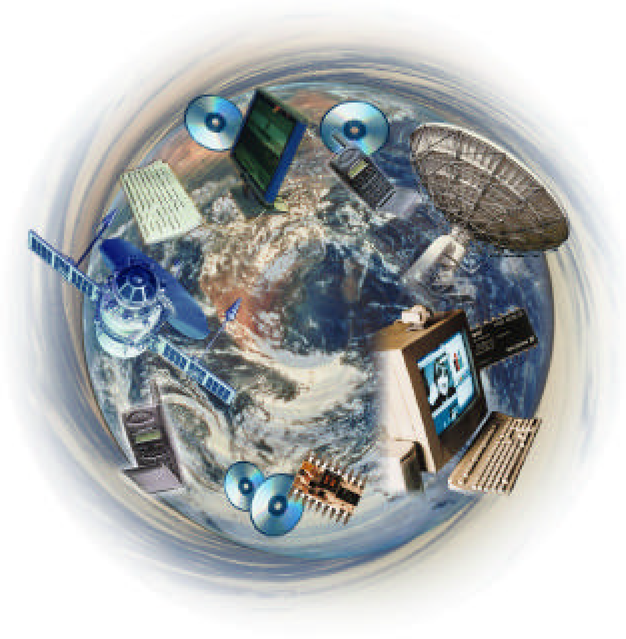
IPv6 in 3G Wireless Networks

White Paper



The information contained in this document represents the current view of Ericsson Radio Systems AB on the issues discussed as of the date of publication. Because Ericsson must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Ericsson, and Ericsson cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. Ericsson MAKES NO WARRANTIES, EXPRESSED OR IMPLIED, IN THIS DOCUMENT.

CONTENTS

THE MOBILE INTERNET

Ericsson's vision is that all mobile users in the near future will be "always connected, always online". This new service paradigm, together with the use of IP technology, open up tremendous opportunities for service providers and network operators to create new and diverse services.

The rapid increase in the number of Internet users, combined with the expected growth in the number of wireless Internet devices requires a scalable and flexible IP technology to accommodate such fast growth. Internet Protocol version 6 (IPv6) was developed by the Internet Engineering Task Force (IETF) to cater for the future Internet.

The mobile Internet evolution starts with the introduction of GPRS, i.e. packet-switched IP services in legacy GSM networks. GPRS is the stepping stone to 3G networks, and the usage of the mobile Internet is expected to grow rapidly within the next few years.

The integration of traditional telephony and best effort packet data, using one common transport protocol, the Internet Protocol, will lower the operational cost and increase the transport efficiency. A common IP transport network topology will be the enabler for introducing different wireless access technologies, using the same transport protocol, enabling the operator to generate new revenues with small or minimum investment in new equipment.

IPv6 is a key technology to realise the vision of large number of users being "always connected, always online". New services, such as IP multimedia assume globally unique addressing for reachability. IPv6, with its very large address space, will guarantee a globally unique IP address for each device.

It is also important to plan for IPv4 to IPv6 migration and coexistence for the wireless networks. An IPv6 network will need to interoperate with IPv4 networks and hosts for a long time. An IPv4 to IPv6 migration based on business needs and benefits for users and operators are to be prioritised. To support a sound migration, it is important that IPv6 and IPv4 can be used in routers or terminals for wireless 3G systems.

The aim of this paper is to explore the different aspects of IPv6 within a 3GPP cellular network. Specifically, addressing, migration, security, spectrum efficiency over the air and mobility are discussed.

THE BENEFITS OF IPV6

Wireless networks have very high requirements in terms of scalability, quality of service and security. IPv6 addresses all these issues. Standardisation of IPv6 has reached a point where it is ready for commercial service and is being promoted through industrial forums of major operators and vendors.

The IPv6 architecture and design include a number of attractive features which makes this a very suitable component of an IP-based 3G wireless network. These include:

- Support for a greatly increased address space
- Built-in security
- Improved support for real time routing performance
- Simplified routing architecture
- Additional features to simplify Network Management

In addition to these features, IPv6 includes support for mobility, multicast and anycast addressing of hosts, which will be components of future wireless architectures.

INCREASED ADDRESS SPACE

Every online device or computer needs a globally unique IP address to connect to the Internet. When Internet Protocol version 4 (IPv4) was designed in the 1970s, hardly anyone could foresee that its 32-bit 4 billion unique addresses would ever be exhausted. However, inefficient address assignment has caused a large portion of the IPv4 addresses to be unavailable or unused.

Demand for IP addresses is growing exponentially due to the Internet's evolution. Further draining the pool of IP addresses is the aggressive rollout of "always connected" access and the proliferation of laptops, PDAs, digital cameras, intelligent home appliances, telemetric devices etc. Current Internet users are using dial-up services with a 1:10 ratio of modems per users at the ISP, and hence a factor ten of addresses are saved compared to “always connected”. Given that there may be several “always connected” devices per user it is obvious that IP addresses are a tight resource.

IPv6 has a 128-bit addressing field, which provides enough of addresses for the foreseeable future. Even with thousands of addresses per square meter on earth the addresses will not be a limiting resource. Any device connected to a data communication network may hence have its own unique address.

As from July 14, 1999 public IPv6 addresses are being allocated through the IANA, the Internet Assigned Numbers Authority, to enable global deployment.

BUILT IN SECURITY

With IPsec built into the IP layer, the security comes “for free” with IPv6. This implies that security mechanisms for authentication and encryption are available to all applications without the need to include such support in the applications themselves. The IPsec algorithms can be updated as new and better cryptographic methods appear.

The benefit of having the same security mechanisms for all applications lies mostly in simpler administration of security policies and security associations. Therefore the cost of ownership can be reduced compared to administering multiple security architectures.

QUALITY OF SERVICE (QOS) FOR REAL TIME SERVICES

From the protocol standpoint, the two main IETF standard frameworks for supporting IP Quality of Service (QoS) differentiation, namely Differentiated Services (DiffServ) and Integrated Services (IntServ), are applicable in a similar way to IPv4 and IPv6. This ensures a smooth transition from IPv4 to IPv6 in terms of QoS. Therefore operators that adopt DiffServ or IntServ for IPv4 will find it relatively simple to do the same for IPv6.

The IPv6 standard also adds future possibilities to enhance the Quality of Service mechanisms beyond what is possible in IPv4 using the 20-bit “Flow Label” field in the basic IPv6 header. Using the Flow Label it is possible to add powerful, flow-based, resource reservation schemes to complement the already existing standards. Its use can range from management of individual end user flows to traffic engineering of flow bundles in an MPLS-like fashion. It should also be possible to mix class-based and flow-based QoS mechanisms, since both are explicitly supported in the same header.

In addition to the QoS support in the protocol itself, the features of the IPv6 protocol in general can improve the quality of IP communications. The simple structure of the IPv6 header, with word-aligned field boundaries and the use of extension headers, allows comparable or even improved performance and silicon implementation efficiency with respect to IPv4, even though the header is twice as large. Also, the reduced size of the routing tables due to efficient aggregation can provide faster lookups and therefore improved routing speeds, which may increase the available QoS. Finally, the necessity to use Network Address Translators (NATs) in IPv4 due to address scarcity is not applicable to IPv6, thus foregoing the end-to-end performance degradation of NAT processing and providing IPv6 with a corresponding QoS advantage.

SIMPLE ROUTING FOR SCALABILITY

Due to the inefficient allocation of addresses, IPv4 is suffering from limited route aggregation possibilities and thus more complex routing. The introduction of arbitrary prefix lengths (Variable Length Subnet Masks, VLSMs) and routing based on these, known as Classless Inter-Domain Routing (CIDR), allowed more aggressive route aggregation and thus a slow-down in the growth of routing tables in the Internet's core which causes, amongst other things, performance limitations and complex management. However this was not enough to overcome the inefficiency created by the previous allocation of addresses and there are still close to 100,000 routes which need to be tracked in the IPv4 Internet’s core.

Having learnt an important lesson from the problems facing IPv4, IPv6 was designed from the start to provide a hierarchical address space, which has topological significance, facilitating route aggregation and thus providing for greater routing efficiency. In this way the routing tables are kept small even if the number of hosts supported is large. Consequently it also provides a scalable address space that can be flexibly partitioned. The only currently defined unicast address format is that of the Aggregatable Global Unicast Address shown in Figure 1.

The globally routable unicast IPv6 address space is subdivided into three aggregator levels: Top-Level Aggregation (TLA), Next-Level Aggregation (NLA) and Site-level Aggregation (SLA). Typically a TLA route is found at the top-level or core of the routing infrastructure, the corresponding NLA is assigned to an organisation (service provider, corporate etc.) with appropriate connectivity to that TLA provider, while the SLA is used by the organisation owning the corresponding TLA to create its own local addressing hierarchy and to identify subnets. IPv6 also supports address formats having other scopes (e.g. link-local, site-local) which can only be utilised on a specific link or site and special addresses such as anycast and multicast.

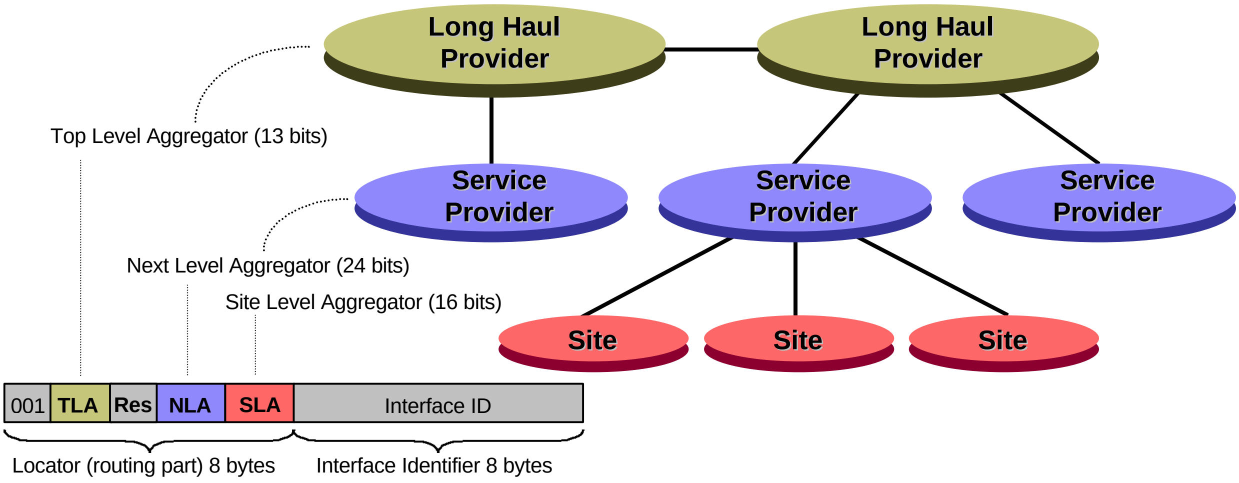

Long Haul Provider
Long Haul Provider
Top Level Aggregator (13 bits)
Service Provider
Service Provider
Service Provider
Next Level Aggregator (24 bits)
Site Level Aggregator (16 bits)
Site
Site
Site
001
TLA
Res
NLA
SLA
Interface ID
Locator (routing part) 8 bytes
Interface Identifier 8 bytes

Figure 1 IPv6 unicast address allocation allows efficient route aggregation

Top level exchanges (in the IPv6 Internet core) will need to handle at most 8192 top level routes (Top Level Aggregators) which is more than a factor of ten times less than the equivalent in the IPv4 Internet core at this point in time.

FEATURES FOR SIMPLIFYING NETWORK MANAGEMENT

IPv6 provides a number of features that will ease the tasks of network management. Stateless address autoconfiguration and automatic DNS configuration will reduce the reliance on DHCP servers and consequently save the effort and cost involved in maintaining such servers.

IPv6 alsoprovides capabilities for automated network renumbering which can not be achieved in today’s IPv4 networks. Router Renumbering mechanisms defined in IETF allow for smooth network renumbering over a period of time without manual interference in each router and/or host. This feature is extremely useful when expanding an existing network, merging two networks or changing ISPs.

The inherent support for multihoming provided by IPv6 is a key enabler for smooth network renumbering. In addition, multihoming can be a useful tool for network administrators to ensure their ability to provide reliable services to their customers. This can be achieved by establishing simultaneous connections to two ISPs, hence providing a backup connection to the Internet in case of failure of one ISP.

IPv6 in GPRS and UMTS

The expected “always connected, always on” paradigm combined with the rapid growth in cellular devices, has led to 3GPP’s decision to mandate IPv6 for all new services, of which the first is IP multimedia. This introduction of IPv6 within the cellular world will impact both cellular terminals and infrastructure significantly. When building an IPv6 cellular network, operators need to consider these impacts and design their networks in a way that allows them to reap the benefits provided by IPv6.

Within a 3GPP network, IP is used for two purposes: End user communication between mobile terminals and application hosts, as well as, the cellular infrastructure networking. Throughout this document, "User-level IP" is used to represent the end-to-end communication between mobile users and application hosts. "Transport-level IP" is used to represent the IP infrastructure connecting the nodes within a 3GPP network. Both User-level IP and Transport-level IP are addressed throughout this document.

IPv6 specific issues are addressed below, starting with addressing for both terminals and the 3GPP core network infrastructure. The necessary tools required for migration and co-existence with IPv4 are described in detail, followed by an analysis of IPv6 security features and their suitability for 3GPP networks.

The scarcity of radio resources in a cellular network, combined with the high prices of 3G licenses, necessitate efficient use of radio resources within a cellular network. The efficiency requirements on IPv6 over the air and necessary mechanisms to support it are further detailed later in the document.

IP mobility is expected to be an important part of future mobile networks. IPv6 provides powerful and flexile mechanisms for handling IP mobility. These features are highlighted and their use in IPv6 wireless systems is explained.

IPv6 Addressing in 3GPP

This chapter highlights the impacts of IPv6 addressing in a 3GPP cellular network and provides information on how to manage address assignment in these networks. Both terminal addressing and network addressing are considered. It should be noted that for operators to successfully select the appropriate address ranges from the addressing registries, careful consideration should be given to the migration mechanisms chosen for both IP levels within the network. A detailed analysis of the relevant migration tools is given later in this paper.

The UMTS/GPRS Backbone (Intra-PLMN) network connects different GSN nodes (SGSN and GGSN) and servers belonging to the same PLMN network. The Gn interface is the interface between different GSN nodes in the same PLMN network, while the Gp is the interface between different PLMN networks. Both the Gn and Gp interfaces support the GPRS Tunnelling Protocol (GTP). The Iu-PS interface between SGSN and UTRAN (UMTS Terrestrial Radio Access Network) also supports the user-plane of GTP (GTP-U). GTP allows IP packets to be tunnelled through the UMTS/GPRS backbone network between GSNs and between SGSN and UTRAN.

The UMTS/GPRS network utilises the Internet Protocol at two different levels within its protocol stack as illustrated for the UMTS case in Figure 2. The Gn, Gp and Gi interfaces are common to GPRS and UMTS. The User-level IP runs between the terminal or User Equipment (UE) and an application server or another fixed or mobile terminal. The terminal is an IP host with respect to the Internet or an Intranet (VPN users). However, the Internet Protocol is also used at the Transport-level to transport traffic and signalling between the devices which make up the Core Network (e.g. GSN nodes). In the case of communication between GSN nodes, the Transport-level IP is used to carry GTP-based traffic and signalling. Similarly we can also distinguish between a network node IP address (e.g. GGSN) and a terminal IP address. Only the latter is visible to end-hosts on the local or external networks.

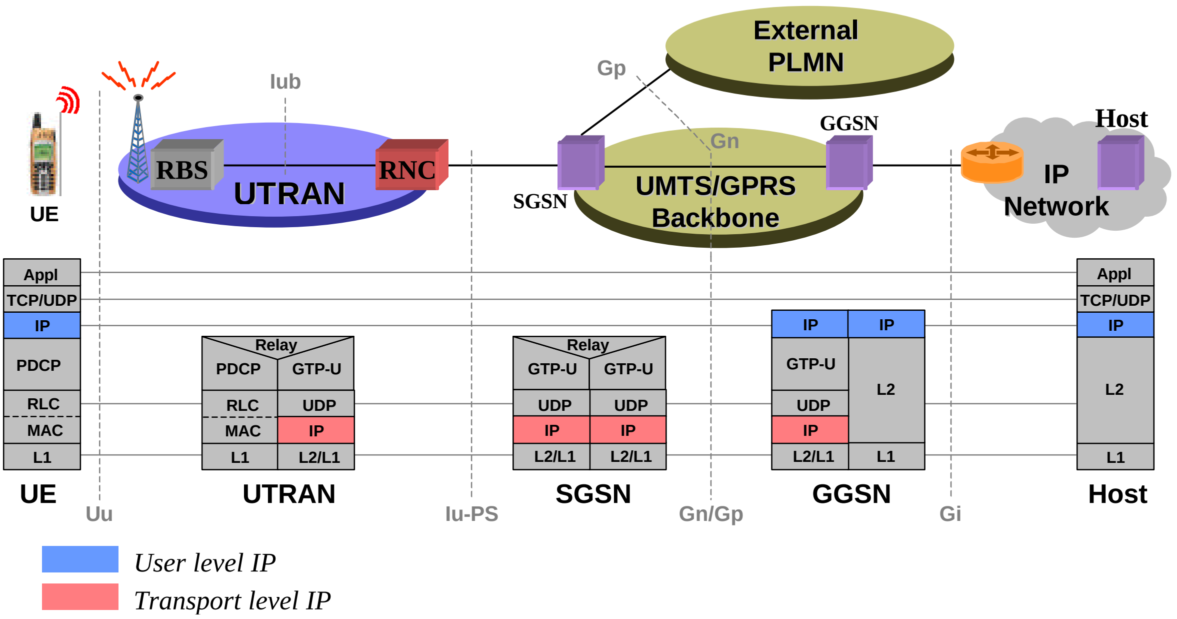


Figure 2 The 3GPP UMTS protocol stack illustrating the two separate IP layers

The Transport-level IP addresses belong to the Gn, Gp and Iu-PS (packet switched user plane) interfaces, while the User-level IP addressing belongs to the Gi interface. Transport-level IP will also exist on the Iub and Iur interfaces within **I**P-based UTRAN, which is being standardised. Therefore these IP addresses must belong to the IP subnets assigned to the corresponding interfaces.

The User-level IP address is allocated to the terminal during 'PDP context Activation' phase, where the SGSN and GGSN establish a context for the session which allows packets to be routed to and from the appropriate external network as requested by the user.

The two layers can use different IP versions. For instance the transport-layer can utilise IPv4 network addresses, while the user-level provides the terminal with global IPv6 connectivity.

In a 3G IPv6 network the operator needs to be allocated some address space by its Internet Registry (RIPE NCC, APNIC or ARIN) to assign addresses to mobile terminals and infrastructure requiring global addresses. As an example, in one solution for 3G cellular systems an operator could treat the network from the user-level IP perspective as one or more Gi subnets and require one or more NLA prefixes (/48) to be allocated for terminal addressing. The appropriate Internet Registry may provide the operator with one prefix having smaller length (e.g. /35) which the operator can subdivide to form the required NLA prefixes. However since dynamic assignment of prefixes to terminals would require further standardisation, the Gi subnets should be allocated smaller SLA prefixes (/64) belonging to the operator's NLA space. These will be aggregated at the borders of the PLMN (where the corresponding NLA prefix belongs topologically). In this case terminals would be allocated /128 addresses. If an operator's 3G core network is spread over a large area, it may be efficient to use more than one border gateway to external networks which may involve the need to request assignment of multiple NLA prefixes depending on their location and connectivity. In addition, the operator may use global or local-scope (e.g. site-local) addresses to build up the network infrastructure (e.g. GGSN node addresses). The Transport-level infrastructure requiring global addresses may use the same address space considered above for terminals or may be assigned a separate (e.g. /48) prefix.

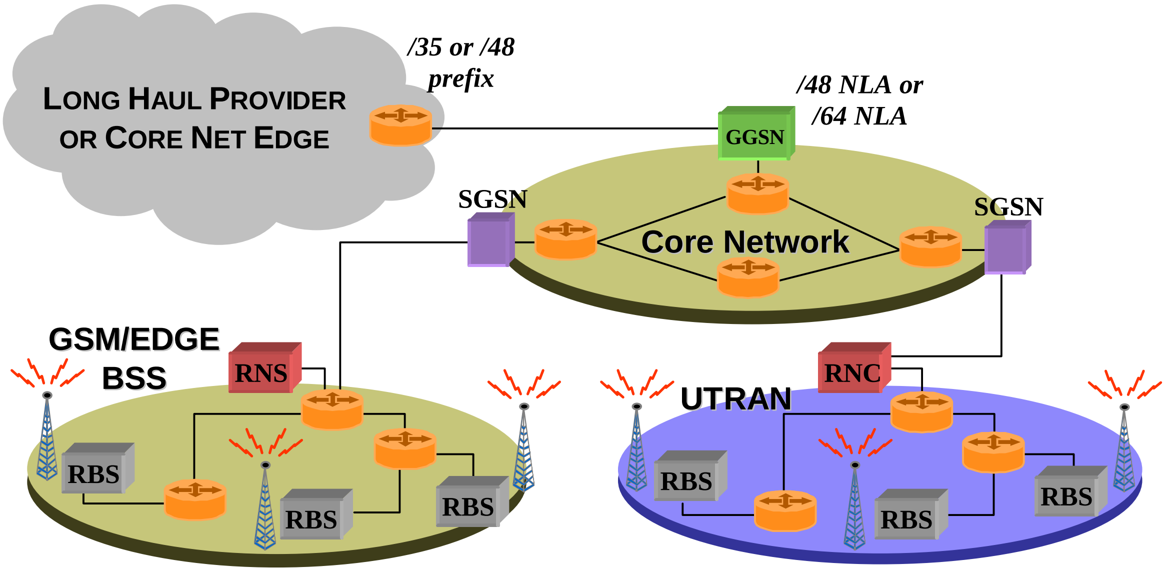


Figure 3 IPv6 Addressing examples for a 3G Network.

Cellular Network Infrastructure (Transport-level) Addressing

The nodes in the UMTS/GPRS Network which require IP addresses are the GSN nodes (SGSN, GGSN), the Border Gateways (BGs), routers, IP Base Stations, O&M nodes, IP Multimedia servers, network servers such as the DNS (Domain Name System) server, NTP (Network Time Protocol) server and so on.

It can be very difficult to manage static IP addresses assignment for many thousands of nodes such as in the case above. Therefore it is useful to deploy an integrated cellular network management system involving a DHCP server which can dynamically assign IP addresses and configure nodes. The IP addresses for the GSN nodes may be statically assigned or dynamically assigned. These IP addresses need to be resolved by the Core Network DNS server, for example, when mapping an Access Point Name (APN) to a GGSN IP address. Therefore dynamic GSN node IP address assignment requires updates to the DNS.

Infrastructure IP addresses may be local-scope or global-scope. Node interfaces, which require communication with external public networks or other PLMNs, require global addresses, while interfaces only visible to cellular network nodes may use local-scope addresses. The following is applicable to infrastructure IP address allocation:

- Global unicast IPv6 addresses for all node interfaces
- Optional Site-local IPv6 addresses for internal network interfaces (e.g. Gn)

In some cases it may be useful to support a "virtual" IP address covering more than one interface rather than to assign an address to a specific interface. This allows redundancy in case of an interface failure (e.g. IPsec VPN on Gi).

The use of IPv4 addressing at the Transport-level for Core Network nodes does not preclude support of IPv6 addresses at the User-level (i.e. in terminals), since the User-level and Transport-level IP-layers in GPRS/UMTS are independent.

User-level IP Addressing

3GPP is defining the support for IPv6 terminals. IPv6 addresses can be assigned statically or dynamically. Just as with IPv4, static address assignment is performed via configuration in the HLR. Only the user having a subscription tied to a static address stored in the HLR may request that address during session (PDP Context) activation. However, this may limit GGSN roaming and the connection to different APNs. Instead dynamic IPv6 address configuration may be obtained using:

- Local assignment from the GGSN address pool/s
- Stateful configuration
- Stateless autoconfiguration

As in the IPv4 case, Stateful configuration involves the assignment of IPv6 addresses from servers such as DHCPv6 servers. Instead stateless autoconfiguration does not have a corresponding mechanism in IPv4 networks. Using stateless autoconfiguration the IPv6 terminal is able to generate its own IPv6 address by combining a prefix with an interface identifier. Such a prefix is contained in the prefix option of ICMP Router Advertisement messages for Global Unicast and Site-Local addresses. When IPv6 is run over PPP (between laptop and 3G terminal), the remote peer suggests the interface identifier. Therefore the GGSN is able to suggest the interface identifier through the PDP Context Activation process and is able to ensure that there will not be a duplication in addresses on the Gi interface. Following PDP Context Activation the terminal will receive a Router Advertisement message from the GGSN and form its IPv6 address.

Aggregatable Global Unicast IPv6 addresses should be used for terminals, which require access to external networks. It is also possible to assign Site Local addresses for access to “local” services in the PLMN. Such local services may be defined using specific APNs. However global unicast addresses are recommended for use in all communications since site-local addresses are not routable outside the site. One specific reason for the use of global addressing as opposed to site-local addressing is GGSN roaming (inter-PLMN) which can allow a terminal to utilise a GGSN at another operator’s site when roaming in that network.

MIGRATION / COEXISTENCE

The need for globally routable IP addresses amongst other benefits has led to the deployment of IPv6 within 3GPP. The key to a wide deployment of IPv6 is the compatibility with the large installed base using IPv4.

This chapter addresses the issues related to IP migration in a 3GPP cellular network. A number of possible migration tools are considered for the mobile terminals as well as the routers within the network. In addition, some recommendations are made as to which migration tools are best suited for operators based on the different network scenarios presented.

For User-level IP migration two different solutions are presented depending on the IP stack supported in the mobile terminal and the availability of IPv4 addresses within the visited domain. For Transport-level IP migration the two most suitable tunnelling approaches are presented.

The migration problem

Two different aspects of the IPv6 migration and coexistence are presented within this chapter, depending on the two stacks used for communication between two nodes. It should be noted that more scenarios can be identified when abstracting the migration problem. However, the scenarios considered in this chapter are limited to the possible scenarios within the 3GPP architecture.

End to End Migration problem

During the initial deployment of IPv6, it is expected that most terminals will implement dual stacks. However, as IPv6 becomes more widely deployed many memory-limited devices will emerge and may support single IPv6 stacks only. Since many existing IPv4 networks are expected to run IPv4 for a long time, it is essential to provide the necessary mechanisms to allow IPv6 terminals to communicate with the existing IPv4 hosts.

Figure 4 illustrates the end to end migration problem. In this case an IPv6 node is communicating with an IPv4 node. For this communication to be successful, an intermediate node is required to translate or re-establish the connection.

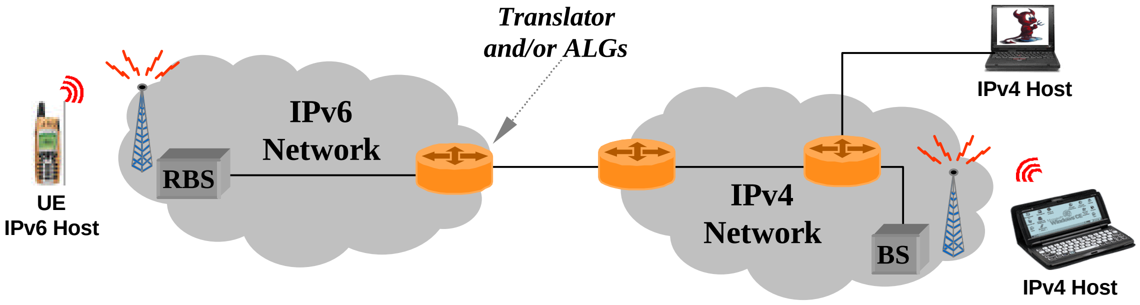


Figure 4 End to End Migration problem

The following section describes the different types of translators available and their applicability.

Connection of IPv6 sites via an IPv4 network

Cellular operators are expected to reuse existing IPv4 backbone networks while introducing IPv6 network islands. For these IPv6 domains to communicate effectively, tunneling of IPv6 packets into IPv4 packets must be supported. Furthermore, given that the Internet is an IPv4 network and will remain so for the foreseeable future, End User IPv6 traffic between the edge of the mobile network (GGSN) and a v6 host at another location will need to be carried over a v4 network. Both these cases are shown in Figure 5.

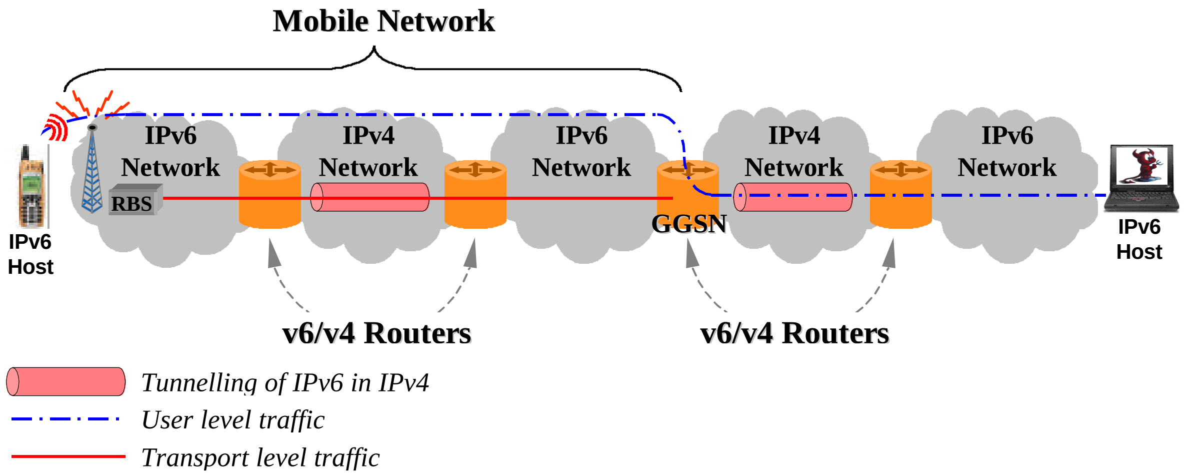


Figure 5 Connection of IPv6 sites via IPv4 networks

It should be noted that tunnelling techniques apply to both Transport-level and User-level traffic. Different tunnelling solutions are explained below in more detail.

Translators and ALGs for end to end migration

The terminal communication scenarios considered in this document are the following:

- IPv6-only terminal communicating with IPv4-only terminal
- IPv4-capable IPv6 terminal communicating with an IPv4 terminal

In this paper, an IPv4-capable IPv6 terminal is a terminal that includes an implementation of an IPv4 stack as well as an IPv6 stack.

For the IPv6-only to IPv4-only scenario several solutions are specified by IETF. The most relevant ones are mentioned and compared below. For the IPv4-capable terminal case, a terminal can simply use its IPv4 stack whenever it needs to communicate with an IPv4 terminal, assuming that enough globally unique IPv4 addresses are available. However, if global IPv4 addresses are not available, the solutions provided for the IPv6-only to IPv4-only scenario are applicable.

Migration Tools for communication between IPv6-only and IPv4-only terminals

Several migration tools exist for the IP layer to enable the communication between IPv6 and IPv4 stacks. Translation mechanisms allow two IP stacks of different versions to communicate. Although the packet translation takes place in the network domain, stateless translators (e.g. SIIT) require that the terminal be aware of this mechanism.

Two types of translators are described below. Distributed translators are considered superior to ALGs and NA(P)T-PT due to their ability to allow end to end communication and lower forwarding delays for real time services. In addition, they support end to end security. However, since distributed SIIT translators require that each node is assigned an IPv4 address for the duration of the connection, several connections from different nodes can not be multiplexed on the same IPv4 address. Hence, in the cases where operators can not provide enough IPv4 addresses, NA(P)T-PT is recommended.

DISTRIBUTED TRANSLATORS (SIIT) FOR OPERATORS WITH SUFFICIENT IPV4 ADDRESSES

The Stateless IP/ICMP Translator (SIIT) was designed to allow IPv6 hosts, which do not have a permanently assigned IPv4 address, to communicate with IPv4 nodes via a stateless IP/ICMP translator. A stateless transition mechanism is one in which no per-connection state is required in the router performing the translation between the IPv4 and IPv6 packet headers. An SIIT router translates the IPv6 header as well as ICMPv6 into IPv4 and ICMPv4 headers respectively. Other headers like Hop by Hop, Routing header and Destination options can not be translated using SIIT.

A distributed translator like SIIT allows stateless translation of packets while keeping the inherent robustness of IP routing. Hence, a failure of one translator does not imply disconnection of any of the sessions going through it. Other advantages include provisioning for end-to-end security and reduced processing delays when compared to ALGs (Application Layer Gateways).

For this translation process to operate successfully, an IPv6 node needs to temporarily acquire an IPv4 address. DSTM (Dual Stack Transition Mechanism) can be used for that purpose using the DHCPv6 extensions. The temporary IPv4 address will be used as an IPv4-translated IPv6 address. DHCP servers provide the SIIT routers within a domain with the mapping information (between IPv4 and IPv6 addresses) to be able to forward inbound packets. Figure 6 illustrates the use of SIIT.

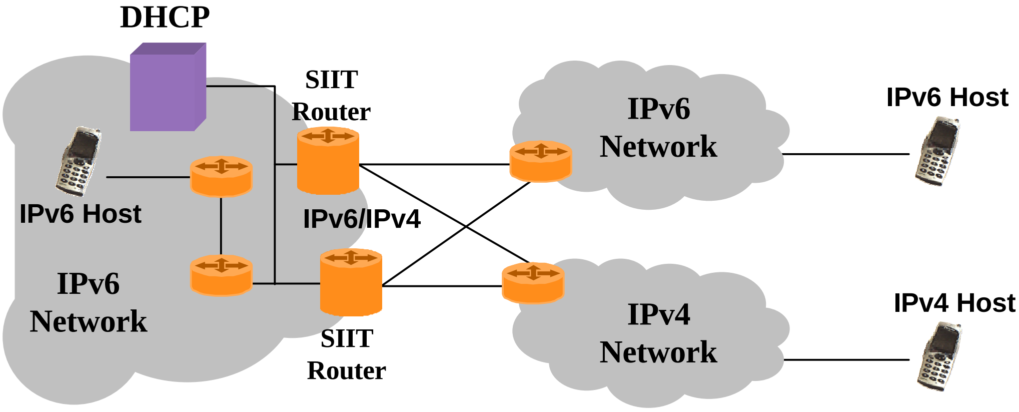


Figure 6 The use of SIIT within an IPv6 network

SIIT USE WITHIN A 3GPP NETWORK

In this case, the mobile terminal acquires its IPv6 addresses statically or dynamically as mentioned earlier. When communication with an IPv4 host is required, the mobile terminal can request an IPv4 address from the local DHCP server. The translation of IPv6 packets to IPv4 packets, and vice versa, can be done within the IP network, as shown in Figure 7, by including SIIT functionality within some of the routers.

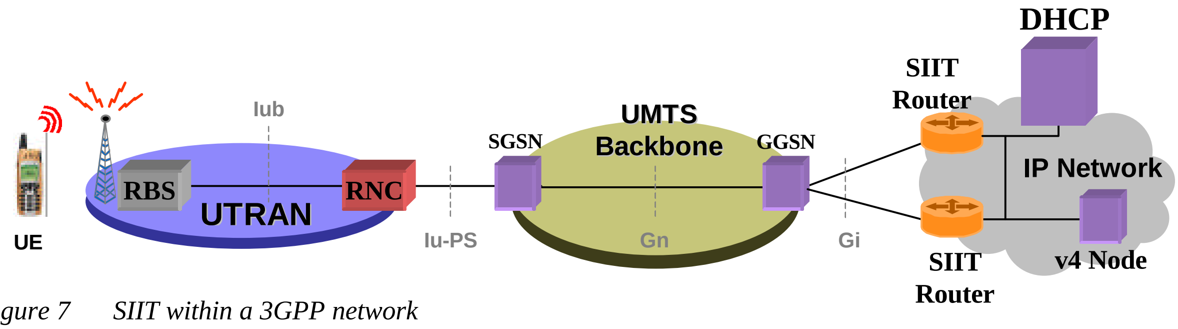


Figure 7 SIIT within a 3GPP network

Mobile terminals will be required to use IPv6 translated addresses to establish connections with IPv4 hosts. Hence, establishing a connection with an IPv4-translated IPv6 address should be supported by the API and the applications using them.

STATEFUL TRANSLATORS AND ALGS (NA(P)T-PT)

Stateful translators like NA(P)T-PT (Network Address, Port Translator and Protocol Translator) are implemented in the border router between IPv6 and IPv4 domains. NA(P)T-PT provides transparent routing to end nodes in an IPv6 realm trying to communicate with end nodes in an IPv4 realm and vice versa. This is achieved using a combination of network address translation and protocol translation. The protocol translation is according to the SIIT specification mentioned above.

The operation of NA(P)T-PT is based on the allocation of temporary IPv4 addresses to IPv6 terminals for the duration of a connection between the two domains. NA(P)T-PT uses a pool of IPv4 addresses for assignment to IPv6 nodes on dynamic or static basis as sessions are initiated across IPv4-IPv6 boundaries. The IPv4 addresses are assumed to be globally unique. NAT-PT binds addresses in the IPv6 network with addresses in the IPv4 network and vice versa (i.e. no assignment of IPv4 addresses to the IPv6 node is performed). Hence transparent routing for the datagrams traversing between IPv4 and IPv6 realms is provided. When using NA(P)T-PT, some application protocols (e.g. SIP) will require Application Level Gateways (ALGs) to be placed in the NAT-PT routers. Operators should consider this requirement when introducing new applications within their networks.

There are different flavours of NAT-PT, for example NAPT-PT allows address and port translation between

IPv6 and IPv4 packets. This provides a more efficient way of handling IPv4 addresses as it allows 64K connections for UDP and TCP sessions to be multiplexed onto the same IPv4 address. While NAT-PT has a number of deficiencies due to the topological restrictions it imposes, lack of end to end security and significant delays in packet forwarding, it may be essential in many scenarios (where operators lack IPv4 addresses) due to its efficient IPv4 address allocation. Figure 8 illustrates the use of NAT-PT or NAPT-PT within an IPv6 network.

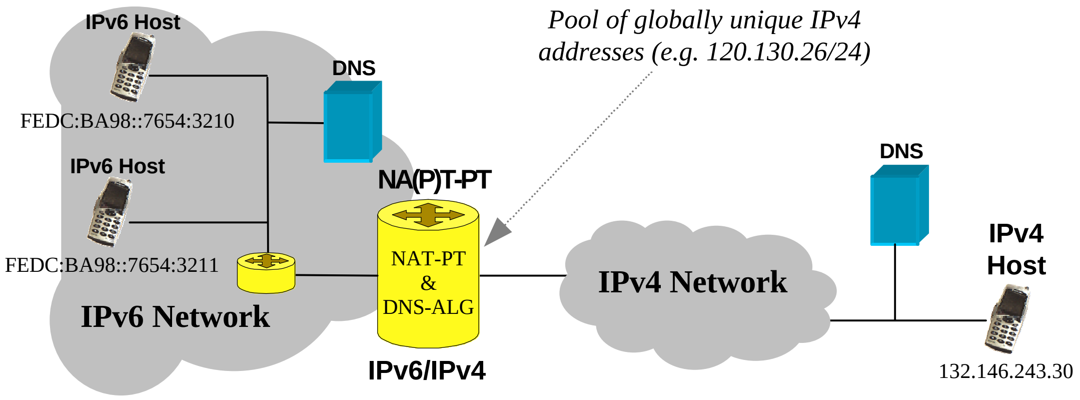


Figure 8 The use of NA(P)T-PT in an IPv6 network.

The use of NA(P)T-PT within a 3GPP network

In this scenario NA(P)T-PT functionality is recommended to allow IPv6 terminals to communicate with IPv4 hosts. The use of NA(P)T-PT allows operators to multiplex a number of connections onto the same IPv4 address. The NAT-PT functionality can be located on the edge of the operator's IPv6 network. In this scenario, NA(P)T-PT is transparent to the end terminals. Hence, no extra requirements are placed on the terminals.

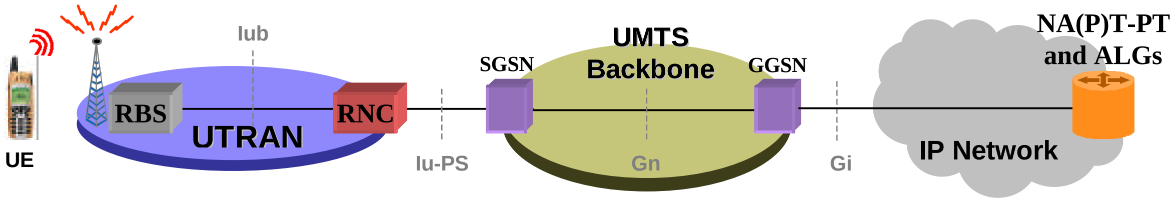


Figure 9 NA(P)T-PT in a 3GPP network

Connecting IPv6 sites over IPv4 backbones using Tunnelling

Tunnelling may be required for User-level and Transport-level traffic to allow IPv6 sites to communicate over existing IPv4 networks.

Tunnelling techniques are usually classified according to the mechanism by which the encapsulating node determines the address of the node at the end of the tunnel. Two different mechanisms are shown below; Configured tunnels and 6-to-4. Both mechanisms can be used for Transport-level IP migration within 3GPP networks.

6-to-4 Tunnelling

The aim of the 6-to-4 tunnelling is to allow IPv6 domains, attached to a wide area network that doesn't support IPv6, to communicate with minimal manual configuration to the border routers. This method allows border routers to discover the IPv4 tunnel-endpoint dynamically by analysing the IPv6 destination address.

To achieve this, a new address format was assigned to enable border routers to find the IPv4 tunnel endpoint from the IPv6 address by allocating one unicast global IPv4 address per 6-to-4 domain. The IPv4 address (V4ADDR below) is included in the 32 bits following the TLA field in a standard IPv6 address. To distinguish this format from a standard IPv6 NLA field, a special prefix (2002::/16) was reserved. Hence, such a prefix would indicate that the following 32 bits represent the IPv4 address of the border 6-to-4 router. Figure 10 shows the reserved address format for a 6-to-4 address.

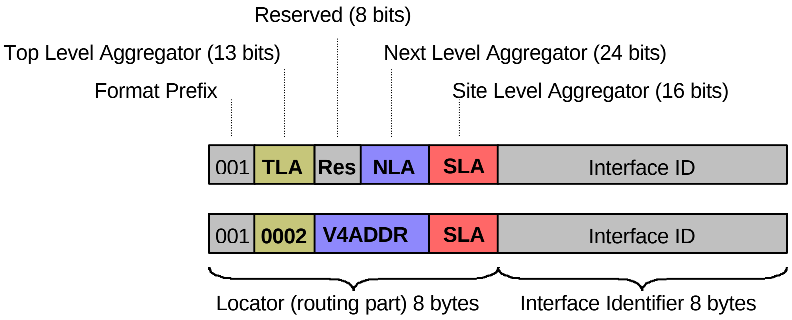

Reserved (8 bits)
Top Level Aggregator (13 bits)
Next Level Aggregator (24 bits)
Format Prefix
Site Level Aggregator (16 bits)
001
TLA
Res
NLA
SLA
Interface ID
001
0002
V4ADDR
SLA
Interface ID
Locator (routing part) 8 bytes
Interface Identifier 8 bytes

Figure 10 A 6-to-4 address format

This mechanism can be applied equally to an individual IPv6 host or an IPv6 site, as long as it has at least one globally unique IPv4 address. However, for a more efficient use of IPv4 addresses, it is recommended that this method be applied to IPv6 sites.

Configured Tunnels

A Configured tunnel can be manually defined in a router or a host’s routing table to associate an IPv6 destination address (or prefix) with an IPv4 tunnel end point. Using this approach IPv6 packets can be tunnelled in IPv4 packets and forwarded over an IPv4 network up to the tunnel endpoint where they will be decapsulated. Both of the encapsulating and decapsulating nodes are required to implement dual stacks to be able to encapsulate/decapsulate IPv6 packets. This mechanism can be used in cases where 6-to-4 addresses are not available, or where there is a limited number of IPv6 destination addresses expected (e.g. between the SGSN and the GGSN).

SECURITY

IPv6 has inherent security features, which may be utilised to protect user-originated and network-originated data and signalling in the cellular network and beyond. Such a protection is required to prevent eventual intruders from accessing or tampering with data and signalling. IPv6 implementations support the IETF IPsec (IP security) standard, which involves two protocol entities:

- Authentication Header (AH) which provides for data integrity and authentication
- Encapsulating Security Payload (ESP) which provides for confidentiality, and optionally data integrity and authentication (more limited than AH)

These protocols may be used on their own or combined in IPv6 packets depending on the security requirements of the communication. They rely on Security Associations (SAs) which must be previously established between the two end-points of the communication in question. Such an SA defines a security “agreement” between entities, mainly consisting of three parts: security algorithm/s, security key/s, and security key lifetime.

In order to use AH and ESP, it is necessary either to configure the secure connection manually with the required parameters (SA), or alternatively use the Internet Key Exchange Protocol (IKE). IKE provides automatic connection establishment for IPsec. It handles the authentication of the peers at the start of the communication, key management, key exchange with negotiation of algorithms and parameters necessary to agree upon the IPsec SAs.

The cellular network utilises the Internet Protocol at different levels within its protocol stack. First, the Mobile Station (MS) is an IP host with respect to the Internet or an Intranet (VPN user). The MS may therefore utilise IPsec to protect traffic and application signalling which it is transmitting. This applies both when the MS is performing an end-to-end communication with entities outside the cellular network (e.g. bank transaction or a confidential call) and within the realms of the cellular network (e.g. signalling between MS and an Application Server within the Service Network). However, the Internet Protocol is also used to transport network-originated signalling and traffic between network nodes. Both the former User-level IP security and the latter Transport-level IP security may be supported as described in the following sections.

Transport-level Security in the Cellular Network

Advanced cellular systems such as GPRS and UMTS benefit from the Internet Protocol's flexibility by relying on it for the transport of traffic and signalling. Such an IP layer operates between cellular network devices, such as the GGSN and the SGSN, for an effective transport of cellular-specific payloads and is different from the "end-to-end" IP layer described in the following section since it only has significance within the cellular network. Operators wanting to avoid a more complex transition from IPv4 to IPv6 in the future may use IPv6 for this purpose. The use of IP in this way allows operators to converge towards an IP-based Multi Service Network.

Since this network may not be implicitly secure, IPsec may be used to secure communications between cellular network nodes such as between the GGSN and the SGSN. As progress is made towards an "All-IP" scenario, communication between the network nodes (and not only the user-level traffic) is more susceptible to attacks, mainly due to the nature of IP technology itself. In this scenario, therefore, internal protection has to be coupled with adequate inter-domain security between operators (e.g. firewalling, security gateways). This may be built up from the security policies based on agreements between operators.

User-level IP Security

Securing the cellular network, as described in the previous paragraph, is a necessity for future generation mobile networks. However, it is also necessary to authenticate, authorise and protect users and their traffic in an end-to-end fashion, such as between a terminal and another terminal or an Internet host, in order to satisfy the need for confidentiality. This leads to a number of different scenarios, where the trust-model and application requirements play a central role.

IPv6 facilitates end-to-end User-level IP security by making IPsec widely available. IPsec has an inherent strength in that it gives users the ability to control the level of security service offered to match the security requirements of individual application flows. Moreover, IKE provides a flexible means for building towards the Public Key Infrastructure (PKI) which may facilitate security in such large-scale scenarios.

However, the implementation of end-to-end User-level IP security in the cellular network may pose limitations on the spectrum efficiency and reliability of IPv6 packets over the air interface, as described in a later chapter, due to limited applicability of header compression mechanisms. The transmission of fully secured packets over the air link is in fact expected to be more costly in terms of spectrum for the cellular channel. The inherent overhead added by IPsec protocols may encourage the use of application-level security as alternative to IPsec. Response to radio-channel induced errors when an encryption scheme is applied, and the applicability of some optimising techniques (e.g. Unequal Error Protection) are also important parameters to be considered. On the other hand, real-time processing requirements for the implementation of security on user devices have equal importance. Ericsson is preparing solutions, which will enable the use of end-to-end security and header compression.

Virtual Private Networks (VPNs)

Mobile users may be Virtual Private Network (VPN) users if they belong to a private network such as a company’s Intranet. Such private networks are normally protected by Firewalls, which allow controlled access to resources, by users on external networks. VPN users communicating using the cellular network require secure tunnelling of traffic in both directions to/from the VPN. In this way VPN users achieve wide-area mobility through the cellular network and still fulfil the security requirements of the private network as if they were directly attached to their VPN. IPv6, through IPsec, allows such functionality by providing secure IPsec tunnelling to the VPN. This may be achieved in two ways: IPsec tunnelling from the MS to the VPN or IPsec tunnelling from the GGSN to the VPN. The first option provides protection of data between the MS and the VPN, but requires transmission of the IPsec tunnel over the air interface, which will impact spectrum efficiency and performance. If the security requirements permit the mobile VPN user to trust the cellular network it is utilising, then the second option allows more efficient transmission over the air interface.

IPv6 “OVER THE AIR”

IPv6 facilitates and opens up new possibilities for the Mobile Internet. This involves the IP “all the way” concept, where the Internet Protocol is carried “end-to-end” from one mobile host to another. In wireless systems this means that IPv6 is carried over the air interface, which is a medium characterized by high bit-error rates and limited resources, therefore requiring high spectrum efficiency. Ericsson has been studying the issues related to IPv6 over the air and is actively working to contribute results to standardization.

The major issue, which stands in the way of IPv6 over the air interface, is the effect of the large header on spectrum efficiency and service quality. For example, voice over IPv6 over wireless would involve an IP header of 40 bytes plus UDP (12 bytes) and RTP (8 bytes) headers which result in a total overhead of 60 bytes. Given that a typical size of the voice payload is 30 bytes, such an overhead would be inefficient both in terms of the expensive radio spectrum and in terms of voice quality, due to the increased likelihood of the packet being damaged by the radio channel.

One way to achieve an improved performance is to terminate the IPv6 protocols before reaching the air interface. This achieves the highest level of spectrum efficiency and service quality but does not follow the IP “all the way” concept and its lack of end-to-end transparency at the IPv6 level makes it inappropriate for use with IPsec and other protocols requiring end-to-end interaction, thus its application is limited.

A solution allowing greater IP-level flexibility is Header Compression (HC), which involves the compression of the large IPv6 headers over the error-prone and capacity-limited air interface while maintaining end-to-end IP-level transparency. Such work has been recently taken up in the IETF through the new Robust Header Compression Working Group (ROHC WG) where the ROHC scheme will be developed. The most relevant existing HC algorithm developed in the IETF was, until recently, CRTP. This algorithm maintains good spectrum efficiency but has been found to result in excessive packet loss rates for realistic cellular links. Ericsson has been a major contributor to the ROHC work through the proposal of the ROCCO (RObust Checksum-based header COmpression) algorithm, which has a high level of compression and robustness suitable for cellular usage. Simulations have shown that ROCCO has superior performance in terms of robustness and compression ratio compared to CRTP. Therefore, using an efficient HC algorithm such as ROHC enables an alternative solution for the deployment of IP “all the way” encompassing a wider set of services.

The maximum compression-ratio profile of ROHC works to reduce the size of IP and higher-layer protocols such as those for the transport of real-time services (UDP and RTP). However, it should be noted that full HC and IPsec/ESP are not compatible, since it is not possible for a HC algorithm to have access to IP headers encrypted by IPsec on an “end-to-end” basis between two hosts. In this particular case, when the maximum header compression is desired, application-layer security is an appropriate alternative to IPsec. In the case in which IPsec is required for confidentiality and application-level security is not applicable, compression is limited to the IPv6 header and the IPsec/ESP header, thus transmitting the full-size encrypted TCP or UDP/RTP headers. The choice of combination between encryption and compression is a matter of security-cost tradeoff. It is then up to the operator whether to levy all or part of the eventual added bandwidth costs on the user.

Performance over the air is also affected when IPsec is used to provide authentication and not confidentiality (i.e. only to provide determination of the identity of the end-users). Header Compression is still applicable, except over the authentication tag, which can itself be considerable in size.

One other point to note regarding the use of IPv6 over the air, is the use of IPv6 extension headers. Due to the need to limit the overhead for the reasons given above, the use of extension headers should be kept to a minimum, at least for conversational multimedia services which require good quality levels and thus reduced error rates. However, their use for best effort services may be permitted at the expense of lower service quality.

IP MOBILITY FOR IPV6

IP mobility results from a mobile node’s topological movement within the Internet. IP mobility should not be confused with a terminal’s mobility within a 3GPP network. Since a terminal’s IP address does not change while moving within a GGSN domain, a terminal’s address is always topologically correct within the Internet.

Mobile IP (MIP) was developed by the IETF to manage a mobile node’s IP mobility and allow nodes to move between IP subnets with minimum interruption to ongoing connections. Like IP, Mobile IP is independent of the underlying link layers, hence it can manage host mobility within an access technology or between different access technologies. MIP can be used to achieve seamless handovers between two different access technologies.

MIPv6 was developed by the IETF to manage IPv6 nodes’ mobility. It contains a number of advantages over the MIPv4 protocol. Most of these advantages are due to the inherent features of IPv6 and the ability to integrate the MIPv6 protocol into the IPv6 stack from day one. Mobility support is mandated in every IPv6 stack, which is essential for producing an effective and inter-operable protocol that can be widely deployed within the Internet.

MIPv6 provides an end to end mechanism for route optimisation between a Mobile Node (MN) and a Correspondent Node (CN). Such feature is important for optimising routing within the Internet and minimising delays in packet delivery.

Due to the very high availability of IPv6 addresses, MIPv6 allows MNs to obtain a topologically correct address when moving to a new subnet. This eliminates the need for additional mobility management functions in the network when compared to Foreign Agents (FAs) in MIPv4. Furthermore, this allows network administrators to use mechanisms like ingress filtering to prevent users from using topologically incorrect addresses within an operator’s administrative domain.

Since IPv6 mandates the support of IPsec in every stack, IPsec is used to secure MIPv6 signalling. This allows for an inter-operable solution that can be integrated within the IPv6 stack.

Mobile IPv6 and 3G

MIP is currently the most accepted solution for IP mobility. MIPv4 is currently supported within the 3GPP standards by the inclusion of the FA functionality in the GGSN. Since no FAs are required in IPv6, MIPv6 does not add any additional requirements on the 3GPP architecture. GTP is used in 3GPP networks for intra-domain mobility. MIPv6 is an attractive candidate to complement this for inter-domain and inter-access technology mobility.

3G Terminals are expected to implement a number of interfaces for use with different access networks. For example, apart from the obvious support for the cellular interfaces, terminals may also support other radio technologies like, Bluetooth, Infra Red etc. Assuming that those access technologies are connected to different access routers, a terminal's IP address may change when moving between those different media. Hence, to ensure seamless mobility and maintenance of ongoing connections, MIPv6 can be utilized. MIPv6 can also be used when roaming between different 3GPP networks, thus allowing a device to be reachable in a route optimized manner.

Figure 11 illustrates the integration of different mobility management protocols for IPv6 wireless systems.

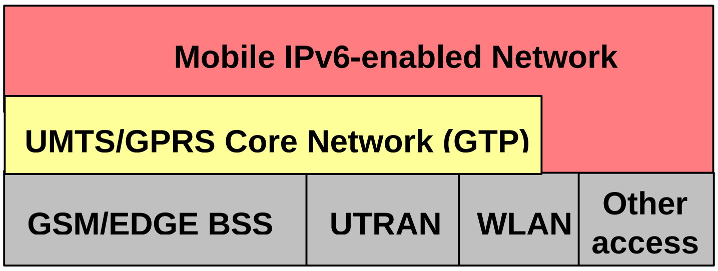


Figure 11 Mobility management within IPv6 wireless systems

CONCLUSION

The future Mobile Internet requires that the chosen Internet Protocol allow a high degree of scalability and efficient management. IPv6 provides a number of features that make it a prime candidate for such environment. These powerful features have led to 3GPP's decision to mandate the use of IPv6 for new services with future releases of UMTS.

For cellular operators to be able to reap the benefits of IPv6, special considerations need to be made when making decisions on for example addressing, security and mobility management within their networks. To be able to utilize the air interface in an efficient manner, network operators and designers must ensure that their networks support the mechanisms defined by the standards bodies to serve this purpose.

When deploying IPv6, it is crucial to consider the necessary migration mechanisms that are needed for both User-level and Transport-level IP within the 3GPP network. This paper has summarized those relevant mechanisms defined by IETF and recommended a set of solutions based on operators' requirements.

APPENDIX

ABBREVIATIONS

3G	Third Generation Mobile Telecommunications
3GPP	3G Partnership Project
AH	Authentication Header
ALG	Application Level Gateway
API	Application Programming Interface
APN	Access Point Name
BG	Border Gateway
BS	Base Station
BSS	Base Station Subsystem
CIDR	Classless Inter-Domain Routing
CN	Correspondent Node
CRTP	Compressed RTP
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DSTM	Dual Stack Transition Mechanism
EDGE	Enhanced Data rates for Global Evolution
ESP	Encrypted Security Payload
FA	Foreign Agent
GGSN	Gateway GPRS Support Node
GSM	Global System for Mobile Communication
GSN	GPRS Support Node
GPRS	General Packet Radio Service
GTP	GPRS Tunnelling Protocol
GTP-U	GTP User plane
HC	Header Compression
HLR	Home Location Registry
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPsec	IP security
ISP	Internet Service Provider
LAN	Local Area Network
MAC	Medium Access Control
MIP	Mobile IP
MN	Mobile Node
MPLS	Multi-Protocol Label Switching
MS	Mobile Station
NAPT-PT	Network Address, Port Translator and Protocol Translator
NAT	Network Address Translator
NAT-PT	Network Address Translator – Protocol Translator
NLA	Next Level Aggregator
NTP	Network Time Protocol
O&M	Operation & Maintenance
PDA	Personal Digital Assistant
PDCP	Packet Data Convergence Protocol
PDP	Packet Data Protocol
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PPP	Point-to-Point Protocol
QoS	Quality of Service
RAB	Radio Access Bearer
RBS	Radio Base Station
RLC	Radio Link Control
RNC	Radio Network Controller
RNS	Radio Network Server
ROCCO	RObust Checksum-based header COmpression
ROHC	Robust Header Compression
RTP	Real-time Transport Protocol
SA	Security Association

SGSN	Serving GPRS Support Node
SIIT	Stateless IP ICMP Translator
SIP	Session Initiation Protocol
SLA	Site Level Aggregator
TCP	Transmission Control Protocol
TLA	Top Level Aggregator
UDP	User Datagram Protocol
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
UTRAN	UMTS Radio Access Network
VLSM	Variable Length Subnet Mask
VPN	Virtual Private Network
WG	Working Group
WLAN	Wireless LAN

READING REFERENCES

Common IPv6 RFCs and drafts

Listed in this section are all Internet specifications that are common for Internet hosts and routers. The specifications are listed by category. All specifications that are Internet drafts are work in progress and may be updated, replaced or obsoleted by other documents at any time.

IPV6 SPECIFICATION

RFC 2460	Internet Protocol, Version 6 (IPv6) Specification
RFC 2461	Neighbour Discovery for IPv6
RFC 2462	Stateless Address Autoconfiguration
RFC 2463	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification

ADDRESSING

RFC 2373	IP Version 6 Addressing Architecture *(draft-ietf-ipngwg-addr-arch-v3-03.txt might obsolete RFC 2373)*
RFC 2374	An IPv6 Aggregatable Global Unicast Address Format
RFC 2526	Reserved IPv6 Subnet Anycast Addresses
RFC 2732	Format for Literal IPv6 Addresses in URL’s

MIGRATION

RFC 2893	Transition Mechanisms for IPv6 Hosts and Routers
RFC 2765	Stateless IP/ICMP Translation Algorithm (SIIT)
draft-ietf-ngtrans-dstm-03.txt	Dual Stack Transition Mechanism (DSTM)

MULTIHOMING

draft-ietf-ipngwg-default-addr-select-01.txt	Default Address Selection for IPv6

HOP BY HOP OPTIONS

RFC 2711	IPv6 Router Alert Option

MULTICAST

RFC 2710	Multicast Listener Discovery (MLD) for IPv6

PATH MTU DISCOVERY

RFC 1981	Path MTU Discovery for IP version 6

HEADER COMPRESSION

RFC 2507	IP Header Compression
RFC 2509	IP Header Compression over PPP
draft-hannu-rohc-signaling-cellular-00.txt	Application signalling over cellular links
draft-ietf-rohc-rtp-rocco-01.txt	RObust Checksum-based header COmpression (ROCCO)

SECURITY

RFC 2401	Security Architecture for the Internet Protocol
RFC 2402	IP Authentication Header
RFC 2406	IP Encapsulating Security Payload (ESP)

DNS

RFC 1886	DNS extensions to support IP version 6
RFC 2874	DNS Extensions to Support IPv6 Address Aggregation and Renumbering

DHCP

draft-ietf-dhc-dhcpv6-15.txt	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
draft-ietf-dhc-dhcpv6exts-12.txt	Extensions for the Dynamic Host Configuration Protocol for IPv6

MOBILITY SUPPORT

draft-ietf-mobileip-ipv6-13.txt	Mobility support for IPv6

INFORMATIONAL RFCS

RFC 1887	An Architecture for IPv6 Unicast Address Allocation
RFC 2185	Routing Aspects of IPv6 Transition
RFC 2292	Advanced sockets API for IPv6
RFC 2375	IPv6 Multicast Address Assignments
RFC 2450	Proposed TLA and NLA Assignment Rules
RFC 2553	Basic Socket interface Extensions for IPv6
RFC 2928	Initial IPv6 Sub-TLA ID Assignment

Router specific IPv6 RFCs and drafts

Listed in this section are all Internet specifications for Internet routers. The specifications are listed by category. All specifications that are Internet drafts are work in progress and may be updated, replaced or obsoleted by other documents at any time.

MIGRATION

RFC 2766	Network Address Translation - Protocol Translation (NAT-PT)
draft-ietf-ngtrans-6to4anycast-00.txt	An anycast prefix for 6to4 relay routers
draft-ietf-ngtrans-siit-dstm-00.txt	Extensions to SIIT and DSTM for enhanced routing of inbound packets
draft-ietf-ngtrans-6to4-07.txt	Connection of IPv6 Domains via IPv4 Clouds

ROUTING

RFC 2858	Multi protocol Extensions for BGP-4
RFC 2545	Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
RFC 2740	OSPF for IPv6
draft-ietf-isis-ipv6-01.txt	Routing IPv6 with IS-IS (Replacing OSPF?)
RFC 2080	RIPng for IPv6

TRANSPORT

RFC 2464	Transmission of IPv6 Packets over Ethernet Networks
RFC 2472	IP Version 6 over PPP
RFC 2492	IPv6 over ATM Networks

TUNNELLING

RFC 2473	Generic Packet Tunnelling in IPv6 Specification
RFC 2529	Transmission of IPv6 over IPv4 Domains without Explicit Tunnels

QOS

RFC 2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
RFC 2475	An Architecture for Differentiated Services

MIBS

RFC 2452	IP Version 6 Management Information Base for the Transmission Control Protocol
RFC 2454	IP Version 6 MIB for the User Datagram Protocol
RFC 2465	MIB for IP Version 6: Textual Conventions and General Group
RFC 2466	MIB for IP Version 6: ICMPv6 Group

OTHER / OPTIONAL RFCS

RFC 2147	TCP and UDP over IPv6 Jumbograms
RFC 2675	IPv6 Jumbograms
RFC 2497	Transmission of IPv6 Packets over ARCnet Networks
RFC 2590	Transmission of IPv6 Packets over Frame Relay Networks Specification
RFC 2467	Transmission of IPv6 Packets over FDDI Networks
RFC 2470	Transmission of IPv6 Packets over Token Ring Networks
RFC 2491	IPv6 over Non-Broadcast Multiple Access (NBMA) networks