International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3401

(03/2007)

SERIES Q: SWITCHING AND SIGNALLING

Signalling requirements and protocols for the NGN – Service and session control protocols

---

NGN NNI signalling profile (protocol set 1)

ITU-T Recommendation Q.3401

ITU-T

International Telecommunication Union

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1–Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4–Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60–Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100–Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4, 5, 6, R1 AND R2	Q.120–Q.499
DIGITAL EXCHANGES	Q.500–Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600–Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM No. 7	Q.700–Q.799
Q3 INTERFACE	Q.800–Q.849
DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1	Q.850–Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000–Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100–Q.1199
INTELLIGENT NETWORK	Q.1200–Q.1699
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000	Q.1700–Q.1799
SPECIFICATIONS OF SIGNALLING RELATED TO BEARER INDEPENDENT CALL CONTROL (BICC)	Q.1900–Q.1999
BROADBAND ISDN	Q.2000–Q.2999
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR THE NGN	Q.3000–Q.3999
General	Q.3000–Q.3029
Network signalling and control functional architecture	Q.3030–Q.3099
Network data organization within the NGN	Q.3100–Q.3129
Bearer control signalling	Q.3130–Q.3179
Signalling and control requirements and protocols to support attachment in NGN environments	Q.3200–Q.3249
Resource control protocols	Q.3300–Q.3369
Service and session control protocols	**Q.3400–Q.3499**
Service and session control protocols – supplementary services	Q.3600–Q.3649
NGN applications	Q.3700–Q.3849
Testing for NGN networks	Q.3900–Q.3999

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation Q.3401

NGN NNI signalling profile (protocol set 1)

Summary

ITU-T Recommendation Q.3401 defines the IP network-to-network interface (NNI) signalling profile for use between NGN carriers of protocol set 1 for voiceband services.

Source

ITU-T Recommendation Q.3401 was approved on 9 March 2007 by ITU-T Study Group 11 (2005-2008) under the ITU-T Recommendation A.8 procedure.

Keywords

NGN, profile, SDP, SIP, signalling.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

ITU-T Recommendation Q.3401

NGN NNI signalling profile (protocol set 1)

1 Scope

This Recommendation contains a service-level profile, i.e., SIP/SDP interface description, between two network operators (NNI signalling profile), where the two different network operators may support different SIP/SDP profiles (i.e., they differ in terms of the SIP extensions, SIP information elements and SDP lines which are supported). Transport-level profile, e.g., RTP, is described as necessary as the media are described in the service-level signalling.

NOTE 1 – Specification of the interworking between the SIP/SDP profile contained in this Recommendation and the SIP/SDP profiles in each operator's network (i.e., the functions contained inside the interworking entity/entities at the network boundary) is out of scope of this Recommendation.

For the protocol set 1 of the NGN NNI signalling profile, this Recommendation covers the voiceband services such as VoIP (audio, text and so on), DTMF and T.38 fax.

NOTE 2 – Support for a mobility management interface is not supported in this version of this interface. However, nomadicity of users between different networks is supported.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

2.1 ITU-T references

[ITU-T G.711] ITU-T Recommendation G.711 (1988), *Pulse code modulation (PCM) of voice frequencies.*

[ITU-T G.722] ITU-T Recommendation G.722 (1988), *7 kHz audio-coding within 64 kbit/s.*

[ITU-T G.722.1] ITU-T Recommendation G.722.1 (2005), *Low-complexity coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss.*

[ITU-T G.722.2] ITU-T Recommendation G.722.2 (2003), *Wideband coding of speech at around 16 kbit/s using Adaptive Multi-Rate Wideband (AMR-WB).*

[ITU-T G.726] ITU-T Recommendation G.726 (1990), *40, 32, 24, 16 kbit/s Adaptive Differential Pulse Code Modulation (ADPCM).*

[ITU-T G.729] ITU-T Recommendation G.729 (1996), *Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP).*

[ITU-T G.729A] ITU-T Recommendation G.729 Annex A (1996), *Reduced complexity 8 kbit/s CS-ACELP speech codec.*

[ITU-T G.729.1] ITU-T Recommendation G.729.1 (2006), *G.729-based embedded variable bit-rate coder: An 8-32 kbit/s scalable wideband coder bitstream interoperable with G.729.*

[ITU-T Q.761] ITU-T Recommendation Q.761 (1999), *Signalling System No. 7 – ISDN User Part functional description.*

[ITU-T Q.762] ITU-T Recommendation Q.762 (1999), *Signalling System No. 7 – ISDN User Part general functions of messages and signals.*

[ITU-T Q.763] ITU-T Recommendation Q.763 (1999), *Signalling System No. 7 – ISDN User Part formats and codes.*

[ITU-T Q.764] ITU-T Recommendation Q.764 (1999), *Signalling System No. 7 – ISDN User Part signalling procedures.*

[ITU-T Q.1912.5] ITU-T Recommendation Q.1912.5 (2004), *Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control protocol or ISDN User Part.*

[ITU-T T.38] ITU-T Recommendation T.38 (2005), *Procedures for real-time Group 3 facsimile communication over IP networks.*

[ITU-T T.140] ITU-T Recommendation T.140 (1998), *Protocol for multimedia application text conversation.*

[ITU-T Y.2012] ITU-T Recommendation Y.2012 (2006), *Functional requirements and architecture of the NGN release 1.*

2.2 IETF references

2.2.1 Service-level signalling specifications

[RFC 2046] IETF RFC 2046 (1996), *Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types*.

[RFC 2327] IETF RFC 2327 (1998), *SDP: Session Description Protocol*.

[RFC 2976] IETF RFC 2976 (2000), *The SIP INFO Method*.

[RFC 3087] IETF RFC 3087 (2001), *Control of Service Context using SIP Request-URI*.

[RFC 3204] IETF RFC 3204 (2001), *MIME media types for ISUP and QSIG Objects*.

[RFC 3261] IETF RFC 3261 (2002), *SIP: Session Initiation Protocol*.

[RFC 3262] IETF RFC 3262 (2002), *Reliability of Provisional Responses in the Session Initiation Protocol (SIP).*

[RFC 3264] IETF RFC 3264 (2002), *An Offer/Answer Model with the Session Description Protocol (SDP).*

[RFC 3265] IETF RFC 3265 (2002), *Session Initiation Protocol (SIP)-Specific Event Notification*.

[RFC 3311] IETF RFC 3311 (2002), *The Session Initiation Protocol (SIP) UPDATE Method.*

[RFC 3312] IETF RFC 3312 (2002), *Integration of Resource Management and Session Initiation Protocol (SIP).*

[RFC 3323] IETF RFC 3323 (2002), *A Privacy Mechanism for the Session Initiation Protocol (SIP)*.

[RFC 3324] IETF RFC 3324 (2002), *Short Term Requirements for Network Asserted Identity*.

[RFC 3325] IETF RFC 3325 (2002), *Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks*.

[RFC 3326] IETF RFC 3326 (2002), *The Reason Header Field for the Session Initiation Protocol (SIP).*

[RFC 3398] IETF RFC 3398 (2002), *Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping*.

[RFC 3420] IETF RFC 3420 (2002), *Internet Media Type message/sipfrag*.

[RFC 3428] IETF RFC 3428 (2002), *Session Initiation Protocol (SIP) Extension for Instant Messaging*.

[RFC 3455] IETF RFC 3455 (2003), *Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP).*

[RFC 3515] IETF RFC 3515 (2003), *The Session Initiation Protocol (SIP) Refer Method*.

[RFC 3824] IETF RFC 3824 (2004), *Using E.164 numbers with the Session Initiation Protocol (SIP).*

[RFC 3840] IETF RFC 3840 (2004), *Indicating User Agent Capabilities in the Session Initiation Protocol (SIP).*

[RFC 3841] IETF RFC 3841 (2004), *Caller Preferences for the Session Initiation Protocol (SIP).*

[RFC 3891] IETF RFC 3891 (2004), *The Session Initiation Protocol (SIP) Replaces Header*.

[RFC 3892] IETF RFC 3892 (2004), *The Session Initiation Protocol (SIP) Referred-By Mechanism*.

[RFC 3893] IETF RFC 3893 (2004), *Session Initiation Protocol (SIP) Authenticated Identity Body (AIB) Format*.

[RFC 3911] IETF RFC 3911 (2004), *The Session Initiation Protocol (SIP) Join Header*.

[RFC 3959] IETF RFC 3959 (2004), *The Early Session Disposition Type for the Session Initiation Protocol (SIP).*

[RFC 3960] IETF RFC 3960 (2004), *Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP).*

[RFC 3966] IETF RFC 3966 (2004), *The tel URI for Telephone Numbers*.

[RFC 4028] IETF RFC 4028 (2005), *Session Timers in the Session Initiation Protocol (SIP).*

[RFC 4032] IETF RFC 4032 (2005), *Update to the Session Initiation Protocol (SIP) Preconditions Framework*.

[RFC 4235] IETF RFC 4235 (2005), *An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP).*

[RFC 4244] IETF RFC 4244 (2005), *An Extension to the Session Initiation Protocol (SIP) for Request History Information*.

[RFC 4412] IETF RFC 4412 (2006), *Communications Resource Priority for the Session Initiation Protocol (SIP).*

[RFC 4458] IETF RFC 4458 (2006), *Session Initiation Protocol (SIP) URIs for Applications such as Voicemail and Interactive Voice Response (IVR).*

[RFC 4483] IETF RFC 4483 (2006), *A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages*.

[RFC 4566] IETF RFC 4566 (2006), *SDP: Session Description Protocol.*

[RFC 4694] IETF RFC 4694 (2006), *Number Portability Parameters for the tel URI*.

2.2.2 Transport-level specifications

[RFC 2833] IETF RFC 2833 (2000), *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals.*

[RFC 3267] IETF RFC 3267 (2002), *Real-Time Transport Protocol (RTP) Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs.*

[RFC 3389] IETF RFC 3389 (2002), *Real-time Transport Protocol (RTP) Payload for Comfort Noise.*

[RFC 3550] IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications.*

[RFC 3551] IETF RFC 3551 (2003), *RTP Profile for Audio and Video Conferences with Minimal Control.*

[RFC 4103] IETF RFC 4103 (2005), *RTP Payload for Text Conversation.*

2.3 ETSI references

[EN 301 703] ETSI EN 301 703 V7.0.2 (1999), *Digital cellular telecommunications system (Phase 2+) (GSM); Adaptive Multi-Rate (AMR); Speech processing functions; General description (GSM 06.71 version 7.0.2 Release 1998).*

2.4 Other references

[TIA-127-A] TIA-127-A (2004), *Enhanced Variable Rate Codec Speech Service Option 3 for Wideband Spread Spectrum Digital Systems.*

[TIA-1016] TIA-1016-A (2006), *Source-Controlled Variable-Rate Multimode Wideband Speech Codec (VMR-WB), Service Options 62 and 63 for Spread Spectrum Systems.*

3 Definitions

For SIP- and SDP-specific terminology, reference shall be made to [RFC 3261], [RFC 3264] and [RFC 2327]. For NGN-specific terminology, reference shall be made to [ITU-T Y.2012]. Definitions for additional terminology used in this Recommendation are as follows:

3.1 codec list: A codec list defines the codecs that should be announced in SIP/SDP messages exchanged over the NNI based on a bilateral agreement established between the NGNs.

NOTE – The purpose of the codec list is to promote interoperability, limit the number of transcodings on network connections and possibly improve network resource management.

3.2 service control functions (**SCF**): The service control functions establish, monitor, support and release multimedia sessions, and manage the user's service interactions.

3.3 SIP back-to-back user agent (B2BUA): A back-to-back user agent (B2BUA) is a concatenation of a SIP user agent client (UAC) and user agent server (UAS).

NOTE – The IETF defines the B2BUA in [RFC 3261] as "a logical entity that receives a request and processes it as a user agent server (UAS). In order to determine how the request should be answered, it acts as a user agent client (UAC) and generates requests. Unlike a proxy server, it maintains dialog state and shall participate in all requests sent on the dialogs it has established. Since it is a concatenation of a UAC and UAS, no explicit definitions are needed for its behavior." (UAC and UAS bahaviors are defined in [RFC 3261].) A B2BUA reformulates a message before sending it as a new request.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ACM	Address Complete Message
AMR	Adaptive Multirate (codec)
ANM	Answer Message
B2BUA	Back-to-Back User Agent
BGC-FE	Breakout Gateway Control Functional Entity
CSC-FE	Call Session Control Functional Entity
EVRC	Enhanced Variable Rate Codec
FQDN	Fully Qualified Domain Name
IAM	Initial Address Message
IBC-FE	Interconnection Border gateway Control Functional Entity
IBG-FE	Interconnection Border Gateway Functional Entity
ISUP	ISDN User Part
MG	Media Gateway
MGC-FE	Media Gateway Control Functional Entity
MIME	Multipurpose Internet Mail Extensions
NGN-TE	NGN Terminal Equipment
NNI	Network-to-Network Interface
PSTN	Public Switched Telephone Network
PT	Payload Type
REL	Release
RFC	Request For Comments
RLC	Release Complete
RTCP	RTP Control Protocol
RTP	Real-time Transport Protocol
SCF	Service Control Functions
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SG-FE	Signalling Gateway Functional Entity
SIP	Session Initiation Protocol
SIP-I	SIP with encapsulated ISUP
SIPS	Session Initiation Protocol Secure
TCP	Transmission Control Protocol
TMG-FE	Trunk Media Gateway Functional Entity
UA	User Agent
UAC	User Agent Client

UAS	User Agent Server
UDP	User Datagram Protocol
UNI	User-to-Network Interface
URI	Universal Resource Identifier
VMR-WB	Variable-Rate Multi-Mode Wideband

5 Reference model

Figure 5-1 illustrates the interface covered by this Recommendation in the NGN architecture defined in [ITU-T Y.2012].

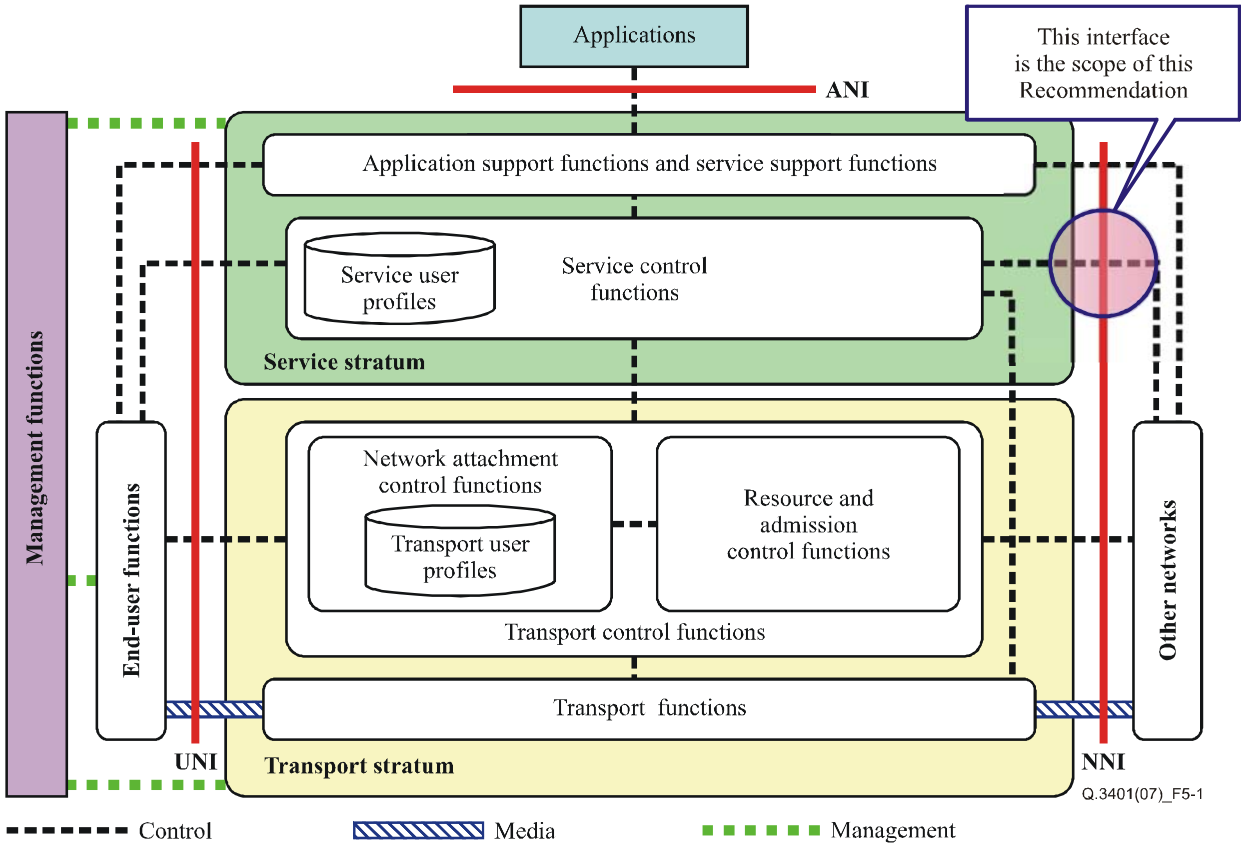


Figure 5-1 – The interface covered by this Recommendation within the NGN architecture

Figure 5-2 illustrates the interconnection reference model for the NNI.

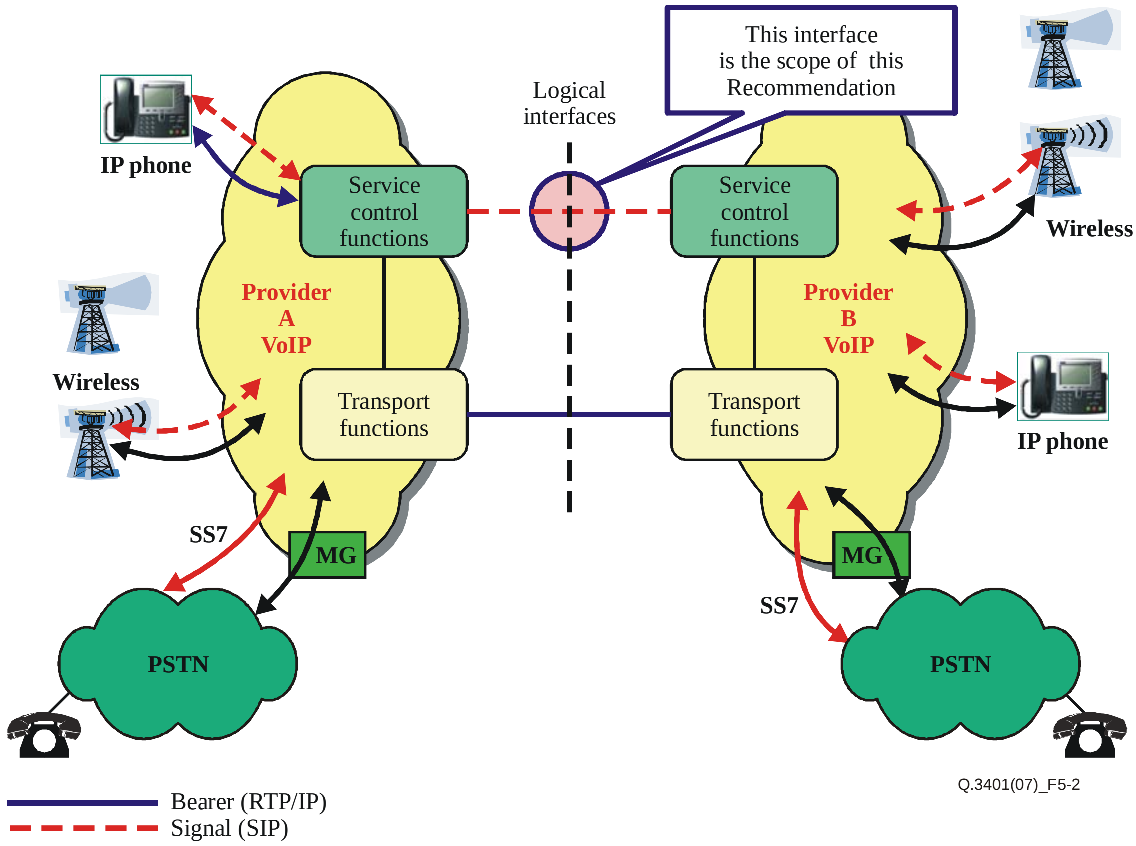


Figure 5-2 – VoIP interconnection reference model

6 Assumptions

This Recommendation is based on the following set of assumptions:

1) It is recognized that data-oriented call control (e.g., http to a web portal on an application server), in addition to SIP-oriented call control, may occur across the NNI. For example, a network-based service may allow a user to initiate calls or control the disposition of incoming calls through a web browser interface using http. It is assumed that such data-oriented call control involves no differentiated treatment from other data traffic, and so is not described further in this Recommendation. Differentiated treatment may be desirable in some cases.

2) The logical interfaces associated with the service control functions in the service stratum and the transport functions in the transport stratum enable interconnection between two service provider networks in a peering environment.

3) Each provider may use a set of service control functions and transport functions to connect to multiple peer networks.

4) SIP back-to-back user agent (B2BUA) functions may be used in support of network interconnection.

5) Only the network-to-network interface (NNI) is supported between two peering VoIP carriers. There may be an IP transit network between two peering VoIP service providers.

6) SIP is used for service-level signalling. The SIP messages may contain MIME encapsulated ISUP in order to facilitate interoperability with the PSTN. ISUP is specified in [ITU-T Q.761]-[ITU-T Q.764].

7) RTP is used for voice transport.

8) IPv4 is supported at the NNI. Support for IPv6 is optional based on bilateral agreement.

9) The IPv6 operator is responsible for IPv4/IPv6 interworking.

7 Media availability in a SIP session

The following apply to any media session established across the NNI using SIP:

a) The terminating-side network of the NNI shall pass any media packets in the direction toward the originating party as soon as they are available. A primary reason is to allow the caller to hear inband call progress tones if PSTN interworking is encountered on a voice call.

b) The originating-side network of the NNI:

- shall pass media packets from the originating party in the direction toward the terminating party upon and after receiving a final SDP answer within a SIP 2xx response to the INVITE for normal dialog;
- may pass media packets from the originating party in the direction toward the terminating party as early as the first SDP answer has occurred, which is in a SIP 1xx response to the INVITE when early dialog has been set up. A network, as a policy, may choose not to send media packets from the originating party until the final SDP offer/answer has been made in order to avoid theft-of-service in cases where usage-sensitive billing is employed.

c) As per [RFC 3261], once a SIP dialog has ended, the flow of media packets shall be halted.

d) The absence of media packets across the NNI over any time interval in either direction shall not be taken by either network as a sufficient reason to clear the SIP session. When the status of media flows is active according to the SDP negotiation, the absence of packets across the NNI for a given duration may constitute a reason to clear the SIP session.

NOTE – The absence of packets across the NNI for a given duration can be a reason to clear the SIP session only when it is sure that it is because of the failure.

8 Codec

8.1 Codec list

It is the responsibility of entities at the rim of the NGN (e.g., NGN-TE) and network equipment originating and terminating the NGN IP media flows to negotiate and select a common codec for each "end-to-end" media session. Therefore, the NGN shall allow end-to-end negotiation within the agreed codec list between NGN entities (terminals and network elements) and may allow it outside the list based on its network policy.

NOTE 1 – In case a common codec cannot be negotiated, this Recommendation does not provide procedures for the NNI.

NOTE 2 – In the interest of promoting interoperability, limiting the number of transcodings on network connections and possibly improving network resource management, it is desirable that the NGNs establish bilateral agreements about the codec list. SIP/SDP messages exchanged over the NNI indicate a request to use one or more of the codecs in this codec list.

The way of handling messages with codecs that are not in the codec list or with no codec in the list depends on the network policy, i.e., some networks may allow the use of codecs that are not in the codec list, while others may reject such messages.

Agreement on a codec list does not put any direct requirement on the codecs that have to be implemented in the network for transcoding purposes, nor does it mean that terminals shall support all the codecs in the list. Hence, conformance of a SIP/SDP offer to the agreed list does not ensure successful codec negotiation.

NOTE 3 – When the codecs to be supported across an NNI is restricted, due to network policy, a bilateral agreement, as in Note 2 is desirable. When such a bilateral agreement cannot be established, the codec list shall contain G.711 A/mu law [ITU-T G.711].

NOTE 4 – While any codec may be used within the codec list based on the bilateral agreement, it is recommended that the list contain AMR NB [EN 301 703], EVRC [TIA-127-A], G.729 [ITU-T G.729], G.729A [ITU-T G.729A], G.722.1 [ITU-T G.722.1] and G.726 [ITU-T G.726]. To enable the provision of voice service with a superior quality, it is highly recommended that the list contain a wideband codec such as AMR-WB [ITU-T G.722.2], VMR-WB [TIA-1016], G.722 [ITU-T G.722], G.729.1 [ITU-T G.729.1]. To support hard of hearing, it is recommended that T.140 [ITU-T T.140] is supported as a codec in the codec list. Where the interconnect is to an existing PSTN/ISDN, it is recommended that T.140 [ITU-T T.140] is adapted to be carried over G.711 A/mu law [ITU-T G.711].

NOTE 5 – For individual sessions, a call signalling element, such as a CSC-FE, an application server or an IBC-FE, that has visibility of the end-to-end codec negotiation may determine the need and may initiate transcoding between the endpoints.

NOTE 6 – Although transcoding should be avoided wherever possible, the network may support transcoding to increase the chance of session establishment (e.g., in configurations where the codecs supported by the endpoints belong to the agreed list but no common codec can be found). However, agreement on a codec list does not imply that the network should support transcoding between one of the codecs in the list and any other codec, nor between any combination of the codecs in the list.

8.2 Packetization size

When a packetization size is not selected by codec negotiation between terminals and/or network elements or agreed by bilateral arrangement, a speech packetization sampling size of 10 ms should be used for G.711 coded speech; this is recommended as an optimum value balancing end-to-end delay with network utilization. It is recognized that there may be network constraints that require that a higher value is agreed by bilateral arrangement; in such cases, a value of 20 ms is recommended. It is also recognized that there should be a bilateral agreement on an upper limit of packetization size that should not be exceeded, e.g., 60 ms.

NOTE – Where a packetization size is selected by codec negotiation between terminals and/or network elements, this Recommendation places no requirements on the value to be selected.

9 Routing and addressing

Table 9-1 describes URI formats that shall be supported on the NNI. Other formats may be supported.

Table 9-1 – URI formats

SIP URI	sip:+[country code][national number]@host;user=phone
	Description: Global E.164 number
	Reference: [RFC 3966]
tel URI	tel:+[country code][national number]
	Description: Global E.164 number
	Reference: [RFC 3966]

There can be several ways for determining the destination of the SIP message based on the tel URI; ENUM-based routing, number-based routing, and so on. In this Recommendation, it is assumed that each network knows the address information of the peer network based on the number.

10 Service level signalling profile

10.1 RFCs to be supported

M: Mandatory. The NNI shall comply with the listed RFC unless otherwise agreed bilaterally between carriers. For further information on the handling of elements in the mandatory RFCs, see the relevant clause below.

O: Optional. The NNI may comply with the listed RFC unless otherwise agreed bilaterally between carriers.

Table 10-1 – RFCs to be supported

SIP Extensions	Title	M/O
RFC 2046 [RFC 2046]	Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types	O
RFC 2327 [RFC 2327]	SDP: Session Description Protocol	M
RFC 2976 [RFC 2976]	The SIP INFO Method	O
RFC 3087 [RFC 3087]	Control of Service Context using SIP Request-URI	O
RFC 3204 [RFC 3204]	MIME media types for ISUP and QSIG Objects	O
RFC 3261 [RFC 3261]	SIP: Session Initiation Protocol	M
RFC 3262 [RFC 3262]	Reliability of Provisional Responses in the Session Initiation Protocol (SIP)	M
RFC 3264 [RFC 3264]	An Offer/Answer Model with the Session Description Protocol (SDP)	M
RFC 3265 [RFC 3265]	Session Initiation Protocol (SIP)-Specific Event Notification	O
RFC 3311 [RFC 3311]	The Session Initiation Protocol (SIP) UPDATE Method	M
RFC 3312 [RFC 3312]	Integration of Resource Management and Session Initiation Protocol (SIP)	O
RFC 3323 [RFC 3323]	A Privacy Mechanism for the Session Initiation Protocol (SIP)	M
RFC 3324 [RFC 3324]	Short Term Requirements for Network Asserted Identity	O
RFC 3325 [RFC 3325]	Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks	M
RFC 3326 [RFC 3326]	The Reason Header Field for the Session Initiation Protocol (SIP)	M
RFC 3398 [RFC 3398]	Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping	O
RFC 3420 [RFC 3420]	Internet Media Type message/sipfrag	O
RFC 3428 [RFC 3428]	Session Initiation Protocol (SIP) Extension for Instant Messaging	O
RFC 3455 [RFC 3455]	Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)	O
RFC 3515 [RFC 3515]	The Session Initiation Protocol (SIP) Refer Method	O
RFC 3824 [RFC 3824]	Using E.164 numbers with the Session Initiation Protocol (SIP)	O
RFC 3840 [RFC 3840]	Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)	O
RFC 3841 [RFC 3841]	Caller Preferences for the Session Initiation Protocol (SIP)	O
RFC 3891 [RFC 3891]	The Session Initiation Protocol (SIP) Replaces Header	O
RFC 3892 [RFC 3892]	The Session Initiation Protocol (SIP) Referred-By Mechanism	O
RFC 3893 [RFC 3893]	Session Initiation Protocol (SIP) Authenticated Identity Body (AIB) Format	O

Table 10-1 – RFCs to be supported

SIP Extensions	Title	M/O
RFC 3911 [RFC 3911]	The Session Initiation Protocol (SIP) Join Header	O
RFC 3959 [RFC 3959]	The Early Session Disposition Type for the Session Initiation Protocol (SIP)	O
RFC 3960 [RFC 3960]	Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)	O
RFC 3966 [RFC 3966]	The tel URI for Telephone Numbers	M
RFC 4028 [RFC 4028]	Session Timers in the Session Initiation Protocol (SIP)	M
RFC 4032 [RFC 4032]	Update to the Session Initiation Protocol (SIP) Preconditions Framework	O
RFC 4235 [RFC 4235]	An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP)	O
RFC 4244 [RFC 4244]	An Extension to the Session Initiation Protocol (SIP) for Request History Information	O
RFC 4412 [RFC 4412]	Communications Resource Priority for the Session Initiation Protocol (SIP)	O
RFC 4458 [RFC 4458]	Session Initiation Protocol (SIP) URIs for Applications such as Voicemail and Interactive Voice Response (IVR)	O
RFC 4483 [RFC 4483]	A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages	O
RFC 4566 [RFC 4566]	SDP: Session Description Protocol	M
RFC 4694 [RFC 4694]	Number Portability Parameters for the tel URI	O

10.2 SIP profile

10.2.1 SIP profile based on RFC 3261

This clause defines a SIP profile for the SCF at the NNI interface. This clause is structured to mirror [RFC 3261] and its section numbering. The following clauses are numbered such that the fourth digit (i.e., x of 10.2.1.x) tracks the section numbers of [RFC 3261], and clause titles track the section titles of [RFC 3261].

This clause defines the set of enhancements of, and restrictions on, a standard SIP implementation based on [RFC 3261].

Unless otherwise stated in this Recommendation, the SCF shall act in accordance with [RFC 3261].

10.2.1.1 Introduction

RFC 3261 section 1 is informational.

10.2.1.2 Overview of SIP functionality

RFC 3261 section 2 is informational.

10.2.1.3 Terminology

RFC 3261 section 3 is informational.

10.2.1.4 Overview of operation

RFC 3261 section 4 is informational.

10.2.1.5 Structure of the protocol

The structure of the protocol can be found in RFC 3261 section 5, which is informational.

10.2.1.6 Definitions

RFC 3261 section 6 defines the terms that have special significance for SIP. Additional definitions can be found in clause 3.

The reader should note that the term "client" in this clause covers both UACs and proxies.

10.2.1.7 SIP messages

The SCF shall set the SIP profile in accordance with RFC 3261 section 7 except as noted in this clause.

10.2.1.7.1 Requests

The SCF shall set the SIP profile in accordance with RFC 3261 section 7.1 except as noted in this clause.

The INVITE, ACK, CANCEL, BYE, UPDATE and PRACK methods shall be supported. The OPTIONS and REGISTER methods may be supported.

The Request-URI shall be a SIP URI, as defined in [RFC 3261], or a tel URI, as defined in [RFC 3966]. The SIPS URI format may be supported.

The Request-URI in an initial INVITE for a basic telephone call[1] shall identify the called party using a tel URI or by using the telephone-subscriber syntax (i.e., the dialled phone number) in a SIP URI. When the Request-URI is a SIP URI, the host part of the Request-URI shall identify the SCF or the entity to which the message is addressed.

The Request-URI for other requests associated with a basic telephone call shall identify the targeted host using the IP address or FQDN, as given by the Contact header.

The host part of the Request-URI typically agrees with one of the host names of the receiving server. However, if the Request-URI of a received INVITE does not so agree, the server should proxy the request to another entity based on saved translation information or pre-provisioned policy information.

10.2.1.7.2 Responses

The SCF shall set the SIP profile in accordance with RFC 3261 section 7.2.

10.2.1.7.3 Header fields

The SCF shall set the SIP profile in accordance with RFC 3261 section 7.3.

10.2.1.7.4 Bodies

The SCF shall set the SIP profile in accordance with RFC 3261 section 7.4 except as noted in this clause.

10.2.1.7.4.1 Message body types

The SCF shall set the SIP profile in accordance with RFC 3261 section 7.4.1 except as noted in this clause.

The SCF shall set the SIP profile to support the message body type "application/sdp"; other message body types may be supported.

---

[1] This includes INVITEs generated as a result of forwarding.

The message body type "application/sdp" shall be supported with the INVITE and UPDATE methods as well as any non-failure response to these methods. And it should be supported with the PRACK method as well as any non-failure response to the method in order to allow interworking with a H.323 network and support of services operating third party call control.

The message body type "application/sdp" may be supported with failure responses, such as 488 (not acceptable here), to the above methods.

10.2.1.7.4.2 Message body length

The SCF shall set the SIP profile in accordance with RFC 3261 section 7.4.2.

10.2.1.7.5 Framing SIP messages

The SCF shall set the SIP profile in accordance with RFC 3261 section 7.5.

10.2.1.8 General user agent bahavior

This clause and its sub-clauses apply only if the SCF acts as a UA, i.e., B2BUA or redirect server.

The SCF shall behave in accordance with RFC 3261 section 8 except as noted in this clause.

Support for multiple simultaneous media streams for a single call is optional.

Note that the bahavior defined in this clause applies only to requests and responses outside a dialog. The bahavior within a dialog is defined in 10.2.1.12.

10.2.1.8.1 UAC bahavior

The SCF shall behave in accordance with RFC 3261 section 8.1 except as noted in this clause.

10.2.1.8.1.1 Generating the request

The SCF shall behave in accordance with RFC 3261 section 8.1.1 except as noted in this clause.

Request-URI in the request contains the address of the called party. This will normally be a telephone number, but it may also be a general SIP URI. The From and To fields in the request might contain random strings that protect the privacy of the session originator.

Refer to clause 10.2.1.20 for further details of various header field values to be used.

10.2.1.8.1.2 Sending the request

The SCF shall behave in accordance with RFC 3261 section 8.1.2.

10.2.1.8.1.3 Processing responses

The SCF shall behave in accordance with RFC 3261 section 8.1.3 except as noted in this clause.

Support for the SIP authorization procedures, which is used when 401 (unauthorized) or 407 (proxy authentication required) is received, is optional. If the support is provided, it shall be as specified in RFC 3261 section 8.1.3.5.

Support for the SIP retry procedures, which is used when 420 (bad extension) is received, is optional. If the support is provided, it shall be as specified in RFC 3261 section 8.1.3.5.

10.2.1.8.2 UAS bahavior

The SCF shall behave in accordance with RFC 3261 section 8.2.

10.2.1.8.3 Redirect servers

The SCF shall behave in accordance with RFC 3261 section 8.3 except as noted in this clause.

The SCF is not required to provide the redirect server function. However, it may provide the redirect server function and invoke redirections for a limited number of INVITE requests. The rationale for limiting the number of redirections is to control SIP signalling traffic across the NNI and processing complexity associated with redirections. The Max-Forwards header (see clause 10.2.1.20), which is mandatory in all SIP requests, serves to limit the number of hops a request can make on the way to its destination. If the redirection function is supported, then the SCF shall be in accordance with RFC 3261 section 8.3.

3xx response codes may be supported at the NNI, based on bilateral agreements to support redirections that may take place in the interconnecting network or in a downstream network receiving the INVITE message.

10.2.1.9 Cancelling a request

In this clause and in its sub-clauses, the handling that is specific to a proxy applies only if the SCF acts as a SIP proxy, the handling that is specific to a UA applies only if the SCF acts as a UA, i.e., B2BUA or redirect server, and the handling that is specific to a registrar applies only if the SCF acts as a registrar.

The SCF shall behave in accordance with RFC 3261 section 9.

10.2.1.10 Registrations

In this clause and in its sub-clauses, the handling that is specific to a proxy applies only if the SCF acts as a SIP proxy, the handling that is specific to a UA applies only if the SCF acts as a UA, i.e., B2BUA or redirect server, and the handling that is specific to a registrar applies only if the SCF acts as a registrar.

Support for the registrations is optional. If the support is provided, it shall be as specified in RFC 3261 section 10.

10.2.1.11 Querying for capabilities

In this clause and in its sub-clauses, the handling that is specific to a proxy applies only if the SCF acts as a SIP proxy, the handling that is specific to a UA applies only if the SCF acts as a UA, i.e., B2BUA or redirect server, and the handling that is specific to a registrar applies only if the SCF acts as a registrar.

Support for querying for capabilities is optional. If the support is provided, it shall be as specified in RFC 3261 section 11.

10.2.1.12 Dialogs

This clause and its sub-clauses apply only if the SCF acts as a UA, i.e., B2BUA or redirect server.

The SCF shall behave in accordance with RFC 3261 section 12 except as noted in this clause.

10.2.1.12.1 Creation of a dialog

Support for SIPS URIs is optional. If the support is provided, it shall be as specified in RFC 3261 section 12.1.

10.2.1.12.2 Requests within a dialog

Support for SIPS URIs is optional. If the support is provided, it shall be as specified in RFC 3261 section 12.2.

10.2.1.12.3 Termination of a dialog

The SCF shall behave in accordance with RFC 3261 section 12.3.

10.2.1.13 Initiating a session

This clause and its sub-clauses apply only if the SCF acts as a UA, i.e., B2BUA or redirect server.

The SCF shall behave in accordance with RFC 3261 section 13 except as noted in this sub-clause.

The UAC should include a message body type "application/sdp" with the initial INVITE whenever possible.

The support of initial INVITE without SDP offer is recommended in order to allow interworking with a H.323 network and support of services operating third party call control.

To support codec selection:

– When the initial INVITE includes an SDP offer, an SDP answer may be included either in the provisional reliable non-failure response to the INVITE (e.g., 183 Session Progress sent reliably) or in the final non-failure response to the INVITE (i.e., 2xx), and, if not included in the provisional reliable non-failure response, shall be included in the final non-failure response.
– When the initial INVITE does not include an SDP offer, the initial SDP offer shall be included in the first provisional reliable non-failure response to the INVITE, that is in the first 18x response sent reliably (e.g., 180 Ringing sent reliably) if any, or in the final non-failure response to the INVITE (i.e., 2xx) if not. If the initial SDP offer is included in a reliable provisional response, the SDP answer shall be included in the PRACK message acknowledging this response. If the initial SDP offer is included in the final non-failure response to the INVITE (i.e., 2xx), the SDP answer shall be included in the ACK message acknowledging this response.

10.2.1.14 Modifying an existing session

This clause and its sub-clauses apply only if the SCF acts as a UA, i.e., B2BUA or redirect server.

The SCF shall behave in accordance with RFC 3261 section 14 except as noted in this clause.

When constructing an SDP answer to a new received SDP offer contained in a re-INVITE or UPDATE method, if the SCF controls the transfer plane, listening IP address and port number negotiated during the initial SDP negotiation procedure for a given media stream should not be modified.

10.2.1.15 Terminating a session

This clause and its sub-clauses apply only if the SCF acts as a UA, i.e., B2BUA or redirect server.

The SCF shall behave in accordance with RFC 3261 section 15.

10.2.1.16 Proxy bahavior

This clause and its sub-clauses apply only if the SCF acts as a SIP proxy.

The SCF shall behave in accordance with RFC 3261 section 16 except as noted in this clause.

Support for multiple simultaneous media streams for a single call is optional. Since parallel forking, as described in [RFC 3960], may result in multiple simultaneous media streams for a single call, the SCF should not use parallel forking. UA or outbound proxy server may restrict forking by using Request-Disposition header with 'no-fork' option tag as specified in [RFC 3841].

10.2.1.17 Transactions

In this clause and in its sub-clauses, the handling that is specific to a proxy applies only if the SCF acts as a SIP proxy, the handling that is specific to a UA apply only if the SCF acts as a UA, i.e., B2BUA or redirect server, and the handling that is specific to a registrar applies only if the SCF acts as a registrar.

The SCF shall behave in accordance with RFC 3261 section 17 except as noted in this clause.

The SCF may return an error code 486 (busy here) to an INVITE request for a user if a dialog already exists for that user and the new INVITE is not part of that dialog.

10.2.1.18 Transport

The SCF shall behave in accordance with RFC 3261 section 18. However, clause 12 takes precedence over RFC 3261 section 18 in case of any conflicts.

10.2.1.19 Common message components

The SCF shall set the SIP profile in accordance with RFC 3261 section 19 except as noted in this clause.

Support for the SIPS URI is optional. If the support is provided, it shall be as specified in RFC 3261 section 19.1.1.

10.2.1.20 Header fields

The SCF shall set the SIP profile in accordance with RFC 3261 section 20 except as noted in this clause.

Below, the SIP headers defined in [RFC 3261] are listed, and the requirements for supporting them in the SCF are identified.

10.2.1.20.1 Accept

Support for the Accept header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.1.

10.2.1.20.2 Accept-Encoding

Support for the Accept-Encoding header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.2 except as noted below.

The Accept-Encoding header may be used by the SCF. The "identity" encoding value shall be supported; other encodings may be supported.

10.2.1.20.3 Accept-Language

Support for the Accept-Language header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.3.

10.2.1.20.4 Alert-Info

Support for the Alert-Info header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.4.

Note that there are security risks associated with acting on the Alert-Info header, as described in RFC 3261 section 20.4.

10.2.1.20.5 Allow

The Allow header shall be supported as specified in RFC 3261 section 20.5 except as noted below.

The Allow header shall be present in the initial INVITE and the 2xx response to the initial INVITE.

The header value shall list all supported methods, i.e., at a minimum, INVITE, ACK, CANCEL, BYE, UPDATE and PRACK.

10.2.1.20.6 Authentication-Info

Support for the Authentication-Info header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.6.

10.2.1.20.7 Authorization

Support for the Authorization header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.7.

10.2.1.20.8 Call-ID

The Call-ID header shall be supported as specified in RFC 3261 section 20.8 except as noted below.

The Call-ID value shall be globally unique as described in RFC 3261 section 8.1.1.4, and it should use a suitably long random value (the value used as the 'tag' for the From header of the request might even be reused) instead of appending the IP address or hostname to the Call-ID as described in [RFC 3323] section 4.1 for protecting privacy. When privacy is requested by the session originator, the UA of the session originator should use a privacy protected Call-ID. In the case a B2BUA within the SCF is used in support of network interconnection, it may generate a privacy protected Call-ID.

10.2.1.20.9 Call-Info

Support for the Call-Info header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.9.

Note that there are security risks associated with acting on the Call-Info header, as described in RFC 3261 section 20.9.

10.2.1.20.10 Contact

The Contact header shall be supported as specified in RFC 3261 section 20.10 except as noted below.

The SCF shall set the SIP profile to populate the Contact header in an INVITE request, a reliable provisional response and in a 2xx response to an INVITE request, with a SIP URI. Support for any other type of URI is optional.

When the user is requesting privacy, the Contact header should not contain any domain names; the IP address form should be used instead. It should be noted that, in systems with multiple network interfaces, use of the (single) IP address form can reduce the overall system reliability. If multiple interfaces exist and reliability is a concern, then refraining from use of the IP address form is considered to be a reasonable trade-off.

The SCF shall set the SIP profile to populate the Contact header in a 3xx response to an INVITE request with a valid SIP URI or tel URI. If the new destination is a telephone number, it shall contain a tel URI with the number of the new destination, as described in clause 10.2.1.7.1. Support for any other type of URI is optional.

10.2.1.20.11 Content-Disposition

Support for the Content-Disposition header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.11 except as noted below.

The Content-Disposition header may be used by the SCF. The value "session" shall be supported; other values may be supported.

Note that the default value for message body type "application/sdp" is "session", whereas the default value for all other message body types (e.g., "message/sipfrag") is "render". If the default value is not desired, then the Content-Disposition header shall be included.

10.2.1.20.12 Content-Encoding

Support for the Content-Encoding header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.12 except as noted below.

The Content-Encoding header may be used by the SCF. The "identity" encoding value shall be supported; other encodings may be supported.

10.2.1.20.13 Content-Language

Support for the Content-Language header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.13.

10.2.1.20.14 Content-Length

The Content-Length header shall be supported as specified in RFC 3261 section 20.14.

10.2.1.20.15 Content-Type

The Content-Type header shall be supported as specified in RFC 3261 section 20.15 except as noted below.

The value "application/sdp" shall be supported; other values may be supported.

10.2.1.20.16 CSeq

The CSeq header shall be supported as specified in RFC 3261 section 20.16.

10.2.1.20.17 Date

Support for the Date header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.17.

10.2.1.20.18 Error-Info

Support for the Error-Info header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.18.

Note that there are security risks associated with acting on the Error-Info header as described in RFC 3261 section 20.18.

10.2.1.20.19 Expires

Support for the Expires header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.19.

10.2.1.20.20 From

The From header shall be supported as specified in RFC 3261 section 20.20 except as noted below.

In support of user privacy, the SCF restricts the allowable contents of the From header.

When the session originator requests privacy, the SCF shall generate a From header according to the following rules:

- The display-name may be "Anonymous".
- The addr-spec shall contain the identifier "anonymous" for userinfo.
- The addr-spec shall contain the non-identifying hostname "anonymous.invalid".

10.2.1.20.21 In-Reply-To

Support for the In-Reply-To header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.21.

10.2.1.20.22 Max-Forwards

The Max-Forwards header shall be supported as specified in RFC 3261 section 20.22 except as noted below.

When a B2BUA within the SCF forwards a request, it shall use a Max-Forwards value equal to the incoming Max-Forwards value minus one.

10.2.1.20.23 Min-Expires

Support for the Min-Expires header is optional (because support for the REGISTER method is optional). If the support is provided, it shall be as specified in RFC 3261 section 20.23.

10.2.1.20.24 MIME-Version

Support for the MIME-Version header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.24 except as noted below.

The version "1.0" value shall be supported; other values may be supported.

10.2.1.20.25 Organization

Support for the Organization header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.25.

10.2.1.20.26 Priority

Support for the Priority header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.26.

Note that there are security ramifications for entities that act on this header.

10.2.1.20.27 Proxy-Authenticate

Support for the Proxy-Authenticate header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.27.

10.2.1.20.28 Proxy-Authorization

Support for the Proxy-Authorization header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.28.

10.2.1.20.29 Proxy-Require

The Proxy-Require header shall be supported as specified in RFC 3261 section 20.29 except as noted below.

The option tag "privacy" shall be supported in accordance with [RFC 3323]; other option tags may be supported.

10.2.1.20.30 Record-Route

The Record-Route header shall be supported as specified in RFC 3261 section 20.30.

10.2.1.20.31 Reply-To

Support for the Reply-To header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.31.

10.2.1.20.32 Require

The Require header shall be supported as specified in RFC 3261 section 20.32 except as noted below.

The option tags "100rel" and "timer" shall be supported in accordance with [RFC 3262] and [RFC 4028], respectively; other option tags may be supported.

10.2.1.20.33 Retry-After

Support for the Retry-After header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.33.

10.2.1.20.34 Route

The Route header shall be supported as specified in RFC 3261 section 20.34.

10.2.1.20.35 Server

Support for the Server header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.35.

10.2.1.20.36 Subject

Support for the Subject header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.36.

10.2.1.20.37 Supported

The Supported header shall be supported as specified in RFC 3261 section 20.37 except as noted below.

The option tags "100rel" and "timer" shall be supported in accordance with [RFC 3262] and [RFC 4028], respectively; other option tags may be supported.

10.2.1.20.38 Timestamp

Support for the Timestamp header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.38 except as noted below.

The SCF may send the Timestamp header in requests; if received, this header shall be processed as described in RFC 3261 section 20.38.

10.2.1.20.39 To

The To header shall be supported as specified in RFC 3261 section 20.39 except as noted below.

In support of user privacy, the SCF may restrict the allowable contents of the To header. Typically, the To header indicates the dialled digits in a tel URI. This information is of end-to-end significance and might reveal information about the caller's location, e.g., enterprise, local, long-distance, or international.

When the call originator requests privacy, the SCF may generate a To header according to the following rules:

- The display-name shall be absent.
- If a global telephone number is used, then the userinfo part of the addr-spec shall contain a full E.164 number, including the country code.
- The host part of the addr-spec shall contain the non-identifying hostname "anonymous.invalid".

If anonymity is not requested by the call originator and the user dialled a telephone number, then the To header should contain a tel URI with the dialled digits.

10.2.1.20.40 Unsupported

The Unsupported header shall be supported as specified in RFC 3261 section 20.40.

10.2.1.20.41 User-Agent

Support for the User-Agent header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.41.

10.2.1.20.42 Via

The Via header shall be supported as specified in RFC 3261 section 20.42.

10.2.1.20.43 Warning

Support for the Warning header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.43.

10.2.1.20.44 WWW-Authenticate

Support for the WWW-Authenticate header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.44.

10.2.1.21 Response codes

The SCF shall set the SIP profile in accordance with RFC 3261 section 21.

10.2.1.22 Usage of HTTP authentication

Support for HTTP authentication is optional. If used, HTTP authentication shall be as specified in RFC 3261 section 22.

10.2.1.23 S/MIME

Support for S/MIME is optional. If used, S/MIME shall be as specified in RFC 3261 section 23.

10.2.1.24 Examples

RFC 3261 section 24 is informational.

10.2.1.25 Augmented BNF for the SIP protocol

The SCF shall set the SIP profile in accordance with RFC 3261 section 25.

10.2.2 SIP profile for extensions to RFC 3261

This clause defines the extended methods, headers and response codes that are defined in the mandatorily supported RFCs except for RFC 3261, as listed in clause 10.1. If the support for the RFC is optional, then the support for the methods, headers and response codes defined in those RFCs is accordingly optional, and this clause does not describe those methods, headers and response codes individually.

10.2.2.1 Extended methods

The UPDATE and PRACK methods shall be supported.

10.2.2.2 Extended headers

10.2.2.2.1 Min-SE

The Min-SE header shall be supported as specified in [RFC 4028].

10.2.2.2.2 P-Asserted-Identity

The P-Asserted-Identity header shall be supported as specified in [RFC 3325].

10.2.2.2.3 P-Preferred-Identity

Support for the P-Preferred-Identity header is not applicable because this header will not traverse the NNI. This header may be required for some SIP/SDP profiles, such as the UNI profile, but is not required for the NNI profile.

10.2.2.2.4 Privacy

The Privacy header shall be supported as specified in [RFC 3323] except as noted below.

The application of the privacy option "id" shall be supported. Other privacy options may be supported based on a bilateral agreement.

10.2.2.2.5 RAck

The RAck header shall be supported as specified in [RFC 3262].

10.2.2.2.6 Reason

Support for the reception of the Reason header is mandatory. However, support of sending the Reason header is optional. If the support is provided, it shall be as specified in [RFC 3326] except as noted below.

The Reason header shall be supported in responses.

10.2.2.2.7 RSeq

The RSeq header shall be supported as specified in [RFC 3262].

10.2.2.2.8 Session-Expires

The Session-Expires header shall be supported as specified in [RFC 4028].

10.2.2.3 Extended response codes

422 (session interval too small) shall be supported as specified in [RFC 4028].

10.2.3 Summary of SIP methods and headers

Support for the following SIP methods and headers by the SCF is mandatory or optional, as specified in Tables 10-2, 10-3, 10-4 and 10-5.

NOTE – For information about supporting the responses, see [RFC 3261].

Table 10-2 – RFC 3261 methods

Method	Send	Recv	Reference
ACK	M	M	See clause 10.2.1.7.1
BYE	M	M	See clause 10.2.1.7.1
CANCEL	M	M	See clause 10.2.1.7.1
INVITE	M	M	See clause 10.2.1.7.1
OPTIONS	O	O	See clause 10.2.1.7.1
REGISTER	O	O	See clause 10.2.1.7.1

Table 10-3 – Extended methods

Method	Send	Recv	Reference	RFC
UPDATE	M	M	See clause 10.2.1.7.1	RFC 3311
PRACK	M	M	See clause 10.2.1.7.1	RFC 3262

Table 10-4 – RFC 3261 headers

Header	Send	Recv	Reference
Accept	O	O	See clause 10.2.1.20.1
Accept-Encoding	O	O	See clause 10.2.1.20.2
Accept-Language	O	O	See clause 10.2.1.20.3
Alert-Info	O	O	See clause 10.2.1.20.4

Table 10-4 – RFC 3261 headers

Header	Send	Recv	Reference
Allow	M	M	See clause 10.2.1.20.5
Authentication-Info	O	O	See clause 10.2.1.20.6
Authorization	O	O	See clause 10.2.1.20.7
Call-ID	M	M	See clause 10.2.1.20.8
Call-Info	O	O	See clause 10.2.1.20.9
Contact	M	M	See clause 10.2.1.20.10
Content-Disposition	O	O	See clause 10.2.1.20.11
Content-Encoding	O	O	See clause 10.2.1.20.12
Content-Language	O	O	See clause 10.2.1.20.13
Content-Length	M	M	See clause 10.2.1.20.14
Content-Type	M	M	See clause 10.2.1.20.15
CSeq	M	M	See clause 10.2.1.20.16
Date	O	O	See clause 10.2.1.20.17
Error-Info	O	O	See clause 10.2.1.20.18
Expires	O	O	See clause 10.2.1.20.19
From	M	M	See clause 10.2.1.20.20
In-Reply-To	O	O	See clause 10.2.1.20.21
Max-Forwards	M	M	See clause 10.2.1.20.22
Min-Expires	O	O	See clause 10.2.1.20.23
MIME-Version	O	O	See clause 10.2.1.20.24
Organization	O	O	See clause 10.2.1.20.25
Priority	O	O	See clause 10.2.1.20.26
Proxy-Authenticate	O	O	See clause 10.2.1.20.27
Proxy-Authorization	O	O	See clause 10.2.1.20.28
Proxy-Require	M	M	See clause 10.2.1.20.29
Record-Route	M	M	See clause 10.2.1.20.30
Reply-To	O	O	See clause 10.2.1.20.31
Require	M	M	See clause 10.2.1.20.32
Retry-After	O	O	See clause 10.2.1.20.33
Route	M	M	See clause 10.2.1.20.34
Server	O	O	See clause 10.2.1.20.35
Subject	O	O	See clause 10.2.1.20.36
Supported	M	M	See clause 10.2.1.20.37
Timestamp	O	O	See clause 10.2.1.20.38
To	M	M	See clause 10.2.1.20.39
Unsupported	M	M	See clause 10.2.1.20.40

Table 10-4 – RFC 3261 headers

Header	Send	Recv	Reference
User-Agent	O	O	See clause 10.2.1.20.41
Via	M	M	See clause 10.2.1.20.42
Warning	O	O	See clause 10.2.1.20.43
WWW-Authenticate	O	O	See clause 10.2.1.20.44

Table 10-5 – Extended headers

Header	Send	Recv	Reference	RFC
Min-SE	M	M	See clause 10.2.2.2.1	RFC 4028
P-Asserted-Identity	M	M	See clause 10.2.2.2.2	RFC 3325
P-Preferred-Identity	N/A	N/A	See clause 10.2.2.2.3	RFC 3325
Privacy	M	M	See clause 10.2.2.2.4	RFC 3323
RAck	M	M	See clause 10.2.2.2.5	RFC 3262
Reason	O	M	See clause 10.2.2.2.6	RFC 3326
RSeq	M	M	See clause 10.2.2.2.7	RFC 3262
Session-Expires	M	M	See clause 10.2.2.2.8	RFC 4028

In the above tables, M, O, C and N/A have the following meanings:

Table 10-6 – Notations of the codes in Tables 10-2, 10-3, 10-4 and 10-5

Code	Code name	Sending side	Receiving side
M	Mandatory	The capability shall be supported at NNI. Supporting sending a SIP message or header at the NNI means that this message or header shall be sent over the NNI if received from the served network. It does not imply that network elements inside the served network or user equipment connected to this network shall support this message or header.	Supporting receiving a SIP message or header at the NNI means that, if received from the NNI, this message or header shall be forwarded to the served network. It does not imply that network elements inside the served network or user equipment connected to this network shall support this message or header. Processing may not continue if required information is unavailable (suitable disconnection/release processing should be performed). However, when a default value has been decided upon, processing is performed using the default value.

Table 10-6 – Notations of the codes in Tables 10-2, 10-3, 10-4 and 10-5

Code	Code name	Sending side	Receiving side
O	Optional	The capability may or may not be supported at NNI. It is an implementation choice.	Same as for the sending side with the following additions: If possible, the processing expected by the sending side should be performed. When the processing expected by the sending side cannot be performed, the received content should be ignored and processing should continue.
C<integer>	Conditional	The requirement on the capability ("M", "O") depends on the support of other optional or conditional items. <integer> is the identifier of the conditional expression.	Same as for the sending side.
N/A	Not applicable	It is impossible to use the capability. No answer in the support column is required.	Same as for the sending side.

Other SIP headers may be supported by the SCF. The SCF should transfer unsupported optional headers unchanged, if possible.

10.3 SDP profile

This clause defines an SDP profile for use in the SCF. It also defines the set of enhancements of and restrictions on a standard SDP implementation based on [RFC 2327] and [RFC 4566]. In Table 10-7, M, O and C have the same meanings as in Table 10-6.

Table 10-7 – SDP profile for usage

Item	Send	Recv
Session description		
v = (protocol version)	M	M
o = (owner/creator and session identifier)	M	M
s = (session name)	M	M
i = (session information)	O	M
u = (URI of description)	O	O
e = (email address)	O	O
p = (phone number)	O	O
c = (connection information)	C1	M
b = (bandwidth information)	O	M
Time description (one or more per description)		
t = (time the session is active)	M	M
r = (zero or more repeat times)	O	O

Table 10-7 – SDP profile for usage

Item	Send	Recv
Session level description (continue)		
z = (time zone adjustments)	O	O
k = (encryption key)	O	O
a = (zero or more session attribute lines)	O	M
Media description (zero or more per description)		
m = (media name and transport address)	C2	M
i = (media title)	O	O
c = (connection information)	C1, C2	M
b = (bandwidth information)	O	M
k = (encryption key)	O	O
a = (zero or more media attribute lines)	O	M
C1: At least one of the c lines in session and media descriptions shall be implemented. C2: If media description is implemented, both m and c lines shall be implemented.		

NOTE – Table 10-7 is described from an implementation point of view as described in Table 10-6, e.g., even if the c line in the media description is implemented, it does not mean that every media description in specific SIP/SDP message includes the c line. When the c line is included in the session description, the c line in the media description may not be included.

11 Transport-level profile

Media themselves are out of the scope of this Recommendation, but the following are supported because they are described in SIP/SDP messages. In Table 11-1, M and O have the same meanings as defined in clause 10.1.

Table 11-1 – Supported transport-level RFCs to be described in SIP/SDP messages

RFC	Title	M/O
RFC 2833 [RFC 2833]	RTP payload for DTMF Digits, Telephony Tones and Telephony Signals	M (Note 1)
RFC 3267 [RFC 3267]	Real-Time Transport Protocol (RTP) Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs	O
RFC 3389 [RFC 3389]	Real-time Transport Protocol (RTP) Payload for Comfort Noise	O (Note 2)
RFC 3550 [RFC 3550]	RTP: A Transport Protocol for Real-Time Applications	M
RFC 3551 [RFC 3551]	RTP Profile for Audio and Video Conferences with Minimal Control	M
T.38 [ITU-T T.38]	Procedures for real-time Group 3 facsimile communication over IP networks	O
RFC 4103 [RFC 4103]	RTP Payload for Text Conversion	O
NOTE 1 – When [ITU-T G.711] is used, [RFC 2833] is not mandatory. NOTE 2 – For use with codecs such as G.711 [ITU-T G.711] and G.726 [ITU-T G.726] that do not themselves inherently support comfort noise.		

12 Call control signalling transport

The NNI should use SIP transport over TCP unless, based on bilateral agreement, SIP transport over UDP or SCTP is used.

NOTE – A service provider may have to support multiple types of SIP signalling transport depending on the peering relationships.

13 IP protocol version

The following IP protocol versions are proposed:

1) Support for IPv4 is mandatory.

2) Support for IPv6 is optional based on bilateral agreement.

3) When IPv4 and IPv6 networks interconnect, the IPv6 network shall perform addressing mapping.

14 Security considerations

Signalling shall be secure and media may be secure based on a bilateral agreement.

Appendix I

Call/signalling flows

(This appendix does not form an integral part of this Recommendation)

This appendix gives example call flows for the following scenarios:

1) PSTN—IP—(NNI)—IP—PSTN.

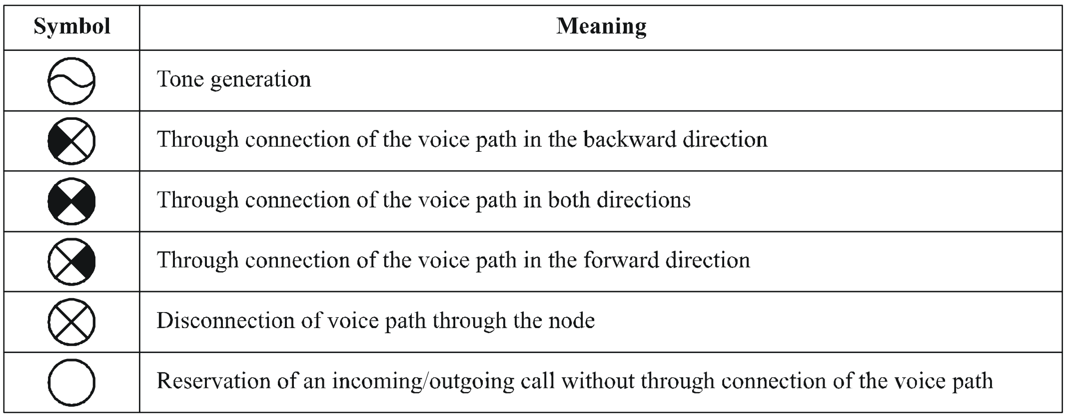
2) PSTN—IP—(NNI)—IP—IP.

3) IP—IP—NNI—IP—PSTN.

4) IP—IP—(NNI)—IP—IP.

The example call flows for scenarios 1, 2 and 3 are based on the flows described in [ITU-T Q.1912.5]. The interworking between ISUP and SIP is shown at the diagrammatic level to illustrate interoperability. [ITU-T Q.1912.5] provides the details of interworking between ISUP (or BICC) and SIP, including the encapsulated ISUP and SIP header precedence rules. The example call flows for scenario 4 are based on [RFC 3261].

The following symbols are used in the figures below:



Symbol	Meaning
	Tone generation
	Through connection of the voice path in the backward direction
	Through connection of the voice path in both directions
	Through connection of the voice path in the forward direction
	Disconnection of voice path through the node
	Reservation of an incoming/outgoing call without through connection of the voice path

Q.3401(07)_Symbol

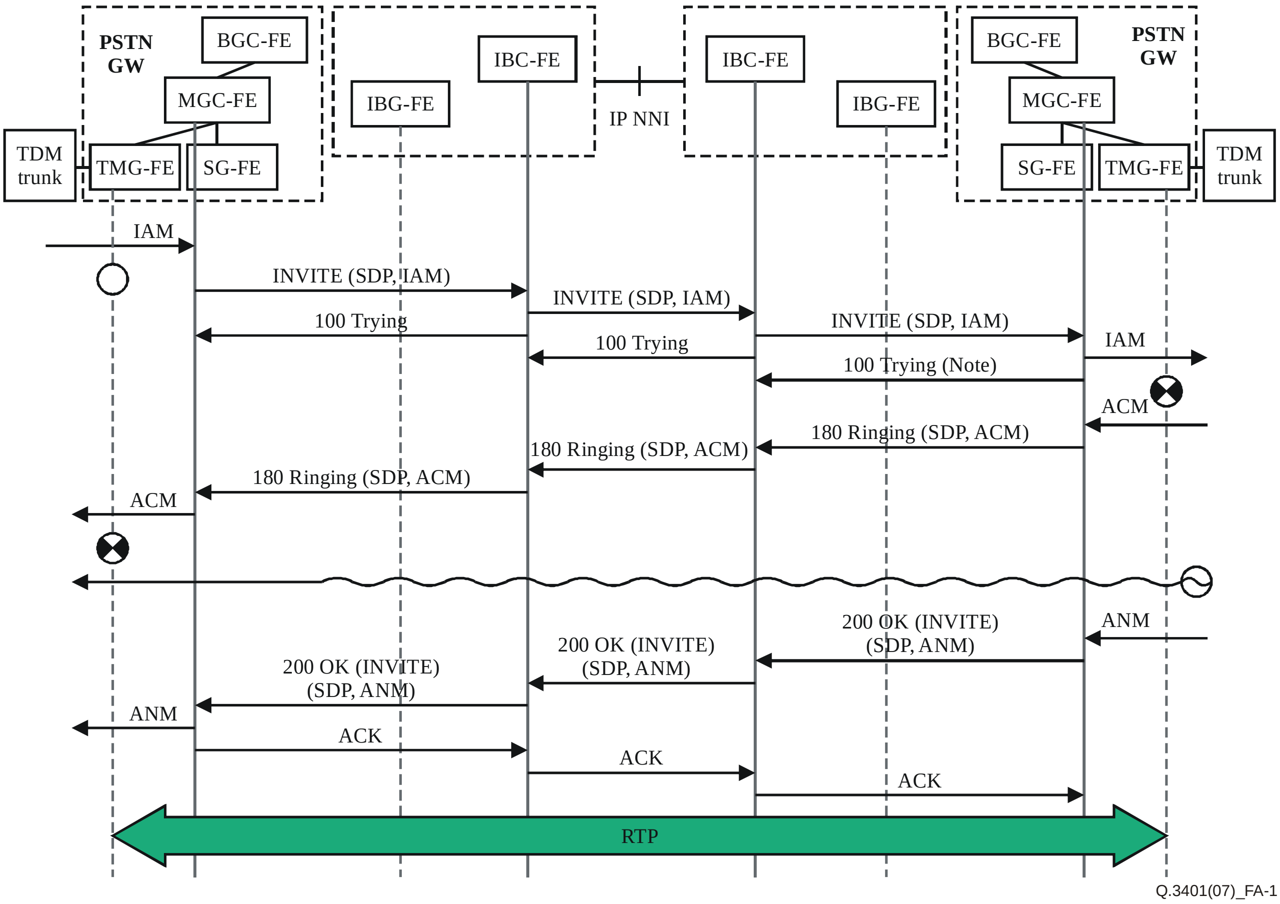
A.1 PSTN—IP—(NNI)—IP—PSTN

This clause illustrates typical interworking scenarios between ISUP and SIP-I. The example call flows assume a call originating and terminating in the PSTN and transiting two IP networks.

A.1.1 Successful call setup (SIP preconditions not used)

Figure A.1 shows a typical sequence of messages for successful call setup for an incoming ISUP call over SIP-I. The PSTN gateway (PSTN GW) performs the through-connection of the bearer path in both directions after the receipt of the SDP answer in the 180 Response.

NOTE – Internal signalling messages within the PSTN gateway and IBC-FE and IBG-FEs are not shown.



NOTE – The generation of the 100 Trying response is necessary if the PSTN gateway knows that it will not generate a provisional or final response.

Figure A.1 – Successful Call Setup

A.1.2 Normal call release

Figure A.2 shows a normal call release interworking procedure without tone provision. A REL message is mapped and encapsulated into a BYE request to preserve ISUP signalling transparency.

NOTE 1 – Internal signalling messages within the PSTN gateway and IBC-FE and IBG-FEs are not shown.

NOTE 2 – This procedure is applicable in those cases where in-band tones/announcements are not provided, e.g., 64 kbit/s unrestricted bearer service.

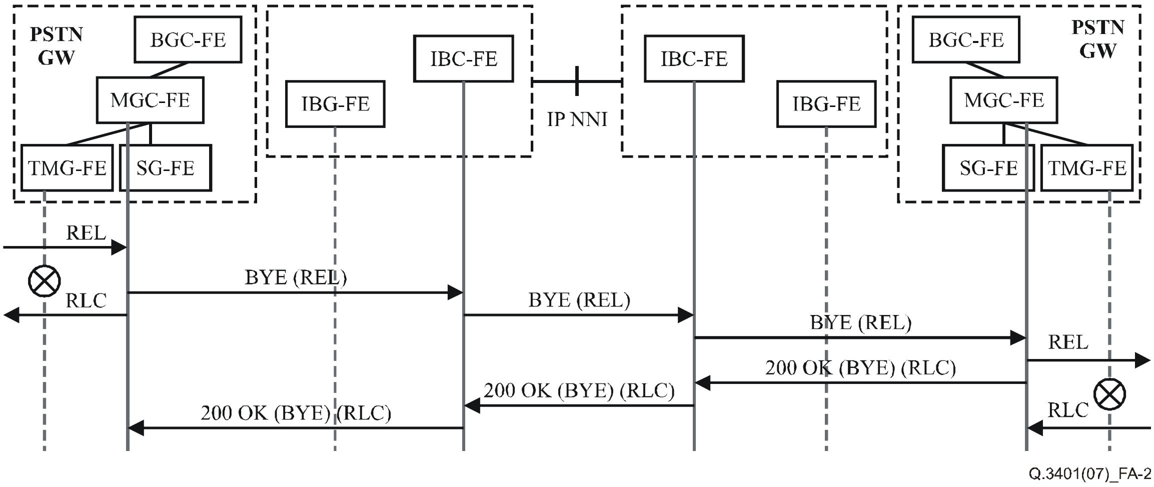


Figure A.2 – Normal call release without tone provision

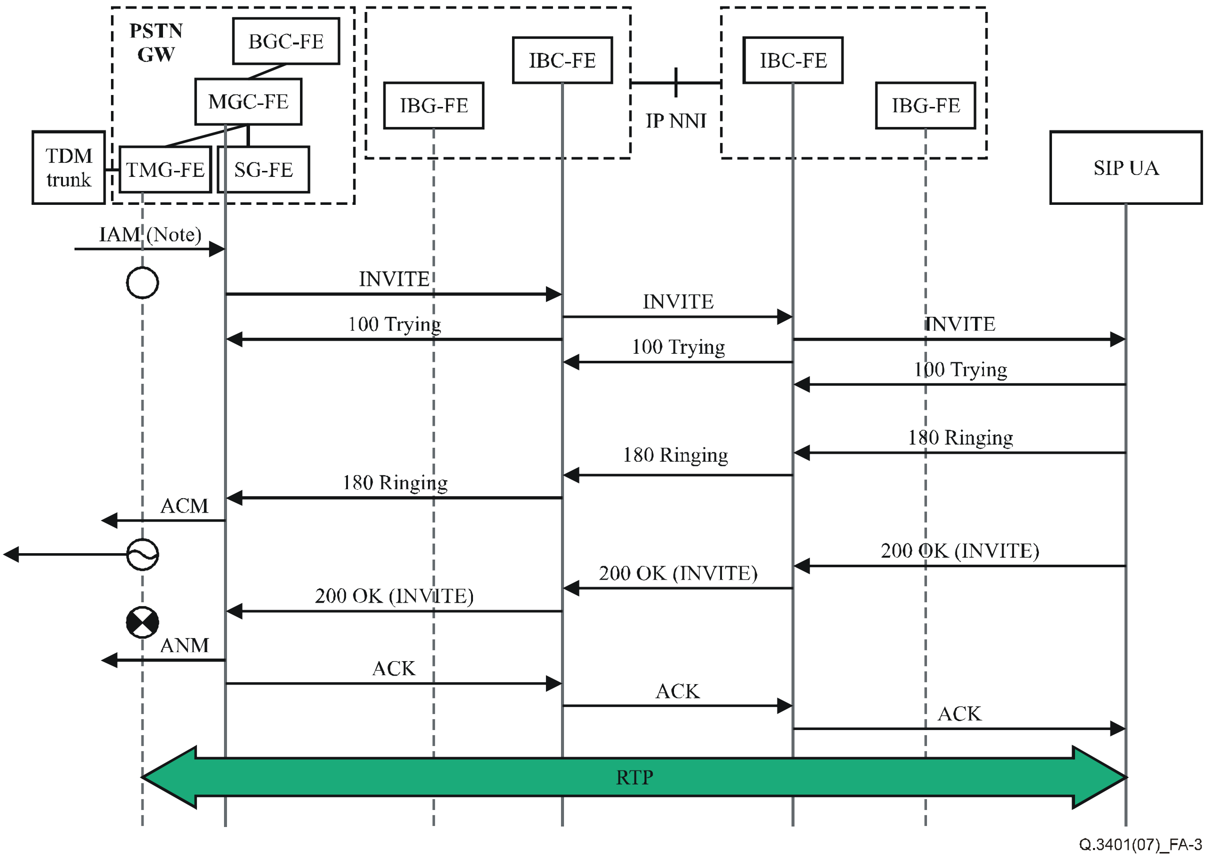
A.2 PSTN—IP—(NNI)—IP—IP

This clause illustrates typical interworking scenarios for successful call setup and release between ISUP and SIP. The call flows assume a call originating in the PSTN and terminating in an IP network.

A.2.1 Successful call setup (SIP preconditions not used)

Figure A.3 shows a typical sequence of messages for successful call setup at a gateway for an incoming ISUP call and an outgoing SIP call, without SIP preconditions. In this example, the PSTN gateway sends the INVITE message upon receipt of an IAM containing the indication "continuity check not required". Upon receipt of the 200 OK (INVITE), the PSTN gateway sends the ANM.

NOTE – Internal signalling messages within the PSTN gateway and IBC-FE and IBG-FEs are not shown.



NOTE – The IAM contains the indication "continuity check not required".

Figure A.3 – Successful call setup from ISUP to SIP

A.2.2 Normal call release

Figure A.4 shows a normal call release procedure initiated from the ISUP side of the call. This call flow assumes that no resource reservation teardown signalling is required on the SIP side of the call.

NOTE – Internal signalling messages within the PSTN gateway and IBC-FE and IBG-FEs are not shown.

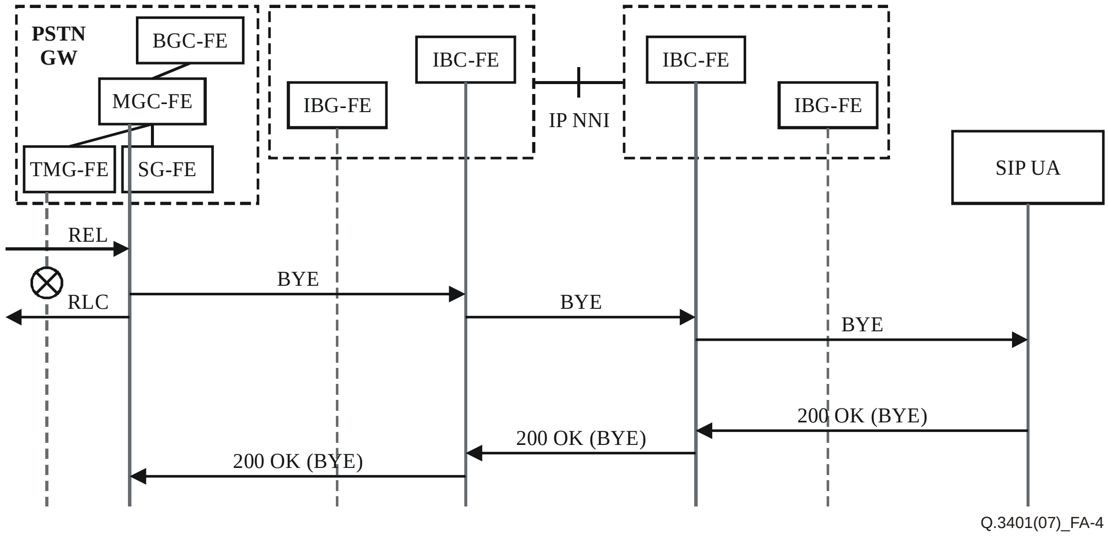


Figure A.4 – Normal call release from ISUP to SIP

A.3 IP—IP—(NNI)—IP—PSTN

This clause illustrates typical interworking scenarios for successful call setup and release between SIP and ISUP. The call flows assume a call originating in an IP network and terminating in the PSTN.

A.3.1 Successful call setup (SIP preconditions not used)

Figure A.5 shows a typical sequence of messages for successful call setup at a gateway for an incoming SIP call and an outgoing ISUP call. Since SIP preconditions are not in use, the PSTN gateway immediately sends out the IAM. Upon receipt of the ANM, the PSTN gateway sends the 200 OK (INVITE).

NOTE – Internal signalling messages within the PSTN gateway and IBC-FE and IBG-FEs are not shown.

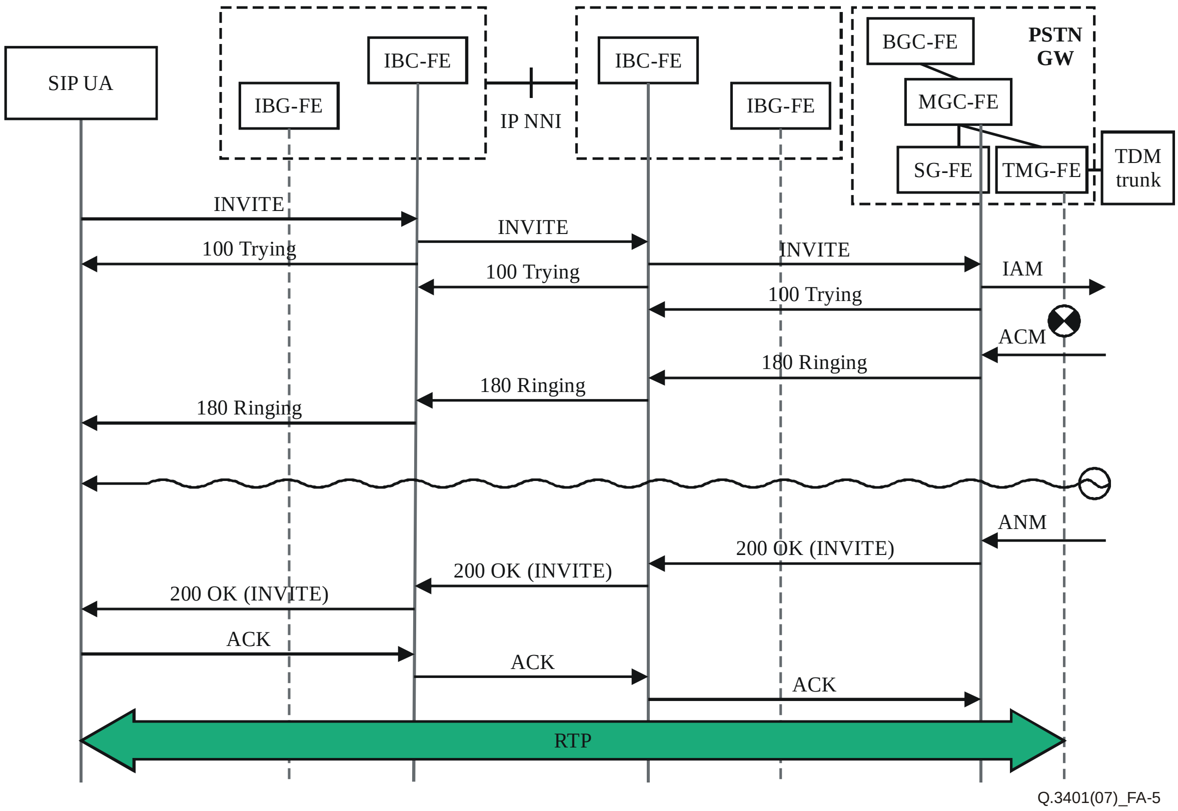


Figure A.5 – Successful call setup from SIP to ISUP

A.3.2 Normal call release

Figure A.6 shows a sequence of messages for the normal call release procedure initiated from the SIP side of the call. This call flow assumes that no resource reservation teardown signalling is required on the SIP side.

NOTE – Internal signalling messages within the PSTN gateway and IBC-FE and IBG-FEs are not shown.

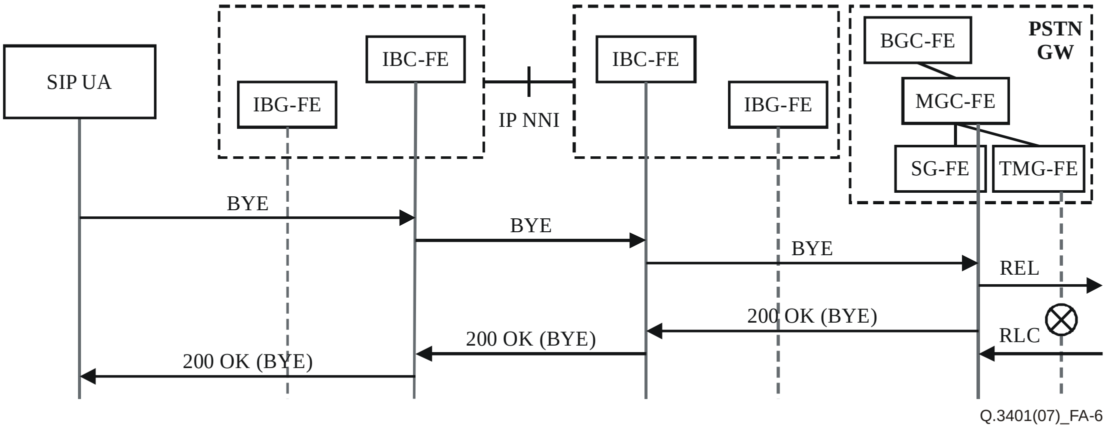


Figure A.6 – Normal call release from SIP to ISUP

A.4 IP—IP—(NNI)—IP—IP

This clause illustrates typical scenarios for successful call setup and release at the SIP IP-IP NNI. The call flows assume a call originating and terminating in IP networks without transiting a non-IP network.

A.4.1 Successful call setup (SIP preconditions not used)

Figure A.7 shows a typical sequence of messages for successful call setup for a basic call at the SIP NNI. No SIP preconditions or messages to support additional SIP services are shown.

NOTE – Internal signalling messages within the IBC-FE and IBG-FEs are not shown.

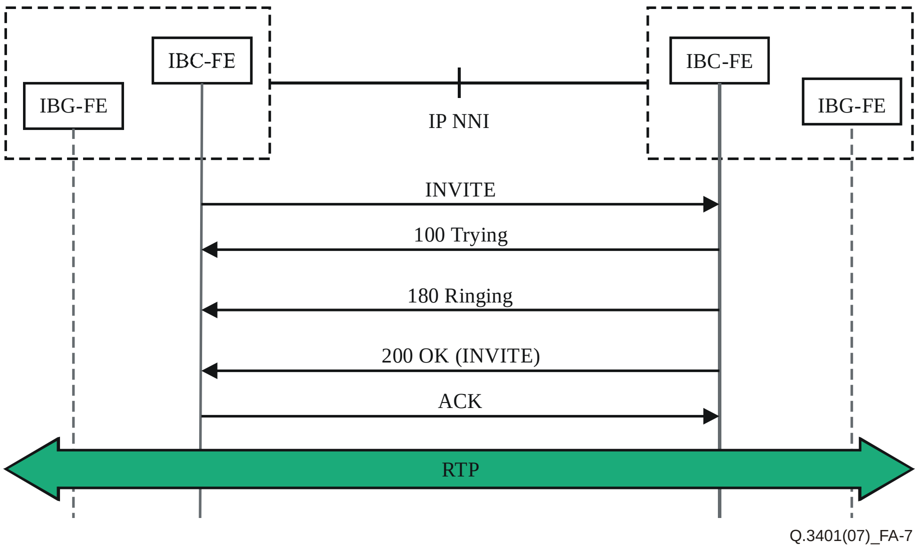


Figure A.7 – Successful call setup at IP-IP SIP NNI

A.4.2 Normal call release

Figure A.8 shows the sequence of messages for normal call release at the SIP NNI.

NOTE – Internal signalling messages within the IBC-FE and IBG-FEs are not shown.

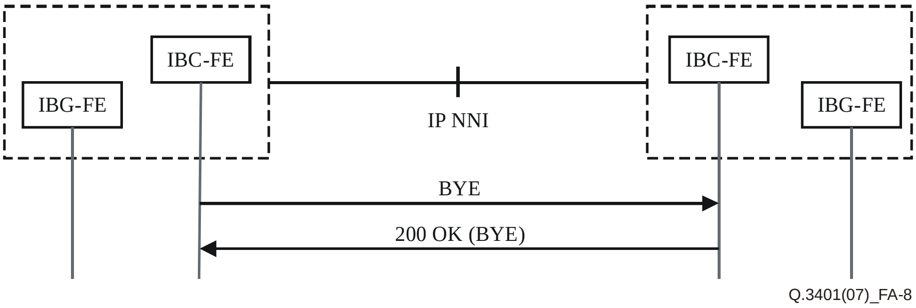


Figure A.8 – Normal call release at IP-IP SIP NNI

Bibliography

[b-ETSI ES 282 007] ETSI ES 282 007 V1.1.1 (2006), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Functional architecture*.

[b-ETSI TS 182 006] ETSI TS 182 006 V1.1.1 (2006), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Stage 2 description*.

[b-ETSI ES 283 003] ETSI ES 283 003 V1.8.0 (2007), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Stage 3*.

[b-3GPP TS 24.229] 3GPP TS 24.229 (2007), *Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3.*

[b-ATIS-PP-1000009] ATIS-PP-1000009 (2006), *IP Network-to-Network Interface (NNI) Standard for VoIP*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	**Switching and signalling**
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2007