Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 9, 2009

M. Baugher
Cisco
E. Nedellec
Orange Labs
M. Saaranen
Nokia
B. Stark
AT&T

March 8, 2009

IPv6 Services for UPnP Residential Networks
draft-bnss-v6ops-upnp-01.txt

Status of this Memo

Copyright Notice

Abstract

This paper considers some IPv6 issues for residential networks, including address scoping and firewalls. The paper describes IPv6 usage in the UPnP Forums's Device Architecture standard; some clarifications and changes are considered. The paper seeks comments on IPv6 address usage, address selection, and the need to develop best practices for IPv6 firewall traversal.

Table of Contents

1. Background 4
   1.1. UPnP and the UPnP Forum 4
   1.2. UPnP on IPv6 5
   1.3. UPnP Security 5
   1.4. Goals of This Document 5
   1.5. Overview of This Document 5
   1.6. Conformance Language 6
2. Requirements 7
   2.1. Private Network Addressability 7
   2.2. Outside-In Access 8
   2.3. Firewall 8
   2.4. Cross-Site Services 9
3. Issues 10
   3.1. Addressing Issues 10
   3.2. Firewall Issues 10
   3.3. Issues List 11
      3.3.1. Routed private networks 11
      3.3.2. Remote access 11
      3.3.3. Site to site access 11
      3.3.4. Firewall control 11
4. Solution Space 12
   4.1. Routed Private Networks 12
   4.2. Remote Access Addressing 12
   4.3. Firewall Control 13
   4.4. Site to Site Access 13
5. Security Considerations 14
   5.1. Assets, Risks and Threats 14
   5.2. Authentication and Authorization 14
   5.3. Problems with Password-based Authentication 15
   5.4. Authenticated Firewall Access 15
6. Summary 16
7. Acknowledgements 17
8. Informative References 18
Authors' Addresses 21

1. Background

This paper considers IPv6 usage in the UPnP(TM) Device Architecture (UDA) [UDA1.1]. Three IPv6 issues for the UDA are described below. Briefly stated, the latest revision of the UPnP Device Architecture deprecates Site-Local Unicast Addresses in accordance with the evolving IPv6 standard [RFC4291] and replaces it with global addresses; the UDA needs to recommend proper usage of IPv6 Unique Local Unicast Addresses (ULA) and Global Unicast Addresses (GUA) in UPnP Site-Local Multicast announcements. Second, new services such as remote access can potentially use alternative IPv6 address types such as ULA or GUA, and the best choices need to be determined. Third, UPnP IPv6 usage is affected by IPv6 firewall policy. The paper focuses on these three IPv6 usage and support issues.

UPnP IPv6 usage and support become more important as dual-stack UPnP devices become more common. A variety of UPnP Device Control Protocols (DCPs) are shipped in tens of millions of devices throughout the world. UPnP DCPs can therefore greatly affect the worldwide deployment of IPv6. This section gives background on UPnP and then describes the goals of the present work.

1.1. UPnP and the UPnP Forum

The UPnP Forum is an industry consortium of companies whose engineers create interoperable standards for PCs, TVs, network storage, and other electronic devices. These standards are for both fixed-location and mobile devices that operate on private networks. Future remote access services, moreover, will operate over the public Internet to securely connect a remote device to a private network [UPnPWC]. UPnP protocols perform device discovery, service description, service control, eventing, and presentation [UDA1.1][UDA1.0] for audio/video, automation and network gateway services, to name a few. The UPnP Internet Gateway Device (IGD) DCP, for example, defines an IPv4 network address translation (NAT) traversal service that is found in most residential IPv4 NATs [UPnPIGD].

The UPnP Device Architecture (UDA) is an ISO/IEC standard (ISO/IEC 29341) that can run over IPv4 or IPv4/IPv6 dual stack. UDA 1.1 is the latest version and is a backward-compatible extension to UDA 1.0. Both versions support a "two-box" configuration of a controlled device ("device") that accepts actions from a controlling device, called a "control point" ("CP"). UPnP also supports a "three-box" configuration where a CP can control one device on behalf of another device. The three-box configuration is used in the UPnP Audio/Video Architecture, for example, where a CP controls A/V sessions between a media server and a renderer [UPnPAV].

1.2. UPnP on IPv6

The UPnP Forum does not specify IPv6 customer premises equipment (CPE) such as cable or DSL modems and refers to other standards organizations for the definition of IPv6 and other basic networking services[BBF][Cable][SW][W]. The UPnP Forum specifies "control interfaces" to IPv4 and dual-stack devices on private networks, such as residential networks that have Wi-Fi and Ethernet local area networks. The UPnP protocol standard today supports IPv6 "dual stack" operation, but IPv4 is mandatory in the UPnP Device Architecture (UDA). Thus, a UPnP device that announces its services and provides them over IPv6 will simultaneously do so over IPv4 as well. Dual stack operation is transparent to UPnP applications except for address selection and usage.

For IPv4, the UPnP discovery protocol, "Simple Service Discovery Protocol," (SSDP) uses an administratively-scoped multicast address assigned by IANA to UPnP; in UDA 1.1, eventing uses a second, IANA administratively-scoped multicast address[IANAIPv4]. For UPnP dual stack operation, IANA reserves IPv6 link-local and variable scope multicast addresses for UPnP[IANAIPv6].

1.3. UPnP Security

Authenticated services are rare on residential networks today. More often than not, the owner of an "unmanaged residential network" [RFC3750] does not know how to configure it. This applies to access controls as well, which are often not used by people who really need them. This is despite the fact that the UPnP Device Security specification was published several years ago to overlay authorization and authentication on UPnP services. The lack of such security resulted in some well-publicized attacks on UPnP devices in recent years [Hemel][FlashAttack]. These attacks can be prevented by effective access controls for services, including IPv6 firewall interfaces.

1.4. Goals of This Document

This paper seeks comments from the IETF on private-network application of IETF IPv6 standards, notably the use of scoped unicast addressing [RFC5220][RFC4193][RFC4007][RFC4291] and the need to establish best practices for IPv6 firewalls and interfaces.

1.5. Overview of This Document

Section 2 considers some requirements for UPnP "dual stack" operation and IPv6 services. Section 3 describes the UPnP "dual stack" issues. Section 4 proposes solutions. Section 5 is Security Considerations,

and section 6 gives the Summary.

1.6. Conformance Language

There is no normative language used in this paper, which is informative only.

2. Requirements

Many of the requirements that are described here for UPnP are generic to residential networks and to many types of private networks. The focus of this paper is UPnP, however, so no attempt is made to survey the differences with Bonjour, sensor networks, various home automation protocols, or other systems that share some requirements with UPnP but which are nonetheless different protocols. Our requirements are for UPnP dual-stack operation and are listed in the following sub-sections. This is not a complete list since most requirements are satisfied by existing IPv6 standards. Rather, the following are requirements that might have different potential solutions given existing standards and practices.

2.1. Private Network Addressability

Most residential networks today consist of a single local area network or a few LANs that are bridged to share a common, administratively-scoped IPv4 address space. Many believe that this is the way it should be and advocate that a single-subnet configuration should be a best practice for small, private networks like residential networks. In IPv6 terms, this would mean that multiple wired and wireless interfaces on the gateway/router would be reachable using link-local scope, which is the only scope that is mandated in the UPnP Device Architecture [UDA1.1][UDA1.0]. Conversely, if the gateway/router managed the multiple network interfaces as distinct sub-networks (links), UPnP messages sent to link-local scope would be confined to a single sub-network and not reach the entire residential network. Vendors and service providers are aware of the connectivity problems that occur when IPv4 network devices are misconfigured to support "nested NATs" resulting in multiple subnets in the home. In the case of IPv4, there is no remedy but to re-configure the residential network. This level of management is beyond what most home users are willing or able to perform, but proper configuration is needed for full connectivity within the residential network. For example, users may want an Ethernet-connected printer to interoperate with a personal computer on the Wi-Fi network.

Traffic that is wholly within the residential network is uncommon today. Published studies have shown that Wi-Fi, Ethernet and other networks in U.S. homes generally provide only Internet access to personal computers. With the possible exception of printing, there is little or no intra-network traffic, and people routinely use email or web sites to transfer files between computers in the home. The problems of multiple subnetworks or "nested NATs" are not all that apparent for Internet access from inside the home. There is a definite trend in new products, however, to support intra-network

transfers such as to network attached storage and for media streaming within the residence. These applications are common among early adopters.

The authors are not aware of any compelling need today for UPnP home networks to be routed rather than bridged. There might be a future need for connecting local and personal area networks that use 64-bit Medium Access Control addressing [RFC4944], however, and protocols that accommodate a variety of network types, topologies and equipment are highly desirable. For this reason, it is taken as a requirement to support routed residential networks.

2.2. Outside-In Access

There are emerging applications that connect a mobile device across the public Internet to a device on a private network, such as to a network attached storage device in the residence. IPv4 applications support this today using such means as Dynamic DNS coupled with a NAT port mapping from a public IPv4 address to an administratively-scoped address on the residential network. UPnP has an IPv4 NAT traversal service that has the side-effect of allowing forwarding through a residential firewall [UPnPIGD]. A similar capability is needed for IPv6. To match the IPv4 service, IPv6 residential gateways need to support "outside-in" access from the public Internet to a private network.

2.3. Firewall

This paper assumes that residential gateways will initially deploy IPv6 firewalls that functionally match IPv4 firewalls. For outside-in access, this functionality filters tuples of addresses and upper-layer protocol values from the IPv6 headers [W] [NSA]. For outside-in (i.e. "inbound") traffic, this means that "...The general operating principle is that transport layer traffic is only permitted into the interior network of a residential IPv6 gateway when it has been solicited explicitly by interior nodes" [W].

Thus, if the residential gateway hosts an IPv6 firewall, then a firewall traversal method is needed by residential network applications to permit external devices to connect to them for so-called "outside-in" access. Unauthenticated IPv4 NAT traversal is common today: There are typically no access controls used for dynamic IPv4 NAT traversal. Should this practice be continued in IPv6? An authoritative best practices standard for firewalls is needed to answer this question. As a start, this paper takes as a requirement that four alternative configurations need to be supported for most residential-network firewalls.

1. Firewall allows all unsolicited traffic through to any device on the residential network

2. Firewall blocks unsolicited traffic and any application can open pinholes

3. Firewall blocks unsolicited traffic and only authorized applications can connect (or open a pinhole)

4. Firewall blocks unsolicited traffic and no outside application can connect (or inside application can open a pinhole)

The Security Considerations of section 5 considers attacks where the first two configurations are practically identical in terms of risk. The third configuration requires a method for strongly identifying, authorizing, and authenticating users and their devices. The third configuration has different solutions such as "authenticated firewall traversal" using an authenticated VPN connection [W], or "authenticated firewall control" by which an application on the inside is authorized and authenticated to open forwarding to its IPv6 transport address.

Another type of remote access allows common services to operate over multiple private networks and is described next.

2.4. Cross-Site Services

Remote Access services can be much more ambitious than simply connecting a single device to some other device on the residential network: Commercial products today can permanently interconnect multiple devices on two or more residential networks, such as for "wellness" monitoring of remote family members or for sharing a media library. In this case, a device on one private network is authorized to share designated services that are hosted on another private network. Whereas "outside-in" access is typically session-based access, cross-site services are permanent.

3. Issues

There are two classes of issues. The first concerns use of IPv6 link-local, site-local, unique-local and global addresses. The second concerns firewall policy. Each are discussed in a separate section below and followed by a summary "Issues List".

3.1. Addressing Issues

UPnP operation on IPv6 has been changed between the two versions of the UPnP Device Architecture (UDA). The principal change is in IPv6 address usage. UDA 1.0 mandates the use of Link-Local Unicast Addresses and allows use of Site-Local Unicast addresses; UDA 1.0 uses link-local and site-local multicast for its service discovery. UDA 1.1 dropped Site-Local Unicast Addresses in accordance with the standard [RFC3879] [RFC4291] but did not adopt Unique Local Unicast Addressing (ULA); this is an issue for routed local networks because link local addressing only works on a single subnetwork (link). Moreover, the UDA 1.1 IPv6 specification uses "global address" in place of Site-Local Unicast Address, which might imply that a global address allocation is needed for operation on a private network. A second issue is in the practical use of ULA and GUA in address selection [RFC5220][RFC3484]. When does the UPnP application choose to use ULA or GUA in a multicast announcement? UPnP address-scoping policy and dual-stack address selection usage may need to be clarified.

3.2. Firewall Issues

As discussed in the Requirements Section above, with an IPv6 firewall comes the need to allow some remote senders to connect from the outside to certain devices on the residential network. Section 2.3 describes the need to support authenticated access as one of several configuration options. This concerns network security policy and is considered in some detail in section 5, Security Considerations. Authenticated firewall access presents a problem for firewall vendors who need to offer a consistent level of security across multiple types of firewall interfaces such as UPnP and Bonjour, for example.

Perhaps the ideal solution would be for the industry to have one interface for IPv6 firewalls. It is likely that multiple protocols for firewall traversal or firewall control might be needed by the different applications that use them. If convergence to a single protocol proves unrealistic, convergence to a set of best practices might be very helpful.

3.3. Issues List

One issue described below stems from the need to define an IPv6 "site" as opposed to a "link" when the private network is routed across multiple subnetworks. A second issue is how to reach a site using IPv6, usually over an IPv4 tunnel. Another issue concerns offering application services over multiple private networks. Yet another issue is IPv6 firewall access. These are discussed below.

3.3.1. Routed private networks

UDA 1.1 mandates use of IPv6 link-local addressing and allows use of site-local multicast for UPnP service discovery but does not specify use of IPv6 Unique Local Unicast Addressing, which is needed for routed residential networks.

3.3.2. Remote access

A remote device can today use IPv4 addressing and Dynamic DNS to access a local network device; the local device uses a UPnP NAT traversal service. A remote IPv6 device can do the same, but the local IPv6 network needs an outside-in access method when there is an IPv6 firewall.

3.3.3. Site to site access

Local and remote IPv6 device can use global unicast IPv6 addresses for a single session. But what is the correct addressing model for a more permanent connection among multiple devices on two or more private networks?

3.3.4. Firewall control

A firewall vendor will need to support a consistent level of service across one or more firewall interfaces, and authenticated access is needed in the firewall.

4. Solution Space

To each of the issues listed above, one or more proposed solutions are given in this section.

4.1. Routed Private Networks

The authors assume that Unique Local IPv6 Unicast Addresses[RFC4193] are the successor to deprecated Site-Local Unicast Addresses [RFC3879][RFC4862]. RFC 3879 explains that a "site" is typically not well-defined. Specifically, sites can overlap; when this happens, unicast site-local addresses can collide. A Unique Local Unicast Address (ULA) contains a 40-bit random number that has a very low probability of colliding.

The motivation for using ULA is of course not security but simplicity of packet forwarding and filtering on a residential network that has multiple subnetworks.

Thus, ULA is preferable to "global addresses" for bridged and routed residential networks - provided a ULA prefix can be properly obtained. Dual stack Devices that comply with UDA 1.1, however, will continue to advertise "global addresses" (GUA) in site-scoped Simple Service Discovery Protocol (SSDP) announcements. UDA 1.0 Devices will advertise Site-Local Unicast Addresses. Dual stack devices on the market today are more likely to support Site-Local Unicast Addresses rather than ULA and so backward-compatibility is essential. A UDA 1.1 Control Point (CP) will accept a site-local unicast in a site-scope SSDP announcement, for backward compatibility, but a UDA 1.1 Device will send only a GUA in a site-scope SSDP announcement. Any backward-compatible revision of UDA 1.1 IPv6 usage, therefore, would require CPs to accept site-local unicast or a GUA in SSDP announcements, but a Device would send ULA, if one is available. If a ULA prefix cannot be acquired on the local network, then GUA would be preferred. IPv6 Address selection logic [RFC3484] thus needs to be specialized for UPnP.

4.2. Remote Access Addressing

The proposed addressing mode is Global Unicast Addresses (GUA) for session-based remote access of a single device into a home network. Since this type of UPnP remote access is performed on a transient, session basis, any needed firewall signaling can be performed at session-establishment time.

4.3. Firewall Control

One compelling solution for IPv6 firewall control is to leave it to the vendors who offer an IPv4 NAT traversal service (e.g. UPnP, Bonjour). This solution is compelling because it is inevitable and already happening in the industry. The industry would likely benefit, however, from a published consensus on best practices for stateless and stateful packet filtering [W] [NSA]. Authenticated firewall access and related issues are discussed below in section 5, Security Considerations.

4.4. Site to Site Access

ULA is one solution for offering and requesting services across two or more private networks. ULA seems to be a good choice for extending services across private networks in a static and transparent manner. Such transparency would be defeated by the need for explicit firewall signaling for each session across the private networks. How sites interconnect to form a single address scope for common services needs to be defined.

5. Security Considerations

This paper considers IPv6 address usage and IPv6 firewall policy. The security considerations of IPv6 addressing are relatively small; RFC 3484 describes an attack on host privacy in which an end system is forced to reveal its own source addresses [RFC3484]. The security considerations of IPv6 firewall control, however, are not so small. A firewall is a residential-network "asset" that depends on residential network security, which is described next.

5.1. Assets, Risks and Threats

Residential networks have critical assets such as gateway devices, personal computers, firewalls and network storage. Among the biggest risks to these assets are the re-configuration of network devices and theft of personal passwords. By re-configuring the DNS server name, for example, an attacker can do a pharming attack. A phishing attack steals passwords to get access to online banking accounts and password-protected devices. Malware is a well-known attack vector for pharming and phishing attacks [FlashAttack]. Computer viruses, trojan horses and other types of malware get routinely downloaded and installed on programmable devices in the residential network. Another attack vector is "war driving", which typically uses an open wireless LAN to gain access to a residential network device. An IPv6 firewall asset is therefore subject to these risks and threats.

5.2. Authentication and Authorization

Strong identification, authentication and authorization can prevent threats to residential networks from war drivers, visitors, and other interlopers who gain access through an open wireless LAN or other means. Also, malware can gain execution privileges on an authorized end system, such as a personal computer that can set the DNS name in a residential gateway. Thus, automated methods of authentication using public-key or secret key cryptography are sometimes insufficient. In the case of malware, multi-factor authentication such as device public-key authentication coupled with a user passphrase puts the user in the loop. Multi-factor authentication can potentially prevent malware from executing its actions on the host device. But there are human-factors problems when the user is in the authorization loop: The user might be conditioned to approve every action and type in a password whenever prompted to do so, for example. As discussed below, password-based authentication comes with additional risks.

5.3. Problems with Password-based Authentication

In general, passwords are a poor authentication method for IPv4 and dual-stack residential networks; this has been true for some time [Neumann][RT79]. And it is truer today given advances in hardware speeds and password cracking [Elcomsoft]. It is possible that advances in password security engineering can improve how people use passwords in an unmanged environment such as the home [Anderson]. Practically speaking, there is no proven, simple method to ensure that passwords are strong and unique across unmanaged residential-network devices. Use of identical and similar passwords for a variety of purposes such as for firewall control and online banking, increases the risks of password compromise. A combination of techniques such as public-key cryptography, passwords with password checkers, strong pre-shared symmetric keys, hardware token devices and other means are referenced in current standards [WPS] [UDS1.0]. These methods potentially apply to firewall access control as well.

5.4. Authenticated Firewall Access

Not all users of residential networks need or want security services. Many prefer to run open-wireless networks and some leave their firewalls turned off to enable convenient access to their residential network devices. The norm for residential gateway device vendors, however, is to ship their products with a firewall enabled. Thus, people who don't want security often need to use some form of authenticated access to disable it.

If by default, the firewall drops unsolicited external traffic but allows any internal device to open it to unsolicited traffic, then there is some question as to value of the firewall. Malware and war drivers will be able to open the firewall to their internal addresses - and in some cases to any address of their choosing. Thus, authenticated access is a reasonable default for an IPv6 firewall interface, but the application needs proper authentication. If the personal computer that controls the firewall is infected by malware, proper authentication might require user input or other methods.

Authentication and authorization are hard problems in un-managed networks. A one-time procedure is usually needed for a human user to prove locality or control as a precondition for an authorization [WE]. An initial authorization for a firewall control interface might be an authorization for packet forwarding for an internal IPv6 GUA according to some filtering specification, for example. A more privileged authorization might be to request packet forwarding for another device, such as a visitor to the residential network. Authorization levels as well as authentication methods need to be considered as part of IPv6 best practices for firewalls.

6. Summary

This paper defines a set of requirements for IPv6 applications, it lists the issues in meeting these requirements, and it describes some possible solutions. Section 4, Solution Space, describes solutions and identifies several new problems for further work. IPv6 Unique Local Unicast Addresses are a solution to site unicast addressing, but how to apply ULA to cross-site services is left as an open question in this paper. More practical experience is needed with UPnP dual-stack operation to understand how well address selection works for addressing scopes beyond link-local. For global access through a firewall, authentication is a required option. Thus, best practices for IPv6 firewalls would be very helpful to vendors and service providers. This paper considers only "outside in" firewall control. "Inside-out" firewalling is not properly considered in this paper.

7. Acknowledgements

The authors thank Jari Arkko, Fred Baker, Jean-Francois Cadiou, Ralph Droms, Eric Vyncke, Bruce Fairman, Thomas Herbst, Alan Messer, Toby Nixon, Dave Oran, Clarke Stevens, Tim Spets, Mark Townsley, Greg White and Dan Wing.

8. Informative References

[Anderson]
Anderson, R., "Security Engineering", 2001.

[BBF] Broadband Forum, "Functional Requirements for Broadband Residential Gateway Devices", TR-124 (http://www.broadband-forum.org/technical/download/TR-124.pdf)", December 2006.

[Cable] Cable Labs, "IPv4 and IPv6 eRouter Specification (http://www.cablelabs.com/specifications/CM-SP-eRouter-I03-070518.pdf)", May 2007.

[Elcomsoft]
Elcomsoft, "ElcomSoft Breaks Wi-Fi Encryption Faster with GPU Acceleration", October 2008.

[FlashAttack]
Gnu Citizen, "Flash UPnP Attack FAQ (http://www.gnucitizen.org/blog/flash-upnp-attack-faq/)", January 2008.

[Hemel] Hemel, A., "Universal Plug and Play: Dead simple or simply deadly? (http://www.upnp-hacks.org/sane2006-paper.pdf)", April 2006.

[IANAIPv4]
IANA, "IANA Multicast Address Assignment (http://www.iana.org/assignments/multicast-addresses)", January 2009.

[IANAIPv6]
http://www.iana.org/assignments/ipv6-multicast-addresses, "IANA IPv6 Multicast Address Assignment", January 2009.

[NSA] Potyraj, C., "Firewall design considerations for IPv6, NSA, Report #1733-041R-2007", October 2007.

[Neumann] Neumann, P., "Risks of Passwords (http://portal.acm.org/citation.cfm?id=175289)", April 1994.

[RFC3484] Draves, R., "Default Address Selection for Internet Protocol version 6 (IPv6)", RFC 3484, February 2003.

[RFC3750] Huitema, C., Austein, R., Satapati, S., and R. van der Pol, "Unmanaged Networks IPv6 Transition Scenarios",

RFC 3750, April 2004.

[RFC3879] Huitema, C. and B. Carpenter, "Deprecating Site Local Addresses", RFC 3879, September 2004.

[RFC3904] Huitema, C., Austein, R., Satapati, S., and R. van der Pol, "Evaluation of IPv6 Transition Mechanisms for Unmanaged Networks", RFC 3904, September 2004.

[RFC4007] Deering, S., Haberman, B., Jinmei, T., Nordmark, E., and B. Zill, "IPv6 Scoped Address Architecture", RFC 4007, March 2005.

[RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, October 2005.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

[RFC4864] Van de Velde, G., Hain, T., Droms, R., Carpenter, B., and E. Klein, "Local Network Protection for IPv6", RFC 4864, May 2007.

[RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, September 2007.

[RFC5220] Matsumoto, A., Fujisaki, T., Hiromi, R., and K. Kanayama, "Problem Statement for Default Address Selection in Multi-Prefix Environments: Operational Issues of RFC 3484 Default Rules", RFC 5220, July 2008.

[RT79] Morris, R. and K. Thompson, "Password Security: A Case History", November 1979.

[SW] Singh, H. and W. Beebee, "IPv6 CPE Router Recommendations (http://tools.ietf.org/html/draft-wbeebee-ipv6-cpe-router-03)", October 2008.

[TR-064] http://www.broadband-forum.org/technical/download/TR-064.pdf, "LAN-Side DSL CPE Configuration", May 2004.

[UDA1.0] UPnP Forum, "UPnP Device Architecture, Version 1.0 (http://www.upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v1.0.pdf)", 2008.

[UDA1.1] UPnP Forum, "UPnP Device Architecture, Version 1.1 (http://www.upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v1.1.pdf)", 2008.

[UDS1.0] Ellison, C., "DeviceSecurity:1 (http://www.upnp.org/standardizeddcps/documents/DeviceSecurity_1.0cc_001.pdf)", November 2003.

[UPnPAV] UPnP Forum, "UPnP AV Architecture:1 (http://www.upnp.org/specs/av/UPnP-av-AVArchitecture-v1.pdf)", September 2008.

[UPnPIGD] UPnP Forum, "UPnP Internet Gateway Device Standardized Device Control Protocol V 1.0 (http://www.upnp.org/standardizeddcps/)", November 2001.

[UPnPWC] UPnP Forum, "UPnP Working Committees (http://www.upnp.org/membership/committees.asp)", February 2009.

[W] Woodyatt, J., "Recommended Simple Security Capabilities in Customer Premises Equipment for Providing Residential IPv6 Internet Service, (draft-ietf-v6ops-cpe-simple-security-03)", July 2008.

[WE] Wlaker, J. and C. Ellison, "UPnP[TM] Security Ceremonies Design Document (www.upnp.org/download/standardizeddcps/UPnPSecurityCeremonies_1_0secure.pdf)", October 2003.

[WPS] Wikipedia, "Wi-Fi Protected Setup (http://en.wikipedia.org/wiki/Wi-Fi_Protected_Setup)", February 2009.

Authors' Addresses

Mark Baugher
Cisco
800 East Tasman Drive
San Jose, CA 95164
US

Phone: (503) 245-4543
Email: mbaugher@cisco.com

Erwan Nedellec
Orange Labs
4 rue du clos courtel
35510 Cesson-Sevigne,
France

Phone: +33 (0) 2 99 36 35 92
Email: erwan.nedellec@orange-ftgroup.com

Mika Saaranen
Nokia
Visiokatu 6
FIN33721 Tampere,
Finland

Phone:
Fax:
Email: Mika.saaranen@nokia.com
URI:

Barbara Stark
AT&T
725 W Peachtree St
Atlanta, GA 30076
US

Phone: +1 (404) 499-7026
Fax:
Email: barbara.stark@att.com
URI: