Network Working Group
Request for Comments: 4215
Category: Informational

J. Wiljakka, Ed.
Nokia

October 2005

Analysis on IPv6 Transition in Third Generation Partnership Project (3GPP) Networks

Status of This Memo

Copyright Notice

Abstract

This document analyzes the transition to IPv6 in Third Generation Partnership Project (3GPP) packet networks. These networks are based on General Packet Radio Service (GPRS) technology, and the radio network architecture is based on Global System for Mobile Communications (GSM) or Universal Mobile Telecommunications System (UMTS)/Wideband Code Division Multiple Access (WCDMA) technology.

The focus is on analyzing different transition scenarios and applicable transition mechanisms and finding solutions for those transition scenarios. In these scenarios, the User Equipment (UE) connects to other nodes, e.g., in the Internet, and IPv6/IPv4 transition mechanisms are needed.

Table of Contents

1. Introduction

This document describes and analyzes the process of transition to IPv6 in Third Generation Partnership Project (3GPP) General Packet Radio Service (GPRS) packet networks [3GPP-23.060], in which the radio network architecture is based on Global System for Mobile Communications (GSM) or Universal Mobile Telecommunications System (UMTS)/Wideband Code Division Multiple Access (WCDMA) technology.

This document analyzes the transition scenarios that may come up in the deployment phase of IPv6 in 3GPP packet data networks.

The 3GPP network architecture is described in [RFC3314], and relevant transition scenarios are documented in [RFC3574]. The reader of this specification should be familiar with the material presented in these documents.

The scenarios analyzed in this document are divided into two categories: general-purpose packet service scenarios, referred to as GPRS scenarios in this document, and IP Multimedia Subsystem (IMS) scenarios, which include Session Initiation Protocol (SIP) considerations. For more information about IMS, see [3GPP-23.228], [3GPP-24.228], and [3GPP-24.229].

GPRS scenarios are the following:

- Dual Stack User Equipment (UE) connecting to IPv4 and IPv6 nodes
- IPv6 UE connecting to an IPv6 node through an IPv4 network
- IPv4 UE connecting to an IPv4 node through an IPv6 network
- IPv6 UE connecting to an IPv4 node

- IPv4 UE connecting to an IPv6 node

IMS scenarios are the following:

- UE connecting to a node in an IPv4 network through IMS
- Two IPv6 IMS connected via an IPv4 network

The focus is on analyzing different transition scenarios and applicable transition mechanisms and finding solutions for those transition scenarios. In the scenarios, the User Equipment (UE) connects to nodes in other networks, e.g., in the Internet, and IPv6/IPv4 transition mechanisms are needed.

1.1. Scope of This Document

The scope of this document is to analyze the possible transition scenarios in the 3GPP-defined GPRS network in which a UE connects to, or is contacted from, another node on the Internet. This document covers scenarios with and without the use of the SIP-based IP Multimedia Core Network Subsystem (IMS). This document does not focus on radio-interface-specific issues; both 3GPP Second and Third Generation radio network architectures (GSM, Enhanced Data rates for GSM Evolution (EDGE) and UMTS/WCDMA) will be covered by this analysis.

The 3GPP2 architecture is similar to 3GPP in many ways, but differs in enough details that this document does not include these variations in its analysis.

The transition mechanisms specified by the IETF Ngtrans and v6ops Working Groups shall be used. This memo shall not specify any new transition mechanisms, but only documents the need for new ones (if appropriate).

1.2. Abbreviations

2G	Second Generation Mobile Telecommunications, e.g., GSM and GPRS technologies
3G	Third Generation Mobile Telecommunications, e.g., UMTS technology
3GPP	Third Generation Partnership Project
ALG	Application Level Gateway
APN	Access Point Name. The APN is a logical name referring to a GGSN and an external network.

B2BUA	Back-to-Back User Agent
CSCF	Call Session Control Function (in 3GPP Release 5 IMS)
DNS	Domain Name System
EDGE	Enhanced Data rates for GSM Evolution
GGSN	Gateway GPRS Support Node (default router for 3GPP User Equipment)
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HLR	Home Location Register
IMS	IP Multimedia (Core Network) Subsystem, 3GPP Release 5 IPv6-only part of the network
ISP	Internet Service Provider
NAT	Network Address Translation
NAPT-PT	Network Address Port Translation - Protocol Translation
NAT-PT	Network Address Translation - Protocol Translation
PCO-IE	Protocol Configuration Options Information Element
PDP	Packet Data Protocol
PPP	Point-to-Point Protocol
SDP	Session Description Protocol
SGSN	Serving GPRS Support Node
SIIT	Stateless IP/ICMP Translation Algorithm
SIP	Session Initiation Protocol
UE	User Equipment, e.g., a UMTS mobile handset
UMTS	Universal Mobile Telecommunications System
WCDMA	Wideband Code Division Multiple Access

1.3. Terminology

Some terms used in 3GPP transition scenarios and analysis documents are briefly defined here.

Dual Stack UE	Dual Stack UE is a 3GPP mobile handset having both IPv4 and IPv6 stacks. It is capable of activating both IPv4 and IPv6 Packet Data Protocol (PDP) contexts. Dual stack UE may be capable of tunneling.
IPv6 UE	IPv6 UE is an IPv6-only 3GPP mobile handset. It is only capable of activating IPv6 PDP contexts.
IPv4 UE	IPv4 UE is an IPv4-only 3GPP mobile handset. It is only capable of activating IPv4 PDP contexts.
IPv4 node	IPv4 node is here defined to be the IPv4-capable node the UE is communicating with. The IPv4 node can be, e.g., an application server or another UE.
IPv6 node	IPv6 node is here defined to be the IPv6-capable node the UE is communicating with. The IPv6 node can be, e.g., an application server or another UE.
PDP Context	Packet Data Protocol (PDP) Context is a connection between the UE and the GGSN, over which the packets are transferred. There are currently three PDP types: IPv4, IPv6, and PPP.

2. Transition Mechanisms and DNS Guidelines

This section briefly introduces these IETF IPv4/IPv6 transition mechanisms:

- dual IPv4/IPv6 stack [RFC4213]
- tunneling [RFC4213]
- protocol translators [RFC2766], [RFC2765]

In addition, DNS recommendations are given. The applicability of different transition mechanisms to 3GPP networks is discussed in sections 3 and 4.

2.1. Dual Stack

The dual IPv4/IPv6 stack is specified in [RFC4213]. If we consider the 3GPP GPRS core network, dual stack implementation in the Gateway GPRS Support Node (GGSN) enables support for IPv4 and IPv6 PDP contexts. UEs with dual stack and public (global) IP addresses can

typically access both IPv4 and IPv6 services without additional translators in the network. However, it is good to remember that private IPv4 addresses and NATs [RFC2663] have been used and will be used in mobile networks. Public/global IP addresses are also needed for peer-to-peer services: the node needs a public/global IP address that is visible to other nodes.

2.2. Tunneling

Tunneling is a transition mechanism that requires dual IPv4/IPv6 stack functionality in the encapsulating and decapsulating nodes. Basic tunneling alternatives are IPv6-in-IPv4 and IPv4-in-IPv6.

Tunneling can be static or dynamic. Static (configured) tunnels are fixed IPv6 links over IPv4, and they are specified in [RFC4213]. Dynamic (automatic) tunnels are virtual IPv6 links over IPv4 where the tunnel endpoints are not configured, i.e., the links are created dynamically.

2.3. Protocol Translators

A translator can be defined as an intermediate component between a native IPv4 node and a native IPv6 node to enable direct communication between them without requiring any modifications to the end nodes.

Header conversion is a translation mechanism. In header conversion, IPv6 packet headers are converted to IPv4 packet headers, or vice versa, and checksums are adjusted or recalculated if necessary. NAT-PT (Network Address Translation/Protocol Translation) [RFC2766] using Stateless IP/ICMP Translation [RFC2765] is an example of such a mechanism.

Translators may be needed in some cases when the communicating nodes do not share the same IP version; in others, it may be possible to avoid such communication altogether. Translation can take place at the network layer (using NAT-like techniques), the transport layer (using a TCP/UDP proxy), or the application layer (using application relays).

2.4. DNS Guidelines for IPv4/IPv6 Transition

To avoid the DNS name space from fragmenting into parts where some parts of DNS are visible only using IPv4 (or IPv6) transport, the recommendation (as of this writing) is to always keep at least one authoritative server IPv4-enabled, and to ensure that recursive DNS servers support IPv4. See DNS IPv6 transport guidelines [RFC3901] for more information.

3. GPRS Transition Scenarios

This section discusses the scenarios that might occur when a GPRS UE contacts services or other nodes, e.g., a web server in the Internet.

The following scenarios described by [RFC3574] are analyzed here. In all of the scenarios, the UE is part of a network where there is at least one router of the same IP version, i.e., the GGSN, and the UE is connecting to a node in a different network.

1) Dual Stack UE connecting to IPv4 and IPv6 nodes

2) IPv6 UE connecting to an IPv6 node through an IPv4 network

3) IPv4 UE connecting to an IPv4 node through an IPv6 network

4) IPv6 UE connecting to an IPv4 node

5) IPv4 UE connecting to an IPv6 node

3.1. Dual Stack UE Connecting to IPv4 and IPv6 Nodes

In this scenario, the dual stack UE is capable of communicating with both IPv4 and IPv6 nodes.

It is recommended to activate an IPv6 PDP context when communicating with an IPv6 peer node and an IPv4 PDP context when communicating with an IPv4 peer node. If the 3GPP network supports both IPv4 and IPv6 PDP contexts, the UE activates the appropriate PDP context depending on the type of application it has started or depending on the address of the peer host it needs to communicate with. The authors leave the PDP context activation policy to be decided by UE implementers, application developers, and operators. One discussed possibility is to activate both IPv4 and IPv6 types of PDP contexts in advance, because activation of a PDP context usually takes some time. However, that probably is not good usage of network resources. Generally speaking, IPv6 PDP contexts should be preferred even if that meant IPv6-in-IPv4 tunneling would be needed in the network (see Section 3.2 for more details). Note that this is transparent to the UE.

Although the UE is dual stack, the UE may find itself attached to a 3GPP network in which the Serving GPRS Support Node (SGSN), the GGSN, and the Home Location Register (HLR) support IPv4 PDP contexts, but do not support IPv6 PDP contexts. This may happen in early phases of IPv6 deployment, or because the UE has "roamed" from a 3GPP network that supports IPv6 to one that does not. If the 3GPP network does not support IPv6 PDP contexts, and an application on the UE needs to

communicate with an IPv6(-only) node, the UE may activate an IPv4 PDP context and encapsulate IPv6 packets in IPv4 packets using a tunneling mechanism.

The tunneling mechanism may require public IPv4 addresses, but there are tunneling mechanisms and deployment scenarios in which private IPv4 addresses may be used, for instance, if the tunnel endpoints are in the same private domain, or the tunneling mechanism works through IPv4 NAT.

One deployment scenario uses a laptop computer and a 3GPP UE as a modem. IPv6 packets are encapsulated in IPv4 packets in the laptop computer and an IPv4 PDP context is activated. The tunneling mechanism depends on the laptop computer's support of tunneling mechanisms. Another deployment scenario is performing IPv6-in-IPv4 tunneling in the UE itself and activating an IPv4 PDP context.

Closer details for an applicable tunneling mechanism are not analyzed in this document. However, a simple host-to-router (automatic) tunneling mechanism can be a good fit. There is not yet consensus on the right approach, and proposed mechanisms so far include [ISATAP] and [STEP]. Especially ISATAP has had some support in the working group. Goals for 3GPP zero-configuration tunneling are documented in [zeroconf].

This document strongly recommends that the 3GPP operators deploy basic IPv6 support in their GPRS networks. That makes it possible to lessen the transition effects in the UEs.

As a general guideline, IPv6 communication is preferred to IPv4 communication going through IPv4 NATs to the same dual stack peer node.

Public IPv4 addresses are often a scarce resource for the operator, and usually it is not possible for a UE to have a public IPv4 address (continuously) allocated for its use. Use of private IPv4 addresses means use of NATs when communicating with a peer node outside the operator's network. In large networks, NAT systems can become very complex, expensive, and difficult to maintain.

3.2. IPv6 UE Connecting to an IPv6 Node through an IPv4 Network

The best solution for this scenario is obtained with tunneling; i.e., IPv6-in-IPv4 tunneling is a requirement. An IPv6 PDP context is activated between the UE and the GGSN. Tunneling is handled in the network, because IPv6 UE does not have the dual stack functionality needed for tunneling. The encapsulating node can be the GGSN, the edge router between the border of the operator's IPv6 network and the

public Internet, or any other dual stack node within the operator's IP network. The encapsulation (uplink) and decapsulation (downlink) can be handled by the same network element. Typically, the tunneling handled by the network elements is transparent to the UEs and IP traffic looks like native IPv6 traffic to them. For the applications and transport protocols, tunneling enables end-to-end IPv6 connectivity.

IPv6-in-IPv4 tunnels between IPv6 islands can be either static or dynamic. The selection of the type of tunneling mechanism is a policy decision for the operator/ISP deployment scenario, and only generic recommendations can be given in this document.

The following subsections are focused on the usage of different tunneling mechanisms when the peer node is in the operator's network or outside the operator's network. The authors note that where the actual 3GPP network ends and which parts of the network belong to the ISP(s) also depend on the deployment scenario. The authors are not commenting on how many ISP functions the 3GPP operator should perform. However, many 3GPP operators are ISPs of some sort themselves. ISP networks' transition to IPv6 is analyzed in [RFC4029].

3.2.1. Tunneling Inside the 3GPP Operator's Network

GPRS operators today have typically deployed IPv4 backbone networks. IPv6 backbones can be considered quite rare in the first phases of the transition.

In initial IPv6 deployment, where a small number of IPv6-in-IPv4 tunnels are required to connect the IPv6 islands over the 3GPP operator's IPv4 network, manually configured tunnels can be used. In a 3GPP network, one IPv6 island can contain the GGSN while another island can contain the operator's IPv6 application servers. However, manually configured tunnels can be an administrative burden when the number of islands and therefore tunnels rises. In that case, upgrading parts of the backbone to dual stack may be the simplest choice. The administrative burden could also be mitigated by using automated management tools.

Connection redundancy should also be noted as an important requirement in 3GPP networks. Static tunnels alone do not provide a routing recovery solution for all scenarios where an IPv6 route goes down. However, they can provide an adequate solution depending on the design of the network and the presence of other router redundancy mechanisms, such as the use of IPv6 routing protocols.

3.2.2. Tunneling Outside the 3GPP Operator's Network

This subsection includes the case in which the peer node is outside the operator's network. In that case, IPv6-in-IPv4 tunneling can be necessary to obtain IPv6 connectivity and reach other IPv6 nodes. In general, configured tunneling can be recommended.

Tunnel starting point can be in the operator's network depending on how far the 3GPP operator has come in implementing IPv6. If the 3GPP operator has not deployed IPv6 in its backbone, the encapsulating node can be the GGSN. If the 3GPP operator has deployed IPv6 in its backbone but the upstream ISP does not provide IPv6 connectivity, the encapsulating node could be the 3GPP operator's border router.

The case is pretty straightforward if the upstream ISP provides IPv6 connectivity to the Internet and the operator's backbone network supports IPv6. Then the 3GPP operator does not have to configure any tunnels, since the upstream ISP will take care of routing IPv6 packets. If the upstream ISP does not provide IPv6 connectivity, an IPv6-in-IPv4 tunnel should be configured, e.g., from the border router to a dual stack border gateway operated by another ISP that is offering IPv6 connectivity.

3.3. IPv4 UE Connecting to an IPv4 Node through an IPv6 Network

3GPP networks are expected to support both IPv4 and IPv6 for a long time, on the UE-GGSN link and between the GGSN and external networks. For this scenario, it is useful to split the end-to-end IPv4 UE to IPv4 node communication into UE-to-GGSN and GGSN-to-v4NODE. This allows an IPv4-only UE to use an IPv4 link (an IPv4 PDP context) to connect to the GGSN without communicating over an IPv6 network.

Regarding the GGSN-to-v4NODE communication, typically the transport network between the GGSN and external networks will support only IPv4 in the early stages and migrate to dual stack, since these networks are already deployed. Therefore, it is not envisaged that tunneling of IPv4-in-IPv6 will be required from the GGSN to external IPv4 networks either. In the longer run, 3GPP operators may choose to phase out IPv4 UEs and the IPv4 transport network. This would leave only IPv6 UEs.

Therefore, overall, the transition scenario involving an IPv4 UE communicating with an IPv4 peer through an IPv6 network is not considered very likely in 3GPP networks.

3.4. IPv6 UE Connecting to an IPv4 Node

Generally speaking, IPv6-only UEs may be easier to manage, but that would require all services to be used over IPv6, and the universal deployment of IPv6 probably is not realistic in the near future. Dual stack implementation requires management of both IPv4 and IPv6 networks, and one approach is that "legacy" applications keep using IPv4 for the foreseeable future and new applications requiring end-to-end connectivity (for example, peer-to-peer services) use IPv6. As a general guideline, IPv6-only UEs are not recommended in the early phases of transition until the IPv6 deployment has become so prevalent that direct communication with IPv4(-only) nodes will be the exception and not the rule. It is assumed that IPv4 will remain useful for quite a long time, so in general, dual stack implementation in the UE can be recommended. This recommendation naturally includes manufacturing dual stack UEs instead of IPv4-only UEs.

However, if there is a need to connect to an IPv4(-only) node from an IPv6-only UE, it is recommended to use specific translation and proxying techniques; generic IP protocol translation is not recommended. There are three main ways for IPv6(-only) nodes to communicate with IPv4(-only) nodes (excluding avoiding such communication in the first place):

1. the use of generic-purpose translator (e.g., NAT-PT [RFC2766]) in the local network (not recommended as a general solution),

2. the use of specific-purpose protocol relays (e.g., IPv6<->IPv4 TCP relay configured for a couple of ports only [RFC3142]) or application proxies (e.g., HTTP proxy, SMTP relay) in the local network, or

3. the use of specific-purpose mechanisms (as described above in 2) in the foreign network; these are indistinguishable from the IPv6-enabled services from the IPv6 UE’s perspective and are not discussed further here.

For many applications, application proxies can be appropriate (e.g., HTTP proxies, SMTP relays, etc.) Such application proxies will not be transparent to the UE. Hence, a flexible mechanism with minimal manual intervention should be used to configure these proxies on IPv6 UEs. Application proxies can be placed, for example, on the GGSN external interface ("Gi"), or inside the service network.

The authors note that [NATPTappl] discusses the applicability of NAT-PT, and [NATPTexp] discusses general issues with all forms of IPv6-IPv4 translation. The problems related to NAT-PT usage in 3GPP networks are documented in Appendix A.

3.5. IPv4 UE Connecting to an IPv6 Node

The legacy IPv4 nodes are typically nodes that support the applications that are popular today in the IPv4 Internet: mostly e-mail and web browsing. These applications will, of course, be supported in the future IPv6 Internet. However, the legacy IPv4 UEs are not going to be updated to support future applications. As these applications are designed for IPv6, and to use the advantages of newer platforms, the legacy IPv4 nodes will not be able to take advantage of them. Thus, they will continue to support legacy services.

Taking the above into account, the traffic to and from the legacy IPv4 UE is restricted to a few applications. These applications already mostly rely on proxies or local servers to communicate between private address space networks and the Internet. The same methods and technology can be used for IPv4-to-IPv6 transition.

4. IMS Transition Scenarios

As IMS is exclusively IPv6, the number of possible transition scenarios is reduced dramatically. The possible IMS scenarios are listed below and analyzed in Sections 4.1 and 4.2.

1) UE connecting to a node in an IPv4 network through IMS
2) Two IPv6 IMS connected via an IPv4 network

For DNS recommendations, we refer to Section 2.4. As DNS traffic is not directly related to the IMS functionality, the recommendations are not in contradiction with the IPv6-only nature of the IMS.

4.1. UE Connecting to a Node in an IPv4 Network through IMS

This scenario occurs when an (IPv6) IMS UE connects to a node in the IPv4 Internet through the IMS, or vice versa. This happens when the other node is a part of a different system than 3GPP, e.g., a fixed PC, with only IPv4 capabilities.

Over time, users will upgrade the legacy IPv4 nodes to dual-stack, often by replacing the entire node, eliminating this particular problem in that specific deployment.

Still, it is difficult to estimate how many non-upgradable legacy IPv4 nodes need to communicate with the IMS UEs. It is assumed that the solution described here is used for limited cases, in which communications with a small number of legacy IPv4 SIP equipment are needed.

As the IMS is exclusively IPv6 [3GPP-23.221], for many of the applications in the IMS, some kind of translators may need to be used in the communication between the IPv6 IMS and the legacy IPv4 hosts in cases where these legacy IPv4 hosts cannot be upgraded to support IPv6.

This section gives a brief analysis of the IMS interworking issues and presents a high-level view of SIP within the IMS. The authors recommend that a detailed solution for the general SIP/SDP/media IPv4/IPv6 transition problem will be specified as soon as possible as a task within the SIP-related Working Groups in the IETF.

The issue of the IPv4/IPv6 interworking in SIP is somewhat more challenging than many other protocols. The control (or signaling) and user (or data) traffic are separated in SIP calls, and thus, the IMS, the transition of IMS traffic from IPv6 to IPv4, must be handled at two levels:

1. Session Initiation Protocol (SIP) [RFC3261], and Session Description Protocol (SDP) [RFC2327] [RFC3266] (Mm-interface)

2. the user data traffic (Mb-interface)

In addition, SIP carries an SDP body containing the addressing and other parameters for establishing the user data traffic (the media). Hence, the two levels of interworking cannot be made independently.

Figure 1 shows an example setup for IPv4 and IPv6 interworking in IMS. The "Interworking Unit" comprises two internal elements a dual stack SIP server and a transition gateway (TrGW) for the media traffic. These two elements are interconnected for synchronizing the interworking of the SIP signaling and the media traffic.

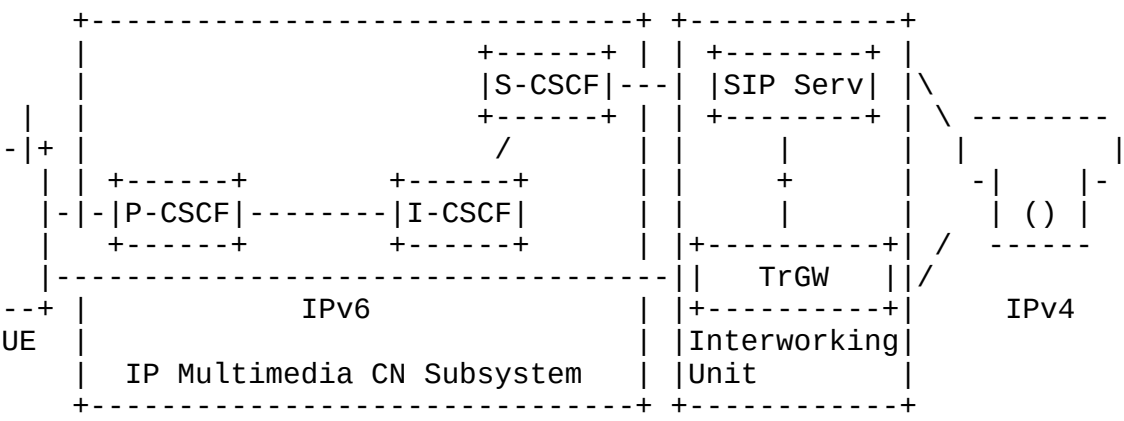

Figure 1: UE using IMS to contact a legacy phone

On reception of an INVITE, the SIP server reserves an IP address and a port from the TrGW both for IPv4 and IPv6. Then, the SIP server acts as a B2BUA (Back-to-Back User Agent) and rewrites the SDP of the INVITE to insert the transition gateway in the middle of the media flow between the two endpoints.

When performing its B2BUA role, the SIP server acts as a UA (User Agent) toward both the IMS and the IPv4 host. Consequently, the SIP server needs to support all the extensions that apply to the session, which are listed in the Require header fields of the SIP messages.

This approach has a number of important drawbacks, however. The biggest drawback is that the rewriting of the SDP in the SIP signaling prevents securing the SDP payload between the two endpoints. In addition, it breaks the end-to-end negotiation of SIP extensions required for each session. Therefore, the extensions to be used in a particular session are limited by the extensions supported by the SIP server acting as a B2BUA. That is, the introduction of a new extension requires upgrading not only the UAs but the B2BUAs as well.

This analysis clearly shows that a new solution for IPv4-IPv6 interworking in SIP networks is needed. The ability to convey multiple alternative addresses in SDP session descriptions [RFC4091] represents a step in this direction.

Given the problems related to the use of B2BUAs, it is recommended that the SIP-related Working Groups quickly work on a solution to overcome the drawbacks of this approach.

4.2. Two IPv6 IMS Connected via an IPv4 Network

At the early stages of IMS deployment, there may be cases where two IMS islands are separated by an IPv4 network such as the legacy Internet. Here both the UEs and the IMS islands are IPv6 only. However, the IPv6 islands are not connected natively with IPv6.

In this scenario, the end-to-end SIP connections are based on IPv6. The only issue is to make connection between two IPv6-only IMS islands over IPv4 network. This scenario is closely related to GPRS scenario represented in Section 3.2. and similar tunneling solutions are applicable also in this scenario.

5. About 3GPP UE IPv4/IPv6 Configuration

This informative section aims to give a brief overview of the configuration needed in the UE in order to access IP-based services. There can also be other application-specific settings in the UE that are not described here.

UE configuration is required in order to access IPv6- or IPv4-based services. The GGSN Access Point has to be defined when using, for example, the web-browsing application. One possibility is to use over-the-air configuration [OMA-CP] to configure the GPRS settings. The user can, for example, visit the operator WWW page and subscribe the GPRS Access Point settings to his/her UE and receive the settings via Short Message Service (SMS). After the user has accepted the settings and a PDP context has been activated, he/she can start browsing. The Access Point settings can also be typed in manually or be pre-configured by the operator or the UE manufacturer.

DNS server addresses typically also need to be configured in the UE. In the case of IPv4 type PDP context, the (IPv4) DNS server addresses can be received in the PDP context activation (a control plane mechanism). A similar mechanism is also available for IPv6: so-called Protocol Configuration Options Information Element (PCO-IE) specified by the 3GPP [3GPP-24.008]. It is also possible to use [RFC3736] (or [RFC3315]) and [RFC3646] for receiving DNS server addresses. Active IETF work on DNS discovery mechanisms is ongoing and might result in other mechanisms becoming available over time. The DNS server addresses can also be received over the air (using SMS) [OMA-CP] or typed in manually in the UE.

When accessing IMS services, the UE needs to know the Proxy-Call Session Control Function (P-CSCF) IPv6 address. Either a 3GPP-specific PCO-IE mechanism or a DHCPv6-based mechanism ([RFC3736] and [RFC3319]) can be used. Manual configuration or configuration over

the air is also possible. IMS subscriber authentication and registration to the IMS and SIP integrity protection are not discussed here.

6. Summary and Recommendations

This document has analyzed five GPRS and two IMS IPv6 transition scenarios. Numerous 3GPP networks are using private IPv4 addresses today, and introducing IPv6 is important. The two first GPRS scenarios and both IMS scenarios are seen as the most relevant. The authors summarize some main recommendations here:

- Dual stack UEs are recommended instead of IPv4-only or IPv6-only UEs. It is important to take care that applications in the UEs support IPv6. In other words, applications should be IP version independent. IPv6-only UEs can become feasible when IPv6 is widely deployed in the networks, and most services work on IPv6.

- It is recommended to activate an IPv6 PDP context when communicating with an IPv6 peer node and an IPv4 PDP context when communicating with an IPv4 peer node.

- IPv6 communication is preferred to IPv4 communication going through IPv4 NATs to the same dual stack peer node.

- This document strongly recommends that the 3GPP operators deploy basic IPv6 support in their GPRS networks as soon as possible. That makes it possible to lessen the transition effects in the UEs.

- A tunneling mechanism in the UE may be needed during the early phases of the IPv6 transition process. A lightweight, automatic tunneling mechanism should be standardized in the IETF. See [zeroconf] for more details.

- Tunneling mechanisms can be used in 3GPP networks, and only generic recommendations are given in this document. More details can be found, for example, in [RFC4029].

- The authors recommend that a detailed solution for the general SIP/SDP/media IPv4/IPv6 transition problem be specified as soon as possible as a task within the SIP-related Working Groups in the IETF.

7. Security Considerations

Deploying IPv6 has some generic security considerations one should be aware of [V6SEC]; however, these are not specific to 3GPP transition and are therefore out of the scope of this memo.

This memo recommends the use of a relatively small number of techniques. Each technique has its own security considerations, including:

- native upstream access or tunneling by the 3GPP network operator,
- use of routing protocols to ensure redundancy,
- use of locally deployed specific-purpose protocol relays and application proxies to reach IPv4(-only) nodes from IPv6-only UEs, or
- a specific mechanism for SIP signaling and media translation.

The threats of configured tunneling are described in [RFC4213]. Attacks against routing protocols are described in the respective documents and in general in [ROUTESEC]. Threats related to protocol relays have been described in [RFC3142]. The security properties of SIP internetworking are to be specified when the mechanism is specified.

In particular, this memo does not recommend the following technique, which has security issues, not further analyzed here:

- NAT-PT or other translator as a general-purpose transition mechanism

8. References

8.1. Normative References

[RFC2663] Srisuresh, P. and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, August 1999.

[RFC2765] Nordmark, E., "Stateless IP/ICMP Translation Algorithm (SIIT)", RFC 2765, February 2000.

[RFC2766] Tsirtsis, G. and P. Srisuresh, "Network Address Translation - Protocol Translation (NAT-PT)", RFC 2766, February 2000.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[RFC3574] Soininen, J., "Transition Scenarios for 3GPP Networks", RFC 3574, August 2003.

[RFC4213] Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", RFC 4213, October 2005.

[3GPP-23.060] 3GPP TS 23.060 V5.4.0, "General Packet Radio Service (GPRS); Service description; Stage 2 (Release 5)", December 2002.

[3GPP-23.221] 3GPP TS 23.221 V5.7.0, "Architectural requirements (Release 5)", December 2002.

[3GPP-23.228] 3GPP TS 23.228 V5.7.0, "IP Multimedia Subsystem (IMS); Stage 2 (Release 5)", December 2002.

[3GPP-24.228] 3GPP TS 24.228 V5.3.0, "Signalling flows for the IP multimedia call control based on SIP and SDP; Stage 3 (Release 5)", December 2002.

[3GPP-24.229] 3GPP TS 24.229 V5.3.0, "IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3 (Release 5)", December 2002.

8.2. Informative References

[RFC2327] Handley, M. and V. Jacobson, "SDP: Session Description Protocol", RFC 2327, April 1998.

[RFC3142] Hagino, J. and K. Yamamoto, "An IPv6-to-IPv4 Transport Relay Translator", RFC 3142, June 2001.

[RFC3266] Olson, S., Camarillo, G., and A. Roach, "Support for IPv6 in Session Description Protocol (SDP)", RFC 3266, June 2002.

[RFC3314] Wasserman, M., "Recommendations for IPv6 in Third Generation Partnership Project (3GPP) Standards", RFC 3314, September 2002.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC3319] Schulzrinne, H. and B. Volz, "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers", RFC 3319, July 2003.

[RFC3646] Droms, R., "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3646, December 2003.

[RFC3736] Droms, R., "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6", RFC 3736, April 2004.

[RFC3901] Durand, A. and J. Ihren, "DNS IPv6 Transport Operational Guidelines", BCP 91, RFC 3901, September 2004.

[RFC4029] Lind, M., Ksinant, V., Park, S., Baudot, A., and P. Savola, "Scenarios and Analysis for Introducing IPv6 into ISP Networks", RFC 4029, March 2005.

[RFC4091] Camarillo, G. and J. Rosenberg, "The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework", RFC 4091, June 2005.

[ISATAP] Templin, F., Gleeson, T., Talwar, M., and D. Thaler, "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)", RFC 4214, September 2005.

[NATPTappl] Satapati, S., Sivakumar, S., Barany, P., Okazaki, S. and H. Wang, "NAT-PT Applicability", Work in Progress, October 2003.

[NATPTexp] Aoun, C. and E. Davies, "Reasons to Move NAT-PT to Experimental", Work in Progress, July 2005.

[ROUTESEC] Barbir, A., Murphy, S., and Y. Yang, "Generic Threats to Routing Protocols", Work in Progress, April 2004.

[STEP] Savola, P.: "Simple IPv6-in-IPv4 Tunnel Establishment Procedure (STEP)", Work in Progress, January 2004.

[V6SEC] Savola, P.: "IPv6 Transition/Co-existence Security Considerations", Work in Progress, February 2004.

[zeroconf] Nielsen, K., Morelli, M., Palet, J., Soininen, J., and J. Wiljakka, "Goals for Zero-Configuration Tunneling in 3GPP", Work in Progress, October 2004.

[3GPP-24.008] 3GPP TS 24.008 V5.8.0, "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3 (Release 5)", June 2003.

[OMA-CP] OMA Client Provisioning: Provisioning Architecture Overview Version 1.1, OMA-WAP-ProvArch-v1_1-20021112-C, Open Mobile Alliance, 12-Nov-2002.

9. Contributors

Pekka Savola has contributed both text and his IPv6 experience to this document. He has provided a large number of helpful comments on the v6ops mailing list. Allison Mankin has contributed text for IMS Scenario 1 (Section 4.1).

10. Authors and Acknowledgements

This document was written by:

Alain Durand, Comcast
<alain_durand@cable.comcast.com>

Karim El-Malki, Ericsson Radio Systems
<Karim.El-Malki@era.ericsson.se>

Niall Richard Murphy, Enigma Consulting Limited
<niallm@enigma.ie>

Hugh Shieh, AT&T Wireless
<hugh.shieh@attws.com>

Jonne Soininen, Nokia
<jonne.soininen@nokia.com>

Hesham Soliman, Flarion
<h.soliman@flarion.com>

Margaret Wasserman, ThingMagic
<margaret@thingmagic.com>

Juha Wiljakka, Nokia
<juha.wiljakka@nokia.com>

The authors would like to give special thanks to Spencer Dawkins for proofreading.

The authors would like to thank Heikki Almay, Gabor Bajko, Gonzalo Camarillo, Ajay Jain, Jarkko Jouppi, David Kessens, Ivan Laloux, Allison Mankin, Jasminko Mulahusic, Janne Rinne, Andreas Schmid, Pedro Serna, Fred Templin, Anand Thakur, and Rod Van Meter for their valuable input.

Appendix A - On the Use of Generic Translators in the 3GPP Networks

This appendix lists mainly 3GPP-specific arguments about generic translators, even though the use of generic translators is discouraged.

Due to the significant lack of IPv4 addresses in some domains, port multiplexing is likely to be a necessary feature for translators (i.e., NAPT-PT). If NAPT-PT is used, it needs to be placed on the GGSN external interface (Gi), typically separate from the GGSN. NAPT-PT can be installed, for example, on the edge of the operator's network and the public Internet. NAPT-PT will intercept DNS requests and other applications that include IP addresses in their payloads, translate the IP header (and payload for some applications if necessary), and forward packets through its IPv4 interface.

NAPT-PT introduces limitations that are expected to be magnified within the 3GPP architecture. [NATPTappl] discusses the applicability of NAT-PT in more detail. [NATPTexp] discusses general issues with all forms of IPv6-IPv4 translation.

3GPP networks are expected to handle a very large number of subscribers on a single GGSN (default router). Each GGSN is expected to handle hundreds of thousands of connections. Furthermore, high reliability is expected for 3GPP networks. Consequently, a single point of failure on the GGSN external interface would raise concerns on the overall network reliability. In addition, IPv6 users are expected to use delay-sensitive applications provided by IMS. Hence, there is a need to minimize forwarding delays within the IP backbone. Furthermore, due to the unprecedented number of connections handled by the default routers (GGSN) in 3GPP networks, a network design that forces traffic to go through a single node at the edge of the network (typical NAPT-PT configuration) is not likely to scale. Translation mechanisms should allow for multiple translators, for load sharing and redundancy purposes.

To minimize the problems associated with NAPT-PT, the following actions can be recommended:

1. Separate the DNS ALG from the NAPT-PT node (in the "IPv6 to IPv4" case).

2. Ensure (if possible) that NAPT-PT does not become a single point of failure.

3. Allow for load sharing between different translators. That is, it should be possible for different connections to go through different translators. Note that load sharing alone does not prevent NAPT-PT from becoming a single point of failure.

Editor's Contact Information

Comments or questions regarding this document should be sent to the v6ops mailing list or directly to the document editor:

Juha Wiljakka
Nokia
Visiokatu 3
FIN-33720 TAMPERE, Finland

Phone: +358 7180 48372
EMail: juha.wiljakka@nokia.com

Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.