Home DNS: Experiences with Seamless Remote Access to Home Services

P. Belimpasakis, A. Saaranen and R. Walsh
Extended Home, Internet Core Technology Center
Nokia Research Center

Abstract

Uniform interfaces and interaction methods between at-home, mobile and nomadic access to content and devices from consumers’ homes, are crucial in making compelling extended home applications and services. It is possible to access these services whether within the user’s home or, remotely, elsewhere. This paper investigates and identifies the benefits of existing remote access methods and presents the new Home DNS solution as a means to ensure remote access connectivity to home services. Through design and implementation of the Home DNS solution, we prove the feasibility of seamless remote access to home services using existing mobile, home CE and PC devices without modification, and so offer a minimal deployment barrier to satisfying these needs in heterogeneous real-world digital home and nomadic cases.

1. Introduction

Standardization bodies, such as the Digital Living Network Alliance (DLNA) [11], are making it possible to experience user services between home devices from multiple vendors, with interoperability over Internet Protocol (IP) connectivity. Such consumer products are already entering the market. Examples include networked personal computers, Personal Video Recorders (PVRs) and Media Adaptors. The amount of these, and other, “smart” devices within the home is expected to significantly increase in the near future. With the latest media adaptor devices, consumers are able to view their movies stored in their local mass storage, usually a PC hard drive, from their (originally not networked) home TV and cinema system in the lounge. It will be also easy to share and view images stored in home PC using wireless photo frames, TVs and other home network devices with a display.

Advanced mobile terminal products, capable of connecting with home devices, are proliferating. The convergence of networked smart home electronics and mobile devices with home connectivity features inevitably lead to user desires to continue the use of home services on the handheld device in the mobile environment – beyond the home. The usage metaphor of continuing the consumption and interaction with the same home-located content and devices also outside the home is natural and intuitive. However, it poses additional technical challenges on top of the home-bound usage.

This usage, technically termed remote access, is only recently appearing in standardization contributions for specific vertical use cases; and is thus still some way from coming to the interoperability required for the competitive multi-vendor mass market. It is widely recognized that a combination of existing (IP-standards-based) technologies can enable some level of remote access for most home connections, although the required level of technical understanding and administration is impractical for consumers in the mass market, and improvements are essential for both interoperability and usability.

The feasibility of any alternative remote access systems is significantly affected by its deployability - that is, how few devices must be reconfigured or replaced, and how few those changes are for technology suppliers or vendors. Thus, this paper aims to test whether an elegant combination of those already deployed technologies can be used to reduce the barriers to deployability whilst ensuring adequate seamless remote access connectivity for non-technical home users.

This paper describes several existing technologies, which alone do not meet the user needs for seamless remote access, and proposes a new approach combining several existing methods in an elegant way minimizing new components. The novel approach enables the use of a single user-friendly name for the home devices, regardless of whether the mobile device is at home or outside it. HTTP-based [16] web technologies (such as WebDAV[18], RSS[4], ATOM[21]) are combined with Dynamic Domain Name Service (DNS) [27], HTTP Proxying [16] and
UPnP [24] to provide the flexibility needed for ubiquitous access to home devices.

This paper next describes a typical home network and then the prior solutions which afford some of the desired remote access functionality. The new Home DNS proposal is described as a design solution, then its prototype implementation. Several key learnings we made in testing the prototype which are further reported as advantages and disadvantages prior to suggestions for further work and conclusions of the effectiveness of the approach and solution.

2. Typical home network

Typically, Internet Service Providers (ISPs) offer Internet connectivity to their home/consumer subscribers, by assigning to their equipment only one public IPv4 address. A normal home setup is shown in Figure 1.

![Figure 1. Typical Home Network](image)

Since modern networked home environments consist of more than one internal device, a NAT [14] solution is used in order to allow all home devices to simultaneously access the Internet. In such a setup, the public IP address is assigned to the home gateway which then acts as a NAT router for all the internal devices. The NAT router assigns, to home devices, private IPv4 addresses, which are not globally routable from the public Internet.

The main problem in the current setup of home networks is that the individual home devices cannot be accessed from the public Internet, as the usage of NAT breaks end-to-end network-layer connectivity. The only device in the home reachable from the Internet is the gateway (GW) device, for example the Digital Subscriber Line (DSL) router that provides the connectivity to the Internet. Thus, the user cannot directly remotely connect to one of the in-home devices as the in-home devices do not have unique and routable addresses in the Internet.

3. Current Understanding & Learning from Earlier Solutions

The problem of the addressability of a home gateway, that uses a public but dynamic IP address, has been already addressed and solved by Dynamic DNS services, such as DynDNS [13] or No-IP [22]. Whereas traditional DNS systems are only suited to mapping static IP addresses to (static) domain names, Dynamic DNS systems allow the mapping of dynamic IP addresses to (static) domain names, by updating a more timely DNS record update mechanism when an IP address change occurs.

Moreover, the reachability of internal home devices, from an external remote client, has been partially addressed by several existing technologies, as described below.

3.1. Port Forwarding

When using the port forwarding technique, the NAT router creates and maintains a mapping table between local private IP addresses and certain inbound transport layer port number. Such that a data packet addressed to the NAT router’s public IP address for a pre-mapped port will automatically be forwarded to the mapped device’s IP address – changing the destination address of the data packets in the process. The mappings must be predefined by the user, and static private IP addresses are needed (such that dynamic host IP address configuration should be avoided).

The biggest advantage of port forwarding is that it works on the TCP and UDP transport protocol level, so that the broken network layer end-to-end connectivity need not be fatal. However, an important disadvantage is that home devices will have to be addressed differently depending on whether they are addressed from the internal network or from an external network, since the private IP address is used internally, and public IP address of gateway is used externally. This means, that if the user has a mobile/portable device, used both internally and externally, there is need to create double bookmarks, double application configurations, and so on, and use them according to the network the mobile device is attached.

3.2. Virtual Private Network (VPN)

The Virtual Private Network (VPN) technique allows a remote client to establish a secure communication channel to a home network, over a public and shared network such as the Internet [8]. Nowadays, some home gateway devices also provide
VPNs have the capability of providing the same security and management policies as the home network. The client establishes an end-to-end tunnel to the VPN gateway, and can use all the resources of the private network, as if it was directly connected there.

The VPN solution has a very clear advantage of making the client seem to be connected directly to the home network. However, the most important disadvantage of the VPN solution is the requirements of special VPN software and settings on the remote/mobile client. Extra software cannot always be installed or configured on remote devices that user does not administrate.

3.3. HTTP Proxy

The HTTP Proxy solution solves one of the biggest disadvantages of IPSec VPNs, which is the requirement for special client software on the remote device. Almost all Internet enabled devices have a web browser and HTTP stack preinstalled for sale, so this could be the user interface and transport protocol for accessing home resources. Web clients do not need to make their HTTP requests directly to the target server, but can communicate them to an HTTP proxy, which then forwards the requests to the appropriate home device. The typical HTTP proxy functionality is specified in [16]. Almost all HTTP clients have an option for specifying an HTTP proxy to be used. Alternatively, some proxies can be used transparently, without the need of specifically configuring the client. This is done by embedding the target device address in the Uniform Resource Locator (URL) [6]. For example, if a remote client needs to access an internal device at the URL http://192.168.1.100/, and the proxy, i.e. home gateway, is located at the public address http://100.100.100.100/proxy, a URL with the following syntax could be used: http://100.100.100.100/proxy/cgi?URL=http://192.168.1.100/. Note that this is just example syntax, since the format is specific to the proxy used.

The main advantage of the HTTP proxy solution is that the client does not need to have any special software, apart from the normal HTTP stack and a related application such as a web browser. Also, the only protocols used are HTTP (plain and secure), so the traffic could be routed via HTTP proxies. However, the disadvantages of this solution are that it only works with HTTP services and it requires different addressing of devices (domain names / URLs), depending on whether the client is attached to the internal network or an external one.

3.4. Internet Protocol v.6 (IPv6)

The problems described are related to the usage of NAT in the home gateway, due to the limited amount of IPv4 addresses that are available for customers. Theoretically, deployment of IPv6 solves some of these problems - if deployed and supported by every device, Internet Service Provider and network router on the Internet. Then, every device connected on the Internet would have a public, globally routable, IP address. Practically thought, only few devices have IPv6 support enabled by default, those being mainly PCs and mobile phones. Currently, most networked home devices are still supporting only IPv4 and, thus even should complete IPv6 roll-out occur, an intermediate IPv4 compatible solution is still required.

4. Home DNS: A New Solution

To solve the major problems that current, mainly IPv4 based, remote access solutions have, such as different addressing schemes depending on client’s location, special software requirements, and complicated settings, we developed a new solution. This solution aims to provide easy remote access connectivity, from the Internet to any internal home network device, for any service that is based on HTTP.

The Home DNS concept is to extend the use of dynamic DNS both outside and inside home network. The proposal is that each home device has a globally unique host name, under the public home domain name, and that host names are resolved to different IP addresses, depending if the DNS lookup request is originating from the internal network or the Internet. Mobile/portable devices are assumed to be the primary clients. They can be used both within the internal home network, as well as in external network from where, using remote access, they should be able to still reach the home services, without any special settings.

4.1. Home Gateway Device

The Home DNS solution requirements are embodied by changes only in the home gateway device. As in most current cases, it is assumed that the home gateway provides Dynamic Host Configuration Protocol (DHCP) [12] and DNS services to the devices in the home network. When a new device is added to the home network the GW device provides it with a private IP address. If a home device needs to contact another one, internal or external, it sends its DNS query, with the host name, to the GW which replies with the DNS information, containing the target IP address. Thus, only a single resource name/address is
needed to find the target device for the identified cases.

The first new requirement for the home GW is that it needs to use the UPnP Simple Service Discovery Protocol (SSDP) [26] to learn the host name, to be used in the DNS information. This way we avoid the manual configuration of the DNS server in the home GW. The home GW listens to the UPnP notification messages the home devices broadcast, stores the self-described “UPnP friendly name” and the respective IP address to the DNS database, which we call “Device Mapping Database” in our system. The basic interactions are shown in Figure 2.

![Figure 2. Initial interactions between gateway and devices](image)

The friendly name of an UPnP device is something that describes it in a human readable form, for example “TIVO-PVR”, and is typically assigned by the manufacturer. This name will be used, when accessing the services of the home device, in form of a URL address.

The Home DNS solution does not require that the home GW device have a static IP address on the public Internet. Instead, the home GW device uses dynamic DNS to update its DNS information in the Internet (the second requirement). Using dynamic DNS, the home gateway device registers its IP address to the Internet-based dynamic DNS server, such as DynDNS [13] or No-IP [22]. For the following examples, the public IP address of the GW is 100.100.100.100, and this is mapped to the domain name myhome.homedns.org.

Dynamic DNS provides wild card functionality. Such that all DNS queries to any sub-domains of the registered host name returns the same registered IP address. So the URLs of the home devices also need to be aggregatable (as the home gateway’s URL represents all the device URLs of the home network). This way the DNS lookup in the Internet will return the IP address of the home gateway for all the URLs of the home devices. For example, the address tivo-pvr.myhome.homedns.org (and any address with the format *.myhome.homedns.org) would be resolved to the one registered public IP address (e.g. 100.100.100.100).

The home GW device has to also provide the home devices with HTTP proxy services to support remote access (the third requirement). When an HTTP request message for a home device arrives at the home GW, from the public Internet, the packet has the IP address of the GW its destination. The HTTP proxy has to identify the final destination of the HTTP request and forward the message to the IP address of that home device. That is done by analysing the HTTP headers.

4.2. Accessing the Home Devices

4.2.1. Inside the Home. Internal home devices can access the other home devices using a URL composed by the device’s friendly name and the static home domain name, for example http://tivo-pvr.myhome.homedns.org. When accessing this address, a device uses the DNS service provided by the home GW to find the IP address of the other home device. In the above example, the DNS reply from the home GW contains the private IP address of the PVR device. After getting this information the user device can start exchanging information with the other home devices, as shown in Figure 3. In this case our solution only provides the DNS information to enable direct communication between home devices.

![Figure 3. Accessing home devices, locally](image)

4.2.2. Remote access. Likewise, when accessing a home device from outside the home, the user can connect to it using exactly the same URL of the device, i.e. http://tivo-pvr.myhome.homedns.org. In this case, the user device is depending on the DNS service available through its current connection. Eventually the DNS query reaches the dynamic DNS server that will provide the IP address of the home gateway device as a response (e.g. 100.100.100.100). After getting this message the user device will make its connection and HTTP request to the home GW device. In that request, the headers’ field “Host”, as specified in the HTTP protocol [16], contains the host and domain name that
the client actually wants to contact, in the form of a URL. Thus, the gateway can differentiate the requests and identify towards where, i.e. which device, they are targeted. Then, it acts as a transparent HTTP proxy, between the client and the home device, as shown in Figure 4.

Figure 4. Accessing home devices, remotely

5. Prototype Implementation

To validate the Home DNS proposal, a prototype of the system was built [5] with the home GW running on a Linux PC. A mobile Internet Tablet, with WLAN connectivity, used as the client, and a device with HTTP server and UPnP functionality used as the static home device to be accessed remotely. An example setup is shown in Figure 5. Also, an external, public, Dynamic DNS provider was used.

On the home gateway, apart from the default components (DHCP server, NAT and firewall functionality, etc.) the following components were used:
- The BIND server [19], also known as “named”, was used as a DNS server
- For an HTTP Proxy, the Reverse Proxy functionality provided by Apache Web Server 2 [1] was used, along with the following modules:
  - mod_proxy [2] supports both types of reverse proxy operation, mod_proxy_http which handles fetching documents with HTTP and HTTPS and mod_headers, which modifies HTTP request and response headers.
  - The Dynamic DNS client used was the “ez-ipupdate” [15] and the service used was the one provide by DynDNS [13].

Configurations were required to the previous components, but no modifications to their source code. In addition to these “off-the-shelf” components, a module named “UPnP Listener” was coded, for coordinating the component interaction.

The UPnP Listener is a UPnP control point which listens for the UPnP Simple Service Discovery Protocol (SSDP) [26] ALIVE NOTIFICATION messages. When a new notification message arrives the UPnP Listener daemon would process the specific UPnP device description in order to get its friendly name. Then, from the source address of the SSDP UDP packet, it would extract the private IP address of the device. These mappings would then be added to the “Device Mapping Database”.

Similar actions would occur if a UPnP device would send a BYE message when leaving the network, or upon a timeout if a device does not re-announce itself for a long period of time, which indicates that it left the network ungracefully.

6. Advantages & Disadvantages of Home DNS Solution

The most important advantage of our system is the seamless addressing of home devices, regardless of the client’s location. The user can connect to a home device using exactly the same URL (e.g. http://tivo-pvr.myhome.homedns.org), no matter if the client used is attached to the home network, or to an external one. Thus, the mobile clients, that can be used both internally and externally, do not need special configurations and settings, since the same names/addresses apply in both cases. Moreover, there is no need for special software since the standard HTTP applications can be used.

The system also keeps the traffic load, via the proxy, to a minimum level. When the client is connecting remotely to a home device, the traffic goes via the proxy. However, when connecting internally, within the home network, the traffic is exchanged only between the communicating devices, and does not
overload the proxy. This allows the gateway device to be low-powered and inexpensive to build.

Minimal configuration is one more important advantage that the system introduces, for optimizing the user experience. The only settings required to be manually entered, by the home owner, are the address of the used dynamic DNS provider, along with the home’s domain name (e.g. myhome.homedns.org) and the corresponding username and password to the service. In any case, those are the settings that users already need to give to their routers that support dynamic DNS. However, there is no need to configure any port forwarding rules, or make any changes when new devices are added to the system, since they are automatically discovered using UPnP and entered in the database.

The only significant technical limitation of this basic Home DNS solution is the mandatory usage of the HTTP protocol, for applications, in the communicating between the home device and the remote client. The home gateway proxy relies on the HTTP headers, embedded in the client’s request, for identifying the target home device. So, the solution becomes HTTP-specific and cannot be directly applied to other application protocols. Nowadays many applications and services are based on top of HTTP, which is probably the most widely used protocol and the basis of continued web services and semantic web applications. Thus, this limitation may not be considered as important for very many cases and applications, especially in the limitations of the home domain. However, as seen later in section VII. 2), this solution can be extended by combining with the port forwarding mechanism to allow any kind of protocol to be used, with similar advantages.

From scalability point of view, this solution adds some extra workload on the dynamic DNS provider, since it has to resolve requests for every connection made from the Internet to the home. However, the solution does not significantly affect the DNS server load of the ISPs where the home network or the remote node is attached.

7. Other Considerations

7.1. Security

All the previous examples assume that no security (authentication or encryption) is applied during the communication of the client device and the home gateway. Since our solution uses the existing HTTP proxy solution, the same security mechanisms used with HTTP, such HTTP authentication and Layer Security (TLS) [10] or Secure Sockets Layer (SSL) [17] encryption, can be applied and are for remote access in the present prototype.

When an external HTTP connection is created to the home gateway, on the non-secure port 80, it can be automatically redirected to a secure port, usually 443. External devices must communicate with secure HTTP (HTTPS) to the gateway, i.e. in an encrypted way. However, the HTTP proxy can still create a normal HTTP connection to the home devices (Figure 6), within the secure and trusted home network since encryption and security is provided there by the network medium used, such as the in-home wireless network security. If it is assumed that home networks are not secure, then a further usability problem of ensuring security without too much user administration or interaction comes into play.

From scalability point of view, this solution adds some extra workload on the dynamic DNS provider, since it has to resolve requests for every connection made from the Internet to the home. However, the solution does not significantly affect the DNS server load of the ISPs where the home network or the remote node is attached.

7.2. Rendezvous Mechanism

Combining the above Home DNS system with the port forwarding technique, this extended Home DNS can be used as a mechanism for allowing signaling between an external device and an internal home device even for non-HTTP communication sessions.

For instance, the case of a standards-based Voice-over-IP (VoIP) phone in the home network and another VoIP device in the external would typically use the Real-time Transport Protocol (RTP) - not HTTP. So it would not work over HTTP proxy, which the initial solution provides. VoIP could work, however, if some specified UDP ports are opened on the home gateway firewall and the incoming traffic to those ports is routed to the internal VoIP phone, as described in section 3.1. The Home DNS solution should assist the initial communication between the two devices, and allow them to exchange the communication parameters so that port forwarding rules can be established (or else some “out-of-band” initial invitation mechanism would
be needed). Using HTTP GET/POST messages, the two devices can have an end-to-end message exchanging mechanism to describe their communication requirements and parameters to one another. Based on those, each device can request, using UPnP, from the home gateway to open some specific TCP/UDP ports and forward the incoming traffic from the public Internet to the specific internal device. Using this port forwarding any kind of traffic can be exchanged, not only HTTP.

If the internal VoIP device is at the example address phone.myhome.homedns.org, and it is running a web server, it could accept HTTP connections both from the internal or external network.

Figure 7. Using Home DNS as a rendezvous mechanism

In detail, the operation (Figure 7) would be as follows:

1. An external device accesses the internal device, using HTTP, at the address http://phone.myhome.homedns.org. In the HTTP request, it indicates its interest for a VoIP communication.

2. The internal device, a VoIP phone in this example, makes an UPnP Internet Gateway Device (IGD) [25] request, to the home gateway, to open a hole in the firewall for specific UDP ports and enable port forwarding of those. Once it is enabled, the gateway confirms the action to the internal device.

3. The internal device replies to the original HTTP request, made by the external device in step 1. In the reply it includes the opened UDP ports where connections can be established.

4. The external device can use the VoIP session protocol to communicate with the internal device, at the specified ports. All traffic is routed to the internal VoIP phone.

Once the communication is completed, the port forwarding is automatically stopped, and the firewall is reactivated on the specific ports.

The usage of VoIP in this case is just an example. This solution would work with any IP based protocol.

Session Initiation Protocol (SIP) and a SIP service are the widely recognized, standard-based, method for VoIP call setup. However, as shown above, the Home DNS framework enables simple initiation of services between devices with the minimum of infrastructure cost.

8. Further Development

Now that the feasibility and functionality of the basic Home DNS system has been prototyped and demonstrated using a generic PC as the home GW, the natural next step is to implement or port this to commercial home gateways, subsequently. The optimal deployment would be to release it as part of an open-source project running on top of embedded Linux distributions, such as the OpenWrt [23], which is already used in many consumer Internet gateway devices. In this way, the applicability of Home DNS to a wide range of commercial devices can be proven and the barrier of multi-vendor acceptance would be addressable.

During our prototyping and testing, we found out that there are a several aspects which merit further study based on the proposed Home DNS system. One is the extension of discovery methods, of new devices, within the home network. Currently UPnP protocol is proposed, but alternative ones can be applied, such as the Apple Bonjour [3] and the Bluetooth [7] discovery mechanism, for devices in proximity.

Another problem observed was the management of the friendly name namespace. Trivially, should two devices be preconfigured with the same UPnP friendly name a simple number is appended (such as “1”). A more general approach would be to adopt a more generic name space which would require future investigation.

Finally, the current solution focuses only on the IPv4 protocol, since the NAT connectivity challenges exist there. With the global deployment of IPv6, the end-to-end network layer connectivity of devices should no longer be a problem, since each device will have a globally routable address. However, the addressing of home devices, in a seamless and transparent for the user way, will still be a problem. Further study is required to assess the applicability and benefits of Home DNS to IPv6 enabled networks, for maximizing the user experience.

9. Conclusions

Existing remote access techniques and solutions introduce challenges such as different addressing schemes depending on client’s location, special
software requirements, and complicated settings. These impose important usability issues, especially in a converged fixed-mobile environment. The Home DNS technique allows easy-to-use remote access to home devices. It does not require any manual configuration of devices by users. The home gateway device connecting the home to the external network, the Internet, must be enhanced with Home DNS support, although no modification or extra software is required for other home and remote Internet devices.

This solution allows the user to address the home devices using the same names both at home and on remote connections. The user is not required to know the IP address of any of the devices involved. The only thing required is the URL of the home device the user wants to access. Moreover, special value is added to mobile devices, which can be used both within the home network and outside of it, and can access the home resources and services with the same automatic naming scheme and application configurations.

The work indicates that eliminating all need for new technology is impractical, and also proves the feasibility of a solution with minimal deployment barriers. It also demonstrates the value of prototyping connectivity proposals for identifying both easy-to-achieve feature enhancements and longer term system improvements that would otherwise jeopardize the viability of a proposal, if agreed for multi-vendor interoperability or standardization.

10. References