IPv6 Challenge
Reach everything from anywhere

Juan Antonio Cordero[*], Ulrich Herberg[†], and Vivek Nigam[‡]

INRIA Saclay – Île-de-France and LIX/École Polytechnique

Route de Saclay, 91128 PALAISEAU Cedex FRANCE

June 4, 2009

Contents

[*] j.a.cordero@gmail.com

[†] ulrich.herberg@polytechnique.edu

[‡] nigam@lix.polytechnique.fr

1 Introduction

With the outcome of the Internet, many visionaries forecasted that soon all devices would be remotely accessible from anywhere. However, as the number of available IPv4 addresses becomes more restricted, the current Internet is not able to fully accommodate such vision. To overcome this lack of addresses, a more advanced Internet Protocol, called IPv6, has been proposed and standardized. Since IPv6 provides a larger addressing space (2^{128} vs 2^{32} in IPv4), it enables any device (such as PCs, smart phones, alarm or heating systems) to have its own IPv6 address[1].

The main objective of this project is to show how IPv6 opens, together with the growing intelligence of home devices, new business opportunities and can be exploited to provide new services, in particular related to remote access of home devices, such as locally-stored music and video streaming, home security, or home devices control and configuration services. We show that, by using standard and well known protocols, we can easily develop devices that can be connected to the Internet in a *plug and play* fashion, which can then be accessed and controlled remotely from anywhere.

The remainder of this document is structured as follows. After discussing, in Section 2, three possible business opportunities that arise with IPv6, we discuss the technical description of our solution in Section 3. In particular, we highlight the technological advantages to both users and developers obtained by using our IPv6 solution. Finally, Section 4 provides a SWOT analysis – strengths, weaknesses, opportunities and threats – of our project.

2 Motivating Example

The great success of the Internet is due to one simple and beautiful idea: *connectivity*. Because of it, many business opportunities have been created providing services that help us in many of our daily tasks, from finding a good restaurant to booking a flight. However, in the past years the demand for IP addresses increased on a large scale, and more and more home networks use private IP addresses and NAT. So this idea of global connectivity is being kept alive not through the uniform and global architecture originally imagined, but through *ad-hoc* solutions, such as specific applications that intermediate the communication between devices, or through standard technologies, such as Virtual Private Networks (VPN), that provide only a limited connectivity. In order to use these techniques, one often has to construct and/or customize network systems which require expertise and resources that are usually not available to both *home users* and *small businesses*. However, if we assume the scenario where every device has its own global (IPv6) address, then these technical and operational barriers would no longer exist, and one could imagine to easily explore this vast and rich consumer market with new products and services. We now discuss three types of opportunities.

- **Before-arrival services** – Often, before arriving a building, a house, or even a car, one wants to be able to remotely access devices such as heaters and air conditioning systems, so that the room temperature is adequate, or home utensils, such as ovens, so that his/her food is ready, by the time he/she arrives. In the current state of affairs, however, the most that one can do is to pre-program these devices to begin functioning at some particular time. As generally using these devices cost money and one is not always sure when one would arrive, this solution is far from ideal.

- **Remote access to data** – The past years have witnessed an incredible change on user behavior. Whereas before users stored their data, such as music, videos and documents in CDs and DVDs, now they usually store this type of data in their home computers. Since users usually have large amounts of data and cannot always carry it everywhere, often they

[1] To realize the extent of the transition, it is worth noting that the IPv6 addressing range is wide enough ($\sim 5{\cdot}10^{28}$ addresses) to assign 100 IPv6 addresses to each atom in the Earth.

need/want to access it remotely from, for example, inside a train, or an office, or someone else's house, but they cannot because their home computer does not have a global address.

- **Home automation and security** – With its mass production and the increase on research and development, home devices have not only accessible prices, but also acquired a considerable level of intelligence. For example, nowadays it is easy to find vacuum cleaners that are fully automated. If these types of home devices were also remotely accessible, then one could, for example, check which home devices are functioning at any moment, or furthermore, remotely change their configuration. Moreover, if surveillance systems, such as cameras, had their own global addresses, then one could easily install security systems and check at any time if, for example, babysitters are not mistreating children.

3 Technical Description

This section describes the technical aspects of the project.

3.1 Problem Statement

When the IP protocol suite was designed and standardized, no-one expected the demand for IP addresses to grow exponentially. Back then, using 32-bit long identifiers (i.e. IP addresses) seemed to be largely sufficient, since IPv4 provides in theory over 4 billion addresses. For example, huge blocks of IP addresses (e.g. class A networks with more than 16 million addresses) were allocated to small entities (such as American universities). However, in the past years, as more and more devices, such as mobile phones, require IP addresses, and as new users, especially in countries like China and India, become online, this number of addresses no longer seems enough to accommodate this increasing demand. It is supposed that within the next few years we will run out of IPv4 addresses.

To counteract running out of addresses, several proposals have been standardized by the IETF: CIDR [7, 3] and NAT [11, 10]. CIDR (Classless Inter-domain Routing) allows for splitting up Class A, B and C networks into smaller parts, thus limiting the number of unused addresses due to fragmentation of the address space. The problem of CIDR is the scalability of routing tables. As of today, the current BGP table size reaches 300,000 entries. Keeping this table in a reasonable size is crucial for the speed of look-ups. In addition, CIDR does not increase the size of the address space itself.

NAT (Network address translation) is another approach to reduce the number of needed IPv4 addresses, in particular for home users. Nowadays, most Internet Service Providers (ISP) allocate only a single public IP address per subscriber (i.e. per household). Current DSL modems often integrate a router at the same time that allows for NAT. All home user devices acquire an IP address out of the private IP address space [8], such as 10/8 or 192.168/16, and the NAT box "translates" between the one external public IP address and all internal private IP addresses. This is based on a table on the NAT box, mapping ports to IP addresses. While NAT seemed to be a very convenient way of limiting the number of used IP addresses, it has some major drawbacks, some of them being discussed in [4]. Amongst others, NAT breaks the end-to-end principle, complicates multi-homing, and enables casual use of private addresses. These uncoordinated addresses are subject to collisions when companies using these addresses merge or want to directly interconnect using VPNs.

One of the "killer"-applications of the Internet was simply the end-to-end principle, meaning that every host could communicate with every other host in the network. Back then, this was something completely new that so far was not possible before. Suddenly, users were able to chat, browse web pages, exchange files, etc. This mutual and overall connectivity enabled the development of many applications that made the Internet popular.

NAT endangers this global connectivity, since an end-to-end communication is not possible anymore. In particular, if a home user wants to enable remote access to several of his or her devices from the Internet, this becomes rather tricky. The standard way is to use port forwarding. If the user has several web servers to share, or uses a nested NAT, then it becomes much more difficult. In the following section, we describe some of the approaches that can enable remote access behind a NAT box.

3.2 IPv4-based Solutions

Using NAT and IPv4 addresses, global remote access to devices behind the NAT box is indeed possible. However, these solutions have some drawbacks such as complexity, address conflicts or are not standardized by organizations such as the IETF. In this section, we discuss different ways of remotely accessing devices behind a NAT.

3.2.1 Port Forwarding

One of the most common ways of offering a service from within a NAT to the Internet is to forward an incoming port to a static IP address. So for example, in order to access a web server from the outside, a port forwarding of incoming TCP requests on port 80 is established to the private IP address of the web server. However, if several web servers are to be offered that run on the same port, this forwarding is not feasible anymore. Other workarounds such as proxies have to be used to redirect the request to the right web server. In addition, setting up port forwarding needs to be done manually by the user on the NAT box, and may thus be too complicated for home users.

3.2.2 Remote Control Management Application

Another possibility to offer remote access to devices behind a NAT is to establish a remote management software on either a server or the NAT box itself. Such a software would respond to incoming requests on a certain port using a predefined protocol. Based on the payload of the incoming request, this application could then forward the remote control request to the corresponding machine. This solution has several drawbacks. To our knowledge, there is no protocol standardized for this kind of remote control. So interoperability is not guaranteed between different devices. Moreover, in order to manage the devices and to forward the remote access requests, there is a high degree of complexity within such an application. Finally, this application has to be trusted, since many security issues could arise on it.

3.2.3 Virtual Private Network

Another approach is using Virtual Private Networks (VPN) [6]. A user can connect from the Internet to the VPN server behind the NAT. By using tunneling mechanisms (e.g. IPsec), communication with all hosts behind the NAT is then possible as if they were on the same Ethernet link. VPN also offers authentication and confidentiality of data transfer. While VPN is commonly used in companies and universities to offer remote access to file servers, printers, etc, it is not often used in home scenarios. This is partly because it is complicated to set up – both on the client and the server side. Another problem when using VPN behind a NAT is possible address conflicts. For example, a user behind a NAT using a 192.168/16 subnet might connect via VPN to another private network using the same subnet. This can lead to conflicts if there are devices with the same IP address in the two different networks.

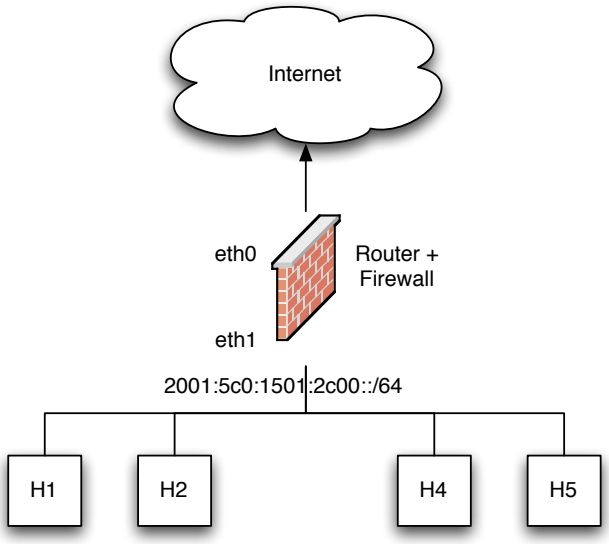

Figure 1: Remote control of hosts behind an IPv6 router

3.3 Our IPv6 Solution

While remote access using IPv4 is possible (as described in Section 3.2), these solutions have several drawbacks. Most importantly, they are difficult to set up and to administrate in a home user setting. By using IPv6, all the presented work-arounds are not necessary any more. A direct IP connection can be established from the Internet to any device behind an IPv6 router. Our demonstrator runs completely on IPv6 and allows remote access to the hosts from the Internet. This section describes the architecture and the configuration of our demonstrator.

3.3.1 Basic Architecture

If the Internet Service Provider provides an IPv6 prefix to a subscriber, the scenario described in the following can be used. This is the normal case and the most simple scenario. As our university does not provide an IPv6 prefix, we had to get one through a tunneling mechanism, so our demonstrator in reality corresponds to the architecture as explained in Section 3.3.2.

As displayed in Figure 1, setting up devices that run over IPv6 and are globally accessible is quite easy. A router with at least two interfaces acquires the prefix from the ISP. Hosts that are attached to the router either run DHCPv6 [2] or IPv6 Stateless Autoconfiguration [12] in order to configure an IPv6 address on their interface. For security reasons, setting up a firewall either on the router or on a different server is reasonable. This is not different to IPv4, where most DSL home routers already include a firewall. Now all hosts can be accessed from the outside knowing the IP address of the host. Protocols such as SSH can be used to remotely access the host.

In addition, a dynamic DNS service (such as the one offered by dns6.org) can be installed for dynamically mapping DNS names to the hosts. The service offered by dns6.org uses HTTP requests to register the IPv6 address to a DNS name.

3.3.2 Architecture of our Demonstrator

While our demonstrator mainly adhered to the architecture presented in the previous section, some more details had to be set up because our computer science department does not offer IPv6. This section describes the exact architecture and configuration of our demonstrator.

We have been provided five machines that only get private IPv4 addresses and are located behind a NAT. In order to test IPv6 connectivity, we installed a tunneling software called gw6c[2] on one of the machines that serves as our router. This software digs a hole into the NAT firewall and creates a point-to-point connection to a host under the administration of gw6c.com (as depicted in Figure 2) creating a new interface on Linux called tun0. Incoming and outgoing IPv6 packets to or from the router are encapsulated in UDP (as standardized in [5]) and can thus traverse the NAT. The gw6c client offers to acquire not only a single IPv6 address for the router, but also a whole prefix that can be used to configure the host interfaces. We obtained the prefix 2001:5c0:1501:2c00::/64 from the service provider. The gw6c client automatically configures 2001:5c0:1501:2c00::1/64 on the ingress interface. It then activates IPv6 Stateless Autoconfiguration (IPv6 SA) on that interface so that all clients configures an address out of the prefix using their MAC address.

In order to avoid that all hosts in the computer science department acquire an IPv6 address out of our prefix when using IPv6 Stateless Autoconfiguration, we set up a VLAN (802.1Q) on the five machines. This means that only the machines within the VLAN receive the Router Advertisements (RA) from the router and thus configure an IPv6 address.

In addition, we set up a firewall based on ip6tables that allows only incoming SSH traffic, outgoing HTTP traffic (for the dynamic DNS service) and ICMPv6 traffic (for the Neighbor Solicitation/Advertisement and Router Solicitation/Advertisement packets). We successfully tested to access each of the four clients from the Internet using SSH.

One possible enhancement of the scenario would be to run UPnP or a Service Location Protocol (SLP) in order to acquire the information on which host which service is remotely accessible.

4 Business Model

As previously discussed, enabling every device (such as PCs, smart phones, ovens, heating and surveillance systems) to have its own global address, via IPv6, provides new and exciting business opportunities that can be exploited. In particular, we have pointed out three types of services that would be empowered or fully deployed due to IPv6 connectivity features: home automation and security devices, before-arrival home services and data traffic exchange. The following subsections summarize the current situation and the general perspectives for these services and present the main features of our approach from a commercial point of view, through a SWOT analysis.

4.1 General Perspectives

The demand for these types of services is expected to stay solid and keep growing despite the current scenario of economic recession. Indeed, the market for home management technologies and services, which include automation and security mechanisms as well as the so-called before-arrival home features, has been expanding in the last years and is expected to reach in 2010 the world-wide total revenue of $2.4 billion (equivalent to 1.7 billion euros) [1]. Although it is a world-wide growth tendency, it becomes more relevant in societies with high standards of living, reliable communication infrastructures and a relatively robust housing sector. In particular, Europe is one of the main regions leading the development of home-based technologies and services, according to the forecasts of [1]. Existing services such as surveillance cameras or remote temperature control, which used to be luxury and minority goods, are now widening their scope and becoming more and more popular among middle-class consumers, due to the fall of installation and maintenance costs. New communication technologies, wireless in particular, encourage the emergence of more complex coordination systems and solutions, while

[2]source: http://www.go6.net

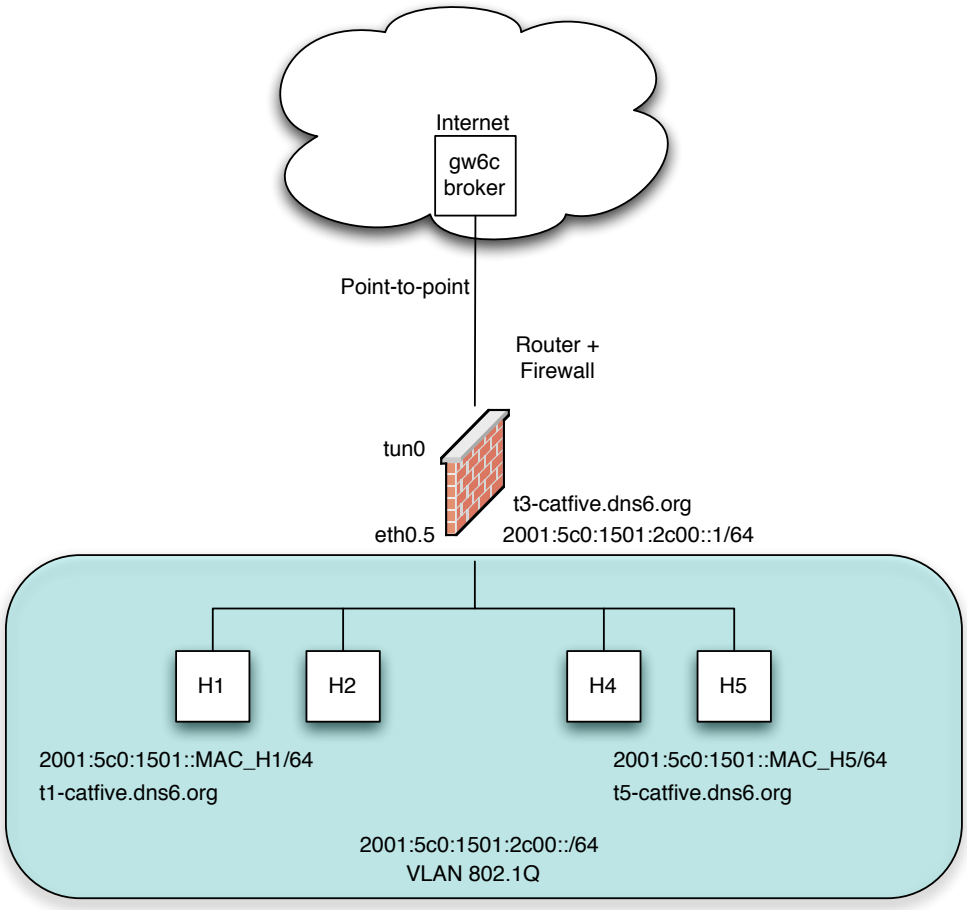

Figure 2: Our demonstrator using a tunnel to acquire the IPv6 prefix

an increasing number of new generation home devices (vacuum cleaners, heaters, light systems, etc) already provide automation features. In this context, remote control abilities from a mobile portable device (such as an iPhone) are a natural extension to the ongoing process and fit in the needs of a society of increasingly mobile individuals who are less than ever willing to spend time in home tasks.

For the third type of service, namely remote data access, again, studies like [13] confirm that the data traffic involving mobile devices keeps heavily increasing in the Internet, due to the growing demand of users and to the availability of new devices providing mobile connectivity (laptops, mobile phones and advanced PDAs)[3]. Not surprisingly, traffic analysis points out that multimedia contents are the fastest growing elements of the mobile traffic. Thus, providing remote user access to any type of data locally stored at home (such as music or movies) is a feature clearly demanded by consumers, as users would no longer need to carry storage devices when being outside from home.

4.2 SWOT Analysis

In the following, we briefly expose the main Strengths, Weaknesses, Opportunities and Threats (SWOT analysis) of our proposal.

[3]The Cisco Visual Networking Index Forecast expects the mobile data traffic to double each year from 2008 to 2013, reaching Compound Annual Growth Rates (CAGRs, average annual growth rate) in this period of 154% for video traffic and 112% for audio and data traffic.

4.2.1 Strengths

- For users:
  - *Universal connectivity.* Our proposal enables users to access and interact with all (remotely configurable) devices within their home network. That can be exploited for several different purposes, such as home automation, data exchange, multimedia content (audio, video and pictures) streaming, surveillance and security mechanisms.
  - *Simple management.* As the IPv6 addressing range is wide enough to assign each device a unique, Internet-wide reachable identity, no additional technology needs to be developed, installed or configured in order to get access to home devices from the outside. Only a small interface application in a mobile or portable device connected to the Internet is required to interact, via standardized and well-known protocols, with home machines, computers or other devices within the local domestic network.
  - *Plug & play feature.* In addition, using standard communication protocols allows the local devices to run properly without manual configuration, that is, in a *plug & play* fashion allowing, hence, the wide spread use of our proposal by home users.

- For goods and services providers (device manufacturers and ISPs):
  - *New partnership opportunities.* The deployment of the presented home-based services require the collaboration of companies providing the Internet connection, on one side, and companies manufacturing devices able to be reached/configured from the Internet, on the other side. This opens a new scenario in which partnerships with ISPs and manufacturers may offer a much wider range of joint products in the fashion of the current Internet + TV + telephone packages, for instance.
  - *Traffic profile and bandwidth.* From the point of view of the mobile connection, irruption of our proposal and consolidation of related services would probably imply a significant increase of the downloaded traffic, in particular related to multimedia streaming (audio and video), with the corresponding benefit increment for companies providing by-time connection or data amount transfers. From the point of view of the home network Internet connection, multimedia streaming might require a more balanced upload/download profile (and thus a more expensive fee) than usual[4].
  - *Differentiation opportunities for device manufacturers.* The implementation of mechanisms allowing remote access and configuration of home devices would enable competition among home device manufacturers, in the sense that companies supporting remote interaction and automation will add value to their products. Remote access compatibility would not be costly for devices already providing local automation features, due to the existence of standardized and well-known protocols to interact remotely, but would encourage innovation in the home devices market sector.

4.2.2 Weaknesses

- *User security issues.* Providing bidirectional connectivity to home devices within a home network also makes possible for a wider range of malicious attacks from the Internet against private devices. Then, not only a firewall is required to protect the home network, but also individual security mechanisms for each connected device need to be implemented. These additional features may turn more complex the home network maintenance.

- *ISP transition costs to IPv6.* The main cause for the slow IPv6 transition (only 1% of the required devices have been updated, according to [9]) stays in the huge costs for ISPs for

[4]Typically, contracted upload rates in home Internet connections are significantly lower than download. In contrast, requesting multimedia contents from the outside would require a higher rate in the uplink (from the point of view of the home connection).

replacing the current IPv4 infrastructure. However, with the lack of IPv4 addresses, this transition will have to happen sooner or later.

- *Short-term unavailability of compatible home devices.* Although the number of configurable home devices providing support to remote configuration is growing, it is still far from covering the current market offer. Some of the foreseen services would require not only compatible home devices, but also adaptations on home infrastructures, which are even slower. In these circumstances, our IPv6-based approach may not deploy all its potential, both in terms of services and profitability. However, with the growth in demand, we expect that these modifications shall already occur in the short-term.

4.2.3 Opportunities

Some of the most relevant opportunities for our approach rely on the conditions of technologies adjacent to the services that our proposal and IPv6 capabilities would enable.

- Growing availability of Internet connections (wi-fi hot spots) and UMTS coverage in public spaces, communication centers (such as airports, train or subway stations), public transport routes (subway lines and train branches) and urban areas. A widespread and even redundant Internet coverage (both through mobile phone networks and wi-fi access points) is an unavoidable requirement so that remote access to home devices in mobility conditions is credible and reliable as much as possible, both in space and in time.
- Development of home wireless networks based on IEEE 802.15 standards (Wireless Personal Area Networks, WPAN), which are able to connect and coordinate the different home devices in a single network reachable from the Internet.

Other than technical frameworks, there are some social implications for which our proposal might be useful, providing further opportunities. For example, with the aging process of developed societies and the increasing attention and investments of government to deploy care-dependency systems, Internet-reachable control mechanisms placed in old people's homes may be very helpful.

4.2.4 Threats

The first and most general threat that any technological approach implying economic investment should face is, undoubtedly, the global economic recession touching all productive sectors, and more strongly those which do not handle essential goods and services and thus depend on a quite elastic demand, as it is in our case. In particular, relationship between our proposal and home-based services and automation make our approach success more sensible to phenomena like housing crisis in part of Europe, which could slow down the adaptation of buildings to remote home automation services based on IPv6.

On the other hand, it is worth considering other threats represented by devices or products which could behave as a partial substitutes to some of the features provided by our approach, in particular the remote access to locally stored data.

- *Portable storage devices* (e.g., memory cards or USB Flash Memories). The increasing miniaturization and integration of these devices in mobile phones and PDA may make them a cheaper alternative (because it implies no traffic charges at all) to streaming of locally stored multimedia contents, at the expense of carrying the memory storage units when moving.
- *Internet multimedia streaming services.* Availability of multimedia contents from a laptop or mobile phone by streaming may be a partial competitor to the remote access to multimedia contents possibilities provided by our approach, only in case that these Internet

streaming services (such as Deezer or Last.fm, smart radios and repositories for music, and other servers for movies) are freely available. Even then, dependency on non-guaranteed-performance servers and ambiguity of their legal status concerning IPR are significant drawbacks with respect to the reliable and free streaming of locally stored multimedia libraries.

References

[1] Global Industry Analysis. Home automation - a global strategic business report, March 2008. Research Report # GIA-MCP1733.

[2] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney. Dynamic host configuration protocol for IPv6 (DHCPv6), July 2003. RFC 3315, Standards Track.

[3] V. Fuller and T. Li. Classless inter-domain routing (CIDR): The internet address assignment and aggregation plan, August 2006. RFC 4632, Best Current Practice.

[4] T. Hain. Architectural implications of NAT, November 2000. RFC 2993, Informational.

[5] C. Huitema. Teredo: Tunneling IPv6 over UDP, February 2006. RFC 4380, Standards Track.

[6] S. Kent and R. Atkinson. Security architecture for the internet protocol, November 1998. RFC 2401, Standards Track.

[7] Y. Rekhter and T. Li. An architecture for IP address allocation with CIDR, September 1993. RFC 1518, Standards Track.

[8] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, and E. Lear. Address allocation for private internets, February 1996. RFC 1918, Best Current Practice, BCP 5.

[9] P. Roberts. Internet society organization member ipv6 study, March 2009.

[10] P. Srisuresh and K. Egevang. Traditional IP network address translator (traditional NAT), January 2001. RFC 3022, Informational.

[11] P. Srisuresh and M. Holdrege. IP network address translator (NAT) terminology and considerations, August 1999. RFC 2663, Informational.

[12] S. Thomson, T. Narten, and T. Jinmei. IPv6 stateless address autoconfiguration, September 2007. RFC 4862, Standards Track.

[13] Various. Cisco visual networking index: Global mobile data traffic forecast update, January 2009. White Paper.