv6上網正常(ipv6-test.com)



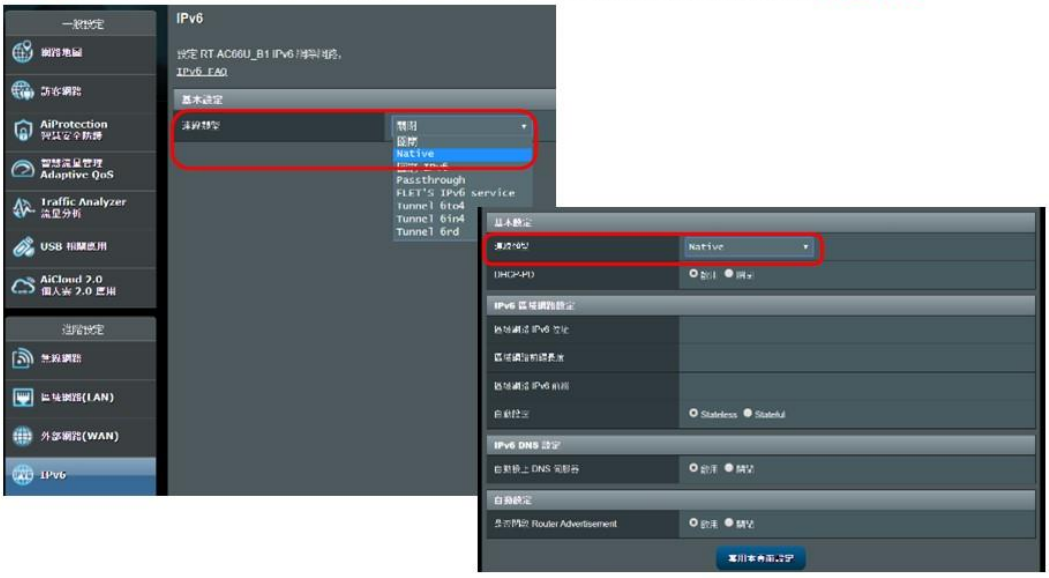
ASUS RT-AC66U CM 測項12

- ✓ 確認IPv6 連線功能隨著IPv4啟用而自動啟用
  - 重新Reset分享器後，依照介面指示設定後，無法使用IPv6



ASUS RT-AC66U CM 測項12 (續)

- ✓ 確認IPv6 連線功能隨著IPv4啟用而自動啟用
  - 在IPv6設定中開啟IPv6功能，並設定連線類型Native



ASUS RT-AC66U CM 測項12 (續)

- ✓ 確認IPv6 連線功能隨著IPv4啟用而自動啟用
  - □ 設定完啟用IPv6後即可正常連線

測試你的 IPv6 連線。



IPv6連線成功



可取得IPv6 WAN及LAN端位址

ASUS RT-AC66U CM 測項13

- ✓ IPv6寬頻分享器IPv6 ACL功能是否正常?
  - □ 測試寬頻分享器 IPv6 ACL功能是否能限制用戶終端IPv6連線

測試你的 IPv6 連線。

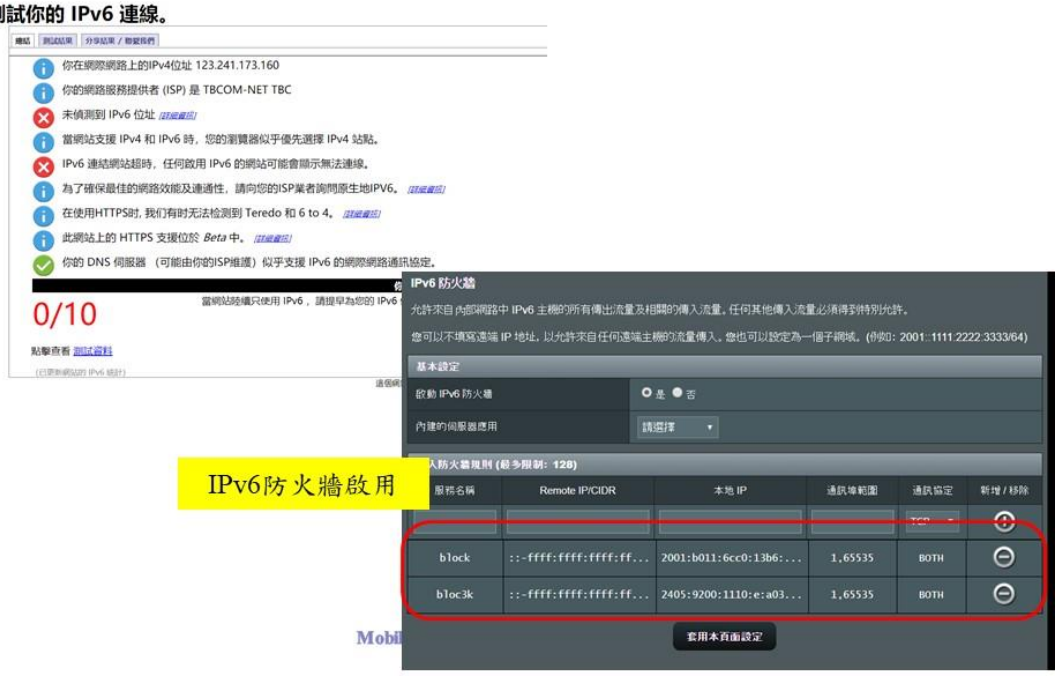


IPv6防火牆關閉



ASUS RT-AC66U CM 測項13(續)

啟用ACL功能後，被設定阻擋的主機無法取得IPv6位址



IPv6防火牆啟用

國立中央大學 National Central University

Mobile broadband networklab

ASUS RT-AC1300UHP

分享器測試成果

測試設備與環境

分享器產品設備資訊	
產品型號	RT-AC1300UHP
產品名稱	Wireless-AC1300UHP同步雙頻無線分享器
硬體版本	B1
韌體版本	3.0.0.4.380.834
製造年份	2019

測試環境資訊	
測試環境	1.HiNet光世代 PPPoE
	2.Cable IPoE
測試終端	Windows 10
終端瀏覽器	Chrome
測試時間	2019-08~2019-10

硬體基本資料



出廠年份:2019年

測試紀錄摘要

HiNet 光世代PPPoE測試		
	測試項目	RT-AC1300UHP
1	分享器PPPoE撥接是否正常?	O
2	分享器IPv6、IPv6 PD、DNSv6取得是否正常?	O
3	用戶IPv6、DNSv6取得是否正常?	O
4	用戶至HiNet路由是否正常?	O
5	用戶IPv6上網是否正常?	O
6	用戶熱門網頁開啟是否正常?	O
7	用戶上網速率是否正常?	O
8	分享器重撥，用戶IPv6更新是否正常?	O
9	用戶使用IPv6之MTU是否正常?	1492
10	用戶連接Wi-Fi上網IPv6、DNSv6是否正常?	O
11	用戶連接Wi-Fi IPv6上網是否正常?	O
12	IPv6 PPPoE（或是PPPoEv6)是否隨著IPv4 PPPoE啟用而自動啟用?	X
13	IPv6 PPPoE（或是PPPoEv6)連線之PPPoE Session是『Share with IPv4』或是『Create a new Session』?	無提供此項設定
14	IPv6寬頻分享器IPv6 ACL功能是否正常?	O

Cable IPoE測試		
	測試項目	RT-AC1300UHP
1	分享器連接Cable Modem是否正常?	O
2	分享器IPv6、IPv6 PD、DNSv6取得是否正常?	O
3	用戶IPv6、DNSv6取得是否正常?	O
4	用戶至Cable業者路由是否正常?	O
5	用戶IPv6上網是否正常?	O
6	用戶熱門網頁開啟是否正常?	O
7	用戶上網速率是否正常?	O
8	分享器重撥Cable Modem，用戶IPv6更新是否正常?	O
9	用戶使用IPv6之MTU是否正常?	1500
10	用戶連接Wi-Fi上網IPv6、DNSv6是否正常?	O
11	用戶連接Wi-Fi IPv6上網是否正常?	O
12	IPv6連線功能是否隨著IPv4啟用而自動啟用?	X
13	IPv6寬頻分享器IPv6 ACL功能是否正常?	O

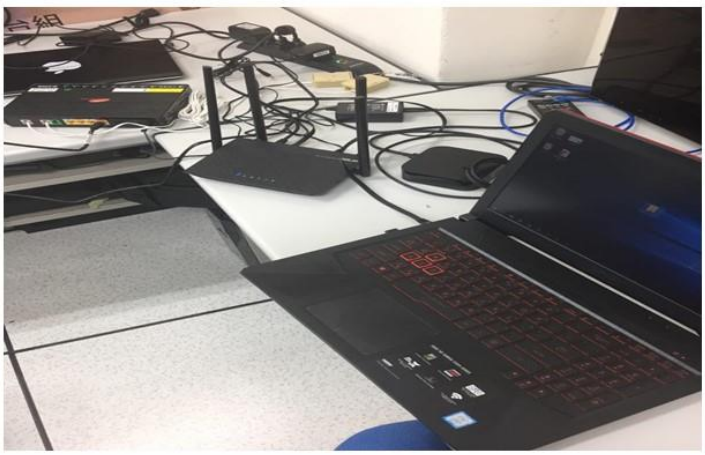
Mobile Broadband Networklab, NCU

測試紀錄摘要說明

- ✓ HiNet PPPoE環境 (Pass測項:12/14)
  - 測項12: 需要手動啟用IPv6
  - 測項13: 無提供此項設定

- ✓ Cable IPoE環境(Pass測項:12/13)
  - 測項12: 需要手動啟用IPv6

分享器測試紀錄
HiNet 光世代 PPPoE環境



ASUS RT-AC1300UHP PPPoE 測項1

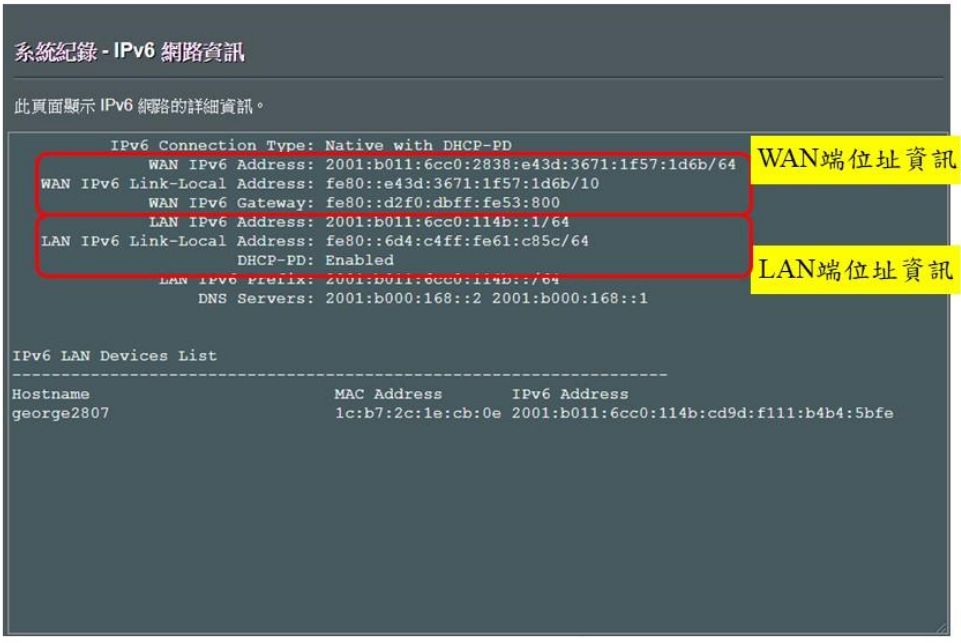
✓ 確認分享器PPPoE撥接正常



Mobile Broadband Networklab, NCU

ASUS RT-AC1300UHP PPPoE 測項2

✓ 確認分享器IPv6、IPv6 PD、DNSv6取得正常



ASUS RT-AC1300UHP PPPoE 測項3

✓ 確認用戶IPv6、DNSv6取得正常

乙太網路卡 乙太網路:

```
   連線特定 DNS 尾碼 . . . . . . . . :
   描述 . . . . . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   實體位址 . . . . . . . . . . . . . : 1C-B7-2C-1E-CB-0E
   DHCP 已啟用 . . . . . . . . . . . : 是
   自動設定啟用 . . . . . . . . . . . : 是
   IPv6 位址. . . . . . . . . . . . . : 2001:b011:6cc0:114b:a032:c63b:766e:c8d4(
偏好選項)
   臨時 IPv6 位址. . . . . . . . . . . : 2001:b011:6cc0:114b:cd9d:f111:b4b4:5bfe(
偏好選項)
   連結-本機 IPv6 位址 . . . . . . . . : fe80::a032:c63b:766e:c8d4%3(偏好選項)
   IPv4 位址 . . . . . . . . . . . . . : 192.168.50.241(偏好選項)
   子網路遮罩 . . . . . . . . . . . . : 255.255.255.0
   租用取得 . . . . . . . . . . . . . : 2019年7月31日 上午 10:19:51
   租用到期 . . . . . . . . . . . . . : 2019年8月1日 上午 10:55:38
   預設閘道 . . . . . . . . . . . . . : fe80::6d4:c4ff:fe61:c85c%3
                                        192.168.50.1
   DHCP 伺服器 . . . . . . . . . . . : 192.168.50.1
   DHCPv6 IAID . . . . . . . . . . . : 52213548
   DHCPv6 用戶端 DUID. . . . . . . . : 00-01-00-01-1C-CC-BE-EF-1C-B7-2C-1E-CB-0E

   DNS 伺服器 . . . . . . . . . . . . : 2001:b011:6cc0:114b::1
                                        168.95.192.1
                                        192.168.50.1
   NetBIOS over Tcpip . . . . . . . . : 啟用
```


ASUS RT-AC1300UHP PPPoE 測項4

✓ 確認用戶至HiNet路由正常

```
C:\Users\ASUS>ping dns.hinet.net

Ping dns.hinet.net [2001:b000:168::2] (使用 32 位元組的資料):
回覆自 2001:b000:168::2: 時間=11ms
回覆自 2001:b000:168::2: 時間=12ms
回覆自 2001:b000:168::2: 時間=9ms
回覆自 2001:b000:168::2: 時間=10ms

2001:b000:168::2 的 Ping 統計資料:
    封包: 已傳送 = 4，已收到 = 4，已遺失 = 0 (0% 遺失)，
大約的來回時間 (毫秒):
    最小值 = 9ms，最大值 = 12ms，平均 = 10ms

C:\Users\ASUS>tracert dns.hinet.net

在上限 30 個躍點上
追蹤 dns.hinet.net [2001:b000:168::2] 的路由:

  1    <1 ms    <1 ms    <1 ms  2001-b011-6cc0-5891-0000-0000-0000-0001.dynamic-ip6.hinet.net [2001:b011:6cc0:
5891::1]
  2    10 ms    10 ms    10 ms  2001:b010:ffff::1
  3    10 ms    10 ms    10 ms  2001-b000-0089-0005-0021-2222-0002-0002.hinet-ip6.hinet.net [2001:b000:89:5:21
:2222:2:2]
  4     *       10 ms     *     2001-b000-0080-0003-0080-0089-0021-000a.hinet-ip6.hinet.net [2001:b000:80:3:80
:89:21:a]
  5    13 ms    10 ms    12 ms  2001-b000-0080-0004-3021-3011-0002-000b.hinet-ip6.hinet.net [2001:b000:80:4:30
21:3011:2:b]
  6    14 ms    15 ms    14 ms  2001-b000-0080-0004-3021-3011-0002-000b.hinet-ip6.hinet.net [2001:b000:80:4:30
21:3011:2:b]
  7    10 ms    10 ms    10 ms  2001-b000-0080-0004-3011-3312-0011-000b.hinet-ip6.hinet.net [2001:b000:80:4:30
11:3312:11:b]
  8     *        *        *     要求等候逾時。
  9    11 ms    11 ms    12 ms  dns.hinet.net [2001:b000:168::2]

追蹤完成。
```

ASUS RT-AC1300UHP PPPoE 測項5

✓ 確認用戶IPv6上網正常(test-ipv6.com)

測試 IPv6 | 常見問題 | 鏡像伺服器

測試你的 IPv6 連線。

總結 | 測試結果 | 分享結果 / 聯繫我們 | 其他 IPv6 網站

- 你在網際網路上的IPv4位址 36.230.24.77
- 你在網際網路上的IPv6位址 2001:b011:6cc0:564d:84d3:39cd:52cf:673f
- 你的網路服務提供者 (ISP) 是 HINET Data Communication Business Group
- Since you have IPv6, we are including a tab that shows how well you can reach other IPv6 sites.
- HTTPS 支援現已在本網站上提供。 [詳細資訊]
- 你的 DNS 伺服器 （可能由你的ISP維護）似乎支援 IPv6 的網際網路通訊協定。

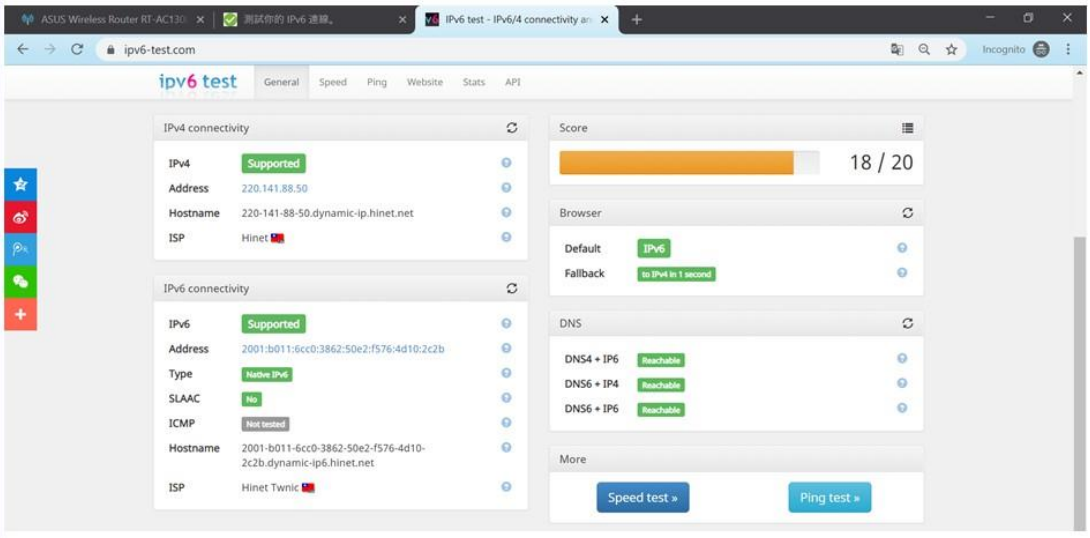
你對於 IPv6 準備的分數

10/10

當網站陸續只使用 IPv6，請提早為您的 IPv6 做準備和設定

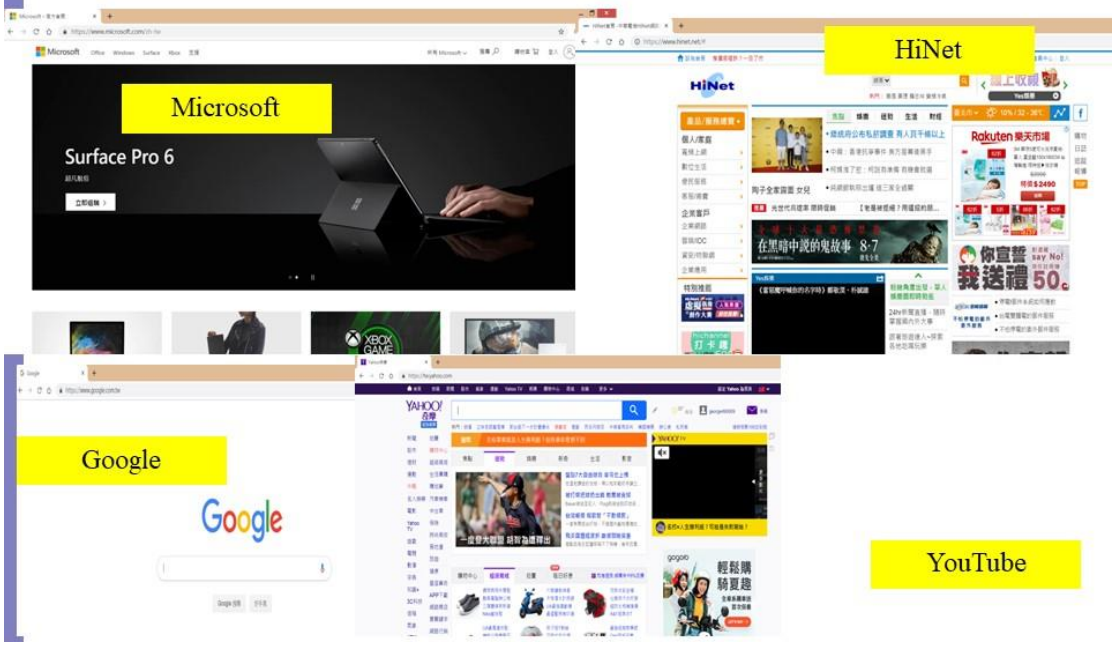
ASUS RT-AC1300UHP PPPoE 測項5 (續)

✓ 確認用戶IPv6上網正常(ipv6-test.com)



ASUS RT-AC1300UHP PPPoE 測項6

✓確認用戶熱門網頁開啟正常



ASUS RT-AC1300UHP PPPoE 測項7

✓確認用戶上網速率正常



Mobile Broadband Networklab, NCU

ASUS RT-AC1300UHP PPPoE 測項8

✓ 確認分享器重撥，用戶IPv6更新正常

分享器重撥之前



分享器重撥之後



ASUS RT-AC1300UHP PPPoE 測項9

✓ 確認用戶使用IPv6之MTU正常

- 乙太網路介面之MTU為1492

```
C:\Users\ASUS>netsh interface ipv6 show subinterface

   MTU  MediaSenseState   接收的位元組  傳送的位元組  介面
------  ---------------  ---------  ---------  -------------
  1492                1    5176679    1249757  乙太網路
4294967295                1          0     836458  Loopback Pseudo-Interface 1
  1500                1    6709310    1213270  Wi-Fi
  1500                5          0       1972  Bluetooth 網路連線
  1500                5          0       7168  區域連線* 3
  1400                5          0       7168  區域連線
```

ASUS RT-AC1300UHP PPPoE 測項10

✓ 確認用戶連接Wi-Fi上網IPv6、DNSv6正常

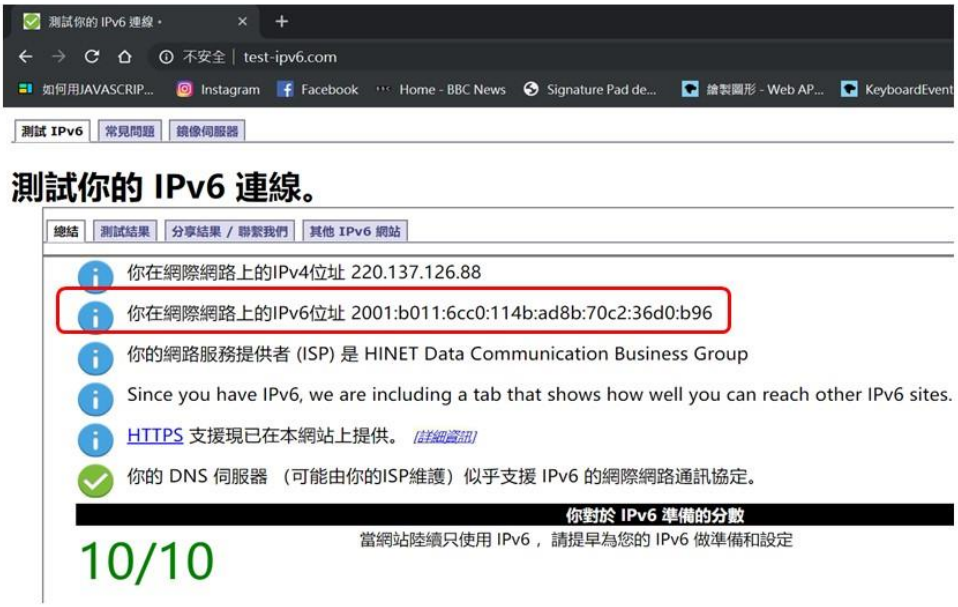
- 用戶獲得IPv6位址

```
無線區域網路介面卡 Wi-Fi:

   連線特定 DNS 尾碼 . . . . . . . . :
   描述 . . . . . . . . . . . . . . : Intel(R) Wireless-AC 9462
   實體位址 . . . . . . . . . . . . : D8-F2-CA-70-16-24
   DHCP 已啟用 . . . . . . . . . . . : 是
   自動設定啟用 . . . . . . . . . . . : 是
   IPv6 位址. . . . . . . . . . . . : 2001:b011:6cc0:564d:9d13:fcbc:8da3:a687(偏好選項)
   臨時 IPv6 位址. . . . . . . . . . : 2001:b011:6cc0:564d:84d3:39cd:52cf:673f(偏好選項)
   連結-本機 IPv6 位址 . . . . . . . : fe80::9d13:fcbc:8da3:a687%7(偏好選項)
   IPv4 位址 . . . . . . . . . . . . : 192.168.50.152(偏好選項)
   子網路遮罩 . . . . . . . . . . . : 255.255.255.0
   租用取得 . . . . . . . . . . . . : 2019年7月31日 上午 11:27:07
   租用到期 . . . . . . . . . . . . : 2019年8月1日 上午 11:27:07
   預設閘道 . . . . . . . . . . . . : fe80::6d4:c4ff:feb5:c6f8%7
                                       192.168.50.1
   DHCP 伺服器 . . . . . . . . . . . : 192.168.50.1
   DHCPv6 IAID . . . . . . . . . . . : 114881226
   DHCPv6 用戶端 DUID. . . . . . . . : 00-01-00-01-24-92-58-57-6C-2B-59-56-E5-DB
   DNS 伺服器 . . . . . . . . . . . : 2001:b011:6cc0:564d::1
                                       192.168.50.1
   NetBIOS over Tcpip . . . . . . . : 啟用
```

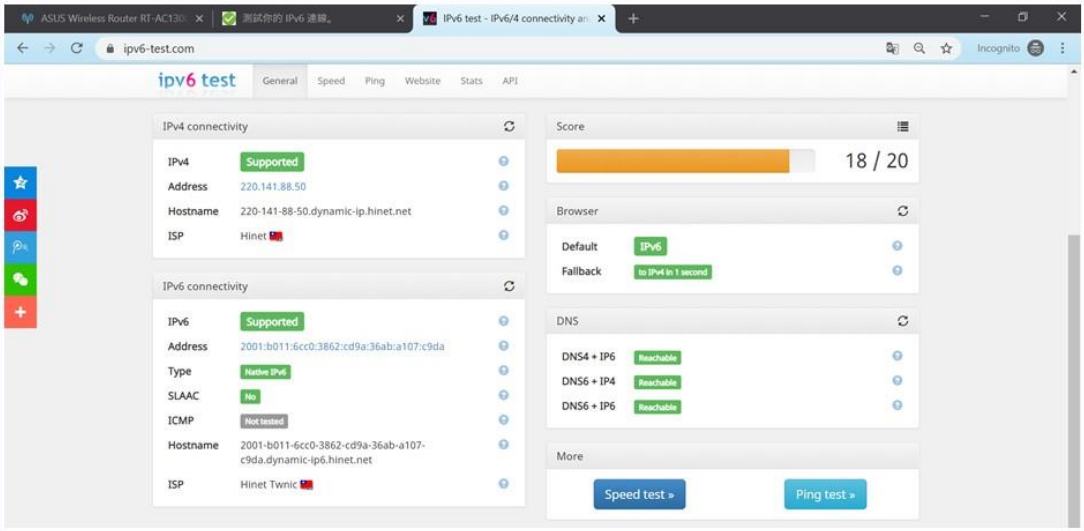

ASUS RT-AC1300UHP PPPoE 測項11

✓ 確認用戶連接Wi-Fi IPv6上網正常(test-ipv6.com)



ASUS RT-AC1300UHP PPPoE 測項11(續)

✓ 確認用戶連接Wi-Fi IPv6上網正常(ipv6-test.com)



ASUS RT-AC1300UHP PPPoE 測項12

✓ IPv6 PPPoE (或是PPPoEv6)是否隨著IPv4 PPPoE啟用而自動啟用

- 重新Reset分享器後，依照"網路設定精靈操作"，無法直接取得IPv6位址



ASUS RT-AC1300UHP PPPoE 測項12(續)

- ✓ IPv6 PPPoE (或是PPPoEv6)是否隨著IPv4 PPPoE啟用而自動啟用
  - 在IPv6設定中開啟IPv6功能，並設定連線類型Native



ASUS RT-AC1300UHP PPPoE 測項12(續)

- ✓ IPv6 PPPoE (或是PPPoEv6)是否隨著IPv4 PPPoE啟用而自動啟用
  - 設定完啟用IPv6後即可正常連線



ASUS RT-AC1300UHP PPPoE 測項13

- ✓ IPv6 PPPoE (或是PPPoEv6)連線之PPPoE Session是『Share with IPv4』或是『Create a new Session』?

華碩分享器並無提供此項功能

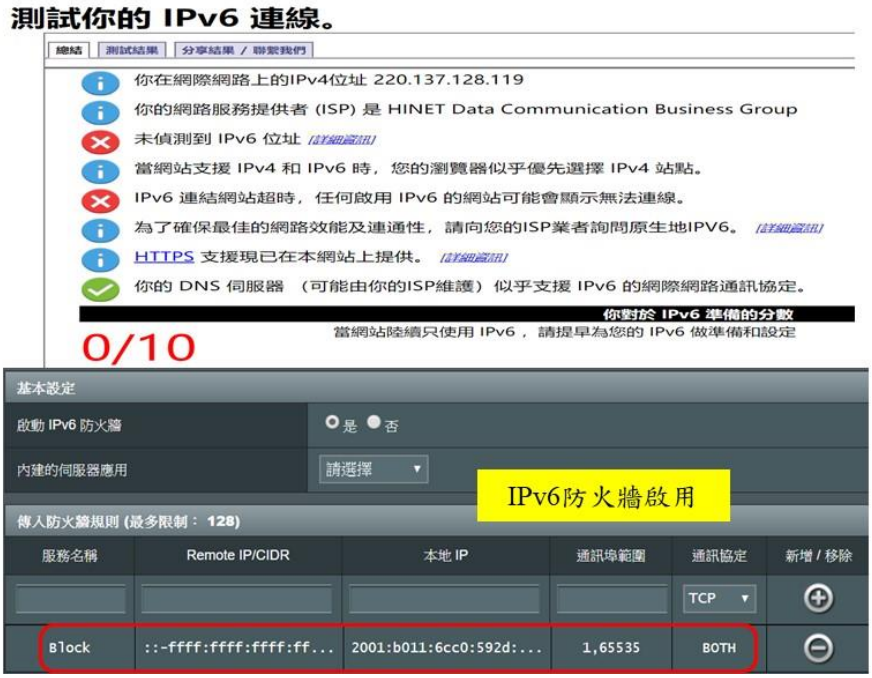
ASUS RT-AC1300UHP PPPoE 測項14

- ✓ IPv6寬頻分享器IPv6 ACL功能是否正常?
  - □ 測試寬頻分享器 IPv6 ACL功能是否能限制用戶終端IPv6連線 **測試你的 IPv6 連線。**

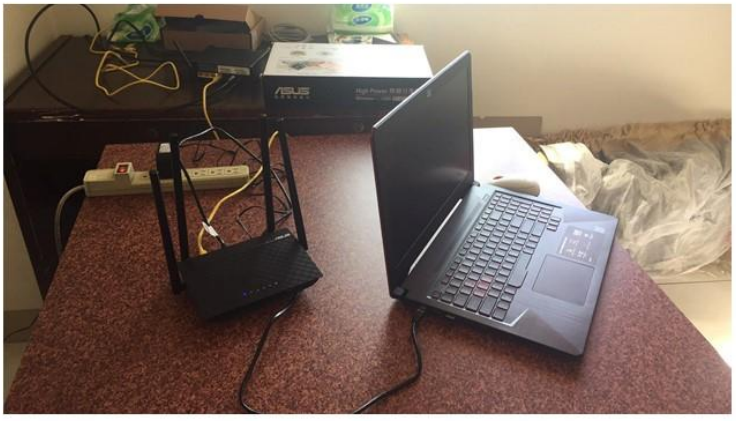


ASUS RT-AC1300UHP PPPoE 測項14(續)

啟用ACL功能後，被設定阻擋的主機無法取得IPv6位址



分享器測試紀錄
Cable 寬頻 IPoE環境



ASUS RT-AC1300UHP CM 測項1

✓ 確認連接cable modem正常

網路已設定

系統時間: **Wed, Jul 31 15:23:42 2019** (GMT+08:00)

外部網路(WAN)

WAN 連線類型	自動取得 IP
外部網路 IP	123.241.152.218

無線網路 (2.4GHz)

網路名稱 (SSID)	ASUS_RT_AC1300_2G
無線加密	Open S

無線網路 (5GHz)

網路名稱 (SSID)	ASUS_
無線加密	Open S

區域網路(LAN)

區域網路 IP	192.16
MAC 位址	04:D4:C

系統紀錄 - IPv6 網路資訊

此頁面顯示 IPv6 網路的詳細資訊。

```
        IPv6 Connection Type: Native with DHCP-PD
             WAN IPv6 Address: 2405:9200:1125::6
  WAN IPv6 Link-Local Address: fe80::6d4:c4ff:fe61:c858/64
         WAN IPv6 Gateway: fe80::201:5cff:fea1:1646
             LAN IPv6 Address: 2405:9200:1110:10::1/64
  LAN IPv6 Link-Local Address: fe80::6d4:c4ff:fe61:c85c/64
                  DHCP-PD: Enabled
           LAN IPv6 Prefix: 2405:9200:1110:10::/64
              DNS Servers: 2404::1 2001:4860:4860::8888 2001:b000:168::1


IPv6 LAN Devices List
------------------------------------------------------------------------
Hostname                    MAC Address       IPv6 Address
DESKTOP-C4E6R0E             6c:2b:59:56:e5:db 2405:9200:1110:10:4016:7534:fbfe:214b
```


ASUS RT-AC1300UHP CM 測項2

✓ 確認取得IPv6、IPv6 PD、DNSv6

系統紀錄 - IPv6 網路資訊

此頁面顯示 IPv6 網路的詳細資訊。

WAN端位址資訊

```
        IPv6 Connection Type: Native with DHCP-PD
             WAN IPv6 Address: 2405:9200:1125::6
  WAN IPv6 Link-Local Address: fe80::6d4:c4ff:fe61:c858/64
         WAN IPv6 Gateway: fe80::201:5cff:fea1:1646
             LAN IPv6 Address: 2405:9200:1110:10::1/64
  LAN IPv6 Link-Local Address: fe80::6d4:c4ff:fe61:c85c/64
                  DHCP-PD: Enabled
           LAN IPv6 Prefix: 2405:9200:1110:10::/64
              DNS Servers: 2404::1 2001:4860:4860::8888 2001:b000:
```

LAN端位址資訊

```
IPv6 LAN Devices List
------------------------------------------------------------------------
Hostname                    MAC Address       IPv6 Address
DESKTOP-C4E6R0E             6c:2b:59:56:e5:db 2405:9200:1110:10:4016:7534:fbfe:214b
```

ASUS RT-AC1300UHP CM 測項3

✓ 確認用戶IPv6、DNSv6取得正常

```
乙太網路卡 乙太網路:

   連線特定 DNS 尾碼 . . . . . . . . :
   描述 . . . . . . . . . . . . . . . : Realtek PCIe FE Family Controller
   實體位址 . . . . . . . . . . . . . : 6C-2B-59-56-E5-DB
   DHCP 已啟用 . . . . . . . . . . . : 是
   自動設定啟用 . . . . . . . . . . . : 是
   IPv6 位址. . . . . . . . . . . . . : 2405:9200:1110:10:1089:df90:502:6cf9(偏好選項)
   臨時 IPv6 位址. . . . . . . . . . . : 2405:9200:1110:10:4016:7534:fbfe:214b(偏好選項)
   連結-本機 IPv6 位址 . . . . . . . . : fe80::1089:df90:502:6cf9%6(偏好選項)
   IPv4 位址 . . . . . . . . . . . . . : 192.168.50.115(偏好選項)
   子網路遮罩 . . . . . . . . . . . . : 255.255.255.0
   租用取得 . . . . . . . . . . . . . : 2019年7月31日 下午 03:17:12
   租用到期 . . . . . . . . . . . . . : 2019年8月1日 下午 03:17:10
   預設閘道 . . . . . . . . . . . . . : fe80::6d4:c4ff:fe61:c85c%6
                                        192.168.50.1
   DHCP 伺服器 . . . . . . . . . . . : 192.168.50.1
   DHCPv6 IAID . . . . . . . . . . . : 72632336
   DHCPv6 用戶端 DUID. . . . . . . . : 00-01-00-01-24-92-58-57-6C-2B-59-56-E5-DB
   DNS 伺服器 . . . . . . . . . . . . : 168.95.192.1
                                        192.168.50.1
                                        2405:9200:1110:10::1
   NetBIOS over Tcpip . . . . . . . . : 啟用
```


ASUS RT-AC1300UHP CM 測項4

✓ 確認用戶至google ipv6路由正常

```
C:\Users\User>tracert ipv6.google.com

在上限 30 個躍點上
追蹤 ipv6.l.google.com [2404:6800:4012:1::200e] 的路由:

  1    <1 ms    <1 ms     1 ms  2405:9200:1110:10::1
  2     *        *        *     要求等候逾時。
  3     9 ms     9 ms     8 ms  2405:9200:1:0:172:16:28:177a
  4    12 ms    13 ms    10 ms  2405:9200:1:0:172:16:31:22a
  5    10 ms    10 ms    11 ms  2404:0:10ff:1:7709:13:1596:712
  6    11 ms    10 ms    10 ms  2404:0:10ff::4:166
  7     9 ms    11 ms    10 ms  2404:0:10ff:1:7709:1:5169:61
  8    11 ms    11 ms    11 ms  2001:4860:0:1014::1
  9    12 ms    12 ms    11 ms  2001:4860:0:1::2e0b
 10    11 ms     9 ms    10 ms  tsa03s06-in-x0e.1e100.net [2404:6800:4012:1::200e]

追蹤完成。

C:\Users\User>ping ipv6.google.com

Ping ipv6.l.google.com [2404:6800:4012:1::200e] (使用 32 位元組的資料):
回覆自 2404:6800:4012:1::200e: 時間=13ms
回覆自 2404:6800:4012:1::200e: 時間=11ms
回覆自 2404:6800:4012:1::200e: 時間=11ms
回覆自 2404:6800:4012:1::200e: 時間=11ms

2404:6800:4012:1::200e 的 Ping 統計資料:
    封包: 已傳送 = 4，已收到 = 4, 已遺失 = 0 (0% 遺失)，
大約的來回時間 (毫秒):
    最小值 = 11ms，最大值 = 13ms，平均 = 11ms
```

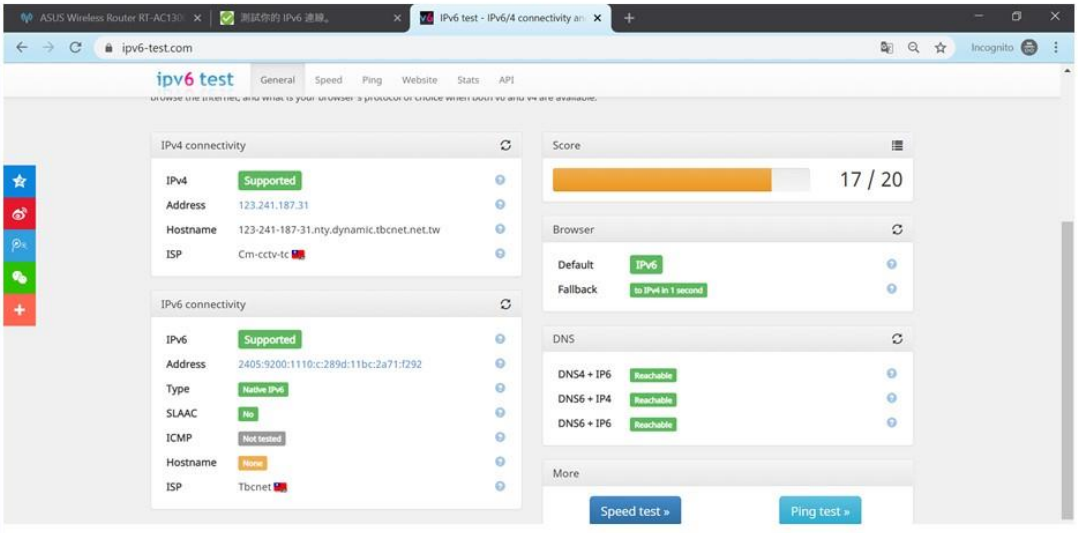
ASUS RT-AC1300UHP CM 測項5

✓ 確認用戶IPv6上網正常(test-ipv6.com)



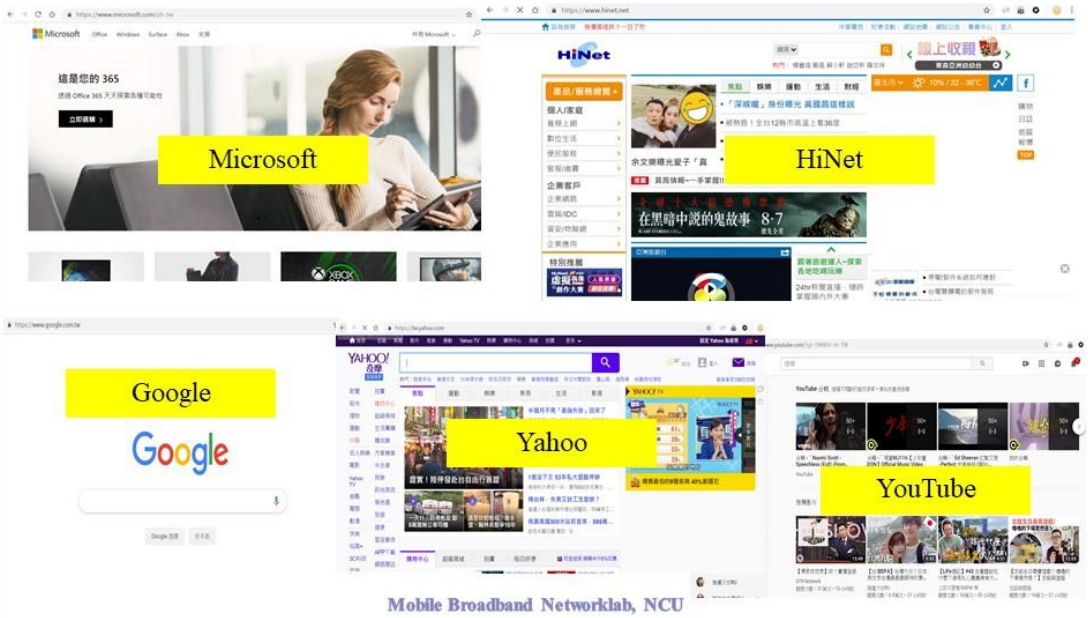
ASUS RT-AC1300UHP CM 測項5(續)

✓ 確認用戶IPv6上網正常(ipv6-test.com)



ASUS RT-AC1300UHP CM 測項6

✓確認用戶熱門網頁開啟正常



Mobile Broadband Networklab, NCU

ASUS RT-AC1300UHP CM 測項7

✓確認用戶上網速率正常



Mobile Broadband Networklab, NCU

ASUS RT-AC1300UHP CM 測項8

✓ 確認分享器重新連接cable modem之後，用戶ipv6相同，且連線正常



ASUS RT-AC1300UHP CM 測項9

✓ 確認用戶使用IPv6乙太網路介面之MTU
- 乙太網路介面之MTU為1500

```
C:\Users\User>netsh interface ipv6 show subinterface

   MTU  MediaSenseState   接收的位元組 傳送的位元組 介面
------  ---------------  ---------  ---------  -------------
4294967295                1          0     118806  Loopback Pseudo-Interface 1
  1500                5          0        152  Wi-Fi
  1500                1  291560654   72004731  乙太網路
  1500                5          0        152  區域連線* 1
  1500                5          0        152  藍牙網路連線
  1500                5          0        152  區域連線* 2
  1500                1          0      52934  VirtualBox Host-Only Network
```

ASUS RT-AC1300UHP CM 測項10

✓ 確認用戶連接Wi-Fi上網IPv6、DNSv6正常

無線區域網路介面卡 Wi-Fi:

```
   連線特定 DNS 尾碼 . . . . . . . . :
   描述 . . . . . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 7265
   實體位址 . . . . . . . . . . . . . : 34-02-86-63-18-11
   DHCP 已啟用 . . . . . . . . . . . : 是
   自動設定啟用 . . . . . . . . . . . : 是
   IPv6 位址. . . . . . . . . . . . . : 2405:9200:1110:10:80c3:57d2:60e7:e27a(偏好選項)
   臨時 IPv6 位址. . . . . . . . . . . : 2405:9200:1110:10:795e:3a30:7604:1e63(偏好選項)
   連結-本機 IPv6 位址 . . . . . . . . : fe80::80c3:57d2:60e7:e27a%6(偏好選項)
   IPv4 位址 . . . . . . . . . . . . . : 192.168.50.67(偏好選項)
   子網路遮罩 . . . . . . . . . . . . : 255.255.255.0
   租用取得 . . . . . . . . . . . . . : 2019年7月31日 下午 03:21:59
   租用到期 . . . . . . . . . . . . . : 2019年8月1日 下午 03:21:59
   預設閘道 . . . . . . . . . . . . . : fe80::6d4:c4ff:fe61:c85c%6
                                        192.168.50.1
   DHCP 伺服器 . . . . . . . . . . . : 192.168.50.1
   DHCPv6 IAID . . . . . . . . . . . : 120849030
   DHCPv6 用戶端 DUID. . . . . . . . : 00-01-00-01-1C-CC-BE-EF-1C-B7-2C-1E-CB-0E
   DNS 伺服器 . . . . . . . . . . . . : 2405:9200:1110:10::1
                                        168.95.192.1
                                        192.168.50.1
   NetBIOS over Tcpip . . . . . . . . : 啟用
```

ASUS RT-AC1300UHP CM 測項11

✓ 確認用戶連接Wi-Fi IPv6上網正常(test-ipv6.com)

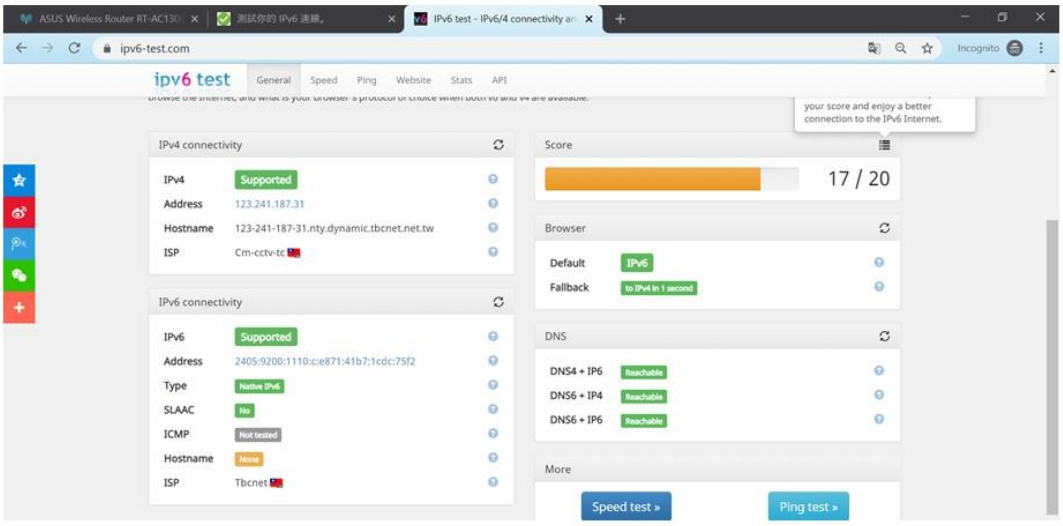
測試你的 IPv6 連線。



Mobile Broadband Networklab, NCU

ASUS RT-AC1300UHP CM 測項11(續)

✓ 確認用戶連接Wi-Fi IPv6上網正常(ipv6-test.com)

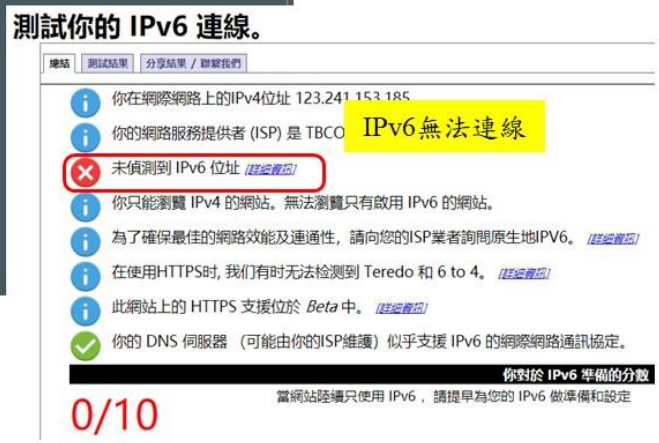


ASUS RT-AC1300UHP CM 測項12

✓ 確認IPv6 連線功能隨著IPv4啟用而自動啟用

- 重新Reset分享器後，依照介面指示設定後，無法使用IPv6

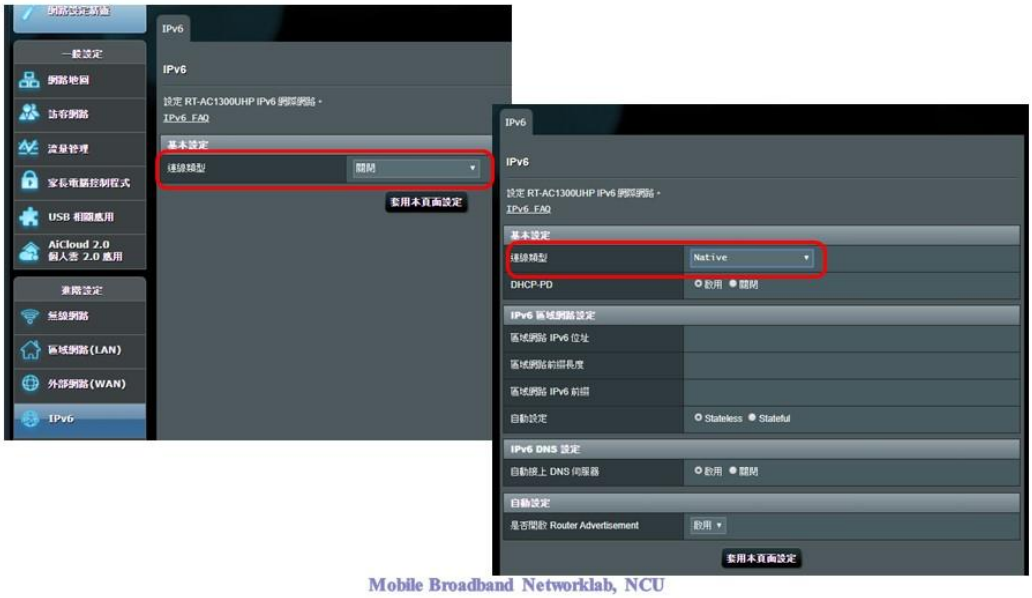




ASUS RT-AC1300UHP CM 測項12(續)

✓ 確認IPv6 連線功能隨著IPv4啟用而自動啟用

- 在IPv6設定中開啟IPv6功能，並設定連線類型Native



ASUS RT-AC1300UHP CM 測項12(續)

✓ 確認IPv6 連線功能隨著IPv4啟用而自動啟用

- 設定完啟用IPv6後即可正常連線

測試你的 IPv6 連線。

總結 | 測試結果 | 分享結果 / 聯繫我們 | 其他 IPv6 網站

IPv6連線成功

你在網際網路上的IPv4位址 123.241.153.185

你在網際網路上的IPv6位址 2405:9200:1110:10:c09f:a30e:31d8:11c7

你的網路服務提供者 (ISP) 是 TBCOM-NET TBC

Since you have IPv6, we are including a tab that shows how well you can reach other IPv6 sites.

此網站上的 HTTPS 支援位於 *Beta* 中。

你的 DNS 伺服器 （可能由你的ISP維護）似乎

10/10



Mobile Broadband Networklab, NCU

ASUS RT-AC1300UHP CM 測項13

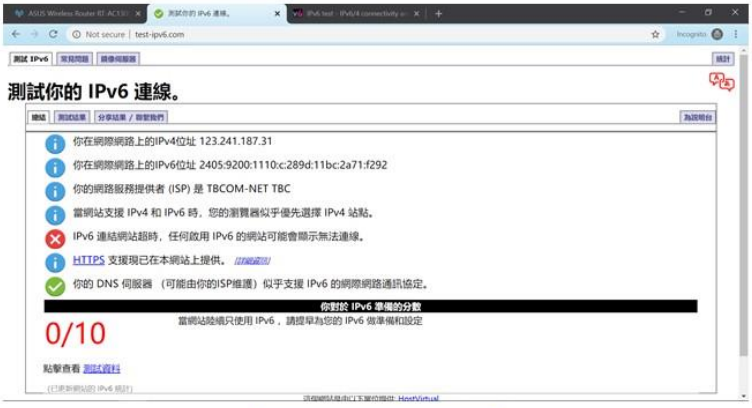
- ✓ IPv6寬頻分享器IPv6 ACL功能是否正常?
  - 測試寬頻分享器 IPv6 ACL功能是否能限制用戶終端IPv6連線





ASUS RT-AC1300UHP CM 測項13(續)

啟用ACL功能後，被設定阻擋的主機無法取得IPv6位址





國立中央大學 National Central University

Mobile broadband networklab

TOTOLINK A950RG

分享器測試成果

1

測試設備與環境

分享器產品設備資訊	
產品型號	A950RG
產品名稱	AC超世代Giga路由器
硬體版本	1.0
韌體版本	5.9c.4006
製造年份	2019

測試環境資訊	
測試環境	1.HiNet光世代 PPPoE
	2.Cable IPoE
測試終端	Windows 10
終端瀏覽器	Chrome
測試時間	2019-08~2019-10



Mobile Broadband Networklab, NCU

測試紀錄摘要

HiNet 光世代PPPoE測試		
	測試項目	A950RG
1	分享器PPPoE撥接是否正常?	O
2	分享器IPv6、IPv6 PD、DNSv6取得是否正常?	O
3	用戶IPv6、DNSv6取得是否正常?	O
4	用戶至HiNet路由是否正常?	O
5	用戶IPv6上網是否正常?	O
6	用戶熱門網頁開啟是否正常?	O
7	用戶上網速率是否正常?	O
8	分享器重撥，用戶IPv6更新是否正常?	O
9	用戶使用IPv6之MTU是否正常?	1500
10	用戶連接Wi-Fi上網IPv6、DNSv6是否正常?	O
11	用戶連接Wi-Fi IPv6上網是否正常?	O
12	IPv6 PPPoE（或是PPPoEv6)是否隨著IPv4 PPPoE啟用而自動啟用?	X
13	IPv6 PPPoE（或是PPPoEv6)連線之PPPoE Session是『Share with IPv4』或是『Create a new Session』?	無提供此項設定
14	IPv6寬頻分享器IPv6 ACL功能是否正常?	無支援IPv6 ACL功能

Cable IPoE測試		
	測試項目	A950RG
1	分享器連接Cable Modem是否正常?	O
2	分享器IPv6、IPv6 PD、DNSv6取得是否正常?	O
3	用戶IPv6、DNSv6取得是否正常?	O
4	用戶至Cable業者路由是否正常?	O
5	用戶IPv6上網是否正常?	O
6	用戶熱門網頁開啟是否正常?	O
7	用戶上網速率是否正常?	O
8	分享器重撥Cable Modem，用戶IPv6更新是否正常?	O
9	用戶使用IPv6之MTU是否正常?	1500
10	用戶連接Wi-Fi上網IPv6、DNSv6是否正常?	O
11	用戶連接Wi-Fi IPv6上網是否正常?	O
12	IPv6連線功能是否隨著IPv4啟用而自動啟用?	X
13	IPv6寬頻分享器IPv6 ACL功能是否正常?	無支援IPv6 ACL功能

測試紀錄摘要說明

- ✓ HiNet PPPoE環境 (Pass測項:10/14)
  - 測項9: RA ICMP option MTU1500，PPPoE環境可能導致用戶端packet too big須重傳
  - 測項12: 需要手動啟用IPv6
  - 測項13: 無提供此項設定
  - 測項14: 無支援IPv6 ACL功能
- ✓ Cable IPoE環境(Pass測項:11/13)
  - 測項12: 需要手動啟用IPv6
  - 測項13: 無支援IPv6 ACL功能

分享器測試紀錄
HiNet 光世代PPPoE環境



5

TOTOLINK A950RG PPPoE 測項1

✓ 確認分享器PPPoE撥接正常

IPv6 網際網路(WAN)	
Link Type	PPP link
Origin Type	浮動 連線成功
全域地址	2001:b011:6cc0:0032:b83c:c87d:b0ee:b23a/64
本機連線位址	fe80:0000:0000:0000:b83c:c87d:b0ee:b23a/10
預設閘道	fe80:0000:0000:0000:d2f0:dbff:fe53:0800
DNS伺服器	2001:b000:0168:0000:0000:0000:0000:0002

WAN端位址資訊

網際網路(WAN)設定

本頁用於設定網際網路(WAN)的各項參數，您可以設定DHCP、固定IP、PPPoE等上網方式。

連接狀態 PPPoE 連線成功

Mobile Broadband Networklab, NCU

TOTOLINK A950RG PPPoE 測項2

✓ 確認分享器IPv6、IPv6 PD、DNSv6取得正常

IPv6 網際網路(WAN)	
Link Type	PPP link
Origin Type	浮
全域地址	2001:b011:6cc0:0032:b83c:c87d:b0ee:b23a/64
本機連線位址	fe80:0000:0000:0000:b83c:c87d:b0ee:b23a/10
預設閘道	fe80:0000:0000:0000:d2f0:dbff:fe53:0800
DNS伺服器	2001:b000:0168:0000:0000:0000:0000:0002

WAN端位址資訊

IPv6 區域網路(LAN)狀態	
全域地址	2001:b011:6cc0:31ef:164d:67ff:fe62:5abc/64
本機連線位址	fe80:0000:0000:0000:164d:67ff:fe62:5abc/64
預設閘道	fe80:0000:0000:0000:164d:67ff:fe62:5abc/64

LAN端位址資訊

TOTOLINK A950RG PPPoE 測項3

✓ 確認用戶IPv6、DNSv6取得正常

乙太網路卡 乙太網路:

```
   連線特定 DNS 尾碼 . . . . . . . . :
   描述 . . . . . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   實體位址 . . . . . . . . . . . . . : 1C-B7-2C-1E-CB-0E
   DHCP 已啟用 . . . . . . . . . . . : 是
   自動設定啟用 . . . . . . . . . . . : 是
   IPv6 位址. . . . . . . . . . . . . : 2001:b011:6cc0:19dd:a032:c63b:766e:c8d4(偏好選項)
   IPv6 位址. . . . . . . . . . . . . : 2001:b011:6cc0:5367::3(偏好選項)
   租用取得 . . . . . . . . . . . . . : 2019年8月14日 下午 07:58:35
   租用到期 . . . . . . . . . . . . . : 2019年8月14日 下午 08:58:36
   臨時 IPv6 位址. . . . . . . . . . . : 2001:b011:6cc0:19dd:38bb:7eb9:9c27:3d93(偏好選項)
   連結-本機 IPv6 位址 . . . . . . . . : fe80::a032:c63b:766e:c8d4%11(偏好選項)
   IPv4 位址 . . . . . . . . . . . . . : 192.168.0.2(偏好選項)
   子網路遮罩 . . . . . . . . . . . . : 255.255.255.0
   租用取得 . . . . . . . . . . . . . : 2019年8月14日 下午 07:58:31
   租用到期 . . . . . . . . . . . . . : 2019年8月15日 下午 07:58:31
   預設閘道 . . . . . . . . . . . . . : fe80::164d:67ff:fe62:5abc%11
                                        192.168.0.1
   DHCP 伺服器 . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 52213548
   DHCPv6 用戶端 DUID. . . . . . . . : 00-01-00-01-1C-CC-BE-EF-1C-B7-2C-1E-CB-0E
   DNS 伺服器 . . . . . . . . . . . . : 2001:b000:168::2
                                        192.168.0.1
   NetBIOS over Tcpip . . . . . . . . : 啟用
```

TOTOLINK A950RG PPPoE 測項4

✓ 確認用戶至HiNet路由正常

```
C:\Users\ASUS>ping dns.hinet.net

Ping dns.hinet.net [2001:b000:168::2] (使用 32 位元組的資料):
回覆自 2001:b000:168::2: 時間=10ms
回覆自 2001:b000:168::2: 時間=12ms
回覆自 2001:b000:168::2: 時間=10ms
回覆自 2001:b000:168::2: 時間=11ms

2001:b000:168::2 的 Ping 統計資料:
    封包: 已傳送 = 4，已收到 = 4，已遺失 = 0 (0% 遺失)，
大約的來回時間 (毫秒):
    最小值 = 10ms，最大值 = 12ms，平均 = 10ms

C:\Users\ASUS>tracert dns.hinet.net

在上限 30 個躍點上
追蹤 dns.hinet.net [2001:b000:168::2] 的路由:

  1    <1 ms    <1 ms    <1 ms  2001-b011-6cc0-52d9-164d-67ff-fe62-5abc.dynamic-ip6.hinet.net [2001:b011:6cc0:52d9:164d:67ff:fe62:5abc]
  2    10 ms     8 ms     9 ms  2001:b010:ffff::1
  3    24 ms    25 ms    10 ms  2001-b000-0089-0005-0021-2222-0002-0002.hinet-ip6.hinet.net [2001:b000:89:5:21:2222:2:2]
  4     *        *       10 ms  2001-b000-0080-0003-0080-0089-0021-000a.hinet-ip6.hinet.net [2001:b000:80:3:80:89:21:a]
  5    13 ms    14 ms    14 ms  2001-b000-0080-0004-3021-3011-0001-000b.hinet-ip6.hinet.net [2001:b000:80:4:3021:3011:1:b]
  6    15 ms    14 ms    14 ms  2001-b000-0080-0004-3021-3011-0001-000b.hinet-ip6.hinet.net [2001:b000:80:4:3021:3011:1:b]
  7    11 ms    10 ms    10 ms  2001-b000-0080-0004-3011-3312-0012-000b.hinet-ip6.hinet.net [2001:b000:80:4:3011:3312:12:b]
  8    12 ms    11 ms    10 ms  2001-b000-0080-0006-3312-0000-0002-0001.hinet-ip6.hinet.net [2001:b000:80:6:3312:0:2:1]
  9    12 ms    12 ms    11 ms  dns.hinet.net [2001:b000:168::2]

追蹤完成。
```

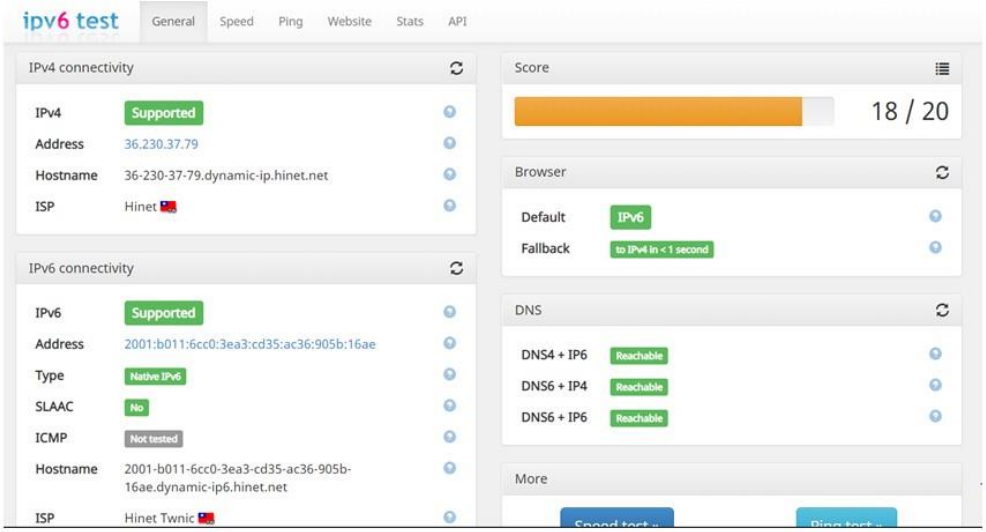

TOTOLINK A950RG PPPoE 測項5

✓ 確認用戶IPv6上網正常(test-ipv6.com)



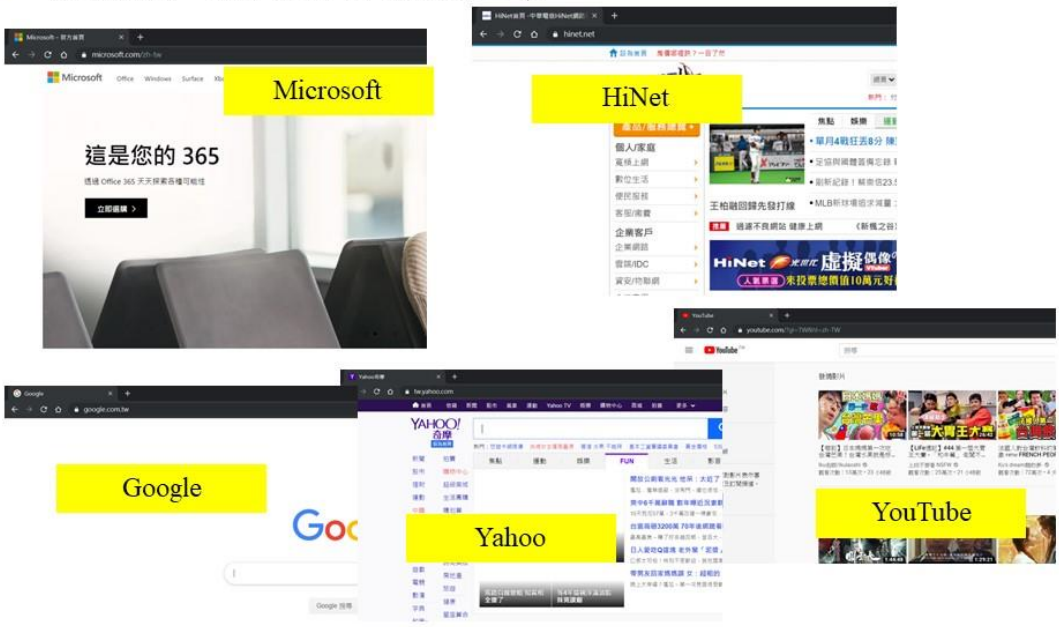
TOTOLINK A950RG PPPoE 測項5(續)

✓ 確認用戶IPv6上網正常(ipv6-test.com)



TOTOLINK A950RG PPPoE 測項6

✓ 確認用戶熱門網頁開啟正常



TOTOLINK A950RG PPPoE 測項7

✓ 確認用戶上網速率正常



TOTOLINK A950RG PPPoE 測項8

✓ 確認分享器重撥，用戶IPv6更新正常

測試你的 IPv6 連線。



測試你的 IPv6 連線。



TOTOLINK A950RG PPPoE 測項9

✓ 確認用戶使用IPv6之MTU為1500而非1492




```
C:\Users\ASUS>netsh interface ipv6 show subinterface

   MTU  MediaSenseState   接收的位元組  傳送的位元組  介面
------  ---------------  ---------  ---------  -------------
  1500                1   48031628    9405683  乙太網路
4294967295                1          0     136746  Loopback Pseudo-Interface 1
  1500                2   31486746    1182523  Wi-Fi
  1500                5          0       1018  區域連線* 2
  1500                5          0       1018  區域連線* 4
  1500                5          0        152  Bluetooth 網路連線
```


TOTOLINK A950RG PPPoE 測項10

✓ 確認用戶連接Wi-Fi上網IPv6、DNSv6正常

```
無線區域網路介面卡 Wi-Fi:

   連線特定 DNS 尾碼 . . . . . . . . :
   描述 . . . . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 7265
   實體位址 . . . . . . . . . . . . : 34-02-86-63-18-11
   DHCP 已啟用 . . . . . . . . . . . : 否
   自動設定啟用 . . . . . . . . . . . : 是
   IPv6 位址. . . . . . . . . . . . : 2001:b011:6cc0:53b5::1(偏好選項)
   租用取得 . . . . . . . . . . . . : 2019年8月14日 下午 08:14:34
   租用到期 . . . . . . . . . . . . : 2019年8月14日 下午 09:14:34
   IPv6 位址. . . . . . . . . . . . : 2001:b011:6cc0:53b5:80c3:57d2:60e7:e27a(偏好選項)
   臨時 IPv6 位址. . . . . . . . . . : 2001:b011:6cc0:53b5:b013:85b:2634:ec75(偏好選項)
   連結-本機 IPv6 位址 . . . . . . . : fe80::80c3:57d2:60e7:e27a%8(偏好選項)
   IPv4 位址 . . . . . . . . . . . . : 192.168.0.199(偏好選項)
   子網路遮罩 . . . . . . . . . . . : 255.255.255.0
   預設閘道 . . . . . . . . . . . . : fe80::164d:67ff:fe62:5abc%8
                                       192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 120849030
   DHCPv6 用戶端 DUID. . . . . . . . : 00-01-00-01-1C-CC-BE-EF-1C-B7-2C-1E-CB-0E
   DNS 伺服器 . . . . . . . . . . . : 2001:b000:168::1
                                       2001:b000:168::2
                                       2001:4860:4860::8888
                                       2001:4860:4860::8844
   NetBIOS over Tcpip . . . . . . . . : 啟用
```

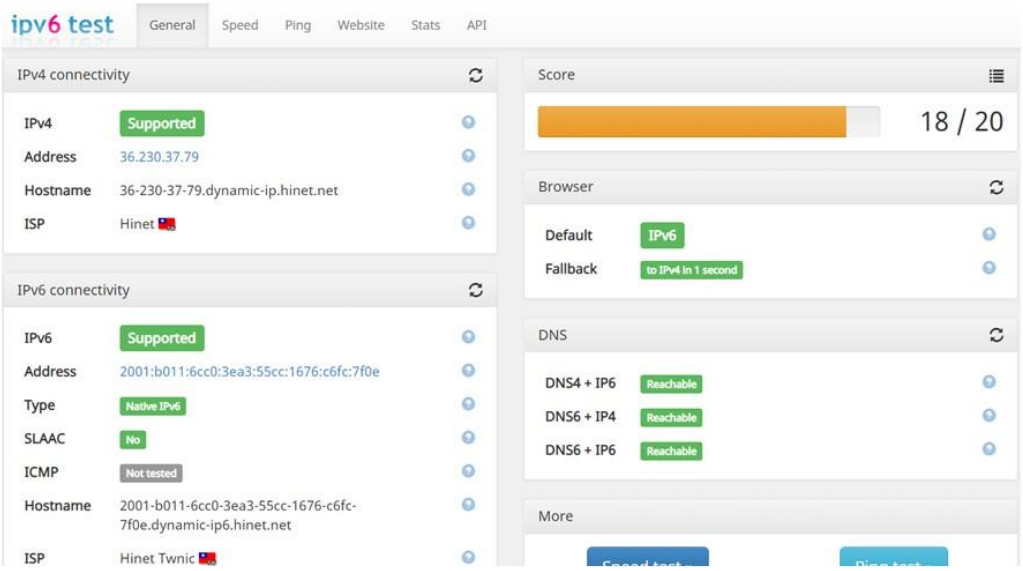
TOTOLINK A950RG PPPoE 測項11

✓ 確認用戶連接Wi-Fi IPv6上網正常(test-ipv6.com)



TOTOLINK A950RG PPPoE 測項11(續)

✓ 確認用戶連接Wi-Fi IPv6上網正常(ipv6-test.com)



TOTOLINK A950RG PPPoE 測項12

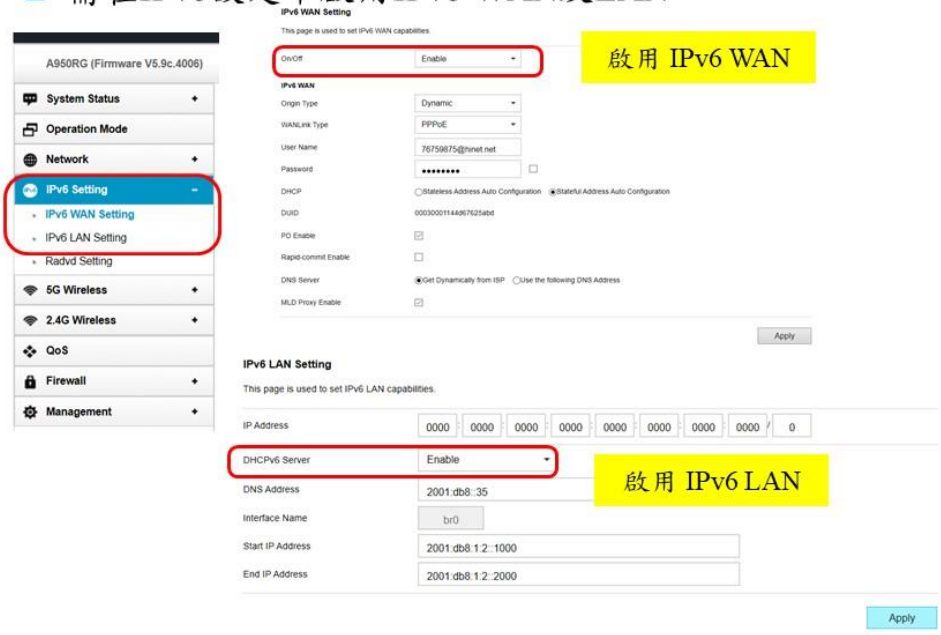
- ✓ IPv6 PPPoE (或是PPPoEv6)是否隨著IPv4 PPPoE啟用而自動啟用
  - ❑ 重新Reset分享器後，依照介面指示設定後，無法使用IPv6



Mobile Broadband Networklab, NCU

TOTOLINK A950RG PPPoE 測項12 (續)

- ✓ 確認IPv6 連線功能隨著IPv4啟用而自動啟用
  - ❑ 需在IPv6設定中啟用IPv6 WAN及LAN



TOTOLINK A950RG PPPoE 測項12 (續)

✓ 確認IPv6 連線功能隨著IPv4啟用而自動啟用

❑ 設定完啟用IPv6後即可正常連線



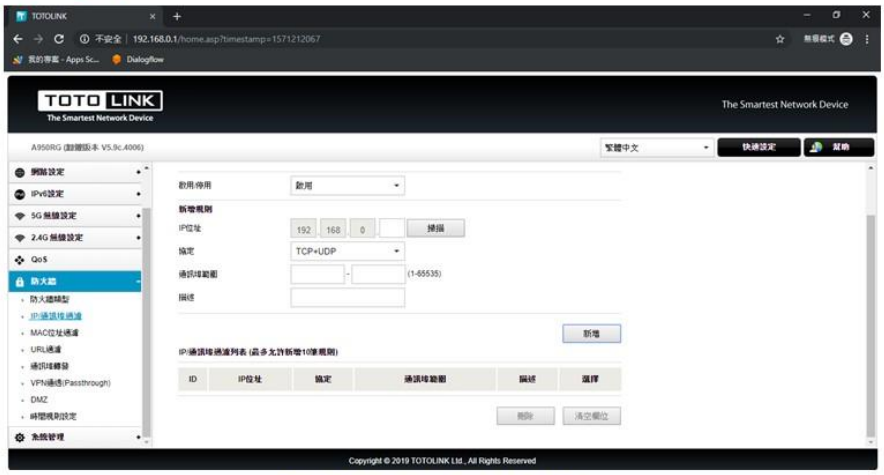
TOTOLINK A950RG PPPoE 測項13

✓ IPv6 PPPoE (或是PPPoEv6)連線之PPPoE Session是『Share with IPv4』或是『Create a new Session』?

❑ 分享器無提供此功能

TOTOLINK A950RG PPPoE 測項14

- ✓ IPv6寬頻分享器IPv6 ACL功能是否正常?
  - 測試寬頻分享器 IPv6 ACL功能是否能限制用戶終端IPv6連線
  - 無支援 IPv6 ACL功能



Mobile Broadband Networklab, NCU

分享器測試紀錄
Cable 寬頻 IPoE環境



TOTOLINK A950RG CM 測項1

✓ 確認連接cable modem正常

IPv6 網際網路(WAN)	
Link Type	IP link
Origin Type	浮動 連線成功
全域地址	2405:9200:1125:0000:0000:0000:0000:0016/64
本機連線位址	fe80:0000:0000:0000:164d:67ff:fe62:5abd/64
預設閘道	fe80:0000:0000:0000:0201:5cff:fea1:1646
DNS伺服器	2404:0000:0000:0000:0000:0000:0000:0001

IPv6 區域網路(LAN)狀態	
全域地址	2001:b011:6cc0:53a7:0000:0000:0000:0000/64
本機連線位址	fe80:0000:0000:0000:164d:67ff:fe62:5abc/64
預設閘道	fe80:0000:0000:0000:164d:67ff:fe62:5abc/64

TOTOLINK A950RG CM 測項2

✓ 確認取得IPv6、IPv6 PD、DNSv6

IPv6 網際網路(WAN)	
Link Type	IP link
Origin Type	浮動 連線 WAN端位址資訊
全域地址	2405:9200:1125:0000:0000:0000:0000:0016/64
本機連線位址	fe80:0000:0000:0000:164d:67ff:fe62:5abd/64
預設閘道	fe80:0000:0000:0000:0201:5cff:fea1:1646
DNS伺服器	2404:0000:0000:0000:0000:0000:0000:0001

IPv6 區域網路(LAN)狀態 LAN端位址資訊	
全域地址	2001:b011:6cc0:53a7:0000:0000:0000:0000/64
本機連線位址	fe80:0000:0000:0000:164d:67ff:fe62:5abc/64
預設閘道	fe80:0000:0000:0000:164d:67ff:fe62:5abc/64

TOTOLINK A950RG CM 測項3

✓ 確認用戶IPv6、DNSv6取得正常

乙太網路卡 乙太網路:

```
連線特定 DNS 尾碼 . . . . . :
描述 . . . . . : Realtek PCIe GBE Family Controller
實體位址 . . . . . : 1C-B7-2C-1E-CB-0E
DHCP 已啟用 . . . . . : 是
自動設定啟用 . . . . . : 是
IPv6 位址. . . . . : 2405:9200:1110:1e:a032:c63b:766e:c8d4(偏好選項)
臨時 IPv6 位址. . . . . : 2405:9200:1110:1e:e80a:fa5f:5d7a:4bed(偏好選項)
連結-本機 IPv6 位址 . . . . . : fe80::a032:c63b:766e:c8d4%11(偏好選項)
IPv4 位址 . . . . . : 192.168.0.4(偏好選項)
子網路遮罩 . . . . . : 255.255.255.0
租用取得 . . . . . : 2019年8月21日 下午 02:42:36
租用到期 . . . . . : 2019年8月22日 下午 02:42:35
預設閘道 . . . . . : fe80::164d:67ff:fe62:5abc%11
                                    192.168.0.1
DHCP 伺服器 . . . . . : 192.168.0.1
DHCPv6 IAID . . . . . : 52213548
DHCPv6 用戶端 DUID. . . . . : 00-01-00-01-1C-CC-BE-EF-1C-B7-2C-1E-CB-0E
DNS 伺服器 . . . . . : 192.168.0.1
NetBIOS over Tcpip . . . . . : 啟用
```


TOTOLINK A950RG CM 測項4

✓ 確認用戶至google ipv6路由正常

```
C:\Users\ASUS>ping ipv6.google.com

Ping ipv6.l.google.com [2404:6800:4008:801::200e] (使用 32 位元組的資料):
回覆自 2404:6800:4008:801::200e: 時間=14ms
回覆自 2404:6800:4008:801::200e: 時間=9ms
回覆自 2404:6800:4008:801::200e: 時間=16ms
回覆自 2404:6800:4008:801::200e: 時間=15ms

2404:6800:4008:801::200e 的 Ping 統計資料:
    封包: 已傳送 = 4，已收到 = 4，已遺失 = 0 (0% 遺失)，
大約的來回時間 (毫秒):
    最小值 = 9ms，最大值 = 16ms，平均 = 13ms

C:\Users\ASUS>tracert ipv6.google.com

在上限 30 個躍點上
追蹤 ipv6.l.google.com [2404:6800:4008:801::200e] 的路由:

  1    <1 ms    <1 ms    <1 ms  2405:9200:1110:1e:164d:67ff:fe62:5abc
  2     *        *        *     要求等候逾時。
  3    17 ms    22 ms     7 ms  2405:9200:1:0:172:16:28:169a
  4    11 ms    17 ms    10 ms  2405:9200:1:0:172:16:31:22a
  5    11 ms     8 ms     *     2404:0:10ff:1:7709:13:1596:812
  6    10 ms    17 ms     9 ms  2404:0:10ff::4:166
  7     9 ms    11 ms    10 ms  2404:0:10ff:1:7709:1:5169:61
  8    14 ms    21 ms    12 ms  2001:4860:0:1012::1
  9    13 ms    11 ms    10 ms  2001:4860:0:1::1e9d
 10    11 ms    11 ms    11 ms  tsa01s08-in-x0e.1e100.net [2404:6800:4008:801::200e]

追蹤完成。
```

TOTOLINK A950RG CM 測項5

✓ 確認用戶IPv6上網正常(test-ipv6.com)

測試你的 IPv6 連線。

總結 | 測試結果 | 分享結果 / 聯繫我們 | 其他 IPv6 網站

你在網際網路上的IPv4位址 123.241.153.196

你在網際網路上的IPv6位址 2405:9200:1110:1e:e80a:fa5f:5d7a:4bed

你的網路服務提供者 (ISP) 是 TBCOM-NET TBC

Since you have IPv6, we are including a tab that shows how well you can reach other IPv6 sites. [詳細資訊]

HTTPS 支援現已在本網站上提供。 [詳細資訊]

你的 DNS 伺服器 （可能由你的ISP維護）似乎支援 IPv6 的網際網路通訊協定。

你對於 IPv6 準備的分數

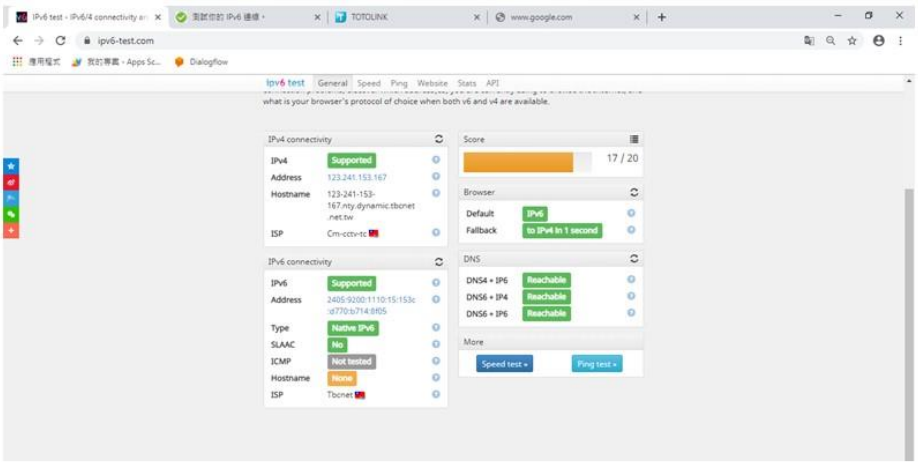
10/10

當網站陸續只使用 IPv6，請提早為您的 IPv6 做準備和設定

點擊查看 測試資料

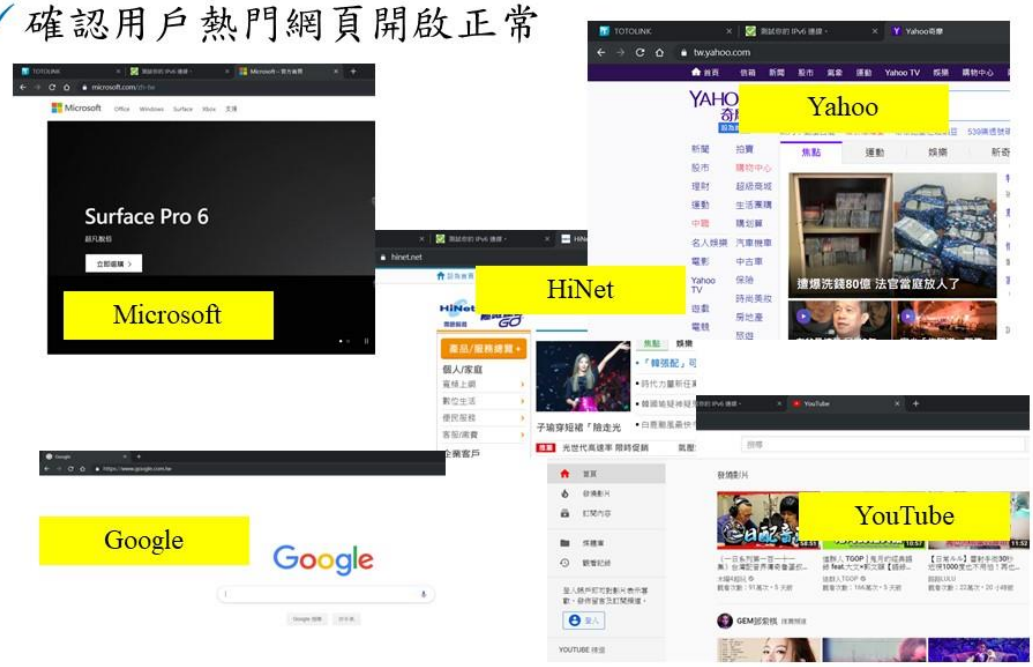
TOTOLINK A950RG CM 測項5(續)

✓ 確認用戶IPv6上網正常(ipv6-test.com)



TOTOLINK A950RG CM 測項6

✓ 確認用戶熱門網頁開啟正常



TOTOLINK A950RG CM 測項7

✓ 確認用戶上網速率正常



TOTOLINK A950RG CM 測項8

✓ 確認分享器重新連接cable modem之後，用戶ipv6相同，且連線正常

測試你的 IPv6 連線。

分享器重接CM前



測試你的 IPv6 連線。

分享器重接CM後



TOTOLINK A950RG CM 測項9

✓ 確認用戶使用IPv6乙太網路介面之MTU為1500

```
C:\Users\ASUS>netsh interface ipv6 show subinterface

   MTU  MediaSenseState   接收的位元組 傳送的位元組 介面
------  ---------------  ---------- ---------- -------------
  1500                1   138641282   73567671  乙太網路
4294967295                1           0    2199428  Loopback Pseudo-Interface 1
  1500                2    21697706    2307464  Wi-Fi
  1500                5           0       1088  區域連線* 2
  1500                5           0       2532  區域連線* 4
  1500                5           0        228  Bluetooth 網路連線
```

TOTOLINK A950RG CM 測項10

✓ 確認用戶連接Wi-Fi上網IPv6、DNSv6正常

無線區域網路介面卡 Wi-Fi:

```
連線特定 DNS 尾碼 . . . . . :
描述 . . . . . : Intel(R) Dual Band Wireless-AC 7265
實體位址 . . . . . : 34-02-86-63-18-11
DHCP 已啟用 . . . . . : 是
自動設定啟用 . . . . . : 是
IPv6 位址. . . . . : 2405:9200:1110:1e:80c3:57d2:60e7:e27a(偏好選項)
臨時 IPv6 位址. . . . . : 2405:9200:1110:1e:9c8d:a54f:cd60:c471(偏好選項)
連結-本機 IPv6 位址 . . . . . : fe80::80c3:57d2:60e7:e27a%8(偏好選項)
IPv4 位址 . . . . . : 192.168.0.5(偏好選項)
子網路遮罩 . . . . . : 255.255.255.0
租用取得 . . . . . : 2019年8月21日 下午 03:07:48
租用到期 . . . . . : 2019年8月22日 下午 03:07:48
預設閘道 . . . . . : fe80::164d:67ff:fe62:5abc%8
                     192.168.0.1
DHCP 伺服器 . . . . . : 192.168.0.1
DHCPv6 IAID . . . . . : 120849030
DHCPv6 用戶端 DUID. . . . . : 00-01-00-01-1C-CC-BE-EF-1C-B7-2C-1E-CB-0E
DNS 伺服器 . . . . . : 192.168.0.1
NetBIOS over Tcpip . . . . . : 啟用
```


TOTOLINK A950RG CM 測項11

✓ 確認用戶連接Wi-Fi IPv6上網正常(test-ipv6.com)

測試你的 IPv6 連線。

總結 | 測試結果 | 分享結果 / 聯繫我們 | 其他 IPv6 網站

- 你在網際網路上的IPv4位址 123.241.153.196
- 你在網際網路上的IPv6位址 2405:9200:1110:1e:9c8d:a54f:cd60:c471
- 你的網路服務提供者 (ISP) 是 TBCOM-NET TBC
- Since you have IPv6, we are including a tab that shows how well you can reach other IPv6 sites. [詳細資訊]
- HTTPS 支援現已在本網站上提供。 [詳細資訊]
- 你的 DNS 伺服器 （可能由你的ISP維護）似乎支援 IPv6 的網際網路通訊協定。

你對於 IPv6 準備的分數

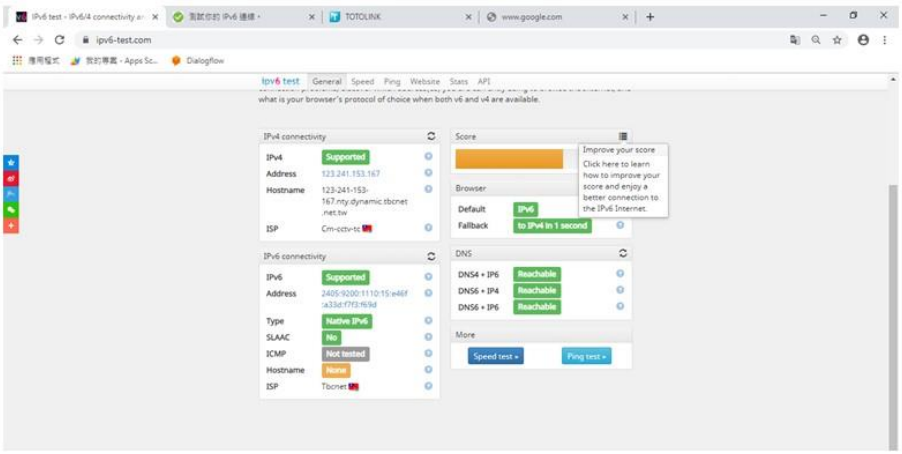
10/10

當網站陸續只使用 IPv6，請提早為您的 IPv6 做準備和設定

點擊查看 測試資料

TOTOLINK A950RG CM 測項11(續)

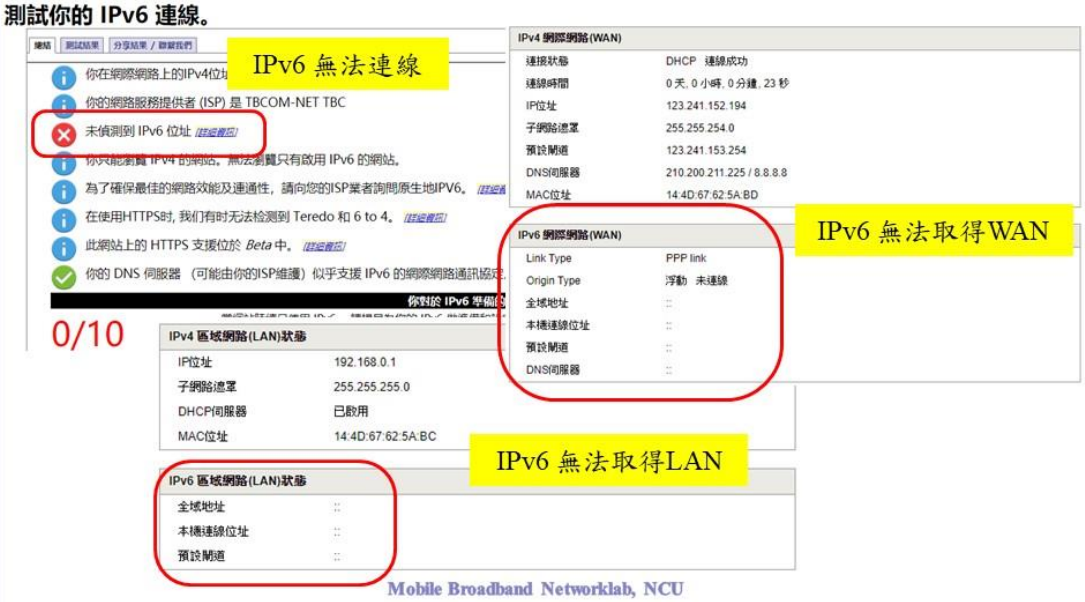
✓ 確認用戶連接Wi-Fi IPv6上網正常(ipv6-test.com)



TOTOLINK A950RG CM 測項12

✓ 確認IPv6 連線功能隨著IPv4啟用而自動啟用

❑ 重新Reset分享器後，依照介面指示設定後，無法使用IPv6



TOTOLINK A950RG CM 測項12 (續)

- ✓ 確認IPv6 連線功能隨著IPv4啟用而自動啟用
  - ❑ 需在IPv6設定中啟用IPv6 WAN及LAN



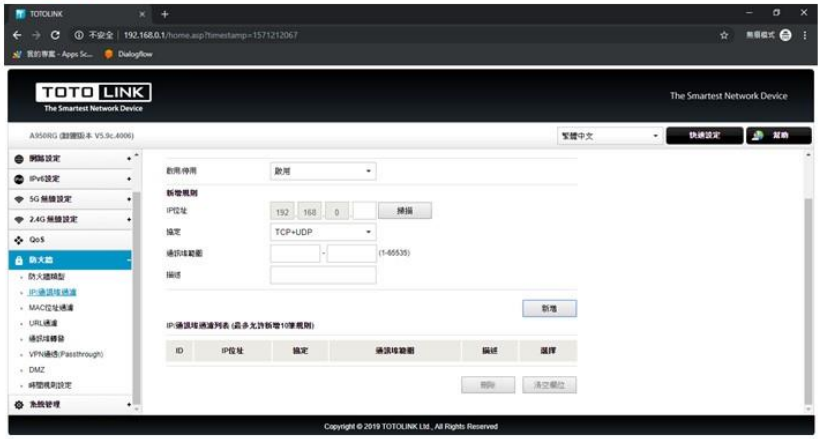
TOTOLINK A950RG CM 測項12 (續)

- ✓ 確認IPv6 連線功能隨著IPv4啟用而自動啟用
  - ❑ 設定完啟用IPv6後即可正常連線



TOTOLINK A950RG CM 測項13

- ✓ IPv6寬頻分享器IPv6 ACL功能是否正常?
  - 測試寬頻分享器 IPv6 ACL功能是否能限制用戶終端IPv6連線
  - 無支援 IPv6 ACL功能



Mobile Broadband Networklab, NCU

國立中央大學
National Central University

TOTOLINK A7000R
分享器測試成果

測試設備與環境

分享器產品設備資訊	
產品型號	A7000R
產品名稱	AC2600超世代Giga路由器
硬體版本	1.0
韌體版本	4.1cu.3965
製造年份	2019



硬體基本資料

測試環境資訊	
測試環境	1.HiNet光世代 PPPoE
	2.Cable IPoE
測試終端	Windows 10
終端瀏覽器	Chrome
測試時間	2019-08~2019-10



出廠年份: 2019年

測試紀錄摘要

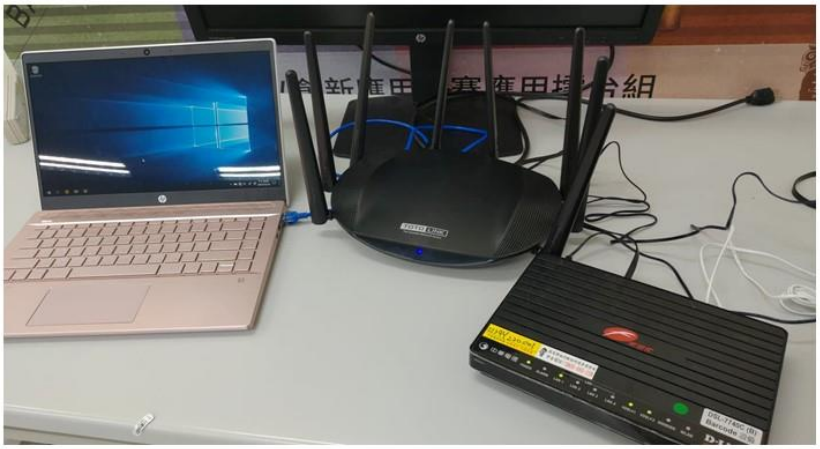
HiNet 光世代PPPoE測試		
	測試項目	A7000R
1	分享器PPPoE撥接是否正常?	O
2	分享器IPv6、IPv6 PD、DNSv6取得是否正常?	O
3	用戶IPv6、DNSv6取得是否正常?	O
4	用戶至HiNet路由是否正常?	O
5	用戶IPv6上網是否正常?	O
6	用戶熱門網頁開啟是否正常?	O
7	用戶上網速率是否正常?	O
8	分享器重撥，用戶IPv6更新是否正常?	O
9	用戶使用IPv6之MTU是否正常?	1484
10	用戶連接Wi-Fi上網IPv6、DNSv6是否正常?	O
11	用戶連接Wi-Fi IPv6上網是否正常?	O
12	IPv6 PPPoE（或是PPPoEv6)是否隨著IPv4 PPPoE啟用而自動啟用?	O
13	IPv6 PPPoE（或是PPPoEv6)連線之PPPoE Session是『Share with IPv4』或是『Create a new Session』?	無提供此項設定
14	IPv6寬頻分享器IPv6 ACL功能是否正常?	無支援IPv6 ACL功能

Cable IPoE測試		
	測試項目	A7000R
1	分享器連接Cable Modem是否正常?	O
2	分享器IPv6、IPv6 PD、DNSv6取得是否正常?	O
3	用戶IPv6、DNSv6取得是否正常?	O
4	用戶至Cable業者路由是否正常?	O
5	用戶IPv6上網是否正常?	O
6	用戶熱門網頁開啟是否正常?	O
7	用戶上網速率是否正常?	O
8	分享器重撥Cable Modem，用戶IPv6更新是否正常?	O
9	用戶使用IPv6之MTU是否正常?	1480
10	用戶連接Wi-Fi上網IPv6、DNSv6是否正常?	O
11	用戶連接Wi-Fi IPv6上網是否正常?	O
12	IPv6連線功能是否隨著IPv4啟用而自動啟用?	X
13	IPv6寬頻分享器IPv6 ACL功能是否正常?	無支援IPv6 ACL功能

測試紀錄摘要說明

- ✓ HiNet PPPoE環境 (Pass測項:13/14)
  - 測項13: 無提供此項設定
  - 測項14: 無支援IPv6 ACL功能
- ✓ Cable IPoE環境(Pass測項:10/13)
  - 測項9: MTU為1480，非1500
  - 測項12: 需要手動啟用IPv6
  - 測項13: 無支援IPv6 ACL功能

分享器測試紀錄
HiNet 光世代 PPPoE環境



TOTOLINK A7000R PPPoE 測項1

✓ 確認分享器PPPoE撥接正常

附註:需使用chrome以外瀏覽器開啟分享器網頁介面

IPv6 網際網路(WAN)	
連線狀態	PPPoE 已連線
IPv6位址	2001:b011:6cc0:4b39:c55e:6a96:391c:4f0c/64/64
預設閘道	fe80::d2f0:dbff:fe53:800
主要DNS	2001:b000:168::2
次要DNS	2001:b000:168::1

WAN端位址資訊

TOTOLINK A7000R PPPoE 測項2

✓ 確認分享器IPv6、IPv6 PD、DNSv6取得正常

IPv6 網際網路(WAN)	
連線狀態	PPPoE 已連線
IPv6位址	2001:b011:6cc0:4b39:c55e:6a96:391c:4f0c/64/64
預設閘道	fe80::d2f0:dbff:fe53:800
主要DNS	2001:b000:168::2
次要DNS	2001:b000:168::1

WAN端位址資訊

Prefix

IPv6 區域網路(LAN)狀態	
IPv6位址類型	RADVD+SLAAC
IPv6位址	2001:b011:6cc0:51a9::1/64
本機連線位址	fe80::164d:67ff:fe5a:c440/64

LAN端位址資訊

TOTOLINK A7000R PPPoE 測項3

✓ 確認用戶IPv6、DNSv6取得正常

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Physical Address. . . . . . . . . : 04-92-26-6E-D1-F8
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:b011:6cc0:51a9:1ce7:3c77:5218:7258(Preferred)
   Temporary IPv6 Address. . . . . . : 2001:b011:6cc0:51a9:79c5:c0d7:7b90:8c13(Preferred)
   Link-local IPv6 Address . . . . . : fe80::1ce7:3c77:5218:7258%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.2(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, August 14, 2019 4:29:03 PM
   Lease Expires . . . . . . . . . . : Thursday, August 15, 2019 4:33:36 PM
   Default Gateway . . . . . . . . . : fe80::164d:67ff:fe5a:c440%3
                                       192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 33853990
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-47-2F-7E-04-92-26-6E-D1-F8
   DNS Servers . . . . . . . . . . . : 2001:b000:168::2
                                       2001:b000:168::1
                                       192.168.0.1
                                       192.168.0.1
                                       2001:b000:168::2
                                       2001:b000:168::1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```


TOTOLINK A7000R PPPoE 測項4

✓ 確認用戶至HiNet路由正常

```
C:\Users\Hestia>ping ipv6.google.com

Pinging ipv6.l.google.com [2404:6800:4012::200e] with 32 bytes of data:
Reply from 2404:6800:4012::200e: time=11ms
Reply from 2404:6800:4012::200e: time=13ms
Reply from 2404:6800:4012::200e: time=13ms
Reply from 2404:6800:4012::200e: time=11ms

Ping statistics for 2404:6800:4012::200e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 13ms, Average = 12ms

C:\Users\Hestia>tracert ipv6.google.com

Tracing route to ipv6.l.google.com [2404:6800:4012::200e]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  2001-b011-6cc0-51a9-0000-0000-0000-0001.dynamic-ip6.hinet.net [2001:b011:6cc0:51a9::1]
  2    10 ms    10 ms    13 ms  2001:b010:ffff::1
  3    11 ms    10 ms    10 ms  2001-b000-0089-0005-0021-2222-0002-0002.hinet-ip6.hinet.net [2001:b000:89:5:21:2222:2:2]
  4     *        *        *     Request timed out.
  5    14 ms    11 ms    11 ms  2001-b000-0088-0004-3015-3305-0011-000b.hinet-ip6.hinet.net [2001:b000:88:4:3015:3305:11:b]
  6    12 ms    10 ms    11 ms  2001:4860:1:1::c70
  7    13 ms    13 ms    13 ms  2001:4860:0:1012::1
  8    12 ms    11 ms    12 ms  2001:4860:0:1::2b33
  9    12 ms    12 ms    12 ms  tsa01s09-in-x0e.1e100.net [2404:6800:4012::200e]

Trace complete.
```

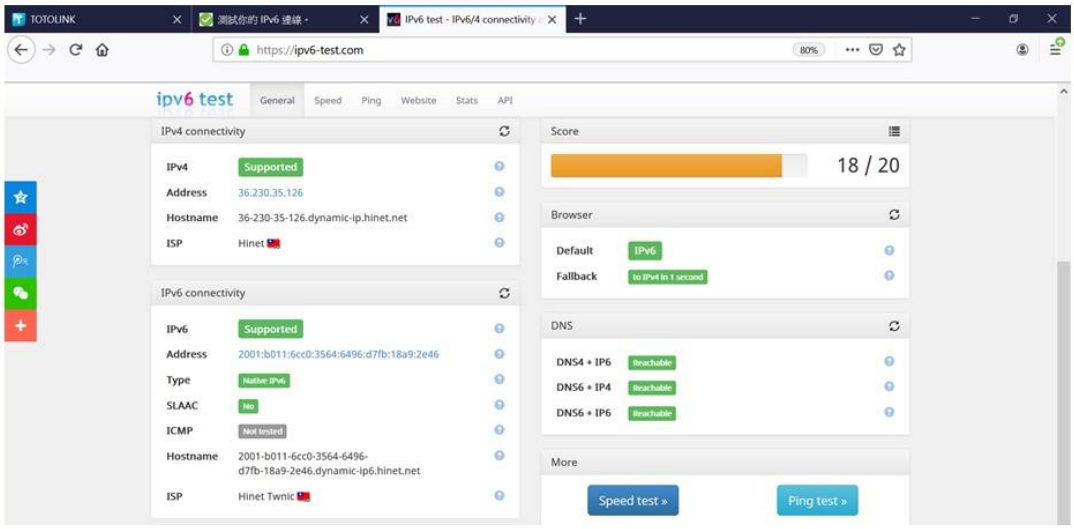
TOTOLINK A7000R PPPoE 測項5

✓ 確認用戶IPv6上網正常(test-ipv6.com)



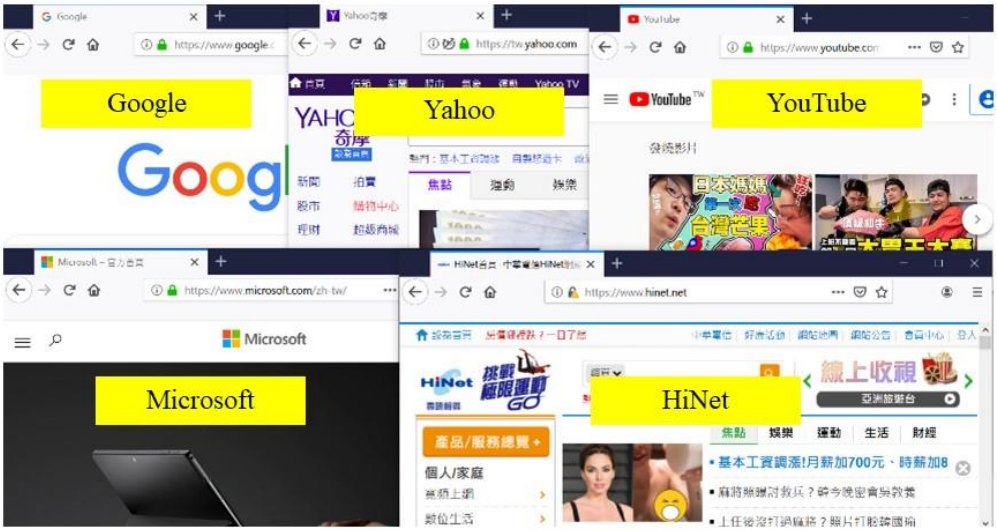
TOTOLINK A7000R PPPoE 測項5 (續)

✓ 確認用戶IPv6上網正常(ipv6-test.com)



TOTOLINK A7000R PPPoE 測項6

✓ 確認用戶熱門網頁開啟正常



TOTOLINK A7000R PPPoE 測項7

✓ 確認用戶上網速率正常



TOTOLINK A7000R PPPoE 測項8

✓ 確認分享器重撥，用戶IPv6更新正常

測試你的 IPv6 連線。

分享器重撥之前



測試你的 IPv6 連線。

分享器重撥之後



TOTOLINK A7000R PPPoE 測項9

✓ 確認用戶使用IPv6之MTU**不為1492**

- MTU設定為1492，但實際測試為1484




```
C:\Users\Hestia>netsh interface ipv6 show subinterface

   MTU  MediaSenseState   Bytes In  Bytes Out  Interface
------  ---------------  ---------  ---------  -------------
4294967295                1          0    1880604  Loopback Pseudo-Interface 1
  1500                2  105317689    3526049  Wi-Fi
  1484                1  264954518   50878591  Ethernet
  1500                5          0      18811  Local Area Connection* 2
  1500                5          0      45415  Bluetooth Network Connection
  1500                5          0      25080  Local Area Connection* 3
  1400                5          0     104094  Local Area Connection* 1
 65536                1          0     358313  Ethernet 2
```

TOTOLINK A7000R PPPoE 測項10

✓ 確認用戶連接Wi-Fi上網IPv6、DNSv6正常

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wireless-AC 9560
   Physical Address. . . . . . . . . : 48-A4-72-42-63-96
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:b011:6cc0:52e3:f115:d539:9dc9:ab66(Preferred)
   Temporary IPv6 Address. . . . . . : 2001:b011:6cc0:52e3:dd29:ed58:e9e7:55b9(Preferred)
   Link-local IPv6 Address . . . . . : fe80::f115:d539:9dc9:ab66%13(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.3(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, August 14, 2019 6:43:25 PM
   Lease Expires . . . . . . . . . . : Thursday, August 15, 2019 6:43:24 PM
   Default Gateway . . . . . . . . . : fe80::164d:67ff:fe5a:c440%13
                                       192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 222864498
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-47-2F-7E-04-92-26-6E-D1-F8
   DNS Servers . . . . . . . . . . . : 2001:b000:168::2
                                       2001:b000:168::1
                                       192.168.0.1
                                       192.168.0.1
                                       2001:b000:168::2
                                       2001:b000:168::1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```


TOTOLINK A7000R PPPoE 測項11

✓ 確認用戶連接Wi-Fi IPv6上網正常(test-ipv6.com)

測試你的 IPv6 連線。

總結 | 測試結果 | 分享結果 / 聯繫我們 | 其他 IPv6 網站

- 你在網際網路上的IPv4位址 36.230.24.13
- 你在網際網路上的IPv6位址 2001:b011:6cc0:52e3:dd29:ed58:e9e7:55b9
- 你的網路服務提供者 (ISP) 是 HINET Data Communication Business Group
- Since you have IPv6, we are including a tab that shows how well you can reach other IPv6 sites.
- 此網站上的 HTTPS 支援位於 *Beta* 中。 [詳細資訊]
- 你的 DNS 伺服器 （可能由你的ISP維護）似乎支援 IPv6 的網際網路通訊協定。

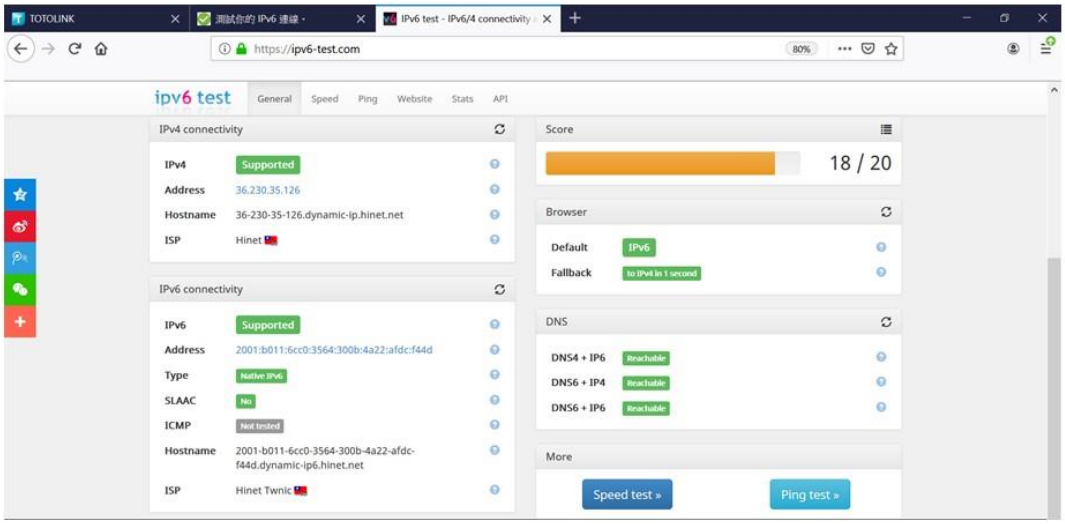
你對於 IPv6 準備的分數

10/10

當網站陸續只使用 IPv6，請提早為您的 IPv6 做準備和設定

TOTOLINK A7000R PPPoE 測項11(續)

✓ 確認用戶連接Wi-Fi IPv6上網正常(ipv6-test.com)



TOTOLINK A7000R PPPoE 測項12

✓ IPv6 PPPoE (或是PPPoEv6)是否隨著IPv4 PPPoE啟用而自動啟用

❑ 重啟IPv4連線設定後，IPv6連線功能自動啟用正常



TOTOLINK A7000R PPPoE 測項13

- ✓ IPv6 PPPoE (或是PPPoEv6)連線之PPPoE Session是『Share with IPv4』或是『Create a new Session』?
  - ❑ 本分享器無提供此功能

TOTOLINK A7000R PPPoE 測項14

- ✓ IPv6寬頻分享器IPv6 ACL功能是否正常?
  - ☐ 測試寬頻分享器 IPv6 ACL功能是否能限制用戶終端IPv6連線
  - ☐ 無支援 IPv6 ACL功能



分享器測試紀錄
Cable 寬頻 IPoE環境



22

TOTOLINK A7000R CM 測項1

✓ 確認連接cable modem正常

IPv6 網際網路(WAN)	
連線狀態	動態IP 已連線
IPv6位址	2405:9200:1125::15
預設閘道	fe80::201:5cff:fea1:1646
主要DNS	2404::1
次要DNS	2001:b000:168::1

Mobile Broadband Networklab, NCU

TOTOLINK A7000R CM 測項2

✓ 確認取得IPv6、IPv6 PD、DNSv6

IPv6 網際網路(WAN)

連線狀態	動態IP 已連線
IPv6位址	2405:9200:1125::15
預設閘道	fe80::201:5cff:fea1:1646
主要DNS	2404::1
次要DNS	2001:b000:168::1

WAN端位址資訊

IPv6 區域網路(LAN)狀態

IPv6位址類型	RADVD+SLAAC
IPv6位址	2405:9200:1110:1d::1/64
本機連線位址	fe80::164d:67ff:fe5a:c440/64

LAN端位址資訊

TOTOLINK A7000R CM 測項3

✓ 確認用戶IPv6、DNSv6取得正常

```
乙太網路卡 乙太網路:

   連線特定 DNS 尾碼 . . . . . . . . :
   描述 . . . . . . . . . . . . . . : Realtek PCIe FE Family Controller
   實體位址 . . . . . . . . . . . . : 6C-2B-59-56-E5-DB
   DHCP 已啟用 . . . . . . . . . . . : 是
   自動設定啟用 . . . . . . . . . . . : 是
   IPv6 位址. . . . . . . . . . . . : 2405:9200:1110:1d:1089:df90:502:6cf9(偏好選項)
   臨時 IPv6 位址. . . . . . . . . . : 2405:9200:1110:1d:25e1:f73c:850a:b865(偏好選項)
   連結-本機 IPv6 位址 . . . . . . . : fe80::1089:df90:502:6cf9%8(偏好選項)
   IPv4 位址 . . . . . . . . . . . . : 192.168.0.3(偏好選項)
   子網路遮罩 . . . . . . . . . . . : 255.255.255.0
   租用取得 . . . . . . . . . . . . : 2019年8月21日 下午 02:28:06
   租用到期 . . . . . . . . . . . . : 2019年8月22日 下午 02:28:06
   預設閘道 . . . . . . . . . . . . : fe80::164d:67ff:fe5a:c440%8
                                       192.168.0.1
   DHCP 伺服器 . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 72632336
   DHCPv6 用戶端 DUID. . . . . . . . : 00-01-00-01-24-92-58-57-6C-2B-59-56-E5-DB
   DNS 伺服器 . . . . . . . . . . . : 2404::1
                                       2001:b000:168::1
                                       192.168.0.1
                                       192.168.0.1
   NetBIOS over Tcpip . . . . . . . : 啟用
```

TOTOLINK A7000R CM 測項4

✓ 確認用戶至google ipv6路由正常

```
C:\Users\User>ping ipv6.google.com

Ping ipv6.l.google.com [2404:6800:4008:801::200e] (使用 32 位元組的資料):
回覆自 2404:6800:4008:801::200e: 時間=11ms
回覆自 2404:6800:4008:801::200e: 時間=14ms
回覆自 2404:6800:4008:801::200e: 時間=12ms
回覆自 2404:6800:4008:801::200e: 時間=22ms

2404:6800:4008:801::200e 的 Ping 統計資料:
    封包: 已傳送 = 4，已收到 = 4, 已遺失 = 0 (0% 遺失)，
大約的來回時間 (毫秒):
    最小值 = 11ms，最大值 = 22ms，平均 = 14ms

C:\Users\User>tracert ipv6.google.com

在上限 30 個躍點上
追蹤 ipv6.l.google.com [2404:6800:4008:801::200e] 的路由:

  1     3 ms     2 ms     1 ms  2405:9200:1110:1d::1
  2     *        *        *     要求等候逾時。
  3     8 ms     8 ms     7 ms  2405:9200:1:0:172:16:28:169a
  4    13 ms    17 ms     9 ms  2405:9200:1:0:172:16:31:22a
  5    11 ms    12 ms     9 ms  2404:0:10ff:1:7709:13:1596:1212
  6    21 ms    17 ms    10 ms  2404:0:10ff::5:66
  7    11 ms    10 ms    10 ms  2404:0:10ff:1:7709:1:5169:61
  8    12 ms    15 ms    15 ms  2001:4860:0:1011::1
  9    10 ms    12 ms    11 ms  2001:4860:0:1::1e9f
 10    11 ms    15 ms    14 ms  tsa01s08-in-x0e.1e100.net [2404:6800:4008:801::200e]

追蹤完成。
```

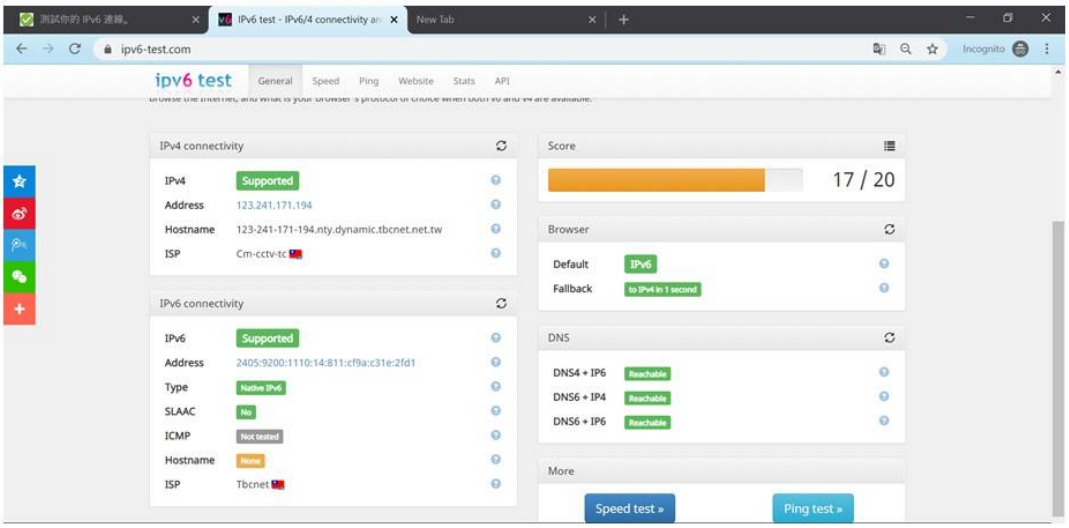

TOTOLINK A7000R CM 測項5

✓ 確認用戶IPv6上網正常(test-ipv6.com)



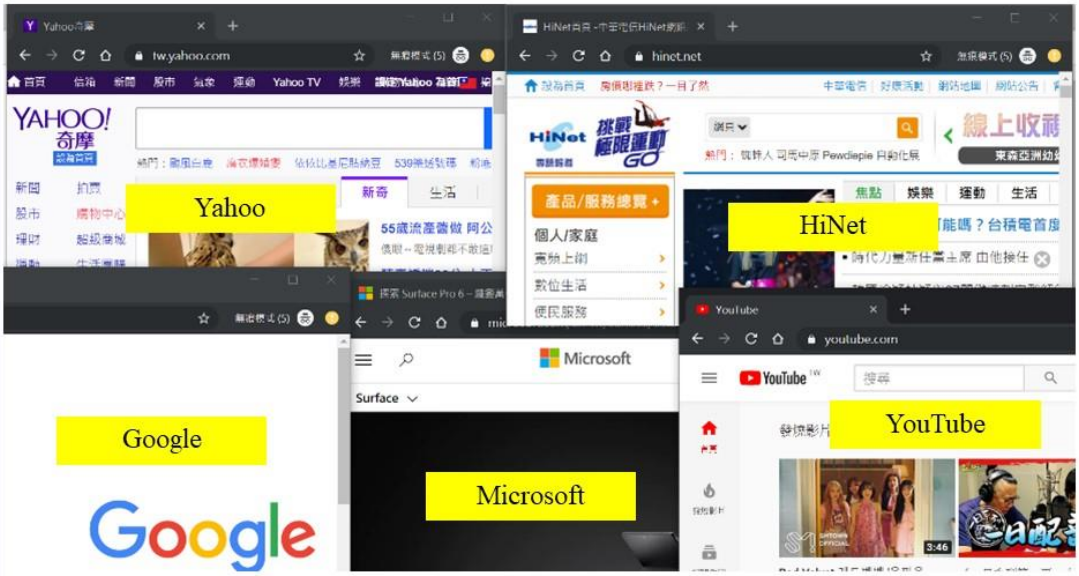
TOTOLINK A7000R CM 測項5(續)

✓ 確認用戶IPv6上網正常(ipv6-test.com)



TOTOLINK A7000R CM 測項6

✓ 確認用戶熱門網頁開啟正常



TOTOLINK A7000R CM 測項7

✓ 確認用戶上網速率正常



TOTOLINK A7000R CM 測項8

✓ 確認分享器重新連接cable modem之後，用戶ipv6相同，且連線正常

分享器重接CM前



分享器重接CM後



TOTOLINK A7000R CM 測項9

✓ 確認用戶使用IPv6之MTU不為1500

- MTU設定為1500，但實際測試為1480

```
C:\Users\User>netsh interface ipv6 show subinterface

   MTU  MediaSenseState   接收的位元組 傳送的位元組  介面
------  ---------------  ---------  ---------  -------------
4294967295                1          0    1278347  Loopback Pseudo-Interface 1
  1500                2    1719191     660262  Wi-Fi
  1480                1   27262107    2753629  乙太網路
  1500                5          0        152  區域連線* 1
  1500                5          0       1022  藍牙網路連線
  1500                5          0        152  區域連線* 2
  1500                1       1016     785857  VirtualBox Host-Only Network
  1500                1          0      85370  Npcap Loopback Adapter
```


TOTOLINK A7000R CM 測項10

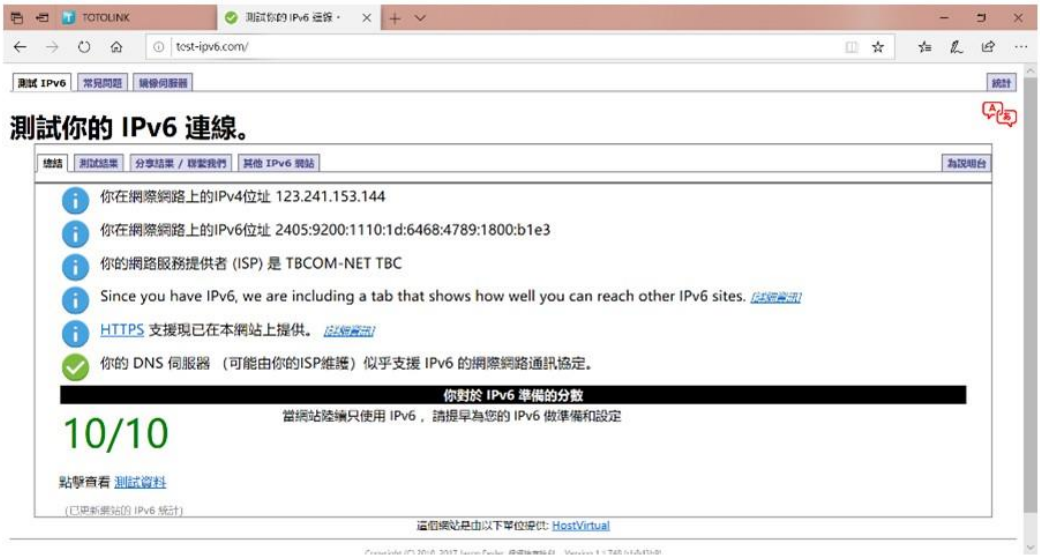
✓ 確認用戶連接Wi-Fi上網IPv6、DNSv6正常

```
無線區域網路介面卡 Wi-Fi:

   連線特定 DNS 尾碼 . . . . . . . . :
   描述 . . . . . . . . . . . . . . : Intel(R) Wireless-AC 9462
   實體位址 . . . . . . . . . . . . : D8-F2-CA-70-16-24
   DHCP 已啟用 . . . . . . . . . . . : 是
   自動設定啟用 . . . . . . . . . . . : 是
   IPv6 位址. . . . . . . . . . . . : 2405:9200:1110:1d:9d13:fcbc:8da3:a687(偏好選項)
   臨時 IPv6 位址. . . . . . . . . . : 2405:9200:1110:1d:6468:4789:1800:b1e3(偏好選項)
   連結-本機 IPv6 位址 . . . . . . . : fe80::9d13:fcbc:8da3:a687%9(偏好選項)
   IPv4 位址 . . . . . . . . . . . . : 192.168.0.4(偏好選項)
   子網路遮罩 . . . . . . . . . . . : 255.255.255.0
   租用取得 . . . . . . . . . . . . : 2019年8月21日 下午 03:12:49
   租用到期 . . . . . . . . . . . . : 2019年8月22日 下午 03:12:48
   預設閘道 . . . . . . . . . . . . : fe80::164d:67ff:fe5a:c440%9
                                       192.168.0.1
   DHCP 伺服器 . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 114881226
   DHCPv6 用戶端 DUID. . . . . . . . : 00-01-00-01-24-92-58-57-6C-2B-59-56-E5-DB
   DNS 伺服器 . . . . . . . . . . . : 2404::1
                                       2001:b000:168::1
                                       192.168.0.1
                                       192.168.0.1
   NetBIOS over Tcpip . . . . . . . : 啟用
```

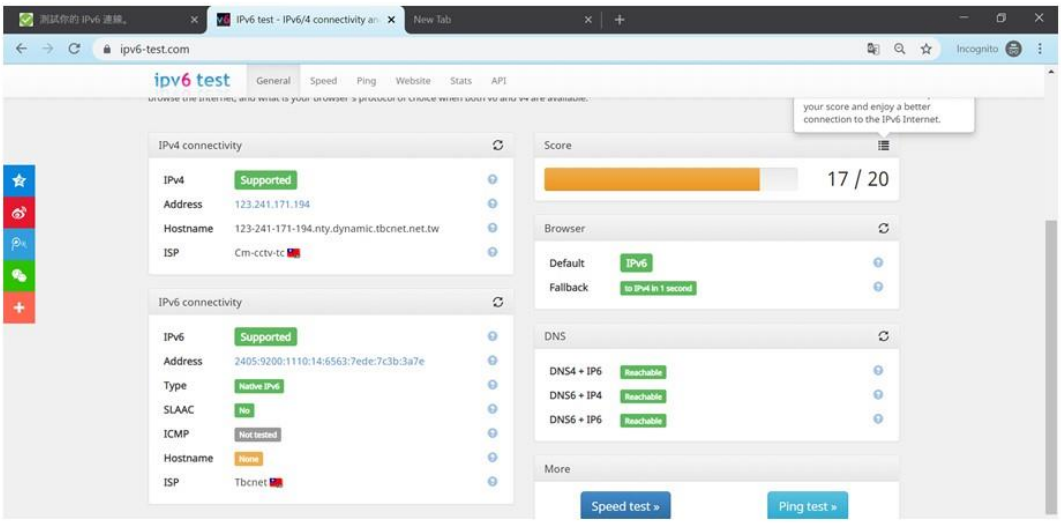
TOTOLINK A7000R CM 測項11

✓ 確認用戶連接Wi-Fi IPv6上網正常(test-ipv6.com)



TOTOLINK A7000R CM 測項11(續)

✓ 確認用戶連接Wi-Fi IPv6上網正常(ipv6-test.com)



TOTOLINK A7000R CM 測項12

- ✓ 確認IPv6 連線功能隨著IPv4啟用而自動啟用
  - ❑ 重新Reset分享器後，依照介面指示設定後，無法使用IPv6



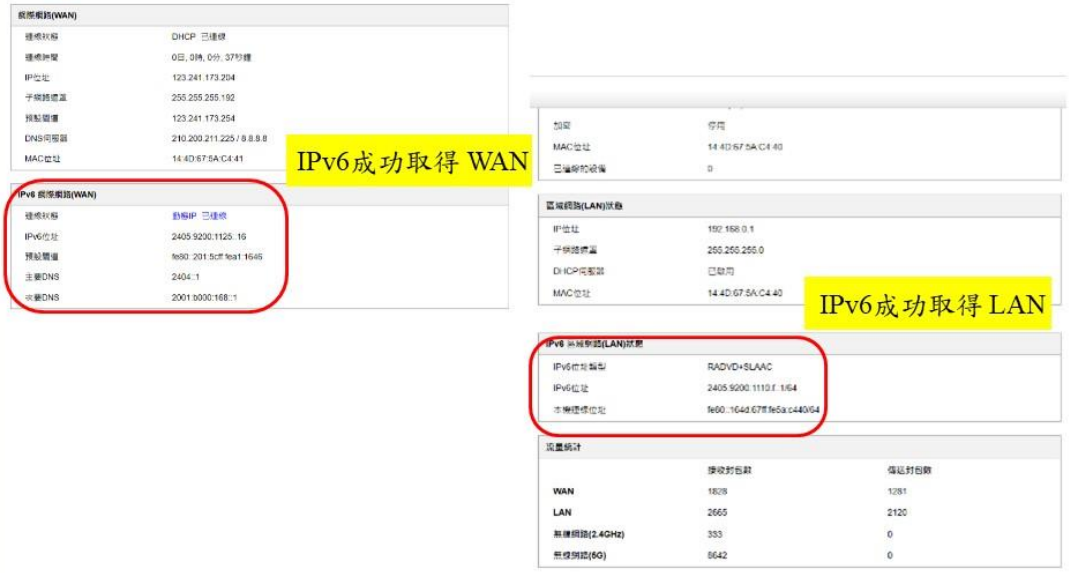
TOTOLINK A7000R CM 測項12 (續)

- ✓ 確認IPv6 連線功能隨著IPv4啟用而自動啟用
  - ❑ 需在IPv6設定中啟用IPv6



TOTOLINK A7000R CM 測項12 (續)

- ✓ 確認IPv6 連線功能隨著IPv4啟用而自動啟用
  - ❑ 設定完啟用IPv6後即可正常連線



TOTOLINK A7000R CM 測項13

- ✓ IPv6寬頻分享器IPv6 ACL功能是否正常?
  - ❑ 測試寬頻分享器 IPv6 ACL功能是否能限制用戶終端IPv6連線
  - ❑ 無支援 IPv6 ACL功能



TP-LINK Archer C1200

分享器測試成果

測試設備與環境

分享器產品設備資訊	
產品型號	Archer C1200
產品名稱	AC1200 無線雙頻Gigabit 路由器
硬體版本	3.0
韌體版本	3.0.4
製造年份	2018



測試環境資訊	
測試環境	1.HiNet光世代 PPPoE
	2.Cable IPoE
測試終端	Windows 10
終端瀏覽器	Chrome
測試時間	2019-08~2019-10



Mobile Broadband Networklab, NCU

測試紀錄摘要

HiNet 光世代PPPoE測試		
	測試項目	AC1200
1	分享器PPPoE撥接是否正常?	O
2	分享器IPv6、IPv6 PD、DNSv6取得是否正常?	O
3	用戶IPv6、DNSv6取得是否正常?	O
4	用戶至HiNet路由是否正常?	O
5	用戶IPv6上網是否正常?	O
6	用戶熱門網頁開啟是否正常?	O
7	用戶上網速率是否正常?	O
8	分享器重撥，用戶IPv6更新是否正常?	O
9	用戶使用IPv6之MTU是否正常?	1492
10	用戶連接Wi-Fi上網IPv6、DNSv6是否正常?	O
11	用戶連接Wi-Fi IPv6上網是否正常?	O
12	IPv6 PPPoE（或是PPPoEv6)是否隨著IPv4 PPPoE啟用而自動啟用?	X
13	IPv6 PPPoE（或是PPPoEv6)連線之PPPoE Session是『Share with IPv4』或是『Create a new Session』?	可設定兩種模式
14	IPv6寬頻分享器IPv6 ACL功能是否正常?	無支援IPv6 ACL功能

Cable IPoE測試		
	測試項目	AC1200
1	分享器連接Cable Modem是否正常?	O
2	分享器IPv6、IPv6 PD、DNSv6取得是否正常?	O
3	用戶IPv6、DNSv6取得是否正常?	O
4	用戶至Cable業者路由是否正常?	O
5	用戶IPv6上網是否正常?	O
6	用戶熱門網頁開啟是否正常?	O
7	用戶上網速率是否正常?	O
8	分享器重撥Cable Modem，用戶IPv6更新是否正常?	O
9	用戶使用IPv6之MTU是否正常?	1492
10	用戶連接Wi-Fi上網IPv6、DNSv6是否正常?	O
11	用戶連接Wi-Fi IPv6上網是否正常?	O
12	IPv6連線功能是否隨著IPv4啟用而自動啟用?	X
13	IPv6寬頻分享器IPv6 ACL功能是否正常?	無支援IPv6 ACL功能

測試紀錄摘要說明

- ✓ HiNet PPPoE環境 (Pass測項:12/14)
  - 測項12: 需要手動啟用IPv6
  - 測項14: 無支援IPv6 ACL功能
- ✓ Cable IPoE環境(Pass測項:10/13)
  - 測項9: MTU為1492，非1500
  - 測項12: 需要手動啟用IPv6
  - 測項13: 無支援IPv6 ACL功能

分享器測試紀錄
HiNet 光世代 PPPoE環境



5

TP-LINK AC1200 PPPoE 測項1

✓ 確認分享器PPPoE撥接正常



WAN端位址資訊

Mobile Broadband Networklab, NCU

TP-LINK AC1200 PPPoE 測項2

✓ 確認分享器IPv6、IPv6 PD、DNSv6取得正常



TP-LINK AC1200 PPPoE 測項3

✓ 確認用戶IPv6、DNSv6取得正常

乙太網路卡 乙太網路:

```
   連線特定 DNS 尾碼 . . . . . . . . :
   描述 . . . . . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   實體位址 . . . . . . . . . . . . . : 1C-B7-2C-1E-CB-0E
   DHCP 已啟用 . . . . . . . . . . . : 是
   自動設定啟用 . . . . . . . . . . . : 是
   IPv6 位址. . . . . . . . . . . . . : 2001:b011:6cc0:308f:a032:c63b:766e:c8d4(偏好選項)
   臨時 IPv6 位址. . . . . . . . . . . : 2001:b011:6cc0:308f:3865:354c:255a:b89d(偏好選項)
   連結-本機 IPv6 位址 . . . . . . . . : fe80::a032:c63b:766e:c8d4%11(偏好選項)
   IPv4 位址 . . . . . . . . . . . . . : 192.168.0.126(偏好選項)
   子網路遮罩 . . . . . . . . . . . . : 255.255.255.0
   租用取得 . . . . . . . . . . . . . : 2019年8月7日 上午 10:17:38
   租用到期 . . . . . . . . . . . . . : 2019年8月7日 下午 12:17:35
   預設閘道 . . . . . . . . . . . . . : fe80::da0d:17ff:fe34:d794%11
                                        192.168.0.1
   DHCP 伺服器 . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 52213548
   DHCPv6 用戶端 DUID. . . . . . . . : 00-01-00-01-1C-CC-BE-EF-1C-B7-2C-1E-CB-0E
   DNS 伺服器 . . . . . . . . . . . . : 2001:b000:168::2
                                        2001:b000:168::1
                                        192.168.0.1
   NetBIOS over Tcpip . . . . . . . . : 啟用
```

TP-LINK AC1200 PPPoE 測項4

✓ 確認用戶至HiNet路由正常

```
C:\Users\ASUS>ping dns.hinet.net

Ping dns.hinet.net [2001:b000:168::2] (使用 32 位元組的資料):
回覆自 2001:b000:168::2: 時間=11ms
回覆自 2001:b000:168::2: 時間=11ms
回覆自 2001:b000:168::2: 時間=11ms
回覆自 2001:b000:168::2: 時間=10ms

2001:b000:168::2 的 Ping 統計資料:
    封包: 已傳送 = 4，已收到 = 4，已遺失 = 0 (0% 遺失)，
大約的來回時間 (毫秒):
    最小值 = 10ms，最大值 = 11ms，平均 = 10ms

C:\Users\ASUS>tracert dns.hinet.net

在上限 30 個躍點上
追蹤 dns.hinet.net [2001:b000:168::2] 的路由:

  1    <1 ms    <1 ms    <1 ms  2001-b011-6cc0-308f-da0d-17ff-fe34-d794.dynamic-ip6.hinet.net [2001:b011:6cc0:308f:da0d:17ff:fe34:
d794]
  2     9 ms     9 ms    10 ms  2001:b010:ffff::1
  3    11 ms    10 ms    10 ms  2001-b000-0089-0005-0022-2222-0002-0002.hinet-ip6.hinet.net [2001:b000:89:5:22:2222:2:2]
  4     *        *      186 ms  2001-b000-0080-0003-0080-0089-0022-000a.hinet-ip6.hinet.net [2001:b000:80:3:80:89:22:a]
  5   207 ms   215 ms   216 ms  2001-b000-0080-0004-3022-3012-0005-000b.hinet-ip6.hinet.net [2001:b000:80:4:3022:3012:5:b]
  6   243 ms   247 ms   255 ms  2001-b000-0080-0004-3022-3012-0005-000b.hinet-ip6.hinet.net [2001:b000:80:4:3022:3012:5:b]
  7   276 ms   289 ms   304 ms  2001-b000-0080-0004-3012-3312-0011-000b.hinet-ip6.hinet.net [2001:b000:80:4:3012:3312:11:b]
  8     *        *        *     要求等候逾時。
  9   119 ms   121 ms   121 ms  dns.hinet.net [2001:b000:168::2]

追蹤完成。
```

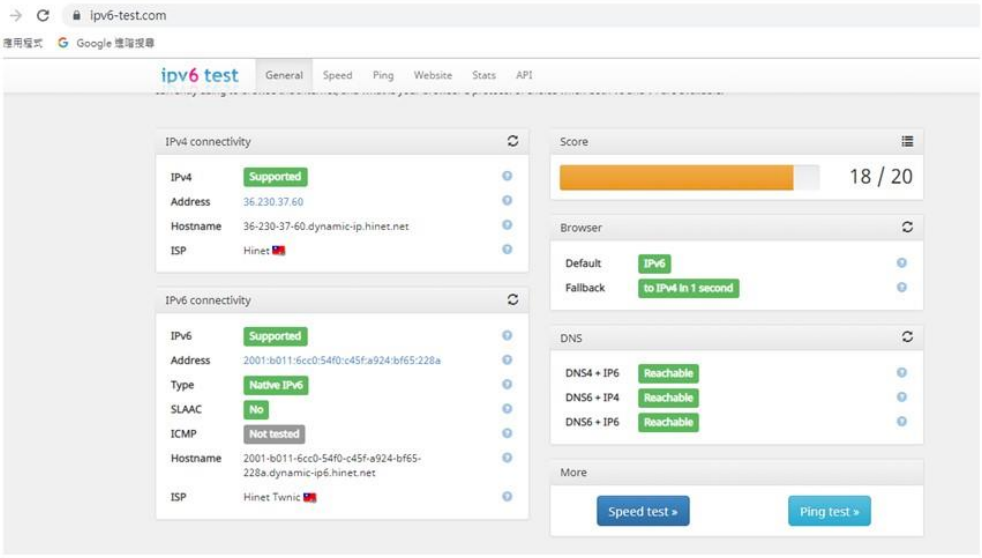

TP-LINK AC1200 PPPoE 測項5

✓ 確認用戶IPv6上網正常(test-ipv6.com)



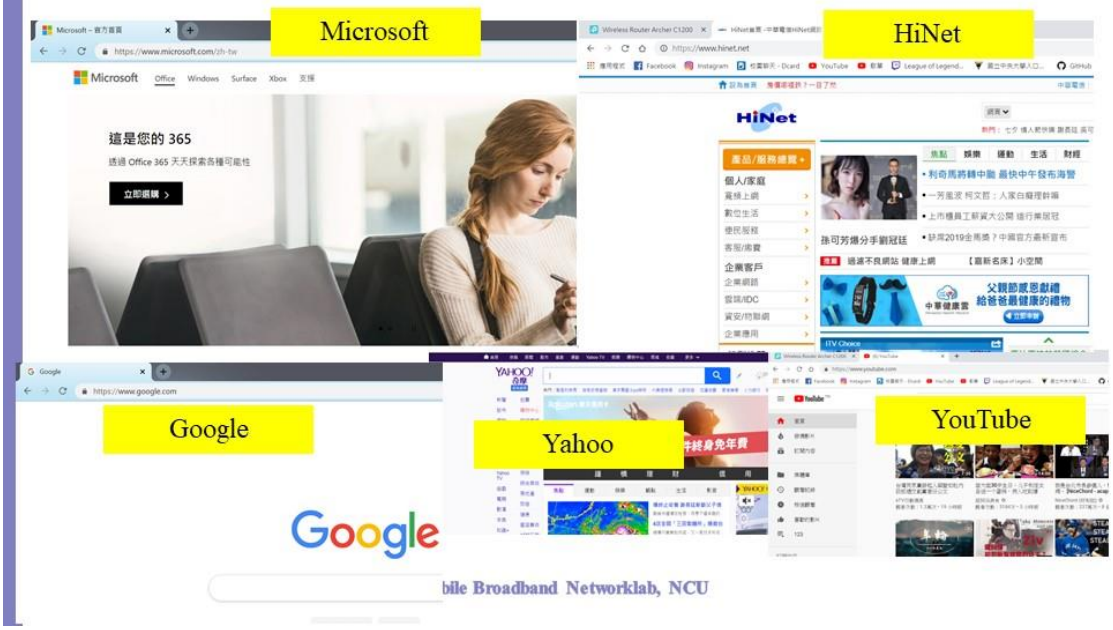
TP-LINK AC1200 PPPoE 測項5(續)

✓ 確認用戶IPv6上網正常(ipv6-test.com)



TP-LINK AC1200 PPPoE 測項6

✓ 確認用戶熱門網頁開啟正常



TP-LINK AC1200 PPPoE 測項7

✓ 確認用戶上網速率正常

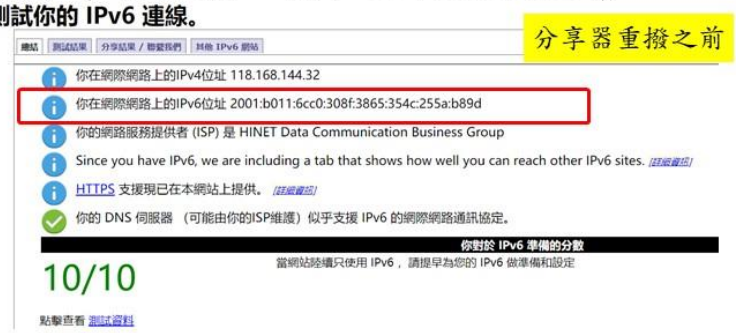


TP-LINK AC1200 PPPoE 測項8

✓ 確認分享器重撥，用戶IPv6更新正常

測試你的 IPv6 連線。

分享器重撥之前



測試你的 IPv6 連線。

分享器重撥之後



TP-LINK AC1200 PPPoE 測項9

✓ 確認用戶使用IPv6之MTU正常 (1492)

```
C:\Users\ASUS>netsh interface ipv6 show subinterface

   MTU  MediaSenseState   接收的位元組 傳送的位元組  介面
------  ---------------  ---------  ---------  -------------
  1492                1   45682651    3186315  乙太網路
4294967295            1          0     139450  Loopback Pseudo-Interface 1
  1500                2    1454123     137604  Wi-Fi
  1500                5          0       1616  區域連線* 2
  1500                5          0       1616  區域連線* 4
  1500                5          0       1616  Bluetooth 網路連線
```


TP-LINK AC1200 PPPoE 測項10

✓ 確認用戶連接Wi-Fi上網IPv6、DNSv6正常

```
無線區域網路介面卡 Wi-Fi:

   連線特定 DNS 尾碼 . . . . . . . . :
   描述 . . . . . . . . . . . . . . : Intel(R) Wireless-AC 9462
   實體位址 . . . . . . . . . . . . : D8-F2-CA-70-16-24
   DHCP 已啟用 . . . . . . . . . . . : 是
   自動設定啟用 . . . . . . . . . . . : 是
   IPv6 位址. . . . . . . . . . . . : 2001:b011:6cc0:308f:9d13:fcbc:8da3:a687(偏好選項)
   臨時 IPv6 位址. . . . . . . . . . : 2001:b011:6cc0:308f:8deb:3e9b:38de:326b(偏好選項)
   連結-本機 IPv6 位址 . . . . . . . : fe80::9d13:fcbc:8da3:a687%7(偏好選項)
   IPv4 位址 . . . . . . . . . . . . : 192.168.0.136(偏好選項)
   子網路遮罩 . . . . . . . . . . . : 255.255.255.0
   租用取得 . . . . . . . . . . . . : 2019年8月7日 上午 10:49:47
   租用到期 . . . . . . . . . . . . : 2019年8月7日 下午 12:49:46
   預設閘道 . . . . . . . . . . . . : fe80::da0d:17ff:fe34:d794%7
                                       192.168.0.1
   DHCP 伺服器 . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 114881226
   DHCPv6 用戶端 DUID. . . . . . . . : 00-01-00-01-24-92-58-57-6C-2B-59-56-E5-DB
   DNS 伺服器 . . . . . . . . . . . : 2001:b000:168::2
                                       2001:b000:168::1
                                       192.168.0.1
   NetBIOS over Tcpip . . . . . . . : 啟用
```

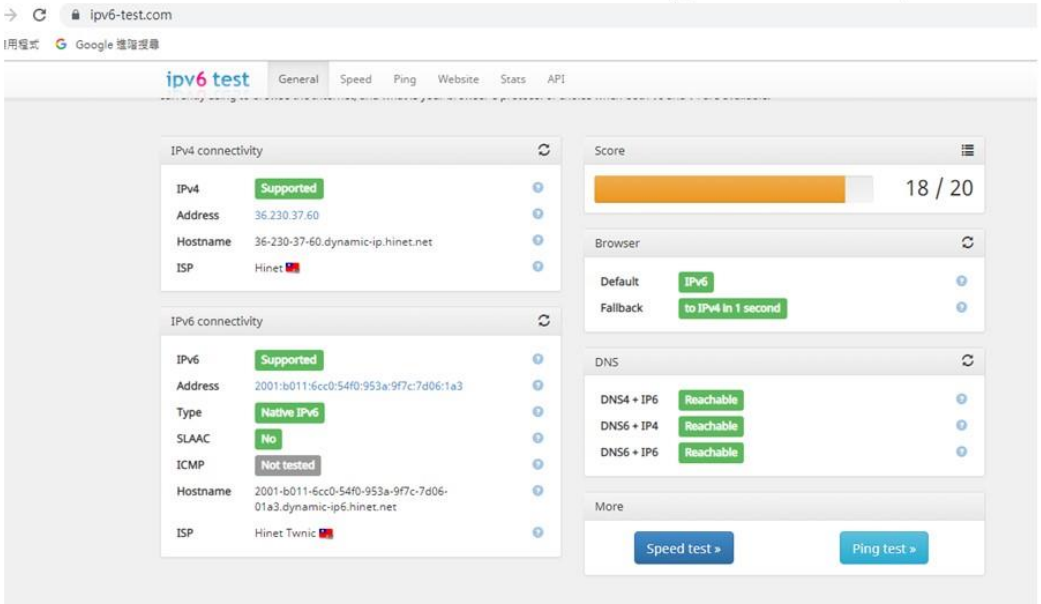
TP-LINK AC1200 PPPoE 測項11

✓ 確認用戶連接Wi-Fi IPv6上網正常(test-ipv6.com)



TP-LINK AC1200 PPPoE 測項11(續)

✓ 確認用戶連接Wi-Fi IPv6上網正常(ipv6-test.com)



TP-LINK AC1200 PPPoE 測項12

- ✓ IPv6 PPPoE (或是PPPoEv6)是否隨著IPv4 PPPoE啟用而自動啟用
  - ❑ 重設分享器，依照介面指示設定後，IPv4啟用後IPv6無法自動連線



TP-LINK AC1200 PPPoE 測項12(續)

- ✓ IPv6 PPPoE (或是PPPoEv6)是否隨著IPv4 PPPoE啟用而自動啟用
  - ❑ 將IPv6設定為PPPoE連線後，即可獲得IPv6 WAN



TP-LINK AC1200 PPPoE 測項12(續)

✓ IPv6 PPPoE (或是PPPoEv6)是否隨著IPv4 PPPoE啟用而自動啟用

❑ 需等待一段時間（約五分鐘）才可使用IPv6連線

測試你的 IPv6 連線。



啟用完IPv6後無法馬上使用IPv6連線

測試你的 IPv6 連線。



等待一段時間後即可使用IPv6

TP-LINK AC1200 PPPoE 測項13

✓ IPv6 PPPoE (或是PPPoEv6)連線之PPPoE Session是『Share with IPv4』或是『Create a new Session』?



將PPPoE工作階段設定為與IPv4相同會話



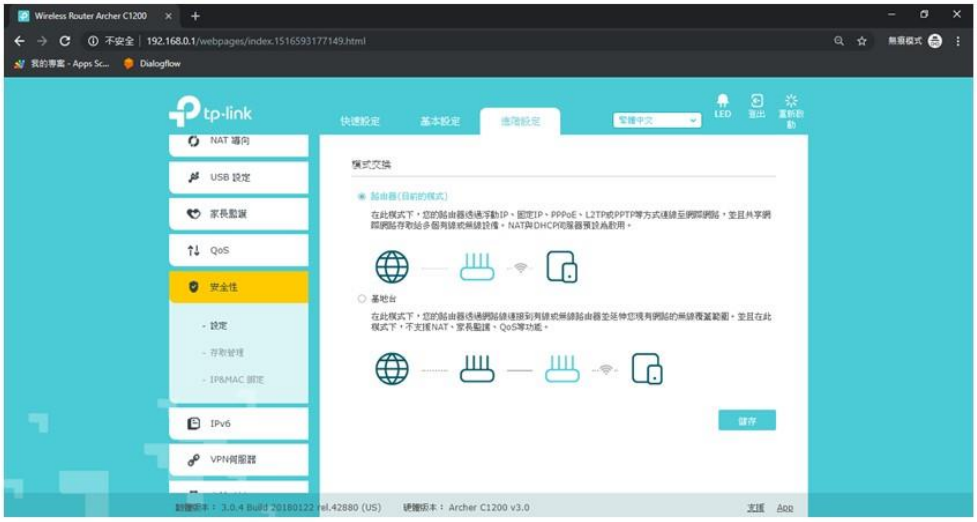
分享器WAN顯示為PPPoE連線

TP-LINK AC1200 PPPoE 測項13 (續)



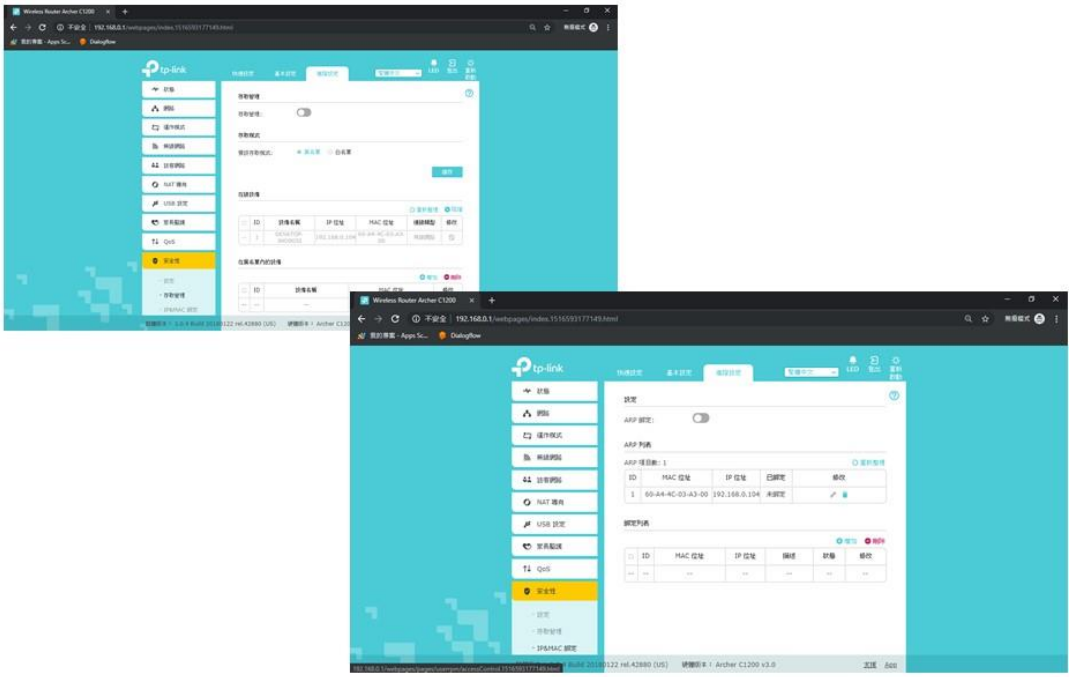
TP-LINK AC1200 PPPoE 測項14

- ✓ IPv6寬頻分享器IPv6 ACL功能是否正常?
  - □ 測試寬頻分享器 IPv6 ACL功能是否能限制用戶終端IPv6連線

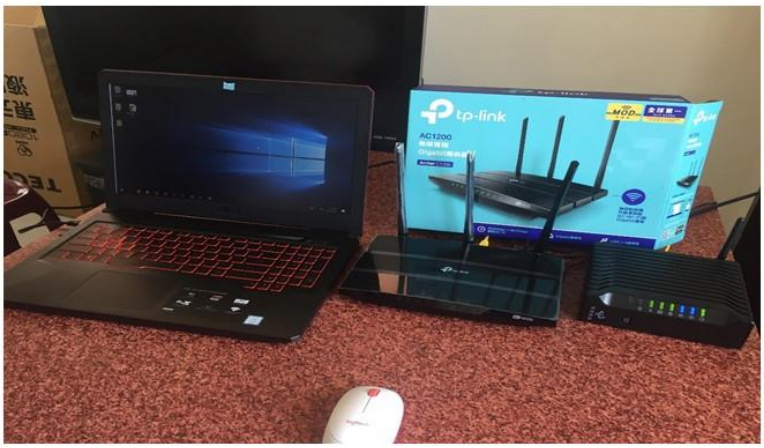


TP-LINK AC1200 PPPoE 測項14 (續)

- 無支援 IPv6 ACL功能



分享器測試紀錄
Cable 寬頻 IPoE環境



TP-LINK AC1200 CM 測項1

✓ 確認連接cable modem正常



TP-LINK AC1200 CM 測項2

✓ 確認取得IPv6、IPv6 PD、DNSv6



TP-LINK AC1200 CM 測項3

✓ 確認用戶IPv6、DNSv6取得正常

乙太網路卡 乙太網路:

```
   連線特定 DNS 尾碼 . . . . . . . . :
   描述 . . . . . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   實體位址 . . . . . . . . . . . . . : 1C-B7-2C-1E-CB-0E
   DHCP 已啟用 . . . . . . . . . . . : 是
   自動設定啟用 . . . . . . . . . . . : 是
   IPv6 位址. . . . . . . . . . . . . : 2405:9200:1110:4:a032:c63b:766e:c8d4(偏好選項)
   臨時 IPv6 位址. . . . . . . . . . . : 2001:b011:6cc0:5dbe:79a0:5a:9722:9629(已過時)
   IPv6 位址. . . . . . . . . . . . . : 2001:b011:6cc0:5dbe:a032:c63b:766e:c8d4(已過時)
   臨時 IPv6 位址. . . . . . . . . . . : 2405:9200:1110:4:6100:e0f6:6fc7:228b(偏好選項)
   連結-本機 IPv6 位址 . . . . . . . . : fe80::a032:c63b:766e:c8d4%11(偏好選項)
   IPv4 位址 . . . . . . . . . . . . . : 192.168.0.126(偏好選項)
   子網路遮罩 . . . . . . . . . . . . : 255.255.255.0
   租用取得 . . . . . . . . . . . . . : 2019年8月14日 下午 02:06:43
   租用到期 . . . . . . . . . . . . . : 2019年8月14日 下午 04:10:02
   預設閘道 . . . . . . . . . . . . . : fe80::da0d:17ff:fe34:d794%11
                                        192.168.0.1
   DHCP 伺服器 . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 52213548
   DHCPv6 用戶端 DUID. . . . . . . . : 00-01-00-01-1C-CC-BE-EF-1C-B7-2C-1E-CB-0E
   DNS 伺服器 . . . . . . . . . . . . : 2001:4860:4860::8888
                                        2001:4860:4860::8844
                                        192.168.0.1
   NetBIOS over Tcpip . . . . . . . . : 啟用
```

TP-LINK AC1200 CM 測項4

✓ 確認用戶至google ipv6路由正常

```
C:\Users\ASUS>ping ipv6.google.com

Ping ipv6.l.google.com [2404:6800:4012:1::200e] (使用 32 位元組的資料):
回覆自 2404:6800:4012:1::200e: 時間=14ms
回覆自 2404:6800:4012:1::200e: 時間=27ms
回覆自 2404:6800:4012:1::200e: 時間=15ms
回覆自 2404:6800:4012:1::200e: 時間=18ms

2404:6800:4012:1::200e 的 Ping 統計資料:
    封包: 已傳送 = 4，已收到 = 4，已遺失 = 0 (0% 遺失)，
大約的來回時間 (毫秒):
    最小值 = 14ms，最大值 = 27ms，平均 = 18ms

C:\Users\ASUS>tracert ipv6.google.com

在上限 30 個躍點上
追蹤 ipv6.l.google.com [2404:6800:4012:1::200e] 的路由:

  1    <1 ms    <1 ms    <1 ms  2405:9200:1110:4:da0d:17ff:fe34:d794
  2     *        *        *     要求等候逾時。
  3    11 ms     8 ms     9 ms  2405:9200:1:0:172:16:28:177a
  4    13 ms    12 ms     9 ms  2405:9200:1:0:172:16:31:18a
  5    12 ms    14 ms    12 ms  2404:0:10ff:1:7709:13:1596:1112
  6    13 ms    11 ms    11 ms  2404:0:10ff::5:66
  7    11 ms    11 ms    17 ms  2404:0:10ff:1:7709:1:5169:61
  8    12 ms    12 ms    11 ms  2001:4860:0:1014::1
  9    13 ms    13 ms    13 ms  2001:4860:0:1::2e0b
 10    11 ms    11 ms    10 ms  tsa03s06-in-x0e.1e100.net [2404:6800:4012:1::200e]

追蹤完成。
```

Mobile Broadband Networklab, NCU

TP-LINK AC1200 CM 測項5

✓ 確認用戶IPv6上網正常(test-ipv6.com)

測試你的 IPv6 連線。

總結 | 測試結果 | 分享結果 / 聯繫我們 | 其他 IPv6 網站

你在網際網路上的IPv4位址 123.241.153.127

你在網際網路上的IPv6位址 2405:9200:1110:4:6100:e0f6:6fc7:228b

你的網路服務提供者 (ISP) 是 TBCOM-NET TBC

Since you have IPv6, we are including a tab that shows how well you can reach other IPv6 sites. [詳細資訊]

HTTPS 支援現已在本網站上提供。 [詳細資訊]

你的 DNS 伺服器 （可能由你的ISP維護）似乎支援 IPv6 的網際網路通訊協定。

你對於 IPv6 準備的分數

10/10

當網站陸續只使用 IPv6， 請提早為您的 IPv6 做準備和設定

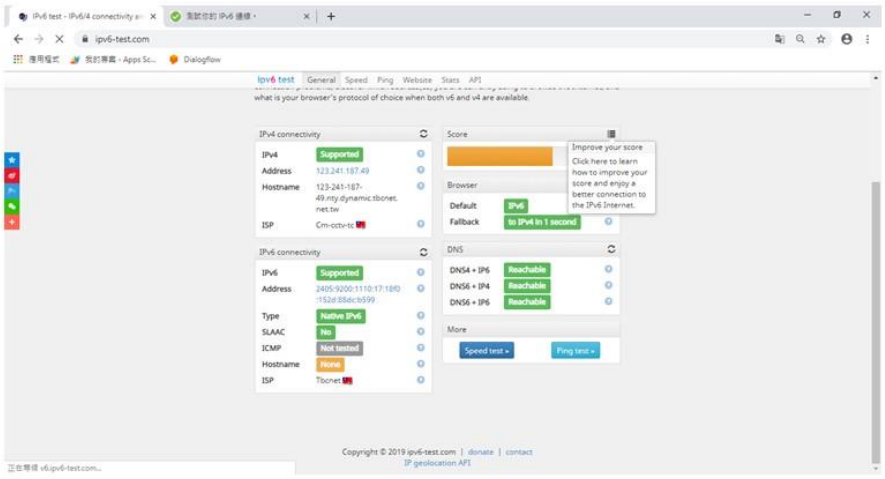
點擊查看 測試資料

(已更新網站的 IPv6 統計)

這個網站是由以下單位提供: HostVirtual

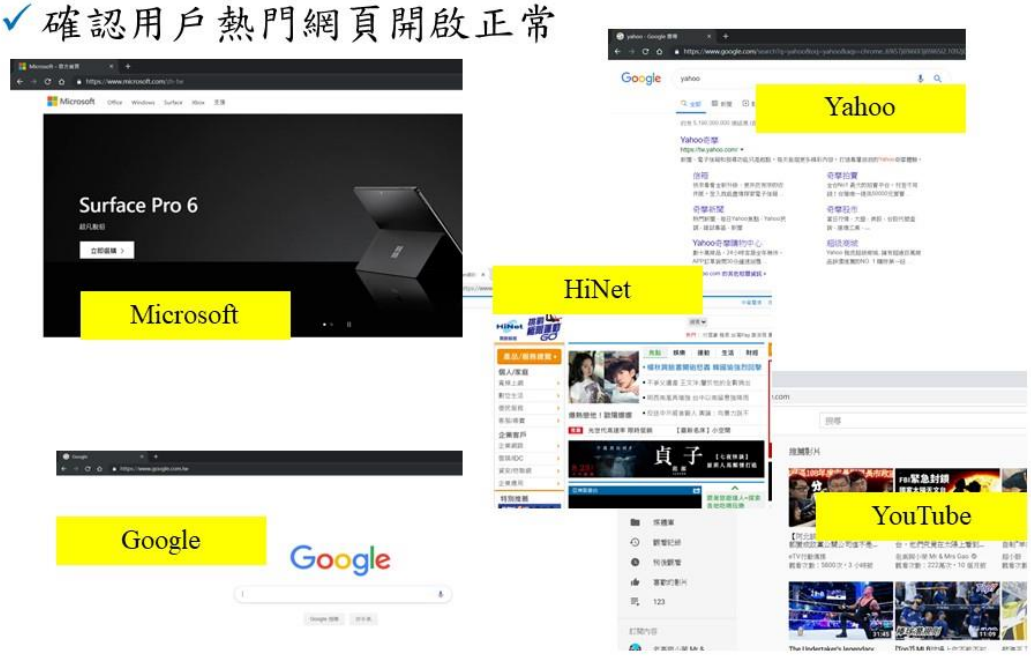
TP-LINK AC1200 CM 測項5(續)

✓ 確認用戶IPv6上網正常(ipv6-test.com)



TP-LINK AC1200 CM 測項6

✓確認用戶熱門網頁開啟正常



TP-LINK AC1200 CM 測項7

✓確認用戶上網速率正常



TP-LINK AC1200 CM 測項8

✓ 確認分享器重新連接cable modem之後，用戶ipv6相同，且連線正常



TP-LINK AC1200 CM 測項9

✓ 確認用戶使用IPv6乙太網路介面之MTU為1492非1500→不正常

```
C:\Users\ASUS>netsh interface ipv6 show subinterface

   MTU  MediaSenseState   接收的位元組 傳送的位元組  介面
------  ---------------  ----------  ----------  -------------
  1492                1   320193112    51181873  乙太網路
4294967295                1           0     1931791  Loopback Pseudo-Interface 1
  1500                2     2367809      471211  Wi-Fi
  1500                5           0        2552  區域連線* 2
  1500                5           0        2552  區域連線* 4
  1500                5           0        1774  Bluetooth 網路連線
```

TP-LINK AC1200 CM 測項10

✓ 確認用戶連接Wi-Fi上網IPv6、DNSv6正常

無線區域網路介面卡 Wi-Fi:

```
連線特定 DNS 尾碼 . . . . . :
描述 . . . . . : Intel(R) Dual Band Wireless-AC 7265
實體位址 . . . . . : 34-02-86-63-18-11
DHCP 已啟用 . . . . . : 是
自動設定啟用 . . . . . : 是
IPv6 位址. . . . . : 2405:9200:1110:15:80c3:57d2:60e7:e27a(偏好選項)
臨時 IPv6 位址. . . . . : 2405:9200:1110:15:382e:312b:f630:2dd8(偏好選項)
連結-本機 IPv6 位址 . . . . . : fe80::80c3:57d2:60e7:e27a%8(偏好選項)
IPv4 位址 . . . . . : 192.168.0.153(偏好選項)
子網路遮罩 . . . . . : 255.255.255.0
租用取得 . . . . . : 2019年8月14日 下午 03:14:28
租用到期 . . . . . : 2019年8月14日 下午 05:14:29
預設閘道 . . . . . : fe80::da0d:17ff:fe34:d794%8
                                192.168.0.1
DHCP 伺服器 . . . . . : 192.168.0.1
DHCPv6 IAID . . . . . : 120849030
DHCPv6 用戶端 DUID . . . . . : 00-01-00-01-1C-CC-BE-EF-1C-B7-2C-1E-CB-0E
DNS 伺服器 . . . . . : 2404::1
                                2001:b000:168::1
                                192.168.0.1
NetBIOS over Tcpip . . . . . : 啟用
```

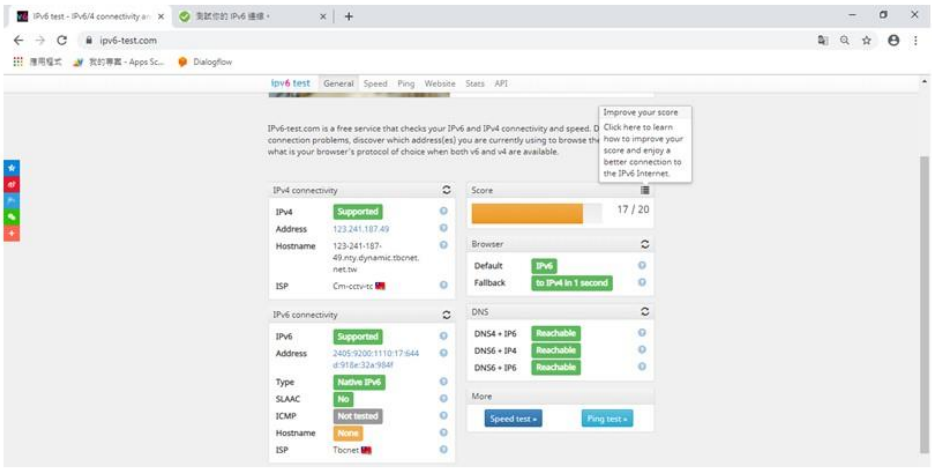

TP-LINK AC1200 CM 測項11

✓ 確認用戶連接Wi-Fi IPv6上網正常(test-ipv6.com)



TP-LINK AC1200 CM 測項11(續)

✓ 確認用戶連接Wi-Fi IPv6上網正常(ipv6-test.com)



TP-LINK AC1200 CM 測項12

✓ 確認IPv6 連線功能隨著IPv4啟用而自動啟用

- 重設分享器，依照介面指示設定後，IPv4啟用後IPv6不會自動啟用

IPv6預設設定



無法獲得IPv6 WAN



TP-LINK AC1200 CM 測項12 (續)

- 更改IPv6設定後，IPv6成功啟用



Mobile Broadband Networklab, NCU

TP-LINK AC1200 CM 測項13

✓ IPv6寬頻分享器IPv6 ACL功能是否正常?

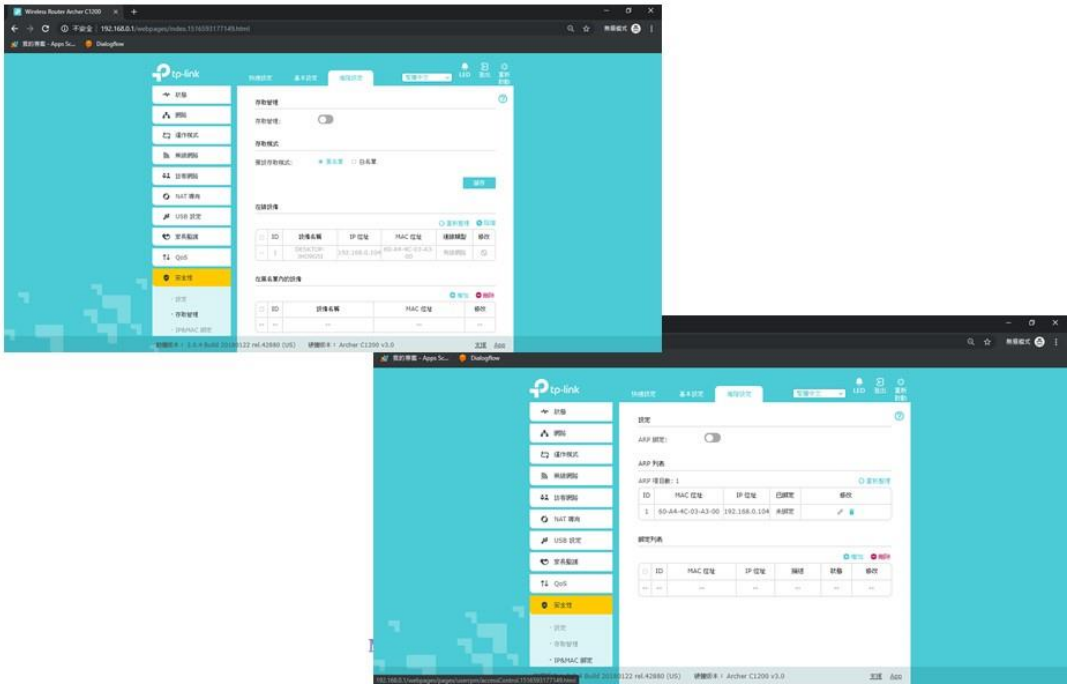
- 測試寬頻分享器 IPv6 ACL功能是否能限制用戶終端IPv6連線



Mobile Broadband Networklab, NCU

TP-LINK AC1200 CM 測項13(續)

- 無支援 IPv6 ACL功能



國立中央大學
National Central University

TP-Link Archer A9
分享器測試成果

測試設備與環境

分享器產品設備資訊	
產品型號	Archer A9
產品名稱	AC1900 Wireless MU-MIMO Gigabit Router
硬體版本	6.0
韌體版本	1.0.1
製造年份	2019

測試環境資訊	
測試環境	1.HiNet光世代 PPPoE
	2.Cable IPoE
測試終端	Windows 10
終端瀏覽器	Chrome
測試時間	2019-08~2019-10



測試紀錄摘要

HiNet 光世代PPPoE測試		
	測試項目	Archer A9
1	分享器PPPoE撥接是否正常?	O
2	分享器IPv6、IPv6 PD、DNSv6取得是否正常?	O
3	用戶IPv6、DNSv6取得是否正常?	O
4	用戶至HiNet路由是否正常?	O
5	用戶IPv6上網是否正常?	O
6	用戶熱門網頁開啟是否正常?	O
7	用戶上網速率是否正常?	O
8	分享器重撥，用戶IPv6更新是否正常?	O
9	用戶使用IPv6之MTU是否正常?	1492
10	用戶連接Wi-Fi上網IPv6、DNSv6是否正常?	O
11	用戶連接Wi-Fi IPv6上網是否正常?	O
12	IPv6 PPPoE（或是PPPoEv6)是否隨著IPv4 PPPoE啟用而自動啟用?	X
13	IPv6 PPPoE（或是PPPoEv6)連線之PPPoE Session是『Share with IPv4』或是『Create a new Session』?	可設定兩種模式
14	IPv6寬頻分享器IPv6 ACL功能是否正常?	無支援IPv6 ACL功能

Cable IPoE測試		
	測試項目	Archer A9
1	分享器連接Cable Modem是否正常?	O
2	分享器IPv6、IPv6 PD、DNSv6取得是否正常?	O
3	用戶IPv6、DNSv6取得是否正常?	O
4	用戶至Cable業者路由是否正常?	O
5	用戶IPv6上網是否正常?	O
6	用戶熱門網頁開啟是否正常?	O
7	用戶上網速率是否正常?	O
8	分享器重撥Cable Modem，用戶IPv6更新是否正常?	O
9	用戶使用IPv6之MTU是否正常?	1500
10	用戶連接Wi-Fi上網IPv6、DNSv6是否正常?	O
11	用戶連接Wi-Fi IPv6上網是否正常?	O
12	IPv6連線功能是否隨著IPv4啟用而自動啟用?	X
13	IPv6寬頻分享器IPv6 ACL功能是否正常?	無支援IPv6 ACL功能

測試紀錄摘要說明

- ✓ HiNet PPPoE環境 (Pass測項:12/14)
  - 測項12: 需要手動啟用IPv6
  - 測項14: 無支援IPv6 ACL功能

- ✓ Cable IPoE環境(Pass測項:11/13)
  - 測項12: 需要手動啟用IPv6
  - 測項13: 無支援IPv6 ACL功能

分享器測試紀錄
HiNet 光世代 PPPoE環境



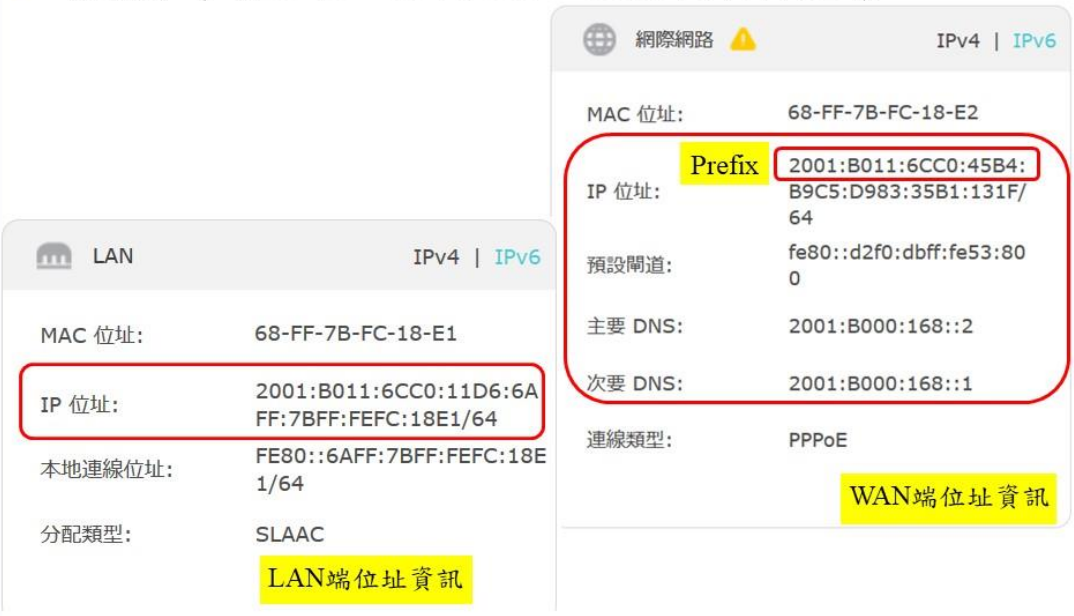
TP-Link Archer A9 PPPoE 測項1

✓ 確認分享器PPPoE撥接正常



TP-Link Archer A9 PPPoE 測項2

✓ 確認分享器IPv6、IPv6 PD、DNSv6取得正常



TP-Link Archer A9 PPPoE 測項3

✓ 確認用戶IPv6、DNSv6取得正常

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Physical Address. . . . . . . . . : 04-92-26-6E-D1-F8
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:b011:6cc0:11d6:1ce7:3c77:5218:7258(Preferred)
   Temporary IPv6 Address. . . . . . : 2001:b011:6cc0:11d6:206e:b496:f83e:dcfc(Preferred)
   Link-local IPv6 Address . . . . . : fe80::1ce7:3c77:5218:7258%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.208(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, August 7, 2019 10:15:46 AM
   Lease Expires . . . . . . . . . . : Wednesday, August 7, 2019 12:15:46 PM
   Default Gateway . . . . . . . . . : fe80::6aff:7bff:fefc:18e1%3
                                       192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 33853990
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-47-2F-7E-04-92-26-6E-D1-F8
   DNS Servers . . . . . . . . . . . : 2001:b000:168::2
                                       2001:b000:168::1
                                       192.168.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```


TP-Link Archer A9 PPPoE 測項4

✓ 確認用戶至HiNet路由正常

```
C:\Users\Hestia>ping dns.hinet.net

Pinging dns.hinet.net [2001:b000:168::2] with 32 bytes of data:
Reply from 2001:b000:168::2: time=10ms
Reply from 2001:b000:168::2: time=9ms
Reply from 2001:b000:168::2: time=11ms
Reply from 2001:b000:168::2: time=10ms

Ping statistics for 2001:b000:168::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 11ms, Average = 10ms

C:\Users\Hestia>tracert dns.hinet.net

Tracing route to dns.hinet.net [2001:b000:168::2]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  2001-b011-6cc0-11d6-6aff-7bff-fefc-18e1.dynamic-ip6.hinet.net [2001:b011:6cc0:11d6:6aff:7bff:fefc:18e1
  2    10 ms    10 ms    10 ms  2001:b010:ffff::1
  3    12 ms    13 ms    11 ms  2001-b000-0089-0005-0021-2222-0001-0002.hinet-ip6.hinet.net [2001:b000:89:5:21:2222:1:2]
  4     *       10 ms     *     2001-b000-0080-0003-0080-0089-0021-000a.hinet-ip6.hinet.net [2001:b000:80:3:80:89:21:a]
  5    14 ms    13 ms    13 ms  2001-b000-0080-0004-3021-3011-0002-000b.hinet-ip6.hinet.net [2001:b000:80:4:3021:3011:2:b]
  6    16 ms    15 ms    11 ms  2001-b000-0080-0004-3021-3011-0002-000b.hinet-ip6.hinet.net [2001:b000:80:4:3021:3011:2:b]
  7    10 ms     9 ms    12 ms  2001-b000-0080-0004-3011-3312-0011-000b.hinet-ip6.hinet.net [2001:b000:80:4:3011:3312:11:b]
  8     *        *        *     Request timed out.
  9    11 ms    10 ms    11 ms  dns.hinet.net [2001:b000:168::2]

Trace complete.
```

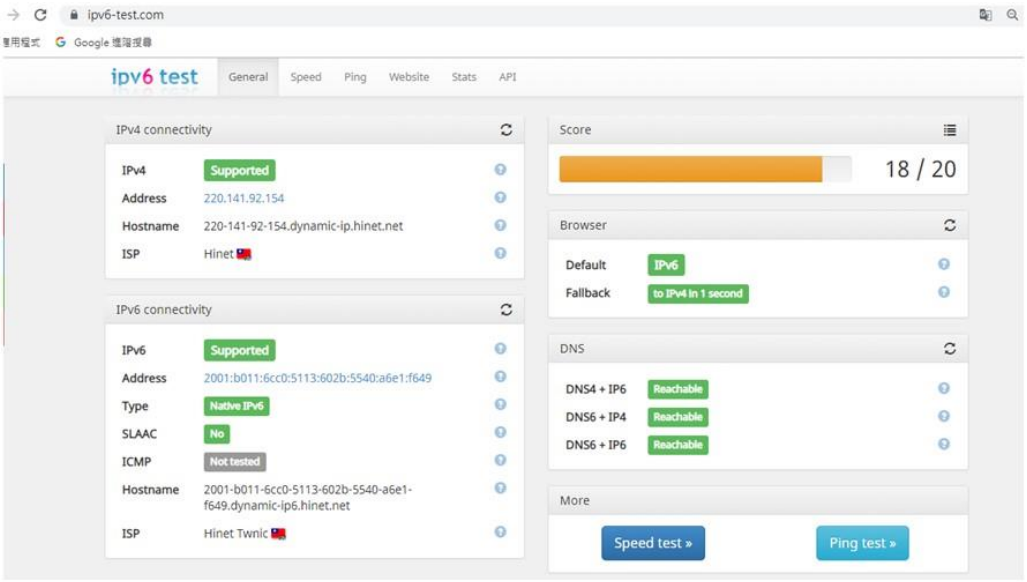
TP-Link Archer A9 PPPoE 測項5

✓ 確認用戶IPv6上網正常(test-ipv6.com)



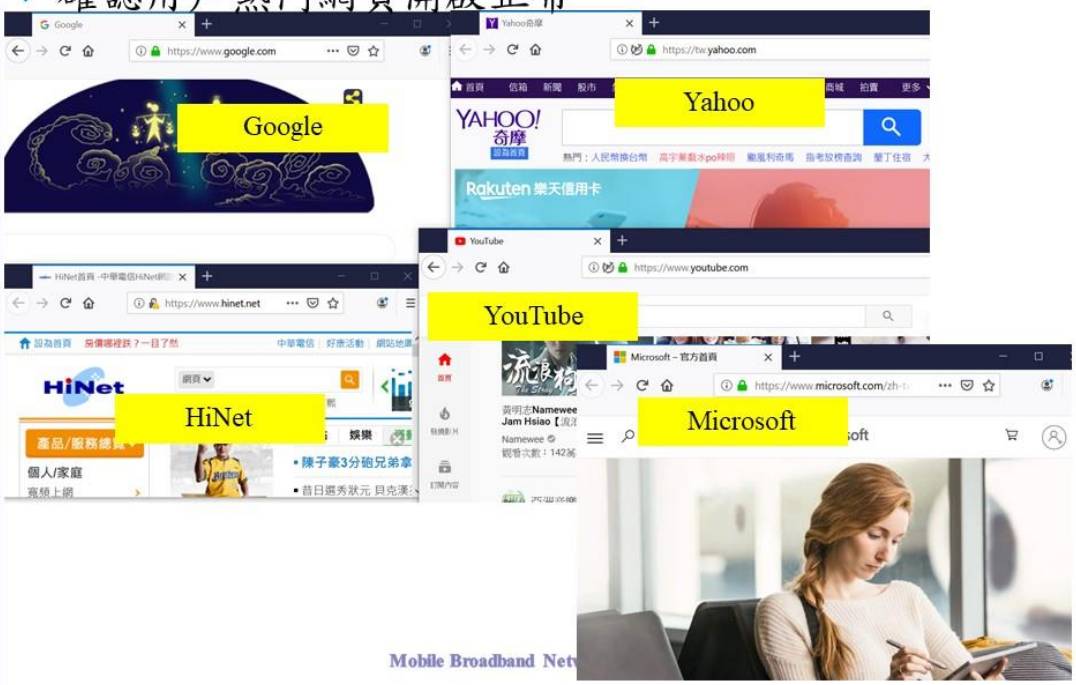
TP-Link Archer A9 PPPoE 測項5(續)

✓ 確認用戶IPv6上網正常(ipv6-test.com)



TP-Link Archer A9 PPPoE 測項6

✓ 確認用戶熱門網頁開啟正常



TP-Link Archer A9 PPPoE 測項7

✓ 確認用戶上網速率正常



TP-Link Archer A9 PPPoE 測項8

✓確認分享器重撥，用戶IPv6更新正常

測試 IPv6 | 常見問題 | 鏡像伺服器

測試你的 IPv6 連線。

分享器重撥之前

總結 | 測試結果 | 分享結果 / 聯繫我們 | 其他 IPv6 網站

你在網際網路上的IPv4位址 220.137.49.217

你在網際網路上的IPv6位址 2001:b011:6cc0:11d6:206e:b496:f83e:dcfc

你的網路服務提供者 (ISP) 是 HINET Data Communication Business Group

Since you have IPv6, we are including a tab that shows how well you can reach other IPv6 sites. [詳細資訊]

此網站上的 HTTPS 支援位於 *Beta* 中。 [詳細資訊]

你的 DNS 伺服器 （可能由你的ISP維護）似乎支援 IPv6 的網際網路通訊協定。

你對於 IPv6 準備的分數

當網站陸續只使用 IPv6， 請提早為您的 IPv6 做準備和設定

10/10

測試你的 IPv6 連線。

分享器重撥之後

總結 | 測試結果 | 分享結果 / 聯繫我們 | 其他 IPv6 網站

你在網際網路上的IPv4位址 220.137.121.131

你在網際網路上的IPv6位址 2001:b011:6cc0:3fc8:b5b3:dc2c:801f:46ed

你的網路服務提供者 (ISP) 是 HINET Data Communication Business Group

Since you have IPv6, we are including a tab that shows how well you can reach other IPv6 sites. [詳細資訊]

此網站上的 HTTPS 支援位於 *Beta* 中。 [詳細資訊]

你的 DNS 伺服器 （可能由你的ISP維護）似乎支援 IPv6 的網際網路通訊協定。

你對於 IPv6 準備的分數

當網站陸續只使用 IPv6， 請提早為您的 IPv6 做準備和設定

10/10

TP-Link Archer A9 PPPoE 測項9

✓確認用戶使用IPv6之MTU正常

```
C:\Users\Hestia>netsh interface ipv6 show subinterface

   MTU  MediaSenseState   Bytes In  Bytes Out  Interface
------  ---------------  ---------  ---------  -------------
4294967295                1          0     934124  Loopback Pseudo-Interface 1
  1500                2    1233612     328780  Wi-Fi
  1492                1 2657586566  135690039  Ethernet
  1500                5          0       5414  Local Area Connection* 2
  1500                5          0      32344  Bluetooth Network Connection
  1500                5          0       6967  Local Area Connection* 3
  1400                5          0      65608  Local Area Connection* 1
 65536                1          0      61308  Ethernet 2
```

TP-Link Archer A9 PPPoE 測項10

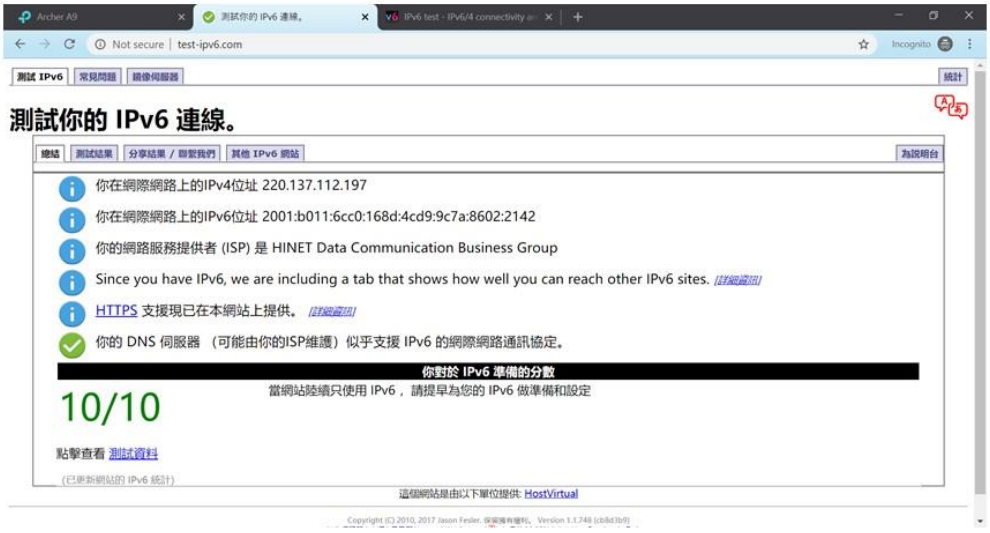
✓ 確認用戶連接Wi-Fi上網IPv6、DNSv6正常

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wireless-AC 9560
   Physical Address. . . . . . . . . : 48-A4-72-42-63-96
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:b011:6cc0:168d:f115:d539:9dc9:ab66(Preferred)
   Temporary IPv6 Address. . . . . . : 2001:b011:6cc0:168d:4cd9:9c7a:8602:2142(Preferred)
   Link-local IPv6 Address . . . . . : fe80::f115:d539:9dc9:ab66%14(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.194(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Friday, October 18, 2019 6:34:10 PM
   Lease Expires . . . . . . . . . . : Friday, October 18, 2019 8:34:10 PM
   Default Gateway . . . . . . . . . : fe80::6aff:7bff:fefc:18e1%14
                                       192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 222864498
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-47-2F-7E-04-92-26-6E-D1-F8
   DNS Servers . . . . . . . . . . . : 2001:b000:168::2
                                       2001:b000:168::1
                                       192.168.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

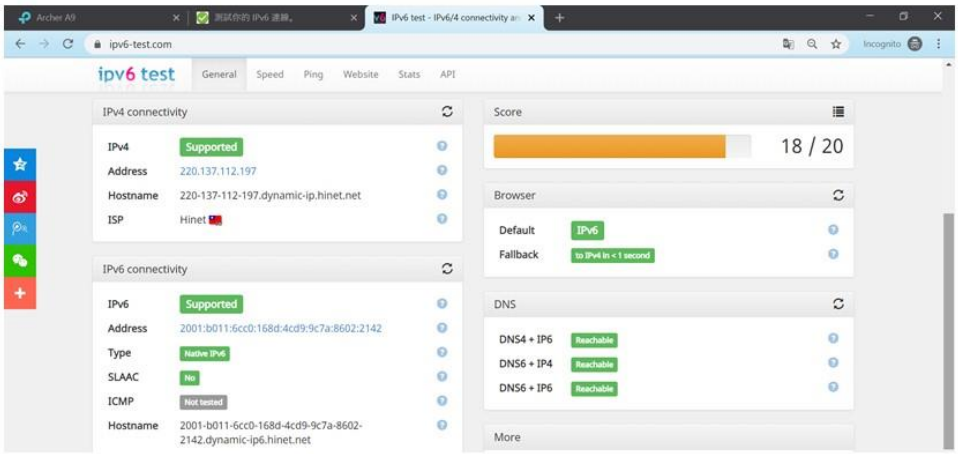

TP-Link Archer A9 PPPoE 測項11

✓ 確認用戶連接Wi-Fi IPv6上網正常(test-ipv6.com)



TP-Link Archer A9 PPPoE 測項11(續)

✓ 確認用戶連接Wi-Fi IPv6上網正常(ipv6-test.com)



TP-Link Archer A9 PPPoE 測項12

✓ IPv6 PPPoE (或是PPPoEv6)是否隨著IPv4 PPPoE啟用而自動啟用

❑ 重設分享器，依照介面指示設定後，IPv4啟用後IPv6無法自動連線

測試你的 IPv6 連線。 IPv6 連線失敗



無法取得IPv6 WAN



TP-Link Archer A9 PPPoE 測項12(續)

- ✓ IPv6 PPPoE (或是PPPoEv6)是否隨著IPv4 PPPoE啟用而自動啟用
  - 將IPv6設定為PPPoE連線後，等待五分鐘，IPv6連線正常

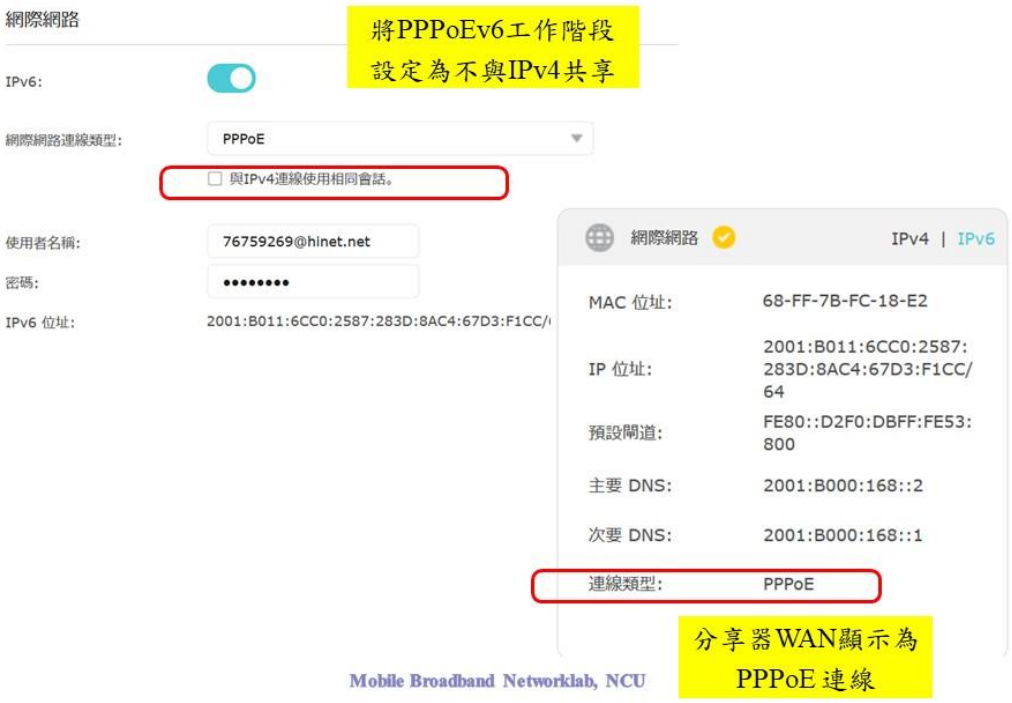


TP-Link Archer A9 PPPoE 測項13

- ✓ IPv6 PPPoE (或是PPPoEv6)連線之PPPoE Session是『Share with IPv4』或是『Create a new Session』?

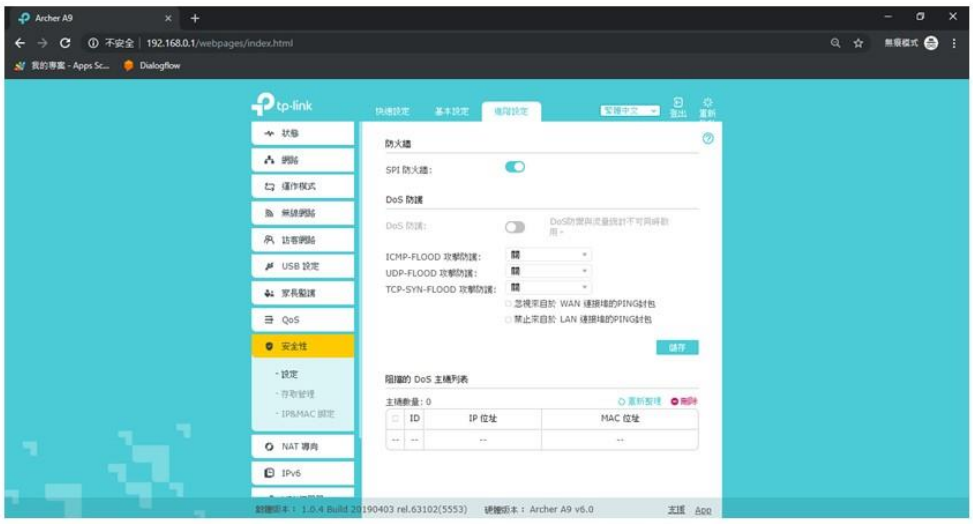


TP-Link Archer A9 PPPoE 測項13 (續)



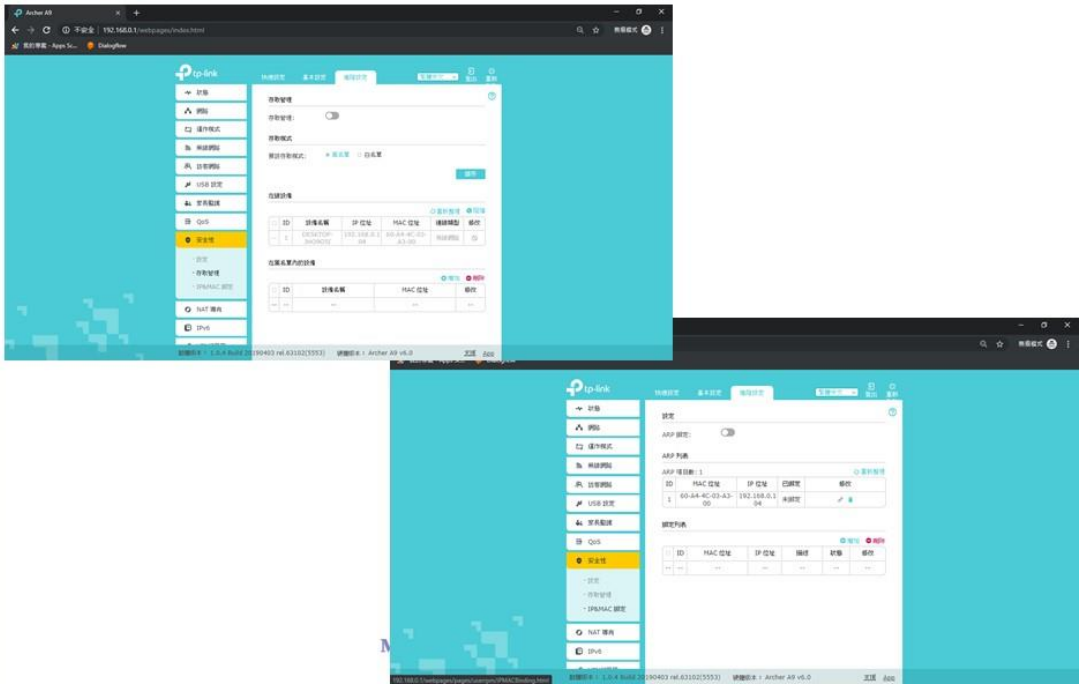
TP-Link Archer A9 PPPoE 測項14

- ✓ IPv6寬頻分享器IPv6 ACL功能是否正常?
  - □ 測試寬頻分享器 IPv6 ACL功能是否能限制用戶終端IPv6連線



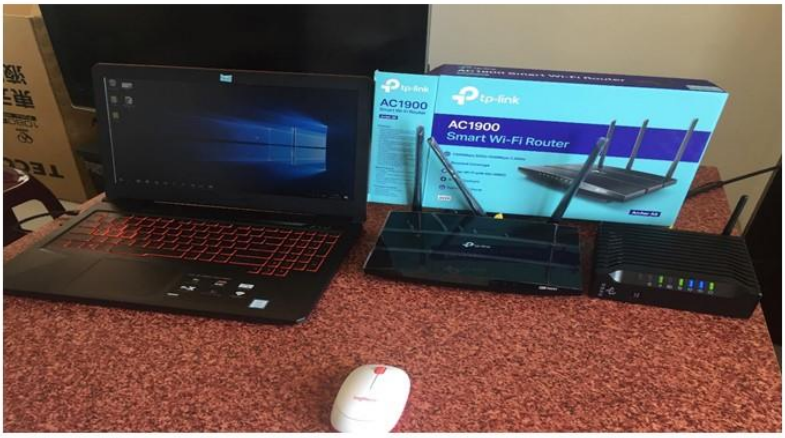
TP-Link Archer A9 PPPoE 測項14(續)

- 無支援 IPv6 ACL功能



分享器測試紀錄

Cable 寬頻 IPoE環境



TP-Link Archer A9 CM 測項1

✓ 確認連接cable modem正常



TP-Link Archer A9 CM 測項2

✓ 確認取得IPv6、IPv6 PD、DNSv6

WAN端位址資訊



LAN端位址資訊



TP-Link Archer A9 CM 測項3

✓ 確認用戶IPv6、DNSv6取得正常

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Physical Address. . . . . . . . . : 04-92-26-6E-D1-F8
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2405:9200:1110:f:1ce7:3c77:5218:7258(Preferred)
   IPv6 Address. . . . . . . . . . . : 2001:b011:6cc0:3fc8:1ce7:3c77:5218:7258(Deprecated)
   Temporary IPv6 Address. . . . . . : 2001:b011:6cc0:3fc8:898b:64f9:725a:ca54(Deprecated)
   Temporary IPv6 Address. . . . . . : 2405:9200:1110:f:898b:64f9:725a:ca54(Preferred)
   Link-local IPv6 Address . . . . . : fe80::1ce7:3c77:5218:7258%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.208(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, August 14, 2019 2:14:17 PM
   Lease Expires . . . . . . . . . . : Wednesday, August 14, 2019 4:14:21 PM
   Default Gateway . . . . . . . . . : fe80::6aff:7bff:fefc:18e1%3
                                       192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 33853990
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-47-2F-7E-04-92-26-6E-D1-F8
   DNS Servers . . . . . . . . . . . : 2001:4860:4860::8888
                                       2001:4860:4860::8844
                                       192.168.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```


TP-Link Archer A9 CM 測項4

✓ 確認用戶至google ipv6路由正常

```
C:\Users\Hestia>ping ipv6.google.com

Pinging ipv6.l.google.com [2404:6800:4012:1::200e] with 32 bytes of data:
Reply from 2404:6800:4012:1::200e: time=11ms
Reply from 2404:6800:4012:1::200e: time=10ms
Reply from 2404:6800:4012:1::200e: time=12ms
Reply from 2404:6800:4012:1::200e: time=11ms

Ping statistics for 2404:6800:4012:1::200e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 12ms, Average = 11ms

C:\Users\Hestia>tracert ipv6.google.com

Tracing route to ipv6.l.google.com [2404:6800:4012:1::200e]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  2405:9200:1110:f:6aff:7bff:fefc:18e1
  2     *        *        *     Request timed out.
  3     8 ms     9 ms     9 ms  2405:9200:1:0:172:16:28:165a
  4    11 ms    13 ms    10 ms  2405:9200:1:0:172:16:31:2a
  5    12 ms    12 ms    15 ms  2404:0:10ff:1:7709:13:1596:710
  6    10 ms    11 ms    11 ms  2404:0:10ff::5:66
  7    11 ms    11 ms    10 ms  2404:0:10ff:1:7709:1:5169:61
  8    12 ms    11 ms    11 ms  2001:4860:0:1013::1
  9    13 ms    11 ms    13 ms  2001:4860:0:1::5ad
 10    10 ms    10 ms    10 ms  tsa03s06-in-x0e.1e100.net [2404:6800:4012:1::200e]

Trace complete.
```

TP-Link Archer A9 CM 測項5

✓ 確認用戶IPv6上網正常(test-ipv6.com)

測試 IPv6 | 常見問題 | 鏡像伺服器

測試你的 IPv6 連線。

總結 | 測試結果 | 分享結果 / 聯繫我們 | 其他 IPv6 網站

- 你在網際網路上的IPv4位址 123.241.153.128
- 你在網際網路上的IPv6位址 2405:9200:1110:f:898b:64f9:725a:ca54
- 你的網路服務提供者 (ISP) 是 TBCOM-NET TBC
- Since you have IPv6, we are including a tab that shows how well you can reach other IPv6 sites.
- HTTPS 支援現已在本網站上提供。 [詳細資訊]
- 你的 DNS 伺服器 （可能由你的ISP維護）似乎支援 IPv6 的網際網路通訊協定。

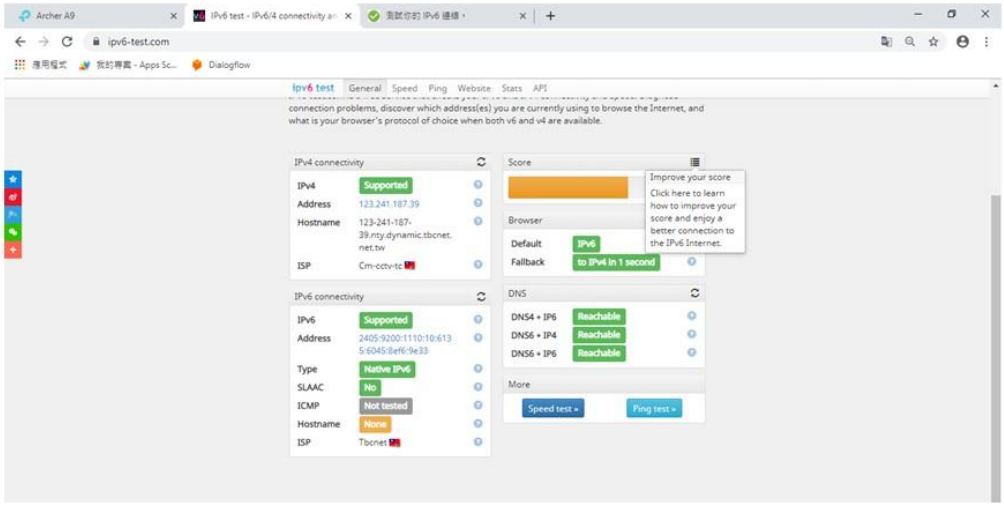
你對於 IPv6 準備的分數

10/10

當網站陸續只使用 IPv6， 請提早為您的 IPv6 做準備和設定

TP-Link Archer A9 CM 測項5(續)

✓ 確認用戶IPv6上網正常(ipv6-test.com)



TP-Link Archer A9 CM 測項6

✓ 確認用戶熱門網頁開啟正常



TP-Link Archer A9 CM 測項7

✓ 確認用戶上網速率正常



TP-Link Archer A9 CM 測項8

✓ 確認分享器重新連接cable modem之後，用戶ipv6相同，且連線正常

分享器重接CM前



分享器重接CM後



TP-Link Archer A9 CM 測項9

✓ 確認用戶使用IPv6乙太網路介面之MTU為1500非1492

```
C:\Users\Hestia>netsh interface ipv6 show subinterface

   MTU  MediaSenseState   Bytes In  Bytes Out  Interface
------  ---------------  ---------  ---------  -------------
4294967295                1          0    1504356  Loopback Pseudo-Interface 1
  1500                2    1927863    1215200  Wi-Fi
  1500                1  224891716   42154332  Ethernet
  1500                5          0      18671  Local Area Connection* 2
  1500                5          0      44537  Bluetooth Network Connection
  1500                5          0      24464  Local Area Connection* 3
  1400                5          0     101063  Local Area Connection* 1
 65536                1          0     191970  Ethernet 2
```

TP-Link Archer A9 CM 測項10

✓ 確認用戶連接Wi-Fi上網IPv6、DNSv6正常

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wireless-AC 9560
   Physical Address. . . . . . . . . : 48-A4-72-42-63-96
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2405:9200:1110:f:f115:d539:9dc9:ab66(Preferred)
   Temporary IPv6 Address. . . . . . : 2405:9200:1110:f:8448:283b:e113:4d82(Preferred)
   Link-local IPv6 Address . . . . . : fe80::f115:d539:9dc9:ab66%13(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.194(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, August 14, 2019 2:06:33 PM
   Lease Expires . . . . . . . . . . : Wednesday, August 14, 2019 4:56:40 PM
   Default Gateway . . . . . . . . . : fe80::6aff:7bff:fefc:18e1%13
                                       192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 222864498
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-47-2F-7E-04-92-26-6E-D1-F8
   DNS Servers . . . . . . . . . . . : 2404::1
                                       2001:b000:168::1
                                       192.168.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

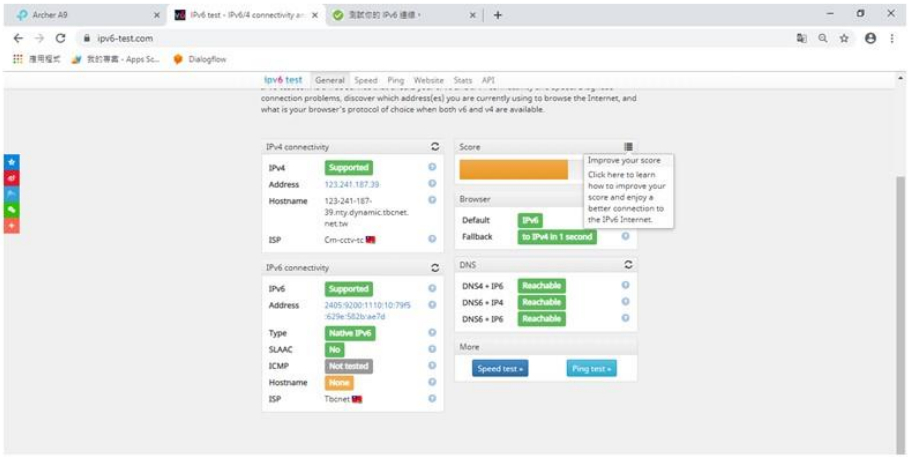

TP-Link Archer A9 CM 測項11

✓ 確認用戶連接Wi-Fi IPv6上網正常(test-ipv6.com)



TP-Link Archer A9 CM 測項11(續)

✓ 確認用戶連接Wi-Fi IPv6上網正常(ipv6-test.com)



TP-Link Archer A9 CM 測項12

✓ 確認IPv6 連線功能隨著IPv4啟用而自動啟用

- 重設分享器，依照介面指示設定後，IPv4啟用後IPv6不會自動啟用

IPv6預設設定



無法獲得IPv6 WAN



TP-Link Archer A9 CM 測項12 (續)

- 更改IPv6設定後，IPv6成功啟用

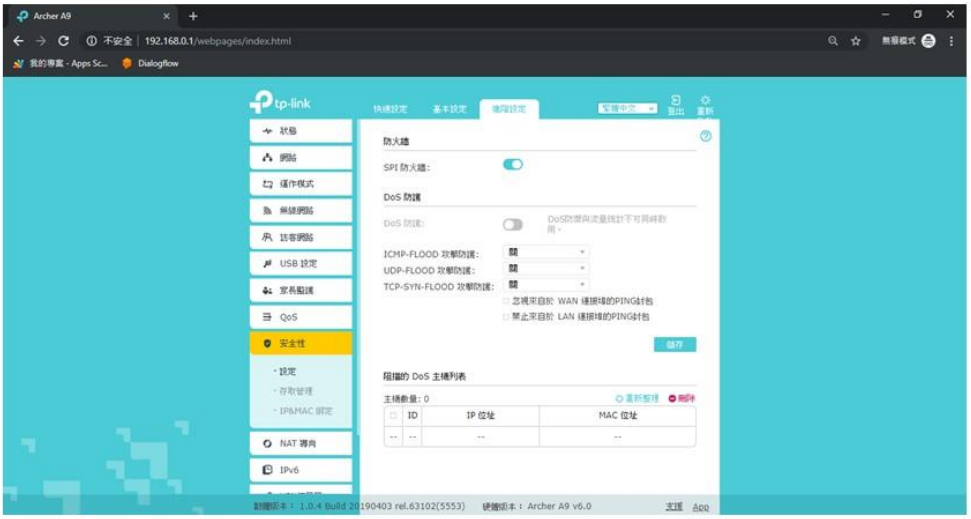
成功獲得IPv6 WAN, LAN

更改IPv6設定



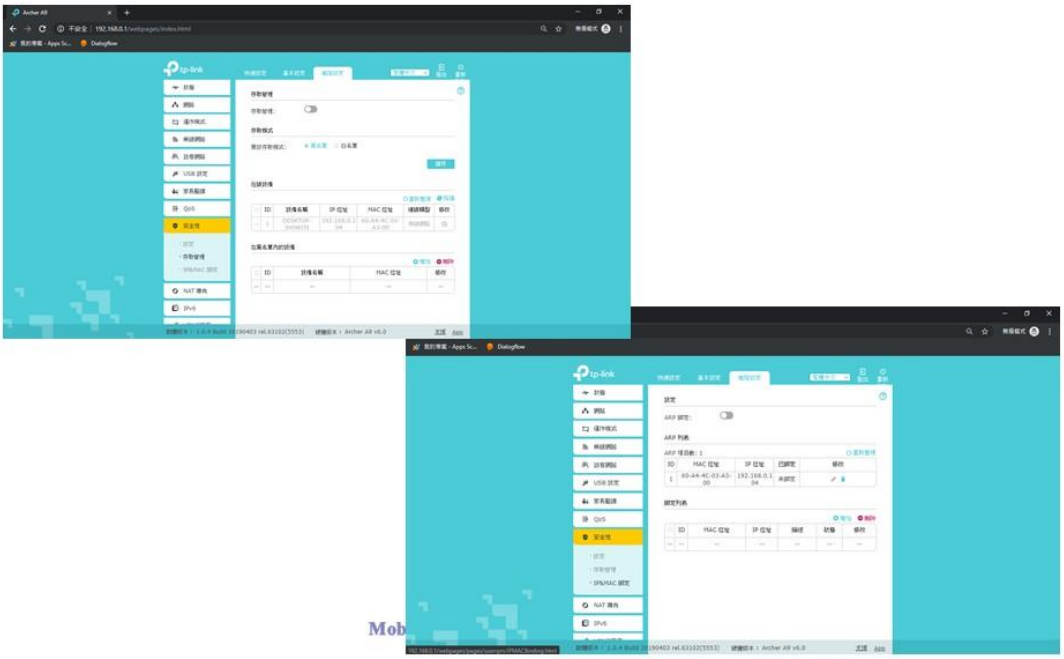
TP-Link Archer A9 CM 測項13

- ✓ IPv6寬頻分享器IPv6 ACL功能是否正常?
  - 測試寬頻分享器 IPv6 ACL功能是否能限制用戶終端IPv6連線



TP-Link Archer A9 CM 測項13(續)

- 無支援 IPv6 ACL功能



附件五、政府採購共同供應契約設備參考規範

政府採購共同供應契約設備參考規範

1

主機設備規範建議

- 既有共同供應契約中主機設備之IPv6規格如下
  - 資料參考台銀共同供應契約LP5-108019電腦設備用品(商用電腦)
    - 第1組 個人電腦之主機
  - https://www.bot.com.tw/Procurement/Procure_supply/Supply_index/Documents/108/LP5-108019/procure_Cmsup_Spec_pc108019_001.htm

既有共同供應契約-IPv6相關規範	本計畫建議IPv6規範
2-1.Windows 10(含)以上 Professional 64bit 中文專業版作業系統【作業系統提供原廠合法系統還原功能內含完整作業系統及相關驅動程式】	1. 必須支援IPv6 Addressing Architecture 定義之位址格式規範 2. 必須支援IPv6 Default Address Selection功能 3. 必須支援Unique Local IPv6 Unicast Addresses (ULA)位址格式 4. 必須支援ICMPv6通訊協定 5. 必須支援DHCPv6規範之Client行為 6. 必須支援Stateless或Stateful位址分配機制 7. 必須支援Path MTU Discovery 功能 8. 必須支援Neighbor Discovery 功能 9. 必須支援IPv6 DNS 資源記錄以及Extension DNS功能 10. 如須支援Tunneling以及DualStack環境，則主機必須支援基本IPv6轉移機制 11. 如須支援Mobile IPv6 環境，則主機必須支援MIPv6機制 12. 必須棄用IPv6 Type 0 Routing Headers

2

伺服器設備規範建議

- 既有共同供應契約中伺服器設備之IPv6規格如下
  - 資料參考台銀共同供應契約LP5-107003電腦設備用品(企業電腦)
    - 第1組 伺服器
  - https://www.bot.com.tw/Procurement/Procure_supply/Supply_index/Documents/107/LP5-107003/procure_Cmsup_Spec_pc107003_001.htm

既有共同供應契約-IPv6相關規範	本計畫建議IPv6規範
14-1.Windows Server 2016(含)以上 Standard(標準版) 16 Core 中文版最新版作業系統含10個Users(1+10存取授權，僅提供10台機器或10個用戶端連線使用權利，若超過10台機器，或用戶端超過10人連線，請加購Windows Server用戶端存取授權最新授權版(User or Device CAL))	1. 必須支援IPv6 Addressing Architecture 定義之位址格式規範 2. 必須支援IPv6 Default Address Selection功能 3. 必須支援Unique Local IPv6 Unicast Addresses (ULA)位址格式 4. 必須支援ICMPv6通訊協定 5. 必須支援DHCPv6規範之Client行為 6. 必須支援Stateless或Stateful位址分配機制 7. 必須支援Path MTU Discovery 功能 8. 必須支援Neighbor Discovery 功能 9. 必須支援IPv6 DNS 資源記錄以及Extension DNS功能 10. 如須支援Tunneling以及DualStack環境，則主機必須支援基本IPv6轉移機制 11. 如須支援Mobile IPv6 環境，則主機必須支援MIPv6機制 12. 必須棄用IPv6 Type 0 Routing Headers
14-2.Windows 10 Pro for Workstations 中文最新版作業系統	
14-3.Red Hat Enterprise Linux 最新版或 SUSE Linux Enterprise Server 最新版或 Oracle Enterprise Linux	
14-4. Enterprise Linux for Workstation 最新版或SUSE Linux Enterprise Desktop 最新版或 Ubuntu Desktop LTS 最新版	

路由器設備規範建議

- 既有共同供應契約中路由器設備之IPv6規格如下
  - 資料參考台銀共同供應契約LP5-101018網路及資訊安全暨加值設備
    - 第1組 交換器及路由器網路設備
  - https://www.bot.com.tw/Procurement/Procure_supply/Supply_index/Documents/101/LP5-101018/LP5_101018_1011201_002.htm
  - 17-1至17-12等子項目之IPv6規格均相同，以17-1子項目之IPv6規格為例

既有共同供應契約-IPv6相關規範	本計畫建議IPv6規範
17-1-14.符合下列任一IPv6功能說明或證明文件 17-1-14-1.通過IPv6組織驗證測試，具備IPv6 Ready Logo Phase2認證文件 17-1-14-2.符合IETF(Internet Engineering Task Force)(網際網路專業任務小組)發展規範Request for Comments之RFC 2460 Internet Protocol, Version 6(IPv6) Specification、RFC 4861 Neighbor Discovery for IP Version 6(IPv6)、RFC 4862 IPv6 Stateless Address Autoconfiguration、RFC 4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification、RFC5095 Deprecation of Type 0 Routing Headers in IPv6及RFC1981 Path MTU Discovery for IP version 6等規範標準 17-1-14-3.經由IPv6組織網站(https://www.ipv6ready.org/db/index.php/public)驗證查詢，取得相關該產品名稱或系列名稱等文件證明(須為通過IPv6 Ready Logo Phase2產品)	1. 必須支援IPv6 Addressing Architecture 定義之位址格式規範 2. 必須支援IPv6 Default Address Selection功能 3. 必須支援Unique Local IPv6 Unicast Addresses (ULA)位址格式 4. 必須支援ICMPv6通訊協定 5. 必須支援SLAAC 功能 6. 應支援Multicast Listener Discovery version 2 (MLDv2)以及MLDv2 snooping功能 7. 必須支援Router-Alert option功能 8. 必須支援Path MTU Discovery 功能 9. 必須支援Neighbor Discovery 功能 10. 必須支援IPv6 QoS 功能 11. 必須棄用IPv6 Type 0 Routing Headers 12. 如須支援Interior Gateway Protocol (IGP)，則Router路由器必須支援RIPng以及OSPFv3 13. 如須使用OSPFv3，則Router路由器必須支援Authentication/Confidentiality for OSPFv3 14. 如須支援Exterior Gateway Protocol (EGP)，則Router路由器必須支援MBGP功能 15. 如須支援Tunneling以及DualStack，則Router路由器必須支援基本IPv6轉移機制 16. 如須支援Mobile IPv6，則Router路由器必須支援MIPv6機制以及Mobile IPv6 Operation With IKEv2 的行為模式 17. 如須支援MPLS，則Router路由器必須支援MPLS Traffic Engineer(TE)以及MPLS Fast Reroute(FRR)功能 18. 如須支援L3 VPN，則Router路由器必須支援BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN

網路保護裝置設備規範建議

- 既有共同供應契約中網路保護裝置設備之IPv6規格如下
  - 資料參考台銀共同供應契約LP5-101018網路及資訊安全暨加值設備
    - 第3組 網路資訊安全設備
  - https://www.bot.com.tw/Procurement/Procure_supply/Supply_index/Documents/101/LP5-101018/LP5_101018_1011201_002.htm
  - 1-1至1-7等子項目之IPv6規格均相同，以1-1子項目之IPv6規格為例
  - 2-1至2-8等子項目之IPv6規格均相同，以2-1子項目之IPv6規格為例

既有共同供應契約-IPv6相關規範 (入侵偵測防禦系統)	既有共同供應契約-IPv6相關規範(防火牆)
1-1-18.符合下列任一 IPv6 功能說明或證明文件 1-1-18-1.通過 IPv6 組織驗證測試，具備 IPv6 Ready Logo Phase2 認證文件 1-1-18-2.符合IETF(Internet Engineering Task Force)(網際網路專案任務小組)發展規範Request for Comments之RFC 2460 Internet Protocol, Version 6(IPv6) Specification、RFC 4861 Neighbor Discovery for IP Version 6(IPv6)、RFC 4862 IPv6 Stateless Address Autoconfiguration、RFC 4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification、RFC5095 Deprecation of Type 0 Routing Headers in IPv6 及RFC1981 Path MTU Discovery for IP version 6 等規範標準 1-1-18-3.經由IPv6 組織網站(https://www.ipv6ready.org/db/index.php/public)驗證查詢，取得相關該產品名稱或系列名稱等文件證明(須為通過IPv6 Ready Logo Phase2 產品) 1-1-18-4.具備單獨偵測IPv4(Native IPv4)與IPv6(Native IPv6)網路封包，並在IPv4 及IPv6 雙軌(Dual Stack)運行之網路環境同時偵測IPv4 與IPv6 網路封包	2-1-11.符合下列任一 IPv6 功能說明或證明文件 2-1-11-1.通過 IPv6 組織驗證測試，具備 IPv6 Ready Logo Phase2 認證文件 2-1-11-2.符合IETF(Internet Engineering Task Force)(網際網路專案任務小組)發展規範Request for Comments之RFC 2460 Internet Protocol, Version 6(IPv6) Specification、RFC 4861 Neighbor Discovery for IP Version 6(IPv6)、RFC 4862 IPv6 Stateless Address Autoconfiguration、RFC 4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification、RFC5095 Deprecation of Type 0 Routing Headers in IPv6 及RFC1981 Path MTU Discovery for IP version 6 等規範標準 2-1-11-3.經由IPv6 組織網站(https://www.ipv6ready.org/db/index.php/public)驗證查詢，取得相關該產品名稱或系列名稱等文件證明(須為通過IPv6 Ready Logo Phase2 產品) 2-1-11-4.具備狀態檢視(stateful packet inspection (SPI) or stateful inspection)過濾IPv4(Native IPv4)與IPv6(Native IPv6)網路封包，並在IPv4 及IPv6 雙軌(Dual Stack)運行之網路環境同時過濾IPv4與IPv6網路封包，另提供IPv6路由協定(Static route)功能

網路保護裝置設備規範建議(續)

本計畫建議網路保護裝置IPv6規範
1. 必須支援IPv6 Addressing Architecture 定義之位址格式規範 2. 必須支援IPv6 Default Address Selection功能 3. 必須支援ICMPv6 功能 4. 必須支援IPv6 StateLess Address AutoConfiguration 功能 (FW, IPS) 5. 必須支援Router-Alert option功能 (FW, IPS) 6. 必須支援Path MTU Discovery功能 7. 必須支援Neighbor Discovery 功能 8. 必須支援IPv6 QoS 功能(FW, APFW) 9. 如須支援Interior Gateway Protocol (IGP)，則裝置必須支援RIPng以及OSPFv3 10. 如須支援Exterior Gateway Protocol (EGP)，則裝置必須支援MBGP 11. 如須使用OSPFv3，則裝置必須支援Authentication/Confidentiality for OSPFv3 12. 如須支援Tunneling，則裝置必須支援基本IPv6轉移機制(FW) 13. 必須棄用IPv6 Type 0 Routing Headers 14. 網路管理不允許IPv6隧道時，需可檢查/阻擋IPv4 header中Type欄位值為41的IPv4封包(IPS/FW) 15. 可過濾ICMPv6封包，並制定封包過濾規則(FW) 16. 可過濾內含Extension Header的IPv6封包，並制定封包過濾規則(FW)

註: 網路保護裝置系指：Firewall (FW), Intrusion prevention device (IPS), 以及Application firewall (APFW)