

科技部

107年度大專學生研究計畫申請書

一、綜合資料：

申請條碼：107CFA0200019



申請人 【學生】	姓 名	林資超	身分證號碼	F12947****
	就 讀 學 校、 科 系 及 年 級	國立政治大學資訊科學系 3 年級	電 話	0222477779
	學 生 研 究 計 畫 名 稱	基於ICMPv6設計輕量化的家庭網路隨插即用服務管理機制		
	研 究 期 間	自107年7月1日至108年2月底止，計8個月		
	計 畫 歸 屬 司 別	工程司		
	研究學門代碼及名稱	E4002 -- 程式語言與軟體工程		
	上年度曾執行本部大專學生研究計畫	否		
指導教授	姓 名	廖峻鋒	身分證號碼	F12386****
	服 務 機 構 及 科 系(所)	國立政治大學資訊科學系		
	職 稱	助理教授	電 話	0229393091#88103
補助經費	每位學生每月6,000元研究助學金，研究期間為8個月，共計48,000元			

表C801

二、研究計畫內容：

(一)摘要

隨著科技進步，智慧家庭核心技術已日漸成熟。智慧家庭藉由整合各種感測器 (sensor)、致動器 (actuator) 及軟體形成智慧家庭服務。不過，智慧家庭擁有許多不同的通訊協定，為處理不同裝置間的通訊與服務管理問題，便有廠商與組織共同制定 UPnP (Universal Plug and Play) 協定，UPnP 是由幾項重要的子協定構成，其中服務發現 (Service Discovery) 和存在性管理 (Presence Management) 更是支援智慧家庭環境服務高度動態特性的重要技術。然而，近年來隨著物聯網技術與服務興起，小型行動裝置和嵌入式裝置數量日益增加，讓 IP 位址枯竭問題雪上加霜，為解決位址短缺，IPv6 (Internet Protocol version 6) 對智慧家庭的通訊協定是必要的趨勢，而且近年來大部份網路與嵌入設備均納入 IPv6 支援。IPv6 除了擴大定址空間外，在設計上也新增功能來改良 IPv4 效率問題。UPnP 在規格書附錄中加入對 IPv6 的支援，可惜的是其設計主要著重相容性，並未本質上善用 IPv6 的特色。本研究希望基於 IPv6 對網際網路控制訊息協定 ICMP (Internet Control Message Protocol) 與群播 (Multicast) 的改進，設計一個新協定讓 UPnP 的服務發現協定 SSDP (Simple Service Discovery Protocol) 能夠更有效率的傳輸，並建構一個網路層工具來支援相關訊息於網路層直接傳輸。希望藉由此協定與工具的建構，使 UPnP 的服務發現機制有更好的效能，讓使用者享受更便利的智慧家庭服務。

(二)研究動機與研究問題

科技日新月異，行動裝置與網際網路技術不斷推陳出新，同時也提供更多便利的服務。其中，智慧家庭 (Smart Home) 可說是對一般民眾最容易觸及的一種智慧生活空間。智慧生活空間系統通常需要「服務管理」，用來處理不同裝置、軟體的偵測、發現、資料傳送及組合等問題。基於此一需求，許多廠商與組織共同制定了 UPnP (Universal Plug and Play) 服務管理機制。UPnP 基於服務發現協定 SSDP (Simple Service Discovery Protocol) 是少數不需要特定服務目錄 (Service Registry) 伺服的分散式協定，由於不需要另外維護伺服器，因而降低維護成本。此外，UPnP 也不仰賴特定的平台、作業系統或程式語言。讓 UPnP 在智慧家庭應用中，享有許多優勢。

然而，根據估計在 2020 年時，物聯網相關裝置將會超過 300 億台。在裝置數量急遽成長的情況下，加上網際網路通訊協定第四版 IPv4 (Internet Protocol version 4) 可使用的位址又將完全用盡。網際網路工程任務組 IETF (Internet Engineering Task Force) 便著手規劃下一代的協定，網際網路通訊協定第六版 IPv6 (Internet Protocol version 6) 的誕生便是為了解決這個問題。在物聯網環境中，因為裝置數量的爆炸成長，與 IPv6 低功率無線個人區域網路 6LowPAN (IPv6 over Low-Power Wireless Personal Area Networks) 擁有低功率 IP 節點與大型網狀網路等特性，可以在 IEEE 802.15.4 定義的連接層架構中，快速傳輸 IPv6 封包，是物聯網發展的重要趨勢，所以物聯網裝置支援 IPv6 有其必要性。為因應此趨勢，UPnP Forum (現

為 Open Connectivity Foundation，OCF）也在原有 UPnP 規格書的附錄加入對 IPv6 的支援。很可惜的是，目前 UPnP 對 IPv6 的支援主要著重在位址的相容性，並沒有善用 IPv6 相對於 IPv4 在設計理念上的躍進。事實上，IPv6 除了定址空間變大外，針對網路層的管理協定 ICMP（Internet Control Message Protocol）與群播（Multicast）機制都做了大幅的強化與修改。我們知道，目前 UPnP 的服務管理主要依賴 IP 群播與在其上運作的 SSDP。因此，本計畫主要感興趣的問題是：是否有可能讓 UPnP 的服務管理機制更加善用 IPv6 在 ICMP 與 IP 群播所做的改進呢？接下來我們更深入一層，針對這個問題詳加說明。

根據 OCF 在文件中的闡述，UPnP 的裝置主要分為兩類：device 與 control point，device 代表提供服務的裝置，例如一台印表機提供列印的服務，一台電視提供影像串流的服務；control point 則是指可以用來控制在 UPnP 網路中的 device 的裝置，其中，control point 可以取得 device 的描述與相關服務列表，並傳送動作訊息來控制 device 的服務。在 IPv6 的支援上，device 與 control point 一般都會利用 EUI-64 方法來參照 MAC 位址產生 IPv6 位址，並搭配鄰居發現協定 ND/NDP（Neighbor Discovery Protocol）來確定位址的唯一性，相較於 IPv4 上使用動態主機設定協定 DHCP（Dynamic Host Configuration Protocol），ND 不需要任何集中管理的伺服器，讓定址（Addressing）階段得以被簡化。在發現（Discovery）階段，control point 和 device 加入網路時，都會向 UPnP 規範的群播位址分別發送 SSDP 訊息，之後再經過傳輸層 User Datagram Protocol（UDP），與實現在 UDP 上的 Hypertext Transfer Protocol（HTTP）：HTTPMU/HTTPU（圖 1），HTTPMU 為 control point 利用群播搜尋感興趣的服務，與 device 通知 control point 自身的服務，HTTPU 則是 device 利用單播（Unicast）來回應 control point 的搜尋請求。然而，從以上兩階段可以發現幾項事實，例如：

- 因為有 ND 的機制，IPv6 在定址上不需要額外的伺服器，相對於 IPv4 定址上容易。
- 必須在應用層制定相關的協定，才能達到 SSDP 的功能，並沒有善用 ICMP 的改進，讓協定實現上有疊床架屋之感。

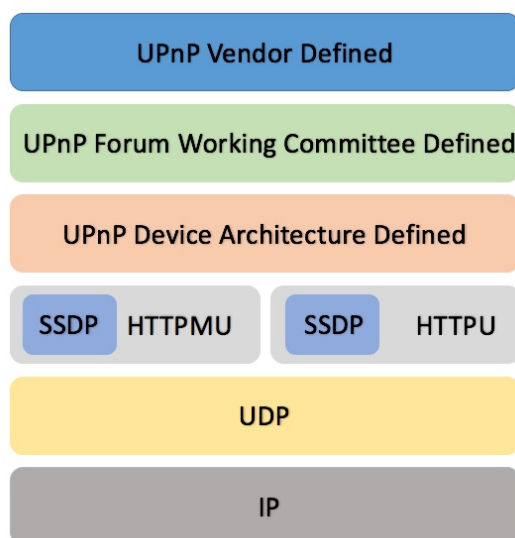


圖 1：SSDP 的協定堆疊。

觀察 IPv6 在網路層做的改進，網際網路控制訊息協定第六版 ICMPv6（Internet Control Message Protocol version 6）在 RFC 4443 被規範其基本協定必須被所有 IPv6 節點所完整支援，

主要目的是用來了解網路封包或是分析路由的情況，例如：ping、traceroute。ICMPv6 的訊息可以依照內容分成：錯誤訊息、資料訊息。決定 ICMPv6 封包為錯誤訊息或資料訊息則取決於標頭的 Type，Type 0 到 127 為錯誤訊息，128 到 255 為資料訊息，其中資料訊息有數個 Type 尚未被定義，可以被定義為具有特殊意義的訊息。IPv6 的 ND 則利用 ICMPv6 的訊息結構，並定義新的 ICMPv6 Type 為 133 到 137（圖 2），各自對應一種 ND 訊息：路由器請求（Router Solicitation）、路由器通告（Router Advertisement）、鄰居請求（Neighbor Solicitation）、鄰居通告（Neighbor Advertisement）、重新導向（Redirect）。其中，IPv6 裝置會向請求節點群播位址（Solicited-Node Multicast Address，註：將自身 IPv6 位址以 ff02::1:ff00:0/104 為前綴所形成的群播位址）發出鄰居請求訊息，用來做重複位址偵測（Duplicate Address Detection），以確定位址的唯一性。此外，IPv6 還透過 ND 達到了 IPv4 的位址解析協定 ARP（Address Resolution Protocol）、ICMPv4 路由器發現（Router Discovery）和路由器重新導向（Router Redirect），並在各方面做了改進來增進封包傳遞過程的強健性（Robustness）。以 ND 對 ICMP 與 IP 群播做的延伸為基礎，我們希望仿效相同的精神，對 SSDP 進行修改，以 ICMPv6 自定義 Type 封包來傳送 UPnP 發現階段的 SSDP 訊息，在網路層中就能實現 SSDP 原有的功能，不需要在應用層上額外制定一個服務發現協定。

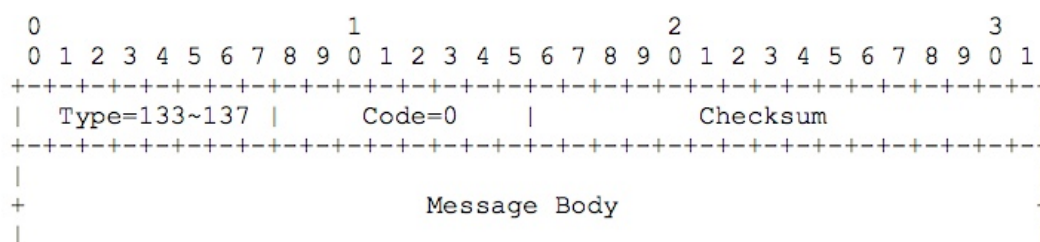


圖 2：以 ICMPv6 為封包為基礎的 Neighbor Discovery 訊息。

本計畫期望以 ND 機制和 ICMPv6 為基礎，讓 UPnP 中 control point 與 device 的 SSDP 訊息能夠直接基於 IPv6 網路層上傳送，並減少網路傳輸成本（overhead）。此外，我們也預期此方法能夠被佈署到 6LowPAN 上，進而提升物聯網與智慧家庭未來的發展。

（三）文獻回顧與探討

UPnP 全名是 Universal Plug and Play，是由前身為 UPnP Forum 的 OCF 發表與推行的一個通訊協定，目的是為了做到隨插即用（Plug and Play）也就是使網域中的所有裝置溝通更為方便並且能夠簡化相關的設定。UPnP 的基本元件有 device、service 與 control point，此外，還有使用許多標準協定如 HTTPU/HTTPMU、SSDP、GENA、SOAP、TCP...等。隨著 UPnP 的普及，與其相關的研究也越來越多，如針對 UPnP 安全性去做改善（Rajkumar & Nair, 2013）不只提供多用戶驗證 UPnP 服務還提供一個無縫的安全協定，以及實作基於不同 IP 協定的 UPnP 裝置達到溝通和互操作性的橋接（Li et al., 2008）。

除了研究 UPnP 外還需了解 IPv6，IPv6 是由 IETF 於 1990 年代開始規劃，希望能解決 IPv4 位址匱乏的問題，並對一些不足的地方進行改進，如路由規則和自動組態方面。相對

於 IPv4，IPv6 有以下優點與特色：簡化的標頭和彈性擴充、即插即用的連線方式、網路層的認證與加密、對移動通訊更好的支援。其中，對 ICMP 改進的 ICMPv6 極其重要，利用 ICMPv6 的訊息格式建立許多機制，例如定義於 RFC 4861 的 ND，用於位址自動組態（Address Autoconfiguration）、位址解析（Address resolution）與重複位址偵測（Duplicate Address Detection）等功能。ND 也有不少相關的研究，如 ND 是假設網域內節點互相信任的基礎上，而易受分散式阻斷服務攻擊 DDoS（Distributed Denial-of-Service attack），因此 Zhang、Wang（2016）針對 ND 的安全性進行分析與建議，還有基於 ND 訊息交換的過程在 6LowPAN 架構中進行位址配置的方法（Luo et al., 2015）。

然而，研讀以上之相關文獻，我們發現 UPnP 的服務發現協定未善用 IPv6 做的改進，讓實現上仍需要其他協定的支援補充。因此，本計劃透過規劃一個初步協定，能夠讓服務發現協定的訊息內容以 ICMPv6 的訊息格式進行傳送，並在網路層上直接進行傳輸，避免冗餘繁複的協定實現造成裝置負擔與網路傳輸上的成本。此外，IPv6 相較於 IPv4 做了相當多功能改進，尤其是要求 ICMPv6 的完善支援，在目前，市面上大部分的網通產品都已經支援 IPv6，所以我們的方法應具有一定的可行性與可普及性。

(四)研究方法及步驟

本計畫主要目的是基於 IPv6 對 ICMPv6 的改進，並希望藉由 ICMPv6 的機制就能完全實現 SSDP 的原有功能，讓 UPnP 的服務管理機制更加善用於 IPv6 上。本計畫具體研究步驟如下：

- 研讀相關文獻
- 問題分析
- 解決方案設計
- 實作與驗證

以下各節分別詳述各步驟的進行方式。

1. 研讀相關文獻

在這個階段中，我們將研讀相關技術以了解 UPnP 及 ICMPv6 的相關概念。為了利用 ICMPv6 達到 UPnP 服務發現的功能，必須先了解 UPnP 機制運作的主要運作層級，如圖 3 為例由低至高分別為：



圖 3：UPnP 運作層級。

- 定址 (Addressing)：當一個 device 加入一個網路中會獲得一個可以和其它 device 通信的網路地址。
- 發現 (Discovery)：control point 尋找網路上提供服務的 device，device 也宣告本身的存在。
- 描述 (Description)：device 使用可延伸標記式語言 XML (eXtensible Markup Language) 來概述它的服務和能力。
- 控制 (Control)：control point 發送動作請求給 device。
- 事件 (Eventing)：當 device 的服務內部狀態改變時會通知註冊的 control point。
- 呈現 (Presentation)：device 可選擇提供一個基於 HTML 的管理介面，允許直接的操作和監控 device 的狀態。

聚焦於發現 (Discovery) 階段，為 UPnP 進行服務管理的主軸，使用簡單服務發現協定 SSDP 來搜尋並管理服務。SSDP 不需要任何組態和管理，被設計用來基於 HTTPMU/HTTPU 在一個網域中簡單的服務發現解決方案。SSDP 有存在性管理 (Presence Management) 和服務搜尋 (Search) 兩種機制。其中存在性管理指的是在一個 UPnP 的 device 加入或離開網域時，會使用 NOTIFY 方法對群播位址分別發出「ssdp:alive」與「ssdp:byebye」訊息，來對整個網域的 control point 發出通知。而服務搜尋是 control point 會使用 M-SEARCH 方法對群播位址發出「ssdp:discover」訊息，對有興趣的裝置類型發出搜尋通知，如果有符合的 device 存在，就會直接以單播回應發出請求的 control point。

在 ICMPv6 方面，相關技術被定義在 RFC 4443，主要用於網路節點之間傳遞控制訊息、錯誤報告、狀態訊息等。作為組成 IPv6 體系的一員，RFC 4443 也清楚的說明 ICMPv6 的訊息格式 (圖 4) 與動作必須完整地由 IPv6 節點實現。其中，ICMPv6 封包標頭具有下列欄位：

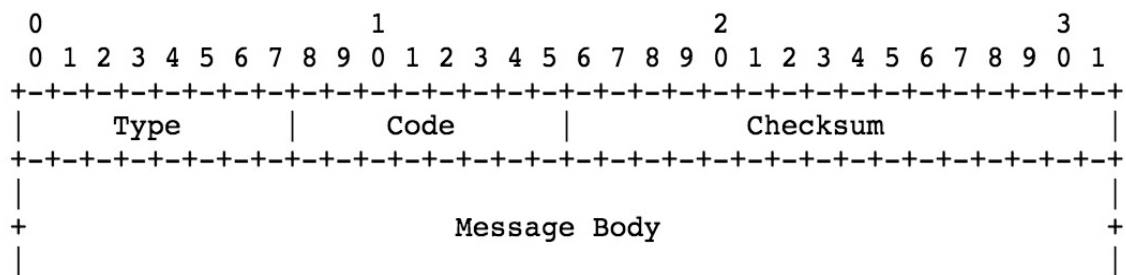


圖 4：ICMPv6 訊息格式。

- 類型 (Type)：用來區分不同類型的訊息，對訊息的內容做了初步的分類，同時決定了剩餘欄位的格式，其中 Type 200 與 201 為實驗類型，不被定義主要用途。
- 代碼 (Code)：根據訊息的內容對相同類型的訊息做更進一步的細分。
- 校驗和 (Checksum)：檢驗 ICMPv6 訊息的資料正確性。
- 訊息本體 (Message Body)：根據類型與代碼，決定訊息本體所攜帶的資料與大小。在大小上，ICMPv6 封包不應該超過 IPv6 封包的最大傳輸單位 MTU (Maximum Transmission Unit) 為 1280 bytes。

2. 問題分析

在此一階段，我們將基於 UPnP 服務模型，分析 ICMPv6 實現 UPnP 服務發現的困難與問題。根據目前初步研討，我們發現，基於 ICMPv6 實現 SSDP 主要會面臨兩個議題。首先，UPnP 在發現階段使用 NOTIFY 與 M-SEARCH 方法傳送的 SSDP 訊息，儘管可以利用 ICMPv6 的類型與代碼將兩種方法的訊息做初步區分，但 SSDP 訊息仍有許多標頭無法被表示（圖 5 與圖 6）。

```
▼ Simple Service Discovery Protocol
  ► NOTIFY * HTTP/1.1\r\n
    Host: [FF02::C]:1900\r\n
    NT: urn:microsoft-com:service:LnvConnectService:1\r\n
    NTS: ssdp:alive\r\n
    Location: http://[fe80::12:981a:57e2:304a]:2869/upnphost/udhisapi.dll?content=uuid:1217e3d3-f544-42eb-bb1d-c846acd4d4fb\r\n
    USN: uuid:1217e3d3-f544-42eb-bb1d-c846acd4d4fb::urn:microsoft-com:service:LnvConnectService:1\r\n
    Cache-Control: max-age=3200\r\n
    Server: Microsoft-Windows/10.0 UPnP/1.0 UPnP-Device-Host/1.0\r\n
    OPT:"http://schemas.upnp.org/upnp/1/0/"; ns=01\r\n
    01-NLS: 4c5bb815f5ece8c3501900644e1a81eb\r\n
    \r\n
    [Full request URI: http://[FF02::C]:1900*]
```

圖 5：ssdp:alive 訊息封包。

```
▼ Simple Service Discovery Protocol
  ► M-SEARCH * HTTP/1.1\r\n
    Host: [FF02::C]:1900\r\n
    ST:urn:Microsoft Windows Peer Name Resolution Protocol: V4:IPv6:LinkLocal\r\n
    Man:"ssdp:discover"\r\n
    MX:3\r\n
    \r\n
    [Full request URI: http://[FF02::C]:1900*]
    [HTTP request 1/124]
    [Next request in frame: 41]
```

圖 6：ssdp:discover 訊息封包。

一個可行的方法是將剩餘標頭置於 ICMPv6 訊息本體。然而，在此卻延伸另一個問題：因為過去並沒有將 SSDP 訊息以 ICMPv6 為基礎傳送的相關協定，故接收端裝置無法解讀訊息本體的意義為何。例如圖 7 是使用 Wireshark 封包分析器初步進行的簡單實驗，由圖中可見，由於 Type 200 沒有相關協定定義，因此訊息本體只會被視為十六進位的資料。

```
▼ Internet Control Message Protocol v6
  Type: Private experimentation (200)
  Code: 0
  Checksum: 0xf8a3 [correct]
  [Checksum Status: Good]
  ► [Expert Info (Note/Undecoded): Dissector for ICMPv6 Type (200) code not implemented, Contact Wireshark developers if you want this supported]
  Data: 00010a096162636465666768696a6b6c6d6e6f7071727374...
```

圖 7：ICMPv6 Type 200 封包。

另一個問題是，常見的 ICMPv6 工具，例如：ping、traceroute，並沒有提供使用者任意修改訊息本體的功能。但訊息本體的內容與類型和代碼關係密不可分，以 ping 與 ND 的 ICMPv6 訊息格式為例，ping 在 ICMPv6 的訊息本體為一隨意的字串，然而，ND 的鄰居請求、鄰居通告的訊息本體有部分是記錄目標的 IPv6 位址。明顯地，現有的 ICMPv6 工具勢必無法滿足預期的效果。

3. 解決方案設計

針對上述問題，本計畫初步構想了一個解決方案，主要可分為兩個部分。第一部分先對 SSDP 訊息以 ICMPv6 類型與代碼進行分類（圖 8），根據 UPnP 規格書，在發現階段主要會有五種 SSDP 訊息：「ssdp:discover」、「discover response」、「ssdp:alive」、「ssdp:byebye」、「ssdp:update」。

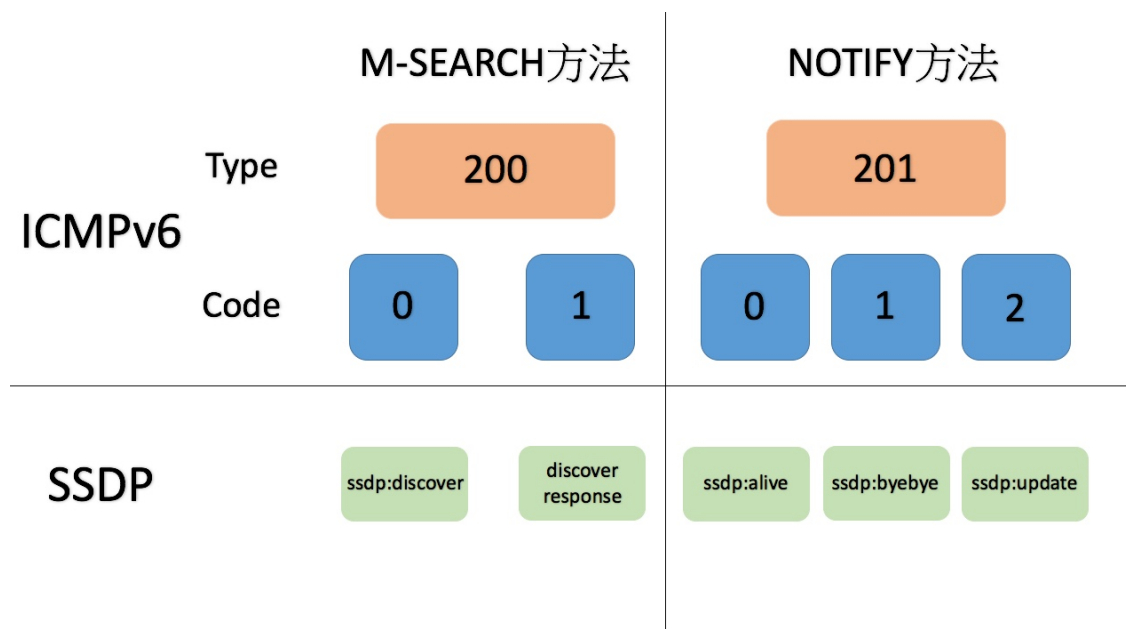


圖 8：SSDP 訊息初步分類。

這五種訊息的標頭格式不盡相同，但 ICMPv6 的訊息本體可以因為不同的類型與代碼而讓大小不同，所以我們將其他標頭資訊置於 ICMPv6 的訊息本體進行傳輸。同時，為了解決裝置解析訊息本體的問題，我們以 Wireshark 軟體作為封包解析的工具，Wireshark 允許使用者利用 Lua 或 C 語言編寫自製化的協定解析器（Dissector），如圖 9 為尚未使用協定解析器的一個基於 TCP 與 IPv4 的封包，透過協定解析器，能夠將「Data」解析為自製的協定（圖 10）。因此，本計畫也希望制定 SSDP 基於 ICMPv6 的初步協定規格，並以協定解析器協助觀察訊息的傳遞。

```
▶ Frame 2: 4134 bytes on wire (33072 bits), 4134 bytes captured (33072 bits) on interface 0
Raw packet data
▶ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▶ Transmission Control Protocol, Src Port: 56261, Dst Port: 2620, Seq: 3, Ack: 1, Len: 4094
▼ Data (4094 bytes)
  Data: 00403c000000180000104000000000000000000000021800000000b...
  [Length: 4094]
```

圖 9：自訂協定的封包。

本計畫預期進行的第二項工作是設計新的 SSDP/ICMPv6 操作的 Testbed 工具。功能上，會向特定的群播位址發送訊息，訊息會以上述五種基於 ICMPv6 的 SSDP 訊息為主，並在訊息主體紀錄標頭相關的資訊。透過 raw socket 機制，允許開發人員在寫作程式在 IP 層以下傳送與接收網路層封包（如圖 11）。因此，可以預期本計畫所發展的服務管理協定在效能應能優於原有的 SSDP，並減少網域傳輸成本。


```

▶ Frame 2: 4134 bytes on wire (33072 bits), 4134 bytes captured (33072 bits)
Raw packet data
▶ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▶ Transmission Control Protocol, Src Port: 56261, Dst Port: 2620, Seq: 3, Ack: 1, Len: 4094
▶ [2 Reassembled TCP Segments (4096 bytes): #1(2), #2(4094)]
▼ FPM Header
  Version: 1
  Type: NETLINK (1)
  Length: 64
▼ Linux netlink (cooked header)
  Link-layer address type: Netlink (824)
  Family: Route (0x0000)
▼ Linux rtnetlink (route netlink) protocol
  ▶ Netlink message header (type: Add network route)
    Address family: AF_INET (2)
    Length of destination: 24
    Length of source: 0
    TOS filter: 0x00
    Routing table ID: 0
    Routing protocol: Zebra (0x0b)
    Route origin: global route (0x00)
    Route type: Gateway or direct route (0x01)
    Route flags: 0x00000000
  ▶ Attribute: Route destination address
  ▶ Attribute: RTA_PRIORITY

```

圖 10：透過協定解析器觀察的自訂協定封包。

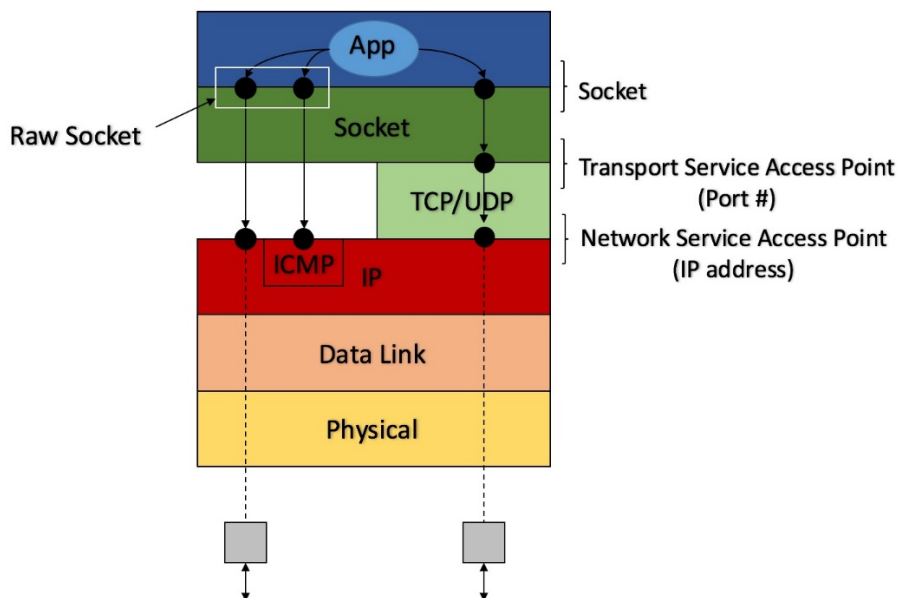


圖 11：raw socket 的協定堆疊。

4. 實作與驗證

為了驗證本計畫提出的設計是否能夠減輕傳輸的成本，且效能上優於原有的 SSDP 機制，我們設計了下列實驗。如圖 12，將原先就具有傳送原有 SSDP 封包能力的裝置作為 control point，而 Raspberry Pi 作為環境中的 device，control point 與 device 都將佈署我們設計的 ICMPv6 工具。此外，為了驗證 device 解析封包標頭的正确性，我們將在 control point 與 device 均安裝 Wireshark 與自製的協定解析器，觀察封包是否有被正确解析。接著 control point 將分別發送兩種 M-SEARCH 封包：原有的 SSDP、基於 ICMPv6 的 SSDP 封包，再透過撰寫程式碼來紀錄 control point 發送 M-SEARCH 封包的時間、device 接收封包的時間、device 解析封包的時間、device 發送 response 封包的時間與 control point 接收 response 封包的時間。

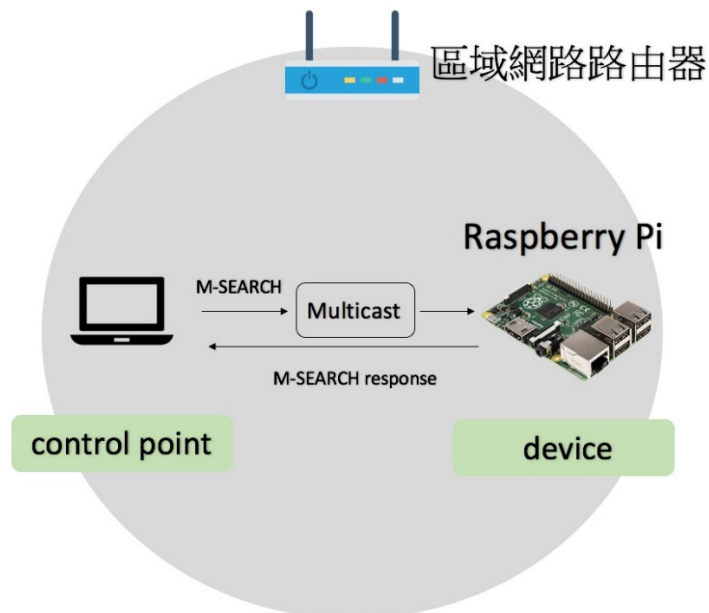


圖 12：實作簡易架構。

Step1：將 control point 與 device 佈署我們設計的 ICMPv6 工具。

Step2：讓作為 control point 的裝置與 Raspberry Pi 都使用同一個區域網路。

Step3：control point 與 device 基於 ND 機制取得 IPv6 位址。

Step4：control point 分別發送兩種 SSDP 封包。

Step5：以程式紀錄封包相關時間數據。

Step6：以 Wireshark 觀察封包是否正確解析。

(五)預期結果

本計畫預期發展的基於 ICMPv6 的 UPnP 簡單服務發現協定的運作方式如圖 13 所示。control point 與 device 事先佈署我們的 ICMPv6 工具，並在 ND 機制下取得位址後，control point 可以透過 M-SEARCH 方法搜尋網域內提供的服務，device 可以透過 NOTIFY 方法向網域內的裝置宣告自身的服務，由此達到 UPnP 中發現階段的 SSDP 原有功能。由於基於 ICMPv6 的 SSDP 不需要透過傳輸層，預期執行效率上能比原先 SSDP 高。

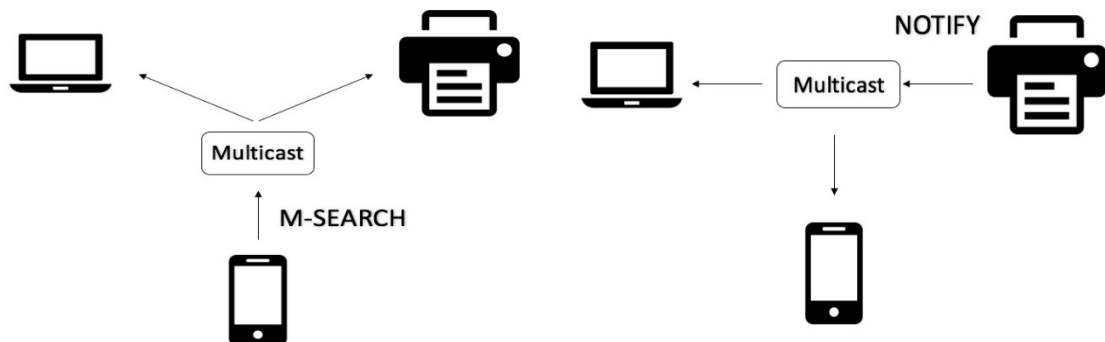


圖 13：預期基於 ICMPv6 的 SSDP 運作方式。

(六)參考文獻

- (1) Rajkumar, P. P., & Nair, A. A. (2013, July). A UPnP extension for multilevel security in pervasive systems. In *Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on* (pp. 1-9). IEEE.
- (2) Li, C. S., Huang, Y. M., & Chao, H. C. (2008). UPnP IPv4/IPv6 bridge for home networking environment. *IEEE Transactions on Consumer Electronics*, 54(4).
- (3) Zhang, T., & Wang, Z. (2016, October). Research on IPv6 Neighbor Discovery Protocol (NDP) security. In *Computer and Communications (ICCC), 2016 2nd IEEE International Conference on* (pp. 2032-2035). IEEE.
- (4) Luo, B., Tang, S., & Sun, Z. (2015, August). Research of neighbor discovery for IPv6 over low-power wireless personal area networks. In *Heterogeneous Networking for Quality, Reliability, Security and Robustness (QSHINE), 2015 11th International Conference on* (pp. 233-238). IEEE.
- (5) Edwards, W. K. (2006). Discovery systems in ubiquitous computing. *IEEE Pervasive Computing*, 5(2), 70-77.
- (6) Park, K. L., Yoon, U. H., & Kim, S. D. (2009). Personalized service discovery in ubiquitous computing environments. *IEEE Pervasive Computing*, 8(1).
- (7) Universal Plug and Play (UPnP) , <https://openconnectivity.org/>
- (8) Internet Control Message Protocol Version 6 (ICMPv6) , <https://tools.ietf.org/html/rfc4443>
- (9) Neighbor Discovery Protocol (ND) , <https://tools.ietf.org/html/rfc4861>
- (10) Simple Service Discovery Protocol (SSDP) , <https://tools.ietf.org/html/draft-cai-ssdp-v1-03>

(七)需要指導教授指導內容

由於本計畫主要的研究領域為智慧家庭，因此我選擇專長為智慧家庭的指導教授廖峻鋒老師，此外，老師在智慧家庭的服務管理機制，尤其是 UPnP 有不少專門著作。若能在這方面受到老師的專業知識指導，想必會讓實作這項計劃更加順利。由於本計畫聚焦於 UPnP 的簡單服務發現協定，並以 ND 機制為基礎，希望定義一套初步協定讓簡單服務發現協定訊息能基於 ICMPv6 的訊息格式，並在網路層直接進行傳輸，主要希望能在老師的指導下，熟習與研讀 UPnP 和 ICMPv6 的相關協定與規範，也需要老師指導建置出以 raw socket 的方式在網路層傳遞訊息的工具。本研究計畫的指導方式為每週固定 meeting 一次，每次 meeting 都會向老師報告目前進度且提出遇到的問題，老師會協助探討問題的本質和推薦閱讀相關文獻來補充相關知識，並提供研究方向的建議。閱讀相關書籍和文獻時，我也會製作簡報或心得向老師報告閱讀內容。相信在老師的專業知識和建議之下，能夠幫助我完成研究的目標。

大專學生研究計畫指導教授初評意見表

一、學生潛力評估：

申請人是本系前 3 名的頂尖學生，本人亦擔任過其二門必修課的授課教師，其在實作與理論上均展現了相當的潛力。本次主題選定基於 IPv6 網路帶來的新機制(ICMPv6 中的 Node discovery 與 Node solicitation)，對於智慧家庭中服務管理機制的改良。相關標準與規格繁多，且較為低階，必須在有限時間中閱讀包含 IPv6、ICMPv6 與 UPnP 等規格書，並設計出基本的解決方案，課業繁重之餘，能在極短時間內，花時間理解，並設計出可行的解決方案，實屬不易，且該生文筆表達能力佳，能夠依照給予的寫作大綱寫出相當流暢的文章，並清楚以例子表達理論。該生已對於要提出的研究規劃了十分具體的構想，具有良好之研究潛力。

二、對學生所提研究計畫內容之評述：

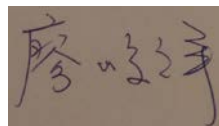
智慧家庭技術已從原型建置階段漸漸進入了實用佈署階段，然而，目前在這方面還有許多挑戰待克服。本計畫的核心理念是著眼於目前 IPv6 的使用與裝置支援已經非常普及，加上如 6LowPAN 等基於 IPv6 的物聯網應用快速成長，運用 IPv6 上的新機制來改善現有服務發現協定的想法已具有實用價值。本計畫提出新穎的概念，基於 IPv6 中 ICMPv6 的特性，改善 UPnP/SSDP 原本以群播為基礎的服務管理協定。計畫主軸是由該生獨立構思完成，本人只進行初期方向的指引與最後的修改。從繳交的計畫書中，該生已對於要提出的研究規劃了一個十分具體的構想，並佐以實際範例與預期結果，規畫十分完整，將來計畫未來完成度預期應該會相當高。同時，計畫內容的完成，也將對產業有所貢獻，相當有潛力且令人期待的計畫。

三、指導方式：

預期每周進行一小時進度討論，討論內容包含 IPv6 與 ICMPv6 規格的技術研討。網路封包的監測與模擬工具訓練、隨插即用服務管理機制的設計架構與如何透過 Raw Socket 實現以 ICMPv6 進行服務管理的構想與實驗。對於較即時、單純的技術或實作問題，會請同學加入實驗室的 FB 社團，在線上透過實驗室學長姐或老師立即回覆，可快速得到解答。最後，在具備具體研究成果後，將其整理發表至國內或國際研討會。

四、本人同意指導學生瞭解並遵照學術倫理規範；本計畫無違反學術倫理。

指導教授簽名：



107 年 2 月 14 日

國立政治大學學生學業成績總表

學號：104703042 姓名：林資超		生日：85/02/16 性別：男		雙主修： 輔系：		106 學年度 (106 年 09 月至 107 年 06 月) 資訊科學系三年級		105 學年度 (105 年 09 月至 106 年 06 月) 資訊科學系二年級		104 學年度 (104 年 09 月至 105 年 06 月) 資訊科學系一年級	
科	目	第一學期 學分	第二學期 學分	第一學期 學分	第二學期 學分	科	目	第一學期 學分	第二學期 學分	第一學期 學分	第二學期 學分
體育[男]	一棒球初級	0.0	75.00	軟體應用導論	3.0	89.00	體育[男女合班]	桌球初級	0.0	IP	IP
國文	一古典詩選讀	2.0	85.00	資料處理	3.0	98.00	電影與國際關係	2.0	90.00	3.0	IP
國文	一中國思想名作選讀	2.0	89.00	體育[男女合班]	0.0	64.00	藥物使用與生活的關係	2.0	92.00	2.0	IP
大學英文	(一)	2.0	90.00	全民國防教育軍事訓練—防衛動員	3.0	92.00	預防醫學與校園健康	3.0	99.00	3.0	IP
大學英文	(二)	2.0	95.00	藝術欣賞與創作	3.0	87.00	作業系統	3.0	97.00	3.0	IP
阿拉伯民族概況		2.0	88.00	數學—邏輯與人生	3.0	79.00	資料庫系統	3.0	97.00	3.0	IP
媒體素養		3.0	78.00	服務學習課程—資訊技術支援志工服務	0.0	P	軟體工程概論	3.0	95.00	3.0	IP
服務學習課程—資訊技術支援志工服務		0.0	P	遊戲數學	3.0	99.00	資訊專題(A)	3.0	95.00	3.0	IP
認識神經疾病		2.0	95.60	物件導向程式設計	3.0	97.00	無線通訊導論	3.0	96.55	3.0	IP
微積分		3.0	89.55	系統式	3.0	97.00	數位金融實務運用	3.0	85.00	3.0	IP
線性代數		3.0	99.00	數位系統實驗	3.0	92.00	3D遊戲程式設計	3.0	95.00	3.0	IP
計算機概論		3.0	92.00	機率論	3.0	87.00	[以下空白]				
普通物理學(一)		3.0	96.00	計算機結構與組網	3.0	92.00					
普通物理學實驗(一)		0.0	89.00	演算法	3.0	87.00					
計算機程式設計(一)		3.0	100.00	程式語言能力檢定	3.0	99.00					
計算機程式設計(二)		3.0	95.00	Java 程式設計	0.0	P					
[以下空白]				網路與通訊概論	3.0	99.00					
				物件導向程式設計實習	3.0	92.00					
				[以下空白]	0.0	96.00					
學期平均成績		91.71	93.46	學期平均成績	91.50	92.91	學期平均成績	94.13	17.0	17.0	學期平均成績
修習學分		21.0	15.0	修習學分	24.0	23.0	修習學分	20.0	0.0	0.0	修習學分
實得學分		21.0	15.0	實得學分	24.0	23.0	實得學分	20.0	0.0	0.0	實得學分
學業成績		21.0	36.0	學業成績	60.0	83.0	學業成績	103.0	103.0	103.0	學業成績
總成績		85.00	85.00	總成績	85.00	85.00	總成績	92.66	92.66	92.66	總成績

附註



學分數：—— 總成績：——

學業成績：——

列印日期：2018/02/12

[全一頁]

國立政治大學學生成績排名證明書

學生姓名	林資超	性 別	男	出生日期	85 年 02 月 16 日
		身份別	本系生		
學 號	104703042	系(組)別 年 級	資訊科學系三年級		

學 年	學 期	系 級	平均 成績 (學分數)	班排名	百分比	系排名	百分比	備註
104/1		資科一	91.71(21.00)	2/46	4%	2/46	4%	
104/2		資科一	93.46(15.00)	2/46	4%	2/46	4%	
105/1		資科二	91.50(24.00)	2/45	4%	2/45	4%	
105/2		資科二	92.91(23.00)	2/45	4%	2/45	4%	

系 級	加權 平均成績	總學 分數	班排名	百分比	系排名	百分比	備註
在校： 資科二	92.30(83)		2/45	4%	2/45	4%	

- 計算「加權平均成績」及「平均成績」之學分數不含科目成績以「通過／不通過」方式評定之學分
- 本證明書影印、塗改無效

核發日期： 107 年 02 月 12 日

核發單位：國立政治大學教務處註冊組

