An Applicability of Transition Mechanisms for IPv6/IPv4 within the Scope of GPRS with an Internet Communication

Preetida Vinayakray-Jani, Reijo Juvonen

Nokia Research Center, P.O.Box 407, FIN-00045, NOKIA GROUP, Finland
preetida.vinayakray-jani@nokia.com

Abstract. Recent years have witnessed a new version of Internet protocol and concepts of new protocol are heavily relied on for transition from the traditional IPv4-based Internet to an IPv6-based Internet. As a result it is expected that mobile node is General Packet Radio Service (GPRS) with IPv6 support likely to use IPv4 services. Therefore great concerns to transition strategy planners is how to provide connectivity between IPv6-enabled end user to IPv4. As a result many interworking techniques in terms transition mechanisms are proposed by researchers. But their applicability between GPRS and Internet influences many factors such as end-to-end integrity of data, security of communication. Therefore paper mainly focuses on the applicability of transition mechanism where these factors are main concern from GPRS user point of view.

1 Introduction

The GPRS Internet-hosted service is a TCP service that can transmit an unstructured stream between a GPRS Mobile Station (MS) and an Internet host. Thus establishing an Internet-hosted service connection involves setting up two segments, the one segment between the MS and Gateway GPRS Support Node (GGSN) and the another segment between the GGSN and Internet host.

Fundamentally GPRS inherits security features of Global System for Mobile Communication (GSM) but its access to packet data network such as, Internet brings more security threats. In other words IP vulnerabilities limit and complicate the use of GPRS networks for sensitive or secure communication. However from security point of view GPRS has quite good user authentication mechanism but confidential data transmission requires additional mechanisms.

With emerging new standard of Internet protocol, it is quite likely that the two end hosts operating over the above mentioned two segments are configured with different versions of Internet Protocol. Therefore the need of Interworking techniques which provides transition mechanisms becomes crucial, when two end hosts like to communicate with each other via different versions of the IP such as IPv4 or IPv6. Any incompetence or misconfiguration of transition mechanisms can easily amplify security threats and thereby degrading the quality of service of data communication. However an applicability of transition mechanisms requires suitable transition

S. Rao and K.I. Sletta (Eds.): INTERWORKING 2000, LNCS 1938, pp. 72-82, 2000.
© Springer-Verlag Berlin Heidelberg 2000

components such as host configuration, routers and routing protocols, domain name systems (DNS) and components dependencies. Therefore this paper focuses on proper applicability of transition mechanisms to maintain inter-operability between GPRS and external IP efficiently.

The paper is organized as follows: section 2 gives brief introduction of GPRS nodes and their functionality followed by GPRS interworking with Packet Data Network in section 3. The transition mechanisms are described in section 4, including protocol encapsulation and IP header translation. Section 5 presents the security threats in GPRS, followed by concluding remarks in section 6.

2 GPRS Support Nodes and Their Functions

Basically GPRS is a new bearer service for GSM that has its own core network and the radio network is shared between the GPRS and GSM core networks. The core network of GPRS is attached to GSM radio network via an open interface. Thus GSM may utilize the GPRS core network to achieve more efficient performance as well as to access packet data network - Internet.

Figure 1 illustrates the basic structure of a GPRS network including possible interception points: Air interface, Base Station Subsystem (BSS), Serving GPRS Support Node (SGSN), GPRS Backbone Network, Gateway GPRS Support Node (GGSN), Border Gateway (BG) and Inter-operator Backbone Network.

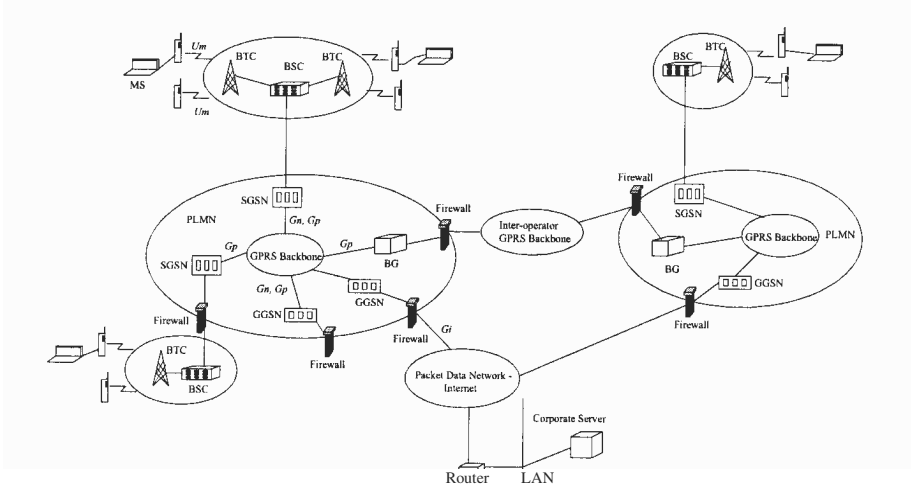

Fig. 1: GPRS Architecture

All the data and signalling is routed through at least one SGSN and at least one GGSN, both in mobile originated and mobile terminated cases. Routing depends on the subscriber IP address allocation point. The SGSN through which the messages are routed, always belongs to the network where the subscriber is currently roaming. The GGSN through which data is delivered (home network GGSN or visited network GGSN) depends on the address allocation point. Messages are routed through the GGSN from whose address pool the used address was allocated.

The SGSN is responsible for the delivery of packets to/from the MSs within its service area and communicates with the GGSN. It also keeps the tracks of the mobiles within its service area. The GGSN acts as a logical interface to external packet data network - Internet and maintains routing information to SGSN that is currently serving MS. The GPRS network can use multiple serving nodes, but requires only one gateway node for connecting to an external network - Internet.

- **Mobile Station** (MS): Generally GPRS mobile stations are classified in 3 different classes - A, B, C, depending on their configured accessibility with GSM and GPRS core. For example:
  - •Class A: mobile can have a normal GSM voice call and GPRS data transfer taking place simultaneously.
  - •Class B: mobiles are capable of using either GSM or GPRS at a time.
  - •Class C: the selection between GSM and the GPRS networks is done manually. Thus Class C mobiles can be attached to either GSM or to the GPRS network but not to both at the same time.
- **Serving GPRS Support Node (SGSN):** This is one of the main component of the GPRS network, which is responsible for handling MS registration and authentication into the GPRS network, to manage MS mobility, to relay traffic and to collect statistics and charging information.
- **Gateway GPRS Support Node (GGSN):** This is the interface between the GPRS backbone and external data networks. In conventional term it is simple IP router as it routes the data to and from external data networks to the SGSN serving the MS.
- **Border Gateway (BG):** The main function of this component is to ensure a secure connection between different GPRS networks over the inter-operator backbone network. The functionality of the BG is not defined in the GPRS specifications. It could consist firewall, security functions, and routing functions. BGs as well as their functionality are selected by the GPRS operator's manual agreement to enable roaming.
- **GPRS Backbone Networks:** There are two kinds of backbone Public Land Mobile Networks (PLMNs) as shown in Figure 1. They are called intra PLMN backbone network and inter-PLMN backbone network.
  - The intra-PLMN backbone is the IP network interconnecting GGSNs within the same PLMN. Every intra-PLMN backbone networks is a private IP network intended for GPRS data and signalling only and there must be some access control mechanism in order to achieve a required level of security. Two intra-PLMN backbone networks are connected via Gp interface using the BGs and inter-PLMN backbone networks.
  - The inter-PLMN backbone network interconnects GGSNs and intraPLMN backbone networks in different PLMNs.

3 GPRS Interworking with Packet Data Network

In GPRS network interworking is inevitable whenever PLMN is involved in communication with packet data network (PDN) to provide end-to-end communication. This interworking may be either directly with Internet or through a

transit networks - intranets. Figure 2 shows the Gi reference point and protocol stack needed for GPRS interworking with IP networks [4].

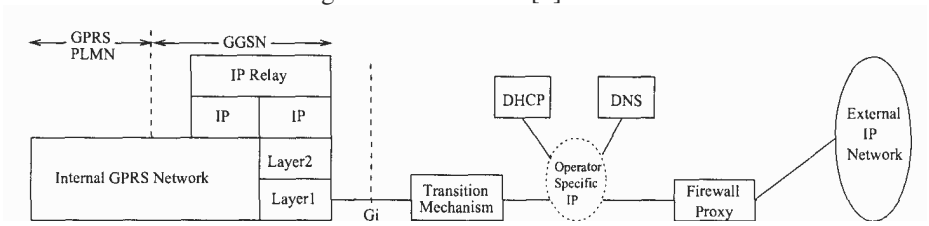

Fig. 2: Gi reference point for GPRS with IP interworking

The GGSN for interworking with the IP network is the access point of the GSM GPRS data network. In this case the GPRS network will look like any other IP network or subnetwork. Distinctively in the IP network, the interworking with subnetworks is done via IP routers. Therefore referring to Gi reference point, external IP can view, GGSN as a normal IP router. Considering generic view there are some assumptions valid between the GGSN and the external IP network:

- A firewall is configured by GPRS operators so that operators can easily make their choice for type of service they can offer.
- The DNS managed by the GPRS operator or it can be managed by the interworking with Packet Switched Data Networks and more specifically with Internet. This interworking may be either direct - Internet or through a transit network - intranet.
- The GGSN may allocate dynamic IP addresses by itself or use an external device such as DHCP server. This external server can be operated by an Internet Service Provider (ISP).
- The deployment an appropriate transition strategy that allows new IPv6 supported mobile terminals to communicate with existing IPv4 hosts or servers.

Focusing on the last assumption the transition requirements are most important for flexibility of deployment and ability of IPv6 hosts to communicate with IPv4 hosts. To place it concisely, there are 3 objectives for the proposed transition to be smooth. They are:

1. To allow IPv6 and IPv4 hosts to inter-operate.
2. To allow IM hosts to be deployed in the Internet in a highly diffuse and incremental fashion, with no interdependencies.
3. The transition should be as easy as possible for end-users, system administrators, and network operators to understand and carry out.

The mechanism of transition is a set of protocols implemented in hosts and routers, along with some operational guidelines for addressing and deployment, designed to make transition to work with as little disruption as possible. Some of the features for implementing the transition mechanism are:

1. An IPv6 addressing structure that embeds IPv4 addresses within IPv6 addresses, and encodes other information used by the transition mechanism.
2. A model of deployment where all hosts and routers upgraded to IPv6 in the early transition phase are dual capable (i.e., implement complete IPv4 and IPv6 protocol stacks).

3. The technique of encapsulating IPv6 packets within IPv4 headers to carry them over segments of the end-to-end path where the routers have not yet been upgraded to IPv6.
4. The header translation technique to allow the eventual introduction of routing topologies that route only IPv6 traffic, and the deployment of hosts that support only IM. Use of this technique is optional and would be used in the later phase of transition if it were used at all.

The proceeding discussion focuses on some of the more innovative and radical changes IPv6 brings to interworking. These interworking mechanisms are integral part of the IPv6 design effort. These techniques include dual-stack IPv4/IPv6 hosts and routers, tunneling of IPv6 via IPv4, and a number of IPv6 services, including DNS, Dynamic Host Configuration Protocol (DHCP), Application Level Gateways (ALGs), relays, proxies, caches and so on. The flexibility and usefulness of the IPv6 transition mechanisms are best gauged through scenarios that address real-world networking requirements. Therefore initial design specification of transition mechanisms specifies the use of three different types of IP nodes such as IPv4-only node, IPv6/IPv4 node (Dual stack) and IM-only node.

4 Transition Mechanisms

On the basis of above objectives and features of transition mechanisms, researchers have proposed few transition mechanisms, which are described below.

4.1 Protocol Encapsulation

When IPv6 hosts on different edges of the network are separated by IPv4 capable routers, an encapsulation mechanism is used to setup 6in4 or 6over4 tunneling [2]. Thus tunneling of IPv6 datagrams takes place by encapsulating them within IPv4 packets. This way IPv6/IPv4 hosts and routers can tunnel IPv6 traffic over regions of IPv4 routing topology which is shown in Figure 3. In simplest form the encapsulating node adds an IPv4 header to the packet and transmits it. The decapsulating node removes the IPv4 header and processes the remaining IPv6 packet as if it were normally received via IPv6 topologies. Generally tunnel can be configured manually or automatically.

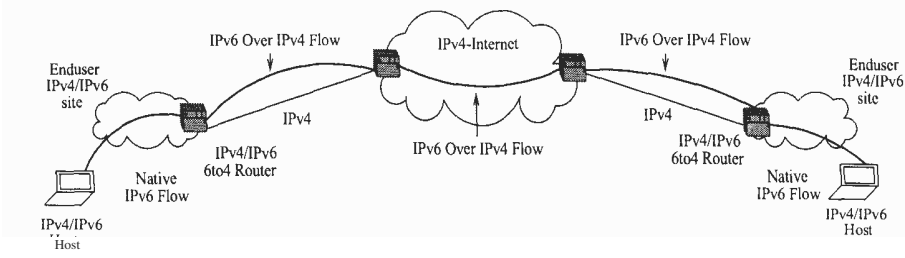

Fig. 3: 6to4 Tunnel Overview

- **Configured Tunneling (6in4):** This configuration does not require any interdependency between IPv4 and IPv6 addresses as the tunnel path endpoint IPv4 address is defined in the configuration of the encapsulating node. But this configuration requires a lot of effort to manage because:
  - Finding candidate networks when the site's choice of IPv4 service does not provide IPv6 service (either tunneling or native),
  - Determining which one are the best IPv4 path to use so that an configured tunnel doesn't inadvertently follow a very unreliable or lowperformance path,
  - Making arrangements with the desired IPv6 service provider for tunneling service, a scenario that may at times be difficult if the selected provider is not ready to provide the service or some other reasons.
- **Automatic Tunneling (6to4):** This mechanism provides a solution to the complexity problem with manually configured tunnels by advertising a site's IPv4 tunnel endpoint (to be used for dynamic tunnel) in a special external routing prefix for that site. Thus IPv6 addresses used must be IPv4compatible addresses [3]. Thus one site trying to reach another will discover the tunnel endpoints from DNS and use a dynamically built tunnel from site to site for the communication. The tunnels are transient in that there is no state maintained for them, lasting only as long as specific transaction uses the path. However this type of tunneling scenario exists when site has:
  - both 6to4 and native IPv6 connectivity, or
  - only 6to4 connectivity and trying to reach a site with both 6to4 and native IPv6 connectivity or
  - both 6to4 and native IPv6 connectivity, and trying to reach native IPv6 connectivity and vice-versa.

  But most interesting when site has only 6to4 connectivity and communicating site with only native IPv6 connectivity. This will be accomplished by the use of a 6to4 relay that supports both 6to4 and native connectivity. The 6to4 relay is nothing more than an IPv4/IPv6 dual-stack router.

4.2 IP Header Translation

To enable the communication between IPv6 node and IPv4 node or vice-versa, a translator needs to perform two main functions: Address translation and Protocol translation. Address translation involves converting address for packet crossing the protocol boundary, whereas protocol translation involves mapping most of the fields from one version of IP to the other. Researchers have exploited this translation feature at network level (SIIT, NAT-PT), Transport level (SOCKS) [5] and Application level (ALGs).

- **Stateless IP/ICMP Translator (SIIT) [7]:** SIIT is the mechanism that allows IM-only nodes to talk with IPv4-only nodes by translating the packet headers between IPv6 to IPv4. Once the traffic is originated by IPv6 host and routed through SIIT node, SIIT makes simple header translation between IPv6 to IPv4 in source field of header and forwards it to IPv4 node. But SIIT proposal do not define how IPv6 host should get its temporary IPv4 address. The applicability of this mechanism is limited as
  - applications like FTP and DNS transfer where IP address is inside the payload, SIIT is unable to perform translation.

- if the arrived packet is embedded with security feature, then authentication header (AH) which is computed from IP header fields gets broken while passing through SILT. Therefore even if Encrypted payload passed through, translator partly breaks the IP security (IPsec)

– **Network Address Translator-Protocol Translator (NAT-PT):** NAT-PT also performs header translation as described in [8]. Actually there are two different methods that assigns the temporary IPv4 address to IPv6 host:

1. The translator reserves the pool of IPv4 addresses, from which it assigns IPv4 address to the IM host and caches this address mapping from IPv6-to-IPv4 for the duration of the session.
2. All IPv6 addresses are mapped to a single IPv4 address, which is the IPv4 address of the translator. This is useful when translator fall flat when the pool of IPv4 addresses assigned for translation purposes is exhausted. As a result the translator considers port number as an transport identifier - TCP/UDP port number or ICMP query identifier.

Although this translation mechanism provides stateful translation there are some limitation associated with it, such as:

- Some applications e.g., rlogind, don't accept the connections if they are not from privileged port.
- when host from outside wants to establish a connection to server which resides inside the NAPT-PT and NAPT-PT can map only one server per service.
- As translator breaks the end-to-end integrity of data it is quite likely that some information may be lost during translation.
- It also breaks IPsec partially by breaking the authentication and bypassing encryption.

– **SOCKS 64:** The SOCKS gateway - SOCKS-GATE tool is a gateway system that accepts enhanced SOCKS - SOCKS-EXT connections from IPv6 hosts and relays it to IPv4 or IPv6 hosts [5], especially for *socksified* sites, which already use SOCKS aware clients and SOCKS server. The mechanism simply replaces the standard socket and DNS resolver libraries with SOCKS versions. Besides this each *socksified* application should be configured with the IP address *of* the local SOCKS gateway. When application makes a DNS query, the SOCKS library intercepts the call and returns an arbitrary IP address for A. This IP address is never seen on the wire. The resolver library associates this address with fully qualified domain name (FQDN). When the application enables the socket call, the SOCKS library makes connection to dual stack gateway. This dual stack gateway makes standard connection to application and protocol translation. No DNS modification or address mapping is needed. Compare to previous translators SOCKS gateways are simple to maintain and configure. Thus when protocol translation is necessary, this transport level translation mechanism should be considered.

– **ALGs, relays, proxies and caches:** It is reasonable to position application level gateways, relays, proxies and caches, especially at Intranet /Internet boundary. This type of mechanism is very helpful when IP address is embedded within payload. Although ALGs provides transparency, they do so in precise way, correctly terminating network, transport and application protocols on both sides. They can however exhibits some shortfalls in ease of configuration and fail-over. However,

in some application level mechanism such as proxies or relays they grab and modify traffic in an inappropriate way and generate totally unforeseeable side effects.

– **Temporary Address Allocation:** Knowing the limitations of protocol translator some proposals such as Allocation of IPv4 address to IPv6 nodes (AIIH), Realm Specific IP (RSIP) [1, 6] are made to provide publicly routable IPv4 address so that dual stack host machine can communicate with IPv4 server.
  - ï The AIIH is essentially a DHCPv6 server, which allocates the temporary IPv4 address to dual stack host using global address extension. When connection is initiated by only IPv4 host then AIIH server also needs to contain DNS server, so that IPv4 host can make DNS query about dual stack host node. The AIIH server will respond this query by assigning temporary IPv4 address and simultaneously sending 'DHCP reconfigure' message to dual stack host so that it can update its interface with new IP address. A dual stack host acknowledges this by sending confirmation to AIIH server which then finally updates DNS record.
  - With RSIP proposal the basic idea is very similar to AIIH but currently existing network stack of client requires modifications. Thus RSIP client makes the request for temporary public IPv4 address from local RSIP server which is located at the boundary between two routing realms. This protocol standard is till evolving but current proposal requires that RSIP clients use a tunnel to the RSIP server, which matches very well with GPRS architecture.

5 Security Threats in GPRS Systems

Here we will examine security threats originating from external IP and leading to different nodes in GPRS.

5.1 Denial of Service (DOS)

This type of threat occurs when malicious party manages to do a bogus registration of a new care-of-address for a particular mobile host within GPRS. Such a bogus registration gives rise to two problems:

1. The particular victim mobile host gets terminated.
2. The malicious party gets to see all traffic directed to victimized mobile host.

The usual protection again DOS is a firewall, but it is not effective in all cases, e.g., protection against viruses is always one step behind the sources.

5.2 Session Stealing/ Spoofing

This is one of the active form of information theft. An attacker performs following steps once the mobile host gets registered with its home agent:

1. An attacker eavesdrops and floods the mobile host with bogus packets, thus putting it out of the action.

2. Thus attacker steals the session by originating packets that seem to have come from the mobile host and at the same time intercepting the packets destined for the mobile host.

Such type of attack could occur either at the foreign link or at some other point between foreign agent and mobile node where foreign agent is not colocated. This can be avoided by applying strong encryption so that even if session gets stolen the attacker cannot get the actual data.

5.3 Incompetent Translator

The major drawback of protocol translator is that it breaks the end-to-end integrity of data as it needs to change IP headers including upper layer header and simultaneously destroying authenticity of data, which shown in Figure 4.

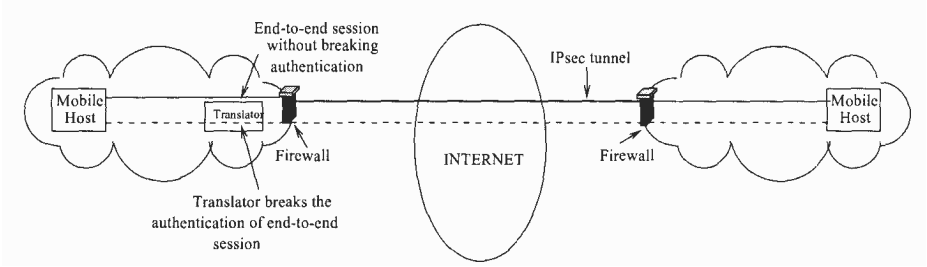

Fig. 4: Translator Applicability

Once the attacker has gained the 'physical' access via unattended network socket, by following first three steps he breaks the mobile host from the network:

1. The attacker figures out a network prefix to use. This can be done by listening for mobile IP agent advertisement, by examining IP address in packets flowing around on the network segment, or even by just doing a DHCP configuration request.
2. Then attacker guesses an available host number to use. This can be done by listening for a while and just picking one that does no appear to be used. Then by making ARP request for the resulting IP address and see if it goes unanswered otherwise again a DHCP request.
3. Once the above steps succeeded the attacker gets access to IP hosts and floods it bogus packets.
4. Another attack path is the external net to backbone through GGSN. Since the GGSN is an IP router, it will handle any packet addressed to a backbone node as any other packet unless firewall at Gi prevents it.
5. A simple attack is from one intranet to another through through GGSN Gi. Since the GGSN is an IP router, it can mediate packets between the two, or even the Internet as mentioned in the above step.
6. In GPRS Tunneling Protocol (GTP) specification are public, as they can be implemented by anyone. The GGSN unwraps the only the outer GTP envelope, supposedly wrapped by the SGSN. If the remaining packet is addressed to a backbone node, it will be forwarded by to that node. This opens attack possibilities via all interfaces. Thus any Internet host can attack the backbone nodes by sending valid GTP packets and target the billing system.

6 Concluding Remarks

The recommended suggestions are not comprehensive, but they do provide the cornerstone for proper applicability of interworking techniques within the scope of GPRS and external IP. The main problem of security is not the available tech nology, but its ease to use it. Concluding above discussion here we suggest some key points to consider so that end-to-end integrity of data can be maintained.

- Applicability of transition mechanism:
  - Viewing carefully transition mechanisms mentioned above 6to4 encapsulating mechanism shows more competitive than others as it allows the isolated IPv6 routing domains to communicate with other IPv6 routing domains even in the total absence of native IPv6 service provider. It is a powerful IPv6 transition mechanism that will allow both traditional IPv4-based Internet sites to utilize IPv6 and operate successfully over existing IPv4/based Internet routing infrastructure.
  - Upgrade the existing IPv4 servers with dual stack support, so that both IPv4 and IPv6 host can communicate easily
  - In case of limited public IPv4 addresses, currently the use of RSIP is more preferred choice as it provides temporary assignment of IPv4 addresses and simultaneously preserving the transparency of data.
- Security Consideration: The loss of transparency of end-to-end data is one of the main concern from security point of view. If network level translator is in the path, then the best that can be done to is to decrypt and re/encrypt IP traffic in the translator. This traffic will therefore be momentarily in clear text and potentially vulnerable. In the environment where this is unacceptable, the encryption must be applied above network layer instead. Anyhow this break in security provides well defined point at which to apply the restriction by using firewalls or Active filters. In case when protocol translation one should use SOCKS or ALGs rather than SIIT or NAT-PT.

In an ideal transition concept the pushing force for transition mechanisms would be the technical advantage and exploit the new features offered by the new version of protocol. However here we try to make the transition concept feasible with GPRS where coexistence of both IPv4 and IPv6 can be arranged in a more practical and efficient way.

References

1. Borella, M et al.: Realm Specific IP: Protocol Specification. Internet Draft, draft-ietf-nat-rsip-framework-01.txt. (1999)
2. Carpenter, B., Moore, K.: Connection of IPv6 Domains via IPv4 Clouds without Explicit Tunnels. Internet Draft, draft-ietf-ngtrans-6to4-02.txt.(1999)
3. Deering, S., Hinden, B.: Internet Protocol, Version 6 (IPv6) Architecture. RFC 2460.(1998)
4. ETSI TS 101 348 V7.1.0.: GSM 09.61: Digital Cellular telecommunications system (Phase 2+); Genreal Pacekt Radio Service (GPRS); Interworking between the Public Land Mobile Network (PLMN) supporting GPRS and Packet Data Networks (PDN). (1999-07)
5. Kitamura, H.: SOCKSv5 Protocol Extensions for IPv6/IPv4 Communication Environment. Internet Draft, draft-ietf-ngtrans-socks-gateway-02.

6. Montengero, G., Borella, M.: RSIP Support for End-to-End IPsec. Internet Draft, draft-ietf-nat-rsip-ipsec-02.txt. (2000)
7. Nordmark, E.: Stateless IP/ICMP Translator (SIIT). Internet Draft, draft—ietf-ngtrans-siit-06. txt. (1999)
8. Tsirtsis, G, Srisuresh, P.: Network Address Translation - Protocol Translation (NAT-PT). Internet Draft, draft-ietf-ngtrans-natpt-06.txt.(1999)