Providing Internet Access to IPv6 Mobile Personal Area Networks through UMTS

Nikolaos Alexiou, Georgios Tsiouris, and Efstathios Sykas

National Technical University of Athens
Department of Electrical and Computer Engineering
Communications, Electronics and Information Engineering Division
9 Heroon Polytechniou St., 157 73 Zografou Athens, Greece
Tel: +30 210 772 1493, Fax: +30 210 772 2534
{alen,gtsiouris,sykas}@telecom.ntua.gr

Abstract. This paper describes a mechanism and suggests a protocol enhancement to provide global Internet access to Mobile Personal Area Networks and support mobility under different scenarios. For this purpose the concept of the user's Mobile Station acting as a Mobile Multilink Subnet Router is introduced, which provides the necessary IPv6 connectivity and mobility service to the nodes connected to the Personal Area Network. The Mobile Station can distinguish between the nodes that need mobility support and the ones that do not in order to provide the appropriate type of IPv6 connectivity service. The main issues discussed are UMTS IPv6 connectivity, routing and mobility for the Mobile Station and the other nodes of the Mobile Personal Area Network.

1 Introduction

IPv6 [1] is the next generation protocol developed to replace the current version of the Internet Protocol, IP Version 4 (IPv4). One of the main issues concerning the use of IPv4 is the growing shortage of addresses. Mobile devices with IP capabilities become more popular and provide new services while their cost decreases. Meanwhile, solutions like private addresses and implementation of Network Address Translators cannot provide efficient support for new applications and services like peer-to-peer and Internet telephony. The allocation of public IP addresses to mobile terminals will be only feasible by the introduction of IPv6 since their number is quite high and is set to grow in the near future. In addition to the addressing issue, IPv6 also provides support for mobility, security and automatic configuration for every IPv6 enabled node.

The future user requirements of a mobile access network will not only include seamless internet connectivity for the mobile handset but for all the various devices with IP functionality that a user may carry. Hence the future user should be treated as a Personal Area Network (PAN) which in many cases may provide internet access to some visitor nodes. Future user requirements may also include mobility support of the PAN, which changes frequently its point of attachment.

M. Conti et al. (Eds.): PWC 2003, LNCS 2775, pp. 640–650, 2003.

This paper proposes a way to connect a PAN through a UMTS Mobile Station by using the concept of the Multi-Link Subnet Router [3], which connects different links belonging to the same subnet. This is based on the large number of available IPv6 addresses to the Mobile Station since it is assigned a unique 64-bit IPv6 prefix [9]. The IPv6 interface identifier can be chosen by the MS and can be changed at any time without any disruption to the IPv6 connectivity service since there is no UMTS network involvement.

The concept of connecting a PAN through a UMTS MS is extended by providing mobility support to the nodes comprising the PAN. This can be achieved by conjugating the concept of the Multilink Subnet Router (MSR) and the Mobile Router (MR) [4], which uses a bidirectional tunnel with its home network. However a distinction has to be made between the nodes that support mobility and the nodes that are mobility unaware for issues such as optimal routing, reduced traffic on mobile router's home network etc. For these reasons, a protocol enhancement is proposed, in order for the MS to be able to distinguish between the nodes that need mobility support and the ones that do not, in order to provide the appropriate type of IPv6 connectivity service.

2 IPv6 PAN Connectivity in UMTS

In order to connect a Personal Area Network (PAN), a subnet prefix must be provided. This subnet prefix has to be globally routable in order to provide end-to-end transparency for applications, protocols, mobility and security. In visited networks, the mobile router should acquire a whole IPv6 subnet prefix from a foreign access network.

A typical wireless IP connectivity scenario in the near future will be through UMTS. The main core network elements of the UMTS packet switched domain (General Packet Radio Services, GPRS) [9] are the Serving GPRS Support Node (SGSN) and the Gateway GPRS Support Node (GGSN). The GGSN is a specialized router that functions as the gateway between the GPRS network and the external networks. From the IP point of view, the GGSN can be seen as the first-hop router between the user and the Internet [13]. The SGSN's main functions include authentication, authorization, mobility management, and collection of billing information.

The main concept in UMTS systems regarding IP connectivity is the PDP context which is the connection between the user equipment and the Gateway GPRS Support Node (GGSN), over which the packets are transferred. In order to acquire IP connectivity, the user must initialize the PDP activation process.

In UMTS systems, IPv6 support is possible through both statefull and stateless autoconfiguration procedures [2] [9] [10]. Statefull address allocation mechanism requires a DHCPv6 server [17] while stateless autoconfiguration [6] involves mainly the IPv6 node in the allocation of addresses and does not require any external entity in the address autoconfiguration procedure. In cellular networks like UMTS, some Neighbor discovery messages can cause unnecessary traffic as

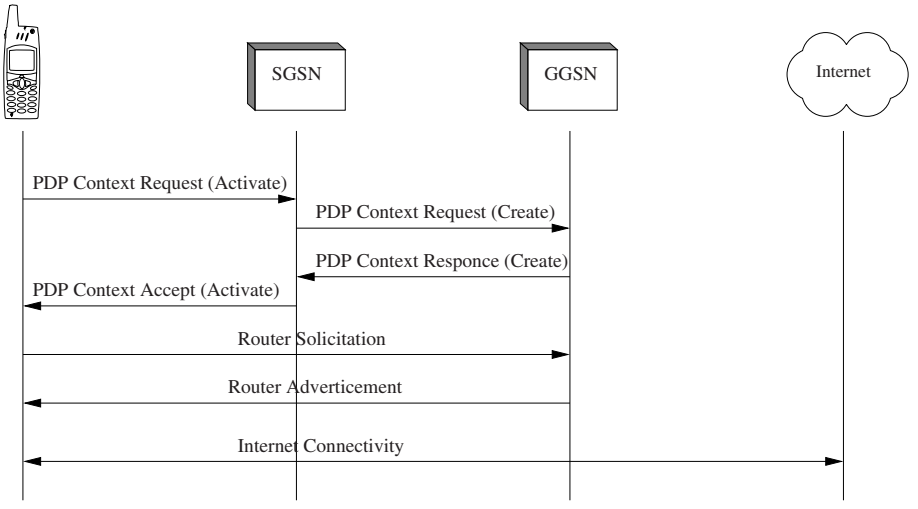

Fig. 1. IPv6 address acquisition in UMTS networks through stateless address autoconfiguration

the established link is a point-to-point link and the host's only neighbor is the default router (the GGSN).

During the autoconfiguration process (see Fig. 1) the Mobile Station uses the interface identifier received from the PDP context activation procedure and the prefix received in the Router advertisement [5] message from the GGSN, in order to create a globally routable IPv6 address. The interface identifier is provided to the mobile station by the GGSN, in order to avoid collisions with the link-local address of the GGSN. The prefix that GGSN provides to mobile station is unique and has a length of 64 bits. A Mobile Station (MS) may be comprised of a standalone IPv6 enabled phone or a Mobile Terminal (MT) and the user's Terminal Equipment (TE), e.g. a laptop or PDA. In the second case, a PPPv6 link [11] exists between MT and TE. The MT performs the PDP context activation on a request from the TE, and provides to the TE the interface identifier suggested by the GGSN.

The mobile station can at any time change the interface identifier used to generate global IPv6 address (e.g. for privacy reasons [7]) without updating the PDP context in the SGSN and the GGSN. Moreover the interface identifier does not need to be unique across all PDP contexts since the MS is considered to be alone on its link toward the GGSN. This practically means that the MS can choose any interface identifier without any network involvement. Thus a full prefix is available to the mobile station.

3 Mobile Station Acting as Multi-link Subnet Router

In this section the concept of a general Multi-link Subnet Router is discussed and the usage of the Mobile Station (MS) as a Multi-link Subnet Router (MSR) is introduced.

3.1 The Concept of a Multi-link Subnet Router

A Multi-link Subnet is defined [3] as a collection of independent links, connected by routers, but sharing a common subnet prefix. A single subnet prefix is sufficient to support multiple physical links.

During start-up the MSR starts as a normal host, discovering routers (if any) in each one of its interfaces. Then it switches to router-mode in all these interfaces where no routers were discovered. In case a router is found in one or more of its interfaces, the MSR chooses one and acts as a proxy mode on that interface. On all the remaining interfaces the MSR advertises itself as the default router and includes copies of the prefix information options that it learned on its proxy-mode interface. In a simple scenario where only one MSR exists, it will have one interface on which will act as a router, and one interface on which will act as a "host", proxying for all nodes on its router interface.

An example of an MSR with a proxy mode interface is depicted in Fig. 2 below. Two links, (1) and (2) are on a common subnet with global prefix G and are connected by an MSR (node B). The top level router of the subnet (node C) is connected on link 1. The MSR discovers that there is a router on link 1 and switches to proxy-mode on that interface. The MSR (node B) is in router-mode on link 2 (since no router exists), where it has link-layer address b2, and IPv6 address Gb2. On link 1, where it acts as a proxy it has link-layer address b1 and IPv6 address Gb1. Node A has link-layer address a on link 2, and has acquired global IPv6 address Ga. Node C has link-layer address c on link 1, and IPv6 address Gc. Node D has link-layer address d on link 2, and IPv6 address Gd.

The MSR depending on its configuration can broadcast router advertisements on the interfaces it acts as a router or respond to router solicitation messages from a specific node by sending a router advertisement message to this node.

3.2 Neighbor Discovery in a Multi-link Subnet

During Neighbor Discovery (ND) there are two possibilities for how an MSR can influence the ND procedure used. This is determined by the value of the flag L at the Prefix Information option of the Routing Advertisement message. It is assumed throughout this document that the hosts perform Autonomous Address Configuration (ADDRCONF) which depends on the flag A be set at the Prefix Information option [5].

Off-link Model. If the MSR sets the L flag all the hosts on the same link will not treat the prefix as being on-link.As a result ND is effectively disabled and

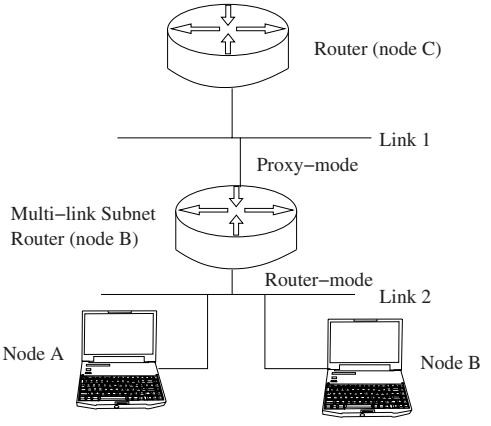

Fig. 2. A simple example of a Multi-link Subnet Router (MSR) connecting two separate physical links on a common prefix. It acts as a proxy on Link 1 where the default router is node C and as the default router on Link 2 where no router exists

packets to new destinations always go to the MSR first, which will then either forward them or redirect them depending on the destination node being on the same or different link. This case is referred as "Off-link Model".

As an example (see Fig. 2), when node A wants to start communication with C, it finds that the destination address matches no on-link prefix, and sends the packet directly to its default router B. B knows that C is on-link to link 1, with link-layer address c, and it forwards the packet to C. When node A wants to communicate with D, it finds that the destination address matches no on-link prefix, and sends the packet directly to its default router B. B knows that D is on-link to the same link as A, and responds with a Redirect message.

On-link Model. When the MSR does not set L the hosts on the link will perform ND by issuing Neighbor Solicitation Messages. The MSR should learn or know a-priori the location of the destination node. Neighbor Advertisements destined for nodes on another link should receive the Link-local Address of the MSR from the MSR. The MSR should refrain from answering Neighbor Solicitation Messages when the nodes are on the same physical link. This case is referred as "On-link Model".

As an example (see Fig. 2), when node A wants to start communication with C, it finds that the destination address matches an on-link prefix, and so sends an Neighbor Solicitation to the solicited-node multicast address. The NS message is received by node B, which listens on all multicast groups. Node B knows that C is on-link to link 1, and responds to A with an Neighbor Advertisement containing its own link-layer address b2 as the Target Link-Layer Address. After this, A can send packets to the address Gc. The packets will be sent to the link address b2 and they will be received by B, which will apply its validation rules (including decrementing the Hop Count in the IPv6 header) and forward them

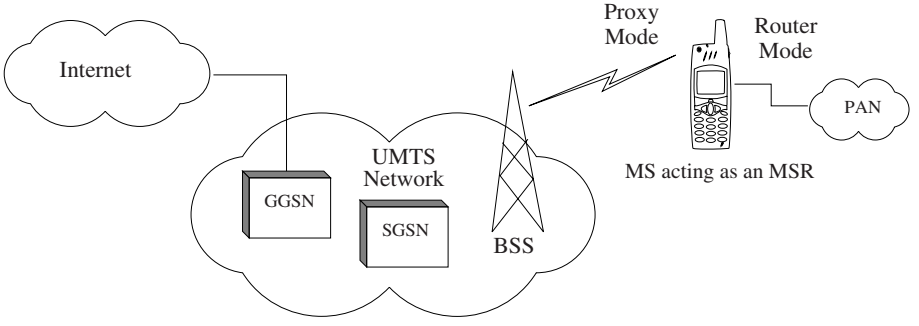

Fig. 3. The use of the mobile terminal as a multi-link subnet router. The MS is in proxy mode from the GGSNs perspective and acts as a router for the PAN

to the address c on link 1. When A wants to communicate with D, it again finds that the destination address matches an on-link prefix, and so sends an NS to its solicited-node multicast address. D receives the NS and responds. B also receives the NS, but knows that D is on the same link as A, and so does not respond.

3.3 Mobile Station Acting as a Multi-link Subnet Router

By conjugating the concept of the Multi-link Subnet Router and the former conclusion drawn, i.e. a full prefix is available to the mobile station, can lead to the concept of using the mobile station as a Multi-link subnet router, in order to make the prefix available to the nodes reside in the PAN.

Figure 3 depicts the use of the Mobile Station as an MSR. It can be seen that the GGSN is the top level router of the subnet and the Mobile Station acts as a Multi-link Subnet Router to the nodes attached to the link below. Assuming the most simple scenario (ie the MS is the only MSR) then a similar situation occurs as in the example mentioned previously. In this case the MS is in proxy mode from the GGSNs perspective and acts as a router for all the connected nodes to it. The point-to-point nature of the MS-GGSN link must be taken into account and the mobile router should not forward any local-scope packets (like Neighbor Solicitation messages) towards the GGSN.

Mobile router must get involved in duplicate address detection for link-local addresses to ensure that all addresses are unique across the personal area network and that the interface identifier provided by the GGSN to the mobile station will not be re-used. The MS can either operate in on-link or off-link mode. The MS acting as a MSR should not forward any local-scope packets towards the interface connecting the MS and the GGSN. The MS should only forward packets with global-scope addresses in the source and destination fields of the IPv6 header.

4 Introducing the Concept of Mobile Multi-link Subnet Router

4.1 Mobility Issues

Mobility support for IP networks is considered important, as a single user can be seen as a personal area network (PAN), due to various devices with IP functionality that the user may carry. There are two kinds of nodes when mobility support is taken into account, the fully enabled nodes that support mobility and the minimal functionality nodes (like embedded devices) that do not support mobility at all.

When a node is mobility-aware, it is desirable to use it's own mobility mechanisms [8] by custom preferences (home address and home agent). The basic requirement for a mobility-aware node is the acquirement of a globally routable IPv6 address. When a node completes the configuration of a global IPv6 care-of address, it exchanges binding update messages with its home agent in order to be reachable through its home address. In order for the mobility-aware node to use route optimization (for example when running real-time applications), it should initiate binding updates to its correspondent nodes so as to use its current care-of address.

There are cases that mobility support for mobility-unaware nodes is desired. One way of providing such support is described in the Mobile Router Tunneling Protocol proposed specification [4] where the concept of the Mobile Router (MR) is introduced. A Mobile Router is responsible for routing and mobility of an IP subnet network which moves with the mobile router. This subnet is attached to one of Mobile Router's network interfaces, while the other interface is connected to Mobile Router's home network. The subnet network (e.g. the PAN) has a routable prefix, which is called Mobile Router's subnet prefix. In general case, the Mobile Router's subnet prefix is different from the prefix of the Mobile Router's home network. The home network forwards every packet with destination an address belonging to the Mobile Router's subnet prefix towards the Mobile Router.

When a Mobile Router is attached to a foreign network, it installs an encapsulation interface towards its home agent, which is comprised of a bi-directional IP tunnel. Through this interface, the MR forwards (reverse-tunnels) all packets not originated from itself towards its home agent. The MR behaves as a normal Mobile Node for packets originating from itself. Hence, when the MR arrives to a visited link it injects a routing path to the reverse tunnel pointing to its home agent for all its depending nodes, which continue to use the same prefix as when the MR is located at home (Mobile Router's subnet prefix). Moreover there exists a default route to its default router on the visited link.

Also, the home agent of the MR injects a routing entry towards the encapsulation interface with ending point the care-of address of MR, for the Mobile Router's subnet prefix. The home agent forwards the packets based on the prefix information and does not need to know what nodes are behind the Mobile Router. The main drawback of this solution is the absence of route optimization

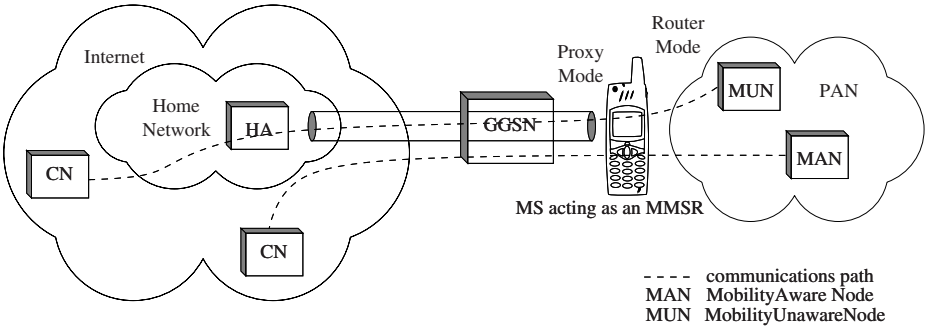

Fig. 4. The IPv6 mobility scenarios. A Mobility Unaware Node (MUN) which has acquired a home prefix address is connected through the bi-directional tunnel between the MS and its Home Agent. A Mobility Aware Node (MAN) which has acquired a foreign prefix address is connected directly

support as the packets get forwarded via the Mobile Router's Home Agent, which could be located far away from the exact access point of the Mobile Personal Area Network.

4.2 Mobile Station Acting as a Mobile Multi-link Subnet Router

By conjugating the concept the Mobile Station being used as a Multi-link subnet router and the mobility issues discussed above, a new concept of using the Mobile Station as a Mobile Multi-link Subnet Router (MMSR) is introduced.

In the case of a mobility-aware node, the IPv6 address that it acquired from the MMSR should belong to the visited network's subnet and the MMSR must advertise the subnet prefix obtained from the foreign network to that particular node. As seen in Fig. 4, the mobility-aware node is connected directly to its home agent and the correspondent nodes. This approach reduces traffic and processing load on mobile router's home network and its home agent.

In the case of a mobility-unaware node, the IPv6 address that it acquired from the MMSR should belong to the Mobile Router's subnet prefix. The MMSR must advertise the Mobile Router's subnet prefix to that particular node, in order to create a global IPv6 address that can be routed through the encapsulation forwarding mechanism mentioned above. If the advertised prefix was different, the packets could not be forwarded through Mobile Router's home network. As seen in Fig. 4, the mobility-unaware node is connected through the bi-directional tunnel between the MS and its Home Agent.

4.3 Introduction of the Mobility Support Bit

Hosts send Router Solicitations messages in order to prompt routers to generate Router Advertisements quickly. In response to a valid solicitation message, a

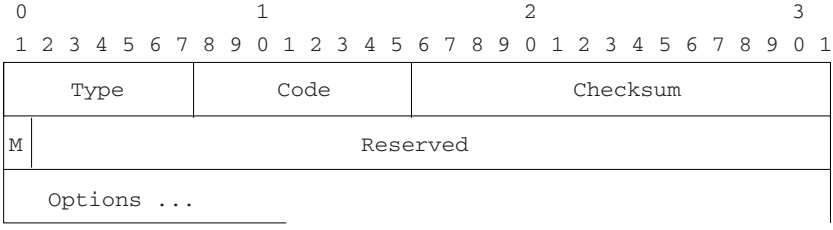

Fig. 5. The enhanced Router Solicitation message showing the position of the Mobility Support bit (M)

router may choose to unicast the response directly to the soliciting host's address or to multicast the response to the all-nodes group [5] [6].

As far as the MMSR is concerned, only the first case should be considered since the MMSR should be able to choose the appropriate network prefix to advertise to a node depending on its mobility support capabilities. For the above reason, a new flag situated at the Reserved Header space of the routing solicitation message is introduced

This flag, which we call Mobility Support Bit (M-bit) should be set by the node if it requests mobility support from the MMSR. In this case, the MMSR responds by a Router Advertisement message containing the Mobile Router's subnet prefix as the prefix to be used in the construction of the IPv6 address. In any other case (the M-bit is not set), the MMSR provides the subnet prefix obtained from the foreign network (e.g. UMTS). The enhanced Router Solicitation message format can be seen in Figure 5

This enhanced routing solicitation message will not affect the functionality of routers that do not support the M-bit, as the particular bit belongs to reserved header space and will be ignored by a normal router.

Based on the above discussion, a node that wishes to have mobility support from the MMSR has to send a router solicitation message with the M-bit on. In such case, the node constructs an IPv6 address with its subnet prefix being the same to the Mobile Router's subnet prefix and has mobility support if the point of attachment of the MMSR changes. Otherwise, a node that does not require mobility support from the MMSR should send a normal router solicitation message (M-bit off) and will receive a subnet prefix belonging to the foreign visited network. Another possibility exists where a mobility-aware node may need to use the mobility support of the MMSR, for example when the communication with its home agent is not possible.

When MMSR is attached to its home network, it advertises the Mobile Router's subnet prefix to be used by all the nodes connected to the PAN, regardless of the M-bit value. However the MMSR must remember the nodes that did not request mobility. This is due to the fact that every time the MMSR changes its point of attachment must sent an unicast Router Advertisement message to the above nodes in order for them to change their network prefix.

In case that the MMSR can not acquire a full prefix from the visited network (e.g. Wireless LAN) and only a global IPv6 address is provided, all the nodes belonging to the Mobile PAN must have addresses with the Mobile Router's subnet prefix in order to use the encapsulation forwarding mechanism, regardless of the value of the M-bit.

5 Security Issues

It is assumed that the user which owns the Mobile Station acting as a Mobile Multi-link Subnet Router and the associated Personal Area Network, will provide access to its network on a restricted basis and not on a freely manner. This means that the link layer access is somehow granted securely, for example by providing cryptographic keys to any friendly nodes that wish to connect to the PAN.

The communication between the MMSR and its Home Agent must be secured when the MMSR is not on its home link. A possible solution would be the use of IPSec [14]. This can be done by the existence of a security association between the mobile router and its home agent [8] [12]. IPSec makes possible the realization of secure connections over insecure networks by using two protocols to provide traffic security, Authentication Header (AH) [15] and Encapsulating Security Payload (ESP) [16]. These protocols may be applied alone or in combination to provide a desired set of security services and access control. The MMSR and its home agent should use ESP to protect payload packets tunnelled between themselves.

6 Conclusions

This paper has presented an approach on providing the necessary connectivity and mobility support to a Personal Area Network through UMTS IPv6 connectivity. UMTS connectivity issues regarding IPv6 mechanisms were examined and the concept of using the Mobile Station as a Multi-link Subnet Router was introduced.

This was extended to include the provision of mobility support to all the nodes comprising the PAN. In this context the concept of the UMTS Mobile Station acting as a Mobile Multi-link Subnet Router was introduced.

A Personal Area Network may contain nodes that support mobile IPv6 as well as nodes that are mobility unaware. In order to provide efficient mobility support for all the nodes of the PAN, the MS needs to treat them differently depending on their mobility capabilities. For the above reason an enhancement to the Router Solicitation mechanism is proposed with the addition of a flag (M-bit) in the reserved header space of the Router Solicitation Message. This should be set by the node that wishes to have mobility support from the PAN's Mobile Multi-link Subnet Router.

Future work should include the statefull autoconfiguration scenario by using a DHCPv6 server [17]. Moreover, security issues as well as the protection

of Routing Solicitation and Advertisement Messages should be further investigated. Furthermore multi-homing environment scenarios should be considered where the Mobile Multi-link Subnet Router is connected to more than one access providers. Also the use of more than one Mobile Multi-link Subnet Router should be investigated where a nested architecture is present e.g. a Mobile PAN is connected to another Mobile PAN.

References

1. Deering S., Hinden R.: Internet protocol version 6 (IPv6) specification, Dec. 1998, RFC 2460
2. Loughney J.: IPv6 node requirements, Internet draft, Oct. 2002. Work in progress
3. Thaler D., Huitema C.: Multi-link Subnet Support in IPv6, Internet draft, June 2002. Work in progress
4. Kniveton T., Malinen J., Devarapalli V., Perkins C.: Mobile Router Tunneling Protocol, Internet draft, Nov. 2002. Work in progress
5. Narten T., Nordmark E., Simpson W.: Neighbor discovery for IPv6, Dec. 1998, RFC 2461
6. Thomson S., Narten T.: IPv6 Stateless address autoconfiguration, Dec. 1998, RFC 2462
7. Narten T., Draves R.: Privacy extensions for stateless address autoconfiguration in IPv6, Jan. 2001, RFC 3041
8. Johnson D., Perkins C., Arkko J.: Mobility support in IPv6, Internet draft, Jan. 2003, Work in progress
9. Universal Mobile Telecommunications System (UMTS); General Packet Radio Service (GPRS) Service description; Stage 2, Mar. 2002. 3GPP TS 23.060 version 5.1.0 for Releases 4, 5, 99
10. Wasserman M.: Recommendations for IPv6 in Third Generation Partnership Project (3GPP) Standards, Sep. 2002. RFC 3314
11. Haskin D., Allen E.: IP Version 6 over PPP, Dec. 1998. RFC 2472
12. Arko J., Devarapalli V., Dupont F.: Using IPsec to Protect Mobile IPv6 Signalling between Mobile Nodes and Home Agents, Internet draft, Jan. 2003. Work in progress
13. Universal Mobile Telecommunications System (UMTS); Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based services and Packet Data Networks (PDN), Mar. 2002, 3GPP TS 29.061 version 5.1.0 for releases 99, 4, 5
14. Kent S., Atkinson R.: Security Architecture for the Internet Protocol, Nov. 1998. RFC 2401
15. Kent S., Atkinson R.: IP Authentication Header, Nov. 1998. RFC 2402
16. Kent S., Atkinson R.: IP Encapsulating Security Payload, Nov. 1998. RFC 2406
17. Droms R., Bound J., Volz B., Lemon T., Perkins C., Carney M.: Dynamic Host Configuration Protocol for IPv6 (DHCPv6), Internet draft, Nov. 2002. Work in progress