IPv6 Prefix Delegation-based Addressing Solution for a Mobile Personal Area Network

P. Pääkkönen, J. Latvakoski
VTT Technical Research Centre of Finland, Kaitoväylä 1, 90571 Oulu, Finland
[Pekka.Paakkonen, Juhani.Latvakoski]@vtt.fi

Abstract

This paper provides a dynamic IPv6 prefix delegation-based addressing solution to enable Internet connectivity when a Personal Area Network (PAN) is moving between sub-networks. A PAN consists of a cluster of mobile devices, which are dynamically connected with each other and move around together. The approach is based on IPv6 stateless address auto-configuration, and Automatic Prefix Delegation Protocol for IPv6. The problems related to addressing, mobility and IPv6 prefix delegation are evaluated with the constructed prototype. The experiences indicate that the solution is quite light and enables session continuity in subnet changes for any mobile node of a PAN. In addition, the solution does not exclude application of Mobile IPv6 (MIPv6), however Mobile IPv6 is not necessarily needed when Session Initiation Protocol (SIP) based mobility is applied. By using SIP, route optimization is also achieved and IPv6 encapsulation is avoided with UDP-based sessions. However, the solution is not necessarily very scalable to big mobile networks.

1. Introduction

Today, the mainstream in the wireless world is the integration of the Internet and cellular mobile systems. This is indicated by heavy industrial participation in the standardization organizations such as 3GPP, 3GPP2 (www.3gpp.org, www.3gpp2.org) and the Internet Engineering Task Force (IETF). One essential effort in these forums has been related to enabling Internet access for a cellular mobile terminal. Another important technology from the mobile terminal viewpoint is the short-range low power radio technologies, such as Bluetooth (www.bluetooth.org). These technologies enable proximity connections between mobile terminals. A set of referred terminals can be seen as a cluster i.e. network of interacting devices, and such a network may be mobile. Today, the mobility of such a network is still a rather open issue. This paper has especially focused on the mobility of a specialized mobile network called a Personal Area Network (PAN) from the IPv6 addressing and end-to-end connectivity viewpoint.

Our initial motivation for this research has been to find a *light-weight* mobile network addressing solution applicable in the context of the PAN. The PAN type of mobile network is assumed to be a dynamically established ad hoc network, which can also work in stand-alone mode, but a natural need is the connectivity into the static network infrastructure. The provided approach is based on the IPv6 Prefix Delegation (PD) mechanism, which is evaluated here in a prototyped PAN environment. The experiences indicate that MIPv6 and IPv6 encapsulation is not needed when SIP-based mobility is used with UDP sessions. In the solution, MR temporarily acquires an aggregated IPv6 prefix (MNP) from a local domain and traffic would go through the local access router. Thus, the contribution of this paper is the evaluation of the IPv6 PD solution applicability for a dynamic PAN type of mobile ad-hoc network. The evaluations indicate that the solution is quite light, and thus quite realistic for application in the PAN context.

Related work is presented in the next chapter, the concept for a mobile network related prefix delegation is presented in chapter 3, the experiments are illustrated in chapter 4, an evaluation of the results is performed in chapter 5 and concluding remarks are presented in chapter 6.

2. Related work

The MANET working group [1] has focused on the networking and routing of a standalone ad-hoc network. A solution for enabling global reachability of a MANET network has been proposed, but this alternative does not consider network mobility [2]. There are some solutions that rely on Mobile IPv6 (MIPv6) in enabling mobile

Proceedings of the 23 rd International Conference on Distributed Computing Systems Workshops (ICDCSW'03)
0-7695-1921-0/03 $17.00 © 2003 IEEE

network connectivity to the Internet [3,4]. In these solutions, one or more Mobile Routers (MR) is used as a gateway between the fixed Internet and the mobile network. A mobile network solution based on MIPv6 extensions is offered in [5], which requires changes to the Home Agent's (HA) binding cache. A new prefix-flag is applied to indicate whether the Home Address -field of a binding cache entry contains a Mobile Network Prefix (MNP) or an IPv6 address. MNP is an IPv6 prefix used to identify a mobile network in the Internet topology. The HA exchanges routing protocol information with the MR of a mobile network by using bi-directional tunneling. When updating routing protocol information, if HA finds an entry in the routing table which has MR Home Address as the next hop address, a new entry for that MNP is added to the binding cache by setting the Care-of-Address (COA) to the MR's COA. This is because the MR is used as a gateway between the Internet and the mobile network. When IPv6 packets are sent to the mobile network with a routing prefix of the mobile network (MNP), a lookup to the binding cache enables communication between an MN and CN. [6] proposes two scenarios for mobile network connectivity: consumer and fully enabled mode. In the former, the MR's HA injects static routing table entries for the MNPs used on the MR's ingress interfaces and has the next hop set to the MR's Home Address. By using this indirect addressing method (Routing table: MNP -> MR's Home Address, Binding cache: MR's Home Address -> MR's CoA) with the routing table and binding cache entries of MIPv6, it is possible to enable mobile network Internet connectivity. In the latter scenario, MR runs a dynamic routing protocol, and bi-directional tunneling is used to exchange up-to-date routing information. In both scenarios the MR forwards IPv6 packets coming from the mobile network to the tunnel towards its HA. Traffic coming from the Internet is tunneled to the MR by the MR's HA. This makes nodes of the mobile network reachable via the MR's HA. IP packets coming from the MR are sent through the foreign router as defined in MIPv6. [7] proposes to use a single MNP for a mobile network. In this solution the MR sends Prefix Scope Binding Updates (PSBU) to its HA and the CNs of the mobile network to inform the MNP by using a new option in the Binding Updates of MIPv6. A new entry for the MNP is created to the binding cache (MNP -> MR's COA) of the CNs and the HAs based on the received PSBUs. A new prefix-flag is also present in the binding cache, which indicates whether the entry corresponds to an IPv6 prefix (MNP) or a 128-bit IPv6 home address. A new prefix-length field in the binding cache indicates the length of the MNP. By using these extensions of MIPv6 it is possible to enable the Internet connectivity of a mobile network.

The mentioned solutions [5,6,7] rely on the assumptions that MIPv6 will be the de facto mobility solution. The NEMO WG in the IETF [8] focuses on enabling transparent session mobility for the nodes of a mobile network. The shortcomings of these solutions are possible modifications into MIPv6 protocol and IPv6 encapsulation [9]. If the mobile network is nested i.e. the mobile network's topology tree consists of multiple MRs, multiple IPv6 encapsulation might be required, which is never an ideal situation.

3. Concept: Dynamic prefix delegation for PAN mobility

A MANET network can be characterized by its dynamic topology and routing aspects. Every node in such a network is free to reorganize with the use of a MANET based ad-hoc routing protocol. A NEMO network is considered to be of static nature and the transparent Internet connectivity of its nodes during mobility is of primary concern to the WG. There is a lack of a solution that combines these two approaches to create a dynamic mobile ad-hoc network with Internet connectivity. PAN is an example of this kind of network. The biggest differences between a PAN type of mobile network and the NEMO network are that MIPv6 is not necessarily used, and the MNP of the PAN is temporarily acquired by using PD as opposed to the static MNP usage required from a NEMO type of network.

A benefit arises from PD usage in a PAN type of mobile network, and it is *route optimization*. If a NEMO typeof mobile network is attached to the Internet in a foreign network, bi-directional tunneling through the MR's HA is used to route traffic to and from the mobile network. This non-optimal routing and IPv6 encapsulation could be avoided by using temporary MNPs for a PAN type of mobile network. The MR could acquire an aggregated IPv6 prefix (MNP) from a foreign domain and traffic would go through a foreign access router. The drawback in this case is that the MNP has to be returned when the network moves to a new domain. Because of these reasons, a PD related to mobile networks is needed. Figure 1 illustrates the situation of an IPv6 PD related to mobile networks. MR, MN1 and MN2 form a mobile network. If the MNs want to establish a connection with any Corresponding Node (CN) of the Internet they must have an IPv6 global unicast address [10]. This paper assumes that these addresses are auto-configured on individual MNs using IPv6 stateless address auto-configuration [11]. In order for this to be possible, the MRs have to somehow acquire an MNP, which will be advertised on their ingress interfaces. A PD will be used for this purpose. Whenever the PAN is attached to an access router, the PD is used to get a local aggregated MNP. When the PAN moves from one access router to another, a new aggregated MNP is received. The old MNP is returned to the old access router. Using dynamic routing table updates in the MR and the local access router enables Internet access of the mobile network.

4. PAN experiments

4.1. Architecture of experiments

The network structure of the solution is illustrated in Figure 2. Because we used no routing protocols in the prototype system, the routing tables had to be configured manually. All the nodes have a Linux operating system with IPv6 support enabled by using USAGI [13] IPv6 implementation. The CN is connected via a hub to the router. The WLAN/Ethernet router has one Ethernet interface and two WLAN interfaces. It has one IPv6 prefix delegator [12] running on each of its WLAN interfaces, and it can be thought of as two separate static routers (router1, router2). The MR has one WLAN interface through which it communicates with the routers and one Ethernet interface, which is used to communicate with the MN of the mobile network. The MR has an IPv6 prefix requestor [12] running on its WLAN interface. The MNhas one Ethernet interface for communication with the MR. The MN and MR form a PAN type of mobile network. All the WLAN cards are ORinoco 11Mb silver cards and have been configured to the ad-hoc mode.

4.2. Prefix delegation

In this use case, the MR acquires a MNP from a router and begins advertising it on its short-range link for IPv6 stateless address auto-configuration. The MR has been preconfigured to be the router for the mobile network. The MNP delegation for a mobile network is illustrated in figure 3 and it is described as follows:

1. The MR receives a Router Advertisement (RA) message from router1. MR autoconfigures a global unicast address (3000::202:2dff:fe3a:d072) on its interface based on the received Prefix Information -option [14] in the RA.
2. The MR sends a Prefix Request with the code Delegator Query to the all-routers multicast address. The purpose of this message is to search for IPv6 prefix delegators on the link.
3. Router1 has a delegator on the link and it listens to all-routers multicast address-related messages and is willing to delegate prefixes to the requestor. A Prefix Delegation with code Prefix Delegator is unicast to the MR.
4. The MR chooses to request an MNP from the delegator and sends a Prefix Request with the code Initial Request to the delegator.

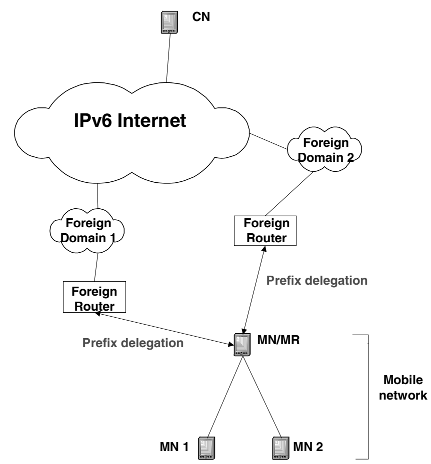

Figure 1. IPv6 prefix delegation in mobile networks.

5. Router1 sends a Prefix Delegation with the code Prefix Delegated to the requestor, and prefix information is contained in the Prefix option. The option contains the length and lifetime of the prefix. Router1 also updates its routing table based on the delegated prefix. This means that all traffic related to the delegated MNP (3000:0:0:1/64) is directed to the MR (3000::202:2dff:fe3a:d072).
6. The MR receives the Prefix Delegation and updates its routing table. This means that router1 is designated as the MR's default router (::/0-> 3000::1). The MR starts acting as a router on its Ethernet interface and begins sending unsolicited RAs on the link advertising the received MNP with the L- and A-flag set in the Prefix Information -option of the RAs. The Router lifetime in the Router Advertisement has to be greater than zero to indicate to the MN that the MN is willing to act as a default router for the MN.

4.3. PAN mobility

After the IPv6 address autoconfiguration the MN establishes a network session on top of UDP with the CN using SIP [15]. This is possible because the MN now has a global IPv6 unicast address, and the MR routes packets between the mobile network and the Internet. The IPv6 prefix/address management is described in the following steps (see figure 4):

1. The MR decides to use router2 instead of router1. It returns the initial MNP to router1 (delegator1) by sending a Prefix Request with the code Prefix Return and includes the MNP information in the Prefix option.
2. The delegator in router1 sends a Prefix Delegation with the code Prefix Returned to the requestor. Now the old MNP has been successfully returned to the old router.

Proceedings of the 23 rd International Conference on Distributed Computing Systems Workshops (ICDCSW'03)
0-7695-1921-0/03 $17.00 © 2003 IEEE

Router1 deletes the entry for the returned MNP from its routing table.

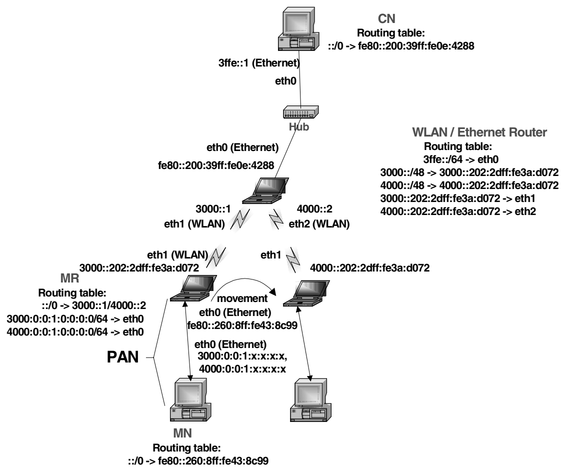

Figure 2. Network structure of the prototype system.

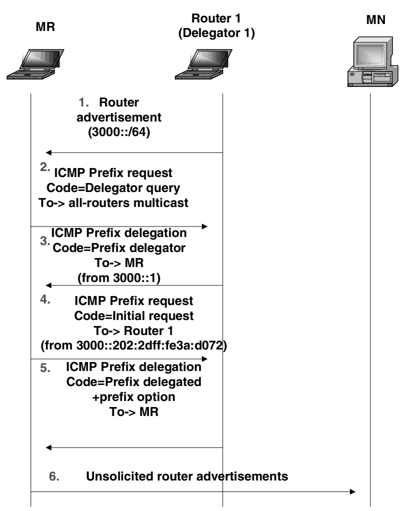

Figure 3. Prefix delegation use case.

3,4,5,6 The PD procedure is executed as described in the PD use case, except that the requestor decides to use the delegator operating in router2. The MR also deletes router1 as its default router and sets router2 as its new default router by refreshing its routing table.

7. After the MR has received a new MNP from router2, it begins advertising it with a new lifetime on its local link using RAs. The MR also advertises the old MNP with a preferred and valid lifetime of 0, to expire the addresses derived from the old MNP.

8. The MN has polled the expiration of its old global IPv6 address and detects that it has changed and a new global IPv6 address is available. The SIP UA sends a re-INVITE to the CN, which contains information about the new location of the SIP UA in the Contact-header and new session information is described in the SDP payload as described in [16].

9. The remote SIP UA sends a 200 OK as an acknowledgment to the INVITE.

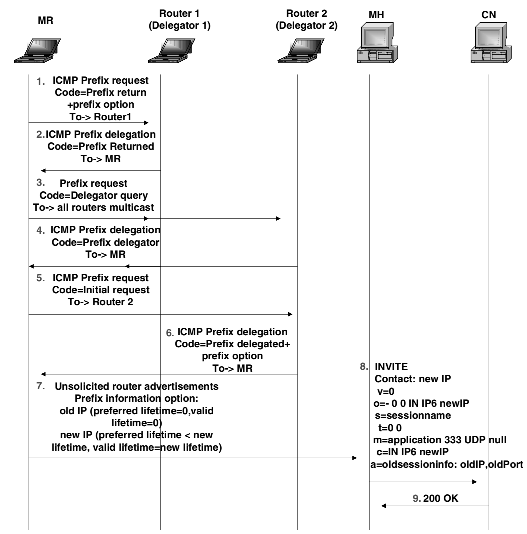

Figure 4. Network mobility.

5. Evaluation

5.1. Addressing

In our experiments it is assumed that router1 and router2 receive an IPv6 prefix and keep track of the longer MNPs derived and delegated from that prefix. The MR then can advertise the delegated prefixes on its short-range radio link. If the MR has multiple links, then it has to request multiple MNPs and advertise each MNP on a separate subnet. Another alternative for the delegator is to advertise MNPs shorter than 64, from which the MR can derive longer aggregated MNPs for multiple subnets.

The experiments indicate how the route stays optimized when using temporary MNPs. In fact, the route was always optimal, because the MNP was always derived in an aggregated way from the IPv6 prefix used in the local access router. This means that no HA is involved in the routing, because MIPv6 is not used.

In the demonstration we chose to use IPv6 stateless address auto-configuration for MNs instead of stateful methods such as Dynamic Host Configuration Protocol v6 (DHCPv6) [17]. This is because stateless address autoconfiguration is much more flexible to use than stateful address allocation. Only one MNP per subnet has to be acquired for stateless address autoconfiguration instead of managing IPv6 addresses of hosts connected to a mobile network with possible multiple subnets. The addresses are generated based on the Prefix Information -options of the received RAs.

MR auto-configures a global IPv6 unicast address based on the RAs received from static routers. [14] does not constrain or define any action for routers receiving Prefix Information -options in RAs from other routers. This means that a global IPv6 address can be autoconfigured in a router based on RA information, but as default it is not done. After the MNP has been delegated to the MR, the MR refreshes its routing table by designating the static router's global IPv6 address as its default router. The static router's IPv6 address is received from the unicast Prefix Delegation message (message 5 in figure 3). Before this, the static router has updated its routing table based on the delegated MNP by directing traffic destined for the delegated MNP to the MR. The MR's COA is received from the Prefix Request message (message 4 in figure 3). This means that two routing table updates are made when PD is performed, one in the static router and one in the MR. This procedure makes Internet connectivity possible for the mobile network.

5.2. Network mobility

In the demonstration, a handover was simulated by manually instructing the MR to initiate the handover procedures. The handover procedures of the MR consisted of returning the old MNP to the old delegator and obtaining a new MNP from the new delegator. As soon as the new one had been received, the MR begun sending RAs, which advertised the old MNP with a preferred and valid lifetime of zero, and the new MNP with new lifetimes. The old MNP has to be advertised with a valid lifetime of zero as for as long as the maximum time the MNs in the mobile network can consider the old addresses generated from the old MNP valid. This has to be done to eventually invalidate old IPv6 addresses autoconfigured from an old MNP.

The MR has to update its routing table in case of a handover to redirect all traffic that went to the old router to the new router. This has to happen after the MR has received a new MNP from the new router and before the MR begins advertising the new MNP, because traffic from the IPv6 addresses autoconfigured from the old MNP reaches its destination with greater probability through the new default router. The downside of the routing table update procedure is that traffic from the CN to the MN's old IPv6 address is not recognized during the handover time.

The handover of sessions of the MNs in the mobile network is made after a change of global IPv6 addresses is detected. This detection will be made by polling the valid addresses in the MN. The delay relating to session handover consists of the autoconfiguration of the new IPv6 address and the handover procedures the MN has to perform after it has detected that the old IPv6 address is no longer valid. In the system, it was possible to initiate the handover of UDP sessions between the MN and the CN. The handover related to TCP transfers with SIP has not been demonstrated here. It could be possible with IPv6 encapsulation and INFO messages as described in [16]. It is left for further work to see how this is done in practice.

The solution presented in this paper should work with any mobility protocol the MNs in the mobile network choose to use. This means that an application layer mobility solution such as SIP can be used, or for example MIPv6. MNs see the MR as just another router that sends RAs and MNs form new COAs based on the content of those messages. The MNs in the mobile network use the routing services of MR as a default router as specified in [14].

If the number of MNs in a mobile network increases, mobility management becomes hard for the MR, because all mobility updates to CNs have to go through the MR, which was illustrated in the use cases. This increases load dramatically on the MR. Still, there is a need for small PANs that could be formed by using the methods defined in this paper, because of the dynamics related to it. This solution does not necessarily require usage of MIPv6 or changes to it. Also routing optimization is achieved and multiple IPv6 encapsulation is avoided in nested mobile network cases.

5.3. Prefix delegation

The Automatic IPv6 Prefix delegation solution [12] is quite light-weight. It still makes delegation, refreshing and return of IPv6 prefixes possible. Because it uses Internet Control Message Protocol (ICMPv6) messages for transport, it has to use retransmission to make the solution reliable. The delegators have to be on the same link as the requestors, because all-routers multicast addresses are used in the solution. This means that there is no multi-hop or relay functionality in the solution. Our reference implementation of the draft included no security-related issues, and thus the security of the solution cannot be evaluated.

There are only a few drafts related to a similar kind of IPv6 prefix delegation, which could be used in this solution. [18] proposes to use a new Prefix Delegation -option in RAs for the delegation of IPv6 prefixes. This solution is limited in that the link between the delegator and requestor has to be point-to-point, meaning that only one prefix delegator and one prefix requestor can be on the same link on which PD occurs. This limits the environment on which PD can take place. This solution also has no functionality to support dynamic prefix leasing, refreshing and return. This means that the delegating router has no way of knowing whether the delegated prefix will be used or not.

[19] proposes to use a new Prefix Delegation -option and Prefix Request -option in the stateful configuration protocol DHCPv6 for PD. It supports the delegation, return, refreshing and reconfiguration of IPv6 prefixes. Reconfiguration means that a DHCPv6 server can initiate a prefix-related update. Because DHCPv6 supports relay agents, the prefix requestor and delegator don't have to be on the same link. With this solution, PD can be supported by adding changes to an existing protocol (DHCPv6). This also means that no additional PD protocol is needed. However, if DHCPv6 is not used for stateful configuration of IPv6 addresses or other information in small embedded devices, PD using DHCPv6 can be too heavy to be used just for PD.

6. Concluding Remarks

An IPv6-based addressing solution for a small-scale type of mobile network (PAN) is provided in this research. It is based on IPv6 stateless address autoconfiguration and Automatic Prefix Delegation Protocol for IPv6. The solution does work even if MIPv6 support is not included in the system, when SIP-based mobility is applied with UDP sessions. In this way, IPv6 encapsulation is avoided in nested cases and route optimization is achieved. It was also observed to support dynamic global addressing related to the MNs of a mobile network, and mobility of the network was also possible. The Automatic Prefix Delegation for IPv6 -protocol was found to be light-weight and have the functionality to support leasing, return and refreshing related to IPv6 prefixes. The solution is not suitable for a large mobile network because of scalability problems. Still, many things are left for study to develop a secure, stable, scalable and functioning addressing solution for a mobile network.

7. References

[1] Mobile Ad-hoc Networks working group IETF URL: http://www.ietf.org/html.charters/manet-charter.html.

[2] R. Wakikawa "Global Connectivity for IPv6 Mobile Ad Hoc Networks" IETF, draft work in progress, URL: http://www.potaroo.net/ietf/ids/draft-wakikawa-manet-globalv6-01.txt.

[3] D. B. Johnson, C.E. Perkins, J. Arkko "Mobility Support in IPv6" IETF draft, work in progress, URL: http://www.ietf.org/internet-drafts/draft-ietf-mobileip-ipv6-18.txt.

[4] C.E. Perkins "Mobility Support in IPv6" Mobicom 1996 November 10-12, New York USA.

[5] I. Okajima, N. Umeda, Y. Yamao "Architecture and Mobile IPv6 Extensions Supporting Mobile Networks In Mobile Communications" Vehicular Technology Conference, 2001. VTC 2001 Fall. IEEE VTS 54th , Volume: 4 , 2001 , Page(s): 2533 -2537.

[6] T. J. Kniveton, J.T. Malinen, V. Devarapalli, C.E. Perkins "Mobile Router Support with Mobile IP" IETF, draft work in progress, URL: http://tj.kniveton.com/specs/draft-kniveton-mobrtr-02.txt.

[7] T. Ernst, A. Olivereau, L. Bellier, C. Castelluccia, H. Lach "Mobile Networks Support in Mobile IPv6" IETF, draft work in progress, URL: http://www.nal.motlabs.com/nemo/drafts/draft-ernst-mobileip-v6-network-03.txt.

[8] Network Mobility working group IETF URL: http://www.ietf.org/html.charters/nemo-charter.html

[9] A. Conta, S. Deering "Generic Packet Tunneling in IPv6 Specification" IETF, RFC 2473, December 1998.

[10] R. Hinden, S. Deering "IP Version 6 Addressing Architecture" IETF, draft work in progress, URL: http://www.ietf.org/internet-drafts/draft-ietf-ipngwg-addr-arch-v3-10.txt

[11] S. Thomson, T. Narten "IPv6 Stateless Address Autoconfiguration" IETF, RFC 2462, December 1998.

[12] B. Haberman, J. Martin "Automatic Prefix Delegation Protocol for Internet Protocol Version 6 (IPv6)" IETF, draft work in progress, URL: http://www.ietf.org/internet-drafts/draft-haberman-ipngwg-auto-prefix-02.txt.

[13] USAGI Project URL: http://www.linux-ipv6.org/

[14] T. Narten, E. Nordmark, W. Simpson "Neighbor Discovery for IP Version 6 (IPv6)" IETF, RFC 2461.

[15] J. Rosenberg et al. "SIP: Session Initiation Protocol" IETF, RFC 3261.

[16] A. Dutta et al. "Application Layer Mobility Management Scheme for Wireless Internet" 3G Wireless 2001, San Francisco.

[17] R. Droms et al "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)" IETF draft, work in progress URL: http://www.ietf.org/internet-drafts/draft-ietf-dhc-dhcpv6-26.txt.

[18] N. Lutchansky "IPv6 Router Advertisement Prefix Delegation Option" IETF draft, work in progress, URL: http://www.join.uni-muenster.de/drafts/draft-lutchann-ipv6-delegate-option-00.txt.

[19] O. Troan, R. Troms "IPv6 Prefix Options for DHCPv6" IETF draft, work in progress, URL: http://www.ietf.org/internet-drafts/draft-troan-dhcpv6-opt-prefix-delegation-01.txt.