

ETSI TR 123 981 V17.0.0 (2022-04)



**Universal Mobile Telecommunications System (UMTS);
LTE;
Interworking aspects and migration scenarios for IPv4-based
IP Multimedia Subsystem (IMS) implementations
(3GPP TR 23.981 version 17.0.0 Release 17)**



Reference

RTR/TSGS-0223981vh00

Keywords

LTE,UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:

<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status.

Information on the current status of this and other ETSI documents is available at

<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommitteeSupportStaff.aspx>

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:

<https://www.etsi.org/standards/coordinated-vulnerability-disclosure>

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2022.
All rights reserved.

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: "*Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards*", which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<https://ipr.etsi.org/>).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Report (TR) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under <http://webapp.etsi.org/key/queryform.asp>.

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Intellectual Property Rights	2
Legal Notice	2
Modal verbs terminology.....	2
Foreword.....	5
Introduction	5
1 Scope	6
2 References	6
3 Definitions, symbols and abbreviations	7
3.1 Definitions	7
3.2 Symbols.....	7
3.3 Abbreviations	7
4 Architectural Requirements.....	8
4.1 General	8
4.2 Operational aspects for GPRS system.....	8
4.2.1 Support of PDP type IPv6.....	8
4.2.2 GPRS network/nodes.....	9
5 Architectural concept	9
5.1 General	9
5.2 UE access to IM CN subsystem	10
5.2.1 Obtaining IP address and P-CSCF discovery	10
5.2.2 Scenarios.....	11
5.2.2.1 IMS dual Stack UE accessing an IM CN subsystem.....	11
5.2.2.2 IPv4 UE and IPv4 based IM CN subsystem Implementation	11
5.2.2.3 IPv4 UE and IPv6 based IM CN subsystem.....	12
5.2.3 IP Versions in UE and P-CSCF	12
5.2.4 IP Versions in SGSN and GGSN.....	12
5.2.4.1 General	12
5.2.4.2 Implications of not supporting IPv6 in SGSN.....	12
5.3 Interworking scenarios	12
5.3.1 Interworking architecture and NATs	12
5.3.1.1 Interworking architecture	12
5.3.1.2 NATs.....	13
5.3.2 Overview	13
5.3.3 Non-roaming access to IMS scenarios.....	14
5.3.3.1 Non-roaming - IPv4 IM CN subsystem	14
5.3.3.2 Non-roaming dual stack IM CN subsystem	14
5.3.3.3 Non-roaming IPv6 IM CN subsystem.....	15
5.3.4 GPRS access scenarios	15
5.3.4.1 Non-roaming scenario, dual stack home network	15
5.3.4.2 Roaming – IPv4 visited network, dual stack home network	15
5.3.4.3 Roaming – IPv4 visited network, IPv6 IMS home network.....	16
5.3.4.4 Roaming – dual stack visited network, IPv4 GGSN and Dual stack IMS.....	17
5.3.4.5 Roaming – dual stack visited network, IPv6 home network	17
5.3.5 Interconnection and end-to-end scenarios.....	18
5.3.5.1 Overall Scenario.....	18
5.3.5.2 NAT/ALG between IMS entities within one operator's IMS network	19
5.3.6 Summary of issues arising from the scenarios.....	20
5.3.7 IP version interworking for services	20
5.3.7.1 Application servers.....	20
5.3.7.2 Interworking support in dual stack IM CN subsystem	21
5.3.7.3 Access to network services	22
5.4 Migration scenarios	22

5.4.1	IPv4 UE and IPv6 IM CN subsystem	22
5.4.2	A partially migrated IPv4 to IPv6 IM CN subsystem	22
5.4.3	Migration aspects for services	22
5.4.3.1	Application Servers	22
5.4.3.2	Migration support in dual stack IM CN subsystem	22
5.4.3.3	Access to network services	22
5.4.4	Example migration paths	23
6	Conclusions and recommendations	23
Annex A: Additional Information		24
A.1	GPRS deployment scenarios	24
A.1.1	IMS roaming access – IPv4 visited network, IPv4 home network	25
A.1.2	IMS roaming access - IPv4 visited network, IPv6 home network	25
A.1.3	IMS roaming access - IPv6 visited network, IPv4 home network	26
A.1.4	IMS roaming access - IPv4 visited network, dual stack home network	26
A.2	End to End scenarios	27
A.2.1	Non-roaming - IPv4 IM CN subsystem with IPv6 IM CN subsystem	27
A.2.2	Non-roaming - IPv4 IM CN subsystem with IPv4 IM CN subsystem	27
A.2.3	Non-roaming IPv4 IM CN subsystem with dual stack IM CN subsystem	28
A.2.4	Non-roaming dual stack IM CN subsystem with dual stack IM CN subsystem	29
A.2.5	Non-roaming IPv6 IM CN subsystem with dual stack IM CN subsystem	29
Annex B: Change history		31
History		32

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
 - 1 presented to TSG for information;
 - 2 presented to TSG for approval;
 - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

3GPP specifications design the IMS to use exclusively IPv6, however early IMS implementations and deployments may use IPv4, as specified in clause 5.1 of TS 23.221 [3]. Therefore it is understood that there will exist IPv4 based IMS implementations, namely initial IMS implementations and IMS implementations based on 3GPP2 specifications. This is the motivation to study interworking and migration scenarios related to IPv4 based IMS implementations.

1 Scope

The present document studies study interworking and migration scenarios related to IPv4 based IMS implementations. The study provides guidelines for operators and vendors on interworking aspects of IPv4 based IMS implementations, and provides guidelines on migrating to 3GPP IMS using IPv6.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

- [1] Void.
- [2] 3GPP TS 21.905: "Vocabulary for 3GPP Specifications".
- [3] 3GPP TS 23.221: "Architectural Requirements".
- [4] 3GPP TS 23.228: "IP Multimedia (IM) Subsystem - Stage 2".
- [5] 3GPP TS 23.141: "Presence Service; Architecture and Functional Description".
- [6] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".
- [7] 3GPP TS 33.203: "3G security; Access security for IP-based services".
- [7a] 3GPP TS 23.002: "Network Architecture".
- [8] draft-ietf-ngtrans-isatap-21.txt (April 2004): "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)", work in progress.

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

- [9] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3".
- [10] IETF RFC 2373: "IP Version 6 Addressing Architecture".
- [11] OMA DM WG: "OMA Device Management 1.1.2".
- [12] OMA: "OMA Client Provisioning 1.1".
- [13] 3GPP TS 24.167: "3GPP IMS Management Objects (MO); Stage 3".
- [14] 3GPP TS 27.060: "Mobile Station (MS) supporting Packet Switched Services".
- [15] IETF RFC 2507: "IP Header Compression".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 21.905 [2] and the following apply.

Dual stack IM CN subsystem: For the purpose of this technical report, a dual stack IM CN subsystem is an IM CN subsystem implementation in which all network entities support IPv4 and IPv6 for IMS communication. It is an IM CN subsystem implementation that supports both IPv6 as per 3GPP Release 5 or later standards, and an IPv4 IM CN subsystem.

IPv4 based IM CN subsystem implementation, IPv4 IM CN subsystem: For the purpose of this technical report, an IPv4 based IM CN subsystem implementation (or short: IPv4 IM CN subsystem) means an IM CN subsystem implementation, which is based on 3GPP Release 5 or later standards, but uses IPv4 rather than IPv6.

IPv4 based UE implementation, IPv4 UE: For the purpose of this technical report, an IPv4 based UE implementation (or short: IPv4 UE) means a UE implementation, which is based on 3GPP Release 5 or later IMS standards, but uses IPv4 rather than IPv6 to access an IM CN subsystem.

IPv6 based IM CN subsystem implementation, IPv6 IM CN subsystem: For the purpose of this technical report, an IPv6 based IM CN subsystem implementation (or short: IPv6 IM CN subsystem) means the IM CN subsystem implementation according to 3GPP Release 5 or later standards that uses IPv6.

IPv6 UE: For the purpose of this technical report, an IPv6 UE means a UE implementation, which is based on 3GPP Release 5 or later IMS standards and uses only IPv6 to access IM CN subsystem even though the IP stack in the UE as such may be a dual IPv4 and IPv6 stack.

IMS dual stack UE: For the purpose of this technical report, an IMS dual stack UE means a UE implementation, which is based on 3GPP Release 5 or later IMS standards, but in addition to IPv6 can use IPv4 to access an IPv4 IM CN subsystem.

3.2 Symbols

For the purposes of the present document, the following symbols apply:

Gi	Reference point between GPRS and a packet data network.
Gm	Reference Point between a UE and a P-CSCF.
Gn	Interface between two GSNs within the same PLMN.
Mb	Reference point to network services.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ALG	Application Level Gateway
CN	Core Network
CSCF	Call/Session Control Function
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSN	GPRS Support Node
I-CSCF	Interrogating CSCF
IM	IP Multimedia
IMS	IP Multimedia Subsystem
IM-MGW	IP Multimedia – Media GateWay
IP	Internet Protocol
IPSec	IP Security protocol
MRFP	Multimedia Resource Function Processor
NAT	Network Address Translation

NA(P)T-PT	Network Address (Port-Multiplexing) Translation-Protocol Translation
OMA	Open Mobile Alliance
OTA	Over the Air Activation
PCO	Protocol Configuration Options
P-CSCF	Proxy-CSCF
PDP	Packet Data Protocol
QoS	Quality of Service
S-CSCF	Serving-CSCF
SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol
SMS	Short Message Service
TrGW	Transition Gateway
UE	User Equipment

4 Architectural Requirements

4.1 General

An IMS dual stack UE shall be able to determine whether to use IPv4 or IPv6 when accessing the IMS.

A dual stack IMS shall be able to determine whether to use IPv4 or IPv6.

IMS security shall be possible for both IPv4 and IPv6 IMS networks and UEs accessing these networks.

SIP Compression shall be possible for both IPv4 and IPv6 IMS networks and UEs accessing these networks.

P-CSCF discovery mechanisms shall be possible for both IPv4 and IPv6 IMS networks and UEs accessing these networks.

An IPv4 IM CN Subsystem shall be able to interwork with an IPv4 IM CN Subsystem.

An IPv4 IM CN Subsystem shall be able to interwork with an IPv6 IM CN Subsystem.

A dual stack IM CN Subsystem shall be able to interwork with an IPv4 IM CN Subsystem.

A dual stack IM CN Subsystem shall be able to interwork with an IPv6 IM CN Subsystem.

A dual stack IM CN Subsystem shall be able to interwork with a dual stack IM CN Subsystem.

A dual stack IM CN Subsystem may support IPv4 UEs.

An IPv4 IM CN Subsystem and a dual stack IM CN Subsystem may support IPv4 private addressing – i.e. the IMS elements shall support the case in which both the IMS network and the user are within (the same) IPv4 private address domain.

The mechanisms described in this TR shall not limit the flexibility with respect to APN usage for IMS.

It is desirable to avoid media tromboning e.g. in case a call traverses a NAT and then is routed back into the same network.

4.2 Operational aspects for GPRS system

4.2.1 Support of PDP type IPv6

If GPRS Roaming is used, i.e. the GGSN and P-CSCF are in the home network, then the support of IMS using IPv6 requires the support of PDP contexts of PDP type IPv6 in both the visited and the home network.

Clause 5.2.2.3 discusses a possible work-around for the case where this requirement is not met because the visited network does not support PDP type IPv6.

4.2.2 GPRS network/nodes

Current deployed GPRS systems are known to be IPv4 only. For early IMS deployment using IPv4, it is expected that GPRS systems as early as Release 1999 would be used and it should be possible to run early IPv4 IMS system without requiring upgrades to GPRS and its support system (i.e. DNS, Gi reference etc.). In order to achieve this, certain assumptions must be made on the deployed networks and also some guidelines must be provided on expected impacts on GPRS system to move towards IPv6 IMS deployment.

Levels of migration and interworking aspects are described below:

- The working principle in this TR is that the deployment of IPv6 networks interworking with IPv4 networks on the application layer does not impose any new requirements on the transport layer;
- The most efficient and transparent way of supporting access to IPv6 services over GPRS is to ensure that GGSN is dual stack;
- It is expected that connection scenarios with a change of PDP Type between SGSN and GGSN are not practical deployment cases and as such are not even considered as part of the scenarios analysis as shown in Annex A.

NOTE 1: A proper SGSN and GGSN configuration and deployment with IPv6 only support is not in any way restricted when considering IPv6 only service environment.

NOTE 2: When dual stack SGSN/GGSN nodes are considered, the mechanism to interconnect using IPv4, IPv6 or both IP version are dependent on the operator's interconnect agreement and deployment.

5 Architectural concept

5.1 General

In order to provide support of early deployment of IPv4 IM CN subsystem, the implications on the terminals, GPRS system, the IM CN subsystem must be considered in the context of the functions provided by IPv6 IMS CN subsystem developed in 3GPP Release 5 and onwards.

In addition, migration towards an IPv6 IM CN subsystem and co-existence of both IPv4 and IPv6 IM CN subsystem and thus interworking among these systems must also be considered using already available mechanism that may/will be used for early deployment scenarios. An IPv4 based IM CN subsystem implementation may need to support interworking with an IPv6 based 3GPP IM CN subsystem.

The 3GPP scope of early IMS implementations using IPv4 shall be primarily focused on considerations regarding the UE-network interface.

For IPv4 based IMS implementations the Mb reference point needs to provide access to IPv4 network services in addition to or instead of IPv6 network services. The relationship to Gi and other aspects of the Mb reference point, as defined in TS 23.002 [7a], remain unchanged.

The following procedures shall be checked for possible impacts regarding the usage of IPv4:

- P-CSCF discovery; It is important to select one single P-CSCF discovery for early IPv4 IMS deployments to make interoperability easier.
- Access security (authentication and integrity protection);
- SIP Compression;
- Service Based Local Policy.

Aside from the P-CSCF address passed as part of the P-CSCF discovery, there are various other IMS entity addresses that are included in the IMS signalling methods. Addresses may be contained in route headers and may be passed in other headers such as to identify the appropriate on-line or off-line charging entities. It is necessary to verify that both IPv4 and IPv6 addresses can be supported. This is necessary to assure that both can be accommodated during the interim as a network evolves from one version to the other such that a flash cut is not required.

5.2 UE access to IM CN subsystem

5.2.1 Obtaining IP address and P-CSCF discovery

Prior to communication with the IM CN subsystem, the UE:

- a) establishes a connection with the IP-CAN;
- b) obtains an IP address using either the standard IETF protocols (e.g., DHCP) or a protocol that is particular to the IP-CAN technology that the UE is utilising;
- c) acquires a P-CSCF address.

The existing P-CSCF discovery mechanism are either IPv6 specific or use Release 5 or later GPRS. For an IPv4 based IMS implementation, operators may need other mechanisms not currently defined as possible options in 3GPP IMS.

The following mechanisms need to be evaluated for P-CSCF discovery in IPv4:

- a) the address of the P-CSCF can be requested by the UE and returned by the GGSN at PDP context establishment time. An IPv4 UE would need to obtain an IPv4 address as part of this exchange.

If the PDP context established is of PDP type IPv4, then the GGSN may provide an IPv4 P-CSCF address. This does not preclude scenarios, where the GGSN returns an IPv6 P-CSCF address at IPv4 PDP context establishment, e.g. for the support of tunnelling (see clause 5.3.4.3), or both IPv4 and IPv6 P-CSCF addresses. If the PDP type is IPv4 then it is recommended that the GGSN always return both IP versions, if it is capable, using the existing capabilities to send multiple P-CSCF addresses within the PCO IE.

According to TS 24.008 [9], the P-CSCF address in the PCO field is an IPv6 address. Thus there are at least two possible approaches: The first approach would be to avoid any changes to or deviations from TS 24.008 [9] and use the existing methods to transfer an IPv4 address as an IPv6 address ("IPv6 address with embedded IPv4 address", as defined in RFC 2373 [10]). In such a case, the use of "IPv4 mapped addresses" as defined in RFC 2373 [10] is recommended.

The second approach would set the PCO field length to 4 and put the IP address in the content field. This would be a straightforward generalization of the specified method.

In a migration period with a dual stack network, it may be useful for an operator to provide a common P-CSCF discovery mechanism for both the early IPv4 only UEs and the IPv6 Release 5 (or later) UEs. In that case, the first approach using embedded addresses is recommended, as it does not require any changes to or deviations from TS 24.008 [9].

- b) based on DHCP. Currently the specifications limit this to the IPv6 methods for DHCP. In order for this method to be used by an IPv4 UE, it needs to be identified how IPv4 DHCP is used to obtain the P-CSCF address. A solution that provides access independence would be that an IPv4 P-CSCF and IPv4 UE support configuration of the appropriate P-CSCF information via DHCPv4. In this solution, use of DHCP provides the UE with the fully qualified domain name of a P-CSCF and the address of a Domain Name Server (DNS) that is capable of resolving the P-CSCF name. When using DHCP/DNS procedure for P-CSCF discovery with IPv4 GPRS-access, the GGSN acts as DHCP Relay agent relaying DHCP messages between UE and the DHCP server. This is necessary to allow the UE to properly interoperate with the GGSN. This solution however requires that a UE supporting early IPv4 implementations would support DHCPv4.
- c) other mechanisms, such as SMS, OTA, OMA device management or other configuration schemes are already in use today by deployed UEs. Some of the provisioning mechanisms in use are vendor specific (such as pre-configuration mechanisms), but it is assumed that most of the early-deployed IPv4 UEs will support OMA specified provisioning mechanisms such as OMA Client Provisioning [12] and OMA Device Management (DM) [11]. It is recommended that provisioning parameters for IPv4 P-CSCF discovery be defined for OMA standardised provisioning mechanisms such as OMA DM [11]. The P-CSCF address provisioned is a FQDN as specified in TS 24.167 [13].

Since the P-CSCF address is a FQDN, the UE shall be able to request the address of a Domain Name Server for resolving the P-CSCF address. Therefore, it is necessary to allow the UE to request a DNS Server IPv4 address(es) by the Protocol Configuration Options IE when activating a PDP context. The DNS IPv4 address can be retrieved according to TS 27.060 [14].

The provisioning mechanism in c) does not require any support from the GPRS infrastructure and is thus expected to be used in early implementations from the beginning. The mechanism in a) may facilitate migration to one of the P-CSCF discovery mechanisms specified in TS 23.228 [4].

It is assumed that a UE, which has a pre-configured P-CSCF address, may try to use the mechanism in a) when activating the PDP context to be used for IMS signalling. If a P-CSCF address is received the UE would use the received address and otherwise the UE would try to connect to the pre-configured P-CSCF before using any other P-CSCF discovery mechanism.

5.2.2 Scenarios

5.2.2.1 IMS dual Stack UE accessing an IM CN subsystem

An IMS dual stack UE may access an IM CN subsystem using IPv4 or IPv6 depending on the IP versions that the IM CN subsystem supports. The IM CN subsystem might then be IPv4 only, dual stack or IPv6 only.

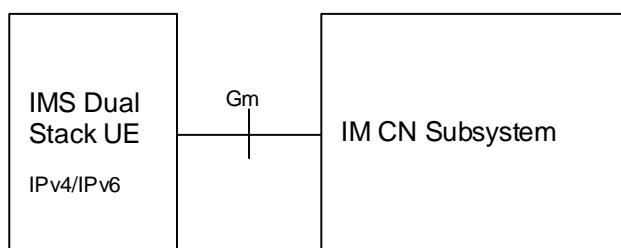


Figure 5-1: IMS dual Stack UE accessing an IM CN subsystem

From an IM CN subsystem perspective, the UE behaves like an IPv4 based UE implementation in this scenario.

The UE needs to determine whether to use IPv4 or IPv6. One possibility is that the UE is pre-configured to use IPv4 or IPv6 for IMS. If the UE is not pre-configured, one approach is that the UE first tries to establish a connection towards an IPv6 based IM CN subsystem; if it cannot gain IPv6 connectivity or cannot access an IPv6 based IM CN subsystem, then it should try to access an IPv4 IM CN subsystem. This way no delay is introduced when an IPv6 based 3GPP IM CN subsystem is in place.

It is important to specify a predictable dual-stack UE behaviour. The following behaviour is recommended:

- IMS dual stack UEs shall always try to initially activate an IPv6 PDP context for IMS communications. If this fails, the UE may try to activate an IPv4 PDP Context.
- In case the IMS dual stack UE has successfully activated an IPv6 PDP context for IMS communications, the UE shall use IPv6 to contact the P-CSCF whenever possible (i.e. whenever it has obtained an IPv6 address for a P-CSCF).

In general, it is recommended for IMS UEs that support IPv4-based connectivity to early IMS deployments to also support IPv6. This makes the migration to a full scale IPv6 IMS considerably easier.

When the UE is connected to IM CN subsystem using IPv4, the UE behaves like an IPv4 UE from IM CN subsystem perspective.

Even if the UE is a dual stack UE, the following needs to be considered:

- If the UE has registered with IPv4 private address, then NAT may be needed at the network borders if private addressing is used within the IMS network.
- If the UE has registered with IPv6, then the dual stack home network will use IPv6 for IMS communication towards the UE, even if it is part of a communication with an IPv4 network.

5.2.2.2 IPv4 UE and IPv4 based IM CN subsystem Implementation

In this scenario an IPv4 UE accesses an IPv4 IM CN subsystem. Interworking and migration aspects applicable for this scenario can be derived from the scenario described in clause 5.2.2.1.

5.2.2.3 IPv4 UE and IPv6 based IM CN subsystem

In this scenario an IPv4 UE attempts to access an IPv6 IM CN subsystem. This scenario is can not be supported while maintaining the architecture principles in clause 5.2.1 and clause 5.2.3 below.

5.2.3 IP Versions in UE and P-CSCF

IMS security relies heavily on the security association between UE and P-CSCF: IPSec is used between P-CSCF and UE according to TS 33.203 [7]. Any intermediary node between UE and P-CSCF, which changes the IP messages exchanged, would create serious security problems and require significant changes to the IMS security architecture. Moreover, if SIP compression is used between P-CSCF and the UE, then SIP messages cannot be read or modified by intermediate nodes. In addition mechanisms for P-CSCF discovery would require modification if IP version interworking was applied between UE and P-CSCF.

Thus it is recommended and assumed in this TR that SIP communication between UE and P-CSCF either uses IPv4 or IPv6 without intermediaries changing the IP version.

5.2.4 IP Versions in SGSN and GGSN

5.2.4.1 General

The IP version in the SGSN and GGSN nodes considered in this document relates to the IP version above the GTP level identified by the PDP type. The implications of the IP version above the GTP layer is also relevant over the Gi reference point, since this reference point determines the IP version connection towards the external/outside of GPRS networks. For example, in case of IMS, it is the Gm reference point between the UE and the P-CSCF through the GGSN over the Gi reference point and the IP version would be critical to be the same between the UE and the P-CSCF for smooth IMS services.

Gi reference point also ties the UE towards the APN used to access GPRS and the relevant IP version supported over this APN. For more details, see TS 23.060 [6] and clause 4.2.2.

The IP version can then be either IPv4 only, or IPv6 only at any instant when the UE is activating a PDP context. A dual stack SGSN/GGSN node supports both PDP types IPv4 and IPv6.

5.2.4.2 Implications of not supporting IPv6 in SGSN

An inter-SGSN RAU may be rejected when using a PDP context with PDP type IPv6 due to the new SGSN does not support PDP type IPv6, or the new SGSN may accept the RAU but would then de-activate the PDP contexts it cannot support. If the behaviour above is followed and there are SGSNs in the roamed to PLMN that do not support PDP type IPv6, UEs accessing IMS from that PLMN may after a while end-up using PDP contexts of PDP type IPv4. That is, the communication towards IMS would be interrupted and the UE would have to re-register in IMS using an IPv4 address.

The UE would have to de-register from IMS and deactivate related PDP contexts before accessing IMS using a PDP context of PDP type IPv6 again, see clause 5.2.2.1 for an IMS dual-stack UE behaviour.

The move to PDP contexts of type IPv4 would be avoided if all SGSNs support PDP type IPv6.

The IMS communication interruption and re-registration with an IPv4 address in IMS could be avoided if the UE uses a tunnelling mechanism like ISATAP [8]. However, as the UE is not on its own aware of IPv6 support in SGSNs, it is not possible for the UE to make a decision when to use and when not to use tunnelling.

5.3 Interworking scenarios

5.3.1 Interworking architecture and NATs

5.3.1.1 Interworking architecture

TS 23.228 [4], clause 5.38, defines an architecture for interworking between an IPv6 based 3GPP IM CN subsystem and IPv4 SIP networks. It uses the concept of IMS-ALG and NATs (TrGWs), based on the general concept of ALGs

and NA(P)T/NA(P)-PT: The IMS ALG is the necessary application level gateway, which is aware of SIP/SDP protocols, and the TrGW is a NA(P)T-PT, which provides the translation function.. An IPv4 based IM CN subsystem is a particular example for an IPv4 SIP network, and thus the interworking architecture may be applied. These mechanisms defined in TS 23.228 [4] are also applicable when an IPv4 IM CN subsystem migrates to IPv6, and needs to interwork with other IPv4 IM CN subsystems or IPv4 SIP networks.

5.3.1.2 NATs

In general, address translation mechanisms have been available for Internet applications for some time now. The disadvantages of such NAT- and ALG-based mechanisms have also been identified a long time ago:

- NAT breaks the end-to-end model of IP;
- Coordination between the ALG processing the signalling and the NAT processing the media stream IP headers is needed;
- NAT is a single point of failure for ongoing connections. A session through a NAT must flow through the same NAT for the entire duration of the session. Thus, if a NAT fails, all its sessions will abruptly terminate.
- Scalability problems of NATs and ALGs.

While NATs (and ALGs) are expected to be used in the future, it can be concluded that their wide scale deployment in a carrier-grade IMS environment shall be avoided whenever possible.

5.3.2 Overview

The following scenarios are those that need to be considered for IMS interworking if it is assumed that there are both IPv6 and IPv4 IMS deployments. This list may not be exhaustive of the possible deployments. The scenarios in the following clauses are divided into the following categories:

1. IMS interworking – non-roaming scenarios, see clause 5.3.3;
2. IMS interworking – roaming scenarios, see clause A.1.1;
3. GPRS access scenarios, see clause 5.3.4;
4. IMS interworking – interconnect and end-to-end scenarios, see clause 5.3.5 and A.2.

In all cases it will be necessary to consider the IP version supported by the UE. Particularly, as networks migrate from IPv4 to IPv6, there may exist IPv4 only terminals attempting to access IMS in networks supporting IPv6.

In considering scenarios, it is necessary to take into account the use of private addressing and the use of NAT at the edge of IPv4 networks and the implications for protocols with embedded IPv4 addresses.

Depending on the scenarios, the term NAT in the description and in the figures of this report can also imply a NA(P)T/NA(P)-PT and SIP/SDP aware ALG as defined in the interworking architecture, see clause 5.3.1.1. For example in scenario 5.3.2.2.1, "Non-roaming - IPv4 IM CN subsystem with IPv6 IM CN subsystem", communication is only possible via NA(P)T/NA(P)-PT if the other end point is IPv6 only.

It is assumed that the NATs are SIP/SDP aware.

Interconnect networks are assumed to support IPv4, or both IPv4 and IPv6.

The main architecture principle assumed for the GPRS system is the use of GGSN in the home network when early deployment and possible migration scenarios of IPv4 based IMS implementation is considered.

In the scenarios in this clause 5.3 and in annex A, the IP version mentioned refers to the IP version used for IMS communication. From the GPRS perspective this is the PDP type used. The PDP type is the IP version used inside the GTP tunnel on top of GTP. For example, an IPv6 IMS may run in a network where transport on Gn (on the IP layer below GTP) uses IPv4. See TS 23.060 [6] for details.

5.3.3 Non-roaming access to IMS scenarios

In this clause the scenarios cover aspects where the IM CN subsystem belongs to one IMS operator's domain, i.e. the UE is connected to Home IMS network.

5.3.3.1 Non-roaming - IPv4 IM CN subsystem

An IPv4 UE or IMS dual stack UE is connected to an IPv4 IM CN subsystem. The UE may originate or receive incoming sessions. A NAT might be used to connect to the other networks.

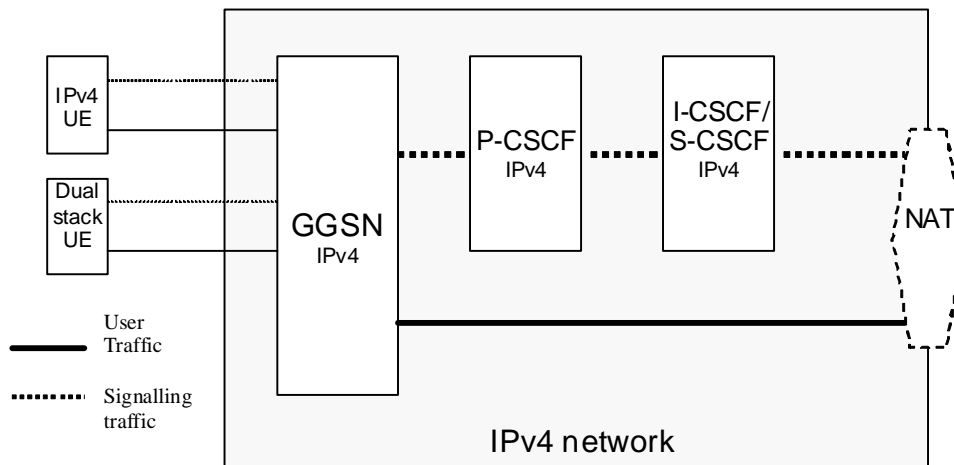


Figure 5-2: Non-roaming IPv4 IM CN subsystem

In this scenario

- clause 5.2.2.1 applies to the dual stack UE accessing the IPv4 IM CN subsystem;
- clause 5.2.2.2 applies to the IPv4 UE accessing the IPv4 IM CN subsystem.

5.3.3.2 Non-roaming dual stack IM CN subsystem

An IPv4 UE, an IMS dual stack UE or an IPv6 UE can be connected to a dual stack IM CN subsystem. The UE may originate or terminate sessions. The dual stack IMS uses IPv4 or IPv6 depending on the UE capability and the network interconnection.

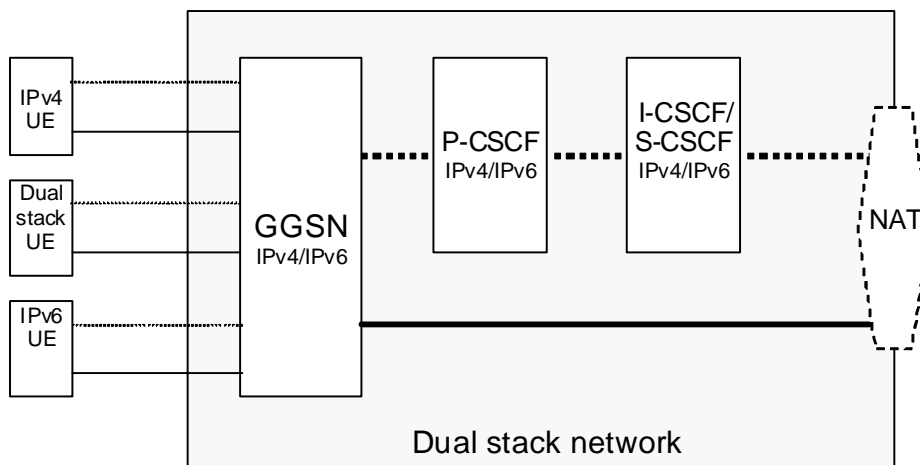


Figure 5-3: Non-roaming dual Stack IM CN subsystem

In this scenario clause 5.2.2.1 and apply to the dual stack IMS UE accessing the dual stack IMS network.

5.3.3.3 Non-roaming IPv6 IM CN subsystem

A dual stack UE or an IPv6 UE can be connected to an IPv6 IM CN subsystem. The UE may originate or terminate sessions.

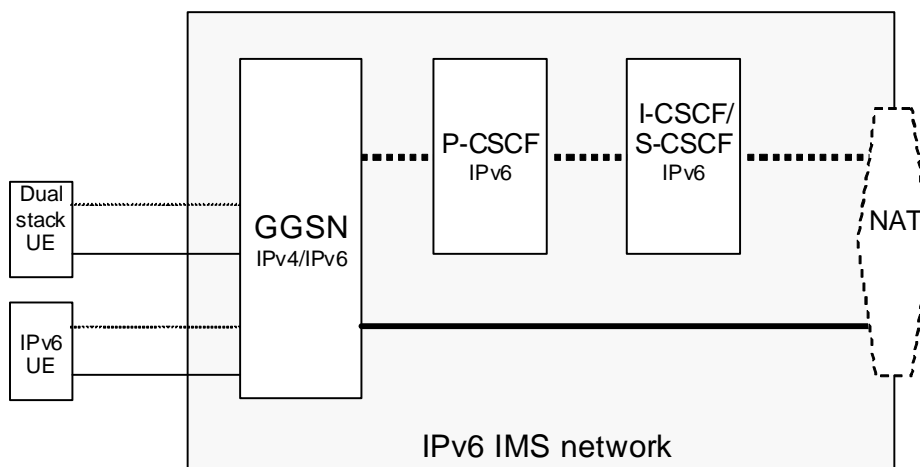


Figure 5-4: Non-roaming IPv6 IM CN subsystem

In this scenario clause 5.2.2.1 apply to the dual stack UE accessing the IPv6 IM CN subsystem.

5.3.4 GPRS access scenarios

5.3.4.1 Non-roaming scenario, dual stack home network

In this scenario, the home network (GPRS and IMS) is dual stack and can support access to IPv4, IPv6 and dual stack UEs.

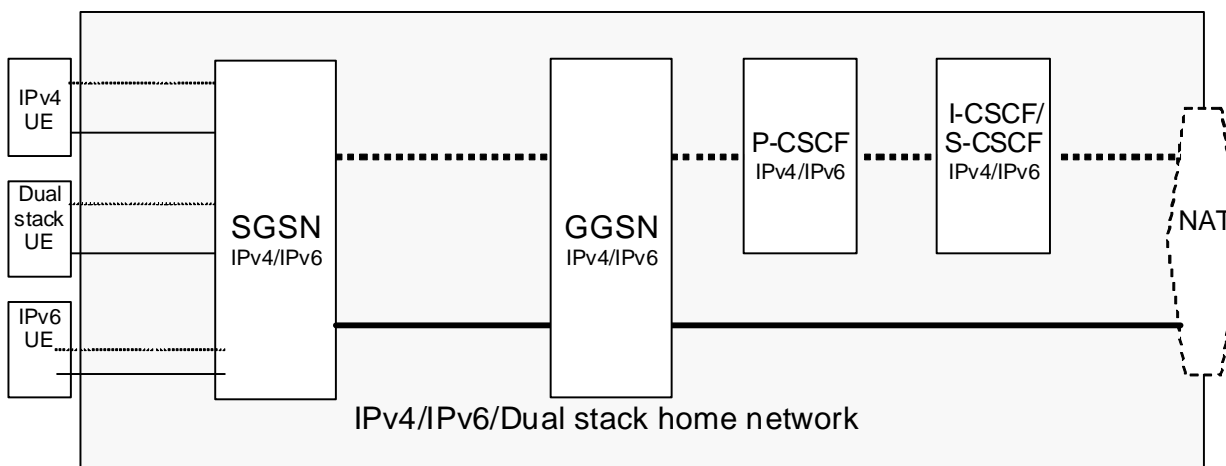


Figure 5-5: GPRS roaming – dual stack visited network, dual stack home network

5.3.4.2 Roaming – IPv4 visited network, dual stack home network

The UE and the SGSN are in the IPv4 visited network. The GGSN, P-CSCF, I-CSCF and S-CSCF are in the dual stack home network. The UE may be an IPv4 only UE or an IMS dual stack UE. Clause 5.2.2.1 applies to the dual stack UE accessing the visited and home network. The visited network does not support IPv6 PDP context.

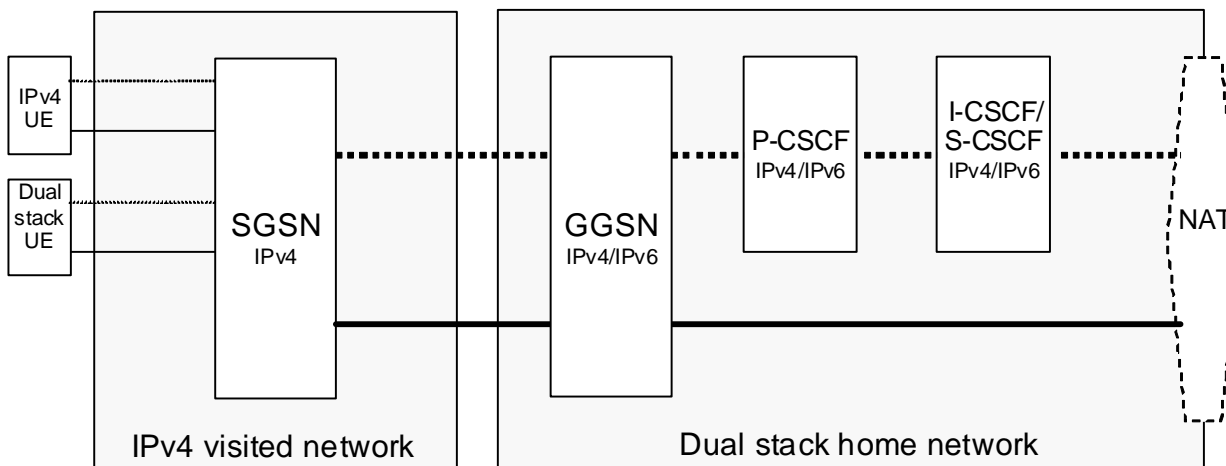


Figure 5-6: GPRS roaming – IPv4 visited network, dual stack home network

Based on the considerations in clause 4.2.1 and 5.2.3, the UE and the P-CSCF cannot use IPv6 for IMS communication, even if both are IPv6 capable. However, in this scenario the UE can fall back to IPv4, if the UE is dual-stack. In this case similar considerations like in clause 5.2.2.1 apply: one approach is that the UE would initially attempt to establish an IPv6 context to its home GGSN and, if this fails, establish an IPv4 context and seek to establish an IPv4 IMS session.

5.3.4.3 Roaming – IPv4 visited network, IPv6 IMS home network

The UE and the SGSN are in the IPv4 visited network. The GGSN, P-CSCF, I-CSCF and S-CSCF are in the IPv6 home network. The IMS home network is IPv6 only. The UE may be IPv6 only or may be IMS dual stack UE. Clause 5.2.2.1 applies to the dual stack UE accessing the visited and home network.

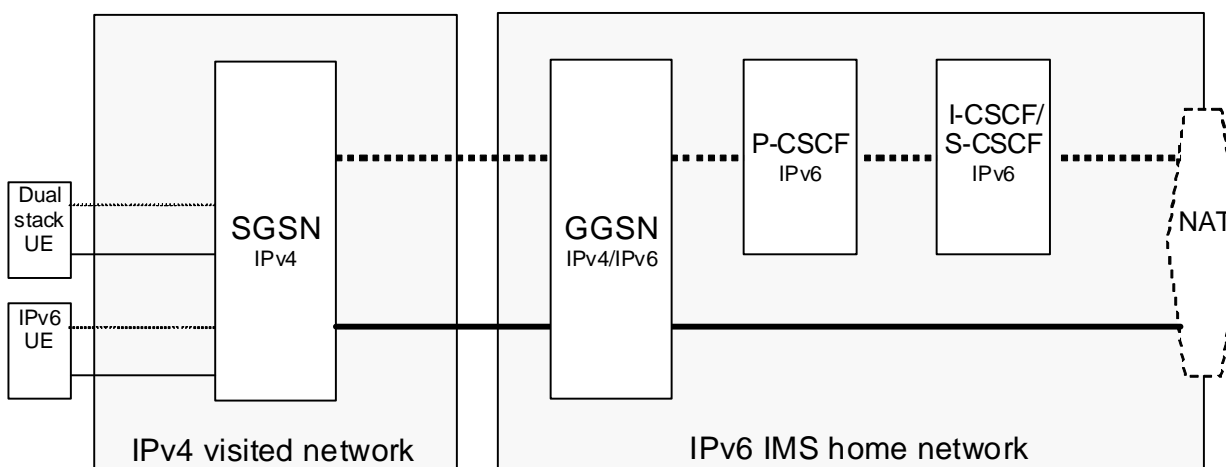


Figure 5-7: GPRS roaming – IPv4 visited network, IPv6 home network

In this scenario the requirement from clause 4.2 is not met.

This is an attractive IMS deployment scenario for operators as it does not rely on the support of any explicit IMS functionality in the visited network; however problems arise through the lack of IPv6 PDP context support in the visited network. As such, operators should wherever possible seek agreements with their roaming partners for the support of IPv6 contexts where IMS roaming is to be supported (this should be the long term objective).

In the event that an IPv6 context is not available in the visited network, the only alternative for the operator deploying an IPv6 only IM CN subsystem is to use a tunnelling method between the UE and home network in order to acquire an IPv6 address. When the UE is IPv6 only, it is assumed that the UE does not have the capability to use a tunnelling method between the UE and the home network to acquire an IPv6 address. Tunnelling of IPv6 packets over IPv4 from the UE to the IMS CN subsystem is a technically feasible, but there are various issues that would need to be addressed. There would be the need for an IPv4-IPv6 gateway acting as the tunnel end-point responsible for packing/unpacking the IPv6 packets. The UE would need to discover and address it. Also, the UE would need the ability to tunnel the packets. Further work would be needed on how the UE would address this entity, however existing IETF work (e.g.

ISATAP [8]) could be used. This implementation would require additional functionality in the UE compared to the minimum IPv6 functionality as stated in TS 23.221 [3] and an additional ISATAP router functionality in the network. Header compression using e.g. RFC 2507 [15] is able to compress both the IPv4 and the IPv6 header. The SBLP mechanisms at the Go interface could not be used between an IPv4 GGSN and an IPv6 P-CSCF, i.e. this solution is not possible if SBLP over Go is required.

Similar considerations like in clause 5.2.2.1 apply: one approach is that the UE would initially attempt to establish an IPv6 context to its home GGSN and, if this fails, establish an IPv4 context and tunnel an IPv6 IMS session over IPv4.

It can be concluded that network operators, who introduce 3GPP IMS using IPv6, have a strong interest that their GPRS roaming partners provide support for PDP contexts of PDP type IPv6.

5.3.4.4 Roaming – dual stack visited network, IPv4 GGSN and Dual stack IMS

In this scenario, the UE can access GPRS using IPv4 PDP type only since GGSN supports IPv4 only. That is, this scenario require the UE to use IPv4 or, using mechanism described in clause 5.3.4.3, the UE may acquire an IPv6 address from home network and use IPv6 IMS.

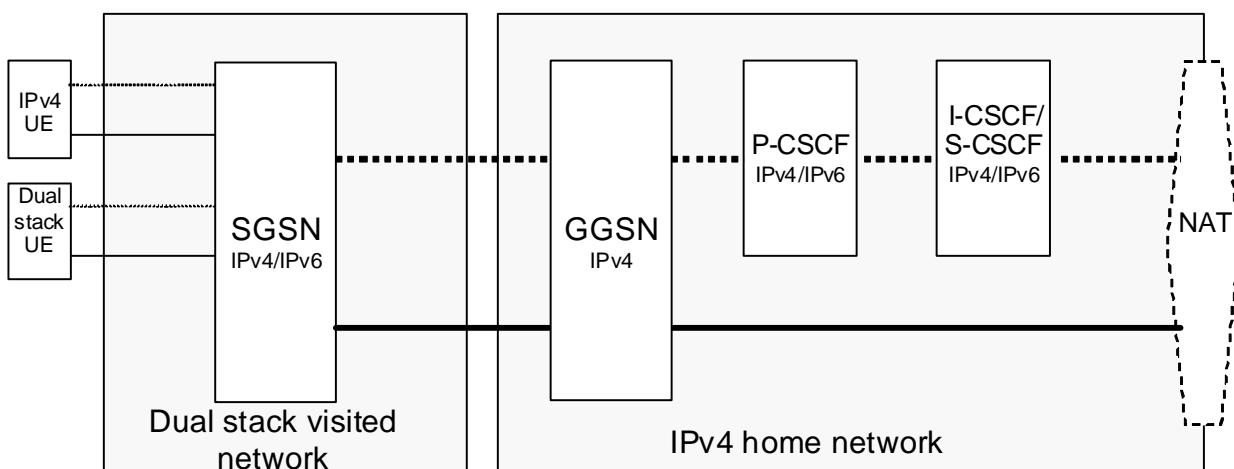


Figure 5-8: Dual stack visited network, IPv4 GGSN

5.3.4.5 Roaming – dual stack visited network, IPv6 home network

In this scenario, the UE can not access GPRS using IPv4 PDP type since GGSN supports IPv6 only. So, only IPv6 IMS access is possible in this scenario.

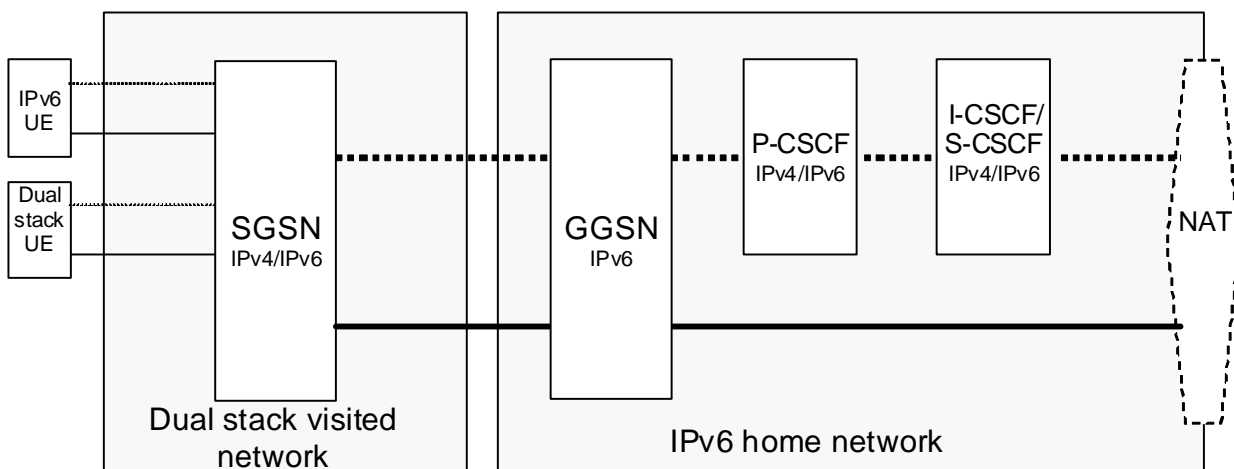


Figure 5-9: Dual stack visited network, IPv6 GGSN

5.3.5 Interconnection and end-to-end scenarios

5.3.5.1 Overall Scenario

Connecting different IMS access scenarios and then interconnecting to external IMS/SIP networks in order to support sessions between two end points define end-to-end scenarios. Some examples of the end-to-end scenarios are defined in the figure and table below. The assumption is that UE#1 initiate the sessions.

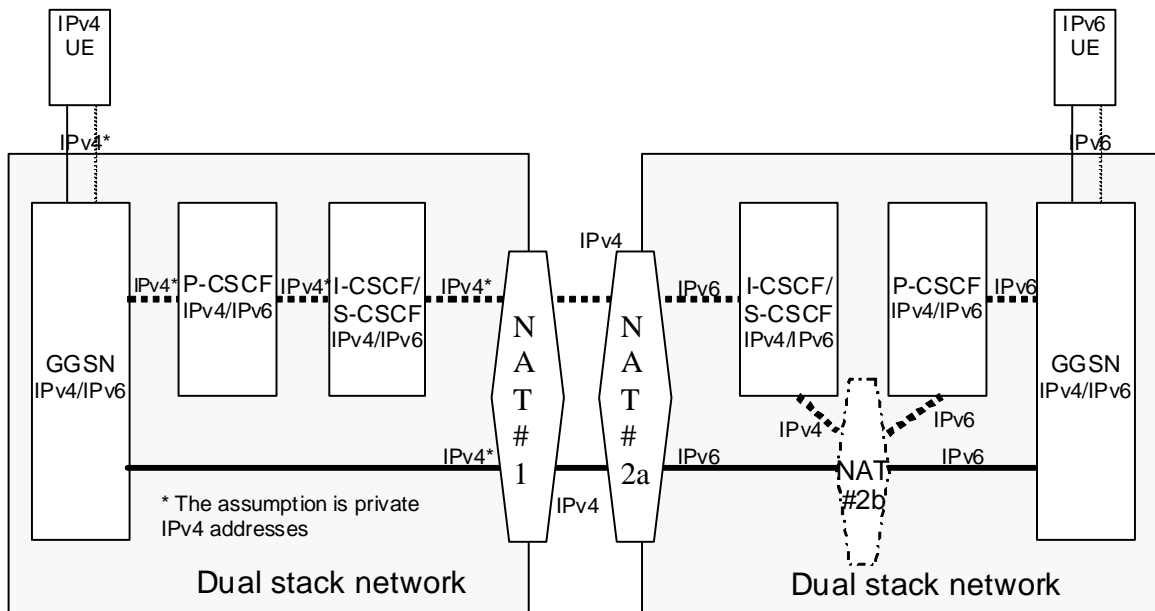


Figure 5-11: Example of an end-to-end scenario

Figure 5-11 above is an illustration of the scenario 5 in the table below. X in the NAT column in the table below means that a NAT/ALG might be necessary and that depends on the IMS service. For some IMS services a NAT/ALG is not necessary as described in clause 5.3.6.2. NAT#1 and NAT#2a are typically at the border of network#1 and the transit network(s). NAT#2b is somewhere between the S-CSCF and P-CSCF in the network#2.

Especially in the case when the networks use dual stacks there might be different alternatives what kind of IP version might be used in the transit network. The network#1 decides the IP version to use in the transit network based on the capability of the transit and network#2 and the policy defined between network#1 and network#2.

Table 5-1: End-to-end scenarios

Scenario	UE#1	Network#1	NAT#1	Transit	NAT#2a	Network#2	NAT#2b	UE#2
1	IPv4	5.3.3.1, IPv4 only	X	IPv4	-	5.3.3.1	-	IPv4
2	Dual stack (IPv4 in use)	5.3.3.1	X	IPv4	-	5.3.3.1	-	IPv4
3	IPv4	5.3.3.1	X	IPv4	-	5.3.3.2 IPv4/IPv6 Note 1	X	Dual stack (IPv6)
4	Dual stack (IPv4 in use)	5.3.3.1	X	IPv4	-	5.3.3.2 IPv4/IPv6 Note 1	X	Dual stack (IPv6)
5	IPv4	5.3.3.2 (IPv4)	X	IPv4	-	5.3.3.2 IPv4/IPv6 Note 1	X	IPv6
6	Dual stack (IPv6 in use)	5.3.3.2 (IPv6)	-	IPv6	-	5.3.3.2 (IPv6)	-	IPv6
7	IPv6	5.3.3.2 (IPv6)	X	IPv4	X	5.3.3.1 IPv4	-	IPv4
8	IPv6	5.3.3.2 (IPv6)	-	IPv6	-	5.3.3.2 IPv6/IPv4 Note 2	X	IPv4
9	IPv6	5.3.3.3	-	IPv6	-	5.3.3.2 IPv6/IPv4 Note 2	X	IPv4
10	IPv6	5.3.3.3	-	IPv6	-	5.3.3.3	-	Dual Stack (IPv6)
NOTE 1: The S-CSCF in the terminating network will recognize that the UE#2 has registered an IPv6 address and a translation to IPv6 is then necessary on the transport layer and possibly also on the application layer.								
NOTE 2: The S-CSCF in the terminating network will recognize that the UE#2 has registered an IPv4 address and a translation to IPv4 is then necessary on the transport layer and possibly also on the application layer.								

5.3.5.2 NAT/ALG between IMS entities within one operator's IMS network

As table 5-1 shows, there are scenarios where NAT#2b cannot be avoided.

For example, in scenario 5 in table 5-1 and figure 5-11, the IPv4 UE1 is assigned a private IPv4 address. There is no way S-CSCF1 can get any knowledge in advance what kind of IP address the destination UE uses. It could be private IPv4, public IPv4 or IPv6. The S-CSCF#1 can only get the knowledge what kind of IP realms the destination network uses (i.e. I-CSCF). It could be public IPv4 or IPv6. In cases where IPv4 is used for transit, the S-CSCF1 must then link in an ALG or edge proxy to bind the private IPv4 address in the SIP/SDP to a public IPv4 address. Most likely a NAT function is included in an edge router.

The network topology of network#2 could be set up so that no NAT need to be traversed in this case to I-CSCF2 (NAT can be by-passed in the edge router). The S-CSCF2 inspects the content of the message and determines that the UE2 uses IPv6. The S-CSCF2 must then link in an ALG or edge proxy to bind the public IPv4 address in the SIP/SDP to an IPv6 address. Whether S-CSCF2 uses IPv4 or IPv6 as transport to the ALG/edge proxy is up to the network#2 policy.

Additionally, when both the UE and the IMS network supports dual stack, use of IPv6 in order to provide IMS service would significantly reduce the number of scenarios where NAT/ALG would be required to be linked in between P-CSCF and S-CSCF for the terminating user.

This TR already provides guidelines regarding dual stack support in the UE and use of dual stack application servers that can provide interworking without use of NAT/ALG. These recommendations reduce the number of cases for the need of NAT/ALG during early deployment of IPv4 based IMS services. That is, the need to link in of an NAT#2b in scenario 5 in table 5-1 would be minimized if IPv6 would be used within network#2, by either using IPv6 for transit routing between networks or by using a NAT#2a.

5.3.6 Summary of issues arising from the scenarios

The following issues arise from the scenarios presented in clauses 5.3.3, 5.3.4 and 5.3.5 above:

1. Address translation between private and public IPv4 address spaces for both signalling and bearer path;

See considerations in clause 5.3.1.2.

2. Address translation and protocol translation between IPv4 and IPv6 for both signalling and bearer path;

As per the considerations under point 1) above, NAT- and ALG-based address and protocol translations shall be avoided whenever possible. The need for address and protocol translation between IPv4 and IPv6 is expected to be limited for the following two cases:

- An IPv4 IM CN subsystem interconnecting with IPv6 IMS networks;
- External non-3GPP IPv4 SIP networks interconnecting with IPv6 IMS networks;

TS 23.228 [4] specifies the architecture as described in clause 5.3.1.1

Additionally, some scenarios (as per clause 5.3.5) might need IP version interworking between the P-CSCF and the S-CSCF. However, it is desired to avoid IP version interworking between P-CSCF and S-CSCF. See clause 5.3.5.2 for details.

3. Address translation and protocol translation for the bearer path;

4. IP version used on the connection between IM CN subsystems, both in roaming and interworking scenarios;

It is recommended for IMS networks to apply an IP version for interconnecting to other networks that minimizes the need for IP address and/or protocol translation. This can be achieved if vast majority of operators migrate towards using IPv6 as early as possible to avoid the need for address (and protocol) translation.

NOTE 1: Early IMS deployments using public IPv4 addressing for their network elements and UEs can interconnect with each other without address translation.

5. IP version used by a dual-stack UE to access the IM CN subsystem in case of IMS roaming;

See clause 5.2.2.1.

6. Use of IMS in the home network through GPRS roaming in a network, which does not support IPv6 PDP contexts.

It is recommended for GPRS networks offering IMS access capabilities to offer support for IPv6 PDP Contexts (i.e. upgrading the SGSNs to support IPv6 type of PDP context).

Alternatively, roaming UEs using IPv6 to connect to their home IMS network would need to use some IPv6-in-IPv4 tunnelling mechanism in the UE (e.g. ISATAP [8], see clause 5.3.4.3). However, such tunnelling solutions would not work well with QoS differentiation mechanisms (e.g. Service Based Local Policy) of the core network.

NOTE 2: Issue 6 is not directly related to IPv4 based IMS implementations.

5.3.7 IP version interworking for services

5.3.7.1 Application servers

Any interworking solution needs to consider the support for Application Servers. Application Servers may be dual stack or support only IPv6 or only IPv4.

5.3.7.2 Interworking support in dual stack IM CN subsystem

A dual stack IM CN subsystem and dual stack application servers may provide the necessary support for interworking between IP versions.

In particular, some IMS based services do not involve any media component but are based on SIP signalling only. Important examples are immediate messaging as described in clause 5.16.1 of TS 23.228 [4] and Presence as described in TS 23.141 [5]. In such cases SIP signalling does not contain any IP addresses which would require a SIP-ALG. The dual stack IM CN subsystem can provide the necessary interworking: each entity forwards the SIP message using the appropriate IP version. Thus the service can be provided without any additional NAT in the network. This allows e.g. immediate messaging between an IPv4 UE and an IPv6 UE or allows a watcher with an IPv6 UE to subscribe to the presence information of a presentity publishing from a IPv4 UE, or vice versa. This is illustrated in figures 5-12a, 5-12b and 5-13 below.

Figures 5-12a and 5-12b illustrate different scenarios for interworking support in dual stack IM CN subsystem. If the originating S-CSCF supports dual stack, the IP version interworking can occur on the originating side, if the terminating S-CSCF supports dual stack, the IP version interworking can also occur on the terminating side.

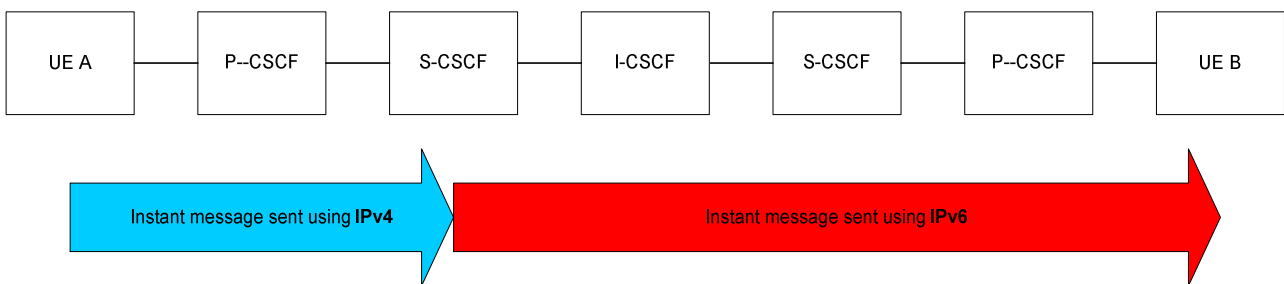


Figure 5-12a: Example with dual stack IM CN subsystem and Immediate Messaging (originating S-CSCF is dual stack)

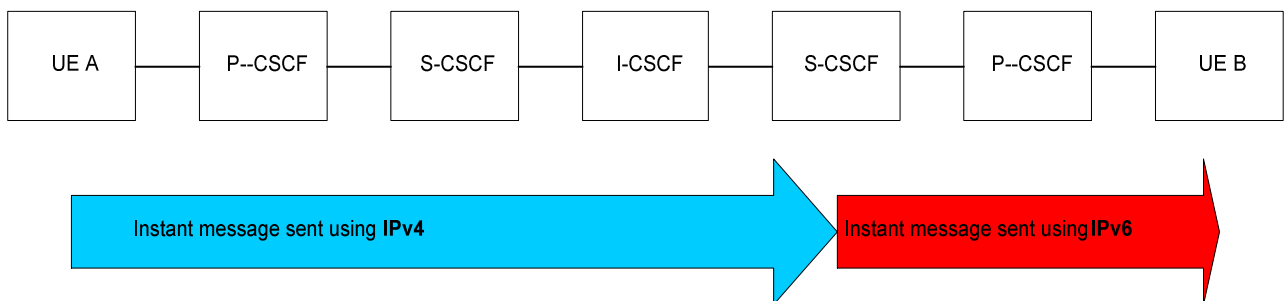


Figure 5-12b: Example with dual stack IM CN subsystem and Immediate Messaging (terminating S-CSCF is dual stack)

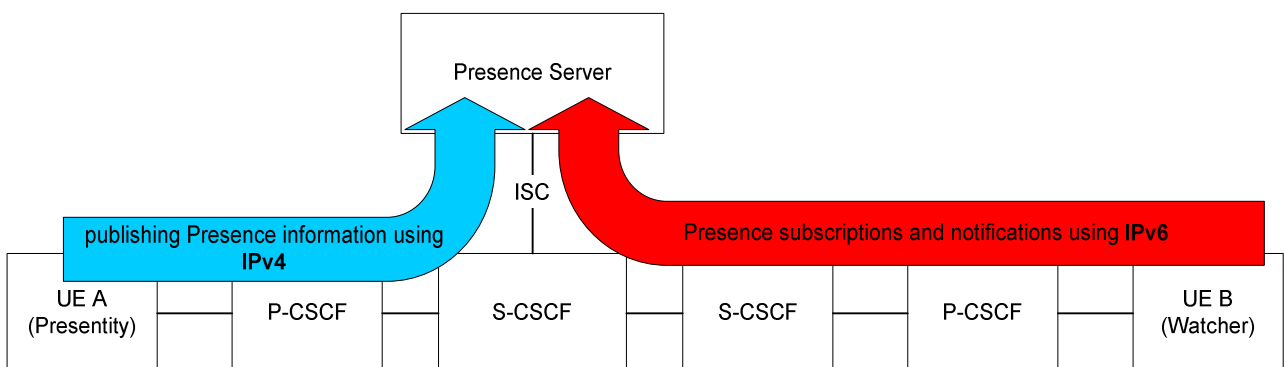


Figure 5-13: Example with dual stack IM CN subsystem and Presence Server

NOTE: In this scenario, if Presence information contains an IP address, then the IP address is not translated but provided as is to the watcher.

5.3.7.3 Access to network services

Access to IMS network services provided for example by MRFP or IM-MGW is done via the Mb reference point, see TS 23.002 [7a]. In the interest of interworking, the entities providing network services may support IPv6 only, IPv4 only or may be dual-stack. Accordingly, the Mb reference point should allow IPv4 access to network services.

5.4 Migration scenarios

5.4.1 IPv4 UE and IPv6 IM CN subsystem

Due to migration, there may be cases where some IMS users still connect to the IMS using their IPv4 UE although the IM CN subsystem has evolved from IPv4 to IPv6.

In this case, the P-CSCF needs to support IPv4 towards the UE. An intermediary node between the UE and the P-CSCF would otherwise jeopardise the security association between the UE and P-CSCF. If the S-CSCF already evolved to IPv6, a NAT between P-CSCF and S-CSCF could provide the possibility for IPv4 UEs to register at an IPv6 S-CSCF with an IPv6 IP address.

While the detailed impact of this mechanism has not been studied within the TR, it is understood that it might have negative impact on security mechanisms, charging correlation and other services or capabilities that make use of the IP address. In line with the overall recommendation to avoid NATs, it is thus recommended to provide the dual stack capability in all IM CN subsystem nodes instead. Also, a NAT in such a scenario would not work on a per session basis, but would need to convert address information on a permanent basis.

The early deployment of IMS dual stack UEs facilitates the migration from IPv4 to IPv6, as it avoids the issue mentioned in this clause.

5.4.2 A partially migrated IPv4 to IPv6 IM CN subsystem

While the final objective is a full scale IPv6 IMS, a combination of IPv4 and IPv6 IM CN subsystem elements may coexist temporarily in the same network due to migration from IPv4 to IPv6. It is for further study how to ensure interworking in this case.

One approach would be to logically divide the network in two parts during the migration period and temporarily deploy NATs between the two parts using the interworking mechanisms described in clause 5.3.

Another approach would be to deploy dual stack capable IMS networks already from the initial phase, which would avoid the issues described in this clause.

In general, it can be seen that dual-stack IMS core network deployments make the migration to a full scale IPv6 IMS considerably easier.

5.4.3 Migration aspects for services

5.4.3.1 Application Servers

Any migration solution needs to consider the support for Application Servers.

5.4.3.2 Migration support in dual stack IM CN subsystem

An IPv4 IM CN subsystem (including application servers), which evolves to a dual stack IM CN subsystem, may provide the necessary support for both IPv4 UEs and IPv6 UEs. The considerations in clause 5.3.7.2 apply also to this scenario.

5.4.3.3 Access to network services

Any migration solution needs to consider the support in entities providing network services, such as MRFP and IM-MGW.

5.4.4 Example migration paths

Based on the considerations in this TR, the following could be example migration paths.

Operator A deploys an IPv4 based IM CN subsystem for the support of a few early server based IMS services. Operator(B) deploys a dual stack IM CN subsystem already for the earliest IMS services. In the initial phase, majority of the UEs available are IPv4 UEs, which support this limited set of services using IMS. In addition there may also be IMS dual stack UEs available. Later IMS dual stack UEs become more widely available and in addition support peer-to-peer services like voice. Gradually, operators A and B start to deploy more services over IMS. At some point the IM CN subsystem of operator A is migrated to a dual stack IM CN subsystem; the system can still support the early IPv4 UEs and the IMS dual stack UEs and in addition it is now possible to support IPv6 UEs. Finally the operators discontinue the support for IPv4 UEs and migrate to pure IPv6 IM CN subsystems.

6 Conclusions and recommendations

Interworking between IPv4 and IPv6 based IMS implementations and migration from IPv4 IMS to IPv6 IMS can and should be facilitated by specification of some of the relevant aspects.

For the specification of IPv4 IMS, the assumption should be made that the relevant roaming scenario for IPv4 is the GPRS roaming scenario with the GGSN in the home network.

If IPv4 is used in an early IMS implementation, there is the need for alternative or modified P-CSCF discovery as the mechanisms specified in TS 23.228 [4] cannot be applied as they are. It is recommended to follow the recommendations for P-CSCF discovery as described in clause 5.2.1.

It is recommended that SIP communication between UE and P-CSCF uses IPv4 or IPv6 without intermediaries changing the IP version.

For some services like PoC, Presence and immediate messaging, dual stack network elements like the PoC Server, the Presence Server or the S-CSCF can provide IP version interworking without use of NATs.

In general, the interworking architecture defined in TS 23.228 [4] with IMS-ALG and NATs (TrGWs) at the network border can be used in principle to support all kinds of IP address and protocol translations possibly needed between early IMS networks. In some cases, there may also be the need for IMS-ALGs and NATs within an IM CN subsystem, see clause 5.3.5.2.

The early deployment of IMS dual stack UEs facilitates migration significantly. To limit the options, it is recommended to specify the IMS dual stack UE behaviour for IMS access, as described in clause 5.2.2.1.

Network operators, who introduce 3GPP IMS using IPv6, have a strong interest that their GPRS roaming partners provide support for PDP contexts of PDP type IPv6 in the SGSN. Thus support of PDP type IPv6 in SGSNs facilitates migration of IMS towards IPv6.

When interconnecting GPRS networks (i.e. SGSN and GGSN) between operators as well as within an operator domain, NAT should not be used and clause 4.2 should be followed.

Annex A: Additional Information

This annex contains information that has been investigated during the development of the TR but has been considered not necessary for further development of the work (A.1) or the scenarios help better understand some end to end scenarios but not useful for further analysis within the feasibility study. But the information has been maintained as reference.

A.1 GPRS deployment scenarios

This clause contains GPRS deployment scenarios that are not considered as likely case for IPv4 based IMS deployment, as it is understood that use of GGSN in the home network may initially be operator's preferred option for IM CN subsystem.

Deployment of an infrastructure with GGSN in the visited network has been possible from standards point of view with the early GPRS systems. But from the information available today, it has not been realised yet in the deployed systems. Considering also that there is a growth of functionality interacting with the GGSNs and that the implications of a GGSN in the VPLMN are quite large (operational, charging, feature availability, maintenance, roaming agreements etc.) it seems like the visited GGSN scenario becomes even more delayed/unlikely.

So, the motivation of upgrading to an IPv6 system seems to be a much more a near term goal than deployment of the GGSN in visited networks. Hence it seems safe to only consider the scenarios where an IPv4 based IMS system always have the GGSN at home.

The general architecture arises from this scenario would look like the following:

In this roaming access scenario, the visited network can be dual stack, supporting both IPv4 and IPv6, while the home network supports only the opposing version of IP. The UE may be IPv4 only or may be IMS dual stack UE.

Further elaboration of the scenarios are described in the following clauses.

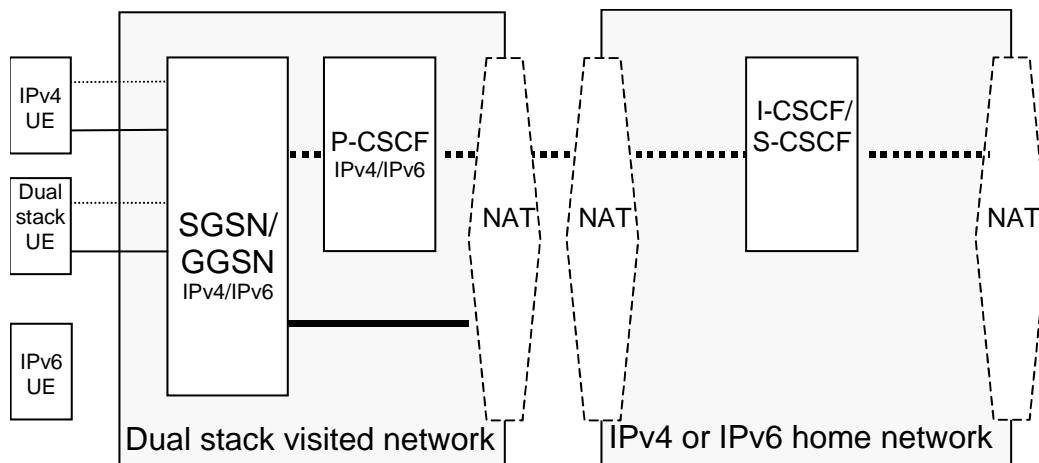


Figure A.1: IMS roaming access – dual stack visited network, IPv4 (or IPv6) home network

Routing of bearer path is for further study – bearer path may be:

- Routed to home network and from there onwards towards the destination network;
- Routed from the visited network directly towards the destination network.

A.1.1 IMS roaming access – IPv4 visited network, IPv4 home network

The call leg is split between different IPv4 networks in a roaming scenario. The GGSN and P-CSCF are in the visited IPv4 network; the I-CSCF and S-CSCF are in the home IPv4 network. The UE in the IPv4 network may be IPv4 only or may be IMS dual stack UE. If either UE is IPv6 only then this scenario can not be supported.

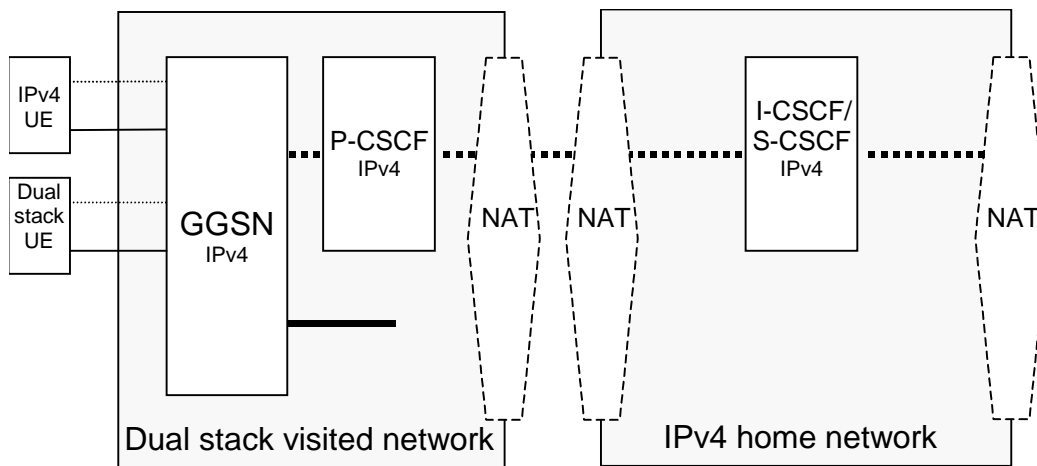


Figure A.1-1: IMS roaming access – IPv4 visited network, IPv4 home network

Issues described in clause A.1 with respect to routing of bearer path are applicable for this scenario as well.

This scenario is not further considered due to the assumption that GGSN at home is the most likely scenario.

A.1.2 IMS roaming access - IPv4 visited network, IPv6 home network

The GGSN and P-CSCF are in the visited IPv4 network; the I-CSCF and S-CSCF are in the home IPv6 network. The UE must support IPv6 in order to interoperate with its Home Network and must support IPv4 in order to interoperate with the IPv4 Visited Network i.e. it is assumed to be IMS dual stack UE. If the UE is IPv6 only (or IPv4 only) then this scenario can not be supported.

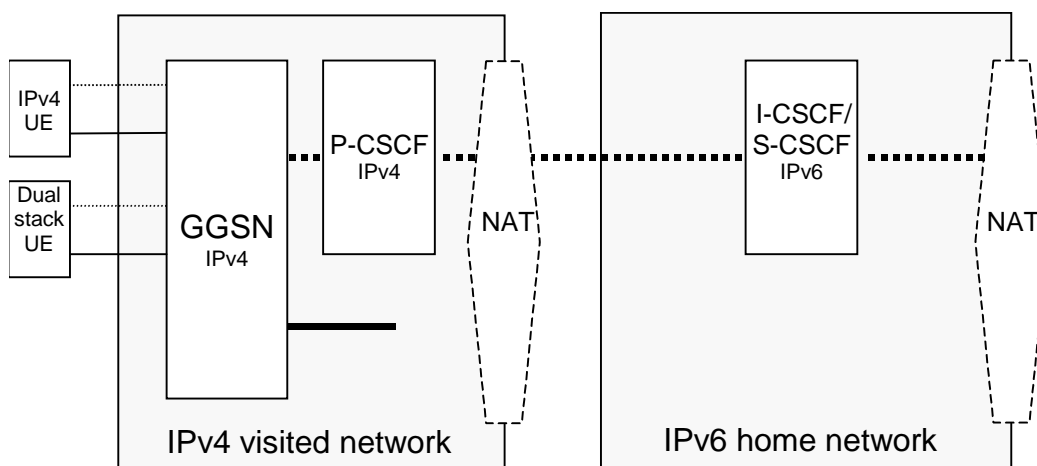


Figure A.1-2: IMS roaming access – IPv4 visited network, IPv6 home network

Issues described in clause A.1 with respect to routing of bearer path are applicable for this scenario as well.

This scenario assumes an IMS dual stack UE, which can access the visited IM CN subsystem with IPv4, but when at home it uses IPv6 to access the home IM CN subsystem.

This scenario is not further considered due to the assumption that GGSN at home is the most likely scenario.

A.1.3 IMS roaming access - IPv6 visited network, IPv4 home network

The GGSN and P-CSCF are in the visited IPv6 network; the I-CSCF and the S-CSCF are in the home IPv4 network. The UE in the IPv6 network must support IPv4 in order to interoperate with its Home Network and must support IPv6 in order to interoperate with the visited network. If the UE is IPv6 only (or IPv4 only) then this scenario can not be supported.

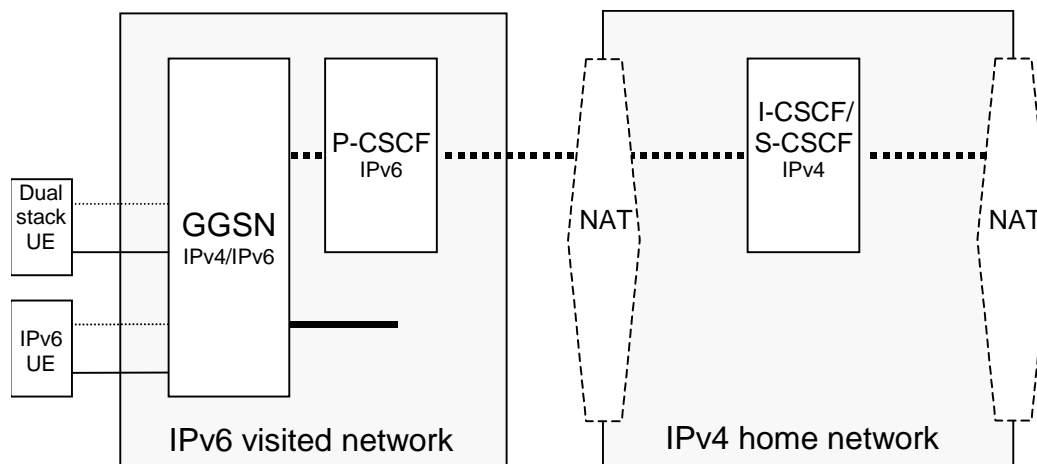


Figure A.1-3: IMS roaming access - IPv6 visited network, IPv4 home network

Issues described in clause A.1 with respect to routing of bearer path are applicable for this scenario as well.

This scenario assumes an IMS dual stack UE, which can access the visited IM CN subsystem with IPv6, but when at home it uses IPv4 to access the home IM CN subsystem.

This scenario is not further considered due to the assumption that GGSN at home is the most likely scenario.

A.1.4 IMS roaming access - IPv4 visited network, dual stack home network

GGSN and P-CSCF are in the IPv4 visited network. The I-CSCF and S-CSCF are in the home network which supports dual stack. The UE may be IPv4 only or may be IMS dual stack UE. If the UE is IPv6 only then this scenario can not be supported.

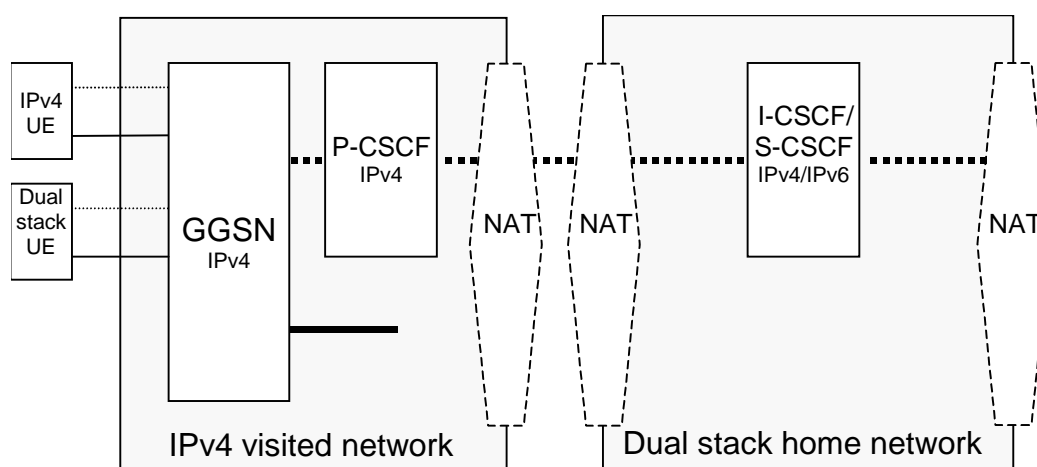


Figure A.1-4: IMS roaming access - IPv4 visited network, dual stack home network

Issues described in clause A.1 with respect to routing of bearer path are applicable for this scenario as well.

This scenario is not further considered due to the assumption that GGSN at home is the most likely scenario.

A.2 End to End scenarios

This clause describes some end to end scenarios for IP version interworking for IMS cases.

A.2.1 Non-roaming - IPv4 IM CN subsystem with IPv6 IM CN subsystem

IPv4 IM CN subsystem and IPv6 IM CN subsystem are in different networks; each leg of the session is contained solely in an IPv4 or IPv6 network. Either network may originate or terminate sessions. The UE in the IPv4 network may be IPv4 only or may be IMS dual stack UE (if it is IPv6 only then this scenario can not be supported).

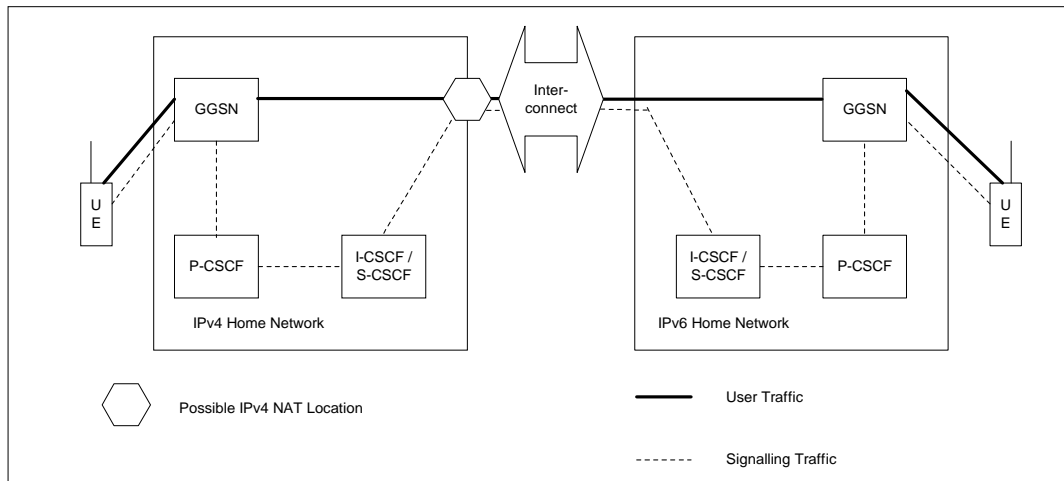


Figure A.2-1: Non-roaming IPv4 IM CN subsystem with IPv6 IM CN subsystem

In this scenario:

- clause 5.2.2.1 and 5.2.2.2 apply to the UE accessing the IPv4 network;
- clause 5.2.2.1 may apply to the UE accessing the IPv6 network;
- clause 5.3.1.1 applies to the interconnection between the networks.

A.2.2 Non-roaming - IPv4 IM CN subsystem with IPv4 IM CN subsystem

The two IPv4 IM CN subsystems are in different networks and hence may use overlapping private IPv4 address spaces. The UE in the IPv4 network may be IPv4 only or may be IMS dual stack UE. If either UE is IPv6 only then this scenario can not be supported.

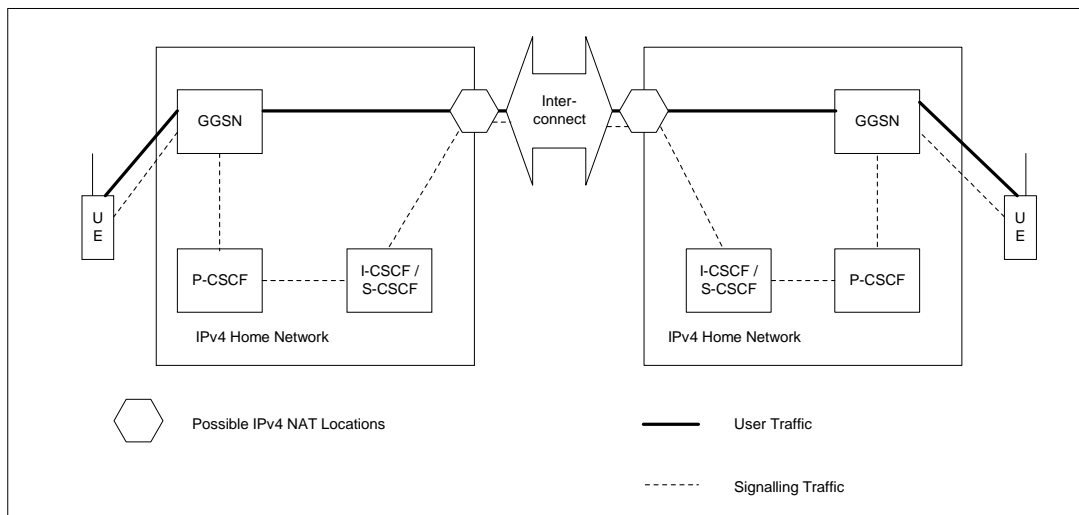


Figure A.2-2: Non-roaming IPv4 IM CN subsystem with IPv4 IM CN subsystem

In this scenario clause 5.2.2.1 and 5.2.2.2 apply to the UEs accessing the IPv4 networks.

A.2.3 Non-roaming IPv4 IM CN subsystem with dual stack IM CN subsystem

The two IM CN subsystems are in different networks. One IM CN subsystem is supporting IPv4 only whereas the second IM CN subsystem is supporting both IPv4 and IPv6. Either network may originate or terminate sessions. The dual stack IMS determines that it is in interacting with an IPv4 IMS and thus uses IPv4 at the network interconnection. The UE in the IPv4 network may be IPv4 only or may be IMS dual stack UE (if it is IPv6 only then this scenario can not be supported).

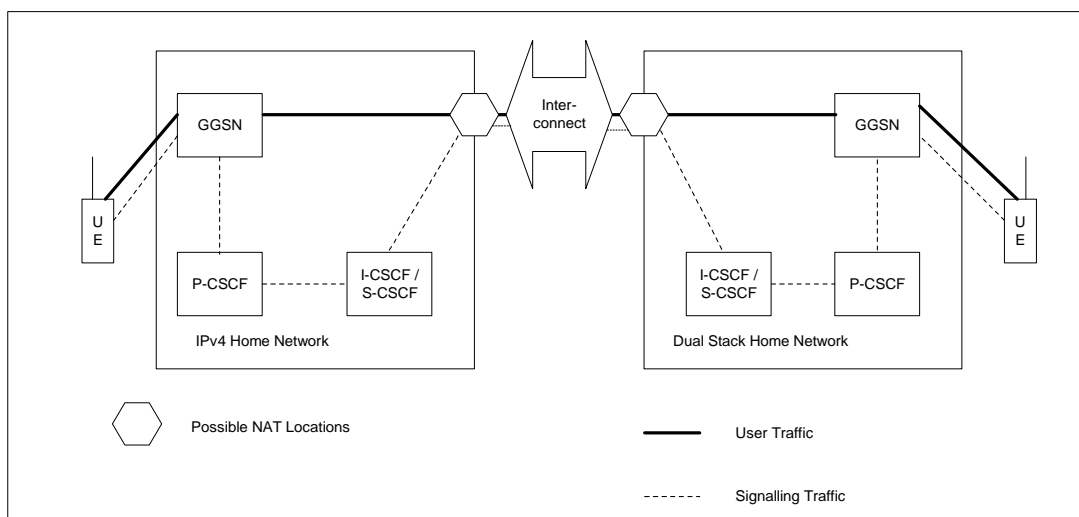


Figure A.2-3: Non-roaming IPv4 IM CN subsystem with Dual Stack IM CN subsystem

In this scenario clause 5.2.2.1 and 5.2.2.2 apply to the UE accessing the IPv4 network.

Clause 5.2.1 is applicable to the interconnection between networks, if IPv6 is used in the dual stack home network.

Even if the UE in the dual stack network is an IMS dual stack UE, the following needs to be considered:

- If the UE has registered with IPv4, then NAT may be needed at the network borders if private addressing is used in the IMS networks.

- If the UE has registered with IPv6, then the dual stack home network will use IPv6 for SIP communication towards the UE, even if it is part of a communication with an IPv4 network.

A.2.4 Non-roaming dual stack IM CN subsystem with dual stack IM CN subsystem

The two IM CN subsystems are in different networks. Both IM CN subsystems are dual stack. The UEs may be IPv4 only, IPv6 only, or may be IMS dual stack UEs.

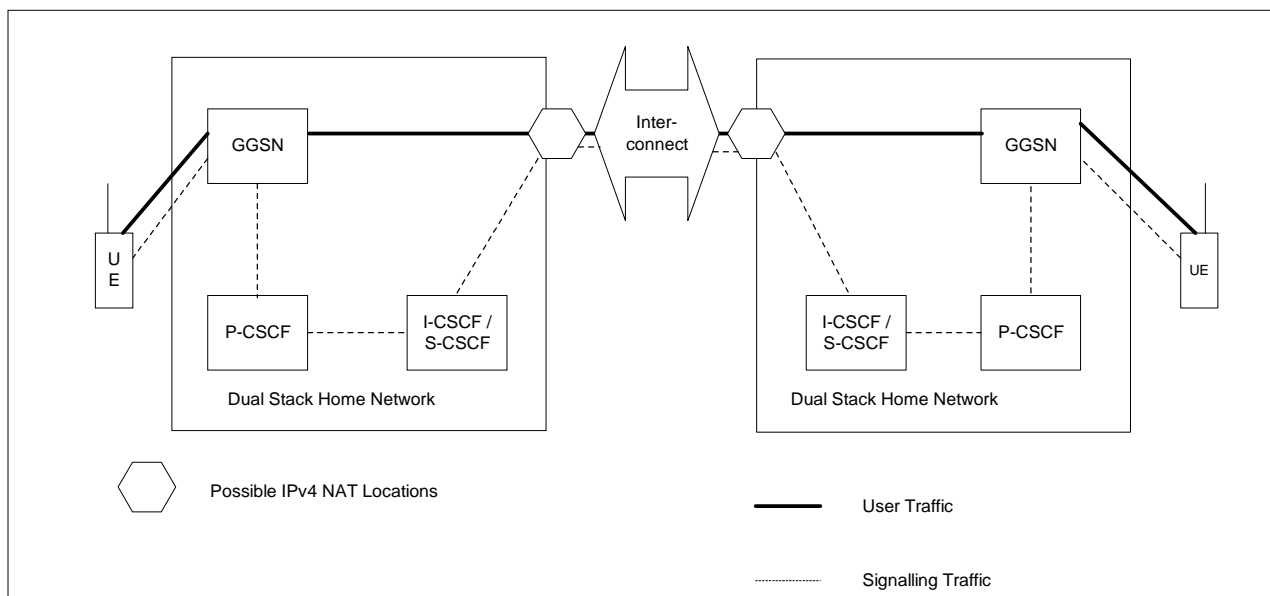


Figure A.2-4: Non-roaming Dual Stack IM CN subsystem with Dual Stack IM CN subsystem

A.2.5 Non-roaming IPv6 IM CN subsystem with dual stack IM CN subsystem

The two IM CN subsystems are in different networks. One IM CN subsystem is supporting IPv6 only whereas the second IM CN subsystem is supporting both IPv4 and IPv6. Either network may originate or terminate sessions. The dual stack IMS determines that it is interacting with an IPv6 IMS and thus uses IPv6 at the network interconnection. The UE in the IPv6 network may be IPv6 only or may be IMS dual stack UE (if it is IPv4 only then this scenario can not be supported).

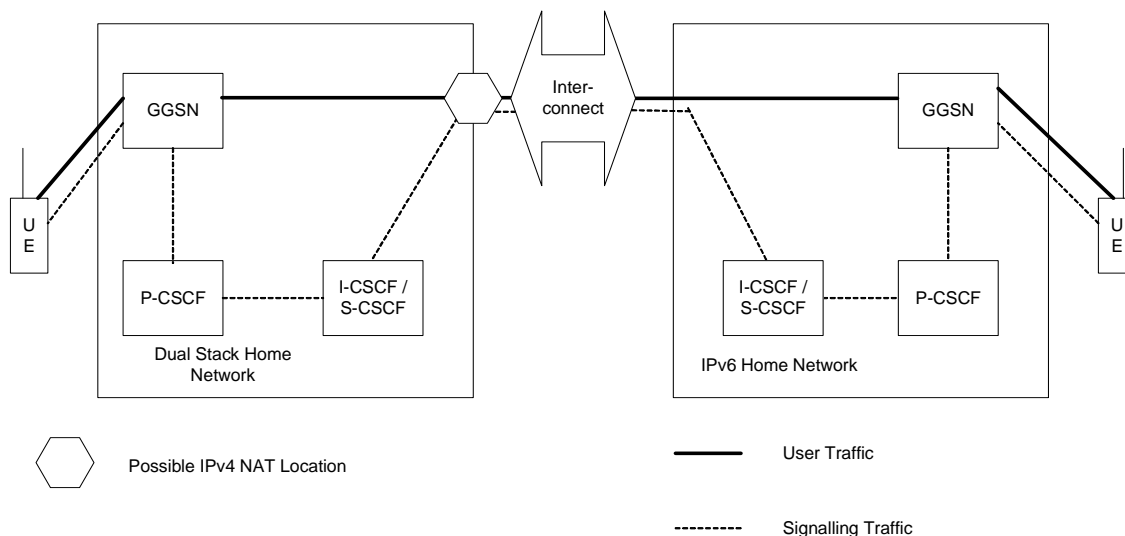


Figure A.2-5: Non-roaming IPv6 IM CN subsystem with Dual Stack IM CN subsystem

If the UE in the dual stack network is an IMS dual stack UE, which has registered with IPv4, then the dual stack home network will use IPv4 for SIP communication towards the UE, even if even if it is part of a communication with an IPv6 network.

Annex B: Change history

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2004-06	SP-24	SP-040337	-	-	-	Raised to v.6.0.0 after approval at SA#24	6.0.0
2004-09	SP-25	SP-040530	000 1	-	-	IPv4 access to multimedia services and Mb reference point	6.1.0
2004-09	SP-25	SP-040530	000 3	1	-	Corrections to scenario – IPv4 visited and IPv6 home	6.1.0
2004-12	SP-26	SP-040761	000 4	1	-	Clarification to the Interworking support in dual stack IM CN subsystem	6.2.0
2005-03	SP-27	SP-050115	000 5	1	-	P-CSCF discovery	6.3.0
2005-09	SP-29	SP-050476	000 6	1	-	P-CSCF address format when configured via DM	6.4.0
2007-06	-	-	-	-	-	Update to Rel-7 version (MCC)	7.0.0
2008-12	SP-42	-	-	-	-	Update to Rel-8 version (MCC)	8.0.0
2009-12	SP-46	-	-	-	-	Update to Rel-9 version (MCC)	9.0.0
2011-03	SP-51	-	-	-	-	Update to Rel-10 version (MCC)	10.0.0
2012-09	-	-	-	-	-	Update to Rel-11 version (MCC)	11.0.0
2014-09	SP-65	-	-	-	-	Update to Rel-12 version (MCC)	12.0.0
2015-12	-	-	-	-	-	Update to Rel-13 version (MCC)	13.0.0
2017-03	-	-	-	-	-	Update to Rel-14 version (MCC)	14.0.0
2018-06	SP-80	-	-	-	-	Update to Rel-15 version (MCC)	15.0.0
2020-07	SP-88E	-	-	-	-	Update to Rel-16 version (MCC)	16.0.0
2022-03	SP-95E	-	-	-	-	Update to Rel-17 version (MCC)	17.0.0

History

Document history		
V17.0.0	April 2022	Publication