Internet Engineering Task Force
Internet Draft
draft-tsang-sip-appliances-do-00.txt
November, 2000
Expires: May, 2001

Simon Tsang
Stan Moyer
Dave Marples
Telcordia Technologies, Inc

Henning Schulzrinne
Columbia University

Arjun Roychowdhury
Hughes Software Systems

SIP Extensions for Communicating with Networked Appliances

STATUS OF THIS MEMO

Abstract

A variety of technologies are available to network appliances and provide home automation and control. However, these do not support wide-area access control and interworking of these Networked Appliances (NA). This document describes a new SIP method, DO, that allows a SIP UA to communicate with NAs.

1. Introduction

There are numerous technologies for networking and controlling appliances within a home. Some examples are X.10 [6], OSGi [1], HAVi [2], VHN [3], and UPnP [4]. However, there is currently no support

for wide-area access communication or control of these Networked

Appliances (NAs) from the Internet, or for interworking the various home networking technologies. The ability to provide such support will radically enhance the ability to provide exciting new services [10][11].

The Session Initiation Protocol (SIP) (RFC 2543) [7] is an ideal protocol for supporting wide-area communication and interworking of NAs. SIP, as defined in the RFC, meets many of the requirements [11] for communicating with NAs: security, authentication, reliability, scalability, universal addressing, support for call setup, and personal mobility.

This document describes a new SIP method æDOÆ for enabling wide-area communication between user agents and NAs. The DO method carries messages or requests for NAs in the body of the DO request, and delivers it into the home environment where the message or request is rendered. The method does not result in a session set up, and can be used within or without an existing session. Examples of DO use include: sending application requests to NAs, updating NA information, and querying the status of NAs.

It should be noted that DO can be used in conjunction with other SIP methods to support wide-area communication between NAs. However, this draft focuses only on the definition and use of DO.

2. Terminology

In this document, the key words æMUSTÆ, æMUST NOTÆ, æREQUIREDÆ, æSHALLÆ, æSHALL NOTÆ, æSHOULDÆ, æSHOULD NOTÆ, æRECOMMENDEDÆ, æMAYÆ, and æOPTIONALÆ are to be interpreted as described in RFC 2119 and indicate requirement levels for the protocol.

3. Definitions

802.11	Wireless LAN networking technology.
Bluetooth	Wireless technology for networked devices.
Domain	An administrative IP domain.
HAVi	Home Audio Video Interoperability: A consortium of audio-visual electronics manufacturers who have developed a common, openly-licensable specification for networking digital home entertainment products.
OSGi	Open Services Gateway initiative: An industry group working to define and promote an open standard for connecting smart consumer and small business appliances with commercial internet services.
Jini	Java based device connectivity and discovery framework.

NA Networked Appliance: A dedicated function consumer devices containing at least one networked processor.

NAT	Network Address Translator.
RGW	Residential Gateway: Point of networking and control access to/from a home environment. The RGW may contain additional functions, such as firewalls and NATs.
Salutation	An open service discovery and session management protocol developed by the Salutation Consortium.
SIP UAC	SIP User Agent Client
SIP UAS	SIP User Agent Server
UpnP	Universal Plug and Play: An open architecture for connectivity of PCs of all form factors, intelligent appliances, and wireless devices.
VHN	Video Electronics Standards Association (VESA) Home Networking: Networking and control for video appliances developed by the VESA consortium.
X.10	Early power line based home networking technology.

4. Overview of Operation

Figure 1 illustrates an example of using the Session Initiation Protocol to communicate with NAs.

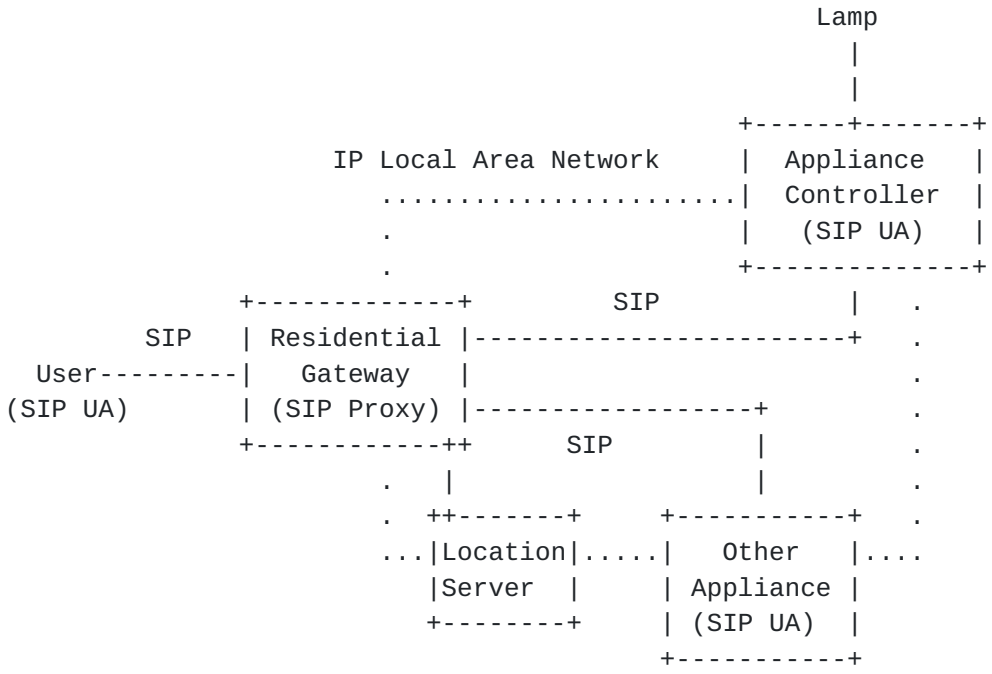

Figure 1: Example architecture using SIP to control NAs

The key components of the architecture are now described.

Residential Gateway (RGW):	The RGW provides IP connectivity outside of the home environment. All external access to the home will be made through the RGW. The RGW will provide a SIP

proxy for handling SIP requests and responses
to/from the home. Additionally, the RGW may provide
firewall and network address translator (NAT)

functions.

Appliance Controller:	The appliance controller enables non-IP devices (e.g., X.10) to be controlled from an IP network. It provides interworking between the IP local area network and the non-IP devices. The Appliance Controller comprises a SIP UA and a device controller, and performs SIP to device protocol interworking.
Lamp:	The lamp is an example of a non-IP appliance. It is controlled by the user on an IP network through the Appliance Controller.
Other Appliance:	Other appliances will be connected in the home environment. This one uses a SIP UA to allow users to control it from the wide-area IP network.
User:	A user controls NAs in the home environment over a wide-area IP network via a SIP UA.
Location Server:	The location server is a database which provides the SIP proxy with information on how to route incoming or outgoing SIP messages.
IP local area network:	The IP local area network in the home network environment connects together the RGW, IP appliances and Appliance Controllers. A variety of networking technologies may be employed. Examples are: 802.3, 802.11, and Bluetooth [8].

Figure 2 shows an example message flow for wide-area NA control.

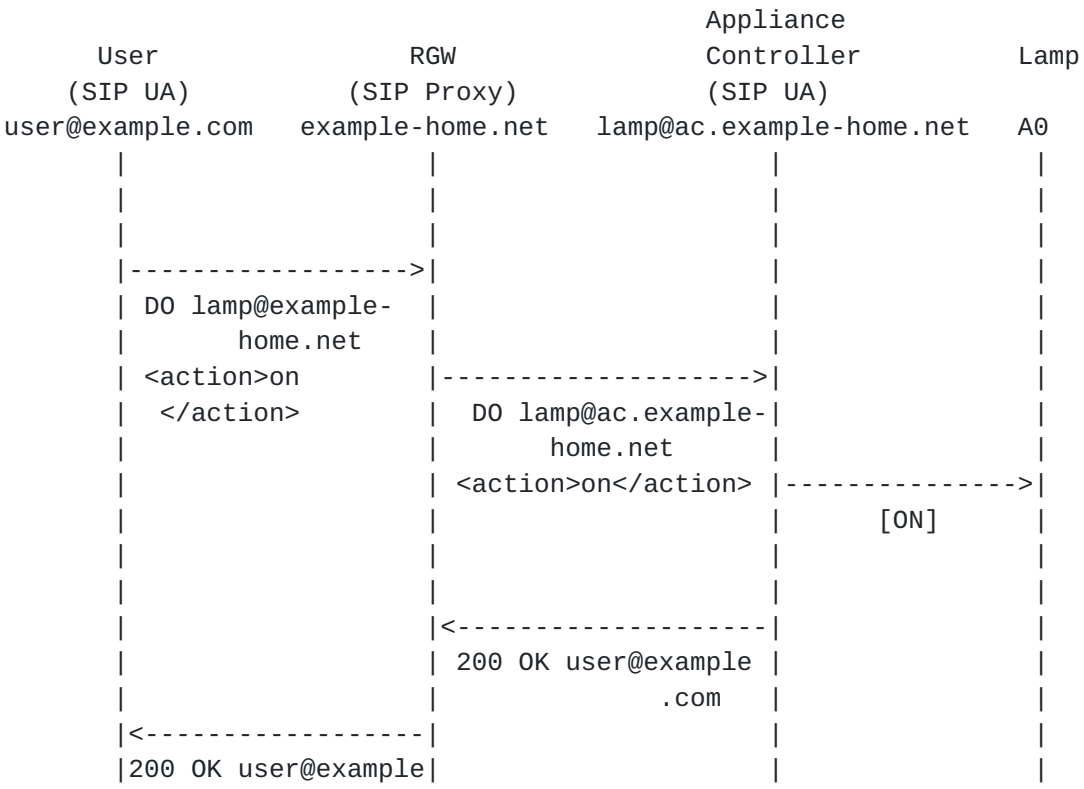

Figure 2: Example message flow for wide-area NA control

In this scenario, a user (SIP UA address user@example.com) remotely turns on a lamp in the home with domain name example-home.net. The Appliance Controller has a SIP UA with SIP address lamp@ac.example-home.net.

The body of the DO message sent by the user contains XML describing the action to be performed by the NA. When the Appliance Controller receives the DO message, it must interpret the action specified in the DO body and send the appropriate command to the lamp (e.g., ôONö). The Appliance Controller will then respond with 200 OK to the user to indicate that the action has been performed.

5. DO Method Definition

This specification defines a new SIP method, DO. The purpose of DO is to enable messages or requests to be sent to NAs without setting up a new session. However, DO can be used within the context of an existing session, and will share the same Call ID as the existing session. The message or request will be carried in the body of the DO message. The BNF for this method is:

Do = "DO"

5.1. Header Field Support for DO Method

The following table is an extension of tables 4 and 5 in the SIP specification. Refer to the SIP Specification for a description of the content of the table.

Header	Where	enc.	e-e	DO
Accept	R		e	o
Accept	415		e	o
Accept-Encoding	R		e	o
Accept-Encoding	415		e	o
Accept-Language	R		e	o
Accept-Language	415		e	o
Allow	200		e	o
Allow	405		e	m
Authorization	R		e	o
Authorization	r		e	o
Call-ID	gc	n	e	m
Contact	R		e	m
Contact	2xx		e	o
Contact	3xx		e	o
Contact	486		e	o
Content-Encoding	e		e	o

Content-Length	e	e	m
Content-Type	e	e	*

Cseq	gc	n	e	m
Date	g		e	o
Encryption	g	n	e	o
Expires	g		e	o
From	gc	n	e	m
Hide	R	n	h	o
Max-Forwards	R	n	e	o
Organization	g	c	h	o
Priority	R	c	e	o
Proxy-Authenticate	407	n	h	o
Proxy-Authorization	R	n	h	o
Proxy-Require	R	n	h	o
Record-Route	R		h	o
Record-Route	2xx,401,484		h	o
Require	R		e	o
Retry-After	R	c	e	-
Retry-After	404,413,480, 486	c	e	o
	500, 503	c	e	o
	600, 603	c	e	o
Response-Key	R	c	e	o
Route	R		h	o
Server	r	c	e	o
Subject	R	c	e	o
Timestamp	g		e	o
To	gc(1)	n	e	m
Unsupported	420		e	o
User-Agent	g	c	e	o
Via	gc(2)	n	e	m
Warning	r		e	o
WWW-Authenticate	R	c	e	o
WWW-Authenticate	401	c	e	o

Table 1. Summary of header fields. (1) copied with possible addition of tags; (2) UAS removes first Via header field.

5.2. Responses to DO Requests

A 200 OK response is sent if the DO request was successful. The message body MAY include additional information to reflect the result of the successful DO request, such as current device status.

Request Failure (4xx), Server Failure (5xx) and Global Failure (6xx) responses can also be sent for the DO Request.

5.3. Message Body Inclusion

DO requests SHOULD contain a message body, which contains information

on the action to be performed by the NA. This document does not specify the format for the DO message body, which may depend on the application domain. For Networked Appliances, there is an

investigation underway to define a Device Messaging Protocol (DMP) MIME type that can be used as a DO message body.

5.4. Behaviour of SIP User Agents

The protocol processing rules applied by the SIP User Agent (UA) are similar to those for non-INVITE requests. DO requests do not set up sessions and do not require session state to be maintained. Each DO request MAY have a distinct Call-ID or several DO requests MAY share the same Call-ID. In the latter case, the receiving UA MUST enforce ordering. DO requests MAY be part of an INVITE-initiated session. (For example, a video camera could use DO requests, using a suitable message body, to control its pan, tilt and zoom operations.)

5.5. Behaviour of SIP Proxy and Redirect Servers

5.5.1 Proxy Server

The protocol rules applied by the SIP Proxy Server shall be similar to those applied used for any other SIP request.

Forking Proxy Server

The protocol rules applied by the SIP Forking Proxy Server are the same as for other non-INVITE requests.

5.5.2 Redirect Server

The protocol rules applied by the SIP Redirect Server shall be similar to those applied used for the INVITE request. The key difference is that the DO message shall not change the state of the session.

6. Security Considerations

Unauthorized use of networked appliances may cause injury or property damage. Thus, implementations SHOULD use authentication to ensure that only authorized entities control network appliances and that the message body cannot be altered without detection, as described in Section 13 of RFC 2543.

7. References

[1] OSGi, http://www.osgi.org
[2] HAVi, http://www.havi.org
[3] æVHN Home Network,Æ EIA 851, Version 1, to be released 4Q00, See http://www.vesa.org for further information.
[4] UPnP, http://www.upnp.org

[5] Jini, http://www.jini.org
[6] X.10, http://www.x10.org

[7] 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.
[8] Bluetooth, http://www.bluetooth.com
[9] Salutation, http://www.salutation.org
[10] S. Moyer et al, ôFramework Draft or Networked Appliances using the Session Initiation Protocolö, Internet Draft, Internet Engineering Task Force, July 2000. Work in progress. http://www.argreenhouse.com/iapp/draft-moyer-sip-appliances-framework-00.txt
[11] S. Tsang et al, ôRequirements for Networked Appliances: Wide-Area Access, Control, and Interworkingö, Internet Draft, Internet Engineering Task Force, September 2000. Work in progress. http://www.argreenhouse.com/iapp/draft-tsang-appliances-reqs-01.txt
[12] http://www.w3.org/XML/

8. Author's Contacts

Simon Tsang
Telcordia Technologies
445 South Street
MCC 1E 206R
Morristown, NJ 07960, USA.
e-mail: stsang@research.telcordia.com

Stan Moyer
Telcordia Technologies
445 South Street
MCC 1A-238R
Morristown, NJ 07960, USA.
e-mail: stanm@research.telcordia.com

Dave Marples
Telcordia Technologies
445 South Street
MCC 1J-226B
Morristown, NJ 07960, USA.
e-mail: dmarples@research.telcordia.com

Henning Schulzrinne
Department of Computer Science
Columbia University
M/S 0401
1214 Amsterdam Avenue
New York, NY 10027-7003, USA.
e-mail: hgs@cs.columbia.edu

Arjun Roychowdhury
Hughes Software Systems

Prestige Opal
146 Infantry Road
Bangalore 560001, India.
e-mail: archow@hss.hns.com