Transition to IPv6 in GPRS and WCDMA Mobile Networks

Juha Wiljakka, Nokia

ABSTRACT

The limited size and structure of the Internet address space of IPv4 has caused difficulties in coping with the explosive increase in the number of Internet users. IPv6 is a feasible solution for the problems identified with IPv4. Efficient interworking between IPv4 and IPv6 is very important, because IPv4 networks and services will exist for quite a long time. The transition period will be lengthy, and network/terminal equipment supporting both IP versions will be needed during the transition period. Thus, IPv4 to IPv6 transition issues need special care and attention. The three main transition methods are dual IPv4/IPv6 stacks in network elements/terminals, tunneling, and translators in the network. Three transition phases from IPv4 to IPv6 can be identified. These phases are described in the article. Different transition scenarios from the 2G/3G mobile network point of view are also analyzed. Finally, some conclusions are drawn, and some recommendations on the use of transition methods are given.

INTRODUCTION

A great number of mobile terminals and other wireless equipment will be connected to the Internet in the near future. The current Internet Protocol version 4 (IPv4) cannot provide a sufficient number of unique IP addresses for all elements connected to the Internet. Neither network address leasing nor translation is ideal for the new generation of applications, such as mobile terminated voice over IP (VoIP) and push applications that assume unique addressing and client reachability.

Introduction of the General Packet Radio Service (GPRS) technology has started packet-switched IP services in the Global System for Mobile Communications (GSM) networks. The most important new network elements installed in the GPRS core network are the serving GPRS support node (SGSN) and gateway GPRS support node (GGSN). Introduction of the wideband code-division multiple access (WCDMA) radio access technology in Third Generation Partnership Project (3GPP) Release 1999 Universal Mobile Telecommunications System (UMTS) networks continues the wireless Internet evolution with growing data speeds.

IPv6 [1] has been standardized by the Internet Engineering Task Force (IETF) to cope with vastly increased demand from a wide range of users, among them mobile networks. GPRS/WCDMA networks and mobile terminals will all soon support IPv6. The IPv6 protocol also has numerous other strengths, such as enhanced support for IP Security (IPsec) and IP Mobility (Mobile IPv6).

When moving toward IPv6 in mobile networks, the biggest changes are needed in the GGSN elements in the GPRS core network and in mobile terminals. Implementing support for the dual IPv4/IPv6 stack [2] is important for these elements.

IPv4 networks and services will continue to exist 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. IPv4 to IPv6 transition phases and selected transition scenarios are analyzed in the article.

IPV6 BENEFITS

IP ADDRESS SPACE

The most important and visible benefit of IPv6 is the huge number of addresses. The 128 bits in the IPv6 address field makes it possible to express 3.4×10^{38} different addresses. That is a sufficient number to give an IP address to almost every grain of sand on the Earth.

An IPv6 address consists of a 64-bit network prefix followed by a 64-bit interface identifier (suffix) [3]. When thinking about Internet routing, the network prefix is the most important part of the address (routing is based on the network prefix). The addressing scenario of an IPv6 node can be static or dynamic based on the strategy for allocating the interface identifiers.

An important benefit of IPv6 is hierarchical addressing. The ability to perform address aggregation, so-called supernetting, makes the routing tables in the routers smaller.

0163-6804/02/$17.00 © 2002 IEEE

Address autoconfiguration is another important new feature of IPv6, enabling plug-and-play-type network configuration. Address autoconfiguration can be stateful or stateless. In stateful address autoconfiguration, external servers such as Dynamic Host Configuration Protocol (DHCP) are used for address allocation. Stateless autoconfiguration is a simpler mechanism and requires no external servers for address allocation. In the case of stateless autoconfiguration, the addresses are allocated dynamically by the GGSN in the mobile network.

To access IPv6 services beyond IPv4 networks a mobile node may need addresses having special prefixes allocated for the use of IPv4/IPv6 transition mechanisms. An example of such a prefix is the TLA624 prefix for *6to4* address [4]. In this address type, the IPv4 address of the encapsulating/decapsulating router is included in the IPv6 address prefix. The IPv4-compatible address can be used only for IPv4/IPv6 dual stack nodes that can receive and decapsulate IPv6 in IPv4 encapsulated packets. The address is constructed of the IPv4 address of the node (v4ADDR) and the preceding zeros. IPv4-mapped IPv6 address can be used only for native IPv4 nodes. This address type is IPv4 address represented as *IPv4-mapped IPv6 address*, used, for example, in the Stateless IP/ICMP Translator (SIIT) protocol translator.

IP Security

The IETF IPsec Working Group has worked on defining protocols to address several major areas, such as data origin authentication, data integrity, data confidentiality, and replay protection, which ensures that an attacker can't intercept a datagram and play it back at some later time.

The IETF IP Security Working Group has worked on defining protocols to address several major areas, such as data origin authentication, data integrity, data confidentiality, and replay protection, which ensures that an attacker can't intercept a datagram and play it back at some later time.

IPsec is an integrated part of IPv6 and provides the capability to secure communications across a LAN, across private/public WANs, and also across the Internet. The power of IPsec is that it can encrypt/authenticate all traffic at the IP level; that is, all applications running over IP can be secured.

There are two extension headers:

- Authentication header (AH)
- Encapsulating security payload (ESP)

AH [5] provides connectionless integrity, data origin authentication, and an optional anti-replay service. AH is a feasible protocol when confidentiality is not required or permitted. ESP [6] provides confidentiality (encryption), data origin authentication, connectionless integrity, anti-replay-service, and limited traffic flow confidentiality. The authentication provided by ESP is not as broad as that provided by AH. ESP protects only those fields coming after the ESP header.

AH and ESP support two modes: transport and tunnel mode. The transport mode IPsec is typically applied between a mobile host and a server computer in the corporate access network. A secure data link over the Internet is established. The tunnel mode IPsec is typically applied between security gateways to form a virtual private network (VPN) over the public Internet.

IP Mobility

IP Mobility is a standardized part of IPv6. In Mobile IPv6 [7], each mobile node is identified with its home address stored by its home agent (HA). The static home address does not depend on the mobile node's current point of attachment to the IP network. When the mobile node is attached to some foreign link, it is also addressable by one or more *care-of addresses*. The subnet prefix of the mobile node's care-of address is the subnet prefix on the foreign link. The association between a mobile node's home address and care-of address is known as "binding" for the mobile node.

IP mobility is also specified for IPv4 (Mobile IPv4), but IPv6 provides more enhanced support for it. The benefits of Mobile IPv6 over Mobile IPv4 include:

- The huge address space of IPv6 makes Mobile IPv6 deployment more straightforward.
- IPv6 address autoconfiguration simplifies the care-of address assignment for the mobile node, also easing the address management in a large network infrastructure.
- Optimized routing: Mobile IPv6 avoids so-called *triangular routing* of packets from a correspondent node to the mobile node via the HA. This reduces transport delay and saves network capacity.
- There is no need for foreign agents in Mobile IPv6.

Mobility inside a mobile network does not necessarily need Mobile IP. Link layer (layer 2) mobility using GTP (GPRS Tunneling Protocol) tunnels is commonly used in GPRS and WCDMA mobile networks. Mobile IPv6 can be used as a complementary mobility mechanism; in particular, mobile terminals with additional noncellular interfaces (e.g., WLAN) benefit from Mobile IPv6 if they need to retain sessions while moving between different access technologies. Such terminals can use Mobile IPv6 for intersystem IP handovers.

Transition from IPv4 to IPv6

The three main IPv4 to IPv6 transition methods are:

- Dual IPv4/IPv6 stacks in network elements and mobile terminals
- Tunneling (automatic and configured)
- IPv4 to IPv6 protocol translators in the network

Transition Methods

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, say, the GGSN is vital to enable both IPv4 and IPv6 access points and to perform IPv6 in IPv4 tunneling. 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.

Tunneling — Tunneling means encapsulating IPv6 packets in IPv4 packets and decapsulating in the other end of the tunnel [2]. Tunneling requires dual IPv4/IPv6 stack functionality in the encapsulating/decapsulating nodes. In configured tunneling, the endpoint of the tunnel is manually configured to a certain IPv4 address. In automatic tunneling, 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

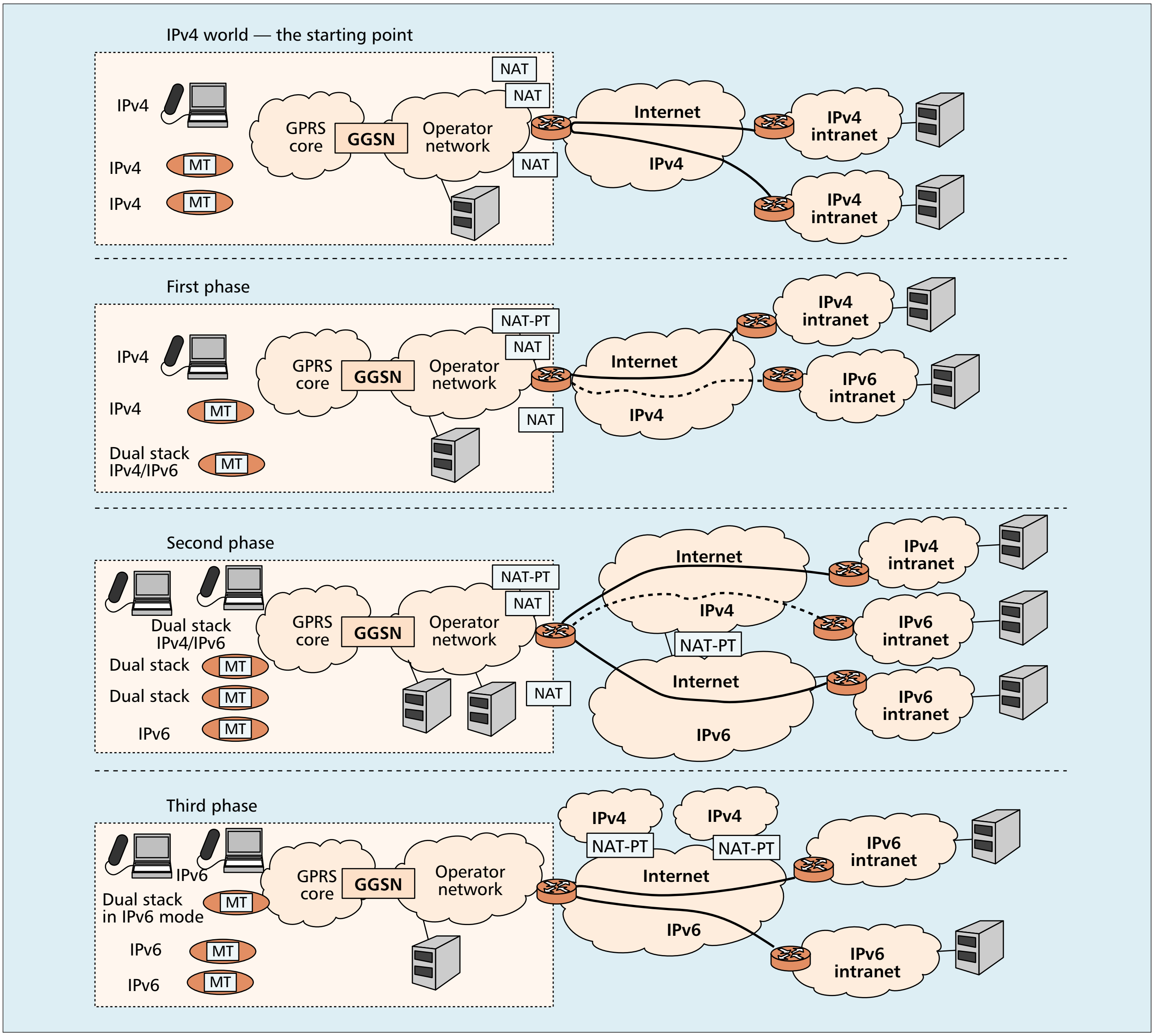


Figure 1. *IPv4 to IPv6 transition phases.*

example of such a tunneling mechanism is so-called 6to4 tunneling [4].

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. Network Address Translator/Protocol Translator (NAT-PT) [8] is an example of such a mechanism.

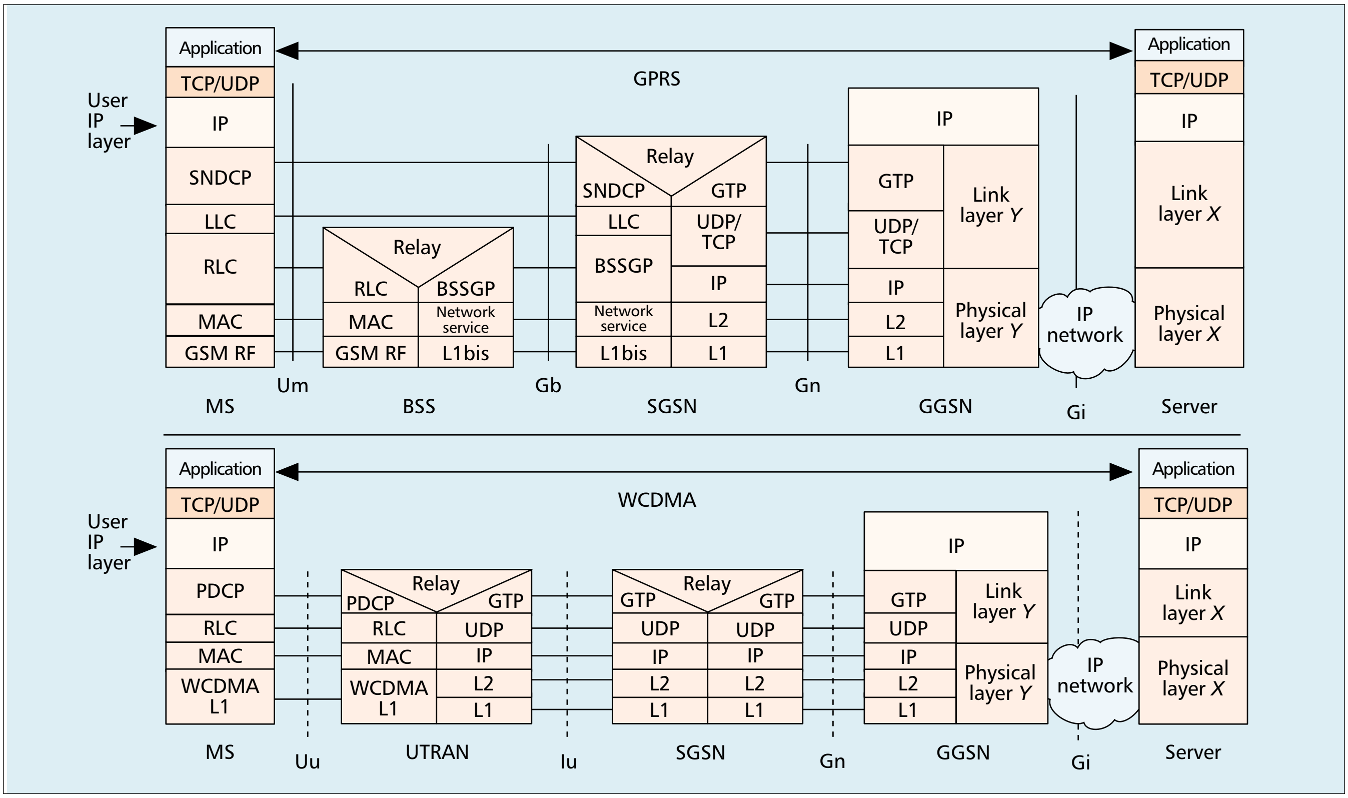
With these types of address/protocol translators, IP packet header conversion brings the problem of breaking end-to-end services (e.g., end-to-end IPsec) and also brings a new potential single point of failure in the network. Using address/protocol translators in the network depends mostly on operator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

There are also other translation mechanisms, but only NAT-PT is considered here.

A good goal is to do the major part of the transition work within the network; for example, IPv6 in IPv4 tunneling performed in the network saves the limited resources of the mobile terminal. Cases where it is vital to perform IPv6 in IPv4 tunneling in the mobile terminal itself have not been identified.

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.



■ **Figure 2.** *Protocol layers in GPRS and WCDMA networks.*

The starting position (the IPv4 world) is the GPRS/WCDMA network supporting only IPv4. All terminals/laptop computers connected to the Internet are native IPv4 equipment. Network Address Translators (NATs) [9] are used due the 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 tunneling. Most IPv6 services provided to mobile users in this phase are in the operator network (intranet). Other IPv6 services, such as a connection to an IPv6 corporate access network, are reachable by configured/automatic tunnels over the IPv4 Internet: conventional IPv4 services are provided to mobile users having IPv4 or dual stack terminals.

In the second phase, IPv6 is widely deployed and numerous services are implemented on the IPv6 platform. IPv6 Internet has wide deployment, but tunneling via IPv4 Internet is sometimes still needed since 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.

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 mobile networks. This enables simplification of the network architecture and leads to easier maintenance.

Transition Scenarios

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

The Scope: User IP Layer

This section outlines the user IP layer (application layer) and the use of IPv6 within it. The backbone/transport IP layer below the GTP tunnel, although also important in the near future, is not considered in this article. Figure 2 shows the protocol stacks for the GPRS and WCDMA cases (3GPP Release 99). Clarifying all protocol stacks and their functions is beyond the scope of this article; more information can be found, for example, from 3GPP technical specification 3G TS 23.060 (GPRS Service Description) [10].

The Network Model

Mobile Terminal Connection to the Network — The simplified Fig. 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 Packet Data Protocol (PDP) 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 tunneled through an IPv4 network to an external IPv6 host.

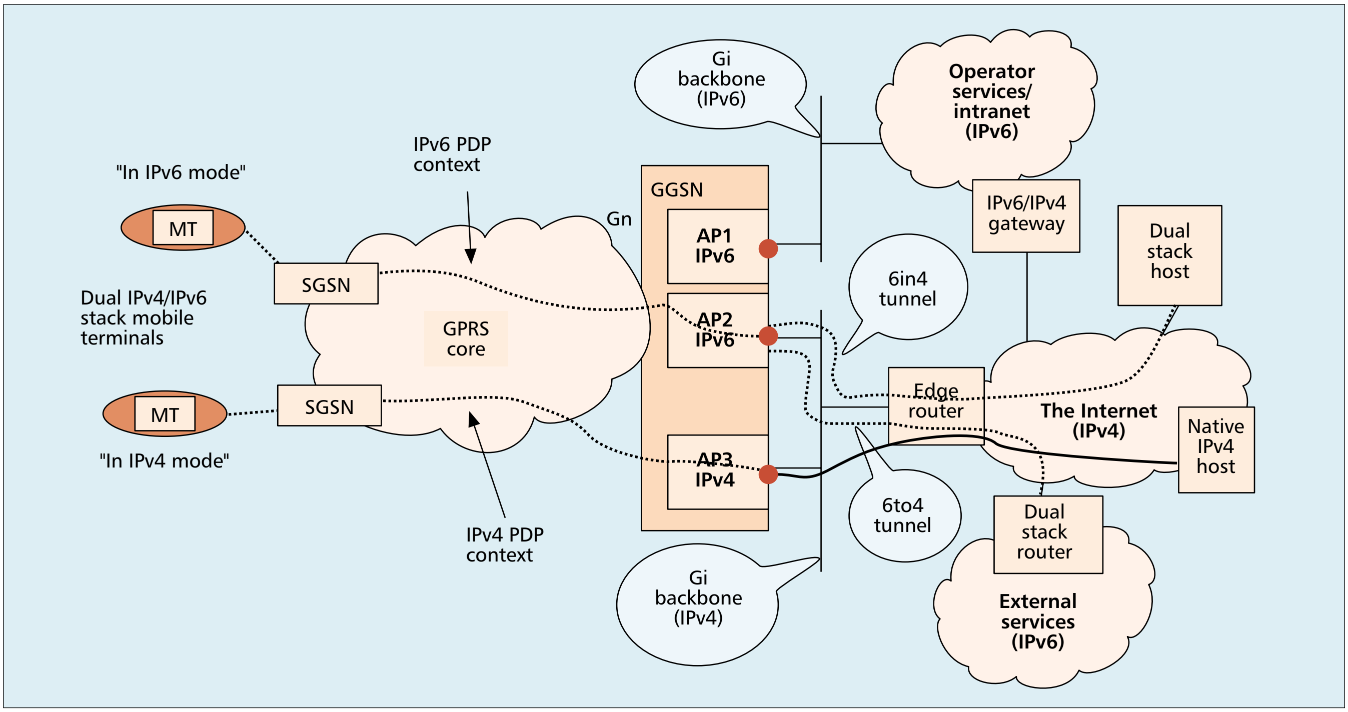


Figure 3. *Connections to GGSN IPv4 and IPv6 access points.*

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.

The Reference Network — The reference network model used in analyzing the transition scenarios 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. When going outside the operator network, traffic goes through the edge router and 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. The MT is very often allocated a private IPv4 address, and mechanisms to make mappings between private and public IPv4 addresses are needed; NAT is an example of such a mechanism.

An IPv4 host in an IPv4 intranet is reached via IPv4 Internet. An IPv6 host in an IPv6 intranet can be reached via IPv4 Internet or directly via IPv6 Internet. Tunneling is needed when connecting to an IPv6 host via an IPv4 network tunneling. The tunnel start point can be GGSN, edge router, or MT; the tunnel endpoint can be the host itself or a router at the edge of the IPv6 network. If the tunnel ends before the host, decapsulation is done in that router.

Different Combinations

When thinking about the mobile network and an MT's IP connection to different hosts, several combinations are possible. Basically, the IP versions of the MT and peer host (which is communicating with the MT) 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 MTs 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 analyzed in this article.

Three different types of network services can be identified:

- Traditional IPv4 services are received via an 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 tunneling over IPv4 Internet/protocol translation is needed.
- IPv6 services over IPv4 network — Communicating IPv6 nodes/networks are connected via IPv4 Internet by tunneling. The use of protocol translation is also possible.

The three types of MTs 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 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 termi-

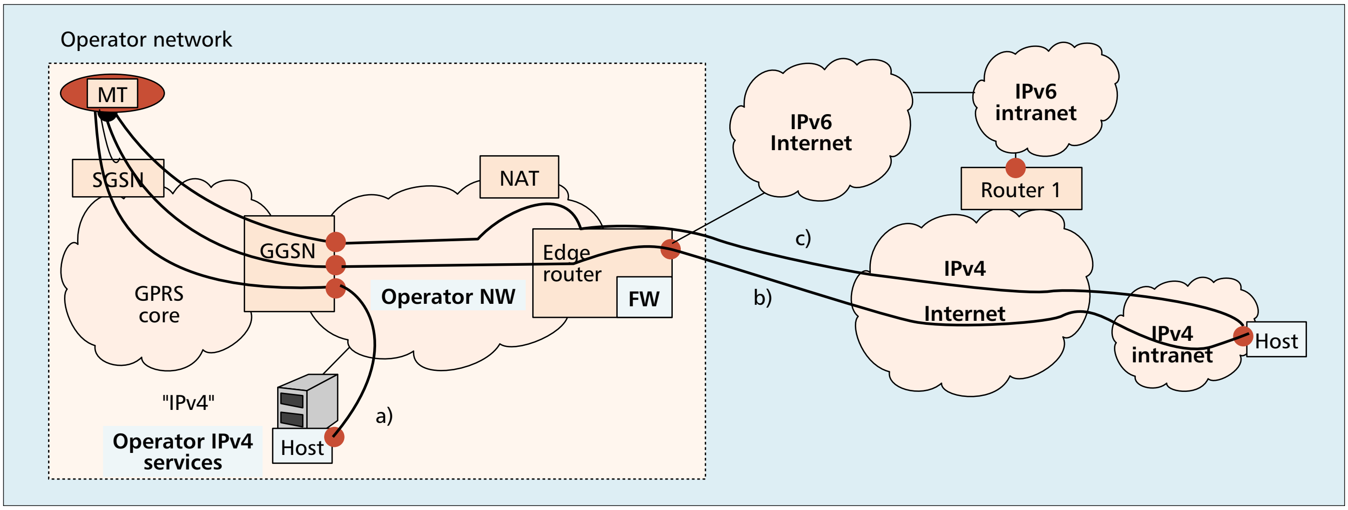


Figure 4. *Different IPv4 host connections for an IPv4 terminal.*

nals: IPv4 services are provided to native IPv4 terminals. In many cases there aren't a sufficient number of public IPv4 addresses for the MTs, and in many cases private IPv4 addresses are allocated. If an MT with a private IPv4 address is connected to a host over public IPv4 Internet, a NAT is needed in the network.

Figure 4 describes three situations. In case a, the MT is connected to a host in the intranet. In this case, private IPv4 addressing is sufficient. In case b, the MT is connected to a host in the public Internet. The MT is allocated a public IPv4 address from the operator address space, and the connection works by global IPv4 routing. Due to a limited pool of public IPv4 addresses, case b will only rarely occur. In case c, the MT has a private IPv4 address, so the NAT function is needed.

Dual Stack Terminal — In Fig. 5, a PDP context is opened between the mobile terminal and the GGSN (the AP 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 that needs a public IPv4 address.

IPv6 packets from the MT 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 an IPv6 network, 6to4 tunneling is not needed; otherwise, the automatic 6to4 tunneling is done between the edge router and router 1.

When the dual stack mobile terminal is connected to a native IPv4 host (e.g., a mail server in the IPv4 corporate access network), it is working in IPv4 mode. The MT is allocated a private IPv4 address due to lack of public IPv4 addresses. The NAT functionality is needed, and communication with the peer host over the public IPv4 Internet is possible.

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 MT and a native IPv4

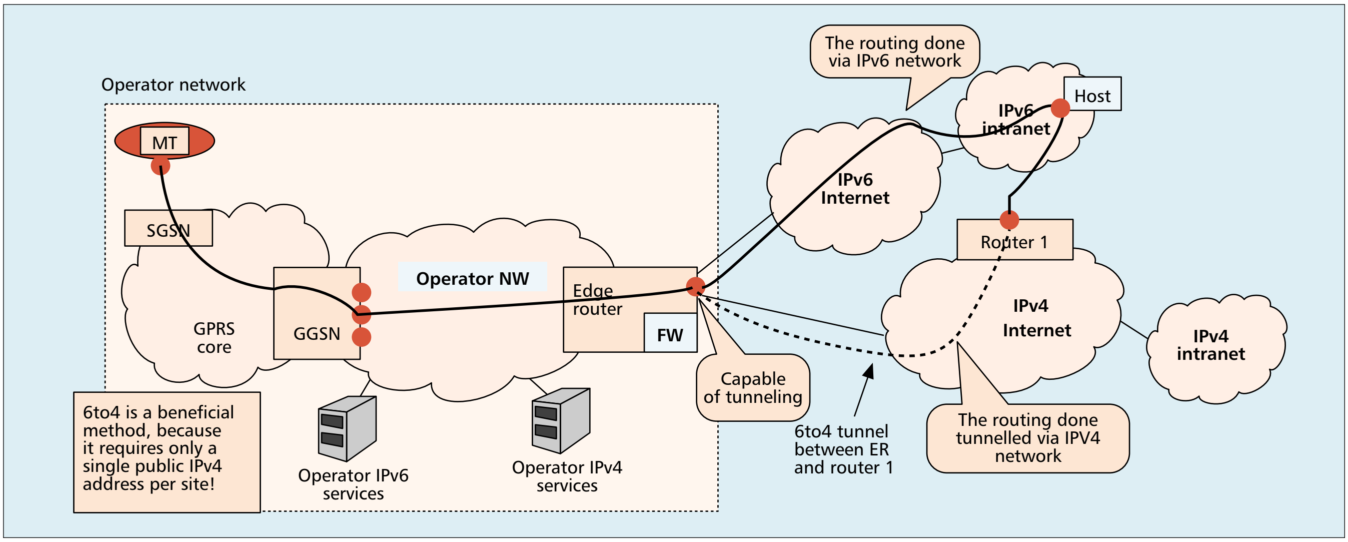

The routing done via IPv6 network
Operator network
MT
SGSN
GPRS core
GGSN
Operator NW
Edge router
FW
IPv6 Internet
IPv6 intranet
Host
Router 1
IPv4 Internet
IPv4 intranet
6to4 is a beneficial method, because it requires only a single public IPv4 address per site!
Operator IPv6 services
Operator IPv4 services
Capable of tunneling
6to4 tunnel between ER and router 1
The routing done tunnelled via IPV4 network

Figure 5. *Connection to IPv6 host via IPv4 Internet or IPv6 Internet.*

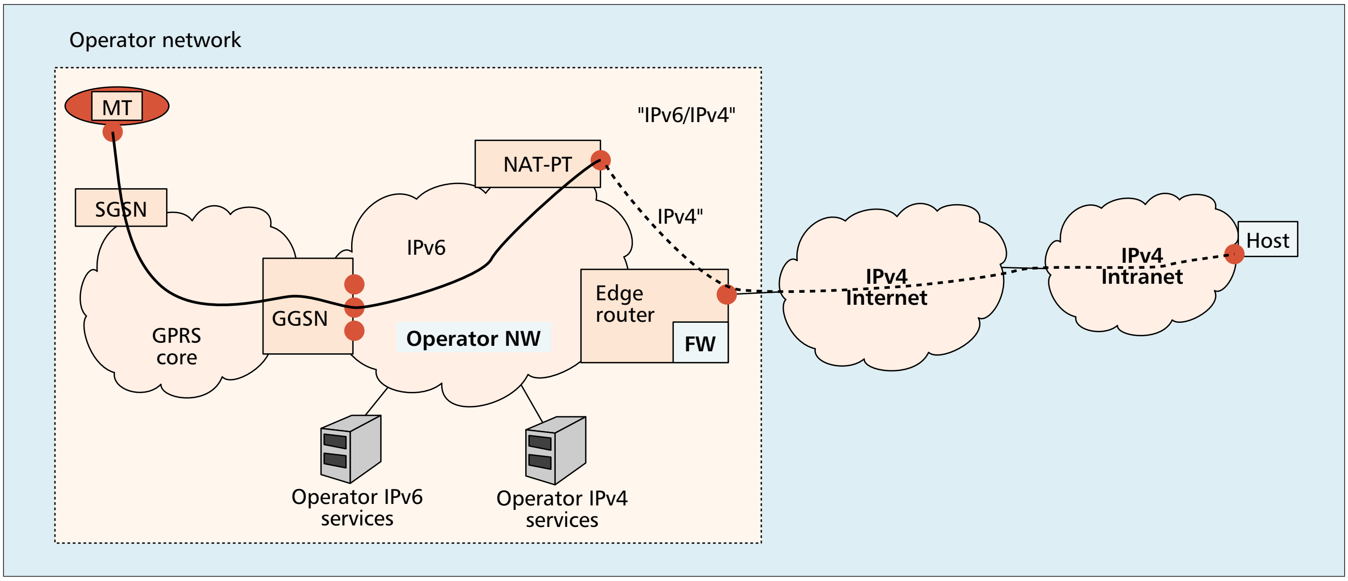


Figure 6. *A native IPv6 mobile terminal connection to a native IPv4 host using a translator.*

host (also IPv4 intranet access) always requires a translator such as NAT-PT in the network.

In Fig. 6, 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 with global IPv4 and IPv6 addresses. A dual stack terminal would work better in this scenario — for 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 very beneficial include mobile-terminated voice over IP (VoIP) Wireless Application Protocol (WAP) 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

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 important, 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.

The principal transition solution can be built using dual IPv4/IPv6 stacks (in mobile terminals, GGSN elements, and also the edge router in the operator network) and automatic tunneling. 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. It is recommended that the majority of the transition mechanisms be provided by the network; the goal is to keep the mobile terminal functionality as light as possible.

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.

References

[1] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," IETF RFC 2460, Dec. 1998.
[2] R. Gilligan and E. Nordmark, "Transition Mechanisms for IPv6 Hosts and Routers," IETF RFC 2893, Aug. 2000.
[3] R. Hinden and S. Deering, "IP Version 6 Addressing Architecture," IETF RFC 2373, July 1998.
[4] B. Carpenter and K. Moore, "Connection of IPv6 Domains via IPv4 Clouds," IETF RFC 3056, Feb. 2001.
[5] S. Kent and R. Atkinson, "IP Authentication Header," RFC 2402, Nov. 1998.
[6] S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)," RFC 2406, Nov. 1998.
[7] D. Johnson and C. Perkins, "Mobility Support in IPv6," IETF draft, draft-ietf-mobileip-ipv6-15.txt, July 2001, work in progress.
[8] G. Tsirtsis and P. Srisuresh, "Network Address Translation – Protocol Translation (NAT-PT)," RFC 2766, Feb. 2000.
[9] P. Srisuresh and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations," RFC 2663, Aug. 1999.
[10] 3GPP 3G TS 23.060, "Technical Specification Group Services and System Aspects, General Packet Radio Service (GPRS), Service Description, Stage 2," Rel. 1999, v. 3.8.0, June 2001.

Biography

Juha Wiljakka (juha.wiljakka@nokia.com) has worked for Nokia Mobile Phones, Tampere, Finland, since early 2000. His tasks include expertise on IPv6 features in mobile terminals. He joined Nokia in 1995, and has also worked with SDH and WDM technologies, transport network architecture, network planning, and techno-economic modeling. He received an M.Sc. degree from Helsinki University of Technology, Finland, in 1996. He majored in systems analysis (applied mathematics). He participates actively in IETF standardization.