109 年研究報告

# 『前瞻及完整之 IPv6 生態系推動方案』
# 期末報告

**計畫補助機關：國家通訊傳播委員會**

**中華民國 109 年 12 月**

109 年研究報告

GRB 系統編號：PG10903-0310

# 前瞻及完整之 IPv6 生態系推動方案


**受委託單位**

財團法人台灣網路資訊中心

**計畫主持人**

顧靜恆

**研究人員**

蔡更達、王彥傑、陳玟羽、許淑芳



**研究期程：中華民國 109 年 03 月至 109 年 12 月**

**研究經費：新臺幣 660.1 萬元**



**本報告不必然代表國家通訊傳播委員會意見**



**中華民國 109 年 12 月**

# 目 次

表　　次 …… V

圖　　次 …… XIII

提　　要 …… XXVIII

英文摘要 …… XL

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 ..... 46

第三節 資源運用檢討 ..... 52

第二章　市售網通產品調查 ..... 53

第一節 市售網通產品調查 ..... 53

第二節 廠商支援 IPv6 意願調查 ..... 68

第三章　國內 IASP 支援 IPv6 普查 ..... 85

第四章　Native IPv6 連網試驗環境建置 ..... 112

第一節 Native IPv6 試驗網路環境建置 ..... 113

第二節 Native IPv6 試驗網路環境測試 ..... 127

第五章　IPv6 動態 DNS 服務軟體開發 ..... 134

第一節 開發 IPv6 動態 DNS 服務軟體 ..... 134

第二節 IPv6 動態 DNS 服務軟體測試 ..... 149

第三節 IPv6 動態 DNS 服務軟體手冊撰寫 ..... 155

第六章　IASP 及 ICP IPv6 升級推廣 ..... 157

第一節 推廣 Cable 用戶申請試用 IPv6 ..... 157

第二節 推廣手機用戶下載 APN 設定 IPv6 APP ..... 161

第三節 與公協會合作推廣 IPv6 ..... 166

第四節 推廣.tw 網站升級 IPv6 ..... 185

第五節 德國 IASP 之 IPv6 推動歷程.....189
第六節 法國 IASP 之 IPv6 推動歷程.....199
第七章 IPv6 用戶資通安全防護研析.....213
第一節 IPv6 家用資通安全防護研析.....216
第二節 IPv6 企業用戶資通安全防護研析.....235
第八章 ICP IPv4/IPv6 雙協定網路安全技術防護人才培訓教育訓練.....249
第一節 第一場教育訓練課程.....250
第二節 第二場教育訓練課程.....256
第三節 第三場教育訓練課程.....263
第四節 第四場教育訓練課程.....267
第五節 第五場教育訓練課程.....271
第六節 第六場教育訓練課程.....275
第七節 第七場教育訓練課程.....279
第八節 第八場教育訓練課程.....282
第九章 蒐集並整理 ISP 之 IPv6 網路安全防護準則.....286
第一節 研析 ISP IPv6 網路安全基本防護要項.....286
第二節 研析 ISP IPv6 網路連線服務安全防護建議事項.....321
第十章 蒐集國內外物聯網服務實際應用案例.....357
第一節 食的物聯網 – 全程冷鏈不斷鏈管理.....357
第二節 醫的物聯網 –LincGo 服務架構與技術.....362
第三節 住的物聯網 – 雲端智慧綠能管理系統.....373
第四節 行的物聯網 – 中華電信智慧停車場.....380
第五節 育的物聯網 – 工業 4.0 模擬研發實驗室.....383
第六節 樂的物聯網 – 智慧導覽與實境遊戲平台.....387
第十一章 研析網際網路技術標準.....391
第一節 IP (Internet Protocol，網際網路協定).....391
第二節 DN (Domain Name，網域名稱).....404

第三節 BGP (Boarder Gateway Protocol，邊界閘道器協定).....430
第四節 RPKI (Resource Public Key Infrastructure，網際網路號碼資源公鑰基礎建設).....440
第五節 DNSSEC (Domain Name System Security Extensions，域名系統安全擴充).....450
第六節 SIP (Session Initiation Protocol，對話啟動協定).....464
第十二章 會議及報告.....480
第一節 每月月報.....480
第十三章 結論與建議.....484
第一節 結論說明.....484
第二節 建議事項.....488
參考資料
中英專有名詞對照

附錄

附錄一　「IASP 問卷調查」報告

附錄二　「ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓教育訓練」教材

附錄三　月報工作進度報告會議資料

附錄四　「市售產品支援 IPv6 調查」報告

附錄五　「Native IPv6 連網環境建置及 IPv6 用戶安全防護研析」報告

附錄六　「IPv6 用戶安全防護研析」手冊

附錄七　「IPv6 動態 DNS 服務軟體開發」報告

附錄八　「蒐集並整理 ISP 之 IPv6 網路安全防護準則」報告

附錄九　「物聯網服務與應用研析及網際網路技術標準研析」報告

# 表 次

表 1、計畫具體衡量之績效指標 ..... 44
表 2、各項工作執行進度 ..... 46
表 3、各項查核進度表 ..... 49
表 4、期末報告量化指標 ..... 50
表 5、執行人力表 ..... 52
表 6、合計總經費運用情形統計表 ..... 52
表 7、調查通路銷售店家數 ..... 56
表 8、民國 106 年及 108 年國內寬頻分享器銷售量比較表 57
表 9、民國 108 年寬頻分享器銷售前 20 名銷售量及佔比 . 60
表 10、民國 108 年寬頻分享器銷售前 20 名產品支援 IPv6 情況 ..... 61
表 11、民國 108 年寬頻分享器品牌銷售統計資料 ..... 62
表 12、民國 106 年及 108 年市售寬頻分享器品牌銷售量排行比較 ..... 66
表 13、支援 IPv4/IPv6 PPPoE 雙軌網路服務之寬頻分享器測試項目 ..... 69

表 14、熱銷前 20 名寬頻分享器和 HINET IPV6 互通性測試結果 ..... 70
表 15、支援 IPV4/IPV6 IPOE 雙軌網路服務之寬頻分享器測試項目 ..... 76
表 16、熱銷前 20 名寬頻分享器和 TBC IPV6 互通性測試結果 ..... 77
表 17、統計 IASP 業者是否有 IPV4 位址面臨不足的問題 86
表 18、IASP 業者預期面臨 IPV4 不足時程表 ..... 87
表 19、IASP 業者問卷統計 IPV6 位址申請及 IPV6 路由狀況 ..... 90
表 20、IASP 業者光纖上網提供 IPV6 時程表 ..... 92
表 21、IASP 業者 CO-LOCATION/IDC 服務提供 IPV6 時程表 ..... 93
表 22、IASP 業者雲端服務提供 IPV6 時程表 ..... 93
表 23、IASP 業者 PWLAN 無線上網提供 IPV6 時程表 .... 94
表 24、IASP 業者提供 IPV6 支援時程統計表 ..... 95
表 25、IASP 業者各項服務支援 IPV6 統計表 ..... 98
表 26、IASP 業者問卷統計支援 IPV6 預計增加支出項目 . 99

表 27、IASP 業者問卷統計支援 IPv6 可能面臨的問題... 101
表 28、IASP 業者問卷統計支援 IPv6 網路發展上希望政府協助項目 ..... 104
表 29、IASP 業者統計支援 IPv6 連線服務位址配發方式 105
表 30、全球 IPv6 使用率排名前 30 國家列表 ..... 108
表 31、台灣主要 IASP 之 IPv6 連網比例 .....110
表 32、NAT64/DNS64 資源體配置 ..... 122
表 33、NAT64/DNS64 網路配置對照資訊 ..... 123
表 34、464XLAT 資源配置 ..... 124
表 35、464XLAT 網路配置 ..... 125
表 36、NAT64/DNS64 基本測試結果..... 129
表 37、NAT64/DNS64 連線測試結果..... 130
表 38、NAT64/DNS64 應用測試結果..... 130
表 39、464XLAT 基本測試結果 ..... 131
表 40、464XLAT 連線測試結果 ..... 132
表 41、464XLAT 應用測試結果 ..... 132
表 42、動態 DNS 服務 SERVER 端應用功能..... 138
表 43、動態 DNS 服務 CLIENT 端軟體功能 ..... 140

表 44、PHP7 的程式語言開發建議事項列表 ..... 144
表 45、ELECTRON 的程式語言開發建議事項列表 ..... 145
表 46、資料庫結構設計建議事項列表 ..... 145
表 47、資訊安全建議事項列表 ..... 146
表 48、COLLATION 格式比較 ..... 148
表 49、CHARACTER SET 格式比較 ..... 148
表 50、IPv4 環境測試檢查清單 ..... 152
表 51、IPv6 環境測試檢查清單 ..... 153
表 52、動態 DNS 重新連線測試檢查清單 ..... 154
表 53、推廣手機用戶下載 APN 設定 IPv6 APP 歷程 ..... 162
表 54、手機啟動 IPv4/IPv6 網路設定 APP 下載次數統計表 ..... 165
表 55、與 TIEA 合作推廣 IPv6 歷程 ..... 167
表 56、與 DTA 合作推廣 IPv6 歷程 ..... 169
表 57、與 TCA 合作推廣 IPv6 歷程 ..... 171
表 58、2020【網路・共贏時代】專家座談會活動議程 .. 176
表 59、2020 TWNIC IPv6 推廣講座活動議程 ..... 182

表 60、109 年計畫和公協會所合作進行各項 IPv6 推廣活動資訊 ..... 184
表 61、推廣.TW 網站升級 IPv6 列表 ..... 185
表 62、德國主要 IASP 之 IPv6 推動歷程 ..... 197
表 63、法國主要 IASP 分配 IPv6 位址數量 ..... 206
表 64、法國主要 IASP 之 IPv6 推動歷程 ..... 212
表 65、IPv6 用戶資通安全防護研析相關 RFC 列表 ..... 214
表 66、IPv6 位址類型及說明 ..... 217
表 67、IPv6 單播位址類型及說明 ..... 218
表 68、NEIGHBOR DISCOVERY (ND) 協定主要目的 ..... 219
表 69、IPv6 之 ND 訊息類別及說明 ..... 220
表 70、IPv6 之 ND 攻擊類型 ..... 222
表 71、IPv6 之 RA 攻擊類型 ..... 225
表 72、IPv6 ACL 網路安全防禦機制測試範例 ..... 233
表 73、IPv6 在網路安全上的強化功能 ..... 236
表 74、IPv4 資安攻擊類別 ..... 238
表 75、企業網路部署 IPv6 需求 ..... 242
表 76、企業網路內部 IPv6 部署階段指引 ..... 243

表 77、企業網路外部 IPv6 部署階段指引 ..... 243
表 78、企業網路資安工作重點 ..... 247
表 79、企業網路導入 IPv6 安全防護檢核清單 ..... 248
表 80、「ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓」課程大綱 ..... 249
表 81、109 年 ICP IPv4/IPv6 教育訓練課程參與人數及問卷統計 ..... 285
表 82、ISP IPv6 網路安全防護相關文獻 ..... 288
表 83、IPv6 定址規劃參考文獻 ..... 289
表 84、單一區域位址 ULA 參考文獻 ..... 290
表 85、點對點鏈接參考文獻 ..... 291
表 86、靜態配置位址參考文獻 ..... 292
表 87、臨時位址參考文獻 ..... 293
表 88、DNS64 參考文獻 ..... 295
表 89、UNIQUE IPV6 PREFIX 參考文獻 ..... 296
表 90、位址隱私參考文獻 ..... 296
表 91、延伸標頭參考文獻 ..... 297
表 92、延伸標頭的順序和重複次數參考文獻 ..... 298

表 93、逐跳選項標頭參考文獻 ..... 299
表 94、分段標頭參考文獻 ..... 300
表 95、IP 安全延伸標頭參考文獻 ..... 300
表 96、IPv6 鏈路層安全考量參考文獻 ..... 301
表 97、使用 IPv6 對 IPv4 轉換機制參考文件 ..... 342
表 98、雲端綠能管理系統軟體服務 ..... 374
表 99、IPv6 和 IPv4 比較表 ..... 393
表 100、IPv6 優勢 ..... 396
表 101、NDP 資訊交換時所提查詢訊息需求類別 ..... 397
表 102、IETF 中 IPv6 相關領域工作組類別 ..... 402
表 103、IETF 之 IPv6 相關重點工作組簡介 ..... 403
表 104、DNS 設計目標 ..... 404
表 105、網域名稱標籤命名規則 ..... 406
表 106、全球知名通用頂級域名類別 ..... 410
表 107、DNS 查詢步驟說明 ..... 412
表 108、TCP 傳輸特性 ..... 418
表 109、支援 IPv6 之 DNS 擴充功能 ..... 418
表 110、DNS 標誌字段組成 ..... 420

表 111、DNS 封包的問題區段 (QUESTION SECTION) 格式421
表 112、DNS 封包的答案區段 (ANSWER SECTION) 格式 422
表 113、常見的資源紀錄類型 ..... 423
表 114、重要 BGP 相關 RFC 列表 ..... 432
表 115、DNSSEC 資源記錄 ..... 452
表 116、DS 和 CDS 加密演算法 ..... 453
表 117、SIP 標頭欄位的簡稱..... 471
表 118、已完成工作項目列表 ..... 480

# 圖 次


圖 1、GOOGLE 統計全球 IPV6 連網使用比例 ..... 2

圖 2、W3TECHS 統計網站支援 IPV6 趨勢 ..... 4

圖 3、W3TECHS 統計網站支援 IPV6 比例 ..... 5

圖 4、IPV4/IPV6 雙軌普行推動方向 ..... 6

圖 5、推動 IPV4/IPV6 雙軌普行方案工作架構 ..... 7

圖 6、計畫施行方法 ..... 15

圖 7、商用網路雙軌普行推動工作項目 ..... 18

圖 8、市售網通產品調查流程 ..... 20

圖 9、國內 IASP 業者支援 IPV6 調查流程 ..... 22

圖 10、464XLAT 在固網網路運作架構 ..... 25

圖 11、464XLAT 在手機 3GPP 行動通訊網路運作架構 ... 25

圖 12、NATIVE IPV6 網路建置及驗證流程 ..... 26

圖 13、IPV6 動態 DNS 服務軟體開發流程 ..... 28

圖 14、IASP 及 ICP IPV6 升級推廣工作項目 ..... 30

圖 15、雙軌連網環境安全研析工作項目 ..... 34

圖 16、物聯網服務與應用研析工作項目 ..... 38

圖 17、市售寬頻分享器調查通路 ..... 54
圖 18、市售產品調查零售店家數量分布 ..... 55
圖 19、民國 106 年及 108 年寬頻分享器銷售通路結構變化圖 ..... 57
圖 20、民國 108 年寬頻分享器銷售前 20 名型號及佔比 .. 59
圖 21、民國 108 年寬頻分享器銷售量前 20 名 IPv6 支援佔比 ..... 61
圖 22、寬頻分享器依品牌統計支援 IPv6 商品數佔比 ..... 63
圖 23、民國 106 年與 108 年市售頻分享器支援 IPv6 比較圖 ..... 64
圖 24、民國 108 年寬頻分享器銷售量前 10 名品牌 ..... 65
圖 25、民國 106 及 108 年寬頻分享器前 4 大品牌佔比 .... 65
圖 26、TP-Link (普聯) TL-WR840N 確認 PPPoE 已連接 71
圖 27、TP-Link (普聯)TL-WR840N 不支援自動啟用 IPv672
圖 28、TP-Link (普聯) TL-WR840N 可正常連線 PPPoEv6 ..... 72
圖 29、TP-Link (普聯) TL-WR840N 驗證 IPv6 上網正常 73

圖 30、TP-LINK (普聯) TL-WR840N 以 IPV6 連結熱門網頁正常 ..... 73
圖 31、TP-LINK (普聯) TL-WR840N 以 IPV6 連結進行重撥正常 ..... 74
圖 32、TP-LINK (普聯) TL-WR840N 以 WI-FI 上網 IPV6、DNSV6 正常 ..... 74
圖 33、TP-LINK (普聯) TL-WR840N 連接 WI-FI IPV6 上網正常 ..... 75
圖 34、ASUS (華碩) 2RT-N12+B1 確認 IPV6 CABLE MODEM 可連接 ..... 78
圖 35、ASUS (華碩) 2RT-N12+B1 不支援自動啟用 IPV6 . 79
圖 36、ASUS (華碩) 2RT-N12+B1 可正常連線 IPOEV6 .... 79
圖 37、ASUS (華碩) 2RT-N12+B1 驗證 IPV6 上網正常 .... 80
圖 38、ASUS (華碩) 2RT-N12+B1 以 IPV6 連結熱門網頁正常 ..... 80
圖 39、ASUS (華碩) 2RT-N12+B1 以 IPV6 連結進行重撥正常 ..... 81

圖 40、ASUS (華碩) 2RT-N12+B1 以 Wi-Fi 上網 IPv6、DNSv6 正常 ..... 81
圖 41、ASUS (華碩) 2RT-N12+B1 連接 Wi-Fi IPv6 上網正常 ..... 82
圖 42、IASP 業者對於 IPv4 位址不足所進行相關策略統計圖 ..... 88
圖 43、IASP 業者問卷 IPv6 位址申請及 IPv6 路由狀況統計圖 ..... 90
圖 44、IASP 業者問卷支援 IPv6 預計增加支出項目統計圖 ..... 99
圖 45、IASP 業者問卷支援 IPv6 可能面臨的問題統計圖 102
圖 46、IASP 業者問卷支援 IPv6 網路發展上希望政府協助項目 ..... 104
圖 47、IASP 業者支援 IPv6 連線服務位址配發方式統計圖 ..... 106
圖 48、台灣 IPv6 使用量測數據圖 ..... 107
圖 49、台灣商用網路 IASP 業者 IPv6 連網比例 ..... 109
圖 50、台灣政府及學術網路 IPv6 連網比例 .....110

圖 51、NAT64/DNS64 網路架構 .....114
圖 52、464XLAT 網路架構 .....115
圖 53、NAT64/DNS64 實驗架構規劃與 IP 配置.....116
圖 54、464XLAT 實驗架構規劃與 IP 配置.....117
圖 55、NAT64/DNS64 設定範例 ..... 120
圖 56、464XLAT 設定範例 ..... 121
圖 57、NAT64/464XLAT 測試架構..... 128
圖 58、動態 DNS 系統架構..... 136
圖 59、動態 DNS 服務之 IP 位址取得流程 ..... 137
圖 60、在動態 DNS 之 SERVER 服務應用上新增主機介面139
圖 61、在動態 DNS 之 SERVER 顯示主機列表介面 ..... 140
圖 62、動態 DNS 之 CLIENT 端應用軟體登入介面圖 ..... 141
圖 63、動態 DNS CLIENT 主機更新介面圖 ..... 142
圖 64、動態 DNS 服務環境建置架構..... 150
圖 65、動態 DNS 軟體下載連結網站截圖 ..... 155
圖 66、動態 DNS 軟體於 TANET 宣傳文宣 ..... 156
圖 67、TBC 之 IPV6 服務申請書網路下載專區 ..... 159
圖 68、TBC 之 IPV6 服務常見問題專區..... 160

圖 69、IP/DNS 論壇進行手機 APP 推廣 ..... 163
圖 70、TWNIC 電子報進行手機 APP 推廣 ..... 163
圖 71、TCA 協助進行手機 APP 推廣 ..... 164
圖 72、GOOGLE PLAY 商店下載統計趨勢圖 ..... 165
圖 73、TIEA 轉發 TWNIC 教育訓練課程資訊..... 168
圖 74、DTA 轉發 TWNIC 教育訓練課程資訊..... 170
圖 75、TCA 於 4 月 28 日在資訊月 ONLINE 進行 IPV6 活動宣傳截圖 ..... 172
圖 76、TCA 於 4 月 30 日在資訊月 ONLINE 進行 IPV6 活動宣傳截圖 ..... 173
圖 77、TCA 於 6 月 11 日協助進行 IPV6 教育訓練宣傳截圖..... 174
圖 78、TCA 於 7 月 3 日協助進行 IPV6 教育訓練宣傳截圖 ..... 174
圖 79、2020【網路・共贏時代】專家座談會活動現場照片 ..... 175
圖 80、TWNIC 於 HITCON 2020 進行〝國際及台灣 IPV6 發展介紹〞..... 180

圖 81、【2020 TWNIC IPv6 推廣講座活動】活動宣傳頁面 ..... 181
圖 82、【2020 TWNIC IPv6 推廣講座活動】現場照片 .. 183
圖 83、驗證網站支援 IPv6 位址資訊截圖 ..... 187
圖 84、檢測網站支援 IPv6 服務可正常連線截圖 ..... 187
圖 85、以 IPv6 test 進行網站 IPv6 支援檢測截圖 ..... 188
圖 86、德國 IPv6 使用比率統計圖 ..... 189
圖 87、德國主要 IASP IPv6 量測統計資料 ..... 190
圖 88、德國電信 TERASTREAM 網路架構 ..... 191
圖 89、德國電信之 IPv6 使用比率統計圖 ..... 192
圖 90、德國 Vodafone 之 IPv6 使用比率統計圖 ..... 193
圖 91、德國 Telefonica 之 IPv6 使用比率統計圖 ..... 194
圖 92、德國 Kabel Deutschland 之 IPv6 使用比率統計圖 ..... 195
圖 93、德國 Versatel 之 IPv6 使用比率統計圖 ..... 196
圖 94、鋐寶科技為 Tele Columbus 設計生產 Cable Gateway 產品 ..... 197
圖 95、法國 IPv6 使用比率統計圖 ..... 199

圖 96、法國主要 IASP IPv6 量測統計資料 ..... 200
圖 97、西元 2019 年法國四大固接網路服務 IASP 支援 IPv6 統計 ..... 201
圖 98、西元 2019 年法國四大 IASP 各項服務支援 IPv6 統計 ..... 202
圖 99、法國四大行動電信業者支援 IPv6 統計及預測資料203
圖 100、法國 ORANGE 之 IPv6 使用比率統計圖 ..... 205
圖 101、法國主要 IASP 分配 IPv6 位址數量比例圖 ..... 206
圖 102、法國 FREE 之 IPv6 使用比率統計圖 ..... 208
圖 103、法國 FREE MOBILE 之 IPv6 使用比率統計圖 ..... 209
圖 104、法國 SFR 之 IPv6 使用比率統計圖 ..... 210
圖 105、法國 SFR 企業用戶之 IPv6 使用比率統計圖 ..... 210
圖 106、法國 BOUYGUES TELECOM 之 IPv6 使用比率統計圖 .....211
圖 107、IPv6 資通安全防護研究架構 ..... 213
圖 108、IPv6 之 ND 攻擊示意圖 ..... 221
圖 109、IPv6 之 RA 攻擊示意圖 ..... 224
圖 110、IPv6 之 ICMPv6 攻擊示意圖 ..... 227

圖 111、家用 CPE IPv6 ACL 測試架構範例..... 231
圖 112、D-LINK CPE IPv6 ACL 設定範例..... 232
圖 113、確認用戶 IPv6 上網正常 ..... 233
圖 114、啟用 ACL 功能後被設定阻擋的主機無法取得 IPv6 位址 ..... 234
圖 115、企業用戶 IPv6 資通安全防護技術研究範疇 ..... 235
圖 116、企業網路架構 ..... 247
圖 117、IP/DNS 論壇教育訓練課程宣傳 ..... 251
圖 118、TWNIC 於 4 月份電子報進行教育訓練課程宣傳251
圖 119、寄送電子郵件給 TWNIC IP 會員進行教育訓練課程宣傳 ..... 252
圖 120、4/29 雲林 ICP IPv4/IPv6 教育訓練活動資訊來源調查 ..... 253
圖 121、4/29 雲林 ICP IPv4/IPv6 教育訓練滿意度統計 . 254
圖 122、4/29 雲林 ICP IPv4/IPv6 教育訓練會場 ..... 255
圖 123、4/29 雲林 ICP IPv4/IPv6 教育訓練線上課程截圖255
圖 124、福華國際文教會館防疫措施公告 ..... 257
圖 125、第二場教育訓練報名資訊網站截圖 ..... 258

圖 126、第二場教育訓練學員上課通知 EMAIL 截圖 ..... 259
圖 127、5/15 台北 ICP IPv4/IPv6 教育訓練活動資訊來源調查 ..... 260
圖 128、5/15 台北 ICP IPv4/IPv6 教育訓練滿意度統計 . 261
圖 129、5/15 台北 ICP IPv4/IPv6 教育訓練會場 ..... 261
圖 130、5/15 台北 ICP IPv4/IPv6 教育訓練線上課程截圖 262
圖 131、第三場教育訓練報名資訊網站截圖 ..... 263
圖 132、6/23 高雄 ICP IPv4/IPv6 教育訓練活動資訊來源調查 ..... 264
圖 133、6/23 高雄 ICP IPv4/IPv6 教育訓練滿意度統計 . 265
圖 134、6/23 高雄 ICP IPv4/IPv6 教育訓練會場 ..... 266
圖 135、6/23 高雄 ICP IPv4/IPv6 教育訓練線上課程截圖 266
圖 136、第四場教育訓練 E-MAIL 推廣招生資訊截圖 ..... 267
圖 137、7/17 雲林 ICP IPv4/IPv6 教育訓練活動資訊來源調查 ..... 268
圖 138、7/17 雲林 ICP IPv4/IPv6 教育訓練滿意度統計 . 269
圖 139、7/17 雲林 ICP IPv4/IPv6 教育訓練會場 ..... 269
圖 140、7/ 17 雲林 ICP IPv4/IPv6 教育訓練線上課程截圖 270

圖 141、第五場教育訓練 E-MAIL 推廣招生資訊截圖 ..... 271
圖 142、7/31 台北 ICP IPv4/IPv6 教育訓練活動資訊來源調查 ..... 272
圖 143、7/31 台北 ICP IPv4/IPv6 教育訓練滿意度統計 . 273
圖 144、7/31 台北 ICP IPv4/IPv6 教育訓練會場 ..... 273
圖 145、7/ 31 台北 ICP IPv4/IPv6 教育訓練線上課程截圖 274
圖 146、第六場教育訓練網站推廣招生資訊截圖 ..... 275
圖 147、8/28 台南 ICP IPv4/IPv6 教育訓練活動資訊來源調查 ..... 276
圖 148、8/28 台南 ICP IPv4/IPv6 教育訓練滿意度統計 . 277
圖 149、8/28 台南 ICP IPv4/IPv6 教育訓練會場 ..... 278
圖 150、第七場教育訓練網站推廣招生資訊截圖 ..... 279
圖 151、9/18 台北 ICP IPv4/IPv6 教育訓練活動資訊來源調查 ..... 280
圖 152、9/18 台北 ICP IPv4/IPv6 教育訓練滿意度統計 . 281
圖 153、9/18 台北 ICP IPv4/IPv6 教育訓練會場 ..... 281
圖 154、第八場教育訓練網站推廣招生資訊截圖 ..... 282

圖 155、9/30 高雄 ICP IPv4/IPv6 教育訓練活動資訊來源調查 ..... 283
圖 156、9/30 高雄 ICP IPv4/IPv6 教育訓練滿意度統計 . 284
圖 157、9/30 高雄 ICP IPv4/IPv6 教育訓練會場 ..... 285
圖 158、ISP 服務架構示意圖 ..... 286
圖 159、電纜寬頻網路架構圖 ..... 322
圖 160、DSL 寬頻網路的架構圖 ..... 325
圖 161、點對點模型協定體系結構 ..... 327
圖 162、使用 PPP 進行連結架構 ..... 328
圖 163、L2TPv2 存取聚合 (LAA) 模型透過 PPP 連接架構 ..... 329
圖 164、混合模型中 IPv6 和 IPv4 的邏輯設計 ..... 330
圖 165、乙太存取網路架構 ..... 333
圖 166、點對點模型協定架構 ..... 334
圖 167、L2TPv2 存取聚合 (LAA) 模型架構 ..... 335
圖 168、行動網路架構 ..... 338
圖 169、公眾無線網路架構 ..... 345

圖 170、當第 2 層交換機位於 AP 和邊緣路由器間的 WLAN 結構 ..... 347
圖 171、存取路由器位於 AP 與邊緣路由器之間時的 WLAN 結構 ..... 349
圖 172、IPv6 WLAN 環境中的 PTA 模型架構 ..... 351
圖 173、IPv6 WLAN 環境中的 LAA 模型架構 ..... 352
圖 174、全程冷鏈不斷鏈解決方案 ..... 358
圖 175、冷鏈物流解決方案系統架構 ..... 359
圖 176、冷鏈物流裝置傳輸架構 ..... 360
圖 177、LINCGO 系統平台提供完整的解決方案 ..... 362
圖 178、建立並監控低功號藍牙無線網路之方法 ..... 365
圖 179、雲端綠能管理系統架構 ..... 373
圖 180、智慧停車場物聯網架構 ..... 380
圖 181、物聯網應用類型及適用網路通訊協定分類 ..... 382
圖 182、慧魚工程模組自動化模擬工廠 ..... 383
圖 183、慧魚工程模組裝置間連接架構 ..... 386
圖 184、線上智慧導覽網站截圖 ..... 387
圖 185、自動介紹與定位導航 ..... 388

圖 186、IP 規格演進歷程 ..... 392
圖 187、IPv4 及 IPv6 表頭結構..... 394
圖 188、IPv6 主要通訊協議架構..... 396
圖 189、DHCPv6 運作過程 ..... 401
圖 190、DNS 命名空間範例..... 407
圖 191、DNS 查詢流程 .....411
圖 192、DNS 遞迴查詢流程..... 415
圖 193、DNS 迭代查詢流程..... 416
圖 194、DNS 封包格式 ..... 419
圖 195、iBGP 和 eBGP 關係圖..... 431
圖 196、iBGP Route Reflector..... 438
圖 197、BGP Confederation..... 438
圖 198、RPKI 憑證頒發機構層級架構圖 ..... 442
圖 199、PKI 實體架構..... 443
圖 200、RPKI Validator 資料同步架構..... 448
圖 201、DNSSEC 運作流程解構圖 ..... 454
圖 202、信任鏈示意圖 ..... 459
圖 203、SIP 基礎架構..... 465

**圖 204、IP 相關協定堆疊 ..... 469**

**圖 205、SIP 註冊流程 ..... 472**

**圖 206、SIP 對話建立及消滅流程 ..... 473**

**圖 207、IMS 架構圖 ..... 475**

**圖 208、VoLTE / Vo5G 架構 ..... 476**

# 提　要

關鍵詞：網際網路、IPv4、IPv6、雙軌 (Dual stack)

## 一、研究緣起

因應全球 IPv4 短缺，IPv6 普行使用已是當前數位時代基礎建設中之重要一環，同時新網路及應用 (如車聯網、智慧城市、智慧家庭) 需求，以及目前我國積極推動之數位國家發展政策，亟需儘速推動 IPv6 網路之普遍建置與普及使用。以藉此延續我國 IPv6 使用成長趨勢，建立前瞻及完整之 IPv6 生態系，並創造發展網路應用服務之基礎，方能面對未來的網際網路世界，並進而尋找產業發展機會。

本計畫將進行 IPv6 相關研究、調查及推廣，並以落實 IPv6 連網環境、強化 IPv6 連網安全及探索 IPv6 連網應用等方面著手，以期達到使用者設備普遍支援 IPv6、增加支援 IPv6 之 IASP 業者、增加支援 IPv6 之應用網站以及消費者宣導，進一步提升我國之 IPv6 使用率與國際同步，並建立我國 IPv6 之完整生態系。

本計畫推動方向，針對使用者設備、IASP 網路、應用網站、企業網路等方面之問題推行解決方案，進行市售網通產品支援 IPv6 調查、國內 IASP 業者支援 IPv4/IPv6 雙軌連網服

務之整備程度調查，推動 Native IPv6 連網試驗環境建置及驗證，開發 IPv6 動態 DNS 服務軟體、推廣 IASP 及 ICP IPv6 升級，持續推動商用網路雙軌普行。透過進行 IPv6 用戶資通安全防護研析及 ICP IPv4/IPv6 雙協定網路安全技術防護人才培訓教育訓練，加強雙軌連網環境安全。蒐集國內外物聯網服務實際應用案例及研析網際網路技術標準，進行物聯網服務與應用研析。

因應國際 IPv6 發展潮流,世界各國皆在推動及發展 IPv6,藉由推動及完善國內 IPv6 網路環境及使用，建設台灣成為優質網路化社會的典範國家，並因應未來各項通訊傳播網路匯流科技發展之趨勢，創造台灣在國際資通訊科技競爭局勢中繼續領先之優勢，本計畫在推動我國 IPv6 發展之目標下，將包含：落實 IPv6 連網環境、強化 IPv6 連網安全及探索 IPv6 連網應用，三個方向進行。

## 二、研究方法及過程

為推動國內完整之 IPv6 生態系，本計畫將具備以下三個工作項目,包括落實 IPv6 連網環境－推動商用網路雙軌普行、強化 IPv6 連網安全－雙軌連網環境安全研析，及探索 IPv6 連網應用－物聯網服務與應用研析。

**(一)** 落實 IPv6 連網環境－推動商用網路雙軌普行

根據民國 107 年「我國 IPv4/v6 雙軌普行關鍵問題調查與可行解決方案研究」調查結果，市售寬頻分享器預設開啟設定支援 IPv6 的比例不高。經過兩年的發展，本計畫將再進行市售寬頻分享器支援 IPv6 的調查，及進行設備和中華電信固網和 TBC 台灣寬頻通訊 IPv6 連通實際測試，以掌握終端用戶設備對 IPv6 支援的狀況。

針對國內 IASP 業者所經營各類服務，調查網路支援 IPv6 建置狀況，以掌握國內 IPv6 連網環境完善程度。

另外本計畫預計開發 IPv6 動態 DNS 服務軟體，方便使用者下載此軟體進行 IPv6 網站架設時使用；延續民國 108 年計畫執行成果將持續進行 ICP IPv6 升級推廣；為推升 IPv6 使用量，將進行推廣手機使用者下載簡易 APN 啟用 IPv6 之 APP，以利持續推升國內 IPv6 使用率。

除了持續推動現有網路環境支援 IPv6 之外，本計畫預計試行建置 Native IPv6 連網實驗環境，為未來推動純 IPv6 連網環境預做準備。

**(二)** 強化 IPv6 連網安全－雙軌連網環境安全研析

延續民國 108 年「推動 IPv4/IPv6 雙軌普行方案」計畫執行內容，本計畫將持續辦理〝ICP IPv4/IPv6 雙協定

網路安全防護技術人才培育〞教育訓練。透過教育訓練課程的推廣，幫助更多 ICP 業者了解 IPv4/IPv6 雙協定網路服務升級及安全防護設定等相關技術，建立其 IPv6 能力，培育技術人才，降低業者所需投入心力，增加業者升級支援 IPv4/IPv6 雙軌網路服務的意願。同時加強 ICP 業者進行網站升級 IPv6 規劃時，能對 IPv6 資訊安全問題重視，以建設國內完善且安全的 IPv6 網路環境

近年資通安全防護議題的重要性，在網際網路應用範疇相當被重視，而 IPv6 網路建置越來越普及，也逐漸吸引駭客對 IPv6 網路進行攻擊的目光，在民國 108 年「推動 IPv4/IPv6 雙軌普行方案」計畫中，進行 ICP IPv4/IPv6 平台架構雙協定網路安全防護差異解析，延續民國 108 年的計畫概念，今 (109) 年計畫將進行 IPv6 用戶資通安全防護研析，執行內容將分為 IPv6 家用及企業用戶資通安全防護技術研究，透過此兩分項工作彙整技術人員對家用網路通訊設備須關注的資訊安全設計及規範，及提升企業 IT 人員對所採用的網路通訊設備，所需加強的 IPv6 資訊安全防護技術能力有所助益。

國內 ISP 在 IPv6 網路服務建置已漸趨普及，同時 IPv6 網路安全的議題近年也越來越受到重視，本分項工作將

透過蒐集及整理 ISP 之 IPv6 網路安全防護準則，提供予 ISP 參考，以期提高 ISP 業者對此議題的重視。

**(三)** 探索 IPv6 連網應用－研析物聯網服務與應用研析

物聯網 (Internet-of-Things，IoT) 新技術發展，持續朝向萬物聯網方向推進，未來將有更多設備連上網路，因此也對 IP 位址需求持續增加。IETF 已達成未來之新標準 (RFC) 皆以 IPv6 為適用平台之共識，IPv6 已成未來技術主流暨網路根基。除了 IPv6 連網環境基礎網路推動計畫外，如何創新為下一代網路新產業鋪路，對國家未來經濟發展至關重要，為蓄積技術能量加強創新產業連結，及對新技術與應用瞭解及掌握，持續對物聯網與網際網路相關技術有更深入的了解，本計畫透過蒐集國內外物聯網服務實際應用案例，以掌握產業發展的脈動；另外，並依據 RFC 技術文件研析 IP (Internet Protocol，網際網路協定)、DN (Domain Name，網域名稱)、BGP (Border Gateway Protocol，邊界閘道器協定)、RPKI (Resource Public Key Infrastructure，資源公鑰基礎建設)、DNSSEC (Domain Name System Security Extensions，網域名稱系統安全擴充) 及 SIP (Session Initation Protocol，對話啟動協定) 等六大網際網路技術標準主題，以充分掌握相關技術重點。

## 三、重要發現

(一)全球 IPv6 使用率不斷攀升，根據 APNIC 統計，依個別國家來看，今 (109) 年就有約 25 個國家 IPv6 連網比例超過 30%。全球總體 IPv6 連網比例也呈現穩定的成長，由此觀察可得知 IPv6 部署建置已經獲得多數國家支持，網際網路向 IPv6 遷移已經是相當明確趨勢。

(二)調查發現去 (108) 年全年度市售寬頻分享器銷售前 20 名商品中有標示支援 IPv6 比例為 75%，和 106 年全年度市售寬頻分享器銷售前 20 名商品中標示支援 IPv6 比率 55%比較，顯示國內寬頻分享器品牌業者，對 IPv6 支援有逐步重視，對國內推動 IPv6 網路升級具有重大象徵性意義。

(三) 去 (108) 年針對 IASP 的調查結果來看，5 家行動電信業者都採用 CGNAT 核發 Private/Shared Address Space IPv4 位址給用戶，以因應 IPv4 不足問題，其中台灣大哥大 (部分) 、亞太電信及台灣之星 3 家業者所採用的 IP 位址共用的比例達到 1:64，增加網路犯罪偵查複雜度。今 (109) 年國內電信業者的大事就是 5G 正式發照，國內電信三雄中華電信、遠傳電信及台灣大哥大，都已經正式取

得 5G 執照，進入 5G 時代行動電信業者對 IP 的需求將再擴張，因應業務成長 IPv4 不足的問題，業者轉進 IPv6 才能解決消費端的需求。

(四)物聯網結合 5G，將引領物聯網進入蓬勃發展階段，從高畫質影音傳輸、智慧生活領域、AR/VR 軟硬技術娛樂應用、智慧交通及遠端醫療等各個應用面加速發展。未來將會有更多設備有連結網際網路的需求，IPv4 已經不足以應對未來網路世界發展，全球對 IPv6 需求將更為明顯。

(五)觀察國內固網 IASP 支援 IPv6 使用率發現，其使用比例不論是一般終端用戶或企業用戶，IPv6 的使用比例仍不高，尤其以企業用戶使用比例更低，要讓國內 IPv6 達到普及化，除推動 IASP 逐步增加各項網路服務支援 IPv6 外，持續推廣 ICP 業者及企業網路支援 IPv6 有其必要性。

(六)推動 ICP 業者及企業網路支援升級 IPv6 的基本要素，需要 IASP 所提供的各項網路服務能夠充分支援，否則 ICP 業者因網路供應者無法支援 IPv6 即阻斷升級的可能性。

持續推動國內 IASP 各項網路服務支援 IPv6，是提升 ICP 升級支援 IPv6 的基本要件之一。

(七)許多 ICP 業者或企業尚未關注到國內網路環境，已經逐步向 IPv6 遷移，而網站或企業內部網路升級支援 IPv6 需要有足夠的時間進行規劃及執行。未來要持續推升國內 IPv6 使用率，讓國內網路環境逐步向下一代網路遷移，網站或企業內部網路升級將是不可或缺的一塊。

(八)今 (109) 年下半年隨著台灣之星開始支援 IPv6 也象徵國內行動IASP已經全面進入IPv4/IPv6雙軌並行時代。

## 四、主要建議事項

觀察國際 IPv6 發展趨勢，除歐美各國相當積極外，近年亞洲區國家，包含台灣、日本、越南、馬來西亞及泰國等國家在 IPv6 連網比例也大幅成長，可見支援 IPv6 已經是國際共識，國內在今 (109) 年 IPv6 連網比例已經突破 50%，使用率持續穩定成長，以此基礎持續推動 IPv6 普及化，以提供新一代網路標準完善支援，根據計畫執行狀況所提建議如下所述：

(一) 立即可行之建議

1. 推動 IASP 各項服務支援 IPv6

根據 IASP 普查結果得知，IASP 除行動網路及固接網路連線服務外，業者還經營其他各項服務如 PWLAN、IDC/Co-Location、雲端服務等，業者提供的服務是否支援 IPv6，也和 IPv6 是否能普及息息相關，業者希望能透過政府單位提供獎勵補助措施，以加速企業投入升級 IPv6 意願。

2. 手機預設開啟支援 IPv6

今 (109) 年已經達成國內 5 家行動網路服務業者全部支援 IPv6，在此基礎上推動手機業者能開啟預設支援 IPv6，以持續推升行動網路連線 IPv6 使用率。

3. 推動寬頻分享器預設開啟支援 IPv6

影響家用戶網路 IPv6 使用率，除固網業者是否預設開啟支援 IPv6 外，消費者所採購的網通商品是否預設支援 IPv6 也至關重要，持續向國內網通商品製造業者宣導國內 IPv6 網路環境的狀況及高使用率，可加強業者支援 IPv6 的意願。

(二) 中長期性建議

1. 持續推動 ICP 網站及企業網路升級支援 IPv6

今 (109) 年推動 ICP 網站升級支援 IPv6 的工作，除持續進行教育訓練推廣外，並透過和公協會合作進行網站升級推廣計畫，可以擴大接觸到更多有架設對外網站的業者，相對提升成功的機會。企業網站和 ICP 網站升級支援 IPv6，需要長時間的佈局，持續加強對 ICP 宣導，讓業者有足夠時間因應，才能讓國內網路環境遷移到 IPv6 的過程更順暢。

2. 提早因應為未來 Native IPv6 網路環境鋪路

全球 IPv6 的使用率逐步推升，加上 IPv4 短缺的情況日益嚴重，5G 開通及物聯網應用加入網路世界，讓 IPv6 網路愈形重要，目前國內以支援 IPv4/IPv6 雙軌服務為主，當 IPv6 使用率持續推升，加上支援雙軌服務增加 IASP 營運複雜及增加人力成本，未來轉向 Native IPv6 網路環境的可能性會逐步提升。而系統轉換需要相當人力、物力及時間成本，透過早期投入小型的試驗，對未來的商業部署計畫有相當大的助益。

3. 加強 ICP 網站及企業網路升級 IPv6 對安全之重視

IPv6 和 IPv4 除位址長度的擴充外，也因應近年資訊安全等議題需求，對網路協議進行強化，除推動 ICP 網站及企業網路升級支援 IPv6 外，同時也需要加強業

者對 IPv6 網路系統資訊安全觀念更為重視，才能讓國內網路逐步遷移到順暢且安全的新一代 IPv6 網路環境。

4. 建議將 ISP 之 IPv6 網路安全項目納入電信事業資通安全規範

全球網際網路不斷快速擴張，維護網路資訊安全成為維運重要課題，計畫中針對 ISP 之 IPv6 網路安全標準文件進行研析，彙整完成網路安全基本防護要項，建議可納入電信事業資通安全規範項目，以強化 IASP 系統維運安全防護守則。

5. 持續關注 IPv6 網路安全議題

網際網路不斷擴張，因此網路技術及標準發展也將與時俱進，利用數位科技發展國家實力是全球多數國家共同目標，在資訊安全即國家安全前提下，面對網路不斷向 IPv6 遷移，勢必吸引駭客攻擊機率，為建設更安全網路環境，應持續關注 IPv6 網路安全技術標準，收集分析各種網路攻擊案例資訊及相關應對措施，才能確保網路環境安全性及可用性。

6. 持續關注 IPv6 網路創新技術

在 5G 和雲端時代， IPv6 從根本上解決了 IP 地址不足的問題。此外，未來應用如自動駕駛、工業自動化、VR (Virtual Reality )、智慧醫療和物聯網等，需要具有突破性的〝IPv6 +〞網路技術，如 SRv6、BIER6 等新協議為代表，並結合 AI 進行網路分析，智慧調整等。而 IETF 也針對未來技術需求持續進行相關標準制定，例如今 (109) 年 3 月正式發布了 SRv6 標準文件 [RFC8754] ( IPv6 Segment Routing Header )。[58]

持續關注 IPv6 網路產業技術標準，才能讓國內網路環境與時俱進，符合未來應用發展需求。

## Abstract

IP (Internet Protocol) specifies the technical format of packets and the addressing scheme for devices to communicate over a network. There are currently two version of IP: IPv4 and a new version called IPv6. IPv6 is and evolutionary upgrade to the Internet Protocol due to the exhaustion of IPv4 addresses. In fact, IPv6 is more advanced and has better features compared to IPv4. There are some differences between IPv4 and IPv6 protocol. Before IPv4 gradually fades out from the Internet, IPv6 will coexist with the older version IPv4 for a while.

IPv4 address resources are gradually exhausted, and the IPv6 communications protocol allows room for the internet to scale with simplicity. As the IPv4 runs out from RIRs, new ISPs can no longer apply IPv4 addresses. ISPs may implement IPv4 NAT (Network Address Translation) within their networks and assign private IPv4 addresses to customers as a short-term solution. As long-term consideration, deployment of IPv6 is the standards-based solution to the IPv4 address shortage. Promoting the use of IPv4/IPv6 dual-stack is an important part of the current digital infrastructure.

In the future, new services such as the Internet of Vehicles (IoV), Smart Cities, and Smart Homes will increase the demand for a large number of devices connected to the

Internet. The digital transformation of more companies has also increased the demand for network IP. The only solution for the sustained and healthy development of the Internet is to support IPv6 connection services. Promoting the IPv6 standard can also help enterprises to carry out digital transformation more smoothly.

The project will conduct research, investigation and promotion related to IPv6. It works from three aspects: the realization of the IPv6 network environment, the enhancement of IPv6 network security and the exploration of IPv6 network applications. The goals of the project come from three aspects: the network communication equipment used by end users can support IPv6, increase the number of IASPs that support IPv6 connection service, and increase the number of websites that allow user to access sites through IPv6. Promote the adoption of IPv6 to increase the percentage of websites accessed via IPv6. Ensure that IPv6 standards are adopted throughout the Internet environment.

In response to the international development trend of IPv6, the project is intent to promote the development of IPv6 and aims at three work items: constructing an IPv6 network environment, enhancing IPv6 network security, and exploring IPv6 network applications.

1. Constructing IPv6 network environment

   The following are the tasks that the project will focus on:

   This project will investigate the Top 20 products ranked by CPE sales in 2019. Based on the survey results, it will investigate and test whether the most popular CPE equipment on the market complies with the IPv6 Internet environment provided by major IASPs. The test included Chunghwa Telecom’s HiNet and TBC Cable IPv6 network connections. To ensure that end user can purchase IPv6 compliant CPE equipment from the market.

   Survey the IASP industry's support for IPv4/IPv6 dual-stack protocol to ensure that the network service providers can well support IPv6 connection for end user. In addition, the project will also develop IPv6 dynamic DNS service software. Even if the user does not apply a static IPv6 address, the user can download and use it to build a website that supports IPv6.

   In order to continue the implementation results of last year, it will continue to carry out some promotion to increase the ICP website to support IPv6. It will hold

some promotional activities to encourage mobile users to download applications that can simply modify the APN settings to enable IPv6. Hope this can make progress in improving IPv6 utilization.

Furthermore, it will continue to promote the existing network environment to support IPv6. The project is also expected to try to establish a native IPv6 network experimental environment to prepare for the promotion of the IPv6-only network environment in the future.

2. Enhancing IPv6 network security

   This project will hold some training courses on the ICP upgrade website to support IPv4/IPv6 dual-stack protocol connection network. The purpose is to help ICP quickly have an overview of the differences between IPv4 and IPv6 website architectures ,and have the ability to form an IPv6 technology development team. It is hoped that these training courses can help more ICPs websites support IPv4/IPv6 dual-stack protocol connection services, and gain knowledge on how to build a secure IPv6 network to protect their services and other related technologies. Is this way, concerns about the stability of website operations are reduced, and the willingness of ICPs to have a development plan to

support IPv4/IPv6 dual-stack network services is increased. At the same time, when ICP plans to upgrade its website to support IPv6, it must have the ability to design and develop a secure IPv6 network environment.

IPv6 user security protection will focus on two aspects of home and enterprise security protection technology. For home user components, it focuses on the security design and specifications of CPE equipment that technicians must pay attention to. For enterprise users, it hopes to collect the technical functions related to IPv6 security protection required by IT personnel when operating enterprise network communication equipment.

The deployment of IPv6 network services by domestic ISPs has gradually become popular. At the same time, IPv6 network security issues have attracted more attention. It will collect and classify IPv6 network security protection guidelines for the daily operations of ISP, and hope that they will pay more attention to these issues.

3. Exploring IPv6 network applications

   In addition to improving the network infrastructure to support IPv6 connections, the project will also collect some IoT (Internet of Things) cases to understand

application and service trends for reference by the domestic industry.

In addition, the project also tried to investigate some detailed information about Internet-related technologies based on RFC documents. It will focus on 6 topics, including IP (Internet Protocol), DN (Domain Name), BGP (Border Gateway Protocol), RPKI (Resource Public Key Infrastructure), DNSSEC (Domain Name System Security Extension, Domain Name System Security Extension) and SIP (Session Initiation Protocol, Session Initiation Protocol).

The global IPv6 usage rate continues to rise. According to APNIC's statistics, the IPv6 usage rate in about 25 countries/regions exceeds 30%. From this perspective, most countries support the deployment and construction of IPv6, and migration is gradually developing. The transition to IPv6 networks is an obvious trend.

With Taiwan Star Telecom starting to support IPv6 in August 2020, this indicates that domestic mobile operators have fully supported IPv4/IPv6 dual protocol stack network connections.

By comparing the Top 20 CPE products sold in 2017 and 2019, it is found that the proportion of CPE products that support IPv6 connections has increased from 55% to 75%. This means that more manufacturers have realized that the IPv6 Internet environment is more mature. It is a basic requirement that products support IPv6 protocol to adapt to the actual conditions.

When IASP and user equipment already support IPv6 connectivity, the next focus is to promote enterprise upgrades to support IPv4/IPv6 dual-stack protocol. This is not only because Internet application services do not support IPv6 connections, but also face the same situation in the corporate Intranet network environment. This field is very weak and more work is needed to build a better IPv6 network environment.

Taiwan's 5G spectrum bidding officially started on December 10, 2019, which is called the prime year of 5G. The three major IASPs Chunghwa, Far EasTone and Taiwan Mobile Telecom have officially obtained 5G licenses. In the 5G era, IASP will further expand its demand for IP based on business growth. Regarding the lack of IPv4, the industry can only solve consumer needs by transitioning to IPv6.

5G will lead IoT into a stage where high-quality video and audio transmission, smart life, AR/VR applications, smart

transportation and medical applications are booming. All new devices need to be connected to the Internet. IPv4 is no longer sufficient to cope with the future development of the Internet, and the global demand for IPv6 will become more obvious. Supporting IPv6 is a global trend. If you are involved in the network industry, no one will ignore it.

# 第一章 計畫執行狀況與檢討

## 第一節 計畫執行內容說明

### 壹、 背景分析

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

「數位國家·創新經濟發展方案」發展重點之一為主軸一：「數位創新基礎環境行動計畫」。本項政策目標希冀推動我國數位基磐建設發展，提昇寬頻基礎建設，其中，推動我國 IPv4/IPv6 雙軌普行使用政策，是當前數位時代基礎建設中之重要一環。

民國 108 年 11 月 RIPE 發布 IPv4 位址正式用罄的消息[4]，未來只能提供少量回收的二手 IPv4 位址給有需求的會員；其他區域的 IPv4 發放單位，所擁有的 IPv4 位址也已經進入倒數階段。雖然使用 NAT 設備讓 IPv4 的消耗生命週期得以延長，但 5G 正式進入商用及物聯網設備大量進入市場，讓 IPv4 位址短缺不再只是傳聞，而是正式成為事實，網際網路接取服務業者 (Internet Access Service Provider，IASP) 難以取得新 IPv4 位址，國際目前 IPv6 之使用率逐年增加，表示 IPv6 之國際生態系穩定成長；隨著網路應用蓬勃發展，若僅提供 IPv4 網路服務，將限制 IASP 之業務擴張的可能性。

國內在民國 106 年底 IPv6 使用者比例僅 0.38%，排名全球第 67；至民國 107 年 12 月達到約 30%，全球排名躍升至第 6 名，成長速度於當 (107) 年創下世界第一；至民國 108 年 12 月國內 IPv6 連網比例來到約 40%，雖然一年來國內 IPv6 連網比例又再向上提升，但全球

排名並未跟著推升。觀察全球發展狀況可以發現，民國 108 年部分東南亞國家如馬來西亞、越南及泰國，IPv6 連網比例已有長足進步；另外歐洲如德國、希臘、瑞士、法國及盧森堡等國家，IPv6 連網比例也大幅提升。由此可以觀察到推動 IPv6 連網服務已經成為全球發展趨勢，雖然國內經過十幾年的努力，終於在這兩年有不錯的成績，持續推動完善的 IPv6 連網環境建置，讓國內連網服務能和世界接軌，並且符合全球網路環境的發展潮流，對國內網路相關產業的未來發展扮演相當重要角色。

全球提供 IPv6 連網服務趨勢近年來轉趨明顯，如下圖所示，根據 Google 統計全球 IPv6 使用率逐年呈現穩定成長，到今 (109) 年 9 月已經達到約 33.6%。

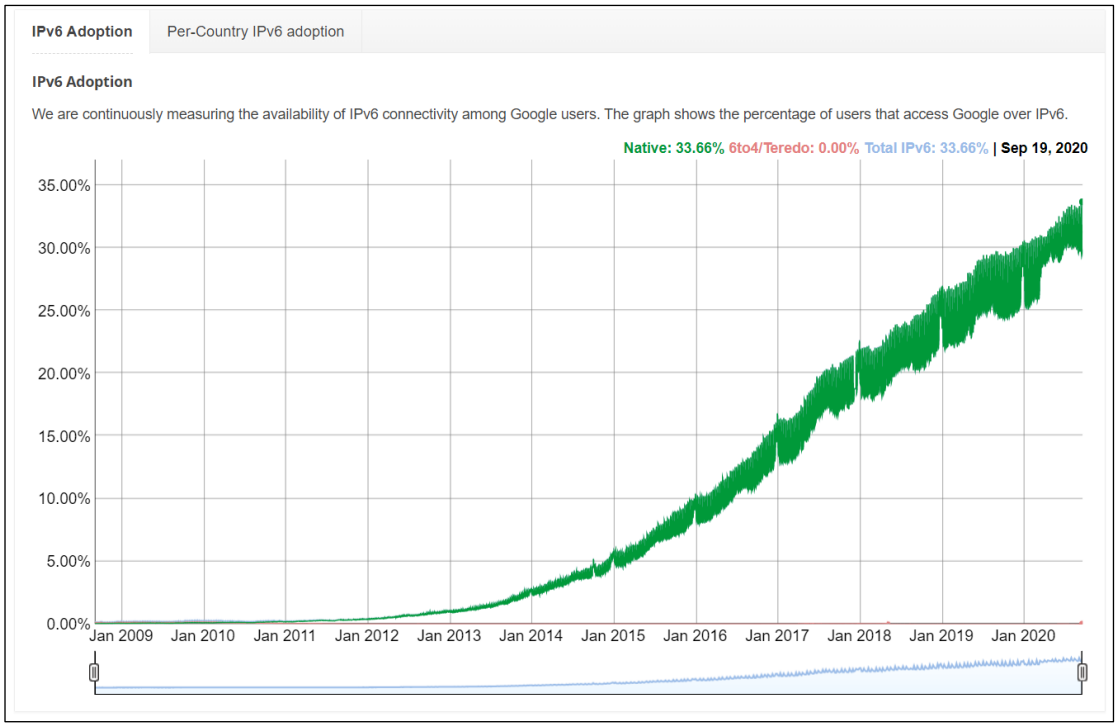



圖 1、Google 統計全球 IPv6 連網使用比例

由上圖可看出全球 IPv6 網路連線比例不斷攀升，導入 IPv6 服務有實質必要性，其原因說明如下：

## 一. IPv4位址枯竭：

全球 IPv4位址已用罄，IASP 難以取得新 IPv4位址，為維持既有服務及拓展未來新業務，導入 IPv6是必然的選擇。[4]

## 二. 解決 NAT 的問題：

導入 IPv6可減少 NAT 設備的投資，僅提供 IPv4網路服務需持續更新 NAT 等設備，反而增加 IASP 之支出。且使用 NAT 技術會有效能與維運障礙問題，增加 IASP 人力的負擔。[1]

## 三. 行動網路發展需求：

行動電信業者對 IP 位址需求大增，近年來因智慧型手機及平板電腦等行動式裝置快速增加，而行動式裝置所具備的基本特性為隨時在線 (always-on) 及上網時間長，要同時提供大量的行動式裝置上網，就必須有足量的 IP 才能提供相對應的服務，以滿足客戶的需求。[1]

## 四. 開拓物聯網 (IoT) 及5G 創新業務：

因應新產業創新服務需求，為建立友善物聯網及5G 產業創新應用服務之通訊環境，需符合物聯網裝置的特性，包含高安全性、高移動性、隨插即用、IP 隨時在線等，產業 IP 需求將隨著服務之擴張而增加。物聯網及5G 的發展勢必帶來 IP 的需求增加，若不提前布局支援 IPv6，可能失去下一代網路應用發展的先機。[1]

## 五. 內容網站透過 IPv6遞送比例逐年增加：

根據 W3Techs 統計資料如下圖2顯示，全球網際網路到今 (109) 年9月有16.9%網站可以支援 IPv6連線，且支援 IPv6連網網站呈現穩定成長趨勢，下圖3顯示今 (109) 年9月統計資料，若統計前1百萬大

網站 (網站流量排比資訊是根據 Alexa 資料為準)，已經有22.4%網站內容支援 IPv6連線；若以全球前1,000大流量網站來看，已經有31.3%網站內容可透過 IPv6遞送；且全球大型網站內容或服務業者如 Google、YouTube、Facebook、Yahoo、Wikipedia 及 Netflix 等都已經支援 IPv6，由此資料反應出支援 IPv6已經是世界潮流，為了符合我國推動數位經濟的願景，建全的 IPv6連網環境乃是數位經濟的基礎，因此佔有相當的重要性。[1~3]

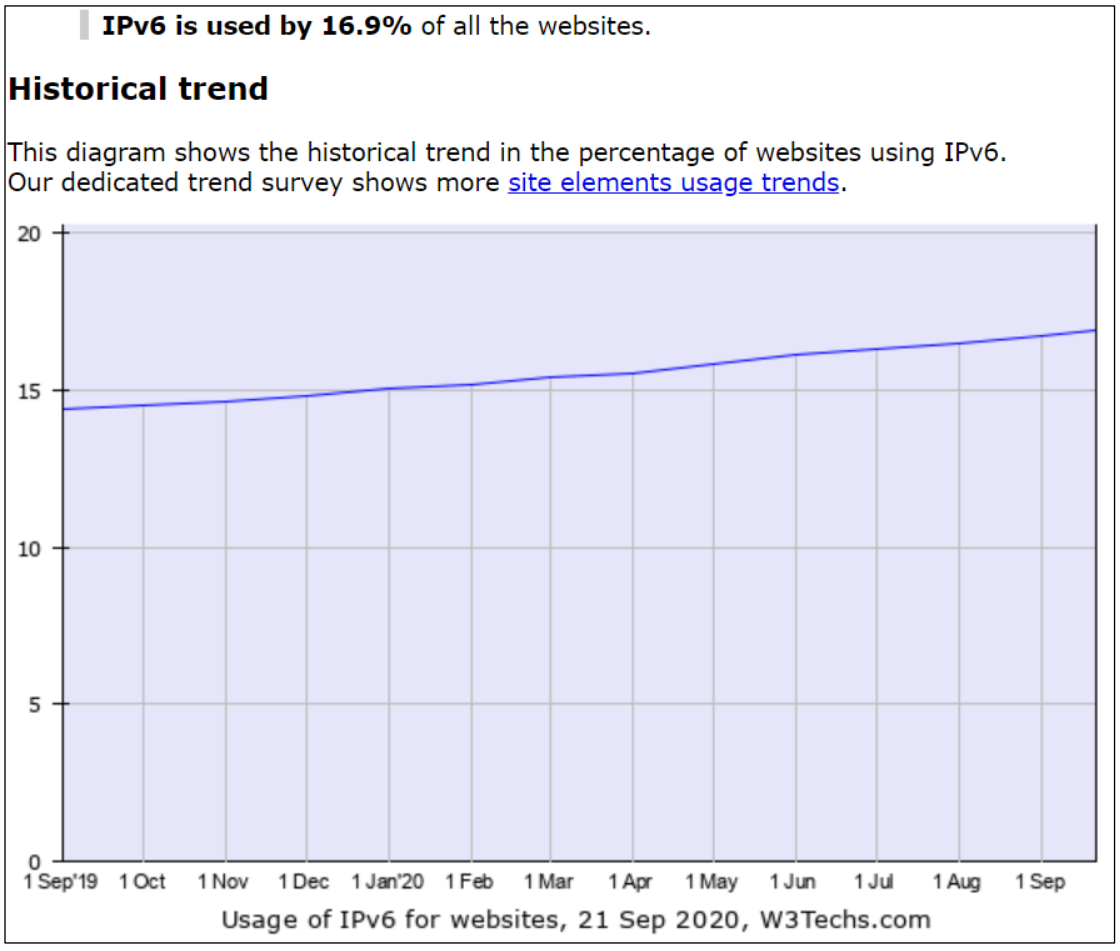



圖 2、W3Techs 統計網站支援 IPv6 趨勢

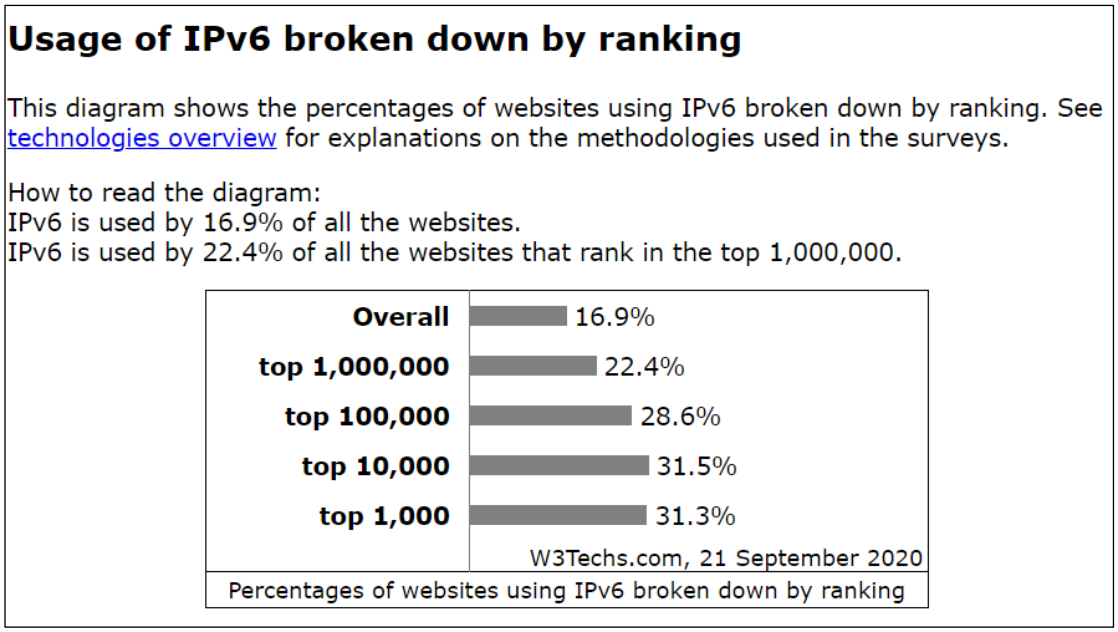



圖 3、W3Techs 統計網站支援 IPv6 比例

## 六. IETF 已達成未來之新標準 (RFC) 皆以 IPv6為適用平臺之共識，IPv6已成未來技術主流與網路的根基：[11]

西元 1990 年 (民國 79 年) 開始，IETF 開始規劃 IPv4 的下一代協定，除了要解決即將面臨 IP 短缺問題之外，還希望發展更多的擴充功能，IPv6 在西元 1998 年 (民國 87 年) 12 月由 IETF 以網路標準規範[RFC 2460]文件正式公布，未來之新標準皆以 IPv6 為適用平台，透過新一代網際網路標準，以建立未來網路可擴充之基礎，目標是取代 IPv4。

因應國際 IPv6 發展潮流，世界各國皆在推動及發展 IPv6，藉由推動及完善國內 IPv6 網路環境及使用，建設台灣成為優質網路化社會的典範國家，並因應未來各項通訊傳播網路匯流科技發展之趨勢，創造台灣在國際資通訊科技競爭局勢中繼續領先之優勢，本計畫將秉持民國 108 年度「推動 IPv4/IPv6 雙軌普行方案」之有效解決方針持續擴大

推動範圍，計畫推動方面將延續民國 108 年計畫以：落實 IPv6 連網環境、強化 IPv6 連網安全及探索 IPv6 連網應用三方面進行。

為整合推動 IPv4/IPv6 雙軌普行，本計畫將執行以下三個分項工作，包括落實 IPv6 連網環境－推動商用網路雙軌普行、強化 IPv6 連網安全－雙軌連網環境安全研析，及探索 IPv6 連網應用－物聯網服務與應用研析。

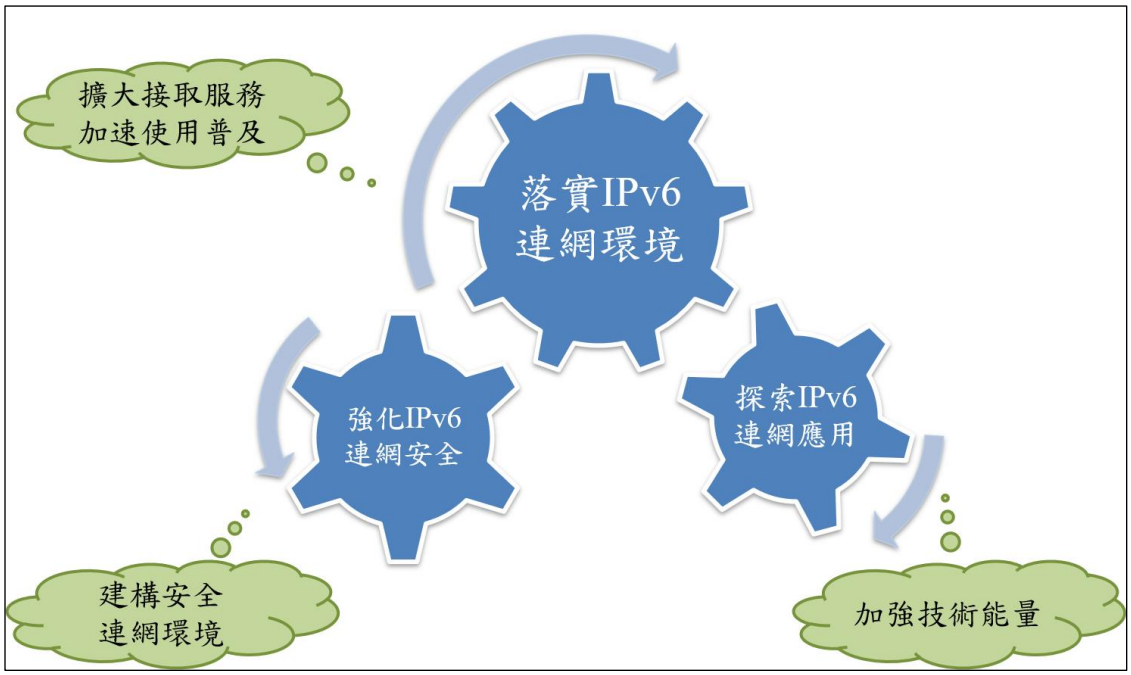



圖 4、IPv4/IPv6 雙軌普行推動方向

本計畫將推動商用網路雙軌普行，藉由普查網際網路全路徑上各連網環節 IPv6 支援情形及遭遇之困難並加以改善，以持續落實建立完善的 IPv6 連網環境；透過進行雙軌連網環境安全研析，建立安全的 IPv6 連網環境；並探索物聯網服務與應用，提升創新服務動能與加強技術能量。以確保我國數位通訊傳播基礎建設發展及國人數位資訊流通或普用與世界先進國家同步，促進國內數位經濟發展。

## 貳、 計畫動機及主題

依照以上所提本計畫進行的 3 大方向規劃，下圖為本案「前瞻及完整之 IPv6 生態系推動方案」計畫工作架構，工作項目依照 3 大方向再細分為 10 個分項工作，以下將逐一說明各項工作重點。

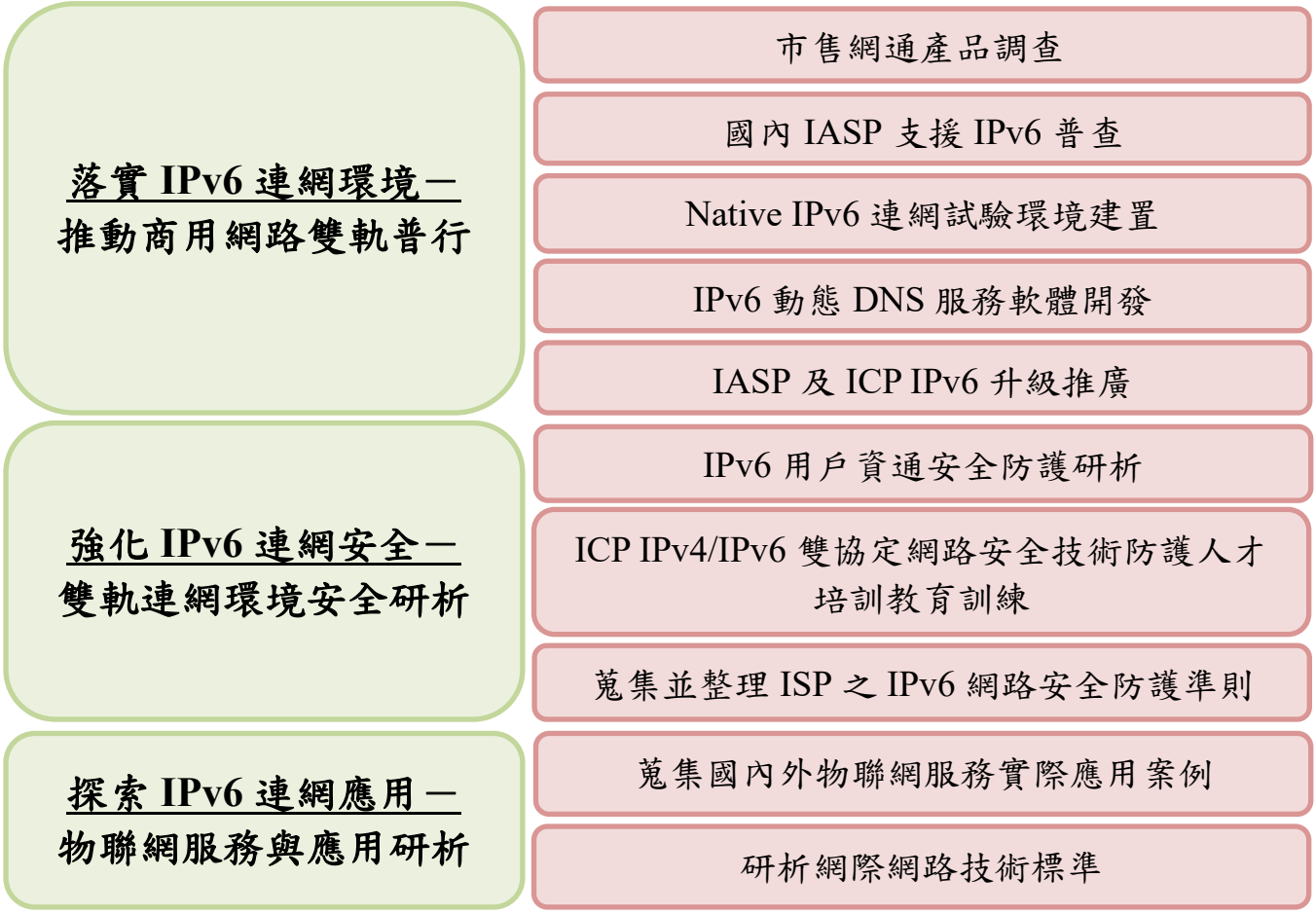



圖 5、推動 IPv4/IPv6 雙軌普行方案工作架構

## 一. 落實 IPv6 連網環境－推動商用網路雙軌普行

本分項計畫為國家通訊傳播委員會民國 107 年度「我國 IPv4/v6 雙軌普行關鍵問題調查與可行解決方案研究計畫」，及民國 108 年「推動 IPv4/IPv6 雙軌普行方案」之延續推動計畫。根據前項研究成果，

包括：

- 依據 WiFi AP、WiFi adaptor、寬頻分享器、路由器、L3 Switch、Home Gateway 等市售前 20 名網通產品市場銷售資訊及支援 IPv6 和 PPPoE 的狀況調查。銷售前 20 名的商品主要為 2 大類，第 1 類為寬頻分享器，第 2 類為 WiFi adaptor (無線網路卡)，其中只有寬頻分享器和連網環境是否設定支援 IPv6 有關。由民國 107 年度計畫調查及民國 108 年實際測試結果得知國內市售網通商品中的寬頻分享器，預設開啟支援 IPv6 的比例仍低。
- 依據民國 107 年及 108 年固網、行動 IASP 普查結果得知，IASP 除行動網路及固接網路連線服務外，業者還經營各項服務如 PWLAN、IDC/Co-Location、雲端服務等，業者提供的服務是否支援 IPv6，也和 IPv6 是否能普及息息相關，持續積極推動業者各項服務支援 IPv6，對提升國內 IPv6 使用率有相當助益。
- 依據臺灣主要網站業者支援 IPv6 情形，及業者相關規劃，了解主要網站業者支援 IPv6 之意願及所遭遇的困難。得知 IDC 提供 IPv6 網路服務的比例整備程度高，但 ICP 提供 IPv6 網路連線服務的支援程度低。

依據民國 107 年 IPv4/IPv6 雙軌普行關鍵問題之研究結果，及民國 108 年推動 IPv4/IPv6 雙軌普行方案補助計畫成果發現，IASP 開通 IPv6 服務，對 IPv6 的使用比例具有關鍵性的影響，今 (109) 年研究計畫將依民國 107 年研究結果及民國 108 年推動狀況依實際成效，針對關鍵問題持續推行解決方案。

關鍵問題解決方案之推動，將針對使用者設備、IASP 業者支援 IPv4/IPv6 之調查，以充分掌握業者的規劃進程，接續民國 108 年推

動計畫將持續推廣 IASP 及 ICP 進行 IPv6 升級，提升我國之 IPv6 使用率，朝向建立我國 IPv6 完整生態系之目標，以符合國際發展潮流。

另外本計畫將開發 IPv6 動態 DNS 服務軟體，以提供有建置網站需求的用戶使用；及建置 Native IPv6 連網試驗環境，為未來網路環境轉向純 IPv6 的連網環境預做準備。

綜合以上結論，為持續推動我國 IPv4/IPv6 雙軌普行連網服務，本分項之研究主題包括：

**(一) 市售網通產品調查：**

根據民國 107 年度「我國 IPv4/v6 雙軌普行關鍵問題調查與可行解決方案研究計畫」，針對國內市售網通產品銷售前 20 名產品對 IPv6 支援狀況調查，及民國 108 年「推動 IPv4/IPv6 雙軌普行方案」計畫，針對主要品牌業者市售寬頻分享器，和中華電信固網所支援的 PPPoEv6 及台灣寬頻通訊 TBC 所支援的 IPoEv6 進行實際測試。延續前兩年的執行成果，今 (109) 年將對市售寬頻分享器支援 IPv6 的狀況進行再次調查，並比較市售產品對 IPv6 支援狀況的變化。

**(二) 國內 IASP 支援 IPv6 普查：**

此分項工作將延續民國 108 年調查方向，針對 IASP 所經營的不同業務，依業者現有之 IPv6 位址使用情境，分為固網、行動網路、公眾無線區域網路 (Public Wireless Local Area Network，PWLAN)、網路數據中心 (Internet Data Center，IDC)、及雲端機房等類別，對業者支援 IPv6 之整備狀況，進行普查，以掌握我國 IPv6 之網路基礎環境建置現況。調查對象將包含國內 5 大行動電信業者，及固網業者新世紀資通、台灣固網共 7 家 IASP 業者。

## (三)Native IPv6 連網試驗環境建置：

在 IPv6 連網環境尚未完善之前，國內網路服務推動方向是以支援 IPv4/IPv6 雙軌並行，但同時支援 IPv4 及 IPv6 會讓網路的維護及營運更形複雜，並可能降低連網效率，未來當 IPv6 網路漸趨成熟，IPv4 即有可能淡出網際網路，而漸漸轉向純 IPv6 的連網環境，本項工作希望透過建置 Native IPv6 連網試驗環境，了解相關技術及 IPv6-only 網路環境的運作，並為未來預做準備。

## (四)IPv6 動態 DNS 服務軟體開發：

「動態 DNS 服務」就是讓使用者能將一個固定的網域名稱(Domain Name)，對應到任意的 IP 位置。其目的是讓電話撥接的使用者能有一個固定的網域名稱，供通訊、架設網站等用途使用。不具固定 IP 的主機，利用動態 DNS 服務，幫助主機可以隨著 IP 改變對應網域名稱與 IP 的關係。當用戶將目前使用 IP 送到動態 DNS 伺服器，更新伺服器的狀況，讓其他使用者可以透過網域名稱連上使用者所架設網站，而不受 IP 資訊變動的影響，對於無法擁有固定 IP 的用戶能透過此種方式達到通訊或架設網站的目的。

## (五)IASP 及 ICP IPv6 升級推廣：

民國 108 年「推動 IPv4/IPv6 雙軌普行方案」計畫，和 Cable 業者合作推動啟用 IPv6 連網服務，完成國內第一家 MSO (Multiple System Operator，多系統業者) 台灣寬頻通訊 TBC 導入 IPv6 技術，目前業者提供用戶申請試用，今 (109) 年計畫將持續和業者合作，進行推廣用戶申請試用，除推升國內 IPv6 連網比例，也透過使用者體驗累積更多經驗，預作正式商業運轉的準備，也可作為其他 Cable 業者推動 IPv6 連網服務的參考。

關於 ICP IPv6 升級推廣，民國 108 年「推動 IPv4/IPv6 雙軌普行方案」計畫，完成〝ICP IPv4/IPv6 平台架構雙協定升級輔導手冊〞，內容介紹 ICP 業者如何進行網站升級及 IPv6 資訊安全防護重點守則，今 (109) 年計畫將持續進行 ICP 網站升級推廣，預計透過和公協會合作，以期能接觸更多網站內容及電子商務經營者，推廣 ICP 進行 IPv6 升級。

## 二. 強化 IPv6 連網安全－雙軌連網環境安全研析

由民國 107 年的調查結果顯示，目前 ICP 業者對支援 IPv6 的意願不高主要的原因可歸納如下：

- 缺乏支援 IPv6 的誘因：目前 ICP 業者的 IPv4 位址充足，且投入建置支援 IPv6 並無法增加相對應的收入。
- 開發部門人力不足，且缺乏熟悉網路 IPv6 建置的技術人才。
- IPv4 和 IPv6 網路通訊協定並不相容，過渡時期必須同時支援 IPv4 及 IPv6 系統共存，對 ICP 業者而言，增加網路系統管理的複雜度，擔心網站連線不通，網頁內容無法顯示，網站回應速度變慢等，且 IPv6 資訊安全防護設定不同於 IPv4，業者擔心網站遭受攻擊，危及網站營運的穩定度。

國內 ICP 業者在支援 IPv6 上，因缺乏相關技術及人才，因此投入意願不高。為推展 ICP 業者對 IPv6 的支援，以期增加支援 IPv4/IPv6 之應用網站為目標，如果能提升業者在建置 IPv6 連網服務上的相關技術能量，縮短業者投入的時程，才能提高其投入建置支援 IPv6 的意願。因此本計畫延續民國 108 年推動方案，持續舉辦技術人才培育教育訓練課程，幫助 ICP 業者能更快速掌握 IPv4 和 IPv6 網路安全防

護平台架構的差異，及養成 IPv6 的技術團隊，幫助 ICP 業者朝向支援下一代網路服務環境前進。

綜合以上分析及描述，因此將本分項之工作內容分為以下主題，包括：

**(一)IPv6 用戶資通安全防護研析：**

民國 108 年度「推動 IPv4/IPv6 雙軌普行方案」計畫，在安全防護議題主要執行方向上，以分析 ICP 業者網站支援 IPv6 所需考慮的資訊安全相關議題。今 (109) 年在 IPv6 資通安全防護議題上，將推動家用及企業用戶資通安全防護研析，以彙整技術人員對家用網路通訊設備須關注的資訊安全規範及設計，及提升企業 IT 人員對所採用的網路通訊設備，所需加強的 IPv6 資訊安全防護技術能力有所助益，加強產業界對資訊安全防護的重視。

**(二)ICP IPv4/IPv6 雙協定網路安全技術防護人才培訓教育訓練：**

民國 108 年度「推動 IPv4/IPv6 雙軌普行方案」計畫執行過程，透過提供 ICP 業者技術人才培訓課程及技術研討的方式，目的幫助業者快速累積相關技術及人才培育，以幫助業者減少需要投入的人力，提高業者支援 IPv6 的意願。今 (109) 年計畫將會持續進行 ICP IPv4/IPv6 網路安全技術人才培訓教育訓練課程，透過教育訓練逐步推廣 IPv6 相關技術。

**(三) 蒐集並整理 ISP 之 IPv6 網路安全防護準則：**

國內 ISP 在 IPv6 的支援上已達相當的程度，目前固網已有中華電信 Hinet 及行動網路包含中華電信、遠傳電信、台灣大哥大、亞太電信及台灣之星共 5 家業者支援 IPv6；國內用戶 IPv6 連網比

例在今 (109) 年 10 月也超越 50%，已經達到相當普及的程度。而 IPv6 網路安全的議題近年也越來越受到重視，本工作項目將透過蒐集及整理 ISP 之 IPv6 網路安全防護準則，提供予 ISP 參考，以期提高 ISP 業者對此議題的重視。

## 三. 探索 IPv6 連網應用－物聯網服務及應用研析

為了解物聯網服務及應用，並對網際網路相關技術有所掌握，透過蒐集國內外物聯網服務實際應用案例，及研析六大主題式網際網路技術標準介紹，以充分掌握技術及應用發展的脈動。因此，本分項之研究主題包括：

### (一) 蒐集國內外物聯網服務實際應用案例：

全球運用物聯網技術所發展出來的應用包羅萬象，和日常生活相關的應用包含食、醫、住、行等各個面向，透過蒐集國內外物聯網服務實際應用案例，以掌握相關產業的市場脈動。

### (二) 研析網際網路技術標準：

依據 RFC 技術文件進行網際網路技術標準主題式研析，本計畫探討的技術包含 IP、DN、BGP、RPKI、DNSSEC 及 SIP 共六大主題，透過國際標準技術文件資料蒐集及研析，以充分掌握網際網路相關技術重點。

# 參、工作架構與施行方法

為達成計畫目標，本計畫架構分為三個分項，各分項包含工作內容如下所述：

- 分項一：推動商用網路雙軌普行

  此分項工作包含以下 5 個項目：

  - 市售網通產品調查。
  - 國內 IASP 支援 IPv6 普查。
  - Native IPv6 連網試驗環境建置。
  - IPv6 動態 DNS 服務軟體開發。
  - IASP 及 ICP IPv6 升級推廣。

- 分項二：雙軌連網環境安全研析

  此分項工作包含以下 3 個項目：

  - IPv6 用戶資通安全防護研析。
  - ICP IPv4/IPv6 雙協定網路安全技術防護人才培育教育訓練。
  - 蒐集並整理 ISP 之 IPv6 網路安全防護準則。

- 分項三：物聯網服務與應用研析

  此分項工作包含以下 2 個項目：

  - 蒐集國內外物聯網服務實際應用案例。
  - 研析網際網路技術標準。

以下將就計畫執行內容，依照各分項工作架構與施行方法逐一說明。

下圖為本計畫施行方法解構圖：

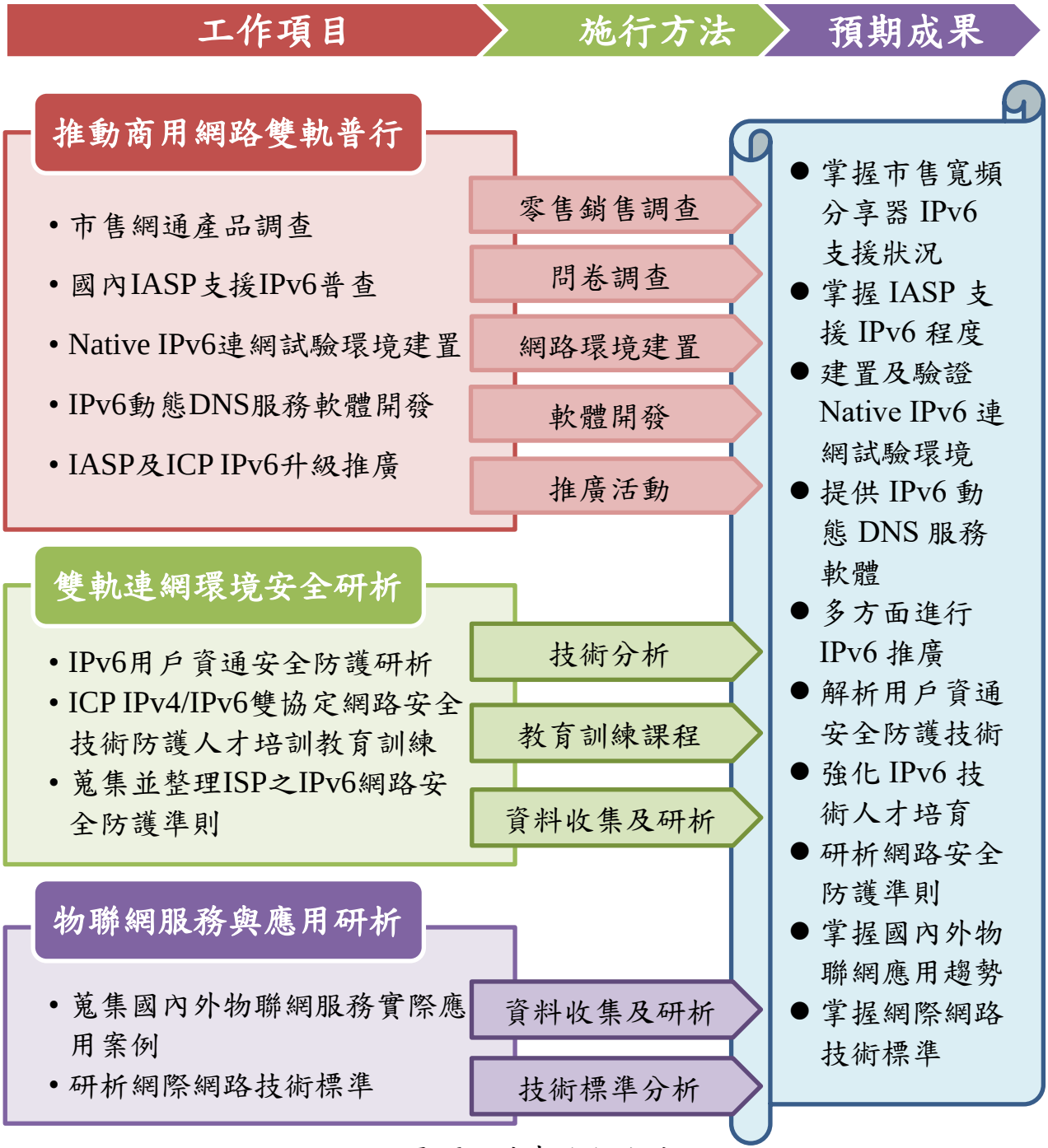



圖 6、計畫施行方法

為有效達成本計畫工作項目任務，推動商用網路雙軌普行，依照各項工作推展性質，其工作項目施行方法分為：

- 市售網通產品調查：

  根據零售銷售調查資料，分析市售寬頻分享器支援IPv6情況。

- 國內 IASP 支援 IPv6 普查：

  透過問卷調查，以了解 IASP 各項服務支援 IPv6 的狀況及計畫。

- Native IPv6 連網試驗環境建置：

  透過建置試驗性 Native IPv6 網路環境，以了解所需技術及進行實際操作。

- IPv6 動態 DNS 服務軟體開發：

  開發 IPv6 動態 DNS 服務軟體，提供有架站需求的使用者採用 IPv6 網路服務。

- IASP 及 ICP IPv6 升級推廣：

  透過推廣活動，持續推升 IPv6 使用率。

雙軌連網環境安全研析，依照各項工作推展性質，各工作項目施行方法分為：

- IPv6 用戶資通安全防護研析：

  透過技術資料收集及分析，掌握 IPv6 家用戶及企業資通安全防護相關技術。

- ICP IPv4/IPv6 雙協定網路安全技術防護人才培訓教育訓練：

  經由教育訓練課程為國內企業培育更多 IPv4/IPv6 雙協定網路安全技術防護人才。

- 蒐集並整理 ISP 之 IPv6 網路安全防護準則：

  透過蒐集及整理 ISP 在 IPv6 網路所需注意的安全防護準則，提供業者參考，以喚起業者對此議題的重視及加強國內網際網

路的連線安全。

物聯網服務與應用研析，依照各項工作推展性質，各工作項目施行方法分為：

- 蒐集國內外物聯網服務實際應用案例：

  透過蒐集國內外物聯網服務實際應用案例，了解市場趨勢及技術需求。

- 研析網際網路技術標準：

  研析網際網路國際技術標準，增加技術的掌握度。

透過以上方法，持續推動國內 IPv6 使用普及，並推動國內網路持續向 IPv6 遷移。各分項計畫執行內容說明如下：

## 一. 推動商用網路雙軌普行

本分項計畫為接續民國 107 年調查結果，及民國 108 年擴大推廣 IPv6 普及支援，持續推動更多的業者加入支援 IPv6 連網服務的行列，透過市售網通產品調查、國內 IASP 支援 IPv6 普查、Native IPv6 連網試驗環境建置、IPv6 動態 DNS 服務軟體開發、及 IASP 及 ICP IPv6 升級推廣等方面，朝向推動增加支援 IPv4/IPv6 雙軌連網服務之建置，以期能持續推升國內 IPv6 連網比例。

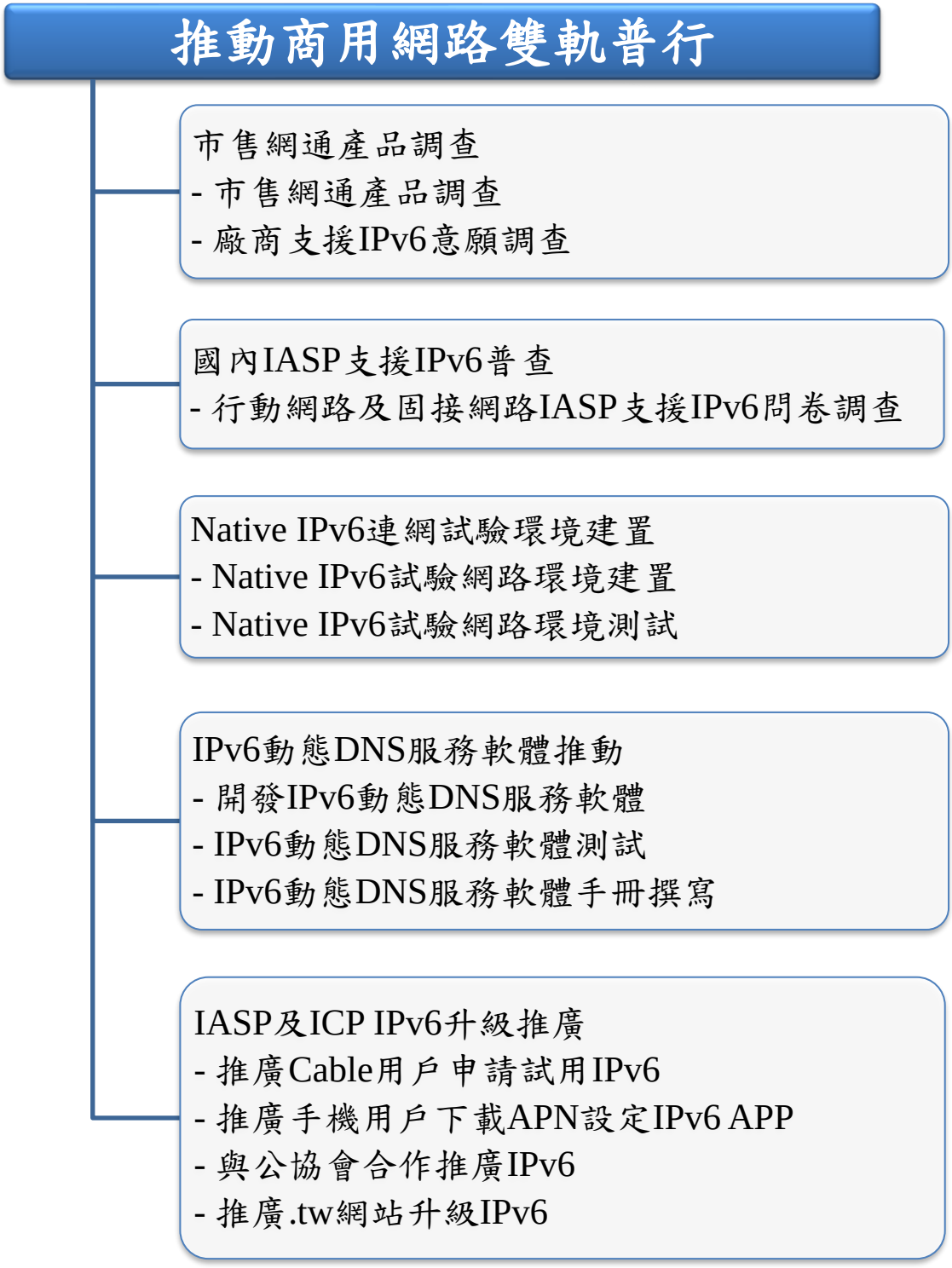



圖 7、商用網路雙軌普行推動工作項目

## (一)市售網通產品調查

本工作項目主要以零售銷量調查法來進行，零售銷量調查法是一規律且不間斷的向樣本店家收集銷售商品給消費者的銷售資料，零售銷量調查提供高度準確的市場銷售資訊，並可細至單一型號的銷售狀況。零售銷量調查流程步驟如下所述：

- 定義調查產品：

  根據民國 107 年「我國 IPv4/v6 雙軌普行關鍵問題調查與可行解決方案研究」調查結果國內市售網通商品主要以寬頻分享器為大宗，因此今 (109) 年市售網通商品調查將以寬頻分享器為主。調查產品在市場銷售期由民國 108 年 1 月 1 日到民國 108 年 12 月 31 日止。

- 定義調查通路：

  市售網通產品調查主要以零售連鎖通路為主，一般獨立店面資料收集較不完整，因此未納入此次調查範圍。零售連鎖通路包含連鎖消費性電子商品通路、連鎖綜合 IT 通路等。

- 進行資料收集：

  資料收集工作將包含依據所定義調查通路進行商店普查、進行樣本數確認、招募店家及收集銷售資訊。

- 分析資料內容：

  根據由店家所收集的銷售數字等資訊，進行資料檢核及推估等工作。

- 產出報告結果：

  依據資料分析結果產出統計報表，並根據統計資料分析彙整成調查報告。

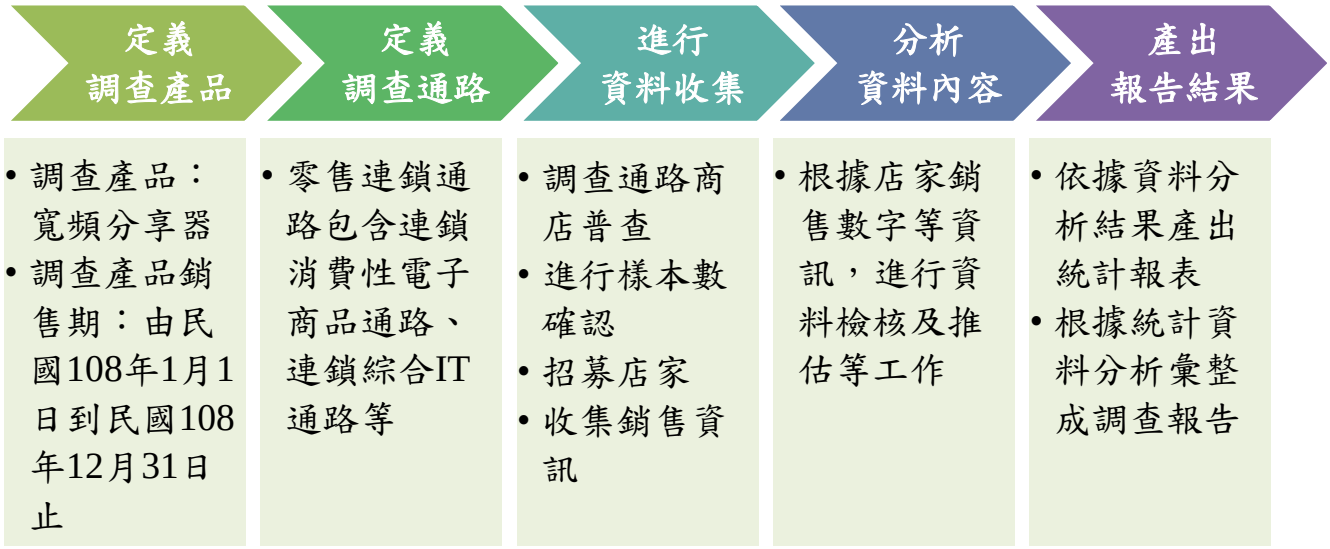



圖 8、市售網通產品調查流程

本項工作區分為，市售網通產品調查及廠商 IPv6 支援意願調查，共 2 個分項：

**1. 市售網通產品調查：**

本項工作以調查民國 108 年國內市場銷售量最高之寬頻分享器，工作內容包含以下所述：

(1) 包含銷售量前 20 名之寬頻分享器產品，並調查前述產品是否支援 IPv4/IPv6 雙軌網路服務、是否可自動偵測使用者網路系統，支援預設為 PPPoEv4/v6、或 IPoEv4/v6，並採用單一帳號密碼；前 20 名之產品中若支援 IPv4/IPv6 雙軌網路服務之產品數量少於 5 項，須增加銷售量調查之範圍至包含 5 項支援 IPv4/IPv6 雙軌網路服務之產品。

(2) 並須附銷售量調查依據、銷售數字來源資訊。

**2. 廠商支援 IPv6 意願調查：**

除市場銷售數字調查外，並將進行廠商 IPv6 支援意願調查，工作內容包含以下所述：

(1) 依上述市售網通產品調查結果，歸納產品品牌。

(2) 依上述市售網通產品調查結果所得之支援 IPv4/IPv6 雙軌網路服務之產品，與至少一家固網 IASP、與至少一家有線電視業者進行 IPv6 互通性測試，並整理測試報告。

(3) 針對上述市售寬頻分享器產品調查所得結果，訪談品牌業者就寬頻分享器產品之 IPv6 連線功能 (包含支援 PPPoEv6 及 IPoEv6) 自動啟用之意願及困難。

## (二) 國內 IASP 支援 IPv6 普查

國內 IASP 支援 IPv6 的普查工作項目，根據業者 IPv6 位址使用情境，將依固網 (如動態分配用、固定用戶種類別)、行動網路、公眾無線區域網路 (Public Wireless Local Area Network，PWLAN)、網路數據中心 (Internet Data Center，IDC)、及雲端機房等類別進行調查。

IASP 支援 IPv6 調查工作是採用問卷調查方式進行。此項工作的重點為，針對國內 5 大行動電信業者，及固網業者新世紀資通及台灣固網，調查其在 IPv6 的整備現況及預定商轉的計畫。

為有效達成本案工作項目任務，IASP 支援 IPv4/IPv6 雙軌連網服務的整備程度調查，將以問卷方式調查法進行。問卷調查法是研究團隊運用統一設計的問卷向被選取的調查對象瞭解情況或徵詢意見的調查方法。此調查的目的為詢問 IASP 業者關於各種網路服務支援 IPv6 的準備情形及時程，及該服務之設備支援 IPv6 之程度。

本工作項目所採用的問卷調查，其進行方式及流程如下圖所示。調查流程包含以下四個步驟：

- 確認調查範圍：定義調查對象及調查主題。
- 設計問卷內容：依據確認調查對象及調查主題設計問卷內容。
- 執行問卷調查：聯絡受訪對象說明調查內容及目的，並設定問卷回收時程。
- 整理問卷結果：依據問卷回覆結果及內容產出統計報表，並根據統計資料分析彙整成調查報告。

圖 9、國內 IASP 業者支援 IPv6 調查流程

## (三)Native IPv6 連網試驗環境建置

本工作項目將建置 Native IPv6 連網試驗環境，參考[RFC 6877]文件其標題為〝464XLAT：Combination of Stateful and Stateless Translation〞，此篇 RFC 主要精神是在客戶端 (Client) 和提供者端 (Provider) 分別做一次位址轉換 (Address Translation)，讓 IPv4 應用在 IPv6-only 的網路上互通。464XLAT 主要訴求在不需要開發

新的網路協定且容易部署，IASP 可以較低成本及較簡單的方式完成 IPv6-only 網路建置。[9]

464XLAT 轉換機制提供 IPv4 網路經過 IPv6 網路再到 IPv4，此技術整合 Stateful NAT64 ([RFC 6146]〝Stateful NAT64：Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers〞) ，及 Stateless NAT64 ([RFC 6145] 〝IP/ICMP Translation Algorithm〞) 技術，其中 Stateless IP/ICMP Translation 簡稱為 SIIT。

464XLAT 允許 IPv6-only 網路上的客戶端訪問 IPv4-only 網路服務，例如 Skype。客戶端使用 SIIT 轉換器將 IPv4 封包 (例如 Skype 客戶端軟體傳送資訊) 轉換為 IPv6，以 (通過 IPv6-only 的網路) 發送到 NAT64 轉換器，後者將其轉換回 IPv4 發送 (通過支援 IPv4 網路) 到支援 IPv4-only 的伺服器 (例如 Skype 伺服器)。該 SIIT 轉換器 (CLAT，Customer Side Translator) 可以是在客戶端本身執行的軟體 (Client Software)，或具有 IPv4 功能 LAN 端 (如果有 IPv4 的網路連接，就沒有必要使用 464XLAT)，和在 NAT64 轉換器 (PLAT，Provider Side Translator) 必須能夠 (通過 CLAT) 到達伺服器 (Server) 和客戶端 (Client)。NAT64 使用限制在以 UDP (User Datagram Protocol，使用者資料傳輸協定)、TCP (Transmission Control Protocol，傳輸控制協定) 和 ICMP (Internet Control Message Protocol，網際網路控制訊息協定) 連接的主從架構模式 (Client- Server Model)。[10]

- 464XLAT PLAT：

PLAT 供應端位址轉換器 (Provider Side Translator)。屬於 Stateful translator，其功能是將公有 IPv4 位址 (Global IPv4) 轉

成公有 IPv6 位址 (Global IPv6)；或將公有 IPv6 位址 (Global IPv6) 轉成公有 IPv4 位址 (Global IPv4)。

- 464XLAT CLAT：

CLAT 客戶端位址轉換器 (Customer Side Translator)。屬於 Stateless Translator，其功能是將私有 IPv4 位址 (Private IPv4) 轉成公有 IPv6 位址 (Global IPv6)；或將公有 IPv6 位址 (Global IPv6) 轉成私有 IPv4 位址 (Private IPv4)。此功能是實作在路由器端或終端設備如手機等。

因為 Stateful 在 PLAT 端轉換功能只需要少量 IPv4 位址即可運作，且 464XLAT 在固定網路和手機 3GPP 網路環境都可以進行位址轉換，讓私有網路上 IPv4 主機可以透過 IPv6 網路，和位於 IPv4 網路上的 IPv4 伺服器或主機進行連結。

以下二個圖形顯示〝464XLAT 在固網網路運作架構〞和〝464XLAT 在手機 3GPP 行動通訊網路運作架構〞[24]

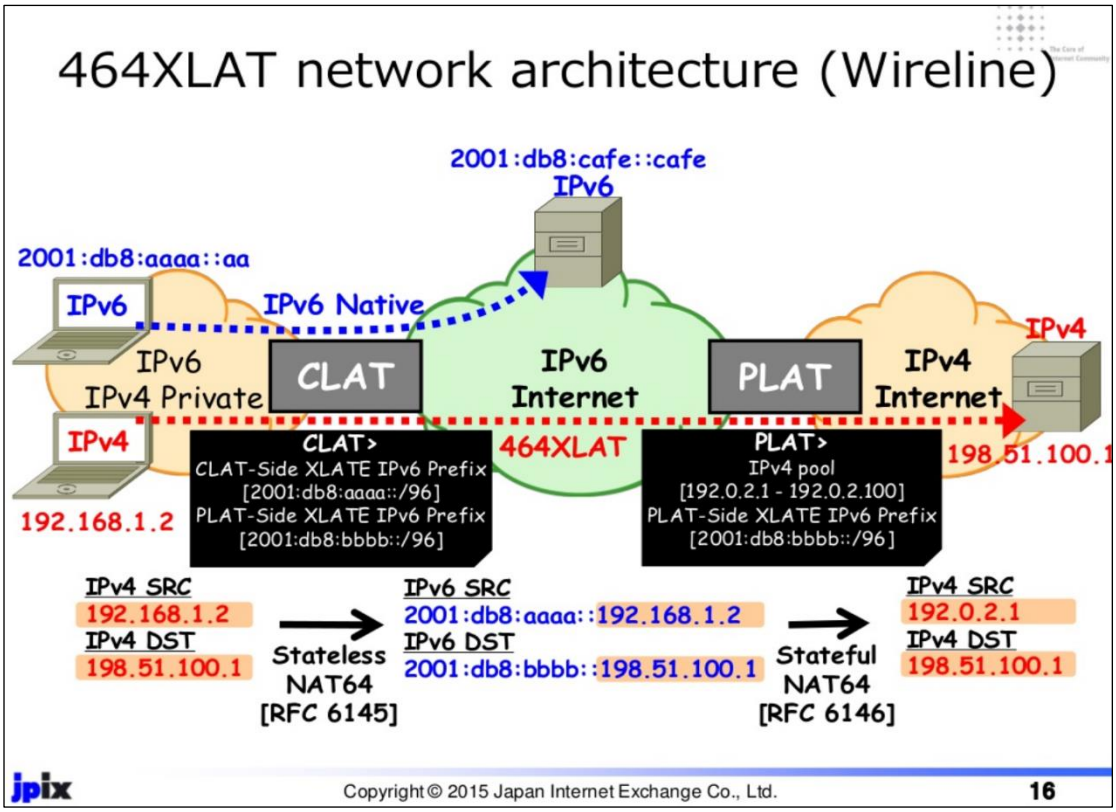



圖 10、464XLAT 在固網網路運作架構

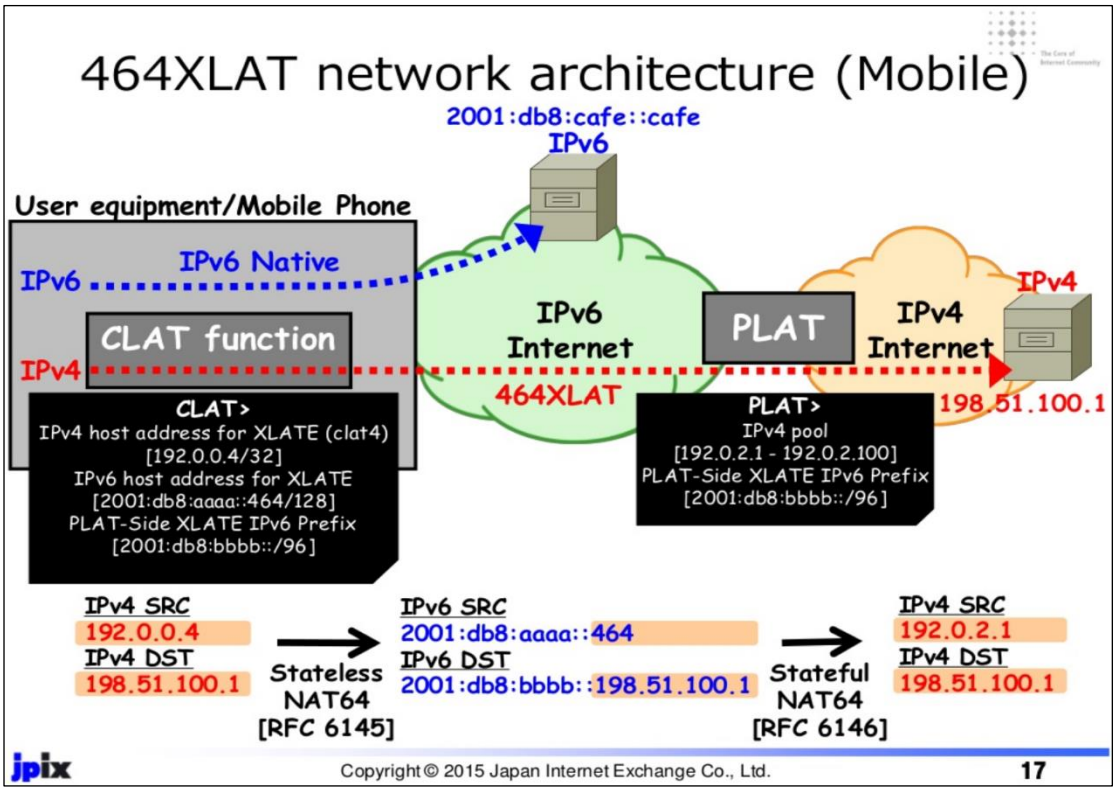



圖 11、464XLAT 在手機 3GPP 行動通訊網路運作架構

本項工作的目標為建立一個 IPv6-only 的試驗環境，並進行連網環境測試，以驗證試驗環境可以真正運作。針對 Native IPv6 網路的工作項目執行流程步驟如下所述：

- 確認需求規格：定義試驗連網環境需求包含連網功能、伺服器端需求、客戶端服務需求等。
- 定義網路架構：依據需求規格設計網路架構。
- 建置網路環境：依據網路架構進行網路環境建置，包括實驗網路環境軟硬體採購及開發。
- 驗證網路環境：經過反覆測試、修正及驗證過程以確認試驗連網環境可正常運作及符合開發規格，終端測試需考慮能支援家用及行動式終端設備。
- 完成建置報告：完成網路試驗環境建置及驗證測試報告。

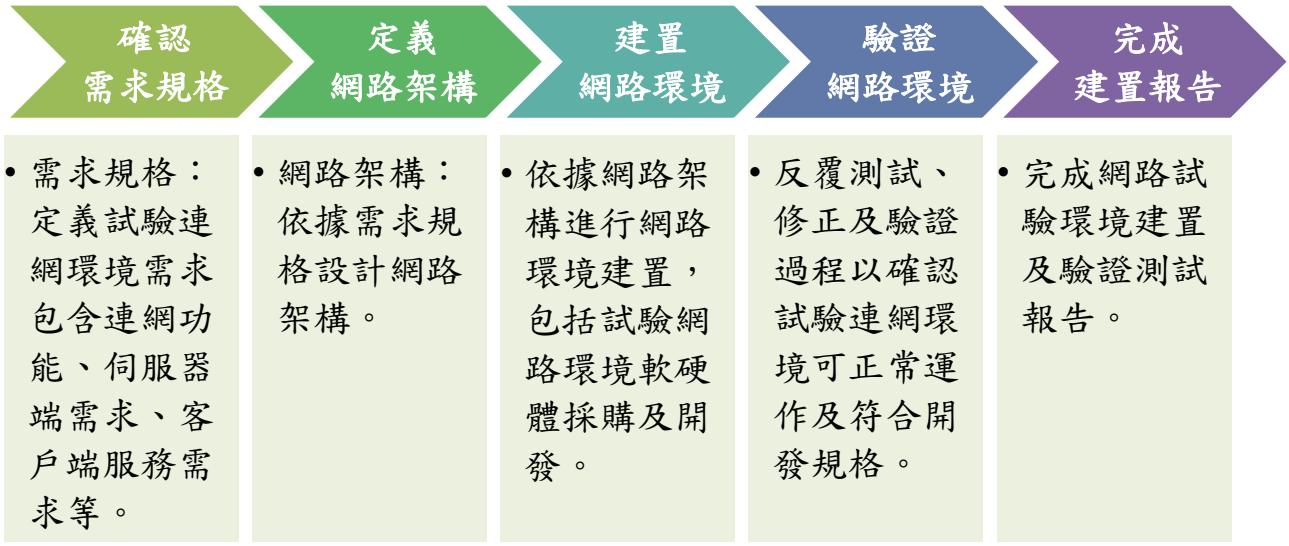



圖 12、Native IPv6 網路建置及驗證流程

針對 Native IPv6 網路建置及驗證的工作項目，執行內容說明如下：

**1. Native IPv6 試驗網路環境建置：**

建置 Native IPv6 試驗網路環境，須符合支援 464XLAT (包含 PLAT 及 CLAT) 規格。並依據實際執行結果撰寫建置報告。

**2. Native IPv6 試驗網路環境測試：**

依據上一工作分項所完成 Native IPv6 試驗網路環境，進行驗證其運作狀況。終端測試環境將包含常用家用平台 Windows 8.x 及 Windows 10.x，行動式終端設備平台 Android 10.x 及 Apple iOS 13.x。驗證的應用服務將包含 Google Search、YoueTube、Facebook、Twitter、Yahoo Search、Skype、Netflix、FTP、SFTP、Windows Outlook、Gmail 等。並依據測試結果完成測試報告。

## (四)IPv6 動態 DNS 服務軟體開發

動態 DNS 是指不具固定 IP 的主機，利用動態 DNS 服務，幫助主機可以隨著 IP 的改變去對應網域名稱與 IP 的關係，目的是為了能夠讓無法擁有固定 IP，但有通訊或架設網站需求的使用者，能有簡單容易達成的解決方案。若用戶能有一個固定的網域名稱，對應到隨時間任意變動的 IP 位址，就可讓使用者能有一個固定的網域名稱，供通訊或架設網站等用途使用。使用環境將包含 Windows (使用於用戶端/Client) 及 Linux (使用於伺服器端/Server) 系統。

本軟體開發工作項目，其進行方式及流程如下圖所示。軟體開發執行流程包含以下步驟：

- 確認服務需求：定義軟體服務需求包含服務內容、系統需求...等。
- 定義軟體架構：依據服務內容設計軟體開發架構，此服務屬於主從式架構 (Client/Server Architecture)。
- 執行軟體開發：根據軟體服務需求及架構進行實際開發工作。
- 測試軟體服務：軟體開發完成後，經過反覆測試、修正及驗證過程。
- 完成軟體開發：完成軟體開發，並提供使用者下載使用。

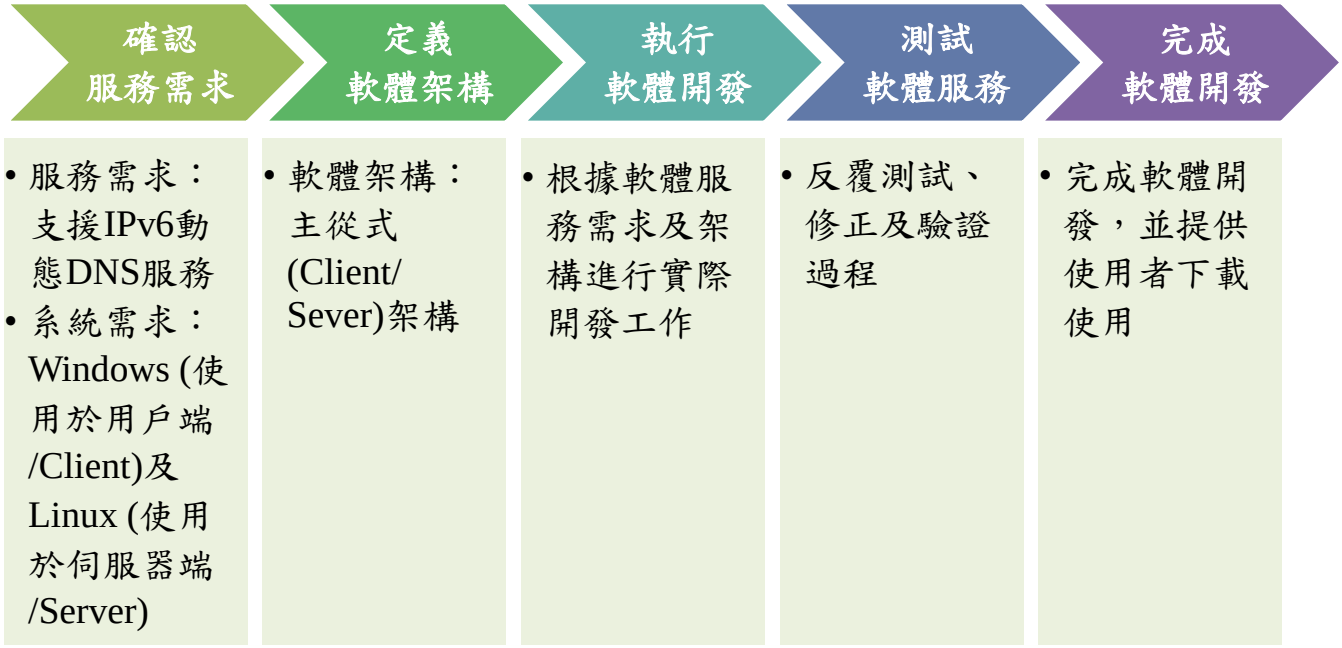



圖 13、IPv6 動態 DNS 服務軟體開發流程

針對 IPv6 動態 DNS 服務軟體開發的工作項目，執行內容說明如下：

**1. 開發 IPv6 動態 DNS 服務軟體：**

IPv6 動態 DNS 服務軟體的開發工作，包含伺服器端及用戶端軟體開發各一套。開發及測試的使用環境，伺服器端將以在 CenOS 7.5 系統平台上運作為準；用戶端將以在 Windows 10.x 系統平台上運作為準。除實際軟體開發工作外，並將撰寫伺服器端及用戶端的軟體開發報告。

**2. IPv6 動態 DNS 服務軟體測試**

針對上一分項所開發軟體進行實際測試，驗證軟體服務運作的正確性，及確認服務的可用性。

**3. IPv6 動態 DNS 服務軟體手冊撰寫：**

手冊撰寫的工作項目內容，將包含 IPv6 動態 DNS 服務軟體安裝及使用手冊等資訊。

## (五)IASP 及 ICP IPv6 升級推廣

IASP 及 ICP IPv6 升級推廣工作主要是延續民國 108 年工作推展成果，並擴大辦理推廣範圍，持續為提升國內 IPv6 網路連線比例努力。本項工作又可細分為 4 個分項工作，內容如下所列：

- IASP IPv6 升級推廣
  - ■ 推廣 Cable 用戶申請試用 IPv6：和有線電視業者合作推廣用戶申請試用 IPv6 網路服務，累積 Cable IPv6 網路服務的經驗。
  - ■ 推廣手機用戶下載 APN 設定 IPv6 APP：推廣快速啟用 APN 設定 IPv6 手機 APP 下載量，以提升手機啟用 IPv6 連網服務。

- ICP IPv6 升級推廣
  - ■ 與公協會合作推廣 IPv6：透過與公協會合作，增加接觸 ICP 業者機會，持續推廣 ICP 升級支援 IPv6。
  - ■ 推廣.tw 網站升級 IPv6：持續推廣.tw 網站升級 IPv6，推升國內網站支援 IPv6 的比例。

下圖列出 IASP 及 ICP IPv6 升級推廣的工作項目，及工作執行程序關係圖。

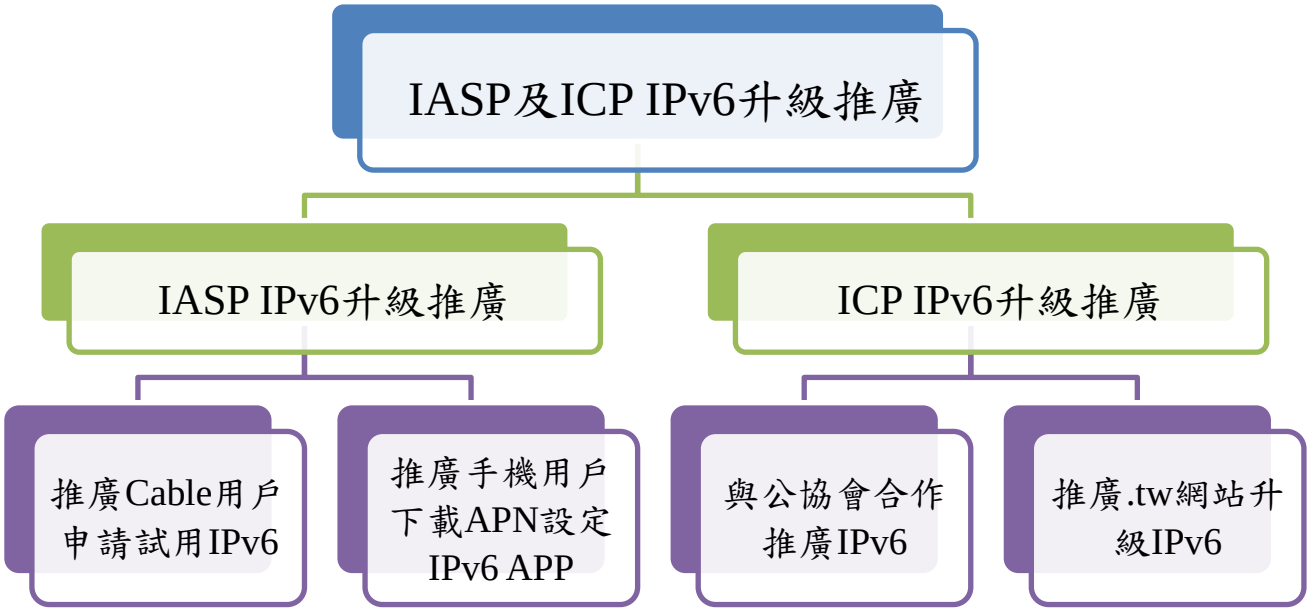



圖 14、IASP 及 ICP IPv6 升級推廣工作項目

以下就各分項工作內容，提列計畫執行方向及預計達成目標，詳細內容如下所述：

**1. 推廣 Cable 用戶申請試用 IPv6：**

民國 108 年「推動 IPv4/IPv6 雙軌普行方案」計畫，執行包含完成和 1 家 Cable 業者合作推廣用戶試用 IPv6 連網服務，終

於在民國 108 年 6 月國內首家 MSO 台灣寬頻通訊 TBC 率先推出 IPv6 連網服務試用，服務區域包含桃園、新竹、苗栗及台中，台灣寬頻通訊旗下服務的有線電視業者名單包含南桃園、北視、信和、吉元及群健。目前 TBC IPv6 服務需要使用者主動申請試用[5]，仍屬於小型試用階段，延續民國 108 年計畫執行成果，今 (109) 年將持續進行和有線電視業者合作推廣用戶申請試用 IPv6 服務，預計達成至少 1,000 個用戶申請試用 IPv6，累積更多用戶使用經驗為未來商業運轉做準備。

**2. 推廣手機用戶下載 APN 設定 IPv6 APP：**

民國 108 年「推動 IPv4/IPv6 雙軌普行方案」計畫，執行包含完成手機設定 IPv6 之 APP 開發工作，今 (109) 年將持續推動手機使用者，下載快速啟用 APN 設定 IPv6 APP，並啟用 IPv4/IPv6 雙軌服務，預計達成用戶下載啟用 IPv6 APP 量達至少 500 次。

**3. 與公協會合作推廣 IPv6：**

關於與公協會合作推廣 IPv6 升級工作，執行內容及希望達成目標說明如下所述：

(1) 與 5 家公協會合作推廣業者進行網站升級支援 IPv4/IPv6 雙軌網路服務。

(2) 合作公協會對象將以和電子商務相關如台灣網路暨電子商務產業發展協會等、電腦產業相關如中華民國資訊軟體協會、台北市電腦商業同業公會等、物聯網產業相關如亞洲矽谷物聯網產業大聯盟等，會員組成以需要架設、經營網站內容或進行電子商務之公協會為優先考量，但不在此限。

(3) 與公協會合作推廣業者網站升級支援 IPv4/IPv6 雙軌連網服務，可以參與會議、展覽及寄發相關技術或宣傳文件進行推廣，但不在此限。

**4. 推廣.tw 網站升級 IPv6：**

關於推廣.tw 網站升級 IPv6 工作，執行內容及希望達成目標說明如下所述：

(1) 推廣對象以電子商務經營者為首選，但不在此限，目標讓業者網站升級支援 IPv4/IPv6 雙軌服務，網站須以.tw 結尾域名。

(2) 網站升級支援 IPv4/IPv6 雙軌服務，須於民國 109 年 1 月 1 日前，尚未在 https://v6directory.twnic.net.tw/ 網站中登錄支援 IPv6 網路服務的業者為準，本計畫預計完成 50 家.tw 網站升級支援 IPv4/IPv6 雙軌服務。

(3) 網站升級支援 IPv4/IPv6 雙軌服務，須經過 IPv6 測試網站檢測完成，檢測網站可採用如：
https://www.gsnv6.tw/inventory/checkservicepub.cgi
或 https://ipv6-test.com/validate.php
等進行檢測並通過，才算完成網站升級 IPv6。

## 二. 雙軌連網環境安全解析

民國 108 年「推動 IPv4/IPv6 雙軌普行方案」，在網路安全防護主題，以側重在推動 ICP 網站升級 IPv6 的研析上，今 (109) 年推動方向將以 IPv6 用戶資通安全防護研析為主，持續擴大探討 IPv6 資訊安全防護技術，加強家用網通設備生產業者及企業內部網路管理人員在資訊安全防護上的技術能力，並加深企業對相關議題的重視。

依照民國 107 年調查結果顯示，ICP 對 IPv6 支援比例並不高，業者經營網站不論是內容服務或電子商務業者，其最關切的是如何衝高使用者的來訪數量，及讓使用者到訪時網站的穩定運作，業者在沒有大量擴大業務的情況下，目前 ICP 對 IP 的需求並未大量增加，對業者來說缺乏支援 IPv6 的誘因。但民國 107 年中華電信固網 Hinet 及民國 108 年中華電信 ADSL，都開始支援 IPv4/IPv6 雙軌網路服務商業運轉；另外自民國 107 年開始國內 5 家行動電信業者也陸續支援 IPv4/IPv6 雙軌網路服務；國人使用手機上網比例逐年攀升，IPv6 連網需求也逐步的成長，網路服務供應商提供 IPv6 網路服務，對 ICP 業者支援 IPv6 多了一項誘因，持續推動 ICP 業者加快支援 IPv6 網路服務，對於完善國內 IPv6 網路環境是一個相當重要的推動方向。

民國 108 年「推動 IPv4/IPv6 雙軌普行方案」， 即針對民國 107 年調查結果，推出〝ICP IPv4/IPv6 雙協定網路安全防護技術人才教育訓練〞，透過訓練課程持續推廣 IPv6 升級，並解決 ICP 業者所遭遇缺乏具有 IPv6 技術能力與管理經驗人員的問題。今 (109) 年持續進行 ICP IPv4/IPv6 人才教育訓練課程，幫助 ICP 業者縮短建置支援 IPv6 網路服務環境的技術門檻，減少業者的阻力，以期能達到增加支援 IPv4/IPv6 之應用網站的目標持續前進。

國內已有多家 ISP 已經支援 IPv6 網路服務，且國內 IPv6 的使用比例在民國 108 年底也已經超越 40%，顯示出 IPv6 網路的安全議題應該被重視，因此今 (109) 年計畫也將針對 ISP 之 IPv6 網路安全防護準則進行探討。

根據上述說明，本分項工作主要推動內容，將包含以下 3 個分項：

- IPv6 用戶資通安全防護研析
- ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓教育訓練
- 蒐集並整理 ISP 之 IPv6 網路安全防護準則

本工作項目雙軌連網環境安全研析分項工作，主要推動內容如下圖所示：

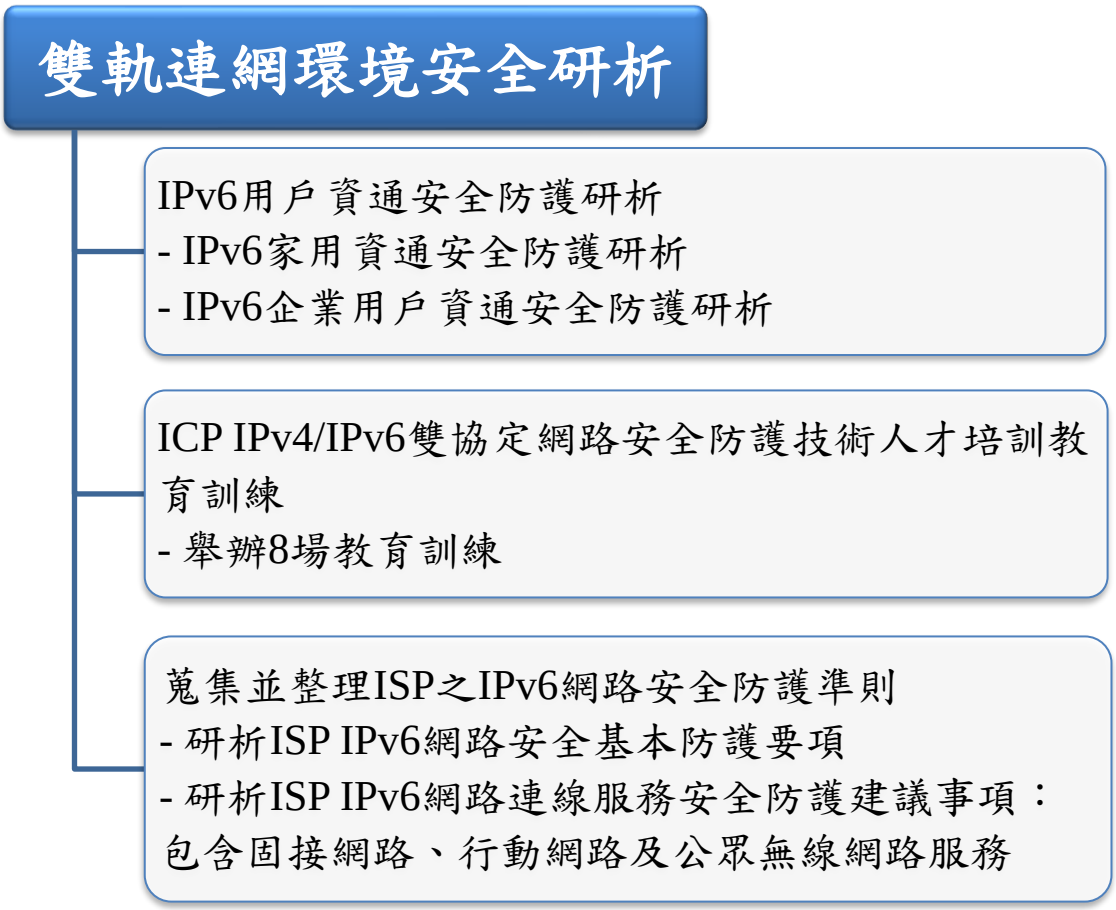



圖 15、雙軌連網環境安全研析工作項目

## (一)IPv6 用戶資通安全防護研析：

網際網路不斷蓬勃發展，不論個人或企業用戶，隨時隨地將大量的資料放上雲端或在網路上流通，這些儲存在雲端資料或網路上流通訊息，對個人或企業都是相當重要的資產，因此也吸引

駭客攻擊的可能性，本計畫將針對如何加強 IPv6 家用資通安全及企業用戶資通安全2大研究方向進行，提供家用及企業用戶參考，並提升網路使用者對資通安全議題的重視。本分項工作將分為以下 2 個工作項目進行：

1. **IPv6 家用資通安全防護研析。**
2. **IPv6 企業用戶資通安全防護研析。**

## (二)ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓教育訓練：

ICP IPv4 網站要升級支援 IPv4/IPv6 雙協定，有許多因雙協定產生的網路安全防護技術問題，民國 108 年「推動 IPv4/IPv6 雙軌普行方案」計畫，產出 IPv4 及 IPv6 平台架構雙協定網路安全防護相關資訊，以製作教學課程內容，並已經舉辦 5 場 IPv4/IPv6 雙協定網路安全防護技術教育訓練，合計 186 人次參與訓練課程，協助 ICP 培育雙協定網路安全防護技術人才。今 (109) 年將延續此項工作，持續推廣 IPv6 升級及資訊安全防護技術，加強 ICP 業者在相關技術上的熟悉度。

針對 ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓教育訓練工作項目，計畫針對 ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓課程，將提供國內網站經營業者、及其他民營業者的相關網路管理技術人員參與培訓計畫。預計於北、中、南部合計辦理 8 場教育訓練，每場至少 20 人次，合計至少 160 人次參與。

### (三) 蒐集並整理 ISP 之 IPv6 網路安全防護準則：

近幾年國內 IPv6 推廣成效相當顯著，主要的原因在於國內 ISP 的積極佈署，目前固網業者中華電信的光世代 Hinet、ADSL 服務，及行動網路業者包含中華電信、遠傳電信、台灣大哥大、亞太電信及台灣之星共 5 家 ISP 都已經支援 IPv6 網路服務，根據 APNIC 統計民國 108 年 12 月國內使用者以 IPv6 連網的比例已經超越 40%。當使用 IPv6 連網比例不斷提升，也意味著網路攻擊的可能性也相對的提高。本分項工作將蒐集並整理 ISP 之 IPv6 網路安全防護準則，提供業者參考，並強化業者對 IPv6 網路安全防護議題能有更多關注，以提供使用者更安全的下一代連網環境。本分項工作將分為以下 2 個工作項目進行：

1. **研析 ISP IPv6 網路安全基本防護要項。**
2. **研析 ISP IPv6 網路連線服務安全防護建議事項：**

內容將針對固接網路、行動網路及公眾無線網路，共 3 個類型的網路服務，提出對應的 IPv6 網路連線服務安全防護建議事項。

## 三. 物聯網服務與應用研析

網際網路 (Internet) 是由各種不同網路連接，並在其上提供包含電子郵件 (E-mail)、檔案傳輸 (FTP) 及全球資訊網 (WWW) 等多元網路服務。讓各種不同網路連接起來，並提供一致性的網路聚合體 (metanetwork) 服務，是網際網路最重要的任務，為達此目的，網際網路定義了傳輸控制通訊協定 (Transmission Control Protocol，TCP) 及網際網路通訊協定 (Internet Protocol，IP)。TCP/IP 通訊協定與各種網路技術互相獨立，透過定義 IP 架在不同網路上的介面，各種網路

不管是區域網路或是廣域網路，只要透過與 IP 的介面都可成為網際網路的子網路。因此利用 TCP/IP 的 IP 與實際網路的介面，網際網路實際連線即可提供一致性服務，使用者看到的就只有一個網路。[6~7]

物聯網是新一代通訊技術的重要組成部分，其英文名稱為〝The Internet of things〞，顧名思義〝物聯網就是物與物相連的網際網路〞，這代表兩層意思：

- 物聯網的核心和基礎仍然是網際網路，是根據網際網路基礎延伸和擴充的網路。
- 其使用者端可以延伸和擴充到任何物與物之間，進行資訊交換和通訊。

因此，物聯網的定義是通過射頻識別 (RFID)、紅外線感應器、全球定位系統、雷射掃描器等通訊傳感設備依照約定協定，讓物品與網際網路相連接，進行訊息交換和通訊，實現物品智慧化識別、定位、跟蹤、監控和管理的一種網路。[8]而物聯網的應用領域也非常的廣泛，包含基本民生食、住、行、育、樂，到醫學等，應用範圍非常廣泛。

本分項計畫的目的為透過蒐集國內外物聯網服務實際應用案例，及研析網際網路技術標準等 2 個方面，以期能更了解物聯網服務應用的市場發展趨勢，及物聯網服務應用將為網際網路帶來哪些變革及對技術的需求，並透過主題式的網際網路技術標準探討，以期對網路相關技術能有更深入的理解及掌握。下圖提列本分項工作內容：

圖 16、物聯網服務與應用研析工作項目

## (一) 蒐集國內外物聯網服務實際應用案例

本工作項目，將蒐集國內外著名物聯網實際應用案例，將包含食、醫、住、行、育、樂等方面應用研析，透過市場上實際應用案例，以了解應用面、產業的發展趨勢及市場需求。並了解產業對技術需求，發掘國內具備潛力可推展的技術方向。

## (二) 研析網際網路技術標準

網際網路的組成技術相當多元且複雜，網路標準協定相當多，本工作項目將依據 RFC 技術文件進行，內容以主題式方式進行網際網路技術標準探索，包含 IP、DN、BGP、RPKI、DNSSEC 及 SIP 共 6 大主題網際網路技術標準研析，以充分掌握網際網路相關技術重點。以下將依各主題研究方向簡要說明：

### 1. IP (Internet Protocol，網際網路協定)

網際網路協定是用於封包交換資料網路的一種協定。IP 是在 TCP/IP 協定中網路層的主要協定，任務是根據來源主機和目的

主機的位址來傳送資料。目前商用網路採行有 IPv4 及 IPv6 共 2 個版本。

**2. DN (Domain Name，網域名稱)**

網域名稱，是由一串用點分隔的字元組成，紀錄網際網路上某一台電腦或網頁名稱，用於在資料傳輸時標識電腦的識別名稱。網域名稱可以說是一個 IP 位址的代稱，目的是為了方便記憶。

**3. BGP (Border Gateway Protocol，邊界閘道器協定)**

邊界閘道器協定是網際網路上一個核心的去中心化自治路由協定。經由維護 IP 路由表來實現自治系統 (AS) 之間的可連通性，屬於向量路由協定。BGP 不使用傳統的內部閘道協定 (IGP，Interior Gateway Protocol) 的指標，而使用路徑、網路策略或規則集來決定路由。因此，更適合被稱為向量性協定，而不是路由協定。

**4. RPKI (Resource Public Key Infrastructure，網際網路號碼資源公鑰基礎設施)**

網際網路碼號資源公鑰基礎設施，目的在使網際網路路由基礎設施使用更安全的公開金鑰基礎建設 (PKI) 的框架。RPKI 提供將網際網路號碼資源資訊 (如自治系統號碼和 IP 位址) 連接到一個信任錨 (Trust anchor) 的方法。其憑證結構反映了網際網路號碼資源的分配方式，即資源最初由 IANA 分配到區域網際網路註冊管理機構 (RIR)，區域機構再將其分配給本地網際網路註冊管理機構 (LIR)，最後由本地機構將資源分配給其客戶。資源的合法持有人可以使用 RPKI 來控制網際網路路由協定的執行，以防止路由劫持和其他攻擊。尤其是 RPKI 可通

過 BGPSEC 保護邊界閘道器協定 (BGP)，以及安全鄰居發現協定 (SEND，Secure Neighbor Discovery) 作為 IPv6 的鄰居發現協定。

**5. DNSSEC (Domain Name System Security Extensions，網域名稱系統安全擴充)**

DNS 技術創立於西元 1980 年代，在當時資訊安全並不是一項重要議題，因此存在許多先天的資訊安全上的弱點。例如在 DNS 的查詢與回應中皆未加密，若有駭客在其中假造 DNS 封包，將使用者原先要連到的網址，回應錯誤的 IP 而導向駭客的機器，其中可能因為網站內容看起來一模一樣，而騙到使用者之帳號密碼。此時就需要 DNSSEC (DNS security extension standard)，DNSSEC 的優點在於可完全兼容於現行的 DNS，更額外提供三項資訊安全：

- 資料完整性 (data integrity)
- 來源可驗證性 (origin authentication of DNS data)
- 可驗證之不存在性 (authenticated denial of existence)

上述三項技術使用了雜湊函式 (Hash Function) 與公開金鑰加密 (Public-key cryptography) 之技術來完成。

**6. SIP (Session Initiation Protocol，對話啟動協定)**

對話啟動協定是一個由 IETF MMUSIC 工作群組開發的協定，作為標準被提議用於建立、修改和終止包括視訊、語音、即時通訊、線上遊戲和虛擬實境等多種多媒體元素在內的互動式用戶對話。西元 2000 年 (民國 89 年) 11 月，SIP 被正式批准成為 3GPP 通訊協定之一。SIP 與 H.323 一樣，是用於 VoIP 最主要的通訊協定之一。

## 四. 工作進度報告會議

每月底前通知委託機關計畫負責人，並依委託機關計畫負責人安排之時間、地點舉行工作進度會議。會議中應簡報目前工作進度、已完成項目、完成項目所得成果，簡報電子檔並應事先送交委託機關計畫負責人。

# 肆、預期成果

本計畫延續民國 108 年度「推動 IPv4/IPv6 雙軌普行方案」計畫推動方向，針對使用者設備、IASP 網路、應用網站、企業網路等方面之問題推行解決方案,進行市售網通產品支援 IPv6 調查、國內 IASP 業者支援 IPv4/IPv6 雙軌連網服務之整備程度調查、推動 Native IPv6 連網試驗環境建置及驗證、開發 IPv6 動態 DNS 服務軟體、持續推廣 IASP 及 ICP IPv6 升級、進行 IPv6 用戶資通安全防護研析、ICP IPv4/IPv6 雙協定網路安全技術防護人才培訓教育訓練、蒐集並整理 ISP 之 IPv6 網路安全防護準則、蒐集國內外物聯網服務實際應用案例、及研析網際網路技術標準。預期產出的主要研究成果與效益如下：

## 一. 推動商用網路雙軌普行

本計畫進行 IASP 整備程度支援 IPv6 調查，以掌握未來 IPv6 相關創新應用之服務基礎，所得成果將可作為我國推動 IPv4/IPv6 普及與建構適合新興創新應用發展所需生態體系之政策參考。

進行民國 108 年市售網通產品調查,以掌握市售寬頻分享器製造廠商所生產銷售的產品對 IPv6 支援狀況。

透過建置 Native IPv6 連網試驗環境，掌握 Native IPv6 網路環境建置技術，為未來網際網路可能向 IPv6-only 環境遷移預作準備。

開發 IPv6 動態 DNS 服務軟體，提供有架設 IPv6 網站的用戶使用，提高網站建置者採用 IPv6 的意願。

持續推廣終端用戶及 ICP 使用 IPv6,包括推廣 Cable 用戶申請啟用 IPv6 服務、推廣用戶下載手機 APP 簡易設定 APN 啟用 IPv6、與公協會合作進行企業升級 IPv6 推廣、推廣網站升級支援 IPv6 網路連

線服務等多方面同時進行。持續推升我國 IPv6 使用比率，今 (109) 年本計畫目標預計提升國內 IPv6 使用率至 50%以上 (以 APNIC 之統計數字為準) 。

## 二.雙軌連網環境安全研析

本計畫將進行家用戶資通安全防護技術研析、及企業用戶資通安全防護技術研析，持續推動用戶對網際網路資訊安全議題的關注。此外，辦理 IPv4/IPv6 升級之網路安全防護教育訓練，協助 ICP 業者培育 IPv4/IPv6 雙協定網路安全防護技術人才，幫助 ICP 業者快速培養技術能力，強化產業界 IPv6 技術能量。蒐集並整理 ISP 之 IPv6 網路安全防護準則要項，加強 ISP 對 IPv6 網路安全防護意識，強化及保障 IPv6 網路的可用性。

## 三.物聯網服務與應用研析

本計畫將研析有關物聯網服務與應用案例，以充分掌握市場應用的發展趨勢，並了解業界對技術的需求，以做為擬定未來創新產業發展方針的參考依據。此外，本分項工作將透過 6 個主題式網際網路技術標準介紹及說明，整理出各主題相關的標準文件重點，以掌握各技術標準內容。

下表依照本計畫推行的 3 大方向分類，提列計畫執行結果將產出的具體衡量之績效指標：

表 1、計畫具體衡量之績效指標

| 績效指標 | 量化指標 | 質化指標 |
|---|---|---|
| 推動商用網路雙軌普行 | | |
| **D1.研究報告** | 1. 民國 108 年市售網通產品調查報告 1 篇<br>2. IASP 業者 IPv6 升級調查報告 1 篇。<br>3. Native IPv6 連網環境建置及測試報告 1 篇。 | 1. 掌握市售寬頻分享器 IPv6 支援狀況，及了解業者所遭遇問題。<br>2. 掌握 IASP 支援 IPv6 程度及遭遇問題。<br>3. 建置及測試 Native IPv6 連網試驗環境。 |
| **其他** | 1. IPv6 動態 DNS 服務軟體 1 套。<br>2. 推廣至少 1,000 個 Cable 用戶申請啟用 IPv6 服務。<br>3. 推廣至少 500 人次簡易 APN 設定啟用 IPv6 手機 APP 下載。<br>4. 至少與 5 個公協會合作推廣 IPv6。<br>5. 推廣至少 50 個網站升級支援 IPv6 網路連線服務。 | 1. 提供 IPv6 動態 DNS 服務軟體，鼓勵架站用戶支援 IPv6 連網服務。<br>2. ~5. 從 Cable 用戶、手機用戶、及 ICP 網站業者，多方面進行 IPv6 推廣。 |
| 雙軌連網環境安全研析 | | |
| **D1.研究報告** | 1. 家用戶資通安全防護技術手冊 1 份。<br>2. 企業用戶資通安全防護技術手冊 1 份。<br>3. ISP 之 IPv6 安全防護準則報告 1 份。 | 1. 解析家用戶資通安全防護技術，加強業者重視資通安全。<br>2. 解析企業用戶資通安全防護技術，強化企業資通安全意識。<br>3. 蒐集並整理 ISP 之 IPv6 安全防護準則，提升業者對網路安全議題的重視。 |
| **其他** | 1. 舉辦 8 場 ICP IPv4/IPv6 雙協定網路安全技術防護人才培訓教育訓練，共培育至少 160 人次。 | 1. 強化 ICP IPv4/IPv6 網路安全防護技術人才培育，加強產業界技術能量。 |

| 績效指標 | 量化指標 | 質化指標 |
| --- | --- | --- |
| 物聯網服務與應用研析 | | |
| **D1.研究報告** | 1.整理物聯網服務與應用案例報告 1 篇。<br>2.整理包含 6 個網際網路主題式技術介紹及說明報告 1 篇。 | 1.掌握國內外物聯網服務與應用發展趨勢及市場需求。<br>2. 掌握網際網路相關國際技術標準內容，增強技術動能。 |

# 第二節與計畫符合情形

## 壹、目標達成狀況

依照計畫內容將工作項目分為 10 個項目，各項目下另規劃數個執行細項，部分工作細項之間存在執行順序的依存性，計畫依照原先規劃於期末應完成所有工作項目，各項工作執行進度如下表所示：

表 2、各項工作執行進度

| 工作項目 | 一月 | 二月 | 三月 | 四月 | 五月 | 六月 | 七月 | 八月 | 九月 | 十月 | 十一月 | 十二月 | 已完成進度 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **市售網通產品調查** | | | | | | | | | | | | | |
| 市售網通產品調查 | | | ■ | ■ | ■ | ■ | ■ | ■ | | | | | 100% |
| 廠商支援 IPv6 意願調查 | | | | | | | ■ | ■ | ■ | ■ | ■ | | 100% |
| **國內 IASP 支援 IPv6 普查** | | | | | | | | | | | | | |
| 國內行動網路及固接網路 IASP 支援 IPv6 問卷調查 | | | | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | | 100% |
| **Native IPv6 連網試驗環境建置** | | | | | | | | | | | | | |
| Native IPv6 試驗網路環境建置 | | | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | | 100% |
| Native IPv6 試驗網路環境測試 | | | | | | | ■ | ■ | ■ | ■ | ■ | | 100% |
| **IPv6 動態 DNS 服務軟體開發** | | | | | | | | | | | | | |
| 開發 IPv6 動態 DNS 服務軟體 | | | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | | | 100% |

| 工作項目 | 一月 | 二月 | 三月 | 四月 | 五月 | 六月 | 七月 | 八月 | 九月 | 十月 | 十一月 | 十二月 | 已完成進度 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| IPv6 動態 DNS 服務軟體測試 | | | | | | | | | | | | | 100% |
| IPv6 動態 DNS 服務軟體手冊撰寫 | | | | | | | | | | | | | 100% |
| **IASP 及 ICP IPv6 升級推廣** | | | | | | | | | | | | | |
| 推廣 Cable 用戶申請試用 IPv6 | | | | | | | | | | | | | 100% |
| 推廣手機用戶下載 APN 設定 IPv6 APP | | | | | | | | | | | | | 100% |
| 與公協會合作推廣 IPv6 | | | | | | | | | | | | | 100% |
| 推廣.tw 網站升級 IPv6 | | | | | | | | | | | | | 100% |
| **IPv6 用戶資通安全防護研析** | | | | | | | | | | | | | |
| IPv6 家用資通安全防護研析 | | | | | | | | | | | | | 100% |
| IPv6 企業用戶資通安全防護研析 | | | | | | | | | | | | | 100% |
| **ICP IPv4/IPv6 雙協定網路安全技術防護人才培訓教育訓練** | | | | | | | | | | | | | |
| ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓教育訓練 | | | | | | | | | | | | | 100% |
| **蒐集並整理 ISP 之 IPv6 網路安全防護準則** | | | | | | | | | | | | | |
| 研析 ISP IPv6 網路安全基本防護要項 | | | | | | | | | | | | | 100% |

| 工作項目 | 一月 | 二月 | 三月 | 四月 | 五月 | 六月 | 七月 | 八月 | 九月 | 十月 | 十一月 | 十二月 | 已完成進度 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 研析 ISP IPv6 網路連線服務安全防護建議事項 | | | | | | | [redacted] | | | | | | 100% |
| 蒐集國內外物聯網服務實際應用案例 | | | | | | | | | | | | | |
| 蒐集國內外物聯網服務實際應用案例 | | | [redacted] | | | | | | | | | | 100% |
| 研析網際網路技術標準 | | | | | | | | | | | | | |
| 研析網際網路技術標準 | | | [redacted] | | | | | | | | | | 100% |

## 貳、進度符合情形

依據計畫規劃目標，各項工作的查核點進度，符合原計畫申請書之規劃內容，完成本年度計畫預定應達成各項工作目標，各項工作詳細細目及工作進度，如下表所示：

表 3、各項查核進度表

| 分類 | 工作項目 | 執行進度 | | | 原因說明 |
|---|---|---|---|---|---|
| | | 超前 | 符合 | 落後 | |
| 市售網通產品調查 | 市售網通產品調查 | | ✓ | | |
| | 廠商支援 IPv6 意願調查 | | ✓ | | |
| 國內 IASP 支援 IPv6 普查 | 國內行動網路及固接網路 IASP 支援 IPv6 問卷調查 | | ✓ | | |
| Native IPv6 連網試驗環境建置 | Native IPv6 試驗網路環境建置 | | ✓ | | |
| | Native IPv6 試驗網路環境測試 | | ✓ | | |
| IPv6 動態 DNS 服務軟體開發 | 開發 IPv6 動態 DNS 服務軟體 | | ✓ | | |
| | IPv6 動態 DNS 服務軟體測試 | | ✓ | | |
| | IPv6 動態 DNS 服務軟體手冊撰寫 | | ✓ | | |
| IASP 及 ICP IPv6 升級推廣 | 推廣 Cable 用戶申請試用 IPv6 | | ✓ | | |
| | 推廣手機用戶下載 APN 設定 IPv6 APP | | ✓ | | |
| | 與公協會合作推廣 IPv6 | | ✓ | | |
| | 推廣網站升級 IPv6 | | ✓ | | |
| IPv6 用戶資通安全防護研析 | IPv6 家用資通安全防護研析 | | ✓ | | |
| | IPv6 企業用戶資通安全防護研析 | | ✓ | | |
| ICP IPv4/IPv6 雙協定網路安全技術防護人才培訓教育訓練 | ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓教育訓練 | | ✓ | | |
| 蒐集並整理 ISP 之 IPv6 網路安全防護準則 | 研析 ISP IPv6 網路安全基本防護要項 | | ✓ | | |
| | 研析 ISP IPv6 網路連線服務安全防護建議事項 | | ✓ | | |
| 蒐集國內外物聯網服務實際應用案例 | 蒐集國內外物聯網服務實際應用案例 | | ✓ | | |
| 研析網際網路技術標準 | 研析網際網路技術標準 | | ✓ | | |

本次計畫執行共有 10 個主要分項，各分項下又分成數個工作子項目，各分項工作內容如上表所列，計畫工作於期末須完成的工作皆已如期完成，期末報告各項工作量化指標如下表所列：

表 4、期末報告量化指標

| 編號 | 計畫工作項目 | 預期期末報告產出 | 實際期末報告產出 |
|---|---|---|---|
| 1 | 市售網通產品調查 | 完成民國 108 年市售網通產品調查報告 1 篇。 | 報告內容包含：<br>●市售網通產品調查。<br>●網通產品連通測試。<br>●網通產品廠商訪談。 |
| 2 | 國內 IASP 支援 IPv6 普查 | 完成 7 家 IASP 業者支援 IPv6 問卷調查報告 1 篇。 | 完成 7 家 IASP 業者支援 IPv6 問卷調查及統計報告。 |
| 3 | Native IPv6 連網試驗環境建置 | 完成 Native IPv6 連網試驗環境建置及測試報告 1 篇。 | 完成 Native IPv6 連網試驗環境建置及測試報告 1 篇。 |
| 4 | IPv6 動態 DNS 服務軟體開發 | 完成 IPv6 動態 DNS 服務架構開發 1 套。 | 完成 IPv6 動態 DNS 服務架構開發 1 套。 |
| 5 | IASP 及 ICP IPv6 升級推廣 | 1. 推廣至少 1000 個 Cable 用戶申請啟用 IPv6 服務。<br>2. 推廣至少 500 人次簡易 APN 設定啟用 IPv6 手機 APP 下載。<br>3. 至少與 5 個公協會合作推廣 IPv6。<br>4. 推廣至少 50 個網站升級支援 IPv6 網路連線服務。 | ●109 年 10 月底共 3,563 個 Cable 用戶啟用 IPv6。<br>●109 年 10 月底共 624 人次下載手機 APP。<br>●完成與 10 個公協會合作推廣 IPv6。<br>●完成推廣 50 個網站升級支援 IPv6 網路連線。 |
| 6 | IPv6 用戶資通安全防護研析 | 完成家用及企業用戶資通安全防護研究技術手冊各 1 份。 | 完成家用及企業用戶資通安全防護研究技術手冊各 1 份。 |
| 7 | ICP IPv4/IPv6 雙協定網路安全技術防護人才培訓教育訓 | 舉辦至少 8 場 ICP IPv4/IPv6 雙協定網路安全技術防護人才培 | 完成 8 場教育訓練。現場 191 及遠端 82 人次參與，合計共 273 人 |

| 編號 | 計畫工作項目 | 預期期末報告產出 | 實際期末報告產出 |
| --- | --- | --- | --- |
| | 練 | 訓教育訓練。每場至少 20 人，至少共 160 人參與。 | 次參與。 |
| **8** | 蒐集並整理 ISP 之 IPv6 網路安全防護準則 | ISP 之 IPv6 網路安全基本防護要項報告 1 份。 | ISP 之 IPv6 網路安全基本防護要項報告 1 份。 |
| **9** | 蒐集國內外物聯網服務實際應用案例 | 完成包含 6 個物聯網服務與應用案例報告 1 篇。 | 完成包含：<br>●LincGo(醫的物聯網)。<br>●雲端智慧綠能(住的物聯網)。<br>●全程冷鏈(食的物聯網)。<br>●中華電信智慧停車場(行的物聯網)。<br>●工業 4.0 模擬研發實驗室(育的物聯網)。<br>●智慧導覽與實境遊戲平台(樂的物聯網)。<br>合計 6 個物聯網服務與應用案例報告 1 篇。 |
| **10** | 研析網際網路技術標準 | 完成包含 6 個主題技術介紹及說明報告 1 篇。 | 完成包含：<br>●IP (Internet Protocol)。<br>●DN (Domain Name)。<br>●BGP (Border Gateway Protocol)。<br>●RPKI (Resource Public Key Infrastructure)。<br>●DNSSEC (DNS Security Extensiobs)。<br>●SIP (Session Initiation Protocol)。<br>共 6 個主題技術介紹及說明報告 1 篇。 |

# 第三節 資源運用檢討

## 壹、人力運用情形

本研究計畫共投入總執行人力 5 人，包含專職人員 1 人，及兼職人員 4 人，與原計畫申請書之規劃相符，各人力擔任之工作如下表所示：

表 5、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 | 顧靜恆 | 組長 | 博士 | 計畫主持人，整體計畫控管與執行督導。 |
| 協同研究人員 | 蔡更達 | 工程師 | 學士 | 負責商用雙軌普行推動，問題研析及解決方案建議。 |
| 協同研究人員 | 王彥傑 | 工程師 | 碩士 | 負責雙軌連網環境安全研析，問題研析及解決方案建議。 |
| 協同研究人員 | 陳玟羽 | 管理師 | 碩士 | 負責物聯網服務與應用研析，問題研析及解決方案建議。 |
| 專任研究人員 | 許淑芳 | 工程師 | 碩士 | 負責資料研析，資料整合建議及計畫報告撰寫。 |

## 貳、經費運用情形

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

表 6、合計總經費運用情形統計表

| 項　目 | 預算金額 | 使用金額 | 使用率 | 備　註 |
|---|---|---|---|---|
| 人事費用 | $1,309,527 | $1,309,527 | 100% | |
| 業務費 | $4,573,499 | $4,573,499 | 100% | |
| 差旅費 | $30,000 | $30,000 | 100% | |
| 行政管理費 | $373,641 | $373,6410 | 100% | |
| 營業稅 | $314,333 | $314,333 | 100% | |
| **合計** | $6,601,000 | $6,601,000 | 100% | |

# 第二章 市售網通產品調查

網際網路經過30年的蓬勃發展，已經和民眾的生活產生密不可分的關係，進入5G時代，將有更多設備及裝置連結上網際網路之需求產生，IPv4位址不足問題將形成一大阻礙，推動下一代網際網路協定IPv6已經是不可擋的趨勢。隨著國內4G行動通信業者全面支援IPv6，用戶端除了手機需預設開啟支援IPv6外，當使用者進到室內環境很可能切換到以無線寬頻分享器連結上網，因此市售無線寬頻分享器是否支援IPv6，對整體使用情境也扮演者至關重要的角色。

本項工作藉由市售網通產品調查，以了解國內無線寬頻分享器全市場輪廓與規模；再藉由訪談及使用者情境測試等方法，以了解市售產品支援 IPv6 的現況。各分項工作成果如下所述。

## 第一節　市售網通產品調查

市售網通產品調查的銷售數字，根據民國 106 年的調查結果顯示，國內家用網通商品以無線寬頻分享器為大宗，其他商品銷售量佔比相對為少量，因此今 (109) 年主要以調查寬頻分享器 (WiFi Router) 在民國 108 年全年銷售量為目標，以下就市售寬頻分享器調查結果，彙整如下。

此次市售寬頻分享器產品調查，涵蓋連鎖綜合 IT 通路、連鎖量販店、連鎖消費性電子商品店及虛擬通路等 4 大銷售通路，各通路主要調查店家包含：

- 連鎖綜合 IT 通路：良興、德誼數位、三井 3C 及順發 3C 共 4 大品牌連鎖綜合 IT 通路實體銷售商店。

- 連鎖量販店：家樂福、愛買及大潤發共 3 大品牌連鎖量販實體銷售商店。
- 連鎖消費性電子商品店：全國電子、燦坤 3C、大同 3C 及集雅社共 4 大品牌連鎖消費性電子商品實體銷售商店。
- 虛擬通路：Tree Mall、大買家、YAHOO、東森購物 (ETMALL)、PCHOME、PAYEASY、MOMO、iBon Mart、U-LIFE (森森購物 U-Mall) 及 FriDay 等，共 10 大網路商店。但不包含拍賣與商店街。

圖 17、市售寬頻分享器調查通路

其中銷售店家數以連鎖消費性電子商品通路為大宗，佔總體調查店家數超過 70%，各通路調查店家數如下表所示。根據本次市售網通商品調查委託由專業市場調查公司 GFK 進行，依照 GFK 過往一般消費性電子商品市場銷售狀況的調查經驗 (如電腦及其周邊商品)，預估本次調查所涵蓋通路約佔整體家用零售市場總體銷售量約 80%。

下圖為本次市售寬頻分享器調查所涵蓋的各大品牌零售店家數量分布：

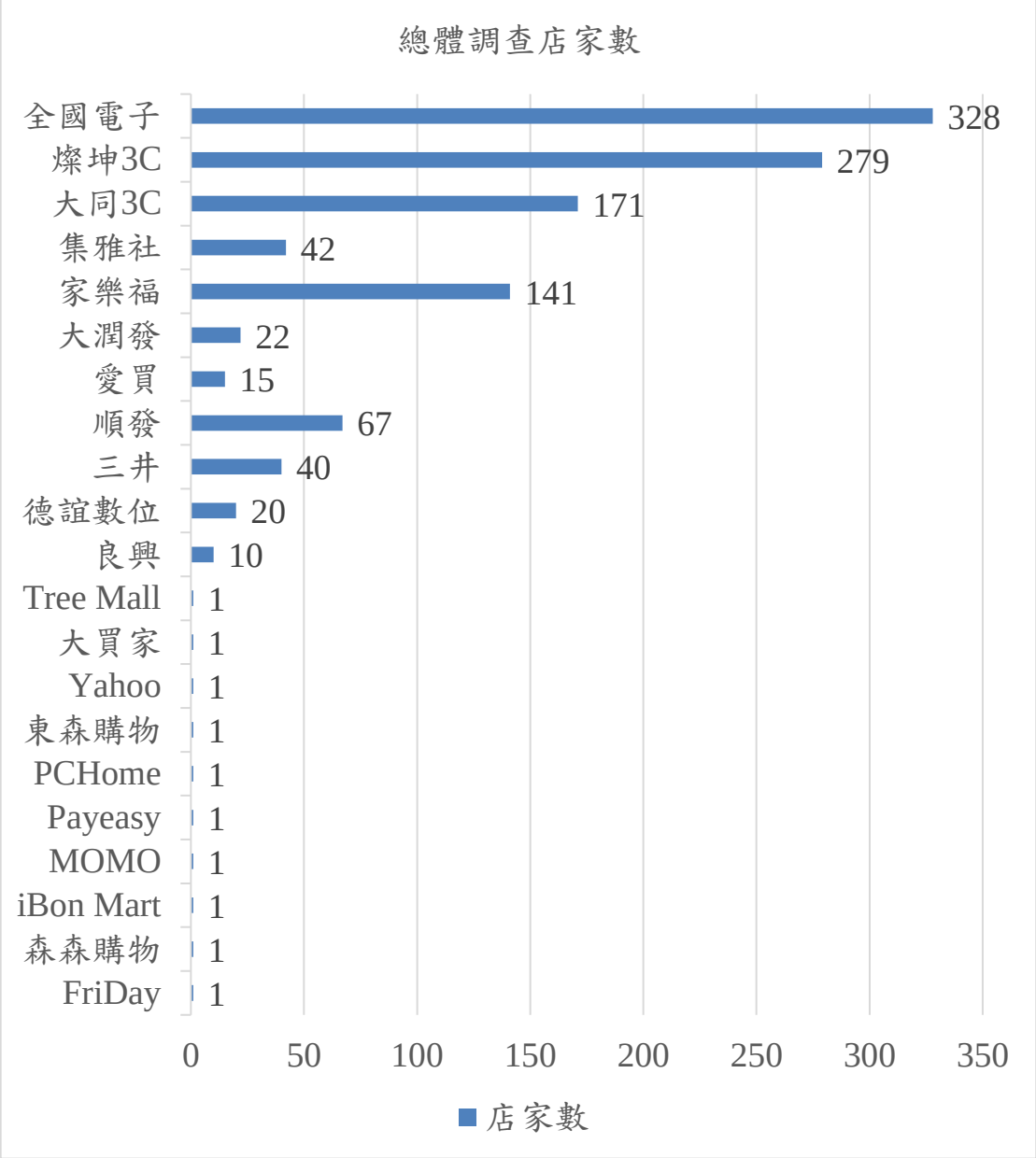



圖 18、市售產品調查零售店家數量分布

下表為本次市售寬頻分享器調查所涵蓋店家總數為 1,145 家，統計其分布於連鎖綜合 IT 通路、連鎖量販店、連鎖消費性電子商品通路及虛擬通路等 4 大通路的零售店家數量分布狀況：

表 7、調查通路銷售店家數

| 編號 | 通路類別 | 店家數 | 店家數佔比 |
|---|---|---|---|
| **1** | 連鎖綜合 IT 通路 | 137 | 12.0% |
| **2** | 連鎖量販店 | 178 | 15.5% |
| **3** | 連鎖消費性電子商品通路 | 820 | 71.6% |
| **4** | 虛擬通路 | 10 | 0.9% |
| **總計** | | **1,145** | **100%** |

此次調查不包含來自於通訊通路 (系統業者)、獨立電子商品店家、獨立通訊行、獨立家電行、網路拍賣網站及網路電子商城之銷售數據。

整體而言，民國 108 年全年寬頻分享器市場銷售規模約為 39.4 萬台，相較於民國 106 年約 45.6 萬台，銷售量減少超過 6 萬台，銷售比例下降約 13.7%。

另外依據銷售量來看通路結構分布狀況，民國 108 年連鎖消費性電子商品通路銷售量佔全通路約 34.5%，相較於民國 106 佔 40.1%下降 5.6%，其次為連鎖綜合 IT 通路佔 20.4%，相較民國 106 年下降 8.5%最多。虛擬通路民國 108 年銷售量佔 38.3%，相較於民國 106 年 26.1%提升最多，整體通路結構中實體通路約 61.7%，相較於民國 106 年 73.9%下降 12.2%，顯見網通商品逐漸普及化，亦或虛擬通路銷售藉由價格優勢及其他優惠轉變消費購買行為。網路原生世代逐漸進入消費市場，引領消費行為的移轉，也可能是改變銷售通路興衰的原因之一。

下表為民國 106 年及 108 年國內寬頻分享器各通路全年銷售數字及銷售比例的比較表：

表 8、民國 106 年及 108 年國內寬頻分享器銷售量比較表

| 通路類別 | 民國 106 年 | | 民國 108 年 | |
|---|---|---|---|---|
| | 銷售量 | 佔比 | 銷售量 | 佔比 |
| 連鎖綜合 IT 通路 | 132,015 | 28.9% | 80,250 | 20.4% |
| 連鎖量販店 | 22,556 | 4.9% | 26,574 | 6.8% |
| 連鎖消費性電子商品通路 | 182,848 | 40.1% | 135,984 | 34.5% |
| 虛擬通路 | 118,968 | 26.1% | 150,838 | 38.3% |
| **總計** | **456,387** | **100%** | **393,646** | **100%** |

以下統計圖顯示民國 106 年及 108 年寬頻分享器銷售通路結構變化：

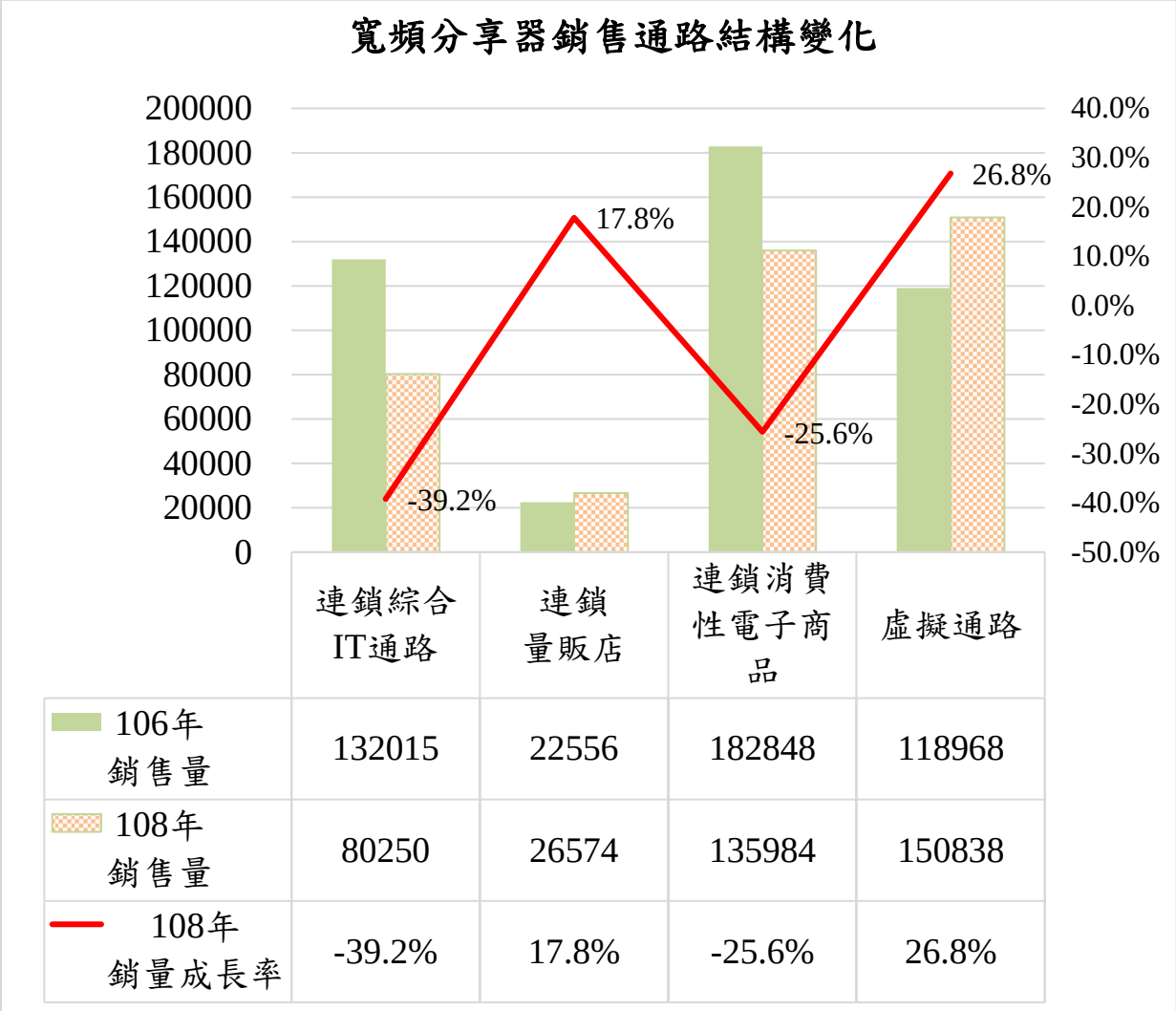



圖 19、民國 106 年及 108 年寬頻分享器銷售通路結構變化圖

下圖列出民國 108 年寬頻分享器前 20 名的銷售量及佔比，前 20 名約佔整體寬頻分享器全年銷售量的 48.5%，與民國 106 年相比銷售比例差異不大。而 D-Link (友訊) 入榜商品數則由 7 個型號降為 4 個，主要型號 DIR-809 也由民國 106 年市佔 4.2%降為民國 108 年市佔 2.5%，ASUS (華碩) 增加 4 項商品，但也有 2 型號產品落入榜外，進榜新型號商品為 RT-AC66U+、RT-AC53、RT-AC1300UHP 及 RT-AC1200G+ (各佔民國 108 年總體銷售量 1.9%、1.5%、1.4%及 1.4%)。其中值得注意的是，TP-Link (普聯) 新進榜型號商品 TL-WR840N (前一代為 TL-841N) 與 ASUS (華碩) 產品 RT-N12+ B1 目前 2 型號產品市佔比例都為 4.6%產品銷售量不相上下，皆為市場上最熱銷商品。但若以售價而言，可以發現 TP-Link (普聯) TL-WR840N 售價約為 ASUS (華碩) RT-N12+ B1 市售價格一半，可見 2 家公司在商品策略有所不同；TP-Link (普聯) 型號 Archer C7 目前市佔 3.9%，與同級售價 ASUS (華碩) 產品 RT-AC1200 相比，後者維持民國 106 年市佔 2.9%稍嫌落後，顯見 TP-LINK (普聯) 在寬頻分享器市場中具有潛力。

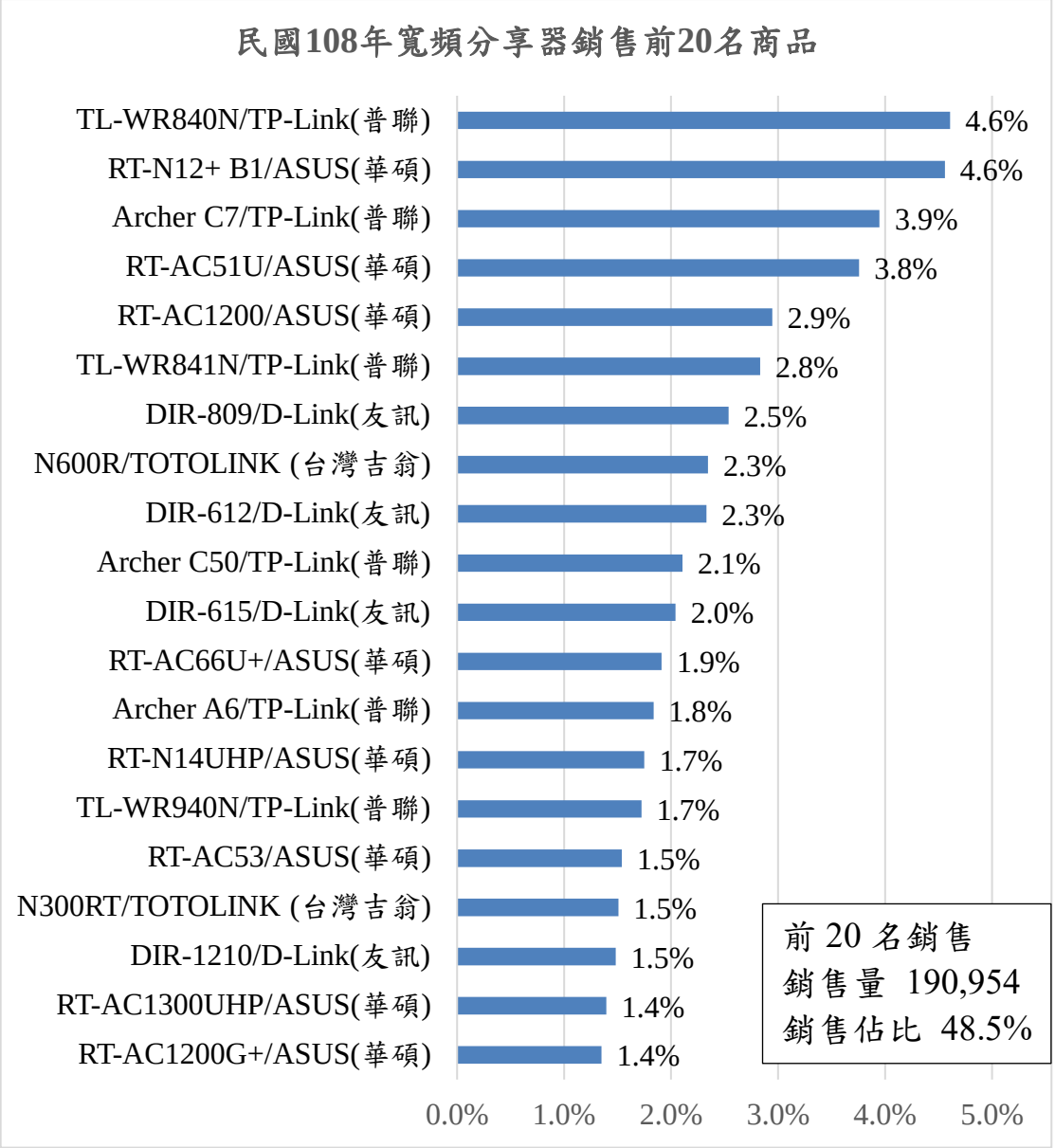



圖 20、民國 108 年寬頻分享器銷售前 20 名型號及佔比

下表根據民國 108 年寬頻分享器銷售調查資料，列出市場熱銷前 20 名商品資訊包含產品品牌、型號、全年銷售量、佔比及是否支援 IPv6。其中是否支援 IPv6 的訊息是根據官網所提供的產品規格資訊標示內容為參考依據。後續將會針對各項商品進行 IPv6 連結測試，以驗證商品對 IPv6 的支援狀況。

表 9、民國 108 年寬頻分享器銷售前 20 名銷售量及佔比

| 排名 | 品牌 | 型號 | 銷售量 | 銷售佔比 | 支援 IPv6 |
|---|---|---|---|---|---|
| **1** | TP-Link (普聯) | TL-WR840N | 18,139 | 4.6% | ✓ |
| **2** | ASUS (華碩) | RT-N12+ B1 | 17,944 | 4.6% | ✓ |
| **3** | TP-Link (普聯) | Archer C7 | 15,543 | 3.9% | ✓* |
| **4** | ASUS (華碩) | RT-AC51U | 14,794 | 3.8% | ✓ |
| **5** | ASUS (華碩) | RT-AC1200 | 11,599 | 2.9% | ✓ |
| **6** | TP-Link (普聯) | TL-WR841N | 11,150 | 2.8% | ✓* |
| **7** | D-Link (友訊) | DIR-809 | 9,987 | 2.5% | |
| **8** | TOTOLINK (台灣吉翁) | N600R | 9,232 | 2.3% | |
| **9** | D-Link (友訊) | DIR-612 | 9,174 | 2.3% | |
| **10** | TP-Link (普聯) | Archer C50 | 8,288 | 2.1% | ✓ |
| **11** | D-Link (友訊) | DIR-615 | 8,039 | 2.0% | |
| **12** | ASUS (華碩) | RT-AC66U+ | 7,523 | 1.9% | ✓ |
| **13** | TP-Link (普聯) | Archer A6 | 7,230 | 1.8% | ✓ |
| **14** | ASUS (華碩) | RT-N14UHP | 6,887 | 1.7% | |
| **15** | TP-Link (普聯) | TL-WR940N | 6,781 | 1.7% | ✓* |
| **16** | ASUS (華碩) | RT-AC53 | 6,060 | 1.5% | ✓ |
| **17** | TOTOLINK (台灣吉翁) | N300RT | 5,937 | 1.5% | ✓ |
| **18** | D-Link (友訊) | DIR-1210 | 5,838 | 1.5% | ✓ |
| **19** | ASUS (華碩) | RT-AC1300UHP | 5,493 | 1.4% | ✓ |
| **20** | ASUS (華碩) | RT-AC1200G+ | 5,316 | 1.4% | ✓ |
| **總計** | | | **190,954** | **48.5%** | **15** |

註*：TP-Link (普聯) Archer C7、TL-WR841N 及 TL-WR940N 共 3 項商品，依韌體版本不同部分可支援 IPv6。

根據上表調查結果顯示，民國 108 年寬頻分享器全年銷售量前 20 名的商品中，若以商品的型號數來計算支援 IPv4/IPv6 雙協定的商品共有 15 個商品，所佔比例為 75%。

下表以銷售量計算，統計出支援 IPv4/IPv6 雙協定的銷量約為 14.8 萬台，佔前 20 名產品的銷售量 77.3%，和以型號數計算佔比數結果

趨同。而不支援 IPv6 的 5 項商品銷售量為約 4.3 萬台，佔前 20 名產品的銷售量 22.7%。顯示民國 108 年寬頻分享器支援 IPv6 佔比較不支援的產品高出許多。

表 10、民國 108 年寬頻分享器銷售前 20 名產品支援 IPv6 情況

| 產品類別 | 商品數 | 銷售量 | 銷售佔比 | 支援 IPv6 商品數 | 支援 IPv6 銷售量 | 支援 IPv6 銷售佔比 | 不支援 IPv6 商品數 | 不支援 IPv6 銷售量 | 不支援 IPv6 銷售佔比 |
|---|---|---|---|---|---|---|---|---|---|
| 寬頻分享器 | 20 | 190,954 | 48.5% | 15 | 147,635 | 77.3% | 5 | 43,319 | 22.7% |

下圖為民國 108 年寬頻分享器銷售量前 20 名 IPv6 支援佔比，分別以型號數和實際銷售數量統計，其支援比例並無太大差異：

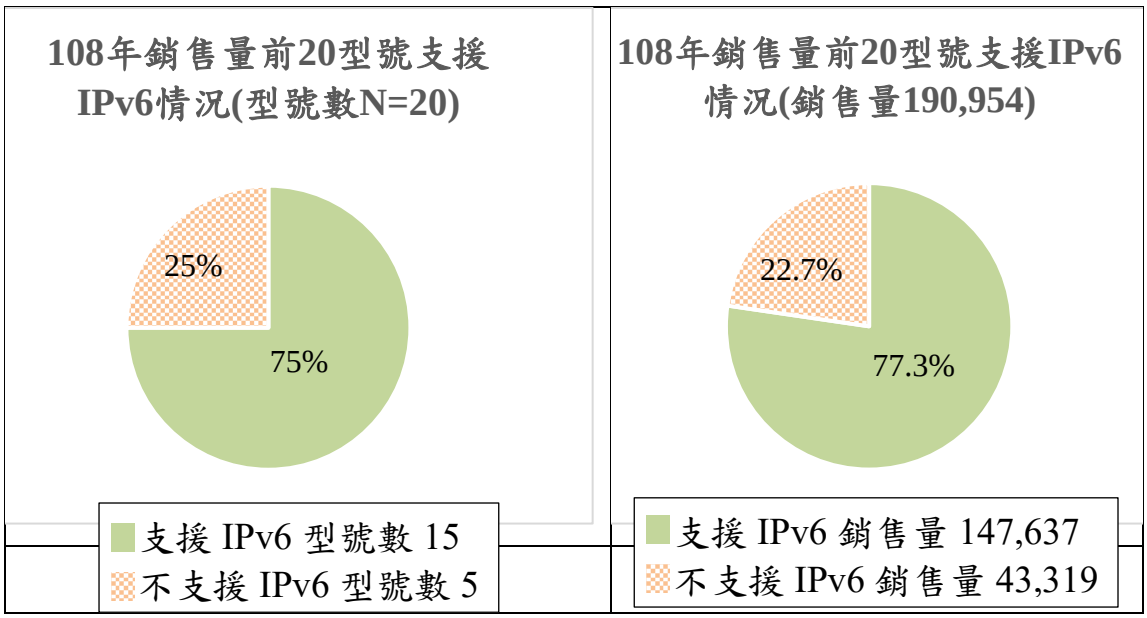



圖 21、民國 108 年寬頻分享器銷售量前 20 名 IPv6 支援佔比

下表將前 20 名的寬頻分享器，依生產業者品牌統計其銷售商品型號數及銷售數字，並列出各廠牌支援 IPv6 的商品型號數、銷售量、及銷售佔比等資料。各品牌銷售佔比是以全年銷售量 (民國 108 年全年銷售量為 393,646) 計算。

表 11、民國 108 年寬頻分享器品牌銷售統計資料

| 品牌 | 商品數量 | 銷售量 | 銷售佔比 | 支援 IPv6 商品數 | 支援 IPv6 銷售量 | 支援 IPv6 銷售佔比 | 不支援 IPv6 商品數 | 不支援 IPv6 銷售量 | 不支援 IPv6 銷售佔比 |
|---|---|---|---|---|---|---|---|---|---|
| ASUS (華碩) | 8 | 75,616 | 19.2% | 7 | 68,729 | 17.5% | 1 | 6,887 | 1.7% |
| TP-LINK (普聯) | 6 | 67,131 | 17.1% | 6 | 67,131 | 17.1% | 0 | 0 | 0% |
| D-Link (友訊) | 4 | 33,038 | 8.4% | 1 | 5,838 | 1.4% | 3 | 27,200 | 6.9% |
| TOTOLINK (台灣吉翁) | 2 | 15,169 | 3.8% | 1 | 5,937 | 1.5% | 1 | 9,232 | 2.4% |
| **總計** | **20** | 190,954 | 48.5% | 15 | 147,635 | 37.5% | 5 | 43,319 | 11.0% |

依台灣寬頻分享器銷售量最高品牌統計結果來看，銷售最高品牌 ASUS (華碩) 入榜的 8 個商品有 1 項商品未標示支援 IPv4/IPv6 雙軌網路服務，其中未標示支援 IPv6 產品型號為 RT-N14UHP。以支援率而言 TP-Link (普聯) 最高，入榜 6 個商品皆明確標示支援 IPv4/IPv6 雙軌網路服務。D-Link (友訊) 入榜 4 產品中只有 1 項商品有明確標示支援 IPv6，其餘 3 項產品並未明確標示支援 IPv4/IPv6 雙軌網路服務。而 TOTOLINK (台灣吉翁) 入榜 2 商品中有 1 商品標示支援 IPv6，另一項產品未明確標示支援 IPv4/IPv6 雙軌網路服務。

下圖為民國 108 年市場銷售前 20 名的寬頻分享器，依生產業者品牌統計各品牌支援 IPv6 的商品數佔比。

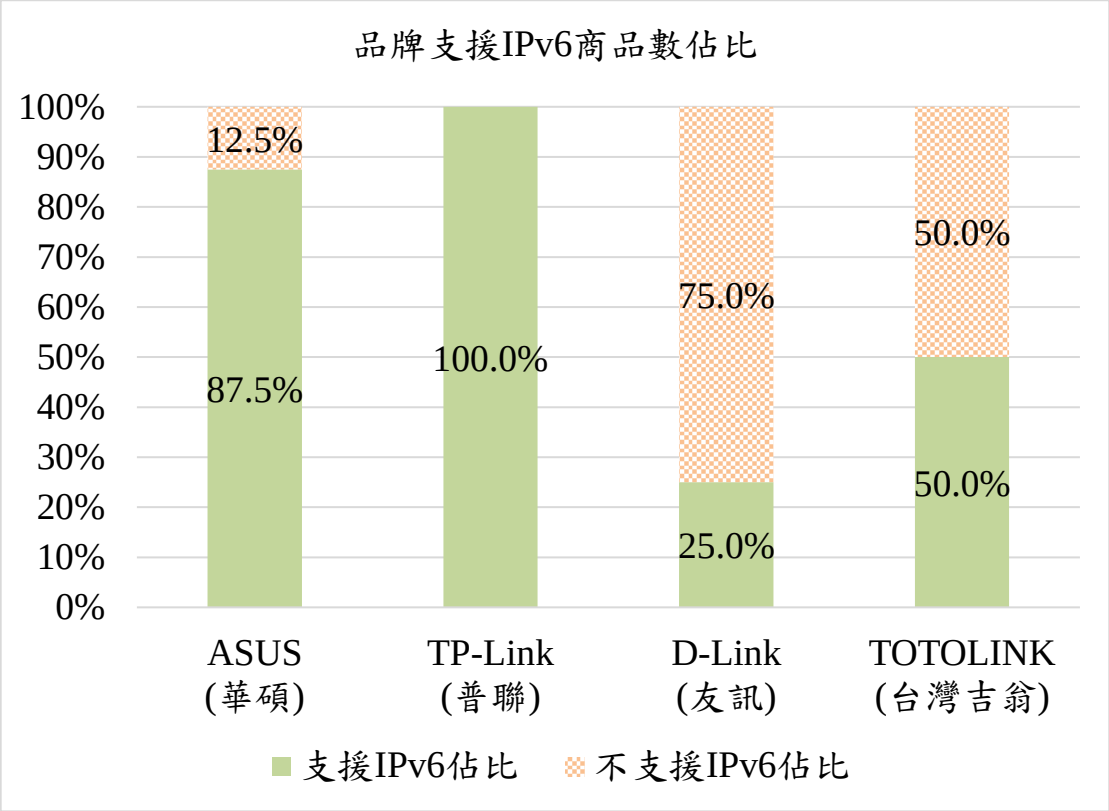



圖 22、寬頻分享器依品牌統計支援 IPv6 商品數佔比

比較民國 106 年與 108 年市售頻分享器支援 IPv6 調查結果發現，民國 106 年當年度排行熱銷產品前 20 名中，初步調查業者有標示可支援 IPv6 的產品型號共有 11 項，不支援 IPv6 的型號數有 9 項。民國 108 年調查結果，當年度排行熱銷產品前 20 名中，初步調查業者有標示可支援 IPv6 的產品型號共有 15 項，不支援 IPv6 的型號數有 5 項，雖然家用網通產品生命周期較長，部分業者以透過韌體升級的方式讓舊有產品支援 IPv4/IPv6 雙軌網路支援服務，原廠官網上更積極標示產品可支援 IPv4/IPv6 雙軌網路服務之資訊，相對於民國 106 年調查結果整體 IPv6 支援率上有明顯提升，並且標示更為明確。

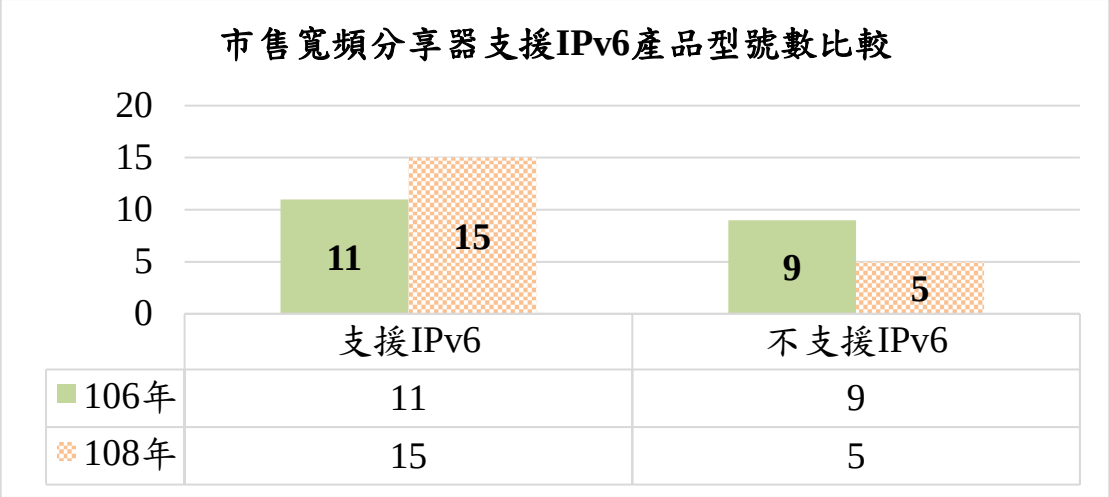



圖 23、民國 106 年與 108 年市售頻分享器支援 IPv6 比較圖

下圖為民國 108 年國內市售寬頻分享器全年度品牌銷售量排行，第一名為 ASUS (華碩) 市佔率為 30.2%、第二名為 TP-Link (普聯) 市佔率為 28.6%、第三名為 D-Link (友訊) 市佔率為 20.1%、及第四名為 TOTOLINK (台灣吉翁) 市佔率為 13.2%，前四大品牌合計銷售量超過 90%，和民國 106 年調查結果由四大品牌佔據超過 90%的狀況雷同，只是市場排名出現些微的變化。根據民國 106 年調查結果，市售寬頻分享器銷售量第一名品牌為 D-Link (友訊) 市佔率為 28.3%、第二名為 ASUS (華碩) 市佔率為 25.7%、第三名為 TP-Link (普聯) 市佔率為 16.8%、及第四名為 TOTOLINK (台灣吉翁) 市佔率為 14.6%。民國 108 年前 4 大品牌以 TP-Link (普聯) 成長最多，而 D-Link (友訊) 減少比例最大。

下圖為民國 108 年寬頻分享器銷售量前 10 名品牌，及各品牌廠當年度銷售佔比：

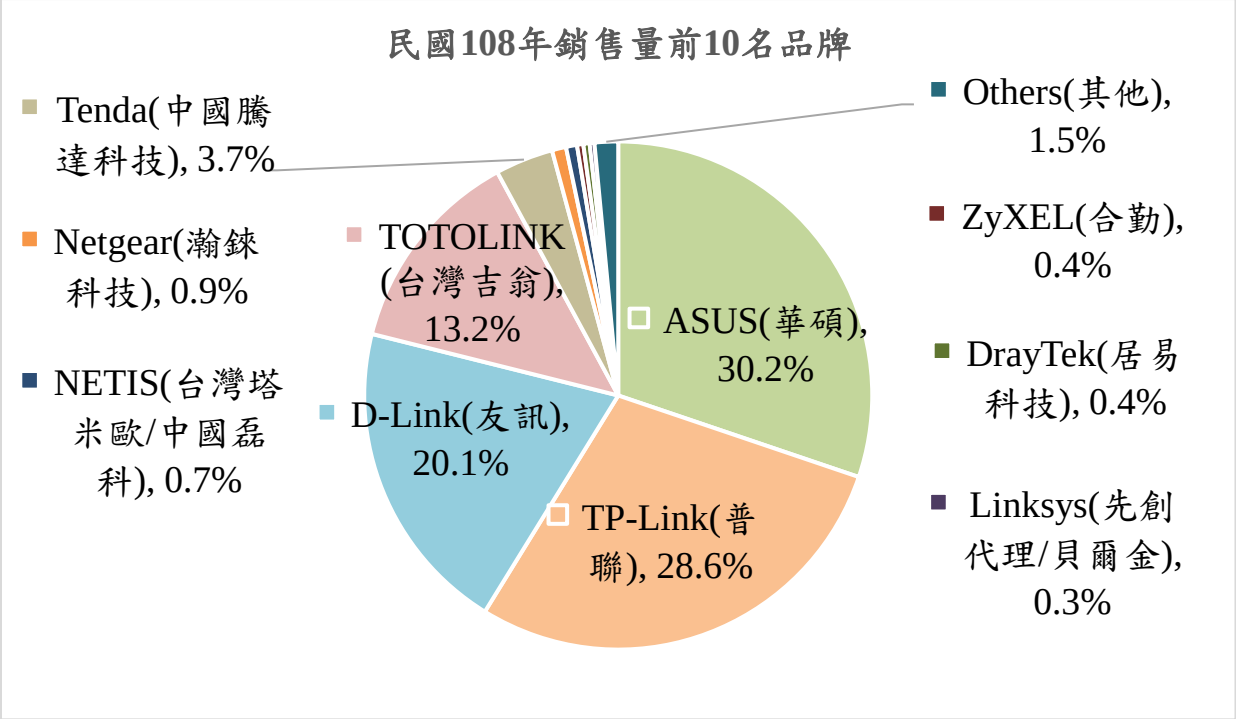
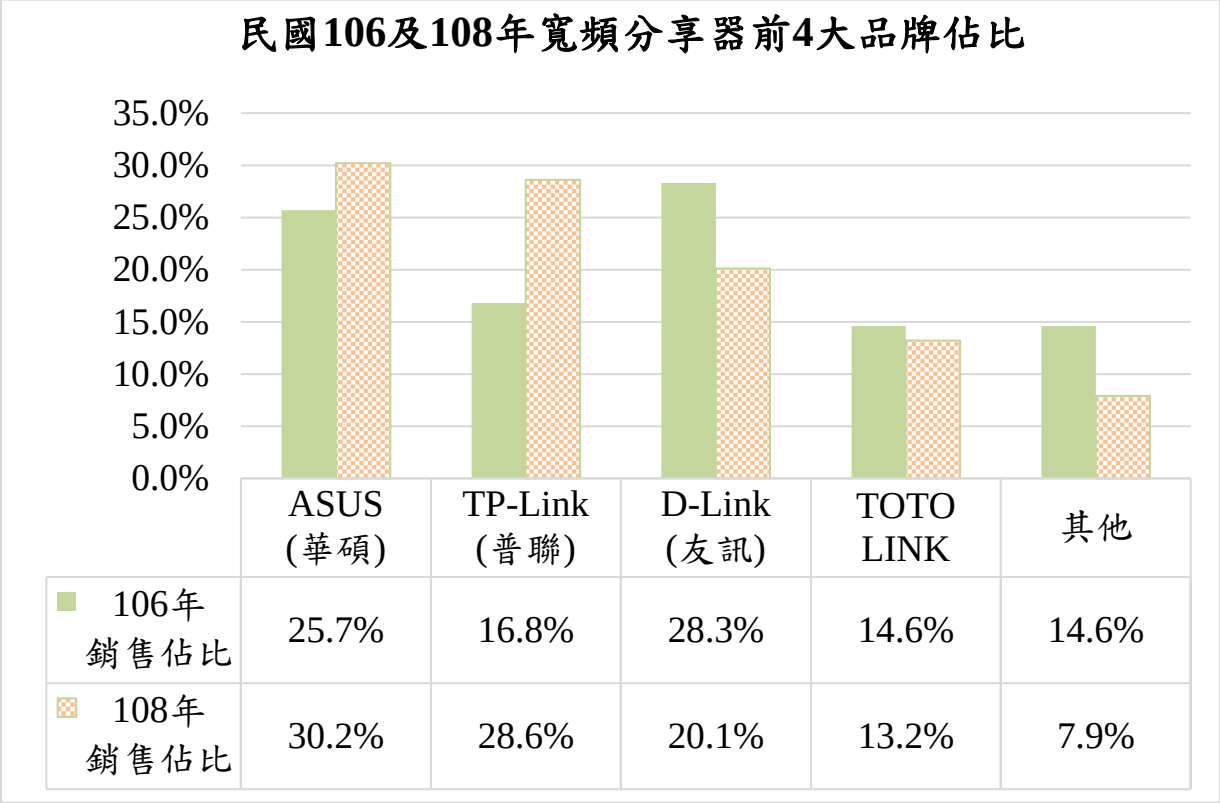



圖 24、民國 108 年寬頻分享器銷售量前 10 名品牌

下圖比較民國 106 及 108 年寬頻分享器前 4 大品牌佔比：




| | ASUS(華碩) | TP-Link(普聯) | D-Link(友訊) | TOTO LINK | 其他 |
|---|---|---|---|---|---|
| 106年銷售佔比 | 25.7% | 16.8% | 28.3% | 14.6% | 14.6% |
| 108年銷售佔比 | 30.2% | 28.6% | 20.1% | 13.2% | 7.9% |

圖 25、民國 106 及 108 年寬頻分享器前 4 大品牌佔比

下表為民國 106 年及 108 年國內市售寬頻分享器全年度品牌銷售量、佔比及排行比較表：

表 12、民國 106 年及 108 年市售寬頻分享器品牌銷售量排行比較

| 排名 | 品牌 | 106 年銷售量 | 106 年佔比 | 品牌 | 108 年銷售量 | 108 年佔比 |
|---|---|---|---|---|---|---|
| 1 | D-Link (友訊) | 129158 | 28.3% | ASUS (華碩) | 118881 | 30.2% |
| 2 | ASUS (華碩) | 117291 | 25.7% | TP-Link (普聯) | 112583 | 28.6% |
| 3 | TP-Link (普聯) | 76673 | 16.8% | D-Link (友訊) | 79123 | 20.1% |
| 4 | TOTOLINK (台灣吉翁) | 66633 | 14.6% | TOTOLINK (台灣吉翁) | 51961 | 13.2% |
| 5 | NETIS (台灣塔米歐/中國磊科) | 21907 | 4.8% | Tenda (中國騰達科技) | 14565 | 3.7% |
| 6 | Tenda (中國騰達科技) | 16886 | 3.7% | Netgear (瀚銖科技) | 3543 | 0.9% |
| 7 | EDIMAX (訊舟) | 7302 | 1.6% | NETIS (台灣塔米歐/中國磊科) | 2756 | 0.7% |
| 8 | HUAWEI (華為) | 5477 | 1.2% | ZyXEL (合勤) | 1575 | 0.4% |
| 9 | Sapido (金智洋科技) | 3195 | 0.7% | DrayTek (居易科技) | 1575 | 0.4% |
| 10 | Netgear (瀚銖科技) | 2738 | 0.6% | Linksys (先創代理/貝爾金) | 1181 | 0.3% |
| | Others (其他) | 9128 | 2.0% | Others (其他) | 5905 | 1.5% |

民國 106 年銷售前五名之品牌依序為 D-Link (友訊) 、ASUS (華碩) 、TP-Link (普聯) 、TOTOLINK (台灣吉翁) 與 NETIS (台灣塔米歐/中國磊科) 。前五名品牌囊括民國 106 年網通商品整體銷售之 90.2%，且第一名的 D-Link (友訊) 佔全年市場 28.3%之銷售份額。民國 108 年銷售前五名品牌則有所轉變，依序為 ASUS (華碩) 30.2% 、TP-Link (普聯) 28.6%，第三位為 D-Link (友訊) ，由民國 106 年市佔 28.3%下降至民國 108 年 20.1%；第四位 TOTOLINK (台灣吉翁) 也下

降 1.4%，民國 108 年佔 13.2%；第五位則為 Tenda (中國騰達科技) 擠下 NETIS，約佔 3.7%。

本調查詳細資料請參閱附錄四報告內容，有更詳細說明。

# 第二節 廠商支援 IPv6 意願調查

根據市售網通產品調查結果顯示，歸納國內主要生產銷售寬頻分享器的品牌業者，主要為 ASUS (華碩)、TP-Link (普聯)、D-Link (友訊) 及 TOTOLINK (台灣吉翁) 等四大品牌為主。本分項工作，將依據市場銷售調查結果，安排面訪及進行商品支援 IPv6 互通性測試 2 大面向進行，工作項目包含：

- 網通產品 IPv6 互通性測試：和中華電信固網 Hinet 及 TBC Cable 寬頻網路，進行國內市售寬頻分享器支援 IPv6 互通性測試。
- 廠商預設開啟支援 IPv6 意願調查：面訪國內主要寬頻分享器業者，以了解國內業者對產品預設支援 IPv6 的意願及規劃。

以下就依上列工作項目，依照執行成果說明。

## 壹、網通產品 IPv6 互通性測試

此分項工作按照「市售網通產品調查」結果，歸納出在民國 108 年國內熱銷的寬頻分享器前 20 名型號產品，和國內已經支援 IPv6 商用固接網路及試用 Cable 網路服務，進行連線互通性測試。以下整理計畫將進行方式。

國內目前已經支援 IPv6 的固接網路 IASP 業者，有中華電信 Hinet 光世代於民國 107 年正式啟動支援 IPv6，並對所有用戶預設開啟；而 Cable 業者 TBC (台灣寬頻通訊)，於民國 108 年開放使用者申請試用 IPv6 網路服務。因此網通產品 IPv6 互通性測試，將以和中華電信 Hinet 及 TBC Cable 寬頻網路為標的，進行互通性測試。此次測試的方法是針對終端用戶的使用需求為主，進行測試項目設計。

## 一. 網通產品和 Hinet 進行 IPv6 互通性測試

中華電信固接網路所採用的是支援 IPv4/IPv6 雙協定，及以 PPPoE 撥接服務通訊協定，下表為測試項目列表：

表 13、支援 IPv4/IPv6 PPPoE 雙軌網路服務之寬頻分享器測試項目

| 序號 | 測試項目 | 測試方法 |
|---|---|---|
| 一 | 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 |
| 二 | 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。 |
| 三 | 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 |
| 四 | 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<br>網址：http://test-ipv6.com/<br>網址：http://ipv6-test.com/ |
| 五 | 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 |
| 六 | 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 |
| 七 | 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 |
| 八 | 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<br>網址：http://test-ipv6.com/<br>網址：http://ipv6-test.com/ |

民國 108 年熱銷前 20 名寬頻分享器商品和中華電信 Hinet 光世代進行 IPv6 互通性測試結果，如下表所示：

表 14、熱銷前 20 名寬頻分享器和 Hinet IPv6 互通性測試結果

| 排名 | 品牌 | 型號 | 一 PPPoE 撥接 | 二 自動啟用 IPv6 | 三 IPv6 取得 | 四 IPv6 上網 | 五 熱門網頁開啟 | 六 驗證重播 | 七 Wi-Fi 上網 | 八 驗證 Wi-Fi IPv6 |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | TP-Link (普聯) | TL-WR840N | V | X | V | V | V | V | V | V |
| 2 | ASUS (華碩) | RT-N12+ B1 | V | X | V | V | V | V | V | V |
| 3 | TP-Link (普聯) | Archer C7 | V | X | V | V | V | V | V | V |
| 4 | ASUS (華碩) | RT-AC51U | V | X | V | V | V | V | V | V |
| 5 | ASUS (華碩) | RT-AC1200 | V | X | V | V | V | V | V | V |
| 6 | TP-Link (普聯) | TL-WR841N | V | X | V | V | V | V | V | V |
| 7 | D-Link (友訊) | DIR-809 | V | X | X | X | X | X | X | X |
| 8 | TOTOLINK (台灣吉翁) | N600R | V | X | X | X | X | X | X | X |
| 9 | D-Link (友訊) | DIR-612 | V | X | X | X | X | X | X | X |
| 10 | TP-Link (普聯) | Archer C50 | V | X | V | V | V | V | V | V |
| 11 | D-Link (友訊) | DIR-615 | 已停售 | | | | | | | |
| 12 | ASUS (華碩) | RT-AC66U+ | V | X | V | V | V | V | V | V |
| 13 | TP-Link (普聯) | Archer A6 | V | X | V | V | V | V | V | V |
| 14 | ASUS (華碩) | RT-N14UHP | V | X | X | X | X | X | X | X |
| 15 | TP-Link (普聯) | TL-WR940N | V | X | V | V | V | V | V | V |
| 16 | ASUS (華碩) | RT-AC53 | V | X | V | V | V | V | V | V |
| 17 | TOTOLINK (台灣吉翁) | N300RT | V | X | X | X | X | X | X | X |
| 18 | D-Link (友訊) | DIR-1210 | V | X | V | V | V | V | V | V |
| 19 | ASUS (華碩) | RT-AC1300UHP | V | X | V | V | V | V | V | V |
| 20 | ASUS (華碩) | RT-AC1200G+ | V | X | V | V | V | V | V | V |

由上表測試結果分析和上一分項工作市售網通產品調查結果進行比對，結果為：

- 民國 108 年全年度熱銷前 20 名寬頻分享器中，D-Link 型號 DIR-615 已停售，無法取得測試結果。
- 完成測試 19 台寬頻分享器中，其中 5 台不支援 IPv6 上網；其餘 14 台皆可透過手動選取啟用 IPv6。
- 和調查結果有 15 台寬頻分享器標示可支援 IPv6 相比，其中只有銷售排名 17 由 TOTOLINK (台灣吉翁) 所生產型號 N300RT 有標示支援 IPv6，但測試和 Hinet PPPoEv6 不合，無法支援 IPv6 連網，其餘 14 台皆可支援 IPv6。
- 14 台有支援 IPv6 寬頻分享器，皆不支援自動啟用 IPv6 功能。

以下以熱銷第一名商品由 TP-Link (普聯) 所生產寬頻分享器型號 TL-WR840N 為例，提列測試所得截圖畫面：

## (一) 驗證分享器 PPPoE 撥接是否正常?

下圖顯示 TP-Link (普聯) TL-WR840N 確認 PPPoE 已連接：

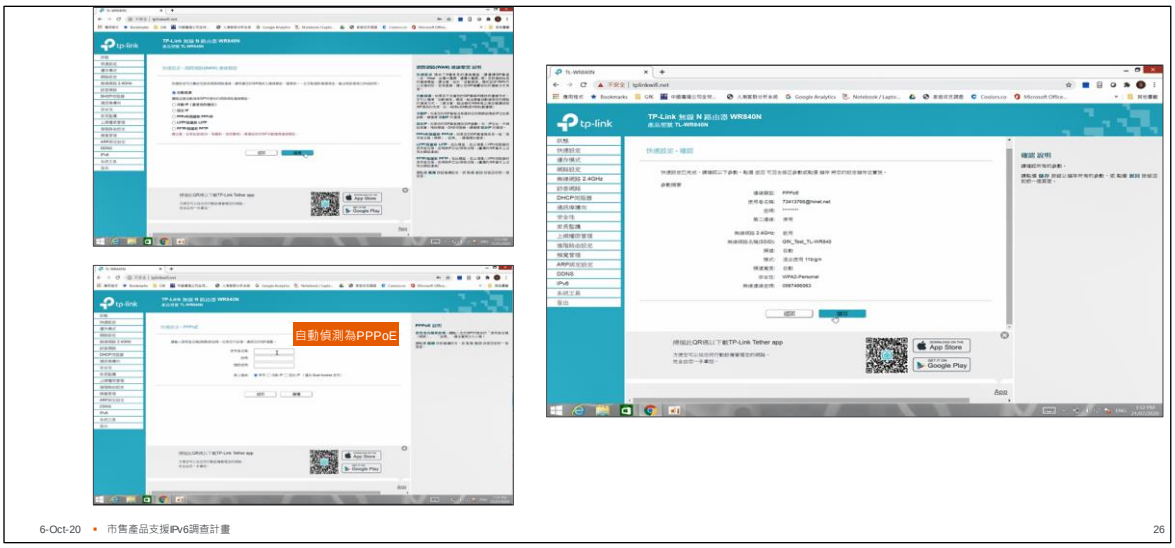



圖 26、TP-Link (普聯) TL-WR840N 確認 PPPoE 已連接

## (二)IPv6 PPPoE (或是 PPPoEv6)是否隨著 IPv4 PPPoE 啟用而自動啟用

下圖為 TP-Link (普聯) TL-WR840N 不支援自動啟用 IPv6：

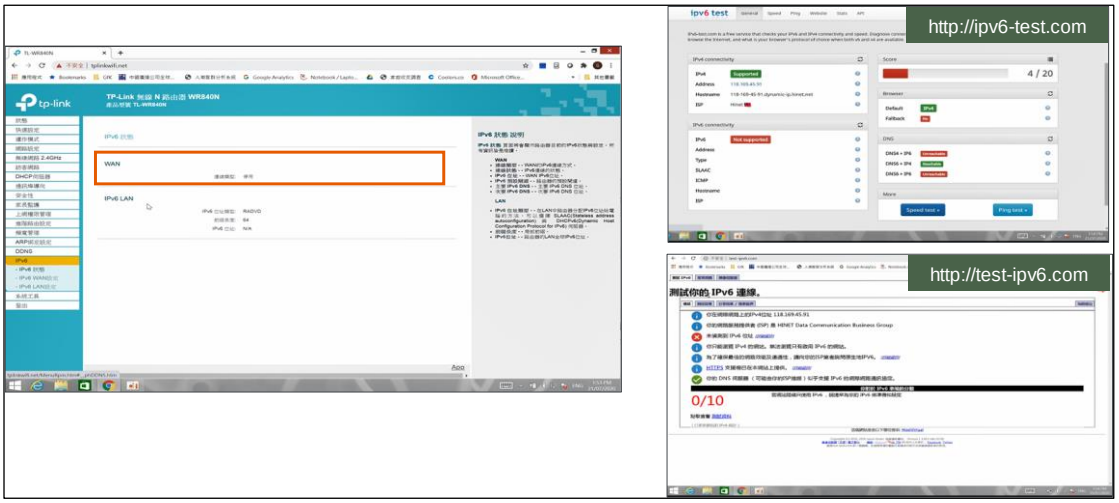



圖 27、TP-Link (普聯)TL-WR840N 不支援自動啟用 IPv6

## (三) 驗證分享器 IPv6、IPv6 PD、DNSv6 取得是否正常?

下圖顯示 TP-Link (普聯) TL-WR840N 在 IPv6 設定中選擇 PPPoE，即可正常連線：

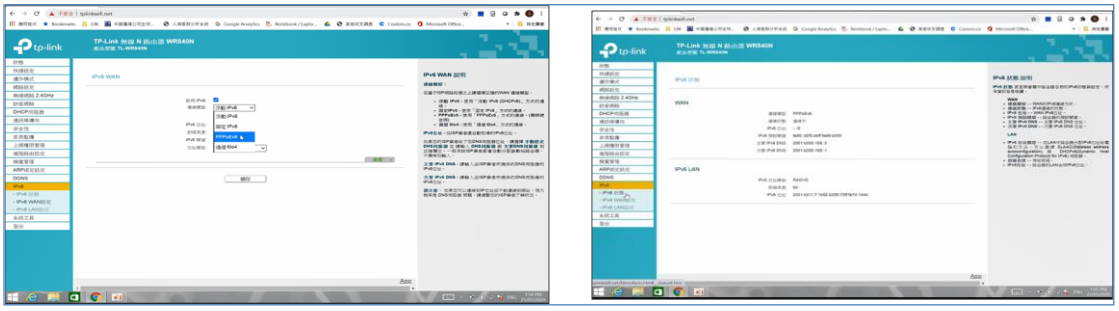


圖 28、TP-Link (普聯) TL-WR840N 可正常連線 PPPoEv6

## (四) 驗證用戶 IPv6 上網是否正常?

下圖顯示 TP-Link (普聯) TL-WR840N 驗證 IPv6 上網可正常連線：

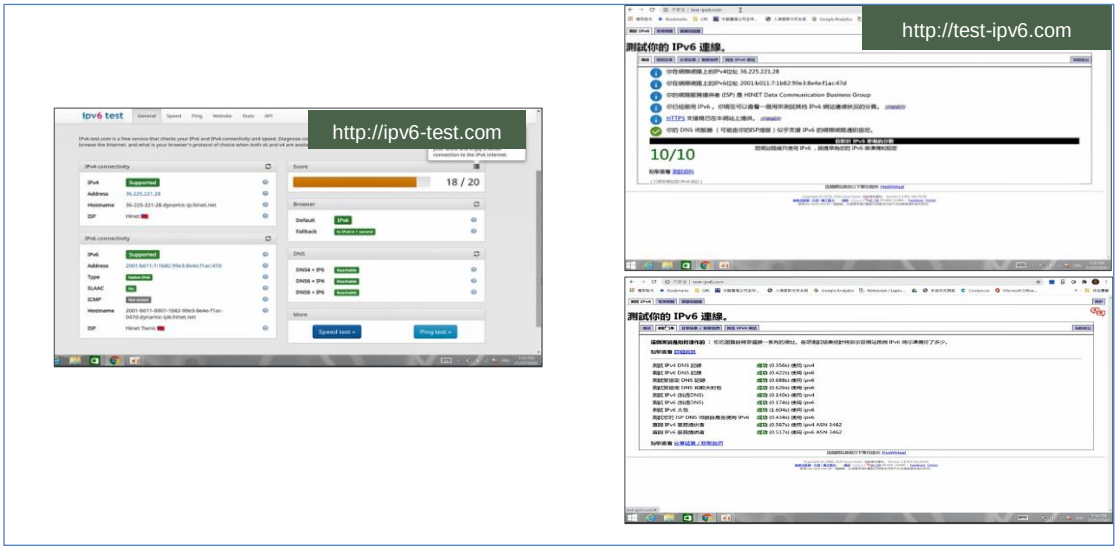



圖 29、TP-Link (普聯) TL-WR840N 驗證 IPv6 上網正常

## (五) 驗證用戶熱門網頁開啟是否正常?

下圖為 TP-Link (普聯) TL-WR840N 以 IPv6 連結至熱門網頁 Google、Youtube、HiNet、Microsoft、Yahoo 等，確認開啟正常：

圖 30、TP-Link (普聯) TL-WR840N 以 IPv6 連結熱門網頁正常

## (六) 驗證分享器重撥，用戶 IPv6 更新是否正常?

下圖顯示 TP-Link (普聯) TL-WR840N 以 IPv6 連結進行寬頻分享器重撥，用戶 IPv6 更新正常：

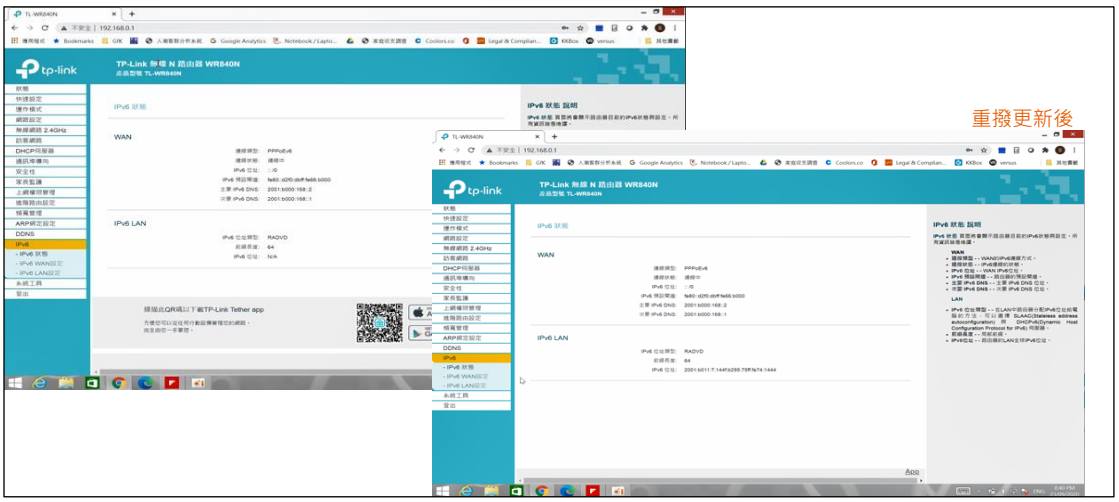



圖 31、TP-Link (普聯) TL-WR840N 以 IPv6 連結進行重撥正常

## (七) 驗證用戶連接 Wi-Fi 上網 IPv6、DNSv6 是否正常?

下圖顯示 TP-Link (普聯) TL-WR840N 連接 Wi-Fi 上網 IPv6、DNSv6 正常：

圖 32、TP-Link (普聯) TL-WR840N 以 Wi-Fi 上網 IPv6、DNSv6 正常

### (八) 驗證用戶連接 Wi-Fi IPv6 上網是否正常?

下圖顯示 TP-Link (普聯) TL-WR840N 驗證用戶連接 Wi-Fi IPv6 上網可正常連線：

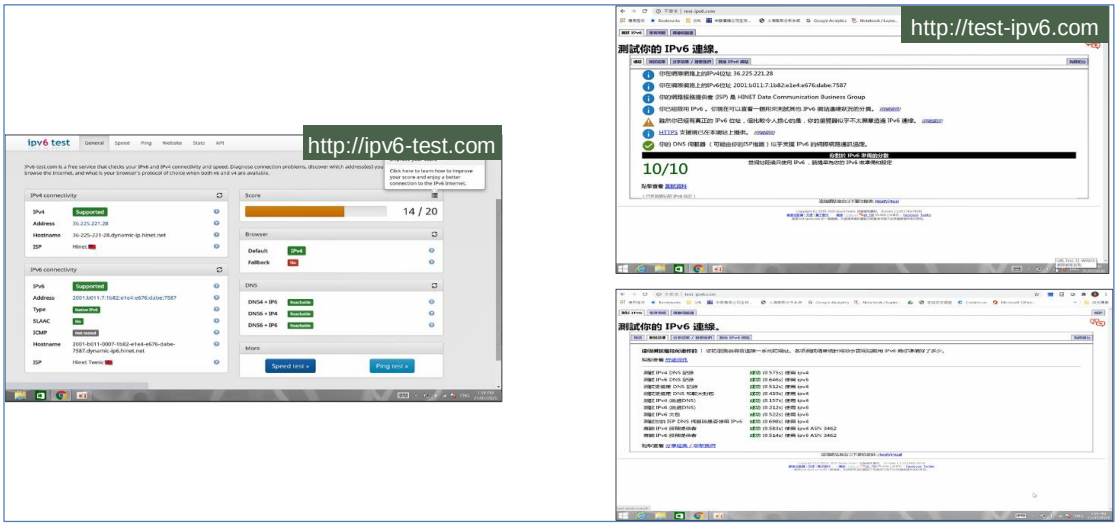



圖 33、TP-Link (普聯) TL-WR840N 連接 Wi-Fi IPv6 上網正常

其他商品測試截圖請參考附錄四有詳細說明。

## 二. 網通產品和 TBC 進行 IPv6 互通性測試

TBC Cable 寬頻網路所採用的是支援 IPv4/IPv6 雙協定，及以 IPoE 撥接服務通訊協定，TBC Cable 系統台包含南桃園、北視、信和、吉元、群健等，涵蓋桃園到台中區域。本次寬頻分享器連通測試，申請以南桃園有線電視寬頻網路服務作為測試實驗環境。

測試項目和 Hinet 之 IPv6 連結測試大部分相同，只有測試項目一〝驗證分享器連接 Cable Modem 是否正常?〞，及測試項目八 Cable 寬頻網路協定為 IPoEv6 而非 PPPoEv6，所以有所不同，但項目測試方法相同。下表為測試項目列表：

表 15、支援 IPv4/IPv6 IPoE 雙軌網路服務之寬頻分享器測試項目

| 序號 | 測試項目 | 測試方法 |
|---|---|---|
| 一 | 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 |
| 二 | IPv6 連線功能是否隨著 IPv6 啟用而自動啟用 | 測試 IPv6 連線功能是否隨著 IPv6 啟用而自動啟用，且正常連線。 |
| 三 | 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 |
| 四 | 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<br>網址：http://test-ipv6.com/<br>網址：http://ipv6-test.com/ |
| 五 | 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 |
| 六 | 驗證分享器重連 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 |
| 七 | 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 |
| 八 | 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<br>網址：http://test-ipv6.com/<br>網址：http://ipv6-test.com/ |

民國 108 年熱銷前 20 名寬頻分享器商品和 TBC 有線寬頻進行 IPv6 互通性測試結果，如下表所示：

表 16、熱銷前 20 名寬頻分享器和 TBC IPv6 互通性測試結果

| 排名 | 品牌 | 型號 | 一 PPPoE 撥接 | 二 自動啟用 IPv6 | 三 IPv6 取得 | 四 IPv6 上網 | 五 熱門網頁開啟 | 六 驗證重播 | 七 Wi-Fi 上網 | 八 驗證 Wi-Fi IPv6 |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | TP-Link (普聯) | TL-WR840N | V | X | V | V | V | V | V | V |
| 2 | ASUS (華碩) | RT-N12+ B1 | V | X | V | V | V | V | V | V |
| 3 | TP-Link (普聯) | Archer C7 | V | X | V | V | V | V | V | V |
| 4 | ASUS (華碩) | RT-AC51U | V | X | V | V | V | V | V | V |
| 5 | ASUS (華碩) | RT-AC1200 | V | X | V | V | V | V | V | V |
| 6 | TP-Link (普聯) | TL-WR841N | V | X | V | V | V | V | V | V |
| 7 | D-Link (友訊) | DIR-809 | V | X | X | X | X | X | X | X |
| 8 | TOTOLINK (台灣吉翁) | N600R | V | X | X | X | X | X | X | X |
| 9 | D-Link (友訊) | DIR-612 | V | X | X | X | X | X | X | X |
| 10 | TP-Link (普聯) | Archer C50 | V | X | V | V | V | V | V | V |
| 11 | D-Link (友訊) | DIR-615 | 已停售 | | | | | | | |
| 12 | ASUS (華碩) | RT-AC66U+ | V | X | V | V | V | V | V | V |
| 13 | TP-Link (普聯) | Archer A6 | V | X | V | V | V | V | V | V |
| 14 | ASUS (華碩) | RT-N14UHP | V | X | X | X | X | X | X | X |
| 15 | TP-Link (普聯) | TL-WR940N | V | X | V | V | V | V | V | V |
| 16 | ASUS (華碩) | RT-AC53 | V | X | V | V | V | V | V | V |
| 17 | TOTOLINK (台灣吉翁) | N300RT | V | X | X | X | X | X | X | X |
| 18 | D-Link (友訊) | DIR-1210 | V | X | V | V | V | V | V | V |
| 19 | ASUS (華碩) | RT-AC1300UHP | V | X | V | V | V | V | V | V |
| 20 | ASUS (華碩) | RT-AC1200G+ | V | X | V | V | V | V | V | V |

由上表 TBC Cable 寬頻網路 IPv6 測試結果，分析和上一分項工作市售網通產品調查結果進行比對，結果為 Hinet 測試結果雷同：

- 民國 108 年全年度熱銷前 20 名寬頻分享器中，D-Link 型號 DIR-615 已停售，無法取得測試結果。
- 完成測試 19 台寬頻分享器中，其中 5 台不支援 IPv6 上網；其餘 14 台皆可透過手動選取啟用 IPv6。
- 和調查結果有 15 台寬頻分享器標示可支援 IPv6 相比，其中只有銷售排名 17 由 TOTOLINK (台灣吉翁) 所生產型號 N300RT 有標示支援 IPv6，但測試結果無法支援 IPv6 連網，其餘 14 台皆可支援 IPv6。
- 14 台有支援 IPv6 寬頻分享器，皆不支援自動啟用 IPv6 功能。

以下以熱銷第二名商品由 ASUS (華碩) 所生產寬頻分享器型號 2RT-N12+B1 為例，提列測試所得截圖畫面：

## (一)驗證分享器連接 Cable Modem 是否正常?

下圖顯示 ASUS (華碩) 寬頻分享器型號 2RT-N12+B1，確認 IPv6 Cable Modem 可連接：

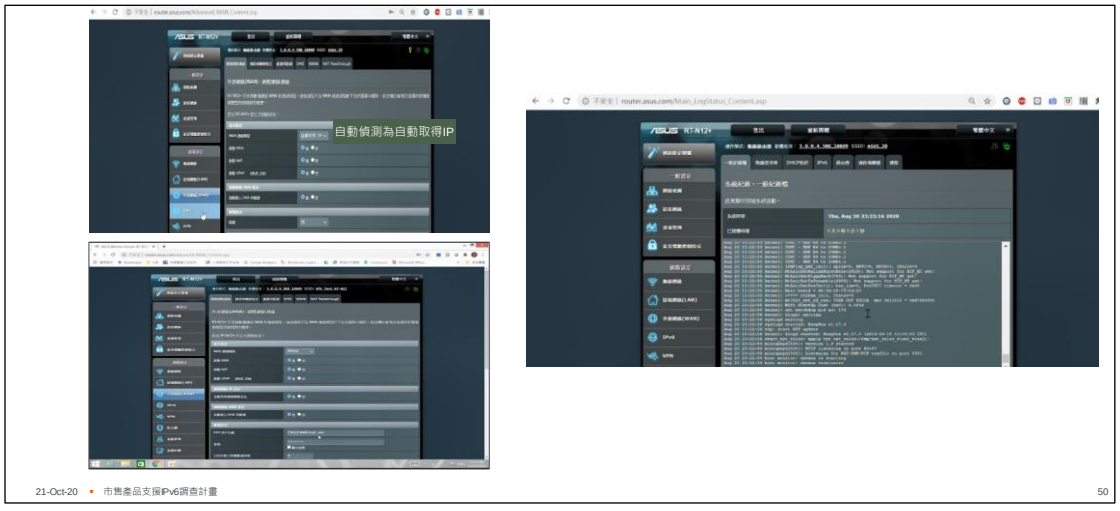



圖 34、ASUS (華碩) 2RT-N12+B1 確認 IPv6 Cable Modem 可連接

## (二)IPv6 PPPoE (或是 PPPoEv6)是否隨著 IPv4 PPPoE 啟用而自動啟用

下圖顯示 ASUS (華碩) 寬頻分享器型號 2RT-N12+B1，不支援自動啟用 IPv6：

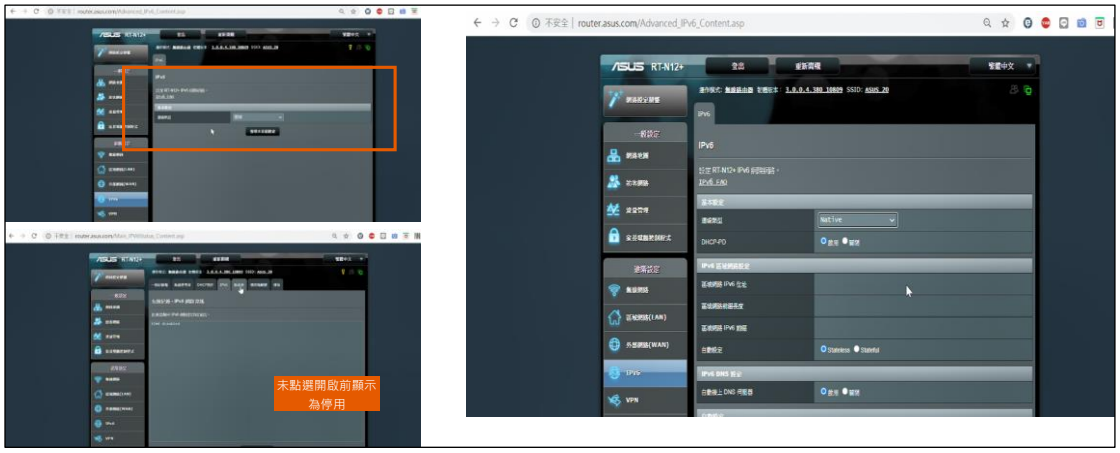



圖 35、ASUS (華碩) 2RT-N12+B1 不支援自動啟用 IPv6

## (三) 驗證分享器 IPv6、IPv6 PD、DNSv6 取得是否正常?

下圖顯示 ASUS (華碩) 寬頻分享器型號 2RT-N12+B1，可正常啟用 IPv6、IPv6PD、DNSv6 連線：

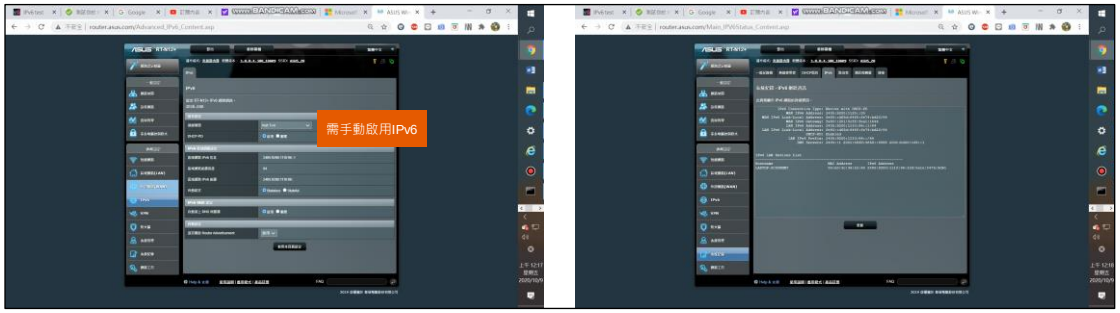



圖 36、ASUS (華碩) 2RT-N12+B1 可正常連線 IPoEv6

## (四) 驗證用戶 IPv6 上網是否正常?

下圖顯示 ASUS (華碩) 寬頻分享器型號 2RT-N12+B1，驗證 IPv6 上網可正常連線：

圖 37、ASUS (華碩) 2RT-N12+B1 驗證 IPv6 上網正常

## (五) 驗證用戶熱門網頁開啟是否正常?

下圖顯示 ASUS (華碩) 寬頻分享器型號 2RT-N12+B1，以 IPv6 連結至熱門網頁 Google、Youtube、HiNet、Microsoft、Yahoo 等，確認開啟正常：

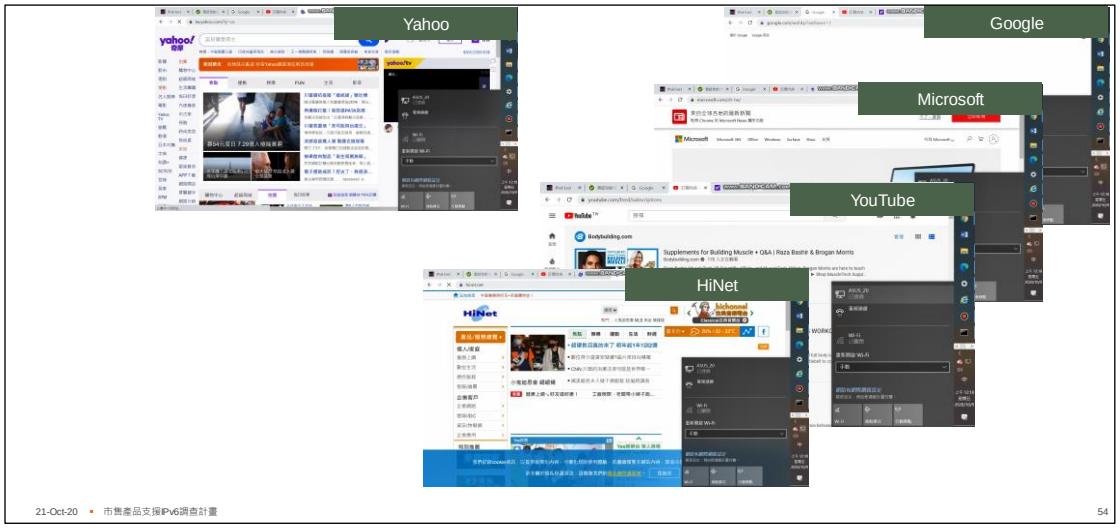



圖 38、ASUS (華碩) 2RT-N12+B1 以 IPv6 連結熱門網頁正常

## (六) 驗證分享器重撥，用戶 IPv6 更新是否正常?

下圖顯示 ASUS (華碩) 寬頻分享器型號 2RT-N12+B1，以 IPv6 連結進行寬頻分享器重撥，用戶 IPv6 更新正常：

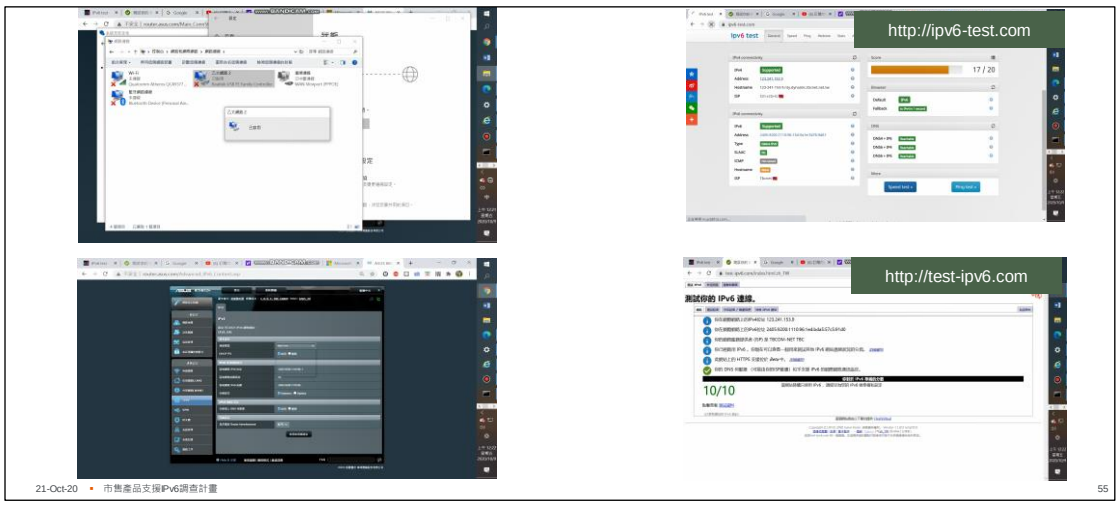



圖 39、ASUS (華碩) 2RT-N12+B1 以 IPv6 連結進行重撥正常

## (七) 驗證用戶連接 Wi-Fi 上網 IPv6、DNSv6 是否正常?

下圖顯示 ASUS (華碩) 寬頻分享器型號 2RT-N12+B1，連接 Wi-Fi 上網 IPv6、DNSv6 正常：

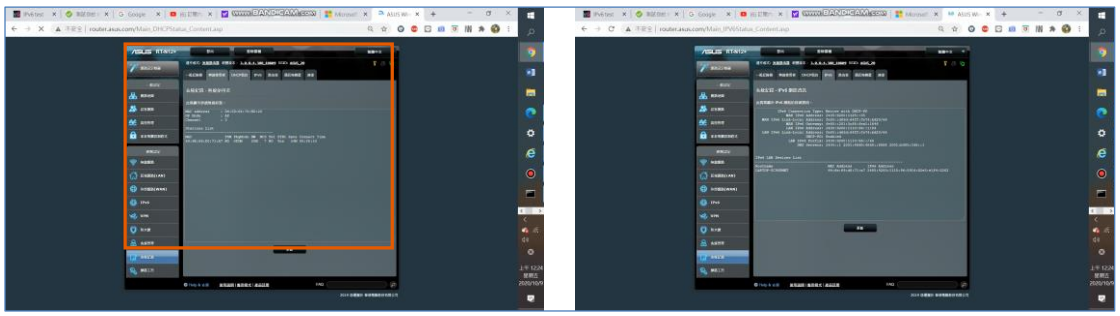


圖 40、ASUS (華碩) 2RT-N12+B1 以 Wi-Fi 上網 IPv6、DNSv6 正常

### (八) 驗證用戶連接 Wi-Fi IPv6 上網是否正常?

下圖顯示 ASUS (華碩) 寬頻分享器型號 2RT-N12+B1，驗證用戶連接 Wi-Fi IPv6 上網可正常連線：

圖 41、ASUS (華碩) 2RT-N12+B1 連接 Wi-Fi IPv6 上網正常

其他商品測試截圖請參考附錄四有詳細說明。

## 貳、廠商預設開啟支援 IPv6 意願調查

廠商預設開啟支援 IPv6 意願調查部分，將依照「市售網通產品調查」內容，歸納出國內主要寬頻分享器的品牌業者，安排和業者進行問卷及面訪，以了解國內主要網通產品業者，對於商品預設開啟支援 IPv6 的想法及規劃。此次約訪對象包含 ASUS (華碩) 及 D-Link (友訊)，訪談內容整理說明如下所述。

### (一) 寬頻分享器 (WIFI ROUTER) 開發新型號數及未來發展趨勢

目前 D-LINK 主要以中低階機種為主;ASUS 專心高階機種，兩家品牌業者皆認為 Mesh WiFi 產品有逐年增長趨勢，中高價寬頻分享器有取代低價產品趨勢。業者普遍認為產品週期平均而言，中低階產品約 2-3 年；中高階產品 1-1.5 年即需汰舊換新。

### (二) 寬頻分享器支援 IPv4/IPv6 雙軌網路服務且自動設定為 Dual Stack 之意願與困難

D-Link 和 ASUS 皆表示若預設自動啟用 IPv6，擔心客服量增加，侵蝕獲利。一般家用使用者不太注重是否支援 IPv6，但高階機種客戶就有技術背景會重視，業者目前有收到部份使用者自己啟用 IPv6，而客訴多半不是 IPv6 本身連線問題，而是網頁或載具功能不支援等。目前 D-Link 和 ASUS 兩業者表示新設計寬頻分享器幾乎皆支援 IPv6，只是尚未自動開啟。

### (三) 寬品分享器自動偵測使用者網路系統及產品標示協助消費者了解已成為基本外包裝標示內容

D-Link和ASUS皆認為此為基本功能，相較於前次訪談結果，業者已將自動偵測網路系統視為外包裝基本標示。

### (四) 寬頻分享器配合 IASP /有線電視業者進行測試及取得 IPv6 Ready Logo 之意願及困難

業者認為 IPv6 Ready Logo 對產品銷售沒有影響，業者多以自行測試處理，以固網測試支援為主，因有線電視具有地域性因素，較難一一進行測試。

### (五) 寬頻分享器支援 IPv6 以及預設為 PPPoEv4/v6 或 IPoEv4/v6(並採用單一帳號密碼)之意願與困難

D-Link 和 ASUS 皆表示若預設自動設定雙軌開啟，會導致部份不支援的內容上有開啟問題，及業者有部份功能目前只支援 IPv4，須等技術部門完成對應功能可支援 IPv6 後，才能進行產品預設啟動 IPv6。

## (六)5G 開通後的產品因應對策

D-Link 和 ASUS 皆認為對一般家用寬頻分享器市場影響不大，5G 和 WiFi 會相輔相成，家用 IoT 設備逐步增加，無法使用 5G 串聯，所以寬頻分享器還是有存在必要性。

## (七) 業者訪談總結

總結訪談內容，寬頻分享器目前普遍支援 IPv6，但對於自動開啟 IPv6 功能，為符合全球市場不同 IASP 系統，較難統一設計單一規格，因此若自動開啟 IPv6 會導致使用者遇到連網問題，衍生出處理客服費用；另也擔心資訊安全管控在 IPv6 目前仍有無法掌握之處。

觀察目前市場現況，國內寬頻分享器品牌業者多朝 Mesh 和高階機種發展，以台灣設計中國生產為主，低階機種多半由陸廠進軍，市場份額具有規模的寬頻分享器 (WIFI ROUTER) 業者，對支援 IPv6 的技術皆已成熟。內容支援是另一項須考量問題，一般使用者較不關心是否支援 IPv6，大型內容供應商普遍支援 IPv6。值得注意的是，低階機種由陸廠侵蝕情況下，加上資訊安全技術在 IPv6 實作上仍待強，在提升 IPv6 普及同時，同時需要重視 IPv6 資安問題。

以上寬頻分享器連通測試過程及結果，品牌業者訪談資料，請參閱附錄四有詳細說明。

# 第三章 國內 IASP 支援 IPv6 普查

國內 IASP 支援 IPv6 普查工作項目，主要目的是透過問卷調查，以掌握國內主要行動電信及固網業者，在支援 IPv6 的建置狀況及規劃；問卷設計方向將依據業者所提供的各類網路連線服務所需 IP 使用情境的不同，如光纖 (Fiber To The x，FTTx) 上網、Co-location/IDC 服務、雲端 (Cloud) 服務..等，針對各項服務在支援 IPv6 的整備程度進行調查，以了解國內 IPv6 普及狀況，並預估未來可能發展。國內主要行動電信業者，由民國 107 年開始陸續開通，並預設支援 IPv6 網路服務，台灣之星也在今 (109) 年 8 月後陸續開通支援 IPv6，因此本次問卷調查內容並未提列 4G 服務項目。

針對國內行動網路及固網 IASP 支援 IPv6 問卷調查，調查對象包含 5 家行動電信業者 (中華電信、台灣大哥大、遠傳電信、亞太電信及台灣之星) 及 2 家固網業者 (新世紀資通、台灣固網)，以下將就此分項工作成果說明。

IASP 支援 IPv6 調查，是以問卷方式進行，調查內容包含業者在各項網路服務支援 IPv6 程度、預計商用服務上線時程及該服務之設備支援 IPv6 建置準備程度等方向。以期能掌握業者部署狀況及提供服務時程計畫。本次固接網路及行動電信 IASP 業者調查共回收 7 份問卷，以下就問卷內容，彙整統計業者回覆結果，並進行分項統計分析及說明。

下表為 IASP 業者是否有 IPv4 位址面臨不足的狀況，針對此問題統計業者回覆結果如下表所示 ：

表 17、統計 IASP 業者是否有 IPv4 位址面臨不足的問題

| IASP 問卷調查內容 | 中華電信 | 台灣大哥大 | 亞太電信 | 遠傳電信 | 台灣之星 | 台灣固網 | 新世紀資通 | 總計 |
|---|---|---|---|---|---|---|---|---|
| 貴公司 IPv4 位址會在何時面臨不足？ | | | | | | | | |
| 沒有 IPv4 位址不足的問題 | | | | | ✓ | | | 1 |
| 預期在西元__？__年發生 IPv4 位址不足 | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | 6 |
| 貴公司是否已在進行 IPv4 位址不足的相關策略? | | | | | | | | |
| 沒有進行 IPv4 位址不足相關策略，請問原因為何? | | | | | | | | 0 |
| 已在進行 IPv4 位址不足相關策略，以下哪些是在進行的項目 (複選) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | 7 |
| 使用 CGNAT 核發 Private/Shared Address Space IPv4 位址給用戶 | ✓ | ✓ | ✓ | ✓ | ✓ | | | 5 |
| 減少各項服務 IPv4 核發數量或以價制量 | | | | ✓ | | ✓ | ✓ | 3 |
| 回收用戶閒置 IPv4 位址 | ✓ | | ✓ | ✓ | | ✓ | ✓ | 5 |
| 從其他 ISP 中取用 IPv4 位址 | | | | | | | | 0 |
| 配發用戶 IPv6 位址提供用戶 Native IPv6 連線服務 | | | ✓ | ✓ | | | | 2 |
| 其他 | ✓ | | | | | | | 1 |

## 一. 貴公司 IPv4 位址會在何時面臨不足？

IASP 業者對於是否有 IPv4 位址面臨不足的問題，在回收的 7 份問卷中，台灣大哥大回覆在西元 2017 年 (民國 106 年) ，即 3 年前就已經有 IPv4 位址不足的情況，是最早面臨 IPv4 資源不足的業者。行動業者亞太電信，預期於明 (110) 年，將面臨 IPv4 位址不足的情況，相較去 (108) 年預估為西元 2020 年 (民國 109 年) ，其 IPv4 資源不足的狀況稍微緩解。而中華電信預期西元 2022 年 (民國 111 年) ，將發生 IPv4 位址不足的情況，相較前 (107) 年預估為西元 2020 年 (民國 109 年) 將出現 IPv4 短缺，目前因為行動網路及固接網路都已經

支援 IPv4/IPv6 雙協定網路服務，而減緩 IPv4 需求，讓 IPv4 資源短缺的問題較為和緩。遠傳電信也因為開始支援 IPv6 讓 IPv4 資源短缺的時程延後。只有台灣之星回覆〝沒有 IPv4 不足的問題〞。業者回覆資訊統計如下表所示：

表 18、IASP 業者預期面臨 IPv4 不足時程表

| 預期面臨 IP 不足時程 | IASP 業者 | 總計 | 比例 |
|---|---|---|---|
| 沒有 IPv4 位址不足的問題 | 台灣之星 | 1 | 14.3% |
| 西元 2017 年 (民國 106 年) | 台灣大哥大 | 1 | 14.3% |
| 西元 2020 年 (民國 109 年) | 台灣固網 | 1 | 14.3% |
| 西元 2021 年 (民國 110 年) | 亞太電信 | 1 | 14.3% |
| 西元 2022 年 (民國 111 年) | 中華電信、遠傳電信、新世紀資通 | 3 | 42.8% |
| **總　計** | | **7** | **100%** |

## 二. 貴公司是否已在進行 IPv4 位址不足的相關策略?

下表針對有關 IASP 業者，目前是否已在進行 IPv4 位址不足相關策略統計表。由問卷回覆結果可看出，所有業者都在積極進行 IPv4 位址不足相關策略。其中業者主要採取的策略為〝使用 CGNAT 核發 Private/Shared Address Space IPv4 位址給用戶〞及〝回收用戶閒置 IPv4 位址〞，2 個項目所佔比例都為約 71%；此外中華電信在〝其他〞的選項回覆如下：

- 上網服務已導入 Dual stack (已經支援 IPv4/IPv6 雙軌服務)。

下圖根據 IASP 業者的問卷回覆表，統整列出有關業者對於 IPv4 位址不足相關策略，已經進行因應項目統計圖。目前中華電信、台灣大哥大、遠傳電信、亞太電信及台灣之星 5 家行動電信業者都已經支援 IPv4/IPv6 雙協定網路服務，其中以中華電信 IPv6 使用率最高目前

已經超過 88%，遠傳電信 IPv6 使用率超過 75%，台灣大哥大 IPv6 使用率超過 65%，亞太電信也超過 50%的比率是以 IPv6 連網。

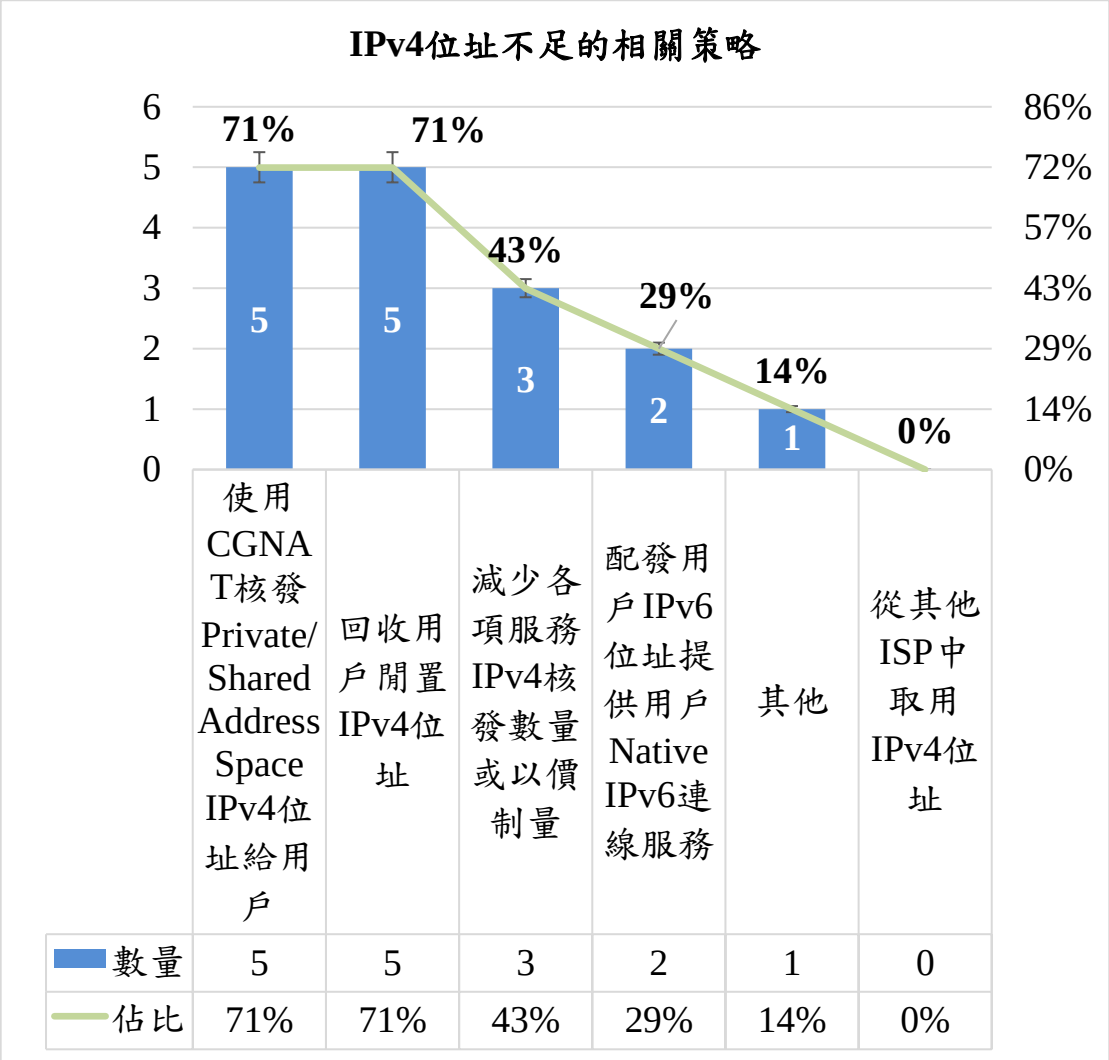



圖 42、IASP 業者對於 IPv4 位址不足所進行相關策略統計圖

## 三. 若貴公司未提供 IPv6 服務考慮的原因為何呢？

目前調查行動電信業者中有 4 家包含中華電信、台灣大哥大、亞太電信及遠傳電信，都已經提供使用者 IPv6 的連線服務，且使用率已經相當高。另外台灣之星回覆於今 (109) 年〝已計畫開放 IPv6 行動上網服務並持續進行中〞。觀察台灣之星整體 IPv6 使用率雖然不高，

但已經陸續有使用者可以 IPv6 連網，今 (109) 年國內行動電信業務完成全面支援 IPv4/IPv6 雙軌網路服務普行階段性任務。

固接網路部分，中華電信已提供部分家庭用戶可以 IPv6 連網，且新申裝用戶預設開啟支援 IPv6，企業用戶可以根據業者需求提供 IPv6 網路服務。台灣固網及新世紀資通針對尚未提供 IPv6 服務考量原因，提出包含以下說明：

- 目前業務以 IPv4 為主。 (台灣固網、新世紀資通)
- 服務升級 IPv6 所需的成本大於使用 IPv4 的成本。(新世紀資通)
- 目前公司大部分軟硬體設備不支援 IPv6。 (新世紀資通)
- 提供 IPv6 不會增加收入。 (新世紀資通)

支援 IPv6 對 IASP 而言並沒有直接收入，而是間接影響公司後續的營運發展及創新服務需求，因此技術部門和決策者可能會有不同的想法，也影響 IPv6 推展的進度，這也是 IPv6 網路服務已經推動超過 20 年，但一直到近年來全球對 IPv6 的部署才趨於積極，主要也是全球 IPv4 短缺問題越來越嚴重，IASP 因應 5G 及物聯網創新服務需求，必須向下一代網路環境遷移。

## 四. 貴公司的 IPv6 位址申請及 IPv6 路由狀況為何？

下表根據 IASP 業者對於 IPv6 位址申請及 IPv6 路由狀況的問題回覆統計表，不論是經營行動電信或固接網路業者，依照業者回覆來看，目前 7 家業者都〝已申請 IPv6 位址且將 IPv6 放在全球路由〞，且設備支援 IPv6 整備達成率為 100%。問卷回覆統計資料請參考下表統計結果。

表 19、IASP 業者問卷統計 IPv6 位址申請及 IPv6 路由狀況

| IASP 問卷調查內容 | 中華電信 | 台灣大哥大 | 亞太電信 | 遠傳電信 | 台灣之星 | 台灣固網 | 新世紀資通 | 總計 |
|---|---|---|---|---|---|---|---|---|
| 貴公司的 IPv6 位址申請及 IPv6 路由狀況為何？ | | | | | | | | |
| 尚未申請 IPv6 位址，預計西元_____年申請 IPv6 | | | | | | | | 0 |
| 已申請 IPv6 位址，但尚未將 IPv6 放在全球路由，預計西元_____年將 IPv6 放在全球路由 | | | | | | | | 0 |
| 已申請 IPv6 位址且將 IPv6 放在全球路由。 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | 7 |

下圖根據IASP 業者問卷調查回覆關於業者 IPv6 位址申請及 IPv6 路由狀況的統計圖：

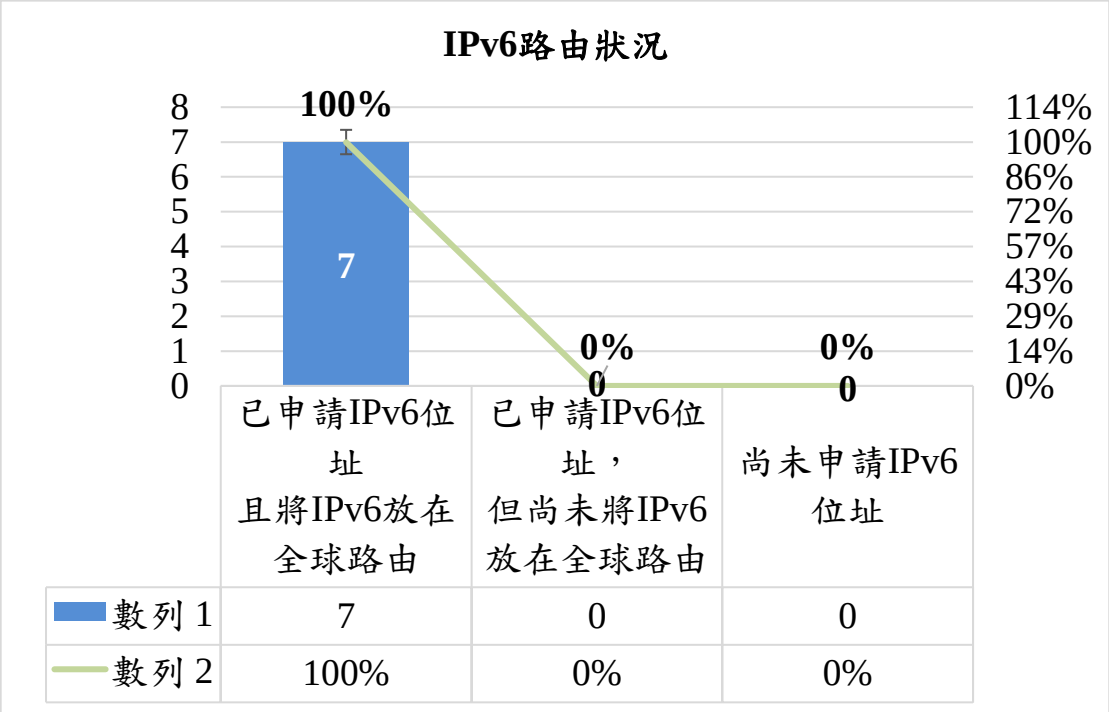



圖 43、IASP 業者問卷 IPv6 位址申請及 IPv6 路由狀況統計圖

## 五. 請問貴公司骨幹及各項產品提供IPv6網路服務設備支援狀況、時程及相關規劃為何？

下表根據IASP業者，對於骨幹及各項產品提供IPv6網路服務設備支援狀況、時程及相關規劃的問題項目回覆統計表，依照IASP業者回覆來看，其中業者針對其骨幹所用路由設備之IPv6支援能力，目前調查7家IASP業者在這部分的整備狀態都已經達到全部設備支援IPv6。而關於骨幹提供IPv6連網服務的時程及相關規劃，台灣之星回覆今(109)年將提供IPv6，其他6家業者包含中華電信、台灣大哥大、亞太電信、遠傳電信、台灣固網及新世紀資通都勾選已經將服務上線；目前調查7家業者網路骨幹都已經支援IPv6網路服務。

另外IASP服務調查，分為光纖(FTTx)上網、Co-Location/IDC服務、雲端(Cloud)服務及PWLAN無線上網等服務類別，以下針對各項服務，統計IASP提供IPv6網路服務設備支援狀況、時程及相關規劃，描述如下：

### (一) 光纖(FTTx)上網

目前調查7家業者，其中中華電信、亞太電信、台灣固網及新世紀資通共4家業者有提供固網光纖上網服務，目前亞太電信在光纖上網服務設備IPv6的支援能力已經達到100%支援，相較於去(108)年業者的準備度已經更為完善；而中華電信在光纖上網服務網路設備之IPv6支援能力還未達到全部設備都支援IPv6。針對中華電信固網光纖(FTTx)上網整備情形調查，其中主要是L3 Switch (HiNet接取設備專線路由器)及家庭閘道器(Home Gateway，HGW)尚未全部支援；目前L3 Switch約完成95.8%設備支援IPv6，和去(108)年問卷回覆約62.5%支援IPv6狀況已經有大幅改善；而Home Gateway支援IPv6比例也由去(108)年約

60.3%成長到約 68.2%，這也反映在中華電信光纖用戶上網 IPv6 使用比例在穩定成長中。

而台灣固網則是 BRAS (broadband remote access server，寬頻遠端接入系統) 設備上目前完全無法支援 IPv6。且根據業者回覆光纖網路服務目前並無支援 IPv6 計畫。新世紀資通仍有部分 Radius Server 設備無法支援 IPv6。但在光纖網路服務已經可支援 IPv6 予企業用戶使用。

下表整理 4 家 IASP 業者在光纖網路服務提供 IPv6 時程統計資料：

表 20、IASP 業者光纖上網提供 IPv6 時程表

| 光纖上網提供 IPv6 時程 | IASP 業者 | 總計 | 比例 |
|---|---|---|---|
| 已提供 | 中華電信、新世紀資通 | 2 | 50% |
| 西元 2021 年 (民國 110 年) 以後 | 亞太電信 | 1 | 25% |
| 無計畫導入 | 台灣固網 | 1 | 25% |
| **總計** | | **4** | **100%** |

### (二) Co-location/IDC 服務

根據業者問卷回覆中華電信、亞太電信台灣固網及新世紀資通共 4 家業者有提供 Co-location/IDC 網路服務，目前 4 家業者在 Co-location/IDC 服務所使用的網路設備 IPv6 支援能力，已經完成全部設備支援 IPv6，且 4 家業者都可提供給企業用戶使用支援 IPv6 網路服務。另外台灣大哥大、遠傳電信及台灣之星，為行動電信業者並無經營此項業務。下表為 IASP 業者 Co-location/IDC 服務提供 IPv6 時程表統計資料：

表 21、IASP 業者 Co-location/IDC 服務提供 IPv6 時程表

| Co-location/IDC 服務提供 IPv6 時程 | IASP 業者 | 總計 | 比例 |
|---|---|---|---|
| 已提供 | 中華電信、亞太電信、台灣固網及新世紀資通 | 4 | 100% |

### (三) 雲端 (Cloud) 服務

針對雲端 (Cloud) 服務目前調查業者中有中華電信、台灣固網及新世紀資通共 3 家業者經營此項業務。中華電信此服務網路設備之 IPv6 支援能力，已經達成 100%支援。相較於去 (108) 年調查回覆尚有極少部分防火牆 (Firewall) 及伺服器負載平衡 (Server Load Balance，SLB) 尚未支援 IPv6 情況有所改善；目前此服務已經提供給企業用戶使用，可以根據客戶需求完全支援 IPv6 網路服務。台灣固網在雲端服務部分目前正在進行 IPv6 服務測試，預計於西元 2021 年 (民國 110 年) 完成測試，但服務正式上線時程業者並未明確回覆。新世紀資通在設備上已經達到 100% 支援 IPv6，同時正式提供給用戶申請使用。IASP 業者雲端服務提供 IPv6 時程，請參閱下表統計資料：

表 22、IASP 業者雲端服務提供 IPv6 時程表

| 雲端服務提供 IPv6 時程 | IASP 業者 | 總計 | 比例 |
|---|---|---|---|
| 已提供 | 中華電信、新世紀資通 | 2 | 67% |
| 西元 2021 年 (民國 110 年) | 台灣固網 | 1 | 33% |
| **總計** | | **3** | **100%** |

### (四) PWLAN 無線上網

根據調查結果目前有中華電信及遠傳電信共 2 家業者有支援 PWLAN (Public Wireless Local Area Network，公眾無線區域網路)

無線上網服務。針對中華電信 PWLAN 無線上網整備情形，目前服務網路設備之 IPv6 支援能力，只有部分 WiFi Gateway 尚未完成全部設備支援能力，但此設備支援 IPv6 比例已經達到 99% 以上，接近完全支援；此服務已經正式上線，可讓用戶使用 IPv6 連線上網。

而遠傳電信支援 PWLAN 無線上網服務部分，目前此服務所採用的〝WiFi Gateway/Controller〞及〝DHCP Server〞設備並不支援 IPv6，且此服務並無計畫導入支援 IPv6，根據業者問卷回覆因〝此服務屬於非收費性質的加值服務，考量投資效益不高，故無提供 IPv6 計畫〞。

其他行動電信業者包含台灣大哥大、亞太電信及台灣之星，並未提供公眾無線區域網路上網服務。下表提列 IASP 業者 PWLAN 無線上網提供 IPv6 時程資訊：

表 23、IASP 業者 PWLAN 無線上網提供 IPv6 時程表

| PWLAN 無線上網提供 IPv6 時程 | IASP 業者 | 總計 | 比例 |
|---|---|---|---|
| 已提供 | 中華電信 | 1 | 50% |
| 無計畫導入 | 遠傳電信 | 1 | 50% |
| **總計** | | **2** | **100%** |

下表針對本次調查 7 家 IASP 業者，對上列各項服務在設備及提供服務時程回覆結果彙整資訊：

表 24、IASP 業者提供 IPv6 支援時程統計表

| IASP 問卷調查內容 | 中華電信 | 台灣大哥大 | 亞太電信 | 遠傳電信 | 台灣之星 | 台灣固網 | 新世紀資通 | 總計 |
|---|---|---|---|---|---|---|---|---|
| 請問貴公司骨幹及各項產品提供 IPv6 網路服務設備支援狀況、時程及相關規劃為何？ (複選) | | | | | | | | |
| (一). 骨幹所用路由設備之 IPv6 支援能力為何? | 100% | 100% | 100% | 100% | 100% | 100% | 100% | |
| 提供 IPv6 的時程及相關規劃? | | | | | | | | |
| 已提供 | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | **6** |
| 西元 2020 年 (民國 109 年) | | | | | ✓ | | | **1** |
| 西元 2021 年 (民國 110 年) | | | | | | | | **0** |
| 西元 2021 年 (民國 110 年) 之後 | | | | | | | | **0** |
| 若無計畫導入，請說明原因 | | | | | | | | **0** |
| (二). 各項服務 (請填寫貴公司有提供的服務項目) | | | | | | | | |
| 光纖 (FTTx) 上網 | | | | | | | | |
| 1. 服務所用網路設備之 IPv6 支援能力為何？ | <100 % | × | 100% | × | × | <100 % | <100 % | |
| 2. 服務是否使用 CGNAT 核發 Private/Shared Address Space IPv4 位址給用戶? | | | | | | | | |
| 否 | | | ✓ | | | ✓ | | **2** |
| 是，若回答是，此服務一個 Public IP 給客戶的比例 | | | | | | | | **0** |
| 3.提供 IPv6 服務的時程? | | | | | | | | |
| 已提供，請填寫此服務的 IPv6 帳號數/用戶數 | ✓ | | | | | | ✓ | **2** |
| 西元 2020 年 (民國 109 年) 提供 | | | | | | | | **0** |
| 西元 2021 年 (民國 110 年) 提供 | | | | | | | | **0** |
| 西元 2021 年 (民國 110 年) 之後提供 | | | ✓ | | | | | **1** |
| 請說明目前進行的階段 | | | | | | | | |
| 規劃中，預計西元_____年完成 | | | | | | | | **0** |
| 測試中，預計西元_____年完成 | | | | | | | | **0** |
| 若無計畫導入，請說明原因 | | | | | | ✓ | | **0** |

| IASP 問卷調查內容 | 中華電信 | 台灣大哥大 | 亞太電信 | 遠傳電信 | 台灣之星 | 台灣固網 | 新世紀資通 | 總計 |
|---|---|---|---|---|---|---|---|---|
| Co-location/IDC 服務 | | | | | | | | |
| 1. 服務所用網路設備之 IPv6 支援能力為何？ | 100% | × | 100% | × | × | 100% | 100% | |
| 2. 提供 IPv6 服務的時程? | | | | | | | | |
| 已提供，請填寫此服務的 IPv6 帳號數/用戶數 | ✓ | | ✓ | | | ✓ | ✓ | **4** |
| 西元 2020 年 (民國 109 年) 提供 | | | | | | | | **0** |
| 西元 2021 年 (民國 110 年) 提供 | | | | | | | | **0** |
| 西元 2021 年 (民國 110 年) 之後提供 | | | | | | | | **0** |
| 請說明目前進行的階段 | | | | | | | | |
| 規劃中，預計西元_____年完成 | | | | | | | | **0** |
| 測試中，預計西元_____年完成 | | | | | | | | **0** |
| 若無計畫導入，請說明原因 | | | | | | | | **0** |
| 雲端 (Cloud) 服務 | | | | | | | | |
| 1. 服務所用網路設備之 IPv6 支援能力為何？ | 100% | × | × | × | × | 100% | 100% | |
| 2. 提供 IPv6 服務的時程? | | | | | | | | |
| 已提供，請填寫此服務的 IPv6 帳號數/用戶數 | ✓ | | | | | | ✓ | **2** |
| 西元 2020 年 (民國 109 年) 提供 | | | | | | | | **0** |
| 西元 2021 年 (民國 110 年) 提供 | | | | | | ✓ | | **1** |
| 西元 2021 年 (民國 110 年) 之後提供 | | | | | | | | **0** |
| 請說明目前進行的階段 | | | | | | | | |
| 規劃中，預計西元_____年完成 | | | | | | | | **0** |
| 測試中，預計西元_____年完成 | | | | | | ✓ | | **1** |
| 若無計畫導入，請說明原因 | | | | | | | | **0** |
| PWLAN 無線上網 | | | | | | | | |
| 1. 服務所用網路設備之 IPv6 支援能力為何？ | <100% | × | × | <100% | × | × | × | |

| IASP 問卷調查內容 | 中華電信 | 台灣大哥大 | 亞太電信 | 遠傳電信 | 台灣之星 | 台灣固網 | 新世紀資通 | 總計 |
|---|---|---|---|---|---|---|---|---|
| 2. 服務是否使用 CGNAT 核發 Private/Shared Address Space IPv4 位址給用戶? | | | | | | | | |
| 否 | | | | ✓ | | | | **1** |
| 是，若回答是，此服務一個 Public IP 給客戶的比例 | ✓ | | | | | | | **1** |
| 3.提供 IPv6 服務的時程? | | | | | | | | |
| 已提供，請填寫此服務的 IPv6 帳號數/用戶數 | ✓ | | | | | | | **1** |
| 西元 2020 年 (民國 109 年) 提供 | | | | | | | | **0** |
| 西元 2021 年 (民國 110 年) 提供 | | | | | | | | **0** |
| 西元 2021 年 (民國 110 年) 之後提供 | | | | | | | | **0** |
| 請說明目前進行的階段 | | | | | | | | |
| 規劃中，預計西元_____年完成 | | | | | | | | **0** |
| 測試中，預計西元_____年完成 | | | | | | | | **0** |
| 若無計畫導入，請說明原因 | | | | ✓ | | | | **1** |

根據上表 IASP 業者問卷回覆,下表針對業者所經營的不同業務，依業者現有之 IPv6 位址使用情境統計目前業者對各項服務是否已經提供 IPv6 連網服務統計結果。目前國內 IASP 除了行動電信業務已經全面支援 IPv6 外，Co-location/IDC 服務也是目前支援 IPv6 比例較高的業務項目，調查 4 家業者都已支援。其他服務如 PWLAN、雲端服務及光纖上網服務，不同業者因商業考量不同，提供 IPv6 時程規劃各異，目前國內以 IASP 龍頭中華電信，在各項服務支援 IPv6 的狀況最佳。下表整理 IASP 業者各項服務支援 IPv6 統計結果：

表 25、IASP 業者各項服務支援 IPv6 統計表

| 服務類別 | 已提供支援 IPv6 | 2021 年或之後計畫支援 IPv6 | 無計畫支援 IPv6 | 服務支援家數 | 已支援 IPv6 家數 |
|---|---|---|---|---|---|
| PWLAN | 中華電信 | x | 遠傳電信 | 2 | 1 |
| 雲端服務 | 中華電信、新世紀資通 | 台灣固網 | x | 3 | 2 |
| Co-location/ IDC 服務 | 中華電信、亞太電信、台灣固網、新世紀資通 | x | x | 4 | 4 |
| 光纖上網 | 中華電信、新世紀資通 | 亞太電信 | 台灣固網 | 4 | 2 |

## 六. 貴公司提供 IPv6 服務時，預計增加支出主要用在哪些項目？

下表根據本次調查 7 家 IASP 業者，對於有關支援 IPv6 預計增加支出項目回覆統計表，依照 IASP 業者回覆來看，最多的預算支出集中在〝更新硬體設備〞及〝更新相關軟體系統〞項目上為支援 IPv6 需要支出預算最多的部分，7 家業者中有 6 家選此項目，比例高達約 85.7%；其次為〝人員教育訓練〞，有 5 家選此項目，比例高達約 71.4%。若依該項目的平均權重計算，排名第一為〝更新硬體設備〞，其次為〝更新相關軟體系統〞，第 3 名為〝人員教育訓練〞。台灣之星在其他部分提列〝網路異動工程〞佔該公司為了支援 IPv6 需要支出預算次多項目。

表 26、IASP 業者問卷統計支援 IPv6 預計增加支出項目

| IASP 問卷調查內容 | 中華電信 | 台灣大哥大 | 亞太電信 | 遠傳電信 | 台灣之星 | 台灣固網 | 新世紀資通 | 總計 |
|---|---|---|---|---|---|---|---|---|
| 貴公司提供 IPv6 服務時，預計增加支出主要用在哪些項目(複選，請於括號內以 1, 2, 3,…標示出該項目所需經費之比重排名，其中 1 最高，2 次高，以此類推)？ | | | | | | | | |
| 更新硬體設備 | 1 | 1 | 1 | 1 | 1 | 1 | | **6** |
| 更新相關軟體系統 (例如 DNS/Radius/DHCP/Web/E-mail 等) | 2 | 1 | 2 | 2 | | 1 | 1 | **6** |
| 人員教育訓練 | 3 | 1 | 3 | 3 | 3 | | | **5** |
| IPv6 連線費用 | | | | 4 | | | | **1** |
| 其他，請說明_____ | | | | | 2 | | | **1** |

註：1, 2, 3,…標示出該項目所需經費之比重排名，其中 1 最高。排名 1 換算成權重 (weight) 指數 5，排名 2 換算成權重指數 4，以此類推。下圖顯示〝w=x〞，代表該選項權重加總；〝a=x〞代表平均權重。

下圖根據業者的問卷回覆，列出有關支援 IPv6 預計增加支出項目統計圖。

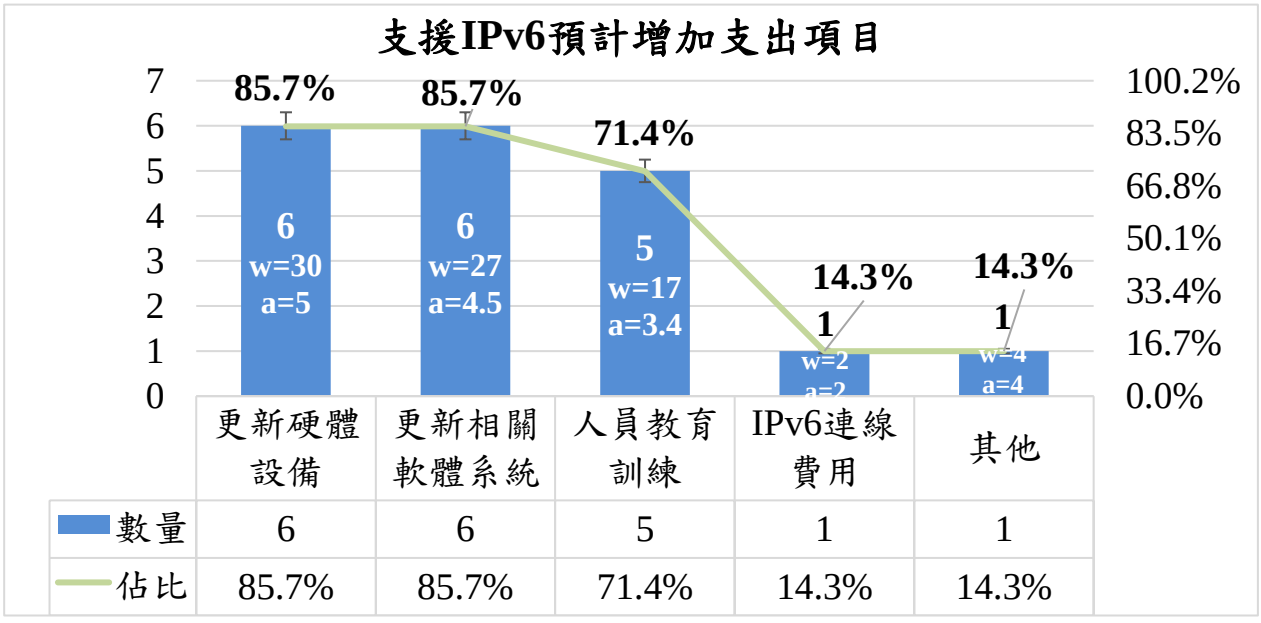



圖 44、IASP 業者問卷支援 IPv6 預計增加支出項目統計圖

## 七. 貴公司在 IPv6 可能面臨的問題有哪些？

下表根據 IASP 業者，對於有關支援 IPv6 可能面臨的問題項目回覆統計表，依照 IASP 業者回覆來看，業者最常遇到的問題是〝投入成本高〞，〝軟硬體支援度不足〞，及〝人員 IPv6 技術能力與管理經驗不足〞等 3 大問題比例約為 57%。另台灣大哥大及遠傳電信反應〝IPv6 無法達成公司原有 IPv4 各服務的功能〞，對其服務造成的影響整理如下所述：

- 〝管理功能〞上，位址資源配發管理。 (遠傳電信)
- 〝安全功能〞上，去 (108) 年台灣大哥大提及需新購防火牆才能達到 IPv4 NAT 阻擋外部主動連線功能。對業者而言將增加設備、人力建置及管理成本。 (台灣大哥大)

各家電信業者因為新服務上線，就技術掌握度可能隱藏一些未知因素，因此業者除了負擔本身技術設備問題外，也會擔心外部使用其服務設備等相關問題。中華電信在〝其他〞項目提列意見，詳細內容如下所述：

- IPv6 缺乏關鍵應用以及吸引用戶之誘因。 (中華電信)
- 國際及國內互連之 ISP 部分業者無提供 IPv6 路由互連。 (中華電信)
- 內容業者 IPv6 支援能力有待加強。 (中華電信)
- 用戶端設備不支援 IPv6。 (中華電信)
- 用戶端設備未開啟 IPv6 功能。 (中華電信)
- 如未藉由新建或汰舊換新機會順勢將 IPv6 導入，將增加額外導入成本。 (中華電信)

由以上資訊可知，IPv6 服務的完善需考慮整體環境，包含網路連

結提供者 IASP，資訊存取服務者 IDC、雲端服務等，通訊設備製造者，內容服務供應商 ICP，一直到終端使用者，都有相關連。

下表整理 IASP 業者問卷回覆，關於支援 IPv6 可能面臨的問題統計資訊；

表 27、IASP 業者問卷統計支援 IPv6 可能面臨的問題

| IASP 問卷調查內容 | 中華電信 | 台灣大哥大 | 亞太電信 | 遠傳電信 | 台灣之星 | 台灣固網 | 新世紀資通 | 總計 |
|---|---|---|---|---|---|---|---|---|
| 貴公司在 IPv6 可能面臨的問題有哪些 (複選) ？ | | | | | | | | |
| 投入成本高 | ✓ | ✓ | ✓ | | | | ✓ | 4 |
| 軟硬體支援度不足 | ✓ | ✓ | | | | ✓ | ✓ | 4 |
| IPv6 無法達成公司原有 IPv4 各服務的功能 (複選) | | ✓ | | ✓ | | | | 2 |
| 管理功能，例如_ | | | | ✓ | | | | 1 |
| 安全功能，例如_ | | ✓ | | | | | | 1 |
| 效能，例如_ | | | | | | | | 0 |
| 其他_ | | | | | | | | 0 |
| 人員 IPv6 技術能力與管理經驗不足 | | ✓ | ✓ | | | ✓ | ✓ | 4 |
| 廠商 IPv6 技術能力不足 | | | | | | ✓ | ✓ | 2 |
| 上游國際 ISP 無提供 IPv6 路由互連 | | | | | | | | 0 |
| 客戶使用 IPv6 服務會產生體驗 (QoE) 不佳之問題 | | | | | | | | 0 |
| 其他 _ | ✓ | | | | | | | 1 |
| 本公司目前並無上述問題 | | | | | ✓ | | | 1 |

下圖根據 IASP 業者的問卷回覆，列出有關支援 IPv6 可能面臨的問題項目的統計圖。

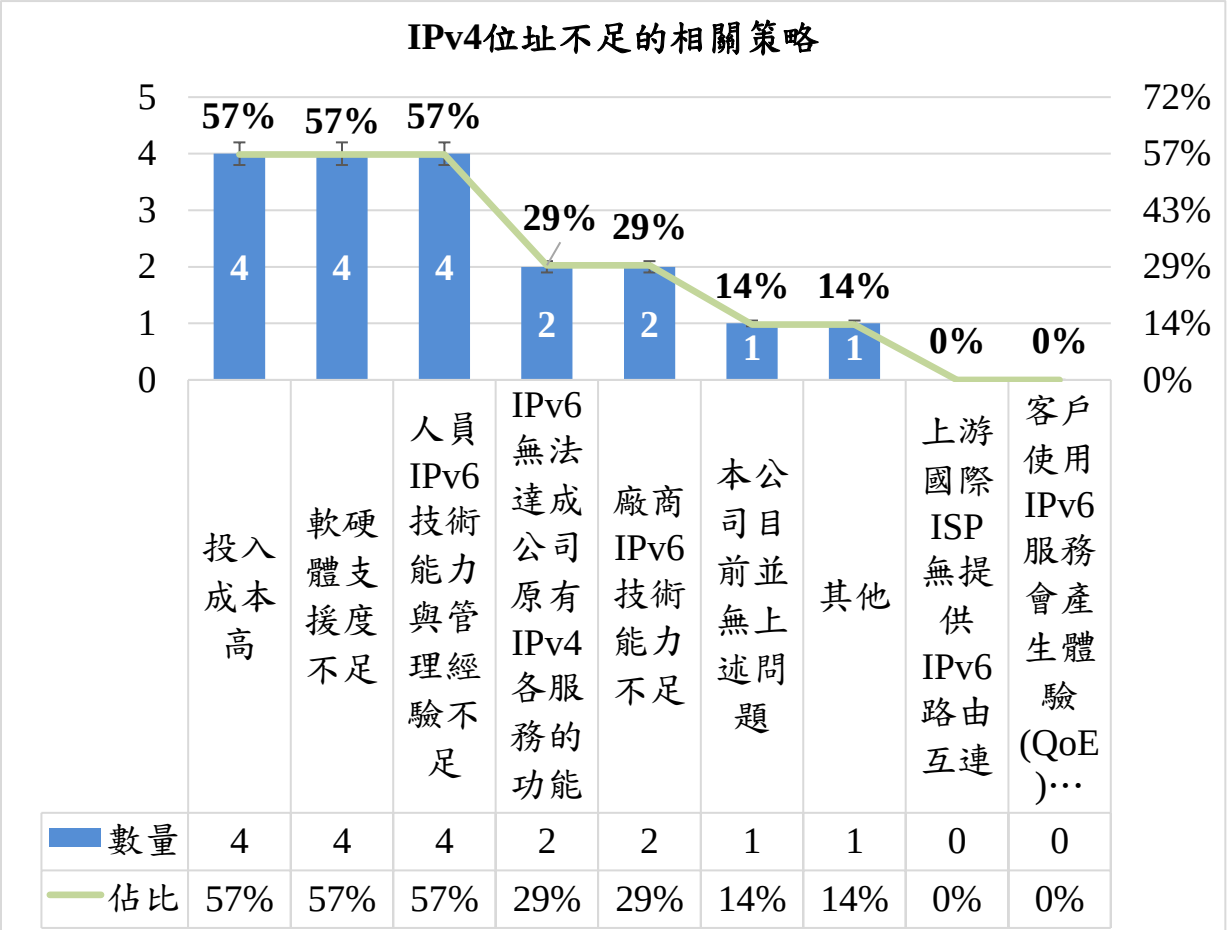



圖 45、IASP 業者問卷支援 IPv6 可能面臨的問題統計圖

## 八. 貴公司是否認為在 IPv6 網路發展上有政府可以協助之項目？

下表根據 IASP 業者，對於有關支援 IPv6 網路發展上希望政府協助項目回覆統計表，依照 IASP 業者回覆來看，就政府可以協助之項目上，大多數業者都希望政府能夠〝提供獎勵補助措施〞及〝提供投資抵減優惠〞，以提高業者的投資意願，加速提高業者更新技術服務的腳步。業者所提建議如下：

- ◆ 提供獎勵補助措施，例如 IPv6 設備採購稅金減免 (韓國或日本案例減免業者 3~5%可做為參考) 、補助固網寬頻升級 IPv6

實施計畫、降低營所稅稅率鼓勵服務創新等獎勵補助措施。(中華電信)

- ◆ 提供獎勵補助措施,例如更新軟硬體投資可抵減稅負或列為額度的獎勵補助。 (遠傳電信)
- ◆ 提供獎勵補助措施，例如獎勵服務升級。 (台灣之星 )
- ◆ 提供投資抵減優惠,例如IPv6相關研究與發展計畫研發補助、設備加速折舊以及人才培訓等投資抵減項目。 (中華電信)

此外在問卷〝其他〞選項中，業者提到多項意見，希望政府能提供相關協助，詳細如下所列：

- ● 協助本公司推動主要相關網通業者市售設備預設支援IPv6功能。 (中華電信)
- ● 協助本公司推廣企業用戶、內容業者導入IPv6。 (中華電信)
- ● 協助尋找IPv6創新應用服務發展商機，增加業者導入IPv6的動能，有助於帶動國內IPv6發展與普及。 (中華電信)
- ● 協助產、官、學、研之資源整合，建立IPv6產業價值鏈，創造新客戶及新市場。 (中華電信)
- ● 促進跨業合作，將有關物聯網產業之產品及技術加以整合至IPv6以創造更大的產業效益。 (中華電信)

以上建議事項和本計畫所規劃的推動及執行方向雷同,目前國內IASP 在 IPv6 網路環境建置逐漸成熟之際，能持續就網通設備、企業用戶、內容業者、物聯網應用加強推動力道，才能讓國內 IPv6 網路環境逐步發展完善。

下表根據 IASP 業者問卷回覆，整理支援 IPv6 網路發展上業者希望政府協助項目。

表 28、IASP 業者問卷統計支援 IPv6 網路發展上希望政府協助項目

| IASP 問卷調查內容 | 中華電信 | 台灣大哥大 | 亞太電信 | 遠傳電信 | 台灣之星 | 台灣固網 | 新世紀資通 | 總計 |
|---|---|---|---|---|---|---|---|---|
| 貴公司是否認為在 IPv6 網路發展上有政府可以協助之項目 (複選)？ | | | | | | | | |
| 提供獎勵補助措施，例如_ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | **7** |
| 提供投資抵減優惠，例如_ | ✓ | ✓ | ✓ | | | ✓ | ✓ | **5** |
| 無需要政府協助 | | | | | | | | **0** |
| 其他 _ | ✓ | | | | | | | **1** |

下圖根據 IASP 業者的問卷回覆，列出有關支援 IPv6 發展上希望政府協助項目的統計圖。

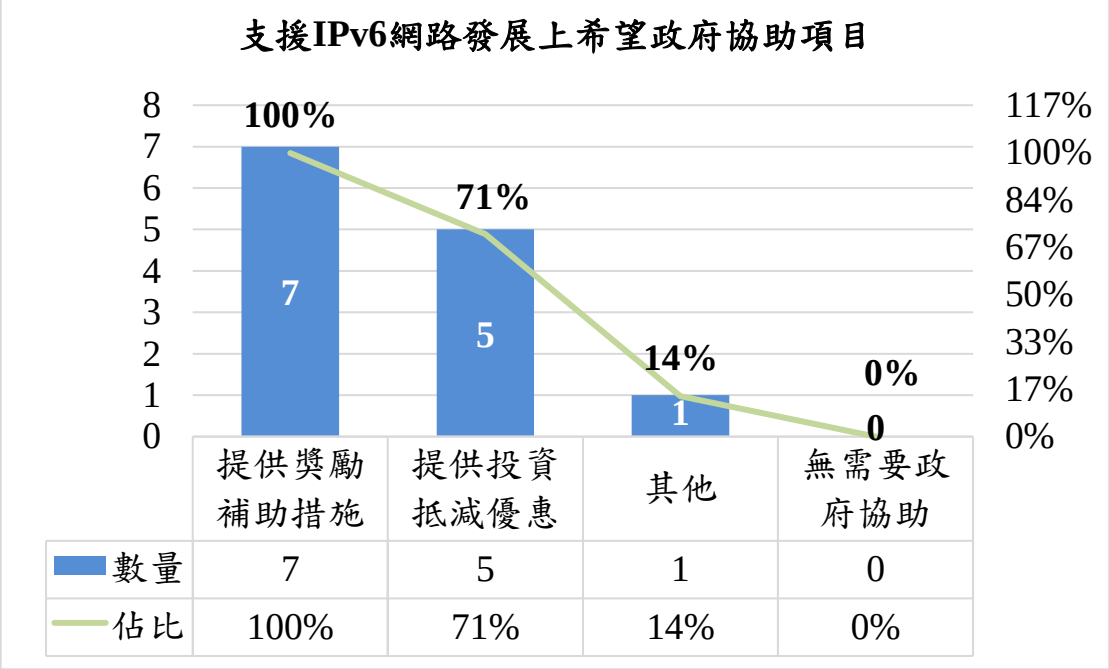



圖 46、IASP 業者問卷支援 IPv6 網路發展上希望政府協助項目

## 九. 貴公司若提供用戶 IPv6 網路連線服務，將會如何提供配發用戶 IPv6 位址？

下表根據 IASP 業者，對於有關支援 IPv6 連線服務位址配發方式項目回覆統計表，依照業者回覆來看，7 家業者中，主要支援〝動態配發 IPv6 位址或網段 (Prefix) 〞，但中華電信及新世紀資通可根據客戶需求選擇〝固定配發 IPv6 位址或網段 (Prefix) 〞。

表 29、IASP 業者統計支援 IPv6 連線服務位址配發方式

| IASP 問卷調查內容 | 中華電信 | 台灣大哥大 | 亞太電信 | 遠傳電信 | 台灣之星 | 台灣固網 | 新世紀資通 | 總計 |
|---|---|---|---|---|---|---|---|---|
| 貴公司若提供用戶 IPv6 網路連線服務，將會如何提供配發用戶 IPv6 位址？ | | | | | | | | |
| 動態配發 IPv6 位址或網段 (Prefix) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | **7** |
| 固定配發 IPv6 位址或網段 (Prefix) | ✓ | | | | | | ✓ | **2** |
| 其他 _ | | | | | | | | **0** |

下圖根據 IASP 業者的問卷回覆，列出有關支援 IPv6 連線服務位址配發方式統計圖。

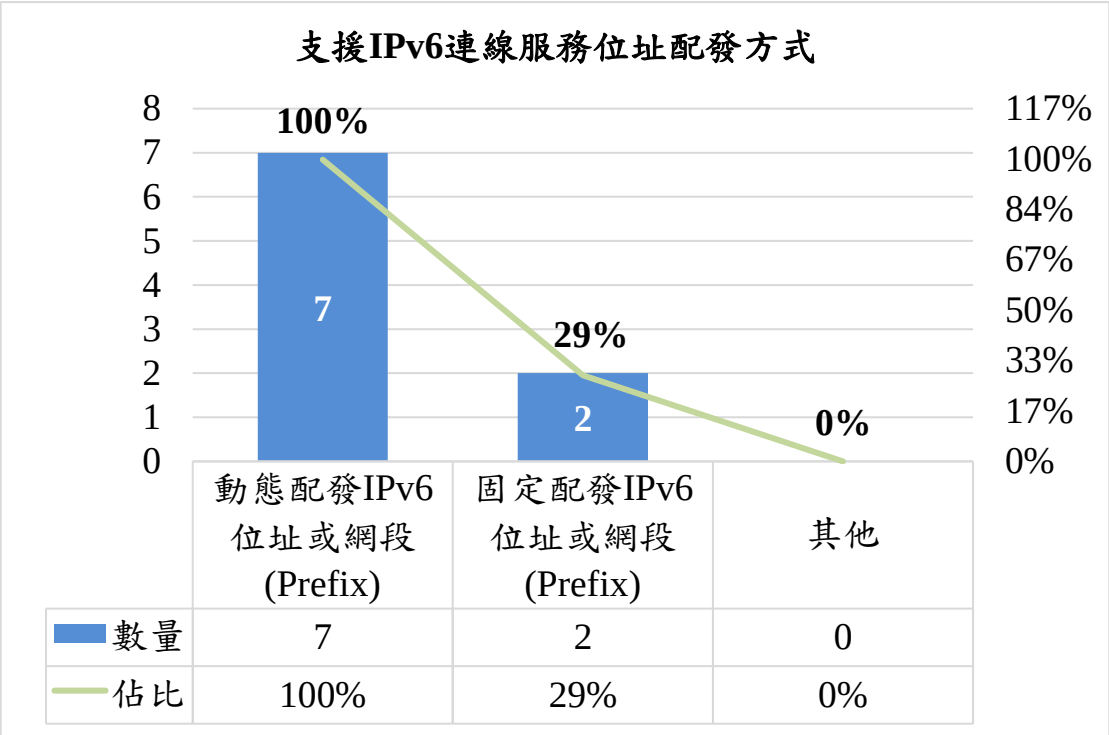



圖 47、IASP 業者支援 IPv6 連線服務位址配發方式統計圖

IASP 業者問卷調查表回覆內容，詳細請參考附錄一，檢附完整回覆資料。

今 (109) 年總體台灣 IPv6 使用率由年初約 42.5%，逐步上升來到約 50%，下半年維持在 47% ~ 50%使用率，全球排名在第 6 ~ 10 名之間。10 月份正式達成國內 IPv6 使用率過半的成就，完成 IPv6 推動歷程一項重要指標，讓國內網路環境逐漸往下一代 IPv6 網路世界邁進。下圖根據 APNIC 統計資料顯示，在今 (109) 年 10 月中台灣 IPv6 使用量測數據，IPv6 使用比例達到約 50.09%，全球排名第 6 名。[43~44]

圖 48、台灣 IPv6 使用量測數據圖

下表根據 APNIC 統計資料列出全球 IPv6 使用率排名前 30 國家，目前第 1 名為印度，印度因為數位化發展較晚，其可分配到的 IPv4 資源相對少，因此部分行動電信業者開始推展 4G 業務時即是採用 IPv6 網路協議，才造就印度 IPv6 高使用率。另外歐洲國家如比利時、德國、希臘等國家，在 IPv6 發展上已經相當久，目前這些國家 IPv6 使用率部分已經超過台灣，有些和台灣使用率相當。其他排在台灣前面還包含美國及馬來西亞等國家。全球有約 25 個國家 IPv6 使用率達 30%或以上。

表 30、全球 IPv6 使用率排名前 30 國家列表

Top 30 List

| SN | CC | Display Name | IPv6 % |
|---|---|---|---|
| 1 | IN | India | 69.77 |
| 2 | BE | Belgium | 60.21 |
| 3 | YT | Mayotte | 59.84 |
| 4 | MY | Malaysia | 52.88 |
| 5 | US | United States of America | 51.68 |
| 6 | TW | Taiwan | 50.09 |
| 7 | DE | Germany | 49.49 |
| 8 | GR | Greece | 48.68 |
| 9 | CH | Switzerland | 46.21 |
| 10 | VN | Vietnam | 44.97 |
| 11 | FR | France | 44.73 |
| 12 | GF | French Guiana | 43.52 |
| 13 | PR | Puerto Rico | 42.8 |
| 14 | JP | Japan | 40.92 |
| 15 | PT | Portugal | 37.28 |
| 16 | FI | Finland | 36.93 |
| 17 | MX | Mexico | 36.79 |
| 18 | LU | Luxembourg | 36.43 |
| 19 | GB | United Kingdom of Great Britain and Northern Ireland | 36.17 |
| 20 | TH | Thailand | 36.08 |
| 21 | UY | Uruguay | 35.45 |
| 22 | BR | Brazil | 34.42 |
| 23 | LK | Sri Lanka | 33.94 |
| 24 | AE | United Arab Emirates | 31.77 |
| 25 | MQ | Martinique | 31.01 |
| 26 | AU | Australia | 30.13 |
| 27 | HU | Hungary | 29.62 |
| 28 | GP | Guadeloupe | 29.53 |
| 29 | NL | Netherlands | 27.55 |
| 30 | CA | Canada | 27.45 |

2020-10-13

根據 APNIC 統計資料，台灣商用網路 IASP 業者 IPv6 連網比例如下圖顯示，目前以行動電信業者 IPv6 使用率佔最大宗，其中又以

中華電信行動網路IPv6使用率達約90%最高，其次為遠傳電信約78%，台灣大哥大緊追在後使用率約為67%，亞太電信也已經達到約55%，僅有台灣之星行動網路在今 (109) 年8月才陸續開始支援IPv6，使用率仍相當低只有0.1%。

固網部分一般主要分家庭用戶分以採用中華電信及Cable寬頻網路兩大系統，目前國內Cable寬頻網路業者都還未有正式提供IPv6商轉計畫，中華電信固網IPv6使用率已經達33.48%，呈現穩定成長趨勢。

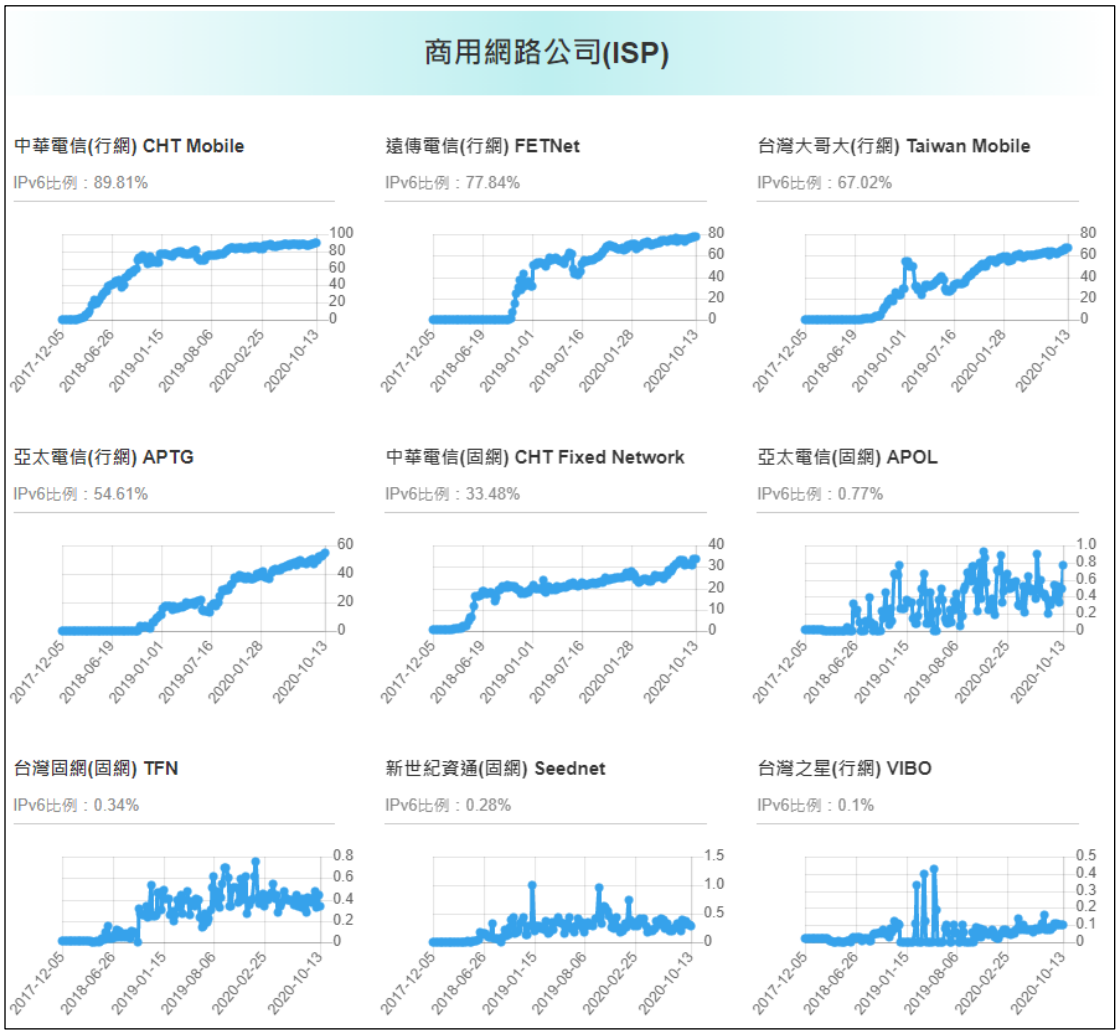



圖 49、台灣商用網路IASP業者IPv6連網比例

但政府及學術網路 IPv6 連網比例則較不理想，下圖根據 APNIC 統計數字顯示國發會 IPv6 使用率約為 8.4%，教育部 TANet IPv6 使用率約為 17.01%，尚有相當大成長空間。

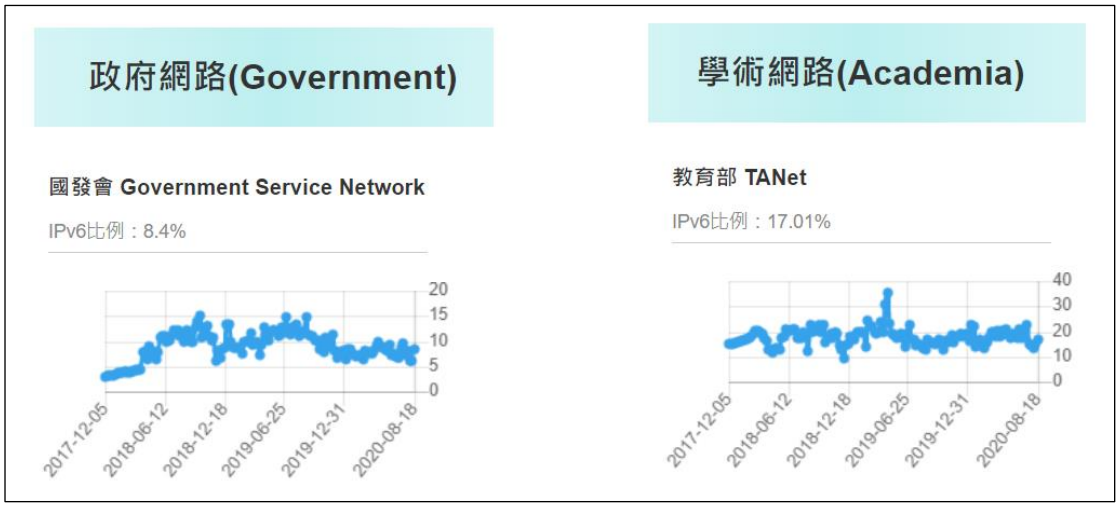



圖 50、台灣政府及學術網路 IPv6 連網比例

根據上述資料統整國內 IASP 之 IPv6 使用率，包含商用網路、政府網路及學術網路：

表 31、台灣主要 IASP 之 IPv6 連網比例

| 序號 | IASP | IPv6 使用率 |
|---|---|---|
| 1 | 中華電信 (行網) | 89.81% |
| 2 | 遠傳電信 (行網) | 77.84% |
| 3 | 台灣大哥大 (行網) | 67.02% |
| 4 | 亞太電信 (行網) | 44.61.% |
| 5 | 台灣之星 (行網) | 0.1% |
| 6 | 中華電信 (固網) | 33.48% |
| 7 | 亞太電信 (固網) | 0.35% |
| 8 | 新世紀資通 (固網) | 0.28% |
| 9 | 台灣固網 (固網) | 0.34% |
| 10 | 國發會 | 8.4% |
| 11 | 教育部 TANet | 17.01% |

中華電信於民國 107 年率先開啟行動網路正式支援 IPv6 服務，大規模對終端用戶預設開啟支援 IPv6，為國內 IPv6 使用率帶來相當亮眼成績，同一年也激勵遠傳電信及台灣大哥大加入支援 IPv6 網路服務行列，民國 107 年台灣贏得 IPv6 使用率成長名列全球第一的成就。民國 108 年亞太電信，也加入支援 IPv6 行列。今 (109) 年 8 月台灣之星陸續開始支援 IPv6 網路服務，國內 5 家行動網路業者，完成國內行動通訊全面進入支援 IPv4/IPv6 雙軌網路服務時代的重要里程碑，對台灣 IPv6 推動具有相當重要意義。[43]

# 第四章 Native IPv6 連網試驗環境建置

全球 IPv4 位址已經枯竭，電信業者 IPv4 位址資源短缺問題日益凸顯，IPv6 能夠提供大量的網路位址資源，是實現萬物互聯，促進科技數位化、網路化以及智慧化發展的關鍵要素。經過多年的發展，網路供應商在 IPv6 建置上逐漸普及，因此 IPv6 使用率亦快速成長。然而，IPv6 仍存在一些議題須持續關注，特別是在 IPv6 與 IPv4 網路互通上。

Native IPv6 亦可寫作 「IPv6-only」的網路，其代表意義為 IPv6 是該網路中唯一運行的 IP 協定。可視作以前 Native IPv4 網路的 IP 升級版。Native IPv6 網路之所以作為 Native IPv4 以及 Dual-Stack 環境的最終目標，主要原因在於運行 Dual-Stack 網路的維運和建置成本過高，且不同網路之間存在不少差異，加之 IPv4 位址用罄，因此建議大部分網路提供商完全關閉 IPv4，改以採納 Native IPv6 做為唯一 IP 協定，以符合國際發展趨勢。然而，雖然 IPv6 的佈署能滿足大部分應用程式的業務需求，但是，在短期內要從 Native IPv4 的環境遷移到 Native IPv6 環境，最大的挑戰在於服務對網路的支援性，並非所有服務提供商皆參與其中。其次面臨的挑戰包括對 Native IPv6 網路環境的安全性、管理方式及傳輸模式不了解。然而，隨著時代的發展，已經有許多大型企業建構了專有的應用程式支援 IPv6，但仍有許多服務提供商尚未完整支援，服務對 Native IPv6 網路的支援存在差異，又隨著 IPv6-only 的佈署不斷擴大，使得面向 Native IPv6 的過渡方式及營運面臨更大的挑戰。而 NAT64 及 464XLAT 被視為 Native IPv6 的過渡方案，乃因其提供支援用戶端不同的連線情境，即使服務尚無

支援 IPv6 服務，亦可升級用戶端及營運商設備至 IPv6 環境，可優先做為 ISP 佈署 Native IPv6 的方案，以符合未來網路發展趨勢。

目前已有部分國外業者實際採用 Native IPv6 環境，如，T-Mobile，即是以 464XLAT 技術作為過渡到 Native IPv6 網路的技術。此外，美國政府於今 (109) 年 11 月 19 日發布《完成向 IPv6 過渡》備忘錄，內容更新了有關聯邦政府營運部署和使用 IPv6 指南，希望加速遷移到 IPv6-only 的網路環境，也加強了 Native IPv6 的推行力道。

至於應用面上，Facebook 已經完成其內部網站連結是用 Native IPv6 做串接，此政策決定在於經過其技術團隊驗證，Native IPv6 可以提供更有效率的網路連結，給用戶更佳的服務體驗，也減少網路維運及管理的複雜度。

Native IPv6 不僅是網際網路演進升級的必然趨勢，更有助於網路產業融合發展、支撐服務創新應用的基礎，對於提升國家未來科技環境競爭優勢來說，IPv6 部署演進具有重要的戰略意義。本工作項目主要是透過建置 Native IPv6 連網環境，提供 464XLAT 即 CLAT/PLAT 位址轉換功能，並於有線與行動裝置測試實際用戶連線使用情況進行驗證。此各分項工作成果將敘述如下。

# 第一節 Native IPv6 試驗網路環境建置

## 一. Native IPv6 試驗網路環境架構規劃

NAT64 (Network Address Translation，網路位址轉換) 為 IPv4 到 IPv6 過渡時期的解決機制之一，配合 DNS64 就可提供 IPv6-only Client 與 IPv4-only Server 之互連，也可提供 IPv6-only 主機與 IPv4-only 主機之間進行點對點傳輸服務，且不需要對 IPv6 或 IPv4 設備做任何變

動。DNS64 則主要是配合 NAT64 工作，主要是將 DNS 查詢訊息中的 A 記錄 (IPv4 位址) 合成到 AAAA 記錄 (IPv6 位址) 中，返回合成的 AAAA 資源記錄給 IPv6 端的用戶。DNS64 也解決了 NAT-PT (Network Address Translation-Protocol Translation) 中的 DNS-ALG (Domain Name System-Application Layer Gateway) 存在的缺陷。下圖為 NAT64/DNS64 網路架構。

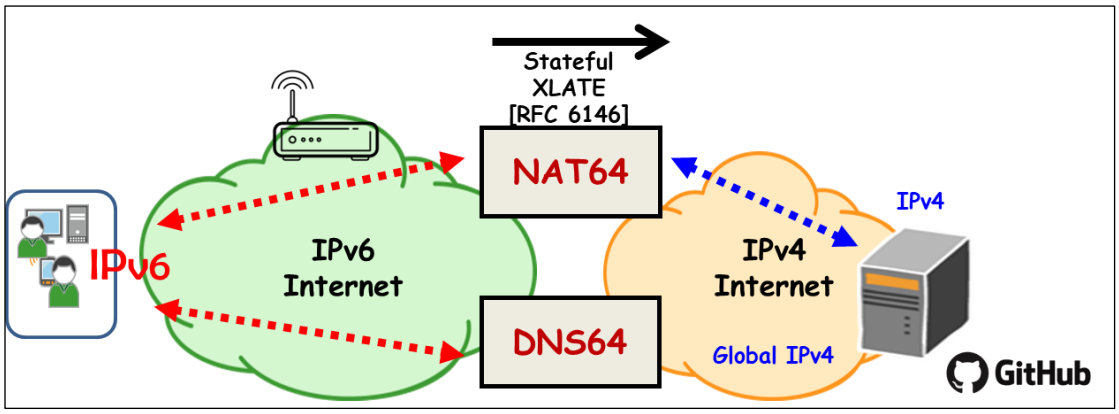



圖 51、NAT64/DNS64 網路架構

NAT64 主要針對位址及協定做轉譯，其中位址轉譯包含 Address 和 Port 兩部分，而協定轉譯部分主要是根據 SIIT (Stateless IP/ICMP Translation)，為了讓 IPv4 位址與 IPv6 位址能夠對應，NAT64 擁有 IPv4 Address pool 與 IPv6 Address pool，如果需要讓 IPv4 位址對應到 IPv6 位址，NAT64 將從 IPv6 Address pool 挑出一個 IPv6 Prefix 並結合 32 位元之 IPv4 位址，成為分配給 IPv4 主機的 128 位元 IPv6 位址。由於 IPv4 Address pool 位址數量相對較為不足，所以在分配位址給 IPv6 主機時通常採用動態分配，即分配暫時性位址，而非永久性位址。

464XLAT (IPv4/IPv6 protocol translation) 是一種無狀態和有狀態結合，用於 IPv4 與 IPv6 通訊轉換，一般是在 CLAT (Customer-side

Translator) 和 PLAT (Provider-Side Tranlator) 上執行，讓私有網路上的 IPv4 主機可以透過 IPv6 網路跟位於 IPv4 網路上的 IPv4 伺服器或主機聯繫。CLAT 上執行無狀態位址 IPv4-IPv6 轉換 (1:1)，主要參考 [RFC 6052]〝IPv6 Addressing of IPv4/IPv6 Translators〞文件內所描述內嵌 IPv4 位址格式；PALT 是執行有狀態位址 IPv4 對 IPv6 位址轉換，集中處理、維護私有網路 IPv4 到公眾網路 IPv4 的 NAT44。NAT64 透過使用 CGN (Carrier Grade NAT) 實現 IPv6 網路連線 IPv4 的網路，464XLAT 擴充了這種功能，允許 IPv4-Only 應用在 IPv6-Only 的網路上進行通訊，使用主機設備上不需要 IPv4 位址。464XLAT 網路架構如下圖所示。

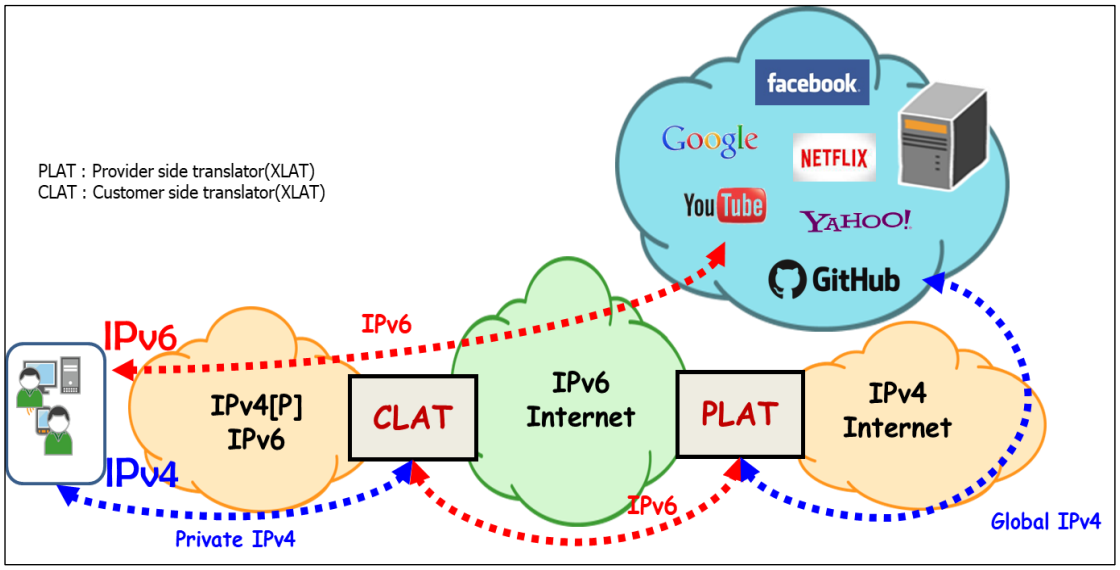



圖 52、464XLAT 網路架構

## 二. Native IPv6 試驗網路環境 IP 配置

本工作項目將分別針對 NAT64/DNS64 及 464XLAT 連網架構，以校園網路作為 IPv4 與 IPv6 接取環境，並於中央大學網路實驗室架設 NAT64/DNS64 及 464XLAT 轉換服務，提供 IPv6 到 IPv4 位址轉換機

制，及 IPv4 到 IPv6 再到 IPv4 位址轉換機制 2 種連線情境，以驗證 Native IPv6 連網環境架構可適當運作。

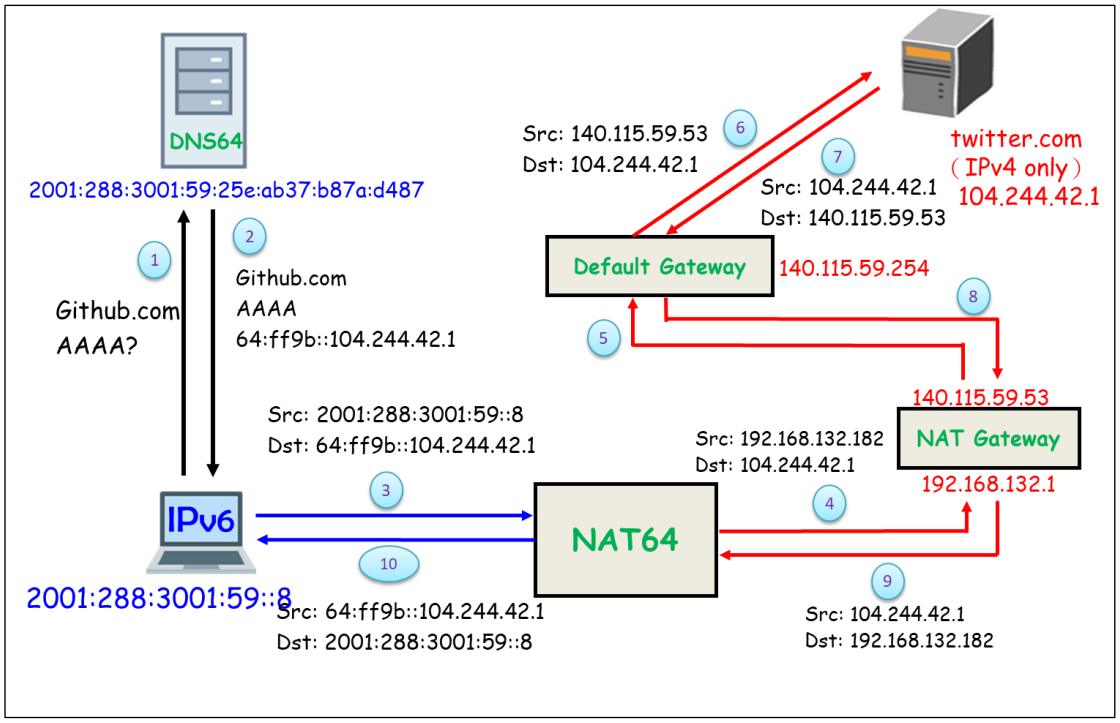



圖 53、NAT64/DNS64 實驗架構規劃與 IP 配置

本次實驗的NAT64/DNS64轉換服務架構與IP配置如上圖所示。圖中左方以 IPv6-only 方式連接實驗室網路之用戶，所到達網段或網域僅限於 IPv6 網路。客戶端如果需要請求連結 IPv4-only 的網站服務(如 github.com)，就需要透過 DNS64 進行轉換。DNS64 架設於學校內網與外部網路之間，在收到來自客戶端有關某個域名 AAAA (IPv6 位址) 紀錄的查詢時，會像平常一般找尋答案，若該域名有 IPv6 的位址，則直接將紀錄回覆給客戶端。相反地，若找不到紀錄，即目的地域名不提供 IPv6 位址，則會嘗試尋找相同域名的 A 紀錄 (IPv4 位址)。DNS64 會將查詢到的 A 記錄〝合成〞相等數量的 AAAA 紀錄，將 32 位元的 IPv4 位址嵌入到 128 位元的 IPv6 位址中，並加上 IPv6

前綴 (此處為 64:ff9b::/96)。DNS64 會將此 IPv6 位址回覆給用戶，讓用戶認為該域名網站有支援 IPv6 服務，可以直接連結。而後，用戶將此域名 (新的 IPv6 位址) 傳送至 NAT64。NAT64 則通過 JOOL 中之 JOOL instance 將 IPv6 位址中之前綴位址取出，留下後綴位址 (原 IPv4 位址)，依此後綴位址可連結到該網站之 IPv4 位址，以存取該服務。

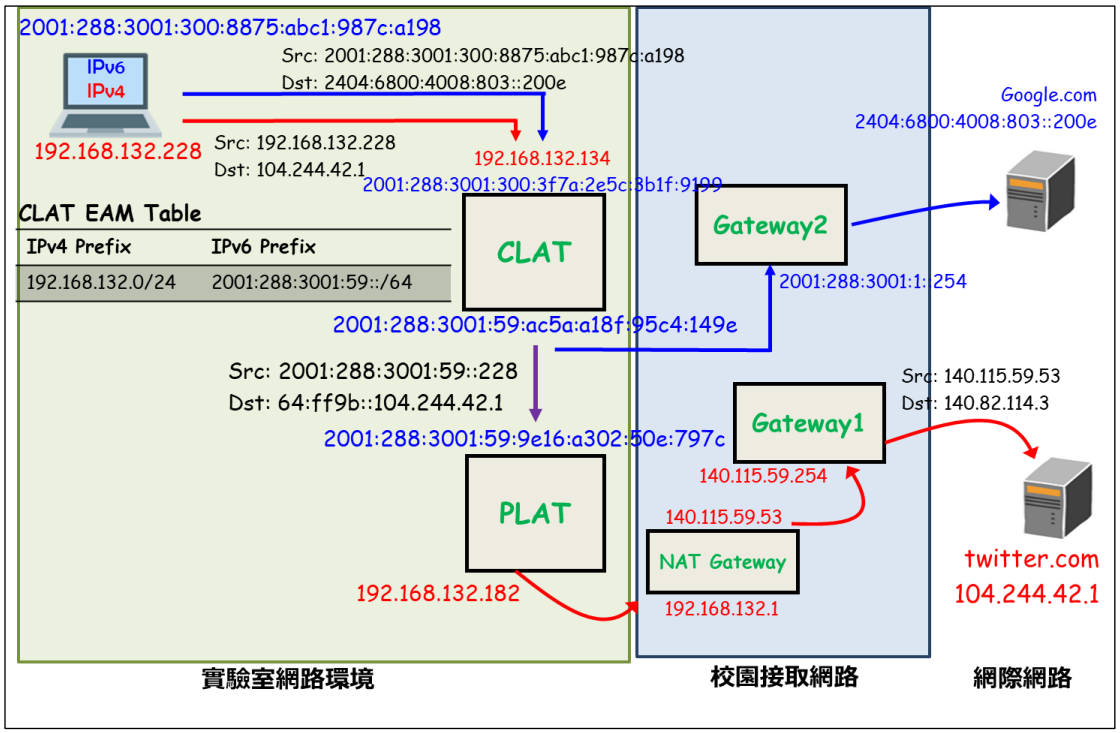



圖 54、464XLAT 實驗架構規劃與 IP 配置

464XLAT 轉換服務架構與 IP 配置如上圖所示。464XLAT 為具有私有位址的 IPv4 客戶端，通過 IPv6 網路連接到 IPv4 主機提供了一種簡單且可擴充的技術。建置過程將於學校實驗室環境中架設一台 CLAT 及一台 PLAT 伺服器，並搭配 JOOL 開源軟體建置。CLAT 通過 JOOL instance 將 IPv4 來源位址和目標位址嵌入 IPv6 前綴中，再透過 EAMT (Explicit Address Mappings Table) 方式將

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

## 三. Native IPv6 試驗網路環境開發工具

NAT64、CLAT 及 PLAT Server 建置規劃以 JOOL 開源軟體在實驗室環境中建置；DNS64 Server 則採用 BIND 9 開源軟體實現。以下分別介紹及說明兩者功能：

### (一) JOOL

JOOL 是在 Linux 作業系統中實現 SIIT (Stateless IP/ICMP Translation)、IPv4/IPv6 Translation、Stateful NAT64 及 Stateless NAT64 的位址轉換功能之方案，最廣泛被使用作為 NAT64 及 464XLAT 環境建置的開源軟體之一，由 NIC Mexico 與蒙特雷科技大學開發。JOOL 以 JOOL instance 的方式來實現 IPv4/IPv6 的轉換。JOOL instance 中記錄著 IPv4/IPv6 轉換的規則，使用者可根據需求將客製化的轉發規則增加至 JOOL instance 中。而 JOOL instance 可被附加至 2 種不同的 Linux 框架中–Netfilter 與 iptables，藉此可達到流量攔截 (Traffic intercepting) 的效果，流量攔截後即

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

## (二) BIND

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

針對 NAT64/DNS64 轉換服務測試環境，本計畫是以 BIND 9 搭配 JOOL 開源軟體進行實作。IPv6-only 用戶可透過 DNS64 獲得目的地 IPv6 位址，再透過 NAT64 轉換存取 IPv4-only 網站或應用程式服務。下圖為 JOOL 及 BIND 開源軟體 NAT64/DNS64 設定範例。

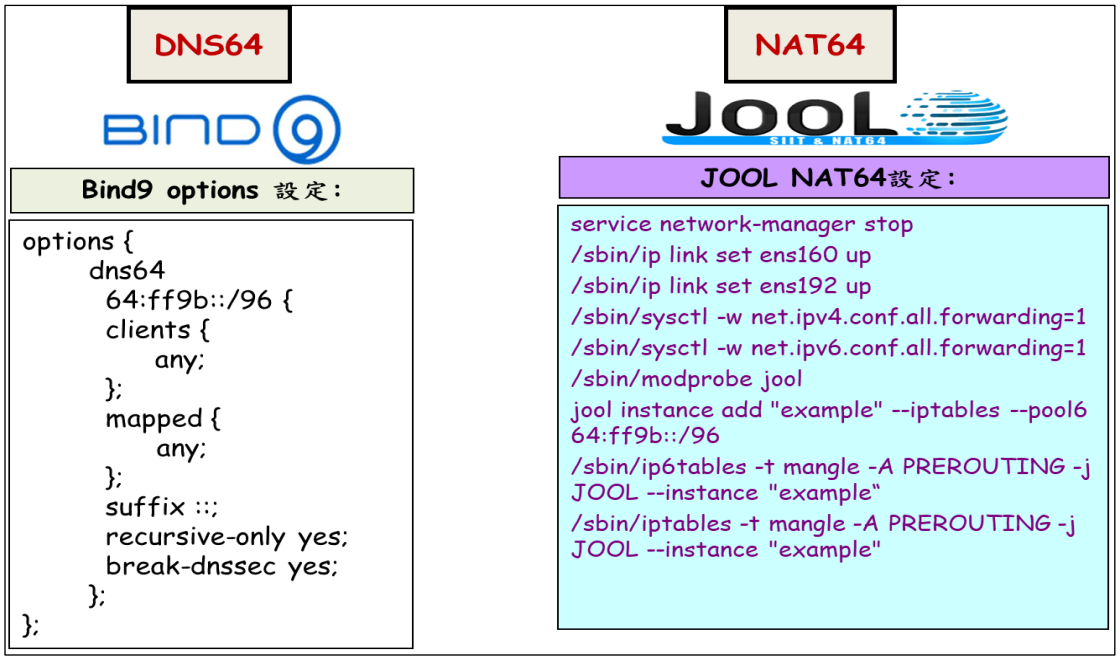



圖 55、NAT64/DNS64 設定範例

464XLAT 之 CLAT 與 PLAT 位址轉換功能同樣以 JOOL 開源軟體建置，無論為 IPv4-only、IPv6-only 或雙協定 (Dual-stack) 用戶，皆可透過 464XLAT 環境存取服務，若存取服務支援 IPv6，則用戶可透過 Native IPv6 環境進行連結，若存取服務只有支援 IPv4 服務，用戶可透過 CLAT 及 PLAT 位址轉換功能，達到存取服務的目的。下圖為 JOOL 開源軟體 464XLAT 設定範例。

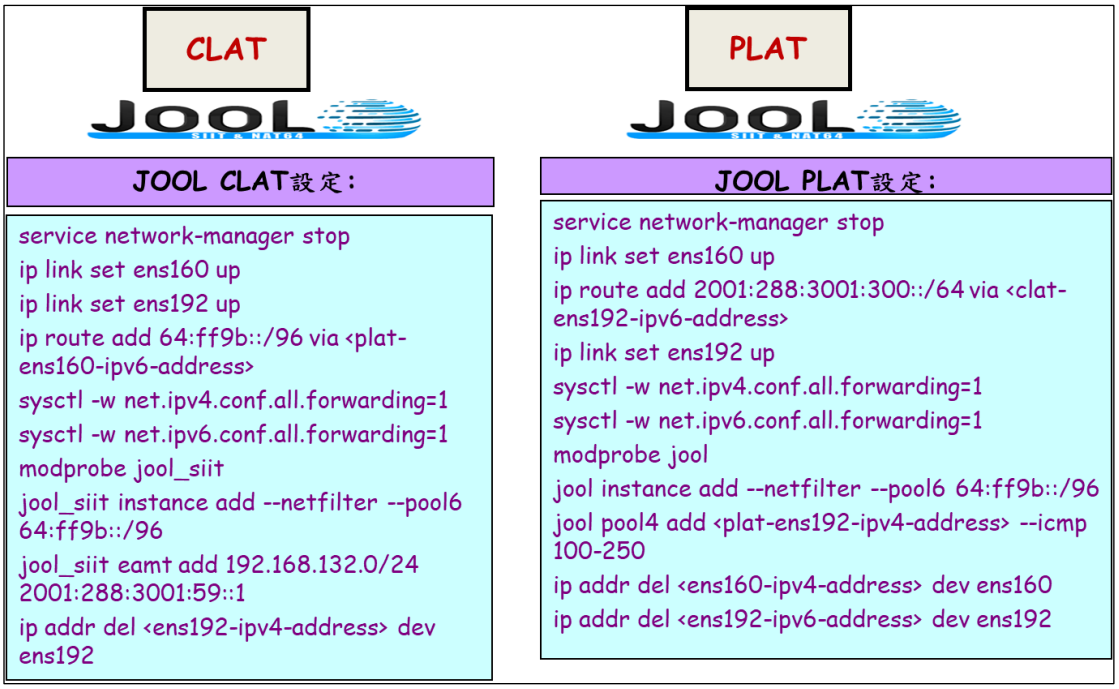



圖 56、464XLAT 設定範例

# 四. Native IPv6 試驗網路環境建置

Native IPv6 試驗網路環境建置分為 2 部分，包含 NAT64/DNS64 及 464XLAT，以下分別摘要說明建置方法：

## (一) NAT64/DNS64 環境建置

### 1. NAT64/DNS64 安裝

NAT64/DNS64 環境將以 JOOL 4.1.1.0 開源軟體搭配 BIND 9.10.3-P4-Ubuntu 建置。NAT64 及 DNS64 皆實作於 Linux based 之虛擬機中，kernel 版本為 5.3.0-62-generic，系統採用 Ubuntu18.04 版本，硬體則配置 2 核心 CPU、4G 記憶體及 60G 的硬碟容量。詳細軟硬體配置如下表所列：

表 32、NAT64/DNS64 資源體配置

| NAT64/DNS64 資源配置 | | | |
|---|---|---|---|
| | | **NAT64** | **DNS64** |
| **硬體資源配置** | **CPU(cores)** | Intel(R) Xeon(R) CPU E5620 @ 2.40GHz 各配置 2 核心 | |
| | **記憶體(GB)** | 4 | 4 |
| | **硬碟(GB)** | 60 | 60 |
| **軟體配置** | **系統** | Ubuntu 18.04 | Ubuntu 18.04 |
| | **版本** | 5.3.0-62-generic | 5.3.0-62-generic |
| | **開發軟體** | JOOL | BIND9 |
| | **版本** | 4.1.1.0 | 9.10.3-P4-Ubuntu |

JOOL 安裝於 Ubuntu18.04 的執行步驟如下：

- 步驟一：更新系統
- 步驟二：安裝 JOOL 必要套件
- 步驟三：下載 JOOL 原始碼
- 步驟四：安裝與編譯
- 步驟五：確認安裝

BIND9 安裝相較於 JOOL 簡易許多，不須下載額外的相依套件，安裝步驟如下：

- 步驟一：下載 BIND9 套件
- 步驟二：啟動 BIND9

JOOL 及 BIND9 安裝完成後，即可進行 NAT64/DNS64 環境建置相關設定。請參閱附錄五有詳細指令說明。

**2. NAT64/DNS64 設定**

NAT64/DNS64 測試環境中主要設備為 NAT64 Server 一台及 DNS64 Server 一台。NAT64 Server 所接觸的網段有二，其一為 IPv6-only 網段，用戶即透過此網段連接至 NAT64；另一網

段為對外網段，對接到 IPv4-only 伺服器，因此 NAT64 需配置兩張網卡。

此外，在 Linux 中 IPv4 和 IPv6 的轉換允許預設為關閉，因此須透過〝sysctl〞指令對 Linux kernel 進行修改，將 NAT64 中 IPv4 和 IPv6 轉換允許設定為〝True〞。JOOL 是以 JOOL instance 的方式來實現 IPv4/IPv6 轉換，須將轉換規則增加至 JOOL instance 中實現 IPv4/IPv6 轉發，然後，將此 JOOL instance 與 Linux iptables 掛接，利用 iptables 過濾、篩選封包特性，達到 NAT64 轉送 IPv4/IPv6 封包之功能。下表為 NAT64 與 DNS64 網路配置對照資訊：

表 33、NAT64/DNS64 網路配置對照資訊

| NAT64/DNS64 網路配置 | | | |
|---|---|---|---|
| | **DNS64** | **NAT64** | |
| **網卡名稱** | ens160 | ens160 | ens192 |
| **網卡位址** | 192.168.132.x / 2001:288:3001:59::x | 2001:288:3001:59::x | 192.168.132.x |
| **接觸網段** | 實驗室內網/外網 | 實驗室內網 (IPv6-only) | 外網 (IPv4-only) |
| **轉發設定** | none | net.ipv4.conf.all.forwarding=1<br>net.ipv6.conf.all.forwarding=1 | |
| **JOOL Instance** | none | iptables | |

DNS64 Server 相對於 NAT64 Server 來說相對單純，只需配發一張 dual stack 網卡，對內連接實驗室內網，對外連接外網與

後端DSN Server。唯須在BIND9設定中增加dns64的statement，用以敘述DNS64的功能以及配發Prefix時之標準。

詳細設定方式請參考參閱附錄五Native IPv6網路環境建置手冊有完整資訊。

## (二) 464XLAT 環境建置

### 1. 464XLAT 安裝

464XLAT環境以JOOL 4.1.1.0開源軟體建置。CLAT及PLAT皆實作於Linux based之虛擬機中，版本為5.3.0-62-generic，系統採用Ubuntu18.04版本，硬體則配置2核心CPU、4G記憶體及60G的硬碟容量。詳細軟硬體配置如下表所示：

表 34、464XLAT 資源配置

| 464XLAT 軟硬體配置 | | | |
|---|---|---|---|
| | | **CLAT** | **PLAT** |
| **硬體資源配置** | **CPU(cores)** | Intel(R) Xeon(R) CPU E5620 @ 2.40GHz 各配置 2 核心 | |
| | **記憶體(GB)** | 4 | 4 |
| | **硬碟(GB)** | 60 | 60 |
| **軟體配置** | **系統** | Ubuntu 18.04 | Ubuntu 18.04 |
| | **版本** | 5.3.0-62-generic | 5.3.0-62-generic |
| | **開發軟體** | JOOL | JOOL |
| | **版本** | 4.1.1.0 | 4.1.1.0 |

JOOL安裝在NAT64/DNS64已經說明，詳細內容請參考附錄五。

## 2. 464XLAT 設定

464XLAT 測試環境中主要設備為 CLAT Server 一台及 PLAT Server 一台。CLAT Server 所接觸的網段有二，其一為 IPv4/IPv6 共存的雙軌網段，IPv4 與 IPv6 用戶即透過此網段連接至 CLAT；另一網段為 IPv6-only 網段，若用戶存取目的地支援 IPv6，即從此網段直接出去，若目的地為 IPv4-only，則將封包轉發到與 CLAT 對接的 PLAT Server。故 CLAT 共配置兩張網卡，一張為 IPv4/IPv6 雙軌，另一則為 IPv6-only。PLAT Server 亦須配置兩張網卡，一張為 IPv6-only，與 CLAT Server 對接，接收需要經過 IPv6/IPv4 位址轉換之封包；另一張為 IPv4-only，對外連接學校網路 Gateway，以 IPv4 的方式連接到目的地。464XLAT 網路配置如下表所示：

表 35、464XLAT 網路配置

| **464XLAT 網路配置** | | | | |
|---|---|---|---|---|
| | **CLAT** | | **PLAT** | |
| **網卡名稱** | ens160 | ens192 | ens160 | ens192 |
| **網卡位址** | 192.168.132.x / 2001:288:3001:300::x | 2001:288:3001:59::x | 2001:288:3001:59::x | 192.168.132.x |
| **接觸網段** | 實驗室內網 | 實驗室內網 (IPv6-only)/ 外網 | 實驗室內網 (IPv6-only) | 外網 (IPv4-only) |
| **轉發設定** | net.ipv4.conf.all.forwarding=1<br>net.ipv6.conf.all.forwarding=1 | | net.ipv4.conf.all.forwarding=1<br>net.ipv6.conf.all.forwarding=1 | |
| **JOOL Instance** | netfilter | | netfilter | |

CLAT 與 PLAT 的 JOOL 設定皆於 Bash 模式下執行。詳細的建置步驟及指令，請參閱附錄五 Native IPv6 網路環境建置手冊。

關於 Native IPv6 試驗網路環境建置說明及相關文件，請參閱附錄五有完整資訊。

# 第二節Native IPv6 試驗網路環境測試

## 壹、 測試說明

Native IPv6 試驗網路環境測試將依據上一節所述的試驗網路環境，架設 NAT64/DNS64 及 464XLAT 轉換服務於實驗室網路環境中，提供以下兩種連線情境：

- IPv6 透過 NAT64/DNS64 服務連結 IPv4 網站
- IPv4 經由 CLAT 服務轉換為 IPv6 再透過 PLAT 服務連結 IPv4 網站

根據使用者常用設備及環境，進行使用情境測試及驗證，測試的軟硬體設施包含：

- 桌上型有線裝置，測試作業系統以 Windows 為主，測試版本包含 Windows 8.x 及 Windows 10.x。
- 行動裝置，測試作業系統將包含 Android 10.x 及 iOS 13.x 兩大系統。
- 測試應用主要以使用者常用服務為主，在上述桌上型有線裝置及行動裝置環境下測試，測試應用服務包含 Google Search、YouTube、Facebook、Twitter、Yahoo Search、Skype、Netflixs、FTP、SFTP、Windows Outlook、Gmail 等。

依照測試項目及測試方案可將測試規劃成三個部分，包含基本測試、連線測試及應用測試，測試架構如下圖所示：

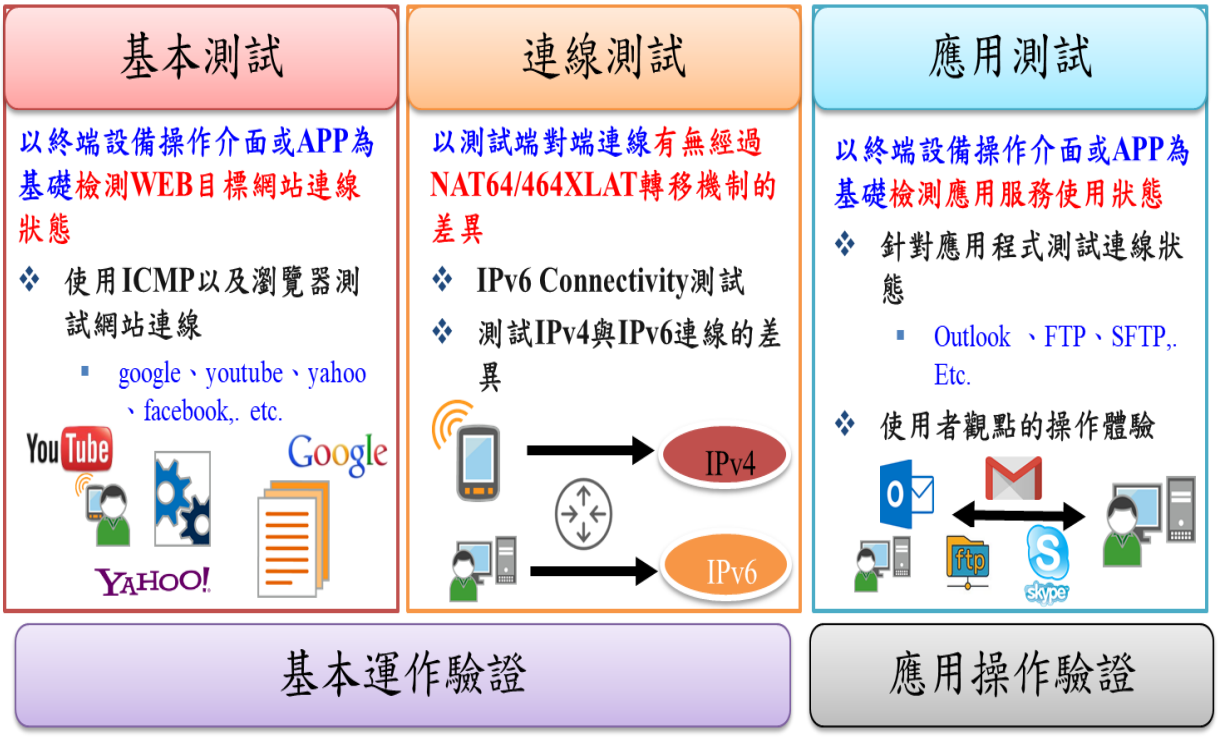



圖 57、NAT64/464XLAT 測試架構

此部分工作依照 Native IPv6 試驗網路環境建置完成成果，根據使用者情境進行實際測試，測試執行成果如下所述。

## 一.基本測試

以終端設備操作介面或應用程式為基礎，檢測目標網站連線狀態，主要為使用者介面配置 IPv6 參數與瀏覽器 IPv6 連網測試。測試方式以 ICMP 及瀏覽器測試網站連線，測試常用網站，包含 Google Search、Youtube、Yahoo Search、Facebook 及 Twitter。

## 二.連線測試

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

### 三.應用測試

以終端設備操作介面或應用程式為基礎，檢測應用服務使用狀態，從使用者角度與觀點來檢測操作或使用上是否會發生錯誤中斷情況。針對應用程式做連線狀態之測試，測試應用包含 Skype、Netflix、FTP、SFTP、Windows Outlook 及 Gmail。

## 貳、測試成果

## 一. NAT64/DNS64 測試結果

NAT64/DNS64 測試分為基本測試、連線測試及應用測試，測試結果摘要如下表所示：

表 36、NAT64/DNS64 基本測試結果

| 項次 | 網站名稱 | 網站類型 | 有線裝置 | | 無線裝置 | |
|---|---|---|---|---|---|---|
| | | | Windows8 | Windows10 | Android | iOS |
| 1 | Google | 入口網站 | v | v | v | v |
| 2 | Youtube | 影音網站 | v | v | v | v |
| 3 | Facebook | 社群網站 | v | v | v | v |
| 4 | Yahoo | 入口網站 | v | v | v | v |
| 5 | Netflix | 影音網站 | v | v | v | v |
| 6 | Twitter | 社群網站 | v | v | v | v |

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

表 37、NAT64/DNS64 連線測試結果

| 項次 | 網站名稱 | 網站類型 | 網站支援協定 | 資訊流是否經過 NAT64 | 反應時間 | Ping | Web |
|---|---|---|---|---|---|---|---|
| 1 | Google | 入口網站 | IPv4/IPv6 | 否 | 4 (ms) | v | v |
| 2 | Youtube | 影音網站 | IPv4/IPv6 | 否 | 3 (ms) | v | v |
| 3 | Facebook | 社群網站 | IPv4/IPv6 | 否 | 3 (ms) | v | v |
| 4 | Yahoo | 入口網站 | IPv4/IPv6 | 否 | 140 (ms) | v | v |
| 5 | Netflix | 影音網站 | IPv4/IPv6 | 否 | 163 (ms) | v | v |
| 6 | Twitter | 社群網站 | IPv4 only | 是 | 56 (ms) | v | v |

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

表 38、NAT64/DNS64 應用測試結果

| 項次 | 服務 | 名稱 | 有線裝置 | | 無線裝置 | |
|---|---|---|---|---|---|---|
| | | | Windows8 | Windows10 | Android | iOS |
| 1 | SKYPE | 通訊服務 | v | v | v | v |
| 2 | FTP | 下載服務 | v | v | v | v |
| 3 | SFTP | 傳輸服務 | v | v | v | v |
| 4 | Outlook | 郵件服務 | v | v | v | v |
| 5 | Gmail | 郵件服務 | v | v | v | v |

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

## 二. 464XLAT 測試結果

464XLAT 測試同樣分為基本測試、連線測試及應用測試，測試結果如下。

464XLAT 基本測試結果顯示所有測項皆可透過 464XLAT 連網環境存取。其中 twitter.com 須經由 IPv4 轉換到 IPv6 再轉換到 IPv4，而其他網站則是由 IPv6 直接連結 IPv6 方式。結果如下表所示：

表 39、464XLAT 基本測試結果

| 項次 | 網站名稱 | 網站類型 | 有線裝置 | | 無線裝置 | |
|---|---|---|---|---|---|---|
| | | | Windows 8 | Windows10 | Android | iOS |
| 1 | Google | 入口網站 | v | v | v | v |
| 2 | Youtube | 影音網站 | v | v | v | v |
| 3 | Facebook | 社群網站 | v | v | v | v |
| 4 | Yahoo | 入口網站 | v | v | v | v |
| 5 | Netflix | 影音網站 | v | v | v | v |
| 6 | Twitter | 社群網站 | v | v | v | v |

結果顯示，464XLAT 基本測試所有測項皆可透過 464XLAT 連網環境存取。其中 twitter.com 須經由 IPv4 到 IPv6 再轉換為 IPv4 連結，而其他網站則是 IPv6 直接連結 IPv6 的方式。

連線測試的部分，6 個目標網站皆可透過 464XLAT 環境存取。從表中 twitter.com 測項結果可看出經由 464XLAT 轉換和 Native IPv4

的連線方式之差異，反應時間只差距 1.3ms，轉換影響甚小。結果如下表所示：

表 40、464XLAT 連線測試結果

| 項次 | 網站名稱 | 網站支援 | 是否經過 CLAT | 是否經過 PLAT | 464XLAT | | | Native IPv4 | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | 反應時間 | Ping | Web | 反應時間 | Ping | Web |
| 1 | Google | IPv4/IPv6 | 是 | 否 | 3 (ms) | v | v | 4 (ms) | v | v |
| 2 | Youtube | IPv4/IPv6 | 是 | 否 | 4 (ms) | v | v | 4 (ms) | v | v |
| 3 | Facebook | IPv4/IPv6 | 是 | 否 | 3 (ms) | v | v | 28 (ms) | v | v |
| 4 | Yahoo | IPv4/IPv6 | 是 | 否 | 167 (ms) | v | v | 165 (ms) | v | v |
| 5 | Netflix | IPv4/IPv6 | 是 | 否 | 165 (ms) | v | v | x | x | v |
| 6 | Twitter | IPv4 only | 是 | 是 | 66.3 (ms) | v | v | 65 (ms) | v | v |

應用測試的部分，Windows10、Windows8、Android 及 iOS 四種作業系統皆可通過所有應用測試。結果如下表所示：

表 41、464XLAT 應用測試結果

| 項次 | 服務 | 名稱 | 有線裝置 | | 無線裝置 | |
|---|---|---|---|---|---|---|
| | | | Windows8 | Windows10 | Android | iOS |
| 1 | SKYPE | 通訊服務 | v | v | v | v |
| 2 | FTP | 下載服務 | v | v | v | v |
| 3 | SFTP | 傳輸服務 | v | v | v | v |
| 4 | Outlook | 郵件服務 | v | v | v | v |
| 5 | Gmail | 郵件服務 | v | v | v | v |

以使用者觀點進行操作測試,比較IPv4和IPv6連線品質的差異。實驗結果顯示 464XLAT 轉換機制在主觀的使用者體驗上影響很小，幾乎可以省略。而客觀數據，如反應時間也顯示有無經過轉換機制差異並不大，總結以 JOOL 等開源軟體建置 464XLAT 轉換環境方案經實驗驗證在小型測試環境具有一定程度可用性。

關於 Native IPv6 試驗網路環境建置測試內容及結果，完整詳細資訊說明請參閱附錄五。

# 第五章 IPv6 動態 DNS 服務軟體開發

隨著 IPv4 公用位址 (Public IP) 用罄，近年來各國政府更為積極投入 IPv6 推廣。國內在政府相關機關不遺餘力推廣之下，整體 IPv6 普及度名列世界前茅。當前大部分網路服務，主要以透過網域名稱系統 (Domain Name System，DNS) 提供服務讓使用者存取各項服務，包括網站、雲端硬碟、共享服務..等。

當小型服務供應商無法取得固定 IP 資源時，將可能以動態 IPv6 位址建置其所希望提供網路相關服務，因此就需要使用到動態網域名稱 (Dynamic DNS，DDNS) 服務，讓網站 DNS 和 IP 可以隨時保持對應及更新，避免用戶透過 DNS 連結時無法取得正確 IPv6 位址而連線失敗。為了推廣 IPv6 使用普及度，並增加 IPv6 可用性，本項工作將開發能同時支援 IPv4 及 IPv6 之動態 DNS 服務套件，其包含客戶端及伺服器端服務軟體，供使用者下載安裝使用，透過此服務套件以建立自己的網路服務應用。各分項工作成果如下所述。

## 第一節 開發 IPv6 動態 DNS 服務軟體

### 一. IPv6 動態 DNS 服務系統架構

IPv6 動態 DNS (Dynamic DNS，DDNS) 系統架構，採用主從式 (Client-Server model) 設計，主要 DN 及 IP 查詢功能系統運作在 Server 端執行，讓 Client 可送出查詢需求給 Server 端。下圖為 DDNS Server 的系統架構，Server 端將設計為執行於作業系統 CentOS 上的軟體，而 Client 端將設計為執行於作業系統 Windows 上的軟體。

CentOS (Community Enterprise Operating System) 是 Linux 發行版之一，來自於 Red Hat Enterprise Linux (RHEL) 依照開放原始碼規定釋出的原始碼所編譯而成。由於出自同樣的原始碼，因此有些要求高度穩定性的伺服器以 CentOS 替代商業版的 Red Hat Enterprise Linux 使用。兩者的不同，在於 CentOS 並不包含封閉原始碼軟體。[36]

Server 端軟體包含資料庫 (MySQL) 及 DNS 軟體 BIND 9 (BIND Version 9)。BIND (Berkeley Internet Name Domain) 是現今網際網路上最常使用的 DNS 軟體，使用 BIND 作為伺服器軟體的 DNS 伺服器約佔所有 DNS 伺服器的九成，市佔率相當高。BIND 現在由網際網路系統協會 (Internet Systems Consortium) 負責開發與維護。[37]

MySQL 是一個開放原始碼的關聯式資料庫管理系統，原開發者為瑞典的 MySQL AB 公司，該公司於西元 2008 年 (民國 97 年) 被昇陽微系統 (Sun Microsystems) 收購。西元 2009 年 (民國 1998 年)，甲骨文公司 (Oracle) 收購昇陽微系統公司，MySQL 成為 Oracle 旗下產品。MySQL 由於效能高、成本低、可靠性好，已經成為最流行的開源資料庫，因此被廣泛地應用在網路上的中小型網站中。隨著 MySQL 的不斷成熟，也逐漸用於更多大規模網站和應用，如 Google 和 Facebook 等網站。[38]

此外，為了可以達到方便快速的資料更新，本架構中使用 BIND 9 啟用了 DLZ (Dynamically Loadable Zones)，用來將網域資料寫入到資料庫內，此資料庫也與動態 DNS Server 的資料庫共用，便於管理，也可以節省自行架設的硬體成本。

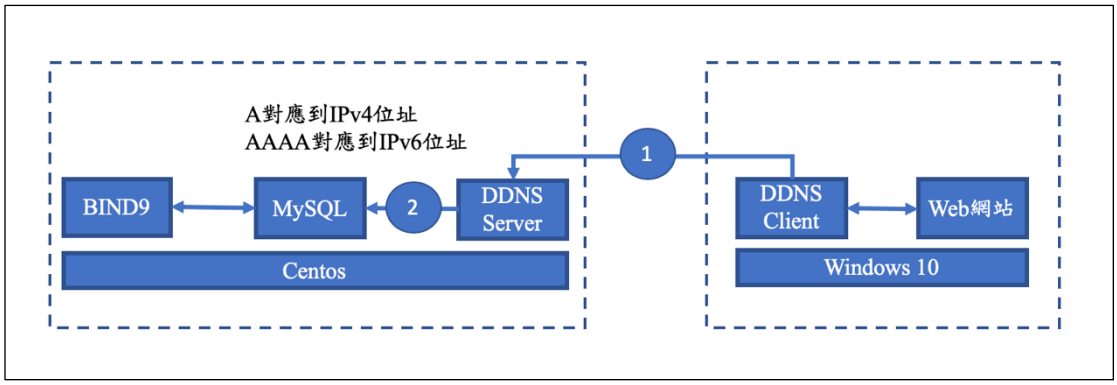



圖 58、動態 DNS 系統架構

在上圖動態 DNS 系統架構中，動態 DNS Client 與動態 DNS Server 串接的流程說明如下：

- 步驟 1：Client 端運作

  動態 DNS Client 取得自己主機上的 IP 位址，將主機的 IP 位址傳遞給動態 DNS Server。

- 步驟 2：Server 端運作

  動態 DNS Server 收到動態 DNS Client 傳過來的 IP 存入到資料庫。BIND 9 透過資料庫取得最新的 IP 位址與網域的對應。

動態 DNS Client 要更新自己的 IP 位址時，其流程為動態 DNS Client 取得自己的公開 IPv4 或 IPv6 位址，及此 IP 位址對應的網域名稱，將資料透過動態 DNS Server 提供的 API 規格，先完成身份驗證，驗證成功之後，動態 DNS Server 可以將動態 DNS Client 傳遞過來的 IP 位址與網域的對應資訊寫入到資料庫內。

當動態 DNS Server 接收到來自動態 DNS Client 的 IP 位址與網域名稱的對應資料，並更新資料庫之後，BIND 9 透過 DLZ 機制可以將資料讀取，供外部查詢使用。

## 二. IPv6 動態 DNS 服務運作流程

用戶利用動態 DNS 架設網站後，需要透過動態 DNS Server 取得最新的 IP 位址，不論是 IPv4 或 IPv6 位址。取得 IP 位址之後，就可以連到 Web 網站，並取得 Web 網站的內容。

下圖為動態 DNS 服務之 IP 位址取得流程示意圖，說明使用者如何透過動態 DNS Server 連結以動態 IP 架設的 Web 網站。

首先，使用者只知道要連的目標網站網址，接著，使用者的瀏覽器會將網址中的網域取出，向 DNS 詢問網站的 IPv4 或 IPv6 位址。取得 IP 位址之後，再將封包傳遞到 Web 網站的 IP 位址，連線就能順利建立。

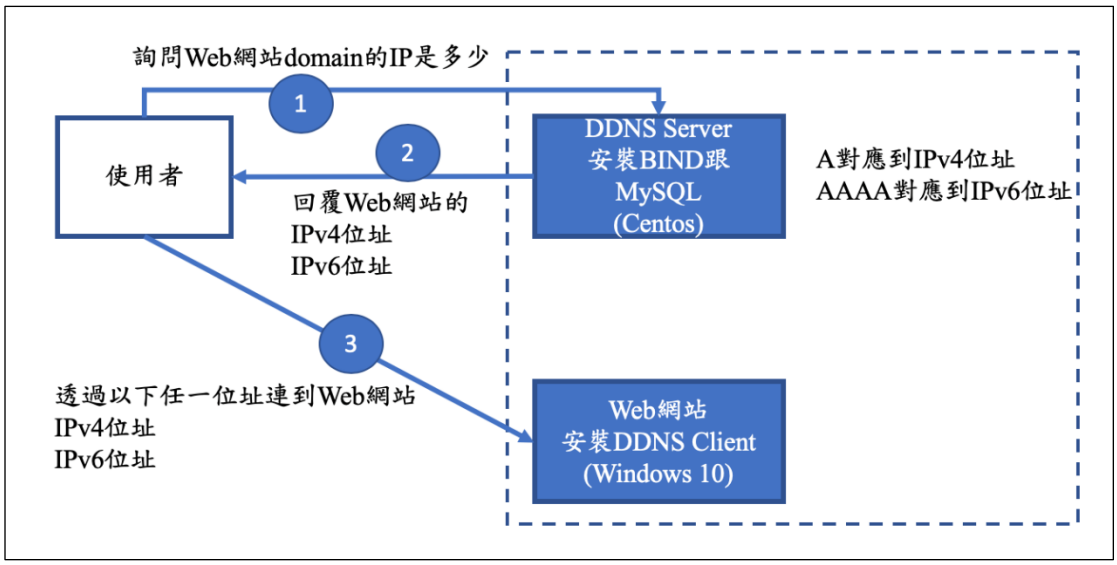



圖 59、動態 DNS 服務之 IP 位址取得流程

上圖動態 DNS 服務之 IP 位址取得流程說明如下：

- 步驟 1：使用者送出連結特定網站需求

  使用者輸入 Web 網站的網址，瀏覽器會將網站的網域名稱取出，並詢問此網域對應的 IPv4 或 IPv6 位址。

- 步驟 2：Server 端運作

  動態 DNS Server 收到查詢需求之後，會將使用者要求連線的 Web 網站 IP 位址傳遞給使用者。

- 步驟 3：使用者取得網站 IP 進行連線

  使用者取得 Web 網站 IP 位址後，直接以 TCP 跟 Web 網站連線，取得內容。

# 三. IPv6 動態 DNS 服務應用功能及介面

## (一) Server 端服務功能及介面

動態 DNS 服務 Server 端應用軟體，提供主機、帳號、金鑰及其他共 4 類功能，各類功能下分為數個子項，下表為功能列表及簡要說明：

表 42、動態 DNS 服務 Server 端應用功能

| 序號 | 功能 | 分項功能說明 |
|---|---|---|
| **1** | 主機 | 1. 新增主機：提供新增主機及網域到資料庫<br>2. 主機列表：提供全部主機及網域在資料庫列表 |
| **2** | 帳號 | 1. 新增帳號：提供管理者可以新增帳號<br>2. 帳號列表：提供管理者查看所有帳號列表 |
| **3** | 金鑰 | 1. 新增 API 金鑰：提供新增 API 金鑰<br>2. API 金鑰列表：提供全部 API 金鑰列表 |
| **4** | 其他 | 1. 變更密碼：依照使用者身分級別，提供管理者/一般使用者變更密碼<br>2. DDNS Server 使用說明：動態 DNS Server 使用說明<br>3. DDNS Client 使用說明：動態 DNS Client 使用說明 |

動態 DNS 服務 Server 端應用軟體介面，設計示意圖如下圖所示，下圖顯示新增主機介面圖，使用者填入新增網站相關資訊後，按〝新增〞鍵功能，即可在資料庫中增加此筆資料。若輸入資料有誤按〝取消〞鍵功能，即放棄此筆資料編輯內容。

圖 60、在動態 DNS 之 Server 服務應用上新增主機介面

新增任一筆紀錄之後，只要是正確格式，資料就會被立即儲存在資料庫內，由於本套系統與 BIND9 串接，因此 BIND9 主機就可以立即讀取新增主機紀錄。

下圖為動態 DNS 服務 Server 端應用軟體，主機列表設計圖，本項功能除提列所有已經新增到資料庫中的主機列表外，使用者可選取任一在資料庫中的主機資料，按〝修改〞功能，即可針對該筆資料進行修改，修改完畢確認變更，即可變更資料庫中所存放的此筆資料內容。若此筆主機資料已經不再使用，可以按〝刪除〞功能鍵，即可將該筆資料由資料庫中刪除。

圖 61、在動態 DNS 之 Server 顯示主機列表介面

其他動態 DNS 服務 Server 端應用軟體的各項功能設計，請參閱附錄七詳細說明。

## (一) Client 端服務功能及介面

動態 DNS 服務 Client 端應用軟體，主要用途在於將本機 IPv4 及 IPv6 位址回傳給動態 DNS Server，讓 Server 知道各網域該正確的對應到哪一個 IP 位址，確保當使用者透過網路連結該網域時，可以正確連結，Client 端應用軟體各項功能如下表所列：

表 43、動態 DNS 服務 Client 端軟體功能

| 序號 | 功能 | 說明 |
|---|---|---|
| 1 | 帳號登入/登出 | 提供帳號登入及登出的功能 |
| 2 | 顯示連線狀態及網域名稱 | 當使用者登入成功後，動態 DNS Server 將目前資料庫內網域及 IP 資訊回傳給 Client。 |
| 3 | 自動更新主機與 IP 對應資訊 | 當 Client 收到資訊後，會以表格方式呈現。使用者可以在畫面上看到網域。 |
| 4 | 設定更新頻率 | 使用者可自訂更新頻率，透過 Client 端介面自行設定。預設值為每 300 秒更新一次。 |

動態 DNS 服務 Client 端應用軟體介面，設計介面如下圖所示，畫面中顯示首先使用者必須登入，才有辦法連上動態 DNS Server 並更新主機 IP 資訊。

圖 62、動態 DNS 之 Client 端應用軟體登入介面圖

主機及網域管理需要在動態 DNS Server 上進行，當使用者在動態 DNS Server 上新增網域及主機後，需要為動態 DNS Client 新增連線用的帳號及密碼。當動態 DNS Client 連上動態 DNS Sever 後，會取得可用網域及主機資訊，並將主機及網域資訊顯示在表格內，使用者依據需求，選擇希望更新主機，介面表格在主機左側會有一個勾選 checkbox 如下圖所示，勾選主機之後按下「更新勾選主機的 IP」按鈕，動態 DNS Client 就會自動抓取目前 IP，並將 IP 傳送給動態 DNS Server，讓 Server 更新資料庫內主機 IP。

圖 63、動態 DNS Client 主機更新介面圖

其他動態 DNS 服務 Client 端應用軟體的各項功能設計，請參閱附錄七。

# 四.IPv6 動態 DNS 服務開發工具

## (一)Server 開發語言 PHP

動態 DNS Server 開發語言是採用 PHP 程式語言。PHP (全名 PHP：Hypertext Preprocessor，PHP：超文字前處理器) 為開源的通用電腦程式語言，尤其適用於網路開發並可嵌入 HTML 中使用。PHP 的語法吸收 C 語言、Java 和 Perl 等流行電腦語言的特點，易於一般程式設計師學習。PHP 的主要目標是允許網路開發人員快速編寫動態頁面，但 PHP 也被用於其他很多領域。PHP 最初是由

勒多夫在西元 1995 年 (民國 84 年) 開始開發；現在 PHP 的標準由 the PHP Group 維護。PHP 以 PHP License 作為許可協議，不過因為此協議限制了 PHP 名稱的使用，所以和開放原始碼許可協議 GPL (General Public License，GNU 通用公共許可協議) 不相容。PHP 應用範圍相當廣泛，特別在網頁程式開發上。一般來說 PHP 大多執行在網頁伺服器上，透過執行 PHP 程式碼來產生使用者瀏覽的網頁。PHP 可以在多數的伺服器和作業系統上執行，且大量被伺服器採用。[39]

## (二)Client 開發語言 Electron

動態 DNS Client 的開發語言為 Electron 開源框架。Electron (原名為 Atom Shell) 是 GitHub 開發的一個開源框架。允許使用 Node.js (作為後端) 和 Chromium (作為前端) 完成桌面 GUI 應用程式的開發。Electron 現已被多個開源 Web 應用程式用於前端與後端的開發，著名專案包括 GitHub 的 Atom 和微軟的 Visual Studio Code，具有高度的可維護性。

一個基礎的 Electron 包含三個檔案：〝package.json〞 (元資料)、〝main.js〞 (代碼) 和 〝index.html〞 (圖形化使用者介面)。框架由 Electron 可執行檔 (Windows 中為 〝electron.exe〞、macOS 中為 〝electron.app〞、Linux 中為 〝electron〞) 提供。開發者可以自行增加標誌、自訂圖示、重新命名或編輯 Electron 可執行檔。[40]

# 五.IPv6 動態 DNS 服務軟體開發考量

軟體開發除系統規劃及採用開發工具規劃外，還需考量應用後續的維護，為確保程式碼在後續維護上的一致性，以下整理動態 DNS Server 開發語言 PHP 程式語言開發建議，以便於後續維護的一致性與完整性。

而動態 DNS Client 的開發語言為 Electron 開源框架，此框架被應用在包括微軟的 Visual Studio Code 等知名的軟體專案上，具有高度的可維護性。

PHP7 的程式語言開發建議事項，如下表所列：

表 44、PHP7 的程式語言開發建議事項列表

| 序號 | 建議事項 |
|---|---|
| 1 | PHP7 的開發語言建議請參考 PHP7 語言 |
| 2 | 程式碼結尾不要採用〝?>〞 |
| 3 | 程式碼開頭不要採用〝<?〞，應該採用〝<?php〞 |
| 4 | 所有檔案都必須是 UTF-8 且沒有 BOM |
| 5 | 所有資料儲存都用 UTC 時區來儲存日期跟時間 |
| 6 | 命名規則可以使用 camelCase 方式 |
| 7 | 可以使用 Tab 來排版 |
| 8 | 每一行程式結尾不要用空白字元 |

Electron 的開發建議事項，如下表所列：

表 45、Electron 的程式語言開發建議事項列表

| 序號 | 建議事項 |
|---|---|
| 1 | 以換行結尾 |
| 2 | 路徑優先順序為：<br>Node 模組 (例如 path) ➔Electron 模組 (例如 ipc，app) ➔本地模組 (使用相對路徑) |
| 3 | 類別 (Class) 順序為：<br>Class (類別) ➔Instance (實例) |
| 4 | 避免使用與平台相關的程式碼，例如：〝path.join( )〞來產生檔案路徑、不要用〝/tmp〞而應該改用〝os.tmpdir( )〞來將資料暫時儲存於暫存路徑 |
| 5 | 在 function 回傳時，請採用〝return〞，不要使用〝return null〞、〝return undefined〞、〝null〞、〝undefined〞 |
| 6 | C++跟 Python 的程式碼撰寫風格請參考程式碼撰寫風格 |
| 7 | 文件請用 remark markdown 形式 |
| 8 | JavaScript 語法請參考 Js 標準語法 |
| 9 | 命名規則：<br>如果是類別，請用〝PascalCase〞，如果是 APIs 請用〝camelCase〞 |

資料庫結構設計建議事項，如下表所列：

表 46、資料庫結構設計建議事項列表

| 序號 | 建議事項 |
|---|---|
| 1 | 請依循 SQL Style Guide |
| 2 | ● 單行註解請用〝#〞<br>● 如果要用〝--〞，則在〝--〞之前需要有一個空白字元或者一個 TAB<br>● 多行註解請用〝/* ... */〞 |
| 3 | 儲存日期跟時間用〝timestamp〞，不要用〝DateTime〞，也不要存〝INT〞 (整數) |
| 4 | 不要使用保留字在欄位、表格名稱 |
| 5 | 需要被查詢的欄位記得都要建立索引，如果是唯一值，則需要建立 UNIQUE KEY 或 PRIMARY KEY |
| 6 | ● 欄位名稱盡量使用英文小寫字母，避免使用大寫英文字母。<br>● 表格名稱盡量用集合名稱，或用複數形式，例如 staff 或 employees |

# 六. IPv6 動態 DNS 服務軟體資訊安全建議

動態 DNS 服務軟體除開發功能面的考量外，以下針對資訊安全事項提出相關建議，詳細資訊如下表所列：

表 47、資訊安全建議事項列表

| 序號 | 建議事項 |
|---|---|
| 1 | 機密資料下載時，資料須設定密碼方可開啟，避免非授權人取得資料後洩漏 |
| 2 | 伺服器端對於自 GET，POST 傳遞的參數須透過驗證使用者輸入資料的正確性 |
| 3 | 針對開放性的資料，需提供檔案 hash 值供下載者驗證 |
| 4 | 須針對 SQL Injection 特別防範，使用 Prepared statements 或 Stored procedures 及輸入驗證來防止 |
| 5 | 須具有防止 Cross-site scripting 的能力 |
| 6 | 記錄以 hash 確保 log 正確性，保證資料不會被竄改 |
| 7 | 除了允許匿名存取的功能之外，其他功能需要通過身份驗證才能存取，且身份驗證機制須集中於 Server 端 |
| 8 | 強制規範使用者密碼須符合高強度密碼規則 (密碼長度 16 個字元以上，包括英文大小寫、數字跟特殊字元) |
| 9 | 帳號 lock 機制，當嘗試登入錯誤達 3 次以上，則該 IP 跟帳號在 30 分鐘內禁止登入 |
| 10 | 具備防止 CSRF 攻擊 (Cross Site Request Forgery，跨站請求攻擊) 之措施 (在發送 form action 前，產生一次性 token) |
| 11 | 記錄身份登入失敗、存取資源失敗、資料庫異動 |
| 12 | 日誌記錄須包括 user id、timestamp、存取功能 |
| 13 | 使用者在登出之後，需要將 session 清除 |
| 14 | 發生錯誤時，頁面僅顯示簡短錯誤及代碼，不包括詳細錯誤 |

# 七. 動態 DNS 之 Server 資料庫設定

## (一) 資料庫設定

動態 DNS Server 的資料庫包括帳號管理、網域管理、系統日誌及 BIND 9 結合 DLZ 使用的資料庫表格，由於數據量不大，因此可以將這些資料庫表格全部集中在同一個資料庫內，各自的資訊分別記錄在各自的表格內。

由於資料庫使用 MySQL，而 MySQL 開始預設的〝character set〞及〝collation〞分別為〝latin1〞及〝latin1_swedish_ci〞，為了確保資訊可以正確被儲存，需要在建立資料庫時，將新建的資料庫〝character〞指定為〝utf8mb4〞，而〝collation〞則指定為〝utf8mb8_unicode_ci〞，這樣當儲存中文時，才不會出現問題。建立一個〝utf8〞的資料庫語法如下：

```
CREATE DATABASE mydb CHARACTER SET utf8 COLLATE utf8_unicode_ci
```

## (二) 資料庫格式比較

在 MySQL 資料庫的 collation (校對) 有許多選擇，這個值會因為操作連線到 MySQL 軟體預設值而有所不同，例如使用 Squel Pro 時，此軟體預設偏好的 collation 為〝utf8mb4_0900_ai_ci〞，而 character 則為〝utfmb4〞。使用 utf8mb4 已經是趨勢，主要是支援多國語言時，可以更精確的儲存資料。

但是在 collation 的部分，如果使用〝utf8mb4_0900_ai_ci〞，可能會造成資料轉移時，進行轉換會出現問題。因此為保險起見，

需在〝utfmb8_general_ci〞及〝utf8mb4_unicode_ci〞兩者之間擇一。下表針對 2 種不同設定格式進行比較：

表 48、collation 格式比較

| 序號 | collation 格式 | 特性 |
|---|---|---|
| 1 | 〝utf8mb8_general_ci〞 | 優點：速度較快<br>缺點：特殊字元時顯示較不精確 |
| 2 | 〝utf8mb4_unicode_ci〞 | 優點：速度稍慢<br>缺點：特殊字元可以精確顯示 |
| 結論 | 資料正確性對於系統後續維護非常重要，因此優先採用〝utf8mb4_unicode_ci〞作為 DDNS Server 的 collation 設定 | |

而 character set 格式選擇比較，如下表所示：

表 49、character set 格式比較

| 序號 | character set 格式 | 特性 |
|---|---|---|
| 1 | 〝utf8〞 | 格式：以 3 bytes 儲存資料 |
| 2 | 〝utf8mb4〞 | 格式：以 4 bytes 儲存資料 |
| 結論 | 〝utf8mb4〞在儲存資料空間比〝utf8〞大，資料儲存更精確，因此選擇使用〝utf8mb4〞 | |

更多詳細資訊請參考附錄七，有詳細說明。

本軟體服務並已完成原始碼檢測、滲透測試及弱點掃描，詳細資訊請參考附錄七之 2，有詳細說明。

# 第二節 IPv6 動態 DNS 服務軟體測試

## 一. 動態 DNS 之 Server 測試規劃

### (一) 動態 DNS 之 Server 測試範圍

Server 端軟體應用測試項目，包括：

- 網頁功能測試，例如帳號的新增、修改跟刪除。
- 網域的維護 (同樣也是包括新增、修改及刪除等行為)。

另外服務是否可以正常運作也是重要考量項目，相關測試項目包括：

- 日誌測試：

  系統會將重要行為記錄到日誌內，例如新增帳號或者修改網域名稱等，這些行為都被系統記錄到資料庫內，作為查詢及稽核使用。因此需要進行驗證。

- 動態 DNS Client-Serve 運作測試：

  動態 DNS Client 是否能正常和 Server 溝通，且將正確資訊傳遞給 DDNS Server，需要列入測試範圍內。

- 動態 DNS Server 在 BIND 9 搭配 DLZ 共同運作：

  Server 端除負責功能運作之外，也需要跟 BIND 9 搭配 DLZ 共同運作，因此需要列入在動態 DNS Server 測試範圍內。

### (二) 動態 DNS 之 Server 測試過程

要測試動態 DNS Server 功能是否正常運作，需要先使用系統預設管理者帳號跟密碼登入，登入之後，再逐步測試以下功能：

- 帳號的管理功能。
- 網域的管理功能。

- 與動態 DNS Client 串接的運作是否正常。
- 與 BIND 9 的資料更新是否正常。
- BIND 9 對外的連線是否正常。

# 二. DDNS 之 Client 測試規劃

## (一) 測試動態 DNS Client 在 IPv4 環境下運作

下圖為測試動態 DNS Client 在網路環境下運作設備配置圖，主要動態 DNS 服務需和中華電信機上盒進行直接連接。

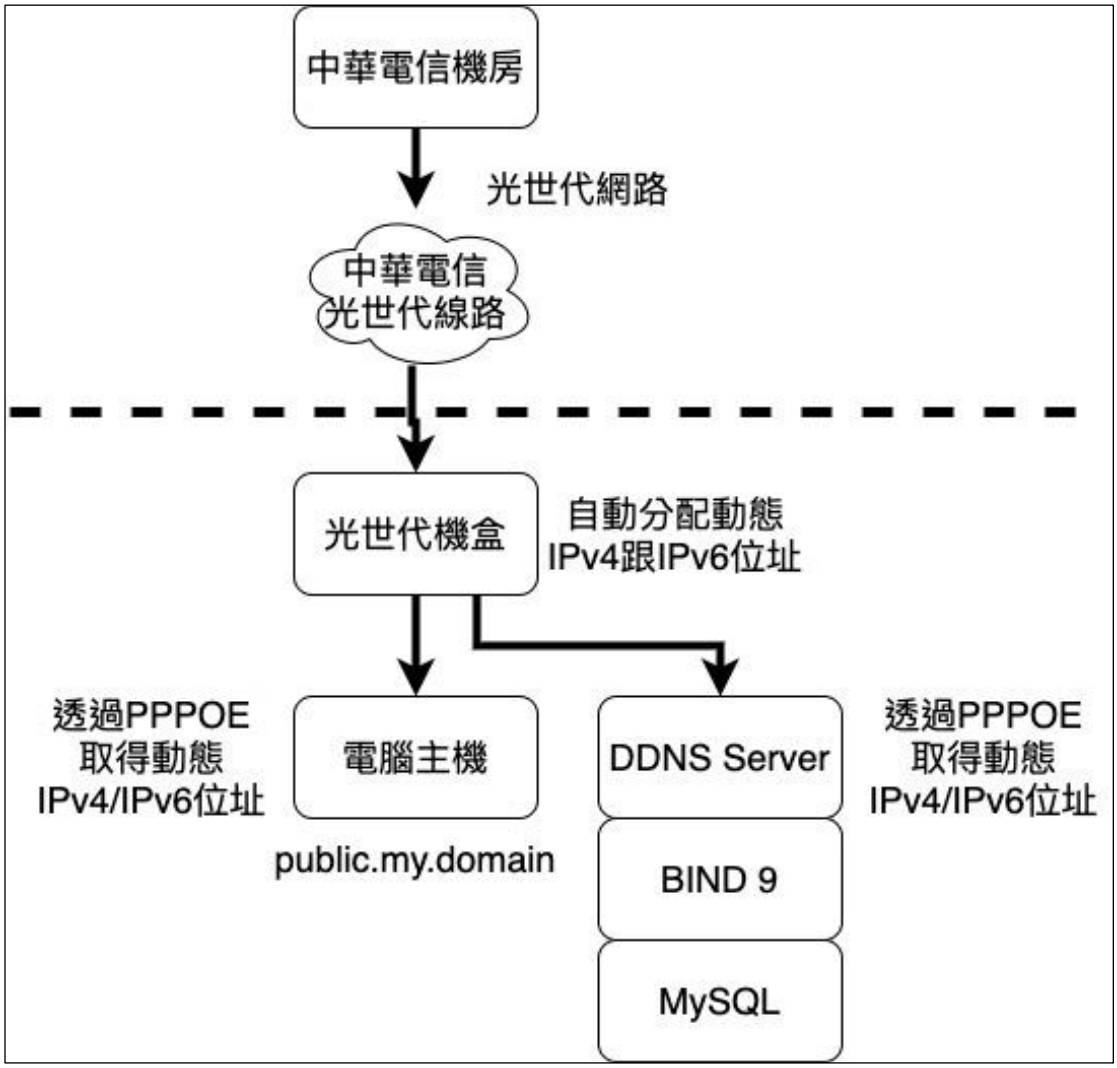



圖 64、動態 DNS 服務環境建置架構

**1. IPv4 環境部署建議**

在台灣申請中華電信光世代網路時,預設會提供動態 IP，並同時提供 IPv4 及 IPv6 雙協定位址，因此在測試動態 DNS 服務時，網路架構圖符合提案設計架構。

首先，不論是安裝動態 DNS Client 主機或架設動態 DNS Server 主機都需直接安裝在光世代機上盒之後直接連結，不可透過 NAT (Network Address Translation，網路位址轉換) 網路 IP 掩蔽機制處理，如果透過 NAT 主機，則 IPv4 會轉成 Private IP (私有 IP) 無法連到外部網路。多數用戶因為有多台電腦設備，因此會安裝 IP 分享器，只要透過 IP 分享器就會使用 NAT 做位址轉換，因此連接 IP 分享器後面的電腦所取得的 IPv4 位址都無法由外部連結，也無法作為動態 DNS 服務使用。

在本測試架構下，服務的主機跟架設動態 DNS Server 的主機都需要直接連結光世代主機，不可以連接在 IP 分享器後面，而且連接上網的方式都會是統一用 PPPoE (Point-to-Point Protocol over Ethernet,網路對等協定) 撥接方式取得 IP 位址。

**2. IPv4 環境下動態 DNS Client 連線測試**

要測試 IPv4 之動態 DNS Client 是否可以正常運作，只要在主機上啟動動態 DNS Client，透過 Windows 作業系統的指令〝ipconfig〞取得網路卡的 IP 位址，再比對動態 DNS Client 取得的 IP 位址是否相同，如果有多張網路卡時，則需要在動態 DNS Client 上指定要使用哪一個網路卡 IP 作為對外連線位址。

在啟動動態 DNS Client 之後，由於動態 DNS Client 需要將取得的 IP 位址傳給動態 DNS Server，以確保 BIND 9 可以

將網域跟 IP 做正確對應，因此測試時，可以連到動態 DNS Server，查看在動態 DNS Server 上記錄的網域與 IP 位址的對應表是否跟動態 DNS Client 傳過來的 IPv4 位址一樣。如果不一樣，則需要檢查網路是否連通、是否有防火牆設定、及動態 DNS Server 是否啟動等問題。下表為 IPv4 環境測試檢查表，本應用服務使用者可以利用本表進行服務運作評估。

表 50、IPv4 環境測試檢查清單

| 編號 | 項目 | 檢查結果 |
|---|---|---|
| 1 | 光世代網路連線是否正常？ | ☐是<br>☐否 |
| 2 | 檢查安裝 DDNS Client 的主機是否是透過 PPPoE 撥接方式取得 IPv4 位址？ | ☐是<br>☐否 |
| 3 | 動態 DNS Client 之 IPv4 是否只有一個 | ☐是<br>☐否 |
| 4 | 動態 DNS Client 顯示網域 IPv4 位址是否與動態 DNS Server 上顯示網域 IPv4 位址一致 | ☐是<br>☐否 |
| 5 | 動態 DNS Server 是否設定防火牆，如有是否允許動態 DNS Client 之 IPv4 位址連線 (Port 80 跟 443) | ☐是<br>☐否 |

## (二) 測試動態 DNS Client 在 IPv6 環境下運作

### 1. IPv6 環境部署建議

在正常情況下，如果直接透過光世代機上盒連結，會取得 2 個 IPv6 位址，在測試 IPv6 動態 DNS 服務是否正常時，需要安裝網路環境架構與 IPv4 相同，都需要直接連結在光世代機上盒後面，不可以連接 IP 分享器。主機獲得 IPv6 方式一樣透過 PPPoE，不要透過 DHCP 方式取得，如果透過 DHCP 取得 IP 位址，表示在該主機上游有使用 IP 分享器，此種情況下 IPv6 可以測試，但 IPv4 就無法測試動態 DNS 服務，為了確保測試

條件跟 IPv4 一致，建議主機透過 PPPoE 取得 IPv6 位址，也可以避免連結若發生問題時，多了 IP 分享器干擾不易除錯。網路測試環境越單純，讓測試方式更精確，降低干擾產生。

### 2. IPv6 環境下動態 DNS Client 連線測試

如果是申請中華電信光世代，並使用 PPPoE 取得 IP 位址，則測試方法跟檢查項目可以參考 IPv4 及 IPv6 環境測試檢查表進行檢測。IPv4 環境測試檢查表，請參考上一小節有詳細敘述及 IPv4 環境測試檢查清單。而 IPv6 環境測試檢查表，請參考下表所列清單，本應用服務使用者可以利用本表進行 IPv6 服務運作評估。

表 51、IPv6 環境測試檢查清單

| 編號 | 項目 | 檢查結果 |
|---|---|---|
| 1 | 光世代網路連線是否正常？ | □是<br>□否 |
| 2 | 檢查安裝 DDNS Client 主機是否是透過 PPPoE 撥接方式取得 IPv6 位址？ | □是<br>□否 |
| 3 | 動態 DNS Client 之 IPv6 是否可取得？ | □是<br>□否 |
| 4 | 動態 DNS Client 顯示網域 IPv6 位址是否與動態 DNS Server 上顯示網域 IPv6 位址一致 | □是<br>□否 |
| 5 | 動態 DNS Server 是否設定防火牆，如有是否允許動態 DNS Client 之 IPv6 位址連線 (Port 80 跟 443) | □是<br>□否 |

## (三)IPv4 及 IPv6 並存環境建置

### 1. IPv4 及 IPv6 並存環境建置

本計畫規劃之初即希望動態 DNS Server 同時支援 IPv4 及 IPv6 雙協定，因此在測試環境規劃上，和 IPv4-only 或 IPv6-only

測試方法一致，測試環境架構圖可參考本節〝(一) 動態 DNS 服務環境建置架構〞圖。

相同測試架構優點是清楚且易於尋找問題與進行故障排除，如果測試環境中增加其他設備如 IP 分享器、防火牆、交換機、路由器等，會讓測試複雜度變高，當發現動態 DNS 無法如預期正常運作時，應該考慮將光世代機上盒到主機之間連結的其他設備都移除，把不必要硬體設備都先移除，等故障排除之後，再逐一將實務上需要使用設備逐一加入。

**2. IPv4 及 IPv6 並存環境下動態 DNS Client 連線測試**

國內 IPv6 普及度已相當高，因此可以讓 IPv4 及 IPv6 同時進行測試。測試在 IPv4 及 IPv6 並存情況下動態 DNS 連線是否正常，可以使用下表檢查清單作為參考依據。

表 52、動態 DNS 重新連線測試檢查清單

| 編號 | 項目 | 檢查結果 |
|---|---|---|
| 1 | 將光世代盒子關閉電源之後重開，確認動態 DNS Client 是否可以取得新的動態 IPv4/IPv6？ | ☐是<br>☐否 |
| 2 | 關閉測試電腦 IPv6 功能，連線動態 DNS Server 時，是否可以透過 IPv4 正確連線到主機？ | ☐是<br>☐否 |
| 3 | 關閉測試電腦 IPv4 功能，連線動態 DNS Server 時，是否可以透過 IPv6 正確連線到主機？ | ☐是<br>☐否 |

在"IPv6 動態 DNS Server 軟體安裝建置手冊"內，有測試結果需要檢查動態 DNS 運作是否有啟動，且有連線成功。

更多詳細資訊請參考附錄七，有完整說明。

# 第三節 IPv6 動態 DNS 服務軟體手冊撰寫

本工作項目將依據〝IPv6 動態 DNS 服務軟體〞開發工作所完成成果，撰寫使用者手冊，供使用者下載、安裝及使用動態 DNS 服務軟體指南。

目前動態 DNS 軟體開發已經完成，包含軟體及使用者手冊都已放在網站上供使用者下載使用。使用者可以經由以下連結下載：

- 動態 DNS 軟體下載連結：

  https://ipv6.twnic.tw/promotion-ipv6-ddns.html

下圖為 IPv6 動態 DNS 軟體下載連結網站截圖：

圖 65、動態 DNS 軟體下載連結網站截圖

動態 DNS 軟體目前於網站上線外，並於 TANET 2020 網路研討會期間進行宣傳，文宣內容如下圖所示。目前動態 DNS 軟體下載數，截至今 (109) 年 10 月底已達 100 次。

圖 66、動態 DNS 軟體於 TANET 宣傳文宣

關於動態 DNS 軟體使用步驟及方法，更多詳細資訊請參考附錄七，有完整說明。

# 第六章 IASP 及 ICP IPv6 升級推廣

關於 IASP 及 ICP IPv6 升級推廣工作，目的在提升終端用戶使用 IPv6 網路服務，及企業網站升級支援 IPv6 連網，兩個面向持續推升國內 IPv6 使用比例，此工作項目共分 4 個子分項，包含：

- 推廣 Cable 用戶申請試用 IPv6。
- 推廣手機用戶下載 APN 設定 IPv6 APP。
- 與公協會合作推廣 IPv6。
- 推廣.tw 網站升級 IPv6。

各分項工作執行狀況及成果，如下所述。

## 第一節 推廣 Cable 用戶申請試用 IPv6

國內 IASP 在 IPv6 的支援上主要以行動和固網業者為主，Cable 業者在支援 IPv6 網路服務的推動上仍處於初期階段，直到去 (108) 年 6 月國內終於迎來第一家 Cable 業者台灣寬頻通訊 TBC 開始進行 IPv6 用戶申請試用。另外根據去 (108) 年對國內 Cable 業者所進行 IPv6 支援調查結果顯示，天外天數位有線電視、國聲有線電視及世新有線電視共3家業者,有在進行相關規劃,今 (109) 年計畫執行期間，再次徵詢業者進度及狀況，目前 3 家業者尚未有明確的時程規畫。因此今 (109) 年針對此工作項目合作推廣的 Cable 業者仍以 TBC 為主。

TBC 在有線電視系統寬頻上網服務支援 IPv6，領先國內其他業者，其推動過程得力於陳振珉執行長政策決定，因此透過設備汰舊換新過程，逐步布建完成基礎設施支援 IPv6 環境，並培養內部技術人員養成 IPv6 相關技能，透過實驗確認連網環境可支援，消費者端設

備也是透過多年逐步更換終端設備，在環境建置完成後，就可透過伺服器端決定是否配發 IPv6 位址，而不需要到府供裝，減少技術支援人力，並降低使用者申請使用 IPv6 的障礙。

因新冠肺炎傳染性疾病流行影響，上半年各式活動如座談會、展覽、論壇..等活動的舉辦大都受到限縮，因此也影響到推廣活動舉辦形式。因此於今 (109) 年 6 月 15 日拜訪 TBC 陳振珉執行長討論目前其 IPv6 推動現況及計畫，以下就會議討論內容整理：

- 目前 TBC 所擁有 IPv4 數量仍相當足夠，尚未有 IP 不足的狀況發生。
- TBC 在正式開放用戶申請試用 IPv6 之前，內部曾進行測試發現啟用 IPv6 會讓伺服器端承載資料流量過大，影響正常使用狀況，整體維運系統仍有技術上難度需克服。
- 目前全球 IPv6 網路環境尚未完善，網路系統仍以 IPv4/IPv6 雙協定運作為主，要支援雙協定系統所需的維運成本及人力負擔都會增加。
- 用戶對上網以穩定為第一要求，部分用戶對轉換新設備及新系統抱持質疑心態，IPv6 屬於基礎設施，較難對用戶行銷。
- Cable 業者若要支援 IPv4 及 IPv6 雙協定運作，同時配發 2 個 IP 給用戶端，需負擔 DHCP 配發 2 個 IP 的授權費用，對業者而言形成不小的成本壓力。
- 目前由需求面、技術面和成本考量，Cable 業者對推行 IPv6 商用仍有多面向問題須克服。
- TBC 目前還是維持開放給用戶申請試用 IPv6 的政策沒有改變。

經過會議討論後，TBC 除開放用戶申請試用，今 (109) 年在銷售策略也進行了 IPv6 發放原則調整，目前申請頻寬 500M (含) 以上的客戶，將採取免申請自動配發 IPv6 的方式，截至 7 月統計發放數累計共 983 客戶。截至今 (109) 年 10 月底完成 3,563 個客戶 IPv6 配發，順利達成年度推廣計畫。

使用者也可以到 TBC 下載專區取得 IPv6 服務申請書，填寫相關資料即可申請，TBC 會由伺服器端完成配發程序，不須到府進行工裝，用戶即可使用 IPv6 網路服務。下圖為 TBC 之 IPv6 服務申請書網路下載專區截圖畫面：

圖 67、TBC 之 IPv6 服務申請書網路下載專區

在 TBC 常見問題專區，另有開闢 IPv6 服務相關問題資訊，供用戶參考。下圖為 TBC 之 IPv6 服務常見問題專區截圖畫面：

圖 68、TBC 之 IPv6 服務常見問題專區

# 第二節 推廣手機用戶下載 APN 設定 IPv6 APP

本工作項目內容承接去 (108) 年「推動 IPv4/IPv6 雙軌普行方案」計畫所完成開發手機 APN 設定 IPv6 之 APP，今 (109) 年將進行 APP 下載推廣，增加手機用戶對 IPv6 使用。國內行動電信業者已經全面支援 IPv6，終端用戶設備同時啟動 IPv6 設定，使用者就可以升級以 IPv6 為優先採用協定，達到使用者無感升級的目標。

今 (109) 年因主要大型會議及展覽等活動延期或取消，因此除部份以實體活動宣傳之外，亦透過網路及教育訓練等方式進行推廣，主要推動管道整理如下：

- 社群論壇貼文推廣：於 IP/DNS 論壇、台灣網路資訊中心 (TWNIC) 電子報等進行貼文推廣。
- 教育訓練活動現場推廣：於「ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓」教育訓練課程現場進行推廣。
- 公協會發文推廣：透過公協會於會員專區、網站貼文、電子報等多廣道行銷。
- 經濟部工業局宣傳推廣：借助經濟部工業局透過電子郵件向國內企業宣傳。
- 中心舉辦交流推廣活動進行宣傳：透過中心舉辦網路、IP、RPKI 教育訓練、IPv6 推廣座談會等活動現場進行推廣。

下表提列今年度計畫執行期間，所進行推廣手機用戶下載 APN 設定 IPv6 APP 歷程紀錄：

表 53、推廣手機用戶下載 APN 設定 IPv6 APP 歷程

| 序號 | 工作項目 | 日期 |
|---|---|---|
| 1 | 於 IP/DNS 論壇，進行手機 APP 推廣。 | 109/3/31 |
| 2 | 於台灣網路資訊中心 (TWNIC) 電子報，4 月份封面故事撰文進行手機 APP 推廣。 | 109/4/1 |
| 3 | 於「ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓」第 1 場教育訓練課程，進行手機 APP 下載推廣。 | 109/4/29 |
| 4 | DTA (數位經濟暨產業發展協會) 協助，對會員進行宣傳手機 APP 下載推廣訊息。 | 109/4/28 |
| 5 | TCA (台北市電腦商業同業公會) 協助，於資訊月 Online 專區進行宣傳手機 APP 下載推廣訊息。 | 109/4/30 |
| 6 | 於「ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓」第 2 場教育訓練課程，進行手機 APP 下載推廣。 | 109/5/15 |
| 7 | 於「ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓」第 3 場教育訓練課程，進行手機 APP 下載推廣。 | 109/6/23 |
| 8 | TWNIC IP 會員會議暨 RPKI 教育訓練，進行手機 APP 下載推廣。 | 109/6/29 |
| 9 | 於「ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓」第 4 場教育訓練課程，進行手機 APP 下載推廣。 | 109/7/17 |
| 10 | 於「ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓」第 5 場教育訓練課程，進行手機 APP 下載推廣。 | 109/7/31 |
| 11 | 於「ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓」第 6 場教育訓練課程，進行手機 APP 下載推廣。 | 109/8/28 |
| 12 | 「ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓」第 7 場教育訓練課程，進行手機 APP 下載推廣。 | 109/9/18 |
| 13 | TWNIC 與高雄市電腦商業同業公會合作舉辦「2020 TWNIC IPv6 推廣講座活動」 | 109/9/25 |
| 14 | 於「ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓」第 8 場教育訓練課程，進行手機 APP 下載推廣。 | 109/9/30 |

下圖為於 IP/DNS 論壇，進行手機 APN 設定 IPv6 APP 下載推廣畫面截圖：

圖 69、IP/DNS 論壇進行手機 APP 推廣

下圖為台灣網路資訊中心 (TWNIC) 電子報，於 4 月份封面故事撰文進行手機 APP 下載推廣截圖畫面：

圖 70、TWNIC 電子報進行手機 APP 推廣

下圖為 TCA 協助，於資訊月 Online 專區，進行宣傳手機 APN 設定 IPv6 APP 下載訊息，推廣畫面截圖：

圖 71、TCA 協助進行手機 APP 推廣

手機啟動 IPv4/IPv6 網路設定 APP 專為 Android 手機所設計應用程式，於民國 108 年 9 月完成，並於同年 10 月完成上架 Google Play。以下提列手機 APN 設定 IPv6 APP 下載次數統計資料，今年計畫目標預計達成總量 500 次下載量已經如期完成，下表為統計結果，截至今(109) 年 10 月 31 日下載總數達 624 次，依照月份統計下載次數資料如下表所示：

表 54、手機啟動 IPv4/IPv6 網路設定 APP 下載次數統計表

| 統計區間 | 下載次數 |
|---|---|
| 民國 108 年 10 月 | 17 |
| 民國 108 年 11 月 | 2 |
| 民國 108 年 12 月 | 6 |
| 民國 109 年 1 月 | 6 |
| 民國 109 年 2 月 | 7 |
| 民國 109 年 3 月 | 19 |
| 民國 109 年 4 月 | 30 |
| 民國 109 年 5 月 | 28 |
| 民國 109 年 6 月 | 41 |
| 民國 109 年 7 月 | 85 |
| 民國 109 年 8 月 | 69 |
| 民國 109 年 9 月 | 260 |
| 民國 109 年 10 月 | 54 |
| **總計** | **624** |

下圖為手機 APN 設定 IPv6 APP 下載次數，在 Google Play 商店下載統計趨勢圖：

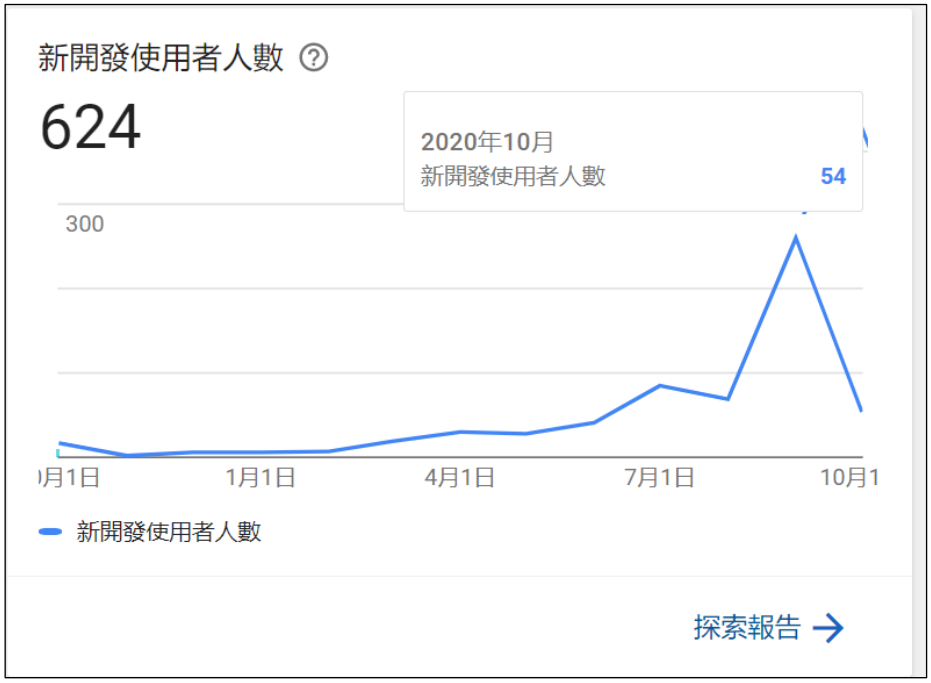



圖 72、Google Play 商店下載統計趨勢圖

# 第三節 與公協會合作推廣 IPv6

今年與各公協會接洽合作對象包含 TiEA (台灣網路暨電子商務產業發展協會)、DTA (數位經濟暨產業發展協會)、TCA (台北市電腦商業同業公會)、CBIT (台灣有線寬頻產業協會)、TWIA (台灣網際網路協會)、DSMA (台灣數位應用多媒體協會)、TAICS (台灣資通產業標準協會)、台灣數位科技與政策協進會、HIT (社團法人台灣駭客協會)、及 KCA (高雄市電腦商業同業公會) 等 10 家。並透過經濟部工業局協助轉發 IPv6 教育訓練課程訊息予 TEEMA (台灣區電機電子工業同業公會，Taiwan Electrical and Electronic Manfacturers' Association)，向協會會員推廣宣傳 IPv6 升級資訊。

詳細與各公協會合作推廣 IPv6 升級所進行相關活動，合作狀況及推動成果將個別敘述如下。

## 一、TiEA (台灣網路暨電子商務產業發展協會)

台灣網路暨電子商務產業發展協會 (Taiwan Internet and E-Commerce Association，TiEA) 成立於西元 2012 年 (民國 101 年) 10 月 24 日，會員涵蓋國際網路公司、台灣電子商務公司、社群網站、網路行銷、網路媒體，以及金融、旅遊、物流、數位內容產業等領域企業，是台灣目前匯集最多網路及電子商務業者的協會組織。[14]

目前 TiEA 會員數超過 170 個，會員名單包含國內外知名電商及平台業者，是極具代表性的電子商務協會。

下表為 TWNIC 與 TiEA 合作進行 IPv6 推廣活動，雙方交流活動及執行資訊列表。

表 55、與 TiEA 合作推廣 IPv6 歷程

| 序號 | 工作項目 | 日期 |
|---|---|---|
| 1 | 拜訪 TiEA，討論向 TiEA 會員宣傳網站升級 IPv6，討論議題包含：<br>● 進行與 TiEA 共同合作舉辦及參與雙方相關講座和活動可行性討論。<br>● 提議 TiEA 協助向其會員宣傳 TWNIC 主辦的 IPv6 教育訓練。 | 109/1/17 |
| 2 | 規劃 IPv6 推廣交流活動建議，徵詢 TiEA 意見及可行性。 | 109/2/7 |
| 3 | TiEA 轉發 TWNIC 於 5 月 15 日所主辦「ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓教育訓練」課程，邀請會員參與。 | 109/5/6 |

TiEA 為本年度最早接觸協會，針對雙方共同合作舉辦及參與雙方相關講座和活動意願相當高，但因新冠肺炎疫情影響上半年的集會活動，因此無法順利進行而改由 TiEA 透過官網、會員社群、E-Mail 等管道，進行靜態推廣活動。

下圖為 TiEA 轉發 TWNIC 教育訓練課程資訊，邀請會員參與 TWNIC 所舉辦的 IPv6 教育訓練課程活動截圖：

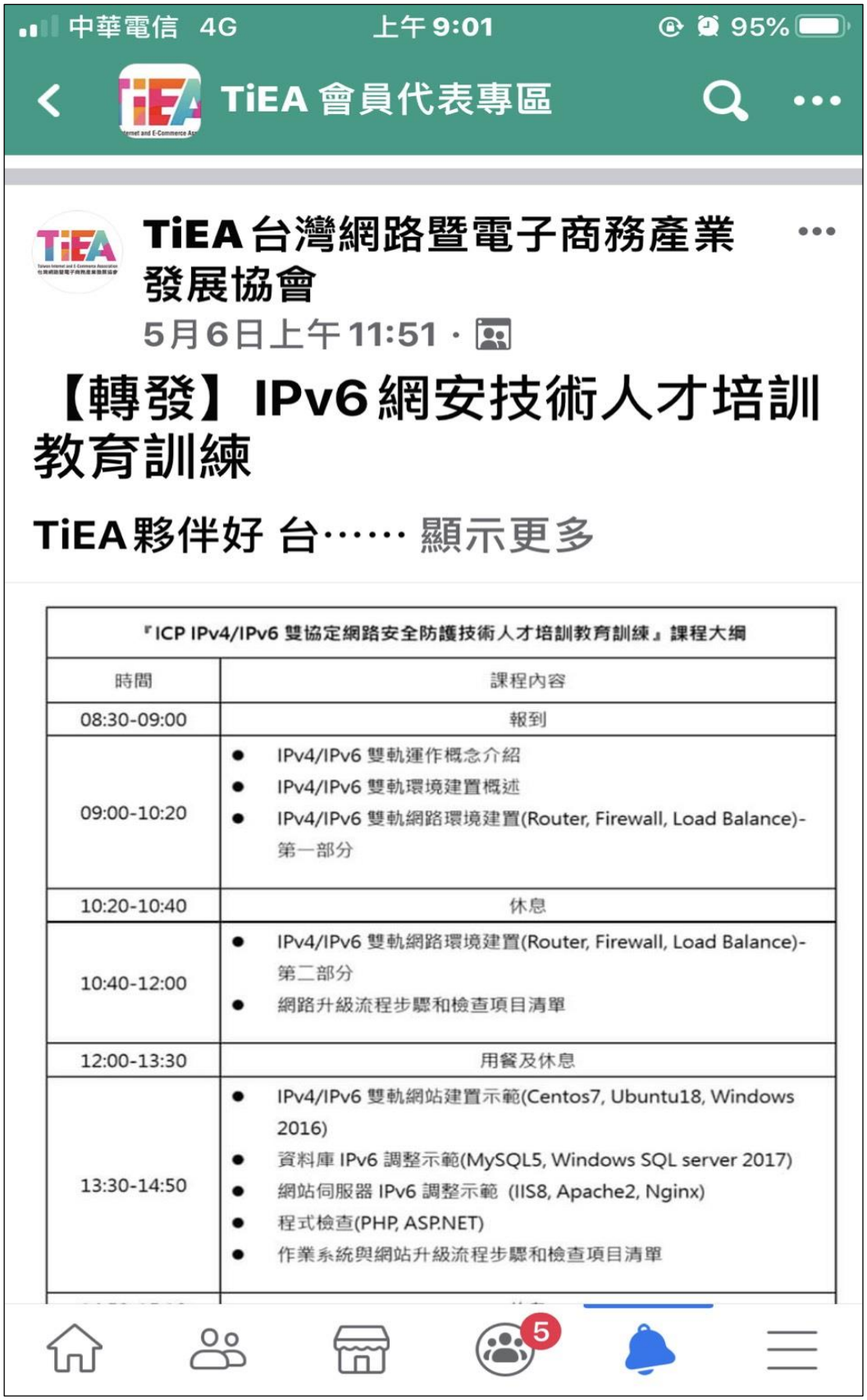



圖 73、TiEA 轉發 TWNIC 教育訓練課程資訊

## 二、DTA (數位經濟暨產業發展協會)

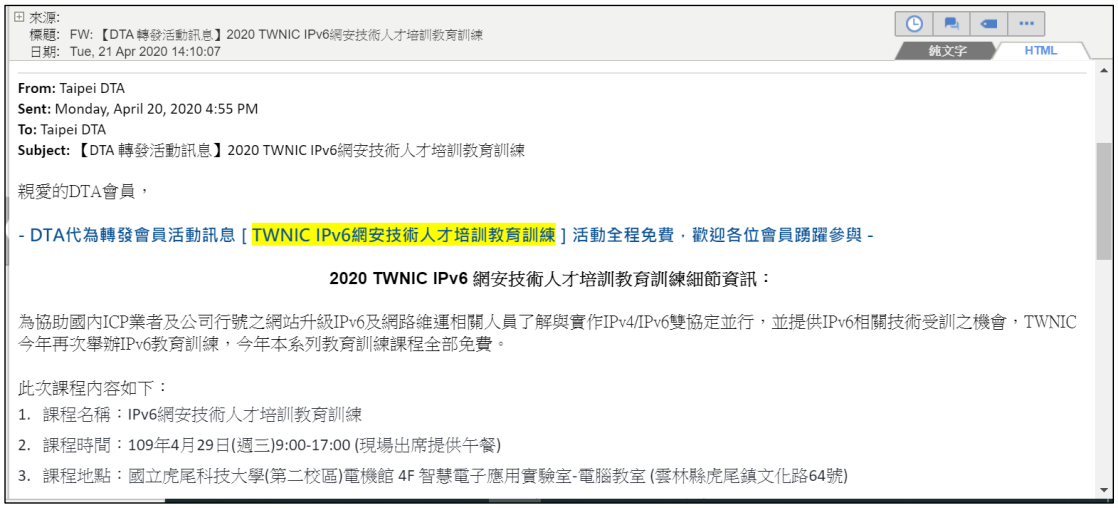
數位經濟暨產業發展協會 (Digital Transformation Association，DTA) 前身為以推廣資訊治理及資訊服務管理為目標的台灣科技化服務協會 (itSMA) 。itSMA 成立超過十年，積極推動公私部門注重資訊治理與資訊服務管理，已產生成效，可謂完成階段性任務。適逢行政院推出「數位國家・創新經濟」發展方案 (簡稱 DIGI+方案) ，旨在推動台灣朝向「數位經濟」 (Digital Economy) 發展。期望透過數位產業帶動經濟活動，以建構富裕數位國家為目標。為掌握趨勢脈動，因應時局變遷，遂進行更名，以符合政府與產業之需求與期待。[15]

下表為 TWNIC 與 DTA 合作進行 IPv6 推廣活動，雙方交流活動及執行資訊列表。

表 56、與 DTA 合作推廣 IPv6 歷程

| 序號 | 工作項目 | 日期 |
|---|---|---|
| 1 | DTA 來訪討論和 TWNIC 年度合作規劃。 | 109/1/17 |
| 2 | ● 討論與 DTA 合作舉辦講座推廣 網站升級 IPv6。<br>● 邀請 DTA 會員和新創團隊參與 TWNIC 舉辦「IPv6 網路安全技術人才培訓」教育訓練。<br>● TWNIC 將提供以下資料予 DTA，待 DTA 內部審核通過後，將於協會官方網站進行刊登推廣 IPv6 的電子報分享資訊。<br>● TWNIC 將提供 IP 位址優惠方案和相關資訊予 DTA，廣邀台灣新創團隊申請優惠方案。 | 109/2/7 |
| 3 | DTA 轉發 TWNIC 於 4 月 29 日所主辦「ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓教育訓練」課程，邀請會員參與。 | 109/4/20 |

下圖為 DTA 轉發 TWNIC 於 4 月 29 日所主辦「ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓教育訓練」課程，邀請會員參與截圖畫面。


來源:
標題: FW:【DTA 轉發活動訊息】2020 TWNIC IPv6網安技術人才培訓教育訓練
日期: Tue, 21 Apr 2020 14:10:07

純文字 HTML

**From:** Taipei DTA
**Sent:** Monday, April 20, 2020 4:55 PM
**To:** Taipei DTA
**Subject:** 【DTA 轉發活動訊息】2020 TWNIC IPv6網安技術人才培訓教育訓練

親愛的DTA會員，

- DTA代為轉發會員活動訊息 [ TWNIC IPv6網安技術人才培訓教育訓練 ] 活動全程免費，歡迎各位會員踴躍參與 -

**2020 TWNIC IPv6 網安技術人才培訓教育訓練細節資訊：**

為協助國內ICP業者及公司行號之網站升級IPv6及網路維運相關人員了解與實作IPv4/IPv6雙協定並行，並提供IPv6相關技術受訓之機會，TWNIC今年再次舉辦IPv6教育訓練，今年本系列教育訓練課程全部免費。

此次課程內容如下：

1. 課程名稱：IPv6網安技術人才培訓教育訓練
2. 課程時間：109年4月29日(週三)9:00-17:00 (現場出席提供午餐)
3. 課程地點：國立虎尾科技大學(第二校區)電機館 4F 智慧電子應用實驗室-電腦教室 (雲林縣虎尾鎮文化路64號)

圖 74、DTA 轉發 TWNIC 教育訓練課程資訊

## 三、TCA (台北市電腦商業同業公會)

台北市電腦商業同業公會 (Taipei Computer Association，TCA) ，簡稱「台北市電腦公會」，於西元 1974 年 (民國 63 年) 11 月 5 日成立，以推廣台灣資訊產業發展為主。除針對資訊產業進行相關交流活動，另外也主辦國內各大資訊展覽，及組團參與國際性資訊展覽，是台灣資訊產業公協會重量級的組織。[16~17]

會員數由西元 1974 年 (民國 63 年) 成立之初的 15 個會員，成長到西元 2019 年 (民國 108 年) 已經有超過 4,000 個會員。台北市電腦商業同業公會的成立，也見證了國內資訊產業蓬勃發展的歷程。

下表為 TWNIC 與 TCA 合作進行 IPv6 推廣活動，雙方交流活動及執行資訊列表。[18~19]

表 57、與 TCA 合作推廣 IPv6 歷程

| 序號 | 工作項目 | 日期 |
|---|---|---|
| **1** | 拜訪 TCA 討論於 TCA 年度主辦活動智慧城市展，進行 IPv6 合作推廣事宜。 | 109/2/25 |
| **2** | TCA 主辦生活智慧科技活動承辦人來訪，討論推廣 IPv6 合作可行方案。 | 109/4/9 |
| **3** | TCA 於資訊月 Online/政府資訊與前瞻服務，推廣「ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓」第 1 場教育訓練課程活動。 | 109/4/28 |
| **4** | TCA 協助推廣 IPv6 部署、第 2 場 ICP IPv4/IPv6 雙協定教育訓練課程活動訊息刊登、及手機啟動 IPv4/IPv6 網路設定 APP 下載連結宣傳。 | 109/4/30 |
| **5** | TCA 協助推廣第 3 場 ICP IPv4/IPv6 雙協定教育訓練課程活動訊息刊登。 | 109/6/11 |
| **6** | TCA 協助推廣第 4 場 ICP IPv4/IPv6 雙協定教育訓練課程活動訊息刊登。 | 109/7/3 |

下圖為 4 月 28 日 TCA 於〝資訊月 Online〞的小編資訊關於〝政府資訊與前瞻服務〞類別，進行 IPv6 推廣介紹，及「ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓」第 1 場教育訓練課程活動推廣截圖畫面。[18]

圖 75、TCA 於 4 月 28 日在資訊月 Online 進行 IPv6 活動宣傳截圖

4 月 30 日 TCA 於〝資訊月 Online〞的小編資訊關於〝政府資訊與前瞻服務〞類別，進行 IPv6 部署推廣、「ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓」第 2 場教育訓練課程活動刊登、及手機啟動 IPv4/IPv6 網路設定 APP 下載連結宣傳。下圖為此次所刊登的內容截圖畫面。[19]

圖 76、TCA 於 4 月 30 日在資訊月 Online 進行 IPv6 活動宣傳截圖

TCA 在 6 月 11 日與 7 月 3 日協助於〝資訊月 Online〞的小編資訊關於〝政府資訊與前瞻服務〞類別，進行「ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓」第 3 場及第 4 場教育訓練課程活動刊登，

並進行台灣 IPv6 高使用率的宣傳內容。以下圖示為所刊登的內容畫面截圖。

圖 77、TCA 於 6 月 11 日協助進行 IPv6 教育訓練宣傳截圖

圖 78、TCA 於 7 月 3 日協助進行 IPv6 教育訓練宣傳截圖

## 四、2020 網路共贏時代專家座談會

由台灣網路資訊中心 (TWNIC) 於7月29日 (星期三) 主辦2020【網路·共贏時代】專家座談會，邀請網際網路產業包含軟體、硬體、服務及應用等相關公協會共同參與及協辦，並派專家代表參與進行座談。[57]

參與此次專家座談活動協會，包含台灣有線寬頻產業協會(Cable Broadband Institute in Taiwan，CBIT)、數位經濟暨產業發展協會 (Digital Tranformation Association，DTA)、台灣網際網路協會(Taiwand Internet Association，TWIA)、台灣數位應用多媒體協會(Digital Solutions Multimedia Asia Taiwan，DSMA Taiwan)、台灣資通產業標準協會 (Taiwan Association of Information and Communication Standards，TAICS)、台灣數位科技與政策協進會(Digital Taiwan Roundtable，DTR)等6家。下圖為當天座談會活動現場照片：

圖 79、2020【網路·共贏時代】專家座談會活動現場照片

當天對談主要聚焦於因應網路數位時代來臨，產業發展數位化已成必然趨勢，唯有打造堅實的數位基磐，建構健全的網路建設環境，才得以讓多元的數位應用、創新技術蓬勃發展。對談內容分為台灣網路發展趨勢及 IPv6 關鍵應用兩大主題。

活動議程如下表所示：

表 58、2020【網路·共贏時代】專家座談會活動議程

| 時間 | 議程 | 講者/與會代表 |
|---|---|---|
| **13:30~14:00** | 來賓報到 | |
| **14:00~14:10** | 【開場引言】 | 黃亮崢／數位時代創新長 |
| **14:10~14:20** | 【趨勢觀點】 | 黃勝雄／財團法人台灣網路資訊中心董事長暨執行長 |
| **14:20~15:40** | 【焦點對談】<br>台灣網路發展趨勢與IPv6關鍵應用 | 主持人:黃亮崢／數位時代創新長<br>與談貴賓 ：<br>● 黃勝雄／財團法人台灣網路資訊中心董事長暨執行長<br>● 沈信雄／國家通訊傳播委員會射頻與資源管理處號碼網址科科長<br>● 陳振珉／台灣有線寬頻產業協會理事<br>● 白璧珍／台灣數位應用多媒體協會理事<br>● 許建昌／台灣資通產業標準協會執行秘書<br>● 詹婷怡／數位經濟暨產業發展協會副理事長<br>● 台灣大哥大 柯正義處長／台灣網際網路協會團體會員代表<br>● 網擎資訊 廖長健執行長／台灣數位科技與政策協進會代表 |
| **15:40~16:00** | 會後交流 | |

以下就專家座談內容進行重點節錄。主持人《數位時代》創新長黃亮崢解析，網際網路在全球爆發以來，IPv6標準已公布20多年，著眼於未來網路建構環境，與會者無不努力落實於應用環境，台灣因應趨勢與挑戰，亟需集思廣益，解決問題。

台灣網路資訊中心董事長黃勝雄於「趨勢觀點」議程中指出，IPv4一直都有位址不足的缺點，亞太網路資訊中心 (APNIC) 統計，台灣IPv6網路普及率提升到47%，加上5G正式商轉，各國陸續發照開台，乃當前共同趨勢，IPv4轉移至全球通用的IPv6勢必加快速度，台灣行動業者的準備度很高，電子商務線上交易應急起直追，尤其在疫情襲捲後，傳統企業不得不轉型網路企業，轉移網路資源不足的IPv4為IPv6，是企業界提前部署的關鍵對策。

黃勝雄董事長直指：「以往推動IPv6的障礙是對企業界缺乏商業誘因。」如今IPv6核心網路交換設備可對接國外，數位環境成熟，國際及全世界最強大的個人裝置Apple要求我國比照全球採行IPv6基礎設施， 臺灣再不轉換也不行，業界為能順利使用網路，動機變強，固網、家用設備同樣隨著汰換以迎接5G世代，例如年輕人不再花錢租用光纖而直接使用手機IPv6上網，情勢樂觀，企產業界應儘早採用IPv6，才不致日後又投資切換IPv6網路服務，影響業務。

議程進行到「焦點對談」，由與談貴賓剖析IPv6關鍵應用與台灣網路發展趨勢。數位經濟暨產業發展協會副理事長詹婷怡發言， 西元2017至2018年之前，因牽涉到網路環境如終端設備、應用內容、網路使用，推動IPv6有困難，西元2017年底之後，站在資訊安全與網路環境建構角度，該協會是重要的協力推動單位，正式宣告IPv6普及，讓終端設備與應用服務跟上來，AIoT尤應準備好使用IPv6，開展未來。

國家通訊傳播委員會射頻與資源管理處號碼及網址管理科科長沈信雄說，IPv6推動後的成長率激增，原來是工程師等一線人員樂於使用，最近調查顯示相關產業者有逾7成使用IPv6，感謝電信業者率先使用，IPv6是未來產業界必然需要採用的技術標準，盡早開始當然較能掌握商機。

台灣數位科技與政策協進會代表廖長健分享，西元2017年底和政府合作開發IPv6，卻缺乏測試環境，直到西元2018年隨著電信業者的拓展腳步，並有大專院校等100所學校成為郵件伺服器 (mail server) 設定後的測試對象，溝通變得容易，此後的網路通訊設備採購上也能支援IPv6，幾乎所有政府單位、學術網路客戶都用IPv6，企業界用戶也跟著要求使用其所開發的雲端伺服器收受郵件，可見政府運用採購的力量加以推動，經過3年多努力，總算讓大家瞭解到要用IPv6，才跟得上未來網路趨勢。

深度交流當中，台灣有線寬頻產業協會理事陳振珉建議，有線寬頻業者要做的就是把支援IPv6機上盒具體實現以展現其實際效用；數位經濟暨產業發展協會副理事長詹婷怡重申，順著數位轉型IoT、5G的趨勢，IPv6網路連線傳輸速度快，具有競爭力，更便利於推行。

台灣網路資訊中心董事長黃勝雄提醒，對於IPv4網址的供應應予控制，防範網路犯罪不停地經由NAT網路位址伺服器，轉換IP位址，偵查不易，再者，以前大家總認為對內網放心、對外網不放心，其實現在資訊安全事件往往是滲透更新頻率較低的封閉型內網所產生，要做到資安防護，就要更新網路，因而每個IP都必須是全球獨一無二的位址才對，中間不再有NAT轉換代理角色存在；台灣網際網路協會團體會員代表柯正義持正面觀點，IPv6做身分認證好用且速度快，不必先發短訊確認身分，更適合電子商務應用。

「網際網路創新應用是必然的趨勢。」主持人黃亮崢結語，臺灣數位環境先進，政府推動IPv6的硬體與電信環境成熟，普及率來到隨時過半的里程碑，譬如中華郵政、台灣土地銀行、統一超商等等機關行號網站都已完成IPv6升級，相信新產業、新應用與IPv6接軌，超前部署資安服務與未來數位化競爭，先練兵再打國際盃，產業輸出、外交雙贏局面可成，台灣一定能做到。

## 五、HIT (社團法人台灣駭客協會)

台灣駭客年會 (Hacks In Taiwan Conference，HITCON) 致力於推廣資訊安全，自 2005 年起舉辦大型研討會與中小型座談會，結合時事探討全世界熱門的資安議題，引入國內外專業講者的教育訓練課程，協助政府、企業、民間建立友善的溝通管道與培訓資源，引領世界資安技術的脈動。並成立社團法人台灣駭客協會 (Hacks In Taiwan，HIT)，為臺灣資訊安全盡一份心力。

HITCON年度會議已經超過15年，為臺灣歷史最悠久、參與人數最多的資安技術社群活動，是國內駭客們一年一度重要技術及交流的聚會。

臺灣因為疫情控制得宜，陸續開始放寬集會規定，讓原本考慮舉辦線上會議的HITCON CMT社群場次，及原本在年底舉辦的HITCON Pacific場次，決定在今 (109) 年9月11日 (星期五) ～ 9月12日 (星期六) 聯合舉辦實體活動，於中央研究院人文社會科學館舉行；為了兼顧許多海外講師以及不克前來現場參加實體活動的會眾，除了實體會議外，同時開放線上參與。

TWNIC為本次贊助者之一，並榮幸受邀進行〝國際及台灣IPv6發展介紹〞，透過本次機會得以和台灣駭客圈進行實質交流及推廣

IPv6，讓更多網路相關產業人士了解下一代網際網路協定IPv6的重要性，藉此向更多網路內容產業相關業者說明台灣IPv6網路環境的進展，讓更多網路業者能提早進行因應措施。下圖為本次進行IPv6介紹及推廣實際現場活動照片。[55]

圖 80、TWNIC 於 HITCON 2020 進行〝國際及台灣 IPv6 發展介紹〞

## 六、KCA (高雄市電腦商業同業公會)

高雄市電腦商業同業公會 (Kaohsiung Computer Association，KCA) 成立於西元1984年 (民國73年)，由設立於高雄市區域之電腦公司所組成，以推廣電腦應用、促進經濟發展、協調同業團結及增進共同利益為宗旨。西元1984年 (民國73年) 7月舉辦第一屆高雄市電腦展，為高雄市推動資訊新知邁開一大步，初期創會時期會員家數為25家，

近幾年來在歷屆理監事及會員的熱心參與及支持下，目前會員編號已超過三仟捌佰，為台灣第二大電腦公會組織。

今 (109) 年IPv6推廣活動，希望擴大推廣地域性，因此由TWNIC協同高雄市電腦商業同業公會合作於高雄舉辦一場活動，本次活動於9月25日舉辦，活動名稱為【2020 TWNIC IPv6推廣講座活動】，內容主要分為兩大部分，分別為主題演講及座談會交流。本次活動主題演講題目包含：[56]

- 國內外IPv6發展現況及應用服務介紹
- IPv6網路安全探討

而座談會將邀請KCA會員進行〝建置支援IPv6網路服務經驗分享〞，希望透過產業實際升級及使用經驗分享，以鼓勵同業之間進行技術交流及連網服務升級支援IPv6的意願，以持續進行產業升級，並向佈建完善的IPv6網路環境前進。

下圖為本次活動刊登於KCA協會網站所進行的活動宣傳推廣頁面截圖：

圖 81、【2020 TWNIC IPv6 推廣講座活動】活動宣傳頁面

本次活動議程如下表所示：

表 59、2020 TWNIC IPv6 推廣講座活動議程

| 時間 | 議程 | 內容 |
|---|---|---|
| **PM 1:30~2:00** | 報到 | |
| **PM 2:00~2:10** | 來賓致詞 | 高雄市電腦商業同業公會<br>陳力新 常務監事 |
| **PM 2:10~3:10** | 主題演講 | 國內外 IPv6 發展現況及應用服務介紹<br>講者：<br>鄭進興 老師 國立高雄科技大學資管系 |
| **PM 3:10~3:30** | 茶敘 | |
| **PM 3:30~4:30** | 主題演講 | IPv6 網路安全探討<br>講者：<br>林敬皇 博士 安華聯網科技股份有限公司<br>技術服務處 協理 |
| **PM 4:30~5:00** | 座談會<br>交流 | 建制支援 IPv6 網路服務經驗分享<br>主持人：鄭進興 老師、林敬皇 博士 |

本次活動為今年計畫在南部唯一一場和協會合作共同舉辦 IPv6 推廣活動，經由高雄市電腦商會同業公會進行推廣，共有 38 人報名參與，隸屬於高雄市電腦商業同業公會會員報名人數為 26 人，另有非隸屬於高雄市電腦商業同業公會的報名人數 12 人，活動參與者以科技公司為主。下圖為本次活動現場照片：

圖 82、【2020 TWNIC IPv6 推廣講座活動】現場照片

今年計畫目標需達成至少和5家公協會合作，進行各項IPv6推廣活動，雖然在疫情影響之下，活動舉辦多所限制，在此嚴苛狀況之下仍依照原定計畫完成多項實體活動及各式靜態推廣宣傳，包括：和3家公協會進行多次IPv6教育訓練課程及APP推廣、參與HITCON會議進行IPv6推廣主題演講、主辦一場IPv6推廣主題演講及講座活動、邀請多家公協會代表進行專家座談會、透過經濟部工業局協助向台灣區電機電子工業同業公會TEEMA發出IPv6教育訓練課程宣傳等。

下表整理本計畫執行期間和各公協會所合作進行各項IPv6推廣活動資訊：

表 60、109 年計畫和公協會所合作進行各項 IPv6 推廣活動資訊

| 序號 | 協會名稱 | 活動類型 | 活動名稱 |
|---|---|---|---|
| 1 | 台灣網路暨電子商務產業發展協會 (TiEA) | 教育訓練推廣 | IPv6網安技術人才培訓教育訓練 |
| 2 | 數位經濟暨產業發展協會 (DTA) | 教育訓練推廣及座談會 | ●IPv6網安技術人才培訓教育訓練<br>●2020【網路·共贏時代】 |
| 3 | 台北市電腦商業同業公會 (TCA) | 教育訓練及APP推廣 | ●IPv6網安技術人才培訓教育訓練<br>●IPv4/IPv6網路設定APP |
| 4 | 台灣有線寬頻產業協會 (CBIT) | 座談會 | 2020【網路·共贏時代】 |
| 5 | 台灣網際網路協會 (TWIA) | 座談會 | 2020【網路·共贏時代】 |
| 6 | 台灣數位應用多媒體協會 (DSMA) | 座談會 | 2020【網路·共贏時代】 |
| 7 | 台灣資通產業標準協會 (TAICS) | 座談會 | 2020【網路·共贏時代】 |
| 8 | 台灣數位科技與政策協進會 | 座談會 | 2020【網路·共贏時代】 |
| 9 | 社團法人台灣駭客協會 (HIT) | 主題演講 | HITCON 2020 |
| 10 | 高雄市電腦商業同業公會 (KCA) | 主題演講及座談會 | 2020 TWNIC IPv6推廣講座活動 |
| 11 | 台灣區電機電子工業同業公會 (TEEMA) | 教育訓練推廣 | IPv6網安技術人才培訓教育訓練 (由經濟部工業局協助) |

## 第四節 推廣.tw 網站升級 IPv6

推廣.tw 網站升級 IPv6 工作項目，主要推動為承接上一項工作，透過和公協會合作進行 IPv6 推廣活動，透過向協會會員推廣網站升級 IPv6 教育課程、國內 IPv6 使用現況分享、IPv6 資訊安全防護議題等資訊。鼓勵各協會會員進行企業網站 IPv6 升級，本次計畫新增 50 家.tw 網站升級 IPv6，目前已經達成計畫目標，新增升級支援 IPv6 網站列表如下所示：

表 61、推廣.tw 網站升級 IPv6 列表

| 序號 | 公司名稱 | 網站 |
|---|---|---|
| 1 | 中華郵政股份有限公司 | www.postmall.com.tw |
| 2 | 台灣明尼蘇達礦業製造股份有限公司 | www.3m.com.tw |
| 3 | 松果購物股份有限公司 | www.pcone.com.tw |
| 4 | 高高科技有限公司 | www.gogovan.tw |
| 5 | 塔圖科技股份有限公司 | www.tagtoo.com.tw |
| 6 | 網鈺數位科技有限公司 | catino.com.tw |
| 7 | 歐德堡股份有限公司 | www.orderble.com.tw |
| 8 | 捷毅國際股份有限公司 | zh-tw.jetone.com.tw |
| 9 | 羽昇國際股份有限公司 | www.wingwill.com.tw |
| 10 | 飛泓科技股份有限公司 | www.pixis.com.tw |
| 11 | 德安資訊股份有限公司 | www.athena.com.tw |
| 12 | 睿采數位科技股份有限公司 | www.smarten.com.tw |
| 13 | 香草魔法學苑 | www.herbcare.com.tw |
| 14 | 創鈺國際科技股份有限公司 | web.creatidea.com.tw |
| 15 | 易利信國際股份有限公司 | www.groundworks.com.tw |
| 16 | 台灣資料科學股份有限公司 | www.tdsc.com.tw |
| 17 | 研華股份有限公司 | www.advantech.tw |
| 18 | 時報資訊股份有限公司 | info.infotimes.com.tw |
| 19 | 辛格瑪國際科技股份有限公司 | www.sigmainfo.com.tw |
| 20 | 眾至資訊股份有限公司 | www.sharetech.com.tw/zh-tw/ |
| 21 | 真福電子股份有限公司 | www.trueful.com.tw |

| 序號 | 公司名稱 | 網站 |
|---|---|---|
| 22 | 佳瑋科技股份有限公司 | www.jarway.com.tw |
| 23 | 全漢企業股份有限公司 | www.fsp-group.com.tw |
| 24 | 法亞科技整合行銷股份有限公司 | www.faya.com.tw |
| 25 | 美商英特爾亞太科技有限公司<br>台灣分公司 | www.intel.com.tw |
| 26 | 大樣光電科技有限公司 | www.proled.com.tw |
| 27 | 巨石電腦有限公司 | www.gscc.net.tw |
| 28 | 瑞朋科技股份有限公司 | www.avlab.com.tw |
| 29 | 創為精密材料股份有限公司 | www.amtouch.com.tw |
| 30 | 普雷威股份有限公司 | www.playwith.com.tw |
| 31 | 知能系統整合股份有限公司 | www.omnisi.com.tw |
| 32 | 伯茂事業股份有限公司 | www.posmart.com.tw |
| 33 | 笛雅科技股份有限公司 | www.diyatech.com.tw |
| 34 | 世雅育樂股份有限公司 | www.segataiwan.com.tw |
| 35 | 柏策科技有限公司 | www.netone.com.tw |
| 36 | 若水國際股份有限公司 | www.flow.tw |
| 37 | 可立可股份有限公司 | www.kkco.com.tw |
| 38 | 信諾科技有限公司 | www.utrust.com.tw |
| 39 | 瑞元資訊股份有限公司 | www.toplink.com.tw |
| 40 | 統一超商股份有限公司 | www.7-11.com.tw |
| 41 | 總太地產開發股份有限公司 | www.zongtai.com.tw |
| 42 | 景岳生物科技股份有限公司 | www.genmont.com.tw |
| 43 | 一零四資訊科技股份有限公司 | corp.104.com.tw |
| 44 | 偉全實業股份有限公司 | www.wisher.com.tw |
| 45 | 翔耀實業股份有限公司 | www.enlightcorp.com.tw |
| 46 | 宣揚電腦顧問股份有限公司 | www.bethel.com.tw |
| 47 | 新算科技股份有限公司 | www.reality.com.tw |
| 48 | 亞欣數位科技有限公司 | www.yesphone.com.tw |
| 49 | 大林電子企業行 | www.dalin.com.tw |
| 50 | 泰緯自動科技有限公司 | www.tai-wei.com.tw |

下列以中華郵政網站作為範例，驗證網站支援 IPv6 網路連結，由以下截圖顯示網站 IP 位址資訊為 IPv6 格式，顯示官網主頁面可以提供用戶設備以 IPv6 連結此網站。

圖 83、驗證網站支援 IPv6 位址資訊截圖

並以 https://www.gsnv6.tw/inventory/checkservicepub.cgi 測試網站，對上列網頁進行支援 IPv6 連線檢驗，其服務可正常連線，結果如下圖所示：

圖 84、檢測網站支援 IPv6 服務可正常連線截圖

下圖以 IPv6 test https://ipv6-test.com/validate.php 測試網站，進行網站 IPv6 支援檢測，顯示本網站已經支援 IPv6，結果如下圖所示：

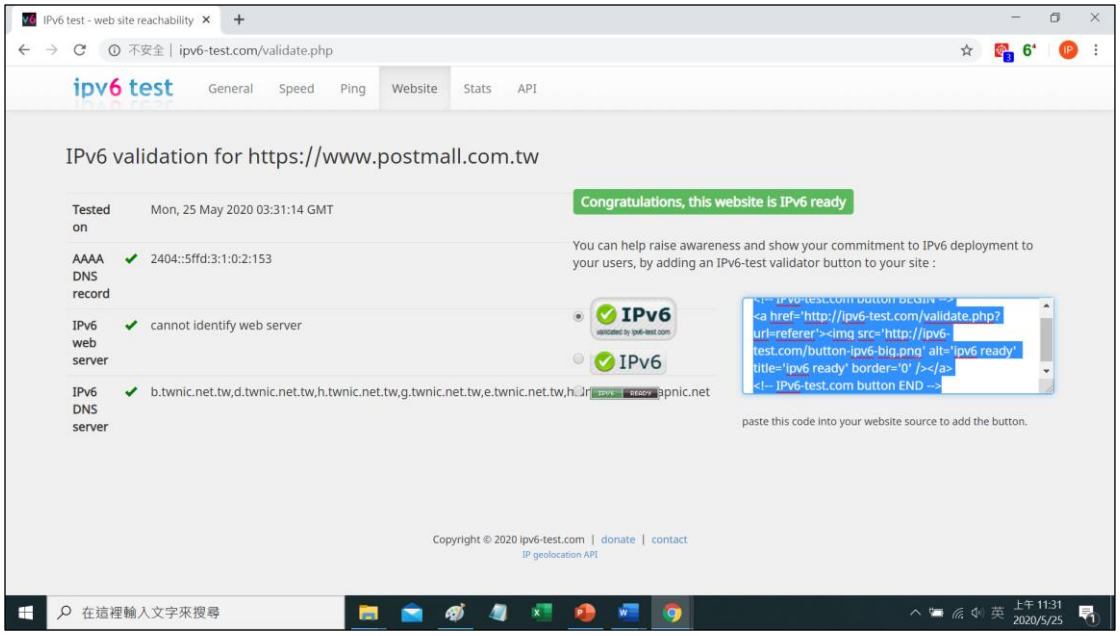



圖 85、以 IPv6 test 進行網站 IPv6 支援檢測截圖

其他網站皆依以上檢驗方式驗證該網站已經升級支援 IPv6，且升級網站網址皆屬於〝.tw〞網域名稱，符合本次升級計畫須達成目標。

# 第五節　德國 IASP 之 IPv6 推動歷程

國內 Cable 業者在 IPv6 的推動上仍處於初步階段，但部分歐洲國家如德國、比利時..等，早期推動 IPv6 的網路供應者是以 Cable 業者為主要推動力，且主要 Cable 業者的 IPv6 使用率皆已經達到相當高的普及性，以下將整理德國主要 IASP 之 IPv6 推動歷程，借由整理國際推動 IPv6 經驗，以做為推估國內 Cable 業者進行 IPv6 升級歷程參考。

德國在 IPv6 的推動上，在相當早期即已經展現積極參與的態度，由 APNIC 的 IPv6 量測數據顯示，德國 IPv6 的推動，由西元 2012 年 (民國 101 年) 當時已慢慢在發展中，到西元 2020 年 (民國 109 年) 5 月 IPv6 連網比率已經成長到約 50%，下圖顯示德國由西元 2012 年 (民國 101 年) 到西元 2020 年 (民國 109 年) ，其整體 IPv6 使用比率成長曲線：[25~26]

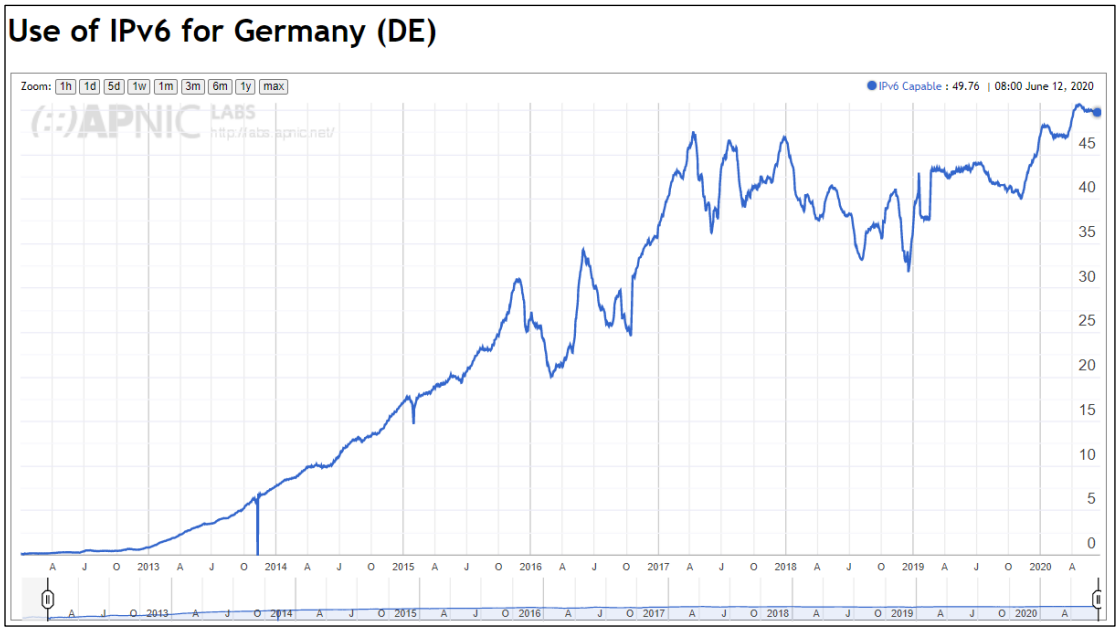



圖 86、德國 IPv6 使用比率統計圖

由上圖可以觀察到德國總體的 IPv6 使用率在西元 2017 年 (民國 106 年) 已經達到約 40%，之後即呈現成長停滯的狀況，一直到今 (109) 年才又出現新的成長動能，一路向 50%的使用率挺進。

下表根據 APNIC 德國 IPv6 統計數據顯示，採集樣本數最多的前 5 大 IASP 分別為德國電信 (Deutsche Telekom AG，DTAG) 、Vodafone、Telefonica、Kabel Deutschland 及 Versatel。

Visible ASes in Germany

| ASN | AS Name | IPv6 Capable | IPv6 Preferred | Samples |
|---|---|---|---|---|
| AS3320 | DTAG Internet service provider operations | 73.73% | 72.65% | 849,471 |
| AS3209 | VODANET International IP-Backbone of Vodafone | 9.83% | 9.69% | 304,071 |
| AS6805 | TDDE-ASN1 | 16.30% | 16.10% | 262,342 |
| AS31334 | KABELDEUTSCHLAND-AS | 72.57% | 72.11% | 226,165 |
| AS8881 | VERSATEL | 88.36% | 87.81% | 122,877 |
| AS24961 | MYLOC-AS | 0.99% | 0.88% | 65,612 |

圖 87、德國主要 IASP IPv6 量測統計資料

針對以上所列 5 家德國主要 IASP 業者，其電信經營業務分布包含固接網路、行動網路及數位有線電視 (Cable 業者) 等，以下將分別介紹各家 IASP 在 IPv6 推動上發展歷程：

## 一. 德國電信 (Deutsche Telekom AG，DTAG)

德國電信為德國第一大電信公司，由德國聯邦郵政的電信部門私有化後分離出來獨立成電信公司，其所經營的電信業務包含固接網路及行動網路等多項業務。

在推動 IPv6 的計畫上，德國電信為了整合所有維運的網路系統，包括維運原有 IPv4 網路系統、營運因應物聯網須具備符合低功耗且低傳輸能力需求的 Non-IP 設備連網、及建置新 IPv6 網路系統，因此推出〝TERASTREAM〞網路架構 (如下圖所示)，希望能整合公司所有營運的網路系統遷移到 Native IPv6 網路架構。凡是連網的設備包

含需要 IP 或 Non-IP 設備 (物聯網設備)，不論設備是透過行動網路、DSL 或光纖網路上網，都將轉換成 IPv6 封包格式，經由 Native IPv6 網路進行資料傳送。不同位址格式，透過轉換機制進行位址轉換後再傳送，讓所有設備能在同一網路系統上傳輸，讓網路架構更簡化，以符合營運的需求，降低維運的成本，並創造更高的效能。[33]

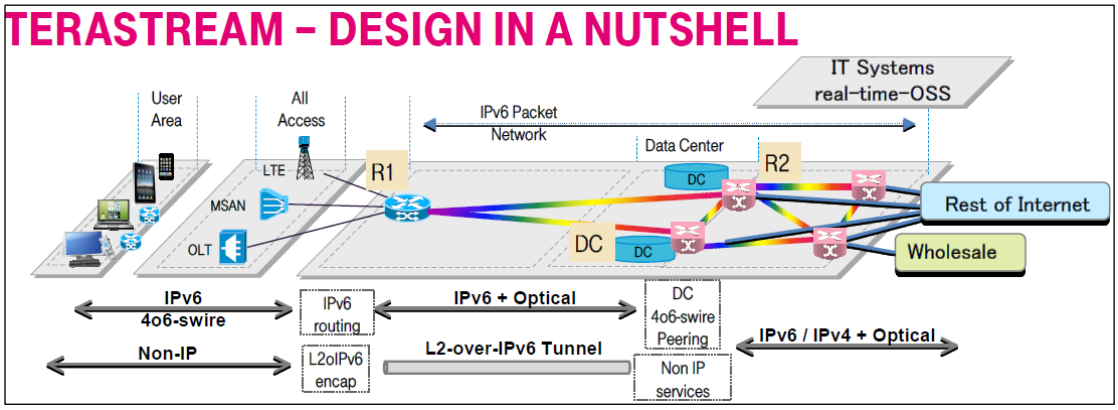



圖 88、德國電信 TERASTREAM 網路架構

德國電信相當早期即已經開始投入推動 IPv6 的網路建置計畫，西元 2012 年 (民國 101 年) 開始提供新申請固網 DSL 客戶支援 IPv6 服務，到西元 2015 年 (民國 104 年) 8 月開始在行動網路提供手機客戶 IPv6 網路服務，下圖為 APNIC 所做統計，德國電信由西元 2012 年 (民國 101 年) 到 2020 年 (民國 109 年) 的 IPv6 使用率成長曲線。

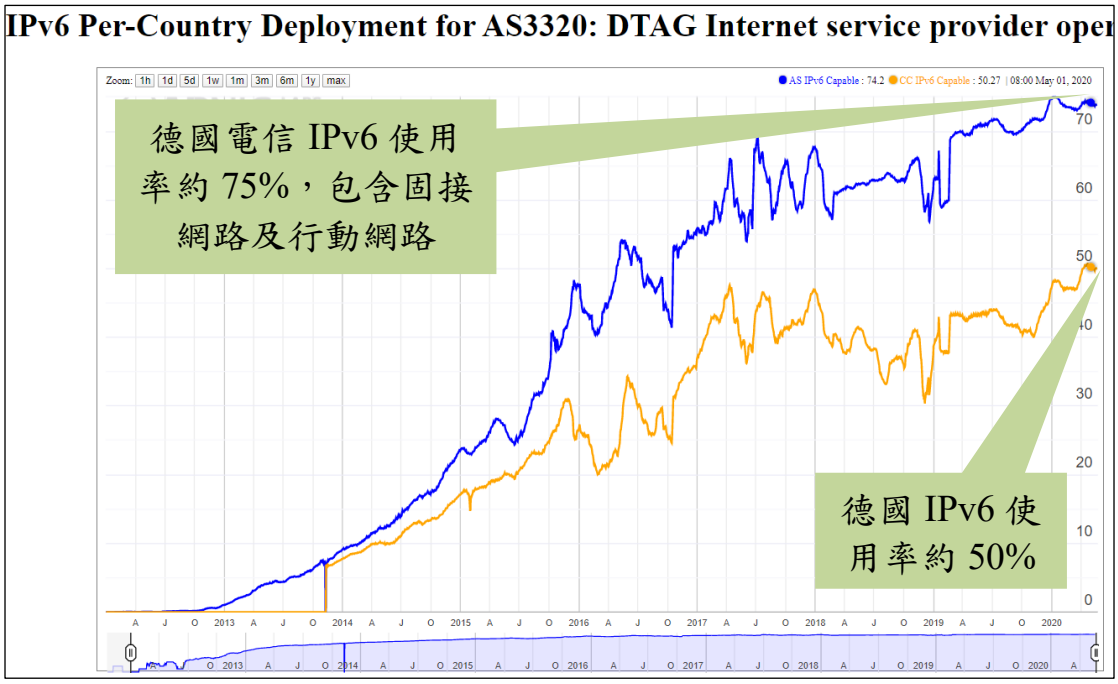



圖 89、德國電信之 IPv6 使用比率統計圖

由上方圖形可看出德國整體在西元 2012 年 (民國 101 年) 到西元 2019 年 (民國 108 年) 的 IPv6 使用率成長曲線，幾乎和德國電信的 IPv6 使用率成長趨勢雷同。但西元 2019 年 (民國 108 年) 第四季開始到西元 2020 年 (民國 109 年) 第二季已經出現一些變化，全德國 IPv6 使用率由 40%成長到 50%，明顯高於德國電信 IPv6 使用成長率，主要原因是除了德國電信外，其他如 Vodafone 及 Telefonica 等主要 IASP，也開始提供 IPv6 網路服務。

## 二. Vodafone

Vodafone 為德國第二大行動電信業者，原規劃在西元 2017 年 (民國 106 年) 開始支援 IPv6 網路服務，實際卻比預期晚了兩年，在西元 2019 年 (民國 108 年) 第四季正式開始支援 IPv6 網路服務，到西元 2020 年 (民國 109 年) 第二季使用率達到約 9.6%，因此也帶動德

國總體 IPv6 使用率的成長。下圖為 APNIC 所做統計，關於德國 Vodafone 的 IPv6 使用率成長趨勢圖。[32]

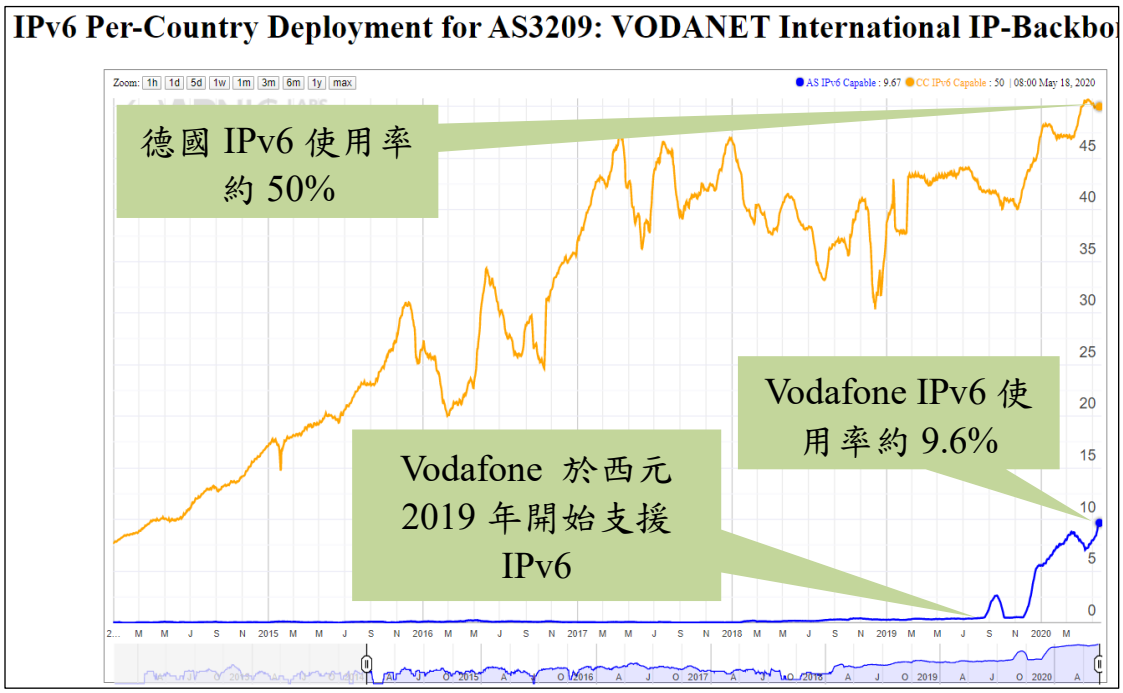



圖 90、德國 Vodafone 之 IPv6 使用比率統計圖

## 三. Telefonica

Telefonica O2 為德國主要 IASP 之一，經營包含固接網路及行動通訊等多項業務電信服務商。不論固接網路或行動網路服務，Telefonica O2 在德國的用戶數都名列在前三大電信業者排行中。Telefonica O2 於西元 2017 年 (民國 106 年) 4 月開始，在固接網路服務上，針對新申請 DSL 服務的客戶，預設支援 IPv6。至於行動網路的部分，公司政策有計畫要支援 IPv6，但尚未公佈明確的時間點。西元 2018 年 (民國 107 年) 其 IPv6 的使用率約維持在 5%~10%，到西元 2020 年 (民國 109 年) 第二季已經上升到約 16.7%，目前其 IPv6 的使用率呈現穩定成長，也持續推升德國總體 IPv6 使用率。[29~31]

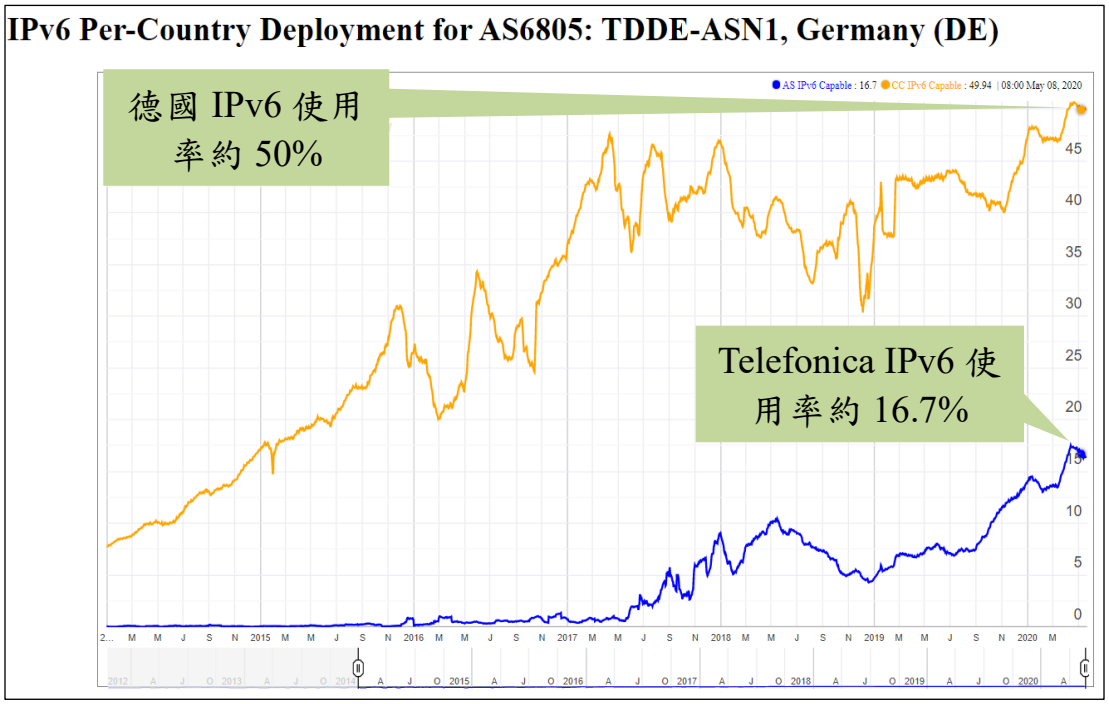



圖 91、德國 Telefonica 之 IPv6 使用比率統計圖

## 四. Kabel Deutschland

Kabel Deutschland 為德國第一大有線電視業者，西元 2014 年 (民國 103 年) 併入 Vodafone 集團，Vodafone 透過多次併購方式，推升集團業務成長為名列全球第二大電信公司。

Kabel Deutschland 投入 IPv6 網路建置的時間點相當早，由下圖 APNIC 統計 Kabel Deutschland 網路 IPv6 使用率觀察得知，其由西元 2012 年 (民國 101 年) 即開始推動 IPv6，透過預設開啟支援 IPv6 網路服務給新申裝用戶使用，持續拉抬 IPv6 用戶數，一直到西元 2017 年 (民國 106 年) 其 IPv6 使用率成長到約 70%，目前維持在此使用率上下，近年來沒有太大的變化。

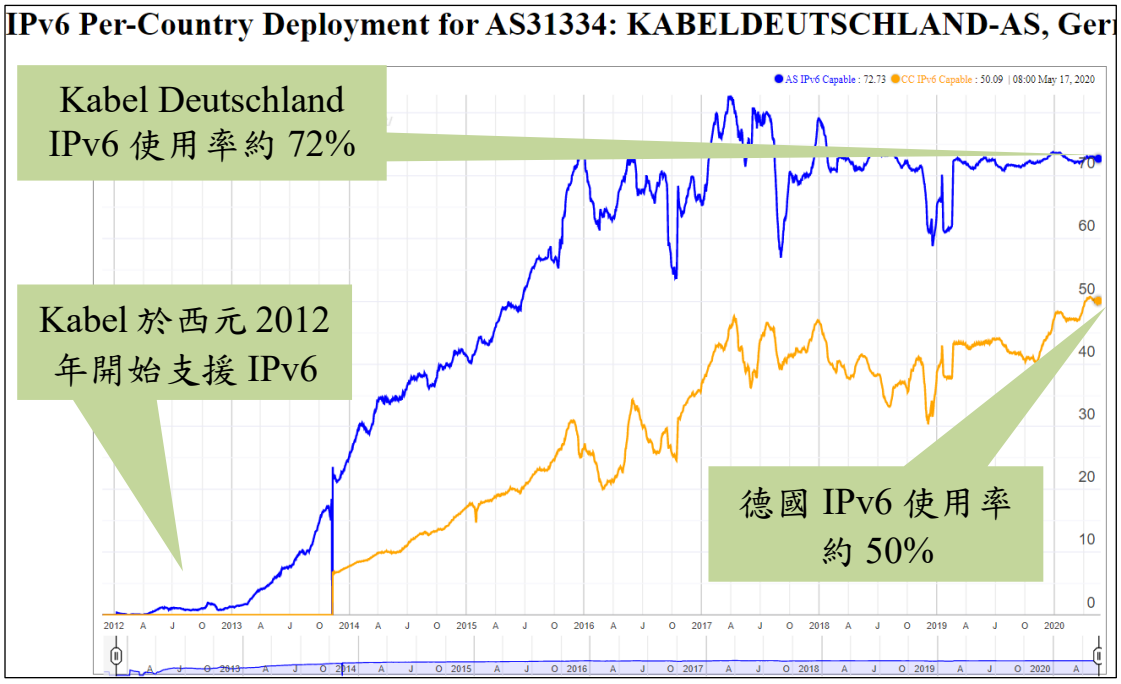



圖 92、德國 Kabel Deutschland 之 IPv6 使用比率統計圖

## 五. Versatel

Versatel 是德國第二大有線電視業者，其用戶 IPv6 使用比率統計圖如下圖所示，根據圖中統計數據顯示，用戶 IPv6 使用比例發展上在西元 2017 年 (民國 106 年) 前都屬於小範圍試用階段，使用率相當低，到西元 2017 年 (民國 106 年) Versatel 正式提供大量用戶 IPv6 網路服務，經過一整年時間到當年年底，其使用率就衝高到約 80%，成長相當快速。之後到西元 2020 年 (民國 109 年) 第二季，又成長到約 88%上下，其推動成效相當驚人。

有線電視業者在推動 IPv6 尚須由系統建置開始，到終端用戶設備一併考慮，設備汰換更新需要相當長的轉換時間，國內有線電視業者在全球 IPv6 逐漸成熟之際，應該加緊腳步進行布局，以因應如數位機上盒系統向 Google Andorid 系統靠攏、國際多媒體影音串流業者

Netflix 要求支援 IPv6 對接等趨勢發展，以避免無法符合系統潮流而錯失商機。

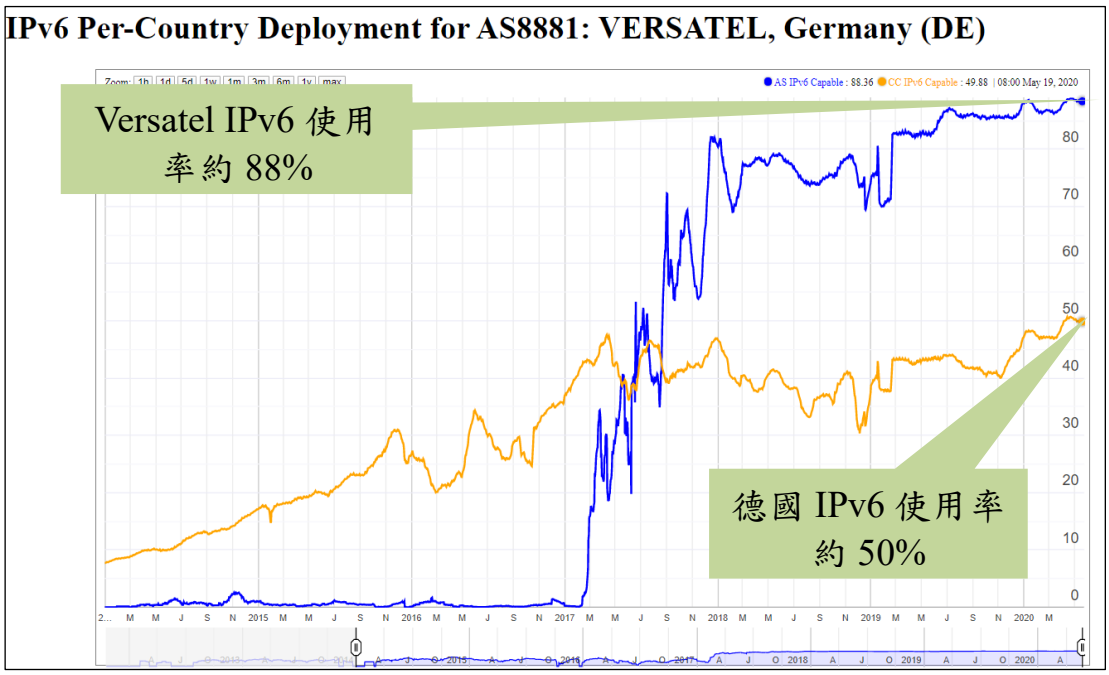



圖 93、德國 Versatel 之 IPv6 使用比率統計圖

德國多家 Cable 業者在 IPv6 的使用率上，都維持相當不錯的比例，主因大多為投入時間相當早，經過多年所累積而成；另透過為新申辦用戶提供預設開啟支援 IPv6，逐步提升用戶數，因而創造出 IPv6 高使用率。以下圖為例，台灣網通商品業者鋐寶科技，於西元 2014 年 (民國 103 年) 為德國 Cable 業者 Tele Columbus，設計生產 Cable Gateway 產品，當時產品已經包含 Wi-Fi、支援 IPv6 等功能。顯示德國 Cable 業者進行 IPv6 網路升級已經經歷相當久的時間，透過多年持續的推動，才能達到 IPv6 使用率高普及化的成就。[28]

Tele Columbus採用鋐寶科技Gateway產品

廖于惲 2014-08-05 讚 0 分享 轉寄 列印 更多報導

鋐寶科技(Compal Broadband Networks；CBN)日前與德國主要有線電視業者Tele Columbus簽署了合作協議，根據此協議，CBN將提供其CH7485E 16x4 DOCSIS 3.0 802.11ac無線閘道器產品給Tele Columbus，以協助Tele Columbus推廣其高速寬頻和電信服務。

CBN的CH7485E Cable Gateway是16x4 DOCSIS 3.0閘道器與新一代802.11ac無線規格的完美結合，其纜線連網速度高達800 Mbps，而802.11ac雙頻的無線網路連網速度更高達1.6 Gbps，其內嵌的3x3 11ac Wi-Fi技術與先進的天線設計，加上最新的波束成形(Beamforming)技術，使其具有極大的無線覆蓋範圍。Tele Columbus將是第一個將此先進Cable Gateway產品引進德國市場的有線電視業者。

點擊圖片放大觀看

德國MSO Tele Columbus採用鋐寶科技新一代16x4 Cable Gateway產品。

除了驚人的連網速度和時尚的外型設計外，CH7485E提供了包含Wi-Fi熱點、全面支援IPv6、多媒體伺服器、NAS、支援遠端頻譜偵測的全頻段調諧器、以及全面的IMS兼容性等先進功能。這種兼具高速連網與先進功能的結合使得CH7485E成為有線電視業者提供高速寬頻應用服務的最佳產品。

Tele Columbus Group執行長Ronny Verhelst表示：為因應客戶對具高速連網、Wi-Fi上網及多媒體功能不斷成長的需求，我們認為鋐寶科技是我們在發展未來的Cable Gateway產品中，相當優秀且重要的合作夥伴。新產品的開發有助於我們在網通產品的持續成長，並開創整合網際網路、影音功能及移動裝置應用的多媒體加值服務的新機會。

圖 94、鋐寶科技為 Tele Columbus 設計生產 Cable Gateway 產品

根據上述德國主要 IASP，在 IPv6 推動及發展歷程，整理成以下比較表：

表 62、德國主要 IASP 之 IPv6 推動歷程

| 序號 | 電信業者 | 業務項目 | IPv6 啟動時間 | IPv6 使用率 |
|---|---|---|---|---|
| 1 | 德國電信 | 固接網路 | 西元 2012 年 | 約 75% |
| | | 行動網路 | 西元 2015 年 | |
| 2 | Vodafone | 行動網路 | 西元 2019 年 | 約 9.6% |
| 3 | Telefonica | 固接網路 | 西元 2012 年 | 約 16.7% |
| | | 行動網路 | 尚未支援 | 0% |
| 4 | Kable Deutschland | Cable 網路 | 西元 2012 年 | 約 72% |
| 5 | Versatel | Cable 網路 | 西元 2017 年 | 約 88% |

總結德國主要IASP之IPv6推展歷程得知，德國在西元2019年 (民國108年) 底到西元2020年 (民國109年) 5月期間，約有10%的IPv6使用率成長，整體IPv6使用率達到約50%，主要是來自於行動電信業者 Vodafone 及 Telefonica O2 支援 DSL 用戶 IPv6 網路服務。至於德國主要Cable業者IPv6皆超過70%的高使用率主要原因，包含Cable業者投入的時間相當早，經過長時間累積才達到IPv6高使用率，及主動提供IPv6網路服務給新申請用戶，以逐步達到IPv6普及化。

# 第六節 法國 IASP 之 IPv6 推動歷程

下圖根據 APNIC 統計法國整體 IPv6 的使用比率趨勢圖，由圖中資料顯示法國在 IPv6 的推動上，早期的投入狀況在全球名列前茅，在西元 2012 年 6 月 6 日世界 IPv6 啟動日 (World IPv6 Launch) 前，法國的 IPv6 使用率就已經達到約 5%，在當時全球網際網路環境中屬於極少數的狀況。

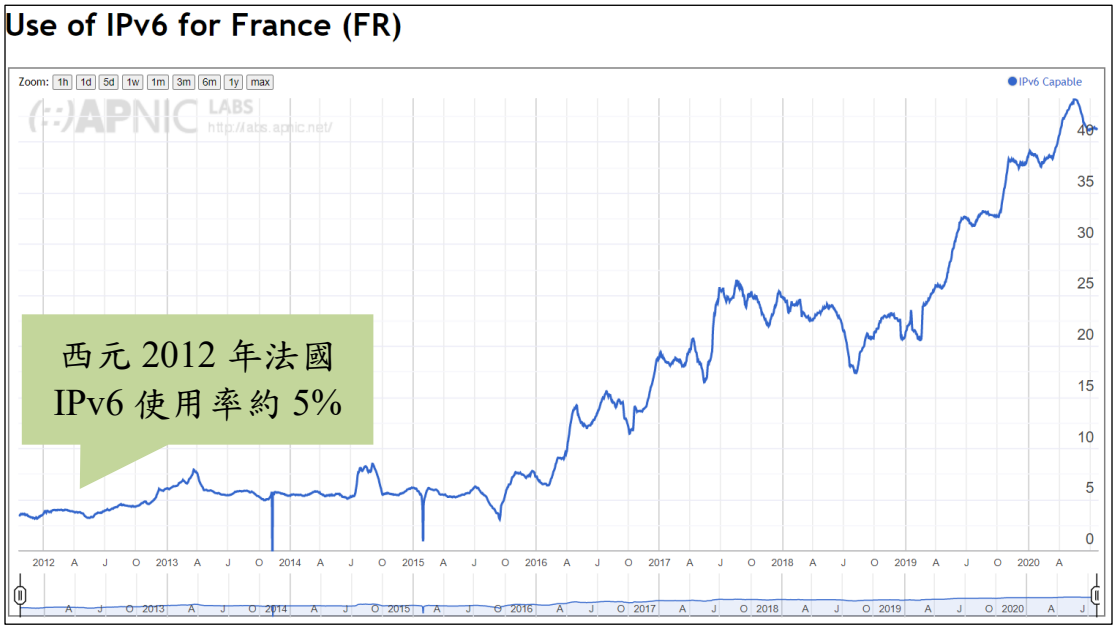



圖 95、法國 IPv6 使用比率統計圖

法國主要有四大電信業者分別為 Bouygues Telecom、Free、Orange 及 SFR，到西元 2019 年 6 月四大電信業者已經分配了大約 94%至 99%的 IPv4 地址，對於未來網路發展已經面臨抉擇點。下表根據 APNIC 法國 IPv6 統計數據顯示，採集樣本數最多的前 5 大 ASN 分別為法國電信 Orange (France Telecom S.A./Orange S.A.)、Proxad (free.fr/Proxad.net，屬於 Free S.A.)、LDCOMNET (LDCom Networks，屬於 SFR S.A.)、BOUYGTEL (Bouygues Telecom) 及 FREEM (Free Mobile，屬於 Free

S.A.)。前 5 大 ASN 分別隸屬於法國的四大電信業者，其中又以法國電信 Orange 所佔比例最高。[45]

Visible ASes in France

| ASN | AS Name | IPv6 Capable | IPv6 Preferred | Samples |
|---|---|---|---|---|
| AS3215 | France Telecom - Orange | 62.81% | 62.48% | 794,375 |
| AS12322 | PROXAD | 92.89% | 92.32% | 472,927 |
| AS15557 | LDCOMNET | 1.19% | 1.09% | 385,949 |
| AS5410 | BOUYGTEL-ISP | 42.20% | 41.86% | 367,481 |
| AS51207 | FREEM | 0.20% | 0.15% | 190,197 |

圖 96、法國主要 IASP IPv6 量測統計資料

根據法國 ARCEP (Autorité de Régulation des Communications Électroniques et des Postes，負責法國電信管制的獨立立法機構) 於西元 2019 年 11 月所發布的新聞稿中所述，由 RIPE 統計當 (2019) 年底歐洲 IPv4 資源即將發罄，新進網際網路市場業者，已經無法由正式官方途徑獲得 IPv4，而讓二手交易市場價格大增，因此呼籲所有網際網路參與者都必須向 IPv6 網路協議遷移，以免錯失參與市場發展的機會。統計目前各大 IASP 之 IPv6 使用狀況，在固接網路服務上擁有超過 3 百萬以上用戶 IASP 共有四家，各 IASP 支援 IPv6 的情況分析如下：[46~47]

- SFR：目前 SFR 的 xDSL (x Digital Subscriber Line，數位用戶線路) 服務已經 100%設備支援 IPv6，在 FTTH (Fiber To The Home，光纖到府) 有 60%設備可支援，在 Cable 服務設備目前完全無法支援 IPv6。但根據統計資料顯示 SFR 客戶端開啟支援 IPv6 網路服務數量仍然非常低，西元 2019 年統計顯示仍少於 7%。
- Bouygues Telecom：觀察 Bouygues Telecom 部署狀況，在西元 2018 年 IPv6 使用比率約為 2.5%，但是到西元 2019 年中已經成

長到超過 20%，儘管 IPv6 使用率仍然不算高，但可預期 Bouygues Telecom 在固接網路上部署 IPv6 的努力仍有可為。

- Free：相對其他電信業者，Free 在 IPv6 的布局上相當積極，在西元 2019 年 5 月已經完成絕大部分設備支援 IPv6，其 IPv6 使用率在西元 2019 已經達到 80%，預計西元 2022 年將達到 100% 支援 IPv6。
- Orange：雖然 Orange 的使用率不及 Free，但 IPv6 使用率在西元 2019 也已經達到約 68%，對法國總體 IPv6 的使用率有相當大的貢獻。估計到西元 2022 年 Orange 在固接網路服務上 IPv6 使用率將超過 85%。

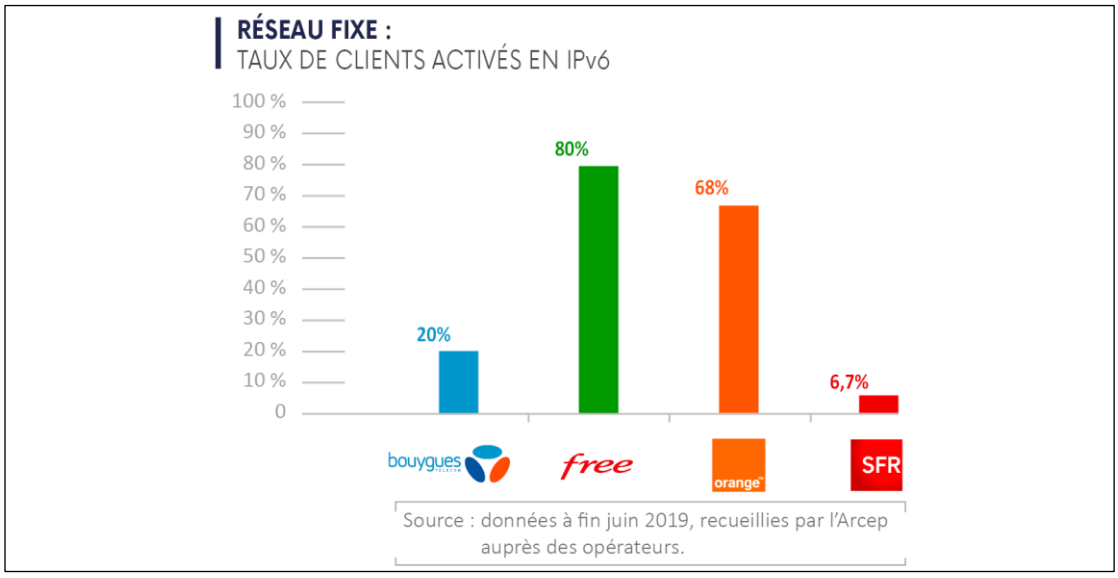



圖 97、西元 2019 年法國四大固接網路服務 IASP 支援 IPv6 統計

下圖為 ARCEP 所發布於西元 2019 年統計法國四大電信業者在各項固接網路服務支援 IPv6 比例，網路服務包含 xDSL、Cable、FTTH 及 4G Fixed 等項目，針對各家業者在用戶比例上分 IPv6-Ready 及 IP-Active 進行統計，目前以 Free 及 Orange 在固接網路服務支援 IPv62

的狀況較佳，SFR 雖然 IPv6-Ready 比例相當高，但用戶終端啟用 IPv6 比例不高，因此總體 IPv6 使用率只有約 6.7%。

**RÉSEAU FIXE :**
TAUX DE CLIENTS IPv6-*READY* ET ACTIVÉS EN IPv6

| | | bouygues | | free | | orange | | SFR | |
|---|---|---|---|---|---|---|---|---|---|
| | | IPv6-*ready* | IPv6 activé | IPv6-*ready* | IPv6 activé | IPv6-*ready* | IPv6 activé | IPv6-*ready* | IPv6 activé |
| xDSL | Réseau propre | 35% | 35% | 100% | 75% | 60% | 59% | 100% | 1,5% |
| | Réseau de collecte | 0% | 0% | 0% | 0% | non concerné | | 100% | 1,5% |
| | Intégralité du réseau | 25% | 25% | 99% | 75% | 60% | 59% | 100% | 1,5% |
| Câble | Réseau propre | non concerné | | non concerné | | non concerné | | 0% | 0% |
| | Réseau de collecte | 0% | 0% | non concerné | | non concerné | | non concerné | |
| | Intégralité du réseau | 0% | 0% | non concerné | | non concerné | | 0% | 0% |
| FttH | Réseau propre | 2% | 2% | 100% | 100% | 100% | 97% | 60% | 38% |
| | Réseau de collecte | non concerné | | non concerné | | non concerné | | 60% | 38% |
| | Intégralité du réseau | 2% | 2% | 100% | 100% | 100% | 97% | 60% | 38% |
| 4G Fixe | Réseau propre | 0% | 0% | non concerné | | 0% | 0% | 0% | 0% |
| Total | Réseau propre | 24% | 24% | 100% | 80% | 70% | 68% | 64% | 6,7% |
| | Réseau de collecte | 0% | 0% | 0% | 0% | non concerné | | 64% | 6,7% |
| | Intégralité du réseau | 20% | **20%** | 99% | **80%** | 70% | **68%** | 64% | **6,7%** |

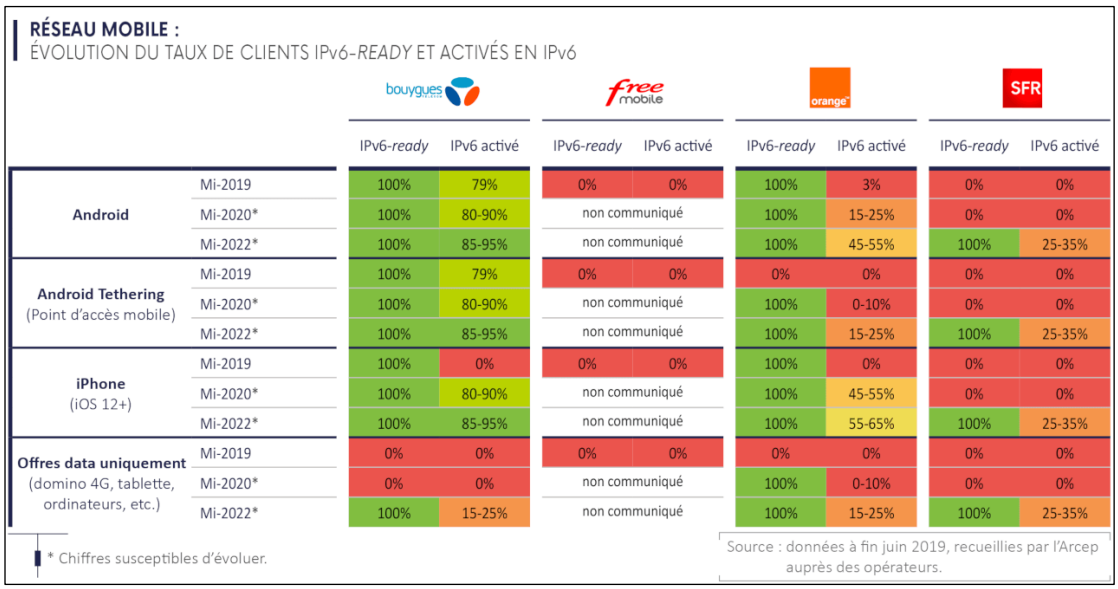
Source : données à fin juin 2019, recueillies par l'Arcep auprès des opérateurs.

圖 98、西元 2019 年法國四大 IASP 各項服務支援 IPv6 統計

而主要行動電信業者，一樣由四大電信 Bouygues Telecom，Free Mobile，Orange，SFR 佔據主要市場，以下就各 IASP 支援 IPv6 的情況分析：[2~3]

- SFR：根據 SFR 的規畫正努力於西元 2022 年在行動通訊服務上開啟支援 IPv6。
- Bouygues Telecom：在行動通訊上 Bouygues Telecom 的用戶中到西元 2019 年 10 月 iPhone 的使用者有約 80%~90%可支援 IPv6 連結網路，而 Android 的用戶可支援 IPv6 比例相當也是約 80%~90%。
- Free Mobile：相對其他行動電信業者，Free Mobile 還沒有明確支援 IPv6 的計畫。

- Orange：目前 Orange 在行動通訊上，有約 45%~55%的 iPhone 用戶可支援 IPv6，而 Android 的用戶有約 15%~25%支援 IPv6。



**RÉSEAU MOBILE :**
ÉVOLUTION DU TAUX DE CLIENTS IPv6-*READY* ET ACTIVÉS EN IPv6

| | | bouygues | | free mobile | | orange | | SFR | |
|---|---|---|---|---|---|---|---|---|---|
| | | IPv6-*ready* | IPv6 activé | IPv6-*ready* | IPv6 activé | IPv6-*ready* | IPv6 activé | IPv6-*ready* | IPv6 activé |
| **Android** | Mi-2019 | 100% | 79% | 0% | 0% | 100% | 3% | 0% | 0% |
| | Mi-2020* | 100% | 80-90% | non communiqué | | 100% | 15-25% | 0% | 0% |
| | Mi-2022* | 100% | 85-95% | non communiqué | | 100% | 45-55% | 100% | 25-35% |
| **Android Tethering** (Point d'accès mobile) | Mi-2019 | 100% | 79% | 0% | 0% | 0% | 0% | 0% | 0% |
| | Mi-2020* | 100% | 80-90% | non communiqué | | 100% | 0-10% | 0% | 0% |
| | Mi-2022* | 100% | 85-95% | non communiqué | | 100% | 15-25% | 100% | 25-35% |
| **iPhone** (iOS 12+) | Mi-2019 | 100% | 0% | 0% | 0% | 100% | 0% | 0% | 0% |
| | Mi-2020* | 100% | 80-90% | non communiqué | | 100% | 45-55% | 0% | 0% |
| | Mi-2022* | 100% | 85-95% | non communiqué | | 100% | 55-65% | 100% | 25-35% |
| **Offres data uniquement** (domino 4G, tablette, ordinateurs, etc.) | Mi-2019 | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% |
| | Mi-2020* | 0% | 0% | non communiqué | | 100% | 0-10% | 0% | 0% |
| | Mi-2022* | 100% | 15-25% | non communiqué | | 100% | 15-25% | 100% | 25-35% |

* Chiffres susceptibles d'évoluer.

Source : données à fin juin 2019, recueillies par l'Arcep auprès des opérateurs.

圖 99、法國四大行動電信業者支援 IPv6 統計及預測資料

法國四大電信業者，在 IPv6 的布局上主要以 xDLS、FTTH 及行動通訊服務為主，目前在 Cable 支援 IPv6 的整體策略較不明確。

針對以上所列法國主要 IASP 業者，以下將分別介紹各家 IASP 在 IPv6 推動上發展歷程：

## 一.Orange (France Telecom Orange S.A.，法國電信)

Orange 為法國第一大電信業者，最早是由法國郵政及通訊局的分支機構，於西元 1988 年正式獨立為法國電信，之後逐步擴大版圖為全球電信跨國公司，其事業群包含 Wanadoo (法國第一大及歐洲第二大網路服務供應商)、Orange S.A. (法國第一大手機服務公司) 及 Equant (負責數位通訊網路商業服務)。西元 2006 年法國電信宣佈停

止使用〝Equant〞及〝Wanadoo〞品牌，並將其整合至〝Orange〞，希望藉由品牌重塑達到公司形象整合與單一化。

根據 Orange 在西元 2013 年公開談論其 IPv6 策略時，提出發展重點包含：[48]

- IPv6 將成為其企業發展基石。
- 企業應該將 IPv6 視為機會，而非限制。
- 在 IPv4 用罄時，IPv6 將成為唯一可長久發展的選擇。
- 支援 IPv6 非一蹴可幾，由 IPv4 轉換到 IPv6 過程中，維持 IPv4 網路服務和發展 IPv6 同等重要。
- 目標要達成一般用戶及企業用戶網路服務都支援 IPv6。
- CGN (Carrier-grade NAT，電信級 NAT) 技術並不會阻礙 IPv6 的部署。

另外 Orange 也針對支援 IPv6 可以為企業帶來的各項好處敘述如下，包含：[49]

- IPv6 可提供共大量的位址空間。
- IPv6 自動位址配置機制，使設備和網路連結可以達成隨插即用 (Plug&Play)，讓網路使用更簡易，也更有效率。
- IPv6 具有安全性上的優勢，對於發展如工業物聯網應用於機器與機器間通訊，智慧家庭用於遠端家庭照明系統監控及室內煙霧偵測等應用都成為可行。

Orange 於西元 2013 年開始在法國進行 FTTH 及行動通訊 IPv6 網路服務內部試驗，經過內部實測後於西元 2015 年開放給法國 FTTH 十萬以上的用戶開始進行實測。到西元 2016 年即開始正式提供給所有 FTTH 及行動用戶預設支援 IPv6 網路服務。[50]

下圖根據 APNIC 所做統計，Orange 由西元 2013 年 (民國 102 年) 到西元 2020 年 (民國 109 年) 的 IPv6 使用率成長曲線。

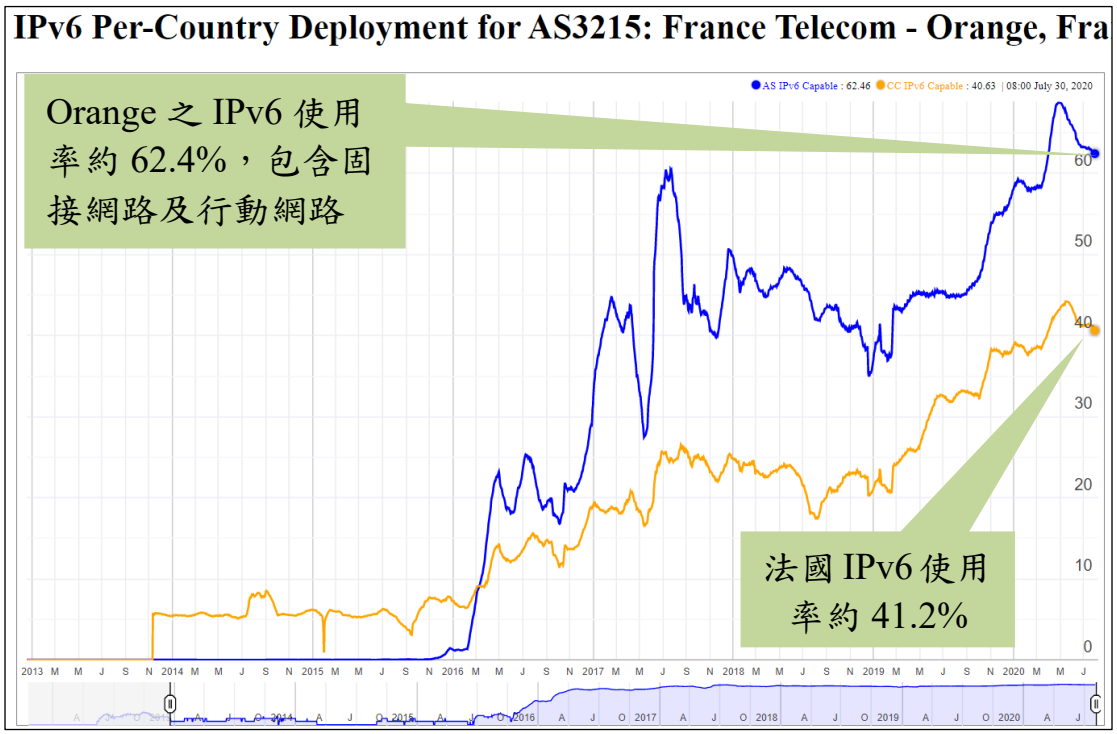



圖 100、法國 Orange 之 IPv6 使用比率統計圖

由上方圖形可看出法國整體 IPv6 使用率在西元 2016 年 (民國 10 年) Orange 開始正式提供 IPv6 網路服務後，其使用率線型和 Orange 的 IPv6 使用率成長曲線趨於相似。可見 Orange 身為法國第一大電信業者對法國整體 IPv6 使用率影響相當大。

下圖根據 RIPE NCC 所公布 IPv6 位址分配統計資料顯示，到西元 2020 年 7 月法國主要 IASP 所分配之 IPv6 位址數量比例，其中以 Orange 數量最多，佔全法國過半的數量比例達到約 58.8%。其他 IASP 申請數量相對低很多。[51]

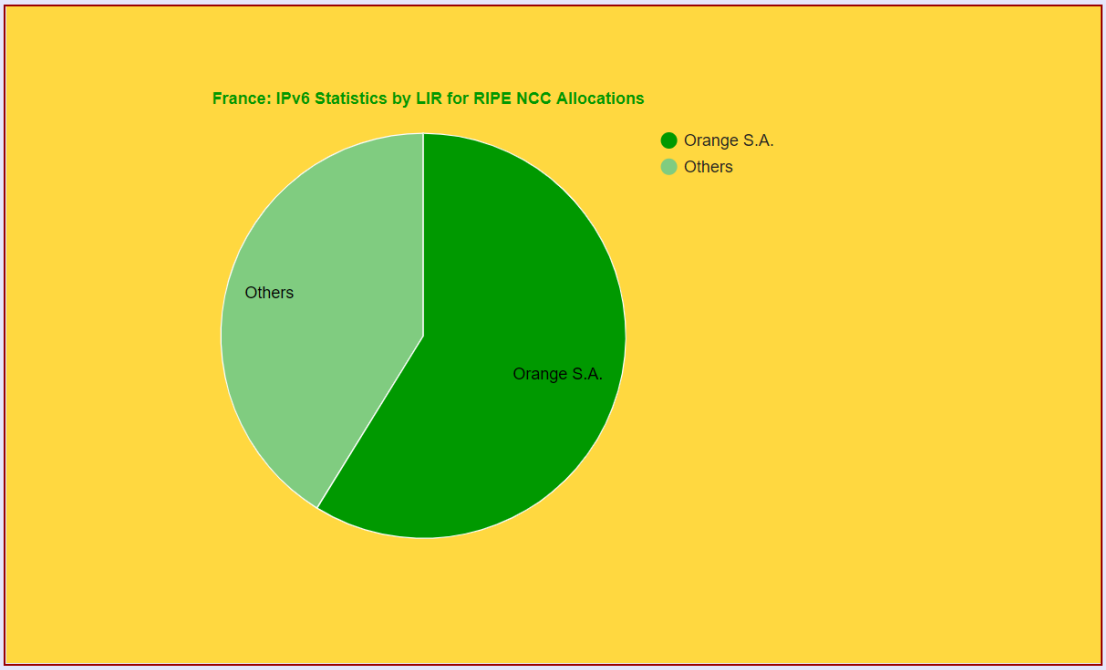



圖 101、法國主要 IASP 分配 IPv6 位址數量比例圖

下表為法國主要 IASP 所分配 IPv6 位址數量，除 Orange 取得過半 IPv6 位址外，其他 IASP 申請的數量都低於 1%以下。

表 63、法國主要 IASP 分配 IPv6 位址數量

| Rank | Local Internet Registry (LIR) | LIR Code | Number of addresses | Percentage | LIR Info |
|---|---|---|---|---|---|
| 1 | Orange S.A. | fr.telecom | 8 193 | 58.799 % | RIPE Info |
| 2 | SFR SA | fr.sfr | 136 | 0.976 % | RIPE Info |
| 3 | Free SAS | fr.proxad | 64 | 0.459 % | RIPE Info |
| 4 | WEBEDIA SA | fr.webedia | 49 | 0.352 % | RIPE Info |
| 5 | Etix Everywhere Ouest | fr.hits | 32 | 0.230 % | RIPE Info |

## 二. Free S.A.

Free 是法國第二大電信業者，成立於西元 1999 年，開始以提供各項固接網路服務為主，經營的業務包含固接網路、語音、數位電視

等。到西元 2012 年開始加入經營行動通信業務，成為法國第四大行動電信業者。

法國最早 IPv6 的主要貢獻者就是 Proxad (free.fr)。根據西元 2008 年 Google 在 RIPE 會議提到當時 IPv6 的流量主要來自於美國 Comcast、法國 free.fr 及日本 NTT Hikari 數位電視。西元 2009 年 Google 發表對當時 IPv6 的流量觀察提到，大部分 IPv6 的流量主要來自於大學網路或學術研究機構為主，但法國 free.fr 是個非常明顯的例外，此現象在當時相當特別。西元 2008 年 free.fr 提供一個名為〝Telesite〞的服務提供 IPv6-only 網路連結，到西元 2009 年底約有 45 萬 free.fr 的用戶加入 IPv6 網路服務，約佔 free.fr 總用戶數的 10%。[52~53]

下圖為 Free 在固接網路服務 IPv6 使用成長曲線，西元 2012 年 (民國 101 年) 在固接網路服務上，已經開始提供 IPv6 連結，當時 IPv6 使用率已經超過 15%。一直到西元 2019 年 (民國 108 年) 中，其 IPv6 的使用率呈現穩定緩慢成長到約 47%，到西元 2019 年 (民國 108 年) 第二季又有一波快速成長到 90%已上，目前西元 2020 年 (民國 109 年) 8 月其 IPv6 的使用率已經來到 92.9%。

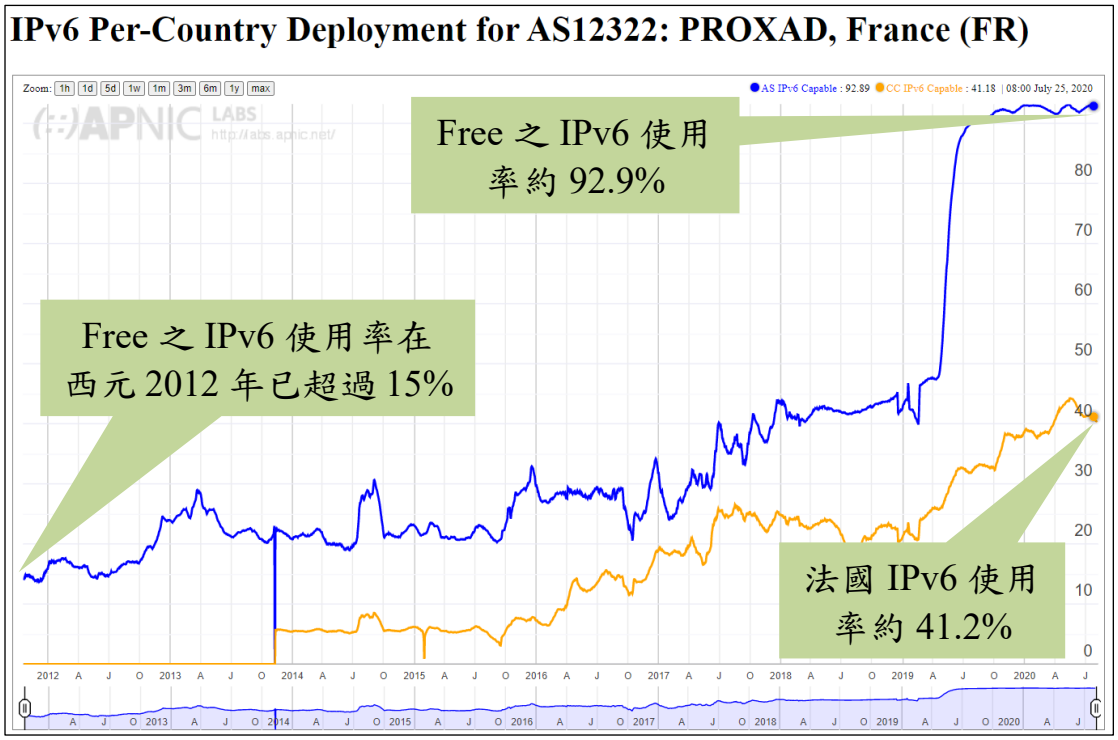



圖 102、法國 Free 之 IPv6 使用比率統計圖

至於行動網路的部分，公司政策對支援 IPv6 計畫，尚未公佈明確的時間點。下圖由 APNIC 統計在西元 2020 年 (民國 109 年) 8 月其 IPv6 使用率約 0.2%。

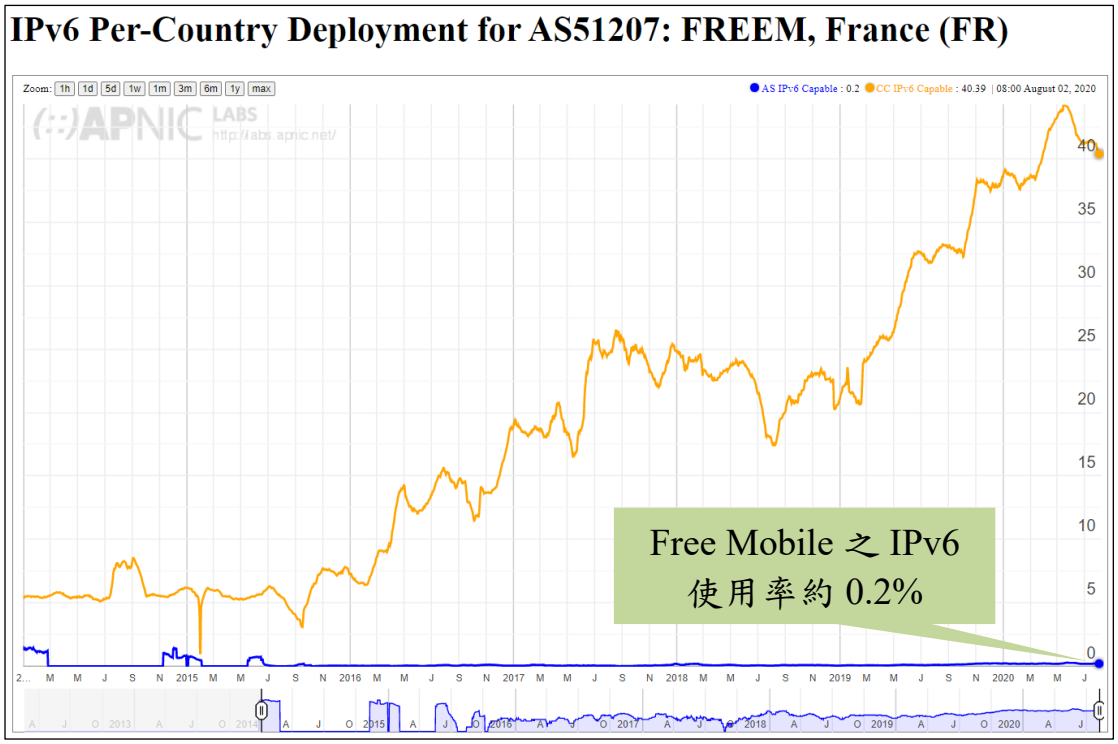



圖 103、法國 Free Mobile 之 IPv6 使用比率統計圖

## 三. SFR

SFR 是法國四大電信業者之一，成立於西元 1987 年，經營的業務包含固接網路、行動通訊、數位電視等。和 Orange 及 Free 比較其在 IPv6 的推動上相對較為緩慢，目前 SFR 在固接網路 xDSL 及 FTTH 網路服務上，設備支援上已經可以支援 IPv6，但在用戶端設備開啟支援的比例仍然很低；而行動通訊的部分，預計要到西元 2022 年才會開始支援 IPv6 網路服務。

下圖為 SFR 網路服務支援 IPv6 使用比例圖，到西元 2020 年 (民國 109 年) 中，其 IPv6 使用率約 1.3%。

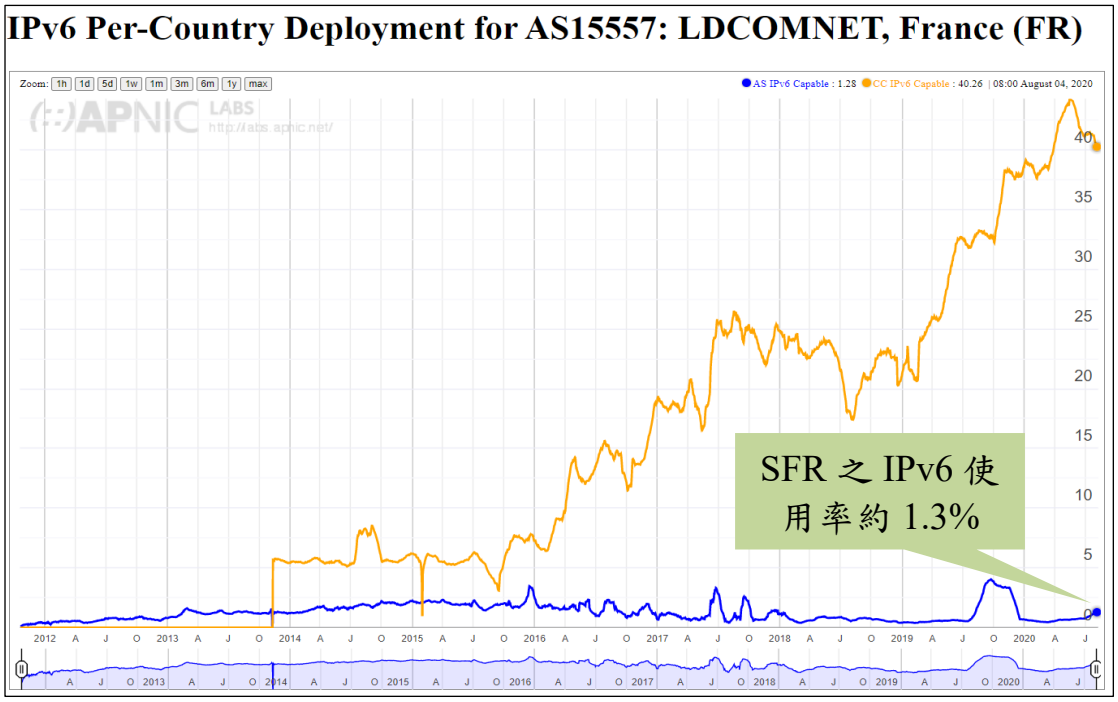



圖 104、法國 SFR 之 IPv6 使用比率統計圖

下圖為 SFR 之企業用戶 IPv6 使用比率統計資訊，略高於一般用戶 IPv6 使用比例，於西元 2020 年 8 月使用比例約 23.4%。但企業用戶所佔樣本數相對比例偏低，對 SFR 整體 IPv6 使用率沒有太大影響。

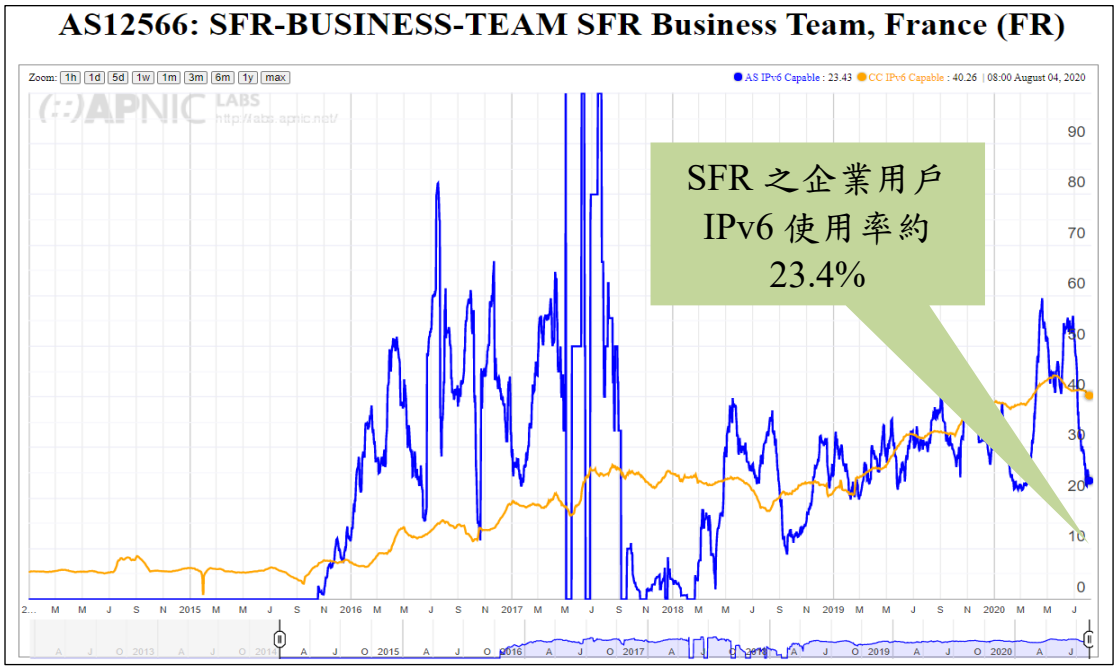



圖 105、法國 SFR 企業用戶之 IPv6 使用比率統計圖

## 四. Bouygues Telecom

Bouygues Telecom 成立於西元 1994 年，於西元 1996 年開始經營行動通訊業務。在西元 2010 年前 Bouygues Telecom 曾對 IPv6 部署進行評估，雖然 IPv6 可能帶來部分商業利益及創新應用的機會，但在當時設備支援度、技術成熟度及網路環境等因素的考量下，總體環境並不成熟，因此 Bouygues Telecom 並未採取積極的態度，但評估新技術導入仍需足夠準備期才能順利進入商業運轉，因此其採用逐步進行策略，以設備汰換需優先採購支援 IPv6 進行方式，逐步建構設備資源度，並根據市場需求及變化進行 IPv6 部署計畫調整。

雖然 Bouygues Telecom 在 IPv6 使用率不及 Free 及 Orange 高，但其行動通訊 IPv6 使用率卻在法國四大電信業者中表現最佳已經達到 80%~90%，但固接網路服務則只有約 20%使用率。下圖根據 APNIC 統計結果顯示，Bouygues Telecom 於西元 2018 年開始支援 IPv6 到西元 2020 年 8 月整體 IPv6 使用率成長到約 41.5%，成長速度相當快。

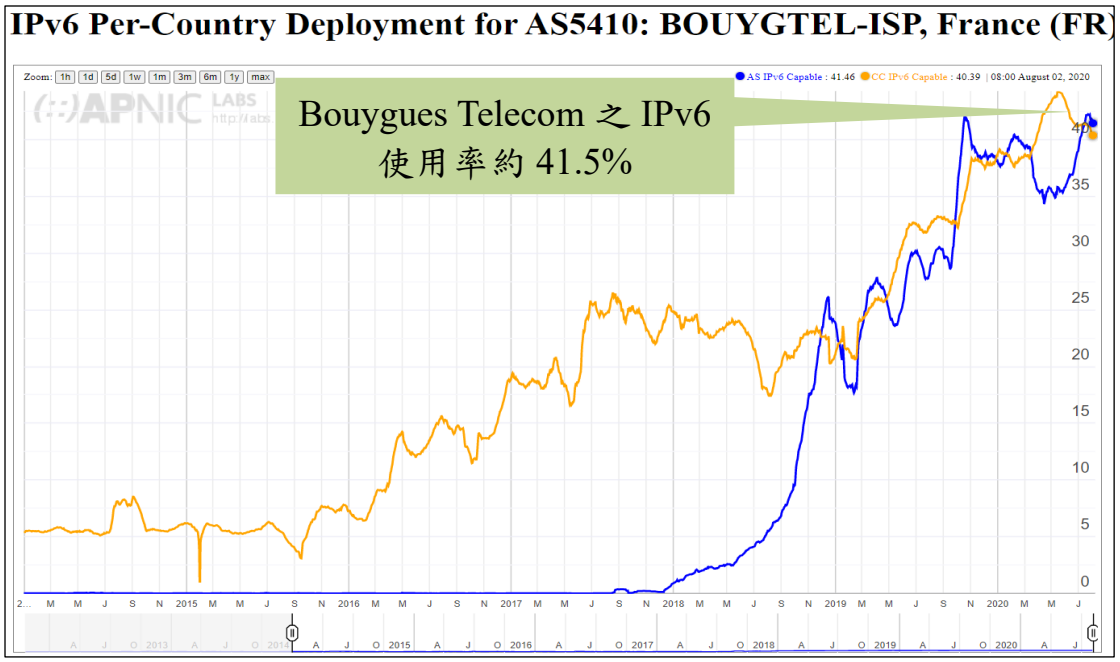



圖 106、法國 Bouygues Telecom 之 IPv6 使用比率統計圖

根據上述法國主要 IASP，在 IPv6 推動及發展歷程，整理成以下比較表：

表 64、法國主要 IASP 之 IPv6 推動歷程

| 序號 | 電信業者 | 業務項目 | IPv6 啟動時間 | IPv6 使用率 |
|---|---|---|---|---|
| 1 | Orange | 固接網路 | 西元 2016 年 | 約 68% |
| | | 行動網路 | 西元 2016 年 | 約 30% |
| | | Cable 網路 | 尚未有明確計畫 | 0% |
| | | 整體 IPv6 使用率：62.4% | | |
| 2 | Free | 固接網路 | 西元 2010 年前 | 約 93% |
| | | 行動網路 | 尚未有明確計畫 | 0% |
| | | Cable 網路 | 尚未有明確計畫 | 0% |
| | | 整體 IPv6 使用率：92.9% (不含 Free Mobile) | | |
| 3 | SFR | 固接網路 | 西元 2014 年 | 約 6.7% |
| | | 行動網路 | 預計西元 2022 年 | 0% |
| | | Cable 網路 | 尚未有明確計畫 | 0% |
| | | 整體 IPv6 使用率：1.3% | | |
| 4 | Bouygues Telecom | 固接網路 | 西元 2018 年 | 約 20% |
| | | 行動網路 | 西元 2018 年 | 約 80% |
| | | Cable 網路 | 尚未有明確計畫 | 0% |
| | | 整體 IPv6 使用率：41.5% | | |

總結法國主要 IASP 之 IPv6 推展歷程得知，法國 IPv6 推動主力為 3 大主要 IASP，包含 Free 固接網路服務、Orange 固接及行動網路服務及 Bouygues Telecom 行動網路服務，尤其以第二大 IASP Free 最早投入，目前其固接網路服務 IPv6 使用率已經超過 90%。但 Orange 由西元 2016 年開始支援 IPv6，是法國近年 IPv6 使用率成長最大貢獻者。至於法國主要 IASP 在 Cable 業務上都還未有明確支援 IPv6 時程規畫。

# 第七章 IPv6 用戶資通安全防護研析

一般家庭用戶使用者所常採用的終端設備，和企業用戶使用者所需的終端設備，會有明顯的差異。因此針對 IPv6 用戶資通安全防護研析工作項目，將分別依家庭用戶及企業用戶資通安全議題進行探討。下圖為 IPv6 用戶資通安全防護研析項目所規畫之研究架構。

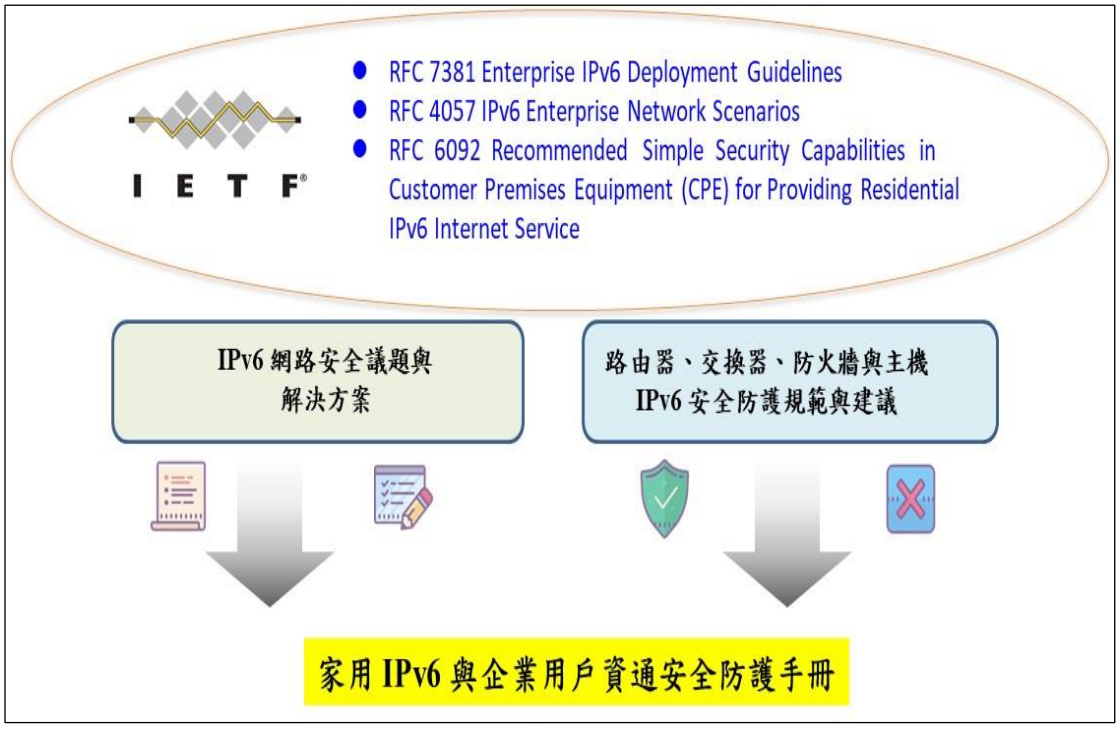



圖 107、IPv6 資通安全防護研究架構

網際網路工程任務組 (Internet Engineering Task Force，IETF) 為專注於網際網路技術的開放性國際標準組織，負責開發和推廣網際網路標準 (Internet Standard，STD)。針對 IPv6 用戶資通安全防護研析，將參考 IETF 所擬定相關文件，作為本工作項目重要技術參考來源。和此工作項目相關的 IETF 標準如下表所列：[20~22]

表 65、IPv6 用戶資通安全防護研析相關 RFC 列表

| 序號 | RFC 編號 | RFC 表頭 | 說明 |
|---|---|---|---|
| **1** | 7381 | Enterprise IPv6 Deployment Guidelines | 提供企業網路架構及管理進行 IPv6 升級之參考準則。 |
| **2** | 4057 | IPv6 Enterprise Network Scenarios | 根據企業網路部署 IPv6 所採取不同方案，提供如何完成升級任務的指南。 |
| **3** | 6092 | Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service | 針對 CPE 設備所訂定之安全能力規範。 |

企業網路的特性為具有一到多個路由器 (Router)，連結多個內部網路，因此在進行 IPv6 升級過渡策略時須考慮到端點 (應用程式/作業系統) 的 IP 能力，連接到企業〝網段〞端點的 IP 能力，及網路服務供應商的網路 IP 能力。企業要進行升級須整體考量所有主機的作業系統，以及所有中間介接軟體須一併進行升級。且在轉換的過渡期，需要考量到能同時支援 IPv4 及 IPv6 雙協定並行，為顧慮到企業網路連結的安全性，針對新增支援 IPv6 網路連結，企業網路的 Proxy 及防火牆 (Firewall) 需考慮實現 IPv6 的安全策略，以增強整體網路安全性。

關於企業網路支援 IPv6 原則，RFC 針對企業網路 IPv6 部署訂定升級之參考準則 (RFC 7381)，及根據企業網路部署 IPv6 所採取不同的升級方案，提供如何完成升級任務的指南 (RFC 4057)。分項工作將參考上列技術標準文件，進行分析及整理出企業網路 IPv6 資通安全防護要點。

另外用戶終端設備CPE是指位於用戶端與電信業者對接服務的網路終端裝置，包括用戶路由器、交換機、防火牆、及主機等裝置，本項工作將參考技術標準文件 (RFC 6092)，探討此類型設備所需具備的資通安全防護要項，進行研究並做重點整理，以提供給設備製造業者參考，及提供企業網路管理技術人員進行 IPv6 部署時作為設備採用參考指標。

# 第一節 IPv6 家用資通安全防護研析

針對家用 IPv6 網路安全防護，寬頻分享器 (WiFi Router) 屬於用戶終端設備 (Customer Premises Equipment，CPE) 之一是 IPv6 終端用戶的第一線設備，也是家庭網路環境常見的網路通訊設備，本工作項目針對家庭 IPv6 資通安全防護的討論主要以寬頻分享器為主。將探討 IPv6 網路攻擊與防禦機制，並針對用戶 IPv6 網路安全管理提出建議。

## 一. 用戶設備 CPE 網路 IPv6 安全議題與解決方案

### (一) IPv6 基本功能與協定探討

IPv4 位址分成 3 種類型：單播 (Unicast)、多播/群播 (Multicast) 及廣播(Broadcast)。

而根據[RFC 4291]文件中定義 IPv6 位址格式，主要也可分為 3 種：單播 (Unicast)、任播 (Anycast) 和多播/群播 (Multicast)。

也就是說 IPv6 不支援廣播(Broadcast)，但新增任播 (Anycast) 格式。總結 IPv4 及 IPv6 共可支援 4 種位址傳播類型。以下就此 4 種類形簡要說明：

- 單播 (Unicast)：是指封包在網路的傳輸中，目的地址為單一目標的一種傳輸方式。是網路應用最為廣泛使用的形式，通常網路協議或服務多採用單播傳輸，例如 TCP 協議。
- 多播/群播 (Multicast)：指把信息同時傳遞給一組目的地址。目的為提高傳輸效率，訊息在每條網路鏈路上只需傳遞一次，而且只有在鏈路分叉的時候，訊息才會被複製。

- 廣播 (Broadcast)：用於封包在網路傳輸時，目的地址為網路中所有設備的一種傳輸方式。實際上，此處所指〝所有設備〞為限定在一個範圍〝廣播域〞之中所有設備。
- 任播 (Anycast)：是一種網路尋址和路由的策略，讓資料可以根據路由拓樸來決定送到〝最近〞或〝最好〞的目的地。

下表針對 IPv6 的 3 種位址類型，加以整理並說明各種位址類型用法：

表 66、IPv6 位址類型及說明

| 序號 | IPv6 位址傳送格式 | 說明 |
|---|---|---|
| 1 | Unicast (單播) | 單播位址 (Unicast Address) 用於單點傳送<br>是指封包在網路傳輸中，目的地位址為單一目標的一種傳輸方式。IPv6 單播位址通常有一個代表特殊位址名字，主要有:<br>● 區域鏈結位址 (Link-local address)。<br>● 單一區域位址 (Unique local address，ULA)。<br>● 全域位址 (Global address)。<br>● 未定位址 (Unspecified address)。<br>● 回送位址 (Loopback address)。 |
| 2 | Anycast (任播) | 任播位址 (Anycast Address) 用於任意點傳送<br>在網路位址和網路節點之間存在一對多的關係：每一個位址對應一群接收節點，但在任何給定時間，只有其中之一可以接收到傳送端來的資訊。通常會根據路由協定，選擇〝最近〞的成員接收。任播位址通常無法輕易分別：任播位址和單播位址結構相同，不容易辨別，差異點只有在路由協定中將多個節點加入網路中。 |
| 3 | Multicast (多播/群播) | 多播位址 (Multicast Address) 用於多點傳送<br>其目的地位址是一組目標，加入該組的成員均是封包的目的地。多播位址的封包會被傳送到所有的目的地位址。多播位址的前 8-bit 由皆為 1 的位元組成，亦即：其前置為〝FF00::/8〞。而第 2 個位元組的後 4 個位元用於表示多播類型。 |

本計畫所討論的 IPv6 位址配發機制主要以單播為主。IPv6 的單播位址和 IPv4 的單播位址傳送模式相同，用在單一節點對單一節點的資料傳送，可再分成下列 5 種型態：[34]

表 67、IPv6 單播位址類型及說明

| 序號 | IPv6 單播位址格式 | 說明 |
|---|---|---|
| 1 | Link-local address (區域鏈結位址) | 僅適用於在同一個網路區段使用 (同一個子網路中)，不可以繞送到其他鏈結 (Link) 或網際網路上。<br>其位址的唯一性僅限於同一個鏈結 (Link) 上。<br>功用如同 IPv4 的 APIPA (Automatic Private IP Addressing) 位址 (〝169.254.X.X〞)。 |
| 2 | Unique local address (單一區域位址) | 位址可以在節點間繞送，但不可被繞送到網際網路。Link-Local 及 Unique-Local 位址的概念就像是 IPv4 中的私有位址，區域網路間自動建立暫時性的通訊非常有用。 |
| 3 | Global address (全域位址) | 如同 IPv4 的公用位址 (Public Address)，在全世界具有唯一性，其它節點不會有相同的位址。 |
| 4 | Unspecified address (未定位址) | 未指定的位址 (〝0:0:0:0:0:0:0:0〞或〝::〞) 僅用於表示此位址是空的，未指定。Unspecified address 只能做為來源位址，不能指定給 interface，也不能做為目的位址。一般而言，當發送封包者還沒有 IPv6 位址或有些封包並不需要指定發送者的 IPv6 位址時，就會將來源位址設為 (〝::〞)。 |
| 5 | Loopback address (回送位址) | 回送位址 (〝0:0:0:0:0:0:0:1〞或〝::1〞) 用於識別迴路介面，使節點可以向自己傳送封包。發往回送位址的封包不能在鏈結 (Link) 上傳送，也不能由路由器 (Router) 轉送。Loopback address 不能當來源位址。 |

前面 3 個類別 Link-local address (區域鏈結位址)、Unique local address (單一區域位址) 及 Global address (全域位址) 屬於一般常用單播位址類型;後面 2 個類別未定位址 (Unspecified address) 及回送位址 (Loopback address) 屬於特殊位址。

網路上的終端設備要能彼此互通，除了用戶端設備 IPv6 網路位址的配發之外，還必須確認用戶端設備與鄰居的關係才行。在 IPv6 的網路環境中，主要是利用 Neighbor Discovery (ND，鄰居發現) 協定所規範的方法來達成，以描述相鄰網路節點之間關係的程序與方法，ND 的主要目的如下表所列：

表 68、Neighbor Discovery (ND) 協定主要目的

| 序號 | Neighbor Discovery (ND) 目的 |
|---|---|
| 1 | 主機用來發現相鄰路由器。 |
| 2 | 主機用來發現位址、網路前置碼 (Network Prefix) 及其它組態參數。 |
| 3 | 主機用來解析 IPv6 封包轉寄到相鄰節點的連結層位址，並確定相鄰節點的連結層位址從何時起發生改變。 |
| 4 | 主機用來確定是否仍然可以連線到相鄰節點。 |
| 5 | 路由器用來通告自己的存在、主機組態參數及網路前置碼。 |

在 IPv6 網路環境上，ND 主要是利用 ICMPv6 (Internet Control Message Protocol Version 6，網際網路控制訊息協定第 6 版) 封包來傳遞並交換訊息，主要訊息類別包含 5 種，如下表所示：[35]

表 69、IPv6 之 ND 訊息類別及說明

| 序號 | 訊息類別 | 說明 |
|---|---|---|
| **1** | Router Solicitation (RS) 路由器請求 | 由主機 (Host) 向路由器 (Router) 發出請求的訊息 (message)。當主機的介面 (Interface) 被啟動時，主機可以發送 RS 訊息要求路由器立即發佈 RA 訊息，不用等待路由器下次自發性發佈 RA 訊息的時間。<br>目的：讓用戶端設備尋找路由器。 |
| **2** | Router Advertisement (RA) 路由器公告 | 路由器會週期性發佈 RA 訊息。當主機發出 RS 訊息時，路由器也會立即發送 RA 訊息。RA 訊息包含 on-link 或 off-link 的前置 (prefix)，hop limit (最大鏈結數)，和 link MTU (Maximum Transmission Unit，最大傳輸單位) 等。經主機發出 RS 訊息而回應的 RA 亦稱為 Solicited RA 訊息 (經由請求後才發送的)。路由器週期性發佈的 RA 亦稱為 Unsolicited RA 訊息 (非經由請求後才發送的)<br>目的：讓路由器主動廣播訊息所用。 |
| **3** | Neighbor Solicitation (NS) 鄰居請求 | 用來解析鄰近節點 (nodes) 的鏈結 (link) 層位址，也可檢測鄰近的節點是否還可連結 (reachable)，還可用來做重複位址檢測 (Duplicate Address Detection，DAD)。<br>目的：讓網路設備彼此交換相鄰節點訊息用。 |
| **4** | Neighbor Advertisement (NA) 鄰居公告 | NA 主要包含發送者的鏈結層位址，用來回應 NS 訊息。此外，當鏈結層位址發生變化時，節點會馬上發佈 NA 來通知所有的節點。回應 NS 的 NA 亦稱為 Solicited NA 訊息，非因回應 NS 而發送的 NA 亦稱為 Unsolicited NA 訊息。<br>目的：讓網路設備彼此交換相鄰節點訊息用。 |
| **5** | Redirect 重新導向 | 路由器用來告知主機使用路徑更佳的下一節點 (next-hop) 將封包送達特定的目的位址。<br>目的：用來將封包轉送用的訊息。 |

在 IPv6 的網路環境中，用戶端設備 IPv6 位址的取得必須建立在 ND 通訊協定的基礎上。

## (二) 家庭網路 IPv6 攻擊途徑與防護方式

家用 IPv6 網路主要可能遭受攻擊類型分為 Neighbor Discovery 攻擊、Router Advertisement 攻擊及 ICMPv6 攻擊等 3 類，以下將就此 3 類的攻擊與防護機制進行探討。

### 1. Neighbor Discovery 攻擊與防護

芳鄰探索機制 Neighbor Discovery 為 IPv6 基本必要之功能無法關閉。下圖為 IPv6 之 ND 攻擊示意圖。

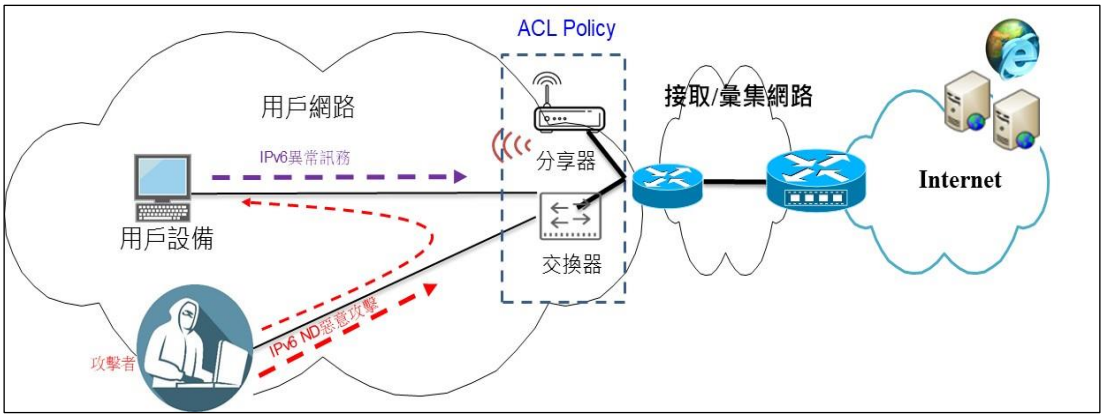



圖 108、IPv6 之 ND 攻擊示意圖

IPv6 之 ND 機制要能夠正確且安全地運作，在同一連結上的各節點必須互相信任，若鄰居探索機制在未受保護的環境中，非常容易受到惡意的攻擊。ND 攻擊方式類似 IPv4 的 ARP (Address Resolution Protocol，位址解析協定) 攻擊，基本上可分為 3 種如下表所示。

表 70、IPv6 之 ND 攻擊類型

| 序號 | 攻擊類型 | 說明 |
|---|---|---|
| 1 | 重導 (Redirect) 攻擊 | 攻擊者惡意將資料轉送至其他位置。 |
| 2 | 服務阻斷 (Denial-of-Service) 攻擊 | 使目標主機的網路或系統資源耗盡，使服務暫時中斷或停止，導致其正常用戶無法存取。 |
| 3 | 偽冒 (Spoofing) 攻擊 | 以假造的 IPv6 位址於網路中進行非法攻擊行為，造成破壞。 |

(1) 重導 (Redirect) 攻擊

重導攻擊必須要先知道 LAN (Local Area Network，區域網路) 原本路由器 IPv6 位址，將 IPv6 路由植入終端針對 Target IPv6 位址之流量重新導向新路由器 IPv6 位址。如果新路由器 IPv6 位址不存在，將可能導致用戶 IPv6 上網的服務中斷。

(2) 服務阻斷 (Denial-of-Service) 攻擊

在 IPv6 位址配置部分，無論 SLAAC (StateLess Address AutoConfiguration，無狀態位址自動設定)、DHCPv6 (Dynamic Host Configuration Protocol for IPv6，動態主機設定協定第 6 版)、或靜態 IPv6 位址設定前都必須發送 DAD NS 封包確認 LAN 環境中無 IPv6 節點使用同一個 IPv6 位址。DAD 重複位址檢測 (Duplicate Address Detection) 作用類似 IPv4 Gratuitous ARP，新的 IP 位址在設定前會先確認網路上是否已經有設備在使用。在 IPv6 網路中，當攻擊者監聽區域網路上所有的 NS 封包，可容易地產生具有偽造目標位址的 NS 封包來假裝重複位址偵測，或是佯裝成相同目標位址主機回應 NA 封包，讓受害節點以為發生碰撞，造成受害者無法正常取得 IP 位址的使用權，此種攻擊即稱為重複位址偵測

DoS。

(3) 偽冒 (Spoofing) 攻擊

在偽冒攻擊部分，由於 ND 訊息並不安全，讓 ND 容易受到鏈結層位址欺騙 (或偽造) 的攻擊。攻擊節點可以通過發送帶有欺騙性的來源 MAC 位址 (Media Access Control) 的鄰居請求訊息，或者透過發送帶有欺騙性目標 MAC 位址的鄰居通告位址，來將合法節點的封包發送到其他某個鏈結層位址，然後其他節點將欺騙的 MAC 位址與合法的網路 IPv6 位址關聯在一起存起來。

在防禦機制方面，防範 ND 攻擊的最主要目標就是防止發生假冒 IP 的情形，可考慮針對 ND 通訊要求進行認證，確認是可信賴的端點後，再進行訊息交換。在[RFC 3971]及[RFC 6494]文件中所規範的 SeND (Secure Neighbor Discovery，安全鄰居發現) 協定對此提出 3 個選項，包含：

- 加密產生位址 (Cryptographically GeneratedAddresses，CGA) 。
- RSA 簽章 (RSAsignature)。
- 時間戳記與 Nonce (Timestamp and Nonce)。

SeND 機制主要實作於網路的終端節點，各節點須產生一組公鑰與私鑰，再利用 CGA 機制產生 IPv6 位址，以保證其位址擁有權；而以私鑰針對 ND 訊息所產生之 RSA 簽章放在所有選項末端，確保訊息的機密性及完整性；至於時間戳記及 Nonce (Number used once，隨機數) 選項則用以防止重送攻擊。

目前 SeND 機制僅有主要網路設備廠商如 Cisco 支援此協定，

一般用戶端 OS 尚未支援，且加解密運算可能影響設備處理效能，建置時須審慎考量其適用範圍。

**2. Router Advertisement 攻擊與防護**

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

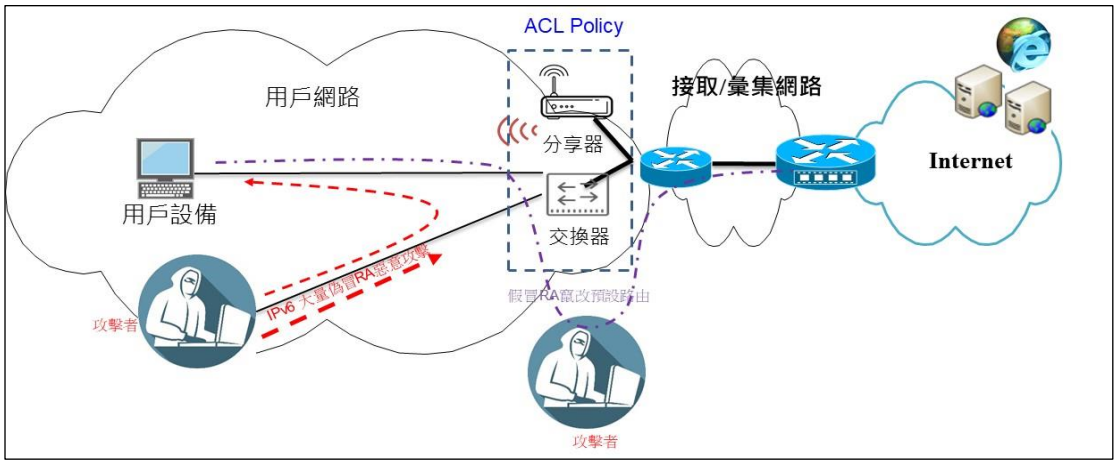



圖 109、IPv6 之 RA 攻擊示意圖

每個 IPv6 節點都可以發送 RA，可讓終端新增公眾 IPv6 位址、新增/刪除預設路由或廣播大量 RA 造成網路效能降低。基本上可分假冒 (Rogue) RA 攻擊及 RA 洪水 (Flooding) 共 2 種典型的 RA 攻擊類型，如下表所示：

表 71、IPv6 之 RA 攻擊類型

| 序號 | 攻擊類型 | 說明 |
|---|---|---|
| **1** | 假冒 (Rogue) RA 攻擊 | 每個 IPv6 節點都可以發送 RA，可讓終端新增公眾 IPv6 位址、新增/刪除預設路由或廣播大量 RA 降低網路效能。 |
| **2** | RA 洪水 (Flooding) 攻擊 | 發送大量 RA 夾帶 IPv6 Prefix 以消耗目標主機系統資源，影響用戶存取效率。 |

(1) 假冒 (Rogue) RA 攻擊

假冒 (Rogue) 攻擊，攻擊者會透過偽造 RA 封包傳送假的路由組態資訊進行攻擊，例如惡意的路由器 (malicious router)、假造位址前綴 (bogus prefix)、假造路由組態參數 (parameters spoofing) 以及假造重導訊息 (spoofed redirect message) 等。攻擊者可佯裝為對外的路由器 (稱之為惡意的路由器)，對本地連結的主機傳送群播的 RA 訊息或回應的 RA 訊息，使本地連結的主機誤認為其為對外連線的路由器，以便接收所有主機對外的連線資料，使攻擊者可以進一步發動中間人攻擊 (Man-in-the-Middle attack，MITM)。

(2) RA 洪水 (Flooding) 攻擊

除了偽冒 RA 攻擊外，IPv6 RA Flooding 則是一種嚴重的 DoS 攻擊，攻擊者發出大量偽冒的 RA 訊息，受攻擊主機資源因為處理大量 RA 訊息而被耗盡，RA Flooding 可能導致整個區域網路服務阻斷，讓所有連到此區域網路的主機系統停止運作無法回應，讓所有用戶都無法使用該網路服務。

IPv6 RA 攻擊防護機制可參考[RFC 6104]〝Rogue IPv6 Router Advertisement Problem Statement〞文件中規範，針對不

同服務與維運情境需要不同防護方式，有幾種不同的防護方式各有優缺點，主要可以以下 2 種方式處理：

- 可透過 Port ACL (Access Control Lists) 阻斷所有來自於終端 (Host) 發送之 ICMPv6。
- 亦可以並用開源碼 NDPmon (Neighbor Discovery Protocol Monitor，鄰居發現協定監視器) 程式以設定檔比對的方式處理。

在[RFC 6105]〝IPv6 Router Advertisement Guard〞文件中也提出 RA 防護機制，把連接在交換器的網路裝置角色區 (Device-role) 分為主機 (Host) 或是路由器 (Router) 共 2 種，只有連接合法 IPv6 路由器的介面套用路由器的裝置角色，允許來自該介面 RA 訊息可以轉送到相同 VLAN (Virtual Local Area Network，虛擬區域網路) 的其他所有介面；其餘介面則套用主機的裝置角色，來自這些介面的 RA 訊息一律阻擋下來，不可轉送到其他介面，如此一來，用戶主機只會接收到來自合法 IPv6 路由器發送的 RA 訊息，便可以有效解決 IPv6 RA 攻擊所帶來的影響。

**3. ICMPv6 攻擊與防護**

Internet Control Messaging Protocol (ICMP) 設計是藉由驗證點對點 (End-to-End) 的可達性，幫助網路的故障排除，ICMP 也能用於回報目標主機上的錯誤，但是 ICMP 的特性和缺乏內建安全機制，使其變成駭客用來攻擊的手段，例如 IPv6 阻斷服務 DoS 就是最典型的 ICMPv6 攻擊。下圖為 ICMPv6 攻擊示意圖。

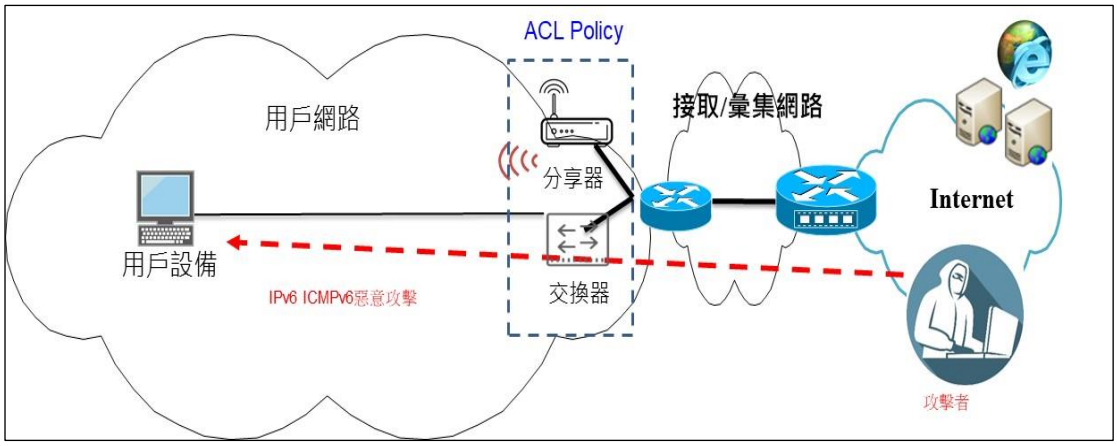



圖 110、IPv6 之 ICMPv6 攻擊示意圖

ICMPv6 阻斷攻擊涉及使用大量流量以最快速度淹沒目標節點或網路，受影響節點會嘗試處理收到的請求 (Request)，因此會使目標節點無法回應其它服務，ICMPv6 的資訊訊息，包含 Echo Request、Echo Reply、RA、NS、NA 及 MLD (Multicast Listener Discovery，群播監聽器發現) 等，皆可用於實現阻斷攻擊使目標主機或網路資源耗盡。此外，由於攻擊者可以改變來源 IPv6 位址，讓攻擊者不容易被辨識出來，因此攻擊的防禦機制更顯重要。

針對 ICMP 防禦機制方面，ICMPv6 和 ICMPv4 兩者完全不同，ICMPv6 是構成 IPv6 通訊基礎，且 IPv6 的操作有賴於 ICMPv6 的特性，基於這些原因無法使用阻檔所有 ICMPv6 訊息類別作為攻擊的防禦機制。

對 IPv4 來說，在設有防火牆的 IPv4 網路中，通常會阻斷大多數 ICMP 訊息的傳送，最主要原因是駭客可利用 ICMP 協定獲取網路異常原因等相關訊息，調整網路探測及攻擊方式，尤其介接網際網路的防火牆必須封鎖 ICMP 的 Echo Request 及

Echo Reply 訊息連線封包。但是在 IPv6 的環境中，ND 協定須依據 ICMPv6 回應訊息，判斷路由器或主機是否存在，因此防火牆須允許特定 ICMPv6 封包通過。為防止 ICMPv6 訊息洩漏可能造成的影響，在[RFC 4980]文件中規範，針對防火牆可能需要開放的規則提出建議，於實際設定時，應秉持最小化原則，針對防火牆規則的來源與目的端設定限制，盡可能設定明確的可連結 IP 範圍，不應貪圖方便而設定為〝Any〞，而增加被攻擊的風險。

## 二. 用戶設備 CPE 之 IPv6 資安防護建議

隨著 IPv6 技術的日漸成熟，家庭用戶 CPE 設備廠商也已陸續支援 IPv6，然而面對駭客的威脅，基本的防禦對策是相當重要的。針對家用設備防護將以[RFC 6092]文件為基礎，重點摘要家用寬頻分享器 IPv6 防護建議，主要分為 IPv6 基本防護功能、Connection Free Filters ICMPv6 功能、VPN 與 IPsec Filters 功能及 Mobile IPv6 Filters 功能，共 4 個類別進行探討，詳細如下所述：

### (一) IPv6 基本防護功能

家庭用戶 CPE 設備應考量不得轉送以下類別訊息，包含：

- 來源 IPv6 位址為群播位址之封包。
- 目的 IPv6 位址為大於或等於路由器群播位址之封包。
- 含已廢除擴充標頭之封包。
- 違反 ingress filtering 之封包。
- Inbound DNS 查詢預設不能被 WAN 介面執行
- Inbound DHCPv6 預設不能被 WAN 介面執行或轉送
- Inbound ICMPv6 錯誤訊息 Destination Unreachable 與 Packet

Too Big 不屬於由內往外通訊 Flow 狀態記錄之封包。

## (二) Connection Free Filters ICMPv6 功能

家庭用戶 CPE 設備應考量 ICMPv6 功能，包含：

- 防火牆 ICMPv6 錯訊訊息套用[RFC 4890]文件的規範。
- 預設讓由外往內 Echo Request、Time Exceeded (Type 3)、Parameter Problem (Type 4) 允許通過。
- Inbound 且不屬於通訊 Flow 狀態記錄之 Destination Unreachable 與 Packet Too Big 錯誤訊息皆丟棄。

## (三) VPN 與 IPsec Filters 功能

家庭用戶 CPE 設備應考量 VPN 及 IPsec Filters 功能，包含：

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

## (四) Mobile IPv6 Filters 功能

家庭用戶 CPE 設備應考量 Mobile IPv6 Filters 功能，包含：

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

policy 需丟棄。

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

## 三. 用戶設備 CPE 之 IPv6 ACL 規則建議

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

- 回送位址 (Loopback Address)，例如〝::1/128〞。
- 未定位址 (Unspecified Address)，類似 IPv4 位址〝0.0.0.0〞，例如〝::/128〞。
- IPv4 對映位址 (IPv4-mapped address)，例如〝::ffff:0:0/96〞。
- 單播區域鏈結位址 (Link-local unicast address)，例如〝fe80::/10〞，〝fe90::/10〞，〝fea0::/10〞，〝feb0::/10〞。
- Site-local 位址，例如〝fc00::/7〞。
- 文件位址 (Documentation address)，例如〝2001:db8::/32〞。
- 在 [RFC 4843] 中所描述的 ORCHID (Overlay Routable Cryptographic Hash Identifiers) 使用位址。因為這些是不可繞送的 IPv6 位址,於加密雜湊識別中使用,例如〝2001:10::/28〞。
- IPv6 Benchmarking 位址，例如〝2001:2::/48〞。
- RTBH (Remote Triggered Black Hole) 路由捨棄前綴 (Discard-only prefix) 位址，例如〝0100::/64〞。

- IANA 保留特別用途的位址區段，例如〝2001:0000::/29〞~〝2001:01f8::/29〞。
- IETF 保留的位址區段，例如〝0000::/8〞、〝0100::/8〞、〝0200::/7〞、〝0400::/6〞、〝0800::/5〞、〝1000::/4〞、〝a000::/3〞、〝e000::/4〞、〝f800::/6〞、〝fe00::/9〞、〝fec0::/100〞、〝3ffe::/16〞 等。

## 四. 用戶設備 CPE 之 IPv6 ACL 設定流程與測試方法

針對 CPE IPv6 資安防護機制，ACL 是 IPv6 基本的防禦機制之一，家庭網路 IPv6 ACL 的安全佈署可應用於分享器/交換器或是一般家庭用戶分享器等位置，針對非經許可的 IPv6 用戶連線進行管控。以下將以 D-Link 寬頻分享器為例，設計 IPv6 ACL 測試架構與流程。下圖為家用 CPE IPv6 ACL 測試架構範例：

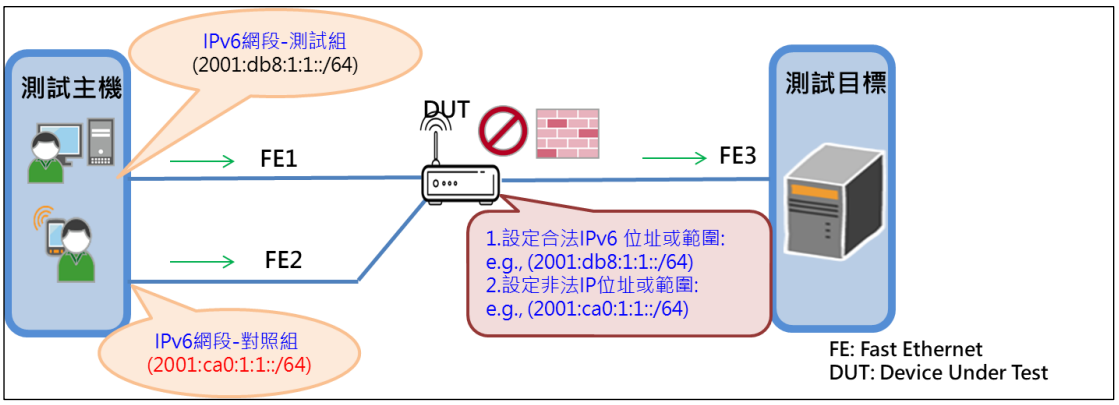



圖 111、家用 CPE IPv6 ACL 測試架構範例

測試主機可用個人終端裝置如電腦或手機等針對目標的 IPv6 網站或服務進行連線測試，中間的 DUT (Device Under Test) 裝置為待測物 CPE，測試範例流程如以下，設計 IPv6 ACL 測試架構與流程如下表所示。ACL 機制針對 IPv6 的阻斷攻擊如 ICMP、RA flooding、IPv6

Extension Header 等攻擊情境。

圖 112、D-Link CPE IPv6 ACL 設定範例

CPE IPv6 ACL 基本操作流程如下:

- 依 CPE 的產品說明書指示,以預設帳號密碼登入 CPE 的 Web 設定頁面,透過此 Web UI 方式進行相關設定。
- 進入 IPv6 設定頁面。
- 選擇禁止或允許下列清單進行存取。
- 依據設定頁面,設定需要禁止或允許通過的來源 IP 位址範圍、目的 IP 位址範圍、協定及連接埠的範圍等。
- 確認新增規則,完成 IPv6 ACL 功能設定。

表 72、IPv6 ACL 網路安全防禦機制測試範例

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

下圖顯示 D-Link 寬頻分享器測試結果，首先測試確認用戶 IPv6 位址可以正常上網無誤。

圖 113、確認用戶 IPv6 上網正常

確認 IPv6 連結正常後啟用 ACL 功能後，確認被設定阻擋的主機無法取得 IPv6 位址，測試結果顯示該設備 IPv6 ACL 可以正常運作。

圖 114、啟用 ACL 功能後被設定阻擋的主機無法取得 IPv6 位址

## 五. 結論

此分項工作主要探討家用網通設備 CPE IPv6 網路安全攻擊與防護措施，研擬家庭網路設備 IPv6 網路安全功能需求建議。整理攻擊類型包含：

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

並針對家用寬頻分享器 CPE IPv6 基礎防護功能進行測試。經測試結果證實，家用寬頻分享器之 ACL 功能可確實阻擋非經許可的 IPv6 用戶連線，達到基本家用網路防護功能。

關於 IPv6 家用資通安全防護內容，詳細資訊請參閱附錄六內容有完整說明。

# 第二節 IPv6 企業用戶資通安全防護研析

此分項工作規劃進行 IPv6 網路安全的基本知識與技術，針對企業網路 IPv6 網路安全功能需求，制定企業用戶網路 IPv6 安全防護規範，提供 IPv6 企業網路安全管理參考建議。內容包含：

- 企業網路 IPv6 安全議題與解決方案
- 企業網路 IPv6 資安防護建議
- 企業網路設備基礎 IPv6 防護機制測試

圖 115、企業用戶 IPv6 資通安全防護技術研究範疇

此項工作將依照原訂計畫規畫時程，於期中之後依序進行相關議題研析，並於期末產出企業用戶 IPv6 資通安全防護手冊一份。以下將就研究成果進行摘要說明。

## 壹、企業網路 IPv6 安全議題與解決方案

以下將針對引進 IPv6 強化資安功能，及引發新資安議題進行分析。其次對於既有 IPv4 資安問題，從 IPv6 角度提出相對建置建議

### 一.IPv6 協定在網路安全上的強化

針對 IPv6 在網路安全上的強化功能有 6 項，整理如下表所示：

表 73、IPv6 在網路安全上的強化功能

| 序號 | IPv6 網路安全強化功能 |
|---|---|
| 1 | **端到端的安全保證**<br>● 移除 NAT 機制，允許所有網路節點使用其唯一位址進行通訊<br>● 端點數據封包進行 IPSec 封裝<br>● 路由器對有 IPSec 擴充表頭的 IPv6 數據封包進行透通傳輸<br>● 完成對通訊端驗證和對數據加密保護，讓數據可以在 IPv6 網路上安全地傳遞<br>無需針對特別的網路應用部署 ALG (應用層閘道器)，即可保證端到端網路透明性，利於提高網路服務速度 |
| 2 | **可聚集 (aggregate-able) 層次化的位址結構**<br>● IPv6 位址構造具可聚集性，且層次化，因此接入路由器易於進行來源位址檢查，使 ISP 可以驗證其客戶位址的合法性 |
| 3 | **有效防止未授權的接取**<br>● IPv6 對身份驗證的支援，及對數據完整性和數據機密性的支援和改進，使得 IPv6 增強並防止未授權接取能力，更適合於對敏感資訊和資源有特別處理要求的應用。 |
| 4 | **強化的網域名稱系統 DNS**<br>● 以 IPv6 為基礎的 DNS 系統可作為公共密鑰基礎設施 (PKI) 系統基礎，有助於抵禦網路身份偽裝與偷竊<br>● 採用 DNS 安全擴展 (DNS Security Extensions) 協定，可增強針對 DNS 新攻擊方式的防護能力，例如〝網路釣魚 (Phishing)〞攻擊、〝DNS 中毒 (DNS poisoning) 〞攻擊等。 |
| 5 | **有效防止網路掃描與病毒蠕蟲傳播**<br>● 感染式病毒和蠕蟲傳播在 IPv4 環境下非常迅速，但在 IPv6 環境下並不適用。因為 IPv6 巨大位址空間讓病毒及網路蠕蟲在 IPv6 的網路中傳播變得困難。 |
| 6 | **有效防止網路放大與碎片 (Fragment) 等攻擊**<br>● ICMPv6 設計上不會回應群播位址和廣播位址的訊息，所以只需要在網路邊緣過濾群播封包即可有效阻止由攻擊者向廣播網段發送數據封包而引發的網路放大攻擊。<br>● IPv6 認為 MTU 小於 1280 位元組的封包為非法，處理時會丟棄 (除非是最後一個封包)，此有助於防止碎片攻擊。 |

## 二.引入 IPv6 可能引發的安全問題

### (一)IPv4 與 IPv6 共存的架構可能存在新資安風險

IPv6 與 IPv4 網路共存，網路同時存在兩者的安全問題，及產生新的安全漏洞。例如駭客可以利用 IPv6 對同時具備 IPv4 和 IPv6 兩種協定的 LAN 網路進行非法接取，惡意攻擊者可以通過安裝雙協定的 IPv6 主機，建立由 IPv6 到 IPv4 的隧道，繞過防火牆對 IPv4 網路進行攻擊。導入 IPv6 協定時，其安全措施必須重新經過慎重的考慮和測試才能安心上線。

### (二)IPv6 的網管設備和網管軟體尚未成熟

目前針對 IPv6 的網管設備和網管軟體支援 IPv6 仍然有限，因此缺乏對 IPv6 網路進行監測和管理的有效方法，亦缺乏對大範圍的網路故障定位和性能分析的機制。

### (三)IPv6 的資安產品尚未成熟

IPv6 網路同樣需要防火牆、VPN、IDS、漏洞掃描、網路過濾、防止病毒閘道器等網路安全設備。事實上 IPv6 環境下的病毒已經出現，但其安全技術研發還尚需時日。IPv6 防火牆需面對挑戰包含：

- 封包表頭差異：在 IPv4 中沒有擴充表頭，因此在設計 IPv6 防火牆時，需特別針對擴充表頭處理，進行封包過濾時要能辨識出含擴充表頭的封包。
- 端對端 (End-to-End)：網際網路最初的概念就是端對端，由於 IPv4 位址不足，而破壞此架構，IPv6 讓網路回歸到端對端的概念。但是防火牆進行封包過濾與執行安全政策時，又剪斷端對端的連結，因此在設計 IPv6 防火牆時，需要找出對應解決方法。

- 行動能力 (Mobility)：在 IPv6 行動能力應用上，一個外地主機都被視為本地設備，因此進行封包過濾時，需解決面對一個移動節點而不能將其視為外地主機的問題。
- IPv6 重要安全機制 IPSec：IPSec 可視為網路加密通道，其允許任何使用者跳過安全性政策的檢查。因此在 IPv6 環境中要使用 IPSec，就必須解決如何過濾在加密通道中傳遞資訊的問題。
- 傳輸路徑上的最大傳輸單位 ( Path MTU)：IPv6 封包只在來源主機進行封包分割，其利用 ICMPv6 協定找出 Path MTU，因此 IPv6 防火牆需要具備辨識和處理 ICMPv6 封包能力。

### (四) 其他新的安全挑戰

IPv6 協定仍需在實踐中持續做改進，例如 IPv6 群播功能僅規定簡單認證功能，所以還難以實現嚴格的用戶限制功能，而行動 IPv6 也存在很多新的安全挑戰待克服。

## 三.IPv6 面對資安弱點的解決方案

在 IPv4 網路環境中，資安攻擊方式可概分為 11 類別，如下表所列：

表 74、IPv4 資安攻擊類別

| 序號 | 類別 | 序號 | 類別 |
|---|---|---|---|
| 1 | 偵查 | 7 | 路由攻擊 |
| 2 | 非法接取 | 8 | 偵聽 |
| 3 | 表頭篡改與數據封包分片 | 9 | 應用層攻擊 |
| 4 | 第三層和四層資訊欺騙 | 10 | 中間人攻擊 |
| 5 | ARP 和 DHCP 攻擊 | 11 | 泛洪 (flooding) |
| 6 | 廣播放大攻擊 (smurf) | | |

以下就從 IPv6 角度,摘要說明如何利用 IPv6 來解決上述各種攻擊。

## (一)偵查：

網路偵查在 IPv4 中很簡單，駭客可以使用 Ping 掃瞄、Port 掃瞄、應用及漏洞掃瞄輕易達到目的，但在 IPv6 環境不同，由於單一 IPv6 子網的 IPv6 位址通常為 2 的 64 次方，掃描相當費力，幾乎不可能，降低 IPv6 網路被掃瞄的機會與意願。

## (二)非法接取

IPv4 網路環境，通常會執行以下動作來避免非法存取：ACL 邊界轉送及 ACL 主機轉送。在 IPv6 網路環境，利用相同動作來避免非法存取，也可進一步啟動 IPSec，有利於進行存取控制。

## (三)表頭篡改與數據封包分片

IPv4 網路環境，存在此類型資安危機包含：

- 利用分片 (fragmentation) 困惑，以繞過路由器或轉送存取控制。
- 利用重疊數據或檔頭，以繞過路由器或轉送存取控制。
- 利用分片癱瘓 IDS 等安全防護工具。引進 IPv6 網路環境後，在[RFC 2460]文件中明定，在 IPv6 網路中分片只能在終端 (end) 執行，任何中間經過分片的封包均被視為攻擊發生而直接丟棄，而重疊分片在 IPv6 不被允許。

## (四)第三層和四層資訊欺騙

IPv4 網路環境,存在此類型資安危機包含:DOS、DDOS、spam、蠕蟲、及病毒攻擊等。在[RFC 2827]文件中明定應實現訊息輸入過濾 (ingress filtering) 功能，將欺騙的第三層資訊流 (L3 traffic) 擋

在源頭，但若駭客使用子網內的 IP 位址，則[RFC 2827]文件仍無法防範。此外，[RFC 2827]對於第四層欺騙 (L4 spoofing) 幫助不大。

引進 IPv6 網路環境，由於 IPv6 位址具有聚合 (aggregated) 特性，讓 ISP 容易實現[RFC 2827] 過濾功能，讓欺騙第三層資訊流停留在客戶端，不會無限制擴散。

## (五) ARP 和 DHCP 攻擊

在 IPv4 網路環境下，存在此類型資安危機包含：

- 駭客竄改 IP-MAC 之間的對應，讓無辜使用者與駭客對話，進而啟動中間人攻擊 (man-in-the-middle attack)。
- 駭客假冒 DHCP server，進而啟動中間人攻擊。
- 駭客利用 flooding 攻擊，癱瘓合法的 DHCP server。

引進 IPv6 網路環境後，由於 ARP 已被 ICMPv6 的 ND 所取代，所以 IPv4 網路環境下的 ARP 資安問題自然消失，但是 IPv6 的 ND 仍繼承既有的 ARP 資安問題。

IPSec 為可能解決辦法，或是實現[RFC 3971]文件中規範 SEND (SEcuring Neighbor Discovery) 亦可解決。

## (六) 廣播放大攻擊

IPv4 網路環境，存在此類型資安危機包含：駭客利用 ICMP Echo 訊息、子網廣播目的位址、假冒來源位址執行〝smurf〞攻擊等。引進 IPv6 網路環境後，IP 廣播動作已被移除，若 IPv6 終端用戶實際實現[RFC2463]文件描述規範，則〝smurf〞或類似攻擊可被有效減緩。

### (七)路由攻擊

IPv4 網路環境，一般使用 MD5 保護路由器之間的路由交換訊息，引進 IPv6 後，啟動 IPSec，對於預防路由攻擊有所助益。

### (八)偵聽

可以使用 IPSec 降低被竊取資料的機會。

### (九)應用層攻擊

病毒及蠕蟲均屬於此類，使用 IPSec 後，安全檢查與防護將落到主機身上，因為傳送過程為加密過的資料。

### (十)中間人攻擊

可以使用 IPSec 降低被攻擊的機會，建議使用 IKE main mode。

### (十一)泛洪攻擊

針對 Flooding，IPv6 並無新增之防護方法，建議沿用 IPv4 既有方法予以防範。

## 四.企業網路導入 IPv6 部署需求與指引

以下主要參考國際 RFC 標準針對企業網路導入 IPv6 部署需求進行探討，並摘要企業網路部署 IPv6 參考指引。

### (一)企業網路部署 IPv6 需求

企業網路部署 IPv6 需求可參考[RFC 4057] Enterprise IPv6 Scenarios 文件規範，摘要說明如下表所示：

表 75、企業網路部署 IPv6 需求

| 序號 | 企業網路部署 IPv6 需求 |
|---|---|
| 1 | **DNS 網域名稱伺服器** |
| | ● 必須同時提供 IPv4 和 IPv6 服務，且要配合做好相關設定以確保連線。 |
| 2 | **路由協定 (Routing)** |
| | ● 內部和外部路由需同時支援 IPv4 和 IPv6 路由協定交換，確認 IPv6 路由拓撲在內網狀況，及與外部連接的介面、供應商網路、過渡機制等。 |
| 3 | **終端用戶配置** |
| | ● 企業終端用戶應採固定的 IPv6 網路設定，或採用 DHCPv6 來進行位址設定，企業也需要確認上游供應商網路是如何分配。 |
| 4 | **安全策略 (Security)** |
| | ● 管理單位需要檢視既有資安工具是否支援 IPv6，並研擬企業網路導入 IPv6 的資安防護計畫。 |
| 5 | **應用服務** |
| | ● 現有的應用服務需要移植或提供新的替代服務，確保同時提供 IPv4 和 IPv6 服務能力。 |
| 6 | **網路管理** |
| | ● 新增的 IPv6 網路基礎設施元件需要被納入管理。<br>● 管理單位必須確認網路管理平台是否提供 IPv6 版本，同時需要規劃 IPv6 網路用以監控網路內的節點。 |
| 7 | **位址規劃** |
| | ● 資訊管理單位需要擬定 IP 申請發放的規定。<br>● 為了應對 IPv6 導入初期的轉換需求，建議保留一組 IPv4 位址提供轉換服務使用 |

## (二) 企業部署 IPv6 指引

企業網路部署 IPv6 指引主要參考 RFC 7381 Enterprise IPv6 Deployment Guidelines 文件，內容針對內部以及外部網路兩個部分進行討論。在企業網路內部 IPv6 部署階段指引摘要如下表所示：

表 76、企業網路內部 IPv6 部署階段指引

| 序號 | 企業網路內部 IPv6 部署階段指引 |
|---|---|
| 1 | **安全政策 (Security)** |
| | ● 內部所有現存於 IPv4 安全策略必需同步擴展支援 IPv6。 |
| 2 | **網路基礎架構** |
| | ● 企業網路必須為用戶提供備援路徑。 |
| 3 | **終端用戶裝置** |
| | ● 主要作業系統均已支援 IPv6，但仍應注意個別用戶終端裝置 IPv6 啟動狀態。 |
| 4 | **系統環境** |
| | ● 部署 IPv6 應整體考量 IT 環境部署情況，所有個別系統如 email、VoIP 或 DNS 等，都需要有詳細 IPv6 部署計畫。 |

針對企業網路外部 IPv6 部署階段指引摘要說明如下表所示：

表 77、企業網路外部 IPv6 部署階段指引

| 序號 | 企業網路外部 IPv6 部署階段指引 |
|---|---|
| 1 | **網路接取** |
| | ● 企業需要與一個或多個服務供應商合作取得網路的連接，並考慮優先以 Native IPv6 連接。 |
| 2 | **安全政策 (Security)** |
| | ● 外部網路 IPv4 與 IPv6 安全政策需一致，同時也必須提供過濾與監控機制。 |
| 3 | **網路監控** |
| | ● IPv6 應做到監控網路連接使用狀況，比照 IPv4 網路連接監控，報告異常流量模式（例如：連接埠掃描、SYN Flooding 及相關的 IP 來源）。 |
| 4 | **服務與應用伺服器** |
| | ● 連接網路服務所經路經上之設備如防火牆、負載平衡裝置、資安設備及相關伺服器建議啟用雙協定 (Dual Stack)。 |
| 5 | **IPv6 NPT 轉換機制** |
| | ● 須了解 NPT 機制部署的必要性與涵義。 |

# 貳、企業網路 IPv6 資安防護建議

## 一.企業網路導入 IPv6 安全指引

IPv6 網路整體安全性至少必須透過四個層面實現：移轉安全、協定安全、網路安全及其他項目，以下將分項簡要說明。

### (一) 移轉安全

IPv6 與 IPv4 網路將會長期共存，網路必然會產生新的安全漏洞。向 IPv6 協定轉移，其安全措施必須經過慎重考慮和測試。目前，IPv4 向 IPv6 過渡技術以雙協定、隧道和協定轉換三種為主。建議向 IPv6 轉移應儘量採用雙協定技術，避免採用協定轉換，若需使用隧道技術則儘量採用靜態隧道，避免採用動態隧道。

### (二) 協定安全

網路安全威脅來自多個層面，包括實體層、數據鏈路層、網路層、傳輸層和應用層等。在實體層以上，安全性隱憂主要來自於針對各種協定的安全威脅，及意在非法佔用網路資源或者耗盡網路資源的安全隱憂，諸如雙 802.1Q 封裝攻擊、廣播包攻擊、MAC 洪泛攻擊、生成樹攻擊等二層攻擊，及假的 ICMP 訊息、ICMP 洪泛攻擊、來源位址欺騙、路由振盪等針對三層協定的攻擊。在應用層，主要有針對 HTTP、FTP/TFTP、Telnet 以及通過電子郵件傳播病毒的攻擊。針對不同攻擊類型應採取對應安全策略加以防範。

### (三) 網路安全

IPSec 隧道和傳輸模式的各種組合應用，可以提供網路各層面的安全保證。諸如：端到端的安全保證、內部網路的保密、通過安全隧道構建安全的 VPN 等。端到端的安全保證在兩端主機上對資料進行 IPSec 封裝，中間路由器實現對有 IPSec 擴充表頭的 IPv6

資料透通，從而實現端到端的安全保證。在內部網路保密方面，由於 IPSec 作為 IPv6 擴充表頭不能被中間路由器而只能被目的節點解析處理，因此，可以透過 IPSec 來保證內部網路的安全。在利用 IPSec 安全隧道實現 VPN 方面，路由器之間建立 IPSec 安全隧道以構成安全的 VPN，是最常用的安全網路建置方式。

### (四) 其他

綜合以上所述，安全網路是眾多安全技術的綜合體，而 IPv6 IPSec 機制是其中重要組成，可提供協定層面上的一致性解決方案，也是 IPv6 對比 IPv4 的重大優越性。其他結合認證機制、路由過濾、分級管理、接取列表和關鍵事件的日誌等措施，也應該一併考慮，才能讓導入 IPv6 網路更為安全。

## 二. 網路設備與主機 IPv6 安全防護建議

以下針對資安設備，網路設備與伺服器與終端設備摘要 IPv6 建議。

### (一) 資安設備

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

- 清查既有防火牆是否支援 IPv6，透過汰舊換新過程逐步更換。
- 取得支援 IPv6 能力，如以韌體升級方式支援 IPv6，須注意檢查 CPU 負載及記憶體消耗狀況，避免效能不足防火牆。
- 支援 IPv6 後可參考 IPv4 規則設定 IPv6 過濾方式 (ACL)，再依據觀測 IPv6 流量資訊，逐步完善 IPv6 防禦規則。

  並針對流量及記錄相關 Log 作為分析及改善依據。

### (二) 網路設備

網路設備係以路由器與交換器為主，在路由器部分，IPv6 防護建議包含啟動 uRPF、啟動 SEND、禁止 RH0 與未知 IPv6 延伸表頭等。針對交換器部分，建議是以 IPv6 First Hop Security 為主，設備須可支援 RA Guard、DHCP Guard、IPv6 Snooping、Source/Prefix Guard 及 Destination Guard 等基本 IPv6 防護功能。

### (三) 伺服器與終端設備

簡要來說，企業網路 IPv6 安全佈署基本上除防火牆必須完整支援 IPv6 外，網路設備也需要能有效過濾與稽核 IPv6 位址，可預防未經授權 IPv6 用戶存取企業網路內部資源，此外，對於用戶網路終端設備管理則可以考慮透過 Static 或 DHCPv6 用戶定址技術來有效管理企業網路內部主機或設備，透過有效的網路管理機制及用戶定址技術，能提升企業佈署 IPv6 的安全性。

## 三.IPv6 網路安全管理建議

在 IPv6 網路安全管理方面，首要任務也是基本原則就是加強網管人員之 IPv6 專業知識教育訓練，以藉此強化 IPv6 安全相關議題之管理。

總結來說，為了降低導入 IPv6 投資成本與風險為主要目標，企業網路導入 IPv6 應考慮提供 IPv6 資安服務行動方案，重點如下表所示：

表 78、企業網路資安工作重點

| 序號 | 名稱 | 說明 |
|---|---|---|
| 1 | IPv6 安全能力調查 | 進行現有相關資訊系統與網路設施之 IPv6 安全防護現況資訊調查，包括 Firewall、IPS、IDS 等。 |
| 2 | IPv6 安全策略規劃 | 針對各公司機關或商用服務規劃 IPv6 網路資安防護導入策略，提高部署效率。 |
| 3 | IPv6 資安技術研究 | 研究前瞻性 IPv6 網路安全防護技術，提高安全防護品質。 |
| 4 | 建立 IPv6 安全管理制度 | 訂定與完善 IPv6 網路安全管理制度，提昇管理有效性。 |
| 5 | IPv6 網路安全教育訓練 | 定期安排 IPv6 網路資訊安全專業訓練。 |

## 參、企業網路設備基礎 IPv6 防護機制測試

企業用戶經由企業內架設交換機、防火牆、路由器再透過 ISP 提供 Hinet 光世代網路連接至外部網路。企業網路架構如下圖所示：

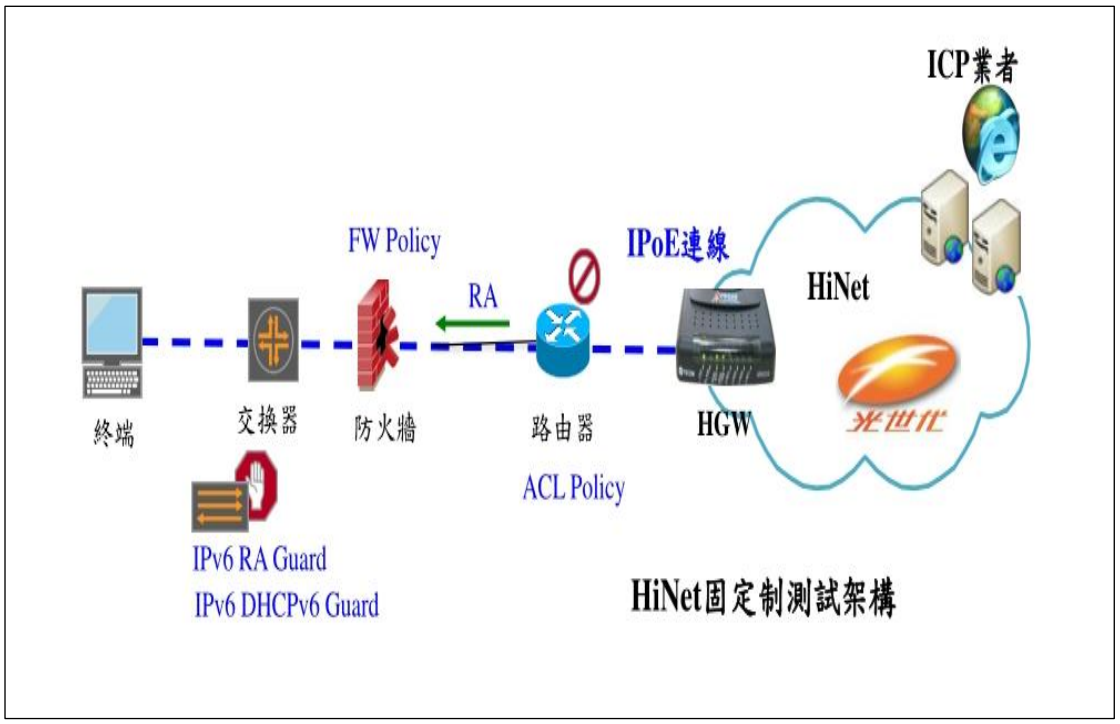



圖 116、企業網路架構

針對企業網路設備測試交換機、防火牆、路由器請參閱附錄六，企業用戶 IPv6 資通安全防護手冊內容，有詳細說明。

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

表 79、企業網路導入 IPv6 安全防護檢核清單

| 項次 | 說明 |
|---|---|
| 1 | 研擬企業網路 IPv6 資安工作計畫。制定 IPv6 安全策略、盤點設備/系統 IPv6 支援能力、建立 IPv6 安全管理制度以及加強 IPv6 網路安全教育訓練等 |
| 2 | 避免企業外部電腦設備直接存取企業內部的網路主機或設備 |
| 3 | 防火牆設備必須能完整支援 IPv6 |
| 4 | 重要資訊系統建議採用固定 IPv6 位址並考慮使用加密認證機制(IPsec 或是其他類似機制) |
| 5 | 管理者需使用安全的遠端存取 SSH (Secure Shell) 機制和確保本通信介面不使用預設密碼 |
| 6 | 強制使用 FQDN 與 DNS 定址，本地端使用者建議使用固定 IPv6 位址或採 DHCPv6 方式 |
| 7 | 決定有效 ICMP 封包過濾執行及 RFC 4890 所建議之封包篩選規定 |
| 8 | 採用 IPv6 unicast reverse path forwarding 拒絕不明來源位址封包 |
| 9 | 阻止一切來自於不安全 IPv6 網路來源位址的訊息流量 |
| 10 | 檢查 Outbound traffic 以及目的位址回應的匹配條件，檢測用戶是否有無意間夾帶任何殭屍網路流量或者惡意訊息 |
| 11 | 攔截所有 Inbound SSL/TLS IPv6 訊息流量，並進行必要檢查 |
| 12 | 通過 IPS 訊息需進行網路傳輸速率限制，避免網路設備流量超載 |
| 13 | 路由協定如 OSPFv3、RIPng、BGP 及 IS-IS 應使用加密認證機制加強保護 |
| 14 | 建議禁止使用 Tunnel 技術，(如 IP Protocol 41、UDP 3544 teredo 等) |
| 15 | 建議啟動 First Hop Security 機制確保 IPv6 用戶接取網路安全 |

關於 IPv6 企業用戶資通安全防護內容，詳細資訊請參閱附錄六有完整說明。

# 第八章 ICP IPv4/IPv6 雙協定網路安全技術防護人才培訓教育訓練

「ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓」教育訓練課程，主要是針對企業有對外網站，計畫進行網站升級支援 IPv4/IPv6 雙協定網路服務之對象為主。

此次教育訓練課程的教材內容，以民國 108 年教育訓練課程內容為基礎，由講師進行修訂以符合授課目標，課程大綱如下表所列：

表 80、「ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓」課程大綱

| 時間 | 課程內容 |
|---|---|
| 08:30-09:00 | 報到 |
| 09:00-10:20 | IPv4/IPv6 雙軌運作概念介紹<br>IPv4/IPv6 雙軌環境建置概述<br>IPv4/IPv6 雙軌網路環境建置 (Router, Firewall, Load Balance) - 第一部分 |
| 10:20-10:40 | 休息 |
| 10:40-12:00 | IPv4/IPv6 雙軌網路環境建置 (Router, Firewall, Load Balance) - 第二部分<br>網路升級流程步驟和檢查項目清單 |
| 12:00-13:30 | 用餐及休息 |
| 13:30-14:50 | 作業系統 IPv6 建置示範 (Centos7, Ubuntu18, Windows 2016)<br>資料庫 IPv6 調整示範 (MySQL5, Windows SQL server 2017)<br>網站伺服器 IPv6 調整示範 (IIS8, Apache2, Nginx)<br>程式檢查 (PHP, ASP.NET)<br>作業系統與網站升級流程步驟和檢查項目清單 |
| 14:50-15:10 | 休息 |
| 15:10-16:30 | IPv4/IPv6 雙軌環境下資訊安全規劃概述<br>IPv4/IPv6 雙軌環境之資訊安全軟體與硬體設定 (IPtables, Firewall)<br>IPv4/IPv6 雙軌環境下資訊安全檢查項目清單 (網路環境、作業系統、網站、資安設備) |
| 16:30-17:00 | Q&A |

教育訓練課程的教材內容依不同場次講師不同而略有差異，今年於北部、中部及南部各由不同講師進行授課，因此共有3份不同教材，內容請參閱附錄二。

今 (109) 年全年預計完成 8 場教育訓練課程，目前已全數完成，分別於雲林、台北、台南及高雄等地舉辦，各場教育訓練課程活動紀錄如下所述。

## 第一節 第一場教育訓練課程

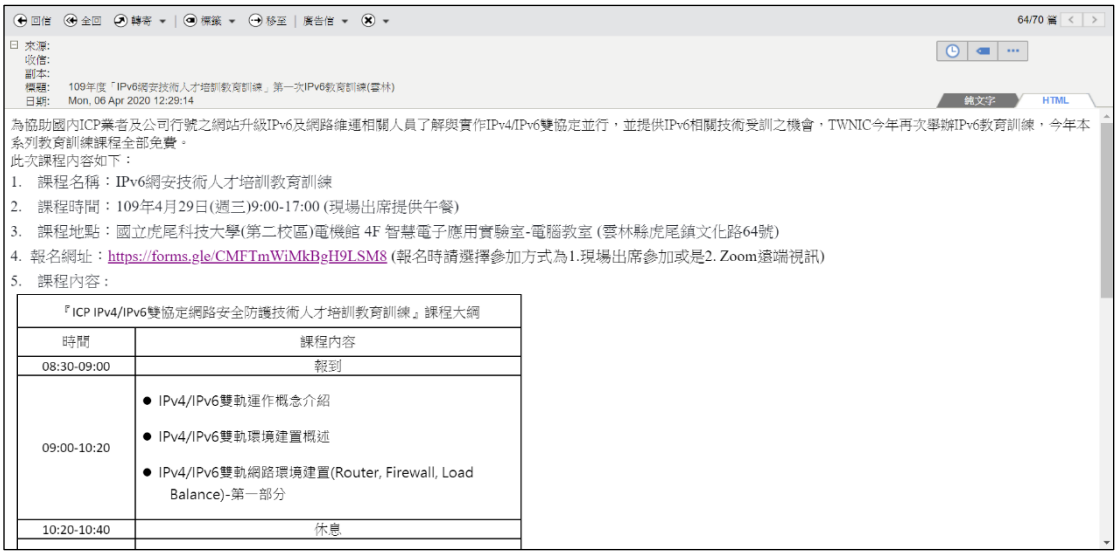
因應今 (109) 年衛生福利部疾病管制署針對嚴重特殊傳染性肺炎冠狀病毒 (Coronavirus disease 2019，COVID-19)，所引發的流行疾病，為維護國人健康而提出集會活動辦理相關建議及社交距離等規定，使得各種集會舉辦不易，本次教育訓練課程於開課前針對課程進行形式做適度彈性調整，研擬開放實體課程及網路課程並行，除了現場教學之外，並開放學員線上參與，針對實體課程教室座位安排及人數進行管控，以避免密閉式空間群聚性傳染的可能性。

並在開課前透過 IP/DNS 論壇、TWNIC 電子報、及以電子郵件方式寄送教育訓練課程資訊給 TWNIC IP 會員等方式進行多方宣傳。以下圖片為教育訓練課程透過各管道進行廣告宣傳截圖畫面。

除此之外，並透過 TiEA (台灣網路暨電子商務產業發展協會)、DTA (數位經濟暨產業發展協會) 及 TCA (台北市電腦商業同業公會) 等協會，對其會員及電子報訂閱客戶等對象，進行教育訓練課程宣傳，以期擴展可觸及學員對象，提升 IPv6 推廣成效。

圖 117、IP/DNS 論壇教育訓練課程宣傳

圖 118、TWNIC 於 4 月份電子報進行教育訓練課程宣傳



回信 全回 轉寄 標籤 移至 廣告信 64/70 篇

來源:
收信:
副本:
標題: 109年度「IPv6網安技術人才培訓教育訓練」第一次IPv6教育訓練(雲林)
日期: Mon, 06 Apr 2020 12:29:14

純文字 HTML

為協助國內ICP業者及公司行號之網站升級IPv6及網路維運相關人員了解與實作IPv4/IPv6雙協定並行，並提供IPv6相關技術受訓之機會，TWNIC今年再次舉辦IPv6教育訓練，今年本系列教育訓練課程全部免費。

此次課程內容如下：

1. 課程名稱：IPv6網安技術人才培訓教育訓練
2. 課程時間：109年4月29日(週三)9:00-17:00 (現場出席提供午餐)
3. 課程地點：國立虎尾科技大學(第二校區)電機館 4F 智慧電子應用實驗室-電腦教室 (雲林縣虎尾鎮文化路64號)
4. 報名網址：https://forms.gle/CMFTmWiMkBgH9LSM8 (報名時請選擇參加方式為1.現場出席參加或是2. Zoom遠端視訊)
5. 課程內容：

| 『ICP IPv4/IPv6雙協定網路安全防護技術人才培訓教育訓練』課程大綱 | |
|---|---|
| 時間 | 課程內容 |
| 08:30-09:00 | 報到 |
| 09:00-10:20 | ● IPv4/IPv6雙軌運作概念介紹<br>● IPv4/IPv6雙軌環境建置概述<br>● IPv4/IPv6雙軌網路環境建置(Router, Firewall, Load Balance)-第一部分 |
| 10:20-10:40 | 休息 |

圖 119、寄送電子郵件給 TWNIC IP 會員進行教育訓練課程宣傳

第一場教育訓練課程於民國 109 年 4 月 29 日舉行，會場地點為國立虎尾科技大學電機館－電腦教室，由蘇暉凱副教授擔任講師。

此次課程參與人數為現場 12 人及遠端視訊 24 人，合計共 36 人參與，回收 22 份問卷，有關教育訓練課程活動資訊來源及滿意度調查，問卷回收率約為 61%，本次教育訓練課程活動整體問卷分數為 4.42 分，高於品質目標分數 3.8。關於學員對問卷內容回覆詳細的統計結果請參考下列圖示。

●問題一：詢問學員獲得活動或課程訊息的來源。

根據問卷回覆統計結果，學員主要〝從 Email 上得知〞獲得課程訊息為主，其次為〝從 TWNIC 相關網站上得知〞，兩項合計超過 85%的比例。

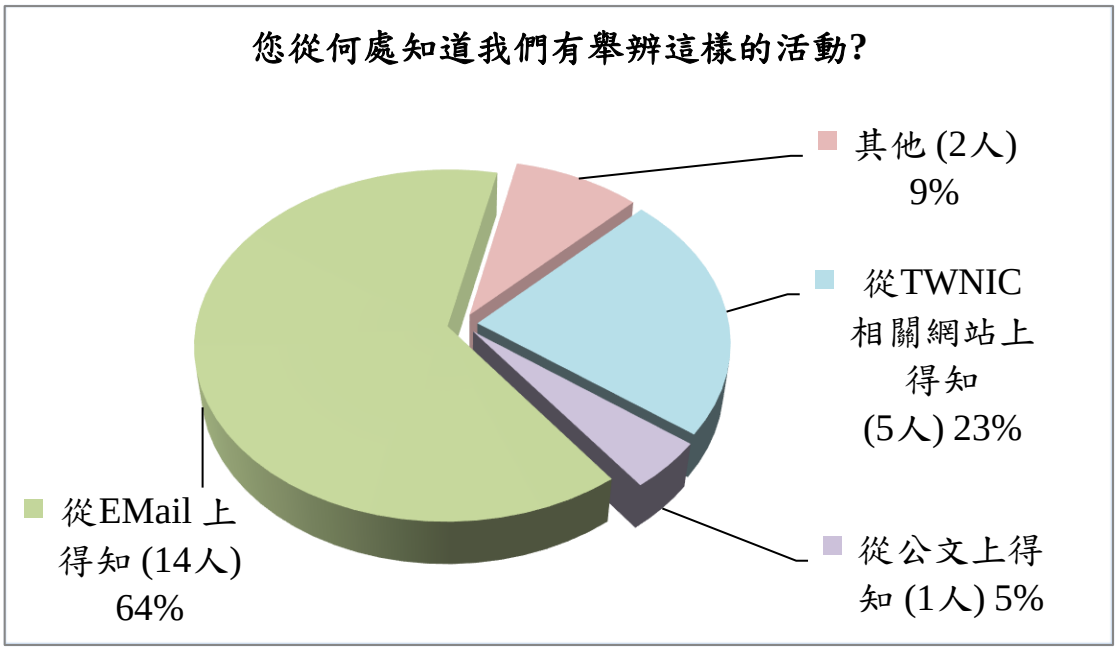



圖 120、4/29 雲林 ICP IPv4/IPv6 教育訓練活動資訊來源調查

●問題二~七：詢問學員對活動或課程內容滿意度調查。

調查項目包含對講師教學、教材內容、場地及設備等，進行學員對課程整體滿意度表現評比。下圖為此次課程滿意度統計圖表。學員對於本次活動大多回覆為〝非常滿意〞及〝滿意〞，所有項目獲得〝滿意〞以上評比的比例高達 90%；只要 1 位學員針對〝教學設備是否足夠?〞回覆為普通；及 2 位學員針對〝場地是否完善?〞回覆為普通。

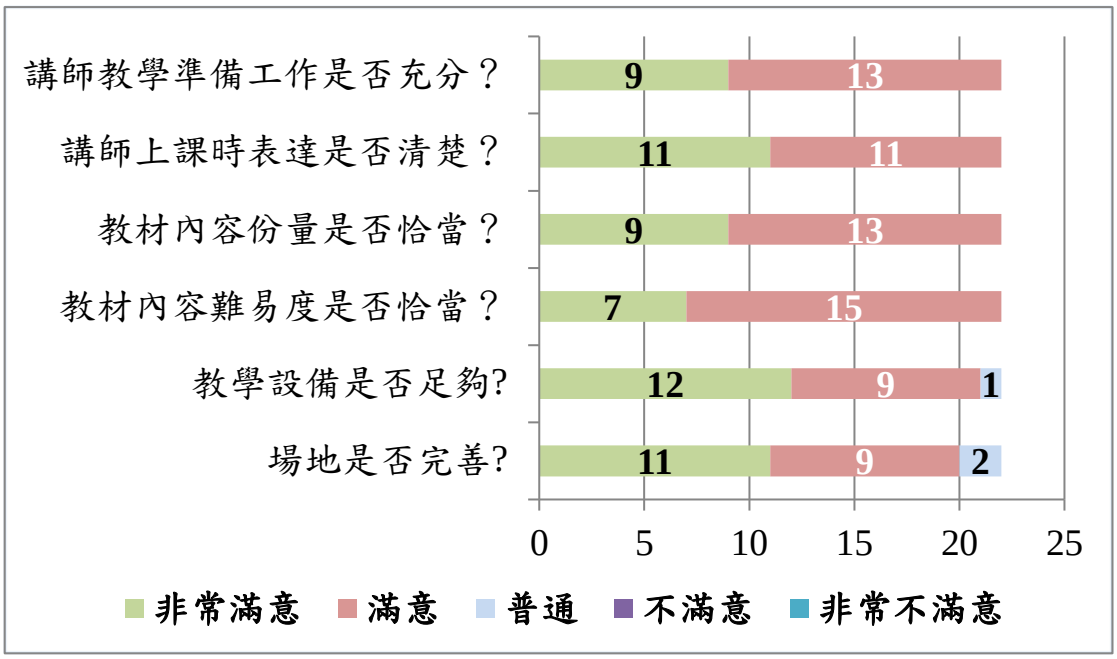



圖 121、4/29 雲林 ICP IPv4/IPv6 教育訓練滿意度統計

問卷調查內容除包含以上統計結果外，因應本次教育訓練除現場實體課程外，部分學員透過遠端視訊參與，針對視訊課程學員提出以下建議：

- 建議可使用直播 (例如:youtube) 進行，可於空閒時間回放複習，避免畫面與音訊傳輸品質不良，且可將教育訓練供一般民眾觀看，以利宣導 IPv6 提升使用效益，謝謝。
- 遠端視訊的聲音可再改善。

針對直播建議須考量講師著作權等議題，需有更通盤考量及規劃，目前暫時不予考慮。至於遠端視訊聲音部分，會持續進行改善。

本次教育訓練會場，及學員上課情形照片如下圖所示：

圖 122、4/29 雲林 ICP IPv4/IPv6 教育訓練會場

學員若透過遠端參與教育訓練課程，是以 Cisco Webex Meetings 參與，以下為遠端課程教材及參與學員截圖畫面：

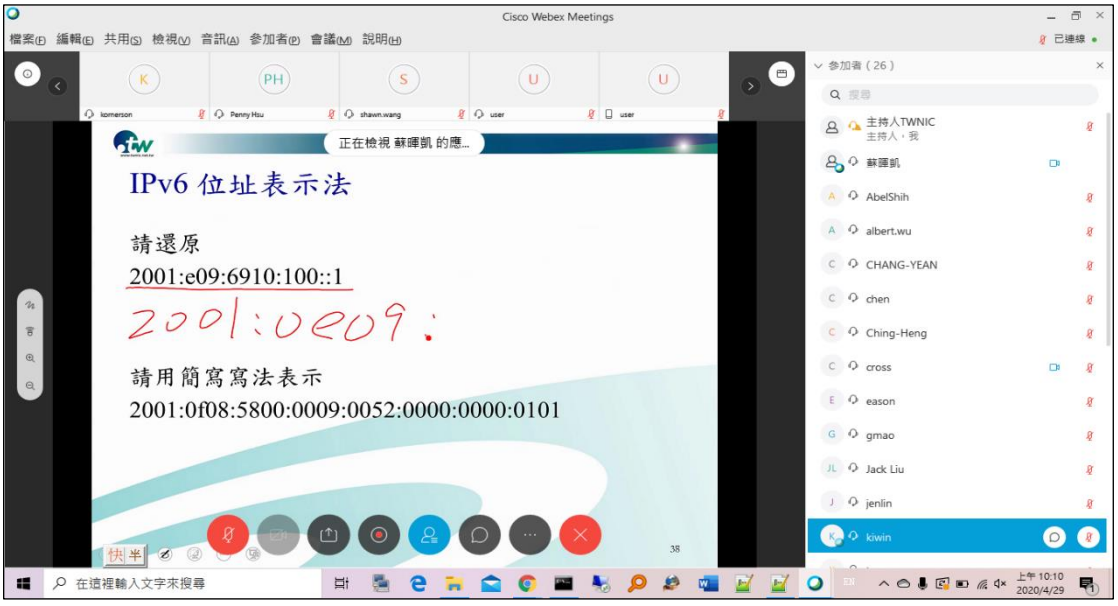



圖 123、4/29 雲林 ICP IPv4/IPv6 教育訓練線上課程截圖

## 第二節 第二場教育訓練課程

第二場教育訓練會場地點為公務人力發展學院福華國際文教會館教室，因應疫情嚴峻期間，為保障參與課程人員健康，會館加強防疫公告以下施行措施：

- 員工及進出本會館之所有廠商皆需配戴口罩及配合測量體溫登記。
- 1 樓住宿櫃檯備有額溫槍，若賓客有體溫疑慮，可主動請 1 樓櫃檯服務人員協助測量體溫，加強防疫。
- 1 樓大廳、B1 休閒中心、各餐廳出入口、會議中心各樓層 (集會棟、教學棟) 及 B2 停車場管理室有放置消毒酒精供客人及員工使用。
- 客房於住客退房後使用消毒劑將傢俱及浴室沖洗擦拭，以守護住宿品質安全。
- 本會館清潔人員定時消毒全館區域以維護環境清潔。
- 前瞻廳、卓越堂及 14 樓貴賓廳等之大型會議提供酒精座供主辦單位對與會者使用。
- 每日會議結束後，使用消毒劑清潔桌面及麥克風，並更換新的麥克風海棉套。

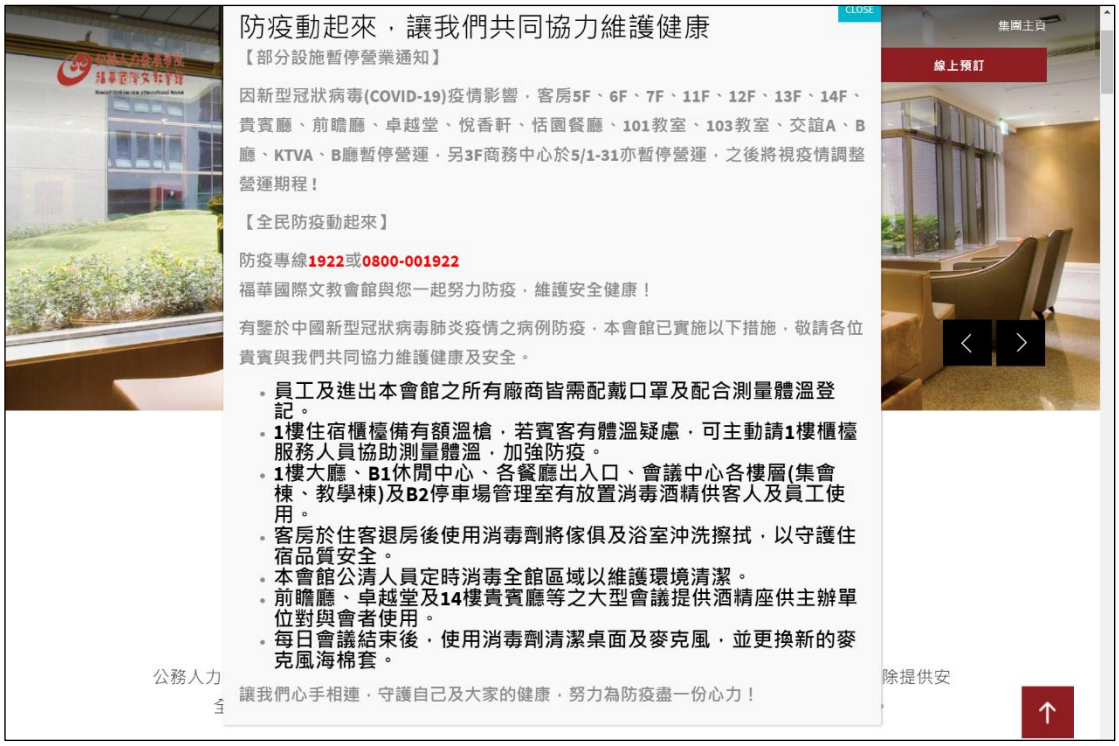



圖 124、福華國際文教會館防疫措施公告

除福華國際文教會館防疫措施公告外，教育訓練課程報名網站及學員上課通知 Email 也加強防疫宣導，所有課程參與人員須配合相關措施，並對參與人數進行管控，報名網站公告防疫措施以下所述：

- 進出場地之所有人員皆需配戴口罩及配合測量體溫及登記檢查。
- 教室內座位採梅花座，保持社交距離，教室人數不超過 30 人。

下圖為 5 月 15 日所舉辦第二場教育訓練報名資訊網站，以及學員上課通知 Email 截圖：

109年度「IPv6網安技術人才培訓教育訓練」第二次IPv6教育訓練(台北)

課程免費(for ICP業者、受邀請公司、人員)，名額有限，請於5月11日前報名，謝謝。

因應新冠肺炎疫情教育訓練防疫措施:
1.進出場地之所有人員皆需配戴口罩及配合測量體溫及登記檢查。
2.教室內座位採梅花座，保持社交距離，教室人數不超過30人。

*必填

電子郵件地址 *

你的電子郵件

財團法人台灣網路資訊中心蒐集個資聲明

您參加財團法人台灣網路資訊中心（以下稱「TWNIC」） 活動所填寫之個人資料（包括：姓名、性別、電子郵件、任職單位、職稱、餐飲需求等）,將由TWNIC進行蒐集、處理及利用。TWNIC僅於處理會議相關參加、通知以及後續TWNIC舉辦相關活動通知之目的範圍內利用您的個人資料前，個人資料將由TWNIC永久保留，惟您得隨時通知TWNIC刪除該等個人資料。TWNIC將依個資法規定保護您的個人資料。

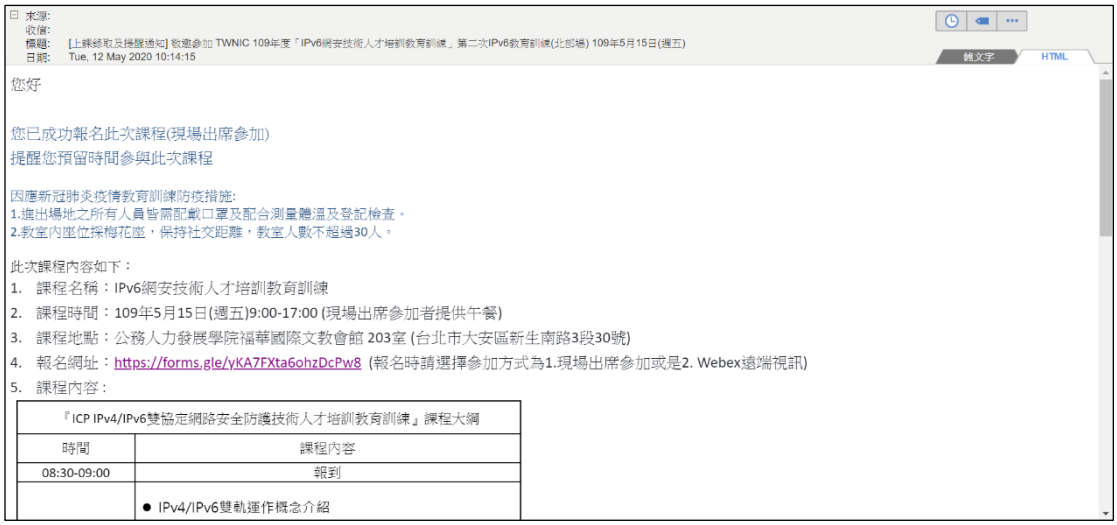
若您同意訂閱TWNIC電子報或其他行銷資訊，您同意TWNIC得對您發送電子報或其他TWNIC活動訊息，您得隨時以電子報上所載之方式取消訂閱。

您依個資法第3條規定得查詢或請求閱覽、製給複製本、補充或更正、停止蒐集、處理、利用或刪除，您得以書面寄送前開請求至臺北市羅斯福路二段9號4樓之2 TWNIC個人資料小組，TWNIC將於法定期間內處理您的請求。

時間：109年5月15日(週五)9:00-17:00 (現場出席參加者提供午餐)
提供精緻午餐便當

地點：公務人力發展學院福華國際文教會館 203室 (台北市大安區新生南路3段30號)

圖 125、第二場教育訓練報名資訊網站截圖



來源:
收信:
標題: [上課經取及提醒通知] 歡迎參加 TWNIC 109年度「IPv6網安技術人才培訓教育訓練」第二次IPv6教育訓練(北部場) 109年5月15日(週五)
日期: Tue, 12 May 2020 10:14:15

純文字 HTML

您好

您已成功報名此次課程(現場出席參加)
提醒您預留時間參與此次課程

因應新冠肺炎疫情教育訓練防疫措施:
1.進出場地之所有人員皆需配戴口罩及配合測量體溫及登記檢查。
2.教室內座位採梅花座，保持社交距離，教室人數不超過30人。

此次課程內容如下：
1. 課程名稱：IPv6網安技術人才培訓教育訓練
2. 課程時間：109年5月15日(週五)9:00-17:00 (現場出席參加者提供午餐)
3. 課程地點：公務人力發展學院福華國際文教會館 203室 (台北市大安區新生南路3段30號)
4. 報名網址：https://forms.gle/yKA7FXta6ohzDcPw8 (報名時請選擇參加方式為1.現場出席參加或是2. Webex遠端視訊)
5. 課程內容：

| 『ICP IPv4/IPv6雙協定網路安全防護技術人才培訓教育訓練』課程大綱 | |
|---|---|
| 時間 | 課程內容 |
| 08:30-09:00 | 報到 |
| | ● IPv4/IPv6雙軌運作概念介紹 |

圖 126、第二場教育訓練學員上課通知 Email 截圖

第二場教育訓練課程於民國 109 年 5 月 15 日舉行，會場地點為公務人力發展學院福華國際文教會館 203 教室，由中華電信研究院曾家偉博士擔任講師。

此次課程參與人數為現場 12 人及遠端視訊 11 人，合計共 23 人參與，回收 20 份問卷，有關教育訓練課程活動資訊來源及滿意度調查，問卷回收率約為 87%，本次教育訓練課程活動整體問卷分數為 4.49 分，高於品質目標分數 3.8。關於學員對問卷內容回覆詳細的統計結果請參考下列圖示。

●問題一：詢問學員獲得活動或課程訊息的來源。

根據問卷回覆統計結果，學員主要〝從 Email 上得知〞獲得課程訊息為主，其次為〝從 TWNIC 相關網站上得知〞，兩項合計超過 85%的比例。

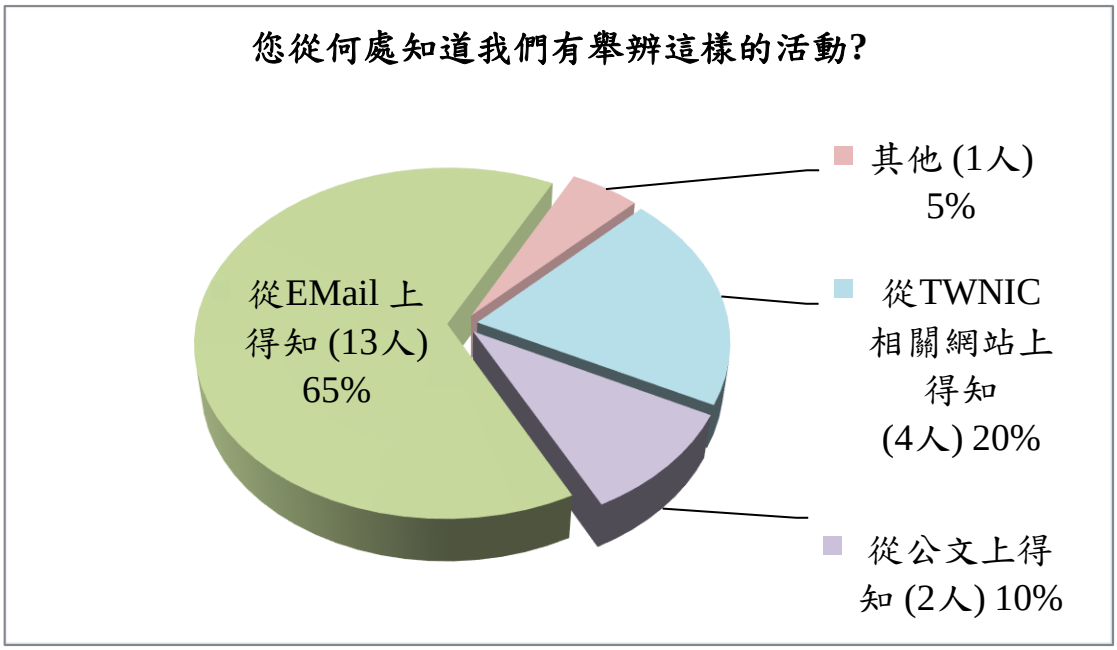



圖 127、5/15 台北 ICP IPv4/IPv6 教育訓練活動資訊來源調查

●問題二~七：詢問學員對活動或課程內容滿意度調查。

調查項目包含對講師教學、教材內容、場地及設備等，進行學員對課程整體滿意度表現評比。下圖為此次課程滿意度統計圖表。根據問卷統計資料顯示，各分項都有獲得 50%以上學員勾選〝非常滿意〞。

學員對於本次課程關於講師上課內容有 95%學員回覆為〝非常滿意〞或〝滿意〞；針對〝教材內容難易度是否恰當?〞有 75%學員回覆為〝非常滿意〞或〝滿意〞；對於〝教學設備是否足夠?〞及〝場地是否完善?〞部分，勾選〝非常滿意〞或〝滿意〞也達到 90%。

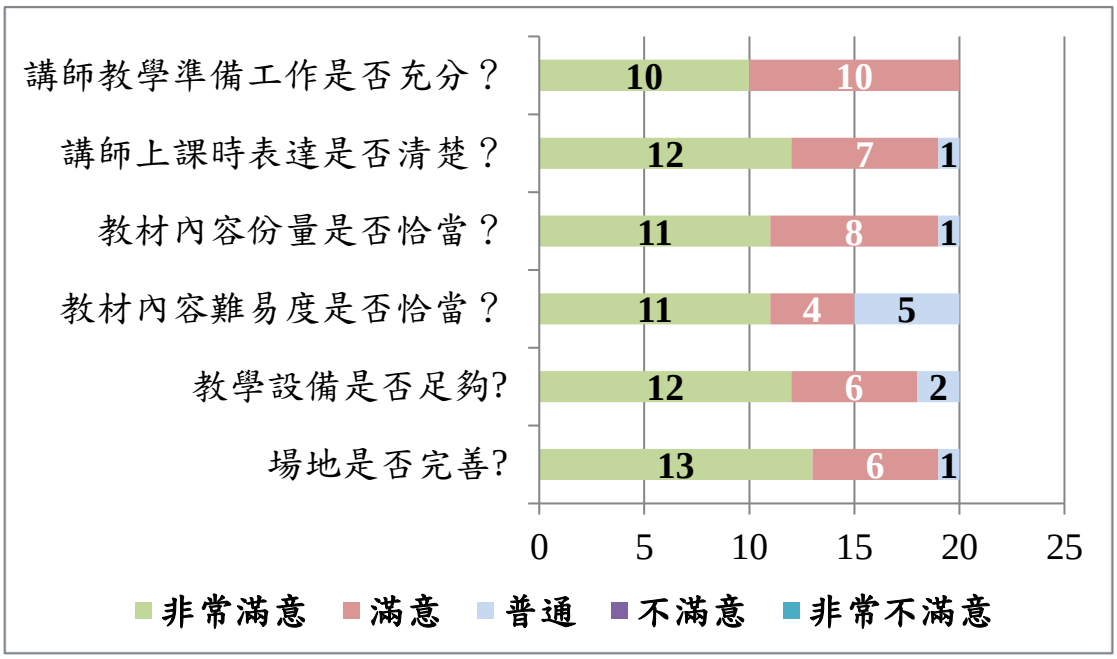



圖 128、5/15 台北 ICP IPv4/IPv6 教育訓練滿意度統計

本次教育訓練會場，及學員上課情形照片如下圖所示：

圖 129、5/15 台北 ICP IPv4/IPv6 教育訓練會場

學員若透過遠端參與教育訓練課程，是以 Cisco Webex Meetings 參與，以下為遠端課程教材及參與學員截圖畫面：

圖 130、5/15 台北 ICP IPv4/IPv6 教育訓練線上課程截圖

## 第三節　第三場教育訓練課程

第三場教育訓練課程於 6 月份舉行，遵循政府防疫措施，於教育訓練課程報名網站及學員上課通知 Email 加強防疫宣導，所有課程參與人員須配合相關措施，並對參與人數進行管控，報名網站公告防疫措施以下所述：

- 進出場地之所有人員皆需配戴口罩及配合測量體溫及登記檢查。
- 教室內座位採梅花座，保持社交距離，教室人數不超過 30 人。

下圖為 6 月 23 日所舉辦第三場教育訓練報名資訊網站截圖：

圖 131、第三場教育訓練報名資訊網站截圖

第三場教育訓練課程於民國 109 年 6 月 23 日舉行，會場地點為國立高雄科技大學管理學院電腦教室，由高雄科技大學鄭進興副教授擔任講師。

此次課程參與人數為現場 16 人及遠端視訊 12 人，合計共 28 人參與，回收 20 份問卷，有關教育訓練課程活動資訊來源及滿意度調查，問卷回收率約為 67%，本次教育訓練課程活動整體問卷分數為 4.36 分，高於品質目標分數 3.8。關於學員對問卷內容回覆詳細的統計結果請參考下列圖示。

●問題一：詢問學員獲得活動或課程訊息的來源。

根據問卷回覆統計結果，學員主要〝從 Email 上得知〞獲得課程訊息為主，其次為〝從 TWNIC 相關網站上得知〞，兩項合計達 90% 的比例。

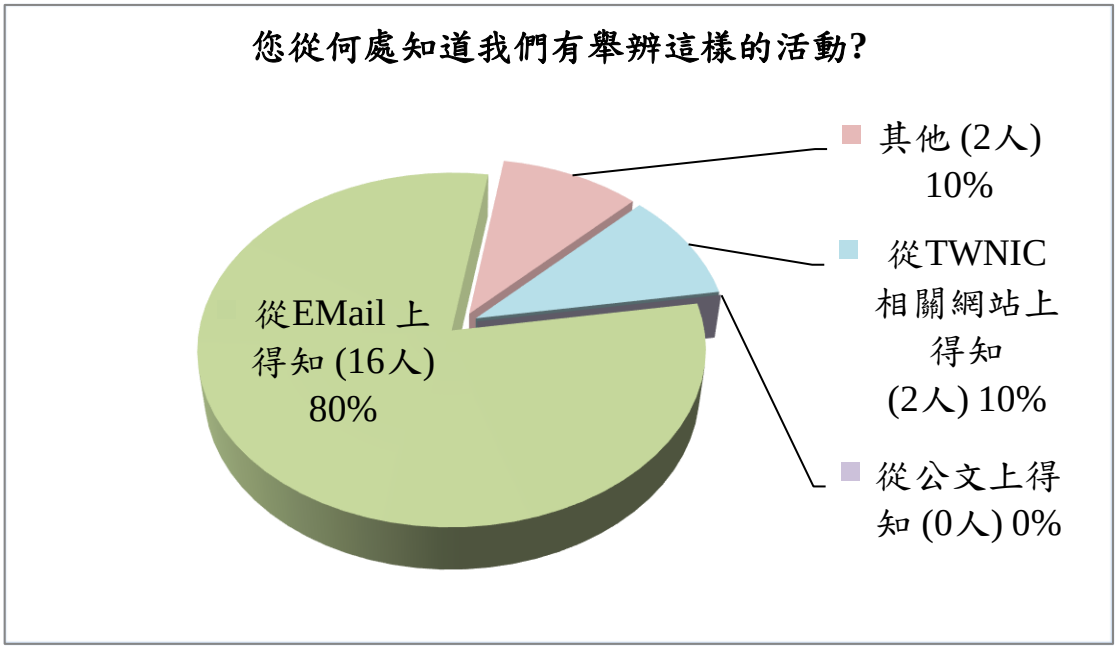



圖 132、6/23 高雄 ICP IPv4/IPv6 教育訓練活動資訊來源調查

●問題二~七：詢問學員對活動或課程內容滿意度調查。

調查項目包含對講師教學、教材內容、場地及設備等，進行學員對課程整體滿意度表現評比。下圖為此次課程滿意度統計圖表。根據問卷統計資料顯示，各分項達〝非常滿意〞及〝滿意〞回覆，合計都有達 90%以上。

學員對於本次課程關於講師準備度及內容表達有 95%學員回覆為〝非常滿意〞或〝滿意〞；針對教材內容、場地及設備等，都有 90%學員回覆為〝非常滿意〞或〝滿意〞。整體課程表現均達到品質目標要求。

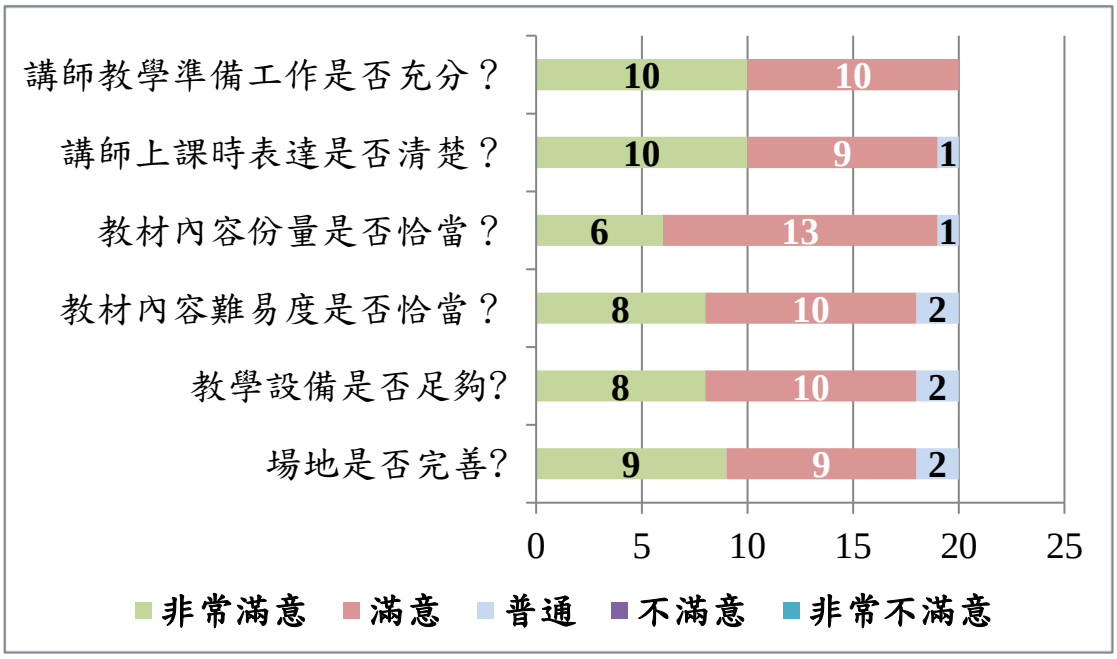



圖 133、6/23 高雄 ICP IPv4/IPv6 教育訓練滿意度統計

本次教育訓練會場，及學員上課情形照片如下圖所示：

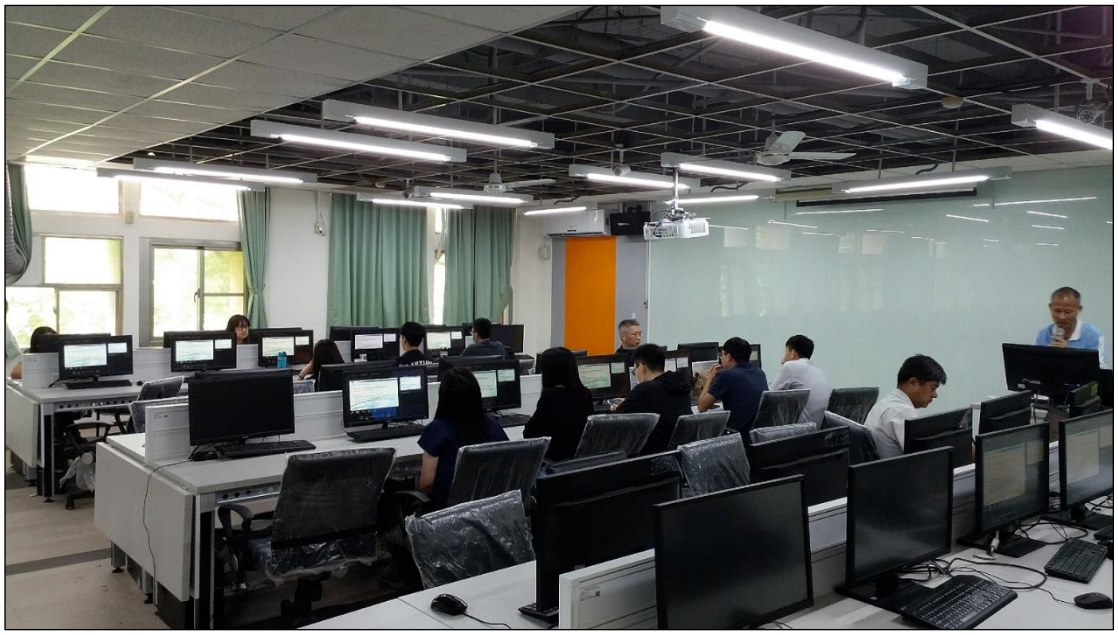


圖 134、6/23 高雄 ICP IPv4/IPv6 教育訓練會場

學員若透過遠端參與教育訓練課程，是以 Cisco Webex Meetings 參與，以下為遠端課程教材及參與學員截圖畫面：

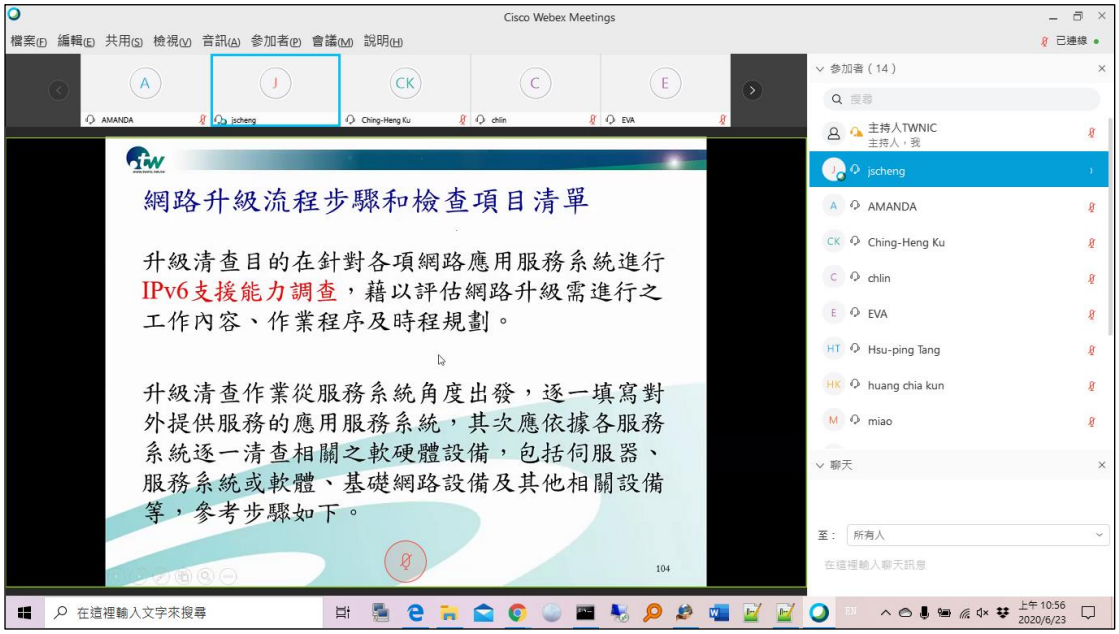



圖 135、6/23 高雄 ICP IPv4/IPv6 教育訓練線上課程截圖

# 第四節　第四場教育訓練課程

第四場教育訓練課程 7 月中旬於雲林舉行，此次教育訓練課程同時提供現場教學及遠距線上課程供學員選擇，下圖為本場次教育訓練 E-mail 推廣招生資訊截圖：

來源:
標題: 歡邀參加 TWNIC 109年度「IPv6網安技術人才培訓教育訓練」第四次IPv6教育訓練(中部場-今年中部最後一場) 109年7月17日(週五)
日期: Fri, 10 Jul 2020 10:01:52
純文字 HTML

您好,
目前全球IPv6平均使用率已超過30%，請參閱https://www.google.com/intl/en/ipv6/statistics.html
台灣也已超過40%, 請參閱https://ipv6now.twnic.net.tw
為協助國內之網站升級IPv6及網路維運相關人員了解與實作IPv4/IPv6雙協定並行，並提供IPv6相關技術受訓之機會，TWNIC今年再次舉辦IPv6教育訓練，今年本系列教育訓練課程全部免費。
此次課程內容如下：
1. 課程名稱：IPv6網安技術人才培訓教育訓練
2. 課程時間：109年7月17日(週五)9:00-17:00 (現場出席參加者提供午餐) (中部場-今年中部最後一場)
3. 課程地點：國立虎尾科技大學(第二校區)電機館 4F 智慧電子應用實驗室-電腦教室 (雲林縣虎尾鎮文化路64號)
4. 報名網址：https://training.twnic.net.tw/ipv6_109/ (報名時請選擇參加方式為1.現場出席參加或是2. Webex遠端視訊)
5. 課程內容：

| 『ICP IPv4/IPv6雙協定網路安全防護技術人才培訓教育訓練』課程大綱 | |
|---|---|
| 時間 | 課程內容 |
| 08:30-09:00 | 報到 |
| | |

圖 136、第四場教育訓練 E-mail 推廣招生資訊截圖

本次教育訓練課程於民國 109 年 7 月 17 日舉行，會場地點為國立虎尾科技大學電機館電腦教室，由虎尾科技大學蘇暉凱副教授擔任講師。

此次課程參與人數為現場 13 人及遠端視訊 20 人，合計共 33 人參與，回收 22 份問卷，有關教育訓練課程活動資訊來源及滿意度調查，問卷回收率約為 67%，本次教育訓練課程活動整體問卷分數為 4.3 分，高於品質目標分數 3.8。關於學員對問卷內容回覆詳細的統計結果請參考下列圖示。

●問題一：詢問學員獲得活動或課程訊息的來源。

根據問卷回覆統計結果，學員主要〝從 Email 上得知〞獲得課程訊息為主，其次為〝從 TWNIC 相關網站上得知〞，兩項合計達 90%以上的比例。

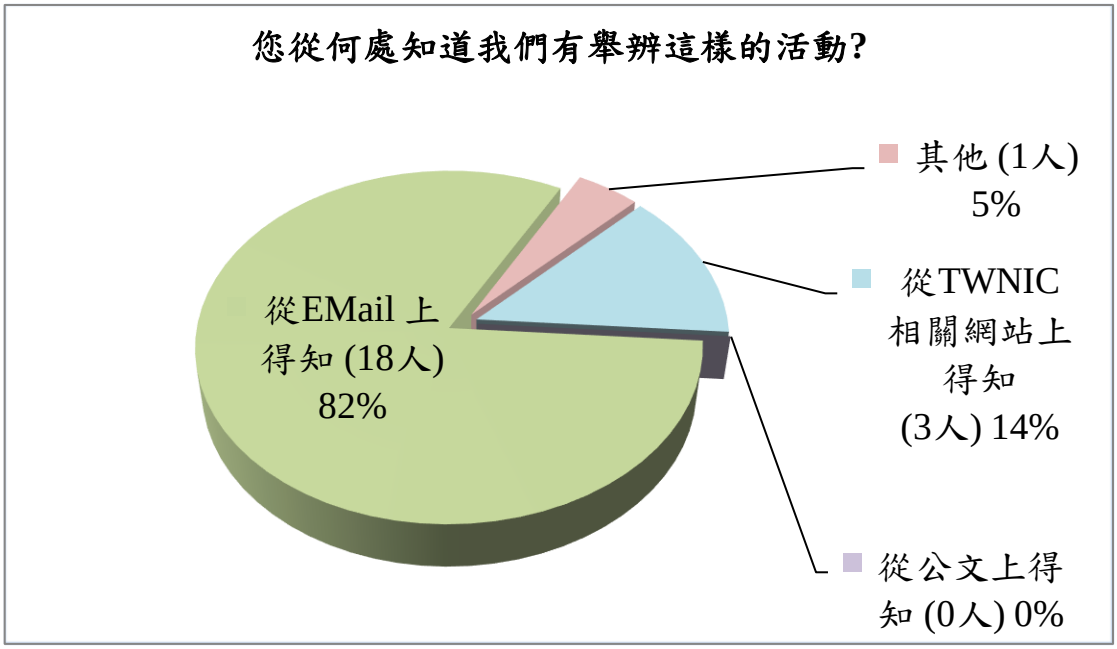



圖 137、7/17 雲林 ICP IPv4/IPv6 教育訓練活動資訊來源調查

●問題二~七：詢問學員對活動或課程內容滿意度調查。

調查項目包含對講師教學、教材內容、場地及設備等，進行學員對課程整體滿意度表現評比。下圖為此次課程滿意度統計圖表。根據問卷統計資料顯示，各分項達〝非常滿意〞及〝滿意〞回覆，合計都有達 95%以上。整體課程表現均達到品質目標要求。

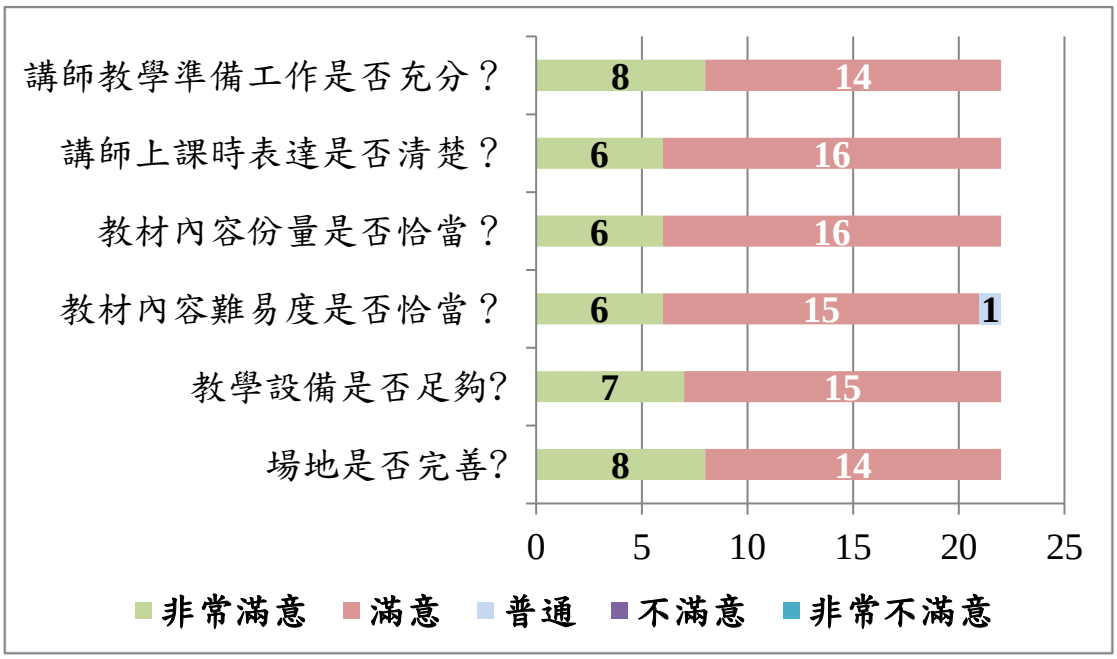



圖 138、7/17 雲林 ICP IPv4/IPv6 教育訓練滿意度統計

本次教育訓練會場，及學員上課情形照片如下圖所示：

圖 139、7/17 雲林 ICP IPv4/IPv6 教育訓練會場

學員若透過遠端參與教育訓練課程，是以 Cisco Webex Meetings 參與，以下為遠端課程教材及參與學員截圖畫面：

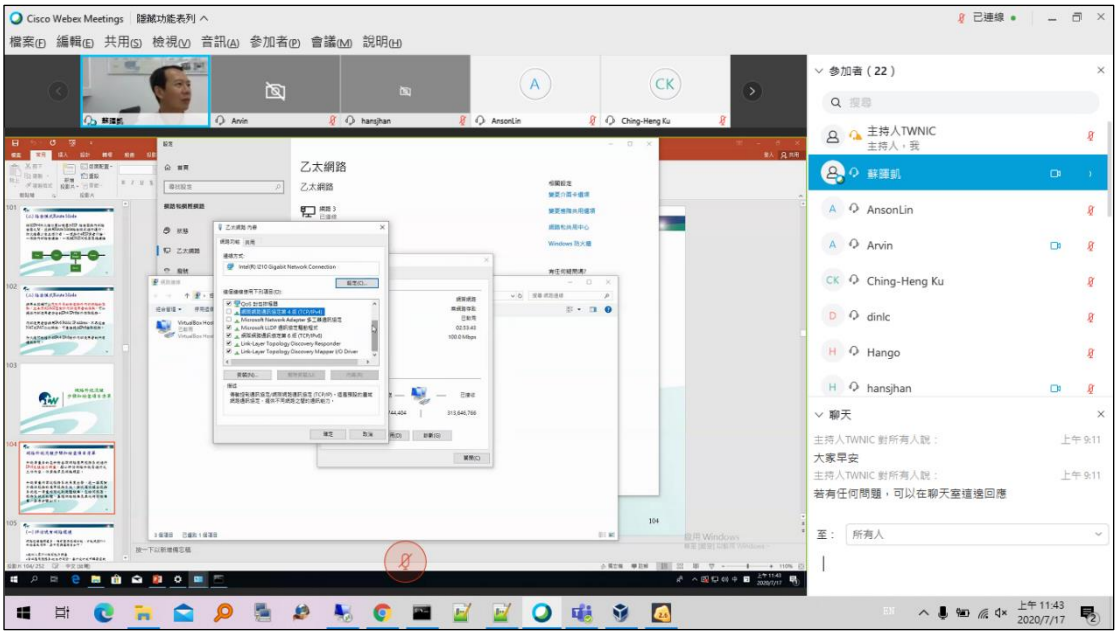



圖 140、7/ 17 雲林 ICP IPv4/IPv6 教育訓練線上課程截圖

# 第五節　第五場教育訓練課程

第五場教育訓練課程 7 月底於台北舉行，此次教育訓練課程同時提供現場教學及遠距線上課程供學員選擇，下圖為本場次教育訓練 E-mail 推廣招生資訊截圖：

您好,
目前全球IPv6平均使用率已超過30%，請參閱https://www.google.com/intl/en/ipv6/statistics.html
台灣也已超過40%, 請參閱https://ipv6now.twnic.net.tw
為協助國內之網站升級IPv6及網路維運相關人員了解與實作IPv4/IPv6雙協定並行，並提供IPv6相關技術受訓之機會，TWNIC今年再次舉辦IPv6教育訓練，今年本系列教育訓練課程全部免費。
此次課程內容如下：

1. 課程名稱：IPv6網安技術人才培訓教育訓練
2. 課程時間：109年7月31日(週五)9:00-17:00 (現場出席參加者提供午餐)
3. 課程地點：公務人力發展學院福華國際文教會館 203室 (台北市大安區新生南路3段30號)
4. 報名網址：https://training.twnic.net.tw/ipv6_109/ (報名時請選擇參加方式為1.現場出席參加或是2. Webex遠端視訊)
5. 課程內容：

| 『ICP IPv4/IPv6雙協定網路安全防護技術人才培訓教育訓練』課程大綱 | |
|---|---|
| 時間 | 課程內容 |
| 08:30-09:00 | 報到 |
| | |

圖 141、第五場教育訓練 E-mail 推廣招生資訊截圖

本次教育訓練課程於民國 109 年 7 月 31 日舉行，會場地點為公務人力發展學院福華國際文教會館，由中華電信曾家偉博士擔任講師。

此次課程參與人數為現場 23 人及遠端視訊 15 人，合計共 38 人參與，回收 28 份問卷，有關教育訓練課程活動資訊來源及滿意度調查，問卷回收率約為 74%，本次教育訓練課程活動整體問卷分數為 4.39 分，高於品質目標分數 3.8。關於學員對問卷內容回覆詳細的統計結果請參考下列圖示。

●問題一：詢問學員獲得活動或課程訊息的來源。

根據問卷回覆統計結果，學員主要〝從 Email 上得知〞獲得課程訊息為主，其次為〝從 TWNIC 相關網站上得知〞，兩項合計約佔 85% 的比例。

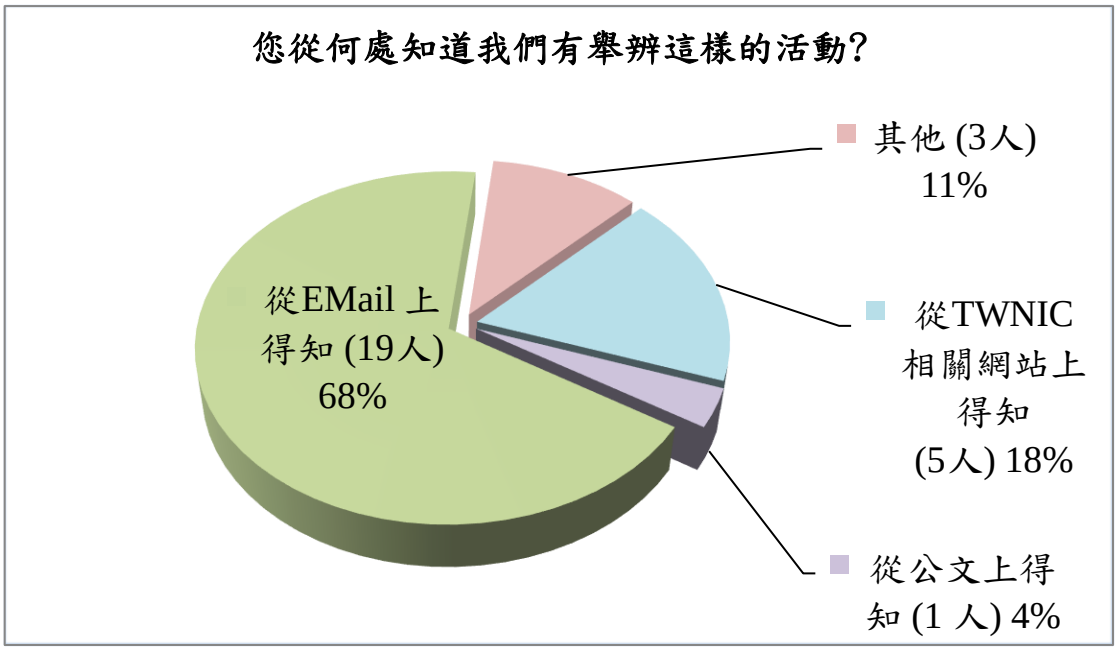



圖 142、7/31 台北 ICP IPv4/IPv6 教育訓練活動資訊來源調查

●問題二~七：詢問學員對活動或課程內容滿意度調查。

調查項目包含對講師教學、教材內容、場地及設備等，進行學員對課程整體滿意度表現評比。下圖為此次課程滿意度統計圖表。根據問卷統計資料顯示，針對講師教學及教材內容部分，學員滿意度達〝非常滿意〞及〝滿意〞，合計達 100%以上。針對場地及教學設備部分，學員滿意度達〝非常滿意〞及〝滿意〞，約達 90%左右。整體課程表現均達到品質目標要求。

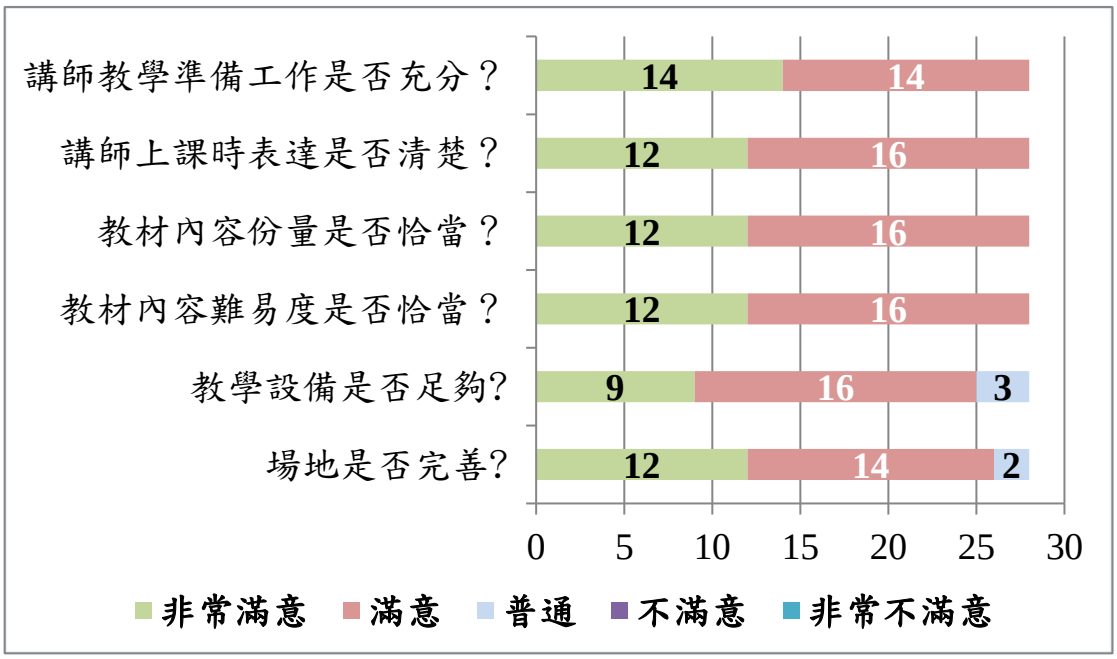



圖 143、7/31 台北 ICP IPv4/IPv6 教育訓練滿意度統計

本次教育訓練會場，及學員上課情形照片如下圖所示：

圖 144、7/31 台北 ICP IPv4/IPv6 教育訓練會場

學員若透過遠端參與教育訓練課程，是以 Cisco Webex Meetings 參與，以下為遠端課程教材及參與學員截圖畫面：

圖 145、7/ 31 台北 ICP IPv4/IPv6 教育訓練線上課程截圖

# 第六節 第六場教育訓練課程

第六場教育訓練課程 8 月底於台南舉行，此次教育訓練課程由〝財團法人國家實驗研究院國家高速網路與計畫中心〞協辦，因國內疫情趨緩，為提升學員現場參與意願，因此本次課程只提供現場教學，下圖為本場次教育訓練網站推廣招生資訊截圖：

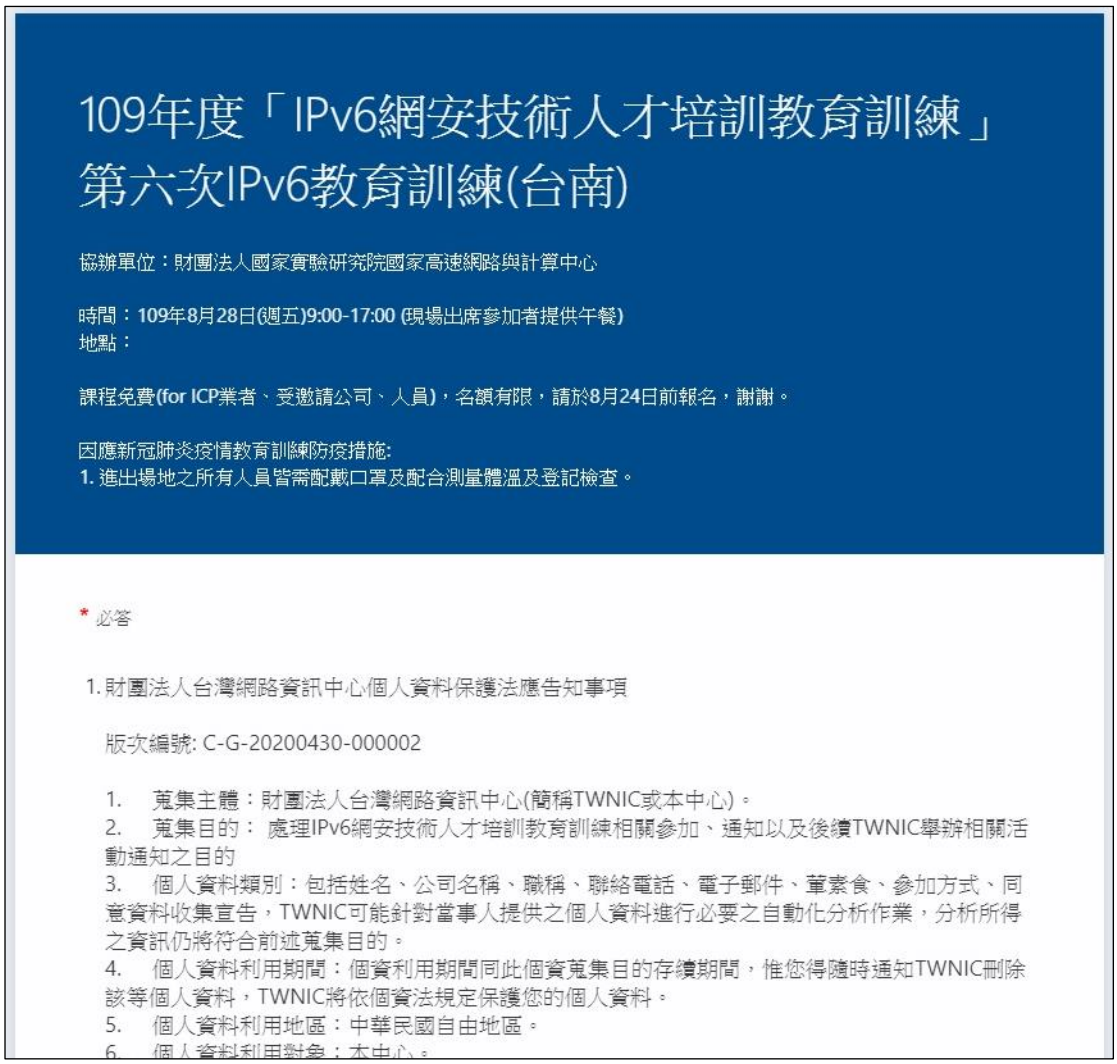



圖 146、第六場教育訓練網站推廣招生資訊截圖

本次教育訓練課程於民國 109 年 8 月 28 日舉行，會場地點為財團法人國家實驗研究院國家高速網路與計算中心，由高雄科技大學鄭進興副教授擔任講師。

此次課程參與人數為現場 36 人參與，回收 26 份問卷，有關教育訓練課程活動資訊來源及滿意度調查，問卷回收率約為 72%，本次教育訓練課程活動整體問卷分數為 4.75 分，高於品質目標分數 3.8。關於學員對問卷內容回覆詳細的統計結果請參考下列圖示。

●問題一：詢問學員獲得活動或課程訊息的來源。

根據問卷回覆統計結果，學員主要〝從 Email 上得知〞獲得課程訊息為主，其次為〝從 TWNIC 相關網站上得知〞，兩項合計超過 95%的比例。

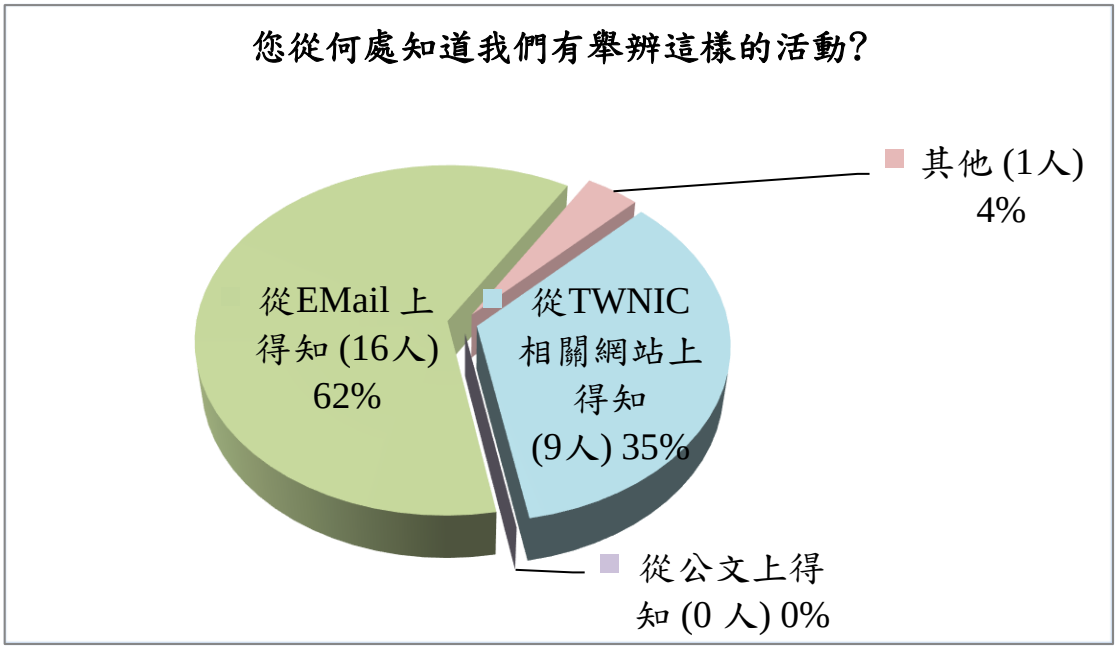



圖 147、8/28 台南 ICP IPv4/IPv6 教育訓練活動資訊來源調查

●問題二~七：詢問學員對活動或課程內容滿意度調查。

調查項目包含對講師教學、教材內容、場地及設備等，進行學員對課程整體滿意度表現評比。下圖為此次課程滿意度統計圖表。根據問卷統計資料顯示，針對講師教學、教材內容、場地及教學設備各部分，學員滿意度都為〝非常滿意〞及〝滿意〞。整體課程表現均達到品質目標要求。

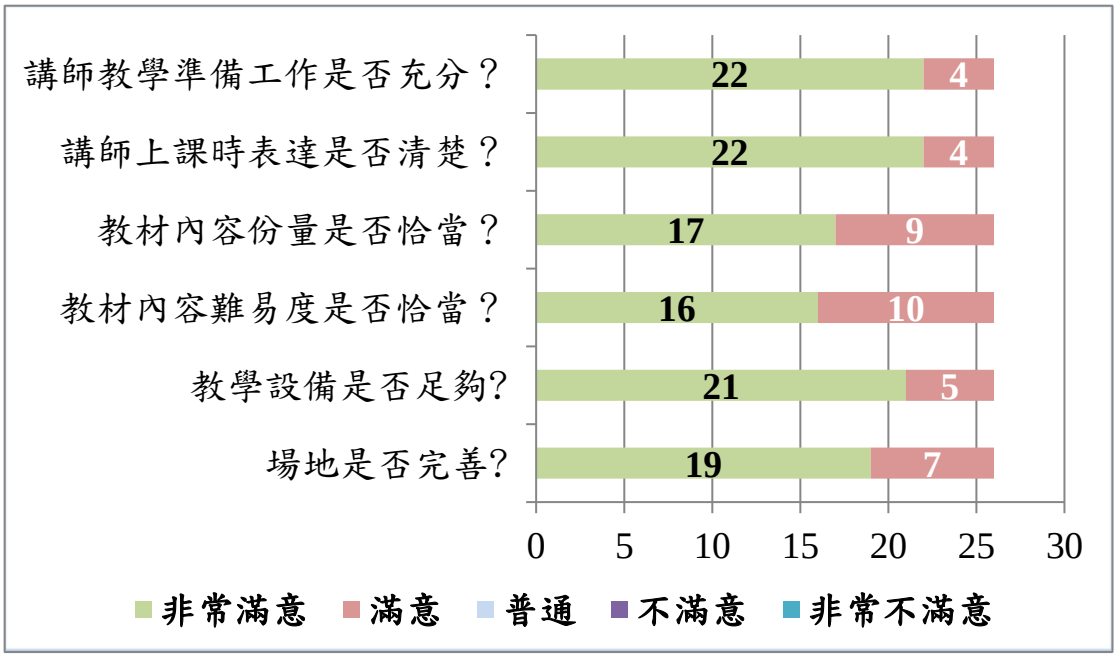



圖 148、8/28 台南 ICP IPv4/IPv6 教育訓練滿意度統計

本次教育訓練會場，及學員上課情形照片如下圖所示：

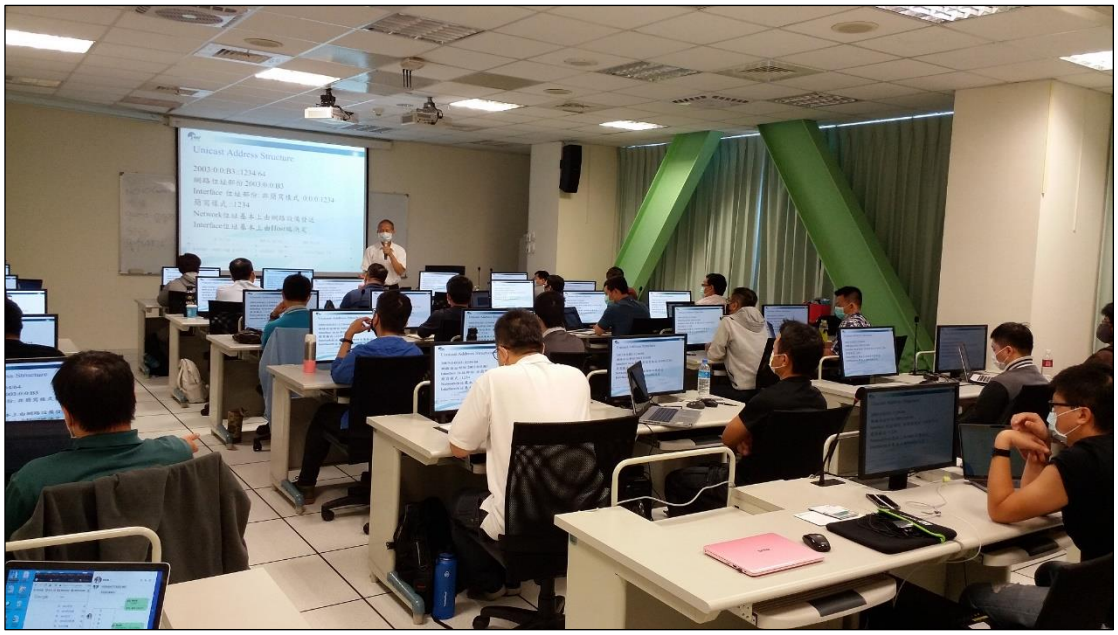
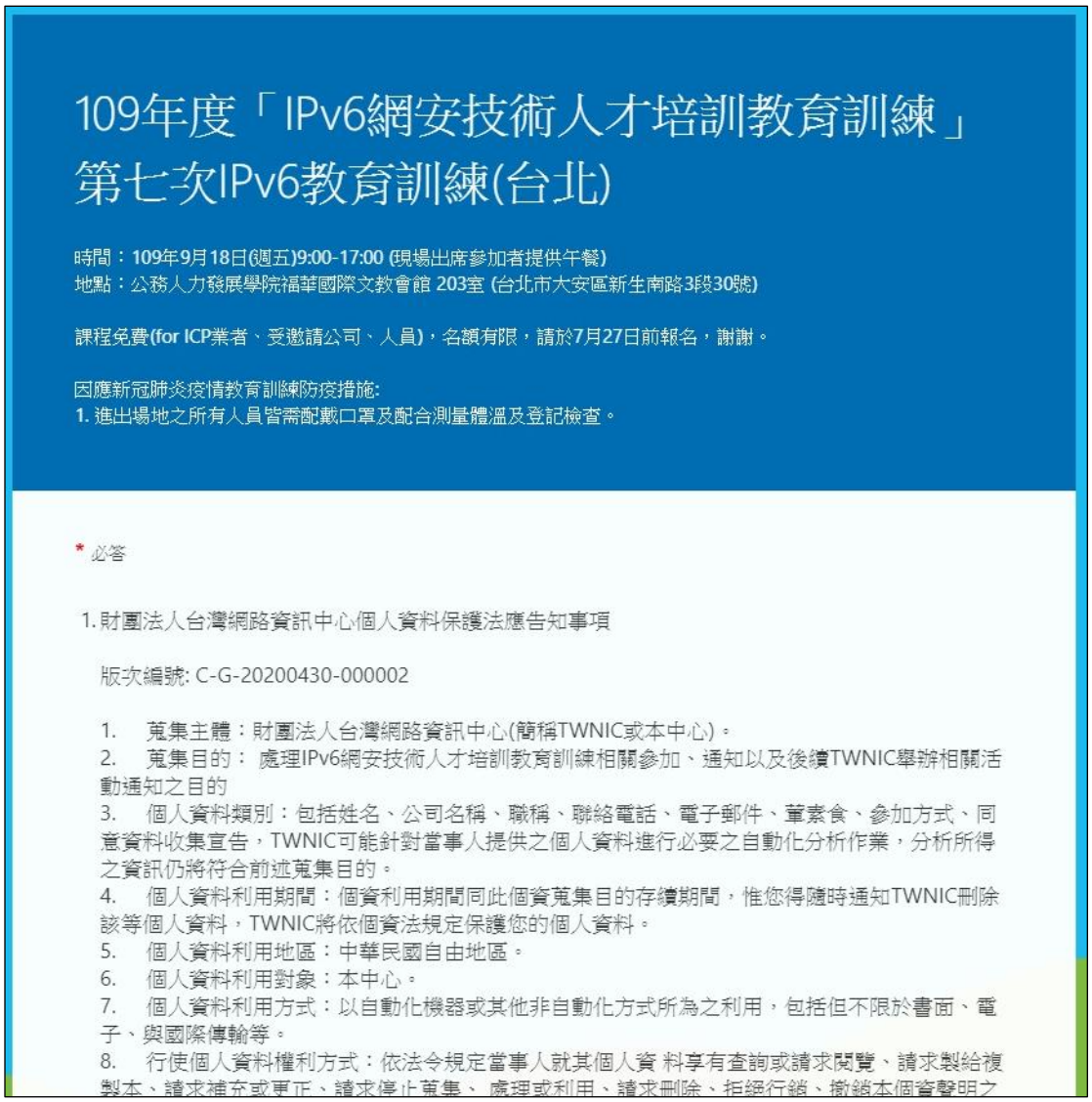



圖 149、8/28 台南 ICP IPv4/IPv6 教育訓練會場

# 第七節　第七場教育訓練課程

第七場教育訓練課程 9 月中於台北舉行，此次教育訓練課程因國內疫情趨緩，為提升學員現場參與意願，因此本次課程只提供現場教學，課程活動現場依然按照衛生福利部疾病管制署規定防疫措施，進行進出人員配戴口罩、測量體溫及登記檢查。下圖為本場次教育訓練網站推廣招生資訊截圖：



109年度「IPv6網安技術人才培訓教育訓練」
第七次IPv6教育訓練(台北)

時間：109年9月18日(週五)9:00-17:00 (現場出席參加者提供午餐)
地點：公務人力發展學院福華國際文教會館 203室 (台北市大安區新生南路3段30號)

課程免費(for ICP業者、受邀請公司、人員)，名額有限，請於7月27日前報名，謝謝。

因應新冠肺炎疫情教育訓練防疫措施:
1. 進出場地之所有人員皆需配戴口罩及配合測量體溫及登記檢查。

* 必答

1. 財團法人台灣網路資訊中心個人資料保護法應告知事項

版次編號: C-G-20200430-000002

1. 蒐集主體：財團法人台灣網路資訊中心(簡稱TWNIC或本中心)。
2. 蒐集目的： 處理IPv6網安技術人才培訓教育訓練相關參加、通知以及後續TWNIC舉辦相關活動通知之目的
3. 個人資料類別：包括姓名、公司名稱、職稱、聯絡電話、電子郵件、葷素食、參加方式、同意資料收集宣告，TWNIC可能針對當事人提供之個人資料進行必要之自動化分析作業，分析所得之資訊仍將符合前述蒐集目的。
4. 個人資料利用期間：個資利用期間同此個資蒐集目的存續期間，惟您得隨時通知TWNIC刪除該等個人資料，TWNIC將依個資法規定保護您的個人資料。
5. 個人資料利用地區：中華民國自由地區。
6. 個人資料利用對象：本中心。
7. 個人資料利用方式：以自動化機器或其他非自動化方式所為之利用，包括但不限於書面、電子、與國際傳輸等。
8. 行使個人資料權利方式：依法令規定當事人就其個人資 料享有查詢或請求閱覽、請求製給複製本、請求補充或更正、請求停止蒐集、 處理或利用、請求刪除、拒絕行銷、撤銷本個資聲明之

圖 150、第七場教育訓練網站推廣招生資訊截圖

本次教育訓練課程於民國 109 年 9 月 18 日舉行，會場地點為公務人員發展學院福華國際文教會館，由中華電信曾家偉博士擔任講師。

此次課程參與人數為現場 38 人參與，回收 28 份問卷，有關教育訓練課程活動資訊來源及滿意度調查，問卷回收率約為 74%，本次教育訓練課程活動整體問卷分數為 4.5 分，高於品質目標分數 3.8。關於學員對問卷內容回覆詳細的統計結果請參考下列圖示。

●問題一：詢問學員獲得活動或課程訊息的來源。

根據問卷回覆統計結果，學員主要〝從 Email 上得知〞獲得課程訊息為主，其次為〝從 TWNIC 相關網站上得知〞，兩項合計超過 95%的比例。

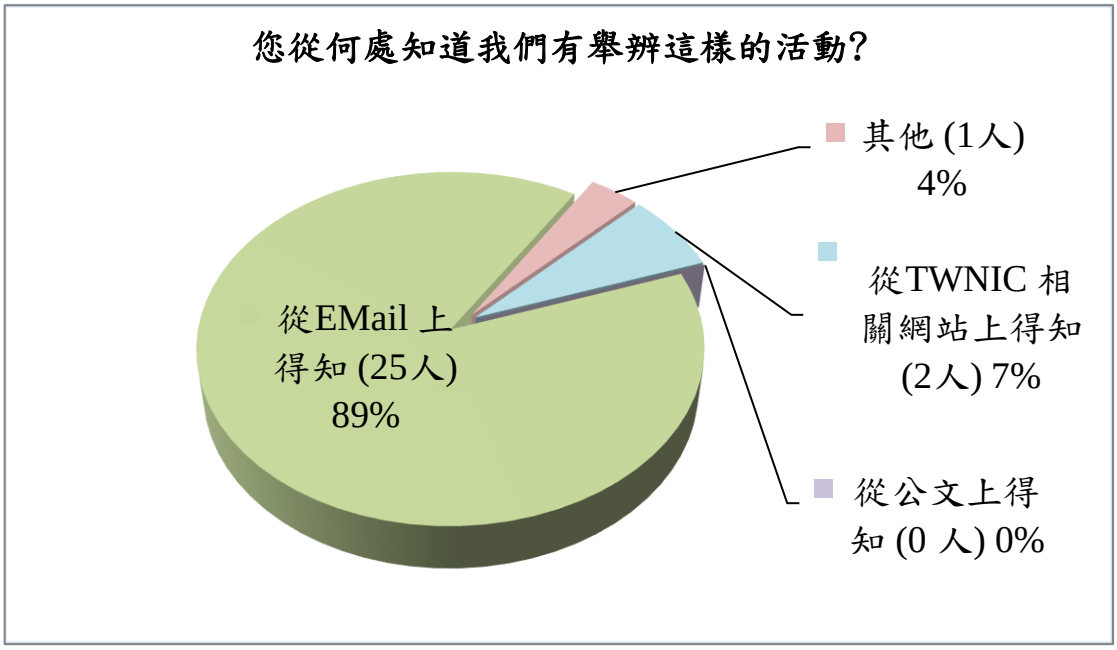



圖 151、9/18 台北 ICP IPv4/IPv6 教育訓練活動資訊來源調查

●問題二~七：詢問學員對活動或課程內容滿意度調查。

調查項目包含對講師教學、教材內容、場地及設備等，進行學員對課程整體滿意度表現評比。下圖為此次課程滿意度統計圖表。根據

問卷統計資料顯示，針對講師教學、教材內容、場地及教學設備各部分，學員滿意度在〝非常滿意〞及〝滿意〞總和都有將近 9 成左右。整體課程表現均達到品質目標要求。

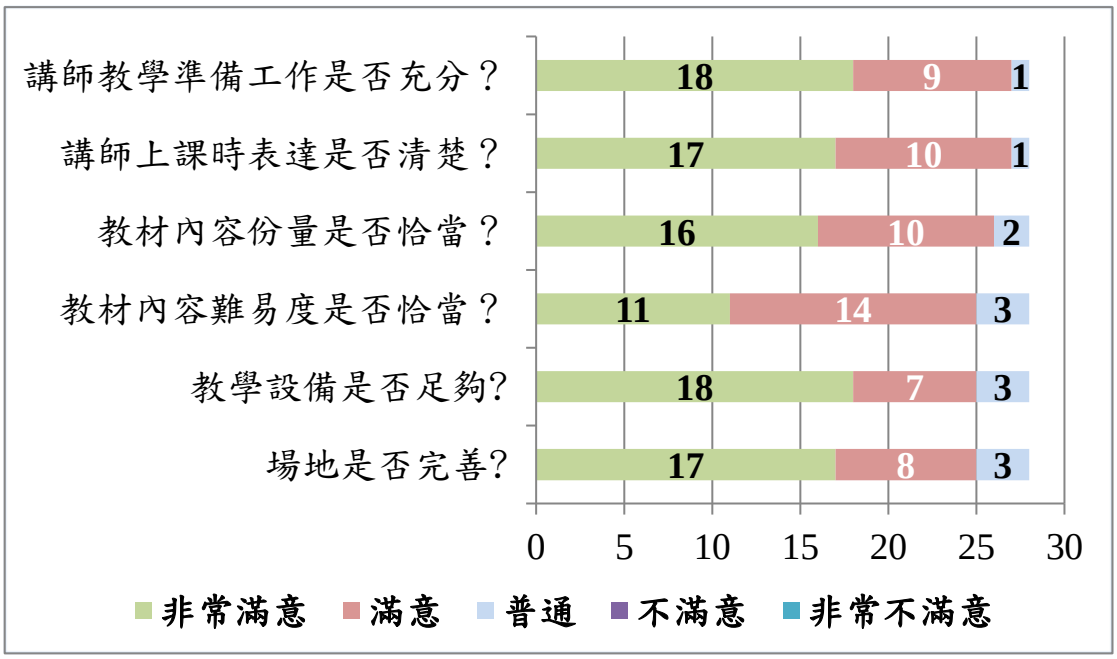



圖 152、9/18 台北 ICP IPv4/IPv6 教育訓練滿意度統計

本次教育訓練會場，及學員上課情形照片如下圖所示：

圖 153、9/18 台北 ICP IPv4/IPv6 教育訓練會場

# 第八節　第八場教育訓練課程

第八場教育訓練課程 9 月底於高雄舉行，此次教育訓練課程因國內疫情趨緩，為提升學員現場參與意願，因此本次課程只提供現場教學，課程活動現場依然按照衛生福利部疾病管制署規定防疫措施，進行進出人員配戴口罩、測量體溫及登記檢查。下圖為本場次教育訓練網站推廣招生資訊截圖：

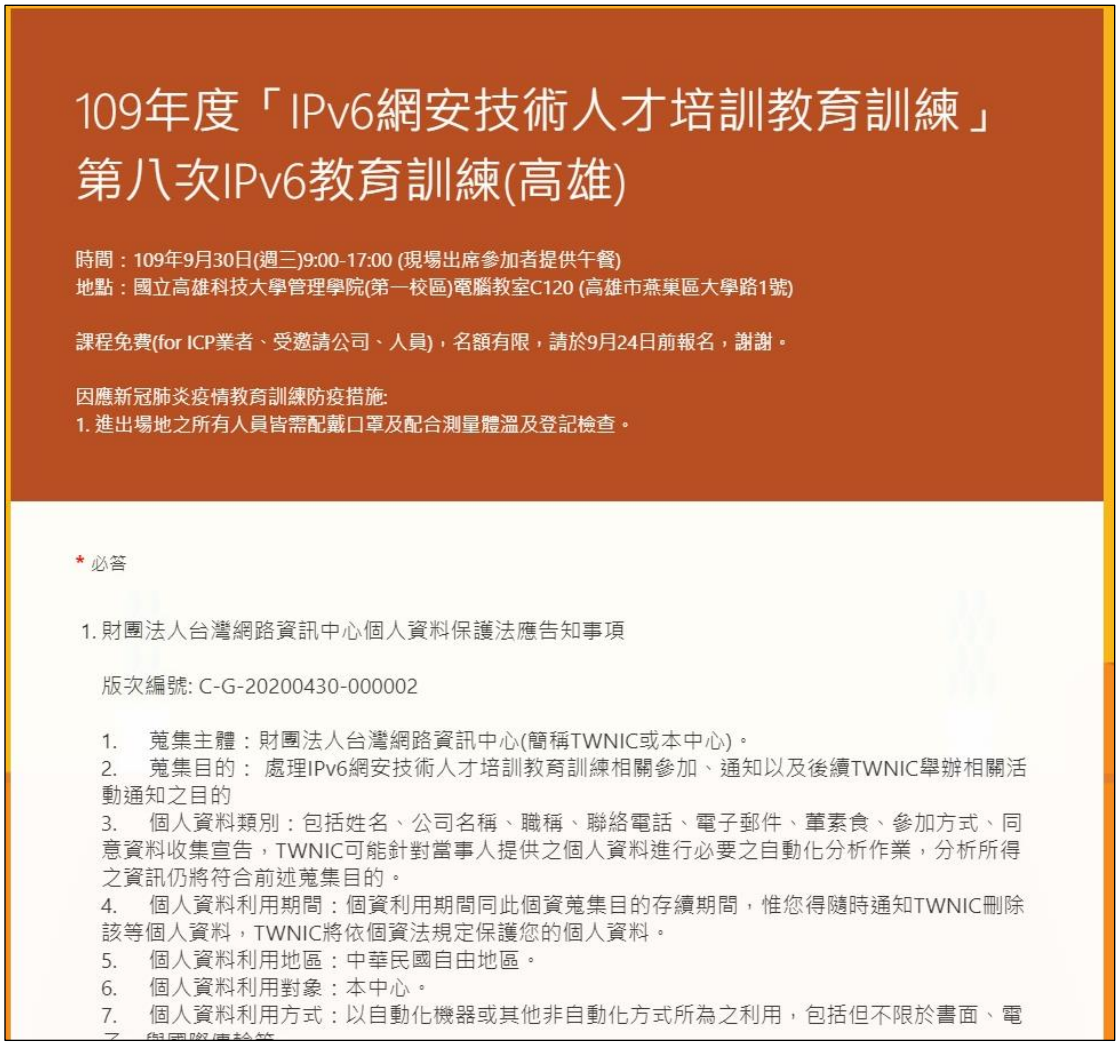



圖 154、第八場教育訓練網站推廣招生資訊截圖

本次教育訓練課程於民國 109 年 9 月 30 日舉行，會場地點為國立高雄科技大學管理學院電腦教室，由國立高雄科技大學鄭進興副教授擔任講師。

此次課程參與人數為現場 41 人參與，回收 31 份問卷，有關教育訓練課程活動資訊來源及滿意度調查，問卷回收率約為 76%，本次教育訓練課程活動整體問卷分數為 4.5 分，高於品質目標分數 3.8。關於學員對問卷內容回覆詳細的統計結果請參考下列圖示。

●問題一：詢問學員獲得活動或課程訊息的來源。

根據問卷回覆統計結果，學員主要〝從 Email 上得知〞獲得課程訊息為主，其次為〝從 TWNIC 相關網站上得知〞，兩項合計約 87%的比例，〝從公文上得知〞及〝其他〞獲得此教育訓練課程訊息者，兩項合計約 13%。

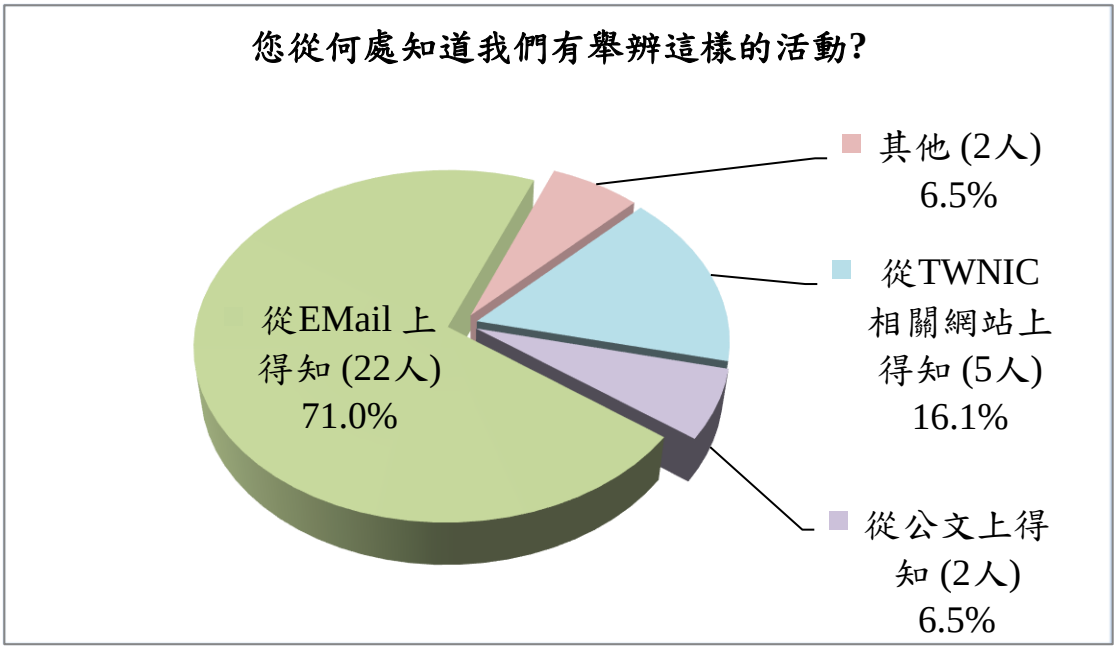



圖 155、9/30 高雄 ICP IPv4/IPv6 教育訓練活動資訊來源調查

●問題二~七：詢問學員對活動或課程內容滿意度調查。

調查項目包含對講師教學、教材內容、場地及設備等，進行學員對課程整體滿意度表現評比。下圖為此次課程滿意度統計圖表。根據問卷統計資料顯示，針對講師教學、教材內容、場地及教學設備各部分，學員滿意度都為〝非常滿意〞及〝滿意〞。整體課程表現均符合品質目標要求。

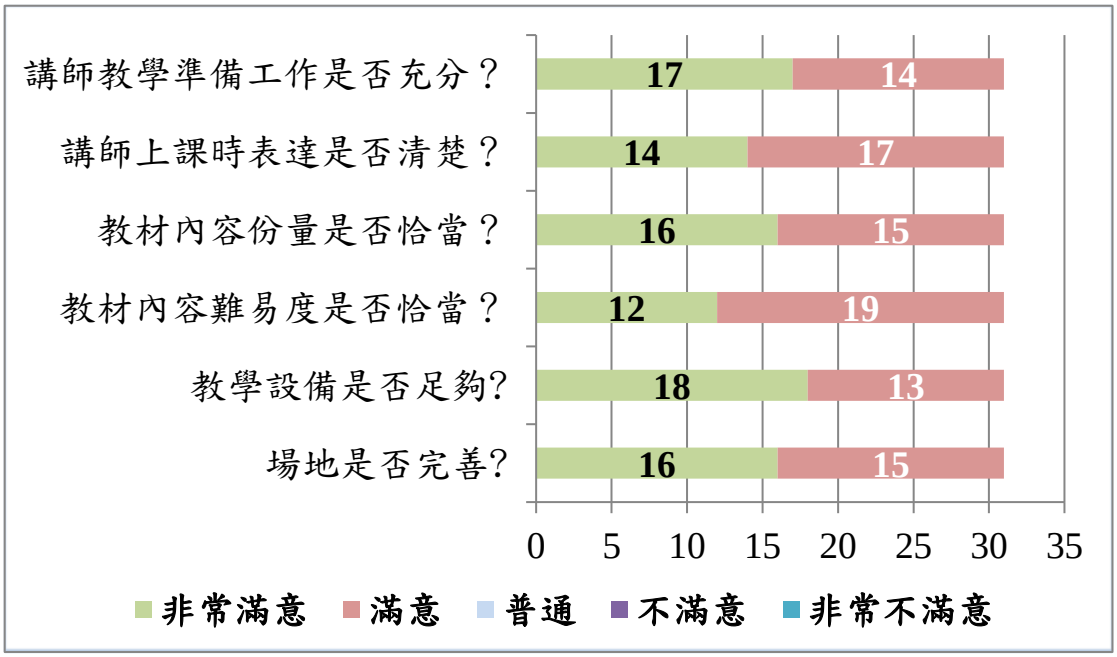



圖 156、9/30 高雄 ICP IPv4/IPv6 教育訓練滿意度統計

本次教育訓練會場，及學員上課情形照片如下圖所示：

圖 157、9/30 高雄 ICP IPv4/IPv6 教育訓練會場

今 (109) 年於北、中、南部合計舉辦 8 場 ICP IPv4/IPv6 教育訓練課程，現場參與人數合計共191 人，線上參與人數合計共 82 人，合計總參與人數共 273 人；問卷共回收 197 份，問卷平均分數約為 4.46；各場次參與統計資訊如下表列：

表 81、109 年 ICP IPv4/IPv6 教育訓練課程參與人數及問卷統計

| 序號 | 地點 | 時間 | 現場參與人數 | 線上參與人數 | 合計參與人數 | 問卷數量 | 問卷分數 |
|---|---|---|---|---|---|---|---|
| **1** | 雲林 | 4/29 | 12 | 24 | 36 | 22 | 4.42 |
| **2** | 台北 | 5/15 | 12 | 11 | 23 | 20 | 4.49 |
| **3** | 高雄 | 6/23 | 16 | 12 | 28 | 20 | 4.36 |
| **4** | 雲林 | 7/17 | 13 | 20 | 33 | 22 | 4.30 |
| **5** | 台北 | 7/31 | 23 | 15 | 38 | 28 | 4.39 |
| **6** | 台南 | 8/28 | 36 | X | 36 | 26 | 4.75 |
| **7** | 台北 | 9/18 | 38 | X | 38 | 28 | 4.5 |
| **8** | 高雄 | 9/30 | 41 | X | 41 | 31 | 4.5 |
| **總計** | | | **191** | **82** | **273** | **197** | |

# 第九章 蒐集並整理 ISP 之 IPv6 網路安全防護準則

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

## 第一節研析 ISP IPv6 網路安全基本防護要項

一般網際網路服務提供者 (Internet Service Provider，ISP) 服務架構如下圖所示：

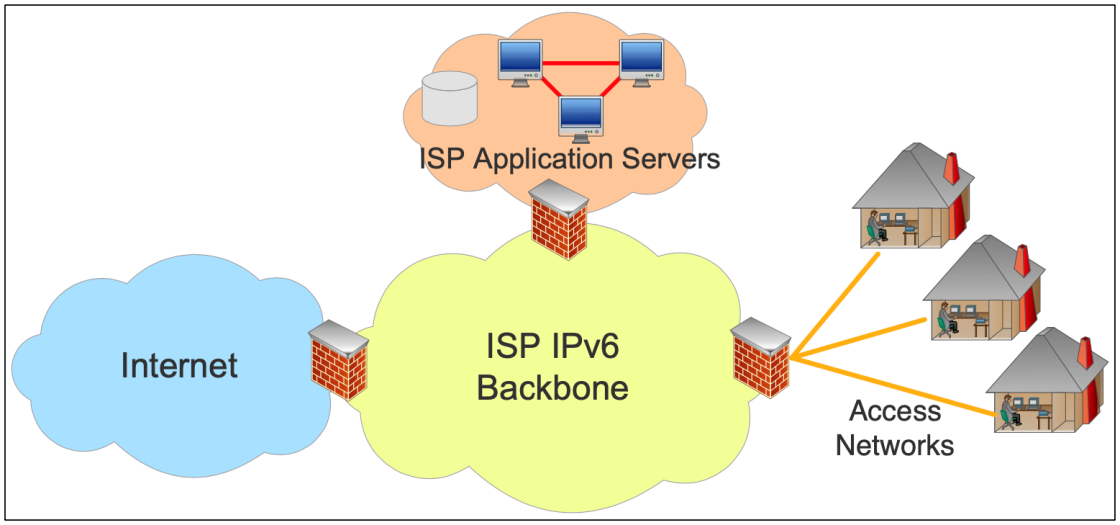



圖 158、ISP 服務架構示意圖

根據上圖 ISP 服務架構圖，可以將 ISP 的服務分為 3 大類別，包含：

- 網際網路互連 (Internet Interworking)：用以實現不同網路可以相互連結。
- 網際網路存取服務 (Internet Access Service)：俗稱上網或連網，讓用戶以各式設備如個人電腦、攜帶式電腦、行動裝置等，透過各種連結技術，連結到網際網路 (Internet) 上，以提供使用者能夠使用網際網路上提供的各種服務。
- 網際網路應用服務 (Internet Service)：網際網路應用服務是由 ISP 提供用戶使用網際網路相關之應用服務，例如：DNS、Web…等。

依照上述 ISP 服務分網際網路互連、網際網路存取服務、網際網路應用服務 3 大類別，下表列出在 IETF 所提列與 ISP IPv6 網路安全防護之相關文獻，如下表所示：

表 82、ISP IPv6 網路安全防護相關文獻

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

以下將依照上述 3 大類別個別探討，在 IETF 所提列與 ISP IPv6 網路安全防護之相關文獻內容。

# 一. 網際網路互連

網際網路互連探討的議題包含 IPv6 定址安全考量、鏈結層安全考量、路由安全考量、紀錄與監視等共 4 個項目，以下將分別就各項進行簡介。

## (一) IPv6 定址安全考量

IPv6 定址安全考量將分位址架構及延伸標頭 2 部分進行探討。

### 1. 位址架構

IPv6 位址分配和整體結構是 IPv6 安全性相當重要部分。設計上可以使用臨時 IPv6 位址增加使用者的私密性。雖然 IPv6 位址可以簡單地重新編號，但如果沒有適當的 IP 位址管理系統 (IP Address Management，IPAM)，則重新編號可能會非常困難。

要成功部署 IPv6 的關鍵任務就需要準備好一個定址規劃策略；由於 IPv6 擁有足夠可用位址空間，可以考慮依服務和地理位置等特性進行 IPv6 位址規劃，將可使位址空間成為更結構化安全策略的基礎，以做為允許或拒絕地理區域之間的服務判斷基本原則。關於 IPv6 定址規劃，主要參考 IETF 之 RFC 文獻如下表所示：

表 83、IPv6 定址規劃參考文獻

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

在[RFC 7381]定義一個常見問題，公司是否應該使用提供商獨立 (Provider Independent，PI) 空間與提供商分配 (Provider Allocated，PA) 空間，從安全角度來看，兩者之間幾乎沒有區別。然而，需要關注的是誰擁有 IPv6 位址空間的管理所有權，以及如果當需要進行 IPv6 位址空間路由強制限制，誰具有技術上責任，例如：源自特定位址空間的惡意犯罪活動，誰該進行強制限制。

在[RFC 7934]中建議 IPv6 網路部署從每個 Prefix 提供多個 IPv6 位址給一般主機，且不建議限制主機對每個 Prefix 僅提供一個 IPv6 位址。同時也建議網路讓主機具有使用新 IPv6 位址能力，而不需要透過明確請求 (例如：使用 SLAAC)。和 IPv4 每個介面設定唯一 IP 位址相比，IPv6 讓每個介面具有多個 IP 位址是一個重大變化。

(1) 使用單一區域位址 (Unique Local Address，ULA)

單一區域位址適用於網路介面不需要連結到網際網路使用情境，例如使用於內部網路連線。參考文獻如下表所列：

表 84、單一區域位址 ULA 參考文獻

| 編號 | RFC 編號 | RFC 相關訊息 | |
|---|---|---|---|
| | | 類別 | 時間 |
| 1 | 4193 | Standards Track | 2005/10 |
| | | 標題：Unique Local IPv6 Unicast Address | |
| 2 | 4864 | Informational | 2007/05 |
| | | 標題：Local Network Protection for IPv6 | |
| 3 | 1918 | Best Current Practice | 1996/02 |
| | | 標題：Address Allocation for Private Internets | |

IPv6 單一區域位址如在[RFC 4193]所描述〝fc00::/8〞與〝fd00::/8〞，其特性類似於 IPv4 私有位址。單一區域位址具有網際網路全域連線範圍，但在[RFC 4193]指定必須在域邊界將其過濾掉。IPv4 私有位址之規範定義在[RFC 1918]，而 IPv6 單一區域位址與 IPv4 私有位址還是不盡相同，在[RFC 4864]中描述 ULA 使用方法及案例，可供參考。

(2) 點對點鏈接 (Point-to-Point Links)

點對點鏈接相關參考文獻如下表所列：

表 85、點對點鏈接參考文獻

| 編號 | RFC 編號 | RFC 相關訊息 | |
|---|---|---|---|
| | | 類別 | 時間 |
| 1 | 6164 | Standards Track | 2011/04 |
| | | 標題：Using 127-Bit IPv6 Prefixed on Inter-Router Links | |
| 2 | 4443 | Standards Track | 2006/03 |
| | | 標題：Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification | |
| 3 | 7404 | Informational | 2014/11 |
| | | 標題：Using Only Link-Local Addressing inside on IPv6 Network | |

在[RFC 6164]文中，指定將/127 用於路由器間點對點鏈接，因為/127 可以用於防止未正確實作在[RFC 4443]所定義 ICMPv6 規格，造成在路由器之間乒乓攻擊，並可以防止對鄰居快取記憶體的 DoS 攻擊。

在部分環境中還可以將區域鏈結位址 (Link-local Address) 使用於點對點鏈接。儘管此種做法可以減少對基礎

設施的攻擊，但操作上也有些缺點需要仔細考慮，詳細請參閱[RFC 7404]文件內容說明。

(3) 回送位址 (Loopback Address)

許多 ISP 會為其基礎架構中的所有 Loopback Address 保留一塊/64 區域，並為每個回送介面 (Loopback Interface) 由此保留/64 Prefix 中分配一個/128。此做法允許簡單地設定存取控制列表 (ACL，Access Control List)，以做為回送位址的安全策略。

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

靜態配置位址相關參考文獻如下表所列：

表 86、靜態配置位址參考文獻

| 編號 | RFC 編號 | RFC 相關訊息 | |
|---|---|---|---|
| | | 類別 | 時間 |
| 1 | 7707 | Informational | 2016/03 |
| | | 標題：Network Reconnaissance in IPv6 Networks | |

在進行分配靜態配置位址時，有必要考慮給定環境中外圍安全的有效性。且須權衡操作簡便性 (可以簡單地識別 IPv6 位址以進行操作調適和故障排除) 與使用於偵察不重要網路掃描風險之間的選擇。[RFC 7707]文件中介紹了科學性的 IP 掃描方法，這些方法用於掃描可連線 IPv6 節點比預期更好。使用已知的 IPv6 位址 (例如所有鏈接區域節點的〝ff02::1〞) 或使用常見的重複位址，可以很容易地確定哪些設備是名稱服務伺服器、路由器或其他關鍵設備。即使是簡單的〝traceroute〞 (用於追蹤顯示封包在 IP 網路經過的

路由器的 IP 位址) 工具，也可以找出路徑上大部分路由器。掃描技術的多樣性，操作人員不應該認為「亂數隨機分配位址就不可能被掃描到」，一般做法將靜態配置位址隨機分佈在/64 子網中，並使用 DNS 進行名稱與位址對應，仍具有安全性風險。

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

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

臨時位址相關參考文獻如下表所列：

表 87、臨時位址參考文獻

| 編號 | RFC 編號 | RFC 相關訊息 | |
|---|---|---|---|
| | | 類別 | 時間 |
| 1 | 8064 | Standards Track | 2017/02 |
| | | 標題：Recommendation on Stable IPv6 Interface Identifiers | |
| 2 | 4941 | Standards Track | 2007/09 |
| | | 標題：Privacy Extensions for Stateless Address Autoconfiguration in IPv6 | |

IPv6 位址配置除保留手動設定固定位址的機制外，另提出的新技術為無狀態位址自動配置 (Stateless Address Autoconfiguration，SLAAC)，是基於 EUI-64 MAC 位址自動生成的 64 位元介面標識碼 (Interface ID，IID)，該標識碼與/64 Prefix 一起構成了網際網路全域唯一的 IPv6 位址；其中

EUI-64 位址是從 48 位元的 MAC 位址生成。[RFC 8064]文中建議不要使用 EUI-64 位址，目前大多數主機作業系統不再使用 EUI-64 位址，而是採用在[RFC 4941]或[RFC 8064]文件中建議的方法。

在[RFC 4941]中描述，隨機生成介面 ID 是 SLAAC 的一部分，具有所謂的隱私延伸位址 (Privacy Extension Addresses)，用於解決使用者上網隱私問題。隱私延伸位址又稱為臨時位址，用於減少同一網路內節點活動相關性，因此可以減少暴露，降低被攻擊之風險。隱私延伸位址可以避免系統管理員建構主機特定的存取控制列表 (Access Control List，ACL)；也可以用於掩蓋部分惡意活動，並且可做為特定的用戶歸屬/責任程序。

[RFC 8064]指定另一種位址生成方式，同時為每個網路 Prefix 保留相同 ID；這使 SLAAC 節點在特定網路上具有相同穩定 IPv6 位址，而在不同網路上具有不同的 IPv6 位址。

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

但對於強烈要求匿名的情況下 (保護用戶隱私比用戶責任更重要)，應使用隱私延伸位址。當[RFC 8064]所定義規則可用時，穩定的隱私位址可能是隱私 (在不同網路之間)和安全/用戶責任 (在網路內) 之間的良好平衡。

(6) DHCP/DNS 注意事項

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

儘管 DNS 的 IPv4 和 IPv6 安全考量沒有不同，但是在 DNS64 環境中需要特別考慮。具體來說，需要了解與 DNSSEC 實施的相互作用和潛在干擾。DNS64 參考文獻如下表所列：

表 88、DNS64 參考文獻

| 編號 | RFC 編號 | RFC 相關訊息 | |
|---|---|---|---|
| | | 類別 | 時間 |
| 1 | 6147 | Standards Track | 2011/04 |
| | | 標題：DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers | |

(7) 每個主機使用/64

按[RFC 8273]文件中關於主機 Unique IPv6 Prefix 的建議，在每個主機上使用/64。由於主機的應用程序可以在/64 內更改其 IPv6 位址，因此其/64 Prefix 可穩定運作，可以簡化用

戶歸屬 (通常為主機 MAC 位址)。Unique IPv6 Prefix 參考文獻如下表所列：

表 89、Unique IPv6 Prefix 參考文獻

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

(8) 位址的隱私考慮

除了 IPv6 位址安全性方面，另隱私方面也需考慮，主要是因為 IPv6 位址具有網際網路全域範圍，且在網際網路全域範圍內可見。[RFC 7721]文件定義透過手動配置的 DHCPv6 或 SLAAC，並詳細介紹 IPv6 位址隱私注意事項。下表提列位址隱私參考文獻：

表 90、位址隱私參考文獻

| 編號 | RFC 編號 | RFC 相關訊息 | |
|---|---|---|---|
| | | 類別 | 時間 |
| 1 | 7721 | Informational | 2016/03 |
| | | 標題：Security and Privacy Considerations for IPv6 Address Generation Mechanisms | |

**2. 延伸標頭**

延伸標頭是 IPv4 和 IPv6 之間的重要區別。在 IPv4 的封包中，查詢上層協議類型和協議標頭很簡單，然而在 IPv6 中，由於必須完全解析延伸標頭，因此更為複雜。IANA 已關閉現有

「Next Header Types」，並根據[RFC 7045]改採用新的「IPv6 Extension Header Types」。

已知丟棄包含延伸標頭封包的轉發節點會導致連接失敗和部署問題，因此在[RFC 7872]以此爭議性主題進行探討。

在[RFC 7045]中可以找到有關中間節點應如何處理具有現有或未來延伸標頭封包的說明，[RFC 6564]中描述了使用於定義未來延伸標頭的統一 TLV 格式。

此外必須注意，若在封包中沒有指示「Next Protocol」欄位指向延伸標頭或指向傳輸層標頭，可能會混淆某些過濾規則。延伸標頭參考文獻如下表所列：

表 91、延伸標頭參考文獻

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

了解可變延伸標頭的作用很重要，以下列舉了需要仔細考慮的延伸標頭。

(1) 延伸標頭的順序和重複

在[RFC 8200]推薦了延伸標頭的順序和最大重複次數，但在 IPv6 實作上，依然可能支援非推薦順序 (例如路由之前的 ESP) 或非法重複 (例如多個路由標題)，延伸標頭中包

含的選項也是如此（在 [I-D.kampanakis-6man-ipv6-eh-parsing] 有詳細說明)。在某些情況下，可能導致節點在接收或轉發格式錯誤的封包時，造成崩潰。因此，應該使用防火牆或邊緣設備來強制執行延伸標頭的建議順序和出現次數。關於延伸標頭的順序和重複次數參考文獻如下表所列：

表 92、延伸標頭的順序和重複次數參考文獻

| 編號 | RFC 編號 | RFC 相關訊息 | |
|---|---|---|---|
| | | 類別 | 時間 |
| 1 | 8200 | Standards Track | 2017/07 |
| | | 標題：Internet Protocol，Version 6 (IPv6) Specification | |
| 2 | draft | Informational | 2014/08 |
| | | 標題：Implementation Guidelines for parsing IPv6 Extension Headers [draft-kampanakis-6man-ipv6-eh-parsing-01] | |

(2) 逐跳選項標頭 (Hop-by-Hop Options Header)

當 IPv6 封包中存在逐跳選項標頭時，逐跳選項標頭會強制路徑中的所有節點，檢查定義於[RFC 2460]原始 IPv6 規範中的此標頭。並不是所有路由器都可以透過硬體處理此類封包，當硬體無法處理此類封包時，該封包將以軟體進行處理，因此大量逐跳選項標頭可能造成服務阻斷 (Denial of Service) 攻擊。目前 IPv6 新標準文獻[RFC 8200]，考慮讓中間路由器可選擇是否對逐跳選項標頭進行處理。關於逐跳選項標頭參考文獻如下表所列：

表 93、逐跳選項標頭參考文獻

| 編號 | RFC 編號 | RFC 相關訊息 | |
|---|---|---|---|
| | | 類別 | 時間 |
| 1 | 8200 | Standards Track | 2017/07 |
| | | 標題：Internet Protocol，Version 6 (IPv6) Specification | |
| 2 | 2460 | Informational | 1998/12 |
| | | 標題：Internet Protocol，Version 6 (IPv6) Specification | |

(3) 分段標頭 (Fragment Header)

當傳送封包過大必須分段時，分段標頭必須在來源端(傳送端) 處理。在[RFC 7112]和[RFC 8200]文件中解釋了其重要性包含：

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

如果設備無法滿足這些要求，則攻擊方可能會繞過無狀態過濾。[RFC 6980]透過強制丟棄分段的 NDP (Neighbor Discovery Protocol，鄰居發現協定) 封包，將更嚴格的規則應用於 NDP。[RFC 7113]文件描述在[RFC 6105]中提及之 RA-guard (Router Advertisement Guard，路由器公告保護) 功能，在分段 RA 封包存在時的處理行為。關於分段標頭參考文獻如下表所列：

表 94、分段標頭參考文獻

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

(4)IP 安全延伸標頭

如果要使用 IPsec 網路級安全功能，就需要使用在[RFC 4301]所描述的 IPsec 延伸標頭，例如在[RFC 4302]所描述 AH (authentication header，認證標頭) 和在[RFC 4303]所描述的 ESP (Encapsulating Security Payload，安全封裝負載)。關於 IP 安全延伸標頭參考文獻如下表所列：

表 95、IP 安全延伸標頭參考文獻

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

## (二)鏈結層安全考量

IPv6 非常依賴於在[RFC 4861]所定義的鄰居發現協議 (NDP)來執行各種鏈接操作，例如發現鏈接上的其他節點 (Discovering Other Nodes)、解析鏈接層位址、及在鏈接上尋找路由器。因此 NDP 的安全極需加強防護，以免容易受到駭客各種攻擊，攻擊的類別可分為路由器/鄰居訊息欺騙、重定向攻擊 (Redirect Attack)、重複位址檢測 (Duplicate Address Detection，DAD)、DoS (Denial-of-Service Attack，DoS) 攻擊…等。關於 NDP 的安全威脅議題，在[RFC 3756]和[RFC 6583]文件中有詳細說明 IPv6 ND 信任模型與威脅。關於 IPv6 鏈路層安全考量參考文獻如下表所列：

表 96、IPv6 鏈路層安全考量參考文獻

| 編號 | RFC 編號 | RFC 相關訊息 | |
|---|---|---|---|
| | | 類別 | 時間 |
| 1 | 4861 | Standards Track | 2007/09 |
| | | 標題：Neighbor Discovery for IP version 6 (IPv6) | |
| 2 | 3756 | Informational | 2004/05 |
| | | 標題：IPv6 Neighbor Discovery (ND) Trust Models and Threats | |
| 3 | 6583 | Informational | 2012/03 |
| | | 標題：Operational Neighbor Discovery Problems | |

## (三)路由安全考量

關於 IPv6 路由安全考量，以下將分為控制層面安全及路由安全 2 個議題個別討論。

### 1. 控制層面安全

在[RFC 6192]定義了路由器控制平面。路由器結構設計將轉發 (Forwarding) 和路由器控制平面硬體及軟體嚴格分開，其功能及使用情況為：

- 路由器控制平面：支援路由和管理功能。控制平面使用於處理設備本身的封包，及發送設備本地產生的封包。
- 路由器轉發平面：轉發平面用於負責在傳入介面上接收封包，執行查詢以識別封包的 IP 下一轉送節點，並確定往目的地的最佳傳出介面轉發封包。

一般轉發平面是以高速硬體處理，但是控制平面常以通用處理器 (稱為路由器處理器 RP) 實現，而無法高速處理封包。因此，可以透過輸入佇列 (Input Queue) 傳送比其處理數量更多的封包來攻擊此處理器。在這種情況下控制平面處理器將無法處理有效的控制封包，並且路由器可能會丟失 OSPF 或 BGP 鄰接關係，因此導致路由問題與嚴重網路中斷狀況發生。以下方法可以降低此狀況發生：

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

以下針對控制協定、管理協定及例外封包 3 個項目進行說明：

(1) 控制協定

- 丟棄從非 link-local address 收到的 OSPFv3 (Next-Header 89) 與 RIPng (UDP port 521) 控制封包。
- 允許從所有 BGP (Border Gateway Protocol，邊界閘道器協定) 鄰居節點收到的 BGP 封包 (TCP port 179)，其他則丟棄。

- 允許所有 ICMP 封包。

(2) 管理協定

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

(3) 例外封包

以下情況必須處理，當硬體無法處理，可以交給路由器 CPU 處理。

- 當資料平面轉送封包過大時，需傳送封包過大 (packet-too-big) 之 ICMP 訊息。
- 當資料平面封包因其跳數限制已到達 0 而無法轉送時，需傳送 ICMP 跳數限制已過期 (hop-limit-expired) 訊息。
- 如果無法轉送資料平面封包時，需傳送 ICMP 目標不可達 (destination-unreachable) 訊息。
- 逐跳選項標頭 (hop-by-hop options header) 處理，根據 [RFC 8200]文件說明，可選擇處理或不處理。
- 特定路由器實現：對於超大延伸標頭鏈，造成硬體無法處理，必須轉到路由器 CPU 處理。

**2. 路由安全 (Routing Security)**

路由安全一般需要考量以下幾點：

(1) 鄰居節點之認證。

(2) 節點 (Peer) 間安全路由之更新。

(3)路由過濾。

## (四)紀錄與監視

為了進行網路鑑識研究，在發生安全事件或偵測到異常行為時，網路接取服務提供商應記錄相關資訊。內容應包含：

- 服務類型 (例如 Web 伺服器)，紀錄所有應用程序使用網路的日誌 (包括 User Space 和 Kernel Space)。
- 自 IP 連線流資訊匯出 (IP Flow Information Export) 的資料，也稱為 IPfix，可參考[RFC 7011]有詳細資訊。
- 管理資訊庫 (Management Information Base，MIB) 的資訊，由各種簡易網路管理協議 (Simple Network Management Protocol，SNMP) 所定義的資料 ，可參考[RFC 4293] 有詳細資訊。
- 鄰居暫存 (Neighbor Cache) 的歷史資料。
- 定義於[RFC 8415]文件中關於有狀態 DHCPv6 租用暫存，尤其是當使用中繼代理時，關於中繼代理可參考[RFC 6221]。
- 於[RFC 7039]文件中所定義的來源位址驗證改善 (Source Address Validation Improvement，SAVI) 事件，尤其是 IPv6 位址與 MAC 位址以及特定交換機或路由器介面的綁定。
- 於 [RFC 2866] 文件中所描述，關於 RADIUS (Remote Authentication Dial In User Service，遠端用戶撥入驗證服務) 統計記錄。

有關如何收集、保存和安全丟棄相關紀錄資訊，及紀錄資訊的隱私問題或法規，ISP 須遵循其國家法律相關使用規定 (例如歐盟的 GDPR)。這些紀錄資訊可以被使用於：

- 網路鑑識：了解行為人在何時，在網路上執行動作。
- 相關性辨別：特定節點使用了哪個 IP 位址 (假設使用定義於[RFC 4941]文件中關於隱私延伸位址)。
- 節點清單：網路上 IPv6 節點清單列表。
- 異常行為檢測：異常流量模式通常是異常行為的症狀，而異常行為又可能構成潛在攻擊，如阻斷服務、網路掃描、節點成為殭屍網路的一部分...等。

# 二. 網際網路存取服務

網際網路存取服務將分為 IPv6 存取網路安全考量及 CPE (Customer-premises equipment，用戶終端設備) 簡易安全功能建議 2 個項目進行討論。

## (一)IPv6 存取網路安全考量

以下將依照不同網路類型，個別進行探討 IPv6 存取網路安全考量要點：

### 1. 寬頻電纜網路

DOCSIS (Data Over Cable Service Interface Specification，有線電纜資料服務介面規範) 電纜網路中的安全性是採用 Baseline Privacy Plus (BPI+) 規範，唯一和 IP 位址相關的部分是加密群播 (Encrypted Multicast) 。群播加密在 IPv6 環境中的工作方式與在 IPv4 網路中的工作方式相同；但是，DOCSIS 規範中需要適當的強化以支援加密的 IPv6 群播。

為了增強安全性，必須對主機進行部分的修改。主機應使用定義於 [RFC 3041] 文件中，用於自動配置

(auto-configuration) 的隱私延伸，如果在主機或 GWR 上可採用，則啟用 IPv6 防火牆功能。

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

CMTS/ER (Cable Modem Termination System) 應該保護 ISP 網路和其他用戶免受其自己客戶的攻擊。因此，應在對用戶的所有介面上使用單播反向路徑轉發 (Unicast Reverse Path Forwarding，uRPF) 規範在[RFC 3704]文件中和存取控制列表 (ACL) 。應根據 IPv6 操作要求進行過濾 IPv6-Security。

CMTS/ER 應該保護其處理資源免受大量有效客戶控制流量侵擾，例如：路由器和鄰居請求，及 MLD (Multicast Listener Discovery) 請求。

與 IPv4 服務一起使用的所有其他安全功能，也需要應用於 IPv6 網路上。

**2. 寬頻 DSL 網路**

為了增強安全性，CPE 必須進行部分修改。主機應使用定義於[RFC 3041]文件中，自動配置的隱私延伸。讓 ISP 可以相對輕鬆地跟踪其分配給用戶的 Prefix。但是，如果法規要求 ISP 在/128 位址級別跟蹤其用戶，則可以利用能提供主機可追溯性的網路管理工具並行以實施隱私延伸。並應在主機或 CPR (Customer Premise Router) 上啟用 IPv6 防火牆功能。

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

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

BRAS (Broadband remote access server，寬頻遠端接入系統) 和邊緣路由器需保護其處理資源，以防止有效的客戶控制流量氾濫，例如：路由器和鄰居請求，及 MLD 請求。速率限制需應用在所有對用戶的介面上實行。將重點放在群播類型流量上，因為 IPv6 控制平面最常使用此類型。

與 IPv4 服務一起使用的所有其他安全功能，也需要應用於 IPv6 網路上。

**3. 寬頻乙太網路**

CPE 必須進行部分修改，以增加安全性。主機應使用定義於[RFC 3041]文件中，自動配置的隱私延伸，且主機須具備可追溯性。應在主機或客戶路由器上啟用 IPv6 防火牆功能。

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

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

作為用戶的第 3 層下一跳的設備 (BRAS 邊緣路由器) 應保護網路和其他用戶免受提供者客戶的攻擊。因此，應在對用戶的所有介面上使用 uRPF (Unicast Reverse Path Forwarding，

逆向轉發) 和 ACL，需根據 IPv6 操作要求進行過濾 IPv6-Security。

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

與 IPv4 服務一起使用的所有其他安全功能，也需應用於 IPv6 網路上。

**4. 無線區域網路**

為了增強安全性，必須對 WLAN 主機/路由器進行部分更改。主機應使用定義於[RFC 3041]文件中，自動配置的隱私延伸，且主機須具備可追溯性。需在 WLAN 主機/路由器上啟用 IPv6 防火牆功能。

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

如果使用 Web 的身份驗證系統完成熱點上的主機身份驗證，則安全級別將取決於如何實現。用戶憑證絕不能通過 HTTP 以明文形式發送，Web 瀏覽器和身份驗證服務器之間應使用安全 HTTP (HTTPS)。身份驗證服務器可以在後端使用 RADIUS (Remote Authentication Dial In User Service，遠端用戶撥入驗證服務) 和 LDAP (Lightweight Directory Access Protocol，輕型目錄存取協定) 服務。

身份驗證是在實施第 3 層安全策略之前確保 WLAN 網路安全的重要事項。此有助於避免對 ND 或無狀態自動配置過程的威脅。802.1x [IEEE8021X]提供了確保網路存取安全的方法。但是，多種類型的 EAP (Extensible Authentication Protocol，擴充認證協定)，如 PEAP，EAP-TLS，EAP-TTLS，EAP-FAST 和 LEAP 等，以及部分主機支援特定功能的能力會讓實施全面一致的策略變得困難。

802.11i [IEEE80211i]修訂版包含許多組件，其中最明顯的兩個新的資料保密協議：臨時密鑰完整性協議 (Temporal Key Integrity Protocol，TKIP) 和計數器模式/CBC-MAC 協議 (Counter with CBC-MAC，CCMP)。802.11i 還使用 802.1X 的密鑰分發系統來控制對網路的存取。由於 802.11 處理單播和群播流量的方式不同，因此每種流量類型都有不同的安全問題。借助幾種資料保密協議和密鑰分發，802.11i 包含協商過程，用於為每種流量類型選擇正確的保密協議和密鑰系統。引入的其他功能包括密鑰暫存和身份驗證。

802.11i 修正是無線安全性的一大進步。該修正增加更強大的加密、身份驗證和密鑰管理策略，可以使無線傳輸和系統更安全。

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

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

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

**5. 寬頻電力線通信 (PLC)**

安全性考慮方面與乙太網路相同。

## (二)CPE 簡易安全功能建議

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

**1. 非狀態式過濾器 (Stateless Filters)**

(1) 在其外部 IPv6 標頭中帶有群播來源位址封包，不得在任何接口上轉發或傳輸。

(2) 在其外部 IPv6 標頭中具有等於或小於範圍的已配置範圍邊界級別 (請參閱[RFC 4007]文件中 IPv6 範圍位址體系結構) 的外部群播目的地 IPv6 封包，絕不能在任何方向上轉發。內定區域邊界級別應該僅限內部區域，並且應該由網路管理員配置。

(3) 禁止將帶有來源位址和/或目標位址的封包顯示在通過公共 Internet 傳輸的封包外部標頭中。特別是，在[RFC 3879]文件中規範棄用 site-local 位址，[RFC 5156]文件明確禁止使用 IPv4 對應 (IPv4-Mapped) 的位址，兼容 IPv4 的位址，

Document Prefix 與 Overlay Routable Cryptographic Hash Identifiers (ORCHID)。

**2. 免連接過濾器 (Connection-Free Filters)**

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

(2) 若以應用程序透明性考量，則對於通用上層傳輸協議，狀態封包過濾器應具有〝和無關端點的過濾〞行為。若以嚴格的過濾行為為考量，則過濾器應具有〝位址相關過濾〞行為。過濾行為可以依網路管理員所希望的配置方法進行，並且可以獨立於其他協議的過濾行為。過濾行為應預設在端點中，且獨立於端點，該端點在沒有服務提供商管理的情況下進行。

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

(1) 必須為出站資料流量和明確允許的入站資料流量，轉發所有有效的 TCP 封包序列 (定義在 [RFC 0793]中)。特別是，必須同時支援正常的 TCP 三向握手操作模式和同時打開操作模式。

(2) 當過濾器在 TCP 3 方交握或同時打開時，未偵測到窗口縮放選項 (window-scale option) (請參閱[RFC 1323]說明)，TCP window 不可以被強制執行。

# 三. 網際網路應用服務

## (一)IPv6 架構

### 1. 位址與子網路分配

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

然而廣域路由系統 (BGP-4) 的縮放屬性，意味著應該限制 PI 位址的數量，只有大型供應商可以合法獲得 PI Prefix，並說服 ISPs 對其進行路由，數以百萬計的企業網路 (包括較小的內容供應商) 將使用 PA Prefix，在這種情況下，若使用[RFC 4192]文件中描述的過程，更改 ISP 將需要更改相對的 PA Prefix。

### 2. 路由

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

通用路由協定，例如[RFC 5340]文件所規範 OSPFv3 (Open Shortest Path First version 3)，[RFC 5308]所定義 IS-IS (Intermediate System to Intermediate System)，甚至在[RFC 2080]及[RFC 2081]文件中所規範下一代路由資訊協定 RIPng (Routing Information Protocol next generation)，都支援 IPv6，值得注意的是，儘管 OSPF 和 RIP 在 IPv4 和 IPv6 之間存在顯著差異，但 IS-IS 的優勢在於可以在協定的單個實例中處理，且

可能簡化操作，在[RFC 5838]文件中所描述的部分版本OSPFv3也可能具有此特點。對於訓練有素的人員，在不干擾IPv4服務的情況下部署IPv6路由應該沒有特別的困難。

在某些情況下，部分網路設備可能需要韌體升級、需要評估雙協定路由的效能影響，特別是，路由器供應商可能要求IPv6 具有一定的傳輸效能，如果傳輸效能明顯不如 IPv4，需考慮這是操作上的問題，還是否需要額外的記憶體或三態內容可定址記憶體 (ternary content addressable memory，TCAM) 空間來容納IPv4和IPv6資訊等。

為了評估以上可能問題，ICP 需要針對初始預計狀況IPv6流量及成長率擬定流量預測模型，如果 ICP 使用多個 PA Prefix，則路由配置將更形複雜化，特別針對來源路由規則，需確保傳出的封包透過適當的邊界路由器和ISP連接，通常不應該透過ISP Y發送由另一個ISP X分配的位址來源封包，以避免經由ISP Y須根據[RFC 2827]及[RFC 3704]文件所定義過濾規範進行輸入來源過濾處理。

其他注意事項可以在 MULTIHOMING-WITHOUT-NAT [RFC 7157]文件中找到，在[RFC 6296]文件中討論的Prefix轉換技術，並未描述提供公開內容伺服器的企業解決方案，每個IPv6子網路支援終端機常使用64 Prefix，剩下的64位元則用於配發給各主機作為介面ID。

典型 IPv4 子網路的主機 ID 不得超過使用 8 位元進行配置，所以子網路被限制為需少於256個主機，雙協定設計通常對IPv4和IPv6會使用相同的實體或VLAN (Virtual Local Area Network，虛擬區域網路) 子網路拓撲，因此也將使用相同的

路由器拓撲，也就是 IPv4 和 IPv6 共用一致的拓撲，這代表即使 IPv6 Prefix 可允許更多的主機，但 IPv4 限定子網路大小規則 (如不超過 256 個主機) 也會被強加給 IPv6，理論上可透過不同的實體或 VLAN 子網路拓撲實現 IPv6 以避免此限制，但並不適用於實際情況，因為當出現問題時，將導致故障診斷變的極其複雜。

**3. DNS**

一旦在 DNS 中發布一個網站名稱 AAAA (pronounced quad A，IPv6 主機位址 DNS 資源紀錄) 記錄，對應的伺服器就會開始接收 IPv6 流量，因此將 IPv6 的 AAAA 記錄增加到 DNS 之前，須徹底進行 ICP 測試以確保 IPv6 在伺服器、負載平衡器等能正常工作，這一點非常重要。

如果 IPv6 的伺服器配置不正確的返回 AAAA 記錄，將可能破壞很多 IPv6 用戶的站點，一旦測試成功，每個 IPv4 位址具有 A (IPv4 主機位址 DNS 資源紀錄) 記錄的外部可見主機 (或虛擬機) 都需要 IPv6 位址具有 AAAA 記錄，詳細資訊可參考[RFC 3596]文件內容，另外還需要一個 DNS 反查紀錄 (紀錄在 ip6.arpa 中) ，如果使用 CNAME (Canonical Name Record，正式名稱紀錄) 記錄，必須在 CNAME 鏈最後面的 A 記錄增加 AAAA 記錄。

根據[RFC 1912]文件描述，不可以讓 AAAA 記錄名稱與用於 CNAME 記錄名稱相同，因為部分用戶端系統 (尤其是 Windows XP) 即使可以將 IPv6 用於應用程序流量，也只能透過 IPv4 解析 DNS 名稱。

此外,雙協定分解器可能會嘗試透過 IPv6 解析對 A 記錄的查詢，或者透過 IPv4 解析對 AAAA 記錄進行查詢，因此，建議所有 DNS 服務器提供可以透過 IPv4 和 IPv6 應對查詢。

## (二)伺服器

### 1. 網路堆疊

目前終端用戶常用系統中,TCP/IP 網路堆疊已經支援 IPv6 多年，多數情況下，啟用 IPv6 和 DHCPv6 就足夠，ICP 網路內部的伺服器，除了簡單雙協定外，不需要支援任何過渡技術，由於部分作業系統針對 IPv4 和 IPv6 具有單獨的防火牆規則，因此 ICP 還需評估這些規則，並確保為 IPv6 配置適當的防火牆規則。

### 2. 應用層

一般基本 HTTP 伺服器能夠處理啟用 IPv6 的網路堆疊,因此有必要更新到新版軟體,如電子郵件協定之類的通用應用程式也是如此。

關於其他應用程式，尤其是專有應用程序，無法做出一般性聲明，因此每個 ASP 需要做出自己的判斷，由於對網路層進行更改以引入 IPv6 位址會在應用程式中引起漣漪效應，因此，在對生產環境進行雙協定升級之前，應在 IPv4-only、IPv6-only 及雙協定個別環境中，分別對用戶端和伺服器應用程式進行測試,一項重要建議是,所有應用程式都應使用與 IP 版本無關的域名，而不是 IP 位址。

對於中介平台應用程式可共同支援 IPv4 和 IPv6，例如 Java，無需進行其他升級工作，安全憑證需包含域名而不單是 IP 位址。

關於 HTTP 伺服器需考慮的特定問題為，對於 IP 位址的 cookie 身份驗證方法需要處理雙協定客戶端，伺服器可能會為 IPv4 連接或 IPv6 連接建立 cookie，此取決於客戶端的設定，及客戶端所使用的作業系統，無法保證給定的客戶端將維持使用相同的 IP 位址，尤其在存取網站集而非單一網站時常發生，例如將 cookie 用於聯合身份驗證時，如果客戶端使用定義於 [RFC 4941]文件中的隱私位址，則 IPv6 位址 (但通常不是其 /64Prefix) 可能會非常頻繁地更改。

任何 32-bit 的 IPv4 位址的 cookie 機制都需要進行重構，在 [RFC 4038]文件中討論關於應用程式轉換的一般注意事項，但其中許多並不適用於雙協定 ICP 方案，ICP 若有自建和維護的應用程式，需要檢查其和 IPv4 的關係及依賴性。

**3. 紀錄**

客戶端的 IPv6 位址常會出現在伺服器紀錄檔的〝客戶端 IP〞欄位中，使用相同的紀錄檔欄位保存客戶端的 IP 位址 (無論是 IPv4 還是 IPv6) 更為方便，因此需要查看記錄檔和客戶端 IP 位址的下游系統也需要進行測試，以確保可以正確處理 IPv6 位址，包括 ICP 記錄客戶端 IP 位址的任何資料庫，例如用於記錄線上購買和註解標語的 IP 位址資料庫。

值得注意的是，從紀錄檔到個人客戶的準確回溯，需要點到點位址透通性，這是 ICP 支援本機 IPv6 連接的另一個動機，否則 IPv6-only 客戶將無法避免需透過其他形式轉換機制進行連接，因而干擾可回溯性功能。

**4. 地理位置**

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

從長期來看，IPv6 不會比 IPv4 的精準度更高，隨著時間推移，可以預期將有更多客戶端轉移到 IPv6，以 IP 位址進行地理位置定位將成為問題，因此可以考慮使用其他更強大的技術，例如啟用在[RFC 5985]文件中所描述的 HTTP 位置傳遞(HTTP-Enabled Location Delivery，HELD) 技術進行定位。

## (三)操作與管理

初期進行 IPv6 升級時，需要對系統人員進行教育訓練，並透過更新路由器等網路元件、更新網路配置等進行調整，才能達到系統可用性，並可提供資訊給用戶，及有足夠能力進行問題診斷。

對於企業網路而言，例如，在許多大學校園中都有具備豐富經驗的操作人員，雙協定運作並不比 IPv4 難。另外對 IPv4 所執行任何管理、監視和紀錄檔資料，必須更新相關網路設備和工具，以達成支援 IPv6 管理資料，重要的是要驗證工具是否已完全更新支援以十六進制格式輸入和顯示的 128-bit 位址，可參考[RFC 5952]文件中描述對 IPv6 位址表示方式的建議。

由於 IPv6 網路可以使用一個以上的 IPv6 Prefix 操作，因此每台主機可以使用一個以上的位址，因此這些工具必須在正常情況下進行處理。包括使用中的任何位址管理工具以及用於 DHCP (Dynamic Host Configuration Protocol，動態主機設定協定) 和 DNS

配置的工具，可參考在[RFC 6879]文件中對 IPv6 重新編號的方法及建議。

在 IPv6 部署的早期階段，很可能主要透過 IPv4 傳輸來管理 IPv6，這使網路管理系統可以測試 IPv4 和 IPv6 管理資料之間的依賴性，例如，是否會正確顯示混合顯示 IPv4 和 IPv6 位址的報告？在第二階段，應使用 IPv6 傳輸來管理網路，需注意即使在遠端工作時，ICP 也有必要為其操作和支援人員提供 IPv6 連接，對於管理資料和傳輸，都需盡可能避免 IPv4 和 IPv6 之間的相互依賴性，以免 IPv4 或 IPv6 網路連結失敗時會相互影響。

避免這種情況的一種預防措施是將網路管理系統雙協定，這樣就可以使用 IPv4 連接來修復 IPv6 配置，反之亦然雙協定有其必要性，但對企業確實會產生管理擴充性和開銷方面的疑慮。

如前所述，長期目標是在網路及其客戶可支援的情況下，轉向單 IPv6-only 協定，在管理系統中應避免 IP 位址家族間相互依賴的另一個原因；若在 IPv6 網路系統中，存在只支援 IPv4 上運行的管理工具，在 IPv4 關閉的那一天將會造成災難性後果，ICP 應確保更新任何點對點可用性監視系統，以通過 IPv4 和 IPv6 監視雙協定伺服器。

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

## (四)應用服務安全考量

許多 ICP 可能仍在試驗和配置 IPv6 的過程中，但惡意軟體對 IPv6 發起攻擊確持續成長，例如：為主機名稱增加 AAAA 的 DNS 記錄後，使用客戶端操作資料庫系統的惡意軟體，可能會自動通過 IPv4 攻擊該主機名稱，轉變為通過 IPv6 攻擊該主機名稱。因此保護伺服器防火牆和其他網路安全設備支援 IPv6 並測試和配置規則十分重要。

可以將 IPv4 安全經驗作為引導，以瞭解 IPv6 中可能存在的威脅，但不應該認為其具有相同的可能性，也不應該將其視為 IPv6 中可能存在的唯一威脅，實際上，存在於 IPv4 的每種威脅或多或少地將存在於 IPv6，因此必須更新防火牆、入侵檢測系統、拒絕服務預防措施和安全審核技術等，以完全支援 IPv6，打開安全機制 (例如 DNS 安全性和 DHCPv6 身份驗證) 也很重要，否則 IPv6 將成為攻擊者的誘人目標。

當使用多個 PA Prefix 時，防火牆規則必須允許所有有效 Prefix，並且必須設置為預設工作，即使數據封包是透過一個 ISP 發送，但返回數據封包則是透過另一個 ISP 到達，必須考慮雙協定防火牆的效能和記憶體大小方面等。

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

在[RFC 4864]文件中概述保護 IPv6 網路不受外部攻擊的技術，假設 ICP 具有本地 IPv6 連接，建議使用 IPv4 協定類型 41 阻

止傳入的 IPv6-in-IPv4 通道流量，除[RFC 6343]文件描述應阻止此類傳出流量，只需根據[RFC 4890]文件描述阻止 ICMPv6 通訊；特別是對路徑 MTU 發現 Packet Too Big 訊息一定不能阻止。

與 IPv4 相比，利用暴力掃描攻擊發現主機存在於 IPv6 網路的機率較低，但 ICP 不可以因此陷入錯誤的安全性思考，因為各種命名或尋址，都有可能會導致 IPv6 位址空間可預測或可猜測。

在極端情況下，IPv6 主機可能配置有非常容易猜測的介面 ID。例如從〝1〞開始的連續介面 ID，手動編號的主機或子網將更容易猜測，應避免這種做法，在[RFC 6583]文件中討論了其他有用的預防措施，同樣的攻擊者可能會在紀錄檔、數據封包、DNS 記錄 (包括反向記錄) 或其他地方找到 IPv6 位址，除此之外還需考慮在[RFC 6105]文件中所提到的防止惡意路由器廣告 (RA Guard)。

在[RFC 5246]文件中所描述的傳輸層安全性 1.2 版 (Transport Layer Security，TLS) 及之前的版本，可與 IPv6 的 TCP 配合使用，意味著 HTTPS 安全性解決方案可立即應用，也同樣適用於任何其他傳輸層或應用層安全技術。

如果 ASP 以任何方式使用在[RFC 4301]文件中規範的 IPsec，和 [RFC 5996] 文件中規範的網路金鑰交換 (Internet Key Exchange，IKE) 協定來保護與客戶端的連接，也完全適用於 IPv6，但前提是兩端的軟體協定已正確更新。

詳細 ISP 之 IPv6 網路安全防護準則報告內容請參閱附錄八。

# 第二節 研析 ISP IPv6 網路連線服務安全防護建議事項

關於 ISP IPv6 網路連線服務安全防護建議事項，將依照一般用戶端最常使用界接網路不同分項探討，包含以下連網方式：

- 固接網路
- 行動網路
- 公眾無線網路

此分項工作內容及成果如下所述。

## 壹、固接網路連線服務安全防護建議

ISP IPv6 固接網路連線服務，包含以下 3 種類型：

- 電纜寬頻網路 (Cable Network)
- DSL(Digital Subscriber Line)寬頻網路
- 寬頻乙太網路

以下將就不同類型服務探討，根據不同網路存取服務特性，提供 ISP IPv6 網路安全防護建議事項。

## 一.電纜寬頻網路 (Cable Network)

針對國內家用電纜寬頻網路 (Cable Network) 現有的基礎設施，以及電纜網路中 IPv6 配置選項與安全事項，整理以下防護建議。

### (一) 電纜寬頻網路元件

電纜寬頻網路能夠向用戶提供 IP 網路傳輸服務，以提供高速網路存取和 IP 語音 (Voice over IP，VoIP) 服務。電纜數據服務介面規範 (Data Over Cable Service Interface Specification，DOCSIS)

[RF-Interface]中概述了透過電纜網路傳輸 IP 流量的機制，及定義如何透過電纜網路承載數據的標準。以下是電纜寬頻網路關鍵元件：

- 混合光纖同軸(Hybrid fiber-coaxial，HFC)：混合光纖同軸電纜，用作基礎運輸。
- CMTS (Cable modem termination system)：電纜數據機終端系統，又稱頭端設備，為第 2 層橋接或第 3 層 CMTS 路由。
- GWR (Gateway Router)：住宅閘道路由器，為主機提供第 3 層服務。
- 主機:PC、筆記本電腦等，連接到 CM (Cable Modem) 或 GWR 作為使用者連結上網終端設備。
- CM (Cable Modem)：電纜數據機。
- ER (Edge Router)：邊緣路由器。
- MSO (Multiple-System Operator)：多服務營運商。

下圖為電纜寬頻網路架構圖：

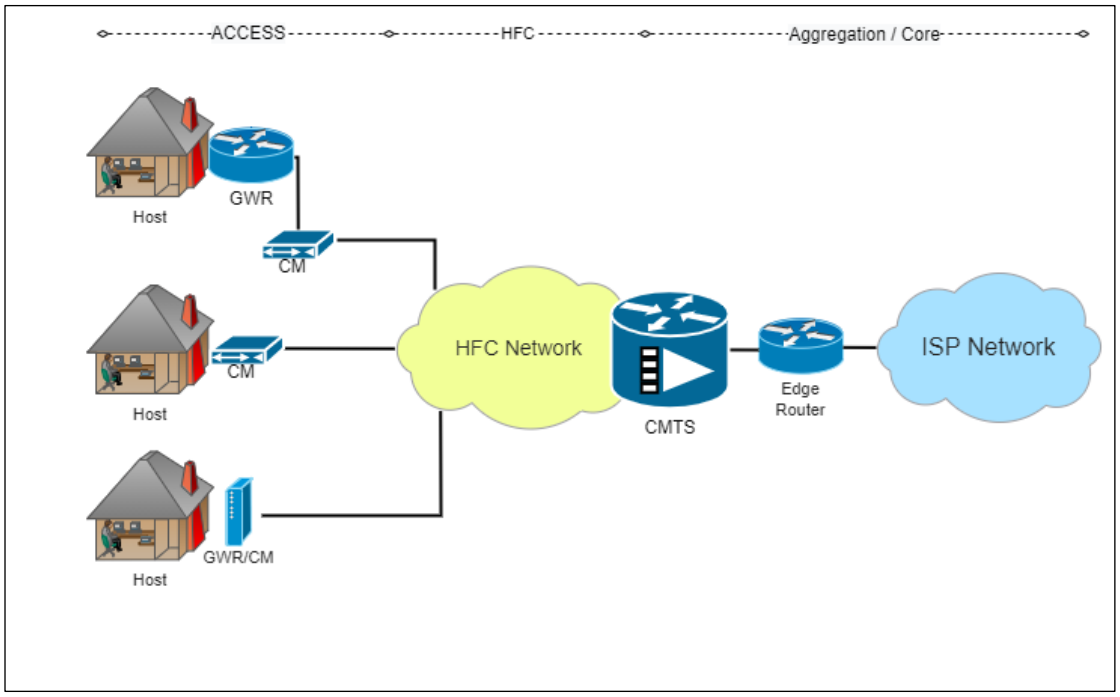



圖 159、電纜寬頻網路架構圖

## (二)於電纜網路中配置 IPv6

### 1. 在電纜網路中配置 IPv6

MSO 在其電纜網路上配置 IPv6 的動機之一是減輕管理負擔。出於管理目的，可以在 CM、CMTS 和 ER 設備上啟用 IPv6。根據[RFC1918]規範目前電纜基礎設施部分使用 IPv4 地址空間，但 IPv4 數量短缺。因此，系統管理者可考慮最初以 IPv6 用於管理平面上，之後將重點放在數據平面上，以用於最終用戶服務。

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

### 2. IPv6 QoS

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

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

重點當對通訊進行端到端加密時，全鏈路上的網路設備將無法存取用於分類目地的封包欄位。在此情況下，路由器很可能會將封包放入預設類中。QoS 設計應考慮此種情況，並嘗試主要使用 IP 表頭欄位進行分類。

### 3. IPv6 安全防護建議

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

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

CMTS 及 ER 設備應該保護 ISP 網路和用戶免受其他用戶的攻擊。因此應在對用戶的所有介面上使用於[RFC3704]文件中提到的單點傳播反向路徑轉發 (uRPF) 和存取控制列表 (ACL)。應該根據 IPv6 的操作要求進行 IPv6 安全性過濾。

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

與 IPv4 服務一起使用的所有其他安全功能也應類似地應用於 IPv6。

## 二.DSL(Digital Subscriber Line)寬頻網路

以下針對高速 DSL 網路中的 IPv6 配置選項與安全事項，整理防護建議及說明。

## (一)DSL 寬頻網路

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

下圖為 DSL 寬頻網路的架構圖：

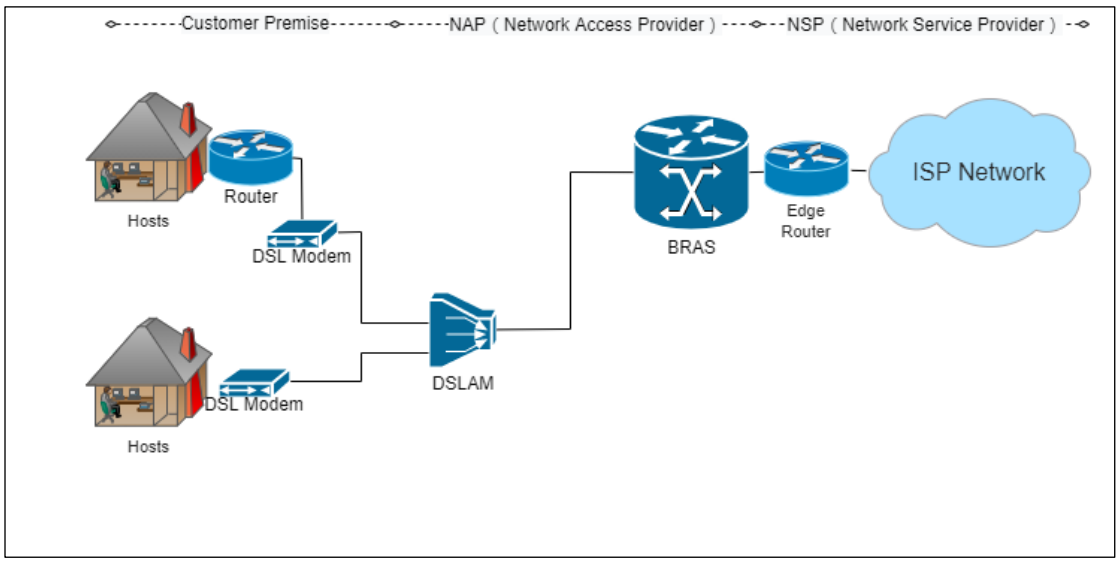



圖 160、DSL 寬頻網路的架構圖

以下網路元件是 DSL 網路的典型代表：

- DSL 調製解調器：是獨立設備、合併到主機中，亦可合併路由器功能，作為 CPE (Customer Premises Equipment) 路由器。
- 用戶終端路由器 (Customer Premises Router，CPR)：為用戶終端網路提供第 3 層服務。通常用於為小型企業提供防火牆功能和分段廣播區域。
- 數位用戶線路存取多工器 (DSLAM)：終止多條雙絞電話

線，並向 BRAS 提供聚合。

- 寬頻遠端存取伺服器 (BRAS, Broadband remote access server)：聚集或終止與用戶 DSL 電路相對應的多個永久虛擬電路 (Permanent Virtual Circuit，PVC)。
- 邊緣路由器 (ER)：提供到 ISP 網路的第 3 層介面。

## (二)於 DSL 寬頻網路部署 IPv6

### 1. 在 IPv4 DSL 網路中配置 IPv6

目前基於 DSL 寬頻存取的 IPv4 配置，在某些情況下，如果需要新的服務類型或服務，則 IPv4 和 IPv6 網路邏輯架構可能會有所不同。

透過 DSL 基礎結構提供 IPv4 連接的主要設計方法有四種包含點對點模型、PPP 終止聚合 (PTA) 模型、L2TPv2 存取聚合 (LAA) 模型、及 IPv4 和 IPv6 服務混合模型，以下將個別說明：

#### (1)點對點模型

每個用戶都透過雙絞線連接到 DSLAM，並配有一個唯一的 PVC，將其連接到服務網路提供者，PVC 可以在 BRAS 或邊緣路由器處終止。在這種情況下，必須在網路維護大量的第 2 層電路。第 2 層領域可透過三種方式在 ER 處終止：

- 在具有虛擬介面的通用網路橋接組中，該介面可將流量路由輸出。
- 透過啟用路由橋接封裝功能，所有用戶都可以屬於同一子網。此為 IPv4 在 DSL 上最常見的配置方法，但對 IPv6 在地址可用性問題上不是最佳選擇。

- 透過在第 3 層終止 PVC，每個 PVC 都有自己的位址前綴 (Prefix)，更適合 IPv6。

這些方法都不要求升級 CPE，在此情況下，來自主機或客戶路由器乙太網路橋接在分配給用戶 PVC 上。下圖為點對點模型協定體系結構：

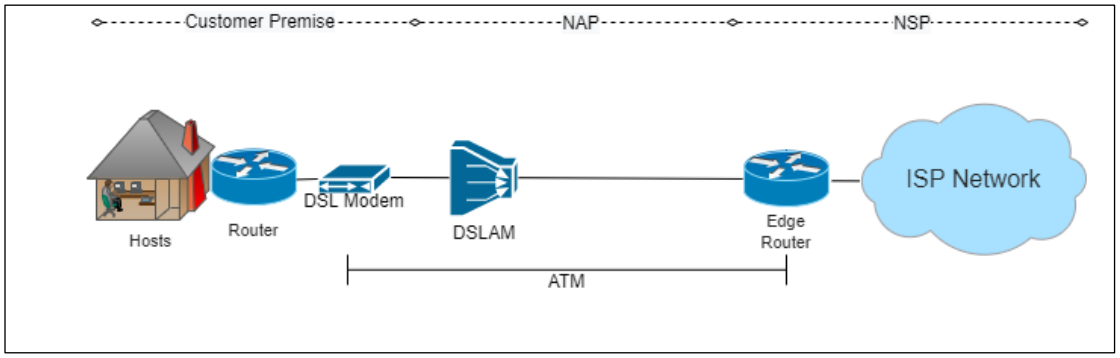



圖 161、點對點模型協定體系結構

**(2) PPP 終止聚合 (PTA) 模型**

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

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

當 NSP 也是 NAP 時，BRAS 和 NSP 邊緣路由器可以是同一台設備，並提供上述功能。此模型可以利用兩種類型的 PPP 封裝：

- 使用 PPPoA 進行連接

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

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

- 使用 PPPoE 進行連

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

不管使用哪種 PPP 封裝類型，PTA 模型的網路設計和操作皆相同。下圖為使用 PPP 封裝進行連結架構圖：

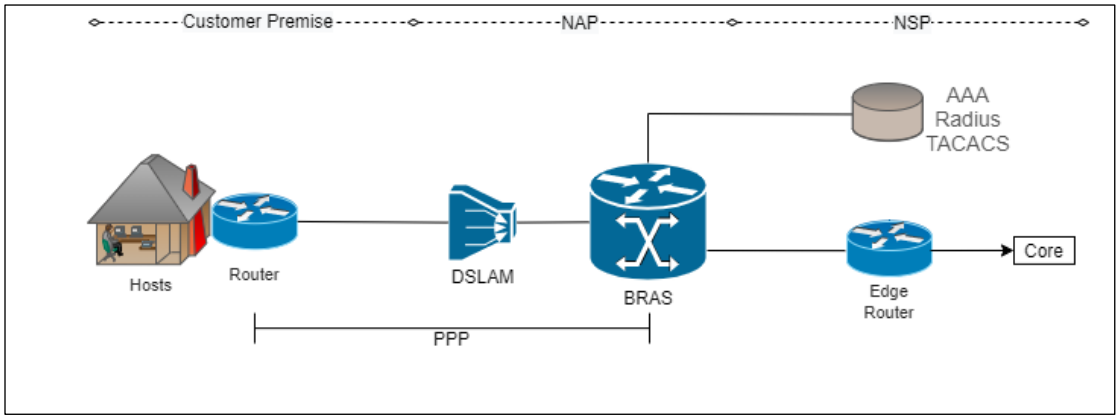



圖 162、使用 PPP 進行連結架構

### (3) L2TPv2 存取聚合 (LAA) 模型

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

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

此模型可以利用兩種類型的 PPP 封裝：

- 透過 PPPoA 連接
- 透過 PPPoE 連接

不管使用哪種 PPP 封裝類型，PTA 模型的網路設計和操作皆相同。下圖為 L2TPv2 存取聚合 (LAA) 模型透過 PPP 連接架構：

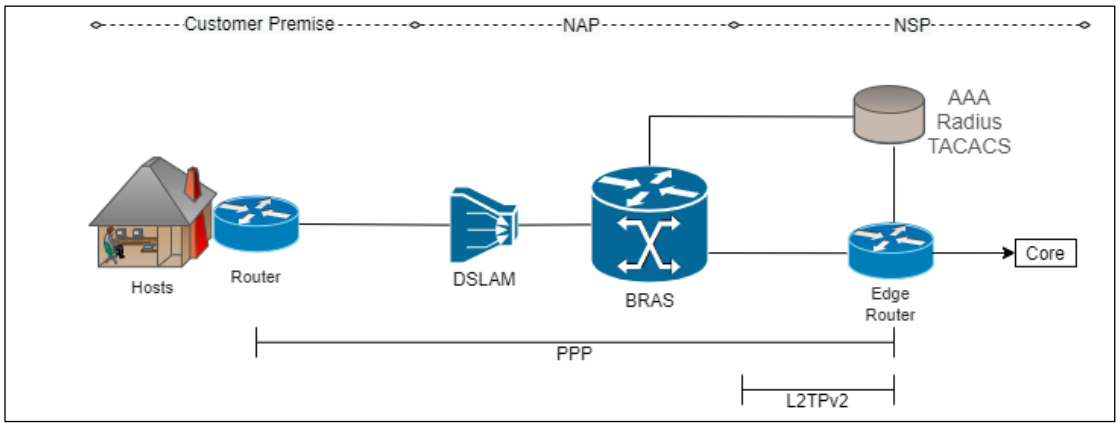



圖 163、L2TPv2 存取聚合 (LAA) 模型透過 PPP 連接架構

### (4) IPv4 和 IPv6 服務混合模型

- LAA 模型中的 IPv4 和 PTA 模型中的 IPv6

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

下圖為混合模型中 IPv6 和 IPv4 的邏輯設計：

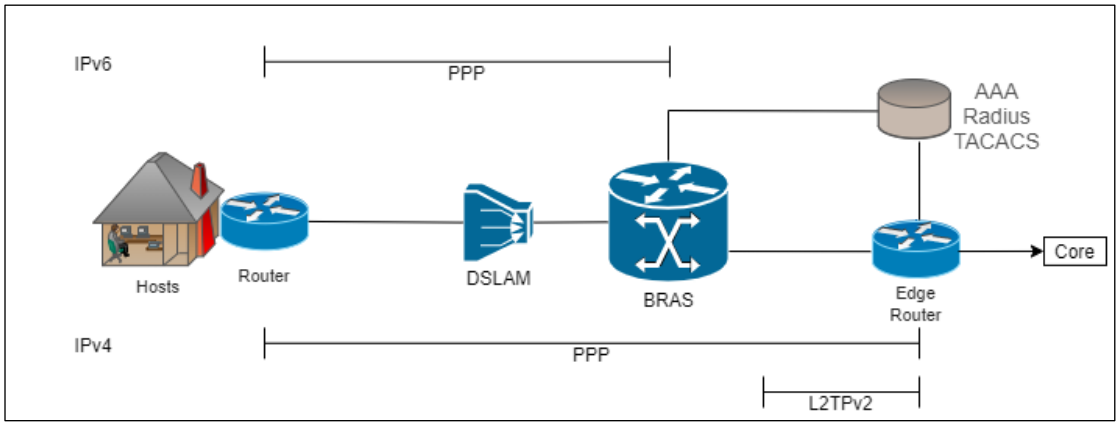



圖 164、混合模型中 IPv6 和 IPv4 的邏輯設計

- 定址

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

此配置模型 BRAS 必須能夠區分必須跨 L2TPv2 隧道橋接的 IPv4 PPP 流量和必須路由至 NSP 的 IPv6 封包。在

此混合設計中，必須在所有具有支援 IPv4 和 IPv6 服務的 PVC 的介面上啟用 IPv6 路由和橋接封裝 (RBE)。

**2. IPv6 QoS**

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

在 DSL 基礎結構中，已經為 IPv4 連接實現一定程度的流量監管。應於整個 NAP 中實現。

在 BRAS 或邊緣路由器上，必須配置連接用戶的介面以管理入站的客戶流量，並根據服務量協定 (SLA) 調整出站到客戶的流量。

為支援各種類型的客戶流量 (數據，語音和影片) 並對使用基礎結構資源最優化，流量分類和標記也應該在距離用戶最近 (第 3 層) 的路由器上進行。每個網路服務提供者 (NAP 或 NSP) 可以實施自己的 QoS 策略和服務，以便可以在 NAP 和 NSP 之間的邊界執行重新分類和標記，以確保 ISP 可以正確處理流量。相同的 IPv4 QoS 概念和方法也應與 IPv6 一起使用。

重點當對通訊進行端到端加密時，遍歷的網路設備將無法存取許多用於分類目的的封包欄位。在此情況下，路由器可能將封包放入預設類中。QoS 設計應考慮此種情況，並嘗試使用 IP 表頭欄位進行分類。

**3. IPv6 安全防護建議**

為了增強安全性，CPE 必須進行部份更改。主機應使用於 [RFC3041]文件中所描述自動配置的隱私延伸。ISP 相對容易地追蹤其分配給用戶的位址前綴。但法規要求 ISP 在/128 地址級

別追蹤其用戶，則可以與可提供主機可追溯性的網路管理工具並行實施隱私延伸。如果存在，則應在主機或 CPR 上啟用 IPv6 防火牆功能。

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

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

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

與 IPv4 服務一起使用的所有其他安全功能也應該應用於 IPv6。

## 三. 寬頻乙太網路

針對寬頻乙太網路存取中的 IPv6 配置選項與安全防護建議整理說明如下。

### (一) 乙太存取網路元件

支援 RJ-45 或光纖 (Fiber To The Home，FTTH) 配置到用戶的基礎結構環境中，提供 10/100 Mbps 乙太網路寬頻服務，在多用

戶的大城市區域中，該區域能以划算的方式配置，以及都會網路服務可向網路服務提供者提供聚合和上行服務。

以下是乙太網網路元件的典型代表：

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

下圖為乙太存取網路架構圖：

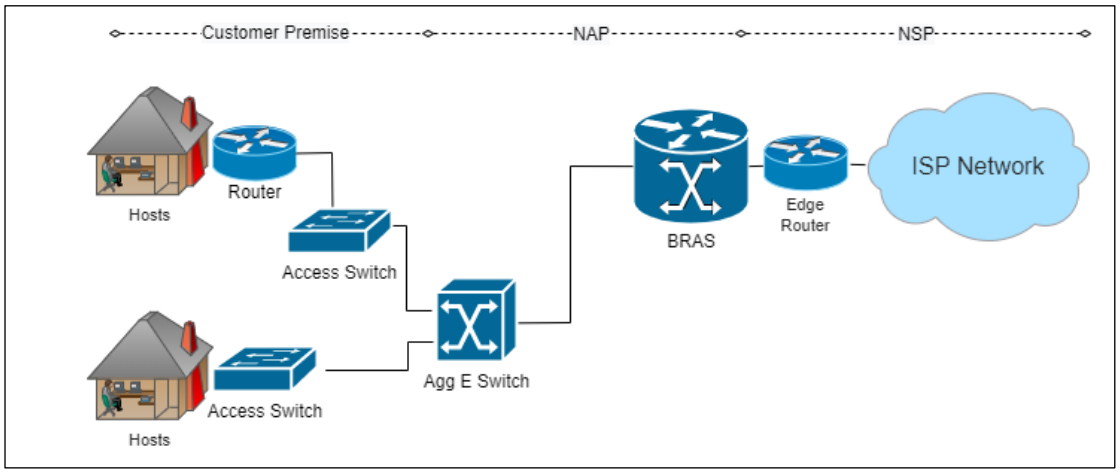



圖 165、乙太存取網路架構

寬頻乙太網的邏輯拓撲和設計與 DSL 寬頻網路非常相似，值得注意的是，一般操作、概念和建議適用於基於 Home PNA 網路環境。在此環境中，部份網路元件可能使用不同的名稱。

## (二)於寬頻乙太網路部署 IPv6

### 1. 在 IPv4 寬頻乙太網路中配置 IPv6

透過乙太網基礎結構提供 IPv4 連接的主要設計方法有三種：

**(1) 點對點模型**

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

透過 VLAN 橋接，主機或客戶前提路由器乙太網路分配給用戶。下圖為點對點模型協定架構圖：

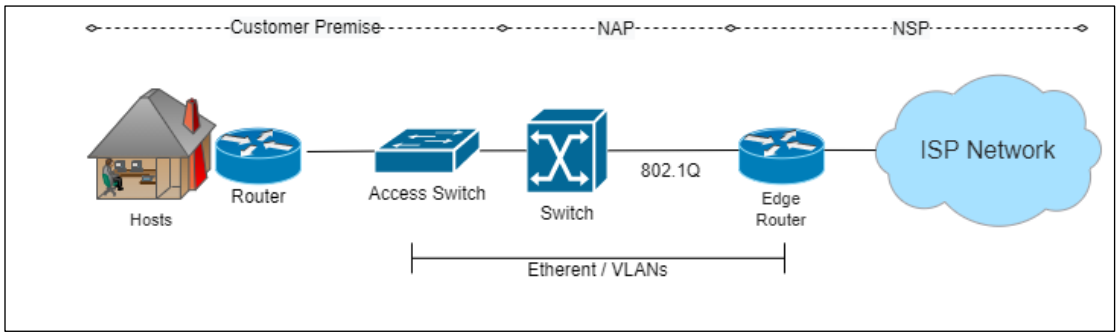



圖 166、點對點模型協定架構

**(2) L2TPv2 存取聚合 (LAA) 模型**

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

在 LAA 模型中，BRAS 透過在 BRAS 與邊緣路由器之間建立的 L2TPv2 隧道將 CPE 發起的會談轉發給 ISP。此情況下，身份驗證、授權和用戶配置由 ISP 本身執行。下圖為 L2TPv2 存取聚合 (LAA) 模型架構圖：

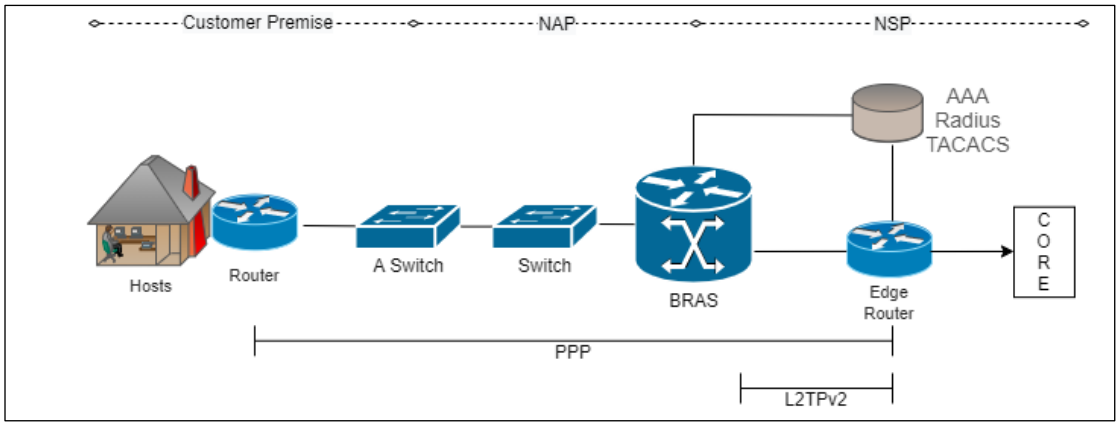



圖 167、L2TPv2 存取聚合 (LAA) 模型架構

**(3) IPv4 和 IPv6 服務的混合模型**

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

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

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

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

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

**2. IPv6QoS**

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

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

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

網路服務提供者 (NAP 或 NSP) 都可實作自己 QoS 策略，利於在 NAP 和 NSP 間的邊界執行重新分類和標記，確保 ISP 可以正確處理流量，也應適用於 IPv6。

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

QoS 設計應考慮，並嘗試以使用 IP 表頭欄位進行分類。

**3. IPv6 安全防護建議**

為增強安全性，CPE 必須進行部份修改。主機應使用於 [RFC3041]文件中描述自動配置隱私擴展與可追溯性，並且應在主機或客戶前提路由器上啟用 IPv6 防火牆功能。

ISP 提供用戶攻擊安全性，也可以實施安全服務，以保護其用戶免受外部網路攻擊，此處討論的網路存取不包含此範圍。

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

作為用戶第 3 層逐跳設備 (BRAS 邊緣路由器) 應保護網路和其他用戶免受網路服務提供者客戶攻擊，應在連結用戶的所有介面上使用 uRPF 和 ACL，根據 IPv6 的操作要求進行 IPv6 安全過濾。

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

## 四.固接網路 IPv6 安全防護建議

綜合以上，ISP IPv6 固接網路連線服務之 IPv6 安全防護建議，如下所列：

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

# 貳、行動網路連線服務安全防護建議

## 一.行動網路架構

行動網路用戶以行動節點 (Mobile Node，MN) 透過本地網路或存取網路連接到行動網路。在 3GPP (Third Generation Partnership

Project) 網路結構中，行動節點透過連接到行動閘道器存取點 (Access Point Name，APN) 存取網路。APN 類似於無線區域網的服務集標識符 (Service Set Identifier，SSID)，可用於指定行動節點的服務類型，例如網際網路存取、視訊、遊戲...等。行動節點在該特定 APN 上可以啟用不同 IP 連接類型，連接類型有 IPv4、IPv6、IPv4/IPv6 雙軌等。下圖為行動網路架構：

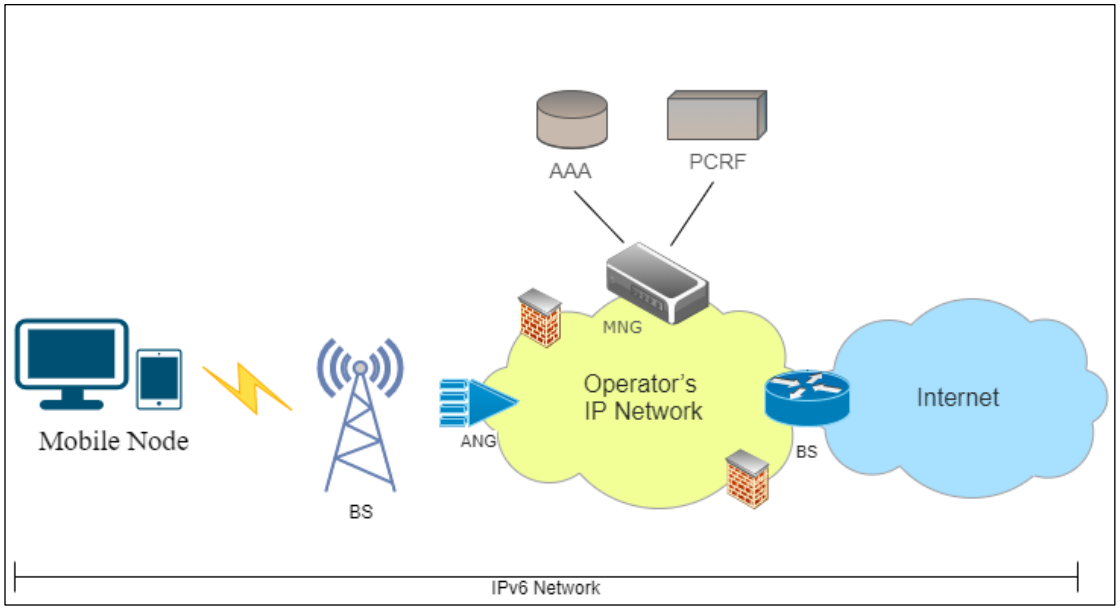



圖 168、行動網路架構

當 APN 將行動節點導向閘道器時，行動節點需要到閘道器的端到端〝連接〞。在 4G 長期演進技術 (4G LTE) 網路中，此連接透過演進分封系統 (Evolved Packet System，EPS) 實現。3G 普遍行動電信系統 (Universal Mobile Telecommunications System，UMTS) 網路中，此連接透過封包協定 (Packet Data Protocol，PDP) 前後關係實現。終端到終端 (end-to-end) 連接透過以下定義多個節點：

- 基地台 (Base Station，BS)：無線電基地台提供到行動節點無線連接。

- 存取網路閘道器 (ANG)：ANG 向行動節點轉發 IP 封包。ANG 不是行動節點預設路由器，不會為行動節點執行 IP 位址分配和管理。
- 行動網路閘道器 (Mobile Network Gateway，MNG)：MNG 是行動節點預設路由器，提供 IP 位址管理。MNG 提供服務品質 (Quality of Service，QoS)，應用於用戶策略以及啟用計費和帳單等功能，稱為〝用戶管理〞操作。介面管理用戶操作，通常位於本地網路。
- 邊界路由器 (Border Router，BR)：BR 與行動網路的網際網路交界。BR 不為行動網路執行用戶管理。
- 身份驗證、授權和計費 (Authentication, Authorization, and Accounting，AAA)：AAA 一般功能用於用戶身份驗證、授權以及生成帳單和計費訊息。
- 策略和計費規則功能 (Policy and Charging Rule Function，PCRF)：PCRF 允許在行動網路閘道器上應用策略和計費規則。

# 二.行動網路 IPv6 考量

## (一)IPv4 地址耗盡

公共 IPv4 地址空間即將耗盡，導致服務提供者必須考慮引進新技術，以維持網際網路運行。現行有兩種方法可行：

- 延遲 IPv4 地址耗盡
- 導入 IPv6

延遲公共 IPv4 地址耗盡的方法，包括為終端用戶分配私有 IPv4 地址或使用介面範圍延伸 IPv4 地址。如網路地址轉換

(Network Address Translator，NAT) 是在網路服務提供者端使用 (而不是客戶端) 的機制來管理私有 IP 地址分配和存取網際網路。

由於行動網路 IPv4 地址用盡的問題。在 3G 和 4G LTE 網路已在 PDP 內容和 PDN 連接形式，支援 IPv6。行動網路營運商可以為自己的應用程序和服務引入 IPv6。換句話說，IETF 的推薦雙協定 IPv6 和 IPv4 網路模型，可適用於與不同 APN 支援和承載 IPv6 流量，於 PDP/PDN 連接行動網路。也就是行動網路服務商須導入 IPv6，必要支援 IPv4IPv6 雙軌 PDN、IPv6 PDN 和 IPv4 PDN 的行動連接。

## (二)行動網路中 NAT 使用

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

行動網路配置 IP 地址空間的分配方式依系統設計有所不同。有些使用〝空間〞是由一個共同的節點管理的〝集中模式〞，如 PDN 的 BR，並且由多個 MNG 共享空間中所有連接到相同的 BR。然而，隨著 3G 網路出現和行動網際網路用戶數量急劇增加，IASP 必須重新檢視其網路設計。換句話說，不得不解決私有 IPv4 空間耗盡以及可擴展的解決方案。

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

考慮行動網際網路用戶可用的私有 IPv4 空間的管理已經成為重要議題。讓可以使用空間的重用機制有其必要性。其次在私有

IPv4 空間管理，NAT 功能的放置具會影響網路配置。常見的 NAT 集中模型具有傳統配置和私有 IPv4 地址重複使用的優點。但仍需要額外功能，如流量管理、用戶 NAT 在 MNG 狀態管理等。分佈式模型也可實現私有 IPv4 地址重複使用，且可以避免行動網路營運商的核心重疊私有 IPv4 流量，因此不需要額外機制。由於 MNG 執行的 IPv4 地址分配並具有標準介面為 AAA 和 PCRF，分佈式模型還可記錄用戶和 NAT 狀態。總之，網路服務提供者若要容易整合 NAT 與其他用戶管理功能，及重複使用私有 IPv4 空間，以分佈式模型為較佳選擇。但另一方面，NAT 共同管理網路服務提供者可能認為集中式模型為較佳選擇。

## (三)IPv6-only 部署注意事項

網路 NAT 功能採用出現許多原本不存在網路的問題。在 IPv6 廣泛使用前，應將 NAT 視為臨時解決方案，盡速導入 IPv6，及了解 IPv6-only 部署注意事項。

IPv6-only 部署需考慮三個面向：網路本身、行動節點和應用程序。目標是從 IPv4 達到三方面 IPv6 部署，目前是以雙協定模型為主，及每個面向都支援 IPv4 和 IPv6 共存。

行動網路中 IPv6-only 部署需要考慮以下注意事項。首先網路和行動節點都必須具有 IPv6 能力。加速網路升級以及使用 IPv6 行動節點。用於 LTE 的 3GPP 網路設計已經要求網路行動節點支援 IPv6。

使用 IPv6-only PDN 連接讓行動節點中應用程式之援 IPv6 具有相當挑戰性。在使用率較高的應用程式開始支援 IPv6 後，希望連

帶地鼓勵提供應用程序層 (例如網路插座介面 socket interface) 升級支援 IPv6。

LTE 語音 (VoLTE) 是另一挑戰。語音具有訊號發送和有效負載間分離特性，無需特別考慮應用程式訊號發送和有效負載流量即可解決連接問題。

IETF 鼓勵網路服務供應商支援 IPv6-only 部署及雙協定模型，並訂定一系列規範。網路服務供應支援 IPv6，需透過適當 APN 和相應的 IPv6-only PDP 或 EPS 承載提供。部份網路服務提供者會考慮 IPv6-only 部署來進行存取。在 IPv6-only 部署中使用 IPv6 對 IPv4 轉換機制時，可參考[RFC6146]和[RFC6145]文件中指定的協定和相關注意事項。可以透過主動地為新款行動節點引入 IPv6，可大大減少對專用 IPv4 位址需求。

表 97、使用 IPv6 對 IPv4 轉換機制參考文件

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

## (四) 固定網路與行動網路的融合

許多網路服務供應商同時提供固定寬頻和行動網路服務，兩個系統存取網路不同，例如固定存取網路中不考慮漫遊、行動網路的語音服務需全 IP 而固定網路服務則不需要等。

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

在同一網路服務提供者，需考慮兩個網路系統共同注意事項，例如 IPv4 位址管理是共同關心的問題、相同機制延遲 IPv4 位址耗盡並導入 IPv6 也適用。每個存取網路部署確切解決方案會有所不同，例如：固定網路中端點通常是電纜或 DSL 數據機，IPv6 內對專用 IPv4 封包進行隧道傳輸是可行方案。在行動網路中端點本身是行動節點，情況並非如此。

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

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

存取網路使用實際解決方案取決於特定服務要求。在存取網路和核心網路間有些可以共享。例如固定網路不需 NAT 用戶感知功能時，可在核心路由器提供該功能，而行動存取網路可以在行動閘道器提供 NAT 功能。

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

網路服務提供者可考慮共享核心網路。通用解決方案更易應用於核心網路。例如，行動和固定網路閘道器已配置隧道或 MPLS VPN 可將流量傳送到核心路由器，讓整個核心網路啟用 IPv6。

## 三.行動網路 IPv6 安全防護

在 3GPP 接入網路時，使用者裝置 ( User Equipment，UE) 和網路進行網路時，須執行相互身份驗證。此外，每次建立 PDP 內容或 PDN 連接時，可以針對 PCC (Policy and Charging Control) 基礎結構授權新連接，對現有連接的修改以及對 IPv6 Prefix 或 IP 地址的分配，和 PDN 的 AAA 服務器。

根據區域法規和行動網路營運商的部署策略，可以保護 UE 與 (e)NodeB 之間 3GPP 連結的無線部分，及 UE 與 MME / SGSN 之間的控制訊息，使用者流量可以受到機密性保護。控制平面至少受到完整性 (integrity) 和重放 (replay) 保護，並且還可能受到機密性保護。網路傳輸部分內的保護取決於行動網路營運商的部署策略。

對於離線 IPv6 攻擊，3GPP EPS 與任何 IPv6 系統一樣容易受到攻擊。

此外，還需考慮使用者裝置 IP 堆疊可能使用永久訂戶身份的識別，如國際行動用戶身份 (IMSI, International Mobile Subscriber Identity)，以 IPv6 地址識別作為永久用戶身份的來源。但此為隱私威脅，並將允許追蹤用戶。因此，禁止將 IMSI (或[TS.23003]定義的任何身份) 用作識別的來源[TS.23401]，但是沒有標準化方法去阻止，如異常行為的使用者裝置。

## 四.行動網路 IPv6 安全防護建議

綜合以上，ISP IPv6 行動網路連線服務之 IPv6 安全防護建議，如下所列：

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

# 參、公眾無線網路連線服務安全防護建議

以下就當前部署無線區域網 (WLAN) 基礎設施 IPv6 部署和整合方法說明，以及目前無線區域網路 (WLAN) 配置基礎結構的 IPv6 配置、合併方式。下圖為 WLAN 的關鍵元件及架構，主機應具無線網路介面卡 (Network Interface Controller，NIC)，才能連接到無線區域網路 (WLAN 為廣播網路，工作方式與乙太網路類似)。

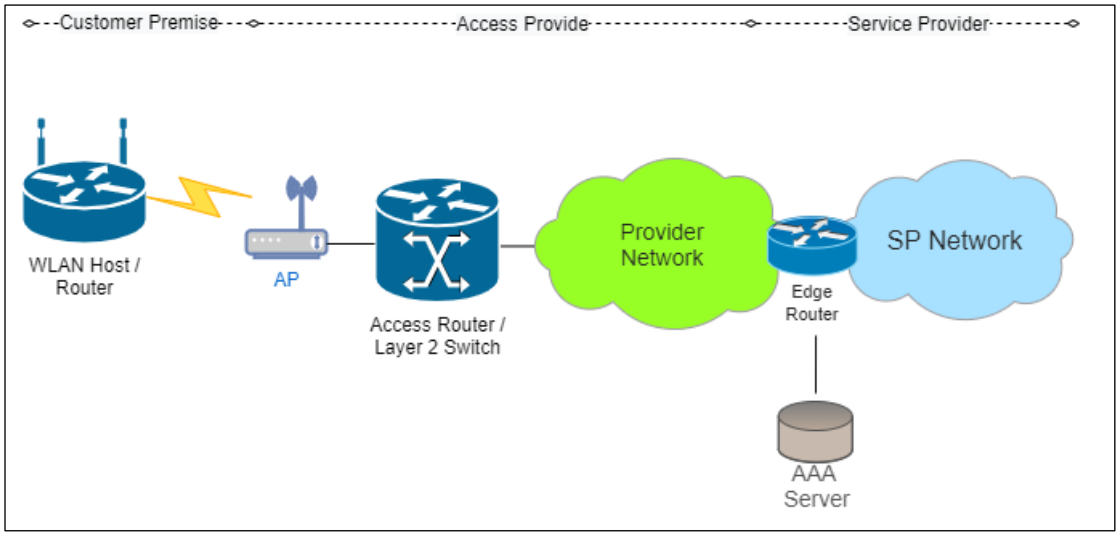



圖 169、公眾無線網路架構

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

AAA 伺服器對主機進行驗證，透過驗證即發送封包。AP 位於主機附近並作為橋接器，將所有來自主機的封包發送到邊緣路由器。AP 和邊緣路由器之間的底層連接可以使用任何存取層技術，如 HFC 電纜、FTTH、xDSL 等。

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

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

# 一.公眾無線網路配置情境

以下就不同公眾無線網路配置情境進行說明。

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

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

開始連接時，WLAN 主機由服務供應者網路的 AAA 伺服器進行驗證。存取點將所有驗證相關參數 (用戶名、密碼等) 轉發到 AAA 伺服器。AAA 伺服器對 WLAN 主機進行驗證，驗證成功為與 WLAN 存取點相關，即可獲取 IPv6 位址。此處，開始和認證過程與 IPv4 中使用的過程相同。

下圖為當第 2 層交換機位於存取點和邊緣路由器間的 WLAN 結構圖：

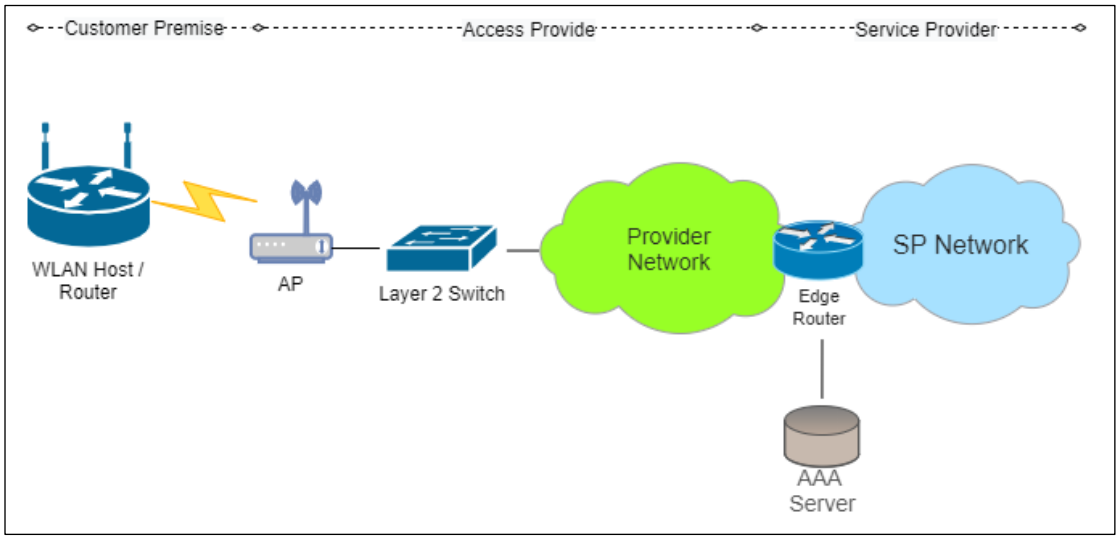



圖 170、當第 2 層交換機位於 AP 和邊緣路由器間的 WLAN 結構

**1. 更改 IPv6 相關基礎架構**

透過將 WLAN 主機，WLAN 路由器和邊緣路由器設備升級到雙協定，配置 IPv6 位址。

**2. 定址**

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

- 由[RFC2462]文件定義，LAN 主機使用無狀態自動配置從邊緣路由器獲取 IPv6 位址。WLAN 上所有主機都屬於邊緣路由器上靜態配置的同一/ 64 子網。IPv6

WLAN 主機可用無狀態 DHCPv6 來獲取相關訊息，例如 DNS 等。

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

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

- 在[RFC3177]文件中，根據網路服務供應者政策和客戶要求，可以在/48 和/64 間為 WLAN 路由器分配位址前綴 Prefix。如果 WLAN 路由器介面連接多個網路，則網路管理員必須為連接客戶站點上 WLAN 主機的路由器介面配置 /64 Prefix。連接到這些介面的 WLAN 主機可用無狀態自動配置進行自身配置。
- WLAN 路由器可以使用本地連接位址與邊緣路由器通訊。並可透過無狀態自動配置動態獲取自身與邊緣路由器間連接位址。此步驟後是透過 DHCP-PD (Prefix Delegation)請求小於/ 64 的 Prefix，並分配給其連接客戶站點上主機介面。

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

當存取點與邊緣路由器間存在存取路由器時，存取點一樣作為橋接器，將 IPv4 和 IPv6 封包從 WLAN 主機或路由器橋接到存取路由器。存取路由器是網路服務提供者網路的一部分，也可以由單獨的存取網路服務提供者所擁有。

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

下圖為存取路由器位於 AP 與邊緣路由器之間時的 WLAN 結構圖：

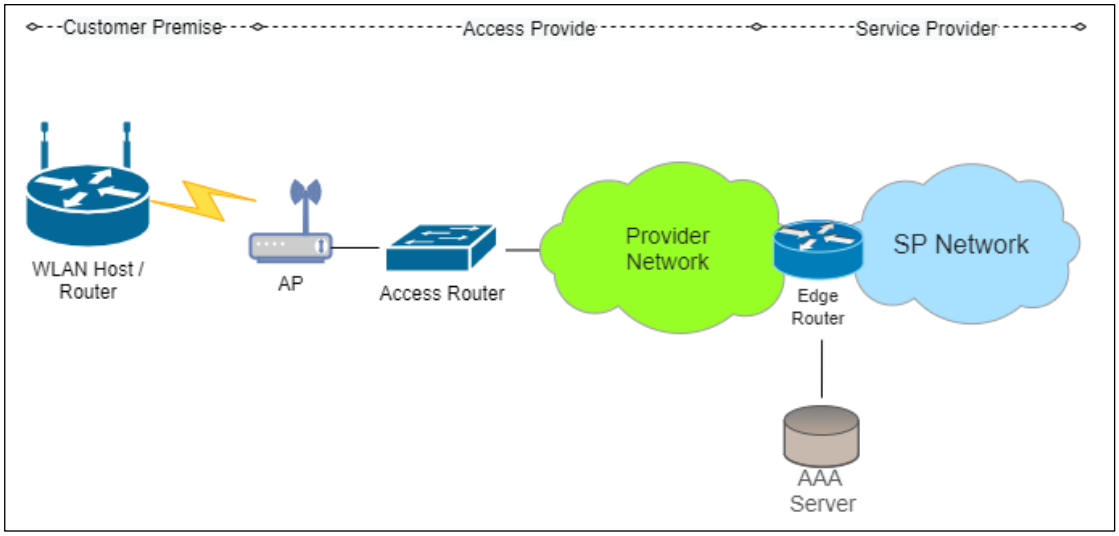



圖 171、存取路由器位於 AP 與邊緣路由器之間時的 WLAN 結構

**1. 更改 IPv6 相關基礎架構**

在此情況下，透過將 WLAN 主機，WLAN 路由器(如果有)，存取路由器和邊緣路由器設備升級到雙協定，並配置 IPv6。

**2. 定址**

在有存取路由器的情況下，可以使用以下 3 個選項來分配 IPv6 位址：

**(1)** 向存取路由器的邊緣路由器介面靜態配置為 /64 Prefix。存取路由器透過無狀態自動配置在連接邊緣路由器的介面上接收並配置 /64 Prefix。網路管理員必須配置 /64 Prefix，存取路由器以解決連接用戶端的問題。連接到該介面的 WLAN 主機及路由器可以使用無狀態自動配置自動進行自身配置。

**(2)** 在[RFC3315]文件中描述此選項使用 DHCPv6 為 WLAN 主機及路由器分配 IPv6 Prefix。此選項中不使用 DHCP PD 或無狀態自動配置。DHCPv6 伺服器可以位於存取路由器，邊緣路由器或網路服務提供者網路中的特定位置。在此情況下，根據 DHCPv6 伺服器的位置，存取路由器或邊緣路由器將中繼 DHCPv6 請求。

**(3)** 可以使用其本地連接位址與邊緣路由器通訊。還可以透過無狀態自動配置動態獲取自身與邊緣路由器之間的連接位址。此步驟之後是透過 DHCP-PD 請求的 Prefix 小於 /64 的 Prefix，並分配給其連接客戶站點上主機的介面。

**3. 路由**

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

如果存取路由器由存取提供者所有，則存取路由器可以具有指向網路服務提供者其網路邊緣路由器的預設路由。邊緣路由器運行網路服務提供者網路中使用的 IGP，例如 OSPFv3 或用於 IPv6 的 IS-IS。連接的 Prefix 必須重新分配。如果使用

DHCP-PD，則邊緣路由器會為每個委派的 Prefix 安裝一條靜態路由。因此，必須重新分配靜態路由。Prefix 概要應在邊緣路由器上進行。

如果存取路由器由網路服務提供者擁有，則存取路由器還需運行 IPv6 IGP，並將成為網路服務提供者 IPv6 路由域 (OSPFv3 或 IS-IS) 的一部分。連接的 Prefix 必須重新分配。

## (三) PPP-Based 模型

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

### 1. IPv6 WLAN 環境中的 PTA 模型

配置 PTA 模型時，存取路由器具有第 3 層感知能力，必須升級以支援 IPv6。由於存取路由器會終止由 WLAN 主機及路由器發起的 PPP 會話，因此必須支援 IPv6 的 PPPoE。下圖為 IPv6 WLAN 環境中的 PTA 模型架構圖：

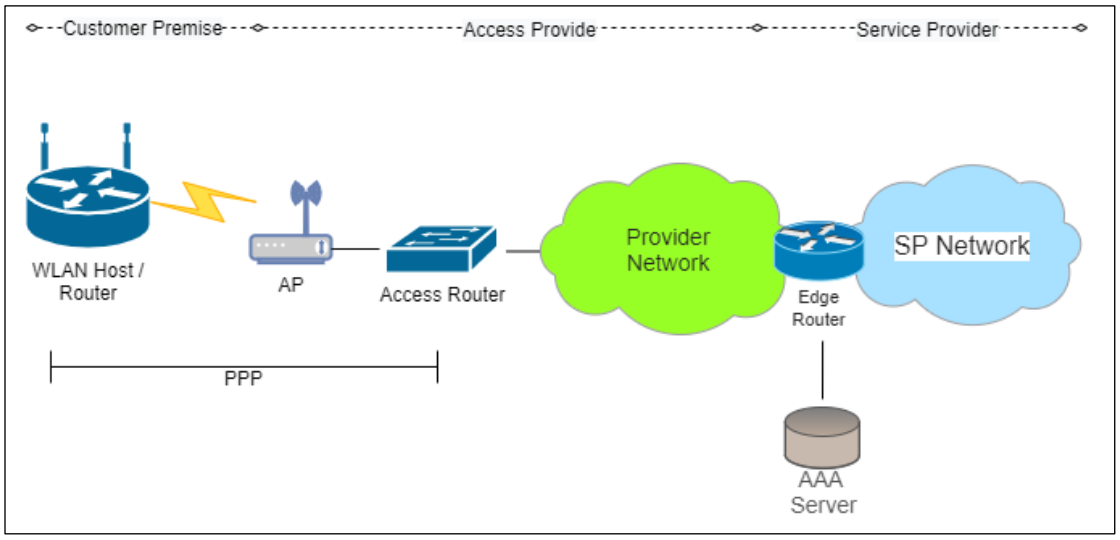



圖 172、IPv6 WLAN 環境中的 PTA 模型架構

**(1) 更改 IPv6 相關基礎架**

在此情況下，透過將 WLAN 主機、WLAN 路由器 (如果有)，存取路由器和邊緣路由器設備升級到雙協定，並配置 IPv6。

**(2) 定址**

DSL 寬頻網路描述的尋址技術也適用於 IPv6 WLAN PTA 場景。

**(3) 路由**

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

**2. IPv6 WLAN 環境中的 LAA 模型**

配置 LAA 模型時，存取路由器具有第 3 層感知能力，必須進行升級以支援 IPv6。由 WLAN 主機及路由器發起的 PPP 會話透過 L2TPv2 隧道轉發到網路提供者網路中的聚合點。存取路由器必須具有為 IPv6 支援 L2TPv2 的能力。下圖為 IPv6 WLAN 環境中的 LAA 模型架構圖：

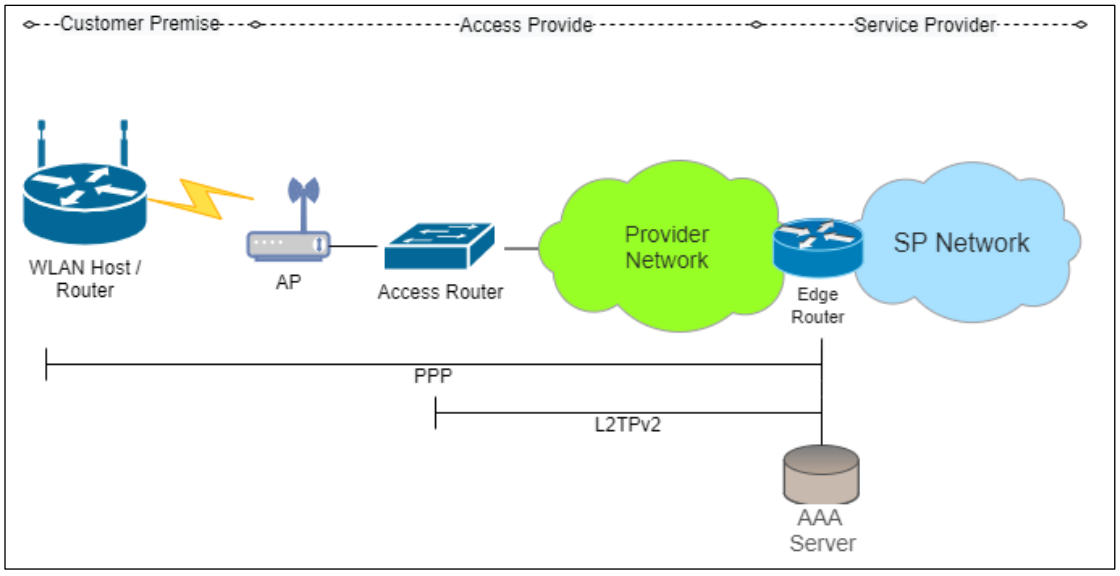



圖 173、IPv6 WLAN 環境中的 LAA 模型架構

**(1) 更改 IPv6 相關基礎架**

在此情況下，透過將 WLAN 主機、WLAN 路由器(如果有)，存取路由器和邊緣路由器設備升級到雙協定，並配置 IPv6。

**(2) 定址**

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

**(3) 路由**

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

## 二. 公眾無線網路 IPv6 QoS

雖然 QoS 是在 WiFi 區域以外進行，但整體配置還是非常重要。QoS 配置在邊緣路由器特別重要，以便管理在多個用戶與各種服務級別協議 (SLA) 的部份資源共享。然而，WLAN 主機、路由器和 Access 路由器也可構成 QoS 實現。包括適當的分類標準支援，需要在 IPv6 單點傳播和多點傳播中實現。

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

重點為當通訊進行端到端加密時，網路設備將無法存取用於分類目的的數據包字段。在此情況下，路由器可能將數據包放入默認的分類中。QoS 設計應考慮此種情況，並使用主要 IP 表頭欄位進行分類。

## 三.公眾無線網路 IPv6 安全防護

為了增強安全性，必須對 WLAN 主機/路由器進行部份更改。主機應該使用自動配置的隱私擴充，並在 WLAN 主機/路由器上啟用 IPv6 防火牆功能。

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

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

身份驗證是在實施第 3 層安全策略之前確保 WLAN 網路安全的重要面向。此有助於避免對 ND 或無狀態自動配置過程的威脅。802.1x [IEEE8021X] 提供了確保網路訪問安全的方法。但是，EAP (PEAP、EAP-TLS、EAPTTLS、EAP-FAST 和 LEAP) 以及主機支援某些功能的能力，讓實施全面一致性策略有困難。

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

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

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

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

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

## 四.公眾無線網路 IPv6 安全防護建議

以下提列無現網路 IPv6 安全防護建議事項：

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

以上 ISP IPv6 網路安全基本防護要項與 ISP IPv6 網路連線服務安全防護建議，並且針對 ISP 網際網路存取服務之固接網路、行動網路與公眾無線網路連線服務安全防護提供建議。詳細內容請參閱附錄八有完整說明。

# 第十章蒐集國內外物聯網服務實際應用案例

物聯網發展促使生活模式創新與轉型，除了為人類生活帶來全新體驗外，物聯網應用也得以有效率方式解決目前生活上或社會上所帶來問題，其應用範圍與種類相當廣泛，包括智慧運輸、智慧節能、智慧生活等各種面向。

本工作項目將透過蒐集並分析具有代表性物聯網服務與應用案例，了解國內外物聯網技術發展。從食、醫、住、行、育、樂等面向蒐集國內外物聯網服務實際應用案例。目前已完成 6 項物聯網應用案例研析。詳細內容請參閱以下說明。

## 第一節 食的物聯網 – 全程冷鏈不斷鏈管理

農產品、冰品、肉品、生鮮、藥品等在運輸過程中，需在全程低溫環境才能維持良好品質。

以往賣場食品安全管理為人工作業，賣場人員隨機抽選冷藏冷凍商品，使用感應式溫度計掃描商品溫度後，再輸入至系統中，此作業方式缺點為人工紀錄及輸入難免會有失誤，就形成食安管理作業上的困擾。

賣場客人從冷藏冷凍櫃拿取商品後忘了關門或沒有關緊，賣場工作人員無法立即發現，導致冰櫃溫度上升，間接影響到食品品質，造成商品損耗與額外電費支出。

為改善上述食品安全管理問題，研華科技提出完整的冷鏈物流解決方案，從生產製造、倉儲、配送到門店零售，其貨物的環境溫濕度將全程監控，確保運送全程冷鏈物流不斷鏈。

圖 174、全程冷鏈不斷鏈解決方案

此即時冷鏈物流，使用車載機、無線感測器，及感測器的 Android APP 和後端管理平台，在食品出廠前，業者可以根據食品所需要的環境溫度，事先設定與調整感測器參數；在食品運送途中，可同時監控食品與車輛狀態，將過程傳回後端管理平台；當食品運送到消費者或商店手上，後端管理平台也會紀錄並即時更新資料，進而確認食品運送過程中是否有缺口。下圖為此冷鏈物流解決方案系統架構：

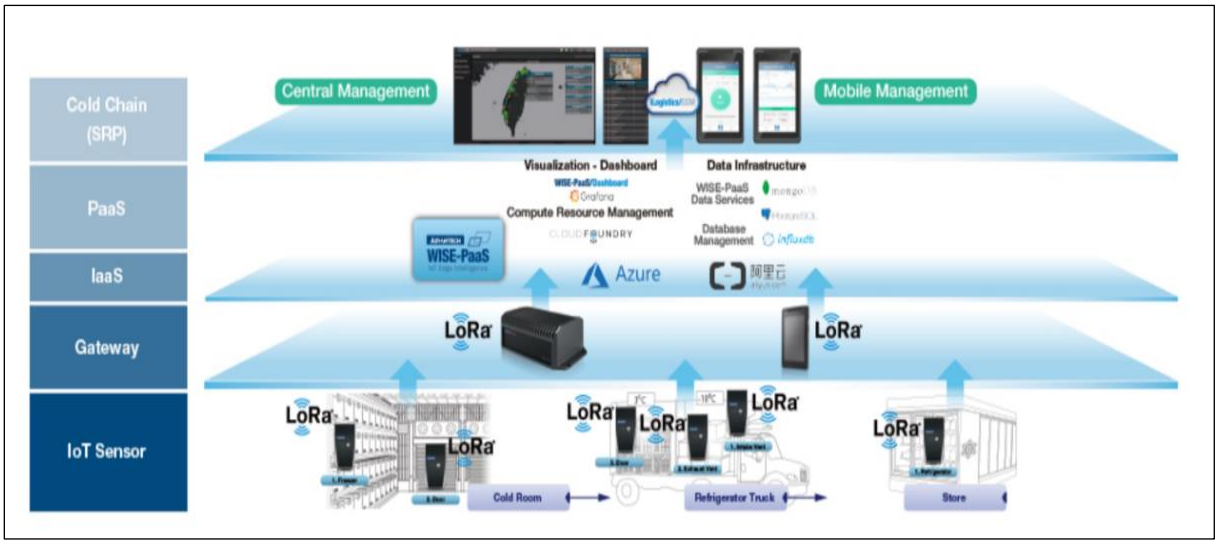



圖 175、冷鏈物流解決方案系統架構

此系統配備硬體裝置包含：

- 溫溼度感測器：

  搭載 NFC 功能，亦使用 LoRa 技術搭配閘道器可即時監控，搭配中央管理服務雲，易控管資料。用於感測環境中的溫度、濕度和衝擊力。

- 紅外線感測器：

  使用 Android 系統開發，支援多種無線傳輸，NFC 和選配 RFID Reader，內建 1 維及 2 維條碼掃描功能，1300 萬畫素相機。

- 車載電腦：

  負責搜集車上所配備感測器資訊、GPS 定位記錄等，並傳輸到雲端，進行資料收集。

透過系統開發 APP 收及感測器監測資訊，將資訊傳輸到雲端以達到即時資訊監控，異常狀況也可透過車載電腦，即時通報運送者進行檢查及處理，以確保運送過程符合標準溫溼度要求。下圖為此冷鏈物流裝置傳輸架構圖：

圖 176、冷鏈物流裝置傳輸架構

物聯網的通訊技術有很多種，如 Sigfox、LoRa、NB-IoT，在全程冷鏈不斷鏈管理中，採用 LoRa 是因為此技術無須額外頻段授權費，法規限制單純易於全球布建，且具備低功耗、可用電池供電、系統可以長時間運作等特性。另外 LoRa 技術穿透率高、傳輸距離更遠勝於其他如 WiFi 或 Bluetooth 等傳輸方式，降低系統架設成本。

雖然 LoRa 具備以上優點，但在網路安全考量須注意，LoRa 主要運行在全球免費頻段，故容易與零售通路業者的無線對講機頻段重疊，造成訊號相互干擾，因此此系統調整 LoRa 運行頻段，同時增設指令，讓感測器在傳輸資料前，先詢問目前是否有訊號佔住通道，以確保資料傳輸的品質與正確性。

此全程冷鏈不斷鏈系統適用於各種場域應用，如倉儲配送中心、醫療院所疫苗及藥品存放、零售門市溫度監測等應用情境。

與 LoRa 較相關的網路協議為低功耗廣域網路 (LPWAN)，在 [RFC 8376]：Low-Power Wide Area Network (LPWAN) Overview 文件

即為 LPWAN 概述內容，講述低功耗廣域網路 (LPWAN) 為一種無線技術，具有覆蓋範圍大，低頻寬，封包和應用層數據大小可能非常小及電池壽命長等特點。 此篇 RFC 是 IETF 正在考慮的一系列 LPWAN 技術，及此類技術的需求與在 LPWAN 中運行 IP 的目標之間存在的差距的資訊性概述內容。

# 第二節　醫的物聯網 – LincGo 服務架構與技術

LincGO 遠距心電圖平台利用雲端技術，提供全世界各地居家之心血管疾病用戶之監控。以一次性心電圖貼片取代原先高成本傳統心電圖 (Holter monitor)，降低醫院成本支出，利用 LincGO 平台可做遠端即時監控以及 72 小時心電圖，即時透過 AI 演算法篩選出高風險以及有問題之心電圖，再交由印度具有美國心臟協會認證之醫事檢驗師進行判讀以確保結果並符合 FDA (U.S. Food and Drug Administration，美國食品藥事管理局) 之要求。

LincGO 系統平台為立創智能股份有限公司所發展出一套整合心電圖監測貼片、閘道遠端通訊、雲端伺服器及醫院端系統解決方案，架構如下圖所示。此產品與服務以銷售給醫院為主，可應用於心血管疾病患者，並適用於家中、醫院門診、醫院病房等場所。使用者貼上貼片後即可開始進行心電監測，透過閘道傳輸數據到雲端，醫院端再接收傳輸資訊進行判讀。本解決方案可取代現有心電圖監測設備，協助醫院數據蒐集及分析數位化、網路化，同時提升患者使用接受度。

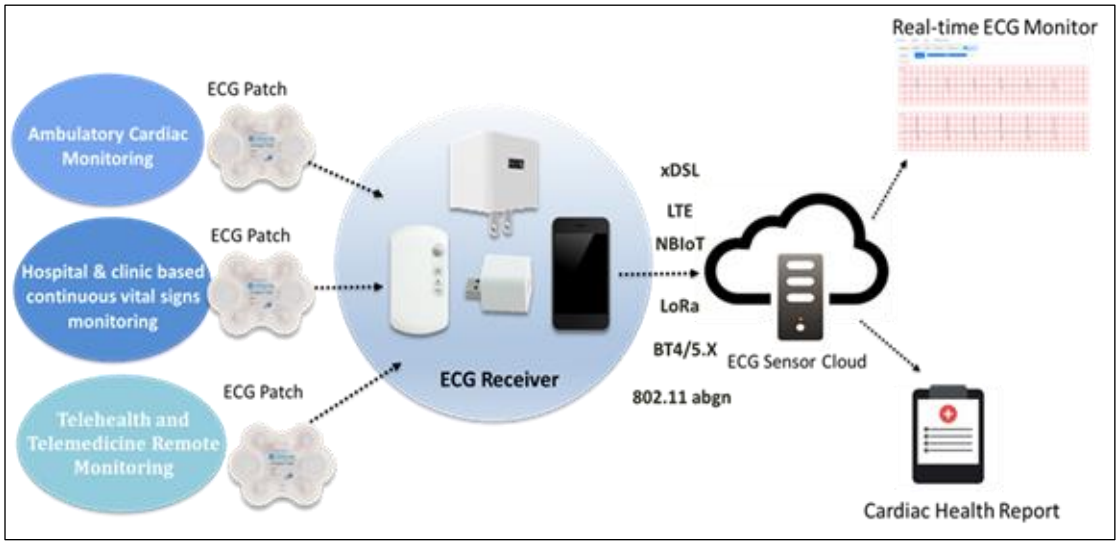



圖 177、LincGO 系統平台提供完整的解決方案

# 一.產品優勢

LincGO 系統平台具有以下優勢：

- 使用便利性：

現有心電監測器笨重昂貴，長時間裝配讓使用者行動不便，只適合在醫療院所實施。LincGO 系統平台解決方案使用者只要貼上輕薄監測貼片，在不影響作息與外觀下即可監測長達 3 天心電數值。監測完不需歸還偵測貼片，僅需簡單按鍵與介面操作即可透過閘道器和雲端系統將數值傳輸到醫院系統端。

- 提升醫療數據取得：

此系統有利於醫事研究以及醫療主管機構數據取得，可提供作為醫學研究、國人健康方析等。

- 實現預防醫療與遠端醫療：

此系統平台協助推進預防醫療與遠端醫療落實，走在醫療趨勢前端。

# 二.產品特性

此系統採用遠距藍牙連線系統連結雲端資料庫。為解決藍牙無線裝置的使用限制，提出以下解決方案。另外如何解決應用在微型處理器運作良好、設備和雲端資料連結的安全性考量等問題提出相對應解決方案。詳細如下所述：

## (一)擴大低功耗藍牙網路規模

低功耗藍牙無線裝置存在 2 個問題：

**1. 無線藍牙裝置無法直接連結**

現今低功耗藍牙無線裝置普及，其普遍使用方式仍局限於點對點連結個人區域性通訊，例如：穿戴式裝置與個人手持式裝置連結，或是居家中影音裝置與無線閘道器連結，各裝置間無法直接通訊並交換資料，裝置間所形成的網路型態屬於星狀結構，僅能透過中央閘道器或集線裝置，例如手持式裝置或個人電腦，與裝置溝通。裝置間無法直接連結。

**2. 無線藍牙網路規模難以擴張**

網路裝置之間的連結受限於低功耗藍牙裝置傳輸距離及裝置低耗電需求，並需要搭配閘道器及電力線建置來增加網路規模以及涵蓋範圍，導致無法簡易有效地將網路規模放大。

**3. 無線藍牙裝置高耗能問題**

現有低功耗藍牙無線網路連結實現方式，以透過低功耗藍牙技術中非連線類型 (connection-less) 通訊形式，此種連結類型由廣播者 (Broadcaster) 及觀察者 (Observer) 角色完成，此種技術形成網路無法有效地發揮低功耗藍牙技術中以連線類型 (connection) 所建立通訊連結省電特性，以滿足低功耗藍牙無線裝置透過小型電力裝置，如：使用 AA 電池、鈕扣電池，來驅動需長時間運作功能。

為解決上述技術問題，立創智能提出建立並監控低功耗藍牙無線網路之方法，讓多個低功耗藍牙無線裝置直接連結，建立一個低功耗藍牙無線網路。該方法包含下列步驟：

- 步驟1：控制低功耗藍牙無線裝置中之第一藍牙無線裝置由〝廣播狀態〞進入〝偵查狀態〞。

- 步驟 2：於偵查狀態中，第一藍牙無線裝置接收第二藍牙無線裝置所發送之連線要求〝廣播訊號〞，此連線要求廣播訊號包含對應於第二藍牙無線裝置之裝置識別碼。
- 步驟 3：待第一藍牙無線裝置由偵查狀態進入建立連線狀態。於建立連線狀態中，第一藍牙無線裝置根據連線要求廣播訊號以及裝置識別碼與第二藍牙無線裝置建立連線。
- 步驟 4：第一藍牙無線裝置透過連線傳送一個觸發指令至第二藍牙無線裝置以控制第二藍牙無線裝置由待命狀態進入偵查狀態。
- 步驟 5：當第二藍牙無線裝置進入偵查狀態後，就可以和下一個藍牙無線裝置進行訊息傳送和連結，如此遞延就可讓所有藍牙無線裝置直接連結形成網路。

下圖為藍牙無線裝置間，建立並監控低功號藍牙無線網路之方法示意圖。

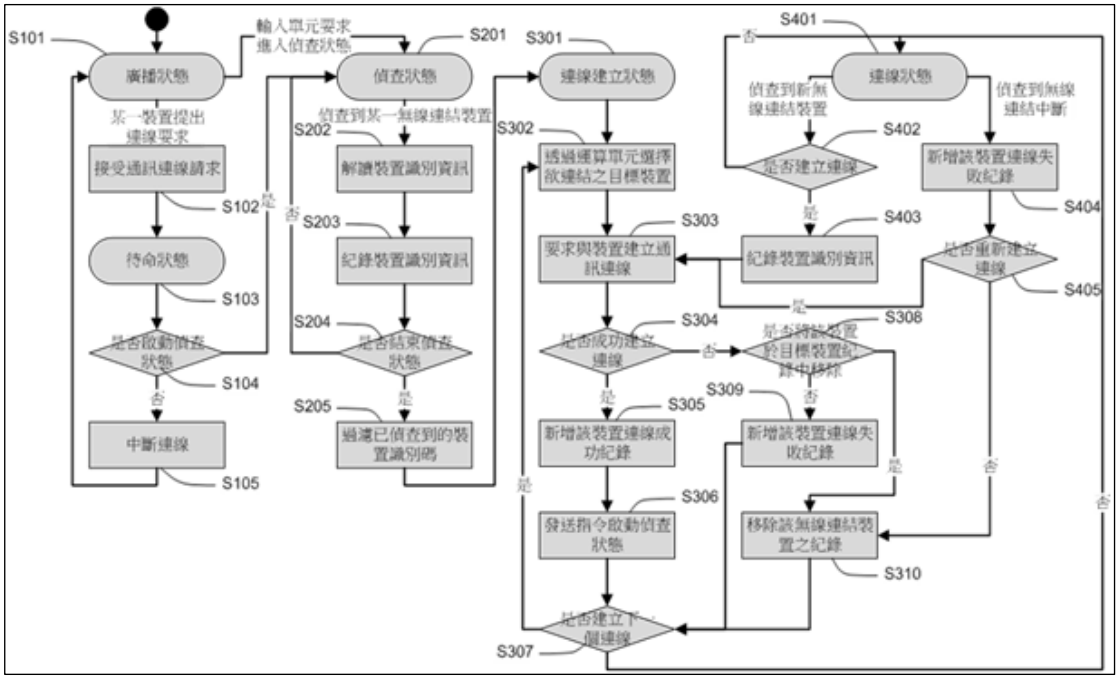



圖 178、建立並監控低功號藍牙無線網路之方法

綜合以上所述，立創智能針對建立並監控低功耗藍牙無線網路之方法，特點如下：

- 無線裝置可相互連結形成網路：讓多個低功耗藍牙無線裝置相互連結，建立一低功耗藍牙無線網路。
- 裝置可相互傳送資料：讓低功耗藍牙無線網路中之裝置可以相互交換資料，並且可透過低功耗藍牙無線網路中之任一裝置，將資料傳遞至該網路中任一其他裝置。
- 自動偵測、回復及擴充裝置連結：於低功耗藍牙無線網路系統中，可偵測連結中斷之裝置，並回復其連線。且可動態地延伸及擴充連結該藍牙無線網路的裝置數量。
- 無線網路裝置資料收集：此網路系統可對裝置進行資料收集、傳送以及分發。

## (二)延長藍牙技術的傳輸距離

使用藍牙無線傳輸技術有許多優點，但傳輸距離問題卻是藍牙技術被廣泛使用最大阻礙，雖然藍牙 4.0 版本讓裝置間傳輸距離從傳統藍牙協定 2~10 公尺提高為 60~100 公尺，但若使用於戶外空間或有建築物遮蔽空間中，通訊距離還是會受影響而縮減，降低實用性。為解決傳輸距離的問題，此平台提供一種遠端藍牙裝置通訊系統，包含管理裝置、藍牙代理裝置及藍牙終端裝置，裝置之間訊息傳遞運作方式如下所述：

- 管理裝置：透過網際網路發送網際網路封包訊息至藍牙代理裝置。

- 藍牙代理裝置：接收到此網際網路封包訊息後，將網際網路封包訊息轉譯成標準藍牙通訊封包訊息，並透過藍牙傳輸發送至藍牙終端裝置。
- 藍牙終端裝置：接收到標準藍牙通訊封包訊息後，執行標準藍牙通訊封包訊息所包含的資訊內容及命令設定之動作。

另外，也可由藍牙終端裝置向管理裝置傳送訊息，裝置訊息傳送方式如下所述：

- 藍牙終端裝置：透過藍牙傳輸發送標準藍牙通訊封包訊息。
- 藍牙代理裝置：接收並轉譯成網際網路封包訊息，然後透過網際網路將封包訊息傳輸至管理裝置。
- 管理裝置：接收封包並執行訊息內容。

此技術利用網際網路傳輸達到遠距離控制藍牙終端裝置目的，克服了藍牙無線傳輸距離限制問題。

## (三)不須安裝應用程式的藍牙閘道器

智慧型感測儀器固然方便，但需要配合相互對應的應用程式操作或存取。因此，本系統開發一種藍牙資料存取系統，包含藍牙終端裝置、藍牙閘道器及應用伺服器。各裝置運作說明如下：

- 藍牙終端裝置：用於發送廣播訊息。
- 藍牙閘道器：連接藍牙終端裝置並接收廣播訊息後，發送包含廣播訊息之閘道訊息。

- 應用伺服器：連接藍牙閘道器用於接收閘道訊息，依據閘道訊息產生並發送應用訊息。藍牙閘道器接收應用訊息，並且依據應用訊息產生並發送控制訊息以讀取或操作藍牙終端裝置。

本系統開發之藍牙資料存取系統利用應用伺服器根據不同之藍牙終端裝置提供相對應的應用程式至藍牙閘道器，使藍牙閘道器不需要內建應用程式即可動態控制或存取各種藍牙終端裝置。一般藍牙閘道器需要內建各種不同藍牙終端設備之應用程式，才能夠控制或存取藍牙終端裝置，因此此系統開發之藍牙閘道器與一般藍牙閘道器相比，不但能節省儲存各種應用程式之記憶體空間容量，更可以讓使用者在不需主動安裝情況下，就能便利操作各種不同藍牙終端裝置。

## (四) 因應網路服務之雲端伺服器架構

實務上 LincGO 系統平台網路服務必須穩定不能斷線。因此本系統需要設計良好網路架構、雲端架構及備用系統，以建構高信賴度的網路服務。此外還需要設計良好防止駭客攻擊的架構與權限設定，才能維護患者的病情隱私，方便醫院單位管理。

除此之外還需考慮滿足大量用戶使用情境。所以，雲端伺服器的架構設計影響層面非常廣，不僅是 LincGO 系統平台的服務核心中樞，也是系統能否維持高品質及運作良好的根本。

## (五) 因應貼身微型醫材之程式碼編譯

現今科技已經可以做到極微型且效能極高處理器，並大量應用在智慧型手機當中。但高功率處理效能伴隨產生高溫度熱能，一般

智慧型手機執行溫度可能落在 40~45℃。但人體皮膚直接接觸超過 40℃物件時，不但會有不適悶熱感，持續接觸超過兩小時以後，即可能造成低溫灼傷 (Cryogenic burns)。

為避免低溫灼傷，此產品心電監測貼片使用低功率處理器及低耗能藍牙傳輸，還須降低電磁波強度，以符合 FDA 醫療器材標準。低功率處理器與記憶體，及其他硬體上限制，使得心電監測貼片不能有效執行複雜程式指令。因此，完成功能齊全，且指令精簡程式碼，也是此解決方案特色之一。

## (六)執行於雲端之手機應用軟體

不同用途藍牙裝置所需藍牙應用層通訊協定並不盡相同，所以各種藍牙裝置分別支援有不同組合通訊協定，也衍生出各自對應的 APP。此平台透過雲端虛擬裝置，模擬手機執行供應商提供 APP 來解決此不便的問題。

此平台開發出一種遠距藍牙連線系統，包含有藍牙閘道器、藍牙設備、雲端虛擬裝置以及藍牙應用程式。運作方式如下所述：

- 藍牙設備：設置於藍牙閘道器之服務範圍內。
- 雲端虛擬裝置：包含有藍牙虛擬層模組及通訊模組。藍牙虛擬層模組提供藍牙程式介面。通訊模組用以建立網路連線至藍牙閘道器。
- 藍牙應用程式：執行於雲端虛擬裝置，透過藍牙程式介面經由藍牙虛擬層模組建立網路通訊控制藍牙閘道器服務範圍內之藍牙設備，或讀取藍牙閘道器服務範圍內之藍牙設備所量測之數值，該網路通訊方式可為藍牙、有線網路、無線區域網路或行動通訊網路。

遠距藍牙連線系統透過雲端虛擬裝置模擬手機安裝並執行藍牙應用程式。因此可解決手機安裝執行應用程式時耗費流量、記憶體及處理器資源問題。藉由藍牙虛擬層模組提供藍牙閘道器與藍牙設備連線所需之指令集。接著透過藍牙閘道器轉換，實現雲端虛擬裝置對藍牙設備的遠端操作。尤其，執行於雲端伺服器的雲端虛擬裝置可以被設定自動與藍牙設備溝通，無須人為操作。甚至，可以讓多個使用者分別使用不同智慧終端登入雲端伺服器，以相同藍牙應用程式操作藍牙設備。

藉由此技術，可以解決部分應用情境中監測貼片讀取到數據需要即時傳輸出去的問題。此應用下不須有終端裝置隨時與監測貼片連線準備接收數據，而是透過閘道器到雲端伺服器接收儲存數據。此外，也不需要長時間開啟智慧終端以操作監測貼片，減少麻煩，提升待監測者使用意願。

# 三.產品應用

## (一)技術或服務應用範圍

此服務可應用於心血管疾病患者、心臟內外科就診者、健康中心定期檢查者、或自覺心臟不適未確診民眾。應用檢查方式可以是運動心電圖、靜態心電圖或全天 24 小時心電圖檢查。使用場域適用於家庭、療養院所、醫療機構一般病房或重症病房。

LincGO 系統平台最主要應用為，就診者受醫師指示進行全天 24 小時心電圖監測，即刻在醫院安裝監測貼片後返家。24 小時之後監測結束，就診者透過住家閘道器或安裝對應軟體手機上傳心電圖數據到雲端。再由雲端伺服器傳輸資料到醫院資料中心。可

利用對應貼片編號或是手機設定以讓醫院資料中心將心電圖資料歸檔至該就診者。

## (二) 實用價值性

LincGO 系統平台還可以進一步提供五種衍生服務，各服務應用情境描述如下：

### 1. 商業合作模式

LincGO 系統平台在不同的商業合作模式之下，可以應用於心血管疾病病患住在醫院病房，或是就診者在心電圖室進行靜態心電圖檢測或運動心電圖檢測時使用。住院病房和心電圖室有預先設定好的院內閘道器，檢測完成後，透過院內閘道器將資料傳輸到雲端伺服器。再由雲端伺服器傳輸資料到醫院資料中心。

### 2. 預防醫療及遠端醫療

此系統平台延伸第二種服務應用於預防醫療與遠端醫療。當使用者自覺有心血管症狀，或是欲進行定期檢測。此時使用者不須到醫院掛號進行診斷，僅需直接至藥局或相關合法機構購買監測貼片。使用者透過安裝對應軟體的手機或閘道器操作，可設定貼片的檢查項目係為靜態心電圖、運動心電圖或 24 小時心電圖。閘道器接收心電圖資料並且附加上使用者輸入其他資訊，再傳輸上述資訊至雲端伺服器。依據使用者設定，雲端伺服器可以傳送最終資訊給醫院、相關醫療人士或親友、或使用者手機。此種服務最能落實預防醫療與遠端醫療。

**3. 多種終端監測器**

第三種加值應用需更多種終端監測器，例如血糖監測器、血壓監測器、血氧監測器等。監測器可與心電圖監測貼片共用同一個閘道器與雲端系統。由監測器上得到數據與心電圖監測貼片數據合併後，更有助於醫事人員對使用者的病情掌握與診療判斷。提供更多檢測種類服務。

**4. 人工智慧判斷系統**

此應用需要在雲端伺服器中建立人工智慧判斷系統，並在雲端伺服器中將心電圖數據透過智慧分析判斷產生初步可用資訊。可應用在心電圖室中，人工智慧產生該使用者心電圖報告，包含異常狀態時間、異常波形間期等資訊彙整。心電圖室醫檢人員不須再從頭製作報告，僅需具名確認報告正確性即可。

**5. 即時 (Real-time) 監測**

此應用也是在雲端伺服器中建立人工智慧判斷系統，但此人工智慧重點在即時 (Real-time) 監測。應用在加護病房或重點觀察病患當中，當病患心電活動發生異常狀態，雲端人工智慧發現數據中產生較大差異值，立即通知相關醫護人員對病患進行關切及醫療處理。

# 第三節 住的物聯網 – 雲端智慧綠能管理系統

東海大學電子計算機中心數據機房建置雲端綠能管理系統，以降低數據訊息中心之 PUE (Power Usage Effectiveness，電力使用效率)與整體用電量為目標。此系統以數位電錶對用電設備進行資料收集，並搭配環境溫濕度與 $CO_2$ 資訊，提供使用者以圖型化界面呈現以利資料分析。透過系統紀錄與用電分析，可隨時隨地以行動裝置對用電設備進行監看。此外，運用大量資料處理與分析架構為基礎，建置一個用電端綠能管理需求為核心的應用服務平台。

## 一.系統架構

此系統提出的雲端系統中有 3 個層面如下圖所示，分為基礎設施 (Infrastructure)、應用平台 (Platform) 及軟體服務 (Service)。

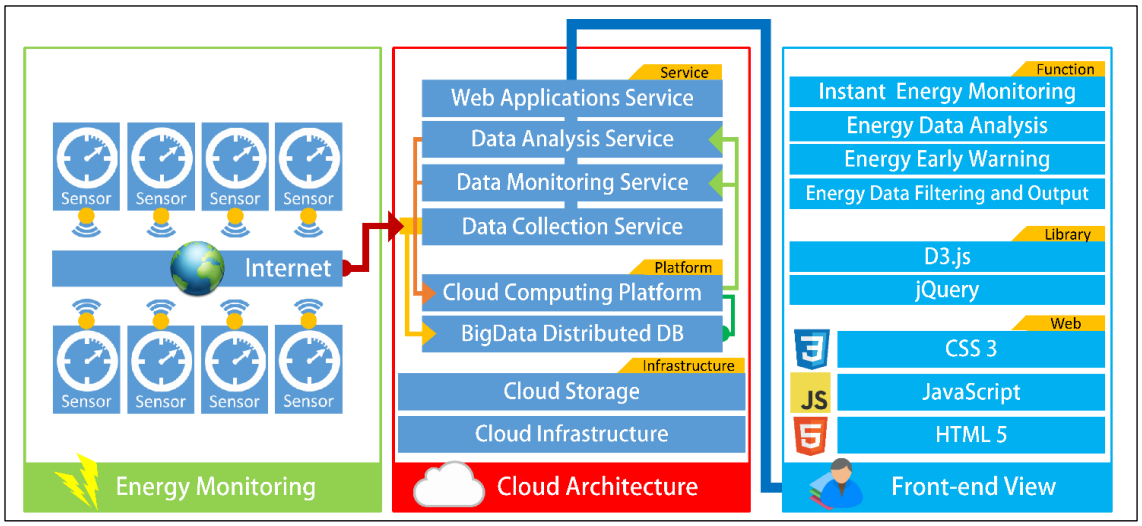



圖 179、雲端綠能管理系統架構

基礎設施是整個雲端系統的基底，此部分提供虛擬機的部署架設及管理，增加整個雲端系統基礎設施可擴充性，此系統累積下來資料

量非常龐大，日積月累資料量需要一個可以延伸擴展基礎設施。這些基礎設施之上架設分散式大數據資料庫 (Big Data Distributed DB) 連結雲端資料計算平台 (Cloud Computing Platform) 提供所需要使用到的資料到應用平台，這些應用平台儲存來自智慧電錶所產生的資料，也提供分析服務所需要計算資料。以上提到基礎設施和應用平台，都算是整個雲端系統中較底層功能，重點在讓每一個環節都有良好延伸及擴充功能，達到降低成本和資源可以獲得最有效利用。

整個雲端系統提供服務的部分為〝軟體服務〞。主要分為 4 項服務如下表所示：

表 98、雲端綠能管理系統軟體服務

| 序號 | 軟體服務 | 說明 |
|---|---|---|
| 1 | 資料蒐集 (Data Collection) | 當智慧電錶產生出資料時將透過此項服務存到資料庫中 |
| 2 | 資料監控 (Data Monitoring) | 即時性監控儲存在資料庫中的電力資料，並做出對於電力設備預警或即時電力切換等動作。 |
| 3 | 資料分析 (Data Analysis) | 將電力資料加以處理後變成有意義資訊，提供網頁服務上產出報表或是圖像式資訊，供管理者判讀。 |
| 4 | 網路應用程式 (Web Applications) | 將資料蒐集、資料監控和資料分析加以應用提供前端使用者操作的使用者網路介面服務。 |

## 二. 系統設計

為了實作雲端用電大量資料平台，此系統設計了 4 種服務，分別是資料收集、資料監控、資料分析及網路應用程式服務，功用如上表所述。以下針對各服務設計說明：

- 資料收集服務 (Data Collection Service)

資料收集服務是一個常駐服務，主要負責接收從網際網路傳送來的資料封包，並將資料做基本篩選後存入大數據資料庫 (Big Data Distributed DB) 中，同時不間斷傳送資料串流至資料監控服務。對於此系統平台而言，電能資料從感測器接受，透過無線傳輸至收集器後，將會使用網際網路方式傳送到此系統之雲端架構，由電能資料收集服務來負責收集，經過初步篩選將不需要存入資料去除，因應資料上感測器 ID 存入相對應資料表中完成資料收集，並傳輸至監控服務做後續應用。

電能資料收集服務是一個 Java 的 Web Service，此系統透過 Java 接收由網際網路傳送來的資料，並且檢查感測器 ID 是否為註冊於本系統的 ID，如果檢查結果為是才將資料收集暫存於記憶體中。

- 資料監控服務 (Data Monitoring Service)

為系統中的常駐服務，主要負責監控此系統大數據資料庫的資訊，並藉由監控規則及預警規則對資料做基本篩選及規則比較，回傳網路應用程式 (Web Applications Service) 提供前端使用者資訊及通知。其中由前端使用者傳送來的監控規則，將資料透過使用者設定的規則或點選頁面規則進行篩選或統計成使用者需要資訊回傳，例如:使用者點選系統即時電量監控頁面，透過網路應用程式服務對本服務提出需求，在接收需求後本服務將透過相關規則後自大數據資料庫中查詢並且篩選資料後做基本的統計後回傳資料。

資料監控預警部分也是由本服務負責，本服務讀取系統中設定監控預警規則，定時對設定的特定資料不斷掃描比對預警規則並在資料超過設定範圍後做出預警，例如:使用者對某幾個感測器電壓感測設定預警，則系統在掃描資料時，就會對於設定的感測器電壓資料做比對，若有超出使用者設定範圍則會做出預警。預警通知部

分可以直接透過網路應用程式服務，對於正在瀏覽網頁使用者發出通知、寄送通知至設定的電子郵件信箱或透過發送簡訊通知等方式進行通知。

- 資料分析服務 (Data Analysis Service)

為系統中的非常駐服務，主要作用是分析儲存於此系統中的大數據資料庫中的電能資料，透過使用者指定資料分析規則，或系統提供的資料規則分析大數據資料庫中的電能資料，並將分析的資料回傳此系統中的網路應用程式 (Web Applications Service) 並顯示於前端介面中，透過分析電能資料能提供使用者相關的有用資訊。比較特別的是本服務並不會常駐於系統中，為了不必要的資源浪費，本服務僅會在使用者有需求時透過其他服務通知喚醒，並分析資料。

- 網路應用程式服務 (Web Applications Service)

為系統中常駐服務，主要提供系統與前端網頁介面資料交換以及作為讓使用者實際操作整套系統的中介，是此系統中非常重要的服務之一，此服務能直接調用資料監控服務 (Data Monitoring Service) 及資料分析服務 (Data Analysis Service) 以達成系統提供的各種功能，透過由前端網頁介面對本服務發出的 HTTP POST 或者是 GET 請求，本服務針對 HTTP 請求的類別經過使用者身分驗證後，將針對發出的請求資料透過設定系統功能的對應，調用資料監控服務或資料分析服務處理，並且等待其他服務處理完成將資料回傳本服務，在收到其他服務的資料後，根據資料格式做編碼及基本篩選並將資料格式回傳至前端網頁介面，顯示於網頁讓使用者得知資訊，例如:使用者想了解現在即時用電資訊，前端網頁介面就會透過傳送請求至網路應用程式服務，網路應用程式服務會根據需

求調用資料監控服務做資料查詢，等待資料監控服務回應後便會依照網頁回傳格式轉換格式後，將資料回傳於網頁透過網頁顯示。

## 三.系統成效

本系統架構分為 3 個部分，包含使用者介面 (User Interface)、雲端系統 (Cloud System) 及電能監控 (Energy Monitoring)。各部分功能說明如下：

- 使用者介面：

包含 Widget 和 Browser。分為手持設備使用者介面及網頁介面 (Browser)，兩者皆需向雲端系統內的分散式網頁伺服器取得相關資料及相關操作，透過網頁伺服器向關聯式資料庫 (MySQL) 進行資料讀取，或進行設定及控制操作 (透過 SQL Node 進行)，在網頁伺服器上及資料庫中的內容，每天需進行備份動作，確保資料完整性。

- 雲端系統：

包含各項網頁應用、資料分析、資料監控及資料收集。雲端平台讓使用者透過網頁介面來檢視資料中心即時能耗資訊，也提供顯示不同區域個別耗電量，讓使用者清楚了解即時耗電狀況。

- 電能監控：

電能監控部份由廠商提供技術，透過 ZigBee 傳輸協定收集機房伺服器迴路資料與空調用電資訊。

建置此系統最重要目的是收集用電相關資訊並加以分析，以達成節電目標，各類資料收集及用途如下所述：

- 伺服器運作狀況：

資料中心伺服器運作監控部分，平台提供伺服器監控儀表板，顯示資料中心伺服器運作狀況、異常運作伺服器清單及整體資料中心運算資源使用比例，可提供管理者在高負載狀況下進行資源調配參考。

- 用電資訊統計及監控：

提供每月份電費紀錄及當月份累計用電與當月用電即時估算，並且能透過每月電費比較表查看各月份用電詳細資訊及 PUE。用電比例頁面能讓使用者了解每一月份的每一天伺服器與空調個別耗電比例，用電 PUE 能讓使用者檢視每月份及每一天的用電 PUE，讓使用者對於機房能源效率做檢視，可用於節能改善後驗證不同節能方法對於機房降低耗能比較依據。

- 歷史用電紀錄比對及分析：

為了達到比較資料中心收集到的多樣化數據，平台提供使用者能對資料做不同交叉比對，將資料中心伺服器用電、空調用電、環境溫度、環境濕度、PUE 等數據放在一起比較，且對數據做倍數調整使得每項數據能夠接近，由此能透過可視化圖表發現各種數據存在一定關聯，例如:當空調能耗增加時溫度與濕度有明顯下降，在用電資訊分析部分可以比較多日後能發現伺服器用電尖峰等資訊。

雲端平台之伺服器功能除了提供資料中心整體概況檢視外，透過直接將各伺服器擺放位置呈現於頁面上，並提供各台伺服器狀態查看、運作負載、網路負載、磁碟 IO…等資訊，能夠提供管理者及維修人員很清楚對照及歷史資訊檢閱。平台也提供各智慧型插座資訊檢視及

控制，利用平台頁面不僅能讓管理者檢視各迴路用電狀況，也能夠在需要時候直接透過平台網頁控制。

以此系統資料為參考，在機房建置一條冷熱通道，讓冷氣集中重點冷卻伺服器區域，就不需要啟動多台冷氣維持整個機房冷度。此外，個別伺服器耗電量監測數據更讓耗電高機器現形，電子計算機中心已陸續關閉原有大型伺服主機包含兩部使用分別將近 11 年與 8 年的 Sun Fire 6800 Servers 與 13 台 Sun Servers，並將原有系統轉換至 VMware 虛擬化平台，達有效降低 PUE 與電能浪費，機房整體用電成本明顯下降。因為冷熱通道啟用後及淘汰老舊伺服器後用電情形有所改善。

東海大學電算中心建置此電能管理系統，透過數位電表對用電設備資料收集，成功降低 PUE 與節省用電。從西元 2015 年 (民國 104 年) 9 到 12 月共可以節省電費約 9 萬元，預估一年可以節省 30 萬元電費。

## 四.獲獎紀錄

以下為本系統獲獎紀錄：

- 於民國 103 及 104 年連續二年榮獲科技部工程司度電子資通領域應用型產學計畫「產學傑出獎」。
- 刊登於科技部工程司產學計畫優良成果專刊 148 期。
- 刊登於科技部工程司民國 104 年度產學計畫優良成果專刊。
- 科技部工程司產學計畫優良成果應用成果獲專文報導。

東海大學於民國 104 年舉行東海博雅雲展示暨智慧綠能機房啟用儀式，正式宣告東海大學資訊化邁入新里程。

# 第四節 行的物聯網 – 中華電信智慧停車場

中華電信積極布局 5G 智慧化應用，與交通部高速公路局聯手，在國道服務區建立「智慧停車資訊服務系統」，也與部份城鄉共同合作，在旅遊區導入智慧停車方案，將人、路、車三者透過 5G 物聯網技術進行無縫銜接，提供即時交通資訊。

此智慧運輸服務系統，整合通訊、電子、導航、資訊、電腦及控制等先進科技技術，將各縣市路邊停車資訊服務整合物聯網技術、地磁感應、行動通訊、CMS (資訊可變標誌，Changeable Message Sign) 等技術，提供即時路邊停車位及路外停車場空位狀況。下圖為此系統架構圖：

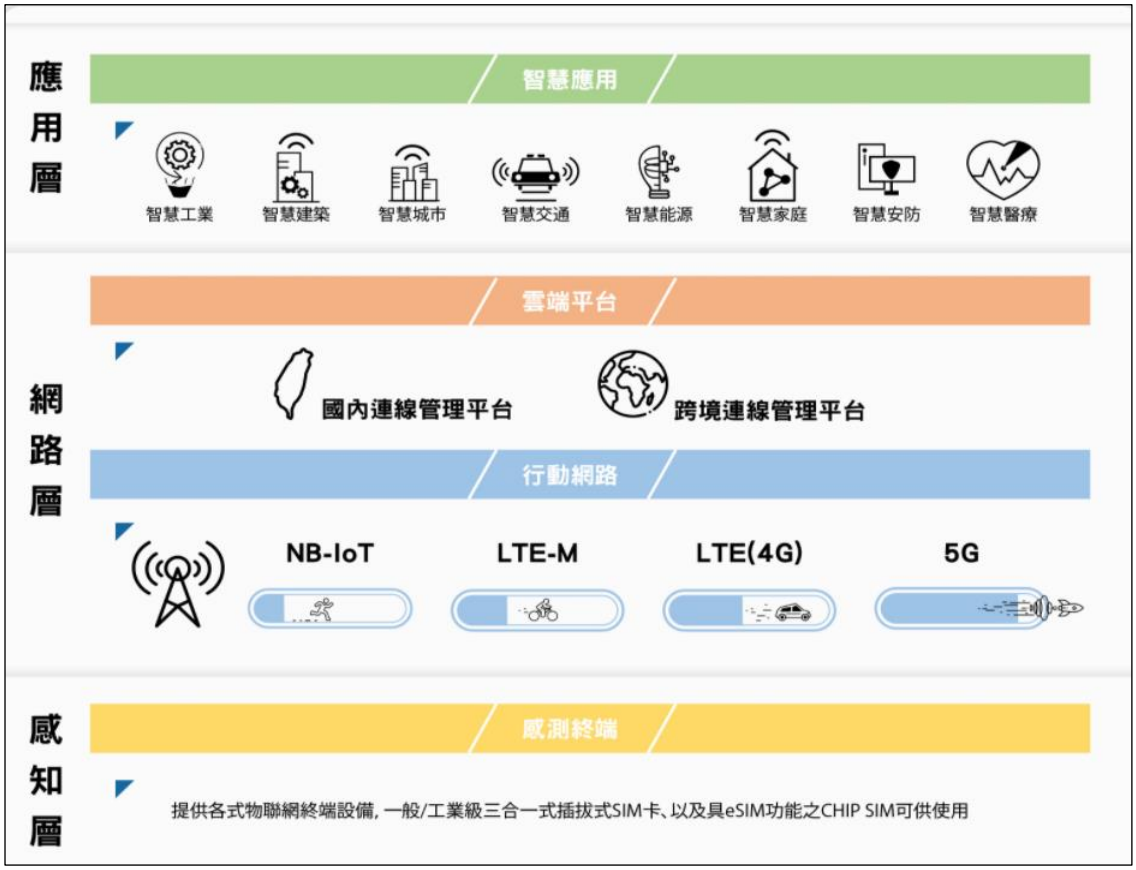



圖 180、智慧停車場物聯網架構

此服務系統依物聯網架構劃分，可分為：

- 感知層：設置各種感測設備如地磁感測或攝影鏡頭等。
- 網路層：使用 NB-IoT 技術並連接雲端平台。
- 應用層：終端應用智慧停車場。民眾可使用手機 APP 或電腦連上網頁進行即時停車資訊查詢。

透過安裝於每格停車位的智慧感測器進行偵測 (地磁在席偵測技術)，當車輛進出造成磁場變化時，即透過 NB-IoT 通訊網路傳送至雲端計算，即時資訊傳遞至智慧停車管理平台，發佈車位資訊至道路旁數位電子看板和停車資料查詢網頁，提供民眾查詢使用。

智慧停車管理平台，可從手機 APP 觀看或是電腦操作網頁觀看資訊，皆可由有線或無線網路方式連結，網頁藉由 HTTPS 方式傳輸。

感測器資訊使用 NB-IoT 技術傳送，行動物聯網無線技術除有 4G LTE 外，3GPP 依據不同裝置需求，發展出低功耗、低成本、廣域覆蓋及大量終端設備連結等特性的窄頻物聯網通訊協定 (Narrow Band Internet of Things，NB-IoT)，使現有 LTE 頻段技術中，直接共享 4G 頻段網路，透過已建置 4G 基地台，直接升級韌體版本為 NB-IoT 或 Cat-M1，藉此達到信號全台覆蓋。根據物聯網應用類型及適用網路通訊協定分類主要為：

- NB-IoT：優勢為較適合在少量封包傳輸設備、非即時資料傳輸應用。
- Cat-M1：因可維持基站交握，對即時性資料傳遞與中等流量封包傳輸，更可以適用在移動物件追蹤等特色產品。
- LTE-M：可讓移動設備持續與不同基地台的訊號做連接，在即時性資料傳遞與中等流量封包傳輸可以提供最佳的通信品質，適合在移動物件追蹤等應用。

下圖為物聯網應用類型及適用網路通訊協定分類：

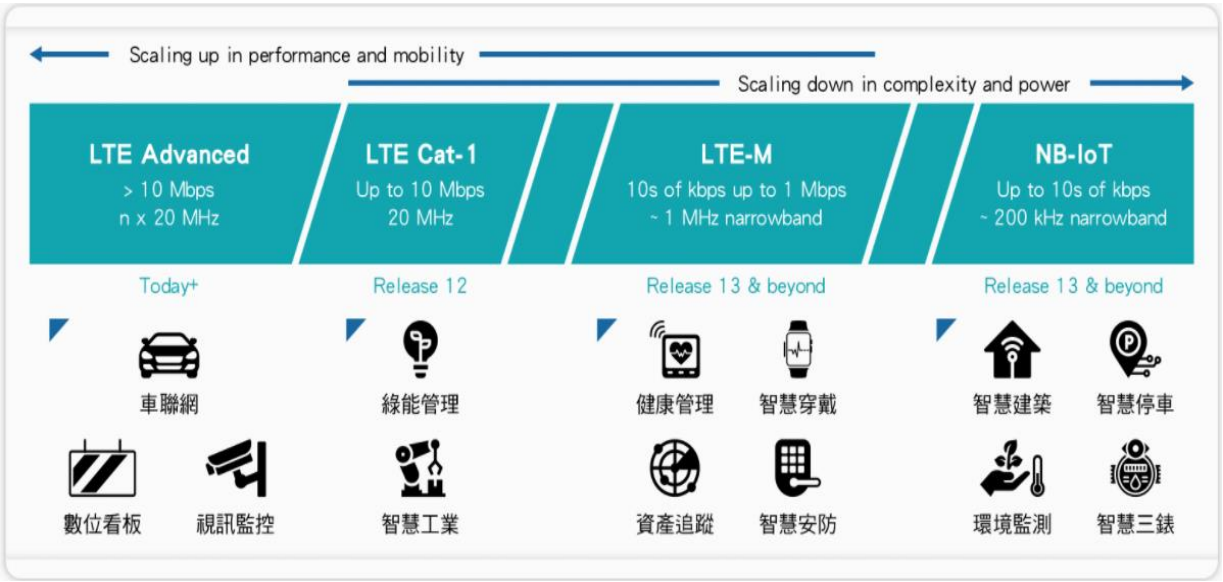



圖 181、物聯網應用類型及適用網路通訊協定分類

[RFC 8376]：Low-Power Wide Area Network (LPWAN) Overview 文件，即是描述低功耗廣域網路 (LPWAN) 概念，文件中提及 LPWAN 技術， NB-IoT 即為其中之一，此文件提及 NB-IoT 具體目標、傳送資料格式、傳送方式與限制、該如何部署等資訊。

針對網路安全考量，物聯網服務常見問題為設備連線異常、成本控管、安全漏洞及營運成本考量等，因此本系統為協助企業客戶解決以上問題，由中華電信自主研發推出具電信資安等級的物聯網連線管理平台 (Connectivity Management Platform，CMP)，支援客戶物聯網設備之網路連線自主管理功能，如連線狀態、異常通報、服務內容調整等，以提升客戶維運效率，並有效降低成本。

本系統服務案例包含國道服務區停車場系統、宜蘭縣路邊停車資訊服務等。

# 第五節　育的物聯網 – 工業 4.0 模擬研發實驗室

在教學現場不易隨時接觸到實體工廠運作架構，也難接觸到大型機器整體運作流程及概念，並進行實際操作，而慧魚工程模組希望透過小型教學模擬組件，讓教學現場能有擬真環境，了解工廠實際運作流程，從下單、製造與傳輸，模擬工業數位化過程等，創造和實體工作運作接軌的教學環境。

國內外已經有多家業者如：Siemens、Audi、BMW、台灣漢翔航太等，採用慧魚工程模組進行工程與生產線模擬與開發。台灣則是由柯達科技作為總代理商。

此套自動化模擬工廠，包含模組有：顏色分類與檢測生產線、真空吸物機械手臂、自動化高架倉儲系統、物聯網工廠感測管理模組、軸機械手臂、傳送帶、控制器等，充分展現工廠生產流程、端對端溝通、生產數據蒐集與分析。下圖為慧魚工程模組自動化模擬工廠產品實體圖：

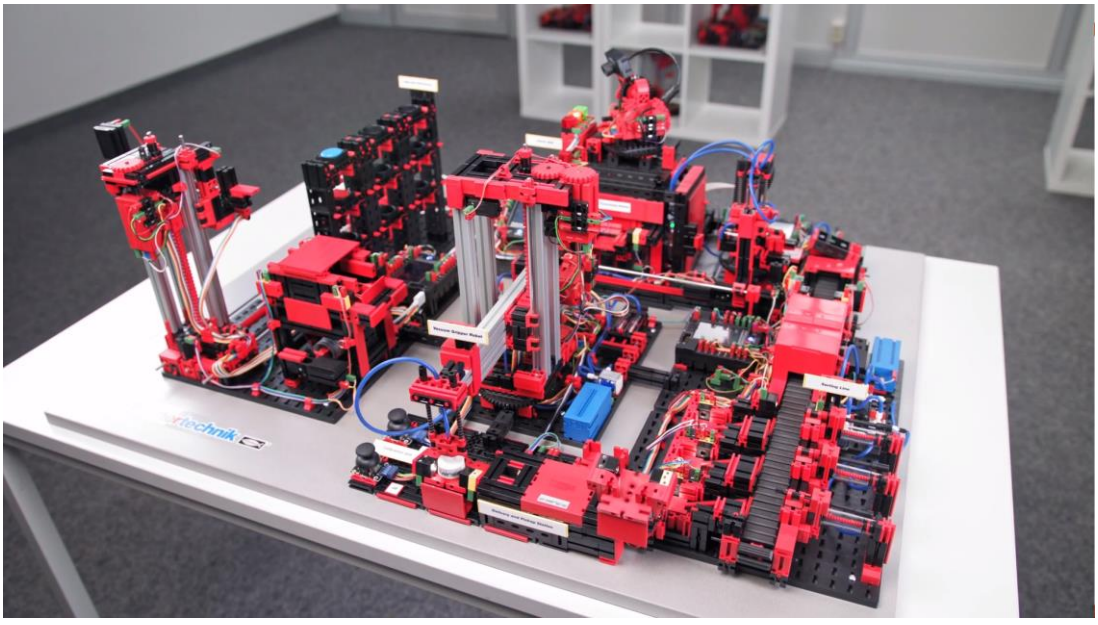


圖 182、慧魚工程模組自動化模擬工廠

以下針對各模組簡要說明：

- 顏色分類與檢測生產線：

  當顏色感測器測到輸送帶上有物件時，會依物件顏色不同讓氣缸運作，將不同顏色的物件推到專屬位置。

- 真空吸物機械手臂：

  機器透過限位開關來決定是否啟用，使用步進馬達做為移動幅度計算，可以快速及精準動作，把物件放置到預設環境中，常與其他模組同時使用。

- 自動化高架倉儲系統：

  透過限位開關控制機器啟動，利用步進馬達計算移動幅度，利用傳動機構、感應器偵測及程式控制，把物件存放於貨架上。

- 物聯網工廠感測管理模組：

  此模組含可轉動攝影鏡頭、環境感測和其他感應器，可測量溫度、濕度、氣壓、空氣品質、音量及環境光源亮度等。主要功能為模擬工廠監控設備，隨時注意廠內狀況。

- 機械手臂：

  利用限位開關控制啟動，能精確且快速動作，並將物件放置或夾取於工廠運作環境中，此機械手臂可以 3 軸運動，其活動範圍可旋轉、前後運動、上下運動，可透過脈衝感測器對力量的脈衝作出及時反應。

- 傳送帶：

  可以拼接成任何長度，模擬物件可在傳送帶上被來回傳送。

- 控制器：

  控制器可經由 Micro SD 卡擴充，配備彩色觸碰螢幕、無線裝置、紅外線二極管針對慧魚控制設置發射器，設有 USB 接口、

攝影機插槽、控制器擴充。透過面板顯示可監控各種傳感器數據,控制攝影機動作,如果環境中件測器感應資訊超過設定值,控制器液晶螢幕會顯示異常，發出警示訊號。

除硬體模組外，此系統並開發相對應軟體服務，軟體介面依三個觀點設計：

- 客戶端觀點，

  網路商店與購物車，用戶可藉由此介面模擬下單訂購，並追蹤目前購物狀況。

- 供應端觀點

  主要顯示下單狀況與出貨進度。

- 製造端觀點

  可以顯示生產區域的環境參數如：空氣品質、溫濕度、氣壓等。工廠狀況、出產進程、倉庫狀況，NFC 或 RFID 感應數據查詢。

在模擬工廠上控制器連接在工廠各個模組，是透過 MQTT (Message、Queuing Telemetry Transport，MQTT) 達到彼此間互動。控制器支援藍牙、WiFi 等傳輸協定，其資料傳輸可透過 USB、藍牙或 WLAN 連接，而控制器與控制器間使用 MQTT 協定進行傳輸。下圖為慧魚工程模組裝置間連接架構：

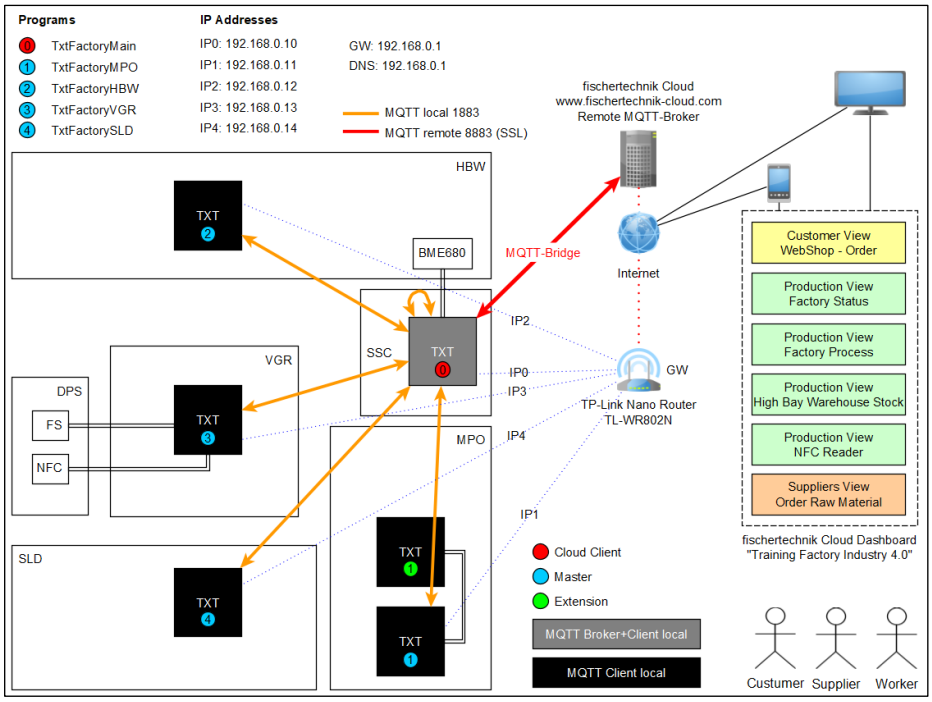



圖 183、慧魚工程模組裝置間連接架構

MQTT 訊息佇列遙測傳輸，於西元 1999 年由 IBM 發明，目的為解決在狹窄網路頻寬與微小電力耗損前提下，提供輕量、可靠的二進制通訊協定。於西元 2014 年正式成為開放的 OASIS 國際標準。適用於設備通訊 (Machine To Machine，M2M)和物聯網環境。

在網路安全考量上，MQTT 預設連接埠為 1883，加密連接埠為 8883。通過雲端連接資料傳輸會經由 8883 埠加密傳送，而藉由閘道器連接至網際網路，則透過 HTTPS 方式利用 SSL/TLS 加密封包再傳送，以保障資料傳送安全性。

此教學模擬系統目前已有多家大專院校採用，如元智大學工管系、健行科技大學工業管理系等。

# 第六節 樂的物聯網 – 智慧導覽與實境遊戲平台

導覽服務對於博物館、美術館有一定需求，隨著網路科技技術不斷更新，傳統的導覽方式已轉變，當人手一支手機，利用 APP 或網頁，隨時連接網路或事先將資訊下載，可立即進行舒適導覽體驗。蹦世界及根據此需求，建置全台首創結合 LBS 定位技術衍生服務和 AR 擴增實境冒險遊戲，為旅遊景點推出數位化創新導覽服務。

場域的佈建利用 Beacon 與 GPS 做定位，將 Beacon 裝置佈建在導覽園區各個角落，使遊客到達園區時，藉由行動裝置得知自身所在地點與園區內可行走路線，在室外有 GPS 定位，室內則透過 Beacon 裝置進行定位，Beacon 為低功耗藍牙裝置，精準度可至 1 公尺，彌補 GPS 只適用戶外定位缺點。

應用端用戶可使用行動裝置相機掃描展品旁之 QRcode 獲取展品相關資訊，在智慧解謎遊戲應用上，可用以找尋線索，透過行動裝置相機，對周圍環境感測後，對應到相對場景，即可觸發 AR 虛擬實境動畫。下圖為線上智慧導覽網站截圖：

圖 184、線上智慧導覽網站截圖

使用 APP 操作，比網頁瀏覽增加多種功能，並可以和遊客增加互動。以下為各功能作介紹：

- 多元族群：視障人士若到達地點自動產生口述語音、藉由語音引導行進方向；錄製手語影片供聽障人士觀賞。
- 自動介紹：運用 Beacon、GPS，遊客只需接近展覽品，語音、文字、圖片資訊即會自動跳出。
- 定位導航：利用 LBS 服務，在園區內不管室內室外即可藉由 APP 地圖為自己導航。

圖 185、自動介紹與定位導航

- 多國語言：提供多國語言翻譯錄音。
- 即時通知：發出訊息通知遊客最新消息，增加遊客回訪頻率。
- 電子集章：利用室內外定位技術讓遊客走到哪集到哪。
- AR 擴增實境：使用擴增實境技術，結合科技與展覽。

此智慧導覽應用系統採用 Wi-Fi、4G-LTE 與藍牙 Beacon 室內定位。利用 Wi-Fi 可從範圍內的無線網路連接到網路，Wi-Fi 保護存取加密 (WPA2) 提供安全連網環境，能讓用戶使用高強度密碼。而 Wi-Fi Multimedia (WMM) 協定，讓 Wi-Fi 更適合於延遲敏感型應用(如語音和影片)，且 WMM 省電機制能提高電池效率。

4G-LTE 目標是簡化和重新設計網路體系結構，使其成為 IP 化網路，有助於減少 3G 轉換中潛在不良因素。LTE 可提供高速移動中的通訊需求，支援多播和廣播流。全 IP 基礎網路結構，也被稱作核心封包網演進，將替代原先的 GPRS 核心封包網，可向較舊網路如 GSM、UMTS 和 CDMA2000 提供語音資料無縫切換。

Beacon 是一種短距離、低功耗無線傳輸技術，以固定頻率，廣播特定 ID (Identification)，行動裝置一旦進入訊號區域，並透過雲端做識別後訊息則會透過專屬 APP 傳送出去，依 Beacon 偵測到的距離範圍，透過藍牙訊號強弱 (RSSI 值)，可用來判斷使用者距離，進而觸發相關事件與使用者互動。

針對網路安全考量，此應用使用 APP 與網頁，在網路連接方式使用 HTTPS，透過 HTTP 進行通訊，但在通訊過程中使用 SSL/TLS 進行加密，由於非對稱加密運算量較高，傳遞回應較慢；實際架構上，會透過公開金鑰加密傳遞出共用金鑰，再透過共用金鑰加密進行後續傳遞，因此可兼顧安全性及傳遞速度。

目前市場上 IPv6 物聯網應用仍未普及，但廠商表明了解 IPv6 對於物聯網應用未來發展很關鍵，建議政府及相關單位可以加強 IPv6 基礎建設普及，並鼓勵國內廠商投入相關之研發。

在物聯網資訊安全，目前並沒有統一標準與最佳實施方式，建議

政府與相關單位規劃開始引導相關廠商投入物聯網資安標準之制定及實施。

關於以上物聯網應用案例報告詳細內容，請參閱附錄九。

# 第十一章研析網際網路技術標準

## 第一節 IP (Internet Protocol，網際網路協定)

### 一. IPv6 基本介紹

#### (一) IP 發展演進

網際網路 (Internet) 主要是指網路層透過網際網路協定 (Internet Protocol，IP)，連接全球數十億部裝置的數位資料傳輸系統。西元 1960 年代冷戰時期，美國國防部高等研究計劃署 (ARPA) 為了能夠分時共用超級電腦，建立以封包交換為基礎的 ARPANET，並於西元 1969 年 (民國 58 年) 10 月首次成功在兩節點間傳送文字，開啟現今網際網路發展新紀元。

西元 1990 年 (民國 79 年) 3 月歐洲 CERN 網路，利用 T1 (1.5Mbit/s) 線路與美國 NSFNet 相連，同年 Timothy John Berners-Lee 開發首套 World-Wide Web 瀏覽器。西元 1991 年 (民國 80 年) 提供商用網路流量交換的 Commercial Internet eXchange 公司 (CIX) 成立，美國國家科學委員會 (NSF) 允許非營利公司 Advanced Network and Services (ANS) 的 ANSNet 與 NSFNet 同用實體主幹。台灣 TANet 則於西元 1991 年 (民國 80 年) 12 月 3 日以 64Kbps 經美國東岸 Princeton University 連上 NSFNet。自西元 1990 年代起，網際網路開始從軍事、學術用途擴大為商用及民用，對網路接取及頻寬需求也愈來愈迫切。至西元 2020 年 (民國 109 年) 1 月，全球估計上網人口已達 45 億人。

西元 1974 年 (民國 63 年) 時 Vint Cerf 和 Bob Kahn 出版了一篇名為〝Protocol for Packet Network Intercommunication〞論文，奠

定整個網際網路架構基礎，後來該架構分為 2 個模組進行發展，分別為傳輸層 TCP 及網路層 IP，即 TCP/IP 架構。第一版正式公開運作 IP 協定為 IPv4，內建於當時的工作站及商用電腦。自西元 1990 年代起，考量到 IPv4 位址空間可能無法負擔未來網路上裝置數量，因此 IETF 在西元 1995 年 (民國 84 年) 制定 IPv6 規格以做為 IPv4 的下一代 IP 協定，下圖為 IP 規格發展演進歷程。

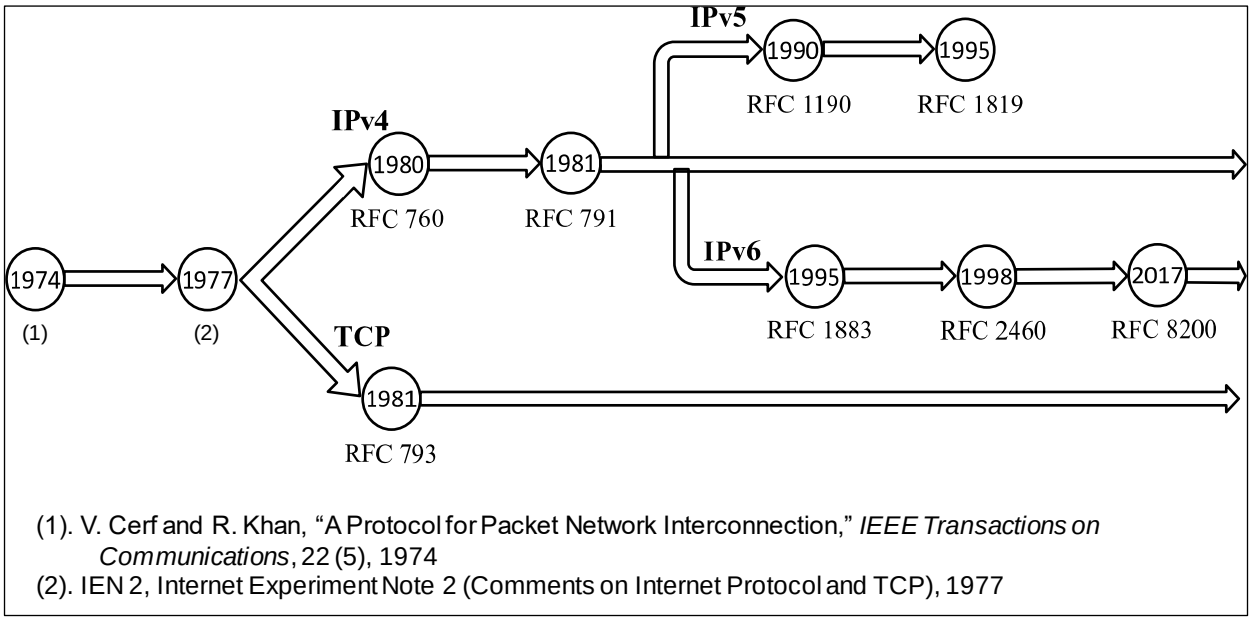



圖 186、IP 規格演進歷程

## (二) IPv6 和 IPv4 差異

IPv6 詳細規範描述於[RFC 8200]文件中，為網際網路協定最新版本，主要是為解決規範在[RFC 791]文件中 IPv4 位址枯竭的問題，兩者主要差別和比較如下表所示。

表 99、IPv6 和 IPv4 比較表

| 序號 | 類別 | IPv4 | IPv6 |
|---|---|---|---|
| 1 | 位址空間 | 32 位元 (4 Bytes) | 128 位元 (16 Bytes) |
| 2 | 位址類型 | Unicast/Multicast/ Broadcast | Unicast/Multicast/ Anycast |
| 3 | 表頭結構 | 可變長度 20~60 Bytes，取決於使用的 IP 選項 | 固定 40Bytes，沒有 IP 表頭選項 (比照傳輸層利用擴充標頭) |
| 4 | 最大傳輸單元 MTU 的最小值 | 典型最小值為 576 Bytes | 最小值為 1280 Bytes |
| 5 | 位址解析 | 使用 ARP 來尋找與 IPv4 位址相關的實體位址 | 利用 NDP 或 SLAAC 將實體位址內含於 IP 進行鄰居偵測和自動配置 |
| 6 | 封包分段 | 標準表頭佔有支援分段的欄位，來源節點或路由器皆可將封包分段 | 利用選擇性分段擴充標頭，只能在來源節點執行分段，在目的地節點執行重組 |
| 7 | QoS 傳輸品質支援 | 選項擴充 6 位元 DSCP 及 2 位元 ECN | 預含包括 8 位元 Traffic Class 及 20 位元 Flow Label |

連接網際網路的每一台主機其連線介面卡，均會自動取得或被設定一個全球或區網內部單一網路 IP 位址 (IP Address)。發送端主機在送出的網路封包中，會在傳送表頭內容 (Header) 表明自己來源 IP 位址 (Source Address)，並指名擬傳送對象目的 IP 位址 (Destination Address)。IP 位址在 IPv4 為 32 位元，而 IPv6 為 128 位元，IPv4 和 IPv6 表頭結構如下圖所示。

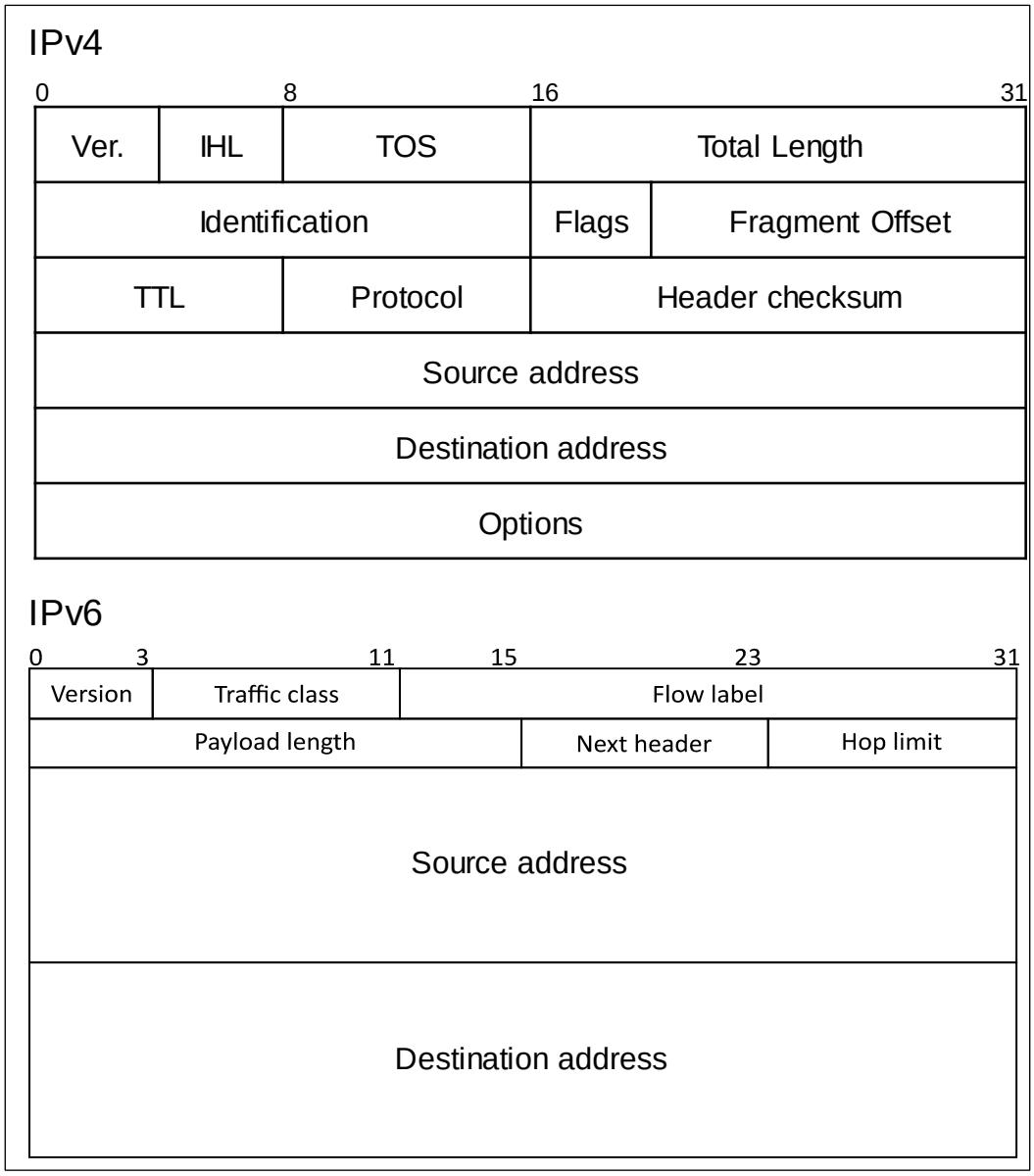



圖 187、IPv4 及 IPv6 表頭結構

## (三) IPv6 和 IPv4 播送方式

在 IPv4 規範傳統網路通訊系統基本上會提供一對一單播 (Unicast)、一對多群播 (Multicast) 及全體廣播 (Broadcast)，3 種播送方式。網路群播已被廣泛應用在視訊、網路校時、內容散佈、mDNS (Multicast DNS，群播 DNS)、路由資訊交換、網路連線遊戲等服務。IPv4 及 IPv6 都支援群播，一般常見 IP 網路層群播服

務模式有支援多對多 ASM (Any-Source Multicast) 及以一對多為主 SSM (Source-Specific Multicast)，兩者皆以一個識別用的群播位址來代表一個群播群組，擬接收群播封包的主機，必須先加入或取得該群組的群播位址，經由路由器才可以收到送往該群播位址的封包。

IPv4 之 IGMP (Internet Group Management Protocol，網路群組管理協定) 及 IPv6 之 MLD (Multicast Listener Discovery，群播監聽器發現協定) ，即是用來支援主機加入、離開群組，及群組一致性維護等。群播研究議題包含探討各種網路環境及使用情境下，如何有效建立群播路由 (Multicast Routing) 或群播樹 (Multicast Tree)，以降低需要重複傳送封包量。

除群播外，IPv6 還支援任播 (Anycast)，針對一個 Anycast 位址內的一群主機，只有一個主機將收到送往該 Anycast 位址封包。一個 Anycast 位址對應一群接收端，但是對任一個發送端，藉由路由器的判斷與協助，只有其中一個最近或最好的接收端會接收到該發送端所傳送出的封包。

群播和任播的差異為：群播讓已加入群組所有成員均會收到群播封包，任播則只有一個成員會收到封包。

## (四) IPv6 優勢

IPv6 優勢如下表所示：

表 100、IPv6 優勢

| 序號 | 類別 | 說明 |
|---|---|---|
| 1 | 擴增<br>位址空間 | ● IPv6 將 IP 位址的大小從 32 位增加到 128 位。<br>● 支援更多級別尋址層次結構、更多數量可尋址節點及更簡單位址自動配置。<br>● 群播位址上加入作用域 (Scope) 區段，改善群播路由可伸縮性。<br>● 新增任播位址用於將封包發送到一組節點中的任何一個。 |
| 2 | 簡化<br>表頭結構 | 部分 IPv4 表頭欄位被棄用或變更為選用欄位，減少處理大多數封包成本，降低 IPv6 表頭傳送成本。 |
| 3 | 改進擴增和選項支援度 | IP 表頭選項編碼方式更動使轉發更有效率、更少的選項長度限制及提高未來新增選項的靈活性。 |
| 4 | 流量標記<br>能力 | IPv6 增加一項可以標記發送端請求封包序列功能，發送端請求封包序列在網路中被視為單一個流量。 |
| 5 | 身份驗證和隱私功能 | IPv6 增加支援身份驗證、資料完整性和資料機密性 (選項) 功能。 |

## (五) IPv6 主要通訊協議

IPv6 正常運作需有許多協議參與其中，最主要協議為 NDP、SLAAC、DAD、DHCPv6、ICMPv6 及 MLDv2 等，各通訊協議運作架構如下圖所示：

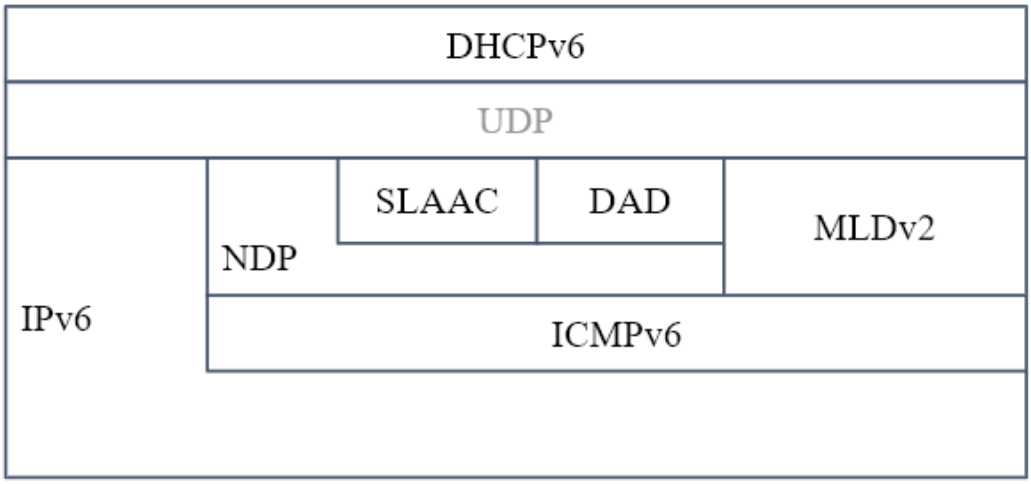



圖 188、IPv6 主要通訊協議架構

以下將針對 IPv6 重要通訊協議進行簡介：

**1. 鄰居發現協議 (Neighbor Discovery Protocol，NDP)**

[RFC 4861]文件中規範鄰居發現協議NDP是IPv6架構中重要通訊協議之一，同一個鏈路中 IPv6 節點透過 NDP 尋找鏈路上其他節點的鏈路位址、尋找可以代替轉送封包的路由器、及持續追蹤鄰居是否可連結及其鏈路位址。

NDP 的定義主要是靠解決兩個在相同鏈路的節點進行資訊交換時所提查詢訊息需求回覆，其主要類別如下表所示：

表 101、NDP 資訊交換時所提查詢訊息需求類別

| 序號 | 類別 | 說明 |
|---|---|---|
| 1 | 路由器發現 | 主機該如何在已銜接的鏈路上找到路由器。 |
| 2 | 前綴發現 | 主機該如何找到已銜接鏈路上的位址前綴集合。 |
| 3 | 參數發現 | 主機該如何知道鏈路參數 (如鏈路 MTU 等) 及網路層參數 (如節點跳躍數量限制等)。 |
| 4 | 位址自動設定 | 節點須進行如[RFC 4862]內提到的無狀態位址自動設定。 |
| 5 | 位址解析 | 節點如何從 IP 位址得出目標節點鏈路位址。 |
| 6 | 決定 Next-Hop | 如何從 IP 位址決定該將流量送給哪個鄰居。 |
| 7 | 鄰居不可達偵測 | 節點該如何知道某個鄰居已經無法連結。若該鄰居為路由器，節點將會嘗試替代的預設路由器。 |
| 8 | 重複位址偵測 | 節點該如何知道欲使用位址已被其他節點使用。 |
| 9 | 重導向 | 路由器該如何告知主機有更佳 First-Hop 通往特定目的地。 |

**2. 無狀態位址自動設定(Stateless Address Autoconfiguration，SLAAC)**

[RFC 4862]文件中規範 SLAAC 位址設定過程包含產生一個區域鏈路位址、透過無狀態位址自動設定產生全域位址並透過重複位址偵測的機制判斷將使用的位址是否已被使用。IPv6 無狀態位址設定顧名思義主機不需要任何額外的手動位址設定，對於路由器也僅須少量的設定且無須額外伺服器輔助。

位址自動設定透過結合本地資訊與路由器建議資訊來產生全域位址。路由器建議鏈路上的前綴及子網路識別碼，主機則會針對每個介面產生一個獨一無二〝介面識別碼〞，兩者結合即為一個 IPv6 位址。若沒有路由器參與，則主機只能產生區域鏈路位址，用於和同一個鏈路下其他節點通訊。

如果不在意主機所使用的確切位址，只在意位址是唯一且可正確被路由，則可使用無狀態的方法。另一方面，如果需要更強烈的位址分配控制，可使用[RFC 8415]所提到的動態主機設定協定 (Dynamic Host Configuration Protocol for IPv6，DHCPv6)，SLAAC 可以和 DHCPv6 同時共存。

**3. 重複位址檢測 (Enhanced Duplicate Address Detection，DAD)**

[RFC 7527]文件中介紹藉由偵測回送 IPv6 ND 訊息方式實現重複位址偵測演算法，並探討在某些特殊接取網路中重複位址偵測方法。

在[RFC 4862]文件的附錄 A 中討論 IPv6 回送抑制機制 (Loopback Suppression) 和重複地位檢測。該文件提到使用硬體

輔助機制來檢測回送 DAD 訊息。如果硬體無法抑制回送 DAD 訊息，則需要軟體解決方案。DAD 所使用的特別 NDP 訊息類型是在[RFC 4861]中所說明的鄰居請求 (Neighbor Solicitation，NS)。NS 是由 DAD 的 IPv6 節點的網路介面產生。

DAD 中所涉及的另一個訊息是鄰居建議 (Neighbor Advertisement，NA)。此文件中的增強型 DAD 演算法重點在於在 DAD 操作期間檢測回送的 NS。檢測回送的 NA 不能解決回送的 DAD 問題。在 DAD 操作期間檢測到任何其他回送 ND 訊息不在此文件定義範圍內。此文件並討論可用於緩解 DAD 回送問題的方法。

**4. 路徑最大傳輸單位 (Path MTU Discovery for IPv6，PMTU)**

[RFC 8201]文件中規範，當一個 IPv6 節點有大量資料要發送到另一個節點時，該資料將以一系列 IPv6 封包進行傳輸。封包大小需小於或等於 PMTU (Path Maximum Transmission Transmission Unit，Path MTU)。如果封包大小超過 PMTU，則需分割成片段，每個片段大小需小於或等於 PMTU。

通常最好的封包大小為從起始節點到目標節點的路徑中的最小鏈路 MTU，讓封包可以順利從起始節點傳送至目標節點，無需進行分割，這個封包大小稱為 PMTU。[RFC 8201]文件定義了用於節點發現任意路徑的 PMTU 標準機制。

IPv6 節點應實作 PMTU 發現。未實作 PMTU 發現的節點必須使用[RFC 8200]中定義的 IPv6 最小鏈路 MTU 作為最大封包大小。大多數情況下，這種方式將導致使用較小封包大小傳送，多數路徑 PMTU 均大於 IPv6 最小鏈路 MTU。發送比 PMTU

所允許的封包大小還要小的封包節點，將形成網路資源浪費，並可能導致流量不足的狀況。

PMTU 發現是依靠 ICMPv6 封包太大 (Packet Too Big，PTB) 來確定路徑的 MTU 大小。如果不發送 ICMPv6 訊息，則實現 PMTU 發現並發送大於 IPv6 最小鏈路 MTU 封包的節點容易出現連接問題。

在[RFC 4821]文件中，可以找到 PMTU 發現的擴充規範。該文件定義了用於封裝層 PMTU 發現 (Packetization Layer Path MTU Discovery，PLPMTUD) 方法，此方法設計用於無法確保向主機傳遞 ICMPv6 訊息的路徑上。

**5. 動態主機設定協定 (Dynamic Host Configuration Protocol for IPv6，DHCPv6)**

在[RFC 8415]文件中描述，DHCPv6 是一種用於自動配置網路配置參數的可擴充機制，如自動配置節點 IP 位址和前綴。網路參數可以為無狀態的方式提供，也可以結合一個或多個 IPv6 位址或 IPv6 前綴來進行有狀態分配參數提供。DHCPv6 可以代替無狀態位址自動配置 (SLAAC) 或與其並存。其運作過程如下圖所示，客戶端使用 HCP_Relay_Agents_and_Servers multicast address (FF02::1:2) 和 DHCP 伺服器溝通，因此 DHCP 伺服器不須額外配置一個位址。

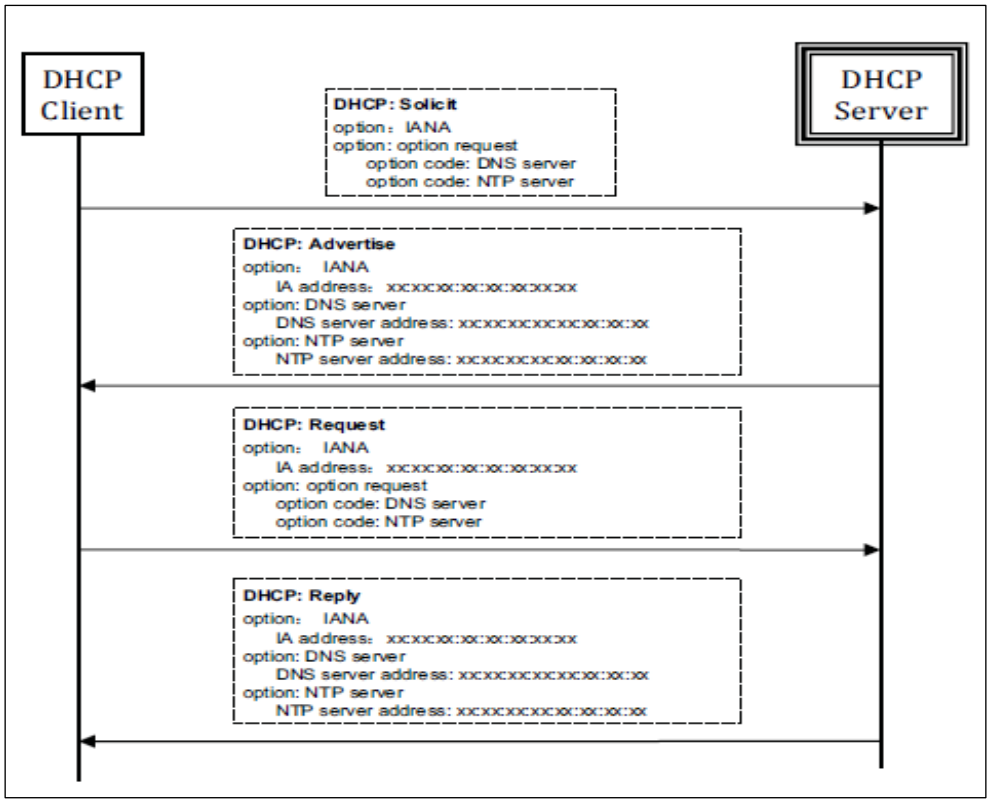



圖 189、DHCPv6 運作過程

### 6. 網際網路控制訊息協定第 6 版 (Internet Control Message Protocol，ICMPv6)

在[RFC 4443]文件中，IPv6 透過 ICMPv6 傳遞控制訊息，如進行 Path MTU Discovery 及 NDP 等，ICMPv6 之 IPv6 Next Header 值為〝58〞。

### 7. 群播監聽器發現協定 (Multicast Listener Discovery Version 2 for IPv6，MLDv2)

在[RFC 3810]文件中定義，IPv6 路由器使用群播監聽器發現協議 (MLD)，探詢在其直接連接鏈路上希望接收群播封包的節點，並偵測鄰居感興趣的特定群播位址。群播路由器本身可以是一個或多個群播位址的監聽器。在此情況下，其執行

MLDv2〝群播路由器部分〞，負責收集其群播路由協議所需的群播監聽器訊息。又執行〝群播位址偵聽器部分〞通知自身和其他相鄰群播路由器的收聽狀態。

# 二. IETF 之 IPv6 標準制定現況

## (一) IPv6 相關領域分析

IETF (Internet Engineering Task Force) 工作組 (Working Group，WG) 中，其中以下 3 類型 WG 研究領域和 IPv6 較為相關：

表 102、IETF 中 IPv6 相關領域工作組類別

| 序號 | 領域 | 技術範籌 |
|---|---|---|
| 1 | 網際網路領域<br>Internet Area<br>(INT) | 核心 (Core) |
| | | 低功耗網路 (Low Power) |
| | | 移動性和多址傳送<br>(Mobility and Multihoming) |
| | | 時間 (Time) |
| 2 | 維護及管理領域<br>Operations and Management Area<br>(OPS) | 網際網路維護 (Internet) |
| | | 路由和域名系統維護<br>(Routing & DNS) |
| | | 自動網路配置維護<br>(Automatic Network Configuration) |
| | | 認證維護(Authentication) |
| 3 | 資訊安全領域<br>Security Area<br>(SEC) | 驗證和授權<br>(Authentication & Authorization) |
| | | 憑證和身份<br>(Certificate & Identity) |
| | | 簽章、加密和密碼學<br>(Signing、Encryption & Cryptography) |
| | | 網路安全<br>(Network Security) |
| | | 應用安全<br>(Application Security) |

下表為 IETF 工作組中和 IPv6 相關的重點工作組簡介：

表 103、IETF 之 IPv6 相關重點工作組簡介

| 序號 | 工作組 | 工作組簡介 |
|---|---|---|
| **網際網路領域 Internet Area (INT)** | | |
| **1** | 6lo<br>(IPv6 over Networks of Resource-constrained Nodes) | 關注資源限制網路節點的連線。 |
| **2** | Lpwan<br>(IPv6 over Low Power Wide-Area Networks) | 負責提出適用於低功耗廣域網路的表頭壓縮，並將其套用在不同的實體層協定上。 |
| **3** | lwig<br>(Light-Weight Implementation Guidance) | 負責制定在資源限制網路節點相容於目前標準且精簡的通訊標準。 |
| **4** | 6tisch<br>(IPv6 over the TSCH mode of IEEE 802.15.4e) | 負責制定基於 IEEE802.15.4 時槽跳頻技術的 IPv6 協定 |
| **5** | ipwave<br>(IP Wireless Access in Vehicular Environments) | 負責車聯網相關的通訊協定制定。 |
| **6** | 6man<br>(IPv6 Maintenance) | 維護和改進 IPv6 協定及位址結構。 |
| **7** | dhc<br>(Dynamic Host Configuration) | 負責如 DHCPv6 等自動網路組態設定協定之制定。 |
| **維護及管理領域 Operations and Management Area** | | |
| **8** | v6ops<br>(IPv6 Operations) | 負責蒐集 IPv6 網路服務供應商和使用者所產生的問題及解決方案。 |
| **資訊安全領域 Security Area** | | |
| **9** | ipsecme<br>(IP Security Maintenance and Extensions) | 負責維護及擴充前代 IPsec 工作組所制定的 IPsec 協議套件，如 IKEv2。 |

其他 IETF 工作組運作和更多 IPv6 相關資料請參閱附錄九，詳細說明。

# 第二節 DN (Domain Name，網域名稱)

## 一. DNS 歷史

DNS 因為網路增長而發展，在 20 世紀 70 年代時候，ARPAnet 只有幾百台主機小型網路社群，原來主機名稱到位址的對應資訊存在由 NIC (Network Information Center) 所維護的 HOSTS.TXT 文件中，每個主機都是由 FTP 傳輸，隨著網路發展，此傳輸方式對 NIC 主機造成很大負擔。網路性質不斷改變，區域組織能夠管理自己的網域名稱與 IP 位址，但需要等到 NIC 將 HOSTS.TXT 修改才能改變全網路網域名稱與 IP 位址。網路應用越來越複雜，需要一個普遍管理方式，因此採用階層式命名空間，以〝.〞分隔不同的階層。下表整理 DNS 設計目標：

表 104、DNS 設計目標

| 序號 | 設計目標 |
|---|---|
| 1 | 要有一致命名空間，避免臨時編碼所引起的問題，名稱中不需包含網路標示字元、位址、路由等資訊 |
| 2 | 資料庫龐大的規模與更新頻率、創建與刪除名稱的機制，都須以分散式的方式維護 |
| 3 | 要在獲取資料成本、更新速度和暫存準確性之間達到平衡 |
| 4 | 應用須具備普遍性，能從名稱找回位址、信箱資訊和其他可擴充的資訊，且與名稱有關聯的資料都歸類成一個類別，在查詢時能限制單一類別做查詢 |
| 5 | 能因應不同類型網路和應用，提供不同協議或位址格式類型服務 |
| 6 | 名稱服務器獨立運作於通訊系統，其他服務只需提供虛擬通訊服務即可使用 |
| 7 | 系統能廣泛使用於不同類型主機 |

## 二. DNS 結構

### (一) 域名空間

域名空間由樹狀結構組成。樹中的每個節點有一個標籤和零個或多個資源記錄 (Resource Record，RR)，包含與域名相關聯的資訊。域名本身由標籤組成，該標籤與其右邊的父節點名稱連接在一起，並用〝.〞分隔。

該樹為從根區域開始的區域。一個 DNS 區域可以由只有一個區域，或者由多個區域和子區域，取決於區域經理管理選擇。還可以根據類別對 DNS 進行分區，可以將單獨的類別視為並行名稱空間樹。

可以透過新增其他區域來劃分對任何區域的管理責任。當新區域的授權被委派給指定的名稱服務器。父區域不再對新區域具有權威性。

### (二) 域名語法

域名由一個或多個部分組成，每個部分稱為標籤，當用戶需要輸入網域名稱時，將省略每個標籤長度，標籤之間使用〝.〞作為分隔。例如：〝example.com〞，而〝example〞與〝com〞都是一個標籤。

網域名稱標籤由左至右讀取，表示最遠離根到最接近根。左側每個標籤都指定右側網域的細分或子網域。例如: 標籤示例指定〝com〞網域的子網域，而〝www〞是〝example.com〞的子網域。此細分樹最多可包含 127 個級別，最右邊的標籤為頂級域名，例如: 域名〝www.example.com〞中〝com〞屬於頂級域名。網域名稱標籤命名規則整理如下表：

表 105、網域名稱標籤命名規則

| 序號 | 標籤規則 |
|---|---|
| **1** | 每個標籤可以包含 0 到 63 個字元 |
| **2** | 長度為零的空標籤保留給根區域 |
| **3** | 完整域名的文字表示形式不得超過 253 個字元 |
| **4** | 在 DNS 的內部二進制表示中，最大長度需要 255 Bytes 存儲，因為其還須包含存儲名稱的長度 |
| **5** | 主機名稱使用首選格式和字元集，由 ASCII 字元 a 到 z、A 到 Z、數字 0 到 9 和連接字元符號組成，此規則稱為 LDH (Letters-Digits-Hyphen) 規則 (字母、數字、連接字元符號)。 |
| **6** | 英文大小寫都可以使用，但網域名稱不區分英文字母大小寫 |
| **7** | 標籤不能以連接字元符號開頭或結尾 |
| **8** | 頂級域名不應該為全數字。 |

DNS 中允許的一組有限的 ASCII 字元，無法支援許多語言的名稱和單詞作為主機名稱。因此，ICANN 批准了應用程序國際化域名 (IDNA) 系統，透過該系統，用戶應用程序 (例如 Web 瀏覽器) 可以使用 Punycode 將 Unicode 字元串對應到有效的 DNS 字元集中。ICANN 在西元 2009 年 (民國 98 年) 批准了國際化域名國家/地區代碼頂級域名 (ccTLD) 的安裝。下圖為 DNS 命名空間範例，在此範例中，根網域有 3 個直接子網域：MIL、EDU 和 ARPA。LCS.MIT.EDU 網域有一個名為 XX.LCS.MIT.EDU 的直接子網域。

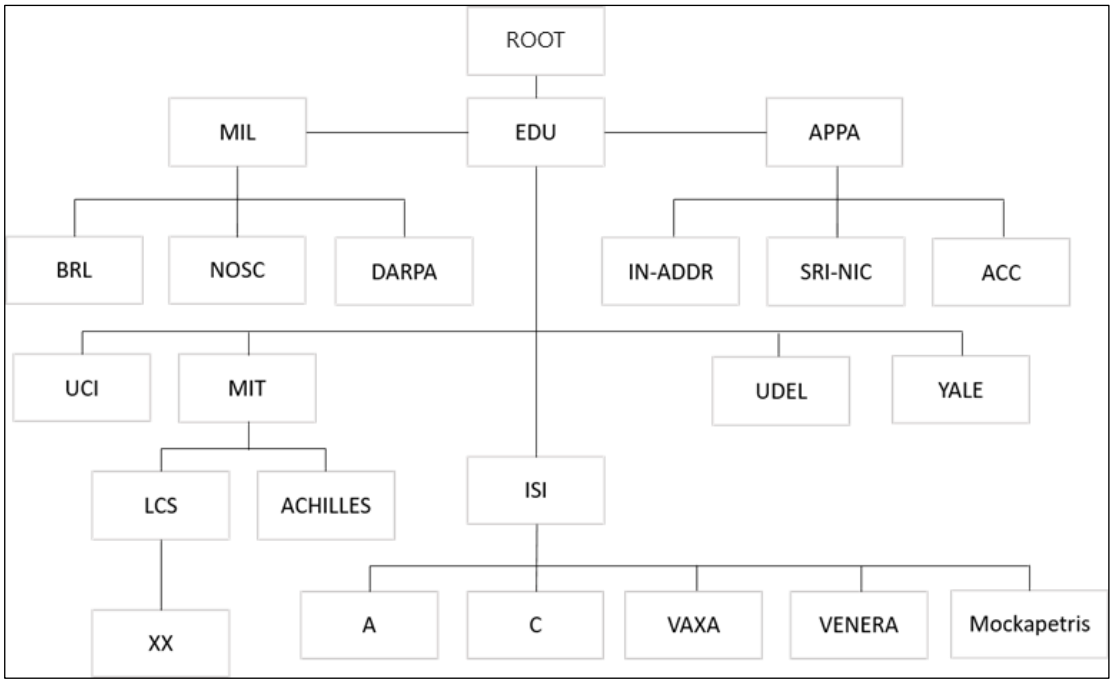



圖 190、DNS 命名空間範例

## (三) 國際化域名

國際化域名 (Internationalized Domain Name，IDN) 發展一直是全球關心的議題之一。由於全球 80%以上使用者來自非英語系國家，多年來 IDN 標準的差異，造成上百萬個 IDN 網址存在著許多互通性與相容性的問題，長期致力於 IDN 標準的發展與研究的 IETF 於西元 2003 年 (民國 92 年) 發布了國際化域名技術標準相關 RFC，分別為[RFC 3490]、[RFC 3491]和[RFC 3492]，這些標準為 IDN 提供了技術參考說明，而 IDN 是一種以標準方式處理域名中非 ASCII 字元的機制，透過將具有非 ASCII 字元的名稱轉換為域名系統可以理解的 ASCII 標籤來作業。在西元 2010 年 (民國 99 年) 發布 6 篇與 IDNA 相關的 RFC，分別為[RFC 5890]、[RFC 5891]、[RFC 5892]、[RFC 5893]、[RFC 5894]與[RFC 5895]，其中[RFC 5890]廢除了[RFC 3490]，並描述了國際化應用程序域名修訂版的協議和

使用環境，而[RFC 5891]則是廢除[RFC 3491]，內容則為國際化域名 (IDNs) 的修訂協議定義。

國際化域名又稱特殊字元域名，是指部分或完全使用特殊的文字或字母組成的網際網路域名，包括法語、阿拉伯語、中文、斯拉夫語、泰米爾語、希伯來語或拉丁字母等非英文字母，這些文字經過多位元組萬國碼編譯而成。在域名系統中，國際化域名使用 Punycode 轉換以 ASCII 字元串列格式儲存。

域名系統的建立是為了將網路搜尋用語變成更加通俗易懂的語言，但由於技術限制和長久實踐，域名使用美國資訊交換標準代碼字元已成為慣用標準。國際化域名透過將各種非英語字元轉化成與現有域名系統相容的美國資訊交換標準代碼字串，並儲存在域名系統中，使得世界各地的用戶可以直接使用母語輸入域名。且此技術並不需要對網際網路結構做任何改變。

對於支援 IDNA 的應用程式，有效標籤的兩種類型為 A 標籤、U 標籤，以下分別定義：

- A 標籤是 IDNA 有效字元串列的 ASCII 兼容編碼 (ACE)。必須是完整標籤，IDNA 是為標籤定義，而不是標籤的一部分，也不是完整的域名。表示每個 A 標籤都將以 IDNA ACE 前綴〝xn-〞開頭，後面接一個字元串列，該字元串列是 Punycode 算法的有效輸出，因此最多 59 個 ASCII 字元長度。前綴和字元串列必須一起滿足可存儲在 DNS 中標籤的所有要求。當滿足以上要求的字元串列可以解碼為 U 標籤時，才是 A 標籤。
- U 標籤是 IDNA 有效的 Unicode 字元串列，以正規化形式 C (Normalization Form C，NFC [Unicode-UAX15]) 且包含至少一個非 ASCII 字元，以標準 Unicode 編碼形式 (例如 UTF-8) 表

示。U 標籤和 A 標籤之間的轉換是根據 Punycode 規範執行，根據需要增加或刪除 ACE 前綴。

## (四)名稱服務器

名稱服務器是構成儲存網域資訊的資料庫。名稱服務器的主要功能是回覆標準網域資料查詢，查詢及其回覆都以標準訊息格式進行。查詢包含 QTYPE、QCLASS 和 QNAME，用於描述所需資訊的類型和類別以及感興趣的名稱。名稱服務器回覆查詢的方式取決於其是否在遞迴模式下運行，非遞迴和遞迴模式的運作如下所述：

- 非遞迴模式：能使用本地資訊進行查詢需求回覆，回覆包含錯誤、答案或引用到某些其他更接近答案的服務器。所有名稱服務器都必須實作非遞迴查詢。
- 遞迴模式：用戶端最簡單的模式是遞迴模式，在此模式下，名稱服務器充當解析器角色，並返回錯誤或答案，但不引用。此服務在名稱服務器中為可選項目，不一定要支援。

## (五)根名稱服務器

每個遞迴解析器都知道全球 13 個 DNS 根名稱服務器，其為遞迴解析器對 DNS 記錄搜尋的第一站。根服務器接受包含域名遞迴解析器的查詢，根名稱服務器根據該域名的擴展網域名稱如；〝.com〞，〝.net〞，〝.org〞 等，透過將遞迴解析器導向 TLD 域名服務器進行回覆。根名稱服務器由 ICANN (Internet for Assigned Names and Numbers) 非營利組織監督。

雖然全球有 13 個根名稱服務器，但不表示根名稱服務器系統中只有 13 台伺服器。根名稱服務器有 13 種類型，但是在全球網際網路範圍內每種都有多個副本，其使用 Anycast 路由提供快速回覆。

## (六)頂級域名名稱服務

TLD (Top-Level Domain，頂級域名) 名稱服務器維護所有共享通用域擴展網域名稱的域名資訊，例如〝.com〞，〝.net〞或 url 中最後一個點之後的任何內容。例如：〝.com 〞，TLD 名稱服務器包含以〝.com〞結尾的每個網站網域名稱資訊。如果用戶正在搜索〝google.com〞，則在收到根域名服務器回覆後，遞迴解析器將向〝.com〞的 TLD 名稱服務器發送查詢，該查詢透過指向該域名的權威名稱服務器進行回覆。

TLD 名稱服務器的管理由網際網路名稱與數位位址分配機構 (IANA) 處理，該機構是 ICANN 的一個分支機構。IANA 將 TLD 服務器分為兩種：

- 通用頂級域名：指非特定國家或地區的域名，下表為全球最知名的通用 TLD 類別：

表 106、全球知名通用頂級域名類別

| 序號 | 通用頂級域名 | 類別 |
|---|---|---|
| **1** | .com | 商業組織 |
| **2** | .org | 非營利組織和其他 |
| **3** | .net | 主要網路支援中心 |
| **4** | .edu | 教育機構 |
| **5** | .gov | 政府機構 |
| **6** | .int | 國際組織 |
| **7** | .mil | 軍事團體 |

- 國家/地區代碼頂級域名: 指域名包括特定於某個國家或州的任何域名。例如: 〝.uk〞、〝.us〞、〝.ru〞、〝.jp〞和〝.tw〞等。

### (七)權威名稱服務器

當遞迴解析器從 TLD 名稱服務器收到回覆時，該回覆會將解析器導向權威名稱服務器。權威名稱服務器通常是解析器在 IP 位址過程中的最後一步。權威名稱服務器包含特定於其所服務的域名資訊 (例如〝google.com〞)，其可為遞迴解析器提供在 DNS A 記錄中找到的服務器 IP 位址，或者該域名具有 CNAME 記錄 (別名)，即為遞迴解析器提供一個別名網域，此時遞迴解析器必須執行一個全新 DNS 查詢，從權威名稱服務器中取得一筆記錄 (通常是一個包含 IP 位址的 A 記錄)。

## 三. DNS 運作方式

DNS 查詢流程如下圖所示：

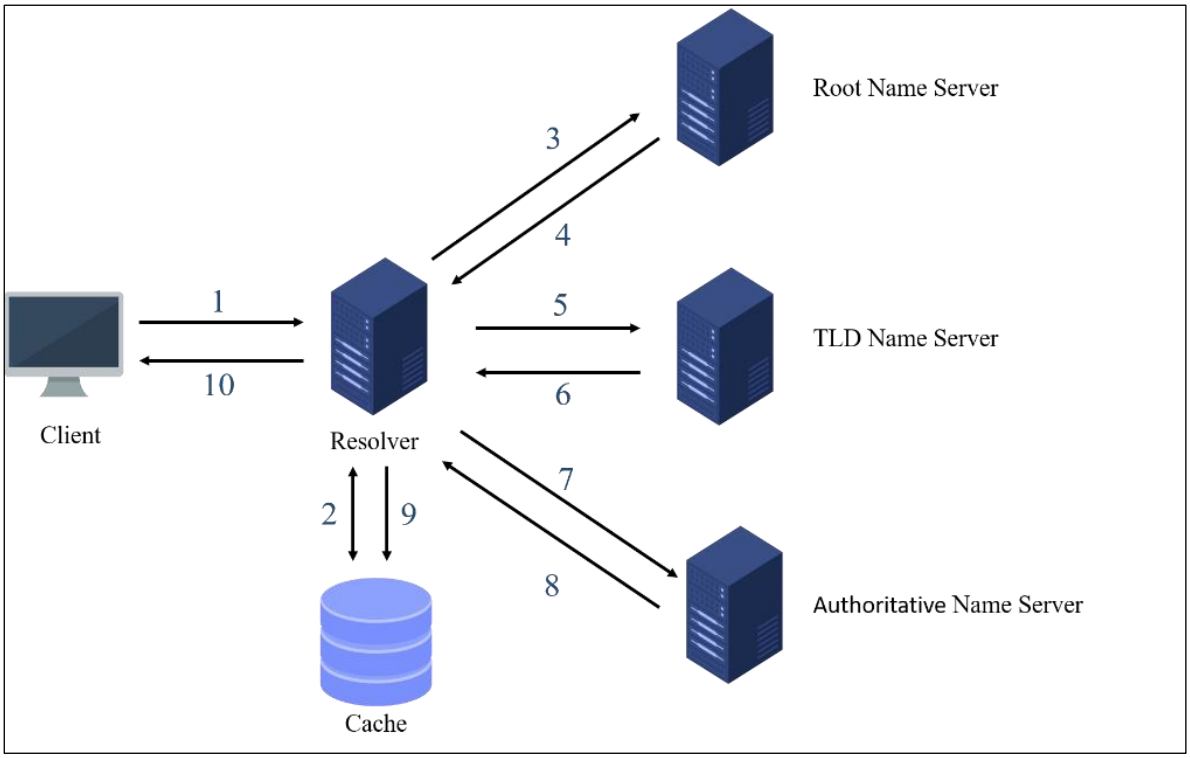



圖 191、DNS 查詢流程

上圖 DNS 查詢流程各步驟說明如下表所示，此範例假設用戶在瀏覽器中欲查詢〝example.com〞網站：

表 107、DNS 查詢步驟說明

| 步驟 | 說明 |
|---|---|
| 1 | 查詢進入網路中，並由 DNS 解析器 (Resolver) 接收。 |
| 2 | 解析器檢查暫存區 (Cache) 是否已經具有該名稱位址，如果存在，將傳回位址至瀏覽器。如果不存在，繼續下一步驟查詢。 |
| 3 | 解析程序查詢 DNS 根名稱服務器。 |
| 4 | 根名稱服務器返回儲存〝.com〞域名的名稱服務器域名和位址。 |
| 5 | 解析程序向〝.com〞的 TLD 名稱服務器發出請求。 |
| 6 | TLD 名稱服務器回覆儲存〝example.com〞域名的名稱服務器域名和位址。 |
| 7 | 遞迴解析器送出查詢需求到 DNS 權威名稱服務器。 |
| 8 | 〝example.com〞的 IP 位址從名稱服務器回覆到解析器。 |
| 9 | 解析器將回覆資料暫存。 |
| 10 | 解析器將位址提供給瀏覽器讓用戶使用該 IP 位址上網。 |

以下根據 DNS 查詢過程的重要元素進行說明：

## (一)解析器

解析器將用戶應用程式發送需求連結到網域名稱服務器程序。最簡單的情況下，解析器以子程序呼叫、系統調用等形式從用戶應用程式 (例如: 郵件、TELNET、FTP) 接收請求，並回覆與本地主機資料格式相容的資訊。解析器與請求解析的應用程式服務的程序位於同一台電腦上。但解析器可能需要查詢多個名稱服務器，或者可能在本地暫存資料中已經擁有所發送請求的資訊，所以解析程序完成所需的時間可能會有所不同，從毫秒到幾秒鐘。解析器重要目標是透過先前暫存資料回覆查詢請求以降低網路延遲和名稱服務

器負載量。解析器分為兩種，分別為存根解析器與遞迴解析器，說明如下：

**1. 存根 (Stub) 解析器**

假設在瀏覽器上輸入〝www.google.com〞時，瀏覽器會向操作系統詢問 IP 位址。該操作系統的存根解析器，用於處理所有 DNS 查詢。解析程序將 DNS 查詢發送到指定的遞迴解析程序 (名稱服務器)，並根據其存活時間 (Time To Live，TTL) 將記錄資訊存儲在其暫存區中。當存根解析器由應用程式收到請求時，首先在其暫存區中搜尋，如果有記錄，將訊息提供給應用程式。如果沒有所需的暫存，則向遞迴解析器發送 DNS 查詢請求。

**2. 遞迴解析器**

遞迴解析器充當用戶端 (Client) 和 DNS 名稱服務器之間的中間人。從用戶端收到 DNS 查詢後，遞迴解析器將以暫存的資料作為回覆，或將查詢請求發送到根名稱服務器，然後將另一個請求發送到 TLD 名稱服務器，再將最後一個請求發送到權威名稱服務器。收到包含請求的 IP 位址的權威名稱服務器的回覆後，遞迴解析器回覆發送給用戶端。

過程中，遞迴解析器將暫存由權威名稱服務器接收的資料。當下一個用戶請求最近查詢過的域名 IP 位址時，若暫存資料未過期，解析程序可以繞過向名稱服務器查詢資料的過程，直接由用戶端的暫存資料取出該筆記錄資料並回傳。

## (二) 紀錄暫存

在應用程序中實作名稱解析的標準做法是透過本地或解析器主機中的暫存資料來減少域名系統服務器的負載量。從 DNS 請求獲得的資料與存活時間 (TTL) 有關，當資料過期，就必須丟棄或更新。TTL 由權威域名服務器的管理員進行設定。有效期可能從幾秒鐘到幾天甚至幾週不等。

由於 DNS 系統採用分散式暫存結構，DNS 記錄更新不會立即在整個網路中傳播，而是要求所有暫存資料在 TTL 過期後進行更新。在[RFC 1912]文件中對適當 TTL 值的基本規則有詳細說明。

負暫存資料是用於表示記錄不存在的暫存資料，由區域內具有權威性名稱服務器確定，當回覆不存在所請求類型的資料時，該區域必須包括授權啟動記錄 (Start of Authority Record，SOA Record) 才能判斷。SOA 記錄的最小字段值和 SOA 本身 TTL，可以用於建立查詢資料不存在的 TTL。

## (三) DNS 查詢

查詢就是向名稱服務器送出要求回覆的請求。在網路中，查詢以 UDP (User Datagram Protocol) 或 TCP (Transmission Control Protocol) 傳輸。名稱服務器回覆可能直接回答查詢請求、或將請求送到另一組名稱服務器，或發出錯誤訊息。查詢可以分為標準查詢或反向查詢說明如下：

### 1. 標準查詢

標準查詢會指定目標網域名稱 (QNAME)、查詢類型 (QTYPE) 和查詢級別 (QCLASS)，請求查詢對應的 RRs

(Resoruce Record) 。此為 DNS 主要查詢行為，此查詢又分為兩種，分別為遞迴查詢與迭代查詢。

- 遞迴查詢 (Recursive DNS Query)：

  DNS 用戶端向 DNS 伺服器發出查詢請求，如果 DNS 伺服器裡面沒有所需要資料，則 DNS 伺服器會代替用戶端向其他 DNS 伺服器進行查詢，其他 DNS 伺服器如果也沒有所需的資料，則再向 DNS 作業系統請求，如果這個時候 DNS 伺服器有對應資料，則會先回覆之前 DNS 伺服器，再依次回覆到最開始的 DNS 伺服器，直到 DNS 的用戶端得到資料。這種傳遞方式，DNS 伺服器必須向用戶端做出回答，一般由 DNS 用戶端提出的查詢都是遞迴查詢。下圖為遞迴查詢流程的示意圖。

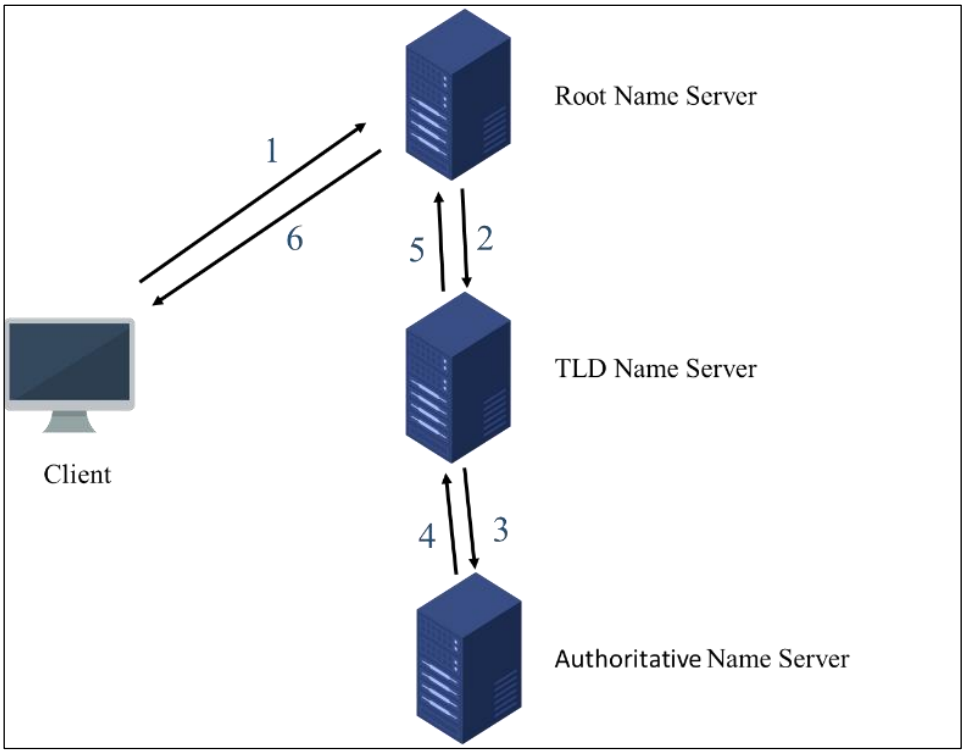



圖 192、DNS 遞迴查詢流程

● 迭代查詢 (Iterative DNS Query)

DNS 用戶端向 DNS 伺服器發出查詢請求，如果 DNS 伺服器裡面沒有所需要的資料，則第一台 DNS 伺服器會告訴用戶端其 DNS 伺服器的 IP 位址，由 DNS 用戶端直接和第一台 DNS 伺服器提出查詢請求，如果第一台 DNS 伺服器也沒有資料，則第一台 DNS 伺服器會告訴用戶端其 DNS 伺服器，即第二台 DNS 伺服器，用戶端直接和第二台伺服器提出請求，直到找到資料為止。讓 DNS 用戶端利用自己的 IP 位址查詢其主機名稱。下圖為迭代查詢流程示意圖。

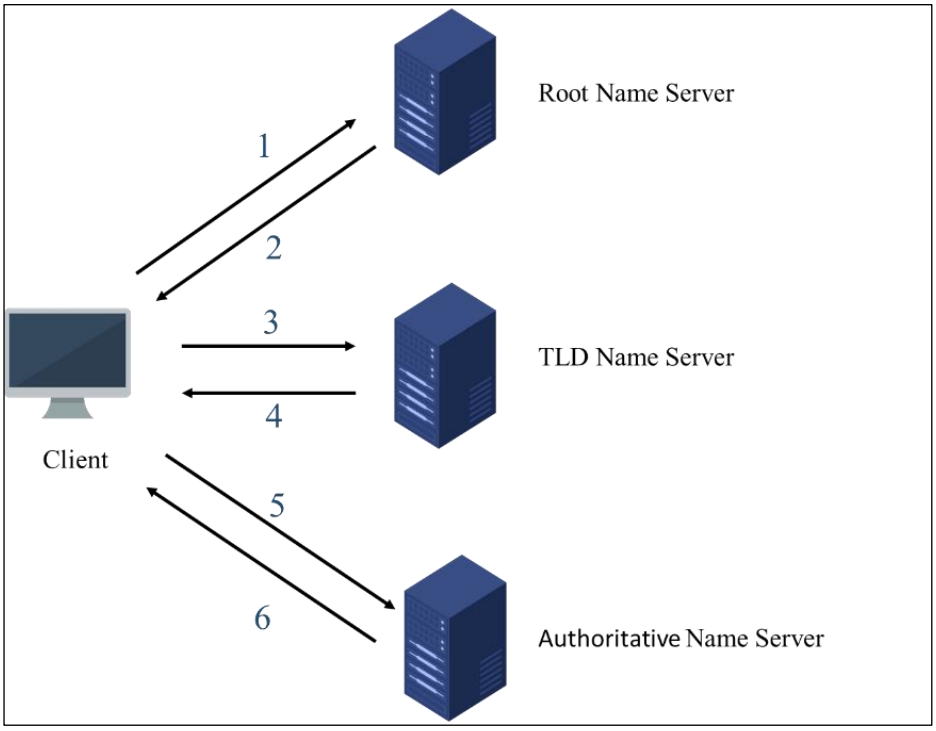



圖 193、DNS 迭代查詢流程

## 2. 反向查詢

反向查詢是依據 DNS 用戶端提供的 IP 位址來查詢其主機名稱，由於 DNS 名字空間中功能變數名稱與 IP 位址之間無法

建立直接對應關係，所以必須在 DNS 伺服器內增加一個反向查詢紀錄。DNS 以域名形式將 IP 位址存儲為頂級域名，arpa〞中的指標記錄 (Pointer to Record，PTR) 的特殊格式名稱。IPv4 反向查詢為〝in-addr.arpa〞，而 IPv6 反向查詢為〝ip6.arpa〞。

名稱服務器可能支援網域名稱或將特定資源對應到具有該資源網域名稱的反向查詢。例如標準查詢能將網域名稱對應到 SOA 之 RR，對應的反向查詢能將 SOA 之 RR 對應回網域名稱。

此服務在名稱服務器為可選不一定要支援，但所有名稱服務器至少必須能夠理解反向查詢資訊，並回覆未實作此服務的錯誤訊息。網域系統無法保證反向查詢的完整性或唯一性，因為網域系統是按照網域名稱而不是主機位址或任何其他資源類型而組成。反向查詢主要用於錯誤偵測和資料庫維護。

反向查詢可能不會返回正確的 TTL，也不會指出標示的資源紀錄 (RR)，例如具有多個位址的主機位址。因此，不可以暫存反向查詢中返回的資源紀錄。

## (四)DNS 傳輸

因 UDP 傳送方式能讓 DNS 伺服器負載更低且快速回應，因此大多數 DNS 透過 UDP 進行傳輸，UDP 封包最大長度限制為 512 位元組，標準用戶端向 DNS 伺服器查詢域名時，一般回覆內容都不超過 512 位元組。

TCP 則用於區域傳輸 (zone transfer)，區域傳輸就是當輔助 DNS 伺服器啟動，需要與主 DNS 伺服器通訊，並載入資料時就是所謂區域傳輸，而 TCP 通常用於大小超過 DNS 協議 512 位元組限制的郵件。DNS 安全性考量和增加傳送 IPv6 位址的需求出現後，

增加回覆資料大小的需求，因此出現增加使用 TCP 傳輸的需求。另外提供防止對位址欺騙 DNS 反射/放大攻擊保護，也推動對 TCP 使用量的需求。另外，為解決 DNS 隱私，例如採用傳輸層安全協議 (Transport Layer Security，TLS) DNS 需求，增加 DNS 採用 TCP 傳輸的另一個因素。TCP 傳輸特性整理如下表所示:

表 108、TCP 傳輸特性

| 序號 | 特性 | 說明 |
|---|---|---|
| 1 | 連接持久性 | TCP 連接在發送第一個回覆後不會被服務器關閉，在收到第一個回覆後也不會被用戶端關閉。 |
| 2 | 連接重用 | 可透過單個 TCP 連接發送多個查詢和回覆。 |
| 3 | 閒置 DNS-over-TCP 期間 | 當沒有任何待發送的查詢需要傳送，且沒有未完成回覆時，DNS 用戶端會認為已建立的 TCP 上 DNS 處於空閒狀態。 |
| 4 | 查詢 Pipeline | 透過單個 TCP 連接發送多個查詢和回覆，但在發送另一個查詢之前並不會等待任何未完成的回覆。 |
| 5 | 亂序處理 | 同時處理多個查詢時，會盡快將個別回覆回傳，不一定按照查詢順序回覆。 |

## (五) IPv6 DNS

由於應用程序假定位址查詢只回覆 32 位元組的 IPv4 位址，因此 IPv6 位址對域名系統中網路位址儲存無法輕易地擴充。為了支援 IPv6 位址在 DNS 中存儲，下表所列 DNS 擴充功能，讓 DNS 能支援 IPv6 位址：

表 109、支援 IPv6 之 DNS 擴充功能

| 序號 | DNS 擴充功能 |
|---|---|
| 1 | 定義一個資源記錄類型，可將域名對應到 IPv6 位址。 |
| 2 | 定義一個域名以支援 IPv6 位址查詢。 |
| 3 | 重新定義執行附加處理以進行 IPv4 位址查詢，並對 IPv4 和 IPv6 位址執行附加處理。 |

此更改是為了與現有軟體並容。保留對 IPv4 位址的支援，且可支援 IPv6。在[RFC 2893]文件中，並對 DNS 中 IPv4 和 IPv6 位址共存轉換問題進行討論。

## 四. DNS 訊息格式

DNS 協議使用兩種類型的 DNS 訊息：〝查詢〞與〝回覆〞，兩者使用相同的標準訊息格式，DNS 封包格式如下圖所示。分為上半部份為表頭 (Header)，下半部份為查詢及回覆內容區段。

| | |
|---|---|
| Identification<br>(識別代碼) | Flags<br>(標誌) |
| Number of questions<br>(問題數目) | Number of answers<br>(答案數目) |
| Number of authority RRs<br>(權威 RRs 數量) | Number of additional RRs<br>(額外 RRs 數) |
| Question Section (問題區段) | |
| Answer Section (答案區段) | |
| Authority Section (權限區段) | |
| Additional Section (附加資訊區段) | |

圖 194、DNS 封包格式

DNS 封包表頭部分長度固定為 12 位元組。其中標誌字段 (Flags) 負責控制封包下半部 4 個內容區段，其長度固定為 2 位元組。標誌 (Flags) 字段組成如下表所示：

表 110、DNS 標誌字段組成

| 序號 | 欄位 | 說明 | 長度 (bits) |
|---|---|---|---|
| **1** | QR | 查詢／回覆，1 為回覆，0 為查詢 | 1 |
| **2** | OPCODE | 類型可以為以下選項之一：<br>● QUERY (標準查詢，0)<br>● IQUERY (反向查詢，1)<br>● STATUS (服務器請求狀態，2) | 4 |
| **3** | AA | Authoritative Answer，DNS 服務器對於所查詢的主機名稱是否具有權威性 | 1 |
| **4** | TC | TrunCation，此訊息是否因長度過長而被截斷 | 1 |
| **5** | RD | Recursion Desired，用戶端是否進行遞迴查詢 | 1 |
| **6** | RA | Recursion Available，回覆的 DNS 服務器是否支援遞迴解析 | 1 |
| **7** | Z | Zero，全 0 保留欄位以備未來擴充使用 | 3 |
| **8** | RCODE | Response Code，常見錯誤訊息如下所列：<br>● NOERROR (0，查詢成功完成)<br>● FORMERR (1，格式錯誤)<br>● SERVFAIL (2，查詢失敗無法給出答案)<br>● NXDOMAIN (3，查詢失敗查詢的域名不存在) | 4 |

問題區段 (Question Section) 是用戶端 (或伺服器) 向名稱伺服器查詢時，所攜帶完整網域名稱所儲存的位置。一般來講，用戶端每次向名稱伺服器查詢一個完整網域名稱 (Question Count=1)，然而客戶端並非每次都只查詢一筆資料，如需要詢問多筆資料時，則會在問題計數欄位中指明後面緊接著有幾個問題區段。問題區段的格式如下表所列：

表 111、DNS 封包的問題區段 (Question Section) 格式

| 序號 | 欄位 | 說明 | 長度 (Bytes) |
|---|---|---|---|
| **1** | QNAME | 存放所要查詢的完整網域名稱，其為一個或多個標識字元的序列。每個標識字串以首字節的值表示為該名稱的長度，每個名稱最後以 0 表示結束，長度為 0 的標識字串為根標識字串 | Variable |
| **2** | QTYPE | 表示要查詢資源紀錄類型，代表要進行的服務類型，常用之紀錄型態如下所列：<br>1 A 查詢 IP 位址<br>2 NS 查詢名稱伺服器<br>5 CNAME 查詢主機別名<br>12 PTR 反向查詢網域名稱<br>13 NINFO 查詢主機資訊<br>15 MX 查詢郵件交換紀錄 | 2 |
| **3** | QCLASS | 表示要在哪一類網路上做查詢，通常為 1 (IN)，表示 Internet 通訊協定的位址，如果不是 1，則表示為其他網路型態 (非 IP 位址格式) 。 | 2 |

答案區段 (Answer Section) 裡所存放的是被查詢之名稱伺服器所回應的資料，一般查詢都只有一筆資料 (Answer RR Count=1)，如有多筆資料回應，則會在答案計數欄位中指明有幾筆資源紀錄 (RR)。答案區段的格式如下表所示：

表 112、DNS 封包的答案區段 (Answer Section) 格式

| 序號 | 欄位 | 說明 | 長度 (Bytes) |
|---|---|---|---|
| **1** | 名稱 (Name) | 資源記錄所屬的節點名稱。 | Variable |
| **2** | 類型 (Type) | 用於指定此資源記錄中資源的類型。類型是指抽象資源。 | 2 |
| **3** | 類別 (Class) | 用於標識協議類別或協議實例。<br>IN Internet 系統<br>CH 混淆 (Chaos) 系統<br>HS Hesiod | 2 |
| **4** | 存活時間 (TTL) | 存活時間以秒為單位，表示該筆資源紀錄可以存活時間 (在 Cache 暫存器有效時間)，主要由解析器暫存 RR 時使用。如超過時間 (一般為 2 天)，則表示該筆資料已失去時效，必須刪除。如果 TTL=0，表示該筆記錄為變動性，而接收端 (用戶端或伺服器) 不必再儲存於快取伺服器 (或快取資料庫) 上。 | 4 |
| **5** | 資源資料長度 (RDLENGTH) | 表示後面資源資料長度，以位元組計算 | 2 |
| **6** | 資源資料 (RDATA) | 表示所回應的資源紀錄答案，例如:<br>RR=A (詢問主機位址)，則資料欄位回應為該主機的 IP 位址。 | Variable |

## 五. DNS 資源紀錄

域名系統指定網路資源資訊元素的資料庫。資訊元素的類型透過 DNS 記錄類型，也就是資源記錄列表進行分類和組織。每個記錄都有一個類型 (名稱和編號)，一個到期時間 (生存時間)，與一個特定該類型的資料。而網域名稱標識一個節點，每個節點都有一組資源資訊，該資訊可以為空。相同類型的資源記錄被組成為資源記錄集 (RRset)，資源記錄集中的個別記錄順序並不重要，且不需要由名稱服務器、解析器或 DNS 的其他部分保留。下表為常見的資源紀錄類型。

表 113、常見的資源紀錄類型

| 序號 | 欄位 | RR 類別 | 說明 |
|---|---|---|---|
| **1** | 1 | A | 主機位址 (Address，A)，紀錄網域名稱到 IPv4 位址 (32 位元) 之間轉換，此為 DNS 資料庫最常見 RR。 |
| **2** | 2 | NS | 網域權威名稱服務器 |
| **3** | 5 | CNAME | 主機別名 (Canonical NAME，CNAME) 提供主機設定一個別名。CNAME 是非常重要資源紀錄，提供不同網域名稱轉譯到同一個 IP 位址，較常用為將 www、ftp、mail 名稱轉譯到同一主機位址，例如：www.cu.edu.tw、ftp.cu.edu.tw、mail.cu.edu.tw 都是 linux-2.cu.edu.tw 別名，都表示同一主機位址。設定時每一主機只能設定一個 A 紀錄，其它 CNAME 便設定到此 A 紀錄的主機上，同一主機可以設定多個 CNAME 紀錄。 |
| **4** | 6 | SOA | 授權啟動 (Start Of Authority，SOA) 是在任何網域區域設定中的第一項紀錄，用來指定 DNS 伺服器或是目前區域上的主要伺服器名稱，及有關伺服器設定內容。在 SOA 紀錄上所設定的內容主要是伺服器版本和到期日期，及區域授權伺服器之間 (主要和次要伺服器之間) 區域傳送頻率。 |
| **5** | 12 | PTR | 指標 (Pointer，PTR) 是用來登錄由 IP 位址轉譯成網域名稱，其功能剛好和 A 紀錄相反。即為使用 PTR 來反向查詢網域名稱。 |
| **6** | 13 | HINFO | 主機資訊 (Host Information，HINFO) 是登錄主機使用的硬體和作業系統的資訊，供查詢使用。 |
| **7** | 15 | MX | 郵件交換器 (Mail Exchanger，MX)，用於將 DNS 域名對應到郵件服務器。電子郵件應用程序使用 MX 記錄根據目標電子郵件位址尋找 DNS 域的郵件服務器。MX 記錄存儲特定域名的郵件服務器資訊。 |
| **8** | 16 | TXT | 文字 (Text，TXT) 紀錄為文字說明，用來說明主機或網環境設定。 |
| **9** | 28 | AAAA | AAAA 資源紀錄將 DNS 域名對應到 IPv6 位址。 |
| **10** | 33 | SRV | 服務位置記錄 (Service Record，SRV)，用於指定伺服器提供服務的位置 (如主機名和埠) 資訊。 |

DNS 萬用字元符號〝*〞記錄，是 DNS 區域中的一條記錄，該記錄將對應不存在域名請求，DNS 中萬用字元符號比其他電腦系統中使用到萬用字元符號受到更多限制。萬用字元符號 DNS 記錄的最左側 DNS 標籤帶有單個〝*〞 (星號)，例如：〝*.example.com〞。域名中其他位置的星號不能當作是萬用字元符號，因此〝*abc.example.com〞和〝abc.*.example.com〞都不能當作是萬用字元符號 DNS 記錄。此外，只有當域名不存在時才可以對應萬用字元符號，而不是只在沒有查詢類型記錄時對應。

DNS 萬用字元符號的原始定義在[RFC 1034]文件中第 4.3.2 和 4.3.3 節中定義，只能透過查詢演算法中的特定步驟確認，因此其規則不直觀也不明確。後來[RFC 4592]文件中對於〝萬用字元符號在域名系統中的作用〞有更明確描述，以幫助確認使用規則。

## 六. DNS 協議擴充

DNS 擴充機制 (Extension mechanisms for DNS，EDNS) 是用於擴充域名系統協議的幾個參數大小的規範，第一組規範由網際網路工程任務組 (IETF) 於西元 1999 年 (民國 88 年) 發布於[RFC 2671]文件中。西元 2013 年 (民國 102 年) 則由[RFC 6891]更新並廢除[RFC 2671]舊版文件內容。

傳統 DNS 傳輸是透過 UDP Port 53 封包，UDP 封包本身限制其大小為 512 位元組，在傳統 DNS 傳輸已經足夠。DNSSEC 因為納入數位簽章功能，使原本 UDP 封包若要包含數位簽章資料，就會出現不敷使用的情況。能夠解決此問題最好方法就是使用 EDNS0，其將

UDP 封包擴充到 4096 位元組，如此才能容納 DNSSEC 資料傳輸需求。

EDNS0 流程是由 DNS 用戶端發起，當解析器可以接受 EDNS0 封包時，就會在封包 Additional 區段放入一個〝opt〞資訊傳遞給伺服器，表示自己支援 EDNS0，而 DNS 伺服器收到 DNS 封包後看到 Additional 區段有〝opt〞資訊，就知道用戶端有支援 EDNS0 封包，在伺服器產生回覆封包後也會在 Additional 區段加入〝opt〞資訊表示此為 EDNS0 封包,所以如果用戶有觀察 DNSSEC 的 Additional 區段，會發現回覆數目加一，表示為 EDNS0 封包，但 EDNS0 封包並不代表是 DNSSEC 封包,在 EDNS0 中有一個 bit:〝DO〞被設定為 1 時，才代表此為 DNSSEC 封包。

## 七. DNS 動態更新

動態 DNS (Dynamic DNS，DDNS) 是域名系統中的一種自動更新名稱伺服器內容的技術。根據網際網路的域名訂立規則，域名必須跟從固定的 IP 位址。但動態 DNS 系統為動態網域提供一個固定的名稱伺服器，透過即時更新，使外界用戶能夠連上動態用戶的網址。

在網路 (ARPANET) 發展初始階段，網路上主機的尋址是透過將主機名對應到 IP 位址的靜態轉換所完成。此表以主機文件形式手動維護。域名系統提供透過遞迴查詢，將線上相同位址資訊自動分發到為每個網路或網域配置的遠程資料庫的方法。該 DNS 設施在每個節點上使用靜態搜尋，IP 位址一但分配給特定主機即很少更動。隨著網路快速增長及工作場所和家庭中個人電腦普及給管理員帶來很大的負擔，因此不得不分散 IP 位址空間管理系統。

動態主機配置協議 (DHCP) 允許企業和網路服務供應商 (ISP) 在開機時自動為終端設備分配位址。此有助於節省可用位址空間，因為並非所有設備都一直處於活動狀態，且可以根據所需分配位址。此功能讓 DNS 服務器也自動保持最新狀態。動態 DNS 即是用於實現此目的，主機獲得來自 DHCP 服務器或透過配置系統收到位址，即通知其各自的 DNS 服務器。此協議的 DNS 更新方法在西元 1997 年 (民國 86 年) IETF 出版[RFC 2136]文件中定義，並已成為 DNS 協議的標準部分。

此術語被用來描述兩種不同概念。對網際網路管理層面來說，動態 DNS 更新是指建立一個 DNS 系統，能夠自動更新傳統 DNS 記錄，而不需要手動編輯。此機制在[RFC 2136]中定義，並利用 TSIG (Transaction Signature) 機制來提供安全性。

在用戶端來說，動態 DNS 提供一個輕量化機制，讓本地 DNS 資料庫可以即時更新。能把網際網路域名指往一個可能經常改變的 IP 位址，讓經常改變位置及組態的裝置，能夠持續性更新 IP 位址。讓網際網路上的其他用戶可以透過一個大家知道的網域名稱，連接到一個可能經常動態改變 IP 位址的設備。其中一個常用的用途是在使用動態 IP 位址連線 (例如在每次接通連線就會被分配一個新 IP 位址撥號連線等) 的電腦上執行伺服器軟體。

要實現動態 DNS，就需要將網域的「最大暫存時間」設定在一個非常短的時間 (一般為數分鐘)。如此可避免其他用戶在暫存中保留舊 IP 位址，讓每個新連線被建立時都會經過名稱伺服器取得該設備的新位址。

動態 DNS 的服務為普遍性的服務。此服務會利用資料庫儲存使用者目前的 IP 位址，並提供使用者更新 IP 位址的方法。當客戶安裝

服務軟體後，會每隔數分鐘執行檢查設備 IP 位址。當發現其 IP 位址變更時，服務軟體會送出一個更新 IP 位址請求至動態 DNS 伺服器。有很多路由器和其他網路裝置也會在其韌體中包含上述功能。

## 八. DNS 安全問題

安全問題不是 DNS 或任何在早期網路上部署軟體主要設計考量，因為該剛開始網路並不開放給公眾使用。但在西元 1990 年代，網際網路向商業領域的擴展，改變了對保護資料完整性和用戶身份驗證的安全措施要求。

惡意用戶發現並利用漏洞問題。DNS 暫存中毒就是一個問題，在這種情況下，資料以偽裝成權威原始服務器的形式分發到暫存解析器，以潛在的偽造資訊和較長的有效期限 (生存時間) 污染存儲資料。合法應用程式進行查詢請求時，可能會重新導向到此出於惡意目的運作的網路主機。

有些網域名稱命名方式可能被用來進行欺騙，例如：paypal.com 和 paypa1.com 是不同名稱，但是根據用戶選擇的字體，用戶可能無法在圖形用戶界面中區分。在許多字體中，〝字母 l〞和〝數字 1〞看起來非常相似甚至相同。在支援國際化域名系統中，此類問題非常嚴重，因為在典型的電腦螢幕上，ISO 10646 中許多字元代碼可能看起來相同。網路釣魚有時會利用此漏洞。如果不注意 DNS 的配置，DNS 也可能從其他安全或私有連接中〝洩漏〞，DNS 有時會被惡意人員用來繞過防火牆並將資料洩露出去。

網域名稱系統安全擴充 (DNS Security Extensions，DNSSEC) 嘗試為 DNS 增加安全性考量，在 DNS 增加身份驗證和資料完整性檢查，同時保持和 DNS 的兼容性。DNSSEC 目的是在保護應用程式 (以及

為這些應用程式提供暫存的解析程式) 免於使用偽造或被操縱的 DNS 資料，例如由 DNS 暫存中毒所產生的資料。由 DNSSEC 保護的所有回覆答案均需經過數位簽章。透過檢查數位簽章，DNS 解析器可以檢查該資訊是否與區域所有者發布並提供給權威 DNS 服務器的資訊相同 (即未修改且完整)。DNSSEC 可以保護 DNS 中發布的任何資料，包括文字記錄 (TXT) 和郵件交換記錄 (MX)，並可以用於引導其他安全系統。

# 九. DNS 隱私問題

## (一) 傳輸層安全性

DNS 傳輸層安全性 (DNS-over-TLS，DoT) 為 IETF 標準協定，可在 DNS 用戶端和 DNS 服務器之間提供整體加密。傳統上，DNS 遭受安全問題的困擾，DNS 用戶端與 DNS 服務器之間的通訊幾乎未加密，因此容易有受到欺騙，攔截等駭客攻擊情況發生。

DoT 是加密 DNS 查詢以確保其安全和隱密性的標準。DoT 使用與 HTTPS 網站用來加密和認證通訊的相同安全協議 TLS (也稱為〝SSL〞)。DoT 用於 DNS 查詢 UDP 上增加 TLS 加密。並確保 DNS 請求和回覆不會被中間人攻擊篡改或偽造。

## (二) HTTPS 安全性

DNS 之 HTTPs 安全性 (DNS-over-HTTPS，DoH) 也是 IETF 安全協議標準，為 DoT 替代方法，用於解決用戶端和 DNS 服務器通訊的安全性，使用 DoH 來讓 DNS 查詢和回覆被加密，其透過 HTTP 或 HTTP/2 協議而不是直接通過 UDP 發送。DoH 在 IETF 之[RFC 8484]文件中規範。TLS 上的 DNS 和 HTTPS 上的 DNS 都

提供了 DNS 用戶端和 DNS 服務器之間的加密，用以實現資料保密性和完整性。但是，DoH 使用與其他 HTTPS 流量相同的 TCP 通訊埠，即通訊埠 443。因此，很難從其他 HTTPS 流量中識別 DoH，由於 DoT 具有專用通訊埠，因此即使請求和回覆本身都經過加密，只要可以解析 DoT 通訊的網路設備都可以進行接收並解析。但使用 DoH，DNS 查詢和回覆在其他 HTTPS 流量中會被遮蔽，原因為共用通訊埠的緣故。

# 第三節 BGP (Boarder Gateway Protocol，邊界閘道器協定)

網際網路是由多個不同型態網路彼此互相連網所構成。封包在不同網路之間傳送時，必須通過路由器 (Router) 協助將封包轉發 (Relay) 到下一個網路。不同網路間，路由器透過查詢路由表 (Route Table) 來決定封包轉發的下一個網路。

網際網路上常見路由協定有兩類，分別為：

- 內部閘道協定 (Interior Gateway Protocol，IGP)

  適合使用在單一自治系統 (Autonomous System，AS) 內，共用同一個 AS Number (ASN)，如 RIP (Routing Information Protocol)、IGRP (Interior Gateway Routing Protocol)、EIGRP (Enhanced Interior Gateway Routing Protocol)、OSPF (Open Shortest Path First)、IS-IS (Intermediate system to intermediate system) 等，這些路由協定所維護的路由資訊通常屬於 OSI 網路模型中的網路層，例如 Internet Protocol (IP)。

- 外部閘道協定 (Exterior Gateway Protocol)

  由多個自治系統構成複雜網路中使用，如 EGP (Exterior Gateway Protocol)，及邊界閘道器協定(Border Gateway Protocol，BGP)。外部閘道協定用來確定在不同自治系統間網路可達性，並透過內部閘道協定來解析某個自治系統內部路由。

ISP 使用 BGP 與其他 ISP 建立路由連接，相互稱通信對端或對等實體 (Peer)。BGP 取代舊協定 EGP，透過 CIDR (Classless Inter-Domain Routing) 和路由聚合 (Route Aggregation) 降低路由表大小。

BGP 允許網路管理者自定 BGP 路由器的路由政策 (Routing Policy)，並給予較高優先權，手動選擇最佳路徑、次佳路徑等，此作法增加 BGP 彈性。但自定路由資訊沒有受到監管，可能在 BGP 廣播時被其他 AS 信任，使得 BGP 路由器收到錯誤或虛假路由資訊，導致路由意外，發生路由外洩、路由劫持等惡意事件。

大型複雜單一自治系統，也可採用 BGP，以改善使用 RIP 或 OSPF 效能瓶頸。iBGP (Interior/Internal BGP，內部 BGP) 指在單一自治網路中使用 BGP，所有 iBGP 對等實體 (Peer) 之間需要全連接。在不同自治網路使用 BGP 則稱為 eBGP (Exterior BGP，外部 BGP)。下圖為 iBGP 和 eBGP 關係圖：

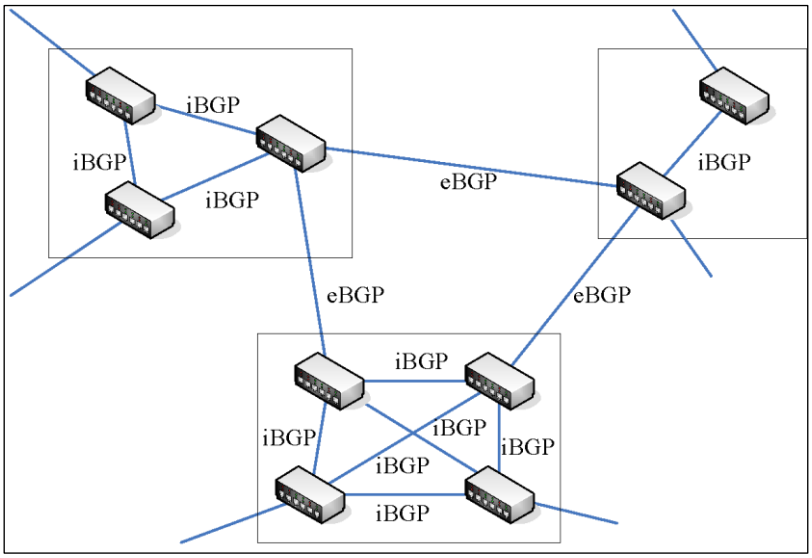



圖 195、iBGP 和 eBGP 關係圖

目前最新版本為 BGP 第 4 版 (BGPv4) 於西元 1994 年公告，西元 1995 年 [RFC 1771] 文件進行修正，同年 [RFC 1883] 定義 IPv6 BGP，並西元 1998 年於 [RFC 2208] 文件中修正，使 BGPv4 能夠支援 IPv4、IPv6 系列位址，因此稱為 Multiprotocol BGP。

之後， RFC 標準陸續發表相關規範，包含 BGP 對自治系統的考量、路由政策規範、實施經驗與分析等。並於西元 2006 年發表最新的 BGP 標準 [RFC 4271] ，和相關伴隨文件 (RFC 4272~4278)。之後又陸續更新既有 RFC，和發表新功能 (如 Graceful Restart) 標準文件。下表為重要 BGP 相關 RFC 列表：

表 114、重要 BGP 相關 RFC 列表

| 序號 | RFC No. | 標題 |
|---|---|---|
| 1 | 1267 | Border Gateway Protocol 3 (BGP-3) |
| 2 | 1772 | Application of the Border Gateway Protocol in the Internet Protocol (BGP-4) using SMIv2 |
| 3 | 1773 | Experience with the BGP-4 protocol |
| 4 | 1774 | BGP-4 Protocol Analysis |
| 5 | 4271 | A Border Gateway Protocol 4 (BGP-4) |
| 6 | 4272 | BGP Security Vulnerabilities Analysis |
| 7 | 4273 | Definitions of Managed Objects for BGP-4 |
| 8 | 4274 | BGP-4 Protocol Analysis |
| 9 | 4275 | BGP-4 MIB Implementation Survey |
| 10 | 4276 | BGP-4 Implementation Report |
| 11 | 4277 | Experience with the BGP-4 Protocol |
| 12 | 4278 | Standards Maturity Variance Regarding the TCP MD5 Signature Option (RFC 2385) and the BGP-4 Specification |
| 13 | 4760 | Multiprotocol Extensions for BGP-4 |
| 14 | 8654 | Extended Message Support for BGP |
| 15 | 2622 | Routing Policy Specification Language (RPSL) |
| 16 | 2725 | Routing Policy System Security |
| 17 | 4012 | Routing Policy Specification Language next generation (RPSLng) |
| 18 | 7909 | Securing Routing Policy Specification Language (RPSL) Objects with Resource Public Key Infrastructure (RPKI) Signatures |
| 19 | 5492 | Capabilities Advertisement with BGP-4 |
| 20 | 8810 | Revision to Capability Codes Registration Procedures |
| 21 | 2918 | Route Refresh Capability for BGP-4 |
| 22 | 7313 | Enhanced Route Refresh Capability for BGP-4 |

| 序號 | RFC No. | 標題 |
|---|---|---|
| 23 | 4456 | BGP Route Reflection – An Alternative to Full Mesh Internal BGP (iBGP) |
| 24 | 6608 | Subcodes for BGP Finite State Machine Error |
| 25 | 7606 | Revised Error Handling for BGP UPDATE Messages |
| 26 | 7911 | Advertisement of Multiple Paths in BGP |
| 27 | 1930 | Guidelines for creation, selection, and registration of an Autonomous System (AS) |
| 28 | 6996 | Autonomous System (AS) Reservation for Private Use |
| 29 | 7300 | Reservation of Last Autonomous System (AS) Numbers |
| 30 | 5065 | Autonomous System Confederations for BGP |
| 31 | 6793 | BGP Support for Four-Octet Autonomous System (AS) Number Space |
| 32 | 6286 | Autonomous-System-Wide Unique BGP Identifier for BGP-4 |
| 33 | 7607 | Codification of AS 0 Processing |
| 34 | 7705 | Autonomous System Migration Mechanisms and Their Effects on the BGP AS_PATH Attribute |
| 35 | 4724 | Graceful Restart Mechanism for BGP |
| 36 | 8538 | Notification Message Support for BGP Graceful Restart |
| 37 | 1997 | BGP Communities Attribute |
| 38 | 4360 | BGP Extended Communities Attribute |
| 39 | 5543 | BGP Traffic Engineering Attribute |
| 40 | 5701 | IPv6 Address Specific BGP Extended Community Attribute |
| 41 | 7153 | IANA Registries for BGP Extended Communities |
| 42 | 8642 | Policy Behavior for Well-Known BGP Communities |
| 43 | 6368 | Internal BGP as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs) |
| 44 | 8212 | Default External BGP (EBGP) Route Propagation Behavior without Policies |
| 45 | 2439 | BGP Route Flap Damping |
| 46 | 3765 | NOPEER Community for Border Gateway Protocol (BGP) Route Scope Control |
| 47 | 5575 | Dissemination of Flow Specification Rules |
| 48 | 7674 | Clarification of the Flowspec Redirect Extended Community |
| 49 | 7752 | North-Bound Distribution of Link-State and Traffic Engineering Information Using BGP |

以下就 BGP 運作進行摘要說明，BGP 為分散路由系統，對等實

體之間的鄰居關係是透過人工組態實現，並通過 TCP 建立對話以進行資料交換，預設連接埠 (Port) 是 179。各種路由協定中，只有 BGP 使用 TCP 作為傳輸層協定。在 AS 網路邊界上與其他 AS 網路交換路由資訊的路由器稱為邊界路由器(Border/Edge Router)，稱為 eBGP 對等實體。對等實體之間通常直接連接。iBGP 和 eBGP 的主要區別在於轉發路由資訊行為。例如，從 eBGP 對等實體獲得的路由資訊會分發給所有 iBGP 對等實體和 eBGP 對等實體，但從 iBGP 對等實體獲得的路由資訊通常僅會分發給所有 eBGP 對等實體。因此同一個 AS 網路中 iBGP 對等實體必須是全連接 (Full-mesh)。使用 BGP Route Reflector (BGP 路由反射器) 可以避免 iBGP 對等實體全連接要求。

BGP 路由器啟動時候，會計算本地路由，並發佈給相連 BGP 對等實體。結束之後，BGP 路由器就是斷斷續續接收一些更新事件，再將路由重新發佈給其 BGP 對等實體。BGP 路由器啟動之後，過程分為兩個部分，一個是初始化路由並發佈，接下來就是正常工作時路由發佈。

## 一.BGP 訊息

BGP 訊息透過 TCP 傳送，只在完整接收後才能進行處理。最大訊息長度是 4096 個字節 (Octet，8 位元組)；最小訊息只有 19 個字節，僅有 BGP 表頭 (Header)。

在[RFC 2918]文件中描述 BGP 使用 5 種訊息，分別是 Open、Update、Notification、Keep-alive 與 Route-Refresh。

- Open 訊息

  在建立 TCP 連線後，每個 BGP 對等實體第一個送出的訊息就是 Open 訊息，接受 Open 訊息後則將回送一個 Keep-alive 訊息作為確認。

- Update

  確認 Open 訊息後，BGP 連接後的首次 Update 訊息會交換整個 BGP 路由表，之後 Update 訊息只會發送有變化路由信息。

- Notification

  當偵測到錯誤狀況時，BGP 路由器送出一個 Notification 訊息，並在送出訊息後立刻中止連線。Notification 訊息包含一個字節錯誤碼、一個字節次錯誤碼和其他相關資料。

- Keep-alive

  BGP 路由器會周期地傳送 Keep-alive 訊息來維護連接，預設周期為 60 秒。Keep-alive 訊息只有表頭 19 字節，沒有資料。

- Route-Refresh

  當 BGP 路由器發現某個路由資訊已經失效，有三種機制通知鄰居。

  - 發送 Update 訊息，將失效路由的位址前綴寫入 Withdrawn Routes 欄位。
  - 發送 Update 訊息，在 NLRI 中發佈該位址前綴新的路由資訊，取代舊的路由資訊。
  - 關閉連線，來自對方的路由資訊就會自動被刪除。

## 二. 多協定擴充 (Multiprotocol BGP)

在 BGP 路由器之間建立對話的握手 (handshake) 期間，交換 Open 訊息時，BGP 路由器彼此可以協商是否使用 BGP 可選功能，包括多協定擴展 (Multiprotocol extensions，或 Multiprotocol BGP) 和各種恢復模式。如果在創建時就決定使用 Multiprotocol BGP，則 BGP 路由器可以為其發布的 NLRI 路由資訊加上位址家族前綴，包括 IPv4 (默認)、IPv6、IPv4/IPv6 VPN 和 Multicast BGP。

## 三.BGP 路由器狀態

BGP 對等實體使用一個簡單的有限狀態機制 (Finite State Machine，FSM)，包含六個狀態：Idle、Connect、Active、Open Sent、Open Confirm 與 Established。BGP 定義每個對等實體在某個狀態下應與對方交換的訊息，以便將對話從一種狀態更改為另一種狀態。

- BGP 路由器的初始狀態是 Idle。在 Idle 狀態下，BGP 路由器初始化所有資源，拒絕外界 BGP 連接嘗試，啟動與對方的 TCP 連接，進入 Connect 狀態。
- 在 Connect 狀態下，BGP 路由器等待 TCP 連接完成，如果成功，則送出 Open 訊息，並進入到第三種狀態 Open Sent。如果不成功，它將啟動 Connect Retry 計時器，並在時間到時進入為 Active 狀態。
- 在 Active 狀態下，路由器將 Connect Retry 計時器重置為零，並返回到 Connect 狀態。
- 在 Open Sent 狀態下，路由器已經發送一個 Open 訊息，正在等待 Keep-alive 訊息確認，以便進入 Open Confirm 狀態。彼此完成交換 Keep-alive 訊息，並在成功接收後，路由器進入 Established 狀態。
- 在 Established 狀態下，路由器可以發送/接收 Keep-alive、Update 與 Notification 訊息。

## 四.BGP 路由過程

概念上，一個 BGP 路由器可以接受來自多個鄰居更新 (Update) 訊息，並將 Update 訊息中的 NLRI 通告給相同或不同組的鄰居。BGP 使用三種 RIB：Adj-RIBs-In、Loc-RIB 和 Adj-RIBs-Out。

- Adj-RIBs-In：本地 BGP 路由器從其他 BGP 路由器收到的路由訊息。
- Loc-RIB：儲存在 Adj-RIBs-In 中未經處理過的路由訊息，經過本地 BGP 路由器的決定程序，依據本地政策所選出的路由資訊。Loc-RIB 記載的每個路由資訊的下一跳都必須是本地 BGP 路由器的路由表可以分辨。
- Adj-RIBs-Out：透過本地 BGP 路由器發送的 Update 訊息通告給特定鄰居的路由資訊。

## 五.BGP 團體屬性 (BGP Communities)

在[RFC 1997]文件中描述 BGP communities 在概念上可以視為屬性標籤 (Attribute Tags)，可應用於傳進或送出位址前綴。例如 BGP 允許管理員設置 ISP 如何處理位址前綴的策略，但實務上通常有困難。例如，BGP 並未允許一個 AS 告訴另一個 AS，限制某個位址前綴的播送 (Advertisement) 只發送給某個區域的對等實體。然而，ISP 可以發佈一個列表，上面列出公開或專有社群，並為每個社群提供描述。RFC 1997 定義三個具有全球意義知名社團：NO_EXPORT 社團、NO_ADVERTISE 社團和 NO_EXPORT_SUBCONFED 社團。RFC 7611 定義 ACCEPT_OWN 社團。RFC 4360 中新增 Extended Community Attribute 定義。由 IANA 管理 BGP Extended Communities Types。

## 六.BGP 路由反射器 (BGP Route Reflector)

大型 AS 網路內，也可選擇使用 iBGP。由於 BGP 使用 TCP 傳送路由訊息，當網路規模夠大，iBGP 比 OSPF 能更加穩定可靠傳輸路由訊息。對於路由器來說，eBGP 和 iBGP 只是對應參數不一樣，但都是通過同一個 BGP 行程 (Process) 運作，不會增加路由器負擔。只

需要建立好eBGP和iBGP之間連接，相對路由就可以通過BGP傳送。同時，AS內部中介路由器 (Intermediate Router) 路由表可以比較小，因為不需要處理AS以外路由信息。

從iBGP對等實體獲得的路由資訊通常只會分發給所有eBGP對等實體，不會傳遞給其他iBGP對等實體，目的防止產生循環 (loop)。

BGP Route Reflector (RFC 4456) 是一種特殊iBGP路由器，它會將學習到的iBGP路由，傳遞給所有連接的BGP Route Reflector客戶端，可以避免iBGP對等實體全連接要求，如下圖所示。

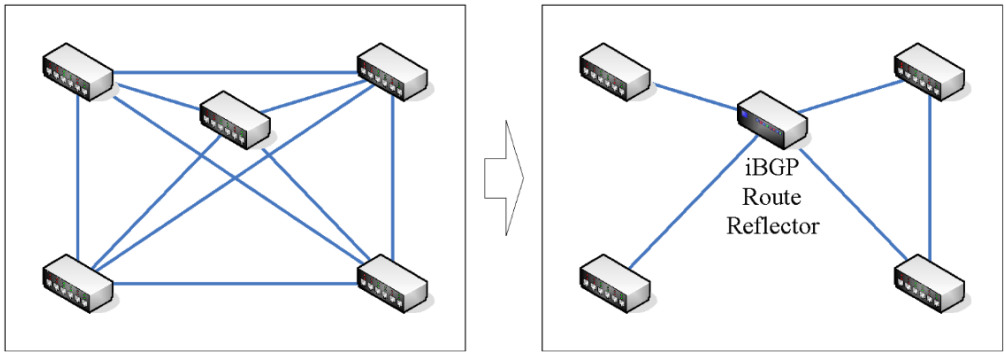



圖 196、iBGP Route Reflector

BGP Confederation (RFC 5065) 為另一種處理方式，如將一個大型AS內iBGP路由器，劃分到多個小的Sub-AS，如下圖所示。

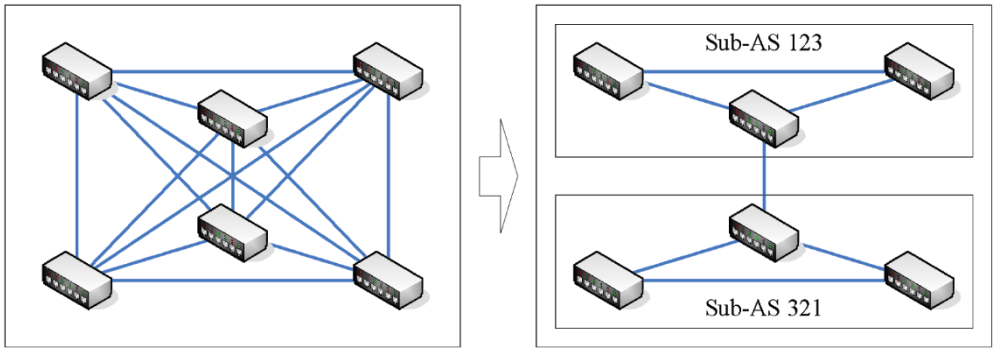



圖 197、BGP Confederation

## 七.BGP 重啟

當一個 BGP 路由器與一個對等實體連接中斷時，會認為此對等實體已經無法運作，因此會刪除之前由此對等實體學習到的路由訊息，希望以最快速度收斂到整個網路最新狀態。但與對等實體連接中斷並不一定代表對路由無法運作，可能只是 TCP 連接有問題，或是〝Keep-alive〞訊息丟失。或對等實體正在重新啟動中，很快就能恢復。此狀況將造成該 BGP 路由器必須重新學習在之前一段相對短時間內才剛剛被刪除掉的路由訊息。

如果對等實體之間連接才剛剛斷開，BGP 路由器就開始刪除相關的路由，短時間又很快重新建立連接、新增路由，可能會造成 BGP 路由器上路由反轉，產生短時間內的路由環路或者路由黑洞。此路由反轉甚至可能傳遞到整個數據中心，消耗路由器控制平面的計算能力，甚至引起整個網路的抖動。特別是現在許多 BGP 路由器是以軟體實作方式，軟體維護與更新經常需要重新啟動 BGP 路由器。

RFC 4724 為 BGPv4 和 Multiprotocol BGP 新增了 Graceful Restar 重啟機制。使用 Graceful Restart，在 BGP 對等實體之間發生連接中斷時，BGP 路由器不會在很短時間內就刪除相對路由信息，以確保網路穩定性。

## 第四節 RPKI (Resource Public Key Infrastructure，網際網路號碼資源公鑰基礎建設)

網路使用 BGP 進行路由資訊交換，達成各 ISP 之間互相溝通。但由於 BGP 協定運作屬於信任制，而發生駭客散布錯誤路由資訊或網路管理者宣布錯誤路由，造成全球網路骨幹流量異常流動與無法連線等現象，為解決此問題全球網路註冊管理機構開始推動資源公鑰基礎建設 (Resource Public Key Infrastructure，RPKI)。

資源公鑰基礎建設是一個基於公共密鑰基礎建設 (Public Key Infrastructure，KPI) 框架，讓各 ISP 在交換路由時，驗證來源的合法性，確保路由安全。特別是在邊界閘道器協定 BGP 上，RPKI 提供將網際網路號碼資源資訊 (如 IP 地址) 連結到信任錨 (Trust Anchor) 的方法。使用 RPKI，號碼資源的合法持有者，能夠掌握網際網路路由協定運作，以防止路由劫持和其他攻擊。

由於路由協定存在可能損害用戶或整體網路操作的攻擊風險，由網際網路工程任務組 (Internet Engineering Task Force，IETF) 訂定的 RPKI 標準提供一種安全的方法來認證網際網路號碼資源的分配，以作為確保路由安全的一個步驟。合理設計及實現 RPKI 是全球路由系統安全的先決條件，也是建立全球網際網路可靠性的先決條件。

RPKI 將 IP 位址以及 ASN 利用公鑰基礎建設對所有權進行驗證，透過最初由網際網路號碼分配局 (Internet Assigned Numbers Authority，IANA) 分配到區域網際網路註冊管理機構 (Regional Internet Registry，RIR)，再由 RIR 分配給本地網路註冊管理機構 (Local Internet Registry，LIR)，最後由 LIR 分配給使用者的網路號碼

資源進行認證，以提高網路資料傳輸安全性。

# 一.資源憑證與子物件

在[RFC 3779]文件中描述，資源公鑰基礎設施 (RPKI) 使用帶有 IP 位址和 AS 識別碼擴充名的 X.509 PKI 證書。允許區域網際網路註冊管理機構成員，即本地網際網路序號產生器取得一個資源憑證，並列出其所持有之網際網路號碼分配局 (IANA) 的資源。此證明其持有之有效性，但該憑證並不含身分資訊。透過使用此資源憑證，本地機構可為其所持有之位址前綴執行路由宣告建立密碼學證明。以上所描述的證明被稱為路由起源授權 (Route Origin Authorization，ROA)。

## (一) 憑證頒發機構 (Certificate Authority，CA)

RPKI 使用 [RFC3779] 文件中定義 X.509 授權憑證格式，將 IP 位址及 ASN 組合進行簽署，憑證結構依據網際網路資源分發方式，每一個網際網路號碼資源的註冊單位都是憑證授權中心，在註冊單位將 IP 位址及 ASN 配發給下級單位時，同時會簽署一張資源憑證給該單位，以確認此資源所有權。

所有網路號碼資源由 IANA 統一分發，所以 IANA 具有所有號碼資源憑證，當 IANA 將號碼資源分配給五個區域網路註冊管理機構 (Regional InternetRegistries，RIRs) 時，也同時簽署資源憑證給 RIRs，當 RIRs (如 APNIC) 再將其資源向下分配給國家網路註冊管理機構 (National InternetRegistries，NIRs) 時，也會同時簽署資源憑證給 NIRs，因此 RIRs 及 NIRs 也需扮演憑證授權中心的角色。下圖為 RPKI 憑證頒發機構層級架構圖：

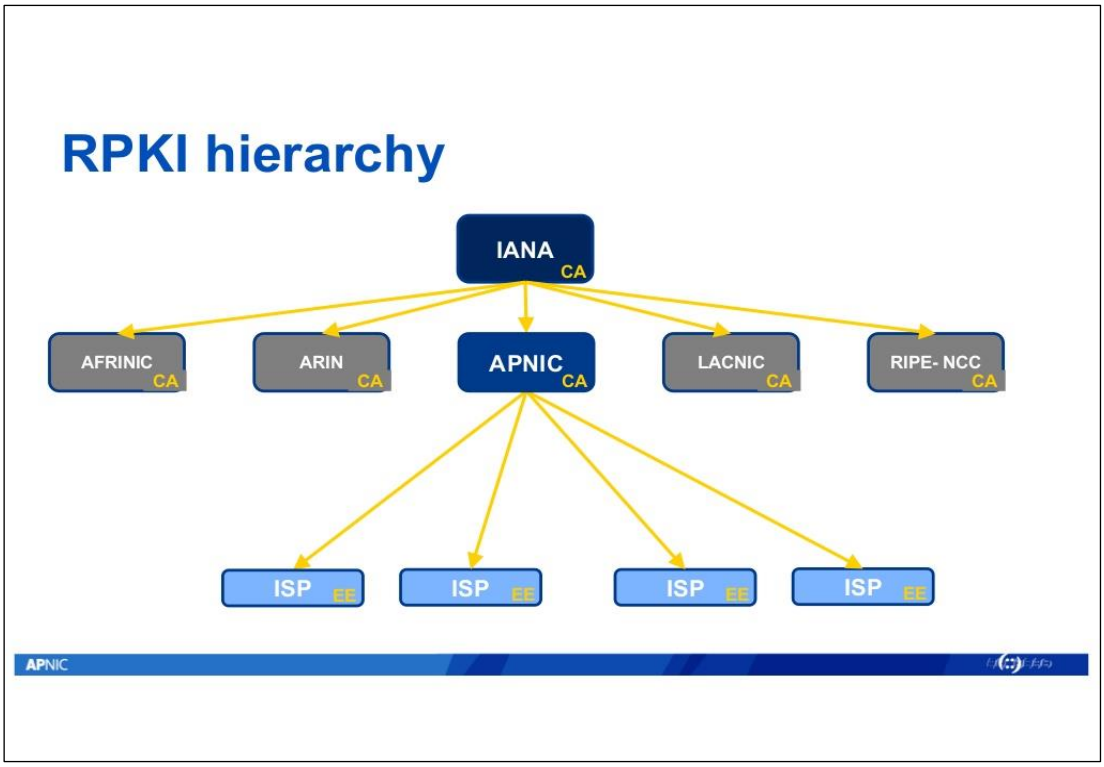



圖 198、RPKI 憑證頒發機構層級架構圖

## (二) 公開金鑰基礎建設 (Public Key Infrastructure，PKI)

公開金鑰認證（Public key certificate），又稱數位憑證（digital certificate）或身分憑證（identity certificate）。是用於公開金鑰基礎建設的電子檔案，用來證明公開金鑰擁有者的身分。此檔案包含了公鑰資訊、擁有者身分資訊（主體）、及數位憑證認證機構（發行者）對這份檔案的數位簽章，以保證此檔案整體內容正確無誤。

X.509 是密碼學裡「公開金鑰認證」 (Public key certificate) 的一種格式標準。X.509 憑證已應用在包括傳輸層安全性協定 (Transport Layer Security，TLS) 及安全通訊協定 (Secure Sockets Layer，SSL) 等網路協定中，同時也使用在很多非線上的應用服務如電子簽章等。X.509 憑證內容含公鑰、身分資訊 (網路主機名、組織名稱或個體名稱等) 和簽章資訊 (可以是憑證授權機構簽章，

或自簽章)。經由可信度高的憑證簽發機構簽章或以其它方式驗證的憑證，憑證擁有者就可以用憑證與相對的私鑰來建立安全通信，對文件進行數位簽章或加密。

除憑證功能之外，X.509 並附帶憑證吊銷列表 (Certificate Revocation List，CRL) 和憑證合法性驗證演算法。

IETF 的公鑰基礎設施 (X.509) 簡稱 PKIX 工作群組將該標準制定成更靈活適用於網際網路組織。X.509 認證在[RFC5280] 文件中定義以 X.509 v3 為參考，對 IETF 的 PKIX 憑證和憑證吊銷列表 (Certificate Revocation List，CRL)，也稱為公開金鑰基礎建設 (Public Key Infrastructure，PKI)。下圖為 PKI 實體架構：

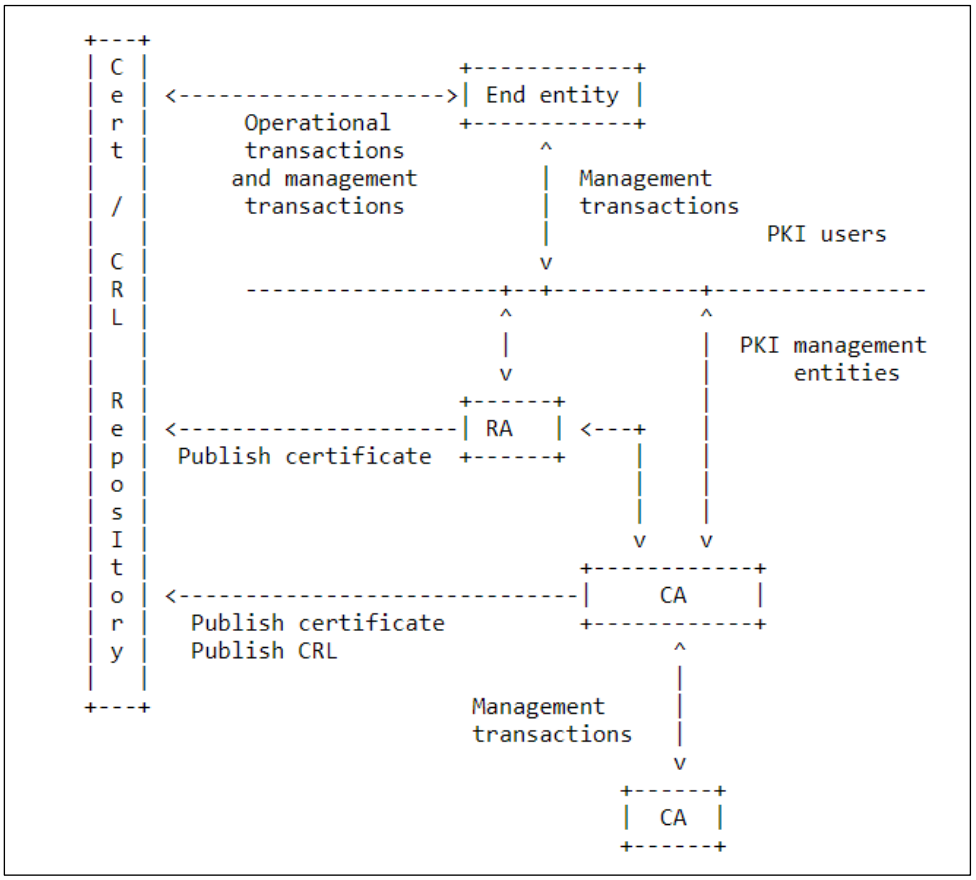



圖 199、PKI 實體架構

憑證頒發機構 CA 負責指明其頒發的證書其吊銷狀態，可使用在[RFC2560]文件中描述透過 Online Certificate Status Protocol (OCSP)、CRLs 或其他機制獲得證書的吊銷狀態。通常情況下，當吊銷狀態由 CRLs 提供時，CA 同時也是 CRL 發行者。然而 CA 可能負責頒發 CRLs 到不同的實體 (Entity)。

## (三)路由來源授權 (Route Origin Authorization，ROA)

ROA 是用來證明 IP 位址和 AS 號碼在 BGP 路由表資訊中為正確組合。ROA 可以用多個前綴來描述，其提供路由器來驗證從網路上公佈的 BGP 路由是否正確。ROA 除了記錄 IP 位址前綴和起源 AS 之外，有一個〝maxlen〞 (最大前綴長度) 的概念，即記錄允許的最大前綴長度，使得 ROA 能夠描述更長的前綴。

一個 ROA 是一個加密簽章物件，指出其自治系統 AS 號碼被授權於某個來源前綴，意味 ROA 說明此地址空間完成 BGP 公告。建立路由 ROA 的好處

- 驗證某個 AS 是否有權發布特定的 IP 位址前綴。
- 盡量減少常見的路由錯誤。
- 防止大多數的意外劫持。

任何其他前綴公告將被視為未經授權。透過發布具體前綴以強制聚合和防止劫持的一種方法。

在[RFC6488]中定義 ROA 使用 RPKI 數位簽章物件的樣板，該樣板為 ROA 內容定義了加密郵件語法 (Cryptographic Message Syntax，CMS)包裝程序，在[RFC5652]文件中有詳細敘述，並為 RPKI 簽章物件定義了通用驗證過程。在[RFC6488]文件第 4 部分中描述完成 ROA 的規範簡述如下：

- 將已簽章物件標識為 ROA 的 OID。

此 OID 出現在 encapContentInfo 物件的 eContentType 以及 signerInfo 物件的 content-typesigned 屬性內。

- ROA eContent 的 ASN.1 語法。

  此為有效負載，用於指定被授權發起路由的 AS 以及該 AS 可以向其發起路由的前綴。ROA eContent 是使用專有編碼規則 (DER) [X.690]進行 ASN.1 編碼。

## (四) 自治系統 (Autonomous System，AS)

由於多個組織可使用各自的自治系統編號，與將其連接到網際網路的 ISP 之間執行「BGP 協定」，因此大多應用[RFC 1930]文件中的定義。雖然 ISP 支援自治系統，但網際網路只能看到該 ISP 的路由策略。所以 ISP 必須具有一個公開且正式登記的自治系統編號 (Autonomous System Number，ASN)。

在 BGP 路由中每個自治系統都被分配一個唯一的自治系統編號 (ASN)。對 BGP 來說，因為 ASN 是區別整個網路中的各個網路的唯一標識，所以這個自治系統編號非常重要。網際網路號碼分配局將 64512 到 65535 的 ASN 編號保留給 (私有) 專用網路使用。

## (五) 信任錨 (Trust Anchors，TAs)

任何 PKI，每個依賴方 (Relying Party，RP) 都會選擇自己的一組信任錨 (TAs)。PKI 一般屬性也適用於此。現有 IP 地址空間和 AS 號碼分配的層次結構，IANA 和五個 RIR 即為此處預設的信任錨。每個 RP 最終選擇一套用於證書驗證信任錨。

## (六) 儲存庫

在[RFC6480]文件中描述，為驗證在 RPKI 中進行的證明，依賴方 (RP) 需要訪問所有 X.509 資源證書，證書吊銷列表 (CRL) 和共同定義 RPKI 已簽章物件。每個證書頒發者，CRL 或已簽章物

件，透過在 RPKI 儲存庫中發布物件來將其下載到 RPs。

RPs 需訪問儲存庫系統中所有已簽章物件。建立證書、CRL 和簽章物件資源庫發佈位置，可由儲存庫下載供 RPs 使用。

- 儲存庫物件：

  是指儲存庫發佈位置中的終端物件。終端物件通常被實作為可公開訪問的目錄中的文件，其中該文件不是目錄本身，該項包括具有與文件相似的公共樣子形式的物件。

- 儲存庫發佈位置：

  是指在公共發佈位置所發布的儲存庫物件集合。實作為由[RFC3986]文件 URI 標識的可公開訪問文件系統中的目錄，其外觀類似於文件的簡單目錄。

- 儲存庫範例：

  是指共享一個公共發布範例的一個或多個儲存庫發佈點集合。此作為共享公用 URI 前綴的文件系統目錄的集合來實作，每個目錄也可以透過其自己的唯一 URI 進行標識。

## 二.管理 RPKI

利用 GitHub 開源工具將頁面存檔備份，並存於網際網路檔案館 (Internet Archive) 可用於執行憑證頒發機構和管理資源憑證以及子物件 (例如 ROA) 且不會因時間延續而使資料消失。此外，在區域機構中若成員設有代管 RPKI 平台，本地機構可以選擇使用代管系統，或執行自己的軟體。

## 三.發布 RPKI

資源持有單位如 ISP，欲發布資料庫與一個或多個 RPKI 憑證點相關聯。與證書授權機構 (CA) 互動與執行時，可以選擇自己發布所

有加密資料，也可以依賴第三方發布。且可利用註冊單位簽署過的 IP 位址終端憑證及 ASN 終端憑證進行 ROA 建立，讓 IP 位址前綴與 ASN 關係連結起來，以下為與 CA 互動方式中的一種。

- CA 證書頒發

  客戶端使用此查詢來請求伺服器的 CA 為已分配或分配給客戶端資源頒發資源證書。若成功處理該請求，則伺服器回應將包含頒發的證書。

  客戶端必須為每個不同資源類使用不同的密鑰配對。

  發出者針對資源類和客戶的公鑰，將請求資源集合的值保存為本地記錄。之後指定相同資源類別和相同客戶端公鑰的證書頒發請求，將請求者資源集合頒發者本地記錄設置為最近指定的值。

- 證書要求

  使用密鑰對的私鑰部分對證書請求進行簽章，該密鑰對的私鑰部分是認證請求中的〝subject〞密鑰值。簽章演算法在[RFC6485]文件中有說明。簽章組件目的在證明擁有私鑰的證據。

  如果可以線上處理請求，則此請求回應為證書頒發回應。如果不能立即執行請求，則伺服器使用適當錯誤代碼回應〝請求未執行〞訊息。

## 四.驗證 RPKI (RPKI Validator)

當為特定源 AS 和位址前綴建立一個 ROA 時，註冊管理機構會將 ROA 紀錄逐筆儲存在本地資料庫中，ROA 是由多個分散資料庫所儲存，RPKI Validator 則是會利用同步機制 (rsync) 週期性同步下載建立好的加密 ROA 元件，並儲存一份本地驗證快取資料。若網路路由設備啟用 RPKI 技術，則可將網路路由設備與 RPKI Validator 建立

連結，將 ROA 元件資料下載網路路由設備中，供設備進行 BGP 路由策略使用，RPKI Validator 資料同步架構如下圖所示：

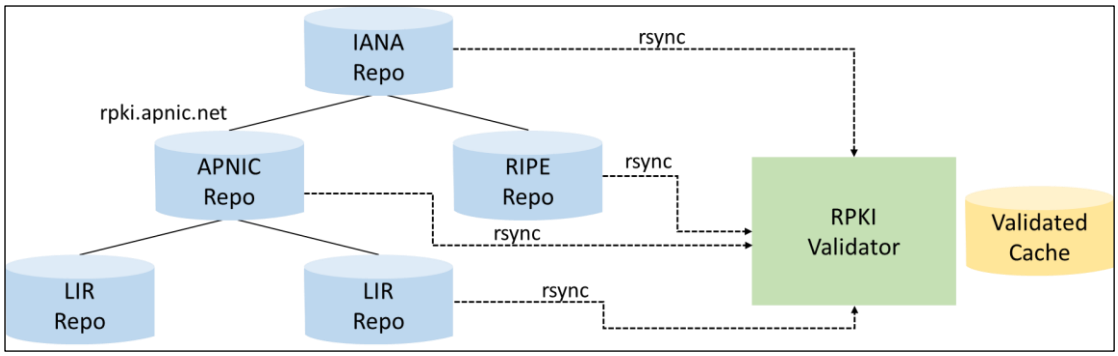



圖 200、RPKI Validator 資料同步架構

當網路路由設備同步完成本地驗證快取後，即可比對路由表中每筆 IP 位址前綴，作為路由表中 IP 網路位址來源有效性驗證使用，每一筆 IP 網路位址比對來源宣告後有以下三種可能結果：

- 有效(Valid)：

  代表該筆 IP 網路位址包含在一個 ROA 元件中，且自治系統號碼一致，是來源合法的 IP 網路位址宣告。

- 無效 (Invalid)：

  代表該筆 IP 網路位址包含在一個 ROA 元件中，且自治系統號碼不一致，表示此 IP 沒有獲得授權，或是此 IP 網路位址宣告長度超過 ROA 中設定的最大長度。

- 未知 (Not found/Unknown)：

  代表該筆 IP 位置未包含於 ROA 紀錄中，無紀錄可供比對，無法確定其來源宣告的合法性。

## 五.路由決策

經過ROA驗證後證明可以與BGP路由一同協助網路業者的決策

過程。此項決策過程可以以手動方式去完成，但已驗證位址前綴原始資料也可以使用[RFC 6810]的 RPKI to Router Protocol 文件描述將 Notify 消息傳送到支援的路由器，關於 RPKI to Router Protocol 運作原理大致如下：

- 當路由器從快取 (cache) 中接收到所有數據記錄時，會將其序列號設置為數據 PDU (Power Distribution Unit) 末尾中的序列號。
- 當快取更新其資料庫時，將向每個連接路由器發送一條 Notify 訊息。此舉將提示路由器現在是調查新版的好時機。
- 該協議要求路由器在任何情況下都定期調查更新 (詳細原理請參考 RFC 6810 第 4 節)。

而相關技術也有多家廠商進行實作，包括思科 Cisco 網路使用 IOS-XR 及 IOS-XE 之作業系統的路由設備，版本在 XR4.3.2 及 XE3.5 版之後，即有支援 RPKI 之技術。其他像是 Quagga 網路路由設備，也利用 BGP Secure Routing Extensions (BGP-SRx) 技術或以 RTRlib 為基礎的一個 RFC-compliant 實作 RPKI 功能。

[RFC 6494] 更新鄰居發現協定 (ND) 安全機制 (即安全鄰居發現協定，SEND) 的憑證驗證方法，可在 IPv6 中使用 RPKI。其使用修改 [RFC 6487] RPKI 憑證組態定義 SEND 憑證組態，包含[RFC 3779] 文件 IP 位址委派擴充。即在 SEND 中使用的證書 (由路由器，代理或地址所有者使用) 必須符合此證書配置文件，並且可以符合 [RFC3971] 中的原始配置文件。

# 第五節 DNSSEC (Domain Name System Security Extensions，域名系統安全擴充)

網域名稱系統 (Domain Name System，DNS)，做為網路名稱轉換數位 IP 地址功能。由 ICANN 對定址系統進行協調，確保所有位址唯一性。因 DNS 存在部份漏洞，而引進 DNS 安全擴展 (DNS Security Extensions，DNSSEC) 技術，以保護網際網路基礎設施。

DNSSEC 使用〝委託簽署者 (Delegation Signer，DS) 資源記錄〞在代理之間的委託點上提供附加級別的間接訪問。驗證 DNS 區域的密鑰資源紀錄集 (Resource Record set，RRset) 需要兩次簽章驗證操作，當子級的主公鑰發生更改時，子級將新的公鑰發送給其父級。父級只需為每個子級儲存一個主公鑰即可。而客戶端在驗證密鑰時必須做第二次驗證操作。

## 一.DNS 常見攻擊

DNS 是多數網際網路請求組成重要部分，使 DNS 成為惡意攻擊主要目標。最常見的攻擊方法如下所列：

- DNS 詐騙/快取記憶體中毒：

  攻擊將偽造的 DNS 資料引入 DNS 解析程式快取記憶體中，造成解析程式傳回不正確的網域 IP 位址。流量可能會被轉移到惡意電腦或攻擊者想要的位置，如分發惡意程式碼或收集登入資訊。

- DNS 通道建立：

  此攻擊使用其他通訊協定，透過 DNS 查詢和回應建立通道。攻擊者可以使用 SSH、TCP 或 HTTP 將惡意程式碼或竊取資訊傳遞至 DNS 查詢中，且不會被大部分防火牆偵測到。

- DNS 劫持：

  在DNS劫持中，攻擊者將查詢重新導向至不同網域名稱伺服器。透過惡意程式碼或未獲授權 DNS 伺服器修改來進行。其結果與DNS詐騙結果相似，但其目標是名稱伺服器上網站的DNS記錄，而不是解析程式快取記憶體。

- NXDOMAIN 攻擊：

  此類為 DNS 洪水攻擊，攻擊者要求不存在的記錄，大量請求讓 DNS 伺服器應接不暇，企圖造成合法流量的阻斷服務。NXDOMAIN 攻擊也能以遞迴解析程式為目標，目的是使用垃圾請求填充解析程式的快取記憶體。

- 幻影網域攻擊：

  幻影網域攻擊的結果與DNS解析程式的NXDOMAIN攻擊相似。攻擊者設定一串「幻影」網域伺服器，以非常緩慢的速度回應請求，或完全不回應請求。解析程式因為網域洪水般的請求而遭受攻擊，被困在等待回應過程中，導致效能緩慢和阻斷服務。

- 隨機網域攻擊：

  攻擊者對某個合法網站的數個不存在的隨機子網域傳送 DNS 查詢。目標是對網域的權威名稱伺服器建立阻斷服務，使其無法從名稱伺服器查閱網站。副作用為攻擊者服務的ISP也可能會受到影響，因為其遞迴解析程式快取記憶體將會載入不良請求。

- 網域鎖定攻擊：

  攻擊者會設定特殊網域和解析程式，用來建立與其他合法解析程式的 TC 連線。當目標解析程式傳送請求時，此網域會傳回緩慢的隨機封包串流，纏住解析程式的資源。

- 殭屍網路式 CPE 攻擊：

此攻擊使用 CPE 裝置（如資料機、路由器、機上盒等）進行。攻擊者入侵 CPE，而裝置就成為殭屍網路的一部分，用來針對某個網站或網域執行隨機子網域攻擊。

## 二.DNSSEC 資源記錄

DNS 透過資源記錄 (Resource Record Type ，RRTYPE) 實現。DNSSEC 使用相同方法，新增或修改 DNS 記錄類型與 DNSSEC 一起使用。下表為 DNSSEC 資源記錄：

表 115、DNSSEC 資源記錄

| 序號 | RR Type | 描述 |
|---|---|---|
| 1 | RRSIG | 資源記錄簽章 (Resource Record Signature)，包含一個記錄集 DNSSEC 簽章。DNS 解析器使用儲存在一個 DNSKEY 記錄中的公開金鑰驗證簽章。 |
| 2 | DNSKEY | 含用來驗證 RRSIG 記錄中 DNSSEC 簽章的 DNS 解析器的公開金鑰。 |
| 3 | DS | 委託簽署者 (Delegation Signer)，存放委託區域的名稱。在子授權區域中引用 DNSKEY 記錄，DS 記錄與委派的 NS 記錄一起放在父區域中。 |
| 4 | NSEC | 下一個安全記錄 (Next Secure Record)，含指向該區域中下一個記錄名稱的鏈接，及該記錄名稱的記錄類型。DNS 解析器使用 NSEC 來驗證記錄名稱和類型的不存在，作為 DNSSEC 驗證一部分。 |
| 5 | NSEC3 | 下一個安全記錄版本 3 (Next Secure Record Version 3)，含指向該區域中下一個記錄名稱的鏈接 (按雜湊名稱排序)，並在 NSEC3 記錄自己名稱的第一個標籤中列出雜湊值所覆蓋名稱的記錄類型。解析程序使用此記錄來驗證記錄名稱和類型的不存在，作為 DNSSEC 驗證的一部分。NSEC3 記錄與 NSEC 記錄相似，但是 NSEC3 使用加密雜湊記錄名稱，避免列舉區域中的記錄名稱 |
| 6 | NSEC3PARAM | 下一個安全記錄版本 3 參數 (Next Secure Record Version 3 parameters)，權威 DNS 伺服器使用此記錄來計算和確定要對不存在的名稱/類型的 DNSSEC 請求進行回應的 NSEC3 記錄。 |

## 三.加密演算法

DNSSEC 被設計為具擴展性，因此當發現針對現有加密演算法攻擊時，可以向後兼容方式引入新演算法。由於業界普遍傾向於橢圓曲線密碼學，DNSSEC 部署推薦使用 ECDSA P-256/SHA256 作為 DNSKEY 演算法，基於 RSA 演算法的使用者應該升級到 ECDSA P-256/SHA256。

與 RSA/SHA-256 或 RSA/SHA-512 相比，ECDSA P-256/SHA-256 以較短的簽章長度提供更高加密強度。ECDSA P-256/SHA-256 已被廣泛部署。驗證和簽章都必須使用。在實現 ECDSA P-256/SHA-256 和 ECDSA P-384/SHA-384 時，建議使用[RFC 6979]文件中指定的橢圓曲線數位簽章演算法 (ECDSA) 的確定性數字簽章生成過程。

下表列出有關[DS-IANA]委託簽署者摘要演算法建議。此建議適用於[RFC7344]中指定的子委託簽署(Child DS，CDS) RRTYPE。

表 116、DS 和 CDS 加密演算法

| 序號 | 演算法 | 選項 | 驗證 |
|---|---|---|---|
| **0** | NULL(CDS only) | MUST NOT [*] | MUST NOT [*] |
| **1** | SHA-1 | MUST NOT | MUST |
| **2** | SHA-256 | MUST | MUST |
| **3** | GOST R 34.11-94 | MUST NOT | MAY |
| **4** | SHA-384 | MAY | RECOMMENDED |

[*]：特殊類型 CDS 記錄，表示在[RFC8078]中刪除父級 DS。

- NULL 是一種特殊情況；請參閱[RFC8078]文件說明。
- SHA-1 廣泛用於委託簽署者 (DS) 記錄，因此驗證器必須實施驗證，但不要用於生成新的 DS 和 CDS 記錄。

- SHA-256 廣泛使用，因此驗證器必須實施驗證及生成新的 DS 和 CDS 記錄。
- GOST R 34.11-94 已在[RFC6986]文件中被 GOST R 34.11-2012 取代。但 GOST R 34.11-2012 尚未標準化用於 DNSSEC。
- SHA-384 與 SHA-256 共享相同屬性，但與 SHA-256 相比具有安全優勢 (384 位元的強度與 256 位元的強度)。對於 DNSSEC 大多數應用，SHA-256 應該令人滿意且強大，因此建議將其用於 DS 和 CDS 記錄。目前沒有需要 384 位元安全強度的 DNSSEC 使用案例出現，但為此類應用程式提供了 SHA 384，但還是可用於生成 DS 和 CDS 記錄。

## 四.DNSSEC 運作流程

下圖為 DNSSEC 運作流程解構圖：

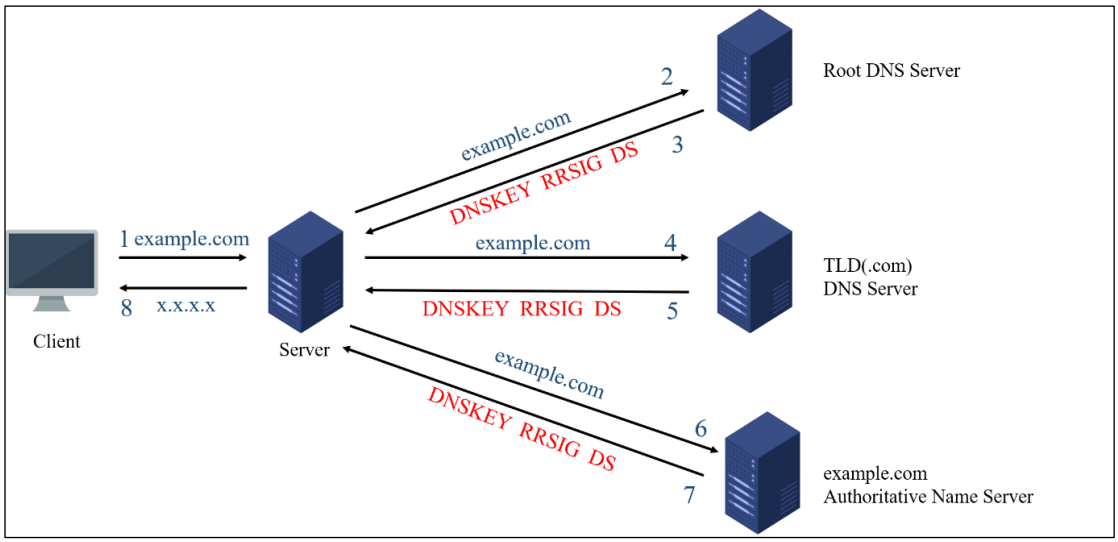



圖 201、DNSSEC 運作流程解構圖

DNSSEC 運作流程如下：

●Step1：使用者向 DNS 伺服器要求解析 example.com 的網址。

- Step2：伺服器向 Root 伺服器詢問。
- Step3：Root 伺服器回應自己的 DNSKEY、RRSIG 和下層伺服器 DS 金鑰。
- Step4：向 com 層級 DNS 伺服器詢問。
- Step5：com 層級 DNS 伺服器回應自己的 DNSKEY、RRSIG 和下層伺服器 DS 金鑰，伺服器利用從 Root 伺服器取得 DS 金鑰比對和.com 所提供的是否一致。
- Step6：向 example.com 所在 DNS 伺服器詢問。
- Step7：example.com 所在 DNS 伺服器回應自己的 DNSKEY、RRSIG，伺服器利用從.com 取得 DS 金鑰比對和 example.com 所提供的是否一致。
- Step8：回應 x.x.x.x 的 IP 位置給使用者。

根據 DNS 搜尋結果，安全的 DNS 解析器可以確保查詢域的權威名稱伺服器是否支援 DNSSEC，所得答案是否安全以及是否存在錯誤。遞迴名稱伺服器和存根解析器，搜尋過程有所不同。以下分別說明：

## (一)遞迴名稱伺服器

使用信任鏈模型，父系網域中的委託簽章者 (DS) 記錄可以用來驗證子域中的 DNSKEY 記錄，子域可包含其他 DS 記錄來驗證進一步的子域。假設遞迴解析器 (比如 ISP 名稱伺服器) 想要獲得功能變數名稱〝www.example.com〞的 IP 位址 (AAAA 記錄)。需執行以下事項：

- 當安全的 DNS 解析器在進行 DNS 查詢中開始會設置〝DO〞(DNSSEC OK） 標誌。由於〝DO〞位於 EDNS 定義的擴展標誌，因此所有 DNSSEC 事務都必須支持 EDNS。EDNS 支援需要允許 DNSSEC 所需更大的封包大小。

- 當解析器透過正常 DNS 搜尋過程收到答案時，將進行檢查以確保答案正確。理想情況下，安全解析器將由驗證 DNS 根目錄處 DS 和 DNSKEY 記錄開始。使用在根目錄中找到的〝com〞頂級域名 DS 記錄來驗證〝com〞區域中的 DNSKEY 記錄。確認在〝com〞區域中是否存在〝example.com〞子域 DS 記錄，如果有，將使用 DS 記錄來驗證在〝example.com〞中找到的 DNSKEY 記錄。最後，驗證在〝www.example.com〞A 記錄答案中找到的 RRSIG 記錄。

上面的範例有幾個例外。首先，如果〝example.com〞不支援 DNSSEC，答案中將沒有 RRSIG 記錄，並且〝com〞區域中沒有〝example.com〞DS 記錄。如果有〝example.com〞DS 記錄，但不包含 RRSIG 記錄，則是出了問題，可能是中間管理人員進行 DNSSEC 訊息修改及修改 A 記錄。或者，可能是一台損壞的安全性名稱伺服器，從查詢中刪除〝DO〞標誌或從回覆中刪除了 RRSIG 記錄。

接下來，可能是沒有域名〝www.example.com〞，在此情況下，不會返回答案中的 RRSIG 記錄，而是一個 NSEC 記錄或 NSEC3 記錄。回覆〝下一個安全〞記錄，可讓解析器證明域名不存在。NSEC/NSEC3 記錄具有 RRSIG 記錄，可以如上所述進行驗證。

最後，可能是〝example.com〞區域實作了 DNSSEC，但是〝com〞區域或根區域都沒有，形成一個〝安全島〞，需要以其他方式進行驗證。西元 2010 年 DNSSEC 根的部署已完成。.com 域已使用有效安全密鑰簽章，且安全委派已西元 2011 年完成增加到根區域。

## (二) 存根解析器

存根解析器是使用遞迴查詢模式將大部分 DNS 解析工作分流

到遞迴名稱伺服器的最小 DNS 解析器。存根解析器將簡單地將請求轉發到遞迴名稱伺服器，並以 Authenticated Data (AD) 位用作為提示，以查明遞迴名稱伺服器是否能夠驗證所有遞迴名稱伺服器回應的答案和權限部分中所有數據的簽章。

驗證存根解析器可能透過其查詢消息設置 Checking Disabled (CD) 位元執行自己的簽章驗證。驗證存根解析器使用 CD 位元執行自己的遞迴身份驗證。使用此驗證存根解析器可以為實作 DNSSEC 的區域提供客戶端的點對點 DNS 安全性。

## 五.信任錨 (Trust anchors)

要證明 DNS 答案是否正確，要從 DNS 以外來源知道至少一個正確金鑰或 DS 記錄。此起點稱為信任錨，通常驗證解析器須通過 DNS 協議之外的某些安全或可信來源獲取其信任錨的初始值。最初設計 DNSSEC 時，認為唯一需要信任錨點是 DNS 根伺服器。根錨首次發佈於西元 2010 年。信任錨是放置在驗證解析器中的密鑰，以便驗證器可以將給定請求的結果驗證返回已知或信任的公開金鑰 (信任錨)。驗證解析器必須至少安裝一個信任錨才能執行 DNSSEC 驗證。

## 六.否定信任錨 (Negative Trust Anchors, NTA)

DNS 遞迴解析器的運營商，例如 ISP 偶爾會發現區域錯誤管理與 DNSSEC 相關的資源記錄。因而觸發 DNSSEC 驗證失敗，導致大量最終用戶無法訪問特定域。用戶會將其解釋為 ISP 或解析器營運商的問題，而切換到非驗證解析器或聯繫其 ISP 進行投訴，而不是認為用戶想要到達的域名失敗。此壓力可能會導致解析程序操作員禁用或不願意部署 DNSSEC 驗證。

在 DNSSEC 部署過渡期間，可以使用否定信任錨 (NTA)。NTA

在驗證 DNS 遞迴解析器上本地配置，以保護終端用戶免受 DNSSEC 相關權威名稱伺服器操作錯誤影響。NTA 一般為臨時性由需要 NTA 的組織實作，而不是由管理邊界之外的組織分發。

使用 NTA 臨時禁用特定配置錯誤域名的 DNSSEC 驗證會立即恢復終端用戶的訪問權限。使網域管理員可以解決其錯誤配置，同時還允許使用 NTA 的組織保持啟用 DNSSEC 驗證的狀態，並且仍然可以訪問錯誤配置的網域。以下為否定信任錨能夠改善的三種情況：

- 緩解域驗證失敗

  域名驗證失敗的原因有兩個：一般的安全性失敗 (例如由於某種攻擊或破壞) 或區域管理員配置錯誤。當網域過渡到 DNSSEC 時，驗證失敗的最常見原因是配置錯誤。

  因不同軟體開發人員對 DNSSEC 標準解釋方式或開發人員選擇實作 DNSSEC 支援方式不同，也可能導致 DNSSEC 驗證失敗。

- 改善最終用戶 (End-User) 體驗

  用戶通常不知道或不了解導致連接發生的解析過程。因此用戶應該不知道 DNSSEC 驗證或任何訊息。若是 DNSSEC 相關錯誤配置，讓用戶誤解無法訪問該網域。用戶可能認為 ISP 故意阻止了對該網域的訪問，或是 ISP 方面 (DNS 伺服器) 性能故障。他們可能會聯繫 ISP 進行投訴，讓 ISP 產生客訴。

  使用 NTA 將允許 ISP 特別糾正無法到達該網域的故障，而不會影響其他站點的安全性，且不需要停用 DNSSEC。讓用戶滿意，對 ISP 影響最小，同時正確維護網域安全性。

- 避免切換到非驗證解析器

  如果網域未通過 DNSSEC 驗證並且無法訪問，很可能有與安全相關的問題。為了安全考量，用戶不應將 DNS 伺服器更改為不

執行 DNSSEC 驗證的方法解決問題。相對於配置錯誤，使 DNSSEC 失敗的網域可能受到駭客控制，或者該網域可能存在其他重大安全問題。因此，不建議切換到非驗證解析器以恢復對 DNSSEC 驗證失敗的網域訪問。

## 七.信任鏈 (Chain of trust)

下圖為信任鏈示意圖：

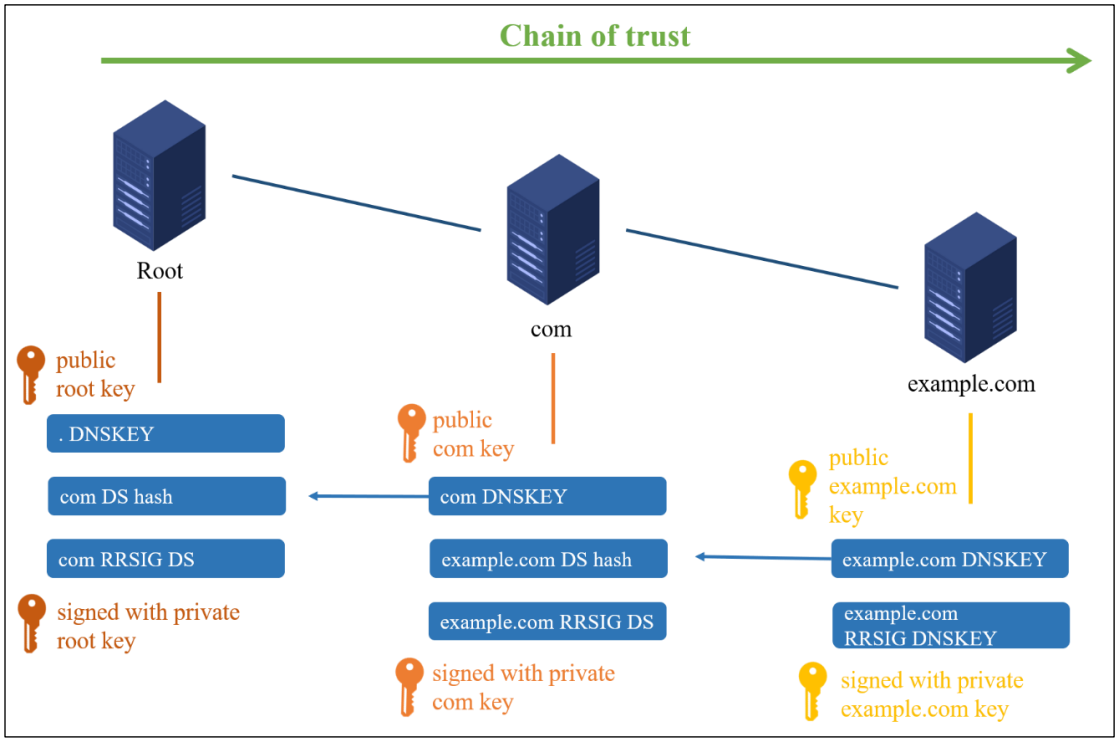



圖 202、信任鏈示意圖

在 DNSSEC 中，查詢名稱伺服器使用區域的公鑰來驗證區域中的簽章數據。而公開金鑰的有效性是由區域的父級別確定。例如，如果我們的簽章區域稱為 example.com，那麼為 example.com 區域的公開金鑰擔保的就是 com 區域。

在 example.com 區域簽章後，管理員會將其公開金鑰的副本以及

確定其為example.com區域的正式授權管理員的所有必要訊息發送給com區域的管理員。一旦com區域的管理員對自己擁有example.com區域的合法公鑰確認，就會將新記錄增加到com區域，稱為DS記錄。DS記錄包含公開金鑰的指紋。com區域管理員在com區域簽章，該區域增加了RRSIG記錄，以證明此新DS記錄的真實性。

當在example.com中解析域名的名稱伺服器查詢其中一個com名稱伺服器時，將收到包含DS記錄的example.com名稱伺服器的引用。而在引用中的NS記錄和DS記錄都會經過簽章。當查詢名稱伺服器查找example.com DNSKEY記錄以驗證已簽章的example.com記錄，首先其將從DS記錄中的指紋驗證DNSKEY記錄。

## 八.數位簽章和區域簽章

為了限制重播攻擊，須採用DNS TTL值，且在RRSIG記錄中還有用於限制簽章有效性的額外時間戳記。與 TTL 值相對於記錄發送的時間不同，時間戳記為絕對值。意味著所有安全 DNS 解析器必須有相當緊密同步的時鐘，比如在幾分鐘內。

此時間戳記必須定期重新簽署區域並將其重新分發到次要伺服器，否則簽章將被驗證解析器拒絕。DNSSEC 引入了簽章區域的概念。簽章區域分別包括 DNS 公鑰 (DNSKEY)、資源記錄簽章 (RRSIG) 、下一安全 (NSEC)、及委託簽章者 (DS) 記錄。

## 九.密鑰管理

DNSSEC 涉及許多不同的密鑰，儲存在 DNSKEY 記錄中，同時也儲存在其他來源中，以形成信任錨。為了允許替換密鑰，除了現有的舊密鑰之外，還涉及在新的 DNSKEY 記錄中出現的新密鑰。當生存時間值超過導致舊密鑰緩存過時，可以使用新密鑰。最後，當使用

舊密鑰的記錄緩存過時，就可以刪除舊的 DNSKEY 記錄。

DNSKEY 記錄中的金鑰可用於兩種不同的事物，通常每種金鑰都使用不同的 DNSKEY 記錄。分別有用於簽章其他 DNSKEY 記錄的 KSK，以及用於簽章其他記錄的 ZSK。

## 十.工具

DNSSEC 部署需要伺服器端和用戶端上的軟體。支援 DNSSEC 的工具包括：

- Windows 7 和 Windows Server 2008 R2 包括一個〝安全感知〞的存根解析器，能夠透過遞迴名稱伺服器區分安全回應和不安全回應。Windows Server 2012 DNSSEC 相容主動目錄集成區域的安全動態更新，以及主動目錄複寫錨鍵到其他此類伺服器。
- BIND 是最流行的 DNS 名稱伺服器 (包括 dig)，其合併較新的 DNSSEC-bis (DS records) 協定及對 NSEC3 記錄的支援。
- Unbound 是一個根據 DNSSEC 概念從頭開始設計的 DNS 名稱伺服器。
- mysqlBind 為 DNS asp 的 GPL DNS 管理軟體已支援 DNSSEC。
- OpenDNSSEC 為 DNSSEC 簽署者工具，使用 PKCS#11 與硬體安全模組介面。
- Knot DNS 在 1.4.0 版本中增加對自動 DNSSEC 簽名的支援。
- 從 3.0 版本開始，PowerDNS 完全支援預簽名和即時簽名模式的 DNSSEC。

## 十一.物聯網 IoT 設備與 DNSSEC

現代具有 IP stack 的 IoT 設備通常與網際網路上的一個或多個遠程服務交換數據，並使用 DNS 服務。因為物聯網設備可以感知物理

環境，因此具有 DNS 功能可以滿足部分安全性、穩定性和透明度要求。例如，連接門鎖控制軟體需要確保其與用戶向其發送解鎖指令的網際網路服務進行對話。如果 IoT 設備驗證了 DNSSEC 簽章，則將能夠發現 DNSSEC 驗證錯誤。DNSSEC 驗證錯誤通常是中間人攻擊的結果，例如，於西元 2018 年 4 月針對亞馬遜的路由劫持。如果沒有 DNSSEC，設備將不會注意到此類攻擊，並且會從惡意目的地發送或接收流量，可能會危害用戶的安全和隱私。但廣泛地用於傳統網際網路應用程式的 DNSSEC 已經具有挑戰性，對於 IoT 而言則更為複雜，因為它需要許多不同的 IoT 操作系統 (例如 OpenWRT，RIOT 和 Contiki) 的支援，並且必須處理更多的硬體 (例如，限制在低功耗硬件上實作密碼功能)。DNSSEC 檢測 IoT 設備主要功能為：

## (一)使用 DNSSEC 檢測 IoT 設備的惡意重新導向

DNSSEC 能為 IoT 設備檢測惡意重新導向的問題，DNSSEC 在 DNS 中提供了訊息完整性，表示解析程序能夠檢測對 DNS 訊息的內容進行更改的駭客行為 (例如透過假訊息加入解析程序緩存中)。這在物聯網中尤其重要，因為操縱 DNS 訊息會將物聯網設備重新定向到惡意服務，而危害用戶隱私和安全。

DNSSEC 透過對 DNS 記錄進行數位簽章，使解析程序可以使用 DNSSEC 的信任鏈來驗證簽章。驗證錯誤表示權威名稱伺服器的回應可能已被篡改，例如，由於中間發生了路由劫持或人員入侵。例如，啟用智慧手錶的 DNSSEC 解析器檢測到重新定向，因為無法驗證從駭客名稱伺服器接收到的 DNS 記錄，因為未簽章或簽章無效。解析器向智慧手錶返回錯誤，以防止將智慧手錶的測量結果傳輸到惡意服務，避免設備被劫持。

## (二)DNS 協議以雙重檢查 IoT 服務的真實性

DNS 安全協議為 IoT 設備提供了其他方法，以在 DNS 解析後檢查從服務接收到證書的真實性。與保護 DNS 消息完整性，這對於避免 IoT 設備與可能影響用戶隱私和安全的惡意服務進行通信非常重要。

其中之一 DNS 命名實體身份驗證 (DNS-based Authentication of Named Entities，DANE)，是 DNSSEC 應用程式，需要 DNSSEC 驗證才能有作用。使 IoT 設備和閘道器能夠驗證其收到的傳輸層安全性 (TLS) 證書，例如當其透過 HTTPS 連接到遠程服務時，如果設備使用 HTTPS 連接到 s1.sp1.example.，則可以在 DNS 中尋找 s1.sp1.example.的證書，並檢查通過 HTTPS 連接收到的證書是否為有效證書，以及綁定到 s1.sp1.example.。

## (三)DNS 與 IoT 面臨的挑戰

DNS 與 IoT 的結合面臨了許多挑戰，而其中幾項與 DNSSEC 相關。

第一個挑戰是開發和維護一個開源 DNS 安全庫，使 DNSSEC 驗證、DANE 和 DoH/DoT 等功能在 IoT 設備上可用。該庫需要包括對常規根 KSK 翻轉的透明支援，例如，自動更改密鑰並通知其中 KSK IoT 設備目前使用的 DNS。主要挑戰為可能無法遠端更新 IoT 設備，且許多 IoT 裝置缺少儲存金鑰所需的儲存體。

另一個挑戰是 IoT 和 DNS 專業人員之間的互動。包含討論 IoT 安全措施 (例如 DNS 安全功能和其他安全協定) 及計算開發和維護相對措施成本。增加對設備和網路安全瞭解，如 DNSSEC 的工作原理。

# 第六節 SIP (Session Initiation Protocol，對話啟動協定)

對話啟動協定 (Session Initiation Protocol, SIP) 為 IETF (Internet Engineering Task Force) 所制定之進行對話管理的應用層通訊協定。SIP 設計目標之一是在 IP 網路上提供類似公用交換電話網 (Public Switched Telephone Network，PSTN) 中訊息處理功能，如撥號、振鈴、回鈴音或者忙線等日常電話操作。SIP 特點如下：

- 簡單且易於擴充：

  SIP 通訊模式與 HTTP 雷同，採用純文字請求 (Request) 與回應 (Response)，SIP 提供數種請求方法 (Method) 及回應狀態代碼 (Status code)，並使用夾帶在標頭的標頭欄位 (Header Fields) 訊息以及通訊內容 (Content)，來完成對話控制。SIP 協定格式以標準字元集編碼的純文字表達，而非二進制封包格式。使得 SIP 封包具有下列優點：

  - 內容為肉眼可辨識之字串，因此容易進行偵錯。
  - 因為增加額外擴充訊息不需要大幅更動原有的解析程式，因此擴充性較佳。

- 良好的移動性支援：

  SIP 制定之初就將移動性支援納入考量，使得 SIP 無論在對話建立階段或是對話進行過程中都可以藉由轉送或是重新邀請 (Re-Invite) 的方式來維持對話暢通。

- 建構於傳輸層之上的協定：

  SIP 位於傳輸層之上的對話層運作，可以根據需求選擇適當的傳輸層協議，例如在封包較容易遺失的網路環境中使用 TCP 作為

傳輸層協議以獲得穩定的連線，而在連線品質較好的環境中可考慮使用 UDP 降低傳輸延遲。

SIP 在應用時通常會搭配 SDP 進行對話描述並且使用 RTP、RTPC 等多媒體傳輸協定在網際網路上進行即時的影像或音訊傳播，即所謂 VoIP 或視訊，且 SIP 並沒有限制僅能維護一對一對話，故多人視訊或語音會議同樣可以利用 SIP 進行對話管理。

# 一.SIP 協定架構

SIP 的基礎架構由 User Agent、Proxy Server、Redirect Server 及 Register Server 組成，其架構如下圖所示。SIP 需要正常運作尚須其他通訊協定協同運作，如 SDP、MSRP、LDAP...等。

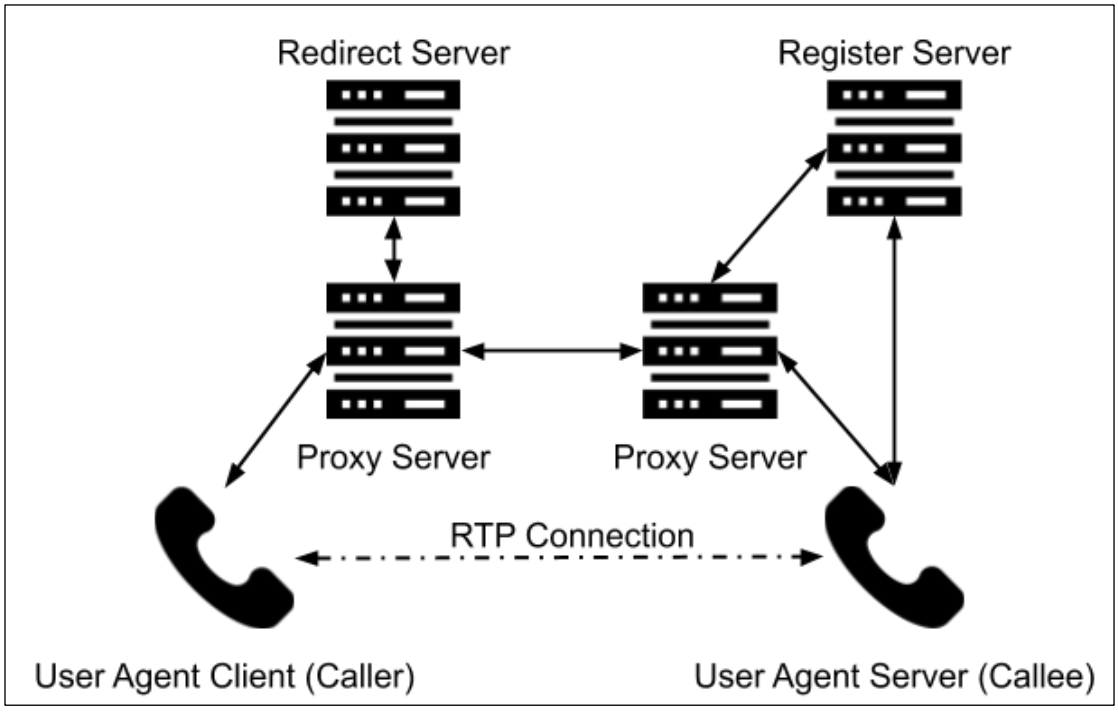



圖 203、SIP 基礎架構

## (一) 基礎元件

### 1. User Agent

User Agent 負責為終端網路語音設備提供 SIP 服務，可細分

為負責提出請求客戶端 User Agent Client (UAC) 和負責進行訊息回覆伺服端 User Agent Server (UAS)。每一個 SIP UA 都可扮演 UAC 或 UAS 但同時只能選擇一個角色，呼叫者 (Caller) 的 UA 扮演 UAC 角色，而被呼叫 (Callee) 的 UA 則扮演 UAS 角色。

**2. Proxy Server**

Proxy Server 是 SIP 運作時的核心，如同網路層的路由器般，Proxy Server 會接受呼叫者的請求並將其轉送到另外一端，因此其同時扮演 UAC 和 UAS 角色。Proxy Server 同時提供一些如身份認證等功能供 UA 使用。

**3. Redirect Server**

為能在固定邏輯位址情況下隨意變更實體位址，SIP 使用 Redirect Server 將邏輯位址和實體位址分離，所謂邏輯地址即為 SIP URI，每個使用者擁有一個固定不變的邏輯位址，而實體位址為 IP 位址等底層通訊協定位址，實體位址可以隨意變動。每當使用者移動時該使用者的 UA 必須負責向 SIP 網路中的其中一個 Redirect Server 註冊，因此其他人可以使用被呼叫者的邏輯位址詢問 Redirect Server 以獲得被呼叫者的實體位址，從而在固定邏輯位址的情況下隨意變更實體位址。Redirect Server 同時可以用來實現如 Call Forward 等功能。然而與 Proxy Server 不同，Redirect Server 不會轉送任何 SIP 訊息。

**4. Register Server**

Register Server 目的為紀錄或更新使用者的邏輯位址及使用者目前狀態。當 User Agent 上線時，會先以 REGISTER 請求方法來更新目前 UA 邏輯位址及狀態紀錄。若有呼叫者對目前 UA

提出對話建立請求時，SIP 網路內相關其他元件就能透過 Register Server 順利找到被呼叫端。UA 註冊時都有一定時效限制，若 UA 沒在相關紀錄過期前重新註冊的話相關對話狀態就無法維護。Register Server 與 Redirect Server 的存在讓 SIP 具有支援移動性的能力。

## (二)相關協定

### 1. Session Description Protocol (SDP)

SDP 為用來描述串流媒體對話初始化參數的通訊協定，被廣泛用於和 RTSP 及 SIP 協同工作，此協定最初為對話發布協定 (Session Announcement Protocol，SAP) 的一個元件。SDP 於西元 1998 年 4 月由 IETF 推出第一版定義於[RFC 2327]文件中，目前最新版本在[RFC 4566]文件中描述，該版本更新 ABNF 語法及整合 IPv6 擴充。

### 2. Message Session Relay Protocol (MSRP)

MSRP 為 SIP 的即時訊息 (Instant Messaging) 協定，可在 SIP 對話中進行一對一或一對多即時通訊、傳送檔案或圖片分享。

### 3. Lightweight Directory Access Protocol (LDAP)

LDAP 為開放且中立的工業標準應用協定，透過 IP 協定提供存取控制和維護分散式資訊的目錄資訊。

目錄服務在開發內部網路和網際網路程式共享用戶、系統、網路、服務和應用過程中占據了重要地位，如目錄服務可能提供組織有序記錄集合，通常有層級結構，如公司電子郵件目錄或包含位址和電話號碼的電話簿。最新 LDAP 由 IETF 的[RFC 4511]文件中定義，使用描述語言 ASN.1 定義。

LDAP 在 SIP 協同運作中的用途主要是用來內部網路註冊階段查詢使用者的密碼或建立對話階段查詢使用者的邏輯位置，可替換技術有 Name/Finger 及 DNS 等。

**4. Resource Reservation Protocol (RSVP)**

RSVP 為通過網路進行資源預留協定，是為實現綜合業務網而設計，其定義於[RFC 2205]文件中。RSVP 要求接收者在連接建立之初進行資源預留。主機或者路由器可以使用 RSVP 滿足不同應用程式資料流所需的不同服務品質 (QoS)。RSVP 定義應用程式如何進行資源預留並在預留資源不用時如何進行預留資源的刪除，同時也會使得路徑上每個節點都進行資源預留。

**5. Real-time Transport Protocol (RTP)**

RTP 為建立在 UDP 協定上的多媒體傳輸協定，最新協定版本定義於[RFC 3550]文件中。RTP 協定詳細說明網際網路上傳遞音訊和視訊標準封包格式。一開始設計為多播協定，但後來被用在許多單播應用中。RTP 也常配合 H.323 或 SIP 用於視訊會議和一鍵通 (Push to Talk) 系統，使其成為 IP 電話產業技術基礎。 RTP 通常和 RTCP 伴隨使用，RTP 負責 Data Plane 而 RTCP 負責 Control Plane。

**6. Real-time Transport Control Protocol (RTCP)**

RTCP 是 RTP 姐妹協議，RTCP 和 RTP 都定義在[RFC 3550]文件。RTCP 為 RTP 媒體串流提供訊息通道外 (out-of-band) 控制。RTCP 本身並不傳輸數據，但和 RTP 一起協作將多媒體數據打包和發送。RTCP 定期在多媒體串流對話參加者之間傳輸控制數據。RTCP 主要功能是為 RTP 所提供服務質量 (Quality of Service) 提供回饋。

RTCP 收集相關媒體連接統計信息，例如：傳輸位元組數、傳輸分組數、丟失分組數、jitter 以及單向和雙向網路延遲等，網路應用程式即可利用 RTCP 統計信息來控制傳輸品質，如網路頻寬高負載時限制訊息流量或改用壓縮比較小的編碼器。另外，RTCP 本身不提供數據加密或身份認證，若有相關需求可以使用 SRTCP 達成。

**7. 協定堆疊**

上述與 SIP 協同運作的通訊協定之間關係如下圖所示。協定主要可以分為 Data Plane 及 Control Plane，Data Plane 主要通訊協定為 RTP 及其控制協定 RTCP，此外為加強安全性亦可以使用上述兩協定安全版本 SRTC 及 SRTCP。Control Plane 則以 SIP 為主要通訊協定，搭配 SDP 及 MSRP 敘述該對話詳細內容，使用 DNS 及 LDAP 查詢實用者的邏輯位置，並搭配 RSVP 進行網路資源保留。此外，Control Plane 安全性主要來自於 IP 層 IPsec 及傳輸層 TLS 安全協定。

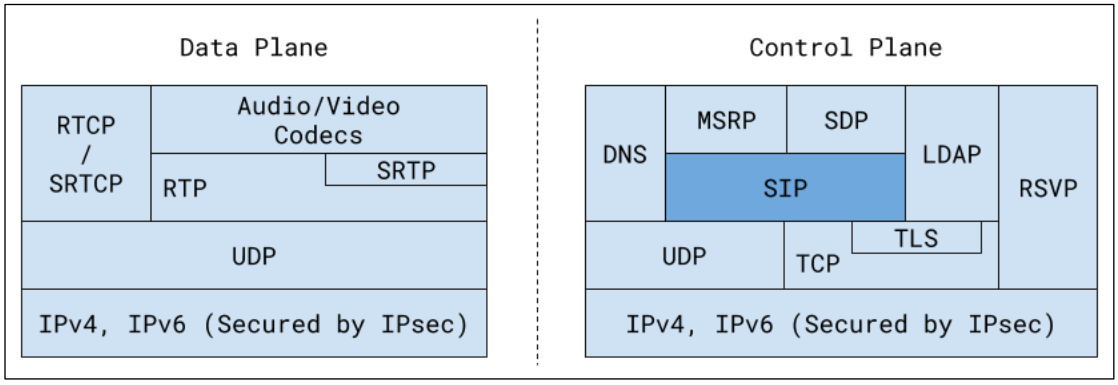



圖 204、IP 相關協定堆疊

## 二.SIP 通訊流程

SIP 的通訊協定內容和 HTTP 很類似，都是以純文字作為協定的內容，且都是一個請求對上一個回覆，由 UAC 發起請求並由 UAS

接受請求並回覆，以下將詳細介紹 SIP 的請求及回覆格式以及基礎的通訊流程。

## (一) 請求格式

SIP 的請求主要有 REGISTER, INVITE, ACK, CANCEL, BYE, OPTION 六種，詳細敘述如下：

- INVITE：邀請 UAS 加入對話。
- ACK：當 UAC 發出 INVITE 請求和 UAS 建立對話且對方回傳最終請求時，UAC 必須利用 ACK 通知對方進行確認。
- BYE：參與對話的雙方其中一方欲結束對話時所發送的請求。
- CANCEL：取消之前所發出的 INVITE 請求。
- REGISTERS：向 Register Server 註冊目前 UA 的相關資訊，以利其他 UA 尋找此 UA。
- OPTIONS：用來詢問伺服器是否支援某些擴充功能。

## (二) 回應格式

SIP 的回覆狀態碼和 HTTP 雷同，都是三個數字位數的狀態碼來表達回覆的各種狀態，詳細敘述如下：

- 1XX—Informational Messages：資訊性消息。
- 2XX—Successful Responses：請求成功。
- 3XX—Redirection Responses：請 UAC 轉發新的連線請求到被 UAS 的其他位址。
- 4XX—Request Failure Responses：請求失敗。
- 5XX—Server Failure Responses：UAS 發生錯誤。
- 6XX—Global Failure Responses：其他錯誤發生。

## (三)標頭欄位

標頭欄位可依照其在 SIP 訊息中的作用分類為要求、回應、僅限要求、僅限回應及訊息主體欄位。SIP 的標頭欄位主要定義在[RFC 3261]文件，其擴充標頭由各相關 RFC 去定義。下表為 SIP 標頭欄位的簡稱：

表 117、SIP 標頭欄位的簡稱

| 原始欄位 | 欄位簡稱 | 原始欄位 | 欄位簡稱 | 原始欄位 | 欄位簡稱 |
|---|---|---|---|---|---|
| Accept-Contact | a | Call-ID | i | Via | v |
| Reject-Contact | j | Refer-To | r | To | t |
| Content-Type | c | Referred-By | b | From | f |
| Content-Encoding | e | Subject | s | Contact | m |
| Content-Length | l | Allow-Event | u | Event | o |

## (四)註冊

SIP 中 User Agent 如何向 Register Server 進行註冊。如下圖所示，在 F1 的請求中 Bob 送出自己的通訊錄給 Register Server，因為需要先使用 HTTP 摘要驗證進行身份確認，因此 Register Server 回覆 401 Unauthorized 並附加挑戰 (challenge) 訊息給 Bob。Bob 收到訊息後再發送一次 REGISTER 請求並附加 HTTP 摘要認證，Register Server 確認 Bob 在其資料庫有資料後便發送 200 OK 回去給 Bob，完成一次註冊流程。此外，為了保障 HTTP 摘要認證的安全，所有通訊都必須在 TLS 上進行以確保訊息不會被劫持甚至是偽造。

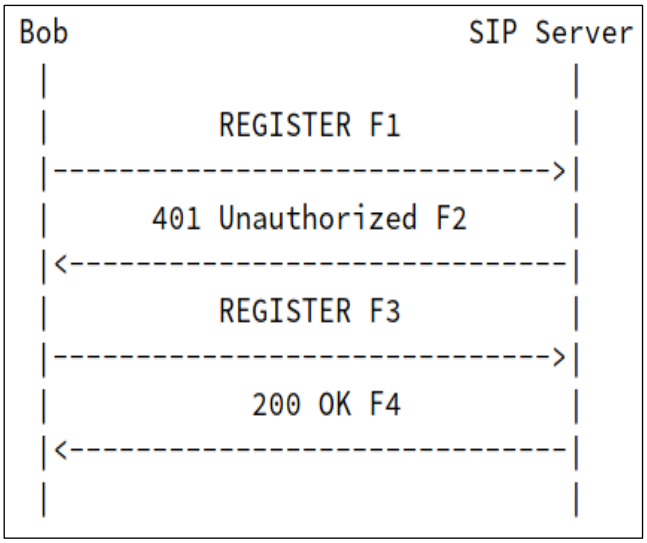



圖 205、SIP 註冊流程

## (五)對話建立/消滅

在下圖中 Alice 透過兩個 Proxy Server 和 Bob 溝通，Proxy 1 被設定為 Alice 的預設 Proxy Server，因此在 F1 的 INVITE 請求的 Route 表頭欄位中含有 Proxy 1 的位址。因為 Alice 還沒有和 Proxy 1 進行身份確認，因此 Proxy 1 駁回 Alice 的請求。Alice 順完成和 Proxy 1 的身份認證後 Proxy 1 便會開始幫 Alice 轉送請求到 Proxy 2，Proxy 2 再幫忙轉送到 Bob，其中兩個 Proxy 都會在轉送的封包表頭的 Record-Route 欄位中加入自身的位址以確保可以沿著原路徑送回去。整個對話的消滅僅須其中一方傳送 BYE 的請求並且對方回傳 200 OK 即可完成。

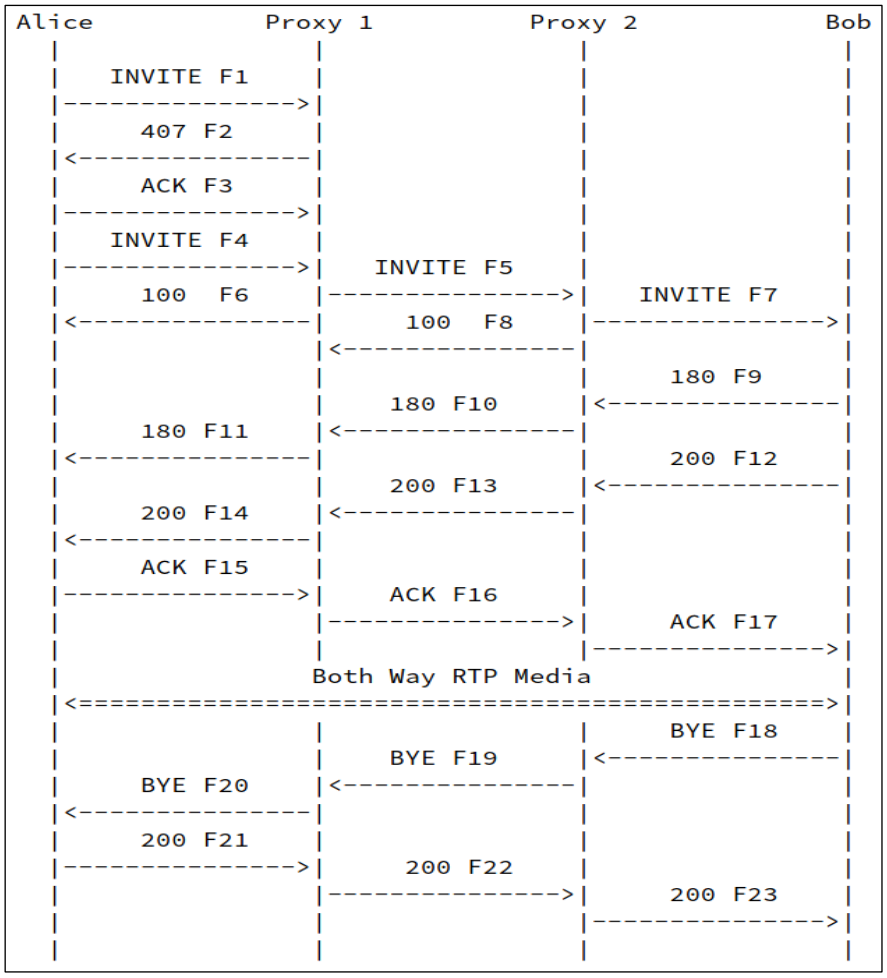



圖 206、SIP 對話建立及消滅流程

# 三.SIP 應用

## (一)SIP for Telephones (SIP-T)

VoIP 網路電話與現有公用交換電話網路 (Public Switched Telephone Network, PSTN) 的互通性為推廣 VoIP 服務時一個重要的議題。作為 VoIP 裡主要訊號通訊協定的 SIP 必須進行相對應的擴充，以整合 SIP 的訊號網路與現有的訊號網路。因 SIP 方便擴展的特性，定義於[RFC 3372]文件的 SIP-T (SIP for Telephone) 便應運而生。SIP-T 為 sipping 小組所制定的通訊協定，該小組和制定 SIP 協定為同一組人。

SIP-T 的主要目的為提供 PSTN 與 IP 網路之間訊號相互轉換與互相運作的一套機制，使得從 PSTN 或是從 IP 網路都能與對方連接或是 PSTN 可以透過 IP 網路互相連接。在 SIP-T 的協定中定義了三種連接的方式，分別為：

- SIP Bridging

  由 PSTN 的使用者發起，透過多媒體網關控制器 (Media Gateway Controller，MGC) 接入以 SIP 做訊息協定的 IP 網路，再透過 MGC 轉到另一個 PSTN 網路接收。

- PSTN origination，IP termination

  由 PSTN 的使用者發起，透過 MGC 轉入 IP 網路後透過 SIP 的 proxy server 轉交 SIP 使用者接收。

- IP origination，PSTN termination

  由 IP 網路的 SIP 使用者發起，並透過連接於 IP 網路的 MGC 轉入 PSTN 網路並由 PSTN 的使用者接收。

## (二)3GPP IMS

傳統行動通訊使用電路交換來進行語音通訊而非 IP 網路封包交換，IP 多媒體子統 (IP Multimedia Subsystem，IMS) 即為 3GPP 所制定以 SIP 為基礎進行訊號與對話管理功能並建構在 IP 網路中的子系統。

IM 的基本架構在 3GPP Relese5 之後已大致確立，相關需求及技術細節可以在[3GPP TS 22.228]文件中找到。IMS 裡定義在 IP 網路裡進行及時語音多媒體傳輸服務會使用到的單元及通訊協定，其中 SIP 被用來執行對話控制和對話管理的即時服務。在 IMS 架構中最重要的單元就是通話狀態控制功能 (Call State Control Function，CSCF)，按照不同任務，CSCF 又可區分為三種：

- 負責處理 SIP 註冊服務通話狀態控制功能 (Serving CSCF，S-CSCF)。
- 作為 SIP proxy server 的代理通話狀態控制功能 (Proxy CSCF，P-CSCF)。
- 負責協助 S-CSCF 進行註冊的詢問通話狀態控制功能 (Interrogating CSCF，I-CSCF)。

下圖為 IMS 架構圖：

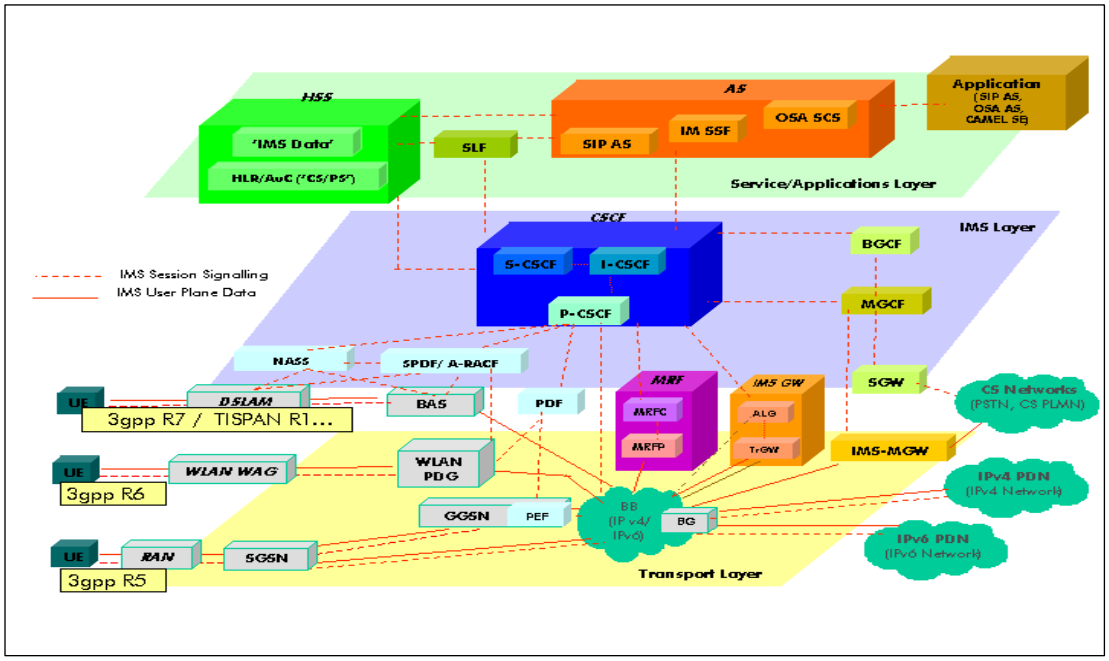



圖 207、IMS 架構圖

## (三) VoLTE/Vo5G

VoLTE (Voice over Long-Term Evolution) 及 Vo5G 是一個手機和資料終端導向的高速無線通訊標準。以 IP 多媒體子系統 (IMS)，在 LTE 上使用為控制層面 (Control plane) 和語音服務的媒體層面 (Media plane) 特定的設定檔。

目的為將語音服務作為資料流並在 LTE 資料承載網路中傳輸，不再需維護和依賴傳統電路交換語音網路。因 VoLTE 封包標頭比未最佳化的 VoIP/LTE 還要小能更有效的利用頻寬，使得 VoLTE 語音和資料容量超過 3G UMTS 三倍以上，超過 2G GSM 六倍以上。下圖為 VoLTE / Vo5G 架構：

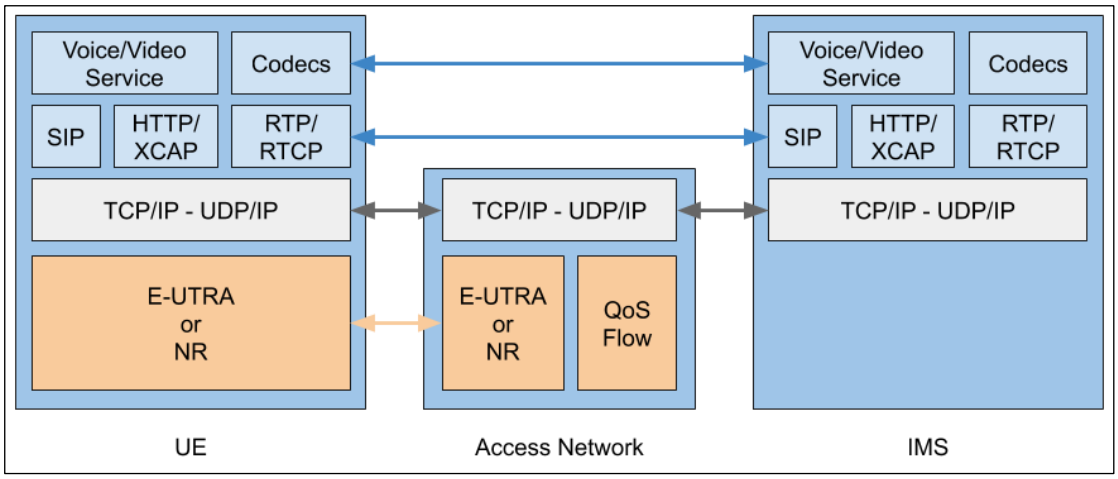



圖 208、VoLTE / Vo5G 架構

## 四.相關議題

### (一)NAT 路由器

SIP 在呼叫過程中需 User Agent Server 確切位址，因此位於 NAT 後方的 User Agent Server 若沒有經過特殊設定將無法接受來自 User Agent Client 的請求，可以靠 SIP 搭配 STUN 來解決此問題。

STUN (Session Traversal Utilities for NAT) 是一種網路協定，該協定定義於[RFC 5389]文件中。STUN 允許位於 NAT (或多重 NAT) 後的客戶端找出自己的公網位址，查出自己位於哪種類型 NAT 之後以及 NAT 為某一個本地連接埠所連結的網際網路端連接埠。這些資訊被用來在兩個同時處於 NAT 路由器之後的主機之間建立 UDP 通訊。

一旦客戶端得知網際網路端 UDP 連接埠，通訊即可開始。如

果 NAT 是完全圓錐型 (Full-cone)，則雙方中任何一方都可以發起通信。如果 NAT 是受限圓錐型 (Restricted cone) 或埠受限圓錐型 (Restricted port)，雙方必須一起開始傳輸。

### (二) 資訊安全

相較於傳統的 Circuit-Switch Based Network，基於 IP 的 SIP 對話資訊容易從軟體方面透過封包捕捉來截取，若對話資訊沒有進行加密，則對話資訊中如電話號碼等敏感資料容易洩漏，因此在[RFC 3329]文件中建議使用 TLS 或是 IPsec 等現存安全機制來保障 SIP 的資料傳輸安全。

原始的SIP沒有進行傳送者身份的認證及資料完整性的確認，導致駭客可以輕易偽造或變更 SIP 訊息，可能會導致假冒身份傳送訊息等問題。因此在[RFC 3329]文件中建議使用 HTTP Digest 進行使用者身份認證及資料完整性確認。不過考量到[RFC 2617]文件中 HTTP Digest 中所規範的 MD5 雜湊函數已經不安全，因此 SIPCORE 工作組於西元 2020 年提出以 SHA-256/512 的[RFC 8760]文件來替代 SIP 中的身份認證及資料完整性確認。

SIP 第三個安全性問題是部份電信營運商的 IMS 沒有檢查傳送者電話號碼是否屬實，造成可以對來源電話號進行偽造，進而形成電話詐騙或偽造公司電話等問題。因此 IETF 的 STIR 工作組於西元 2018 年在[RFC 8225]文件中提出以密碼學且可以驗證 SIP 來源身份的 Token — PASSporT。

## 五.IETF 活躍中的 Working Groups

### (一) Session Initiation Protocol Core (SIPCORE)

SIPCore 工作組的目的是維護和持續 SIP 協定開發，目前已為 SIP 協定標準包含 RFC 3261、RFC 3262、RFC 3263、RFC 3264 和

RFC 6665 文件規範。目標為努力維護 SIP 定義的基本模型和體系結構。特別是：

- 盡可能以端到端的方式提供服務和功能。
- 重用 Internet 協議和體系結構及與其他 Internet 應用整合。
- Standards-track 擴展和新功能必須通用，而不是僅適用於特定的對話類型。
- 使用簡單的解決方案。

## (二) Secure Telephone Identity Revisited (STIR)

STIR 工作組將針對允許驗證呼叫機構使用特定電話號碼進行傳入呼叫授權提出規範。與電子郵件一樣，未經身份驗證的 SIP 請求的來源身份不會得到驗證，使得未經授權使用該來源身份成為欺騙性和強制性活動。

由於提供不正確的來源電話號碼變得相當容易，過去出現越來越多的問題，例如自動呼叫 (大量未經請求的商業通信)，誘捕 (語音郵件駭客和冒充銀行)等。

STIR 工作組主要在開發電話號碼解決方案。此小組於[RFC 8225]文件中提出一種用於個人身份驗證的密碼學 Token，名為 PASSporT。

## (三) Automatic SIP trunking And Peering (ASAP)

ASAP 工作組將定義一個描述性功能集，該功能集由 SIP 服務提供商提供，並在與企業網路通信時封裝對應訊息，以與服務提供商網路建立 SIP 中繼。 除了定義描述性功能集之外，ASAP 工作組還將定義功能集的數據模型，服務發現機制和功能集的傳輸機制。ASAP 工作組的上述交付成果統稱為〝SIP Auto Peer〞。

關於 IP (Internet Protocol，網際網路協定)、DN (Domain Name，網域名稱)、BGP (Border Gateway Protocol，邊界閘道器協定)、RPKI (Resource Public Key Infrastructure，網際網路號碼資源公鑰基礎設施)、DNSSEC (Domain Name System Security Extensions，域名系統安全擴充)、SIP (Session Initiation Protocol，對話啟動協定) 技術內容，相關內容詳細資訊請參閱附錄九。。

# 第十二章 會議及報告

## 第一節 每月月報

每月工作進度報告，於每月底完成彙總報告內容，並於隔月月初召開工作進度報告會議，向委託機關國家通訊傳播委員會本計畫承辦單位進行報告，內容包含目前工作進度、已完成項目、及完成項目所得結果等。

詳細的月報報告內容，請參考附錄三；已完成工作項目，如下表所示：

表 118、已完成工作項目列表

| 序號 | 工作項目 | 完成日期 |
|---|---|---|
| 1 | 「前瞻及完整之 IPv6 生態系推動方案」開標，確認 TWNIC 投標文件符合資格。 | 109/2/21 |
| 2 | 完成評審會議。 | 109/2/27 |
| 3 | 確認 TWNIC 為第 1 優勝廠商。 | 109/3/9 |
| 4 | 完成議價，合約生效。 | 109/3/24 |
| 5 | 完成 GRB 登錄。 | 109/3/25 |
| 6 | 完成 4 件委託執行案需求規格書，並進行公告。<br>1. 「IPv6 動態 DNS 服務軟體開發」。<br>2. 「Native IPv6 連網環境建置及 IPv6 用戶安全防護研析」。<br>3. 「市售產品支援 IPv6 調查」。<br>4. 「物聯網服務與應用研析及網際網路技術標準研析」。 | 109/3/26 |
| 7 | 完成第 1 場「ICP IPv4/IPv6 雙協定網路安全技術防護人才培育教育訓練」規劃及開始招生。 | 109/3/30 |
| 8 | 簽訂並繳交「履約人員約定同意書」。 | 109/4/8 |
| 9 | 完成合約用印。 | 109/4/21 |
| 10 | 完成 4 件委託執行案評審會議及議價程序。 | 109/4/24 |
| 11 | 完成第 1 場「ICP IPv4/IPv6 雙協定網路安全技術 | 109/4/29 |

| 序號 | 工作項目 | 完成日期 |
|---|---|---|
| | 防護人才培育教育訓練」。 | |
| **12** | 完成 4 月份月報會議。 | 109/5/7 |
| **13** | 完成第 2 場「ICP IPv4/IPv6 雙協定網路安全技術防護人才培育教育訓練」。 | 109/5/15 |
| **14** | 完成 IASP 支援 IPv6 問卷調查內容。 | 109/5/19 |
| **15** | 以下 4 件委託執行案繳交 5 月份進度報告：<br>●「市售產品支援 IPv6 調查」。<br>●「物聯網服務與應用研析及網際網路技術標準研析」。<br>●「IPv6 動態 DNS 服務軟體開發」。<br>●「Native IPv6 連網環境建置及 IPv6 用戶安全防護研析」。 | 109/5/25 |
| **16** | 完成「市售產品支援 IPv6 調查」委託執行案 5 月份月報會議。 | 109/5/26 |
| **17** | 完成「物聯網服務與應用研析及網際網路技術標準研析」委託執行案 5 月份月報會議。 | 109/5/27 |
| **18** | 完成「IPv6 動態 DNS 服務軟體開發」委託執行案 5 月份月報會議。 | 109/5/28 |
| **19** | 完成「Native IPv6 連網環境建置及 IPv6 用戶安全防護研析」委託執行案 5 月份月報會議。 | 109/5/29 |
| **20** | 完成 5 月份月報會議。 | 109/6/4 |
| **21** | 完成第 3 場「ICP IPv4/IPv6 雙協定網路安全技術防護人才培育教育訓練」。 | 109/6/23 |
| **22** | 以下 4 件委託執行案繳交 6 月份進度報告：<br>●「市售產品支援 IPv6 調查」。<br>●「物聯網服務與應用研析及網際網路技術標準研析」。<br>●「IPv6 動態 DNS 服務軟體開發」。<br>「Native IPv6 連網環境建置及 IPv6 用戶安全防護研析」。 | 109/6/25 |
| **23** | 完成「IPv6 動態 DNS 服務軟體開發」委託執行案 6 月份月報會議。 | 109/6/30 |
| **24** | 完成「市售產品支援 IPv6 調查」委託執行案 6 月份月報會議。 | 109/7/2 |
| **25** | 完成「Native IPv6 連網環境建置及 IPv6 用戶安全防護研析」委託執行案 6 月份月報會議。 | 109/7/2 |

| 序號 | 工作項目 | 完成日期 |
|---|---|---|
| **26** | 完成「物聯網服務與應用研析及網際網路技術標準研析」委託執行案 6 月份月報會議。 | 109/7/2 |
| **27** | 完成 6 月份月報會議。 | 109/7/7 |
| **28** | 完成第 4 場「ICP IPv4/IPv6 雙協定網路安全技術防護人才培育教育訓練」課程。 | 109/7/17 |
| **29** | 完成並繳交期中報告 | 109/7/22 |
| **30** | 以下 4 件委託執行案繳交期中報告及 7 月份進度報告：<br>● 「IPv6 動態 DNS 服務軟體開發」。<br>● 「Native IPv6 連網環境建置及 IPv6 用戶安全防護研析」。<br>● 「市售產品支援 IPv6 調查」。<br>● 「物聯網服務與應用研析及網際網路技術標準研析」。 | 109/7/24 |
| **31** | 完成 7 月份月報會議。 | 109/7/28 |
| **32** | 和公協會共同合作舉辦【2020 網路共贏時代】專家座談會 | 109/7/29 |
| **33** | 完成第 5 場「ICP IPv4/IPv6 雙協定網路安全技術防護人才培育教育訓練」課程。 | 109/7/31 |
| **34** | 完成期中審查會議。 | 109/8/4 |
| **35** | 回覆期中審查委員意見。 | 109/8/7 |
| **36** | 於 GRB 系統完成期中成果繳交 | 109/8/11 |
| **37** | 確認通過期中報告內容審查，已達成第一期履約事項 | 109/8/17 |
| **38** | 完成以下委託執行案期中報告審查：<br>「物聯網服務與應用研析及網際網路技術標準研析」。 | 109/8/19 |
| **39** | 完成以下 2 件委託執行案期中報告審查：<br>● 「IPv6 動態 DNS 服務軟體開發」。<br>● 「Native IPv6 連網環境建置及 IPv6 用戶安全防護研析」。 | 109/8/20 |
| **40** | 完成第 6 場「ICP IPv4/IPv6 雙協定網路安全技術防護人才培育教育訓練」課程。 | 109/8/28 |
| **41** | 完成 8 月份月報會議。 | 109/9/4 |
| **42** | 拜訪 D-Link 訪談寬頻分享器產品支援 IPv6 規劃 | 109/9/8 |
| **43** | 拜訪 ASUS 訪談寬頻分享器產品支援 IPv6 規劃 | 109/9/8 |

| 序號 | 工作項目 | 完成日期 |
|---|---|---|
| **44** | 於【HITCON 2020 駭客年會】進行〝國際及台灣 IPv6 發展介紹〞 | 109/9/12 |
| **45** | 完成第 7 場「ICP IPv4/IPv6 雙協定網路安全技術防護人才培育教育訓練」課程。 | 109/9/18 |
| **46** | 和高雄市電腦商業同業公會合作舉辦 1 場 IPv6 推廣講座活動 | 109/9/25 |
| **47** | 完成第 8 場「ICP IPv4/IPv6 雙協定網路安全技術防護人才培育教育訓練」課程。 | 109/9/30 |
| **48** | 完成 9 月份月報會議。 | 109/10/6 |
| **49** | 「IPv6 動態 DNS 服務軟體開發」<br>完成軟體使用教育訓練課程 | 109/10/13 |
| **50** | 以下 4 件委託執行案繳交期末報告：<br>● 「IPv6 動態 DNS 服務軟體開發」。<br>● 「Native IPv6 連網環境建置及 IPv6 用戶安全防護研析」。<br>● 「市售產品支援 IPv6 調查」。<br>「物聯網服務與應用研析及網際網路技術標準研析」。 | 109/10/20 |

# 第十三章結論與建議

## 第一節 結論說明

### 一、全球網路加速向 IPv6 遷移

全球 IPv6 的使用率不斷攀升，根據 APNIC 統計，依個別國家來看，今 (109) 年就有超過 25 個國家 IPv6 連網比例超過 30%。全球總體 IPv6 連網比例也呈現穩定的成長，由此觀察可得知 IPv6 部署建置已經獲得多數國家支持，網路向 IPv6 遷移已經是相當明確趨勢。

另外全球流量排行前一萬大網站，支援 IPv6 比例已經超過 31%，逐年呈現穩定成長，由以上觀察發現不論是網路連線服務或網站應用服務，支援 IPv6 已經成為共識。

再加上去 (108) 年 11 月歐洲區網路協調中心 RIPE，正式發布 IPv4 位址已經發罄，業者若有 IPv4 需求只能等待小量回收再分配或是透過市場交易取得，在 IPv4 位址成為稀有且缺乏資源之後，業者要取得足夠新配發 IPv4 位址變得相對不易，且成本提高，因此轉向 IPv6 將是不得不採取的未來趨勢。

### 二、國內市售寬頻分享器支援 IPv6 比例提升，預設開啟支援 IPv6 比例下降

調查發現去 (108) 年全年度市售寬頻分享器銷售前 20 名商品中有標示支援 IPv6 比例為 75%，和 106 年全年度市售寬頻分享器銷售前 20 名商品中標示支援 IPv6 比率 55%比較，顯示國內寬頻分享器品牌業者，對 IPv6 支援有逐步重視，對國內推動 IPv6 網路升級具有重大象徵性意義。

但經過實際測試比較發現，因為品牌銷售消長因素影響，108 年度市售寬頻分享器銷售前 20 名商品中能預設開啟支援 IPv6 比例較 106 年低，4 大品牌商對商品預設支援 IPv6 狀況並未改善。

## 三、電信業者對 IP 需求持續增加

去 (108) 年針對 IASP 調查結果來看，5 家行動電信業者都採用 CGNAT 核發 Private/Shared Address Space IPv4 位址給用戶，以因應 IPv4 不足問題，其中台灣大哥大 (部分)、亞太電信及台灣之星 3 家業者所採用的 IP 位址共用比例達到 1 : 64，增加網路犯罪偵查複雜度。今 (109) 年國內電信業者的大事就是 5G 正式發照，國內電信三雄中華電信、遠傳電信及台灣大哥大，都已經正式取得 5G 執照，進入 5G 時代行動電信業者對 IP 需求將再擴張，因應業務成長 IPv4 不足問題將加劇，業者轉進 IPv6 才能解決及滿足消費端的需求，為新業務提供發展的空間。

## 四、5G 時代將加速物聯網發展

物聯網在雲端、AI、邊緣計算等技術發展下，再加上 5G 超高速、低延時特性推波助瀾，物聯網將正式進入蓬勃發展階段，從高畫質影音傳輸、智慧生活領域、AR/VR 軟硬技術娛樂應用、智慧交通及遠端醫療等各個應用面加速發展。未來除家用電腦、電視、行動電話及平板電腦需連結網路外，將會有更多設備有連結網際網路的需求，IP 資源需求將更為殷切，IPv4 已經不足以應對未來網路世界發展，全球對 IPv6 需求將更為明顯。

## 五、 固網 IPv6 連網比例仍待提升

觀察國內固網 IASP 支援 IPv6 使用率發現，一般家庭用戶固接網路服務供應商以中華電信為主，中華電信固網 IPv6 使用率，目前已成長到約 33%，但國內 Cable 業者在 IPv6 推動上仍然相當緩慢；而國內企業用戶 IPv6 使用比例仍然很低，要讓國內 IPv6 達到普及化，除推動 IASP 逐步增加各項網路服務支援 IPv6 外，持續推廣 ICP 業者及企業網路支援 IPv6 仍有相當長的歷程要走。

## 六、 IASP 對 IPv6 支援狀況對 ICP 支援 IPv6 推動至為關鍵

推動 ICP 業者及企業網路支援升級 IPv6 的基本要素，需要 IASP 所提供的各項網路服務能夠充分支援，否則 ICP 業者或企業網路因網路供應者無法支援 IPv6 即阻斷升級的可能性。持續推動國內 IASP 各項網路服務支援 IPv6，是提升 ICP 升級支援 IPv6 的基本要件之一。

## 七、 持續推動企業升級支援 IPv6 才能達到國內 IPv6 網路普及化

國內 IPv6 的使用率主要由行動用戶及家庭用戶所支撐，企業網站及內部網路目前支援 IPv6 的比例依然不高，許多 ICP 業者或企業尚未關注到國內網路環境，已經逐步向 IPv6 遷移，而網站或企業內部網路升級支援 IPv6 需要投入相對人力及物力，且要有足夠的時間進行規劃及執行，而非一蹴可幾。目前國內雖然 IPv6 的使用比例已經超過 50%，未來要持續推升國內 IPv6 使用率，讓國內網路環境逐

步向下一代網路遷移，網站或企業內部網路升級將是不可或缺的一環。

## 八、 國內行動電信業者全面升級支援 IPv6

今 (109) 年 8 月台灣之星陸續開通支援 IPv6 網路服務，目前雖然使用率仍低，但在業者陸續更新設備逐步進行情況下，隨著時間遞移一定能逐步提升整體 IPv6 使用比例。而台灣之星開始支援 IPv6 也象徵國內行動 IASP 已經全面進入 IPv4/IPv6 雙軌並行時代。

# 第二節 建議事項

觀察國際 IPv6 發展趨勢，除歐美各國相當積極外，近年亞洲區國家，包含台灣、日本、越南、馬來西亞及泰國等國家在 IPv6 連網比例也大幅成長，可見支援 IPv6 已經是國際共識，國內行動電信業者已經全面預設開啟支援 IPv6 網路服務，中華電信 Hinet 之 IPv6 使用率也已經超過 33%，整體 IPv6 使用率超過 50%，國內在行動及固接網路都有良好支援 IPv4/IPv6 雙軌服務根基，以此基礎持續推動 IPv6 普及化，以提供新一代網路標準完善支援，根據計畫執行狀況所提建議如下所述：

## 一. 推動 IASP 各項服務支援 IPv6

根據 IASP 普查結果得知，IASP 除行動網路及固接網路連線外，業者還經營其他各項服務如 PWLAN、IDC/Co-Location、雲端服務等，網路連線服務供應業者所提供服務是否支援 IPv6，和 IPv6 是否能普及息息相關，持續積極推動業者各項服務支援 IPv6，對提升國內 IPv6 使用率有相當助益。

IASP 業者大多希望透過政府單位提供獎勵補助措施，例如 IPv6 設備採購稅金減免、補助固網寬頻升級 IPv6 實施計畫、降低營所稅稅率、鼓勵服務創新獎勵補助措施等，利用實質補貼計畫提升業者進行 IPv6 升級意願。尤其國內 Cable 業者在寬頻網路服務上，僅有一家業者可提供 IPv6 申請試用，在初期發展階段若政府能提供獎勵或補助業者為家用戶更換新一代連線數據機、提供獎勵金鼓勵 Cable 業者設立小型 IPv6 實驗環境等方式，減少業者所需負擔成本，進而推動業者進行升級 IPv6 網路的步調。

## 二. 手機預設開啟支援 IPv6

在國內行動網路服務業者完成全面預設開啟支援 IPv6 網路服務後，即能在此基礎上推動手機業者新產品上市能預設開啟支援 IPv6，可以透過訪談手機品牌業者方式讓業者了解國內網路環境已經到位，設備預設支援就能讓終端用戶無感升級使用 IPv6 網路連結。讓使用者不論是經由向電信業者購買綁約手機，或是透過零售市場購入，新手機都能預設支援 IPv6，以持續提升國內 IPv6 網路連線使用率。終端設備支援 IPv6 越普及，同時也能增加網站及企業內部網路加速支援 IPv6 的誘因。

## 三. 推動寬頻分享器預設開啟支援 IPv6

影響家用戶網路IPv6使用率，除固網業者是否預設開啟支援IPv6外，消費者所採購的網通商品是否預設支援 IPv6 也至關重要，持續向國內網通商品製造業者宣導國內IPv6網路環境的狀況及高使用率，可加強業者支援 IPv6 的意願。

或可以參考如馬來西亞、中國等做法，要求直接連接到電信網路之終端設備產品包含寬頻分享器、手機等提供 IPv6 測試報告，並給予批准證書，設備上市前須取得相關批准證書始可在市場上銷售，以加快業者新產品設計符合預設支援 IPv6 規範。[41~42]

## 四. 持續推動 ICP 網站及企業網路升級支援 IPv6

國內經濟主要依靠為數可觀中、小企業撐起一片天，近來各項產業進行數位轉型趨勢越加明顯，國內各大公協會為企業提供技術交流

平台，因此也成為推廣 IPv6 極佳場域。今 (109) 年推動 ICP 網站升級支援 IPv6 工作，除持續進行教育訓練推廣外，並透過和公協會合作進行網站升級推廣計畫，可以擴大接觸到更多有架設對外網站業者，相對提升成功機會。並針對新創公司加強 IPv6 推廣，讓新進入市場業者，在一開始就選擇新技術避免日後升級需付出更多人力及物力投資成本。持續和公協會合作進行推廣 IPv6，有助於國內企業在數位網路科技選擇技術能走在對的方向上。

企業網路和 ICP 網站升級支援 IPv6，需要長時間布局，加強對 ICP 宣導，除持續和公協會合作外，亦可透過主管機關經濟部、IASP 等共同合作推廣，希冀透過舉辦座談或教育訓練課程等活動，以接觸更多國內企業，讓業者能了解國內 IPv4/IPv6 雙軌環境現況，促進企業用戶及內容業者提早因應，才能讓國內網路環境遷移到 IPv6 過程更為順暢。

## 五. 提早因應為未來 Native IPv6 網路環境鋪路

全球 IPv6 使用率逐步推升，加上 IPv4 短缺情況日益嚴重，5G 開通及物聯網應用加入網路世界，讓 IPv6 網路愈形重要，目前國內以支援 IPv4/IPv6 雙軌服務為主，當 IPv6 使用率持續推升，加上支援雙軌服務增加 IASP 營運複雜及增加人力成本，未來轉向 Native IPv6 網路環境可能性會逐步提升。而系統轉換需要相當人力、物力及時間成本，透過早期投入小型試驗，對未來建置有相當大助益。

Native IPv6 網路環境牽涉到如何支援使用者以 IPv4 設備連結網路，及如何連結僅支援 IPv4 網站內容，其中牽涉到複雜 IPv4/IPv6 轉換機制，及網路組態設定等，需要更完整網路試驗及應用測試，持續

進行相關研究及試驗，能為未來網路環境轉換累積足夠經驗和技術能量。[54]

## 六. 加強 ICP 網站及企業網路升級 IPv6 對安全之重視

IPv6 和 IPv4 除位址長度擴充外，也因應近年資訊安全等議題需求，對網路協議進行強化，除推動 ICP 網站及企業網路升級支援 IPv6 外，同時也需要加強業者對 IPv6 網路系統資訊安全觀念更為重視，才能讓國內網路除了可以逐步遷移到新一代 IPv6 網路環境外，同時能建立起更為順暢且安全的下一代網路世界。

可以在 ICP 網站升級支援 IPv6 之教育訓練課程，持續強化及精進 IPv6 網路環境資訊安全相關議題探討：亦可透過電子報或部落格技術文件分享，持續提高企業對網路安全關注及重視。

## 七. 建議將 ISP 之 IPv6 網路安全項目納入電信事業資通安全規範

全球網際網路不斷快速擴張，維護網路資訊安全成為維運重要課題。計畫報告針對 ISP 網際網路存取服務之固接網路、行動網路與公眾無線網路連線服務安全防護提供建議。網際網路服務提供者 (ISP，Internet Service Provider) 為關鍵基礎設施提供者，根據「資通安全管理法」，關鍵基礎設施提供者應符合其所屬資通安全責任等級之要求；且根據電信管理法第 15 條第 2 項第 5 款其他主管機關指定有助於資通安全之管理措施，以及第 38 條第 3 項第 8 款之經主管機關指定與網路設置相關項目，建議 ISP 網際網路存取服務與 ISP IPv6 網路連

線服務安全防護建議可納入資通安全之特定非公務機關應辦事項，以強化資通安全防護。

## 八. 持續關注 IPv6 網路安全議題

網際網路不斷擴張，因此網路技術及標準發展也將與時俱進，利用數位科技發展國家實力是全球多數國家共同目標，在資訊安全即國家安全前提下，面對網路不斷向 IPv6 遷移，勢必吸引駭客攻擊機率，為建設更安全網路環境，應持續關注 IPv6 網路安全技術標準，收集分析各種網路攻擊案例資訊及相關應對措施，才能確保網路環境安全及可用性。

## 九. 持續關注 IPv6 網路創新技術

在 5G 和雲端時代，連接到網路的設備數量將超過 1,000 億。IPv6 從根本上解決了 IP 地址不足的問題。此外，未來應用如自動駕駛、工業自動化、VR (Virtual Reality )、智慧醫療和物聯網等，需要大量網路連接服務。這些應用對網路自動化，智慧化和連線品質保證要求更高。為了滿足要求，IPv6 需要與創新技術相結合，以產生具有突破性的〝IPv6 +〞網路。

IPv6 +是因應 5G 和雲端時代的 IPv6 加強創新，以 SRv6、BIER6 等新協議為代表，並結合 AI 進行網路分析，智慧調整等，以滿足路徑規劃，快速服務調配的要求。以達成 SLA 保證，自動維運，品質可視化等。而 IETF 也針對未來技術需求持續進行相關標準制定，例如今 (109) 年 3 月正式發布了 SRv6 標準文件 [RFC8754] ( IPv6 Segment Routing Header )。[58]

持續關注 IPv6 網路產業技術標準，作為制定產業政策參考依據，

才能讓國內網路環境與時俱進，符合未來應用發展需求，以維護國內網路產業鏈的蓬勃發展。

## 十. 參考國際推動 IPv6 普行方案持續推動國內 IPv6 網路普行

美國《總統行政辦公室》《行政管理和預算局》 於今 (西元 2020) 年 11 月 19 日發布給行政部門和機構負責人《完成向 IPv6 過渡》備忘錄，內容更新了有關聯邦政府營運部署和使用 IPv6 指南。

備忘錄提及隨著連接到網際網路的用戶、設備和虛擬實體數量不斷增長，全球對 IP 位址需求也隨之呈指數增長，導致世界各地區現有的 IPv4 位址即將用盡。向 IPv6 全面過渡是確保網路技術和服務未來增長和創新的唯一可行選擇。聯邦政府必須擴大和增強其向 IPv6 過渡的戰略承諾。

從西元 2005 年開始，聯邦政府 IPv6 計劃，成功促進 IPv6 技術商業開發和採用，因大規模 IPv6 商業部署讓成本降低，複雜性降低，安全性也相對提高。但當前網路系統同時支援 IPv4/IPv6 雙協定，增加維運複雜性、建置成本和安全威脅，因此希望各機關加速遷移到 IPv6-only 網路環境，以減少維護兩個不同網路體系營運問題。

以下為本備忘錄預定執行時程：

- 備忘錄發布 45 天內機構需成立專業負責小組進行改造計畫。
- 西元 2023 年末完成所有聯邦網路資訊系統支援 IPv6，逐步取消支援 IPv4。
- 西元 2021 年末至少完成一個 IPv6-only 試點上線。

- 西元 2023 年末至少需有 20% 聯邦網路資訊系統支援 IPv6-only 環境。
- 西元 2024 年末至少 50% 聯邦網路資訊系統支援 IPv6-only 環境。
- 西元 2025 年末至少 80% 聯邦網路資訊系統支援 IPv6-only 環境。

同時此備忘錄要求行政部門和機構的外部合作夥伴及與聯邦網路系統介接連結，需制定計畫將所有網路介接移轉支援 IPv6。公用/外部服務（例如，Web，電子郵件，DNS 和 ISP 服務）和內部用戶端應用服務升級支援 IPv6-only。[59]

IPv6 推動較難具備外顯的商業利益，因此多有政府或學術機構起帶頭作用，美國聯邦政府透過行政命令訂定機構內網路基礎到服務的全面性改造，以此帶動設備及服務業者支援以達技術成熟，更有利於推動到一般企業採用，加速網路向 IPv6-only 發展。國內相關機構可參考此作法，以政府示範帶動企業跟進，加速國內整體網路服務向 IPv6 遷移。

# 參考資料


[1] 中華電信 IPv6 服務發展與應用趨勢
https://map.twnic.net.tw/28th/pdf/2-3.pdf

[2] W3Techs Usage statistics of IPv6 for websites
https://w3techs.com/technologies/details/ce-ipv6

[3] W3Techs Usage of IPv6 broken down by ranking
https://w3techs.com/technologies/breakdown/ce-ipv6/ranking

[4] 歐洲的 IPv4 位址正式用罄
https://www.ithome.com.tw/news/134437

[5] TBC IPv6 服務申請單
https://www.tbc.net.tw/Upload/Download/39bd18e1-25e8-482a-a59e-a908d2127026.pdf

[6] 資訊與科技教育司網際網路 (Internet) 簡介
https://depart.moe.edu.tw/ED2700/News_Content.aspx?n=697CD84F427DE922&sms=954B3E2521E9F948&s=33FDC49817347991

[7] 網際網路服務介紹
http://bit.kuas.edu.tw/~csshieh/teach/ia/service.html

[8] 定義、概念到應用，一文了解物聯網
https://kknews.cc/zh-tw/tech/nmr6njg.html

[9] APNIC 40 ~ 464XLAT Tutorial~
https://www.slideshare.net/apnic/464xlat-tutorial

[10]IPv6 translation mechanism
https://en.wikipedia.org/wiki/IPv6_transition_mechanism

[11]IPv6 https://zh.wikipedia.org/wiki/IPv6

[12]台網中心民國 109 年 4 月份電子報封面故事「手機啟動 IPv4/IPv6 網路設定 APP 」https://blog.twnic.net.tw/2020/03/31/6721/

[13]2020 TWNIC IPv6 網安技術人才培訓教育訓練開課預告

https://blog.twnic.net.tw/2020/03/31/6764/

[14]關於台灣網路暨電子商務產業發展協會 (TiEA ) https://tieataiwan.org/about-tiea/

[15]關於數位經濟暨產業發展協會 https://www.dtataiwan.org/

[16]關於台北市電腦商業同業公會 https://www.tca.org.tw/

[17]台北市電腦商業同業公會 WiKi https://zh.wikipedia.org/wiki/台北市電腦商業同業公會

[18]IPv4-IPv6 雙協定網路安全防護技術讓你一次搞定 https://itmonth.blog/2020/04/28/twnic-超前部署-ipv4-ipv6 雙協定

[19]迎接 5G 新世代-IPv6 也將全面部署 https://itmonth.blog/2020/04/30/迎接 5g 新世代-ipv6 也將全面部署

[20]IPv6 RFCs and Standards Working Groups http://ipv6now.com.au/RFC.php

[21]IPv4 to IPv6 Translation https://hsc.com/DesktopModules/DigArticle/Print.aspx?PortalId=0&ModuleId=1215&Article=180

[22]IPv6 Essentials https://books.google.com.tw/books

[23]State of IPv6 Deployment 2018 https://www.internetsociety.org/resources/2018/state-of-ipv6-deployment-2018/

[24]Six Years After: State of IPv6 Deployment 2018 https://www.internetsociety.org/blog/2018/06/six-years-after-state-of-ipv6-deployment-2018/

[25]DTAG Deutsche Telekom AG enables IPv6 on their proxy servers https://myserverblog.wordpress.com/2013/06/24/dtag-deutsche-telekom-ag-enables-ipv6-on-their/

[26]APNIC Use of IPv6 for Germany (DE)

https://stats.labs.apnic.net/ipv6/DE

[27]IPv6 deployment https://en.wikipedia.org/wiki/IPv6_deployment

[28]Tele Columbus 採用鎵寶科技 Gateway 產品

https://www.digitimes.com.tw/iot/article.asp?cat=130&cat1=45&cat2=20&id=0000388812_9di72aul2g8rsb1pnltj9

[29]IPv6 and the future at O2

https://hilfe.o2online.de/router-software-internet-telefonie-34/ipv6-und-die-zukunft-bei-o2-41130/index5.html

[30]Telefonica O2 mobile IPv6

https://twitter.com/o2de/status/1141362166773276672

[31]O2 Community Unlock IPv6

https://hilfe.o2online.de/router-software-internet-telefonie-34/ipv6-freischalten-498748/index2.html

[32]APN settings for IPv6 on the smartphone

https://www.thomas--schaefer.de/apn-ipv4-ipv6.html

[33]德國電信在 RIPE 67 介紹 TeraStream

https://ripe67.ripe.net/presentations/131-ripe2-2.pdf

[34]IPv6 通訊協定 IPv6 簡介

http://hanteye01.blog.fc2.com/blog-entry-1.html

[35]IPv6 通訊協定 ND 簡介

http://hanteye01.blog.fc2.com/blog-entry-4.html

[36]CentOS https://zh.wikipedia.org/wiki/CentOS

[37]BIND 9 https://zh.wikipedia.org/wiki/BIND

[38]MySQL https://zh.wikipedia.org/wiki/MySQL

[39]PHP https://zh.wikipedia.org/wiki/PHP

[40]Electron https://zh.wikipedia.org/wiki/Electron

[41]馬來西亞電信網路產品 IPv6 測試報告規範

https://taiwan.ul.com/gma/202007-malaysia-sirim/

[42] 中國 MIIT 要求網路產品需支援 IPv6
https://taiwan.ul.com/gma/201812_2/
[43] 台灣 IPv6 使用率 https://ipv6now.twnic.net.tw/ipv6/index.html
[44] 全球 IPv6 使用率排名前 30 名國家
https://ipv6now.twnic.net.tw/ipv6/apnic_lab_7day_top.html
[45] APNIC 關於法國 IPv6 使用率統計資料
https://stats.labs.apnic.net/ipv6/FR?c=FR&x=1&v=1&p=1&r=1&w=30&p=0
[46] ARCEP 於西元 2019 年 11 月發布關於法國 IPv6 發展狀況
https://www.arcep.fr/actualites/les-communiques-de-presse/detail/n/transition-vers-ipv6-1.html
[47] ARCEP 於西元 2019 年 11 月發布關於法國 IPv6 發展年度報告
https://www.arcep.fr/cartes-et-donnees/nos-publications-chiffrees/transition-ipv6/barometre-annuel-de-la-transition-vers-ipv6-en-france.html
[48] An Introduction to Orange IPv6 Strategy
https://colloque-ipv6.greyc.fr/Slides/J2-01.pdf
[49] 〝World IPv6 Day〞：Orange plans ahead and prepares for the new internet protocol
https://www.orange-business.com/en/press/world-ipv6-day-orange-plans-ahead-and-prepares-for-the-new-internet-protocol
[50] IPv6 Best Practices
http://www.intercomms.net/issue-24/pdfs/articles/ipv6-best-practices-2015.pdf
[51] RIPE NCC 統計資料
https://www-public.imtbs-tsp.eu/~maigron/RIR_Stats/RIPE_Allocations/IPv6/ByNb/FR.html

[52]IPv6 at Google
https://www.ripe.net/participate/meetings/roundtable/february-2009/LorenzoIPv6atGoogle.pdf
[53]Internet Addressing：Measuring Deployment of IPv6
https://www.oecd.org/internet/ieconomy/44953210.pdf
[54]Testing transition mechanis,s in IPv6-only networks
https://blog.apnic.net/2020/08/11/testing-transition-mechanisms-in-ipv6-only-networks/
[55]"台灣駭客年會 HITCON 2020" https://hitcon.org/2020/
[56]"2020 IPv6 推廣講座活動"
http://www.kca.org.tw/sub_news.php?subkd=1&mskd=4&msid=2020091001
[57] 2020【網路・共贏時代】專家座談會
https://www.openfind.com.tw/taiwan/activity_detail.php?news_id=6961
[58]IETF RFC8754 〝IPv6 Segment Routing Header (SRH)〞
https://tools.ietf.org/html/rfc8754
[59]美國聯邦政府發布《完成向 IPv6 過渡》備忘錄
https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf

# 中英專有名詞對照

3G 第三代行動電話
(3rd-Generation, 3G)
4G 第四代行動電話
(4rd-Generation, 4G)
5G 第五代行動電話
(5rd-Generation, 5G)
6RD IPv6 快速部署(IPv6 Rapid Deployment, 6RD)

A

ACL 存取控制列表(Access Control List, ACL)
ADSL 非對稱式數位用戶迴路(Asymmetric digital subscriber line, ADSL)
ALG 應用層閘道器(Application Layer Gateway, ALG)
AH 認證標頭(authentication header, AH)
AI 人工智慧(Artifical Intelligence, AI)
Akamai 阿卡邁(Akamai Technologies)
Always-on 隨時在線(Always-on)
Anycast 任播(Anycast)
APNIC 亞太網路資訊中心(Asia-Pacific Network Information Centre, APNIC)
ARIN 美國網際網路號碼註冊中心(American Registry for Internet Numbers, ARIN)

B

Backbone 網路骨幹(Backbone)
BGP 邊界閘道器協定(Border Gateway Protocol, BGP)
BRAS 寬頻遠程接入伺服器(Broadband Remote Access Server, BRAS)

C

CDN 內容傳遞網路(Content Delivery Network, CDN)
CGN/CGNAT 電信級 NAT (Garrier Grade NAT, CGN/CGN)
Cloud Computing 雲端計算(Cloud Computing)
Co-Location 主機代管(Co-Location)
CPE 用戶終端設備(Customer Premises Equipment, CPE)
CRAN 收斂區域網路(Converged Regional Area Networks, CRAN)
CSRF 跨站請求攻擊(Cross Site Request Forgery, CSRF)

D

DAD 重複位址檢測(Duplicate Address Detection, DAD)
DDNS 動態網域名稱系統(Domain Name System, DDNS)
DHCP 動態主機組態協定(Dynamic Host Configuration Protocol)
DLZ 動態載入區域(Dynamically Loadable Zones, DLZ)
DNS 網域名稱系統(Domain Name System, DNS)
DNSSEC 網域名稱系統安全擴充(DNS security extension standard, DNSSSEC)
Dual Stack 雙協定(Dual Stack)
Data Packet 資料封包(Data Packet)
DOCSIS 纜線數據服務介面規格(Data Over Cable Service Interface Specification, DOCSIS)
DoS Attack 服務阻斷攻擊(Denial of Service Attack, DoS Attack)
DPI 深度封包檢測(Deep Packet Inspection, DPI)
DTA 數位經濟暨產業發展協會(Digital Transformation Association, DTA)

E

eHRPD 演進高速分組網路(Evolved High Rate Packet Data, eHRPD)
Email 電子郵件(Electronic mail, Email)
ESP 安全封裝負載(Encapsulating Security Payload, ESP)

F

FTTx 光纖網路(Fiber To The x, FTTx)
Firmware 韌體(Firmware)

G

Gateway 閘道器(Gateway)
Global address 全域位址(Global address)
GOLD Logo 金質標章(GOLD Logo)
GPL 通用公共許可協議(General Public License, GPL)
GRB 政府研究資訊系統(Government Research Bulletin, GRB)
GSN 政府網際服務網(Government Service Network , GSN)

H

Hot Spot 熱點(Hot Spot)
HGW 家庭閘道器(Home Gateway, HGW)
HGW-O 家庭閘道器(Home Gateway-Optiocal, HGW-O)

I

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

ICP 網際網路內容提供者(Internet Content Provider, ICP)

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

IDC 資訊機房(Internet Data Center, IDC)

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

IID 介面標識碼(Interface ID, IID)

Information Security 資訊安全(Information Security)

Internet APN 網際網路接入點名稱(Internet Access Point Name, Internet APN)

IoT 物聯網(Internet of Things, IoT)

IP 網際網路協議(Internet Protocol, IP)

IPAM 位址管理系統(IP Address Management, IPAM)

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

IPSecv6 IPv6 網際網路安全機制(Internet Protocol Security of IPv6, IPSecv6)

IPSO IP 智慧物件(Internet Protocol Smart Objects, IPSO)

IPTV 網路電視(Internet Protocol Television, IPTV)

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)

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

IT 資訊技術(Information Technology, IT)

L

L3 Switch 第三層交換器(Layer 3 Switch)

Link-local address 區域鏈結位址(Link-local address)

Load Balancer 負載平衡器(Load Balancer)

Loopback address 回送位址(Loopback address)

LSN 大規模 NAT(Large-Scale NAT, LSN)

LTE 長程演進技術(Long Term Evolution, LTE)

M

MIB 管理資訊庫(Management Information Base, MIB)
Mobile Internet 行動上網(Mobile Internet)
Multicast 多播/群播(Multicast)

N

NAT 網路位址轉換(Network Address Translation, NAT)
NAT Traversal NAT 穿越(NAT Traversal)
NDP 鄰居發現協議(Neighbor Discovery Protocol, NDP)
NCC 國家通訊傳播委員會(National Communications Commission, NCC)
Neighbor Cache 鄰居暫存(Neighbor Cache)
Network Layer 網路層(Network Layer)
NRO 號碼資源組織(Number Resource Organization, NRO)

O

OTT 網路隨選串流影片服務(Over- The-Top, OTT)

P

P2P 點對點對等網路架構(Peer to Peer , P2P)
PnP 隨插即用(Plug and Play , PnP)
PPPoE 網路對等協定(Point-to-Point Protocol Over Ethernet, PPPoE)
Prefix 網段(Prefix)
Private IP 私有位址(Private IP)
Profile 設定檔(Profile)
Public IP 公用位址(Public IP)
PWLAN 公眾無線區域網路(Public Wireless Local Area Networks, PWLAN)

R

RADIUS 遠端用戶撥入驗證服務(Remote Authentication Dial In User Service, RADIUS)
RAN 無線接取網路(Radio Access Network, RAN)
RIR 區域網路註冊管理機構(Regional Internet registry, RIR)
Router 路由器(Router)
RFC 網際網路協定規範(Reuest For Comments, RFC)
Routing Security 路由安全(Routing Security)
RPKI 網際網路號碼資源公鑰基礎設施(Resource Public Key Infrastructure, RPKI)

S

SAVI 來源位址驗證改善(Source Address Validation Improvement, SAVI)
SIP 對話啟動協定(Session Initiation Protocol, SAP)
SLAAC 無狀態位址自動配置(Stateless Address Autoconfiguration, SLAAC)

Smart Meter 智慧量表(Smart Meter)
SNMP 簡易網路管理協議(Simple Network Management Protocol, SNMP)
STB 數位機上盒(Set-Top Box, STB)
SOP 標準作業程序(Standatd Operating Procedure, SOP)

T

TANet 臺灣學術網路(Taiwan Academic Network, TANet)
TCA 台北市電腦商業同業公會(Taipei Computer Association, TCA)
TCP 傳輸控制協定(Transmission Control Protocol, TCP)
TiEA 台灣網路暨電子商務產業發展協會(Taiwan Internet and E-Commerce Association, TiEA)
Tunnel Broker 通道代理伺服器(Tunnel Broker)
TWNIC 財團法人台灣網路資訊中心(Taiwan Network Information Center, TWNIC)

U

UDP 使用者資料傳輸協定(User Datagram Protocol, UDP)
ULA 單一區域位址(Unique local address, ULA)
UMB 超行動寬頻 (Ultra Mobile Broadband, UMB)
Unicast 單播(Unicast)
Unspecified address 未定位址(Unspecified address)
USGv6 美國聯邦政府 IPv6 網通設備支援標準(United States Government IPv6 Profile, USGv6)

V

VDSL 超高速數位用戶迴路(Very-High-Bit-Rate Digital Subscriber Line, VDSL)
VOD 隨選視訊(Video on Demand, VOD)
VoIP 網路電話(Voice over Internet Protocol, VoIP)
VTUR VDSL 數據機(VDSL Modem, VTUR)

W

WiFi Router 寬頻分享器(WiFi Router)