

# Service Discovery between Multiple Home Networks

Tan Miaoqing  
Helsinki University of Technology  
mitan@cc.hut.fi

## Abstract

In this article we propose a gateway-based architecture for service discovery between multiple home networks across the Internet. The gateway deploys a proxy, which maps remote devices to local network using the gateway's IP address and collects all services within the local home network and exchanges the list of local services with other gateways of remote home networks. When a local device queries some specific services, the gateway will answer it on behalf of remote devices if there are matched services. In addition, SIP is utilized for initiating, managing and terminating the intercommunication between multiple home networks while TLS is used to protect the critical user data.

**KEYWORDS:** Home Networking, Service Discovery, UPnP, Zeroconf, Home-to-Home Communication, Gateway, SIP

## 1 Introduction

The modern home [1] is becoming a place where multiple networked devices are interconnected with each other, for instance, sharing a printer or ADSL connection among several PCs. Furthermore, commonplace home appliances [10], such as air conditioners, heaters, refrigerators, and lighting systems, are finding new useful services through connections to the Internet. Additionally, small personal computing devices such as smartphones, PDAs, and Internet tablets are becoming a part of daily life. These intelligent devices should be able to discover and communicate with each other so that the home network can provide better functionality and usability. It is difficult to configure heterogeneous devices to be interoperable, thus professional administrators are usually required. However, in the home network, administration and configuration are impractical, devices should easily and automatically join and leave the home network and also learn about other connected devices.

Service discovery protocols [2] allow appliances to find all available instances of a particular type of services in closed environments without prior configuration. There are several architectures aimed at service discovery within a home network, for instance, UPnP and Zeroconf. On the contrary, there is not so much research aimed at service discovery between multiple home networks. However, since the demanding for intercommunication between homes is increasing, new technologies that enable service discovery between multiple home networks are also essential. In this paper we will present a gateway-based architecture for service discov-

ery between multiple homes across the Internet.

The remaining article is organized as follow. Section 2 will introduce the concept of service orientation [5], and review two service discovery technologies [3, 5, 6] used in closed environment; section 3 will discuss the service discovery between home networks, and propose a gateway-based architecture with proxy component, as well as intercommunication between home networks using SIP [10]; section 4 will analyze further issues such as security [16] and interaction between different service discovery technologies [14]; and in the end, section 5 will draw the conclusion.

## 2 Service Discovery within One Home Network

### 2.1 Service Orientation

Before we discuss the issue of service discovery, it is better to first justify why interoperability among networked home appliances should adopt a service-oriented approach rather than a hardware-oriented one. [5] illustrates the concept of service orientation. In the device-centric view, the network consists of a couple of devices, each of which has a set of services. For instance, the network contains a client PC and a server PC. The client would query the server for what types of services are available. However, device-centric view works not so well for common users, since they care about the service rather which machine is running the service. The user would probably ask: "I need a printing service, is it available in this room?" If a device has the service, it would answer the user. There is no point to let the user query every machine if they have the service he wants. Therefore, service discovery should be made according to the type of service needed, not the devices running them.

In the following two sections, we will review two widely used service discovery technologies: UPnP and Zeroconf, and justify how they implement the service-oriented approach.

### 2.2 UPnP

The UPnP [3] architecture enables pervasive P2P network connectivity of PCs, intelligent appliances and wireless devices. The UPnP architecture introduces the control point as a device manager entity. When a device wants to use service from other devices, it will also be a control point, monitoring a standard multicast address for notifications of available services; otherwise it will only perform the functionality of a

device, multicasting notification messages to inform its services.

When an UPnP device joins a local network, it first requests an IP address via DHCP. If no DHCP server responds, the device uses automatic IP addressing [4]. After obtaining an IP address, the device can advertise to and discover services from the local network. In the following part, we will describe five phases of interaction specified by the UPnP architecture, these phases depict how service is discovered and operated in an UPnP network.

**Discovery.** The UPnP discovery protocol is based on the Simple Service Discovery Protocol (SSDP). When a new device joins the network, it utilizes the UPnP discovery protocol to advertise its services to control points on the network. On the other hand, when a new control point joins the network, it applies the same protocol to search for services on the network. The discovery message employed by the protocol contains a few specific attributes of the device or one of its services, such as its type, identifier, and a pointer to more detailed information.

**Description.** After a control point has discovered a device, in order to interact with it, the control point must use a URL contained in the discovery message to request an XML-based UPnP description from the device, the description includes a device description and one or more service descriptions. The device description includes vendor-specific, manufacturer information such as the model name and number, serial number, manufacturer name, etc. The device description also includes a list of services provided by the device, as well as URLs for control, eventing, and presentation. Each service has a service description which includes a list of the actions to which the service responds, and arguments for each action, and a list of state variables.

**Control.** After a control point has retrieved a description of the device, the control point can invoke actions from services provided by the device. Actions are invoked by sending a control message to the control URL obtained in the device description for the service. Control messages are expressed in XML using the SOAP and sent via HTTP requests; results and errors are returned via HTTP responses.

**Eventing.** As we stated before, an UPnP service description includes a list of state variables. The service publishes updates when these variables change, and a control point may subscribe to receive this information.

**Presentation.** The devices can also provide a presentation URL so that the control point can retrieve a page from this URL, allowing a user to view and control device from a Web browser.

## 2.3 Zeroconf

Devices that support Zeroconf [5, 6] use Multicast DNS to store service information in DNS resource records within a local network. Zeroconf employs DNS Service Discovery (DNS-SD) to allow applications to find the available instances of a particular type of service. DNS-SD is simpler and easier to implement than UPnP because it uses standard DNS programming interfaces, servers, and packet formats to browse the network for services. Zeroconf consists of three fundamental mechanisms.

- **Publication:** advertising a service.
- **Discovery:** browsing for available services.
- **Resolution:** translating service names to address and port numbers for use.

**Publication.** Multicast DNS (mDNS) provides the ability to do DNS-like operations on the local link. In addition, mDNS designates a portion of the DNS namespace to be free for local use, without the need to configure a conventional DNS server to answer for those names.

To publish a service, the device must register the service with a multicast DNS responder. After registration, the DNS responder will create a SRV record and a PTR record. There is also an optional TXT record which contains additional information for resolving or using the service.

The SRV record specifies information on available services, including service name, protocol (usually either TCP or UDP), domain name, TTL, port, target, etc. The target is the host name of the machine providing the service, and the port number identifies the UDP or TCP port for the service.

The PTR record only contains one piece of information: the name of the service. PTR record is significant for service discovery, which will be depicted later.

The TXT Record is similar to the corresponding SRV record, except containing a small amount of additional information about the service instance.

**Discovery.** DNS-based Service Discovery utilizes DNS records registered during publication for a specific type of service by querying for PTR records matching a service type. The multicast DNS responders of each device within the local network return PTR records with service instance names.

**Resolution.** To resolve a service to address and port numbers for use, an application performs a DNS look-up for a SRV record with the service name. The multicast DNS responder responds with the matching SRV record.

## 2.4 Summary

Above service discovery technologies share several design principle, particularly, both of UPnP and Zeroconf are aimed at solving the service discovery problem in a closed environment, such as home and small office, and they both utilize IP multicast, an approach that is not intended to support service discovery across the Internet. Therefore, they can not scale to service discovery between home networks.

# 3 Service Discovery between Multiple Home Networks

## 3.1 Usage Scenarios

Let us consider the following usage scenarios. The first one is controlling the home devices such as refrigerator and air-condition remotely. This can happen when you visit your friend's home or when you have your vacation in another house. The second one is watching video with a remote peer: the sender has a video and streaming server, and he wants to share his recording to friends. The third one is concerning

UPnP: since Nokia's N series smartphones utilize UPnP to share content stored on the phone with other UPnP devices and can access content on other UPnP devices, it would be nicer to share your home media content with your friends across the Internet without too much configuration.

### 3.2 Architecture Overview

As the above usage scenarios depict, the demanding for service discovery between multiple home networks is also increasing. Thereby, technologies that support announce and discover services between multiple home networks become also essential for home networking. Obviously, intercommunication and service discovery should be done via the public Internet.

Web Services [7] are typically utilized to discover services over the Internet. Its architecture focuses on interoperations among applications through the Internet standards such as WSDL and XML, thus different services can easily be intercommunicated regardless of underlying implementation details. However, Web Services technology is not suitable for home networking: firstly, the discovery and configuration process for UDDI, which is the service discovery protocol for Web Services, can involve programmers and administrators, thus too complex for home networking, which should keep the process of service discovery as simple and automatic as possible; secondly, Web Services require centralized management, e.g. a services directory, whereas in home networking, centralized network management is undesirable.

In the remaining paper, we will propose a gateway-based architecture for service discovery between multiple home networks across the Internet. Generally speaking, the architecture deploys a gateway which serves as a proxy for all services within its home network, thus reducing the complexity of communication between multiple home networks.

Furthermore, we simplify our architecture, which contains only two UPnP home networks, as shown in Fig. 1, and we assume that their gateways know IP address and port number of each other. We will discuss how they function within their local home networks, as well as how they intercommunicate. Then we will consider more complex situations, such as intercommunication between multiple home networks, and co-existence of different service discovery technologies within one local home network.

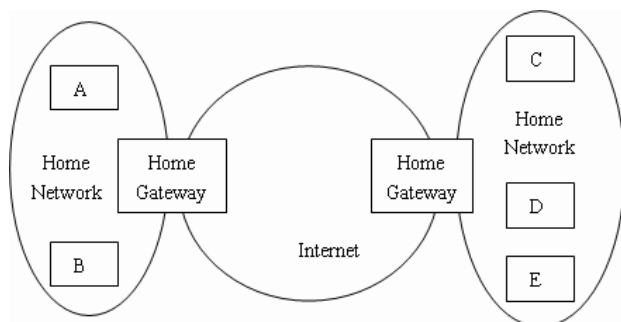


Figure 1: Home network architecture

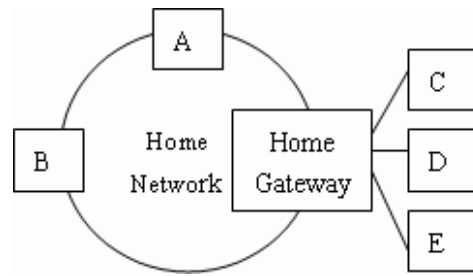


Figure 2: Gateway mapping mechanism

### 3.3 Gateway Architecture

There are several advantages of utilizing gateways [8]. Particularly, a gateway can be served as a proxy. As Fig. 2 describes, through some mapping mechanisms, devices and services in remote home networks will map to the gateway device, meaning that they will have the same IP address as the gateway when local devices want to communicate with them, hence the remote devices are available within the local UPnP network but are separated at the gateway side.

In this way, the gateway actually performs the NAT [9] functionality involving the mapping of port numbers, since devices with a local home network tends to have private IP addresses. As Fig. 2 depicts, firstly, since all remote devices appear as local devices by using the local gateway's IP address, different remote devices are distinguished by port numbers; secondly, the local gateway maps the addresses of different devices to the IP addresses of their corresponding gateways, for instance, the gateway maps the address of remote device C to C's gateway's IP address, and the remote gateway further maps device C's IP address to C's original address, probably a private address.

An UPnP proxy deployed in the gateway is defined in [8]. The UPnP proxy will be responsible for collecting local services, as well as mapping remote services to the local network. In the following, we will investigate how the UPnP proxy enables home-to-home service discovery by applying complementary mechanisms to the UPnP protocol.

**Discovery.** The UPnP proxy is responsible for collecting all available services within the local home network, thereby, it behaves as a control point, searching services by multicasting the discovery message. Then it will generate a list of local services, so when two home networks initialize communication, only the gateways need to exchange the lists, thus reducing the overall traffic. After the gateway receives the list of services from remote home network, it will publish these services to local home network by multicast, following the mapping mechanism presented above. Furthermore, when a local device queries some specific services, the gateway will answer it on behalf of remote devices if there are matched services.

Additionally, since the home network is highly likely to be dynamic, meaning devices will connect and disconnect at any time, how to synchronize the list of services between different home networks become a significant issue.

**Description.** Since all remote devices are mapped as local ones in the gateway, the device description of the UPnP Proxy comprises two parts: one part is the description of

the UPnP Proxy itself; the other is a device list of all remote UPnP Proxies and their connected devices and services. Furthermore, retrieving a remote UPnP device description, typically by sending an HTTP GET request, is pointed at the local UPnP Proxy, in other words, interested control points can request for the device and service description of a remote device locally. Therefore, before publishing a new remote UPnP device within the local network, it is essential for the local UPnP Proxy to acquire its device and service description at first.

**Control.** When the local device wants to use some remote services, the local gateway will tunnel the requesting packet to the remote gateway, which will then relay the packet to the corresponding device. As illustrated in section 2.2, actions to request the services are invoked by sending a SOAP-based control message to a corresponding control URL via HTTP request, typically by POST method. Therefore, only the control URL of HTTP header needs to be changed through above tunneling procedure, control message itself remains the same. Additionally, the delivery of response messages will apply the same tunneling mechanism.

### 3.4 Intercommunication between Multiple Home Networks

In the above discussion, we simply assume that two gateways know IP address and port number of each other. However, to be practical and scalable, we need a more sophisticated approach to initiate, manage and terminate the intercommunication between multiple home networks.

[10] presents a SIP-based approach for wide-area networked appliance communication, and it particularly describes problems associated with remotely accessing networked appliances, thereby, the solution can be also applied to the situation of home-to-home communication and our gateway architecture.

SIP [11] is suitable for initiating, managing and terminating the intercommunication between multiple home networks, for it allows abstract naming and can carry a flexible payload. When gateways initiate the communication, one gateway sends an INVITE message, in which the name of the gateway is identified as SIP URL, and signaling messages to be exchanged between gateways can be included in the SIP body.

In [10], the gateway serves as a SIP proxy, since the remote device directly access the home devices. However, in our architecture, home devices are transparent to remote devices, since they are mapped to the IP address of the gateway, therefore, we simply let the gateway serve as SIP user agent, as show in Fig. 3.

Furthermore, [10] also presents the support for notification and eventing. SIP utilizes two methods, namely, SUBSCRIBE and NOTIFY to achieve such asynchronous communications. This facilitates eventing between gateways, for instance, a gateway notifies the new service lists to another one.

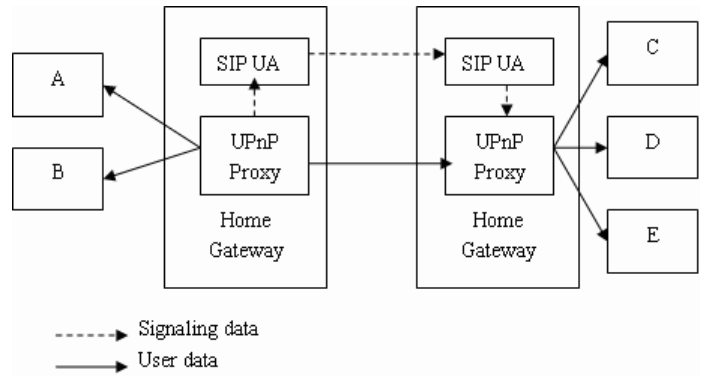


Figure 3: Gateway as SIP UA

## 4 Architecture Analysis

### 4.1 Advantages of Service Gateway

In section 3.3, we mentioned one particular advantage of utilizing gateway, namely, it can be served as a proxy, which can map remote devices and services on the gateway. And since home devices are usually assigned private addresses, such benefit is quite obvious.

However, comparing to other devices such as the bridge and router which can serve the similar functionality, what is the benefit of using the gateway? An obvious difference is that gateways work at the application layer while routers operate at network layer and bridges are at link layer, therefore, it is easier to interconnect two or more different protocols using gateways, in our case, they are SIP and UPnP. Additionally, in practice, when a variety of service discovery protocols are used on home networks to enable communication between devices, the advantage of using gateways is more prominent. We will further discuss the interconnection between multiple these protocols in section 4.4.

### 4.2 Home Networks Management

How to manage the list of peer home networks is another problem. It is likely that home users are usually not willing to share their services with anyone in the Internet, on the contrary, they may determine with which home networks they would like to share services, as well as determine whether to accept the request from other home networks. Therefore, unlike automatic service discovery within a home network, service discovery between home networks should not be done completely automatically. In addition, users should also be able to configure which services to share outside.

[12] suggests an Internet service provider that provides SIP services, such as the VoIP network operator, can support the home network environment without any modification, as well as assign SIP URL for networked appliance such as our gateway product.

### 4.3 Security

Our gateway architecture has not covered security yet. Obviously, security mechanisms are essential to protect the home-

to-home communication. For signaling data, SIP can provide both authentication and encryption. However, sometimes critical user data may also need encryption. [15] introduces a VPN-based approach to address this problem. Since a VPN can send data, especially media data, across secured and encrypted private channels between two points, it is possible to protect the home networks.

However, how to integrate VPN in home network products is a question. Since VPN is typically used by companies or organizations, thus might be too heavyweight for home users; and furthermore, the operating system of the gateway must support IPsec in order to run VPN, and because supporting IPsec needs to modify the IP stack, the gateway product has to be tight to some specific platforms.

Therefore, alternative lightweight security mechanism may be better for home networks. Since the service discovery between multiple home networks is done via the Internet, TLS [16] seems to be a reasonable choice. Firstly, it is application-level protocol, thus independent from Operating Systems, and no need to change the IP stack; secondly, when compared to IPsec VPN technologies, TLS has some inherent advantages in firewall and NAT traversal. Nevertheless, PKI is required to provide mutual authentication, thereby, different gateway vendors have to negotiate to select a common trusted third party.

#### 4.4 Interaction between Multiple Service Discovery Protocols

The above architecture assumes that the local home network only consists of UPnP devices. However, in practice, home devices may support different service discovery technologies, such as UPnP [3], Zeroconf [5], Jini [17], and Bluetooth SDP [18]. Therefore, the gateway should also enable interoperability among these different technologies.

The Open Services Gateway Initiative (OSGi) [14] technology provides specifications for home network gateways which coordinate many device technologies and enable compound services across different networking technologies. OSGi specifies only the API, not the underlying implementation, consequently, OSGi gateway is platform independent.

For a home network that consists of several subnetworks, each of which has its own discovery technology, the OSGi gateway can bridge higher-layer discovery protocols by importing services from different discovery protocols and register them as generalized OSGi services, thus allowing different discovery protocols to interact with one another.

A further question is how to integrate OSGi gateway and proxy components seamlessly. It is possible that each service discovery protocol needs a proxy component deployed in the gateway, similar to the UPnP proxy we discussed in section 3.3. Further research is needed to address the problem.

## 5 Conclusion

In this article we present a gateway-based architecture for service discovery between multiple home networks. A service gateway is a central element of the home network. It integrates various protocols used on home networks, discov-

ers and manages appliances, serves as a proxy for all services within its home network, and protects security. The gateway can be a home server, PC, or other device. SIP is used for initiating, managing and terminating the intercommunication between multiple home networks, and an Internet service provider that provides SIP services may be involved to assign SIP URL for home networks. In addition, TLS is utilized to protect critical user data while OSGi is used to bridge different discovery protocols. Future work includes: synchronizing the list of services between different home networks, and integrating OSGi gateway with proxy components seamlessly.

Our discussion about service discovery is limited to the scope of home-to-home communication. However, the proposed gateway architecture can be applied to other applications as well. Home network services, such as AV home networking, home automation, VoIP, home security, and networked sensors (e.g. checking gas meter), are often provided by different service providers via the Internet. And because of heterogeneous network architecture and networked home appliances, various providers usually provide services using their own service platform. Our gateway architecture can facilitate the cooperation between heterogeneous technology standards. Related research has been conducted by NTT Cyber Solutions Labs, which have developed a service aggregation platform that can provide a uniform service distribution framework [19].

## References

- [1] Sandy Teger, David J. Waks. End-User perspectives on Home Networking. April 2002. IEEE Communications Magazine.
- [2] Feng Zhu, Matt W. Mutka, Lionel M. Ni. Service Discovery in Pervasive Computing Environments. 2005 IEEE. IEEE CS and IEEE ComSoc.
- [3] Brent A. Miller, Toby Nixon, Charlie Tai, Mark D. Wood. Home Networking with Universal Plug and Play. December 2001. IEEE Communications Magazine.
- [4] Ryan Troll. Automatically Choosing an IP Address in an Ad-Hoc IPv4 Network. IETF draft, draft-ietf-dhc-ipv4-autoconfig-04.txt.
- [5] David Stirling and Firas Al-Ali. Zero Configuration Networking. June 2003. ACM Crossroads.
- [6] Heath Johns. Understanding Zeroconf and Multicast DNS. O'Reilly Network.
- [7] Web Services, W3C. <http://www.w3.org/2002/ws/>
- [8] Gertjan Bogers. UPnP-JXTA Bridging. <http://www.win.tue.nl/~mtjiong/EES5413/>
- [9] P. Srisuresh, Jasmine Networks, K. Egevang. Traditional IP Network Address Translator. January 2001. RFC 3022.

- [10] Stan Moyer, Dave Marples, Simon Tsang. A Protocol for Wide-Area Secure Networked Appliance Communication October 2001. IEEE Communications Magazine.
- [11] Henning Schulzrinne, Jonathan Rosenberg. The Session Initiation Protocol: Internet-Centric Signaling. October 2000. IEEE Communications Magazine.
- [12] Toru Okugawa, Hitoshi Masutani, Ikuo Yoda. A Home Network Service Environment for Wide-Area Communications October 2005. 2005 Asia-Pacific Conference on Communications, Perth, Western Australia.
- [13] NTT Develops "Home Service Harmony," a Service Control Platform based on Network Management Technologies <http://www.ntt.co.jp/news/news04e/0403/040308.html>
- [14] Pavlin Dobrev, David Famolari, Christian Kurzke, Brent A. Miller. Device and Service Discovery in Home Networks with OSGi. August 2002. IEEE Communications Magazine.
- [15] Kwan Wu Chin, Arthur Dimitrelis, John T. Judge, Andrew E. White. Setting Up a Name Resolution System for Home-to-Home Communications. US Patent Application Publication, US 2005/0066041 A1.
- [16] T. Dierks, C. Allen. The TLS Protocol Version 1.0. January 1999. RFC 2246.
- [17] Sun Microsystems, Jini Network Technology. <http://www.sun.com/jini>
- [18] Eugene A. Gryazin. Service Discovery in Bluetooth. Released at TKK Tik-86.174 "Bluetooth technology and utilization" course, 09.11.2001, Helsinki, Finland. Published at NEC CiteSeer, Scientific Literature Digital Library. <http://citeseer.nj.nec.com/392311.html>
- [19] Akihiro Tsutsui. Management Architecture and Distribution Framework for Home Network Services. NTT Cyber Solutions Labs.