Comparing IPv4 and IPv6 Mobility and autoconfiguration for residential networks

Antti Järvinen
Helsinki University of Technology
Department of Computer Science and Engineering
46566U
Antti.J.Jarvinen@hut.fi

Abstract

In the future most of electric devices at home will communicate between each other using internet protocols. Nowadays most of the internet nodes use internet protocol version 4. New protocol version 6 will solve version 4 problems, but it is currently used only in laboratories. This paper will compare which one of the protocol versions will work better in residential networks from mobility and autoconfiguration point of view.

1 Introduction

Number of computers used at home is increasing all the time. At the same time various broadband technologies like xDSL are becoming more and more common at home. Prices of wireless LAN cards are going down. New digital television set-top boxes are connected to the Internet and even some new refrigerators have the Internet access. There is a clear trend that in the future most of the devices at home will be connected to each other and they will use the internet protocol when communicating with each other.

Residential networks might not have an administrator who takes care of the network. Users of the network might not have skills or simply they do not want to configure the network by them self. Residential network nodes are not necessarily constantly at one fixed place but rather they are moving around. Both IPv4 and IPv6 have solutions for these autoconfiguration and mobility problems. This paper will analyze are there notable differences between IPv4 and IPv6 and should the user prefer either of them.

The paper has the following outline. Chapter 2 identifies needs for mobility and autoconfiguration in residential networks. Chapter 3 describes different ways how a client can auto-configure itself in order to communicate in the Internet. Chapter 4 discusses advantages and disadvantages of mobility in residential networks. Chapter 5 summarizes how different solutions fit into the residential network and which solution home users should prefer.

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

2 Mobility and Autoconfiguration Requirements in Residential Networks

Mobility and autoconfiguration solutions has to fulfill following requirements in order to be successive in a residential network:

- Configuration has to be as easy as possible. If the user has to spend lot of time in administration, widespread adoption of technology cannot happen.
- New kind of devices, also with a slow processor and little memory must be able to communicate with other devices on the residential network.
- Communication between devices should not be restricted only to wired networks. Devices can also use wireless LANs, bluetooth, firewire etc. for communication. Used access technology has to be transparent to the user.
- The user will also access their residential networks from remote locations. This requires that devices have a public IP address or in some other way they are in the same virtual network.
- Devices have to have capabilities to communicate securely with each other.

If all of this is too complicated only people who are willing to spend time on learning new technology will use the new technology.[12]

3 Autoconfiguration

With autoconfiguration devices can configure themselves so that they can communicate with each other. There are both stateless and stateful solutions. In both cases client configuration can be quite easy. But in stateful methods there is need for a server, which remembers what kind of configurations it has given out.

3.1 DHCPv4

The Dynamic Host Configuration Protocol (DHCP) is designed for supply configuration parameters to clients. [7] A client can obtain all needed parameters with DHCP to communicate with any host on the internet. These parameters include an IP address, a subnet mask, a default gateway and DNS servers. In the client side no configuration is needed. DHCP is stateful, so there has to be a DHCP server, which knows what addresses it, has given to the clients.

The client tries to find a DHCP server by sending broadcast to local network broadcast address, i.e. 255.255.255.255. This means that in practice every home network must have a DHCP server and somebody has to configure it. Fortunately a DHCP server is not so complicated, so it can be included e.g. in an ADSL router and ISP has configured it before giving it to the customer. If network configuration changes there are no automatic ways for

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

reconfiguring the DHCP server. ISP has to take remote session to the server and reconfigure it manually.

There is shortage of IPv4 addresses, so in practice these DHCP servers give out private addresses, which are not routable in the public Internet. So there has to be a NAPT device between public and private internet. The NAPT device changes source address of outgoing packets and keep track of connections. So it is able to make translation other way around when packets are coming from the public Internet. Having the NAPT device between a residential network and the public Internet blocks connectivity from outside to the residential network effectively.

3.2 IPv6 Stateless Autoconfiguration

IP version 6 addressing architecture differs from IP version 4 in such way that addresses are for interfaces not for nodes. Every node must have at least link-local address on its every interface. [10]

IPv6 offers a simple way for IPv6 clients to configure their IP addresses. IPv6 nodes can obtain non-conflicting link-local addresses without any configuration. Link-local addresses consist of two parts. Prefix FE80::0 and an interface identifier. Typically an interface identifier has 64 bits and it can be constructed from interface's link-layer address. Interface's link-layer addresses are globally unique, so there should be no problems creating an unique link-local address. Because of privacy problems, everybody does not want to use a link-layer address. Physical location of individual can be easily find out, if individual's link-layer address is known. E.g. using traceroute. [9]

Stateless autoconfiguration can also handle situations where a node has selected an interface identifier that already exists in the network. Before the IP address is actually taken into use, the node sends neighbor solicitation messages to all nodes in the same subnet. If some node already has the same IP address, it answers to the original node. In this case the node has to create a new interface identifier and start over.

In normal situations a node can easily configure itself. With stateless autoconfiguration the node can obtain a valid IP address without authentication on the local site. This can cause problems if a home network has a wireless network. Anyone on the coverage area can get an IP address and starts communicate. And even worse they can do denial of service attacks by answering to all neighbor solicitation messages and thus prevent any other node's access. These kind of DOS attacks can also happen in IPv4.

Home networks will also use network resources outside the local network. Stateless autoconfiguration can also configure site-local and global addresses. A router sends periodically router advertisements that may have multiple site-local and global prefixes. A client assembles its site-local and global addresses simply by attaching its interface identifier after prefixes.

So in spite of its name, stateless autoconfiguration needs some configuration in the router. This is not a problem if the router is from ISP and ISP has already configured the router. Much bigger problem is that stateless autoconfiguration provides no ways for determine DNS servers. Some applications can work without DNS servers, e.g. Jini services and file

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

and printer sharing using the SAMBA protocol. However web surfing with IP addresses is quite cumbersome.

3.3 DHCPv6

DHCP for IPv6 allows more precisely and controlled configuration than just stateless autoconfiguration. However they both can work in the same environment. DHCP for IPv6 offers same features as its IPv4 counterpart and also some extra features due IPv6 additional features. [8]

Some of these additional features might be too heavy for home environments. For example features like secure dynamic updates to a DNS server might not be needed in home environments, where used devices do not change frequently.

DHCPv6 draft itself does not define all possible configuration options. Additional options can be defined easily, because all options share common format. DHCP options can also be added to DHCPv4 for, but adding new options afterwards brings certainly problems with interoperability. DNS configuration options are one of the options, which are not defined in the draft. DNS configuration is so common that all clients and servers will know it, but situation can be different in seldom used options. Other options, which might be useful, are IP addresses of printers and WWW browser proxy.

Like DHCPv4, DHCPv6 does not require that the DHCP server resides on the same link as the client. In this case there has to be a DHCP relay on the same subnet as the client resides. In IPv4 this is not widely used option, mainly because a DHCPv4 server is quite simple and adding relay increases administration work because relay has to know the DHCP server address. In IPv6 it is not needed to configure the relay, because it can use all DHCP server's multicast address when it wants to communicate with the DHCP server.

In DHCPv4 a client always initiates changes. In DHCPv6 a server also can inform the client about changes. This is quite handy in situations where there are new services on the network or current settings have been changed.

3.4 DNS discovery without DHCP

There are also drafts about discovering a DNS server without a DHCP server. If the DNS server can be discovered without any configuration on the local network, then it would be ideal for home networks.

Some solutions, like IPv6 Stateless DNS discovery [11], require that DNS servers have a well-known site-local IP address. In this case the DNS server has to be on the same site with home. Typically homes do not have a DNS server, but residential gateway can relay these DNS requests to ISP's DNS server.

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

4 Mobility

IP addresses consists of a varying length network part and a host part. The network part defines IP address' topological location in the Internet and IP packets are routed with that information to the right destination. When a user changes his/her attachment point to the Internet, his/her IP address has to change and existing connections will not work anymore. [1]

This will cause problems also in residential networks. A Residential network can also have different subnets. A secure wired intranet where no encryption is needed and an insecure wireless LAN that can be eavesdropped by everyone. When a device moves between these subnets connections will break because an IP address changes.

Mobile IP can solve these problems in the network layer. Because the problem is solved in the IP layer all existing protocols above IP and applications will work without any changes. In IPv4 mobility is added to the stack afterwards. In IPv6 mobility is taken into account when designing the protocol.

Main idea in Mobile IP is that a user has a home network where user's home agent is situated. A node that can change its attachment to the Internet is called a mobile node. The Mobile node informs always the home agent when it has changed its location. Other nodes communicating with the mobile node are called correspondent nodes and they do not know mobile node's current location, at least when starting to communicate with a mobile node. So they first sent datagrams to the home network where the home agent will intercept packets and encapsulate them to mobile node's current care-of address. After that how communications continue depends on used protocol version.

Figure 1 show simplified example of mobile IP. A correspondent node sends a datagram to a home agent, which tunnels it to a foreign agent. A mobile node sends datagrams directly to a correspondent node.

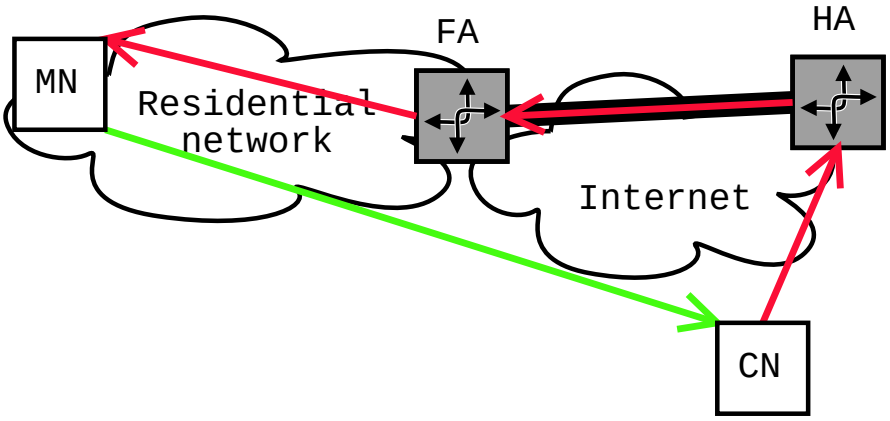

Figure 1: Mobile IP simplified example

If mobile IP is used at home, most probably the home agent is not located at home. Because home agent is a router, which can handle several mobile node's communications, it is more logical to put it in the ISP's core network.

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

In the following subsections will be discussion about following topics:

- Overview of the different mobility solutions
- Autoconfiguring mobility
- Security issues

4.1 Mobile IPv4

First mobile IPv4 specification was completed in 1996, fifteen years later than the IPv4 specification [2]. The protocol had to be designed so that it works with all IP nodes whether they support mobility or not.

When a mobile node is in its home network it works like any other IPv4 node. Packets are sent to mobile node's home address and packets sent by the mobile node have its home address as source address. When the mobile node is not in the home network it acquires care-of address, i.e. mobile node's current point of attachment to the internet. It registers this new care-of address to its home agent. Registration has to be authenticated somehow. Otherwise anybody can register with somebody else home address and get his/her IP packets. Registration requests are also protected against replay attacks, meaning that if a malicious user sends later already sent registration request, the home agent discards it.

Mobile IPv4 protects only registration messages. Securing other traffic has nothing to do with mobility. However mobile IPv4 can work both with application level (SSH or SSL) or network level (IPSEC) security solutions.

There are two different ways for acquiring care-of address in the foreign network. There can be a special a router called a foreign agent, which advertises it to visiting mobile nodes. In that case a mobile node registers through this foreign agent. If there are no foreign agents, the mobile node acquires care-of address usually using DHCP and register itself directly to the home agent. When a correspondent node sends IP packet to mobile node's home address, the home agent intercepts it and tunnels packet to the care-of address. A Foreign agent or the mobile node detunnels packet and forwards it to the mobile node. To other direction packets can be sent directly to the correspondent node.

4.1.1 Problems

Sending packets directly to the correspondent node do not work always. Packets have mobile node's home address as source address and if there is a firewall or a router doing ingress filtering, it will drop the packet. The router thinks that somebody is trying to spoof the IP address because a source address is not topologically correct. Using reverse tunnels can circumvent problem. A Foreign agent or a mobile node itself puts responses back to the correspondent node to a tunnel that is destined to the home agent. The Home agent decapsulates this tunnel and send it further. According to the new IPv4 mobility support RFC, this is mandatory to all nodes. [1]

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

Because of IPv4 address shortage home networks will most probably get IP addresses which IANA has reserved only for private use. A node with a private address cannot communicate directly to the public Internet, instead between public and private internet there is a NAPT device, which translates addresses.

The Home agent cannot tunnel packets to mobile node's care-of address. There is an IETF draft how this can be overcome by tunneling all traffic inside UDP packets. A mobile node always starts communication by sending a registration request to its home agent. Same time connection is opened through the NAPT device and the home agent can tunnel packets through this UDP session. Solution is not very elegant, but in practice it works if a firewall has not blocked used UDP ports. Moreover correspondent nodes can initiate connection to a mobile node while the mobile node is behind the NAPT device.

One of biggest problems in Mobile IPv4 is that in practice all traffic goes through a home agent. If communicating nodes are in the other side of the Internet than the home agent, packets consume bandwidth and resources in many links and routers. If a mobile node is in a residential network and communicating with some other node outside the residential network, problem is not so bad. Because the home agent is located in the ISP's premises packets will in every case go near the home agent. However when the residential network nodes communicate with each other, routes are very sub-optimal.

In theory a correspondent node can tunnel packets directly to mobile node's care-of address according to Route Optimization in mipv4[6]. In practice this won't work, because normal IPv4 nodes do not know anything about route optimization. There are also security problems, because correspondent nodes cannot blindly trust location updates from a mobile node. In a residential network route optimization might work, nodes can quite easily create security associations between each other, because the same person administrates nodes.

4.1.2 Autoconfiguration

The old mobility RFC[2] was not very user-friendly. The user had to know his/her home agent, home address and shared security associations between those. Fortunately newer RFCs has improved this a lot. [3, 1]. A Mobile node does not need to know its home address beforehand. The user can be globally identified with NAI, which has form user@realm. Authentication can be done on an existing server, which also serves customers who are dialing in with a modem.

Finding the home agent is little harder. The mobile node can send a registration request to the broadcast address of its home subnet. Problem is that the mobile node does not know its home subnet. One solution for finding the home agent is to use DHCP mobile IP home agent option. If a residential network has some gateway device from ISP, it can be already configured to advertise user's home agent. If the address changes unfortunately it has to be reconfigured to every of these devices.

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

4.1.3 Residential network without real network

With the help of mobile IP a residential network can be created without any physical network, if devices just acquires care-of address. Nobody wants to offer internet access for free, but if there is a foreign agent, network access can be controlled. The foreign agent does not authenticate mobile nodes itself. Instead it asks a local AAA server to verify that the mobile node has valid credentials. A local server might not have enough information to do that so an AAA server from mobile node's home domain is consulted. After the mobile node is authenticated and authorized to access network, accounting can start. [4]

Local and home AAA servers need a security association between them. If they are owned by same organization or there are just a few organization, creating security associations is not a problem. In practice there could be thousands of different organizations or even individuals setting up wireless hot-spots. It is not reasonable that everybody share a security association between each other. Instead broker could be used. In figure 2 all parties trust the broker and the broker can help the local and the home domain creating a security association between them even if they don't know each other.

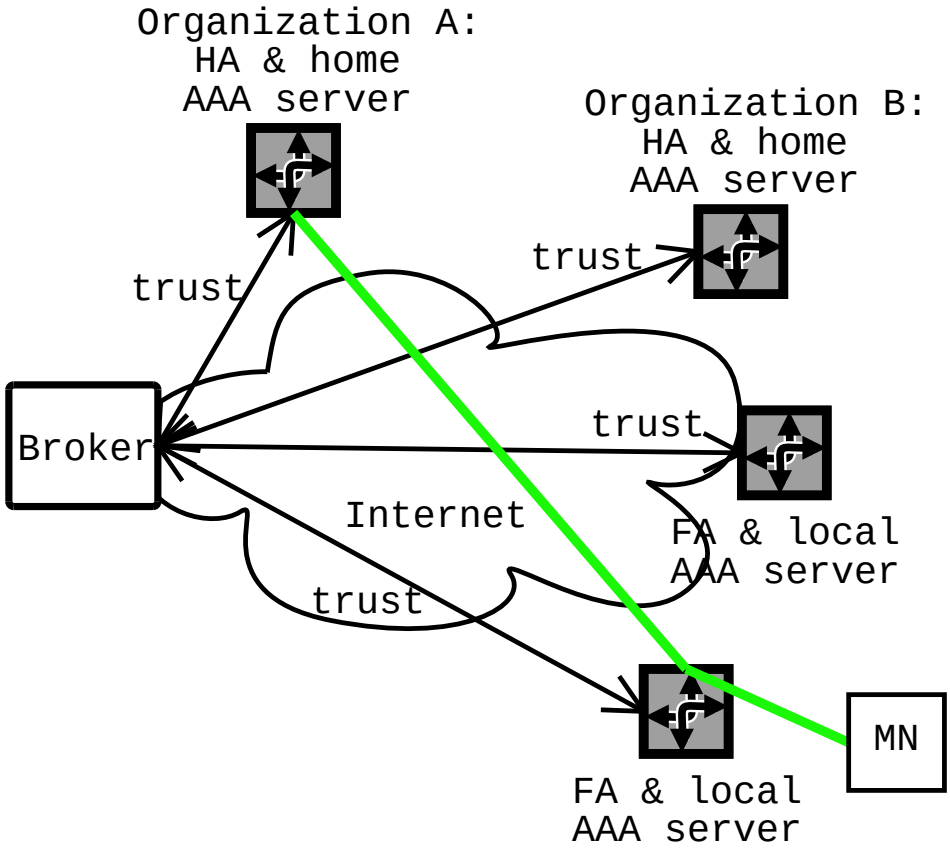

Figure 2: AAA broker

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

4.2 Mobile IPv6

Mobile IPv6 specification is based on Mobile IPv4. Although there are many improvements, basic concept is still the same. A mobile node has a home agent on its home network, which always knows mobile node's current location and can tunnel packets to the mobile node. Mobility is integrated into IPv6 and also stationary nodes are required to understand it. [5]

4.2.1 Changes from Mobile IPv4

Mobile nodes does not need to send control messages in separate IP datagrams. Instead those messages can be piggybacked to normal IP datagrams.

Route optimization is required part of the protocol. In mobile IPv4 this was separate function and needed different messages. Now a same message is used as in registration to a home agent. A mobile node sends a binding update about its current care-of address to a correspondent node. The correspondent node stores it in a binding cache. When the correspondent node sends datagrams to the mobile node it checks if it has a valid entry in the binding cache and inserts a routing header to a datagram. The routing header specifies that the datagram is first sent to the care-of address and after that to the home address inside same node.

Problems with a firewall doing ingress filtering are also solved with IP headers. Datagrams sent by a mobile node uses the care-of address as a source address. A home address destination option is added to a datagram and correspondent node's IPv6 stack will hide the care-of address and instead show the home address to upper layers.

IPv6 nodes should implement enough strong authentication and encryption methods, mainly IPSec, by themselves. This simplifies Mobile IPv6 protocol because it can assume that there is a working security model underneath. Devices in residential networks can verify that the identity of other devices is what they claim to be.

Mobile IPv6 does not have foreign agents anymore. They are not needed anymore. There are plenty of public IP addresses and mobile nodes can obtain care-of addresses e.g. using stateless autoconfiguration. When there are no foreign agents, Mobile IPv6 does not try to solve access control on foreign networks.

4.2.2 Autoconfiguration

In mobile IPv6 a mobile node can discovery the home agent address dynamically by sending an ICMP home agent address discovery request to mobile IPv6 home-agents anycast address to its home prefix. This procedure might be needed also if home subnet is reconfigured and mobile node's home agent has changed. Mobile IPv6 can also tolerate changes with its home prefix. The home agent sends mobile prefix advertisements messages to the mobile node. When the mobile node receives these messages and notices that its home prefix has changed, it takes the new prefix in use and removes the old one.

In mobile IPv6 there is no need to obtain a home address from the home agent like in

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

mobile IPv4. Mobile node can construct it, when it knows its home prefix, using e.g. stateless autoconfiguration. Even if mobile IPv6 can more easily change its home address, there is still same problem as in mobile IPv4, how to initially obtain a home prefix.

5 Conclusions

Autoconfiguration and mobility for residential networks are not yet so easy to use that everybody will use it. In IPv4 there has to be a DHCP server, which offer IP addresses and DNS server addresses to clients. If these settings change somebody has to manually reconfigure the DHCP server. There are also problems with NAT breaking connectivity towards a residential network. If devices are using mobile IP, some of the problems can be solved. There are still problems with sub-optimal routes when communicating with correspondent nodes.

Mobile IPv6 does not suffer from sub-optimal routes. However there are no methods for whole Internet wide key management, so in practice route optimization will not yet work. IPv6 based-solutions has better support for security, because all implementations has to support IPSEC. In IPv4 some third party products are required.

Mobile IPv6 also does not have access control in a foreign network like mobile IPv4 foreign agents. Mobile IPv6 mobile nodes also do not yet have a common way to present its credentials like NAI in Mobile IPv4. Authentication in mobile IPv4 for the end-user can be as easy as authentication when dialing with a modem to the ISP. A mobile IPv6 user has to struggle with security parameter indexes and shared keys.

Mobile IPv6 specifications are still Internet-Drafts, while there are several mobile IPv4 products on the market. If a residential network user wants to have a mobility enabled network she should prefer IPv4, at least until networks in general use IPv6 and problems with Mobile IPv6 accounting and authentication are solved.

6 Abbreviations

AAA Authentication, Authorization and Accounting

CN Correspondent Node

DNS Domain Name System

DOS Denial Of Service

FA Foreign Agent

HA Home Agent

ISP Internet Service Provider

IP Internet Protocol

LAN Local Area Network

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

MN Mobile Node

NAT Network Address Translation

NAPT Network Address Port Translation

NAI Network Access Identifier

References

[1] Charles E. Perkins, editor, IP Mobility Support for IPv4, RFC 3220, IETF Network Working Group, January 2002

[2] Charles E. Perkins, editor, IP Mobility Support, RFC 2002, IETF Network Working Group, October 1996

[3] Pat R. Calhoun, Charles E. Perkins, Mobile IP Network Access Identifier Extension for IPv4, RFC 2794, IETF Network Working Group, March 2000.

[4] Steven M. Glass, et al. Mobile IP Authentication, Authorization, and Accounting Requirements RFC 2977, IETF Network Working Group, October 2000.

[5] David B. Johnson, Charles E. Perkins, Mobility Support in IPv6, Internet Draft, IETF Mobile IP Working Group, March 2002. *(work in progress)*

[6] Charles E. Perkins, David B. Johnson, Route Optimization in Mobile IP, Internet Draft, IETF Mobile IP Working Group, September 2001. *(work in progress)*

[7] Ralph Droms, Dynamic Host Configuration Protocol RFC 2131, IETF Network Working Group, March 1997

[8] Ralph Droms, editor, Dynamic Host Configuration Protocol for IPv6 (DHCPv6), Internet Draft, IETF DHC Working Group, December 2001. *(work in progress)*

[9] Susan Thomson, Thomas Narten, IPv6 Stateless Address Autoconfiguration, RFC 2462, IETF Network Working Group, December 1998

[10] Robert M. Hinden, Stephen E. Deering, IP Version 6 Addressing Architecture, RFC 2373, IETF Network Working Group, July 1998

[11] Dave Thaler, Jun-ichiro itojun Hagino, IPv6 Stateless DNS Discovery, Internet Draft, IETF Network Working Group, November 2001. *(work in progress)*

[12] Brian Haberman, George Tsirtsis, Home Networking with IPv6, IPv6 forum, http://www.ipv6forum.org/navbar/papers/Home_Networking_IPv6_2000.pdf [referred 26.2.2002]