109 年委託研究報告

物聯網服務與應用研析及網際網路技術標準研析

受委託單位

東海大學資訊管理學系

計畫主持人

林正偉

研究人員

賴囿嘉、陳晏羚、陳示珮、胡詠翔、

吳宜庭、古庭瑋、彭鍾碩、張巧宜、

陳臻、吳光軒、許桓禎、王品力

研究期程：中華民國 109 年 4 月至 109 年 12 月

研究經費：新臺幣 70 萬元

中華民國 109 年 12 月

目　　次

表　次

圖　　次

第一章　IETF 系列標準

第一節　IP (Internet Protocol)

一、IPv6 基本介紹

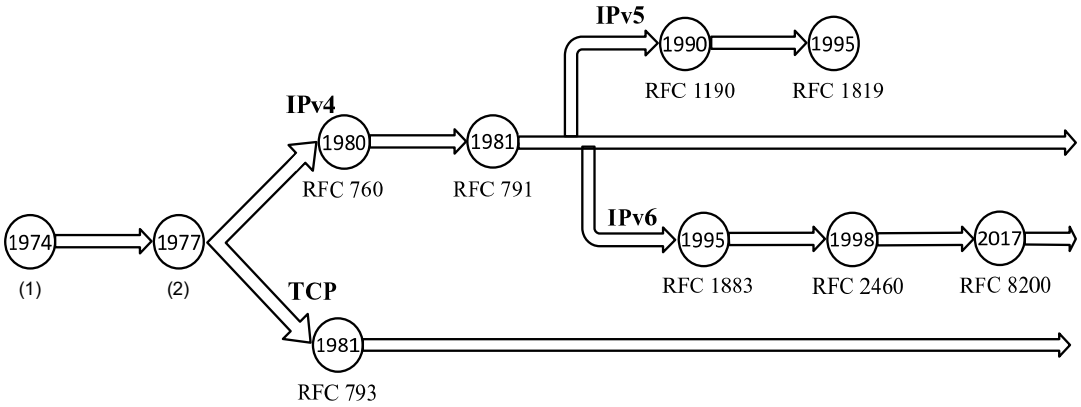
(一)　IP 的發展演進

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。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，投入建立以封包交換為基礎的 ARPANET，並於 1969 年 10 月首次成功在兩節點間傳送輸入的文字，開啟了現今網際網路發展的新紀元。

1990 年 3 月歐洲的 CERN 網路利用 T1(1.5Mbit/s)線路與美國 NSFNet 相連，同年 Timothy John Berners-Lee 開發了首套 World-Wide Web 的瀏覽器。1991 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)也允許非營利公司 Advanced Network and Services (ANS)的 ANSNet 與 NSFNet 同用實體主幹。台灣 TANet 則於 1991 年 12 月 3 日以 64Kbps 經美國東岸 Princeton University 連上 NSFNet。自 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，對網路接取及頻寬的需求也愈來

愈迫切。至 2020 年 1 月，全球估計上網人口已達 45 億人。

1974 年時 Vint Cerf 和 Bob Kahn 出版了一篇名為「Protocol for Packet Network Intercommunication」的論文，奠定了整個網際網路架構的基礎，後來該架構分為兩個模組分別進行發展，分別為傳輸層的 TCP 及網路層的 IP，亦即我們熟知的 TCP/IP 架構。第一版正式公開運作的 IP 是 IPv4，內建於當時的工作站及商用電腦。但是自 1990 年代起，考量到 IPv4 的位址空間可能無法負擔未來網路上的裝置數量，因此 IETF 在 1995 年制定了第一版 IPv6 規格以做為 IPv4 的繼任者，整個 IP 的規格發展如圖 1 所示。



(1). V. Cerf and R. Khan, "A Protocol for Packet Network Interconnection," *IEEE Transactions on Communications*, 22 (5), 1974
(2). IEN 2, Internet Experiment Note 2 (Comments on Internet Protocol and TCP), 1977

圖 1、IP 的規格演進(引用自維基百科)

(二)　IPv6 和 IPv4 的主要差異

IPv6 (RFC 8200)是網際網路協定的最新版本，主要是為了解決 IPv4 (RFC 791)位址枯竭的問題，兩者的主要差別可以分為以下幾類，

其比較如表 1 所示。

表 1、IPv4 與 IPv6 主要差異

	IPv4	IPv6
位址空間	32 位元 (4 Bytes)	128 位元 (16 Bytes)
位址類型	Unicast / Multicast / Broadcast	Unicast / Multicast / Anycast
表頭結構	可變長度 20-60Bytes，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)
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
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 進行芳鄰偵測和自動配置
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	利用選擇性的分段擴充標頭，只能在來源節點執行分段且在目的地節點執行重組
QoS 品保支援	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

每一台主機的每一個連線介面卡，均會自動取得或被設定一個全球或區網內部唯一的網路 IP 位址(IP Address)。發送端主機在送出的網路封包中，會在傳送的表頭內容(Header)表明自己的來源 IP 位址(Source Address)，並指名擬傳送對象的目的 IP 位址(Destination

Address)，表頭結構如圖 2 所示。IP 位址在 IPv4 為 32 位元，在 IPv6 為 128 位元。

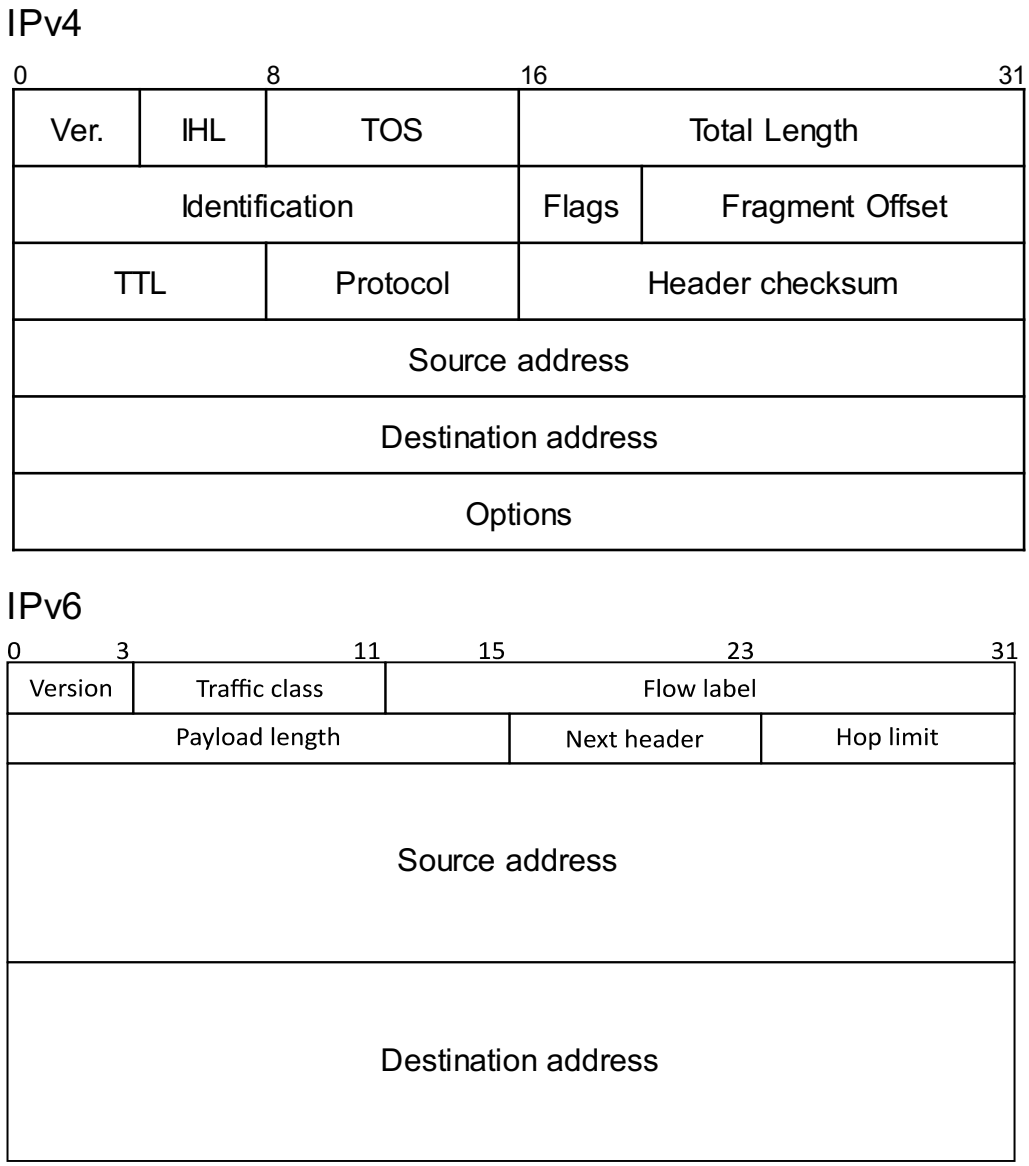


圖 2、IPv4 與 IPv6 表頭結構

傳統的網路通訊系統基本上都會提供一對一的單播(Unicast)、一對多的群播(Multicast)，或全體廣播(Broadcast)。網路群播已被廣泛應用在視訊、網路校時、內容散佈、mDNS、路由資訊交換、網路連線

遊戲等服務。IPv4 與 IPv6 也都支援群播(Multicast)，一般常見的 IP 網路層群播服務模式有支援多對多的 Any-Source Multicast (ASM)及以一對多為主的 Source-Specific Multicast (SSM)，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，經由路由器的幫忙，後續才可以收到送往該群播位址的封包。

IPv4 的 Internet Group Management Protocol (IGMP)及 IPv6 的 Multicast Listener Discovery (MLD)，即是被提出來支援主機加入、離開群組，以及群組一致性的維護等。群播一直是非常熱門的研究議題，很多文獻都注重在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的封包量。

除了群播外，IPv6 支援任播(Anycast)，針對一個 Anycast 位址內的一群主機，只有一個主機會收到送往該 Anycast 位址的封包。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。現有的群播方法中，傳統的 Multicast 群播是讓已加入群組的所有成員均會收到群播封包，Anycast 則只有一個成員會收到封包。

IPv6 具有以下的多個優勢：

1、 擴增的位址空間：IPv6 將 IP 地址的大小從 32 位增加到 128 位，以支援更多級別的尋址層次結構、更多數量的可尋址節點以及更簡單的地址自動配置。在多播地址上加入作用域(Scope)區段，可以改善多播路由的可伸縮性。IPv6 還定義了一種新型的地址，稱為「任播地址(Anycast Address)」，用於將封包發送到一組節點中的任何一個。

2、 簡化表頭結構：某些 IPv4 表頭欄位已被棄用或成為選用欄位，以減少處理絕大多數封包的成本並限制 IPv6 表頭的頻寬成本。

3、 改進擴增和選項支援度：IP 表頭選項編碼方式的更動使得轉發更有效率、更少的選項長度限制以及提高將來引入新選項的靈活性。

4、 流量標記能力：IPv6 增加了一項可以標記發送端請求封包序列的功能，發送端請求的封包序列在網絡中被視為單一個流量。

5、 身份驗證和隱私功能：IPv6 中的擴增支援了身份驗證、資料完整性和資料機密性(選項)的功能。

(三) IPv6 和 IPv4 對物聯網的差異

相較於 IPv4，IPv6 擁有大量位址空間以及不需透過網路位址轉換(NAT)連接的特性，使其對物聯網的相關應用極為友善。事實上，有關 IPv6 與物聯網的相關標準為 IETF 目前的重點之一，如已經結束的 6LoWPAN，目前仍在運作的 6Lo、lpwan 及 lwig 等都是與物聯網及資源限制裝置上的 IPv6 連接標準相關的工作組。

IPv6 的一大特點為其對低功耗無線個人區域網路(LoWPAN)及低功耗廣域網路(LPWAN)中的鏈路支援，這是 IPv4 中所沒有的特性。能達成這個特性的主要原因為 IPv6 針對不同種類的 LoWPAN 鏈路或是 LPWAN 鏈路制定了不同的轉換層。如 6LoWPAN 工作組制定了 IPv6 與 IEEE 802.15.4 間的轉換層。6Lo 工作組將 6LoWPAN 的成果進一步推廣，制定了 IPv6 到常見的 LoWPAN 鏈路協定(如 BLE、ITU-T G.9959、NFC、IEEE 802.11ah)的轉換層。而 lpwan 則制定了 IPv6 到如 SigFox、LoRa、Wi-SUM、NB-IoT 等 LPWAN 的轉換層。

由於 LoWPAN 和 LPWAN 的鏈路拓樸、MTU 與上下行鏈路模型皆與以大頻寬、高效能為訴求的 Ethernet 或是 WLAN 技術不同，因此上述這些轉換層的目的皆為將標準 IPv6 轉換至適合 LoWPAN 及 LPWAN 鏈路的大小與格式，其功能主要可以分為表頭壓縮、分段、群播轉換及鄰居發現。

IPv6 對物聯網有以下優勢：

1、 表頭壓縮降低成本：

若在 LoWPAN 及 LPWAN 的鏈路中使用標準 IPv6 40Bytes 的表頭，將會在鏈路訊框上消耗大量的空間，使得載酬的空間受到壓縮而降低傳輸效率，同時也會浪費多餘的能源與頻寬在傳輸 IPv6 的表頭。有鑑於此，IPv6 到 LoWPAN 或是 IPv6 到 LPWAN 的轉換層會執行表頭壓縮，表頭壓縮可以分為無狀態及有狀態兩種壓縮方式。無狀態表頭壓縮會透過鏈路層的表頭來推導出部分 IPv6 的表頭(如來源位址、Datagram 長度等)，或者透過將 IPv6 表頭的特定欄位設為一典型值來進行 IPv6 的表頭壓縮，如由 6LoWPAN 工作組所提出的 6LoWPAN-HC 其中的一種運作模式即為此方式。另一方面，有狀態表頭壓縮則透過雙方共享如位址前綴等語境的方式來使得可以在鏈路訊框中使用較短的識別碼即可還原出原 IPv6 的表頭，由 lpwan 工作組所提出靜態語境表頭壓縮(SCHC)即為此種壓縮方式，而 IPv4 僅能使用如 Robust Header Compression (ROHC)等編碼方式來實現表頭壓縮。

2、 取消分段並簡化錯誤檢查提升效率：

許多 LoWPAN 與 LPWAN 的 PHY/MAC 層技術為了簡化錯誤檢查機制、降低系統記憶體和處理器的需求以及達到較低的耗電量，僅會在鏈路層提供數十到數百 Bytes 的 MTU，這與 Ethernet 動輒 1500 Bytes 起跳的 MTU 差距甚大。此外，標準 IPv6 所要求的最小 MTU

為 1280 Bytes，顯然 LoWPAN 與 LPWAN 的部分鏈路無法滿足此一要求。因此，若 LoWPAN 與 LPWAN 的鏈路層沒有提供分段與重組功能的話,轉換層就必須負擔起將標準 IPv6 封包分段及重組的工作。此外，IPv6 並不允許中間節點進行封包的分段，這與 IPv4 相比大幅降低了節點的複雜度。

3、 可省略群播降低複雜度：

LoWPAN 與 LPWAN 的底層鏈路中通常只有單播或是廣播，只有如 IEEE 802.11ah 等少量的鏈路提供群播的功能，因此轉換層需透過直接將群播映射到廣播或是透過多次的單播來實現群播的轉換。相較之下 IPv4 並無此功能。

4、 優化鄰居發現：

鄰居發現是 IPv6 中一個優良的特性，該特性提供了物聯網自動設定位址及其他資訊的可能性，但是 LoWPAN 與 LPWAN 中的節點常常會進行休眠，其鏈路也為週期性可用，這些鏈路特性使得標準 IPv6 中的鄰居發現難以適用於 LoWPAN 與 LPWAN 的網路中。因此轉換層中需透過如 6LoWPAN ND 中節點主動和路由器溝通的方式進行鄰居發現。相較之下 IPv4 仍須透過如 ARP 等通訊協定來進行鄰居發現。

(四) IPv6 主要通訊協定

IPv6 正常運作需有許多協議參與其中,最主要的幾個協議為 NDP、SLAAC、DAD、ICMPv6、MLDv2 及 DHCPv6，這些協定運作時的架構如圖 3 所示，以下將針對上述幾個通訊協定進行簡介。

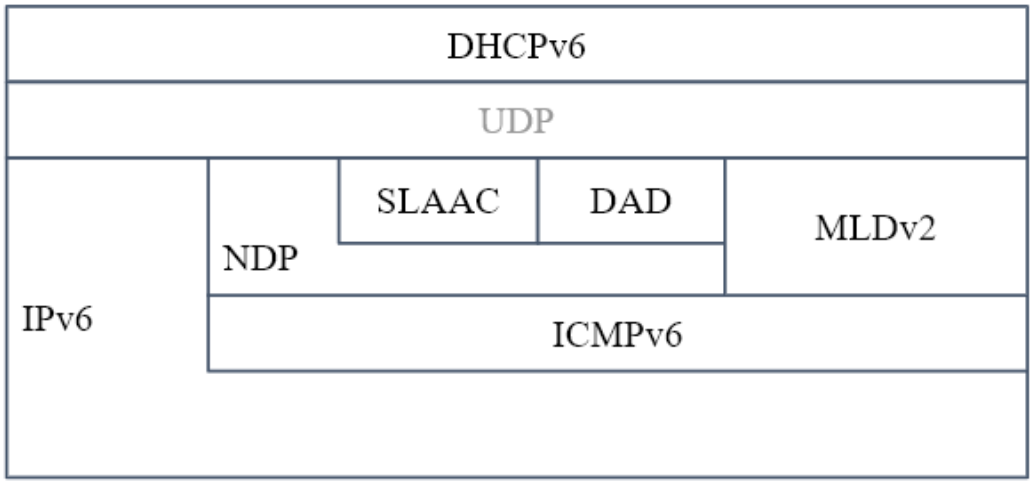


圖 3、IPv4 與 IPv6 表頭結構

1、 NDP (Neighbor Discovery Protocol, RFC 4861)

鄰居發現協議(Neighbor Discovery Protocol, NDP)是 IPv6 架構中一個極為重要的通訊協議，同一個鍊路中的 IPv6 節點透過鄰居發現協議尋找鍊路上其他節點的鍊路位址、尋找可以代替轉送封包的路由器並持續追蹤鄰居是否可達及其鍊路位址。

NDP 的定義主要是靠解決兩個在相同鍊路的節點進行資訊交換時所發生的問題來給出，其主要問題如下：

(1) 路由器發現：主機該如何在已銜接的鍊路上找到路由器。

(2) 前綴發現:主機該如何找到已銜接鍊路上的位址前綴集合。

(3) 參數發現:主機該如何知道鍊路的參數(如鍊路的MTU等)及網路層的參數(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 位址得出目標節點的鍊路位址。

(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不可達。若該鄰居是路由器的話，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的位址已經被其他節點使用。

(9) 重導向:路由器該如何告知主機有更佳的 First-Hop 通往特定的目的地。

2、 SLAAC (Stateless Address Autoconfiguration, RFC 4862)

自動位址設定的過程包含產生一個本地鍊路位址、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欲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的伺服器輔助。

位址自動設定透過結合本地資訊與路由器建議的資訊來產生全域位址。路由器建議鍊路上的前綴及子網路識別碼，而主機則會針對每個介面產生一個獨一無二的「介面識別碼」，兩者結合即為一個IPv6 的地址。若沒有路由器的參與，則主機只能產生本地鍊路位址來和同一個鍊路下的其他節點通訊。

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則可使用 RFC 8415 所提到的動態主機設定協定(Dynamic Host Configuration Protocol for IPv6, DHCPv6)，無狀態位址自動設定可以和 DHCPv6 同時共存。

3、 DAD (Enhanced Duplicate Address Detection, RFC 7527)

此文件介紹了一種藉由偵測回送 IPv6 ND 訊息方式所實現的重複位址偵測(Duplicate Address Detection, DAD)演算法，此外此文件還探討了在某些特殊接取網路中的重複位址偵測。

在 RFC 4862 的附錄 A 中討論了 IPv6 回送抑制(Loopback Suppression)和重複地址檢測（Duplicate Address Detection, DAD）。該文件提到了一種硬體輔助機制來檢測回送的 DAD 消息。如果硬體無法抑制回送的 DAD 消息，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 由 DAD 的 IPv6 節點的網介面產生。

DAD 中所涉及的另一個消息是鄰居建議(Neighbor Advertisement, NA)。此文件中的增強型 DAD 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 訊息不在此文檔的範圍之內。此文檔還包括有關一節的章節,討論了可用於緩解 DAD 回送問題的方法。

4、 PMTU (Path MTU Discovery for IPv6, RFC 8201)

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。這些封包的大小可以小於或等於路徑 MTU(Path MTU, PMTU)。或者是封包會被分成一系列片段，每個片段的大小小於或等於 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鍊路 MTU，這讓封包可以順利從起始節點傳送至目標節點從而無需 IPv6 分段，這個封包大小稱為路徑 MTU(Path MTU, PMTU)。此文件定義了一種用於節點發現任意路徑的 PMTU 的標準機制。

IPv6 節點應實作路徑 MTU 發現，以便發現並利用 PMTU 大於 IPv6 最小鏈路 MTU 的路徑。最小的 IPv6 實現（例如在開機 ROM 中）可以選擇省略路徑 MTU 發現的實作。

未實作路徑 MTU 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。在大多數情況下，這將導致使用較小的封包大小，因為大多數路徑的 PMTU 均大於 IPv6 最小鏈路 MTU。發送比路徑 MTU 所允許的封包大小還要小得多的封包的節點正在浪費網絡資源，並可能導致吞吐量不足。

如果阻止或不發送 ICMPv6 訊息，則實現路徑 MTU 發現並發送大於 IPv6 最小鏈路 MTU 的數據包的節點容易出現連接問題。例如，這將導致連接正確完成 TCP 三向握手，但是在傳輸數據時掛起，此狀態稱為黑洞連接(RFC2923)。路徑 MTU 發現依靠 ICMPv6 封包太大（Packet Too Big, PTB）來確定路徑的 MTU。

在 RFC4821 中可以找到路徑 MTU 發現的擴展。 RFC 4821 定義了一種用於打包層路徑 MTU 發現（Packetization Layer Path MTU Discovery, PLPMTUD）的方法，該方法設計用於無法確保向主機傳遞 ICMPv6 訊息的路徑上。

5、 DHCPv6 (Dynamic Host Configuration Protocol for IPv6 (RFC 8415)

DHCPv6 是一種用於自動配置網絡配置參數的可擴展機制，如自動配置節點的 IP 位址和前綴。網路參數可以以無狀態的方式提供，也可以結合一個或多個 IPv6 地址或 IPv6 前綴來進行有狀態分配參數提供。 DHCPv6 可以代替無狀態地址自動配置（SLAAC）或與其並

存。其運作過程如圖 4 所示，客戶端使用 DHCP_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。

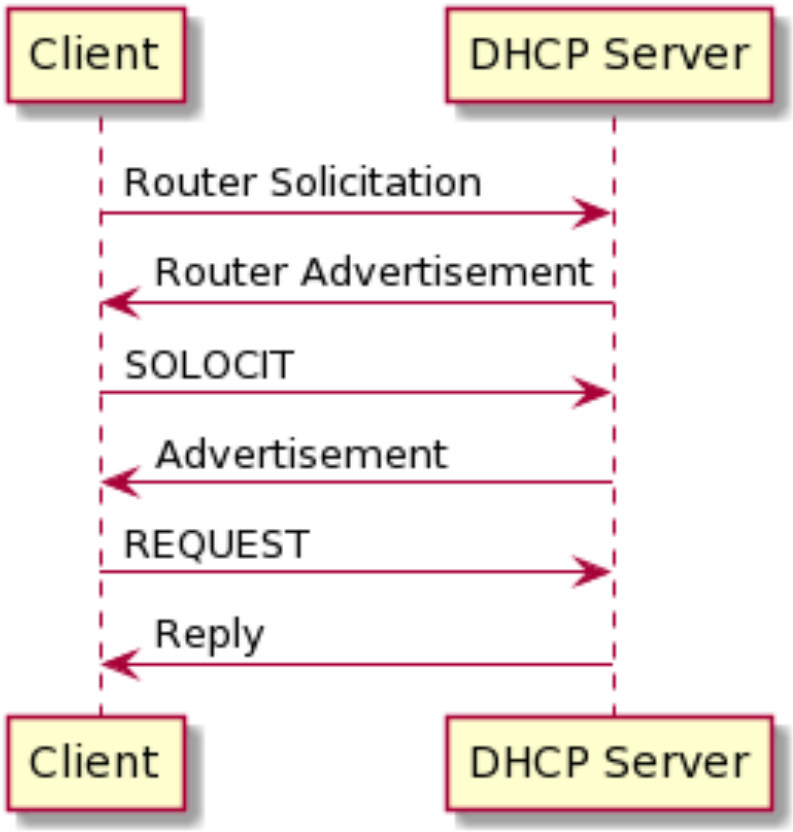


圖 4、DHCPv6 的運作過程

6、 ICMPv6 (Internet Control Message Protocol, RFC 4443)

IPv6 透過 ICMPv6 來傳遞控制訊息，如進行 Path MTU Discovery 及 NDP 等，ICMPv6 的 IPv6 Next Header 值為 58。

7、 MLDv2 (Multicast Listener Discovery Version 2 for IPv6, RFC 3810)

IPv6 路由器使用群播監聽器發現協議（MLD）來發現在其直接連接的鏈路上且希望接收群播封包的節點，並發現鄰居所感興趣的特定群播地址。群播路由器本身可以是一個或多個群播地址的監聽器。在這種情況下，它既執行 MLDv2 的“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。另一方面又執行“群播地址偵聽器部分”通知自身和其他相鄰的多播路由器它的收聽狀態。

二、IETF IPv6 標準制定現況

(一)　IPv6 相關領域分析

Internet Engineering Steering Group (IESG) 將 Internet Engineering Task Force (IETF) 的工作組 (Working Group, WG) 劃分為七個領域，分別是應用及即時通訊領域 (Applications and Real-Time Area, ART)、傳輸領域 (Transport Area, TSV)、路由領域 (Routing Area, RTG)、網際網路領域 (Internet Area, INT)、維護及管理領域 (Operations and Management Area, OPS)、資訊安全領域 (Security Area, SEC) 和一般事務領域 (General Area, GEN)。

其中，INT、OPS 及 SEC 為三個和 IPv6 較為相關的領域，INT 領域中因工作組眾多，故可再依據技術領域將工作組分類為專注在 IP 核心通訊協定的核心技術領域 (Core)、專注在資源限制較為嚴格節點上的低功耗網路技術領域 (Low Power) 、專注在移動性及備援

容錯機制的移動性和多址傳送技術領域(Mobility and Multihoming)及專注在時間相關通訊協定的時間技術領域 (Time) 等，各技術領域內相關的工作組及各工作組的目前階段如表 6 所示，其中各領域都另有同名、持續進行中的工作組未另外列出。

核心技術領域中共有七個工作組，分別是 Adaptive DNS Discovery (add)、Extensions for Scalable DNS Service Discovery (dnssd)、DNS PRIVate Exchange (dprive)、IPv6 Maintenance (6man)、Internet Area Working Group (intarea)、Home Networking (homenet) 和 Dynamic Host Configuration (dhc)。 add 負責進行自適應 DNS 解析器發現協定制定，其內容包括定義一種適用於公開或私有網路並支援加密的 DNS 解析器發現機制、制定客戶端和 DNS 解析器通訊的機制，使 DNS 解析器能提供一些訊息作為客戶端決策的依據。 dnssd 負責將原本僅限於本地鍊路連接 DNS 服務發現協定擴充成可以跨多個鍊路的協定，以方便無組態網路設定進行。 dprive 則負責提供 DNS 解析器和權威域名伺服器之間訊息交換的機密性，以避免使用者的個人訊息透過 DNS 洩漏。 6man 工作組的主要的工作為維護、修復和改進 IPv6 的協定及位址結構。 homenet 負責利用 IPv6 制定多路由器的家庭網路的架構及。dhc 則負責如 DHCPv6 等自動網路組態設定協定之制定。

低功耗網路技術領域內有四個工作組 IPv6 over Low Power Wide-Area Networks (lpwan)、IPv6 over Networks of Resource-constrained Nodes (6lo)、Light-Weight Implementation Guidance (lwig) 和 IPv6 over the TSCH mode of IEEE 802.15.4e (6tisch)。 lpwan 提出了可以在低功耗廣域網路壓縮標頭及分段標頭的靜態語境標頭壓縮與分段 (Static Context Header Compression and Fragmentation, SCHC) 標準，該工作組將繼續維護 SCHC 及提出將 SCHC IPv6/UDP 應用於目前技術的標準。 6lo 關注資源限制網路節點的連線，負責制定 IPv6 及由 6LoWPAN 所定的鍊結層技術間的轉換層標準及低複雜度標頭壓縮等通用標準。 lwig 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。 即將進入收尾階段的 6tisch 則負責制定基於 IEEE802.15.4 時槽跳頻技術的 IPv6 協定。

移動性和多址傳送技術領域內有 IP Wireless Access in Vehicular Environments (ipwave)、Distributed Mobility Management (dmm) 和 Host Identity Protocol (hip) 三個工作組。 ipwave 負責車對基礎設施通訊 (Vehicle-to-Infrastructure Communication, V2I) 及車對車通訊 (Vehicle-to-Vehicle Communications, V2V) 等車連網相關的網路通訊協定制定。 dmm 負責制定分散式移動設備管理及增強型移動性錨點的標準，以利無線網路中的移動性設備在移動時維持可用網路。 hip

提供了將終端節點識別與 IP 位址分開的方法，在該方法中終端節點使用公開金鑰來識別身份而非 IP 位址。

時間技術領域內有 Network Time Protocol (ntp) 及 Timing over IP Connection and Transfer of Clock(tictoc) 兩個工作組。ntp 負責制定第四版網路時間通訊協定 (NTPv4)的標準。 而 tictoc 則專注於提供高精準度的網路時鐘同步。

剩下的 IETF 研究領域中，OPS 及 SEC 都有和 IPv6 相關的工作組，以下將介紹所有有關的工作組。OPS 內的 IPv6 Operations (v6ops) 負責蒐集 IPv6 營運商和使用者所產生的問題及解決方案，以解決 IPv6 的營運問題。SEC 內的 IP Security Maintenance and Extensions (ipsecme)負責維護及擴充前代 IPsec 工作組所制定的 IPsec 協議套件，如 IKEv1、IKEv2 等，各工作組的目前階段如表 2 所示。

本報告將在上述工作組中挑出和 IPv6 相關的工作組，從中挑出和 IPv6 較為相關的 Standard Track RFC 和 Internet Draft，並進行更進一步的報告。Internet Area 的核心技術領域內總共挑出 6man 和 dhc 等和 IPv6 較為相關的工作組，低功耗網路內總共挑選了 6lo、lpwan、lwig 及 6tisch 等工作組，負責車連網相關標準制定的 ipwave 也在本報告的範圍內。最後，本報告從 Security Area 及 Operations and Management Area 內挑出 ipsecme 及 v6ops 等與 IPv6 的資訊安全

及維護有關的工作組進行報告，欲報告工作組如表 3 所列。

表 2、IETF IPv6 相關領域的工作組概況

領域	技術範籌	啟動階段	穩定運作	收尾階段
Internet Area (共 17WGs)	核心(Core)	add, dprive	dnssd, **dhc**, **6man**	homenet
	低功耗網路(Low Power)		**lpwan**, **6lo**	**lwig**, **6tisch**
	移動性和多址傳送 (Mobility and Multihoming)	drip	dmm	**ipwave**, hip
	時間(Time)		ntp, tictoc	
Operations and Management Area (共 14WGs)	網際網路維護(Internet)	mops	mboned, opsec, bmwg	**v6ops**
	路由和域名系統維護 (Routing & DNS)		grow, sidrops, dnsop	
	自動網路配置維護 (Automatic Network Configuration)	anima	netmod	netconf
	認證維護 (Authentication)	radext	dime	
Security Area (共 23WGs)	驗證和授權 (Authentication & Authorization)	emu, lake	oauth, kitten	ace
	憑證和身份 (Certificate & Identity)	rats	acme, sacm	
	簽章、加密和密碼學 (Signing, Encryption & Cryptography)	cose. lamps	trans, curdle	
	網路安全 (Network Security)	mls	tls, **ipsecme**, i2nfs	dots

	應用安全 (Application Security)		secevent, teep, tokbind, suit, mile	

表 3、IETF IPv6 相關重點工作組簡介

工作組名稱	工作組全名	領域	工作組介紹
6lo （8 Active Drafts, 11 RFCs）	IPv6 over Networks of Resource-constrained Nodes	Internet Area	關注資源限制網路節點的連線。
lpwan （5 Active Drafts, 2 RFCs）	IPv6 over Low Power Wide-Area Networks	Internet Area	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。
lwig （5 Active Drafts, 4 RFCs）	Light-Weight Implementation Guidance	Internet Area	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。
6tisch （4 Active Drafts, 3 RFCs）	IPv6 over the TSCH mode of IEEE 802.15.4e	Internet Area	負責制定基於 IEEE802.15.4 時槽跳頻技術的 IPv6 協定
ipwave （1 Active Drafts, 1 RFCs）	IP Wireless Access in Vehicular Environments	Internet Area	負責車連網相關的通訊協定制定。
6man （6 Active Drafts, 49 RFCs）	IPv6 Maintenance	Internet Area	維護和改進 IPv6 協定及位址結構。
dhc （5 Active Drafts, 100 RFCs）	Dynamic Host Configuration	Internet Area	負責如 DHCPv6 等自動網路組態設定協定之制定。
v6ops （4 Active Drafts, 78 RFCs）	IPv6 Operations	Operations and Management Area	負責蒐集 IPv6 營運商和使用者所產生的問題及解決方案。

ipsecme （6 Active Drafts, 28 RFCs）	IP Security Maintenance and Extensions	Security Area	負責維護及擴充前代IPsec 工作組所制定的IPsec 協議套件，如IKEv2。

(二)　IPv6 活躍工作組分析

1、 6lo - 負責 IPv6 在低功耗網路節點上的標準制定

(1) 工作組說明

6lo 致力於促進資源受限節點網絡上的 IPv6 連接的工作，這些節點的特點是：

- 有限的電源，記憶體和處理器資源
- 嚴格限制的狀態、程式碼空間及處理週期
- 最佳化的能源和網路頻寬使用
- 缺乏某些鏈路層服務，例如完整的設備連接和廣播/群播

具體來說，6lo 將在以下方面工作：

- 適用於資源受限節點的 IPv6-over-foo 的轉換層規範，使用 6LoWPAN 技術（RFC4944，RFC6282，RFC6775）作為鏈路層技術
- 上述轉換層用於基本監控和故障排除的訊息和資料模型（例如 MIB 模組）。
- 適用於多個轉換層規範的規範，例如低複雜度表頭壓縮

(2) 相關 RFCs

i RFC 4944 (Transmission of IPv6 Packets over IEEE 802.15.4 Networks, Proposed Standard RFC)：介紹了 IPv6 封包傳輸的幀格式以及在 IEEE 802.15.4 網絡上形成 IPv6 鏈路本地地址和無狀態自動配置地址的方法。此文件提到的其他規範包括使用共享上下文的簡單標頭壓縮方案以及 IEEE 802.15.4 網格中的封包傳遞規定。

ii RFC 6282 (Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks, Proposed Standard RFC)：此文件為 6LoWPAN 中的 IPv6 封包傳遞指定了 IPv6 表頭壓縮格式。壓縮格式依靠共享上下文來允許壓縮任意前綴。 如何在共享上下文中維護信息不在此文件的範圍。此文件指定了多播地址的壓縮和用於壓縮下一個標頭的框架。UDP 標頭壓縮是在此框架中指定的。

iii RFC 6775 (Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs), Proposed Standard RFC)：介紹了針對 6LoWPAN 和類似網絡的 IPv6 鄰居發現的簡單優化、尋址機制以及重複地址檢測。

iv RFC 7388 (Definition of Managed Objects for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs), Proposed Standard RFC)：定義了一個管理資訊庫(Management Information Base, MIB)上的物件，用來管理在無線個人區域網路上的 IPv6。

v RFC 7400 (6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs), Proposed Standard RFC)：擴充了 RFC 6282 所定義之 6LoWPAN 中的表頭壓縮，使其能支援通用表頭(generic headers) 及表頭狀載酬(header-like payloads)之壓縮，從而避免為了上述兩種資料重新定義資料壓縮格式。

vi RFC 7428 (Transmission of IPv6 Packets over ITU-T G.9959 Networks, Proposed Standard RFC)：描述了在 ITU-T G.9959 網路上進行 IPv6 傳輸時的訊框(frame)格式、本地鍊路位址(link-local address)及無狀態自動位址設定的方法。

vii RFC 7668 (IPv6 over BLUETOOTH(R) Low Energy, Proposed Standard RFC)：介紹了如何在藍芽低功耗網路上進行 IPv6 的傳輸，包括鍊路模型(Link Model)、無狀態位址自動設定及鄰居發現等等。

viii RFC 7973 (Assignment of an Ethertype for IPv6 with Low-Power Wireless Personal Area Network (LoWPAN) Encapsulation, Informational RFC)：描述了使用 LoWPAN 的 IPv6 的 datagram 若被 Ethernet 封裝時，其訊框之 EtherType 應為 0xA0ED 。EtherType 列表可以參考 http://standards-oui.ieee.org/ethertype/eth.txt。

ix RFC 8025 (IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Paging Dispatch, Proposed Standard RFC)：補充 RFC4944，介紹了一種適用於 6LoWPAN 表頭壓縮的 contex-switch 機制，該機制以分頁表示，並以新的機制調度分頁。

x RFC 8065 (Privacy Considerations for IPv6 Adaptation-Layer Mechanisms, Informational RFC)：討論了當 IPv6 設計跨越了多種 link-layer 時會發生的幾種隱私威脅，並提供如何識別那些威脅的方法。

xi RFC 8066 (IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) ESC Dispatch Code Points and Guidelines, Proposed Standard RFC)：補充了 RFC 4944 中所提到的 ESC

dispatch type，該 dispatch type 可以讓 6LoWPAN 的 header 調度多個位元組。

xii RFC 8105 (Transmission of IPv6 Packets over Digital Enhanced Cordless Telecommunications (DECT) Ultra Low Energy (ULE), Proposed Standard RFC)：超低功耗數位增強無線電話 (DECT ULE) 是一個由 DECT 論壇所推出並由 ETSI 制定規格的低功耗空中介面技術。該文件描述了當使用 DECT ULE 進行 IPv6 傳輸時的通訊協議堆疊及鍊路模型。

xiii RFC 8163 (Transmission of IPv6 over Master-Slave/Token-Passing (MS/TP) Networks, Proposed Standard RFC)：MS/TP 是一個 RS-485 的媒體存取控制方法，該文件定義了在 MS/TP 網路上傳輸 IPv6 封包時的訊框格式、鍊路形成的方法及無狀態自動位址設定的方法。

xiv RFC 8505 (Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery, Proposed Standard RFC)：簡化了 RFC 6775 6LoWPAN 鄰居發現協議的註冊過程，以增進註冊的容量及不同網路拓樸間移動的偵測。

(3) 進行中的 Internet Drafts

i Address Protected Neighbor Discovery for Low-power and Lossy Networks (draft-ietf-6lo-ap-nd-23, Date: 2020-04-30)：提出了一種在 6LoWPAN 上可以防止位置被竊盜的鄰居發現協定擴充。在該方法中，節點須先以密碼識別號碼(Crypto-ID) 註冊位址並證明持有該 Crypto-ID，使用 Crypto-ID 可以防止已註冊的位址在低功耗易遺失網路上(Low-power and Lossy Network, LLN)被竊盜。

ii IPv6 Backbone Router (draft-ietf-6lo-backbone-router-20, Date: 2020-03-23)：該文件擴充了 RFC 6775 以使用骨架路由器(Backbone Router)代理居發現協定的服務，骨架路由器被放置於骨幹網路的邊緣，以整合多個無線鍊路形成一個子網路。

iii IPv6 Mesh over BLUETOOTH(R) Low Energy using IPSP (draft-ietf-6lo-blemesh-07, Date: 2019-12-14)：該文件將 IPv6 over BLE (RFC 7668) 的拓樸由星狀網路改為網狀網路，並敘述建立鍊路的機制，該文件並不包含在 BLE Mesh 上進行路由的部份。

iv Packet Delivery Deadline time in 6LoWPAN Routing Header (draft-ietf-6lo-deadline-time-05, 2019-07-08)：定義了一個新的 6LoWPAN 路由類型，該路由類型還有一個截止時限，使得

在具有時間同步網路內的路由排程器可以決定時間緊迫的機器對機器溝通(M2M) 之路由順序。

v 6LoWPAN Selective Fragment Recovery (draft-ietf-6lo-fragment-recovery-21, Date: 2020-03-23)：提出了一種可以單獨傳送個別分段(fragment)到終端且具有壅塞控制的通訊協定，使得大資料傳輸失敗時只須重傳失敗的部份就好，不須重傳整段資料。

vi On Forwarding 6LoWPAN Fragments over a Multihop IPv6 Network (draft-ietf-6lo-minimal-fragment-15 , Date: 2020-03-23)：提供了一個泛化的規則讓 6LoWPAN 的 fragment 可以被轉送到 route-over network，如此的轉送可以降低延遲、提昇可靠度並降低中間節點的緩衝區需求。

vii Transmission of IPv6 Packets over Near Field Communication (draft-ietf-6lo-nfc-15, Date: 2019-07-08)：敘述如何在近場通訊(NFC)上進行 IPv6 的傳輸，包括協定堆疊、鍊路模型、無狀態自動位址設定、本地鍊路位址、鄰居發現、表頭壓縮等。

viii Transmission of IPv6 Packets over PLC Networks (draft-ietf-6lo-plc-03, Date: 2020-04-29)：敘述如何在如 ITU-T G.9903, IEEE 1901.1 和 IEEE 1901.2 等電力線通訊(PLC)上進行 IPv6 的

傳輸，包括協定堆疊、無狀態自動位址設定、本地鍊路位址、鄰居發現、表頭壓縮等。

2、 lpwan - 負責 IPv6 在低功耗廣域網路上的標準制定

(1) 工作組說明

SIGFOX，LoRa，WI-SUN 和 NB-IOT 等低功耗廣域網路(LPWAN)的技術出現帶給物連網領域不小的衝擊。這些技術都有一些共同的特徵，如最佳化的無線電調製、星形拓撲、以超低速每天傳輸幾十個位元組、有時可變的 MTU 且大部分是上行傳輸模式，這些特性使得設備可以將大部分時間花費在低能耗深度睡眠模式下，以節約耗電量並延長電池壽命。

然而這些好處是有代價的，低功耗廣域網路的鏈路層幀格式已針對每種技術進行了優化和特化。由於沒有網路層，所以應用程式通常直接連接到鏈路層。這導致不同技術間的部署及管理必須單獨進行且從一種 LPWAN 技術遷移到另一種 LPWAN 技術意味著要重新建構整個通訊鏈。因此需引入網路層的 IPv6 來提供一個統一的介面讓不同技術間互相溝通。

LPWAN 的特徵為稀疏且廣泛的不平衡空中傳輸，且幾乎沒有辦法透過改變幀格式引入 IPv6，這使得現有的 IETF 工作（6lo）無法被簡單地應用。因此 lpwan 工作組將：

- 維護 SCHC，包括為上層協議啟用 SCHC 機制。
- 產出在現有技術上應使用 SCHC IPv6 / UDP 的標準文件。
- 生成一份標準文件，以定義通用資料模型，用以正式化 LPWAN 的壓縮和分段上下文。
- 產出一份對 LPWAN 設備的操作，管理和維護（OAM）的標準文件，包括對延遲或代理存活性驗證（Ping）的支援。

(2) 相關 RFCs

i RFC 8376 (Low-Power Wide Area Network (LPWAN) Overview, Informational RFC)：低功耗廣域網路(Low-Power Wide Area Network, LPWAN) 是一種涵蓋範圍很廣的無線技術，該網路的頻寬低、封包大小可能很小 、 裝置電池壽命長。本文件涵蓋了多種被 IETF 所考慮進來的 LPWAN 技術介紹，包括 LoRaWAN、NB-IoT、Sigfox 及 Wi-SUN Alliance Field Area Network (FAN)，同時也介紹目前技術和 LPWAN WG 目標間的差異。

ii RFC 8724 (SCHC: Generic Framework for Static Context Header Compression and Fragmentation, Proposed Standard RFC)：定義了靜態語境表頭壓縮及分段(Static Context Header Compression and fragmentation, SCHC)的框架，該框架提供了

表頭壓縮和一個最佳化的分段機制。SCHC 的壓縮是基於儲存在 LPWAN 裝置和網路基礎建設內的共同靜態語境(Common Static Context) ，此文件定義了一個泛化的表頭壓縮機制和其在 IPv6/UDP 表頭壓縮上的應用。

3、 lwig - 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

(1) 工作組說明

通信技術已嵌入到我們的環境中，我們的建築物，車輛，設備和其他物體中的不同類型的設備需要進行通信，並且可以預期大多數設備將採用 IPv6 進行通信。但是，不同類型的設備之間的功能差異很大，並且嵌入所有必需的功能並不是那麼容易。

輕量級實施指南（Light-Weight Implementation Guidance, LWIG）工作組致力於幫助最小裝置上的實作。目標是能夠為最受限制的環境構建最小但具有可交互操作 IP 功能的設備。

(2) 相關 RFCs

i RFC 7228 (Terminology for Constrained-Node Networks, Informational RFC)：該文件敘述了如 Constrained Nodes、Constrained Networks 、 Challenged Networks 、 LLN 和 LoWPAN 的解釋。

ii RFC 7815 (Minimal Internet Key Exchange Version 2 (IKEv2) Initiator Implementation, Informational RFC)：介紹了 IPsec 中用來進行驗證的 IKEv2 通訊協定之最小實作版本，以利資源限制網路節點使用。IKEv2 中有幾個選項特色在此文件的實作中被認為是不需要的特色而被移除，此文件只保留 IKEv2 能正常使用且相容於原版 IKEv2 的實作。

iii RFC 8352 (Energy-Efficient Features of Internet of Things Protocols, Informational RFC)：介紹了具能源效率之通訊協定的挑戰以及現今如何跨越這些挑戰，並總結出鍊路層進行俱能源效率之通訊協定設計時的技巧。本文件同時也提供了不同層在制定俱能源效率之通訊協定時的技巧概覽。

iv RFC 8387 (Practical Considerations and Implementation Experiences in Securing Smart Object Networks, Informational RFC)：敘述了設計安全且資源受限之智能物件的挑戰，並提出一個可以被該種物件使用的部屬模型。該文件也討論了現行密碼程式庫在資源受限裝置上的可用性，並實驗在資源受限裝置上進行數位簽章的效能。最後，該文件探討了不同逼近安全方法的優缺點。

(3) 進行中的 Internet Drafts

i Virtual reassembly buffers in 6LoWPAN (draft-ietf-lwig-6lowpan-virtual-reassembly-02, Date: 2020-03-09)：敘述 6LoWPAN 在進行分段時可能會產生的問題，並提出了方法解決該分段問題。

ii Building Power-Efficient CoAP Devices for Cellular Networks (draft-ietf-lwig-cellular-06, Date: 2016-01-04)：討論了受限應用通訊協定(Constrained Application Protocol, CoAP) 在透過蜂窩網路連接的感測網上的使用。該文件聚焦在如何降低使用功率。

iii Alternative Elliptic Curve Representations (draft-ietf-lwig-curve-representations-10, Date: 2020-04-23)：敘述了如何將 Montgomery curves 和 (twisted) Edwards curves 等橢圓曲線用 short-Weierstrass form 表達，並展示如何使用這個格式實作如 ECDSA 及 ECDH 等橢圓曲線密碼學。

iv TCP Usage Guidance in the Internet of Things (IoT) (draft-ietf-lwig-tcp-constrained-node-networks-09, Date: 2019-11-04)：提供了如何在資源受限裝置上實作輕量化的 TCP 協定的引導。基於 IP 的 IoT 中目前主要的傳輸層協議是 UDP 和 TCP。但是，TCP 通常被不公平的批評為不適用於 IoT 協定。事實上

某些 TCP 功能對於物聯網應用情境不是最佳的，例如相對較長的表頭大小、不適合多播以及始終確認的資料傳遞。但是關於 TCP 不適合物聯網的許多典型主張（例如，高複雜性，連接導向的方法與無線電佔空比的不相容以及無線鏈路中的虛假擁塞控制）是無效的且可以解決的。或者也可以找到公認的物聯網節點到節點可靠性機制。在應用層，CoAP 是使用 UDP (RFC7252)開發的。但是某些 CoAP 部署與現有基礎架構的集成正受到中間節點（如防火牆）的挑戰，這可能會限制甚至阻止基於 UDP 的通訊。這是開發基於 TCP 的 CoAP 規範(RFC8323)的主要原因。

v Terminology for Constrained-Node Networks (draft-bormann-lwig-7228bis-06, Date: 2020-03-09)：敘述了如 Constrained Nodes、Constrained Networks、Challenged Networks、LLN 和 LoWPAN 的解釋，這份文件可能會更新 RFC 7228。

vi Security Classes for IoT devices (draft-urien-lwig-security-classes-03, Date: 2020-05-24)：定義了資源受限裝置的安全分類，使用五個布林指標進行分類：一次性可程式記憶體(one time programmable memory, OTP)、韌體載入器(firmware loader, FLD)、安全韌體載入器(secure firmware loader, FLD-

SEC)、抗竄改密鑰(tamper resistant key, TRT-KEY) 及多元化密鑰(diversified key, DIV-KEY)。

4、 6tisch - IPv6 在 IEEE 802.15.4e 的 TSCH 模式下的規範制定

(1) 工作組說明

低功率有損網路（LLN）可能連接了大量的資源受限節點，以形成無線網狀網絡。 6LoWPAN，ROLL 和 CoRE IETF 工作組在協議堆疊的各個層上定義了協定，包括 IPv6 轉換層，路由協定和 Web 傳輸協定。該協議堆疊已使用在 IEEE802.15.4 低功耗無線電上。

時槽跳頻（TSCH）模式於 2012 年引入，是對 IEEE802.15.4 標準的媒體訪問控制（MAC）部分的修正。 TSCH 是工業自動化和過程控制 LLN 的新興標準，直接繼承自 WirelessHART 和 ISA100.11a。6TiSCH 通過 TSCH 定義了 IPv6，為在工業標準中進一步採用 IPv6 以及將運營技術（OT）與信息技術（IT）融合的關鍵。

6tisch 將致力於通過 IEEE802.15.4 標準的 TSCH 模式啟用 IPv6。其工作組的問題範圍是一個或多個 LLN，可能通過一個或多個 LLN 邊界路由器（LLN Border Router, LBR）透過公共主幹鏈路結合。6tisch 將依賴於現有的 LBR 認證機制，並在必要時進行擴展。

(2) 相關 RFCs

i RFC 8180 (Minimal IPv6 over the TSCH Mode of IEEE 802.15.4e (6TiSCH) Configuration, Best Current Practice RFC)：敘述了 IPv6 over TSCH mode of IEEE 802.15.4e 的最小設定，並定義了連接其他 IETF 通訊協定的介面，該設定應該被所有與 6TiSCH 相容的裝置實作。

ii RFC 8480 (6TiSCH Operation Sublayer (6top) Protocol (6P), Proposed Standard RFC)：敘述了 6TiSCH 的作業子層(Operation Sublayer)的協定，該子層可以使 6TiSCH 網路具有分散式排程的功能。6TiSCH 網路中的所有通信均按排程表進行安排。 排程表由單元格組成，每個單元格均有（slotOffset，channelOffset）標識。 此規範接手定義了尚未被6top工作組定義完成的6TiSCH操作子層（6top）協議（6P）。6P 允許節點與鄰居節點通信，以相互添加/刪除時槽跳頻（TSCH）單元。 這讓節點得以在 6TiSCH 網路中進行分散式排程管理。 6top 由一個或多個調度功能（SF）和此文件中定義的 6top 協議組成。

(3) 進行中的 Internet Drafts

i Constrained Join Protocol (CoJP) for 6TiSCH (draft-ietf-6tisch-minimal-security-15, Date: 2019-12-10)：敘述了新裝置安全加

入 6TiSCH 網路的最小框架，該框架要求新加入的節點和 JRC (join registrar/coordinator, a central entity) 共享一把對稱金鑰，並透過 CoAP 傳送請求的方式取得網路參數並加入 6TiSCH 的網路。

ii 6TiSCH Minimal Scheduling Function (MSF) (draft-ietf-6tisch-msf-16, Date: 2020-04-02)：敘述了 6TiSCH 的最小排程函數 (MSF)，排程函數決定了一個新節點加入網路時的行為及節點間的通訊如何排程。

5、 ipwave - 負責車連網相關的網路通訊協定制定

(1) 工作組說明

越來越多的汽車和車輛連接到網際網路。2020 年左右汽車有望在道路上使用如增強舒適性的娛樂應用、使用雙向資料流的道路安全應用以及聯網的自動駕駛的一些新功能。

如今有幾種已部署的車輛到網際網路技術（V2Internet），它們利用嵌入式網際網路模組或乘客的智慧手機，如 mirrorlink，carplay，android auto。車輛到基礎設施（Vehicle-to-Infrastructure, V2I）通信用於車輛和道路基礎設施之間無線交換重要的安全性和運作資料，主要目的是避免汽車碰撞。車輛到車輛通信（Vehicle-to-Vehicle Communications, V2V）用於車輛之間的短距離通信，以交換車輛信息，

例如車輛速度、前進方向和製動狀態。

ipwave 將研究非常適合以 IP 作為網絡技術的 V2V 和 V2I 使用案例，並將開發基於 IPv6 的解決方案，以在車輛與其他車輛或固定系統之間建立直接和安全的連接。這些車連網的特徵在於動態改變網絡拓撲和連接性。

(2) 相關 RFCs

i. RFC 8691 (Basic Support for IPv6 Networks Operating Outside the Context of a Basic Service Set over IEEE Std 802.11, Proposed Standard RFC)：描述了如何使用 IPv6 連接兩個以單一 IEEE 802.11-OCB 鍊路連接在一起的節點。並討論了該方法的相關缺點，此文件並沒有描述最佳化方法及複雜的 IPv6 使用情境，這些議題將在未來的文件被討論。

(3) 進行中的 Internet Drafts

i IPv6 Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases (draft-ietf-ipwave-vehicular-networking-14, Date: 2020-3-9)：該文件敘述了在車連網使用 IPv6 時的問題描述及使用案例。該文件也描述了車對車(vehicle-to-vehicle, V2V)、車對基設施(vehicle-to-infrastructure, V2I)及車對任何物品(vehicle-to-everything, V2X)的主要情境。

這份文件同時也構成了以 IPv6 為基底的車連網的需求，如鄰居發現、移動性管理、資訊安全及隱私等。

ii Context-Aware Navigator Protocol for IP-Based Vehicular Networks (draft-jeong-ipwave-context-aware-navigator-01, Date: 2020-05-07)：提出了一種語境敏感之導航通訊協定(Context-Aware Navigator Protocol, CAN)，其目標為透過輕量化的資訊共享增進 IP 車連網的駕駛安全性。CAN 使用 IPv6 的鄰居發現協定中的選填欄位傳遞駕駛資訊，如車輛位置、行車速度、加速減速狀態、行使方向及駕駛人的操作。

iii DNS Name Autoconfiguration for Internet-of-Things Devices in IP-Based Vehicular Networks (draft-jeong-ipwave-iot-dns-autoconf-08, Date: 2020-05-07)：描述了一種適用於 IP 車連網的自動網路設定、裝置發現及服務發現方案。此方案中，IoT 裝置的 DNS 名稱可以被自動設定。使用者或是其他 IoT 裝置可以透過 DNS 名稱來識別該裝置。

iv Basic Support for Security and Privacy in IP-Based Vehicular Networks (draft-jeong-ipwave-security-privacy-01, Date: 2020-05-07)：聚焦在 IP 車連網可能的安全及隱私問題，並對這些問題提出對策。可能的攻擊方式有假訊息攻擊、身份偽造攻

擊、服務阻斷攻擊、訊息擱置攻擊、竄改攻擊及追蹤的可能性。

v Vehicular Mobility Management for IP-Based Vehicular Networks (draft-jeong-ipwave-vehicular-mobility-management-03, Date: 2020-05-07)：定義了載具移動管理(Vehicular Mobility Management , VMM) 的方案。此方案為基於多鍊路子網(multi-link subnet)的車連網模型，車輛可在移動時透過該方案傳遞自身的位置及速度資料。

vi Vehicular Neighbor Discovery for IP-Based Vehicular Networks (draft-jeong-ipwave-vehicular-neighbor-discovery-09, Date: 2020-05-07)：定義了 IPv6 鄰居發現協定的擴充—載具鄰居發現協定(Vehicular Neighbor Discovery, VND)。該方法使用了最佳化的地址註冊(Address Registration)及多跳重複位址發現機制(Duplicate Address Detection, DAD)。

vii Considerations for ID/Location Separation Protocols in IPv6-based Vehicular Networks (draft-kjsun-ipwave-id-loc-separation-02, Date: 2020-03-09)：為了達到可擴展的路由、加強移動性及增進隱私，ID/位置分離協定在 IP 車連網中被提出。此文

件分析了要如何將 ID/位置分離協定導入 IP 車連網及提出有效的 ID/位置分離協定建議。

viii Data Aggregation in IPv6-based Vehicular Networks (draft-yan-ipwave-aggregation-01, Date: 2020-05-17)：由於在 IP 車連網中所交換的通常是小且多的訊息，所以為了更有效的交換資料，這份文件描繪了基於訊息中心網路(Information-centric networking, ICN) 的資料聚合的需求，以提昇 IP 車連網中的訊息交換效率。

ix Service and Neighbor Vehicle Discovery in IPv6-Based Vehicular Network (draft-yan-ipwave-nd-06, Date: 2020-05-17)：使用了 DNS-SD/mDNS 去實作 IP 車連網中的鄰居發現及載具的鍊路層位址發現，其目標為協同自適應巡航控制(Cooperative Adaptive Cruise Control, C-ACC)。

6、 6man - 負責 IPv6 的維護、演化、進場以及 IPv4 的退場

(1) 工作組說明

6man 工作組負責 IPv6 協議規範和定址體系結構的維護，維護和改進，並不會對 IPv6 規范進行重大更改或添加。6man 將解決在部署和操作過程中發現的協議限制、問題，同時也是在 IETF 中討論及處理 IPv6 相關問題的適當場所。

6man 是對 IPv6 協定進行擴展和修改的設計機構。6man 可以自行決定審查在另一個工作組中擴展或修改 IPv6 協定的任何文件、進行兩個工作組的 AD 協商並可以向 IESG 建議在這些文件中的任何一個出版前都須和 6man 工作組達成共識。

(2) 相關 RFCs

i RFC 6437 (IPv6 Flow Label Specification, Proposed Standard RFC)：流量標籤為 IPv6 的一大特色，流量標籤使得 IPv6 僅須檢查表頭的固定欄位即可分類流量，提高了分類的效率。此文件為 IPv6 流量標籤的規格書，其中敘述了流量標籤的欄位、IPv6 節點對流量最標籤時的最低要求及流量狀態建立的方式。以網路層的觀點來看，流量是指從同一個來源透過單播、群播、任播的方式送給同一個或是同一群目的地的一連串封包。傳統僅能透過一個五元組(5-tuple)去區分不同的流量，這五個欄位分別是來源位址、來源連接阜、目的位址、目的連接阜及傳輸層類型，但是，這其中有些欄位常常因為分段或是加密的原因使得他們讀會同時出現在同一個封包，因此 IPv6 採用以流量標籤、來源位址及目的位址所構成的三元組來區分各個流量，如此便能更有效率的進行流量的分類。

ii RFC 6438 (Using the IPv6 Flow Label for Equal Cost Multipath Routing and Link Aggregation in Tunnels, Proposed Standard RFC)：流量標籤使用上固然方便，但是其有一些使用限制。此文件便在描述流量標籤在使用多氯徑路由進行負載平衡並面對相同路徑成本的多條路徑時的使用限制。

iii RFC 6553 (The Routing Protocol for Low-Power and Lossy Networks (RPL) Option for Carrying RPL Information in Data-Plane Datagrams, Proposed Standard RFC)：描述低功耗且易遺失路由協定(Routing Protocol for Low-Power and Lossy Networks, RPL) 的選項欄位，該選項欄位能儲存如路由訊息等資訊。

iv RFC 6554 (An IPv6 Routing Header for Source Routes with the Routing Protocol for Low-Power and Lossy Networks (RPL), Proposed Standard RFC)：低功耗且易遺失路由協定(Routing Protocol for Low-Power and Lossy Networks, RPL) 為低功耗且易遺失網路上的一種重要的路由協定，通常運作在記憶體受限制的網路節點上。為此，本文件制定了一個新的 IPv6 路由表頭選項，使得可以 IPv6 節點可以使用 RPL 進行路由。

v RFC 6935 (IPv6 and UDP Checksums for Tunneled Packets, Proposed Standard RFC)：為了增進 UDP datagram 使用 IPv6

隧道進行傳輸時的效率，本文件描述了一種透過放寬 IPv6 UDP 校驗和的需求來增進效能的方式。

vi RFC 6946 (Processing of IPv6 "Atomic" Fragments, Proposed Standard RFC)：IPv6 的規格內允許封包含有分段表頭但是該封包卻不會分段，這種封包稱為原子分段(Atomic Fragments)。這種封包通常是被那些收到 ICMPv6 “Packet Too Big”錯誤訊息的節點所發出，用來建議 Next-Hop MTU 設定為小於 1280 bytes 並開始傳送分段流量。此文件在討論原子分段的產生以及相關的資訊安全議題。

vii RFC 6980 (Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery, Proposed Standard RFC)：分析使用了 IPv6 分段的鄰居發現之安全議題，並討論了使用 IPv6 分段和安全鄰居發現 (SEcure Neighbor Discovery, SEND) 如何減輕上述問題。

viii RFC 7048 (Neighbor Unreachability Detection Is Too Impatient, Proposed Standard RFC)：敘述了一個潛藏在 IPv6 鄰居發現協定裡的一個會造成效能下降的問題—鄰居不可達偵測(Neighbor Unreachability Detection)，發生問題的是其預設等待時間為三秒。對於沒有替代鄰居(alternative neighbors)的情

境下，預設等待時間顯的有點冗長。因此此文件提出一套相對寬鬆的鄰居發現規則以改善上述問題。

ix RFC 7217 (A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC), Proposed Standard RFC)：當使用者改變其通訊介面時，舊有的方法會根據新的 MAC Address 產生新的介面識別碼(Interface Identifier, IID)，造成使用者使用無狀態位址自動設定(Stateless Address Autoconfiguration, SLAAC) 時會在網路上遷移。此文件提出了一種新的介面識別碼產失機制，該方法在使用者切換通訊介面時並不會改變通訊介面識別碼，進而不會影響到無狀態位址自動設定及使用者在網路上的位置，其最大優點是可以在不犧牲使用者隱私權的前提下讓使用者在網路上的位置可以固定。

x RFC 8781 (Discovering PREF64 in Router Advertisements, Proposed Standard RFC)：具有 DNS 擴展的 NAT64（RFC6146）網路地址轉換（DNS64）（RFC6147），是一種廣泛部署的機制，用於在純 IPv6 的網路上提供 IPv4 存取。 在各種情況下，主機必須知道網路正在使用的 NAT64 前綴。 此文件指

定在路由器建議（Router Advertisements, RA）中使用的鄰居發現（RFC4861）選項將 NAT64 前綴傳達給主機。

(3) 進行中的 Internet Drafts

i Gratuitous Neighbor Discovery: Creating Neighbor Cache Entries on First-Hop Routers (draft-ietf-6man-grand-00, Date: 2020-03-09)：IPv6 使用鄰居發現來決定和鄰居節點的鍊路位址，該文件敘述了當新的 IPv6 位址被分配到新節點上時，路由器可以主動建立鄰居的快取紀錄(Neighbor Cache entry)以降低和新節點建立連線時因鍊路尚未初始化所造成的封包遺失。

ii IPv6 Neighbor Discovery on Wireless Networks (draft-thubert-6man-ipv6-over-wireless-05, Date: 2020-03-31)：介紹了在無線網路的環境下如何進行無線鄰居發現(Wireless Neighbor Discovery, WiND)。WiND 透過將鄰居發現封包透過 Host Router 轉送來避免用無線廣播來建立連居。

iii IPv6 Source Routing for ultralow Latency (draft-foglar-ipv6-ull-routing-06, Date: 2020-01-2)：介紹了 IPv6 的階層式的定址方案，透過盡量簡化的架構加速 Source Routing 的速度。

7、 dhc - 負責如 DHCPv6 等自動網路組態設定協定之制定

(1) 工作組說明

動態主機配置工作組（Dynamic Host Configuration Working Group, DHC WG）開發了 DHCP，用於自動分配、配置和管理 IP 地址、IPv6 前綴、IP 協定堆疊和其他參數。 DHCPv4 目前是草案標準，並在 RFC 2131 和 RFC 2132 中進行了記錄。DHCPv6 目前是提議的標準，正在更新中。 dhc 計劃將 DHCPv6 協定提升到網際網路標準。

(2) 相關 RFCs

i RFC 7341 (DHCPv4-over-DHCPv6 (DHCP 4o6) Transport, Proposed Standard RFC)：描述了如何在 IPv6 的網路中動態獲取 IPv4 的設定。該方法是將 DHCPv4 的封包訊息透過 DHCPv6 傳輸，為此 dhc 制定了兩種新的 DHCPv6 訊息及兩個新的選項。

ii RFC 7653 (DHCPv6 Active Leasequery, Proposed Standard RFC)：描述了 DHCPv6 的租賃查詢，此機制可以請求者對 DHCP 伺服器發出配對資料的請求。同時 DHCPv6 也支援使用 TCP 進行連續的查詢。

iii RFC 8156 (DHCPv6 Failover Protocol, Proposed Standard RFC)：描述了 DHCPv6 的降級通訊協定。該文件也提到在同一個

broadcast domain 有兩台不同版本的 DHCP Server 可能會造成伺服器錯誤或是網路分割。

iv RFC 8415 (Dynamic Host Configuration Protocol for IPv6 (DHCPv6), Proposed Standard RFC)：介紹了用於 IPv6 的動態主機配置協議(DHCPv6)：一種用於使用網路配置參數、IP 地址和前綴配置節點的可擴展機制。可以無狀態提供參數，也可以結合一個或多個 IPv6 地址和/或 IPv6 前綴的有狀態分配來提供參數。DHCPv6 可以代替無狀態地址自動配置(SLAAC)或在其之外運行。此文件描述了 DHCPv6 的詳細規格，包含 Operational Models、Message Format, Rely, Agents...等。

v RFC 8539 (Softwire Provisioning Using DHCPv4 over DHCPv6, Proposed Standard RFC)：基於 DHCPv6 的 DHCPv4(RFC 7341)是一種動態配置 IPv4 的機制，以在純 IPv6 網路中用作上層服務。Softwire 就是這種服務的一個例子。為了使 DHCPv4 over DHCPv6（DHCP 4o6）與某些 IPv4 over IPv6 Softwire 機制和部署方案（例如 RFC 7596 或 RFC 7597）一起工作，運營商需要知道客戶端將用作 IP 地址來源的 IPv6 地址。IPv4-in-IPv6 Softwire 隧道。該地址與客戶端的 IPv4 地址以及(在某些部署中)連接阜集 ID 一起用於在運營商的 Softwire

隧道集中器中建立綁定表條目。此文件定義了一個 DHCPv6 選項，以傳達用於建立 Softwire 隧道的 IPv6 參數，以及一個 DHCPv4 選項（僅與 DHCP 4o6 一起使用），以在 DHCP 4o6 客戶端和伺服器之間傳遞來源隧道 IPv6 地址。 它旨在與 IPv4 地址分配過程結合使用。

8、 v6ops - 蒐集 IPv6 營運商和使用者所產生的問題及解決方案

(1) 工作組說明

IPv6 的全球部署正在進行中，這創造了一個由單純 IPv4、單純 IPv6、IPv4-IPv6 Dual Stack 以及 IPv6 +轉換網路的節點組成的網際網路。 必須正確處理此部署，以避免將網際網路劃分為單獨的 IPv4 和 IPv6 網絡，從而確保所有 IPv4 和 IPv6 節點的定址和連接性。IPv6 運營工作組（IPv6 Operations, 6ops）為新的和現有的 IPv6 網路部署和運營製定了指南。

(2) 相關 RFCs

i RFC 7526 (Deprecating the Anycast Prefix for 6to4 Relay Routers, Best Current Practice RFC)：經過實驗證實，RFC 3056 所提出的 6to4 的機制並不適合大量部屬且不適合網際網路的任播路由拓樸。因此，此文件要求 RFC 3068 及 RFC 6732 應該被設置為過期的狀態。

ii RFC 8215 (Local-Use IPv4/IPv6 Translation Prefix, Proposed Standard RFC)：說明 IPv6 中的前綴 64:ff9b:1::/48 應該被保留給本地的 IPv4/IPv6 轉譯使用。

iii RFC 8305 (Happy Eyeballs Version 2: Better Connectivity Using Concurrency, Proposed Standard RFC)：在現代網際網路上運作的許多通訊協定都使用主機名稱。 這些主機名稱通常解析為多個 IP 地址，每個 IP 地址可能具有不同的性能和連接特性。 由於特定的地址或地址族（IPv4 或 IPv6）在網路上可能被阻止、破壞或不理想，因此嘗試並行進行多個連接的客戶端可以更快地建立連接。 此文件指定了減少該用戶建立連線延遲的演算法要求，並提供了番理演算法，稱為「Happy Eyeballs」。

(3) 進行中的 Internet Drafts

i Neighbor Cache Entries on First-Hop Routers: Operational Considerations (draft-ietf-v6ops-nd-cache-init-01, Date: 2019-12-10)：這份文件在探討當使用鄰居快取(Neighbor Cache Entries)並且一個新的 IPv6 位址被使用時，first-hop router 上的狀態機會出問題。

9、 ipsecme - 維護及擴充前代 IPsec 工作組所制定的 IPsec 協議

(1) 工作組說明

IPsec 協議套件包括 IKEv1（RFC 2409，現已淘汰），IKEv2（RFC 7296）和 IPsec 安全體系結構（RFC 4301）。 IPsec 廣泛部署在閘道器及 VPN 遠端存取客戶端中，並作為主機到主機、主機到網路和網路到網路安全性的基礎。

IPsec 維護和擴展工作組(IPsec Maintenance and Extensions, ipsecme)繼續了 2005 年結束的早期 IPsec 工作組的工作。其目的是維護 IPsec 標準並促進對 IPsec（主要是 ESP 和 IKEv2）的澄清，改進和擴展的討論。 該工作組還作為其他在其自己的協議中使用 IPsec 的 IETF 工作組的焦點。

(2) 進行中的 Internet Drafts

i IP Traffic Flow Security (draft-ietf-ipsecme-iptfs-01, Date: 2020-03-02)：介紹了一種增進 IPsec 流量安全的機制，運作原理為使用固定大小的流量和頻率來增加流量機密性。流量分析是提取有關通過網路發送資料的信息的操作。儘管可能會通過使用加密(RFC4303)直接遮蓋資料，但流量模式本身會由於其形狀和時間的變化而暴露信息。隱藏流量的大小和頻率根據(RFC4303)被稱為流量流機密性(Traffic Flow Confidentiality, TFC)。RFC4303 透過將填充添加到加密的 IP

封包並允許傳輸所有填充封包（使用協議 59 表示）來提供 TFC。這種方法的主要局限性在於它可能會嚴重利用可用頻寬。IP-TFS 解決方案提供了完整的 TFC，而沒有上述頻寬限制。為此，我們使用具有固定大小的封裝封包的恆定發送速率 IPsec (RFC4303)隧道。但是，這些固定大小的封包可以包含部分、整個或多個 IP 數據包，以最大化隧道的頻寬。另外，IP-TFS 提供了處理網絡擁塞的功能(RFC2914)。當 IP-TFS 使用者無法完全控制 IP-TFS 隧道路徑流經的網路領域時，這非常重要。