3GPP TR 24.819 V7.0.0 (2005-12)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Core Network;
Protocol impact from providing IMS services via fixed broadband;
Stage 3
(Release 7)

Keywords

IMS, SIP, fixed broadband access

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Contents

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.

1 Scope

The present document is a temporary container for the functional models, flows and protocol details for the IM CN subsystem behaviour when providing IMS services via fixed broadband access. This service is based on the Session Initiation Protocol (SIP), the Session Description Protocol (SDP), other protocols, the Gq interface and the Cx interface. The contents of this report will be moved into appropriate 3GPP Technical Specifications.

Editor's note: The "other protocols" that are mentioned here need to be listed in detail, in order to replace the phrase "other protocols".

Editor's note: This TR will not be published.

The document focuses on scenarios where a non-3GPP terminal is connected via a fixed broadband access network to the IMS.

Where possible the present document specifies the requirements for the above mentioned protocols by reference to specifications produced by the IETF within the scope of SIP, SDP and other protocols, either directly, or as modified by 3GPP specifications. Where this is not possible, extensions are defined within the present document..

The present document includes information applicable to network operators, service providers and manufacturers.

Editor's note: Agreed material is held in this TR for an interim period of time, and the material is transferred into release 7 versions of the corresponding specifications at a later time. This has the advantage that:

It creates a location where the material may stabilise outside a document under CR control, thus fulfilling the function of the original annexes in the IM CN subsystem documents.

It provides a single specification for all changes to the IM CN subsystem coming from the WID “Protocol impact from providing IMS services via fixed broadband”.

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] 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3"..

[2] 3GPP TS 24.228: "Signalling flows for the IP multimedia call control based on SIP and SDP; Stage 3".

[3] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[4] IETF RFC 3261: "SIP: Session Initiation Protocol".

[5] IETF RFC 3312: "Integration of Resource Management and Session Initiation Protocol (SIP)".

[6] IETF RFC 3262: "Reliability of Provisional Responses in Session Initiation Protocol (SIP)".

[7] IETF RFC 3311: "The Session Initiation Protocol (SIP) UPDATE Method".

[8] IETF RFC 3264: "An Offer/Answer Model with Session Description Protocol (SDP)".

[9] 3GPP TS 29.208: "End to end Quality of Service (QoS) signalling flows".

[10] 3GPP TS 32.225: "Telecommunication management; Charging management; Charging data description for the IP Multimedia Subsystem (IMS)".3 Definitions and abbreviations

[11] 3GPP TS 29.209: "Policy control over Gq interface".

Editor's note: The following references are needed for material in clause 5 of this specification. The numbering of these references is according to the order in 24.229 and is therefore not consecutive.

[20F] RFC 2132 (March 1997): "DHCP Options and BOOTP Vendor Extensions".

Editor's note: The following reference is needed for material in clause 5 of this specification. The numbering of these reference is according to the order in 24.147 and is therefore not consecutive.

[27A] RFC 3263 (June 2002): " Session Initiation Protocol (SIP): Locating SIP Servers".

[33] RFC 3891 (September 2004): "The Session Inititation Protocol (SIP) "Replaces" Header".

[35A] RFC 3361 (August 2002): "Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers".

[40A] IETF RFC 2131 (March 1997): “Dynamic host configuration protocol”.

[41] RFC 3319 (July 2003): "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers".

[41A] IETF RFC 3361 (August 2002): “Dynamic Host Configuration Protocol (DHCP-for-IPv4)- Option for Session Initiation Protocol (SIP) Servers”.

Editor's note: The following references are needed for material in clause 5 of this specification. The numbering of these references is according to the order in 24.229 and is therefore not consecutive.

[64] RFC 3842 (August 2004) "A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)"

[80] draft-ietf-sip-history-info-06 (Janary 2005): "An Extension to the Session Initiation Protocol for Request History Information".

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

[81] draft-elwell-sipping-redirection-reason-02 (June 2005): "SIP Reason header extension for indicating redirection reasons".

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

Editor's note: The following references are needed for material in clause 5 of this specification. The numbering of these references is according to the order in 24.229 and is therefore not consecutive.

[82] DSL Forum TR-092 "Broadband Remote Access Server (BRAS) Requirements Document".

Editor's note: The following references are needed for material in clause 5 of this specification. The numbering of these references is according to the order in 24.229 and is therefore not consecutive.

[83] draft-jesske-sipping-etsi-ngn-reason-00 (July 2005) "Use of the Reason header filed in Session Initiation Protocol (SIP) responses”

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

Editor's note: The following references are needed for material in clause 8 of this specification. The numbering of these references is according to the order in 29.163 and is therefore not consecutive.

[60] DRAFT ETSI TS 183 004 Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN Signalling Control Protocol; Communication Diversion (CDIV), PSTN/ISDN simulation services

Editor's note: The above document cannot be formally referenced until it is published as TISPAN TS

[61] DRAFT ETSI TS 183 005 Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN Signalling Control Protocol; Conference call (CONF) PSTN/ISDN simulation services

Editor's note: The above document cannot be formally referenced until it is published as TISPAN TS

[62] DRAFT ETSI TS 183 006 Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN Signalling Control Protocol; Message Waiting Indication (MWI), PSTN/ISDN simulation services

Editor's note: The above document cannot be formally referenced until it is published as TISPAN TS

[63] DRAFT ETSI TS 183 007 Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN Signalling Control Protocol; Originating Identification Presentation (OIP) and Originating Identification Restriction (OIR); PSTN/ISDN simulation services

Editor's note: The above document cannot be formally referenced until it is published as TISPAN TS

[64a] DRAFT ETSI TS 183 008 Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN Signalling Control Protocol; Terminating Identification Presentation (TIP) and Terminating Identification Restriction (TIR); PSTN/ISDN simulation services

Editor's note: The above document cannot be formally referenced until it is published as TISPAN TS

[65] DRAFT ETSI TS 183 009 Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN Signalling Control Protocol; Communication Waiting (CW), PSTN/ISDN simulation services

Editor's note: The above document cannot be formally referenced until it is published as TISPAN TS

[66] DRAFT ETSI TS 183 011 Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN Signalling Control Protocol; Communication Hold (HOLD) PSTN/ISDN simulation services

Editor's note: The above document cannot be formally referenced until it is published as TISPAN TS

[67] Draft ETSI TS 183 012 Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN Signalling Control Protocol; Anonymous Communication Rejection (ACR) and Communication Barring (CB) PSTN/ISDN simulation services

Editor's note: The above document cannot be formally referenced until it is published as TISPAN TS

[68] DRAFT ETSI TS 183 013 Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN Signalling Control Protocol; Advice of Charge (AoC) (AOC) PSTN/ISDN simulation services

Editor's note: The above document cannot be formally referenced until it is published as TISPAN TS

[69] DRAFT ETSI TS 183 015 Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN Signalling Control Protocol; Completion of Communications of Busy Subscriber (CCBS) PSTN/ISDN simulation services

Editor's note: The above document cannot be formally referenced until it is published as TISPAN TS

[70] DRAFT ETSI TS 183 016 Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN Signalling Control Protocol; Malicious Communication Identification (MCID) PSTN/ISDN simulation services

Editor's note: The above document cannot be formally referenced until it is published as TISPAN TS

3 Definitions, symbols and abbreviations

3.1 Definitions

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

3.2 Symbols

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

3.3 Abbreviations

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

AMR	Adaptive Multi-Rate
AS	Application Server
BRAS	Broadband Remote Access Server
CLF	Connectivity Session Location Function
CN	Core Network
CSCF	Call Session Control Function
DSL	Digital Subscriber Line
FQDN	Fully Qualified Domain Name
HSS	Home Subscriber Server
HTTP	Hyper Text Transfer Protocol
I-CSCF	Interrogating CSCF
IM	IP Multimedia
IMS	IP Multimedia CN subsystem
IP	Internet Protocol
IP-CAN	IP-Connectivity Access Network
MGCF	Media Gateway Control Function
MRFC	Multimedia Resource Function Controller
MRFP	Multimedia Resource Function Processor
NASS	Network Attachment Subsystem
NGN	Next Generation Network
PVC	Permanent Virtual CircuitSDP Session Description Protocol
SBLP	Service Based Local Policy
P-CSCF	Proxy CSCF
PSI	Public Service Identity
S-CSCF	Serving CSCF
SDP	Session Description Protocol
SIP	Session Initiation Protocol
UE	User Equipment
xDSL	refers to different variations of DSL, such as ADSL, HDSL

4 IMS services via fixed broadband overview

Editor's note: This is a introductory clause to the TR and is not intended to be introduced to any other 3GPP Specification. This clause shall give an overview of IMS services when provided via fixed broadband access.

5 Application Usage of SIP

Editor's note: This clause is under the responsibility of CT1. Material for this clause must be submitted to CT1.

Editor's note: This clause will cover requirements from providing IMS via fixed broadband with regards to the usage of SIP.

5.1 Profiles of IETF RFCs for 3GPP usage

Editor's note: It is intended that material from this clause will be added to Annex A of TS 24.229.

Table A.4 of 3GPP TS 24.229 is modified with the following additional rows:

	Extensions			
26H	application of the privacy option "history" such that privacy of the History-Info header is provided by the network?	[80] 7.2	c37	c37
47	an extension to the session initiation protocol for request history information?	[80]	o	o
48	the Reason header field in Responses	[83]	o	o
49	An SIP Reason header extension for indicating redirection/ communication diversion reasons?	[81]	o	c38
c37 c38	IF A.4/47 THEN o.3 ELSE n/a. IF A.4/47 THEN m ELSE n/a - - an SIP Reason header extension for indicating redirection/ communication diversion reasons.			

Table A.4A of 3GPP TS 24.229 is modified with the following additional row:

8	message-summary package?	[64]	c1	c23	[64] 3	c2	c24
c23: c24:	IF (A.3/1 OR A.3/7A OR A.3/7B) AND A.4/23 THEN o ELSE n/a - - UE, AS acting as terminating UA, or redirect server, AS acting as originating UA all as subscriber of event information. IF (A.3/1 OR A.3/7A OR A.3/7B) AND A.4/22 THEN o ELSE n/a - - UE, AS acting as terminating UA, or redirect server, AS acting as originating UA all as notifier of event information.						

Table A.46 of 3GPP TS 24.229 is modified with the following additional row:

20A	History-Info	[80] 4.1	c31	c31	[80] 4.1	c31	c31
c31:	IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.						

Table A.49 of 3GPP TS 24.229 is modified with the following additional row:

11FA	Reason	[83]	c14	c14	[83]	c15	c15
20A	History-Info	[80] 4.1	c13	c13	[80] 4.1	c13	c13
c13: c14: c15:	IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information. IF A.4/48 AND (A3/6 OR A3/7 OR A3/8) THEN o ELSE n/a - - the Reason header field in Responses. IF A.4/48 THEN o ELSE n/a - - the Reason header field in Responses.						

Table A.62A of 3GPP TS 24.229 is modified with the following additional row:

14A	History-Info	[80] 4.1	c27	c27	[80] 4.1	c27	c27
c27:	IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.						

Table A.62C of 3GPP TS 24.229 is modified with the following additional row:

10A	History-Info	[80] 4.1	c13	c13	[80] 4.1	c13	c13
12FA	Reason	[83]	c14	c14	[83]	c15	c15
c13:	IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.						
c14:	IF A.4/48 AND (A3/6 OR A3/7) THEN o ELSE n/a - - the Reason header field in Responses.						
c15:	IF A.4/48 THEN o ELSE n/a - - the Reason header field in Responses.						

Table A.63 of 3GPP TS 24.229 is modified with the following additional row:

15A	History-Info	[80] 4.1	c22	c22	[80] 4.1	c22	c22
c22:	IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.						

Table A.77 of 3GPP TS 24.229 is modified with the following additional row:

16A	History-Info	[80] 4.1	c25	c25	[80] 4.1	c25	c25
c25:	IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.						

Table A.80 of 3GPP TS 24.229 is modified with the following additional row:

9A	History-Info	[80] 4.1	c13	c13	[80] 4.1	c13	c13
10FA	Reason	[83]	c14	c14	[83]	c15	c15
c13:	IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.						
c14:	IF A.4/48 AND (A3/6 OR A3/7) THEN o ELSE n/a - - the Reason header field in Responses.						
c15:	IF A.4/48 THEN o ELSE n/a - - the Reason header field in Responses						

Table A.104A of 3GPP TS 24.229 is modified with the following additional row:

17A	History-Info	[80] 4.1	c27	c27	[80] 4.1	c27	c27
c27:	IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.						

Table A.104C: of 3GPP TS 24.229 is modified with the following additional row:

10A	History-Info	[80] 4.1	c13	c13	[80] 4.1	c13	c13
c13:	IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.						

Table A.105 of 3GPP TS 24.229 is modified with the following additional row:

11A	History-Info	[80] 4.1	c24	c24	[80] 4.1	c24	c24
c24:	IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.						

Table A.108 of 3GPP TS 24.229 is modified with the following additional row:

8A	History-Info	[80] 4.1	c14	c14	[80] 4.1	c14	c14
10FA	Reason	[83]	c15	c15	[83]	c16	c16
c14: c15: c16:	IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information. IF A.4/48 AND (A3/6 OR A3/7) THEN o ELSE n/a - - the Reason header field in Responses. IF A.4/48 THEN o ELSE n/a - - the Reason header field in Responses						

Table A.119 of 3GPP TS 24.229 is modified with the following additional row:

17A	History-Info	[80] 4.1	c28	c28	[80] 4.1	c28	c28
c28:	IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.						

Table A.122 of 3GPP TS 24.229 is modified with the following additional row:

9A	History-Info	[80] 4.1	c9	c9	[80] 4.1	c9	c9
c9:	IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.						

Table A.134: of 3GPP TS 24.229 is modified with the following additional row:

16A	History-Info	[80] 4.1	c25	c25	[80] 4.1	c25	c25
c25:	IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.						

Table A.136 of 3GPP TS 24.229 is modified with the following additional row:

9A	History-Info	[80] 4.1	c13	c13	[80] 4.1	c13	c13
10FA	Reason	[83]	c14	c15	[83]	c15	c16
c13: c14: c15:	IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information. IF A.4/48 AND (A3/6 OR A3/7) THEN o ELSE n/a - - the Reason header field in Responses. IF A.4/48 THEN o ELSE n/a - - the Reason header field in Responses.						

Table A.162 of 3GPP TS 24.229 is modified with the following additional rows:

31H	application of the privacy option "history" such that privacy of the History-Info header is provided by the network?	[80] 7.2	c34	c34
57	an extension to the session initiation protocol for request history information?	[80]	o	o
58	the Reason header field in Responses	[83]	o	o
59	An SIP Reason header extension for indicating redirection/ communication diversion reasons?	[81]	o	c34
c34	IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.			

Table A.204 of 3GPP TS 24.229 is modified with the following additional row:

20A	History-Info	[80] 4.1	c43	c43	[80] 4.1	c43	c43
c43:	IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.						

Table A.207 of 3GPP TS 24.229 is modified with the following additional row:

9A	History-Info	[80] 4.1	c17	c17	[80] 4.1	c17	c17
11FA	Reason	[83]	c18	c18	[83]	c19	c19
c17: c18: c19:	IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information. IF A.162/58 THEN m ELSE n/a- - the Reason header field in Responses IF A.162/58 THEN i ELSE n/a- - the Reason header field in Responses						

Table A.218A of 3GPP TS 24.229 is modified with the following additional row:

14A	History-Info	[80] 4.1	c32	c32	[80] 4.1	c32	c32
c32:	IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.						

Table A.218C of 3GPP TS 24.229 is modified with the following additional row:

10A	History-Info	[80] 4.1	c16	c16	[80] 4.1	c16	c16
12FA	Reason	[83]	c17	c17	[83]	c18	c18
c16: c17: c18:	IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information. IF A.162/58 THEN m ELSE n/a- - the Reason header field in Responses IF A.162/58 THEN i ELSE n/a- - the Reason header field in Responses						

Table A.219 of 3GPP TS 24.229 is modified with the following additional row:

15A	History-Info	[80] 4.1	c25	c25	[80] 4.1	c25	c25
c25:	IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.						

Table A.233 of 3GPP TS 24.229 is modified with the following additional row:

16A	History-Info	[80] 4.1	c32	c32	[80] 4.1	c32	c32
c32:	IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.						

Table A.236 of 3GPP TS 24.229 is modified with the following additional row:

9A	History-Info	[80] 4.1	c16	c16	[80] 4.1	c16	c16
10FA	Reason	[83]	c17	c17	[83]	c18	c18
c16:	IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.						
c17:	IF A.162/58 THEN m ELSE n/a- - the Reason header field in Responses						
c18:	IF A.162/58 THEN i ELSE n/a- - the Reason header field in Responses						

Table A.260A of 3GPP TS 24.229 is modified with the following additional row:

16A	History-Info	[80] 4.1	c32	c32	[80] 4.1	c32	c32
c32:	IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.						

Table A.260C of 3GPP TS 24.229 is modified with the following additional row:

10A	History-Info	[80] 4.1	c16	c16	[80] 4.1	c16	c16
c16:	IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.						

Table A.261 of 3GPP TS 24.229 is modified with the following additional row:

11A	History-Info	[80] 4.1	c31	c31	[80] 4.1	c31	c31
c31:	IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.						

Table A.264 of 3GPP TS 24.229 is modified with the following additional row:

8A	History-Info	[80] 4.1	c15	c15	[80] 4.1	c15	c15
10FA	Reason	[83]	c16	c16	[83]	c17	c17
c15:	IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.						
c15:	IF A.162/58 THEN m ELSE n/a- - the Reason header field in Responses						
c16:	IF A.162/58 THEN i ELSE n/a- - the Reason header field in Responses						

Table A.275 of 3GPP TS 24.229 is modified with the following additional row:

17A	History-Info	[80] 4.1	c24	c24	[80] 4.1	c24	c24
c24:	IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.						

Table A.278 of 3GPP TS 24.229 is modified with the following additional row:

9A	History-Info	[80] 4.1	c12	c12	[80] 4.1	c12	c12
c12:	IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.						

Table A.290 of 3GPP TS 24.229 is modified with the following additional row:

16A	History-Info	[80] 4.1	c31	c31	[80] 4.1	c31	c31
c31:	IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.						

Table A.292 of 3GPP TS 24.229 is modified with the following additional row:

9A	History-Info	[80] 4.1	c15	c15	[80] 4.1	c15	c15
11FA	Reason	[83]	c16	c16	[83]	c17	c17
c15: c16: c17:	IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information. IF A.162/58 THEN m ELSE n/a- - the Reason header field in Responses IF A.162/58 THEN i ELSE n/a- - the Reason header field in Responses						

5.2 Interoperability with different IP-CAN

Editor's note: It is intended that material from this clause will be added as subclause 3A to TS 24.229.

Editor's note: References in this subclause are made according to the numbering of references in TS 24.229.

The IM CN subsystem can be accessed by UEs resident in different types of IP-CAN. The main body of this document, and annex A, are general to UEs and IM CN subsystems that are accessed using any type of IP-CAN. Requirements that are dependent on the type of IP-CAN are covered in annexes B for GPRS, Y for xDSL or in separate specifications.

5.3 Void

5.4 P-Access-Network-Info header

5.4.1 Introduction

Editor's note: It is intended that material from this clause will be added as subclause 7.2A.4.1 to TS 24.229.

Editor's note: References in this subclause are made according to the numbering of references in TS 24.229.

The P-Access-Network-Info header is extended to include specific information relating to particular access technologies.

5.4.2 Syntax

Editor's note: It is intended that material from this clause will be added as subclause 7.2A.4.2 to TS 24.229.

Editor's note: References in this subclause are made according to the numbering of references in TS 24.229.

The syntax of the P-Access-Network-Info header is described in RFC 3455 [52]. There may be additional coding rules for this header depending on the type of IP-CAN, according to access technology specific descriptions.

Table 7.3 describes 3GPP-specific extensions to the P-Charging-Vector header field defined in RFC 3455 [52].

Table 7.2: Syntax of extensions to P-Access-Network-Info header

```
access-type             = "IEEE-802.11a" / "IEEE-802.11b" / "3GPP-GERAN" / "3GPP-UTRAN-FDD" /
                          "3GPP-UTRAN-TDD" / "3GPP-CDMA2000" / "ADSL" / "ADSL2" / "ADSL2+" /
                          "RADSL" / "SDSL" / "HDSL" / "HDSL2" / "G.SHDSL" / "VDSL" / "IDSL" /
                          token
access-info             = cgi-3gpp / utran-cell-id-3gpp / dsl-location / extension-access-info
extension-access-info   = gen-value
cgi-3gpp                = "cgi-3gpp" EQUAL (token / quoted-string)
utran-cell-id-3gpp      = "utran-cell-id-3gpp" EQUAL (token / quoted-string)
dsl-location            = "dsl-location" EQUAL (token / quoted-string)
```

5.4.3 Additional coding rules for P-Access-Network-Info header

Editor's note: It is intended that material from this clause will be added as subclause 7.2A.4.3 to TS 24.229.

Editor's note: References in this subclause are made according to the numbering of references in TS 24.229.

The UE shall populate the P-Access-Network-Info header, where use is specified in subclause 5.1, with the following contents:

1) the access-type field set to one of "3GPP-GERAN","3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD", "3GPP-CDMA2000", "IEEE-802.11a", or "IEEE-802.11b", "ADSL", "ADSL2", "ADSL2+", "RADSL", "SDSL", "HDSL", "HDSL2", "G.SHDSL", "VDSL" or "IDSL" as appropriate to the radio/xDSL access technology in use.

Editor’s note: A P-CSCF generally may support more than one access network type. Where this information is inserted should be considered, because the end UE may not be aware of the access network type. Also it should be clarified what would be a potential application of the access network type information.

Editor’s note: Dynamically provisioned xDSL bearer(s), i.e., activation and modification of xDSL bearer(s), are for further study. Further contributions are needed to get more insight in the proper support of dynamic establishment of PVC connections.

2) if the access type field is set to "3GPP-GERAN", a cgi-3gpp parameter set to the Cell Global Identity obtained from lower layers of the UE. The Cell Global Identity is a concatenation of MCC, MNC, LAC and CI (as described in 3GPP TS 23.003 [3]). The value of "cgi-3gpp" parameter is therefore coded as a text string as follows:

   Starting with the most significant bit, MCC (3 digits), MNC (2 or 3 digits depending on MCC value), LAC (fixed length code of 16 bits using full hexadecimal representation) and CI (fixed length code of 16 bits using a full hexadecimal representation);

3) if the access type field is equal to "3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD" or "3GPP-CDMA2000", a "utran-cell-id-3gpp" parameter set to a concatenation of the MCC, MNC, LAC (as described in 3GPP TS 23.003 [3]) and the UMTS Cell Identity (as described in 3GPP TS 25.331 [9A]), obtained from lower layers of the UE, and is coded as a text string as follows:

   Starting with the most significant bit, MCC (3 digits), MNC (2 or 3 digits depending on MCC value), LAC (fixed length code of 16 bits using full hexadecimal representation) and UMTS Cell Identity (fixed length code of 28 bits).

4) if the access-type field set to one of "IEEE-802.11a" or "IEEE-WLAN-802.11b" the access info parameter is set to a null value. This release of this specification does not define values for use in this parameter

5) If the access-type field is set to one of "ADSL", "ADSL2", "ADSL2+", "RADSL", "SDSL", "HDSL", "HDSL2", "G.SHDSL", "VDSL", "IDSL", the access-info field shall contain a dsl-location parameter obtained from the CLF (see NASS functional architecture) and derived from the binding information (IP edge ID, allocated IP address, line ID).

Editor's note: The dsl-location field would need to be structured in a standardized format. This does not necessarily contain Geographic Location Information suitable to locate an emergency situation.

Editor’s note: The structure of the P-Access-Network-Info header should reflect the fact that the information is User Provided or Network Provided.

5.5 P-Charging-Vector header

5.5.1 Introduction

Editor's note: It is intended that material from this clause will be added as subclause 7.2A.5.1 to TS 24.229.

Editor's note: References in this subclause are made according to the numbering of references in TS 24.229.

The P-Charging-Vector header field is extended to include specific charging correlation information needed for IM CN subsystem functional entities.

5.5.2 Syntax

5.5.2.1 General

Editor's note: It is intended that material from this clause will be added as subclause 7.2A.5.2.1 to TS 24.229.

Editor's note: References in this subclause are made according to the numbering of references in TS 24.229.

The syntax of the P-Charging-Vector header field is described in RFC 3455 [52]. There may be additional coding rules for this header depending on the type of IP-CAN, according to access technology specific descriptions.

Table 7.3 describes 3GPP-specific extensions to the P-Charging-Vector header field defined in RFC 3455 [52].

Table 7.3: Syntax of extensions to P-Charging-Vector header

```
access-network-charging-info = (gprs-charging-info / i-wlan-charging-info / xdsl-charging-info /
      generic-param)
gprs-charging-info = ggsn SEMI auth-token [SEMI pdp-info-hierarchy] *(SEMI extension-param)
ggsn = "ggsn" EQUAL gen-value
pdp-info-hierarchy = "pdp-info" EQUAL LDQUOT pdp-info *(COMMA pdp-info) RDQUOT
pdp-info = pdp-item SEMI pdp-sig SEMI gcid [SEMI flow-id]
pdp-item = "pdp-item" EQUAL DIGIT
pdp-sig = "pdp-sig" EQUAL ("yes" / "no")
gcid = "gcid" 1*HEXDIG
auth-token = "auth-token" EQUAL 1*HEXDIG
flow-id = "flow-id" EQUAL "(" "{" 1*DIGIT COMMA 1*DIGIT "}" *(COMMA "{" 1*DIGIT COMMA 1*DIGIT
     "}")")"
extension-param = token [EQUAL token]
i-wlan-charging-info = "pdg"
xdsl-charging-info = bras SEMI auth-token [SEMI xDSL-bearer-info] *(SEMI extension-param)
bras = "bras" EQUAL gen-value
xDSL-bearer-info = "dsl-bearer-info" EQUAL LDQUOT dsl-bearer-info *(COMMA dsl-bearer-info) RDQUOT
dsl-bearer-info = dsl-bearer-item SEMI dsl-bearer-sig SEMI dslcid [SEMI flow-id]
dsl-bearer-item = "dsl-bearer-item" EQUAL DIGIT
dsl-bearer-sig = "dsl-bearer-sig" EQUAL ("yes" / "no")
dslcid = "dslcid" 1*HEXDIG
```

The access-network-charging-info parameter is an instance of generic-param from the current charge-params component of P-Charging-Vector header.

The access-network-charging-info parameter includes alternative definitions for different types access networks. The description of these parameters are given in the subsequent subclauses.

The access network charging information is not included in the P-Charging-Vector for SIP signalling that is not associated with a session.

When the access network charging information is included in the P-Charging-Vector and necessary information is not available from the Go/Gq interface reference points then null or zero values are included.

5.5.2.2 xDSL as IP-CAN

Editor's note: It is intended that material from this clause will be added as subclause 7.2A.5.2.4 to TS 24.229.

Editor's note: References in this clause are made according to the numbering of references in TS 24.229.

The access-network-charging-info parameter is an instance of generic-param from the current charge-params component of P-Charging-Vector header. The access-network-charging-info parameter includes alternative definitions for different types of access networks. This subclause defines the components of the xDSL instance of the access-network-charging-info.

For xDSL, there are the following components to track: BRAS address (bras parameter), media authorization token (auth-token parameter), and a set of dsl-bearer-info parameters that contains the information for one or more xDSL bearers.

The dsl-bearer-info contains one or more dsl-bearer-item values followed by a collection of parameters (dsl-bearer-sig, dslcid, and flow-id). The value of the dsl-bearer-item is a unique number that identifies each of the dsl-bearer-related charging information within the P-Charging-Vector header. Each dsl-bearer-info has an indicator if it is an IM CN subsystem signalling dsl-bearer (dsl-bearer-sig parameter), an associated DSL Charging Identifier (dslcid parameter), and a identifier (flow-id parameter). The flow-id parameter contains a sequence of curly bracket delimited flow identifier tuples that identify associated m-lines and relative order of port numbers in an m-line within the SDP from the SIP signalling to which the dsl-bearer charging information applies. For a complete description of the semantics of the flow-id parameter see 3GPP TS 29.207 [12] Annex C.

The format of the dslcid parameter is identical to that of ggsn parameter. On receipt of this header, a node receiving a dslcid shall decode from hexadecimal into binary format.

For a dedicated dsl-bearer for SIP signalling, i.e. no media stream requested for a session, then there is no authorisation activity or information exchange over the Go and Gq interfaces. Since there are no dslcid, media authorization token or flow identifiers in this case, the dslcid and media authorization token are set to zero and no flow identifier parameters are constructed by the PDF.

5.6 Handling of the IPCan

Editor's note: It is intended that material from this clause will be added as subclause 9.2.2 to TS 24.229.

Editor's note: References in this subclause are made according to the numbering of references in TS 24.229.

The UE shall ensure that appropriate resources are available for the media flow(s) on the IP-CAN(s) related to a SIP-session. The means to ensure this is dependant on the characteristics for each IP-CAN, and is described separately for each IP-CAN in question.

GPRS is described in annex B. xDSL is described in annex Y.

5.7 IP-Connectivity Access Network specific concepts when using xDSL to access IM CN subsystem

Editor's note: It is intended that material from this clause will be added as annex Y to TS 24.229.

Editor's note: References in this subclause are made according to the numbering of references in TS 24.229.

5.7.1 Scope

The present annex defines IP-CAN specific requirements for a call control protocol for use in the IP Multimedia (IM) Core Network (CN) subsystem based on the Session Initiation Protocol (SIP), and the associated Session Description Protocol (SDP), where the IP-CAN is xDSL.

5.7.2 xDSL aspects when connected to the IM CN subsystem

5.7.2.1 Introduction

A UE accessing the IM CN subsystem, and the IM CN subsystem itself, utilise the services provided by the xDSL access network to provide packet-mode communication between the UE and the IM CN subsystem.

Requirements for the UE on the use of these packet-mode services are specified in this clause. Requirements for the BRAS in support of this communication are specified in DSL Forum TR-092 [80].

Editor’s note: Additional requirements pertaining to the support of Ethernet regional access type are FFS.

From the UEs perspective, it is assumed that one or more IP-CAN bearer(s) are provided, in the form of connection(s) managed by the DSL modem supporting the UE.

In the first instance, it is assumed that the IP-CAN bearer(s) is (are) statically provisioned between the UE and the BRAS according to the user’s subscription.

Editor’s note: Further contributions are needed to get more insight in the proper support of dynamic establishment of connections.

It is out of the scope of the current Release to specify whether a single IP-CAN bearer is used to convey both signalling and media flows, or whether several PVC connections are used to isolate various types of IP flows (signalling flows, conversational media, non conversational media…).

The end-to-end characteristics of the xDSL IP-CAN bearer depend on the type of regional access network, and on network configuration. The description of the network PVC termination (e.g., located in the DSLAM, in the BRAS…) is out of the scope of this annex.

5.7.2.2 Procedures at the UE

5.7.2.2.1 P-CSCF discovery

5.7.2.2.1.1 P-CSCF discovery

Prior to communication with the IM CN subsystem, the UE shall perform a Network Attachment procedure using DHCP mode or PPP mode. When using xDSL, both IPv4 and IPv6 UEs may access the IM CN subsystem. The UE may request a DNS Server IPv4 address(es) via RFC 2132 [20F] or a DNS Server IPv6 address(es) via RFC 3315 [40].

5.7.2.2.1.2 Procedure at the UE when using IPv4

The UE may acquires a P-CSCF address(es) by using the DHCP (see RFC 2132 [20F]), the DHCPv4 options for SIP servers (see RFC 3361 [35A]), and RFC 3263 [27A].

In case the DHCP server provides several P-CSCF addresses or FQDNs to the UE, the UE shall select the P-CSCF address or FQDN as indicated in RFC 3361 [35A]. If sufficient information for P-CSCF address selection is not available, selection of the P-CSCF address by the UE is implementation specific.

5.7.2.2.1.3 Procedure at the UE when using IPv6

The UE may acquires a P-CSCF address(es) by using the DHCPv6 (seeRFC 3315 [40]), the DHCPv6 options for SIP servers (see RFC 3319 [41]), and RFC 3263 [20H].

In case the DHCP server provides several P-CSCF addresses or FQDNs to the UE, the UE shall select the P-CSCF address or FQDN as indicated in RFC 3319 [41]. If sufficient information for P-CSCF address selection is not available, selection of the P-CSCF address by the UE is implementation specific.

5.7.2.2.2 xDSL bearer provisioning

5.7.2.2.2.1 Statically provisioned xDSL bearer(s)

xDSL bearer(s) is (are) statically provisioned in the current Release.

Editor’s note: Dynamically provisioned xDSL bearer(s), i.e., activation and modification of xDSL bearer(s), are for further study. Further contributions are needed to get more insight in the proper support of dynamic establishment of PVC connections.

5.7.2.2.3 xDSL bearer(s) for media

5.7.2.2.3.1 General requirements

The UE can establish media streams that belong to different SIP sessions on the same xDSL bearer.

5.7.2.2.3.2 Media grouping

If the UE receives indication within the SDP according to RFC 3524 [54] that media stream(s) belong to group(s), and if several xDSL bearers are available to the UE for the session, the media stream(s) may be sent on separate xDSL bearers according to the indication of grouping. The UE may freely group media streams to xDSL bearers in case no indication of grouping is received from the P-CSCF.

If the UE receives media grouping attributes in accordance with RFC 3524[54] that it cannot provide within the available xDSL bearer(s), then the UE shall handle such SDP offers in accordance with RFC 3388[53].

5.7.2.2.3.3 Media authorization

The UE can receive a media authorization token in the P-Media-Authorization header from the P-CSCF according to RFC 3313 [31]. If a media authorization token is received in the P-Media-Authorization header when a SIP session is initiated, the UE shall reuse the existing xDSL bearer(s) and ignore the media authorization token.

Editor’s note: Activation and modification of xDSL bearer(s) are for further study.

5.7.2.2.3.4 Special requirements applying to forked responses

Since the UE is unable to perform bearer modification, forked responses place no special requirements on the UE.

5.7.3 SIP timers

5.7.3.1 SIP timers between IM CN subsystem entities

Editor's note: It is intended that material from this clause will be added as subclause 7.7 to TS 24.229.

Editor's note: Reference in the marked change is made according to the numbering of references in TS 24.229.

Editor's note: Underlined text will be added to TS 24.229 while stroken out text will be deleted in TS 24.229.

The timers defined in RFC 3261 [26] need modification in some cases to accommodate the delays introduced by the air interface processing and transmission delays for UEs supporting cellular access. Table 7.8 shows recommended values for IM CN subsystem.

Table 7.8 lists in the first column, titled "SIP Timer" the timer names as defined in RFC 3261 [26].

The second column, titled "value to be applied between IM CN subsystem elements" lists the values recommended for network elements e.g. P-CSCF, S-CSCF, MGCF, when communicating with each other i.e. when no air interface leg is included. These values are identical to those recommended by RFC 3261 [26].

The third column, titled "value to be applied at the UE" lists the values recommended for the UE, when in normal operation the UE generates requests or responses containing a P-Access-Network-Info header which included a value of "3GPP-GERAN","3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD", "3GPP2-1X", "3GPP2-1X-HRPD", "IEEE-802.11", "IEEE-802.11a", "IEEE-802.11b", or "IEEE-802.11g". These are modified when compared to RFC 3261 [26] to accommodate the air interface delays. In all other cases, the UE should use the values specified in RFC 3261 [26] as indicated in the second column of table 7.8.

The fourth column, titled "value to be applied at the P-CSCF toward a UE" lists the values recommended for the P-CSCF when an air interface leg is traversed, and which are used on all SIP transactions on a specific security association where the security association was established using a REGISTER request containing a P-Access-Network-Info header which included a value of "3GPP-GERAN","3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD", "3GPP2-1X", "3GPP2-1X-HRPD", "IEEE-802.11", "IEEE-802.11a" or "IEEE-802.11b", or "IEEE-802.11g". These are modified when compared to RFC 3261 [26]. In all other cases, the P-CSCF should use the values specified in RFC 3261 [26] as indicated in the second column of table 7.8.

Editor’s note: For WLAN, it is FFS if it is considered as a radio access or a broadband access for the recommended timer values.

Editor's note: Further study is needed as to whether there are better means of determining the access technology delays between the P-CSCF and a UE, and therefore the conditions under which the extended values of the timers should apply.

The final column reflects the timer meaning as defined in RFC 3261 [26].

Table 7.8: SIP timers

SIP Timer	Value to be applied between IM CN subsystem elements	Value to be applied at the UE	Value to be applied at the P-CSCF toward a UE	Meaning
T1	500ms default	2s default	2s default	RTT estimate
T2	4s	16s	16s	The maximum retransmit interval for non-INVITE requests and INVITE responses
T4	5s	17s	17s	Maximum duration a message will remain in the network
Timer A	initially T1	initially T1	initially T1	INVITE request retransmit interval, for UDP only
Timer B	64*T1	64*T1	64*T1	INVITE transaction timeout timer
Timer C	> 3min	> 3 min	> 3 min	proxy INVITE transaction timeout
Timer D	> 32s for UDP	>128s	>128s	Wait time for response retransmits
	0s for TCP/SCTP	0s for TCP/SCTP	0s for TCP/SCTP	
Timer E	initially T1	initially T1	initially T1	non-INVITE request retransmit interval, UDP only
Timer F	64*T1	64*T1	64*T1	non-INVITE transaction timeout timer
Timer G	initially T1	initially T1	initially T1	INVITE response retransmit interval
Timer H	64*T1	64*T1	64*T1	Wait time for ACK receipt.
Timer I	T4 for UDP	T4 for UDP	T4 for UDP	Wait time for ACK retransmits
	0s for TCP/SCTP	0s for TCP/SCTP	0s for TCP/SCTP	
Timer J	64*T1 for UDP	64*T1 for UDP	64*T1 for UDP	Wait time for non-INVITE request retransmits
	0s for TCP/SCTP	0s for TCP/SCTP	0s for TCP/SCTP	
Timer K	T4 for UDP	T4 for UDP	T4 for UDP	Wait time for response retransmits
	0s for TCP/SCTP	0s for TCP/SCTP	0s for TCP/SCTP	

5.7.4 SIP compression procedures

Editor's Note: a subclause B.X is created for GPRS to describe the SIP compression.

Editor's note: Further study is needed as to whether there are better means of determining the access technology delays between the P-CSCF and a UE, and therefore the conditions under which compression should apply.

5.7.4.1 SIP compression

Editor's note: It is intended that material from this clause will be added as subclause 8.1.1 to TS 24.229.

Editor's note: Underlined text will be added to TS 24.229 while stroken out text will be deleted in TS 24.229.

If in normal operation the UE generates requests or responses containing a P-Access-Network-Info header which included a value of "3GPP-GERAN","3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD", "3GPP2-1X", "3GPP2-1X-HRPD", "IEEE-802.11", "IEEE-802.11a", "IEEE-802.11b" or "IEEE-802.11g", then the UE shall ~~shall~~ support SigComp as specified in RFC 3320 [32]. When using SigComp the UE shall send compressed SIP messages in accordance with RFC 3486 [55]. When the UE will create the compartment is implementation specific, but the compartment shall not be created until a set of security associations are set up. The compartment shall finish when the UE is deregistered. State creations and announcements shall be allowed only for messages received in a security association.

Editor's note: For WLAN, it is FFS if it is considered as a radio access or a broadband access for the recommended use of compression.

NOTE: Exchange of bytecodes during registration will prevent unnecessary delays during session setup.

Editor's note: The draft-ietf-rohc-sigcomp-sip-01 [79] can lead to the need for additional changes or clarifications.

If the UE supports SigComp, then the UE supports the SIP dictionary specified in RFC 3485 [42]. If compression is enabled, the UE shall use the dictionary to compress the first message.

The following apply when signalling compression is used:

- State Memory Size greater than zero is needed to give room for the UDVM byte code and make dynamic compression possible. A State Memory Size of at least 4096 bytes shall be a minimum value; and
- A Decompression Memory Size of at least 8192 bytes should be a minimum value.

5.7.4.2 Compression of SIP requests and responses transmitted to the P-CSCF

Editor's note: It is intended that material from this clause will be added as subclause 8.1.2 to TS 24.229.

Editor's note: Underlined text will be added to TS 24.229 while stroken out text will be deleted in TS 24.229.

If in normal operation the UE generates requests or responses containing a P-Access-Network-Info header which included a value of "3GPP-GERAN","3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD", "3GPP2-1X", "3GPP2-1X-HRPD", "IEEE-802.11", "IEEE-802.11a", "IEEE-802.11b" or IEEE-802.11g", then the UE should ~~should~~ compress the requests and responses transmitted to the P-CSCF according to subclause 8.1.1. In other cases where SigComp is supported, it need not

Editor's note: For WLAN, it is FFS if it is considered as a radio access or a broadband access for the recommended use of compression.

NOTE 1: Compression of SIP messages is an implementation option. However, compression is strongly recommended.

NOTE 2: In an IP-CAN where ~~Since~~ compression support is mandatory, the UE may send even the first message compressed. Sigcomp provides mechanisms to allow the UE to know if state has been created in the P-CSCF or not.

5.7.4.3 Decompression of SIP requests and responses received from the P-CSCF

Editor's note: It is intended that material from this clause will be added as subclause 8.1.3 to TS 24.229.

Editor's note: Underlined text will be added to TS 24.229 while stroken out text will be deleted in TS 24.229.

If the UE supports SigComp, then the UE shall decompress the compressed requests and responses received from the P-CSCF according to subclause 8.1.1.

If the UE detects a decompression failure at the P-CSCF, the recovery mechanism is implementation specific and this may, as an example, include resetting the compartment or changing the algorithm.

5.7.4.4 Compression of SIP requests and responses transmitted to the UE

Editor's note: It is intended that material from this clause will be added as subclause 8.2.2 to TS 24.229.

Editor's note: Underlined text will be added to TS 24.229 while stroken out text will be deleted in TS 24.229.

Editor's note: Further study is needed as to whether there are better means of determining the access technology delays between the P-CSCF and a UE, and therefore the conditions under which compression should apply.

For all SIP transactions on a specific security association where the security association was established using a REGISTER request containing a P-Access-Network-Info header which included a value of "3GPP-GERAN","3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD", "3GPP2-1X", "3GPP2-1X-HRPD", "IEEE-802.11", "IEEE-802.11a", "IEEE-802.11b" or "IEEE-802.11g" then the P-CSCF should compress the requests and responses transmitted to the UE according to subclause 8.2.1. In other cases where SigComp is supported, it need not.

Editor’s note: For WLAN, it is FFS if it is considered as a radio access or a broadband access for the recommended use of compression.

NOTE: Compression of SIP messages is an implementation option. However, compression is strongly recommended.

5.7.5 Void

5.7.6 Void

5.7.7 Profile changes for compression

5.7.7.1 Roles

Editor's note: It is intended that material from this clause will be added to subclause A..1.3 to TS 24.229.

Editor's note: Underlined text will be added to TS 24.229 while stroken out text will be deleted in TS 24.229.

Table A.3B: Roles with respect to access technology

Item	Value used in P-Access-Network-Info header	Reference	RFC status	Profile status
1	3GPP-GERAN	[52] 4.4	o	c1
2	3GPP-UTRAN-FDD	[52] 4.4	o	c1
3	3GPP-UTRAN-TDD	[52] 4.4	o	c1
4	3GPP2-1X	[52] 4.4	o	c1
5	3GPP2-1X-HRPD	[52] 4.4	o	c1
11	IEEE-802.11	[52] 4.4	o	c1
12	IEEE-802.11°	[52] 4.4	o	c1
13	IEEE-802.11b	[52] 4.4	o	c1
14	IEEE-802.11g	[52] 4.4	o	c1
21	ADSL	[52] 4.4	o	c1
22	ADSL2	[52] 4.4	o	c1
23	ADSL2+	[52] 4.4	o	c1
24	RADSL	[52] 4.4	o	c1
25	SDSL	[52] 4.4	o	c1
26	HDSL	[52] 4.4	o	c1
27	HDSL2	[52] 4.4	o	c1
28	G.SHDSL	[52] 4.4	o	c1
29	VDSL	[52] 4.4	o	c1
30	IDSL	[52] 4.4	o	c1
c1: If A.3/1 OR A.3/2 THEN o.1 ELSE n/a. o.1: It is mandatory to support at least one of these items.				

5.7.7.2 UE major capabilities

Editor's note: It is intended that material from this clause will be added as subclause A.2.1.2 to TS 24.229.

Editor's note: Underlined text will be added to TS 24.229 while stroken out text will be deleted in TS 24.229.

Table A.4: Major capabilities

Item	Does the implementation support	Reference	RFC status	Profile status
	Capabilities within main protocol			
	Extensions			
29	compressing the session initiation protocol?	[55]	o	c8
c8: IF A.3/1 THEN (IF (A.3B/1 OR A.3B/2 OR A.3B/3 OR A.3B/4 OR A.3B/5 OR A.3B/11 OR A.3B/12 OR A.3B/13 OR A.3B/14) THEN m ELSE o) ELSE n/a - - UE behaviour (based on P-Access-Network-Info usage).				

Editor's note: For WLAN, it is FFS if it is considered as a radio access or a broadband access for the recommended use of compression.

5.7.8 Support of SIP for SigComp

5.7.8.1 Requests initiated by the UE

Editor's note: It is intended that material from this clause will be added as subclause 5.2.6.3 to TS 24.229.

Editor's note: Underlined text will be added to TS 24.229 while stroken out text will be deleted in TS 24.229.

When the P-CSCF receives an initial request for a dialog or a request for a standalone transaction, and the request contains a P-Preferred-Identity header that matches one of the registered public user identities, the P-CSCF shall identify the initiator of the request by that public user identity.

When the P-CSCF receives an initial request for a dialog or a request for a standalone transaction, and the request contains a P-Preferred-Identity header that does not match one of the registered public user identities, or does not contain a P-Preferred-Identity header, the P-CSCF shall identify the initiator of the request by a default public user identity. If there is more then one default public user identity available, the P-CSCF shall randomly select one of them.

NOTE 1: The contents of the From header do not form any part of this decision process.

When the P-CSCF receives from the UE an initial request for a dialog, and a Service-Route header list exists for the initiator of the request, the P-CSCF shall:

1) verify that the list of URIs received in the Service-Route header (during the last successful registration or re-registration) matches the preloaded Route headers in the received request. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCFshall either:

   a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 2 onwards; or

   b) replace the preloaded Route header value in the request with the value of the Service-Route header received during the last 200 (OK) response for a registration or reregistration;

2) add its own address to the Via header. The P-CSCF Via header entry is built in a format that contains the port number of the P-CSCF in accordance with the procedures of RFC3261 [26], and either:

   a) the P-CSCF FQDN that resolves to the IP address, or

   b) the P-CSCF IP address;

3) when adding its own SIP URI to the top of the Record-Route header, build the P-CSCF SIP URI in a format that contains the port number of the P-CSCF where it awaits subsequent requests from the called party, and either:

   a) the P-CSCF FQDN that resolves to the IP address; or

   b) the P-CSCF IP address;

4) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value representing the initiator of the request;

5) add a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17]; and

6) if the request is an INVITE request, save the Contact, CSeq and Record-Route header field values received in the request such that the P-CSCF is able to release the session if needed;

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives any 1xx or 2xx response to the above request, the P-CSCF shall:

1) store the values received in the P-Charging-Function-Addresses header;

2) store the list of Record-Route headers from the received response;

3) store the dialog ID and associate it with the private user identity and public user identity involved in the session;

4) rewrite the port number of its own Record Route entry to its own protected server port number negotiated with the calling UE~~, and append the comp parameter in accordance with the procedures of RFC 3486 [55]~~; and

NOTE 2: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details on the selection of the protected port values see 3GPP TS 33.203 [19].

5) if the response corresponds to an INVITE request, save the Contact, From, To and Record-Route header field values received in the response such that the P-CSCF is able to release the session if needed;

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives from the UE a target refresh request for a dialog, the P-CSCF shall:

1) verify if the request relates to a dialog in which the originator of the request is involved:

    a) if the request does not relates to an existing dialog in which the originator is involved, then the P-CSCF shall answer the request by sending a 403 (Forbidden) response back to the originator. The response may include a Warning header containing the warn-code 399. The P-CSCF will not forward the request. No other actions are required; or

    b) if the request relates to an existing dialog in which the originator is involved, then the P-CSCF shall continue with the following steps;

2) verify that the list of Route headers in the request matches the stored list of Record-Route headers for the same dialog. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

    a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 3 onwards; or

    b) replace the Route header value in the request with the stored list of Record-Route headers for the same dialog;

3) add its own address to the Via header. The P-CSCF Via header entry is built in a format that contains the port number of the P-CSCF where it awaits the responses to come, and either:

    a) the P-CSCF FQDN that resolves to the IP address, or

    b) the P-CSCF IP address;

4) when adding its own SIP URI to the top of Record-Route header, build the P-CSCF SIP URI in a format that contains the port number of the P-CSCF where it awaits subsequent requests from the called party, and either:

    a) the P-CSCF FQDN that resolves to the IP address; or

    b) the P-CSCF IP address; and

5) for INVITE dialogs (i.e. dialogs initiated by an INVITE request), replace the saved Contact and Cseq header filed values received in the request such that the P-CSCF is able to release the session if needed;

NOTE 3: The replaced Contact header field value is valid only if a 1xx or 2xx response will be received for the request. In other cases the old value is still valid.

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives a 1xx or 2xx response to the above request, the P-CSCF shall:

1) rewrite the port number of its own Record Route entry to the same value as for the response to the initial request for the dialog~~, and append the comp parameter in accordance with the procedures of RFC 3486 [55]~~; and

2) replace the saved Contact header value received in the response such that the P-CSCF is able to release the session if needed;

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives from the UE the request for a standalone transaction, and a Service-Route header list exists for the initiator of the request, the P-CSCF shall:

1) verify that the list of URIs received in the Service-Route header (during the last successful registration or re-registration) matches the preloaded Route headers in the received request. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

    a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 3 onwards; or

    b) replace the preloaded Route header value in the request with the one received during the last registration in the Service-Route header of the 200 (OK) response;

2) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value representing the initiator of the request; and

3) add a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17];

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives any response to the above request, the P-CSCF shall:

1) store the values received in the P-Charging-Function-Addresses header;

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives from the UE subsequent requests other than a target refresh request (including requests relating to an existing dialog where the method is unknown), the P-CSCF shall:

1) verify if the request relates to a dialog in which the originator of the request is involved:

   a) if the request does not relates to an existing dialog in which the originator is involved, then the P-CSCF shall answer the request by sending a 403 (Forbidden) response back to the originator. The response may include a Warning header containing the warn-code 399. The P-CSCF will not forward the request. No other actions are required; or

   b) if the request relates to an existing dialog in which the originator is involved, then the P-CSCF shall continue with the following steps;

2) verify that the list of Route headers in the request matches the stored list of Record-Route headers for the same dialog. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

   a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 3 onwards; or

   b) replace the Route header value in the request with the stored list of Record-Route headers for the same dialog;

3) for dialogs that are not INVITE dialogs, add a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17]; and

4) for INVITE dialogs, replace the saved Cseq header value received in the request such that the P-CSCF is able to release the session if needed;

before forwarding the request, (based on the topmost Route header,) in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives from the UE the request for an unknown method (that does not relate to an existing dialog), and a Service-Route header list exists for the initiator of the request, the P-CSCF shall:

1) verify that the list of URIs received in the Service-Route header (during the last successful registration or re-registration) is included, preserving the same order, as a subset of the preloaded Route headers in the received request. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

   a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 2 onwards; or

   b) replace the Route header value in the request with the one received during the last registration in the Service-Route header of the 200 (OK) response; and

2) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value representing the initiator of the request;

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

5.7.8.2 Requests terminated by the UE

Editor's note: It is intended that material from this clause will be added as subclause 5.2.6.4 to TS 24.229.

Editor's note: Underlined text will be added to TS 24.229 while stroken out text will be deleted in TS 24.229.

When the P-CSCF receives, destined for the UE, an initial request for a dialog, prior to forwarding the request, the P-CSCF shall:

1) convert the list of Record-Route header values into a list of Route header values and save this list of Route headers;

2) if the request is an INVITE request, save a copy of the Contact, CSeq and Record-Route header field values received in the request such that the P-CSCF is able to release the session if needed;

3) when adding its own SIP URI to the top of the list of Record-Route headers and save the list, build the P-CSCF SIP URI in a format that contains ~~the comp parameter in accordance with the procedures of RFC 3486 [55], and~~ the protected server port number of the security association established from the UE to the P-CSCF and either:

   a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or

   b) the P-CSCF IP address of the security association established from the UE to the P-CSCF;

4) when adding its own address to the top of the received list of Via header and save the list, build the P-CSCF Via header entry in a format that contains ~~the comp parameter in accordance with the procedures of RFC 3486 [55], and~~ the protected server port number of the security association established from the UE to the P-CSCF and either:

   a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or

   b) the P-CSCF IP address of the security association established from the UE to the P-CSCF;

NOTE 1: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details of the usage of the two ports see 3GPP TS 33.203 [19].

5) store the values received in the P-Charging-Function-Addresses header;

6) remove and store the icid parameter received in the P-Charging-Vector header; and

7) save a copy of the P-Called-Party-ID header;

before forwarding the request to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives any 1xx or 2xx response to the above request, the P-CSCF shall:

1) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with the value saved from the P-Called-Party-ID header that was received in the request;

2) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

   a) discard the response; or

   b) replace the Via header values with those received in the request;

3) verify that the list of URIs received in the Record-Route header of the request corresponding to the same dialog is included, preserving the same order, as a subset of the Record-Route header list of this response. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

   a) discard the response; or

b) replace the Record-Route header values with those received in the request, rewrite the port number of its own Record-Route entry to the port number where it awaits subsequent requests from the calling party and remove the comp parameter.

If the verification is successful, the P-CSCF shall rewrite the port number of its own Record-Route entry to the port number where it awaits subsequent requests from the calling party and remove the comp parameter;

4) store the dialog ID and associate it with the private user identity and public user identity involved in the session; and

5) if the response corresponds to an INVITE request, save the Contact, To, From and Record-Route header field value received in the response such that the P-CSCF is able to release the session if needed;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives any other response to the above request, the P-CSCF shall:

1) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If these lists do not match, then the P-CSCF shall either:

a) discard the response; or

b) replace the Via header values with those received in the request;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives, destined for the UE, a target refresh request for a dialog, prior to forwarding the request, the P-CSCF shall:

1) add its own address to the top of the received list of Via header and save the list. The P-CSCF Via header entry is built in a format that contains ~~the comp parameter in accordance with the procedures of RFC 3486 [55], and~~ the protected server port number of the security association established from the UE to the P-CSCF and either:

a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or

b) the P-CSCF IP address of the security association established from the UE to the P-CSCF;

NOTE 2: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details of the usage of the two ports see 3GPP TS 33.203 [19].

2) when adding its own SIP URI to the top of the list of Record-Route headers and save the list, build the P-CSCF SIP URI in a format that contains the ~~comp parameter in accordance with the procedures of RFC 3486 [55], and~~ the protected server port number of the security association established from the UE to the P-CSCF and either:

a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or

b) the P-CSCF IP address of the security association established from the UE to the P-CSCF; and

3) for INVITE dialogs, replace the saved Contact and Cseq header field values received in the request such that the P-CSCF is able to release the session if needed;

NOTE 3: The replaced Contact header field value is valid only if a 1xx or 2xx response will be received for the request. In other cases the old value is still valid.

before forwarding the request to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives a 1xx or 2xx response to the above request, the P-CSCF shall:

1) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

a) discard the response; or

   b) replace the Via header values with those received in the request;

2) rewrite the port number of its own Record-Route entry to the same value as for the response to the initial request for the dialog and remove the comp parameter; and

3) replace the saved Contact header field value received in the response such that the P-CSCF is able to release the session if needed;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives any other response to the above request, the P-CSCF shall:

1) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

   a) discard the response; or

   b) replace the Via header values with those received in the request; and

2) rewrite the port number of its own Record-Route entry to the port number where it awaits subsequent requests from the calling party and remove the comp parameter;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives, destined for the UE, a request for a standalone transaction, or a request for an unknown method (that does not relate to an existing dialog), prior to forwarding the request, the P-CSCF shall:

1) add its own address to the top of the received list of Via header and save the list. The P-CSCF Via header entry is built in a format that contains ~~the comp parameter in accordance with the procedures of RFC 3486 [55], and~~ the protected server port number of the security association established from the UE to the P-CSCF and either:

   a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or

   b) the P-CSCF IP address of the security association established from the UE to the P-CSCF;

NOTE 4: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details of the usage of the two ports see 3GPP TS 33.203 [19].

2) store the values received in the P-Charging-Function-Addresses header;

3) remove and store the icid parameter received in the P-Charging-Vector header; and

4) save a copy of the P-Called-Party-ID header;

before forwarding the request to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives any response to the above request, the P-CSCF shall:

1) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If these lists do not match, then the P-CSCF shall either:

   a) discard the response; or

   b) replace the Via header values with those received in the request; and

2) remove the P-Preferred-Identity header, if present, and insert an P-Asserted-Identity header with the value saved from the P-Called-Party-ID header of the request;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives, destined for the UE, a subsequent request for a dialog that is not a target refresh request (including requests relating to an existing dialog where the method is unknown), prior to forwarding the request, the P-CSCF shall:

1) add its own address to the top of the received list of Via header and save the list The P-CSCF Via header entry is built in a format that contains ~~the comp parameter in accordance with the procedures of RFC 3486 [55], and~~ the protected server port number of the security association established from the UE to the P-CSCF and either:

   a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or

   b) the P-CSCF IP address of the security association established from the UE to the P-CSCF;

NOTE 5: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details of the usage of the two ports see 3GPP TS 33.203 [19].

2) remove and store the icid parameter from P-Charging-Vector header; and

3) for INVITE dialogs, replace the saved Cseq header value received in the request such that the P-CSCF is able to release the session if needed;

before forwarding the request to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives any response to the above request, the P-CSCF shall:

1) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If these lists do not match, then the P-CSCF shall either:

   a) discard the response; or

   b) replace the Via header values with those received in the request;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

5.8 IP version considerations for fixed broadband

Editor's note: A LS on the issue of IP version used when accessing the IMS was sent to SA2 to ask their opinion on the architectural aspects. The answer from SA2 needs to be considered before including the content of this sub-clause into TS 24.229.

Editor's note: References in this subclause are made according to the numbering of references in TS 24.229.

5.8.1 URI and address assignments

Editor's note: It is intended that material from this clause will modify sub-clause 4.2 of TS 24.229

Editor's note: Underlined text will be added to TS 24.229 while stroken out text will be deleted in TS 24.229.

In order for SIP and SDP to operate, the following preconditions apply:

1) I-CSCFs used in registration are allocated SIP URIs. Other IM CN subsystem entities may be allocated SIP URIs. For example sip:pcscf.home1.net and sip:<impl-specific-info>@pcscf.home1.net are valid SIP URIs. If the user part exists, it is an essential part of the address and shall not be omitted when copying or moving the address. How these addresses are assigned to the logical entities is up to the network operator. For example, a single SIP URI may be assigned to all I-CSCFs, and the load shared between various physical boxes by underlying IP capabilities, or separate SIP URIs may be assigned to each I-CSCF, and the load shared between various physical boxes using DNS SRV capabilities.

2) All IM CN subsystem entities are allocated IP~~v6~~ addresses. For systems providing access to IMS using a fixed broadband interconnection, any IM CN Subsystem entities can be allocated IPv4 only, IPv6 only or both IPv4 and IPv6 addresses. Otherwise, systems shall support IP addresses as ~~in accordance with the constraints~~ specified in 3GPP TS 23.221 [6] subclause 5.1.

3) The subscriber is allocated a private user identity by the home network operator, and this is contained within the ISIM application, if present. Where no ISIM application is present but USIM is present, the private user identity is derived (see subclause 5.1.1.1A). This private user identity is available to the SIP application within the UE.

NOTE: The SIP URIs may be resolved by using any of public DNSs, private DNSs, or peer-to-peer agreements.

4) The subscriber is allocated one or more public user identities by the home network operator. The public user identity shall take the form of SIP URI as specified in RFC 3261 [26] or tel URI as specified in RFC 3966 [22]. At least one of these is SIP URI and it is contained within the ISIM application, if ISIM application is present. Where no ISIM application is present but USIM is present, the UE derives a temporary public user identity (see subclause 5.1.1.1A). All registered public user identities are available to the SIP application within the UE, after registration.

5) The public user identities may be shared across multiple UEs. A particular public user identity may be simultaneously registered from multiple UEs that use different private user identities and different contact addresses. When reregistering and deregistering a given public user identity and associated contact address, the UE will use the same private user identity that it has used during the initial registration of the respective public user identity and associated contact address.

6) For the purpose of access to the IM CN subsystem, UEs are assigned IPv6 prefixes in accordance with the constraints specified in 3GPP TS 23.221 [6] subclause 5.1 (see subclause 9.2.1 for the assignment procedures). In the particular case of UEs accessing the IMS using a fixed broadband interconnection, UEs can be allocated IPv4 only, IPv6 only or both IPv4 and IPv6 addresses.

5.8.2 Impacts on S-CSCF

Editor's note: It is intended that material from this clause will modify sub-clause 5.4.3.2 of TS 24.229

Editor's note: Underlined text will be added to TS 24.229 while stroken out text will be deleted in TS 24.229.

When the S-CSCF receives from the served user or from a PSI an initial request for a dialog or a request for a standalone transaction, prior to forwarding the request, the S-CSCF shall:

Editor's Note: It needs to be stated, that the S-CSCF will only perform the following steps if the request was received from a trusted entity, e.g. an entity within the trust domain.

1) determine whether the request contains a barred public user identity in the P-Asserted-Identity header field of the request or not. In case the said header field contains a barred public user identity for the user, then the S-CSCF shall reject the request by generating a 403 (Forbidden) response. The response may include a Warning header containing the warn-code 399. Otherwise, continue with the rest of the steps;

NOTE 1: If the P-Asserted-Identity header field contains a barred public user identity, then the message has been received, either directly or indirectly, from a non-compliant entity which should have had generated the content with a non-barred public user identity.

2) remove its own SIP URI from the topmost Route header;

3) check if an original dialog identifier that the S-CSCF previously placed in a Route header is present in the topmost Route header of the incoming request. If present, it indicates an association with an existing dialog, the request has been sent from an AS in response to a previously sent request;

4) check whether the initial request matches the next unexecuted initial filter criteria based on a public user identity in the P-Asserted-Identity header in the priority order as described in 3GPP TS 23.218 [5], and if it does, the S-CSCF shall:

   a) insert the AS URI to be contacted into the Route header as the topmost entry followed by its own URI populated as specified in the subclause 5.4.3.4; and

   b) if the AS is located outside the trust domain then the S-CSCF shall remove the P-Access-Network-Info header field and its values in the request; if the AS is located within the trust domain, then the S-CSCF shall retain the P-Access-Network-Info header field and its values in the request that is forwarded to the AS;

NOTE 2: Depending on the result of processing the filter criteria the S-CSCF might contact one or more AS(s) before processing the outgoing Request URI.

5) if there is no original dialog identifier present in the topmost Route header of the incoming request store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header. Optionally, the S-CSCF may generate a new, globally unique icid and insert the new value in the icid parameter of the P-Charging-Vector header when forwarding the message. If the S-CSCF creates a new icid, then it is responsible for maintaining the two icid values in the subsequent messaging;

6) if there is no original dialog identifier present in the topmost Route header of the incoming request insert an orig-ioi parameter into the P-Charging-Vector header. The S-CSCF shall set the orig-ioi parameter to a value that identifies the sending network. The S-CSCF shall not include the term-ioi parameter;

7) if there is no original dialog identifier present in the topmost Route header of the incoming request insert a P-Charging-Function-Addresses header populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS;

8) if there is no original dialog identifier present in the topmost Route header of the incoming request and if the S-CSCF has knowledge of an associated tel-URI for a SIP URI contained in the received P-Asserted-Identity header, add a second P-Asserted-Identity header containing this tel-URI;

9) if the request is not forwarded to an AS and if the outgoing Request-URI is a tel URI, the S-CSCF shall translate the E.164 address (see RFC 3966 [22]) to a globally routeable SIP URI using an ENUM/DNS translation mechanism with the format specified in RFC 3761 24]. Databases aspects of ENUM are outside the scope of the present document. If this translation fails, the request may be forwarded to a BGCF or any other appropriate entity (e.g a MRFC to play an announcement) in the originator's home network or the S-CSCF may send an appropriate SIP response to the originator. If the outgoing Request-URI is a pres URI or an im URI, the S-CSCF shall forward the request as specified in RFC 3861 [63]. In this case, the S-CSCF shall not modify the received Request-URI;

10) determine the destination address (e.g. DNS access) using the URI placed in the topmost Route header if present, otherwise based on the Request-URI. If the destination address is of an IP address type other than the IP address type used in the IM CN subsystem, then the S-CSCF shall forward the request to the IMS-ALG if the IM CN subsytem supports interworking to networks with different IP address type;

11) if network hiding is needed due to local policy, put the address of the I-CSCF(THIG) to the topmost route header;

12) in case of an initial request for a dialog originated from a served user, either:

    - if the request is routed to an AS which is part of the trust domain, the S-CSCF can decide whether to record-route or not. The decision is configured in the S-CSCF using any information in the received request that may otherwise be used for the initial filter criteria. If the request is record-routed the S-CSCF shall create a Record-Route header containing its own SIP URI; or

    - if the request is routed elsewhere, create a Record-Route header containing its own SIP URI;

NOTE 3: For requests originated from a PSI the S-CSCF can decide whether to record-route or not.

Editor's Note: It needs to be clarified how the S-CSCF decides whether to put its address into the Record-Route header in the case of handling a request that originates from a PSI. It might be part of the operators policy.

13) based on the destination user (Request-URI), remove the P-Access-Network-Info header prior to forwarding the message;

14) route the request based on SIP routeing procedures; and

15) if the request is an INVITE request, save the Contact, Cseq and Record-Route header field values received in the request such that the S-CSCF is able to release the session if needed.

If the S-CSCF fails to receive a SIP response or receives a 408 (Request Timeout) response or a 5xx response from the AS, the S-CSCF shall:

- if the default handling defined in the filter criteria indicates the value "SESSION_CONTINUED" as specified in 3GPP TS 29.228 [14] or no default handling is indicated, execute the procedure from step 4; and

- if the default handling defined in the filter criteria indicates the value "SESSION_TERMINATED" as specified in 3GPP TS 29.228 [14], either forward the received response or send a 408 (Request Timeout) response or a 5xx response towards the served UE as appropriate (without verifying the matching of filter criteria of lower priority and without proceeding for further steps).

If the S-CSCF receives any final response from the AS, it shall forward the response towards the served UE (without verifying the matching of filter criteria of lower priority and without proceeding for further steps).

When the S-CSCF receives any response to the above request, the S-CSCF may:

1) apply any privacy required by RFC 3323 [33] and RFC 3325 [34] to the P-Asserted-Identity header.

NOTE 4: The P-Asserted-Identity header would normally only be expected in 1xx or 2xx responses.

NOTE 5: The optional procedure above is in addition to any procedure for the application of privacy at the edge of the trust domain specified by RFC 3325 [34].

When the S-CSCF receives any response to the above request containing a term-ioi parameter, the S-CSCF shall store the value of the received term-ioi parameter received in the P-Charging-Vector header, if present. The term-ioi parameter identifies the sending network of the response message. The term-ioi parameter and the orig-ioi parameter shall only be retained in the P-Charging-Vector header if the next hop is to an AS.

When the S-CSCF receives a 1xx or 2xx response to the initial request for a dialog, if the response corresponds to an INVITE request, the S-CSCF shall save the Contact and Record-Route header field values in the response in order to be able to release the session if needed.

When the S-CSCF, upon sending an initial INVITE request that includes an IP~~v6~~ address in the SDP offer (in "c=" parameter), receives an error response indicating that the IP address type used i~~n the IM CN subsystem~~ is not supported, (e.g., the S-CSCF receives the 488 (Not Acceptable Here) with 301 Warning header indicating "incompatible network address format"), the S-CSCF shall either:

- fork the initial INVITE request to the IMS-ALG; or

- process the error response and forward it using the Via header.

When the S-CSCF receives from the served user a target refresh request for a dialog, prior to forwarding the request the S-CSCF shall:

1) remove its own URI from the topmost Route header;

2) create a Record-Route header containing its own SIP URI;

3) if the request is an INVITE request, save the Contact, Cseq and Record-Route header field values received in the request such that the S-CSCF is able to release the session if needed;

4) in case the request is routed towards the destination user (Request-URI) or in case the request is routed to an AS located outside the trust domain, remove the P-Access-Network-Info header; and

5) route the request based on the topmost Route header.

When the S-CSCF receives a 1xx or 2xx response to the target refresh request for a dialog, if the response corresponds to an INVITE request, the S-CSCF shall save the Contact and Record-Route header field values in the response such that the S-CSCF is able to release the session if needed.

When the S-CSCF receives from the served user a subsequent request other than a target refresh request for a dialog, prior to forwarding the request the S-CSCF shall:

1) remove its own URI from the topmost Route header;

2) in case the request is routed towards the destination user (Request-URI) or in case the request is routed to an AS located outside the trust domain, remove the P-Access-Network-Info header; and

3) route the request based on the topmost Route header.

5.8.3 Impacts on UE

Editor's note: It is intended that material from this clause will modify sub-clause 9.2.1 of TS 24.229

Editor's note: Underlined text will be added to TS 24.229 while stroken out text will be deleted in TS 24.229.

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

a) establish a connection with the IP-CAN;

b) obtain an IP address using either the standard IETF protocols (e.g., DHCP or IPCP) or a protocol that is particular to the IP-CAN technology that the UE is utilising. The obtained IP address shall be fixed throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the last deregistration; and

c) acquire a P-CSCF address(es).

The methods for acquiring a P-CSCF address(es) are:

I. Employ Dynamic Host Configuration Protocol for IPv4 RFC 2131 [40A] or for IPv6 (DHCPv6) RFC 3315 [40] and the DHCP~~v6~~ options for SIP servers (RFC 3319 [41] in case of IPv6 and RFC 3361 [41A] in case of IPv4).

The UE shall either:

- in the DHCP query, request a list of SIP server domain names of P-CSCF(s) and the list of Domain Name Servers (DNS); or

- request a list of SIP server IP~~v6~~ addresses of P-CSCF(s).

II. Obtain the P-CSCF address(es) by employing a procedure that the IP-CAN technology supports. (e.g. GPRS).

When acquiring a P-CSCF address(es) the UE can freely select either method I or II.

The UE may also request a DNS Server IP~~v6~~ address(es) as specified in RFC 3315 [40] or RFC 2131 [40A].

5.9 Additional procedures in support for hosted NAT

Editor's note: It is intended that material from this clause will add in a normative annex of TS 24.229.

NOTE: this subclause describes the mechanism for support of the hosted NAT scenario. This does not preclude other mechanisms but they are out of the scope of the specification.

5.9.1 Scope

This annex describes the P-CSCF procedures in support of hosted NAT. In this scenario, both the media flows and the SIP signalling both traverse a NA(P)T device located in the customer premises domain. The term "hosted NAT" is used to address this function. More details can found in TS.182.006 [xx]

The P-CSCF can, by comparing the address information in the top-most SIP Via header of a SIP REGISTER request, received from the UE, with the IP level address information from where the request was received, determine whether to perform the hosted NAT procedures for the user identified by the REGISTER request. The P-CSCF will use the hosted NAT procedure only when the address information do not match. If the top-most Via header contains a domain name the P-CSCF shall perform the appropriate DNS procedures in order to retrieve the address information to be used for the comparison.

Editor's Note: The security solution currently specified for Release 6 by 3GPP for access to IMS does not allow SIP-unaware NAT devices to be inserted in the signalling path. Hence, if scenarios with SIP-unaware NAT devices in the signalling path are to be supported in Release 1, alternative IMS access security mechanisms are needed.

5.9.2 P-CSCF usage of SIP

5.9.2.1 Introduction

This clause describes the SIP procedures for supporting hosted NAT scenarios.

5.9.2.2 Registration

The procedures described in clause 5.2.2 apply with the additional procedures described in the present clause.

When the P-CSCF receives a REGISTER request from the UE, the P-CSCF shall add the "received" and "rport" parameters to the Via header set to the source IP address and port of the packet header in accordance with the procedure defined in RFC 3261 [26] and RFC 3581 [56A]. Furthermore, the P-CSCF performs the following actions on the Contact header depending on its content:

- if the Contact header contains a contact address in the form of an IP address (NOTE), the P-CSCF shall save this IP address for the duration of the registration and replace it by the source IP address of the packet containing the REGISTER request before forwarding the message;
- if the Contact header contains more than one contact addresses in the form of an IP address, the P-CSCF shall apply the above procedure to one of those contact addresses (i.e. by chosing the one with the hightest qvalue parameter) and delete any other contact addresses containing an IP address.

Editor's note: Need to indicate what happens when two with same qvalue

NOTE: When the host parameter in the Contact address is in the form of a FQDN, the P-CSCF has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address and port pointing towards the hosted NAT and bound to this UE.

When the P-CSCF received a response to the above request, if the Contact header contains a contact address in the form of an IP address, the P-CSCF shall replace this IP address by the saved IP address contained in the REGISTER request before forwarding the associated response to the UE.

5.9.2.3 General treatment for all dialogs and standalone transactions excluding the REGISTER method

5.9.2.3.1 Introduction

The procedures described in subclause 5.2.6 apply with the additional procedures described in subclause 5.9.2.3.

5.9.2.3.2 Request initiated by the UE

When the P-CSCF receives an initial request for a dialog or a request for a standalone transaction, the P-CSCF shall add the "received" and "rport" parameters to the Via header set to the source IP address and port in the packet header as defined in RFC 3261 [26] and RFC 3581 [56A]. Furthermore, if the contact address in the Contact header is in the form of an IP address, the P-CSCF shall save this IP address for the duration of the dialog or standalone transaction and replace it by the source IP address of the packet containing the REGISTER request.

When the P-CSCF received a response to the above request, if the Contact header contains a contact address in the form of an IP address, the P-CSCF shall replace this IP address by the saved IP address contained as per the previous paragraph.

5.9.2.3.3 Request terminated by the UE

When the P-CSCF receives a response to an initial request for a dialog or a request for a standalone transaction, if the contact address in the Contact header is in the form of an IP address, the P-CSCF shall save this IP address for the duration of the dialog or standalone transaction and replace it by the source IP address of the packet containing the REGISTER request.

5.9.3 P-CSCF usage of SDP

5.9.3.1 Introduction

Subclause 5.9.3 describes the SDP related procedures performed by the P-CSCF in support of hosted NAT.

5.9.3.2 Receipt of an SDP offer

When the P-CSCF receives an SDP offer during session establishment, if this offer comes from a UE located behind a hosted NAT, the P-CSCF shall modify the SDP offer by replacing the IP address(es) and port number previously set in the SDP offer by the IP address(es) and port number(s) received from the IMS Access Gateway over the Iq interface.

5.9.3.3 Receipt of an SDP answer

When the P-CSCF receives any SDP answer to an SDP offer described in subclause 5.9.3.2, if this answer comes from a UE located behind a hosted NAT, the P-CSCF shall modify the SDP answer by replacing the IP address(es) and port number previously set in the SDP answer by the IP address(es) and port number(s) received from the IMS Access Gateway over the Iq interface.

5.9.3.4 Change of media connection data

After the session is established, it is possible for both ends of the session to change the media connection data for the session. When the P-CSCF receives a SDP offer/answer coming from a UE located behind a hosted NAT with port number(s) or IP address(es) included, there are three different possibilities:

- IP address(es) or/and port number(s) have been added. In this case, the P-CSCF shall apply the procedures as described in subclause 5.9.3.2 and 5.9.3.3 as appropriate for those additionnal IP address(es) or/and port number(s);
- IP address(es) and port number(s) have been reassigned to the end points. In this case, the P-CSCF shall apply the procedures as described in subclause 5.9.3.2 and 5.9.3.3 as appropriate for those reassigned IP address(es) and port number(s);
- no change has been made to the IP address(es) and port number(s). The P-CSCF shall apply procedures described in subclause 5.9.3.2 using the previously stored IP address(es) and port number(s).

5.10 Additional procedures in support of NA(P)T and NA(P)T-PT controlled by the P-CSCF

Editor's note: It is intended that material from this clause will add in a normative annex of TS 24.229.

Editor's note: This subclause could be merged in a next version of the TR with the section 5.9 that describes additional procedures at the P-CSCF for support of hosted NAT scenario defined in TS 23.228.

NOTE: This subclause describes the mechanism for support of NA(P)T and NA(P)T-PT controlled by the P-CSCF scenario defined in TS 23.228. This does not preclude other mechanisms but they are out of the scope of the specification.

5.10.1 Scope

This annex describes the P-CSCF procedures for supporting the scenario where IP address and/or port conversions occur at the IMS Access Gateway level in the media path between the UE and the backbone. Two types of address conversions are covered:

- IP version interworking (NA(P)T-PT); and;
- IP address/port translation (NA(P)T).

The annex assumes that signalling procedure take place over the Iq interface to enable the P-CSCF to request and retrieve the address bindings reserved in the transport plane.

Editor's note: It is for further study if the Iq reference point can be merged with the Rx+ reference point. If they are not merged then the IMS Access Gateway may be a TrGW and the Iq may be equivalent to the Ix reference point.

Editor's Note: Different access architectures, possibly due to different access technologies, may need to be supported by the same P-CSCF. An understanding of the exact mechanism by which the P-CSCF determines whether the procedures described in the present annex is applicable for any individual session or not, is needed.

5.10.2 P-CSCF usage of SDP

5.10.2.1 Introduction

The subclause 5.10.2 describes the P-CSCF procedures for supporting IP address and/or port conversions in SDP that occur in the media path between the UE and the backbone.

NOTE: In the particular case of RTP flows, port conversions also apply to the associated RTCP flows.

5.10.2.2 Receipt of an SDP offer

When the P-CSCF receives any SDP offer during session establishment, the P-CSCF shall modify the SDP offer by replacing the IP address(es) and port number previously set in the SDP offer by the IP address(es) and port number(s) received from the IMS Access Gateway over the Iq interface.

5.10.2.3 Receipt of an SDP answer

When the P-CSCF receives any SDP answer to an SDP offer described in subclause 5.10.2.2, the P-CSCF shall modify the SDP answer by replacing the IP address(es) and port number previously set in the SDP answer by the IP address(es) and port number(s) received from the IMS Access Gateway over the Iq interface.

The P-CSCF may receive multiple provisional responses with an SDP answer due to forking of a request before the first final answer is received. For each SDP answer received in such subsequent provisional responses, the P-CSCF shall apply the procedure in this subclause.

5.10.2.4 Change of media connection data

After the session is established, it is possible for both ends of the session to change the media connection data for the session. When the P-CSCF receives a SDP offer/answer where port number(s) or IP address(es) is/are included, there are three different possibilities:

- IP address(es) or/and port number(s) have been added. In this case, the P-CSCF shall apply the procedures as described in subclause 5.10.2.2 or subclause 5.10.2.3 as appropriate for those additional IP address(es) or/and port number(s); or

- IP address(es) and port number(s) have been reassigned to the end points. In this case, the P-CSCF shall apply the procedures as described in subclause 5.10.2.2 or subclause 5.10.2.3 as appropriate for those reassigned IP address(es) and port number(s); or

- no change has been made to the IP address(es) and port number(s). The P-CSCF shall apply procedures described in subclause 5.10.2.2 using the previously stored IP address(es) and port number(s).

5.11 Conference establishment

Editor's note: It is intended that material from this clause (changemarks) will be added in the regarding chapters of TS 24.147.

Editor's note: References in this subclause are made according to the numbering of references in TS 24.147. The numbering of the chapters in this subclause is made according to TS 24.147.

5.11.1 User joining a conference by using a conference URI

Editor's note: It is intended that material from this clause will modify sub-clause 5.3.1.4.1 of TS 24.147

Editor's note: Underlined text will be added to TS 24.147 while stroken out text will be deleted in TS 24.147.

Upon generating an initial INVITE request to join a conference for which the conference URI is known to the conference participant, the conference participant shall:

1) set the request URI of the INVITE request to the conference URI; and

2) send the INVITE request towards the conferencing AS that is hosting the conference.

NOTE 1: The initial INVITE request is generated in accordance with 3GPP TS 24.229 [5].

NOTE 2: The mechanisms by which the conference participant / user gets aware of the conference URI are outside the scope of the present document.

On receiving a 200 (OK) response to the INVITE request with the "isfocus" feature parameter indicated in Contact header, the conference participant shall store the contents of the received Contact header as the conference URI. In addition to that the conference participant may subscribe to the conference event package as described in draft-ietf-sipping-conference-package [11] by using the stored conference URI.

NOTE 3: A conference participant can decide not to subscribe to the conference event package for conferences with a large number of attendees, due to the signalling traffic caused by the notifications about e.g. users joining or leaving the conference.

Upon receipt of an INVITE request that includes a Replaces header, the UE shall apply the procedures described in RFC 3891 [33] to the INVITE request.

5.11.2 User invites other user to a conference by sending a REFER request to the conference focus

Editor's note: It is intended that material from this clause will modify sub-clause 5.3.1.5.3 of TS 24.147

Editor's note: Underlined text will be added to TS 24.147 while stroken out text will be deleted in TS 24.147.

Upon generating a REFER request that is destined to the conference focus in order to invite another user to a specific conference, the conference participant shall:

1) set the request URI of the REFER request to the conference URI to which the user is invited to;

2) set the Refer-To header of the REFER request to the SIP URI or tel URL of the user who is invited to the conference;

3) include the "method" parameter with the value "INVITE" in the Refer-To header; and

NOTE: Other headers of the REFER request will be set in accordance with 3GPP TS 24.229 [5].

4) send the REFER request towards the conference focus that is hosting the conference.

The UE may additionally include the Referred-By header to the REFER request and set it to the URI of the conference participant that is sending the REFER request.

In case of an active session the UE may additionally include the Replaces header in the header portion of the SIP URI of the Refer-to header of the REFER request. The included Replaces header shall refer to the active dialog that is replaced by the ad-hoc conference. The Replaces header shall comply with RFC 3891 [33].

Afterwards the UE shall treat incoming NOTIFY requests that are related to the previously sent REFER request in accordance with RFC 3515 [17].

5.11.3 Request from a user to invite another user to a conference

Editor's note: It is intended that material from this clause will modify sub-clause 5.3.2.5.2 of TS 24.147

Editor's note: Underlined text will be added to TS 24.147 while stroken out text will be deleted in TS 24.147.

Upon receipt of an REFER request that includes:

a) a conference URI in the request URI; and

b) a Refer-To header including:

- a valid SIP URI or tel URL; and,
- the "method" parameter set to "INVITE";

the conference focus shall:

1) check if the conference URI is allocated. If the conference URI is not allocated, the conference focus shall reject the request in accordance with RFC 3261 [7]. The following actions in this subclause shall only be performed if the conference URI is allocated;

2) verify the identity of the user as described in subclause 5.7.1.4 of 3GPP TS 24.229 [5] and authorize the request as described in subclause 5.7.1.5 of 3GPP TS 24.229 [5]. The following actions in this subclause shall only be performed if the request can be authorized;

3) generate a final response to the REFER request in accordance with RFC 3515 [17];

4) invite the user indicated in the Refer-To header by performing the procedures as described in subclause 5.3.2.5.3;

5) if the received REFER request included a Referred-By header, include the Referred-By header in accordance with RFC 3892 [20] in the INVITE request that is sent for joining the conference; ~~and~~

5a) if the received REFER request included a Replaces header, include the Replaces header in accordance with RFC 3891 [33] and 3GPP TS 24.229 [5] in the INVITE request that is sent for joining the conference; and

6) based on the progress of this invitation, send NOTIFY messages in accordance with the procedures of RFC 3515 [17] towards the user who sent the REFER request.

5.11.4 Inviting a user to a conference by sending an INVITE request

Editor's note: It is intended that material from this clause will modify sub-clause 5.3.2.5.3 of TS 24.147

Editor's note: Underlined text will be added to TS 24.147 while stroken out text will be deleted in TS 24.147.

When generating an INVITE request in order to invite a user to a specific conference, the conference focus shall:

1) set the request URI of the INVITE request to the address of the user who is invited to the conference;

2) set the P-Asserted-Identity header of the INVITE request to the conference URI of the conference that the user shall be invited to;

3) set the Contact header of the INVITE request to the conference URI of the conference that the user shall be invited to, including the "isfocus" feature parameter;

4) if the INVITE request is generated due to a received REFER request from another conference participant and that received REFER request included a Referred-By header, include the Referred-By header in accordance with RFC 3892 [20] in the INVITE request;

4a) if the INVITE request is generated due to a received REFER request from another conference participant and the received REFER request included a Replaces header, include the Replaces header in accordance with RFC 3891 [33] and 3GPP TS 24.229 [5] in the INVITE request;

5) request the resources required for the new user from the conference focus; and

6) send the INVITE request towards the user who is invited to the conference.

NOTE: Requests are generated in accordance with 3GPP TS 24.229 [5].

Afterwards the conference focus shall proceed the session establishment as described in 3GPP TS 24.229 [5].

5.11.5 Flows demonstrating the use of the Replaces header

Editor's note: It is intended that material from this clause will modify be added as annex A.9 to TS 24.147

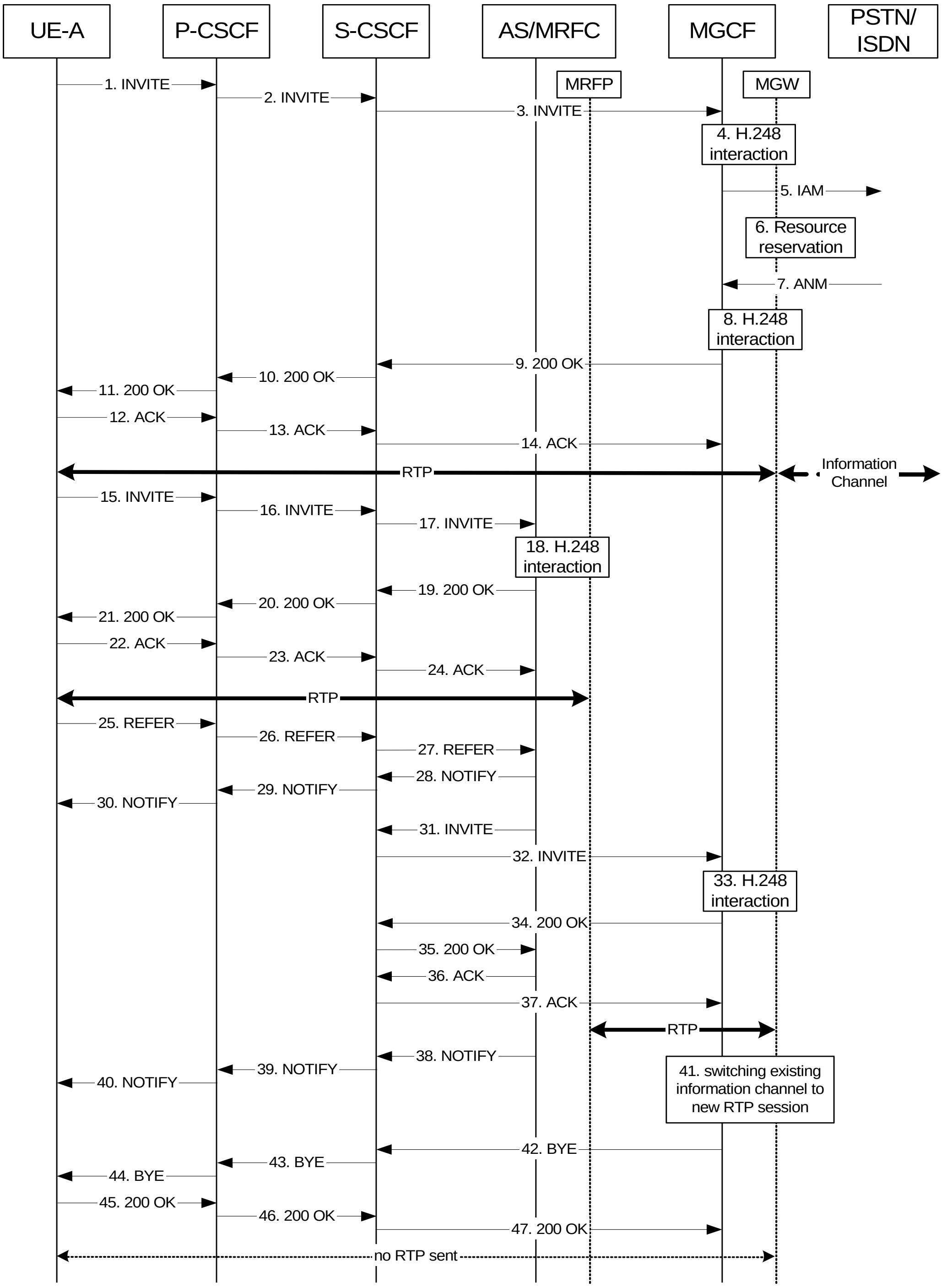

Figure A.9-1: CONF interworking signalling flow in case of an active session between NGN and PSTN

Description Figure A.9-1

Note: Only the most relevant messages are shown in Figure A.1

UE-A is in an active voice session with a PSTN/ISDN TE (SIP dialog with Call-ID, to-tag and from-tag between UE-A and MGCF). It then creates a conference and invites the PSTN/ISDN TE to the conference by sending a REFER to the conference focus, which invites the PSTN/ISDN TE to the conference by sending an INVITE which includes the Replaces header to the MGCF. The MGCF confirms the session, switches the existing information channel to the new RTP session, and terminates the session which is replaced.

1. – 3. UE-A initiates a voice session with a PSTN/ISDN TE by sending an INVITE to the MGCF.

Table A.9-1: 1.INVITE (UE-A to P-CSCF)

```
INVITE tel:+1-212-555-2222 SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
Route: <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>, <sip:scscf1.home1.net;lr>
P-Preferred-Identity: "John Doe" <sip:user1_public1@home1.net>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Require: precondition, sec-agree
Proxy-Require: sec-agree
Supported: 100rel
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-s=87654321; port-c=8642;
port-s=7531
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Content-Type: application/sdp
Content-Length: (…)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
a=rtpmap:99 MP4V-ES
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=rtpmap:96 telephone-event
```

4. H.248 interaction

5. SS7: IAM

6. resource reservation

7. SS7: ANM

8. H.248 interaction

9. – 11. The MGCF sends a final response back to the session originator.

Table A.9-2: 9. 200 OK (MGCF to S-CSCF)

```
SIP/2.0 200 OK
```

```
Via: SIP/2.0/UDP bgcf1.home1.net;branch=z9hG4bK6546q2.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1,
SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity: <tel:+1-212-555-2222>
P-Charging-Vector:
Privacy: none
From:
To: <tel:+1-212-555-2222>;tag=314159
Call-ID:
CSeq:
Require: 100rel
Contact: <sip:mgcf1.home1.net>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE
RSeq: 9021
Content-Type: application/sdp
Content-Length: (…)

v=0
o=- 2987933623 2987933623 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 0 RTP/AVP 98 99
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=rtpmap:96 telephone-event
```

12. – 14. The Calling party acknowledges the final response with an ACK request.

15. – 24. UE-A creates a conference by sending an INVITE to the Conference URI and connects to the conference.

Table A.9-3: 15. INVITE request (UE-A to P-CSCF)

```
INVITE sip:conference-factory1@mrfc1.home1.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
Route: <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>, <sip:orig@scscf1.home1.net;lr>
P-Preferred-Identity: "John Doe" <sip:user1_public1@home1.net>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: none
From: <sip:user1_public1@home1.net>; tag=171829
To: <sip:conference-factory1@mrfc1.home1.net>
Call-ID: cb03a0s09a2sdfglkj490444
Cseq: 127 INVITE
Require: precondition, sec-agree
Proxy-Require: sec-agree
Supported: 100rel
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-s=87654321;
   port-c=8642; port-s=7531
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE, SUBSCRIBE, NOTIFY
Content-Type: application/sdp
Content-Length: (…)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
a=rtpmap:99:MPVMP4V-ES
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=rtpmap:96 telephone-event
```

25. – 27. UE-A invites the PSTN/ISDN TE to the conference by sending a REFER reqest to the conference focus, the ‘method’ parameter set to ‘INVITE’. The REFER request includes the Replaces header with Call-ID, to-tag and from-tag from the existing SIP dialog.

Table A.9-4: 25. REFER request (UE-A to P-CSCF)

```
REFER sip: conference1@mrfc1.home1.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
Route: <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>, <sip:orig@scscf1.home1.net;lr>
P-Preferred-Identity: "John Doe" <sip:user1_public1@home1.net>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: none
From: <sip:user1_public1@home1.net>; tag=171829
To: <sip:user2_public1@home2.net>
Call-ID: cb03a0s09a2sdfglkj490444
Cseq: 127 REFER
Require: sec-agree
Refer-To: <tel:+1-212-555-2222?Replaces=cb03a0s09a2sdfglkj490333%3Bto-tag314159%3Bfrom-
   tag171828;method=INVITE>
Referred-By: <sip:user1_public1@home1.net>
Proxy-Require: sec-agree
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-s=87654321;
   port-c=8642; port-s=7531
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Content-Length: 0
```

28. – 30. The conference focus sends a NOTIFY request containing information about the progress of the REFER request processing. The Subscription-State is set to 'active'.

31. – 32.. The conference focus invites the PSTN/ISDN TE by sending a INVITE request to the MGCF. The INVITE request includes the Replaces header with Call-ID, to-tag and from-tag from the existing SIP dialog.

Table A.9-5: INVITE request (MRFC/AS to S-CSCF)

```
INVITE sip: tel:+1-212-555-2222 SIP/2.0
Via: SIP/2.0/UDP mrfc1.home1.net;branch=z9hG4bK23273846
Max-Forwards: 70
P-Asserted-Identity: <sip:conference1@mrfc1.home1.net>
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"; orig-ioi=home1.net
Privacy: none
From: <sip:conference1@mrfc1.home1.net>;tag=171123
To: <sip:user2_public1@home2.net>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Require: replaces
Replaces: cb03a0s09a2sdfglkj490333;to-tag=314159;from-tag=171828
Supported: 100rel
Referred-By: <sip:user1_public1@home1.net>
Contact: <sip:conference1@mrfc1.home1.net>;isfocus
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE, SUBSCRIBE, NOTIFY
Allow-Events: conference
Content-Type: application/sdp
Content-Length: (…)

v=0
o=- 2987933615 2987933615 IN IP6 5555::abc:def:abc:abc
s=-
c=IN IP6 5555::abc:def:abc:def
t=0 0
m=video 10001 RTP/AVP 98
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=rtpmap:96 telephone-event
```

33. H.248 interaction.

34. – 35. The MGCF sends a final response back to the session originator.

36. – 37. The Calling party acknowledges the final response with an ACK request.

38. – 40. The conference focus sends a NOTIFY request containing information about the progress of the REFER request processing. The Subscription-State is set to 'terminated'.

41. The MGCF replaces the existing RTP stream to UE-A with the new RTP stream to the conference bridge.

42. – 44. The MGCF releases the session with UE-A by sending a BYE request to UE-A.

45. – 47. UE-A responds with a 200 OK response.

5.12 Procedures at the MGCF

5.11.1 Calls originated from circuit-switched networks

Editor's note: It is intended that material from this clause will be added as subclause 5.5.3.1.1 to TS 24.229.

Editor's note: Underlined text will be added to TS 24.229 while stroken out text will be deleted in TS 24.229.

When the MGCF receives an indication of an incoming call from a circuit-switched network, the MGCF shall:

- generate and send an INVITE request to I-CSCF:
    - set the Request-URI to the "tel" format using an E.164 address or to the “sip” format using an E164 address in the user portion and set user=phone;

Note: Details how to set the host portion are out of scope of the document. However, when a SIP URI is used the host portion needs to be part of the domain name space owned by the I-CSCF

- set the Supported header to "100rel" (see RFC 3312 [30] as updated by draft-ietf-sip-rfc3312-update [64]));
- include an P-Asserted-Identity header, depending on corresponding information in the circuit-switched network;
- create a new, globally unique value for the icid parameter and insert it into the P-Charging-Vector header; and
- insert an orig-ioi parameter into the P-Charging-Vector header. The orig-ioi parameter shall be set to a value that identifies the sending network in which the MGCF resides and the term-ioi parameter shall not be included.

When the MGCF receives a 1xx or 2xx response to an initial request for a dialog, the MGCF shall store the value of the received term-ioi parameter received in the P-Charging-Vector header, if present. The term-ioi parameter identifies the sending network of the response message.

6 Application Usage of SDP

Editor's note: This clause is under the responsibility of CT1. Material for this clause must be submitted to CT1.

Editor's note: This clause will cover requirements from providing IMS via fixed broadband with regards to the usage of SDP It is intended that material from this clause will be added to clause 6 of TS 24.229.

7 Gq interface

Editor's note: This clause is under the responsibility of CT3. Material for this clause must be submitted to CT3. CT1 will not review the content of this clause.

Editor's note: This clause will cover requirements from providing IMS via fixed broadband with regards to QoS and SBLP. It is intended that material from this clause will be added to TS 29.208 and TS 29.209.

8 Interworking towards CS networks

Editor's note: This clause is under the responsibility of CT3. Material for this clause must be submitted to CT3. CT1 will not review the content of this clause.

Editor's note: This clause will cover requirements from providing IMS via fixed broadband with regards to interworking of SIP with ISUP/BICC networks. It is intended that material from this clause will be added to TS 29.163.

Editor's note: The mapping of reason headers towards the ISDN may be misused due to possible user creation of the reason header since there is no screening in IMS.

8.1 Coding of the REL

Editor's note: Underlined text will be added to TS 29.163 while stroken out text will be deleted in TS 29.163. Table 8a is new.

Editor's note: Subclause 7.2.3.1.7 of TS 29.163 will be modified as follows:

If the Reason header field with Q.850 Cause Value is included in the BYE or CANCEL, then the Cause Value shall be mapped to the ISUP Cause Value field in the ISUP REL . The mapping of the Cause Indicators parameter to the Reason header is shown in Table 8a. Table 8 shows the coding of the Cause Value in the REL if it is not available from the Reason header field. In both cases, the Location Field shall be set to "*network beyond interworking point*". ~~The SIP BYE and CANCEL requests are mapped into a REL message with cause value #16 and #31 respectively as indicated in table 8.~~

Table 8: Coding of REL

SIP Message →	REL →
Request	**cause parameter**
BYE	Cause value No. 16 (nomal clearing)
CANCEL	Cause value No. 31 (nomal unspecified)

~~NOTE: If an optional Reason header field is included in the BYE or CANCEL, then the Cause Value can be mapped to the ISUP Cause Value field in the ISUP REL. The mapping between the Cause Indicators parameter and the Reason header is out of the scope of the present specification.~~

Table 8a – Mapping of SIP Reason header fields into Cause Indicators parameter

Component of SIP Reason header field	Component value	BICC/ISUP Parameter field	Value
Protocol	"*Q.850*"	Cause Indicators parameter	–
protocol-cause	"*cause = XX*" (Note 1)	Cause Value	"*XX*" (Note 1)
–	–	Location	"*network beyond interworking point*"
NOTE 1 – "XX" is the Cause Value as defined in ITU-T Rec. Q.850.			

8.2 Receipt of the Release Message

Editor's note: Underlined text will be added to TS 29.163 while stroken out text will be deleted in TS 29.163. Table 9a is new.

Editor's note: Subclause 7.2.3.1.8 of TS 29.163 will be modified as follows:

If the REL message is received and a final response (i.e. 200 OK (INVITE)) has already been sent, the I-MGCF shall send a BYE message.

NOTE: According to SIP procedures, in the case that the REL message is received and a final response (e.g. 200 OK (INVITE)) has already been sent (but no ACK has been received) on the incoming side of the I-MGCF then the I- MGCF does not send a 487 Request terminated and instead waits until the ACK is received before sending a BYE message.

A Reason header field containing the received (Q.850) Cause Value of the REL shall be added to the SIP final response or BYE sent as a result of this clause. The mapping of the Cause Indicators parameter to the Reason header is shown in Table 9a.

Table 9a – Mapping of Cause Indicators parameter into SIP Reason header fields

Cause indicators parameter field	Value of parameter field	component of SIP Reason header field	component value
–	–	protocol	"*Q.850*"
Cause Value	"*XX*" (Note 1)	protocol-cause	"*cause = XX*" (Note 1)
–	–	reason-text	Should be filled with the definition text as stated in ITU-T Rec. Q.850 (Note 2)
NOTE 1 – "XX" is the Cause Value as defined in ITU-T Rec. Q.850. NOTE 2 – Due to the fact that the Cause Indicators parameter does not include the definition text as defined in Table 1/Q.850, this is based on provisioning in the I-MGCF.			

Editor note: Is it really required to fill the component value with text ?

8.3 Autonomous Release at I-MGCF

Editor's note: Underlined text will be added to TS 29.163 while stroken out text will be deleted in TS 29.163

Editor's note: Subclause 7.2.3.1.10 of TS 29.163 will be modified as follows:

Table 10 shows the trigger events at the MGCF and the release initiated by the MGCF when the call is traversing from SIP to ISUP/BICC.

A Reason header field containing the (Q.850) Cause Value of the REL message sent by the I-IWU shall be added to the SIP Message (BYE or final response) sent by the SIP side of the I-MGCF.

Editor's note: Is it meaningsful to indicate cause value for internal error in the network to the users.

8.4 Receipt of Status Codes 4xx, 5xx or 6xx

Editor's note: Underlined text will be added to TS 29.163 while stroken out text will be deleted in TS 29.163

Editor's note: Subclause 7.2.3.1.12 of TS 29.163 will be modified as follows:

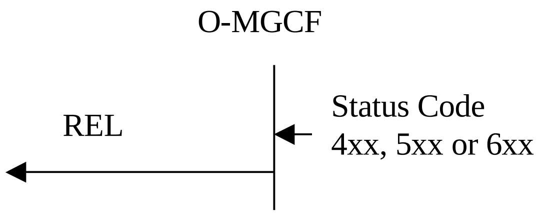

Figure 21: Receipt of Status codes 4xx, 5xx or 6xx

If a Reason header is included in a 4XX, 5XX, 6XX, then the Cause Value of the Reason header shall be mapped to the ISUP Cause Value field in the ISUP REL message. The mapping of the Reason header to the Cause Indicators parameter is shown in Table 8a (see 7.2.3.1.7). Otherwise ~~When receiving SIP response with status codes 4xx, 5xx or 6xx, the O-MGCF shall send a REL message. The~~ coding of the Cause parameter value in the REL message is derived from the SIP Status code received according to table 18. The Cause Parameter Values are defined in ITU-T Recommendation Q.850 [38].

8.5 Receipt Receipt of a BYE

Editor's note: Underlined text will be added to TS 29.163 while stroken out text will be deleted in TS 29.163

Editor's note: Subclause 7.2.3.1.13 of TS 29.163 will be modified as follows:

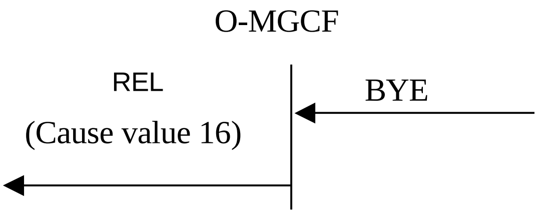

Figure 22: Receipt of BYE method

~~NOTE: If an optional Reason header field is included in the BYE, then the Cause Value can be mapped to the ISUP Cause Value field in the ISUP REL. The mapping of the Reason header to the Cause Indicators parameter is out of the scope of the present specification.~~

If a Reason header field with Q.850 Cause Value is included in the BYE, then the Cause Value shall be mapped to the ISUP Cause Value field in the ISUP REL. The mapping of the Reason header to the Cause Indicators parameter is shown in Table 8a (see 7.2.3.1.7).

On receipt of a BYE method, the O-MGCF sends a REL message with Cause Code value 16 (Normal Call Clearing).

8.6 Receipt of the Release Message

Editor's note: Underlined text will be added to TS 29.163 while stroken out text will be deleted in TS 29.163

Editor's note: Subclause 7.2.3.1.14 of TS 29.163 will be modified as follows:

In the case that the REL message is received and a final response (i.e. 200 OK (INVITE)) has already been received the O-MGCF shall send a BYE method. If the final response (i.e. 200 OK (INVITE)) has not already been received the O-MGCF shall send a CANCEL method.

A Reason header field containing the received (Q.850) Cause Value of the REL message shall be added to the CANCEL or BYE request. The mapping of the Cause Indicators parameter to the Reason header is shown in Table 9a (see 7.2.3.1.8).

8.7 Receipt of RSC, GRS or CGB (H/W oriented)

Editor's note: Underlined text will be added to TS 29.163 while stroken out text will be deleted in TS 29.163

Editor's note: Subclause 7.2.3.1.15 of TS 29.163 will be modified as follows:

Editor's note: Is it meaningsful to indicate cause value for internal error in the network to the users.

If a RSC, GRS or CGB (H/W oriented) message is received and a final response (i.e. 200 OK (INVITE) has already been received the O-MGCF shall send a BYE method. If a final response (i.e. 200 OK (INVITE)) has not already been received the O-MGCF shall send a CANCEL method.

A Reason header field containing the (Q.850) Cause Value of the REL message sent by the O-MGCF shall be added to the SIP message (BYE or CANCEL) to be sent by the SIP side of the O-IWU.

8.8 Autonomous Release at O-MGCF

Editor's note: Underlined text will be added to TS 29.163 while stroken out text will be deleted in TS 29.163

Editor's note: Subclause 7.2.3.1.16 of TS 29.163 will be modified as follows:

Editor's note: Is it meaningsful to indicate cause value for internal error in the network to the users.

If the O-MGCF determines due to internal procedures that the call shall be released then the MGCF shall send

- A BYE method if the ACK has been sent.
- A CANCEL method before 200 OK (INVITE) has been received.

NOTE: The MGCF shall send the ACK method before it sends the BYE, if 200 OK (INVITE) is received.

A Reason header field containing the (Q.850) Cause Value of the REL message sent by the O-IWU shall be added to the SIP Message (BYE or CANCEL) to be sent by the SIP side of the O-IWU.

8.9 TISPAN Simulation Services

Editor's note: This clause will be inserted as new Clause 7.5 into TS 29.163 once the referenced specifications [60] to [70] are approved. The following subchapters without number will then be numbered accordingly.

Editors Note: Piror to accept this text into normative documents there is a need for pleanery aggreement how to deal with simmulation services which do not contain a similar service in other regional versions of ISUP. This issue is related to the issue of wether ISUP document, should be reffering or using regional specific ISUPs.

The following sub-clauses describe the MGCF behaviour related to simulation services as defined in ETSI TISPAN Recommendations TS181 004 [60] – TS181 013. [68], TS181 015. [69], TS181 016. [70].

8.9.1 Originating Identification Presentation (OIP) and Originating Identification Restriction (OIR)

The mapping of Originating Identification Presentation (OIP) and Originating Identification Restriction (OIR); simulation service with the CLIP/CLIR PSTN/ISDN Supplementary Service is the same mapping as describen in Cause 7.4.1. The Service itself is described within ETSI TS 183 007 [63]

8.9.2 Terminating Identification Presentation (TIP) and Terminating Identification Restriction (TIR)

The mapping of Terminating Identification Presentation (TIP) and Terminating Identification Restriction (TIR) simulation service with the COLP/COLR PSTN/ISDN Supplementary Service is the same mapping as described in Cause 7.4.2. The Service itself is described describen within ETSI TS 183 008 [64a]

8.9.3 Malicious Communication Identification (MCID)

The mapping of Malicious Communication Identification simulation service with Malicious Call Identification services PSTN/ISDN Supplementary Service is describen within ETSI TS 183 016 [70]

8.9.4 Communication Diversion (CDIV)

The mapping of Communication Diversion simulation service with Call Diversion services PSTN/ISDN Supplementary Service is describen within ETSI TS 183 004 [60]

8.9.5 Communication Waiting (CW)

The mapping of Communication Waiting simulation service with Communication Waiting PSTN/ISDN Supplementary Service is describen within ETSI TS 183 009 [65]

8.9.6 Communication Hold (HOLD)

The mapping of Communication Hold simulation service with Call Hold PSTN/ISDN Supplementary Service is the same mapping as describen in Cause 7.4.10. The Service itself is described within ETSI TS 183 010 [66]

8.9.7 Communication Completion on busy subscriber (CCBS)

The mapping of Completion of Communications of Busy Subscriber simulation service with Completion of Calls of Busy Subscriber PSTN/ISDN Supplementary Service is describen within ETSI TS 183 015 [69]

8.9.8 Completion of Communications on No Reply (CCNR)

The mapping of Completion of Communications on No Reply simulation service with Completion of Calls on No Reply PSTN/ISDN Supplementary Service is describen within ETSI TS 183 015 [69]

8.9.10 Conference call (CONF)

The mapping of Conference call simulation service with Conference call PSTN/ISDN Supplementary Service is describen within ETSI TS 183 005 [61]

8.9.11 Incomming Communication Barring (ICB)

The mapping of Anonymus Communication Rejection simulation service with Anonymus Call Rejection PSTN/ISDN Supplementary Service is describen within ETSI TS 183 011 [67]

8.9.12 Advice of Carge (AoC)

The mapping of Advice of Carge simulation service with the Advice of Carge PSTN/ISDN Supplementary Service is describen within ETSI TS 183 012 [68]

8.9.13 Message Waiting Indication (MWI)

The mapping of Message Waiting Indication simulation service with the Message Waiting Indication PSTN/ISDN Supplementary Service is describen within ETSI TS 183 006 [62]

9 Cx interface

Editor's note: This clause is under the responsibility of CN4. Material for this clause must be submitted to CN4. CT1 will not review the content of this clause.

Editor's note: This clause will cover for requirements from providing IMS via fixed broadband with regards to the usage of DIAMETER on the Cx interface. It is intended that material from this clause will be added to TS 29.228 and TS 29.229.

Annex A (informative): Application Server (AS) establishing multiple dialogs with originating UE

Editor's note: This clause is under the responsibility of CT1. Material for this clause must be submitted to CT1.

A.1 General

Editor's note: The following text is agreed as the working assumption to establish multiple dialogs from an AS. The material in this clause is not intended to be included in any of the existing CT1 specifications.

If the AS needs to establish an early dialog between itself and the originating UE (or originating network), for example in order to establish a media path in order to send announcements or other kind of early media backwards, it shall do so by sending a provisional response towards the originating UE. The setup procedures between the originating UE and the AS are identical to normal setup procedures. The To header tag value in the dialog between the originating UE and the AS shall, in order to separate the dialogs, be different than the To header tag value in messages used on the dialog used between the originating and terminating UEs. The AS normally receives the To header tag value for the dialog between the UEs from the terminating UE (or the terminating network), but if the AS acts as a B2BUA it may also, depending on the functionality, generate a new To header value. The need for the AS to establish an early dialog between itself and the originating UE is determined on the services offered to the originating UE.

NOTE 1: Unless the originating UE can determine that the messages sent on the early dialog between itself and the AS are originated from the AS, it will assume that forking has accured in the network.

NOTE 2: If the originating UE has indicated that it does not want the initial INVITE to be forked the AS may still establish a separate early dialog between itself and the originating UE, since eventhough the originating UE may assume that the call has been forked only one terminating UE will actually received the UE (unless forking is done by another node in the signalling path).

NOTE 3: Once the originating UE has received 200 (OK) from the terminating UE the early dialog between the originating UE and the AS will be terminated, as described in RFC 3261 [4].

Annex B: Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2005-02					skeleton of the TR	0.0.0	0.0.0
2005-03					Version 0.1.0 created as a result of CT1#37 The following CR's were incorporated and the editor adopted their content / structure to the revised TR structure: N1-05-05088 - History Info Header N1-050185 - Early media using multiple dialogs N1-050375 - MWI RFC3842	0.0.0	0.1.0
2005-05					The following CR's were incorporated and the editor adopted their content / structure to the structure of the TR: C1-050570 --Improvement of representation of draft-ietf-sip-history-info C1-050763 -- move Annex A to clause 5 C1-050765 --xDSL access C3-050421 -- Addition of Interworking of TISPAN Reason header	0.1.0	0.2.0
2005-07					The following CR's were incorporated and the editor adopted their content / structure to the structure of the TR: 07TD053r2 – Inclusion of Reason in Responses in TS 24.229 07TD347r1 – Corrections to 3GPP TR 24.819 07TD395r1 – IP version considerations for fixed broadband	0.2.0	0.3.0
2005-07					The following CR’s were incorporated and the editor adopted their content / structure to the structure of the TR C1-051150 – 24.819 Editorial C1-051154 - Addition in TR 24.819 of NAT traversal scenario C1-051155 - Changes in TR 24.819 C1-051200 - Usage of Replaces Header for Conference Session Initiation C1-051207 - Addition in TR 24.819 of SIP timers and SIP compression C3-050629 - Interworking of Simulation Services	0.3.0	0.4.0
2005-09					Creation 1.0.0 was created as outcome of CT#29	0.4.0	1.0.0
2005-10					The following CR's were incorporated and the editor adopted their content / structure to the structure of the TR: C1-051257 -- Addition in TR 24.819 of NAT traversal scenario	1.0.0	1.1.0
2005-11					The following CR’s were incorporated and the editor adopted their content / structure to the structure of the TR: C1-051601 -- P-CSCF selection C1-051639 -- SIP timers in the IM CN subsystem C1-051640 – Compression in the IM CN subsystem C1-051658 – Use of SIP URI at the MGCF	1.1.0	1.2.0
2005-11					Version 2.0.0 created by MCC to be sent to TSG CT#30 for approval	1.2.0	2.0.0
2005-12	CT-30	CP-050532			Version 2.0.0 was approved and version 7.0.0 is created by MCC	2.0.0	7.0.0