Service Location Survey

曾則勤
中華大學資訊工程學系
m09502015@chu.edu.tw

陳旻秀
中華大學資訊工程學系
mxchen@chu.edu.tw

摘要

Service Location 可以提供使用者所需要的服務，以完成特定的工作。隨著網際網路、數位家庭網路快速發展的情形下，使用者所需要使用的服務也漸漸變多，因此就有了許多 Service Location 的協定來幫助使用者尋找、發現各式各樣存在於網路中的服務，這些協定分別為 Service Location Protocol、Juxtapose、Universal Plug and Play、Lightweight Directory Access Protocol、和 Naming Authority Pointer。而本篇論文將介紹這些協定所使用的各種元件、功能以及技術，以提供日後在針對 Service Location 協定的議題上，有更深一層的認知、了解，使得在不同的網路環境下，選擇合適的協定來操作使用。

關鍵詞：Service Location、網際網路、數位家庭網路

一 序論

Service Location，顧名思義就是指服務的位置。所謂的服務，在此定義為能在網路上使用的服務資源，供應人們完成各式各樣不同種類的工作，像是 PC 提供線上觀看影片、線上英漢字典、網路印表機、代理伺服器等等。而在網路上要提供服務的裝置，必須至少要有一個位置，也就是 IP address 或是 hostname，用來做為資料的傳遞時，有明確的來源以及目的地位置，而能進行封包繞送的動作，讓其他人使用此服務。然而在傳統上，使用者在網路上想要使用某些服務時，必須要事先知道這些服務的網路位址，隨著目前家用網路逐漸興起，在任何家電產品以及多媒體設備都需要上網提供服務的情形下，所要記得服務的位置就可能變成上百種。

如果服務位址還是一個一個的牢記在心裡，這樣不僅缺乏彈性，而且很沒有效率。尤其是當我們來到了一個陌生的地方，想要使用當地的服務，若是能有個入口網站，來幫助使用者動態地發現所需的服務位置以及詳細描述，這樣不就變的方便許多。因此在目前市面上，就有一些關於 Service Location 的協定，它們使用了一系列的代理程式來幫助使用者動態的尋找、更新、提供、刪除、控制目前在網路上的服務。

本篇論文將介紹 5 種關於 Service Location 的協定，依序是 Service Location Protocol(SLP)、Juxtapose(JXTA)、Universal Plug and Play(UPnP)、Lightweight Directory Access Protocol(LDAP)、Naming Authority Pointer(NAPTR)。最後將在結論裡闡述關於此 5 種協定的比較結果。[1]

二 Service Location Protocol

2.1 SLP 簡介

Service Location Protocol(SLP)是由 IETF 所制定的標準協定，它提供了一種可擴展、有彈性的架

[1] 本論文研究成果之經費由國科會計畫編號 NSC95-2221-E-216-039 與 96-2221-E-216-010, 與中華大學計劃編號 CHU95-2221-E-216-039 與 CHU96-2221-E-216-010 贊助提供。

構，讓使用者無論走到何地，皆可以透過 SLP 在網路上動態的找尋可用的服務位置及其相關資訊，這樣的彈性，大大提升了電腦設備的可攜性。SLP 可讓使用者自行設定想要提供的服務類型，並設定屬性描述此服務，再使用 SLP 發佈在網路上，供他人取用。此外，當使用者想取得特定服務時，亦可使用 SLP 過濾篩選，以取得所需要使用的服務。

SLP 的應用環境除了在企業區域網路外，一些商用區域網路也很適用。而 SLP 在提供網路服務時，是採用 client/server 的架構，client 向 server 提出所要尋找的服務需求，以取得 server 回應的服務資訊。另一方面，server 則是負責蒐集網路下各種不同的服務資訊，以提供給 client 查詢使用。

2.2 SLP 元件

根據文件[2]規範，SLP 的元件主要分成三個部份：

1.User Agent(使用者代理人 UA)：為一個應用程式，用來替使用者向 Service Agent 或是 Directory Agent 查詢所需要服務的位置以及相關資訊。多半為一台 PDA、手機、或是 Note Book 等可移動的電腦設備。

2.Service Agent(服務代理人 SA)：為一個應用程式，用來向 UA 或 DA 宣傳一或多種的服務，較適用於一般小型區域網路。

3.Directory Agent(目錄代理人 DA)：為一個應用程式，用來蒐集多個 SA 所宣傳的服務，以供 UA 查詢使用。

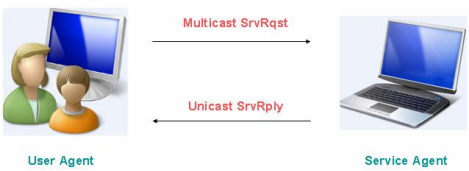
2.3 SLP 元件運作模式

由 SLP 的規範[2]得知 UA、SA、與 DA 的搭配運作，可分為兩種，分別是分散式互動與集中式互動。分散式互動環境適用於小型的區域網路裡，可為一或多個 SA 以及一或多個 UA 所構成。而集中式互動環境較適用於中型或大型的企業網路裡，通常都會擁有較多個 SA，相對的網路負載也會比較重，因此可使用一或多個 DA 來當做服務資訊的集中地，cache 多個 SA 所註冊的服務，並定時從 SA 中取得更新或註銷的訊息，使 UA 不再需要向多個 SA 進行查詢，以降低網路負載，提高速率。而多個 DA 可儲存相同的 SA 資訊，以免某個 DA 壞了導致癱瘓，容錯力高。

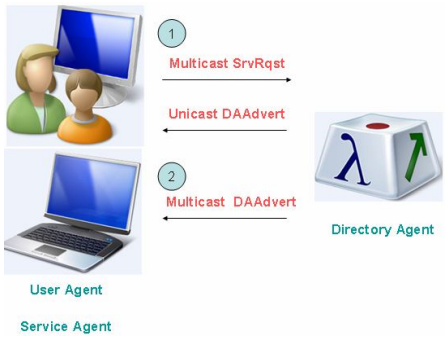
以下即將介紹上述兩種互動環境的過程，圖一所示之架構為 SLP 分散式互動的環境，為一個小型區域網路，由多個 SA 負責宣傳本身提供的服務，供 UA 做查詢。首先，由 UA 主動向多個 SA 發出 Multicast Service Request 的請求訊息，以取得所需服務資訊。之後每個 SA 便核對適當的服務資訊，分別回應 Unicast Service Reply 訊息給 UA。如果說該網路沒有支援 Multicast 的話，即採用 Broadcast。

在圖二中說明了 UA 以及 SA 如何發現 DA 的所在位置。DA 有兩種方式可以被 UA 以及 SA 發現。第一種是由 DA 主動定時發出 Multicast DA Advertisement 訊息給 UA 和 SA。第二種是當 UA 或 SA 剛連上網路時錯過了某時段 DA 的 Advertisement 訊息，卻又想立即使用 DA，則 UA 或 SA 將主動發出 Multicast Service Request 的請求訊息，其服務類型為 service：directory-agent，用以表示要尋找 DA 這項服務。當網路上多個 DA 收到之後，即會分別回應 Unicast DA Advertisement 訊息給 UA 或 SA，告知其所在。而 UA 要發現 SA 也跟上述方式一致，只是將請求訊息的服務類型改為 service：service-agent 即可。

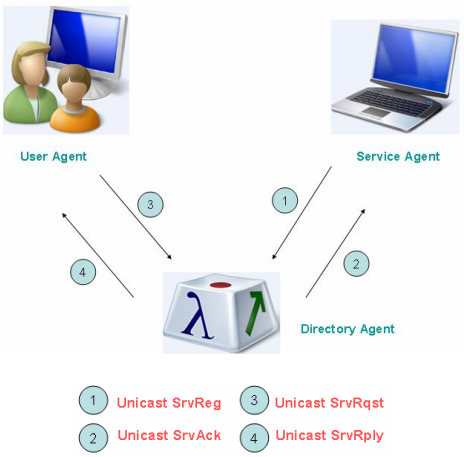
圖三所示之架構為 SLP 集中式互動的環境。通常為中型或較大型的企業網路，多個 SA 向一或多個 DA 註冊本身所提供的服務資訊，供 UA 做查詢。首先由每個 SA 發出 Unicast Service Register 的訊息，向 DA 註冊自己所提供的服務資訊，接著 DA 回應 Unicast Service Acknowledgement 訊息給 SA，用以確認註冊是否順利完成。之後 UA 只需向單一個 DA 發出 Unicast Service Request 訊息，索取所需服務資訊，等待 DA 回傳 Unicast Service Reply 訊息，當中挾帶服務資訊給 UA 即可。



圖一 UA 向多個 SA 查詢並取得服務資訊的過程



圖二 UA 和 SA 如何發現 DA 的過程



圖三 多個 SA 向一或多個 DA 註冊所提供的服務，UA 向 DA 取得服務資訊

2.4 SLP 服務位置

在 SLP 裡，服務的位置格式為 **service：<srvtype>：//<addrspec>**，<srvtype>即為 SLP 服務類型，可分為一般類型以及抽象類型。在一般類型上，通常為任何標準網路通訊的協定，如 http、lpr，例如：**service：http**。而在抽象類型方面，其格式為

service：<abstract-type>：<concrete-type>

<abstract-type>代表抽象的服務類型，如 printer，<concrete-type>則表示實際的服務類型，如 http，例如：**service：printer：http**。<addrspec>則為 Hostname 或是 IP Address。

在一般類型以及抽象類型之後可加入特殊的子字串，以"."字元做為區隔，此子字串稱為 Naming Authority。同樣的服務類型使用不同的 Naming Authority 代表不同的服務類型。例如：**service：printer.one：lpr** 和 **service：printer.two：lpr**，詳細介紹請參考[1]及[2]。

以下為 SLP 服務位置的範例：假設 UA 發出 Service Request 訊息給 DA，要求服務型態為 service：printer，則經配對過濾之後，找出兩個符合此服務類型需求的 service URL，分別為 service：printer：lpr：//myprinter.com、service：printer：http：//hostprinter.com。

2.5 SLP 服務範圍

SA 和 DA 通常在使用時，一定會涵蓋一或多個有效範圍(Scope)，像是一層樓、一棟建築、一間實驗室裡有哪些服務資訊，用以群組方式管理，方便在查詢時過濾使用。Scope 預設以 DEFAULT 表示。至於 UA 則是可有可無，可以設定一或多個 Scope，也可以不用設定。

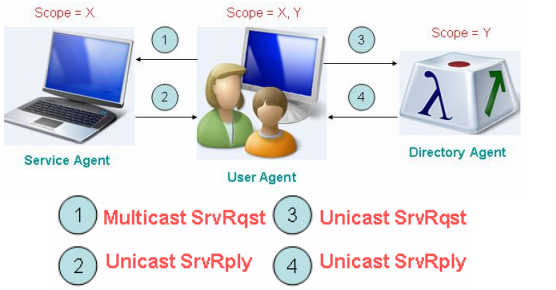
在不用設定 Scope 的情形下，表示 UA 在查詢時能發現網路上任何有效 Scope 裡所提供的服務資訊。在此有兩個例外，當 UA 發出 Service Request 訊息中，其服務類型分別為 service:directory-agent 和 service:service-agent 時，也就是要發現 DA 或 SA 時，Scope-List 為 0。

圖四為假設 UA 要找尋 X 和 Y 兩個 Scope 裡的服務資訊，因為 X Scope 的網路環境為分散式互動網路，因此 UA 則使用 Multicast Service Request 給多個 SA。而 Y Scope 為集中式網路，因此使用 Unicast Service Request 給一個 DA。

2.6 SLP 訊息

SLP Header：所有 SLP 訊息開頭皆帶有一個標頭，用以得知 SLP 的版本、標頭後面緊跟著是何種訊息、訊息總長、控制旗標、連線序號、以及訊息發出需求以及回應時所要使用的共同語言(如 en、de)。而控制旗標共有三個，分別為：

<O>：OVERFLOW Flag(0x80)。表示訊息是否有超過資料包的長度限制。UA 一般發佈 Service Request 訊息時，通常是使用 UDP 資料包來發送，除了 UDP 以及其他標頭以外，在此預設最大的傳輸單元為 1400bytes。若是 UA 向 DA 查詢某個服務類型的資訊，則當 DA 回傳給 UA 符合的服務資訊大於最大傳輸單元時，會將此回傳訊息縮減為符合最大傳輸單元長度，將 OVERFLOW Flag 設定之後回傳。此時 UA 收到之後，就會改以 TCP



圖四 UA 設定 DA 和 SA 所支援的 Scope 分別進行查詢的過程

連線的方式，重新傳輸。

<F>：FRESH Flag(0x40)。當 SA 向 DA 重新註冊某服務時，若設定此旗標，則表示蓋過原先的服務訊息，若沒設定則代表更新原先服務訊息的某些內容。

<R>：REQUEST MCAST Flag(0x20)。用來決定發佈的訊息是否要使用 Multicast。SLP 用來監聽收到訊息的慣用埠號為 427，以提供回應及確認訊息使用。而傳送訊息則使用非慣用臨時性的埠號。Multicast Address 為 239.255.255.253，預設 TTL 值為 255。

以下為 SLP Header 之後，所接的 11 種訊息：Service Request：為 UA 向 SA 或 DA 發出查詢服務需求以及 UA 或 SA 尋找 DA 時使用。使用者可依照個人的喜好，設定想搜尋的服務類型、服務範圍、以及設定某些服務的屬性透過 LDAPv3 Search Filter 進行查詢過濾。而在 Service Request 比較特別的欄位為 Previous Responder List，當 UA 使用 Multicast 傳送時，可能會因為傳送途中發生某些錯誤，而導致傳送的群組中只有某幾個 SA 或 DA 有收到訊息而回應。

因此 UA 可由回應訊息中，得知哪幾個 SA 或 DA 有收到訊息，而將它們的 IP Address 紀錄至此欄位。當再次發送 Multicast 重傳時，可用來分辨哪個 IP Address 之前已經傳送過，不需要再次傳送。若要求訊息使用 Unicast，則此欄位總是為空。

以下為三個 UA 發出 Service Request 進行查詢服務的簡單例子，其中<t>代表 Service Type，<s>代表 Scope，<p>代表 Predicate(依照個人喜好設定所需服務的屬性及其值，以透過 LDAPv3 Search Filter 進行過濾篩選)。

<t>=service:http <s>=DEFAULT <p>= (empty string)

此 Service Request 查詢在 DEFAULT Scope 裡，所有 http 服務類型的資訊。

<t>=service:pop3 <s>=SALES, DEFAULT <p>=(user=wump)

此 Service Request 查詢在 SALES 或 DEFAULT Scope 裡，所有 pop3 服務類型中，擁有屬性為 user，其值為 wump 的資訊。

<t>=service：directory-agent <s>= DEFAULT <p>=

此 Service Request 查詢在 DEFAULT Scope 裡，所有 DA 服務類型中的資訊，也就是上述提到搜尋 DA 的方法。當 DEFAULT Scope 裡的 DA 收到此訊息時，皆會回傳 DA Advertisement 給 UA 或 SA。

Service Reply：為 SA 或 DA 回傳 URL Entries 或錯誤訊息給 UA。URL Entry 為 SLP 實際上傳輸服務資訊的基本單元，其中包含了服務位置、服務有效的存活時間等等。

Service Registration：為 SA 向一或多個 DA 註冊所提供的服務訊息，包括 URL Entry、服務類型、服務範圍以及相關屬性。

Service Deregister：SA 發出註銷訊息告訴 DA 它所註冊是哪個服務或者是服務的哪些屬性需要被註銷，而若是 DA 回傳 Service Acknowledgment 確認訊息的話，代表註銷成功。

Service Acknowledge：為 DA 回應 SA 註冊訊息是否成功。

Attribute Request：UA 可以使用此訊息來得知某個服務所提供的屬性(如 service：http：//myhost.com)或某服務類型範圍內，所有服務的屬性(如 service：http)。並可依 Tag-list 欄位來取得所需要的幾個屬性值。

Attribute Reply：為 SA 或 DA 回傳符合的屬性資訊給 UA。

三 Juxtapose

3.1 JXTA 簡介

JXTA 為 juxtapose 的簡寫，源自於 2001 年

Sun Microsystems 的構想，為一個開放式原始碼的計畫，由許多 Peer-to-Peer 的協定所構成，這些協定定義了一組 XML 訊息，允許任何網路設備(蜂巢式行動電話、PDA、大型電腦、伺服器)視為一個 Peer 來彼此互相通訊、監控、組成群體、發現、宣傳服務，以達成分散式的網路架構。根據規範[10]得知，使用 JXTA 所開發出來的 P2P 應用程式可以具備以下幾個特點:1.可以動態的找尋其他 Peer，而不受到防火牆以及 NAT 的限制 2.簡單的分享服務，不需在意網路拓撲 3.可找尋網路位置資訊 4.創造 Peer 群體來提供服務 5.遠端監控 6.Peer 間通訊相當安全可靠。

3.2 JXTA 架構

JXTA 的軟體架構分為三層，如圖五所示。

Core Layer：負責處理 Peer、Peer Group 的建立、通訊、安全、管理、以及路由等功能。

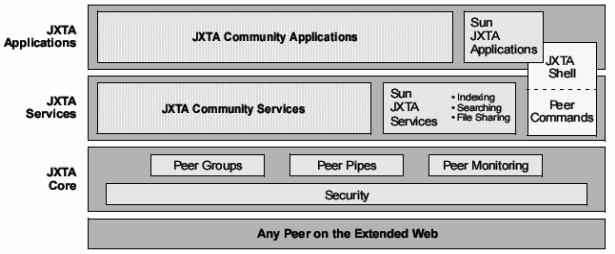
Service Layer：負責較高階的網路服務概念，像是編排、修改、搜尋、資源聚集、協定轉換、認證以及檔案分享等功能。

Application Layer：包含了一些整合性的 P2P 應用程式實作，像是 P2P 即時訊息、P2P 電子郵件系統、分散式拍賣系統等等。

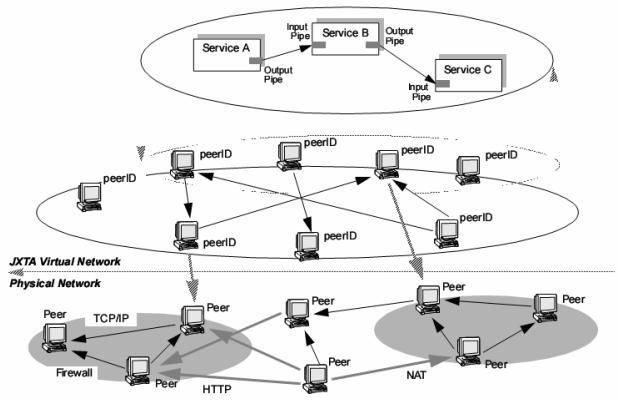
3.3 JXTA 元件

由規範[10]得知，在 JXTA 中定義了幾個基本元件，以下將簡單介紹它們的功用：

1.Peer：JXTA 網路是由一群互相連接的節點所構成，此節點稱為 Peer。Peer 可為任何一種類型的網路設備(感應器、PC、PDA、手機)，並實作 JXTA 計畫中所定義的協定。在一個實體的設備中，可以運作多個 Peer，而多個設備亦可合作扮演著一個 Peer 的角色。Peer 可以使用各種不同的通訊協定，像是 TCP/IP、HTTP、Bluetooth、以及 GSM。每一個 Peer 皆擁有獨一無二的識別碼 Peer ID。如圖六所示，根據規範[12]，每一個 Peer 依照它們的 Peer ID 來當作邏輯位置互相連結，成立虛擬網路於網際網路以及非 IP 網路之上，這使得 Peer 與 Peer 即使位在不同的網路架構下，像是有 NAT 或防火牆，或是 Peer 移動至別的網路，而導致更改了原先的 IP Address，Peer 與 Peer 仍然能夠彼此互相通



圖五 JXTA 軟體架構



圖六 JXTA 虛擬網路架構

訊。

2.Peer Group：由一群 Peer 所構成，提供一些一般常用、本身所需要、有興趣的服務，並可建立不同等級的安全區域。Peer Group 也擁有 Peer Group ID。Peer 可以同時屬於多個 Peer Group，在預設的情形下，通常所有 Peer 是被加入至 Net Peer Group 裡。

3.Network Services：Peer 與 Peer 間通常彼此會發佈、尋找、請求服務，此服務分為兩種類型：
Peer Services：僅 Peer 所發佈的服務，若此 Peer 離線或是損毀，則此服務實體也會跟者消失。
Peer Group Services：由多個 Peer 服務實體所組成，當某一個 Peer 離線或是損毀時，並不影響服務的傳送，容錯力較高。JXTA 定義了必備的 Peer Group Services，只要 Peer 加入了此群組，就必須實作這些服務。這些服務為：

Endpoint Service：負責 Peer 與 Peer 間傳遞與接收訊息使用(Endpoint Routing Protocol)。

Resolver Service：負責發送詢問訊息至其他的 Peer，以取得任何資訊。

此外，其他選擇性的標準服務也可以被實作

於 Peer 中，這些服務為：

Discovery Service：Peer 成員查詢 Peer Group 裡有提供哪些服務。

Membership Service：Peer 成員建立安全性 ID，此 ID 允許應用程式以及服務決定誰需要執行運作，以及此運作是否被允許。

Access Service：負責接收、決定、認證某 Peer 所送來的請求是否生效。

Pipe Service:負責創造以及管理 Peer Group 成員裡，Pipe 的連線。

Monitoring Service：Peer Group 裡的成員監控其他的成員。

4.Modules：提供了一些 Java class、jar file、DLL、XML file、或是 script，為抽象化的概念，被 Peer 使用來實作服務、訊息傳輸等功能。此抽象化 Module 包含了三個部份，分別為：

Module Class：定義一個行為，供實作使用，每一個 Module Class 皆有一個獨一無二的 ID，稱為 ModuleClassID。

Module Specification：主要用來存取 Module 的資訊，像是 Pipe Advertisement 用來與服務通訊，因此 Module Specification 必定包含了 Module Class，以提供某些功能。每一個 Module Specification 亦有一個 ID，稱為 ModulSpecID，ModulSpecID 內嵌了 ModuleClassID，以指示連接的 Module Class。

Module Implementation：實作 Module Specification。同一個 Module Specification 可以實作出多個 Module Implementation。

5.IDs：每一個 JXTA 的資源(如 Peer、Peer Group 、Advertisement、Service 等等)需要唯一的識別碼，遵循 URN 命名空間。以下為 peer ID 的例子：

urn:jxta:uuid-59616261646162614A7874615032503
3F3BC76FF13C2414CBC0AB663666DA53903

jxta 格式表示其 ID 屬於 World Peer Group，而 uuid 格式則是隨機產生。

6.Advertisement：由 XML 組成，Peer 用來命名、描述、發佈網路資源(Peer、Peer Group、Pipe、Service)的存在。Peer 可宣傳 Advertisements，或是取得其它 Peer 的 Advertisements。每一個 Advertisement 皆有其存活時間，以表示資源的有效期限。以下為 JXTA 的 Advertisements 類型：

Peer Advertisement：描述 Peer 的資源，像是 Peer 名稱、Peer ID、屬性等。

Peer Group Advertisement：描述 Peer Group 的資源，像是 Peer Group 名稱、Peer Group ID、服務參數等。

Pipe Advertisement：描述 Pipe 通訊管道，被 Pipe Service 用來連結 Input、Output Pipe 端點。其內容包含有 Pipe 類型、Pipe ID 等。

ModuleClassAdvertisement：用來描述 Module Class，宣告它的存在，其內容為 Class Name、描述、以及 ID(ModuleClassID)。

ModuleSpecAdvertisement：定義了一個 Module 的規格。

ModuleImplAdvertisement:定義一個 Module Specification 的實作。

Rendezvous Advertisement：描述一個 Peer 扮演著一個 Peer Group 裡的 Rendezvous Peer。

Peer Info Advertisement：描述 Peer 的狀態資訊，像是運行時間、最後一次送收訊息的時間等。

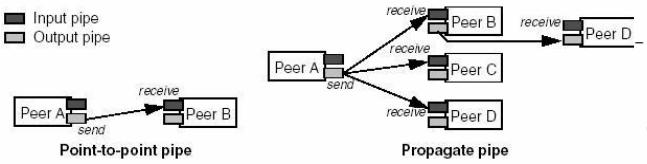
每個 Advertisement 皆代表者一份 XML 的文件，由許多屬性階層式的組成，用以描述相關資源。如圖七所示為一個 Pipe Advertisement。

7.Messages：JXTA 的服務以及應用程式通訊時，所傳輸的訊息。由 XML 構成，Peer 之間交換資訊的基本單元，透過 Endpoint Service、Pipe Service、JXTASocket、JXTABiDiPipe 來進行傳輸。

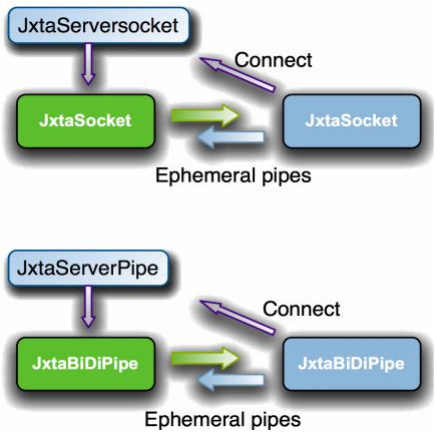
8.Pipe：傳送或接收上述 Messages，非同步、單向、不可靠、虛擬的，分為 Input(收)和 Output(送)

```
<?xml version="1.0"?>
<!DOCTYPE jxta:PipeAdvertisement>
<jxta:PipeAdvertisement xmlns:jxta="http://jxta.org">
<Id>
 urn:jxta:uuid-59616261646162614E50472050325033 8E3E786229EA460DADC1A176B69B73 1504
</Id>
<Type>
 JxtaUnicast
</Type>
<Name>
 TestPipe
</Name>
</jxta:PipeAdvertisement>
```

圖七 Pipe Advertisement 的例子



圖八 Point-to-Point 和 Propagate Pipes



圖九 JXTASocket 和 JXTABiDiPipe

Pipe。Pipe 能夠動態的繫結至一或多個 Peer 的端點上，以便當某 Peer 離線或是發生損壞時，能重新做動態繫結，高容錯力。Pipe 提供三種模式做通訊：

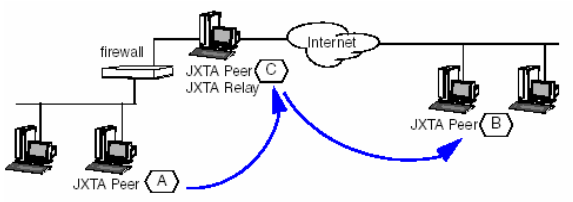
Point-to-Point Pipes：兩 Pipe 做單向傳輸，一個 Pipe 送，另一個 Pipe 收。

Propagate Pipes：一個 Pipe 送，多個 Pipe 收，如圖八所示。

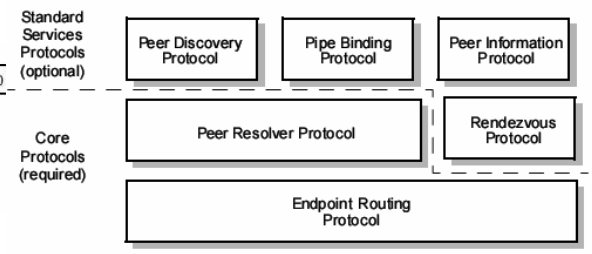
Secure Unicast Pipes：為上述 Point-to-Point Pipe 的一種類型，提供安全、可靠的通訊管道。

9.JXTASocket and JXTABiDiPipe：屬於較高階的傳輸方式，雙向、可靠、安全，優於 Pipe 傳輸，如圖九所示。

10.Security：P2P 網路中的資源，需要有不同安全級別的存取限制。其被提出的五個安全需求為保密、認證、授權、資料完整性、是否已經正確的送達過。



圖十 Peer 通過防火牆交由 Relay Peer 轉送路由的過程



圖十一 JXTA 通訊協定架構

3.4 Peer 種類

JXTA 屬於 Ad-Hoc、Multi-Hop 網路。在網路的概念上，將 Peer 分為四種類型：

1.Minimal Edge Peer：單純能送和收 Messages，本身無法暫存 Advertisements，亦無攜帶至其他 Peer 的路由資訊，為小型設備，如 PDA、手機等等。

2.Full-Featured Edge Peer：能送和收 Messages，並且能夠暫存 Advertisements，供其它 Peer 查詢所暫存的 Advertisements。若本身並無提供符合 Peer 要查詢的 Advertisements 時，沒有提供幫忙轉送查詢需求的服務。

3.Rendezous Peer：通常做為 Peer Group 的集中地，暫存大量的 Advertisements 和路由資訊，並且維護此群組 Peer 的拓撲結構。Peer Group 裡可以有很多個 Rendezous Peer，且任一個 Peer 均可以變為 Rendezous Peer。

4.Relay Peer：維護 Peer 之間的路由資訊。Peer 要傳送訊息至另一個 Peer 時，會先查看本身是否有暫存此路由資訊，若沒有，則向 Relay Peer 查詢，以取得資訊，亦可以幫忙轉送 Messages，通常協助在防火牆及 NAT 之後的 Peer 路由。如圖十所示：

3.5 JXTA 協定

以下將簡單介紹 JXTA 計畫所使用的一些協定，如圖十一所示，為 JXTA 通訊協定的架構。

Peer Discovery Protocol：Peer 發佈本身所提

供的 Advertisements，以及發現、尋找其它 Peer 所提供的 Advertisements(Peer、Peer Group、Pipe 等等)。

Peer Resolver Protocol：Peer 可以查詢其他 Peer 的任何解析資訊，不論是否屬於同一個 Group，如 Peer Name 對應的 IP Address(DNS)，IP Socket 對應的埠號，以及服務對應的網路位置(LDAP)。

Peer Information Protocol：Peer 取得其他 Peer 的狀態資訊，如是否在線、運行時間、流量等屬性值。

Rendezvous Protocol：Peer 能向 Rendezvous Peer 訂閱所暫存的服務資訊。若本身為 Rendezvous Peer 則可負責傳播服務資訊給所屬 Peer Group 範圍內的 Peer。

Pipe Binding Protocol：Peer 繫結二或多個 Pipe 端點至另一個 Peer 的端點上，進行訊息傳送。

Endpoint Routing Protocol：Peer 要傳送訊息至另一個 Peer 時，可使用此協定來尋找路徑，向 Relay Peer 詢問路由訊息。

四 Universal Plug and Play

4.1 UPnP 簡介

UPnP 全名為 Universal Plug and Play，由微軟所提出，做為隨插即用週邊設備模型的延伸，由一群標準協定所構成，像是 HTTP、TCP、UDP、IP、XML 等，用於 Peer-to-Peer 網路下，任何設備不需要安裝驅動程式即可彼此互相通信，進一步啟用同層級的網路功能。由規範[19]知，此構想源自於 DHCP，希望除了讓設備的網路位址自動取得之外，其它設定也能自動化取得，以達到操作容易、有彈性，只要設備一連上網路，無論是在家裏或是在公司等任何地點，皆能和其他設備互相發現、連結、使用以及控制，一切都不需要做任何的設定。

4.2 UPnP 元件

根據規範[19]以及[20]，UPnP 的基本元件有三個，如圖十二所示：

1.服務(Service)：在 UPnP 裡，一個服務提供了一組紀錄此服務目前狀態的變數，用以表現服務的動作。例如：印表機列印服務，它可能包含了像是開始、停止列印的動作，以及目前是否為空閒或忙碌的狀態變數等資訊。

2.裝置(Device)：存放上述服務和巢狀裝置的容器，稱為裝置。像是印表機提供列印服務。

3.控制點(Control Point)：用來取得某裝置的描述說明、服務資訊、傳送動作訊息來控制服務、向有興趣的服務訂閱其狀態資訊，當服務狀態發生改變時，事件伺服器便會回傳事件給控制點。

4.3 UPnP 協定堆疊

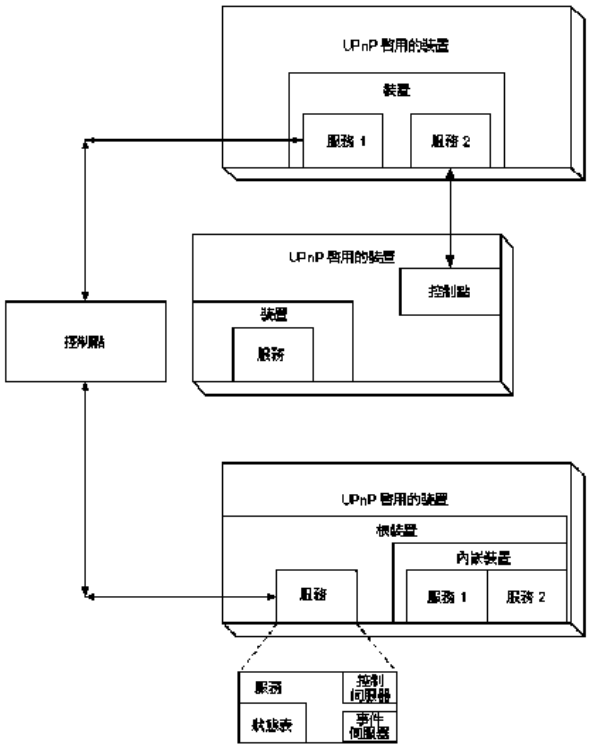
以下為 UPnP 的協定堆疊，如圖十三所示，由於 UPnP 沿用既有的標準通訊協定(HTTP、UDP、TCP、IP、XML)，所以能夠達到輕易的跨平台。以下將簡單描述比較少見協定的基本功能：

1.HTTPMU(Multicast)和 HTTPU(Unicast)：為 HTTP 的延伸，以 UDP/IP 傳送訊息，被 SSDP 所使用。

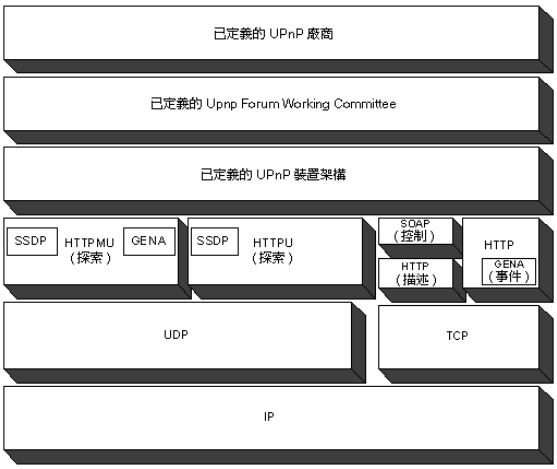
2.SSDP(Simple Service Discovery Protocol)：簡單服務發現協定，內建於 HTTPMU 和 HTTPU 裡，使裝置宣傳本身有提供哪些服務，以及控制點如何發現網路上有哪些服務，並進而取得服務的資訊。

3.GENA(Generic Event Notification Architecture)：一般事件通知結構，用來處理如何傳送訂閱的訊息以及如何接收通知訊息。

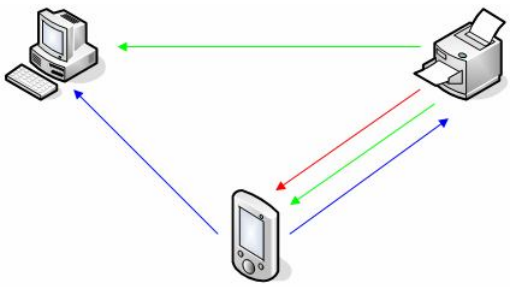
4.SOAP(Simple Object Access Protocol)：簡單物件存取協定，定義如何使用 XML 和 HTTP 來執行遠端程序呼叫的方式，為網際網路上進行 RPC 通訊的標準，主要功能用來控制裝置。



圖十二 UPnP 元件



圖十三 UPnP 協定堆疊



圖十四 Discovery

4.4 UPnP 運作流程

以下將一步一步的介紹 UPnP 的運作流程：

1.Addressing：所有在網路上的裝置要互相溝通連結時，必須要先有網路位址，UPnP 的裝置會先以 DHCP 的方式，動態取得 IP 位址，若無 DHCP 伺服器存在的話，會先以 Auto-IP(從一組保留的私人位址中，以智慧的方式選擇 IP 位址)的方式來做設定，並持續監聽有無 DHCP 伺服器的存在，若發現則改用 DHCP。

2.Discovery：當有了位址，即開始使用 SSDP 透過 HTTPMU 和 HTTPU 來做服務的發現以及宣傳自身提供的服務。當裝置加入網路時，會告知網路上控制點它的存在，如圖十四所示，印表機發出 Device Advertisement(綠色)告知其它控制點它的存在。當控制點加入網路時，即可搜尋有興趣的服務裝置類別。例如 PDA 發出 Search Request(藍色)訊息，而印表機收到後，回應 Device Reply(紅色)訊息。

3.Description：當控制點由上述 Discovery 步驟中知道某裝置的存在時，想更進一步了解它的功能，便可去向此裝置尋求它的描述文件(型號、序號、製造廠商名稱、廠商專屬網站、狀態變數等資訊)。如上圖 PDA 發出 Get Description 訊息，Printer 回應 Device Description XML Document。

4.Control：當透過 Description 取得裝置詳細描述之後，控制點就知道如何對裝置做控制使用，其控制的過程透過 SOAP 傳送 XML 文件，若成功，則產生動作並回傳狀態改變的變數資訊，若失敗，則回傳錯誤碼。如 PDA 發出 Action SetPower On 控制印表機開啟，當收到訊息後，印表機則回傳 Return Action Result。

5.Event：控制點可以針對有興趣裝置的狀態碼做訂閱的動作，當裝置狀態發生改變時，則觸發事件，利用 GENA 傳送 XML 文件。如 PDA 發出訂閱 Printer 狀態資訊，當 PC 發出開啟 Printer 的動作而使印表機開啟時，觸發事件，通知 PDA 印表機此時狀態改變為開啟。

6.Presentation：倘若裝置有提供呈現資訊網頁的 URL，則控制點可直接透過瀏覽器擷取裝置的狀態資訊，並且進而控制此裝置。如 PDA 發出 Get Presentation 使用瀏覽器來觀看印表機目前狀態變數，並可加以控制。

五 Lightweight Directory Access Procotol

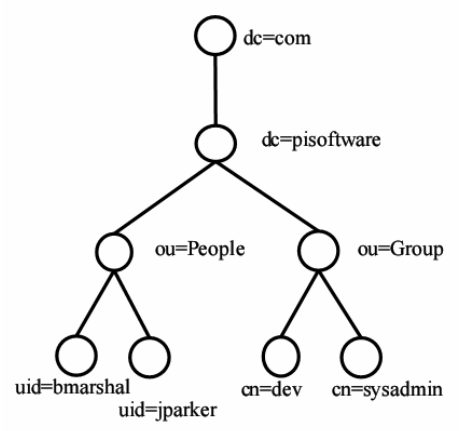
5.1 LDAP 簡介

一個目錄是由許多個物件所構成，而在這些物件中，包含了許多個屬性。像是電話簿由許多人名所構成，而每個人名中又存取了許多的相關資訊(電話號碼、地址)。LDAP 全名為 Lightweight Directory Access Protocol，輕量級目錄訪問協定，用來查詢以及修改目錄服務(RFC1777)，運作於 TCP/IP 之上，為 Client/Server 的網路架構，首先由密西根大學所實作出來，因為基於 X.500(Heavyweight Service)此目錄服務功能過於複雜，而從中移去某些功能，使其簡化，較為廣泛的使用。目前 LDAP 所使用的版本為 LDAPv3，詳述細節記載於 RFC4510。

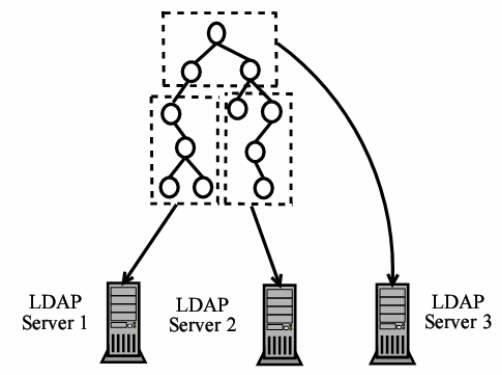
5.2 LDAP 資料結構

LDAP 的資料部屬方式採用了 DNS 架構的階層式節點命名來儲存，而此階層式架構稱為目錄資訊樹(Directory Information Tree)，簡稱為 DIT。

根據規範[21]和[22]得知，LDAP Entry 為 DIT 樹的基本儲存單元，由一個 Distinguished Name(DN)和一群屬性所構成，屬性可設為單值或多值。如圖十五所示，一個節點即為一個 Entry。多台 LDAP 伺服器的目錄資訊樹再拼湊成更大的一棵目錄資訊樹，如圖十六所示：



圖十五 LDAP 目錄資訊樹(Directory Information Tree)



圖十六 多台 LDAP 伺服器的目錄資訊樹

表一 LDAP 屬性

Uid	User ID
Cn	Common Name
Sn	Surname
L	Location
Ou	Organisational Unit
O	Organisation
Dc	Domain Component
St	State
C	Country

5.3 LDAP Entry

LDAP 樹中的 Entry 使用唯一鍵來做辨識，此唯一鍵稱為 Distinguished Name(DN)，它的命名方式是由該 Entry 開始算起，由下而上依序將每一個節點的屬性結合所構成，如圖十五最左下的 Entry，其 DN 為(uid=bmarshal，ou=People，dc=pisoftware，dc=com)。DN 又細分成兩個部份，最左的屬性稱為 Relative Distinguished Name(RDN)，而剩餘的部份則稱為 Base Distinguished Name。同上述 DN，其 RDN 為 uid=bmarshal，而 Base DN 為 ou=People，dc=pisoftware，dc=com。

5.4 LDAP Entry Format

在上個小節中提到 Entry 是由許多屬性所構成，以下將簡介幾個 LDAP Entry 的屬性縮寫的實際名稱，如表一，若想了解如何定義屬性的語法，請參考 RFC2256。而 LDAP Entry 的內容可用文字的方式表示稱為 LDIF(LDAP Data Interchange Format)，如圖十七所示。

5.5 LDAP Search Filters

當資料即 Entry 儲存至 LDAP Server 中時，LDAP Client 可以向 Server 查詢所需要的 Entry 資訊，而 LDAP Search Filters 即是提供此方面的功能。由 Client 端下屬性及其值的術語向 Server 端做查詢，經過濾之後，Server 端回傳符合的 Entry 資訊給 Client 端。目前較為大眾所熟悉的標準為 RFC 2254 LDAPv3 Search Filters。Search Filters 可以使用的運算子像是&(and)、|(or)、!(not)、~=(approx equal)、>=(greater than or equal)、<=(less than or equal)、*(any)等等。以下為 Search Filters 的簡單例子：

(objectclass=posixAccount)

(cn=Mickey M*)

(| (uid=fred)(uid=bill))

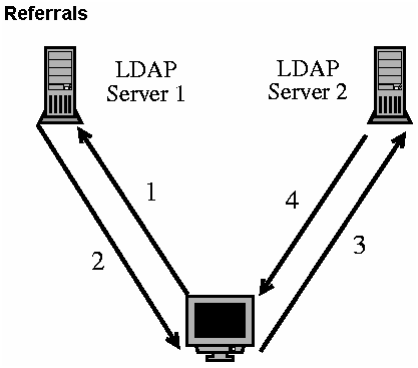
(&(| (uid=jack)(uid=jill))(objectclass=posixAccount))

5.6 LDAP Search Scope

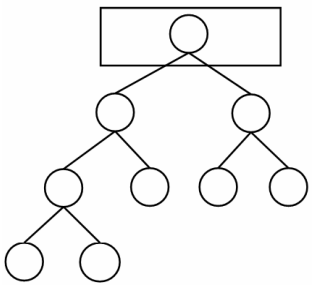
當 LDAP Client 下術語搜尋 Entry 時，其方式類似 DNS 層層搜尋、重新導向，如圖十八所示，1.由 LDAP Client 先向 Server1 查詢，2.Server1 重新導向 Client 參考至 Server2 做查詢，3.Client 再向 Server2 查詢，4.Server2 回傳資訊給 Client。依照查詢的術語不同，其搜尋範圍可分為三種，圖十九為 Base(僅搜尋 Base Object)，圖二十為 Onelevel(搜尋 Base Object 的下一層，即是 Base Object 的兒子)，圖二十一 Subtree(搜尋 Base Object 以下的子樹)。

```
dn: uid=bmarshal,ou=People,dc=pisoftware,dc=com
uid: bmarshal
cn: Brad Marshall
objectclass: account
objectclass: posixAccount
objectclass: top
loginshell: /bin/bash
uidnumber: 500
gidnumber: 120
homedirectory: /mnt/home/bmarshal
gecos: Brad Marshall,,,,
userpassword: {crypt}KDnOoUYN7Neac
```

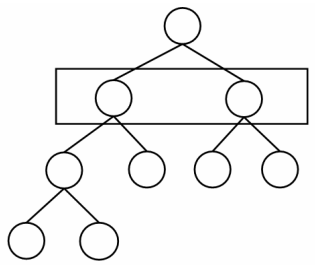
圖十七 LDAP Data Interchange Format



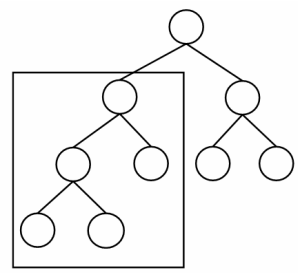
圖十八 LDAP Search



圖十九 Base Scope



圖二十 Onelevel Scope



圖二十一 Subtree Scope

5.7 LDAP URL Format

LDAP Client 端可使用像是 LDAP Browser 的 GUI 介面程式向 LDAP Server 做查詢，以取得所需的資訊。其連繫的位址稱為 LDAP URL，而它的格式如下所示：

ldap://<hostname>:<port>/<dn>?<attributes>?<scope>?<filter>

以下為 LDAP URL 的例子：

ldap://ldap.myhost.com/dc=bar,dc=com??sub?uid=ba

rney

ldap://ldap.myhost.com/dc=bar,dc=com?cn?sub?uid=barney

六 Naming Authority Pointer

6.1 NAPTR 簡介

NAPTR 全名為 Naming Authority Pointer，出自於 RFC2915，為 DNS 紀錄的一種類型，可將一個網域名稱對應到一個或多個 URI 上，並有其優先順序，而使用不同的服務。為 ENUM 服務中一項重要的功能，定義電話號碼與服務選項之間的對應關係，即一個電話號碼可以對應多個服務項目。

6.2 ENUM 使用 NAPTR 的服務流程

由規範[24]和[25]得知，NAPTR 常應用在 ENUM 的操作過程裡。ENUM 為 IETF 的 ENUM 工作小組，可將現有的 IP 設備指定一個 E.164 號碼，使一個號碼依各種不同情況指定到不同的設備。其運作模式首先是將 E.164 號碼轉換成網域名稱格式，再到 DNS 查詢此網域名稱之 NAPTR 紀錄，連線到 NAPTR 所指定的 URI，使用所需服務。

如下所呈現的是將傳統電話號碼 +886-6-2-2341-3131 依相反順序轉換為 1.3.1.3.1.4.3.2.2.6.8.8.e164.arpa 網域名稱格式，再到 DNS 查詢此網域名稱 NAPTR 資源紀錄。查詢結果顯示的三筆資訊，將依序連到 3 筆之 URI，直到成功為止。第一筆為 SIP URI，第二筆為傳統電話號碼，第三筆為 E-MAIL。

$ORIGIN 1.3.1.3.1.4.3.2.2.6.8.8.e164.arpa

IN NAPTR 10 10 "u" "SIP+E2U" "!^.*$!sip:abel@twnic.net.tw"

IN NAPTR 20 10 "u" "TEL+E2U" "!^.*$!tel:+886223413300"

IN NAPTR 30 10 "u" "mailto+E2U "!^.*$!mailto:ant@chu.edu.tw"

6.3 運用 ENUM 和 NAPTR 取得 SIP URI

如圖二十二所示，當 User1 想和 User2 建立通話時，首先播打+886-3-5914495 電話號碼，透過 SIP Proxy Server 幫忙轉送，向 ENUM Server 查詢 User2 的 SIP URI 以建立通話。

七 結論

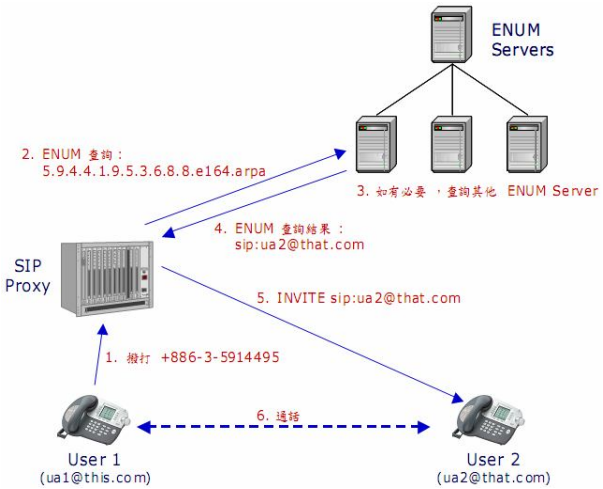
最後將上述介紹的 Service Location 議題做個整理，如表二所示。隨著數位家庭網路的時代來臨，各種大大小小的電器用品將來皆能在網路上提供不同的服務，Service Location 的議題也會顯得越來越重要。經過上表簡單的比較發現，議題多半是採用 IETF 所制定的標準。而 SLP 除了為 IETF 標準通用的協定之外，有 DA 可以集中管理服務資訊，降低網路負載，且沿用了 LDAP 的一些相關過濾篩選機制，在安全性上，又有認證可使用，因此前景相當看好。並且如果能與現在熱門的電信技術 SIP 互相搭配使用，以 SLP 先動態取得某地所提供的服務資訊，再利用 SIP 的高移動、All IP 特性去對有興趣的服務進行控制，將在未來的高行動網路裡，提供更強大的前瞻性。

參考文獻

[1]. J. Veizades, E. Guttman, C. Perkins and S. Kaplan, "Service Location Protocol", RFC 2165, IETF, July 1997

表二 Service Location 比較

	SLP	JXTA	UPnP	LDAP	NAPTR
來源	IETF	Sun	Microsoft	IETF	IETF
架構	Client/Server	Peer-to-Peer	Peer-to-Peer	Client/Server	Client/Server
服務位置	SLP Entry	XML	XML	LDAP Entry	NAPTR URI
搜尋服務	Service Request	Peer Discovery Protocol	Simple Service Discovery Protocol	LDAP Search	DNS Resource Record Search
應用	OpenSLP JSLP	JXTA(TM) Community Projects	UPnP Forum	OpenLDAP	Enum



圖二十二運用 ENUM 和 NAPTR 取得 SIP URI

[2]. E. Guttman, C. Perkins, J. Veizades, M. Day, "Service Location Protocol, Version 2", RFC 2608, IETF, June 1999

[3]. S. Holger, Teodora Guenkova-Luy, H. Franz J., "Service Location using the Session Initiation Protocol (SIP) "，IEEE, 2006

[4]. S. Ron, S. Henning, T. Srisakul, K. Wolfgang, "The Virtual Device: Expanding Wireless Communication Services through Service Discovery and Session Mobility", IEEE, 2005

[5]. S. Henning, W. Xiaotao, S. Stylianos, B. Stefan, "Ubiquitous Computing in Home Networks", IEEE, 2003

[6]. K. Christos I., K. Dimitrios A., K. Eleftherios A., T. Nikolaos D., V. Iakovos S., "Architecture for Reliable Service Discovery and Delivery in MANETs Based on Power Management Employing SLP Extensions", IEEE, 2006

[7]. P. Charles E. , "Service Location Protocol for mobile users", IEEE, 1998

[8]. G. Erik., "Service location protocol automatic discovery of IP network services", IEEE, 1999

[9]. JXTA(TM) Community Projects, https://jxta.dev.java.net

[10]. Sun Microsystems, "JXTA Java(TM) Standard Edition v2.5 Programmers Guide", September 2007

[11]. G. Li, "Project JXTA: A Technology Overview", October 2002

[12]. T. Bernard, A. Mohamed, D. Mike, H. Jean-Christophe, P. Eric, Y. Bill, "Project JXTA Virtual Network", October 2002

[13]. G. Li, "JXTA: A Network Programming Environment", IEEE, 2001

[14]. J. Mathieu, "JXTA Overview", http://www.irisa.fr/paris/web/Member-Home-Pages/view.html

[15]. S. Simon, "JXTA Technology Overview", https://jxta.dev.java.net

[16]. S. Kaarthik, "Project JXTA", http://lsdis.cs.uga.edu/~kaarthik/SemEnt/Project%20JXTA.ppt

[17]. UPnP Forum, http://www.upnp.org

[18]. UPnP Forum,"UPnP Device Architecture 1.0 ", July 2006

[19]. 蔡孟甫，曹世強，林盈達，"UPnP: 自動化網路設定", 2001 年 10 月，http://speed.cis.nctu.edu.tw/~ydlin/miscpub/survey_UPnP.pdf

[20]. F. Tom, "Windows XP 的通用隨插即用功能", 2001 年 10 月，http://www.microsoft.com/taiwan/technet/prodtechnol/winxppro/evaluate/upnpxp.aspx

[21]. M. Brad, "Introduction to LDAP ", http://quark.humbug.org.au/publications/ldap/ldap_tut_v2.pdf

[22]. M. Brad, "Introduction to LDAP ",http://quark.humbug.org.au/publications/ldap/ldap_tut.html

[23]. M. Mealling, R. Daniel, "The Naming Authority Pointer(NAPTR) DNS Resource Record", RFC2915, September, 2000

[24]. 許乃文, "ENUM 技術標準", 2004 年 3 月, http://www.twnic.net/seminar2004/html/31h.ppt

[25]. 江為國、許鴻基、蔡尚志、黃俊堯、洪鼎凱、余泰興，"我國 ENUM 註冊政策及服務模式規劃", 2003 年 8 月, http://www.twnic.net.tw/file/TWNIC-DN-92001.doc