



Transition to IPv6 in 2G and 3G mobile networks

NOKIA
CONNECTING PEOPLE



Contents

Executive Summary	3
IPv4 to IPv6 Transition	4
Transition methods	4
Dual IPv4/IPv6 stack	4
Tunnelling	4
Translators	4
IPv4 to IPv6 transition phases	4
IPv4 to IPv6 transition scenarios	6
The scope – Application layer IP	6
The network model	7
Mobile terminal connection to the network	7
The reference network	8
Different combinations	9
Examples of transition scenarios	9
Native IPv4 terminal	9
Dual stack terminal	11
Native IPv6 terminal	13
Application/service aspects	13
Conclusions	13
Abbreviations	14

Executive Summary

The limited size and structure of the current Internet address space provided by Internet Protocol version 4 (IPv4) is proving to be incapable of coping with the explosive increase in the number of Internet users. Neither network address leasing nor translation are ideal for the new generation of applications such as IP telephony, mobile IP, and push applications that assume unique addressing and client reachability. To deal with these problems, Internet Protocol version 6 (IPv6) has been adopted as a functional and durable solution.

IPv6 has been standardised by IETF (Internet Engineering Task Force), with a basic set of standards finalised in 1998. It is now ready for use. The 3GPP (3G Partnership Project) has specified IPv6 as a mandatory IP protocol in Release 2000 IM CN (IP Multimedia Core Network) subsystems, as there are not enough public IPv4 addresses available for all the mobile terminals connected to the Internet. Use of private IPv4 addresses and address translators would greatly complicate the network infrastructure.

The most important benefit of IPv6 is the huge address base, meaning that all nodes can have their own globally unique IP addresses. Security is also a major feature of IPv6, with IP Security (IPSec) providing the ability to encrypt/authenticate all traffic at the IP level, i.e. all applications running over IP can be secured.

Mobility is also catered for, with IP Mobility (Mobile IPv6) being a standardised part of the protocol. In Mobile IPv6, each mobile element (mobile node) is identified with a home address stored by its Home Agent (HA). When the mobile is attached to some foreign link, it is addressable by one or more care-of addresses, in addition to its home address.

When moving towards IPv6 in mobile networks, the biggest changes are needed in the GGSN (Gateway GPRS Support Node) elements in the mobile core network and in the mobile terminals. Implementing support for the dual IPv4/IPv6 stack is important for these elements.

IPv4 networks and services will continue in existence for quite a long time, making efficient interworking between IPv4 and IPv6 very important. The transition from IPv4 to IPv6 requires special care and attention. The transition period will be lengthy and network/terminal equipment supporting both IP versions will be needed. The ultimate aim is to make all services function on the IPv6 platform.

The three main transition methods are dual IPv4/IPv6 stacks in network elements/ terminals, tunnelling and translators in the network. Nokia sees the main mechanisms as dual stacks and tunnelling, with translators needed only if the communicating elements do not share the same version of IP.

From the mobile network point of view, three transition phases can be identified. In the first phase, there are separate IPv6 islands in the network, which can be connected by IPv4 Internet using automatically or manually configured "IPv6 in IPv4" tunnelling.

In the second phase, IPv6 is widely deployed and numerous services are implemented on the IPv6 platform. IPv6 Internet has a wide deployment, but on some occasions tunnelling via IPv4 Internet is still needed to connect communicating IPv6 nodes. Implementing all new services on the IPv6 platform accelerates IPv6 deployment – mobile networks are leading this development.

In the third phase, IPv6 has achieved a dominant position. IPv6 Internet has global connectivity and all services work on the IPv6 platform. No dual stack functionality or address/protocol translators are needed. This enables the simplification of the network architecture and leads to easier maintenance.

In summary, Nokia promotes IPv6 and supports a gradual, controlled shift to IPv6 in mobile networks.

IPv4 to IPv6 Transition

Transition methods

The three main IPv4 to IPv6 transition methods are

- dual IPv4/IPv6 stacks in network elements and mobile terminals
- tunnelling (automatic and configured)
- IPv4 – IPv6 protocol translators in the network.

Dual IPv4/IPv6 stack

The dual IPv4/IPv6 stack is a very important transition mechanism. On the network side, implementation of the dual stack to, for example, the GGSN, is vital to enable both IPv4 and IPv6 Access Points and to perform IPv6 in IPv4 tunnelling. In addition, the edge router at the border of the operator's IP network and the public Internet should also be a dual stack router. Mobile terminals need dual stacks in order to access both IPv4 and IPv6 services without additional translators in the network.

Tunnelling

Tunnelling, i.e. encapsulating IPv6 packets in IPv4 packets and decapsulating at the other end of the tunnel, is a very important transition method. Tunnelling requires dual IPv4/IPv6 stack functionality in the encapsulating/decapsulating nodes. In configured tunnelling, the endpoint of the tunnel is manually configured to a certain IPv4 address. In automatic tunnelling, the encapsulation is done automatically in the encapsulating router/host, and the tunnel endpoint IPv4 address is

included in the IPv6 destination address of the packet. An example of such tunnelling mechanism is the so-called "6to4" tunnelling.

Translators

A translator can be defined as an intermediate component between a native IPv4 host and a native IPv6 host to enable direct communication between them without requiring any modifications to the hosts. The use of translators is typically transparent to the mobile terminals. Header conversion is an important translation mechanism. In this method, IPv6 packet headers are converted to IPv4 packet headers, or vice versa, and checksums are adjusted or recalculated if necessary. NAT-PT (Network Address Translator / Protocol Translator) is an example of such a mechanism.

With these type of address/protocol translators, IP packet header conversion brings the problem of breaking the end-to-end services such as end-to-end IP Security and also bringing a new potential single point of failure in the network. Using address/protocol translators in the network depends mostly on the operator decision and the availability of other transition methods. Translators are recommended only when the two communicating nodes do not share the same IP version.

IPv4 to IPv6 transition phases

Figure 1 gives a simplified picture of the transition phases. These are described from the GPRS/WCDMA mobile network point of view but the principles are also applicable for other network types.

The starting position (the IPv4 world) is the GPRS/WCDMA network supporting only IPv4. All the terminals/laptop computers connected to the Internet are native IPv4 equipment. Network Address Translators (NATs) are used due to limited amount of available public IP addresses.

In the first phase, there are separate IPv6 islands in the network, connected by IPv4 Internet using automatic and/or configured "IPv6 in IPv4" tunnelling. Most IPv6 services provided to mobile users in this phase are in the operator network (Intranet). Other IPv6 services, such as a connection to IPv6 corporate access network, are reachable by configured/automatic tunnels over the IPv4 Internet: conventional IPv4 services are provided to the mobile users having IPv4 or dual stack terminals. There can also be NATs in the operator network which deal with the limited pool of public IPv4 addresses by distributing temporary ones. Also translators such as NAT-PT can be installed in the operator network to perform the IPv4 <-> IPv6 protocol translation.

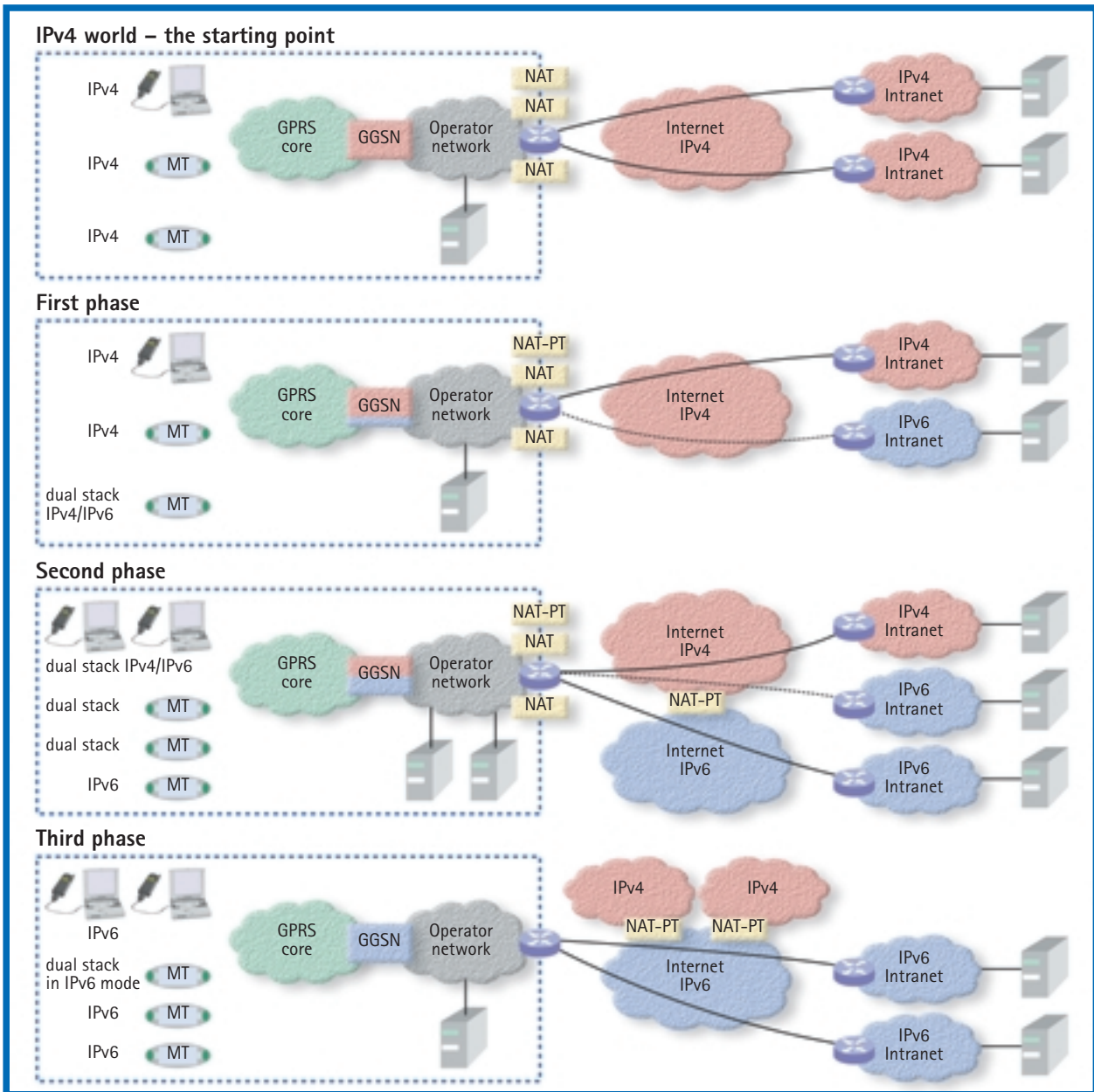


Figure 1. IPv4 to IPv6 transition phases.

In the second phase, IPv6 is widely deployed and numerous services are implemented on the IPv6 platform. IPv6 Internet has a wide deployment, but tunnelling via IPv4 Internet is sometimes still needed as IPv6 Internet does not yet have full connectivity. Implementing all new services on the IPv6 platform accelerates the IPv6 deployment – mobile

networks (e.g. GPRS, WCDMA) help lead this development. Numerous conventional IPv4 services still exist and dual IPv4/IPv6 stacks are installed in many nodes.

In the third phase, IPv6 has achieved a dominant position. IPv6 Internet has global connectivity and all services work on the IPv6 platform.

No dual stack functionality or address or protocol translators are vitally needed in the mobile networks. This enables the simplification of the network architecture and leads to easier maintenance.

IPv6 makes it possible to have a unique, globally routable address for each node in the network.

IPv4 to IPv6 transition scenarios

In this section, the concept of application layer IP is clarified, followed by an introduction to the reference network and the mobile terminal connection. Finally, some transition scenarios are analysed.

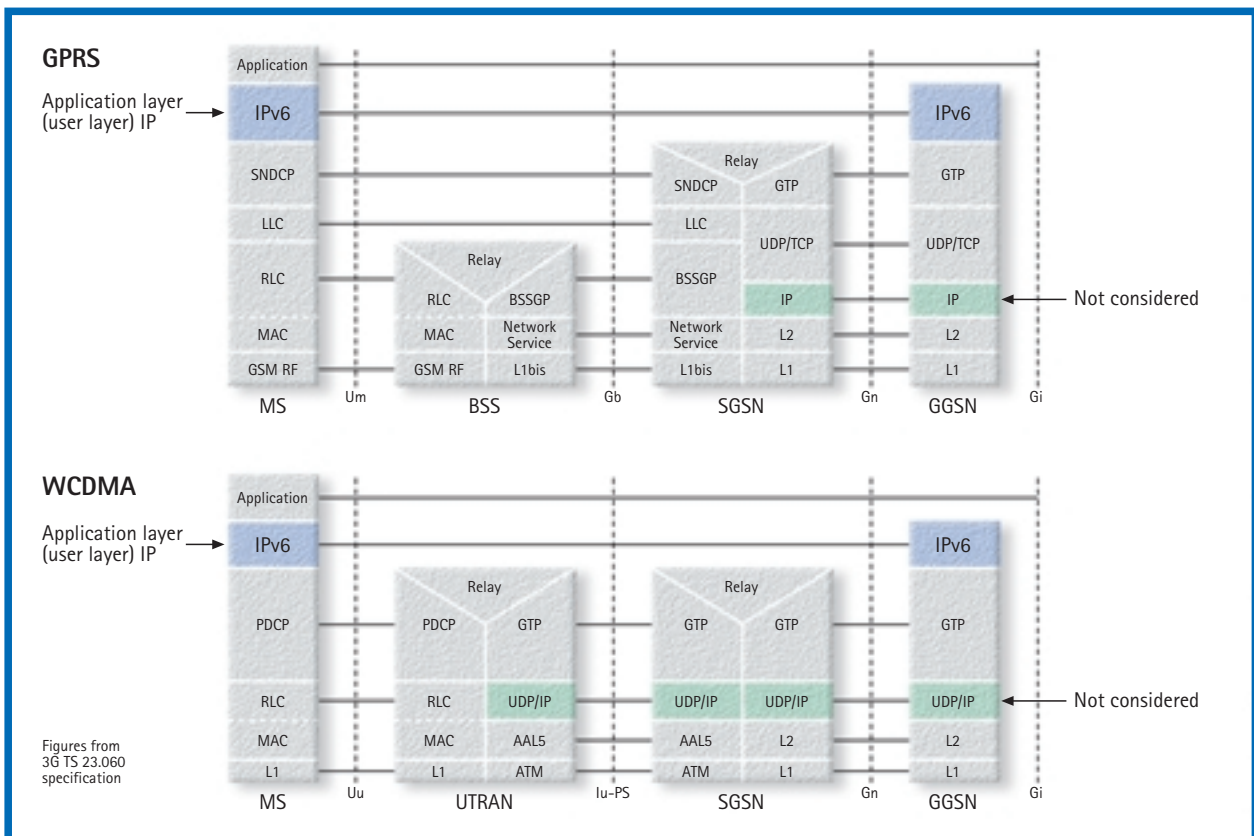
The scope – Application layer IP

This paper outlines the application layer (user layer) IP and the use of IPv6 within it. The transport layer IP (for example, in GPRS networks the core network between SGSN and GGSN elements), although also important in the near future, is not considered.

Figure 2 shows the protocol stacks for the GPRS and WCDMA cases. Clarifying all protocol stacks and their functions is beyond the scope of this paper – more information can be found for example, from 3GPP technical specification 3G TS 23.060 (GPRS Service Description).

The required protocol stacks in figure 2 are described for MS (Mobile Station), BSS (Base Station Subsystem) / UTRAN (UMTS Radio Access Network), SGSN (Serving GPRS Support Node) and GGSN. The application layer IP is on top of the protocol stack (below the applications). Different interfaces (for example, the Gn interface between SGSN and GGSN) are also shown. According to the picture, if the application layer IPv6 support is implemented, mobile terminals (MS) and the GGSN need to support it.

Figure 2. Protocol layers in GPRS and WCDMA.



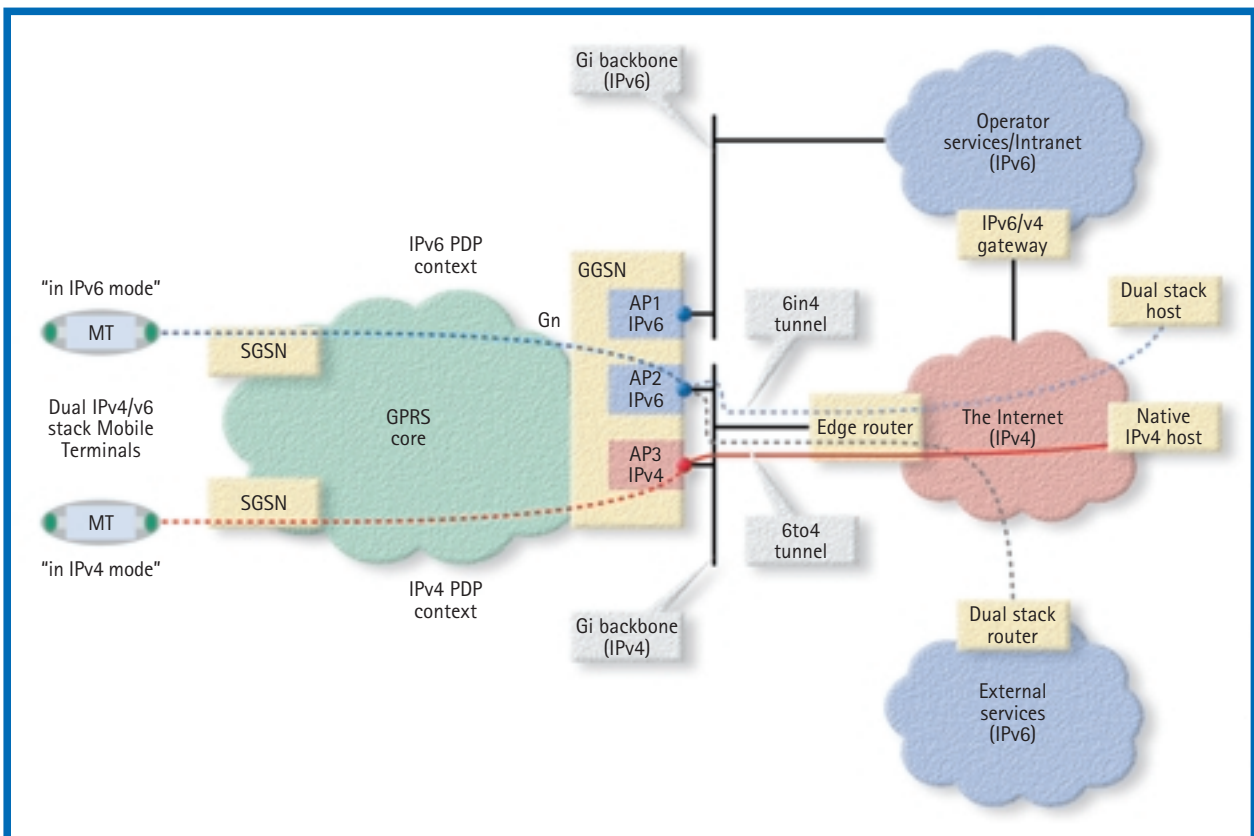
The network model

Mobile terminal connection to the network

The simplified figure 3 shows only the mobile terminals and their connection to the GPRS core network. In a real system, the whole mobile network is between the terminal and the GPRS core network. The connection established between the mobile terminal and GGSN Access Point (AP) is called a PDP (Packet Data Protocol) context. The mobile receives its IP address (IPv4 or IPv6) in the activation of the PDP context. The figure shows two different mobile terminal connections to two different APs of the GGSN.

The topmost branch (AP1) is native IPv6, where the connection never leaves the IPv6 environment (i.e. the connection remains in IPv6 Intranet). Initially, it is assumed that the mobile (GPRS/WCDMA) operator will be the main provider of IPv6 services. The middle branch (AP2) offers IPv6 connections that are tunnelled through an IPv4 network to an external IPv6 host. The tunnel is either “6to4”, if the connection is made to an external IPv6 cloud, or “6in4”, if the other end is a single host in the IPv4 network. “6in4” is a general IPv6 encapsulation inside IPv4 and does not describe how tunnel endpoint addresses are defined. The lowest branch (AP3) is native IPv4 – it provides connections to native IPv4 services/hosts.

Figure 3. Connections to GGSN IPv4 and IPv6 access points.



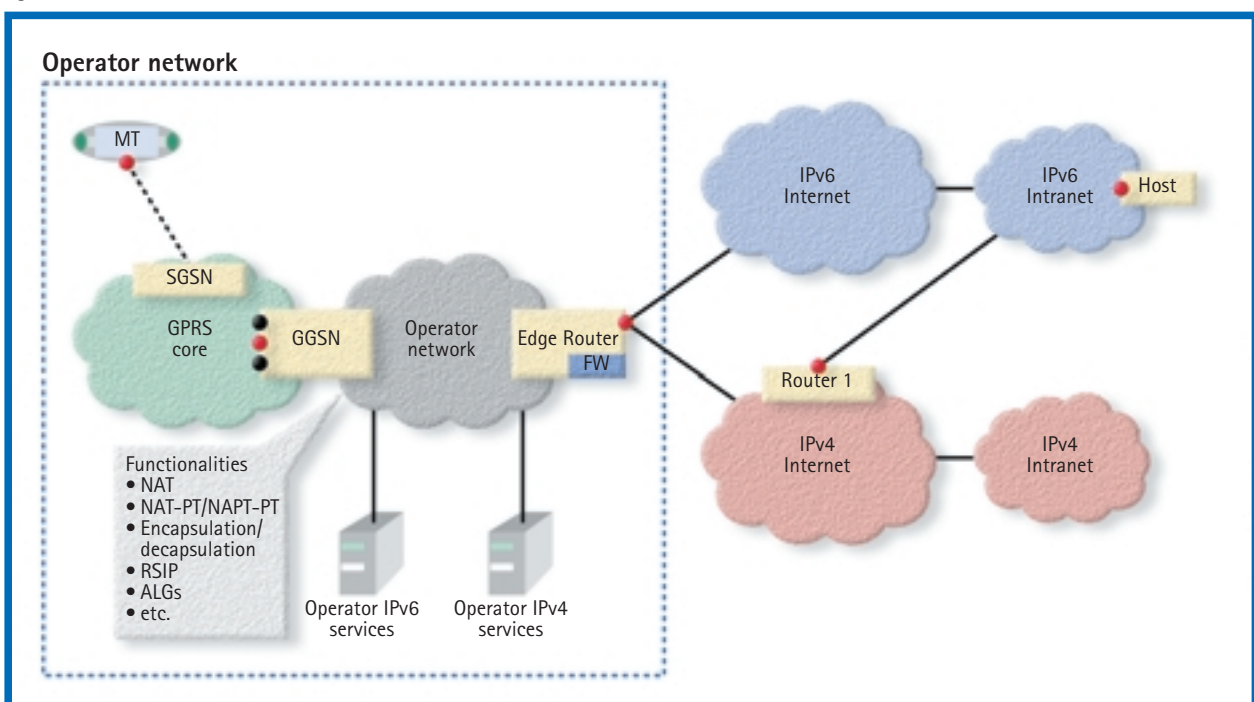
The reference network

Figure 4 represents the network model used in analysing the transition scenarios. The figure is simplified – only mobile terminal (MT) connection to the GPRS core network is shown. The operator’s own IPv4 and IPv6 services (Intranet services) do not necessarily require public IPv4 addresses (private IPv4 addressing is sufficient) or global IPv6 addresses (site local IPv6 addressing is sufficient). When leaving the operator network, traffic goes through the edge router and the firewall. In this case, public IPv4 addresses and global IPv6 addresses are needed. Getting global IPv6 addresses is not a problem, but the typical situation is that the operator has a limited pool of public IPv4 addresses. Mechanisms to provide temporary public IPv4 addresses are needed – NAT is an example of such a mechanism.

IPv4 host in IPv4 Intranet is reached via IPv4 Internet. IPv6 host in IPv6 Intranet can be reached via IPv4 Internet or directly via IPv6 Internet. Tunnelling is needed when connecting to an IPv6 host via a IPv4 network. The tunnel startpoint can be GGSN, edge router, or mobile terminal – the tunnel endpoint can be the host itself or a router (e.g. Router 1 in figure 4) in the edge of the IPv6 network. If the tunnel ends before the host, decapsulation is done in that router. There is also a list of potentially necessary transition functionalities in figure 4.

Figure 5 shows the situation where the dual stack mobile terminal is roaming in a visited network that supports only IPv4, but the user wants to connect to an IPv6 host. The link layer mobility is such that the mobile terminal can connect to its home GGSN and get an access to the IPv6 network. The SGSN in the visited network connects the mobile terminal via GTP tunnelling in the inter-PLMN (Public Land Mobile Network) backbone network to the home GGSN. The Inter-PLMN network connects the operators’ GPRS core networks and requires operators to have a roaming agreement.

Figure 4. The network model in the transition scenarios.



Different combinations

When thinking about the mobile network and a mobile terminal's IP connection to different hosts, several combinations are possible. Basically, the IP versions of the mobile terminal and the peer host (which the mobile terminal is communicating with) are the two fundamental things. However, the network type between those two nodes can vary (native IPv4, native IPv6 or a mixture of IPv4 and IPv6). As a basic rule, if the two communicating IP nodes do not share the same version of IP, protocol translators are needed at some point in the network. Implementing dual IPv4/IPv6 stacks for network elements and mobile terminals is a good solution to ensure that the communicating nodes share the same version of IP.

We can see that there are various scenarios – some of them are described and analysed in the following chapters.

Three different types of network services can be identified:

- Traditional IPv4 services are received via a IPv4 network that has global connectivity – private IPv4 addresses and NATs may be needed due to lack of public IPv4 addresses.
- IPv6 services over IPv6 network – in this case native IPv6 routing is done and no tunnelling over IPv4 Internet/protocol translation is needed.
- IPv6 services over IPv4 network – communicating IPv6 nodes/networks are connected via IPv4 Internet by tunnelling. The use of protocol translation is also possible.

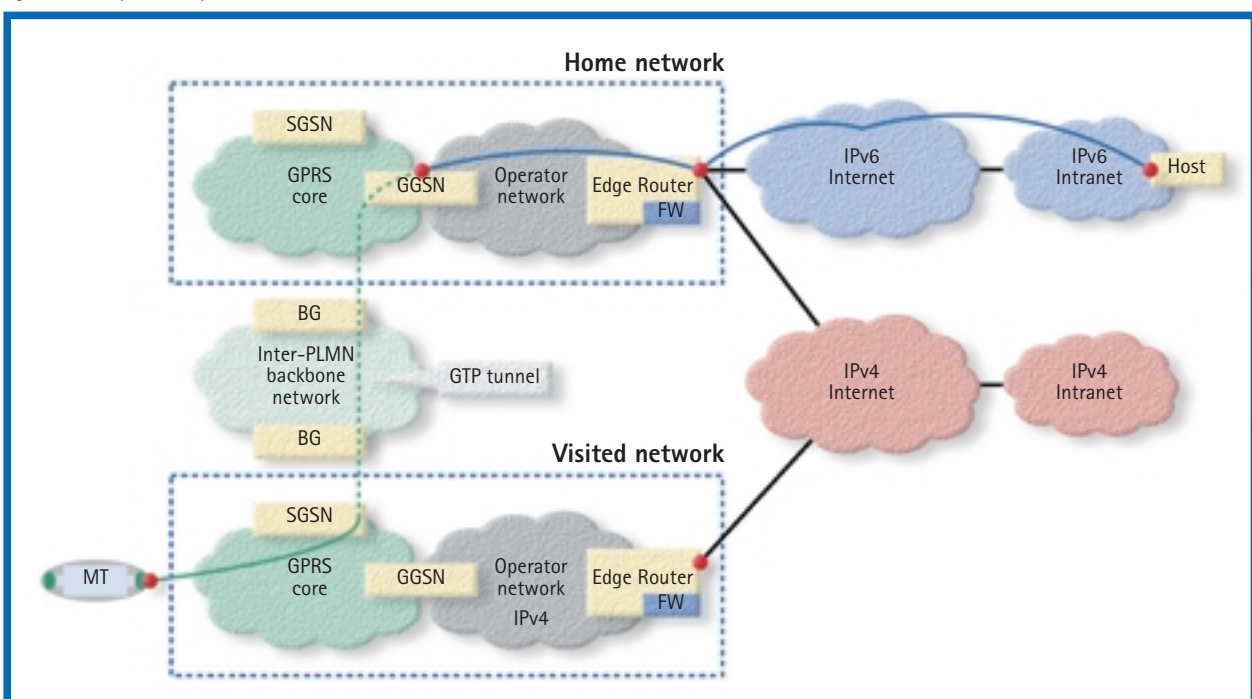
The three types of mobile terminals are native IPv4 terminals (usually the first generation of GPRS/WCDMA terminals), dual IPv4/IPv6 stack terminals, and native IPv6 terminals (in the later phase of the development). Also, peer hosts can be dual stack, native IPv4 or native IPv6.

Examples of transition scenarios

Native IPv4 terminal

Native IPv4 terminals are typically the first versions of GPRS terminals: IPv4 services are provided to native IPv4 terminals. In many cases there isn't a sufficient number of public IPv4 addresses for the mobile terminals and in many cases private IPv4

Figure 5. Link layer mobility – connection to the home network GGSN and an IPv6 host from a visited network via inter-PLMN backbone network.



addresses are allocated. If a mobile terminal with a private IPv4 address is connected to a host over public IPv4 internet, a NAT is needed in the network.

Figure 6 describes three situations. In case a) the mobile terminal is connected to a host in the Intranet. In this case, private IPv4 addressing is sufficient. In case b) the mobile

terminal is connected to a host in the public Internet. The mobile terminal is allocated a public IPv4 address from the operator address space and the connection works

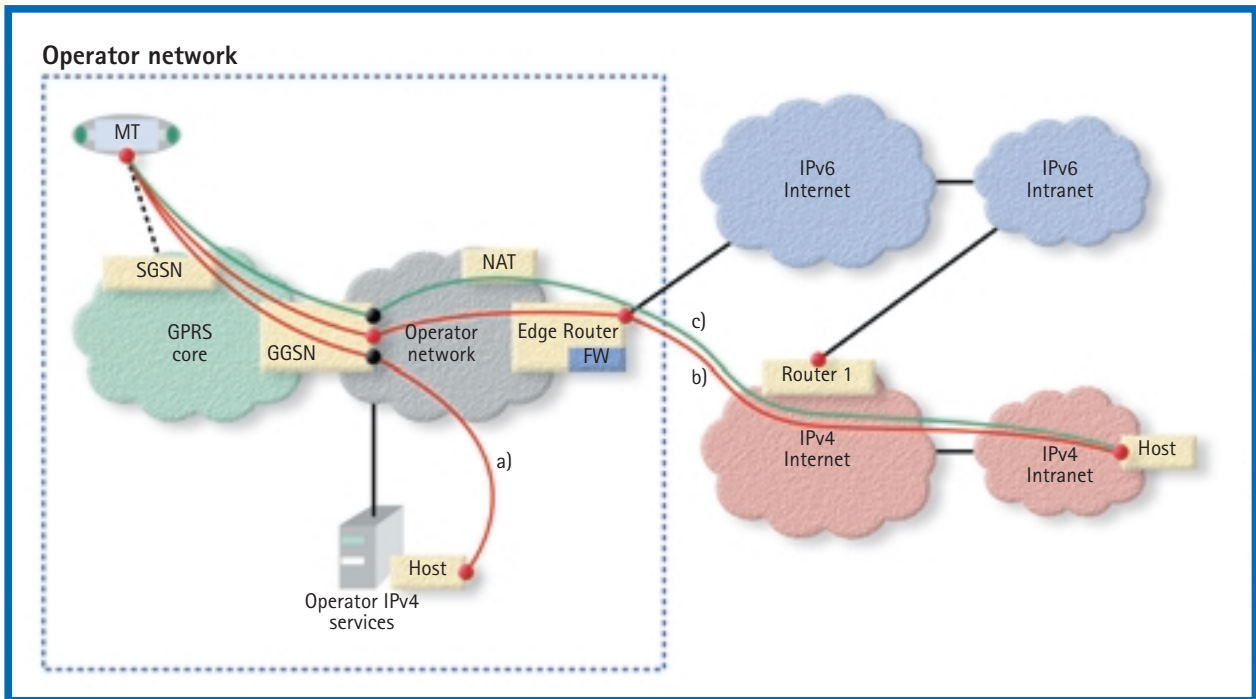
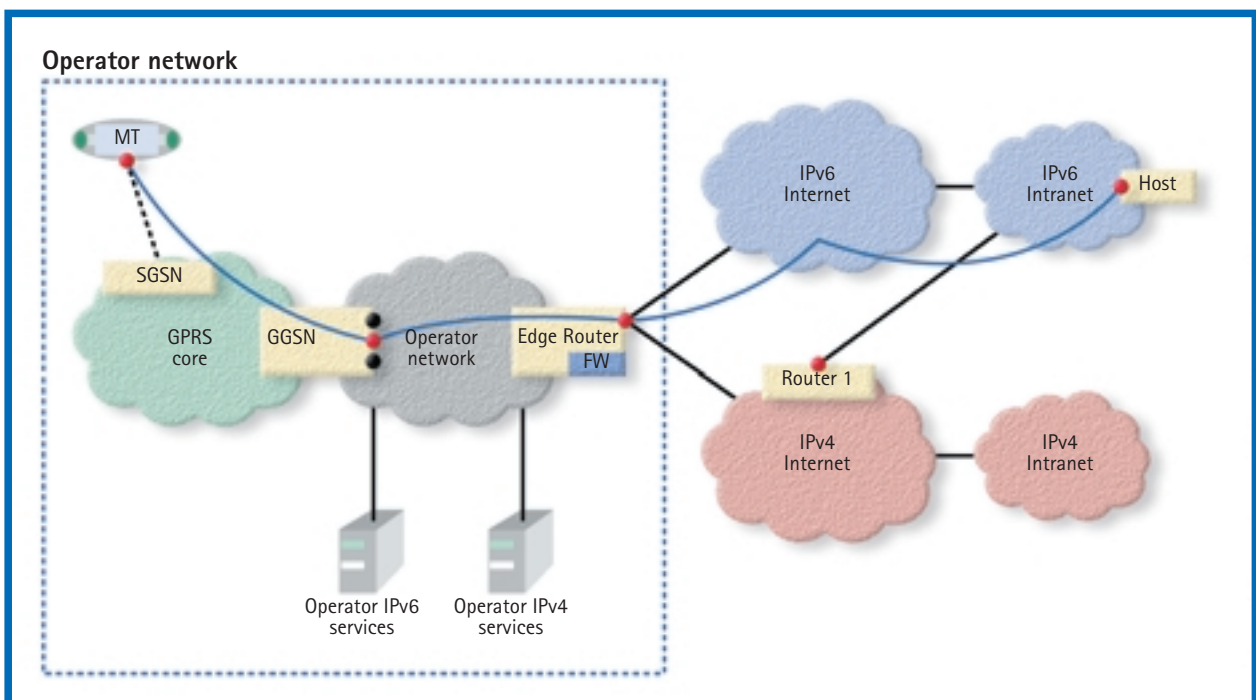


Figure 6. Different IPv4 host connections for IPv4 terminal.

Figure 7. A mobile terminal connection to a native IPv6 host.



by global IPv4 routing. Due to a limited pool of public IPv4 addresses, case b) will only rarely occur. In case c) the mobile has a private IPv4 address, so a NAT function is needed. NAT allocates a temporary public IPv4 address to the mobile in order to make the connection possible.

Dual stack terminal

A basic case is represented in figure 7. The dual stack mobile terminal is operating in IPv6 mode – it opens an IPv6 type PDP context and receives a global IPv6 address from the GGSN. The terminal is connected to a native IPv6 host in the network via IPv6 Internet i.e. all routing is done in the IPv6 domain and no specific transition mechanism is needed. In this scenario, a native IPv6 terminal would work in the same way as the dual stack terminal.

In figure 8, a PDP context is opened between the mobile and the GGSN (the Access Point type is IPv6). In this scenario, the edge router is configured to make the IPv6 packet encapsulation/decapsulation; thus the edge router is the only equipment in the operator’s network which needs a public IPv4 address.

needed; otherwise the automatic “6to4” tunnelling is done between the edge router and Router 1.

IPv6 packets from the mobile node to the host can be sent tunneled via the IPv4 network or directly via the IPv6 network. In many cases, sending via the IPv6 network is not possible, because there is no direct connection. Packets to the host are sent using the “6to4” type address of the host – the IPv4 address of Router 1 is embedded into the host address. If the packets are routed all the way via IPv6 network, “6to4” tunnelling is not

Figure 8. Connection to IPv6 host via IPv4 Internet or IPv6 Internet.

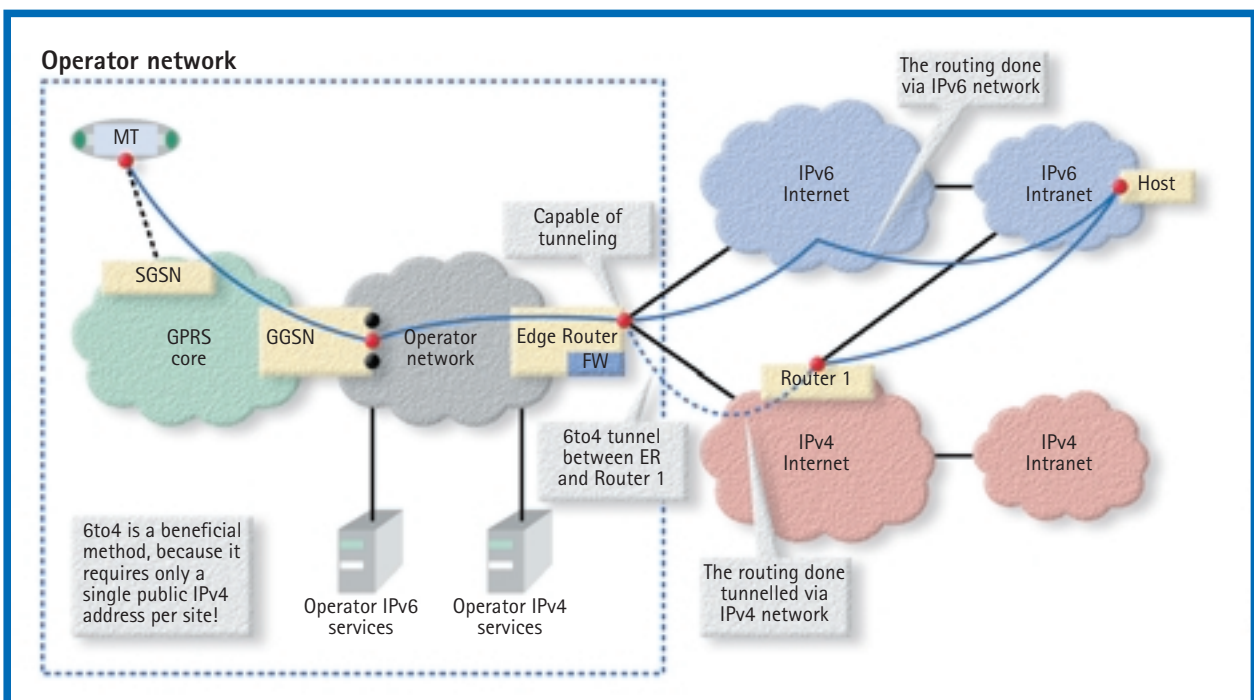


Figure 9 shows the dual stack mobile terminal connection to a native IPv4 host, which could be, for example, a mail server in the IPv4 corporate access network.

The dual stack mobile terminal, which is working in IPv4 mode, is allocated a private IPv4 address due to lack of public IPv4 addresses. The NAT functionality

is needed to provide a temporary public IPv4 address for the mobile terminal. Communication with the peer host over the public IPv4 Internet is then possible.

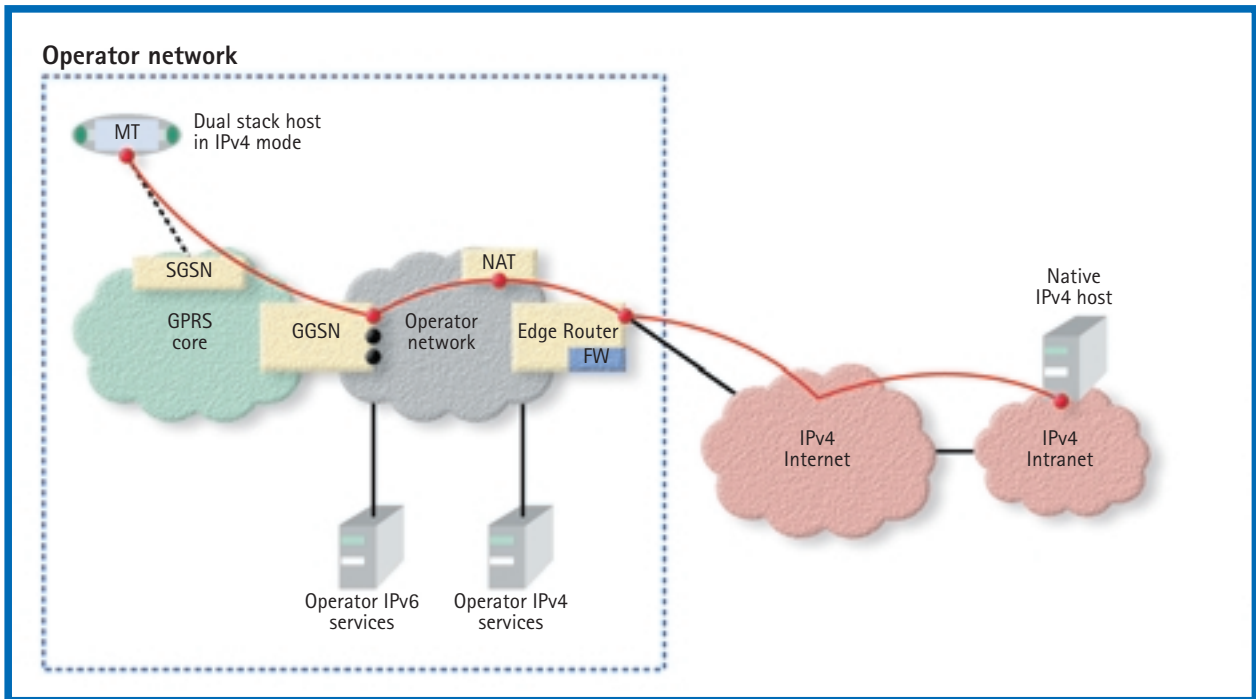
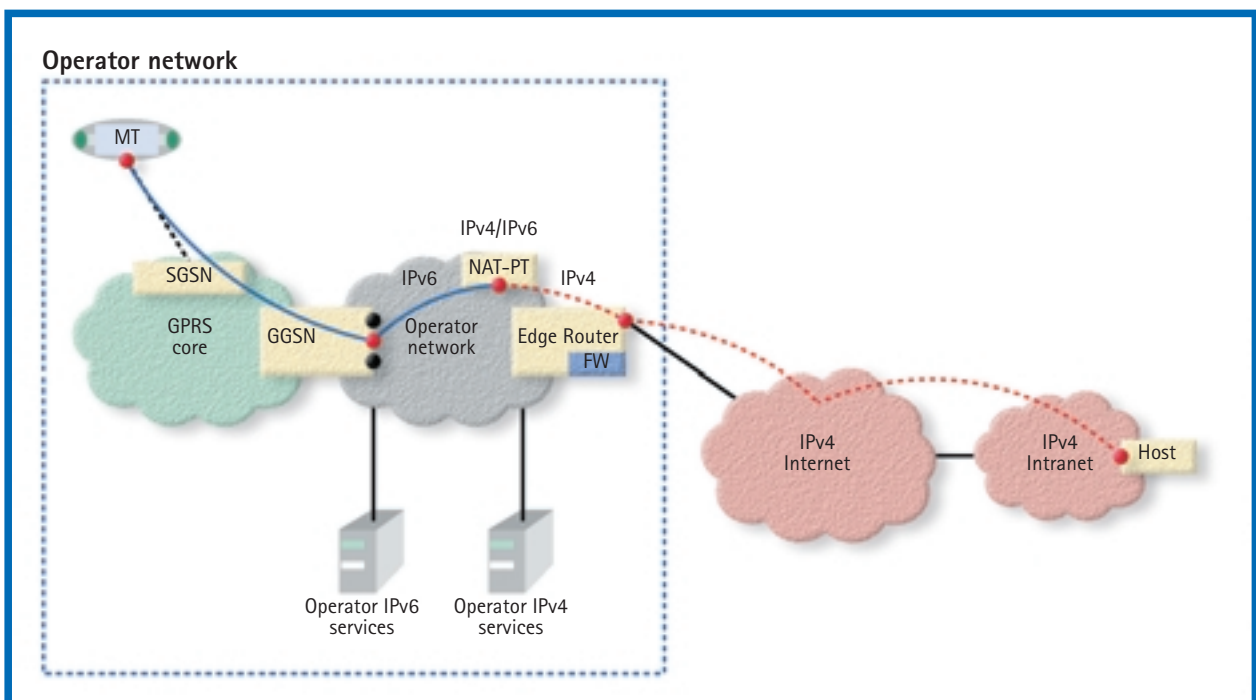


Figure 9. A dual stack mobile terminal connection to a native IPv4 host.

Figure 10. A native IPv6 mobile terminal connection to a native IPv4 host using a translator.



Native IPv6 terminal

The communications of a native IPv6 terminal differ from that of a dual stack terminal. The main difference is that communications between the mobile terminal and a native IPv4 host (also IPv4 Intranet access) always requires a translator such as NAT-PT in the network.

In figure 10, a native IPv6 mobile node gets a global IPv6 address from the GGSN (GGSN AP type IPv6). Because the native IPv6 mobile is connected to a native IPv4 host having a global IPv4 address, a NAT-PT or other translation mechanism is needed to make the IPv6 <-> IPv4 protocol and address translation. The edge router is a dual stack router having global IPv4 and IPv6 addresses. A dual stack terminal would work better in this scenario – in the case of a dual stack terminal a NAT-PT would be unnecessary. A NAT may be needed due to lack of public IPv4 addresses.

Application/service aspects

Applications for which IPv6 is vital include mobile terminated VoIP (Voice over IP), WAP (Wireless Application Protocol) push and other services needing ‘always-on’ support (e.g. real-time connections).

Transition scenarios are not as application dependent. It is recommended that all new services are implemented on the IPv6 platform. In practice, all services can be moved to the IPv6 platform.

Conclusions

Nokia promotes IPv6 and supports gradual transition to it and sees a gradual, controlled shift to IPv6 in mobile networks as imminently feasible.

Transition mechanisms are vital, because the change from IPv4 to IPv6 will not happen overnight and many services will still be working on IPv4. More importantly, IPv6 networks will not at first provide global connectivity. Thus, many IPv6 connections have to be transported over the IPv4 Internet. IPv4 to IPv6 transition issues need special care and attention.

In the opinion of Nokia, the principal transition solution is based on using a dual IPv4/IPv6 stack (in mobile terminals, GGSN elements, and also the edge router in the operator network) and automatic tunnelling. Protocol/address translators, such as NAT-PT, are needed if the connected nodes do not share the same version of IP. Translators have the problem of breaking end-to-end services and it is recommended that the majority of the transition mechanisms are provided by the network – the goal is to keep the mobile terminal functionality as light as possible.

Use cases where the “IPv6 in IPv4” tunnelling in the mobile terminal itself would be vital, have not been identified.

It is also recommended that all new services are implemented on the IPv6 platform. IPv6 provides equivalent or better support than IPv4 for different services. The protocol will soon be in wide spread use, so the time to prepare for it is now.

When the transition to IPv6 has been completed successfully, there will be enough IP addresses for every piece of equipment. The mobile network architecture has been simplified remarkably, because there is no longer a vital need for protocol/address translators or private IP address spaces.

Abbreviations

2G	Second Generation Mobile Telecommunications, including GSM and GPRS technologies	MH	Mobile Host
3G	Third Generation Mobile Telecommunications, including WCDMA technology	MN	Mobile Node
3GPP	3G Partnership Project	MS	Mobile System
ALG	Application Level Gateway	MT	Mobile Terminal
AP	Access Point	NAT	Network Address Translator
BG	Border Gateway	NAT-PT	Network Address Translator-Protocol Translator
BSS	Base Station Subsystem	NAPT-PT	Network Address Port Translator-Protocol Translator
CN	Core Network	PDP	Packet Data Protocol
FW	Firewall	PLMN	Public Land Mobile Network
GGSN	Gateway GPRS Support Node	PPP	Point-to-Point Protocol
GPRS	General Packet Radio Service	QoS	Quality of Service
GTP	GPRS Tunnelling Protocol	RAN	Radio Access Network
HA	Home Agent	RFC	Request For Comments (by IETF)
IETF	Internet Engineering Task Force	RSIP	Realm Specific IP
IM	IP Multimedia (e.g. IM CN subsystem = IP Multimedia Core Network subsystem)	SGSN	Serving GPRS Support Node
IP	Internet Protocol	TCP	Transmission Control Protocol
IPv4	Internet Protocol version 4	TE	Terminal Equipment
IPv6	Internet Protocol version 6	UDP	User Datagram Protocol
IPSec	IP Security	UMTS	Universal Mobile Telecommunications System
		UTRAN	UMTS Radio Access Network
		WAP	Wireless Application Protocol
		WCDMA	Wideband Code Division Multiple Access

Copyright © Nokia Networks Oy 2000. All rights reserved.

No part of this publication may be copied, distributed, transmitted, transcribed, stored in a retrieval system, or translated into any human or computer language without the prior written permission of Nokia Networks Oy.

The manufacturer has made every effort to ensure that the instructions contained in the documents are adequate and free of errors and omissions. The manufacturer will, if necessary, explain issues which may not be covered by the documents. The manufacturer's liability for any errors in the documents is limited to the correction of errors and the aforementioned advisory services.

The documents have been prepared to be used by professional and properly trained personnel, and the customer assumes full responsibility when using them. The manufacturer welcomes customer comments as part of the process of continual development and improvement of the documentation in the best way possible from the user's viewpoint. Please submit your comments to the nearest Nokia sales representative.

NOKIA is a registered trademark of Nokia Corporation. Any other trademarks mentioned in this document are the properties of their respective owners.



Nokia Networks
P.O. Box 300
FIN-00045 NOKIA GROUP, Finland
Phone: +358 9 51121
Fax: +358 9 5113 8200
www.nokia.com

NOKIA
CONNECTING PEOPLE

Nokia code: 10632
0900 Libris
© Nokia Networks 2000. All rights reserved.
Nokia and Nokia Connecting People are registered trademarks of Nokia Corporation.
Other product and company names mentioned herein may be trademarks or trade names of their respective owners.
Products are subject to change without notice.