HOMENET
Internet-Draft
Intended status: Standards Track
Expires: May 10, 2013

D. Migault (Ed)
Francetelecom - Orange
W. Cloetens
SoftAtHome
P. Lemordant
Francetelecom - Orange
C. Griffiths
Comcast Cable Communications

November 6, 2012

IPv6 Home Network Front End Naming Delegation
draft-mglt-homenet-front-end-naming-delegation-01.txt

Abstract

CPEs are designed to provide IP connectivity to the Home Network. Most of the CPEs are also providing the IP addresses of the nodes of the Home Network. This makes CPEs good candidates for hosting the Naming Service that would make devices reachable from the Home Network but also from the Internet.

CPEs have not been designed to host a Naming Service reachable from the Internet. This would expose the CPEs and the Home Network to resource exhaustion which would result in making the Home Network unreachable, and most probably would also affect the Home Network inner communications.

This document describes an Front End Naming Architecture where the CPEs manage the DNS(SEC) zone for its Home Network, and outsource the zone to Public Server for resolution coming from the Internet.

The goal of the document is first to describe a Naming Architecture that fulfills Home Network Naming requirements without exposing the CPE to resource exhaustion. Then we intend the CPEs to be easily configured by the End Users, and describe the necessary information the End User is expect to provide to the CPE.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 10, 2013.

Copyright Notice

Table of Contents

1. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Introduction

IPv6 provides global IP reachability to almost all nodes of the Home Network even outside the Home Network. However End Users do not want to access to the Services hosted in the Home Network with IPv6 addresses, but prefer to use names.

CPEs are already providing IPv6 connectivity to the Home Network and generally provide IPv6 addresses or prefixes to the nodes of the Home Network. This makes the CPEs a good candidate to manage binding between names and IP addresses of the nodes. In other words, the CPE is the natural candidate for setting the DNS(SEC) zone file.

CPEs are usually low powered devices designed for the Home Network, but not for heavy traffic. CPEs can host the Naming Service for the Home Network but should not be exposed on the Internet. This would expose the CPE to resource exhaustion. As a consequence, it may isolate the Home Network from the Internet and affects the services hosted by the CPEs, thus affecting Home Network communications. As a result, CPE SHOULD NOT host the Naming Service of the Home Network for resolutions coming from the Internet.

In this document, we propose that the CPE sets the DNS(SEC) zone of the Home Network. The CPE may generate different zones one for the queries coming from the Home Network, and one for queries coming from the Internet. We respectively call these Zones Homenet View and Public View. The CPE hosts the Homenet View and responds to the associated DNS(SEC) queries coming from the Home Network. For queries coming from the Internet, the CPE outsources the Public View to Public DNS(SEC) Servers that responds to the queries.

This document describes the Front End Naming Architecture where the CPE hosts the Naming Service for the Home Network and outsources it for queries from outside the Home Network. We especially insists on the parameters the CPE requires to properly set up the Front End Naming Architecture.

Section 3 describes the Front End Naming Architecture requirements. Section 4 presents the different functional entities involved in the Front End Naming Architecture. Section 5 details configuration of the various functional entities as well as how they interact each

other.Section 6 is informative and sums up the different inputs the CPE requires from the End User to set up the Front End Naming Architecture. Section 7 positions the described architecture toward the Home Network Architecture. Finally Section 8 provides security considerations.

3. Front End Naming Architecture Requirements

This section lists and details goals and requirements of Front End Naming Architecture.

- REQUIREMENT 1: DNS(SEC) queries for subdomain of the Homenet Domain Name MUST be responded by the Public DNS(SEC) Servers when issued from outside the Home Network. CPE could hardly cope with heavy traffic coming from the Internet. To avoid exposing the CPE to resource exhaustion, the Naming Service is outsourced on the Public DNS(SEC) Servers for traffic coming from the Internet.

- REQUIREMENT 2: The CPE MUST NOT, by default, accept any DNS(SEC) queries from outside the Home Network. In some aspects, it rewords the previous requirement.

- REQUIREMENT 3: The IP address of the CPE SHOULD NOT be publicly published. This requirement avoids the DNS(SEC) queries incidentally ends up on the CPE.

- REQUIREMENT 5: DNS(SEC) queries for subdomain of the Homenet Domain Name MUST be responded by the CPE when issued from the Home Network. To guarantee the Home Network independence in case the Home Network has no connectivity on the Internet, the CPE MUST respond to DNS(SEC) queries for subdomain of the Homenet Domain Name coming from the Home Network.

- REQUIREMENT 6: The CPE MUST be able to update the Home Network Zone hosted on the Public DNS(SEC) Servers.

- REQUIREMENT 7: The CPE SHOULD be able to provide different views. At least the CPE should be able to handle a view for the Home Network nodes and a view for the nodes outside the Home Network. Home Network nodes that are not supposed to be reachable from outside the Home Network are not expected to be part of the latest view.

4. Front End Naming Architecture Presentation

This section describes the Front End Naming Architecture and defines the notations used in this document.

- Home Network: designates all devices that are behind and managed by the CPE.

- Internet: designates the network the CPE is attached to.

The CPE connects the Home Network to the Internet. Although the different functional entities listed below MUST NOT necessarily be hosted on the CPE, we assume in this document they are hosted on the CPE:

- Homenet Resolving Server: is the DNS Resolver Server of the Home Network. Typically its IP address is announced via DHCPv6. Most of DNS(SEC) queries from nodes on the Home Network are expected to be addressed to this Homenet Resolving Server. The Homenet Resolving Server is expected to receive queries only from the Home Network.

- Homenet Authoritative Server: is the Authoritative Server of the Home Network. This server hosts bindings between FQDNs and IP addresses. Unless cached, most of the DNS(SEC) queries sent from the Home Network that concerns a node in the Home Network are expected to be forwarded to this Homenet Authoritative Server. More specifically DNS(SEC) resolutions sent from the Home Network are expected to be sent to the Homenet Resolving Server. The Homenet Resolver Server is a forwarder and forwards to the Homenet Authoritative Server queries for domain names or subdomain of the Homenet Domain Name. For other resolutions, the Homenet Resolving Server proceeds to traditional DNS(SEC) resolutions over the public DNS(SEC) infrastructure.

- Homenet View: is the DNS(SEC) zone that contains all bindings between FQDNs associated to the Homenet Domain Name and IP addresses. The Home Network may have multiple views, but for most Home Networks, a single Homenet View is expected. Information of this Homenet View is only visible from the Home Network.

- Public View: is the view that contains the bindings between FQDNs and IP addresses. Unlike the Homenet View, the Public View is expected to be publicly published. The Public View contains information visible from the Internet. It is expected that the Public View is constituted by a subset of the names of the

Homenet View. More specifically, devices that are not expected to be reachable from the Internet should not be part of the Public View. In some implementations, the Public View may be equivalent to the the Homenet View. In this latter case Public Views and Homenet Views will be represented by a single file.

- Master Public Server: is the part of the CPE that deals with the Public view of the Home Network. The Master Public Server is in charge of providing the Public View to the Public DNS(SEC) Servers. It is not necessarily a DNS(SEC) server. However, in this document we are using DNS mechanisms to synchronize the Public View in the Public DNS(SEC) Servers and the Public View on the CPE.

- WAN Interface: the CPE Interface on the Internet.

- Homenet Interfaces: the CPE Interfaces on the Home Network. There might be a single or multiple interfaces.

The other involved entities are:

- Public DNS(SEC) Servers: are the servers on the Internet hosting the Public View of the Home Network.

- Homenet Node: a Node of the Home Network

- Node: a Node located on the Internet. This Node is expected to be in most of the cases a resolving server.

- Homenet Domain Name: The domain name associated to the Home Network. There may be one or multiple domain names.

Figure 1 illustrates how a DNS(SEC) resolution is performed from a Node in the Home Network or from a node on the Internet.

The Homenet Node sends a DNS(SEC) query to the Homenet Resolving Server (1). When the Homenet Resolving Server receives the DNS(SEC) it notices that query name is a subdomain of the Homenet Domain Name (example.com), and forwards the query to the Homenet Authoritative Server that hosts the Homenet View (2). The Homenet Authoritative Server sends the response to the Homenet Resolving Server (3), which finally sends the response to the Homenet Node (4).

For a node located on the Internet, the DNS(SEC) query is requesting the Public DNS infrastructure (.com) which redirects the DNS(SEC) query to the Public DNS(SEC) Servers (a). The Public DNS(SEC) Server sends the response back to the Node (b).

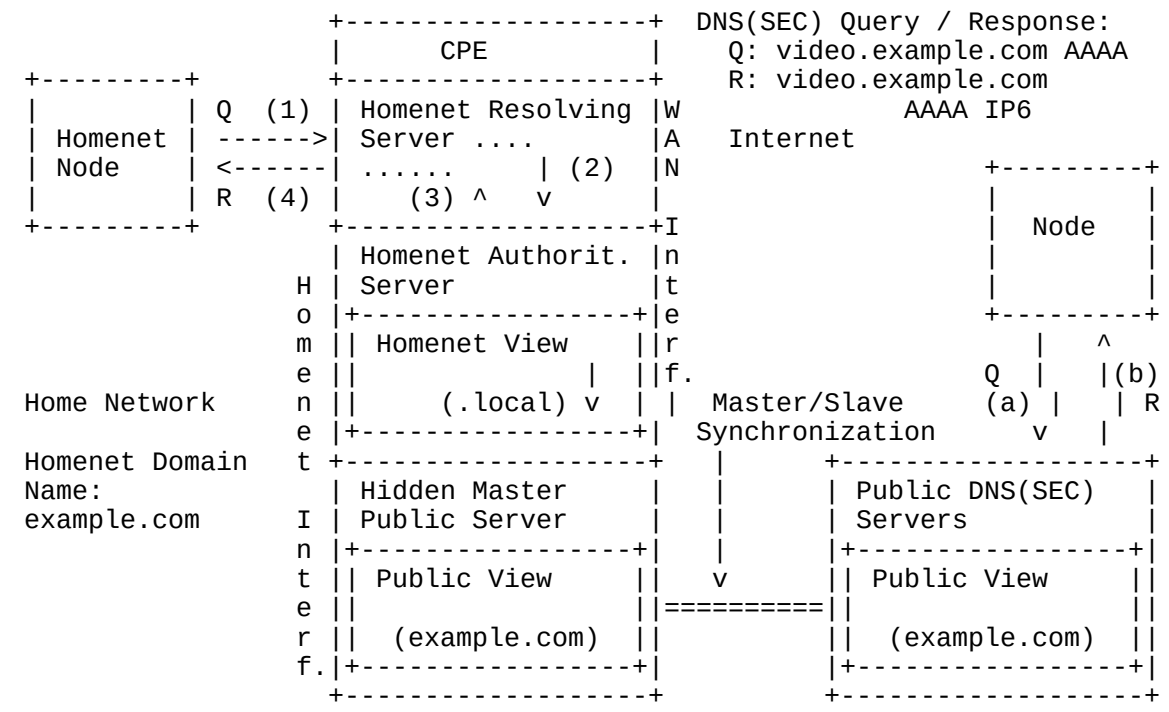

Figure 1: Front End Naming Architecture Description

5. Front End Naming Architecture Description

This section provides a more detailed description of the Front End Naming Architecture. More specifically it shows how the entities described in Section 4 are organized to fulfill the requirements of Section 3.

5.1. Setting the Homenet Authoritative Server

The Homenet Authoritative MUST be configured to reject any queries coming from outside the Home Network, i.e. not from the Homenet Interface. In other words, DNS queries related to the Homenet Domain Names MUST never be received from the WAN Interface.

5.2. Setting the Homenet View

The Homenet Authoritative Server may be authoritative for multiple Homenet Domain Names and each Homenet Domain Name may be associated with multiple views.

The CPE is expected to be provided the various Homenet Domain Names so it can properly generate the associated Homenet Zone files and the appropriate DNS(SEC) settings.

5.3. Setting the Public View

The Public DNS(SEC) Servers MUST handle all DNS(SEC) queries related to any Homenet Domain Names that are sent from outside the Home Network.

The CPE MUST generate the Public View. In the case of multiple Homenet Domain Names, multiple views MUST be generated, and in order to fill properly the SOA and NS field, the CPE must be provided for each Homenet Domain Name the corresponding Public DNS(SEC) name, and IP addresses.

5.4. Synchronizing the Public View

Uploading and dynamically updating the zone file on the Public Servers can be seen as zone provisioning between the CPE (Hidden Master) and the Public Server (Slave Server). This can be handled either in band or out of band. DNS dynamic update [RFC2136] may be used. However, in this section we detail how to take advantage of the DNS slave / master architecture to deploy updates to public zones.

The Public DNS Server is configured as a slave for the Homenet Domain Name. This slave configuration has been previously agreed between the End User and the provider of the Public DNS Servers. The CPE is hosting the Public Zone files associated to the various Homenet Domain Names and associated views. Each of these files are associated a Public Server. In order to set the master/ slave architecture, the CPE acts as a Hidden Master Public Server, which is a regular Authoritative DNS(SEC) Server listening on the WAN interface.

The Hidden Master Public Server is only expected to initiate AXFR [RFC1034], IXFR [RFC1995] transfers to configured slave DNS servers. The Hidden Master Public Server should send NOTIFY messages [RFC1996] in order to update Public DNS server zones as updates occur.

The CPE MUST be configured to send NOTIFY only when necessary. It is recommended for example that it checks first the SOA on the Public DNS Server before sending a NOTIFY. In other words, rebooting a CPE SHOULD NOT systematically trigger a NOTIFY message.

Hidden Master Public Server differs from the Homenet Authoritative Server by:

- Interface: the Homenet Authoritative Server listens on the Homenet Interface whereas the Hidden Master Public Server listen on the WAN Interface

- View: Homenet Authoritative Server hosts the names that are available on the Home Network, whereas the Hidden Master Public Server hosts the names that are publicly available. These two zones may differ since some of the nodes may not be reached from outside the Home Network.

- Traffic: Homenet Authoritative Server expects traffic from the Home Network, whereas the Hidden Master Public Server only accepts traffic from the Public Servers.

- Function: Homenet Authoritative Servers acts as an authoritative DNS Server on the Home Network, whereas the Hidden Master Public Server only synchronizes with the Public DNS Servers.

In this document, Master Public Server differs from the Homenet Authoritative Server as different functions. Both functions may be implemented by a single running instance of Authoritative Servers.

5.5. Securing the Synchronization

Exchange between the Public Servers and the CPE MUST be secured, at least for integrity protection and for authentication. This is the case whatever mechanism is used between the CPE and the Public DNS(SEC) Servers.

TSIG [RFC2845] can be used to secure the DNS communications between the CPE and the Public DNS(SEC) Servers. TKEY [RFC2931] can be used for re-keying the key used for TSIG. Using TSIG and TKEY requires that this mechanism is implemented on the DNS(SEC) Server's implementation running on the CPE. One disadvantage is that TKEY does not provides authentication mechanism, and the initial shared secret must be set manually.

Protocols like TLS [RFC5246] / DTLS [RFC6347] can be used to secure the transactions between the Public Servers and the CPE. Their use would require the implementations to integrate TLS/DTLS as a security layer. TLS/DTLS can use certificates to authenticate the Public Server and the CPE. For example, the certificates can be hosted on a dongle.

IPsec [RFC4301] IKEv2 [RFC5996] can also be used to secure the transactions between the CPE and the Public Servers. IKEv2 provides multiple authentications possibilities with its EAP framework. Then, IPsec security does not require any changes of the DNS applications.

For these reasons, we recommend using IPsec.

5.6. Setting the Homenet Resolution Server

The Homenet Resolving Server MUST be configured as a DNS forwarder. When a DNS(SEC) query coming from the Home Network concerns a Homenet Domain Name or a Homenet Subdomain Name, the resolution MUST be performed with the Homenet Authoritative Server. If the Home Network has multiple Homenet Domain Names, multiple forwarding rules may be applied.

To properly configure a basic configuration, the Homenet Resolving Server needs to be informed of the Homenet Domain Names and associated Homenet Authoritative Server. They may be one or multiple associated Homenet Authoritative Servers. The same Authoritative Naming Server may be used for multiple Homenet Domain Names.

5.7. Additional Views

In this document, we considered the Public and Homenet View. Each of these Views may have additional views.

6. CPE’s interface Recommendations

This section describes the various objects that are required to properly set the Front End Naming Architecture. This section is informational, and is intended to clarify the information handled by the CPE and the various settings to be done.

A Public Server is defined with the following information:

- Public Server Name: The associated FQDN of the Public Server

- IP addresses: The list of IP addresses associated to the Public Server. This list should not be provided by the End User. Instead, it should be provided by performing a DNSSEC exchange. If the Public Server Name DNS resolution cannot be performed with DNSSEC, then it is recommended to provide this field. This list of IP address is used to generate the Public View with the proper values for SOA and NS and associated AAAA fields.

- Public Server Management Name: The FQDN of the management interface. This Management interface designated who the CPE is synchronizing its Public View with.

- Public Server Management IP addresses: The list of IP addresses associated to the Public Server Management Name. This field is not expected to be filled by the End User, but to be derived from the Public Server Management Name with a DNS(SEC) query.

- Authentication Method: How the CPE authenticates itself to the Public Server.

- Authentication data: Associated Data.

To set a View one needs to have the following information:

- Homenet Domain Name: The Domain Name of the zone.

- Public Server Name (optional): The Server that are expected to host the View. It is required both to field the SOA, NS and associated AAAA as well as to define where the View has to be uploaded. If the View is the Homenet View and the Homenet Authoritative Server is hosted on the CPE, then, this information is not required.

- Rules: Defines specific rules for deriving the View. Example of rule s may be a list of FQDNs or IP addresses that MUST be included or removed...

- DNSSEC Data: DNSSEC data required to generate the DNSSEC zone. This can be the various DNSSEC Keys for example.

First the CPE MUST reject DNS queries received from the WAN Interface. Then the CPE MUST list the Homenet Views and Public Views. Homenet Views are those without the Public Server Name specified and are loaded on the Homenet Authoritative Server. The Homenet Resolving Server is configured as a forwarder for these Views. Public Views are loaded on the Master Public Server, the communications between the Master Public Server and the Public Servers are secured, with an IPsec authenticated and encrypted traffic flow for example.

7. Position toward Homenet Architecture

This section positions the Front End Naming Architecture toward the Naming recommendation of [I-D.chown-homenet-arch].

The Front End Naming Architecture has been designed to favor unmanaged operations. Naming configuration is automatically performed by the CPE.

The Front End Naming Architecture provides the End User a mean to assign names to their devices and associate these names to an Internet domain. With traditional naming configuration that sets an "search" field for the resolvers, the Front End Naming Architecture provides relative naming resolution. The search field is configurable on the DHCPv6 Server hosted on the CPE.

Homenet devices can be attached in multiple local and Internet name spaces. The Front End Naming Architecture works internally and externally depending where the End User is. With Views, not all devices are visible from the Internet.

The Front End Naming Architecture completely coexists with the Internet name services.

With the Homenet View hosted on the CPE, Name resolution and service discovery for reachable devices must continue to function if the local network is disconnected from the global Internet.

8. Security Considerations

The Front End Naming Architecture described in this document solves exposing the CPE's DNS service as a DoS attack vector.

8.1. Names are less secure than IP addresses

This document describes how an End User can make his services and devices from his Home Network reachable on the Internet with Names rather than IP addresses. This exposes the Home Network to attackers since names are expected to provide less randomness than IP addresses. The naming delegation protects the End User's privacy by not providing the complete zone of the Home Network to the ISP. However, using the DNS with names for the Home Network exposes the Home Network and its components to dictionary attacks. In fact, with IP addresses, the Interface Identifier is 64 bit length leading to 2^64 possibilities for a given subnetwork. This is not to mention that the subnet prefix is also of 64 bit length, thus providing another 2^64 possibilities. On the other hand, names used either for the Home Network domain or for the devices present less randomness (livebox, router, printer, nicolas, jennifer, ...) and thus exposes the devices to dictionary attacks.

8.2. Names are less volatile than IP addresses

IP addresses may be used to locate a device, a host or a Service. However, Home Networks are not expected to be assigned the same Prefix over time. As a result observing IP addresses provides some

ephemeral information about who is accessing the service. On the other hand, Names are not expected to be has volatile as IP addresses. As a result, logging Names, over time, may be more valuable that logging IP addresses, especially to profile End User's characteristics.

PTR provides a way to bind an IP address to a Name. In that sense responding to PTR DNS queries may affect the End User's Privacy. For that reason we recommend that End Users may choose to respond or not to PTR DNS queries and may return a NXDOMAIN response.

8.3. DNSSEC is recommended to authenticate DNS hosted data

The document describes how the Secure Delegation can be set between the Delegating DNS Server and the Delegated DNS Server.

Deploying DNSSEC is recommended since in some cases the information stored in the DNS is used by the ISP or an IT departments to grant access. For example some Servers may performed a PTR DNS query to grant access based on host names. With the described Delegating Naming Architecture, the ISP or the IT department MUST take into consideration that the CPE is outside its area of control. As such, with DNS, DNS responses may be forged, resulting in isolating a Service, or not enabling a host to access a service. ISPs or IT department may not base their access policies on PTR or any DNS information. DNSSEC fulfills the DNS lack of trust, and we recommend to deploy DNSSEC on CPEs.

9. IANA Considerations

This document has no actions for IANA.

10. Acknowledgment

The authors wish to thank Ole Troan for pointing out issues with the IPv6 routed home concept and placing the scope of this document in a wider picture, Mark Townsley for encouragement and injecting a healthy debate on the merits of the idea, Ulrik de Bie for providing alternative solutions, Paul Mockapetris for pointing out issues of the trustworthiness of a reverse lookup, and Christian Jacquenet for seeing the value from a Service Provider point of view.

11. References

11.1. Normative References

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

[RFC1995] Ohta, M., "Incremental Zone Transfer in DNS", RFC 1995, August 1996.

[RFC1996] Vixie, P., "A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)", RFC 1996, August 1996.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2136] Vixie, P., Thomson, S., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, April 1997.

[RFC2845] Vixie, P., Gudmundsson, O., Eastlake, D., and B. Wellington, "Secret Key Transaction Authentication for DNS (TSIG)", RFC 2845, May 2000.

[RFC2931] Eastlake, D., "DNS Request and Transaction Signatures (SIG(0)s)", RFC 2931, September 2000.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996, September 2010.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, January 2012.

11.2. Informational References

[I-D.chown-homenet-arch] Arkko, J., Chown, T., Weil, J., and O. Troan, "Home Networking Architecture for IPv6", draft-chown-homenet-arch-01 (work in progress), October 2011.

Appendix A. Document Change Log

[RFC Editor: This section is to be removed before publication]

-01:

* Added C. Griffiths as co-author.

* Updated section 5.4 and other sections of draft to update section on Hidden Master / Slave functions with CPE as Hidden Master/Homenet Server.

* For next version, address functions of MDNS within Homenet Lan and publishing details northbound via Hidden Master.

-00: First version published.

Authors' Addresses

Daniel Migault
Francetelecom - Orange
38 rue du General Leclerc
92794 Issy-les-Moulineaux Cedex 9
France

Phone: +33 1 45 29 60 52
Email: mglt.ietf@gmail.com

Wouter Cloetens
SoftAtHome
vaartdijk 3 701
3018 Wijgmaal
Belgium

Phone:
Email: wouter.cloetens@softathome.com

Philippe Lemordant
Francetelecom - Orange
2 avenue Pierre Marzin
22300 Lannion
France

Phone: +33 2 96 05 35 11
Email: philippe.lemordant@orange.com

Chris Griffiths
Comcast Cable Communications
One Comcast Center
Philadelphia, PA 19103
US

Phone:
Fax:
Email: chris_griffiths@cable.comcast.com
URI: http://www.comcast.com