3GPP TS 29.421 V8.1.0 (2010-09)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Core Network and Terminals;
Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN);
NGN Release 1;
Endorsement of 3GPP TS 29.162 Interworking between IM CN Sub-system and IP networks
(Release 8)

Keywords

3GPP, LTE, endorsement, interworking

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 Specification (TS) was been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN) and originally published as ETSI TS 183 021 [13]. It was transferred to the 3rd Generation Partnership Project (3GPP) in in January 2008.

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 describes the interworking between the TISPAN IMS and an external IP network including other IMS networks for IP multimedia service support.

The present document addresses the areas of control and user plane interworking through the network functions, which include the IBCF and I-BGF. For the specification of control plane interworking, the interworking between IMS SIP and an external SIP profile are detailed in terms of the procedures required for the support of both IMS originated and terminated SIP sessions.

In particular, the present document describes the protocol mappings for support of communications between networks using different IP versions or between networks with NATs operating at their border.

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*.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

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

[2] IETF RFC 791: "Internet Protocol".

[3] IETF RFC 2460: "Internet Protocol, Version 6 (IPv6) Specification".

[4] IETF RFC 2766: "Network Address Translation - Protocol Translation (NAT-PT)".

[5] IETF RFC 2663: "IP Network Address Translator (NAT) Terminology and Considerations".

[6] IETF RFC 3022: "Traditional IP Network Address Translator (Traditional NAT)".

[7] IETF RFC 3323: "A Privacy Mechanism for the Session Initiation Protocol (SIP)".

[8] IETF RFC 3325: "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks".

[9] IETF RFC 2475: "An Architecture for Differentiated Services".

[10] IETF RFC 792: "Internet Control Message Protocol".

[11] IETF RFC 2463: "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification".

[12] ITU-T Recommendation Q.1912.5: "Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control protocol or ISDN User Part".

[13] ETSI TS 183 021 V1.1.1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Release 1; Endorsement of 3GPP TS 29.162 Interworking between IM CN Sub-system and IP networks".

3 Abbreviations

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

B2BUA	Back-to-Back User Agent
BGCF	Border Gateway Control Function
BGF	Border Gateway Function
CDR	Call Data Record
CSCF	Call Session Control Function
DS	Differentiated Services
IBCF	Interconnection Border Control Function
I-BGF	Interconnection Border Gateway Function
IM	IP Multimedia
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPv4	IP version 4
IPv6	IP version 6
IWF	InterWorking Function
MRFP	Multimedia Resource Function Processor
NAT	Network Address Translation
NAPT	Network Address and Port Translation
NA(P)T-PT	Network Address (Port-Multiplexing) Translation-Protocol Translation
RACS	Resource and Admission Control Subsystem
RSVP	Resource reSerVation Protocol
SDP	Session Description Protocol
SIP UA	SIP User Agent
SIP	Session Initiation Protocol
UE	User Equipment

4 General

4.1 General interconnection overview

The IM Subsystem interworks with SIP RFC 3261 [11] based IP Multimedia networks. These IP Multimedia networks include:

- SIP User Agents (UAs);

- SIP Servers.

The IM Subsystem also interworks with non SIP-based IP multimedia networks (e.g. network controlled using H.323).

The general interworking model is shown in figure 1. The IMS network and the SIP based Multimedia networks may use IP version 4 RFC 791 [22] or IP version 6 RFC 2460 [33].

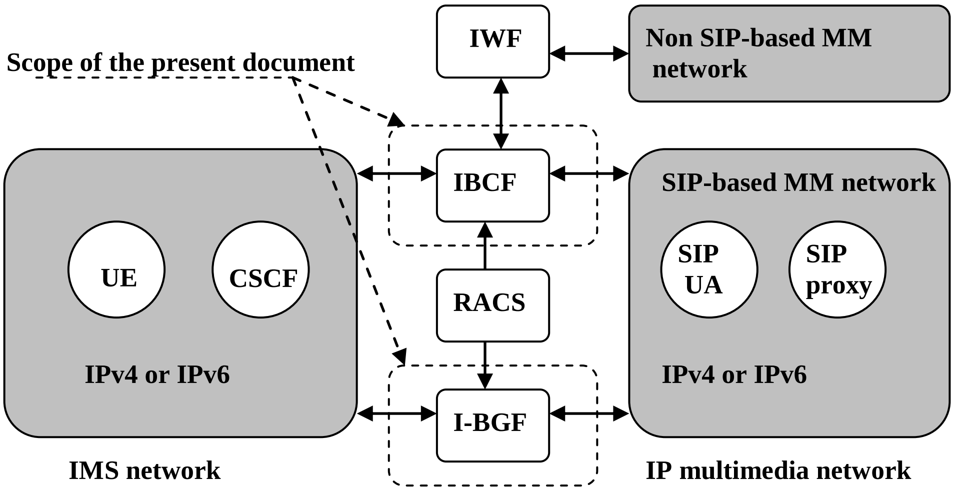

Figure 1: Interworking Model for IMS to IP Multimedia Network

The IMS uses the IBCF/I-BGF and possibly the IWF entity in order to communicate with external IP multimedia entities.

The IBCF is inserted on the SIP signalling path between the CSCF/BGCF and external IP Multimedia networks.
The I-BGF is inserted along the media path at IP interconnect between the IMS network and an external IP multimedia network.

The IBCF and the I-BGF may be implemented as a part of other physical entities in the IMS.

The IWF performs the interworking between the TISPAN SIP profile (ES 283 003 - see bibliography) and other IP multimedia protocols when required (e.g.H.323 or SIP-I as defined for profile C ITU-T Recommendation Q.1912.5 [12]).

4.2 Interworking scenarios

4.2.1 UE with TISPAN SIP profile capability connecting to an external SIP device

ES 283 003 (see bibliography) specifies the procedures used by a UE compliant to the TISPAN SIP profile to communicate with an external SIP device possibly lacking TISPAN SIP profile capabilities.

5 Network characteristics

5.1 Key characteristics of IP Multimedia Networks

The Internet is a conglomeration of networks utilizing a common set of protocols. IP protocols are defined in the relevant IETF RFCs.

IP multimedia networks provide the ability for users to invoke IP multimedia applications in order to send and receive (where applicable) voice and data communications. One protocol used to manage IP multimedia sessions is the Session Initiation Protocol (SIP) (RFC 3261 [11]).

5.2 Key characteristics of IP Multimedia Subsystem

The IMS uses the SIP protocol to manage IP multimedia sessions, and uses IP as the transport mechanism for both SIP session signalling and media transport.

6 Reference Model for control plane interworking and user plane interworking

Figure 2 details the reference architecture required to support interworking between the IM subsystem and IP networks for IM services.

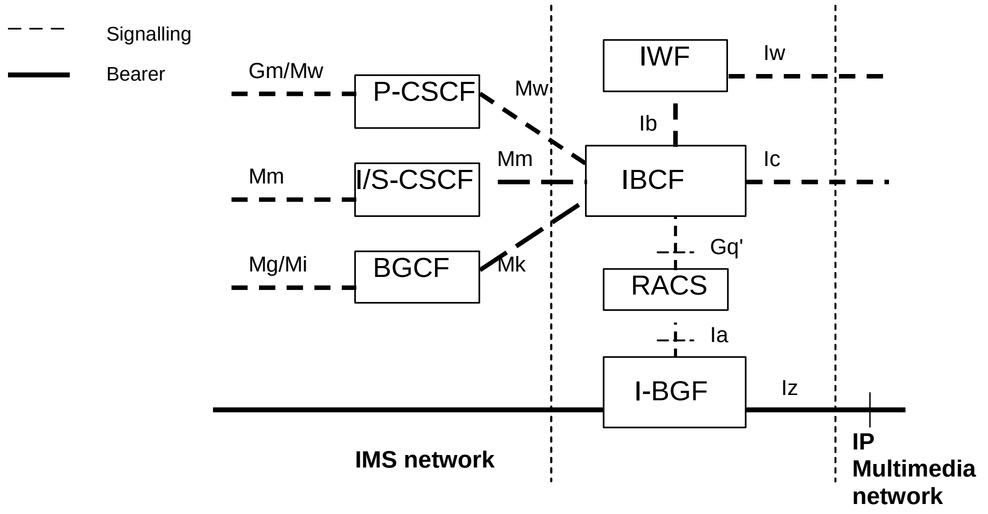

Figure 2: IM Subsystem to external IM network interworking reference architecture

Mm reference point: The call control protocol applied to the Mm interface between CSCF and IBCF is based on SIP as detailed in ES 283 003 (see bibliography).

Gq' reference point: The protocol applied at the Gq' reference point is based on Diameter and specified in TS 183 017 (see bibliography).

Ia reference point: The protocol applied at the Ia reference point is based on H.248 and is specified in ES 283 018 (see bibliography).

Ib reference point: The protocol applied at the Ib reference point between the IBCF and the IWF is based on SIP.

Ic reference point: The protocol applied at the Iw reference point is based on SIP. The SIP end point located in the external multimedia network may not support all the SIP extensions mandated by TISPAN.

6.1 Interworking Functional Entities

6.1.1 IBCF

When used for interconnecting the IMS to an external SIP based multimedia network, the IBCF behaves as a SIP B2BUA.

Further details of the functionality of the IBCF can found in ES 282 003 (see bibliography).

6.1.2 I-BGF

The I-BGF is a transport level entity containing a set of optional functionalities including but not limited to NA(P)T, Gate functionality, and IP version interworking. The complete set of standard I-BGF functionalities is specified in ES 282 003 (see bibliography).

The I-BGF shall comply with the border gateway profile specified in ES 283 018 (see bibliography).

When used as a traditional NAT (Basic NAT or NAPT), the I-BGF uses two pools of IPv4 addresses and/or ports belonging to separate realms for dynamic assignment as sessions are initiated. More detailed information on traditional NAT is given in RFC 3022 [66].

When used for IP version interworking, the I-BGF uses a pool of globally unique IPv4 addresses for assignment to IPv6 nodes on a dynamic basis as sessions are initiated across the IP version boundaries. NAT-PT binds addresses in IPv6 network with addresses in IPv4 network and vice versa to provide transparent routing between the two IP domains without requiring any changes to end points. NAPT-PT provides additional translation of transport identifier (TCP and UDP port numbers). More detailed information on the NAT-PT/NAPT-PT is given in RFC 2766 [44] and RFC 2663 [55].

The I-BGF may also act as a "Gate". A gate operates on a unidirectional flow of packets, i.e. in either the upstream or downstream direction. A gate consists of a packet classifier, and a gate status (open/closed). When a gate is open, the packets in a flow are accepted. When a gate is closed, all of the packets in the flow are dropped.

When the I-BGF provides a DiffServ Edge Function, its behaviour shall comply with the IETF specifications for Differentiated Services [99]. Parameters for the DiffServ Edge Function (i.e. classifiers, meters, packet handling actions) may be statically configured on the I-BGF or derived from RSVP signalling. The DS field values to be used may be derived from signalling at the Ia interface.

6.1.3 IWF

The IWF performs interworking between the IMS SIP profile and other multimedia signalling protocols such as H.323 or SIP-I as defined in ITU-T Recommendation Q.1912.5 Profile C [1212]. In the latter case the IWF acts as a B2BUA. The details of the interworking procedures are not specified in the present document.

7 Control plane interworking

7.1 SIP with TISPAN IMS Profile to non-IMS SIP Interworking

ES 283 003 (see bibliography) defines the behaviour of an IMS UE when communicating with SIP terminal with missing SIP capabilities required by the IMS.

7.2 Procedures at the IBCF

7.2.1 IBCF usage of SIP

The IBCF acting as a B2BUA forwards all SIP messages transparently with respect to all methods, result codes, headers with the following exceptions:

- the IBCF shall include its own SIP URI to the top of the Record-Route header within an initial request for a dialog, to place itself on the path for subsequent requests within the dialog;
- the IBCF may modify the Contact, Record-Route and Via headers to remove routing information received from an incoming SIP message before forwarding it;
- the IBCF shall apply any privacy required by RFC 3323 [77] and RFC 3325 [88] to the P-Asserted-Identity header and;
- if specified by local policy rules, the IBCF may omit or modify any other received SIP headers prior to forwarding SIP messages.

The behaviour of the IBCF regarding SIP message bodies (including SDP) is described in the following clause.

7.2.2 IBCF procedures on SIP message bodies

If IP address translation (NA(P)T or IP version interworking) occurs on the user plane, the IBCF shall modify SDP according to the corresponding clauses 9 or 10;

Additionally, the IBCF may take the followings action upon SIP message bodies:

- examine the length of a SIP message body and if required by local policy, and take an appropriate action (e.g. forward the message body transparently, reject the INVITE, remove the body), and possibly record the event in the CDR;

- examine the characteristics of the message body (i.e. check the values of any "Content-type", "Content-disposition", and "Content-language" headers), take an appropriate action defined by local policy (e.g. transit the body, remove the body, reject the call), and possibly record the event in the CDR;

- examine the content of SIP bodies, and take appropriate action defined by local policy (e.g. transit the body, remove the body, reject the call), and possibly record the event in the CDR.

8 User Plane Interworking

8.1 Overview

The present specification addresses user plane interworking between codec types used for either voice or video.

8.2 Transparent User Plane

The user plane may be transported through the IMS without being processed by any IMS functionnal entity.

8.3 Non Transparent User Plane

The MRFP may provide transcoding of the user plane if a codec mismatch occurs. It is not specified in the present release how the MRFP is inserted and controlled to provide transcoding.

9 IP Version Interworking at the IBCF/I-BGF

9.1 Control plane interworking

9.1.1 Originating Session Set-up to SIP network using different IP version

9.1.1.1 Receipt of the first SDP offer

Upon receipt of the first SDP offer the IBCF:

- provides to the RACS the IPv6 address(es) (respectively IPv4 address(es)) and port number(s) as received in the c-line(s) and m-line(s) in the SDP; and

- requests the RACS to bind corresponding IPv4 address(es) (respectively IPv6 address(es)) and port number(s) from its pool to the received IPv6 address(es) (respectively IPv4 address(es))and port number(s) to enable the routing of user plane traffic from the SIP network using different IP version through the I-BGF.

When the IBCF has received the requested information from the RACS the IBCF shall include the IPv4 address(es) (respectively IPv6 address(es)) and port number(s) in a new offer, which shall be sent to the IPv4 network (respectively IPv6 network). The IBCF shall create a SIP message in accordance with the rules for the IBCF described in ES 283 003 (see bibliography) with the following clarification:

- The IPv4 address(es) (respectively IPv6 address(es)) and port number(s) shall replace the IPv6 address(es) (respectively IPv4 address(es)) and port number(s) in the SDP.
- The IBCF shall create a Record-Route header containing its own SIP URI.

9.1.1.2 Receipt of the first SDP answer

At the receipt of the first SDP answer from the IPv4 network (respectively IPv6 network) the IBCF:

- provides to the RACS the IPv4 address(es) (respectively IPv6 address(es)) and port number(s) as received in the c-line(s) and m-line(s) in the SDP; and
- requests the RACS to bind corresponding IPv6 address(es) (respectively IPv4 address(es)) and port number(s) from its pool to the received IPv4 address(es) (respectively IPv6 address(es)) and port number(s) to enable the routing of user plane traffic towards the IPv4 network (respectively IPv6 network) through the I-BGF.

When the IBCF has received the requested information, the IBCF shall send an SDP answer to the IPv6 network (respectively IPv4 network). The IBCF shall create the SIP message in accordance with the rules for the IBCF described in ES 283 003 (see bibliography) with the following clarification:

- The IPv6 address(es) (respectively IPv4 address(es)) and port number(s) shall replace the received IPv4 address(es) (respectively IPv6 address(es)) and port number(s) in the SDP.

9.1.2 Terminating Session set-up from SIP network using different IP version

9.1.2.1 Receipt of an SDP offer

At the receipt of the first SDP offer the IBCF:

- provides to the RACS the IPv4 address(es) (respectively IPv6 address(es)) and port number(s) as received in the c-lin(es) and m-lin(es) in the SDP; and
- requests the RACS to bind corresponding IPv6 address(es) (respectively IPv4 address(es)) and port number(s) from its pool to the received IPv4 address(es) (respectively IPv6 address(es)) and port number(s) to enable the routing of user plane traffic towards the IPv4 network (respectively IPv6 network) through the I-BGF.

When the IBCF has received the requested information from the RACS the IBCF shall send an SDP offer to the IPv6 network (respectively IPv4 network). The IBCF shall create a SIP message in accordance with the rules for the IBCF described in ES 283 003 (see bibliography) with the following clarifications:

- The IPv6 address(es) (respectively IPv4 address(es)) and port number(s) shall replace the received IPv4 address(es) (respectively IPv6 address(es)) and port number(s) in the SDP.
- The IBCF shall create a Record-Route header containing its own SIP URI if the SIP message is a request.

9.1.2.2 Receipt of SDP answer

At the receipt of a SDP answer from the IPv6 network (respectively IPv4 network) the IBCF:

- Provides to the RACS the IPv6 address(es) (respectively IPv4 address(es)) and port number(s) as received in the c-line(s) and m-line(s) in the SDP.
- Requests the RACS to bind corresponding IPv4 address(es) (respectively IPv6 address(es)) and port number(s) from its pool with the received IPv6 address(es) (respectively IPv4 address(es)) and port number(s) to enable the routing of user plane traffic from the IPv4 network (respectively IPv6 network) through the I-BGF.

When the IBCF has received the requested information, the IBCF shall send a SDP answer to the IPv4 network (respectively IPv6 network). The IBCF shall create the SIP message in accordance with the rules for the IBCF described in ES 283 003 (see bibliography) with the following clarification:

- The IPv4 address(es) (respectively IPv6 network) and port number(s) shall replace the received IPv6 address(es) (respectively IPv4 address(es)) and port number(s) in the SDP.

9.1.3 Change of connection information

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

1) IP address(es) or/and port number(s) have been added. In this case additional binding(s) shall be provided by the RACS to the IBCF as detailed for the first SDP offer in the clauses above;

2) IP address(es) or/and port number(s) have been deleted. In this case binding(s) shall be made free by the RACS;

3) IP address(es) and port number(s) have been reassigned of the users. In this case the binding(s) shall reflect the reassignment;

4) No change has been made to the IP address(es) and port number(s). In this case no change shall be made to the existing binding(s).

9.1.4 Release of the session

At the receipt of BYE, CANCEL request or non 200 final responses the IBCF shall release the session and request the RACS to release the bindings established for the session.

9.2 User plane transport

9.2.1 Payload transport

The I-BGF shall use the established bindings described above to transport the messages between the IPv6 network and IPv4 network in the following way.

At the receipt of a payload message the I-BGF shall:

- Replace the received IPv4 address(es) and port number(s) in the payload message with the corresponding IPv6 address(es) and port number(s).

- Replace the received IPv6 address(es) and port number(s) in the payload message with the corresponding IPv4 address(es) and port number(s).

9.2.2 IP header interworking

9.2.2.1 IPv4 to IPv6

When the I-BGF receives an IPv4 message the following codings shall be set in the IPv6 headers of the message sent to the IPv6 network.

- If the DF bit is set and the packet is not a fragment (i.e. the MF flag is not set and the Fragment Offset is zero) The IPv6 headers shall be set as described in table 1.

- If the DF bit is not set or the packet is a fragment the IPv6 headers shall be set as described in table 2.

Table 1: Derivation of IPv6 Header from IPv4 header (no fragmentation)

IPv6 field	Value
Version	6
Traffic Class	The default behaviour is that the value of the IPv6 field Traffic Class field is the value of the IPv4 Type Of Service field (all 8 bits are copied). An implementation of a I-BGF should also provide the ability to ignore the value of the IPv4 Type of Service and always set the IPv6 traffic class field to zero.
Flow label	The Ipv6 Flow Label Field is set to 0 (all zero bits).
Payload Length	The IPv6 Payload Length field value is the IPv4 Total length field value minus the size of the IPv4 header and IPv4 options field length, if present.
Next Header	The IPv6 Next Header value is copied from IPv4 Protocol field.
Hop Limit	The IPv6 Hop Limit value is The value of IPv4 field Time To Live minus 1.
Source Address	Shall be handled as the addresses of the payload message as described in clause 9.2.1.
Destination Address	Shall be handled as the addresses of the payload message as described in clause 9.2.1.

Table 2: Derivation of IPv6 Header from IPv4 Header (fragmentation)

IPv6 field	Value
Version	6
Traffic Class	The default behaviour is that the value of the IPv6 field Traffic Class field is the value of the IPv4 Type Of Service field (all 8 bits are copied). An implementation of a I-BGF should also provide the ability to ignore the value of the IPv4 Type of Service and always set the IPv6 traffic class field to zero.
Flow label	The Ipv6 Flow Label Field is set to 0 (all zero bits).
Payload Length	The IPv6 Payload Length field value is the IPv4 Total length field value plus 8 for the fragment header minus the size of the IPv4 header and IPv4 options field length, if present.
Next Header	The IPv6 Next header field is set to Fragment header (44).
Hop Limit	The IPv6 Hop Limit value is The value of IPv4 field Time To Live minus 1.
Source Address	Shall be handled as the addresses of the payload message as described in clause 9.2.1.
Destination Address	Shall be handled as the addresses of the payload message as described in clause 9.2.1.

IPv6 field	Value
Version	6
Fragments headers a) next header b) fragment Offset c) More fragment bit d) Identification	 Copied from IPv4 Protocol field. Copied from the IPv4 Fragment offset field. Copied from the value of the more fragment bit in the IPv4 flags field. The value of this field should be mapped from the triple of the source address, destination address and IPv4 identification field of the incoming packet/fragments to a unique value for the source and destination address of the outgoing IPv6 packet/fragments.

9.2.2.2 Abnormal cases

If IPv4 options are present in the IPv4 packet, they should be ignored i.e. there is no attempt to translate them. However, if an unexpired source route option is present then the packet shall instead be discarded, and an ICMPv4 "destination unreachable/source route failed" Type 3/Code 5 error message shall be returned to the sender as defined in RFC 792 [1010].

When a translator receives the first fragment of a fragmented UDP IPv4 packet and the checksum field is zero the translator should drop the packet and generate a system management event specifying at least the IP addresses and port numbers in the packet. When it receives fragments other than the first it should silently drop the packet since there is no port information to log.

When a translator receives an unfragmented UDP IPv4 packet and the checksum field is zero the translator shall compute the missing UDP checksum as part of translating the packet. Also, the translator should maintain a counter of how many UDP checksums are generated in this manner.

9.2.2.3 IPv6 to IPv4

When the I-BGF receives an IPv6 message the following codings shall be set in the IPv4 headers of the message sent to the IPv4 network.

- If there is no IPv6 fragment header, the IPv4 header fields shall be set as described in table 3.
- If there is an IPv6 fragment header, the IPv4 header fields shall be set as described in table 4.

Table 3: Derivation of IPv4 Header from IPv6 Header (no fragmentation)

IPv4 field	Value
Version	4
Internet header length	5 (No IPv4 options).
Type of Service	The default behaviour is that the value of the IPv4 field Type of service field is the value of the IPv6 Traffic class field (all 8 bits are copied). An implementation of a I-BGF should also provide the ability to ignore the value of the IPv6 Traffic Class and always set the IPv4 Type of Service field to zero.
Total length	The IPv4 Total Length field value is the IPv6 Payload length value plus the size of the IPv4 headers.
Identification	All bits are set to zero.
Flags	The more fragment flag is set to zero. The Don't fragment flag is set to one.
Fragment offset	Set to zero

IPv4 field	Value
Version	4
Time to live (TTL)	The value of the field shall be set to the received IPv6 Hop Limit field value minus 1.
Protocol	The IPv4 field Protocol shall be set to the value of IPv6 field The next header value.
Header checksum	Computed once the IPv4 header has been created.
Source Address	Shall be handled as the addresses of the payload message as described in clause 9.2.1.
Destination Address	Shall be handled as the addresses of the payload message as described in clause 9.2.1.

Table 4: Derivation of IPv4 Header from IPv6 Header (fragmentation)

IPv4 field	Value
Version	4
Internet header length	5 (No IPv4 options).
Type of Service and Precedence	The default behaviour is that the value of the IPv4 field Type of service field is the value of the IPv6 Traffic class field (all 8 bits are copied). An implementation of a I-BGF should also provide the ability to ignore the value of the IPv6 Traffic Class and always set the IPv4 Type of Service field to zero.
Total length	The IPv4 Total Length field value is the IPv6 Payload length value plus the size of the IPv4 headers minus 8 for the Fragment header.
Identification	The value of this field should be mapped from the triple of the source address, destination address and IPv6 fragmentation header field “identification” of the incoming packet/fragments to a unique value for the source and destination address of the outgoing IPv4 packet/fragments.
Flags	The IPv4 More Fragments flag is copied from the IPv6 M flag in the IPv6 Fragment header. The IPv4 Don't Fragments flag is set to zero allowing this packet to be fragmented by IPv4 routers.
Time to live (TTL)	The value of the field shall be set to the received IPv6 Hop Limit field value minus 1.
Protocol	The IPv4 field Protocol shall be set to the value of IPv6 field The next header value.
Header checksum	Computed once the IPv4 header has been created.
Source Address	Shall be handled as the addresses of the payload message as described in clause 9.2.1.
Destination Address	Shall be handled as the addresses of the payload message as described in clause 9.2.1.

9.2.2.4 Abnormal cases

If any of an IPv6 hop-by-hop options header, destination options header, or routing header with the Segments Left field equal to zero are present in the IPv6 packet, they are ignored i.e. there is no attempt to translate them. However, the Total Length field and the Protocol field shall be adjusted to "skip" these extension headers.

If a routing header with a non-zero Segments Left field is present then the packet shall be translated, and an ICMPv6 "parameter problem/erroneous header field encountered" Type 4/Code 0 error message as defined in RFC 2463 [1111], with the Pointer field indicating the first byte of the Segments Left field should be returned to the sender.

9.2.3 Fragmentation

If the DF flag is not set and the IPv4 packet will result in an IPv6 packet larger than 1 280 bytes the I-BGF shall prior to transferring it in the IPv6 network:

- Add the fragment header to the message.
- Fragment the IPv4 packets so that their length, excluding the IPv4 header, is at most 1 232 bytes (1 280 - 40 for the IPv6 header and 8 for the Fragment header).

9.2.4 Abnormal cases

As a part of decrementing the Time To Live/Hop Limit value and the I-BGF discovers that the zero value is reached the I-BGF shall send an ICMPv4/ICMPv6 message with the error "time to live exceeded in transit" type 11 code 0 as defined in RFC 792 [1010] and "hop limit exceeded in transit" type 3 code 0 as defined in RFC 2463 [1111].

10 Procedures for NAT at the IBCF/I-BGF

10.1 Control plane interworking

10.1.1 Session set-up

10.1.1.1 Receipt of the first SDP offer

Upon receipt of the first SDP offer, the IBCF shall:

- provide the RACS with the IP address(es) and port number(s) received in the c-line(s) and m-line(s) in the SDP body, and
- request the RACS to bind corresponding IP address(es) and port number(s) from its pool to the received IP address(es) and port number(s).

Upon receipt of requested information from the RACS, the IBCF shall include the IP address(es) and port number(s) received from the RACS in a new SDP offer to be forwarded. The IBCF shall create a SIP message in accordance with the rules for the IBCF described in the present specification with the following clarification:

- the IP address(es) and port number(s) received from the RACS shall replace the IP address(es) and port number(s) previously set in the SDP offer.

10.1.1.2 Receipt of the SDP answer

Upon receipt of the SDP answer, the IBCF shall:

- provide the RACS with the IP address(es) and port number(s) as received in the c-line(s) and m-line(s) in the SDP body, and
- request the RACS to bind corresponding IP address(es) and port number(s) from its pool to the IP address(es) and port number(s) received in the SDP answer.

Upon receipt of requested information from the RACS, the IBCF shall include the IP address(es) and port number(s) received from the RACS in a new SDP answer to be forwarded. The IBCF shall create a SIP message in accordance with the rules for the IBCF described in the present specification with the following clarification:

- the IP address(es) and port number(s) received from the RACS shall replace the IP address(es) and port number(s) previously set in the SDP answer.

10.1.1.3 Procedures in support of forking

The IBCF may receive multiple provisional responses with an SDP body due to forking of a request before the first final answer is received. For each SDP body received in such subsequent provisional responses, the IBCF shall apply the same procedures as described in clauses 10.1.1.1 and 10.1.1.2.

Upon receipt of the first 200 (OK) response to an INVITE request, the IBCF shall release any existing bindings corresponding to reservations made on receipt of provisional responses for which no final response has yet been received.

Upon receipt of any subsequent 200 (OK) response to an INVITE request, the IBCF shall not reserve any new bindings.

10.1.2 Change of media connection data

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

1) IP address(es) or/and port number(s) have been added. In this case, the additional binding(s) shall be provided by the IBCF to the RACS as detailed for the first SDP clauses above;

2) IP address(es) or/and port number(s) have been deleted. In this case, the corresponding binding(s) shall be made free by the IBCF;

3) IP address(es) and port number(s) have been reassigned to the users. In this case the binding(s) shall reflect this reassignment;

4) no change has been made to the IP address(es) and port number(s). In this case no change shall be made to existing binding(s).

10.1.3 Release of the session

Upon receipt of BYE, CANCEL request or non 2XX final responses, the IBCF shall release the session and request the RACS to release the bindings established for the session.

10.2 User plane

The H.248 Border Gateway profile specified in ES 283 018 (see bibliography) enables the RACS to efficiently manage the IP flows transiting through the I-BGF.

For example, when the RACS requests the I-BGF for a local IP address, the I-BGF reserves an address in its pool, and returns the address to the RACS. A binding is created between this address where the I-BGF will receive packets and the address specified by the RACS where the I-BGF is expected to forward those received packets. The destination address and ports are hence modified according to the properties of the two ephemeral terminations involved in the context.

The I-BGF may also modify the source address and port of forwarded IP packets. The source address and port of the packets sent by a given termination of the I-BGF can be set either to the address and port at which packets are received by this termination (value specified in the local descriptor) or to the address and port specified by the RACS (see annex B of ES 283 018 (see bibliography)).

The above mechanisms allow the RACS to control media level NAT within the I-BGF.

Annex A (informative): Bibliography

ETSI ES 282 007: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Release 1; Core IMS architecture".

ETSI TS 182 006: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Release 1; NGN-IMS Stage 2 definition (endorsement of TS.23.228)".

ETSI ES 282 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Release 1: Functional Architecture; Resource and Admission Control Sub-system (RACS)".

ETSI ES 283 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Endorsement of "IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Stage 3 (Release 6)" for NGN Release 1".

ETSI ES 283 018: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); H.248 Profile For The Ia Interface".

ETSI TS 183 017: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN Release 1; Stage 3 description of the Gq' interface".

IETF RFC 2765: "Stateless IP/ICMP Translation Algorithm (SITT)".

Annex B (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2005-09					Publication as **ETSI TS 183 021**		1.1.1
2008-01					Conversion to **3GPP TS 29.421**		1.1.2
2008-03	TSG#39				MCC update to version 7.0.0 after approval at TSG CT#39	1.1.2	7.0.0
2008-03	TSG#39				MCC update to version 8.0.0 after approval at TSG CT#39	7.7.0	8.0.0
2008-12	TSG#42				Upgraded to v8.0.1 due to simple upgrade without no technical change	8.0.0	8.0.1
2010-09	TSG#49	CP-100605	2	1	Processing of fragmentation	8.0.1	8.1.0