Service Portability of Networked Appliances

Stan Moyer, Dave Marples, Simon Tsang, Abhrajit Ghosh
Telcordia Technologies, Inc., 445 South St., Morristown, NJ 07960
[stanm|dmarples|stsang|aghosh]@research.telcordia.com

Abstract

This document outlines an approach for delivering services to Networked Appliances using techniques that allow mobility of these services both in a conventional location independent sense and between physical devices. Key requirements to address this market are identified and the document then goes on to present a technical solution to meet these requirements together with worked examples. It concludes with suggestions for further work.

1 Introduction

Networked Appliances are popularly viewed as one of the next major Internet growth areas. Example appliances include an alarm clock that can adjust its wake-up time based on your calendar, current weather and traffic conditions and an Internet-enabled home security system which allows you to see the people approaching your home when you are in the office. Another example, seen in a recent US TV advertisement, is a refrigerator that reports to a service station when it needs maintenance, without ever needing to inform the owner. The application of Internet technology to appliance devices opens up whole new vistas of opportunity, the extent of which we can only guess at today.

For the purposes of our work, a Networked Appliance (NA) is considered to be *a dedicated function consumer device with an embedded processor and a network connection.*

Often, the end-user service is tied to the actual appliance (as in the case of the Internet Refrigerator), and provides an enhancement to the functionality of the device, which is at a specific fixed location. There are, however, many instances where the service can be separated from the physical appliance. A good example of this is the Internet Alarm Clock [1]. In this case the service itself is the 'first class citizen' and the appliance is simply a convenient way to present, or *render*, the service for presentation to a user. Indeed, when the service is separable from the appliance, the network architecture and protocols should help enable this *Service Portability*, allowing the service to be rendered onto any suitable delivery platform. For example, the service that automatically starts your coffee maker in the morning should work whether you are at home or in a hotel room. The Alarm Clock should also work no matter if you are in New York or London.

This portability brings with it many fringe benefits; the end user is no longer tied to a particular physical location, upgrades can be done centrally and a rental rather than sale revenue model becomes more practical to give but three examples.

This paper describes a network architecture and protocol that supports both of these dimensions of service portability - *device portability* and *location independence*. These portable services bring with them many challenges, but even more opportunities.

2 Implementing Portability

Portability, both in terms of device and location, implies a large number of requirements. In this section these requirements, and the reasoning behind them, is presented. Following on from this, an architecture capable of meeting the identified requirements is presented, based on the IETF Session Initiation Protocol (SIP) [3].

2.1 Requirements

More information about each of the requirements in this section is available to the interested reader in [7].

2.1.1 Naming and Addressing

Since both the location of the device and the physical device itself can vary, the naming and addressing scheme adopted must be capable of supporting both *location* and *device* independence.

- A NA must be assigned a generic globally unique name such that any communicating entity can unambiguously refer to it.
- There must be support for classification of addresses and selection between multiple instances. For example, it must be possible to search for "all lamps" or to allow refinement of a search to a particular lamp.
- It must be possible to search for particular capabilities and to identify which NAs possess those capabilities.

- The number and type of NAs available within an environment may not be known a priori so a mechanism must exist to browse for available NAs and/or capabilities using a well-known language/naming schema.
- The movement of NAs within a given domain and across domains should not be restricted.
- Support must be provided for locating and accessing NAs as they move across different domains.

2.1.2 Security Considerations

Since a multiplicity of NAs may exist within any given environment, each with it own capabilities, it is easy to recognize the requirement for effective security;

- When Networked Appliances first enter any environment, they and their users must be authenticated and authorized.
- Authentication, authorization, privacy and replay protection are required in all communications.
- To prevent eavesdropping and the malicious creation of 'home contents' lists, message contents and target device name must not be susceptible to eavesdroppers.
- Authorization checks may be performed at different granularity levels. Examples include: per registration (visit), per message or periodically based on a timer.
- Support for audit capabilities must be provided so that traceback and fault control can be performed.
- Non-repudiation must optionally be supported in all communications.

2.1.3 Wide-area Accessibility

In order for one of the true values of this new service model to be realized it is necessary to be able to access NAs in a controlled fashion from outside of the local domain (e.g. house);

- NAs must be accessible from outside of the home environment.
- For NAs without sophisticated networking capabilities, an appliance controller may be used to provide interworking (proxying) between the NA and external networks.
- Only a subset of the NAs within a domain may need to be addressable from outside of it. It should be possible to query the domain to be able to discover the externally accessible devices.

2.1.4 Protocol Transparency and Independence

Since the service presentation from the wide area will not necessarily know the exact characteristics and capabilities of the target device which is being used to render the service to the user it is important that the wide area communication is independent of any particular or specific protocol implementation;

- It must be possible to work with different in-domain networking technologies transparently. This requirement applies to both physical networking and application networking technologies.

2.1.5 Communication Protocol Requirements

The communication protocol used for communication with NAs must support all of the different operational modes that NAs may wish to present;

- The communication protocol must provide a flexible payload that will allow the transport of commands to, and responses from, individual NAs.
- The protocol must support efficient messaging for control. It is expected that control messages for NAs will be short and may or may not form part of an ongoing dialogue.
- The communication protocol must be able to encapsulate various appliances characteristics such as the fact that some appliances may act and respond immediately, while others may only respond after a non-determinate amount of time.
- Support for the following communications modes is required:
    - **Control:** e.g. *Turn on the outside light*.
    - **Queries:** e.g. *What is the temperature in the house?*
    - **Asynchronous events (notification):** e.g. *Notify me when the security alarm goes off*.
    - **Discovery:** e.g. *What device can meet requirement X?*
    - **Description:** e.g. *What features can device X support?*
    - **Media streaming (sessions):** e.g. *View the babysitter-cam*.

2.2 Architecture

Figure 1 presents an example of a home-based appliance network, with services provided by a network-based

service provider. Network-based service providers are key in enabling portability. They provide:

- Support for mobility — i.e. *device portability* across physical locations.
- Higher reliability and availability than would be cost-effective for a single endpoint.
- Optimal bandwidth utilization.
- Economies of scale in service and server administration.

The role of the Service Providers in the network can be split into two parts, the Application Service Provider (ASP) provides the platform for service logic execution and will most probably be constant for a given service. The Network Service Provider (NSP) is responsible for the transport infrastructure from the ASP to the NA, and may vary for a given service, especially if the NA is mobile.

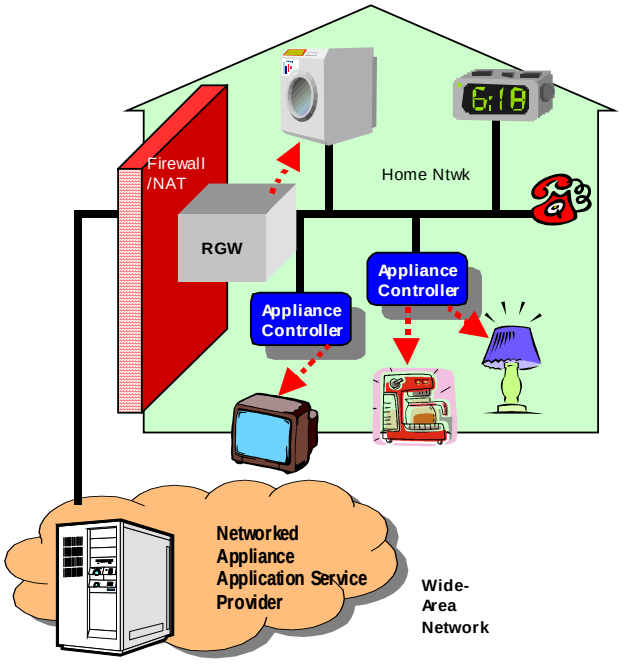

Figure 1. Architecture for Service Portability

An ASP providing a service to a NA needs to address service portability issues if they wish to deliver the service to a number of potentially different devices. If the service is 'tied' to a single NA (as in the case of the refrigerator) then these issues are not important.

ASP services may vary based on the current geographical or logical location of the user at a given point in time. This implies a need to determine geographical location as well as the capabilities of devices at a particular location.

In the case of a mobile user, the ASP may need to maintain session state so that a suspended or interrupted session could be continued later. This resumption could be from a different device at a possibly different location. Such a session store could be provided by a Network Service Provider (NSP) and could be updated by the NSP based on appliance location so that the ASP could resume a session in a location independent manner, although it is more likely that the ASP would maintain session state explicitly.

Many networked appliances will make use of wireless network connections. Such links may well exhibit low bandwidth, lossy, characteristics. The ASP may make use of compression and retransmission services to communicate effectively with appliances that use such networks, and may also devolve processing down to the appliance in order to maximize availability. This is inevitably a design time tradeoff – in a typical Networked Appliance as much processing as possible should be performed by the supporting network in order that costs can be amortized across multiple endpoints. The ASP would need to rely on the NSP to provide a bandwidth optimized communication path to the Networked Appliance even in the face of appliance mobility.

The same ASP service could be rendered to a diverse collection of appliances. In this case it is essential for the ASP to be able to obtain a set of device capabilities from a list of device profiles to provide a meaningful service.

Within the home, a Residential Gateway (RGW) provides secure access to the wide-area network (e.g. the Internet) and the ASP within that network. At a minimum, the RGW provides firewall capabilities, and may additionally provide Network Address Translation (NAT), application, NA and IP interworking capabilities. Appliances that are IP capable may connect to the RGW through a home local area network (LAN). Non-IP appliances will connect to the LAN through appliance controllers, which will provide interworking capabilities.

2.3 Network Protocol

We propose the IETF Session Initiation Protocol (SIP) [2][3] to meet the requirements identified above. Figure 2 illustrates how SIP can be used to support networked appliance services in the home scenario presented in Figure 1.

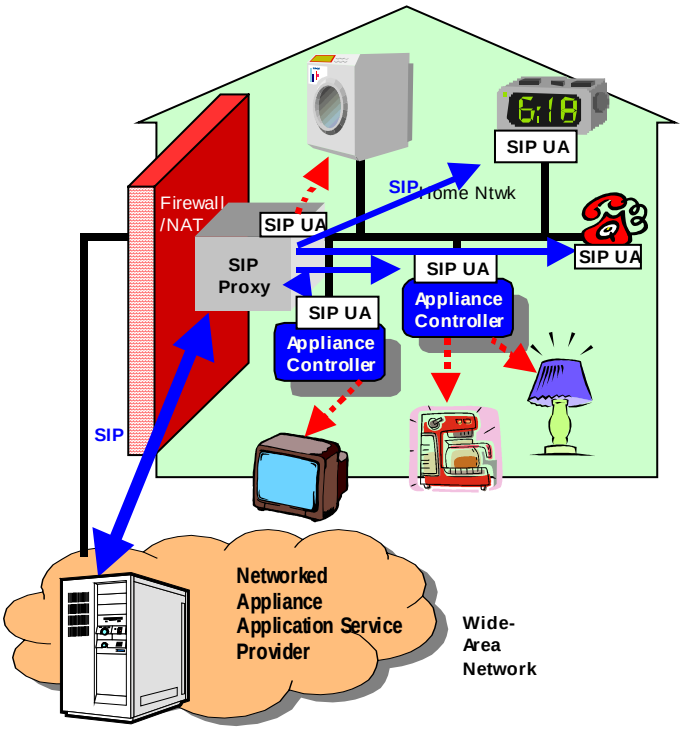

Figure 2. Use of SIP for Service Portability

No modifications are needed to SIP, though some of the extensions specified in the sip-impp drafts [4][5] are required, specifically the new methods MESSAGE, SUBSCRIBE, and NOTIFY. MESSAGE is required to support simple, datagram-style messaging and SUBSCRIBE and NOTIFY are required for asynchronous event notifications.

To better meet the naming and addressing requirements for NAs, a modified SIP URL addressing scheme [8] is proposed. A device naming scheme (e.g. Service Location Protocol (SLP) URL) is encoded to the left of "@" sign in the To: field. This may then be encrypted to ensure privacy. For example:

```
[slp:/d=lamp,r=bedroom,u=stsang]@simon.home.net
```

where the information in the square brackets would be BASE-64 encoded and (optionally) encrypted.

In addition, a new payload type, specific to devices, is required. A new MIME type, called Device Messaging Protocol (DMP), is proposed to carry the information required to excite NAs and which can carry responses back to the originator. There is no reason that other payloads (e.g., SOAP [9]) could not be carried too (either as another MIME type or as part of the DMP).

3 Examples

This section provides examples of how SIP supports service portability of networked appliance services and meets the requirements identified above.

In this example a network-based alarm clock service attempts to deliver a wake-up alert and announcement (containing the latest news, traffic, and weather conditions) to the user. The premise is that the user has previously configured the service to be delivered to him/her. The 'alarm clock' used to deliver the service does not have to be a physical clock, but simply a device, discovered by the service, capable of receiving an audio stream. This demonstrates *device portability*. SIP is used to set-up the audio session. The network-based alarm clock service provider, alarmclock.net, establishes the audio session and plays the audio announcement(s) at the appropriate wake-up time (e.g., configured through the user's personal calendar and adjusted based on current traffic and weather conditions). The example message flows are depicted in Figure 3 and described in detail below. Note that the portion of the addresses in [square brackets] in the examples would likely be encrypted for privacy, but have been left in clear-text for these examples.

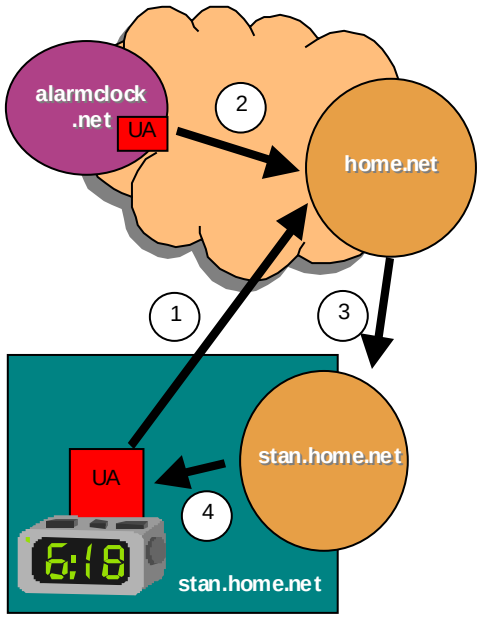

Figure 3 . Alarm Clock Service Message Flow

```
1.  REGISTER registrar@home.net
    To:
    [slp:/d=alarmclock,r=bedroom,u=stanm]@ua.stan
    .home.net
    From:
    [slp:/d=alarmclock,r=bedroom,u=stanm]@ua.stan
    .home.net
    Content-type: application/ddp
    [Device Address]
```

2. INVITE
sip:[*slp://d=alarmclock,r=bedroom,u=stanm*]@home.net SIP/2.0
From: sip:announcement@alarmclock.net
To:
sip:[*slp://d=lamp,r=bedroom,u=stanm*]@stan.home.net
Via: alarmclock.net
Content-type: application/sdp
[SDP for uni-directional RTP stream]

3. INVITE
sip:[*slp://d=lamp,r=bedroom,u=stanm*]@stan.home.net SIP/2.0
From: sip:announcement@alarmclock.net
To:
sip:[*slp://d=lamp,r=bedroom,u=stanm*]@stan.home.net
Via: home.net
Via: alarmclock.net
Content-type: application/sdp
[SDP for uni-directional RTP stream]

4. INVITE
sip:[*slp://d=lamp,r=bedroom,u=stanm*]@ua.stan.home.net SIP/2.0
From: sip: announcement@alarmclock.net
To: sip:
sip:[*slp://d=lamp,r=bedroom,u=stanm*]@stan.home.net
Via: stan.home.net
Via: home.net
Via: alarmclock.net
Content-type: application/sdp
[SDP for uni-directional RTP stream]

A response is returned to the alarm clock service provider containing the clock's RTP parameters. An audio stream is then initiated to the alarm clock from the service provider.

The next part of this example illustrates *location independence*. In this step, the user is staying over at a friend's house and would like the alarm clock service to wake them up there. So, the user either (1) brings the alarm clock from home to his friend's house and registers it there or (2) uses his friend's alarm clock and registers it with his own ASP. Figure 4 illustrates the SIP message flows for this service portability example, and the detail of each message is shown below.

1. REGISTER sip:registrar@home.net SIP/2.0
From: sip:[*slp:/d=alarmclock, r=bedroom,u=stanm*]@ua.stan.home.net
To: sip:[*slp:/d=alarmclock, r=bedroom,u=stanm*]@ua.stan.home.net
Contact: * ; expires=0

This first REGISTER message, cancels the previous registration for the alarm clock. Obviously this message needs to be authenticated and authorized.

2. REGISTER sip:registrar@home.net SIP/2.0
From: [*slp:/d=alarmclock, r=bedroom,u=stanm*]@ua.stan.home.net
To: sip:[*slp:/d=alarmclock, r=bedroom, u=stanm*]@ua.stan.home.net
Contact: sip:[slp:/d=alarmclock, r=guest_bedroom, u=stanm]@ua.dave.home.net
Content-type: application/ddp
[Device Description follows here]

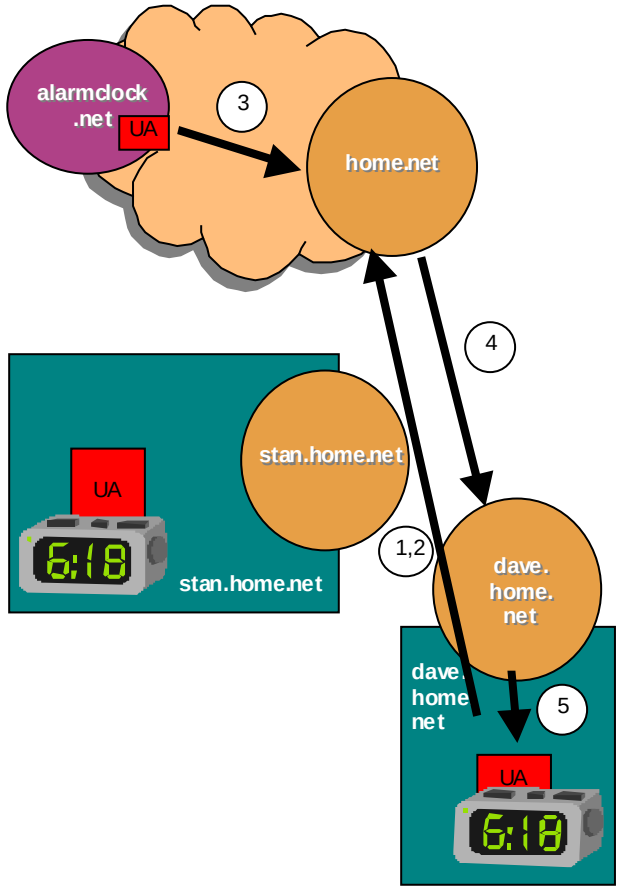

Figure 4 . Service Portability SIP Message Flow

This second REGISTER message registers the alarm clock in the guest bedroom of Dave's house as the device that should receive requests for the alarm clock in Stan's house.

3. INVITE sip:[*slp://d=alarmclock, r=bedroom, u=stanm*]@home.net SIP/2.0
From: sip:announcement@alarmclock.net
To: sip:[*slp://d=lamp, r=bedroom, u=stanm*]@stan.home.net
Via: alarmclock.net
Content-type: application/sdp
[SDP for uni-directional RTP stream]

The SIP Proxy in home.net looks up

[slp://d=lamp, r=bedroom, u=stanm]@stan.home.net

…and determines that this device is at

[slp://d=alarmclock,r=guest_bedroom,u=stanm]
@ua.dave.home.net

So it forwards the message to the SIP Proxy at dave.home.net;

4. INVITE sip:[*slp://d=lamp, r=guest_bedroom, u=stanm*]@dave.home.net SIP/2.0
   From: sip:announcement@alarmclock.net
   To: sip:[*slp://d=lamp, r=bedroom, u=stanm*]@stan.home.net
   Via: home.net
   Via: alarmclock.net
   Content-type: application/sdp
   [SDP for uni-directional RTP stream]

5. INVITE sip:[*slp://d=lamp, r=guest_bedroom, u=stanm*]@ua.dave.home.net SIP/2.0
   From: sip: announcement@alarmclock.net
   To: sip: sip:[*slp://d=lamp, r=bedroom, u=stanm*]@stan.home.net
   Via: dave.home.net
   Via: home.net
   Via: alarmclock.net
   Content-type: application/sdp
   [SDP for uni-directional RTP stream]

A response is then returned to the alarm clock service provider with the alarm clock's RTP parameters and an audio RTP stream is initiated (sent to the alarm clock in Dave's guest bedroom).

4 Future Work

In order to produce an inter-operable and open framework, detailed designs and specifications of the SIP message payloads for device control and device registration will be produced. The relevance of, and relationship to, other protocols – such as SOAP [9] and UPnP [10] – are being assessed and will be included into the framework described in this paper if appropriate. The possibility of interworking the SIP based service portability framework with the Open Services Gateway Initiative (OSGi [11]) framework is under investigation and the roles and capabilities that can be provided by the home gateway will also be evaluated.

5 Summary

The context of this work is wide area access and interworking of networked appliances. The results of early work show that portability of service functionality, both between devices, and in a more conventional mobility sense, is capable of being addressed using powerful but straightforward techniques that were originally developed for significantly different application.

6 References

[1] S. Moyer and D. Marples, "The Internet Alarm Clock - A Networked Appliances Case Study," White Paper, http://argreenhouse.com/iapp/ac-whitepaper.pdf, March 2000.

[2] S. Moyer et al., "Framework Draft for Networked Appliances using the Session Initiation Protocol," Internet Draft draft-moyer-sip-appliances-framework-00.txt, July 2000.

[3] M. Handley, H. Schulzrinne, E. Schooler, and J. Rosenberg, "SIP: session initiation protocol," Request for Comments (Proposed Standard) 2543, Internet Engineering Task Force, March 1999.

[4] J. Rosenberg et al., "SIP Extensions for Instant Messaging," Internet Draft draft-rosenberg-impp-im-00.txt, June 15, 2000.

[5] J. Rosenberg et al., "SIP Extensions for Presence," Internet Draft draft-rosenberg-impp-presence-00.txt, June 15, 2000.

[6] E. Guttman, C. Perkins, J. Veizades, and M. Day, "Service Location Protocol, Version 2", Request For Comments 2608, June 1999

[7] S. Tsang et al, "Requirements for Networked Appliances: Wide-Area Access, Control, and Interworking", Internet Draft draft-tsang-appliances-reqs-01.txt, September 2000.

[8] E. Guttman, C. Perkins, and J. Kemp, "Service Templates and Service: Schemes", Request For Comments 2609, June 1999.

[9] N. Pearson, "SIP and SOAP", Internet Draft draft-deason-sip-soap-00.txt, June 2000.

[10] Universal Plug and Play, http://www.upnp.org

[11] Open Services Gateway Initiative, http://www.osgi.org