

Internet Engineering Task Force
Internet Draft
[draft-tsang-appliances-reqs-00.txt](#)
September, 2000
Expires: March, 2001

Simon Tsang
Stan Moyer
Dave Marples
Telcordia Technologies, Inc

Henning Schulzrinne
Columbia University

Arjun Roychowdhury
Hughes Software Systems

Requirements for Networked Appliances:
Wide-Area Access, Control, and Interworking

STATUS OF THIS MEMO

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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.

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

Abstract

Today, there are a variety of technologies available to network appliances and provide degrees of home automation and control. However, there is a lack of support for wide-area access control and interworking of these Networked Appliances (NA). The ability to provide such support will radically enhance people's ability to provide exciting new services. This document outlines a set of requirements for providing such support.

[1. Introduction](#)

1.1 Networked Appliances

The next wave of the Internet is widely predicted to be the Networked Appliance (NA) - the refrigerator that can keep an inventory of your groceries and re-order when necessary or perhaps the alarm clock that can co-ordinate your agenda, check the weather and the road conditions to determine the correct time to wake you up. It is clear that these appliances will need to communicate amongst themselves. For example, an alarm clock may be configured to switch on the bedroom lights at 7am as a wake-up indication to the user.

The term Networked Appliance (NA) is difficult to define as it can cover a very large range of devices. However, for the purposes of this document, a Networked Appliance is defined as being a dedicated function consumer devices containing at least one networked processor. Examples of NAs include: lamps, refrigerators, toasters, and TVs.

There are numerous networking technologies which allow the scenarios outlined above to be realized within a single home or administrative domain. Some examples are X.10 [6], HAVi [2], VHN [3], and UPnP [4].

However, there is currently no support for wide-area access control of these networked appliances 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.

For example, before leaving the office, a user could contact his (or her) home and ask it to pre-heat the oven, record the news on TV, and set the house temperature to 70 degrees F. While on a business trip, a plumber comes to the house to fix a leaky sink. The user is notified when the plumber rings the doorbell and a camera at the door transmits an image of the plumber to the user's laptop PC. The plumber's ID card has an electronic signature which is also transmitted with the image and verified by the user's client software. The user remotely unlocks the door and allows the plumber in, all the while viewing and conversing with the plumber via micro-cameras and microphones in the home.

This document outlines a set of requirements for providing Networked Appliance wide-area accessibility and interworking. Required capabilities include: control of NAs, event subscription and notification, and remote sensor reading.

1.2 Example Home Network Environment

Figure 1 shows an example of a possible Home Network environment. Within the home, a variety of home networking technologies are used

(X.10, HAVi, 802.11). An IP-based Local Area Network (LAN) interconnects the various networks. Access to the wider Internet is

provided through a Residential Gateway (RGW). The RGW may optionally provide additional functions such as firewall and Network Address Translator (NAT).

Each Home Environment has a domain name given to the RGW for access to or from appliances and devices with the home. For example, this could be in the form of example_user.example_home.net or for precise appliance addressing, example_appliance.example_user.example_home.net. The domain name will be used to address users and appliances networked behind the RGW.

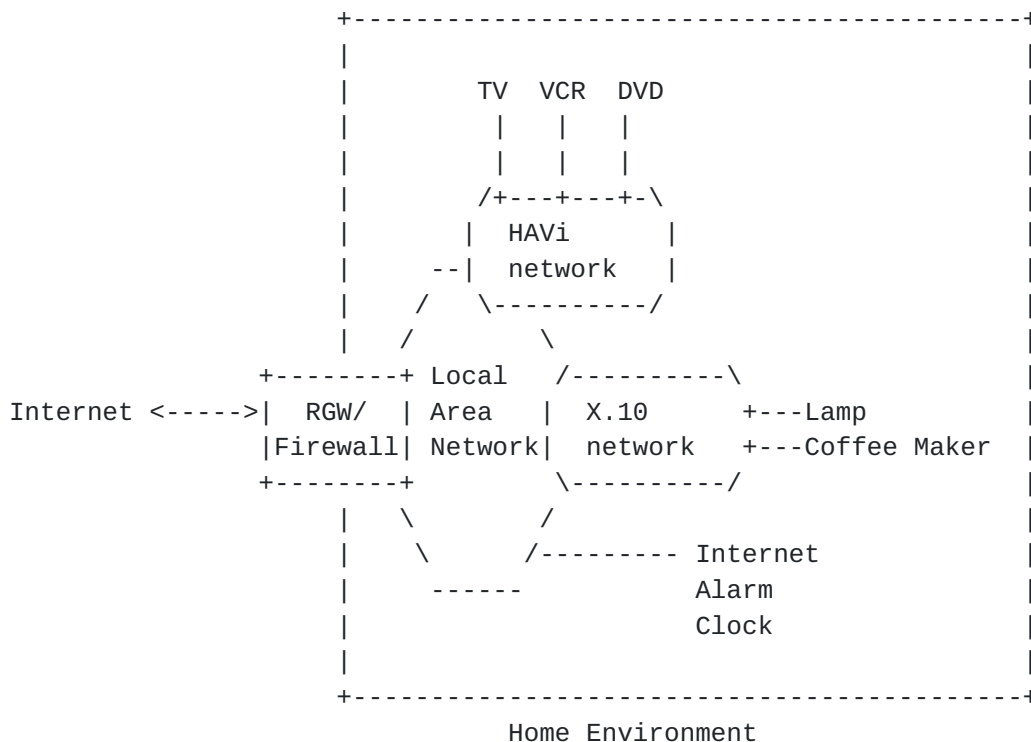


FIGURE 1. Different networks comprise the Home Environment

[1.3](#) Interworking Different Networks in the Home Environment

Figure 2 illustrates how different networks within the home environment may communicate with each other and the RGW over the LAN via an interworking protocol.

Home networking technologies which do not communicate using IP are connected to the home LAN via an Appliance Controller. Appliance Controllers provide interworking between home networking technologies and IP, and may additionally provide application layer interworking. Appliance Controllers should operate transparently.

It is envisaged that Appliance Controllers will be required for every home networking technology used in the home environment (such as HAVi and X.10 as illustrated in Figure 2).

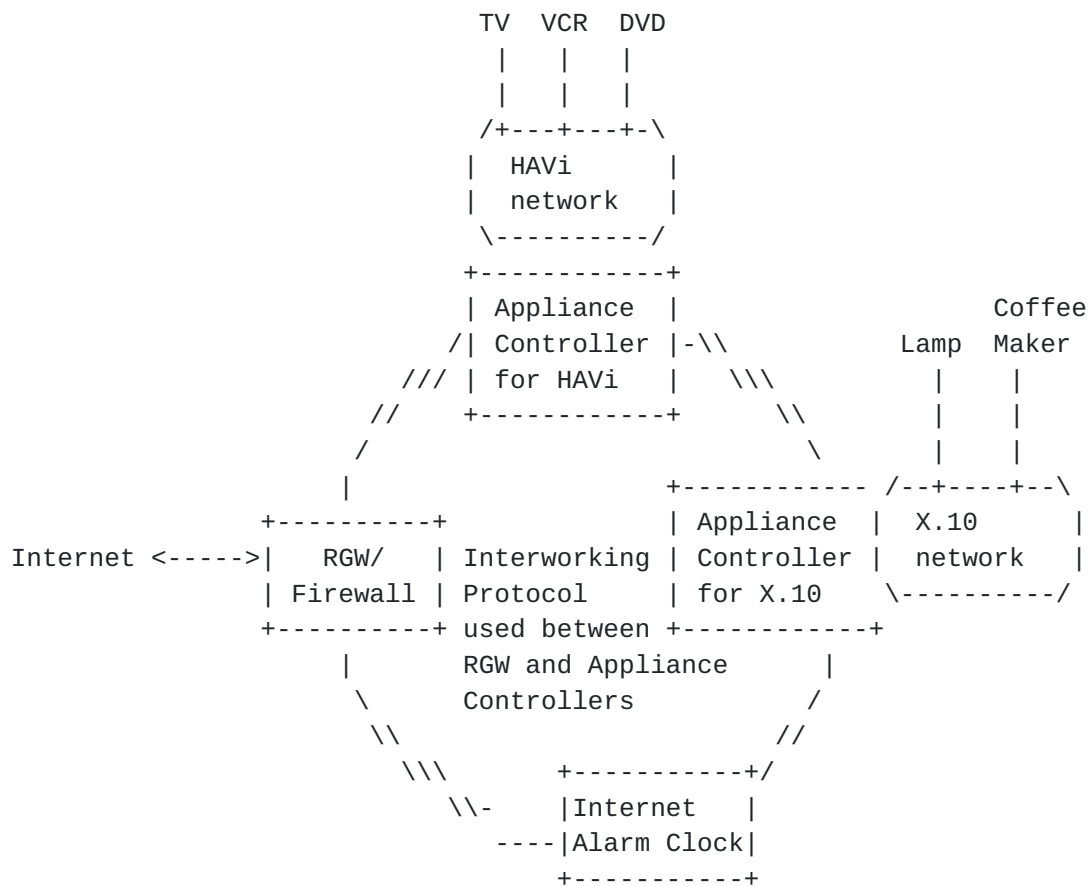


FIGURE 2. Interworking different networks in the Home Environment

This document discusses the requirements for the interworking protocol.

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

S. Tsang et al

[Page 4]

	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.
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. General Requirements

4.1 Wide-area accessibility of Networked Appliances.

4.1.1 NAs must be accessible from outside of the home environment.

4.1.2 For NAs without IP networking capabilities, an Appliance Controller should be used to provide interworking between the NA and the IP network.

4.1.3 Only a subset of NAs need to be addressable outside of the home. It should be possible to query the home in some way to find those that are.

4.2 Protocol transparency and independence.

4.2.1 It must be possible to interwork between different in-home networking technologies transparently. This requirement applies to both physical networking (e.g., X.10 [6], 802.3, 802.11, Bluetooth [7]) and application networking technologies. (e.g., HAVi [2], UPnP [4], Jini [5], Salutation [8]).

4.3 Personal mobility support.

4.3.1 Networked Appliances must be able to move within the home domain, across home domains, within the service provider's domain, and across service provider domains.

4.3.2 Support must be provided for locating and controlling Networked Appliances as they move across different home environments and networks.

4.4 Configuration.

4.4.1 Networked Appliances should (as far as possible) be auto-configuring. There should be minimal user interaction, though users should be allowed to manually configure their appliances if desired.

4.5 Usage Monitoring and Charging

4.5.1 The home networking environment may optionally allow usage records to be created at a variety of granularity levels. For example, usage records may be created on a per session or per message basis.

5. Naming & Addressing Requirements

5.1 NAs must be assigned a generic addressing format which can be used to refer to it by any communicating entity.

5.1.1 NAs may have global IP addresses or local IP addresses (in the case when NAs are behind a firewall or proxy).

5.1.2 In the cases when NAs are not IP-based, the NAs must be assigned a generic address.

5.2 There must be support for classification of addresses and selection between multiple instances. For example, it must be possible to search for æall lampsÆ or to allow refinement of a search for a particular lamp.

5.3 Since the specific name for a NA may not be known, a mechanism must exist to æsearchÆ for the NA using a well-known language/naming schema.

5.4 The addressing scheme MUST use UTF-8 for character representation.

6. Communication Protocol Requirements

6.1 The communication protocol must provide a flexible payload capability which will allow the transport of commands to, and responses from, individual NAs or classes of NAs. More explicitly, there must be a separation of transport and data.

6.2 The protocol must provide reliability against all forms of

communication errors. This includes both short æglitchesÆ and long term æbreakdownsÆ. If the communication breakdown is unrecoverable,

the protocol must be able to signal this to the communicating entities.

6.3 The protocol must support efficient messaging for control. It is expected that control messages for NAs will be short and optionally may not form part of an ongoing dialogue. These messages should therefore be delivered in the form of datagrams (sessionless) but with reliable semantics.

6.4 The protocol must support event subscription and notification (e.g., the ability to be notified when a lamp is switched on or off).

6.5 The protocol must support the ability to obtain the output of remote sensors (e.g., the output from temperature sensors).

6.4 The communication protocol must be able to encapsulate various appliances characteristics. For example, some appliances may act and respond immediately, while others may only respond after a non-determinate amount of time.

7. Communication Mode Requirements

7.1 Support for the following communications modes is required:

7.1.1 Control: for example "Turn on the outside light".

7.1.2 Queries (e.g., of device state): for example "What is the temperature in the house?".

7.1.3 Asynchronous events ("notification"): for example "Notify me when the security alarm goes off".

7.1.4 Discovery: for example "What device can meet requirement x?".

7.1.5 Support Media streaming (sessions): for example "View the babysitter-cam".

8. Security Considerations

Interconnecting home appliances to each other and especially to devices outside the home environment introduces a serious possibility of "internet theft". It may now be possible for a rogue entity to gain control of home appliances in a way that is very adverse to the home owner. The importance of having a strong security policy is of prime importance in such a network. This section highlights security requirements that will need to be followed for such a network. Note that while it is important to protect shared appliances, it is equally important to decide which devices are to be shared by

external entities.

8.1 Authentication, authorization, privacy, and replay protection are required in all communications.

8.1.1 It should be possible to check communications with devices from the wide area at different granularity levels. Examples include: once per session, per message, or periodically.

8.2 The contents and device name of the messages must be kept private so that eavesdroppers cannot learn about what is in people's homes.

8.3 When Networked Appliances move into environments other than their home environment, the visiting appliances and their users must be authenticated and authorized.

8.3.1 Authorization checks may be performed at different granularity levels. Examples include: per registration (visit), per message or periodically.

8.4 Support for audit capabilities may optionally be supported so that traceback and fault control can be performed.

8.5 Non-repudiation may optionally be supported in all communications.

8.6 Resilience under security attacks.

8.6.1 It should be possible to dynamically isolate NAs within the home environment selectively or completely from external networks.

8.6.2 The appliances must be able to perform a minimum of functions correctly, even in the absence of external communications.

9. 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] Bluetooth, <http://www.bluetooth.com>
- [8] Salutation, <http://www.salutation.org>

10. Author's Contacts

Simon Tsang

Telcordia Technologies
445 South Street

S. Tsang et al

[Page 8]

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

