ATIS-1000009.2006

IP NETWORK-TO-NETWORK INTERFACE (NNI) STANDARD FOR VOIP

AMERICAN NATIONAL STANDARD FOR TELECOMMUNICATIONS

The Alliance for Telecommunication Industry Solutions (ATIS) is a technical planning and standards development organization that is committed to rapidly developing and promoting technical and operations standards for the communications and related information technologies industry worldwide using a pragmatic, flexible and open approach. Over 1,100 participants from more than 350 communications companies are active in ATIS' 23 industry committees and its Incubator Solutions Program.

< http://www.atis.org/ >

AMERICAN NATIONAL STANDARD

Approval of an American National Standard requires review by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer.

Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made towards their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards.

The American National Standards Institute does not develop standards and will in no circumstances give an interpretation of any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretations should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken periodically to reaffirm, revise, or withdraw this standard. Purchasers of American National Standards may receive current information on all standards by calling or writing the American National Standards Institute.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to the validity of this claim or any patent rights in connection therewith. The patent holder has, however, filed a statement of willingness to grant license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license. Details may be obtained from the publisher.

ATIS-1000009.2006, *IP Network-to-Network Interface (NNI) Standard for VoIP*

Is an American National Standard developed by the **Signaling, Architecture, and Control (SAC) Subcommittee** under the **ATIS Packet Technologies and Systems Committee (PTSC)**.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

ATIS-1000009.2006

American National Standard for Telecommunications

IP NETWORK-TO-NETWORK INTERFACE (NNI) STANDARD FOR VOIP

Secretariat

Alliance for Telecommunications Industry Solutions

Approved May 16, 2006

American National Standards Institute, Inc.

Abstract

This document defines a standard approach to support IP-IP interconnection for VoIP between carriers.

FOREWORD

The information contained in this Foreword is not part of this American National Standard (ANS) and has not been processed in accordance with ANSI's requirements for an ANS. As such, this Foreword may contain material that has not been subjected to public review or a consensus process. In addition, it does not contain requirements necessary for conformance to the Standard.

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The Packet Technologies and Systems Committee (PTSC) -- formerly T1S1 -- develops and recommends standards and technical reports related to services, architectures, and signaling, in addition to related subjects under consideration in other North American and international standards bodies. PTSC coordinates and develops standards and technical reports relevant to telecommunications networks in the U.S., reviews and prepares contributions on such matters for submission to U.S. ITU-T and U.S. ITU-R Study Groups or other standards organizations, and reviews for acceptability or per contra the positions of other countries in related standards development and takes or recommends appropriate actions.

ANSI guidelines specify two categories of requirements: mandatory and recommendation. The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, PTSC Secretariat, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time it approved this document, PTSC, which is responsible for the development of this Standard, had the following members:

B. Hall, PTSC Chair
J. Zebarth, PTSC Vice-Chair
S. Carioti, ATIS Disciplines
S. Barclay, ATIS Secretariat
C. Underkoffler, ATIS Chief Editor
M. Dolly & V. Shaikh, PTSC Technical Editors

Organization Represented	Name of Representative
AcmePacket	Kevin Klett
Alcatel USA Inc.	Kevin Biholar
AT&T	Bob Hall George Stanek (Alt..)
BellSouth Telecommunications	Rick McNealy
C.S.I. Telecommunications	Michael S. Newman Thomas G. Croda (Alt.)
Cingular Wireless LLC	Don Zelmer Marc Grant (Alt.)
Cisco Systems	Rajiv Kapoor Mike Hammer (Alt.)
Department of Defense	Chris Fitzgerald Ryan Kuseski (Alt.)
Ericsson Incorporated	Susana Sabater-Maroto Stephen Hayes (Alt.)
FBI ESTS	Robert Holman Edward Ignacio(Alt.)
Harris Corporation	Marlis Humphrey
Hewlett-Packard	Steve Mills
Intelsat	Mark T. Neibert
Lucent Technologies	Stuart O. Goldman

Organization Represented	Name of Representative
National Communications System	Nicholas Andrew Carol-Lyn Taylor (Alt.)
Neustar	Chris Celiberti
Nokia Telecommunications Inc.	Joyabrata Mukherjee Ed Ehrlich (Alt.)
Nortel	Joseph Zebarth
Owest	Steve Showell Michael Fargano(Alt.)
Siemens Communications, Inc.	Ron Franks David E. Francisco(Alt.)
Sprint LTD	Jack Mooningham
Sprint Nextel	Mark L. Jones
Telcordia Technologies	Wesley Downum Cliff Halevi (Alt.)
Tellabs Operations, Inc.	William A. Walker
Tridea Works	Greg Ratta
VerisSign, Inc.	Anthony M. Rutkowski
Verizon Communications	Thomas Helmes Christine Huff

The Signaling, Architecture, and Control (SAC) Subcommittee was responsible for the development of this document.

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

American National Standard for Telecommunications –

IP Network-to-Network Interface (NNI) Standard for VoIP

SUMMARY

This document defines a standard approach to support IP-IP interconnection for VoIP between carriers.

1 SCOPE, PURPOSE, AND APPLICATION

This standard defines the IP Network-to -Network Interface (NNI) for VoIP between carriers. It addresses the need for a standard interface as telecom networks migrate the NNI from TDM circuit-switched to IP. The focus of this standard is to support VoIP. This standard defines:

- Interconnection architecture;
- SIP call/session control signaling;
- Signaling and media transport;
- Quality of Service (QoS);
- Association between call control and media control; and
- Mandatory SIP URIs to be Supported.

There is also an informative annex on items for consideration in SLAs.

The following related topics are not defined in this document:

- Call Routing;
- Security;
- Session Border Controller Functions; or
- Call Admission Control and Traffic Management.

Figure 1 illustrates the relationship of this document to other related IP-NNI documents.

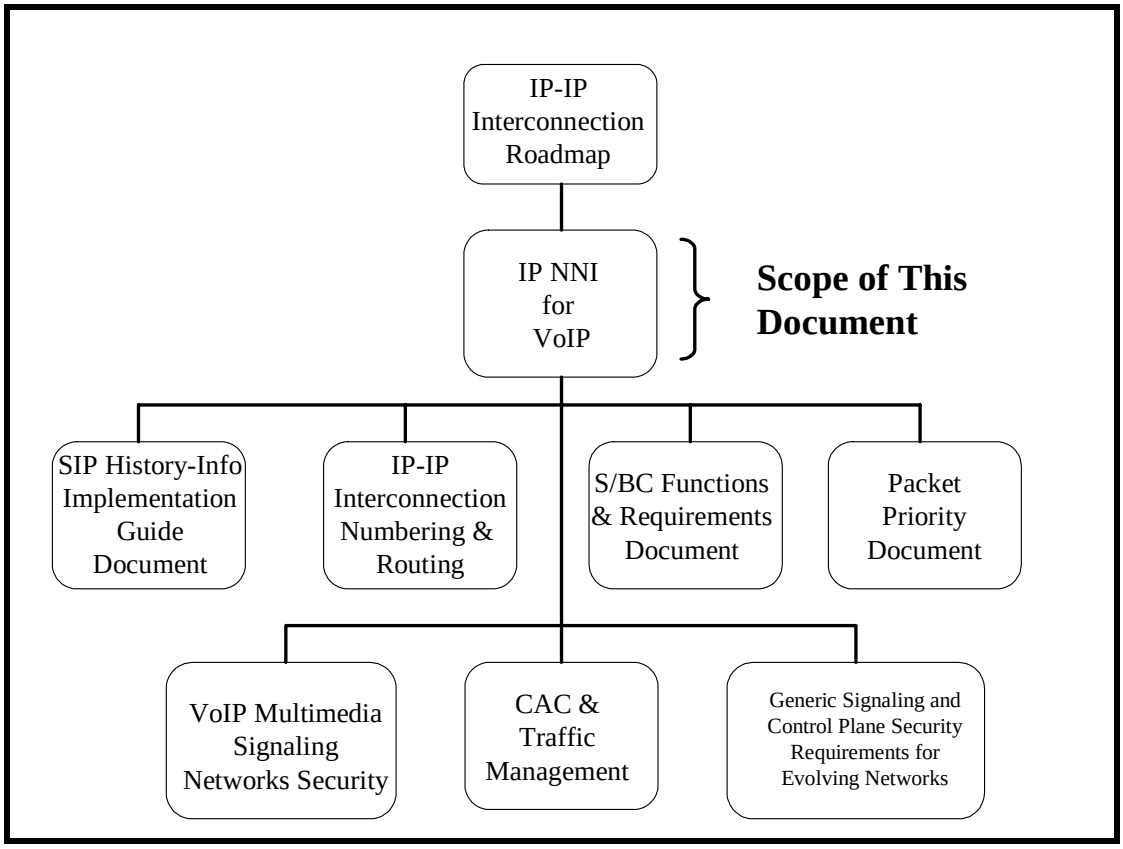


Figure 1 - Scope of Document

1.1 Assumptions

This document is based on the following set of assumptions:

1. It is recognized that there may be data-oriented call control (e.g., http to a web portal on a Application Server) in addition to SIP-oriented call control occurring 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. Even though differentiated treatment *may* be desirable in some cases (e.g., initiating a GETS call through a web portal), 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 document.
2. The logical interfaces associated with the call control, call routing, and bearer functional entities enable interconnection between two service provider networks in a peering environment.
3. Each provider may use a set of call control, call routing, and bearer functional entities to connect to multiple peer networks.
4. SIP Back-to-Back User Agent (B2BUA) functions may be used in support of network interconnection.
5. There may be an IP Transit Network between two peering VoIP Service Providers.
6. SIP is used for call control signaling. The SIP messages may contain MIME'd ISUP in order to facilitate interoperability with the PSTN.
7. RTP is used for voice transport.

8. Perimeter defense (e.g., topology hiding, DoS prevention, and detection) functionality is supported, but the specification of this functionality is outside the scope of this standard.
9. Traffic management (e.g., traffic monitoring, shaping, and QoS) is supported, but the specification of traffic management functionality is outside the scope of this standard.
10. IPv4 is required to be supported at the NNI.
11. The IPv6 carrier is responsible for interworking between IPv4 and IPv6.

2 NORMATIVE REFERENCES

2.1 ANSI References[1]

1. T1.113-2000, *Signaling System No. 7 (SS7) - Integrated Service Digital Network User Part (ISUP)*.
2. T1.508-2003, *Loss Plans for Evolving Networks*.
3. T1.607-2000 (R2004), *Digital Subscriber Signaling System No. 1 - Layer 3 Signaling Specification for Circuit-switched Bearer Service*.
4. T1.611-1991 (R2003), *SS7 - Supplementary Services for non-ISDN Subscribers*.
5. T1.613-1991 (R2002), *DSS1 - ISDN Call Waiting*.
6. T1.616-1992 (R2004), *ISDN - Call Hold Supplementary Services*.
7. T1.621-1992 (R2004), *User-to-User Signaling - Supplementary Service Description*.
8. T1.622-1999 (R2003), *Message Waiting Indicator Control and Notification and Associated Switching and Signaling Specifications*.
9. T1.625-1993 (R2003), *ISDN - Calling Line Identification Presentation and Restriction Supplementary Services*.
10. T1.625a-1998 (R2003), *ISDN - Calling Line Identification Presentation and Restriction - Application of Standard to Wireless PCS*.
11. T1.628-2000 (R2005), *Emergency Calling Service*.
12. T1.628a-2001 (R2005), *Connection and Ringback*.
13. T1.632-1993 (R2004), *ISDN Supplementary Service Normal Call Transfer*.
14. T1.639-1995 (R2001), *Calling Name Identification Restriction*.
15. T1.639a-2001 (R2006), *Supplement to Calling Name Identification Restriction*.
16. T1.641-1995 (R2004), *Calling Name Identification Presentation*.
17. T1.642-1995 (R2004), *ISDN - Supplementary Service Call Deflection*.
18. T1.643-1998 (R2003), *ISDN - Explicit Call Transfer Supplementary Service*.
19. T1.647-1995 (R2000), *ISDN - Conference Calling Supplementary Service*.
20. T1.647a-1998 (R2002), *Integrated Services Digital Network (ISDN) - Conference Calling Supplementary Service - Operations Across Multiple Interfaces*.
21. T1.653-1996 (R2000), *ISDN - Call Park Supplementary Service*.
22. T1.653a-1998 (R2005), *ISDN - Call Park Supplementary Service - Clarification for Number Identification*.

[1] These documents are available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005. < https://www.atis.org/docstore/default.aspx >

23. T1.673-2002, *BICC Capability Set 1+*.
24. T1.679-2004, *Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control or ISDN User Part*.
25. ATIS-PP-1000007.2006, *Generic Signaling and Control Plane Security Requirements for Evolving Networks*.

2.2 ITU References[2]

1. ITU-T Recommendation T.38 (02/00), *Procedures for real-time Group 3 facsimile communication over IP networks*.
2. ITU-T Recommendation G.131 (08/96), *Control of talker echo*.
3. ITU-T Recommendation G.136 (09/99), *Application rules for automatic level control devices*.
4. ITU-T Recommendation G.165 (03/93), *Echo cancellers*.
5. ITU-T Recommendation G.168 (08/04), *Digital network echo cancellers*.
6. ITU-T Recommendation G.711 (11/88), *Pulse code modulation (PCM) of voice frequencies*.

2.3 IETF References[3]

2.3.1 Call Control Signaling

1. IETF RFC 2046 (1996), *Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types*.
2. IETF RFC 2327 (1998), *SDP: Session Description Protocol*.
3. IETF RFC 2806 (2000), *URLs for Telephone Calls*.
4. IETF RFC 2976 (2000), *The SIP INFO Method*.
5. IETF RFC 3204 (2001), *MIME media types for ISUP and QSIG Objects*.
6. IETF RFC 3261 (2002), *SIP: Session Initiation Protocol*.
7. IETF RFC 3264 (2002), *An Offer/Answer Model with the Session Description Protocol (SDP)*.
8. IETF RFC 3325 (2002), *Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks*.
9. IETF RFC 3326 (2002), *The Reason Header Field for the Session Initiation Protocol (SIP)*.
10. IETF RFC 3323, *A Privacy Mechanism for the Session Initiation Protocol (SIP)*.
11. IETF RFC 3324, *Short Term Requirements for Network Asserted Identity*.
12. IETF RFC 3398, *Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping*.
13. IETF RFC 3420, *Internet Media Type message/sipfrag*.
14. IETF RFC 3428, *Session Initiation Protocol (SIP) Extension for Instant Messaging*.
15. IETF RFC 3515, *The Session Initiation Protocol (SIP) Refer Method*.
16. IETF RFC 3824, *Using E.164 numbers with the Session Initiation Protocol (SIP)*.
17. IETF RFC 3966, *The tel URI for Telephone Calls*.

---

[2] These documents are available from the International Telecommunications Union. < http://www.itu.int/ITU-T/

[3] These documents are available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >

18. draft-ietf-iptel-trunk-group-06.txt, *Representing Trunk Goups in tel/sip URIs* (status: stable- AD watching).
19. IETF RFC 3959, *The Early Session Disposition Type for the SIP*.
20. IETF RFC 3893, *SIP Authenticated Identity Body (AIB) Format*.
21. IETF RFC 3911, *The Session Initiation Protocol (SIP) "Join" Header*.
22. IETF RFC 3892, *The SIP Referred-By Mechanism*.
23. IETF RFC 3891, *The Session Initiation Protocol (SIP) "Replaces" Header*.
24. IETF RFC 4412, *Communications Resource Priority for the Session Initiation Protocol (SIP)*.
25. IETF RFC 4028, *Session Timers in SIP*.
26. IETF RFC 3960, *Early Media and Ringback Tone Generation in the Session Initiation Protocol*.
27. draft-ietf-iptel-tel-np-08.txt, *New Parameters for the "tel" URI to Support Number Portability* (status: stable- AD Evaluation).
28. IETF RFC 3087, *Control of Service Context using SIP Request-URI*.

2.3.2 Media References

1. IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*.
2. IETF RFC 3551 (2003), *RTP Profile for Audio and Video Conferences with Minimal Control*.
3. IETF RFC 2833 (2000), *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*.
4. 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*.
5. IETF RFC 3389 (2002), *RTP Payload for Comfort Noise*.

2.4 Other References[4]

1. TIA-920, *Telecommunication Telephone Terminal Equipment Transmission Requirements for Wideband Digital Wireline Telephones*.

3 DEFINITIONS

For ISUP specific terminology, refer to T1.113.2. For SIP and SDP specific terminology, refer to IETF RFC 3261 and IETF RFC 2327, respectively. Definitions for additional terms used in this standard are as follows:

3.1 Border B2BUA: A SIP B2BUA that performs IP network border functions in its reformulation of SIP messages.

NOTE - These functions include NAT/NAPT editing of IP address, port number of the session, and application content of SIP messages. They may also include media relay resource assignments with corresponding execution of control functions that establish NAPT building in the media relay.

[4] This document is available from the Telecommunications Industry Association (TIA).
< http://www.tiaonline.org/standards/overview.cfm >

3.2 NAT: Network Address Translation (NAT) is a method of converting one IP address space to another IP address space.

NOTE - It is primarily used to interface internal (private) IP address space of a network with the global (public) address space of the internet.

3.3 Outgoing SIP or ISUP [Network]: With the term "network", this phrase refers to the network to which the outgoing calls are sent. The adjective "SIP" or "ISUP" refers to the protocol used in the outgoing network. Without the term "network", the phrase refers only to the protocol in the outgoing network.

3.4 Redirect Server: A user agent server that generates 3XX responses to requests it receives, directing the client to contact an alternate set of URIs.

3.5 SIP 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 IETF 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 must 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 behavior is defined in IETF RFC 3261.) A B2BUA reformulates a message before sending it as a new request.

3.6 SIP with Encapsulated ISUP (SIP-I): This phrase refers to the use of SIP with a message body that encapsulates the ISUP information according to the requirements in T1.679.

NOTE - In addition, this Standard makes use of the terms *header field*, *message*, *message body*, *method*, *provisional response*, and *User Agent*, which are defined in IETF RFC 3261, clause 6. It uses the term *payload type* as defined in IETF RFC 3550, and *static* and *dynamic* payload type as defined in that RFC. Finally, it uses the terms *attribute* and *session* as defined in IETF RFC 2327.

4 ABBREVIATIONS & ACRONYMS

This document uses the following abbreviations:

GENERAL

ABNF	Augmented Backus-Naur Form
ALG	Application Layer Gateway
AMR	Adaptive Multirate (codec)
ASN	Adjacent SIP Node
B2BUA	Back-to-Back User Agent
BFE	Bearer Functional Entity
CC	Country Code
CCFE	Call Control Functional Entity
CLI	Calling Line Identification
DoS	Denial of Service
FFS	For further study
IANA	Internet Assigned Numbers Authority
IETF	Internet Engineering Task Force

IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISN	Interface Serving Node
ISUP	ISDN User Part
IWU	Interworking Unit
MGC	Media Gateway Controller
MIME	Multi-purpose Internet Mail Extensions
NAPT	Network Address and Port Translation
NAT	Network Address Translation
NDC	National Destination Code
NNI	Network To Network Interface
NP	Number Portability
PSTN	Public Switched Telephone Network
PT	Payload Type
RCTP	Real-Time Transport Control Protocol
RFC	Request For Comments
RTP	Real-Time Transport Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SIP-I	SIP with encapsulated ISUP
SN	Subscriber Number
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UNI	User To Network Interface
URI	Universal Resource Identifier

ISUP MESSAGES

ACM	Address Complete Message
ANM	Answer Message
APM	Application Transport Mechanism
BAT	Bearer Association Transport
CGB	Circuit Group Blocking
COT	Continuity
CPG	Call Progress
EXM	Exit
GRS	Circuit Group Reset
IAM	Initial Address Message
REL	Release
RES	Resume
RLC	Release Complete
RSC	Reset Circuit
SGM	Segmentation Message
SUS	Suspend

ISUP PARAMETERS AND VALUES

APP	Application Transport Parameter
APRI	Address Presentation Restricted Indicator
ATP	Access Transport Parameter
BCI	Backward Call Indicators
CgPN	Calling Party Number
CIC	Circuit Identification Code (ISUP)
	Call Instance Code (BICC)
FCI	Forward Call Indicators
HLC	High Layer Compatibility
NOA	Nature of Address indicator
NP	"*network provided*" (Screening Indicator value)
UPVP	"*user provided, verified and passed*" (Screening Indicator value)
USI	User Service Information

5 REFERENCE MODEL

Figure 2 illustrates the interconnection reference model for IP NNI supporting VoIP. The following Functional Elements are illustrated:

- *CCFE*: Performs SIP-based call/session control signaling functions with its counterpart in the peering network.
- *BFE*: Performs bearer/media-path-related functions with its counterpart in the peering network.
- *CRFE*: A placeholder for a future Call Routing FE that, if present, exchanges call routing information with its counterpart in the peering network. This entity is not utilized or defined further in this edition of this standard.

CCFE, BFE, and CRFE provide Session Border Controller functions.

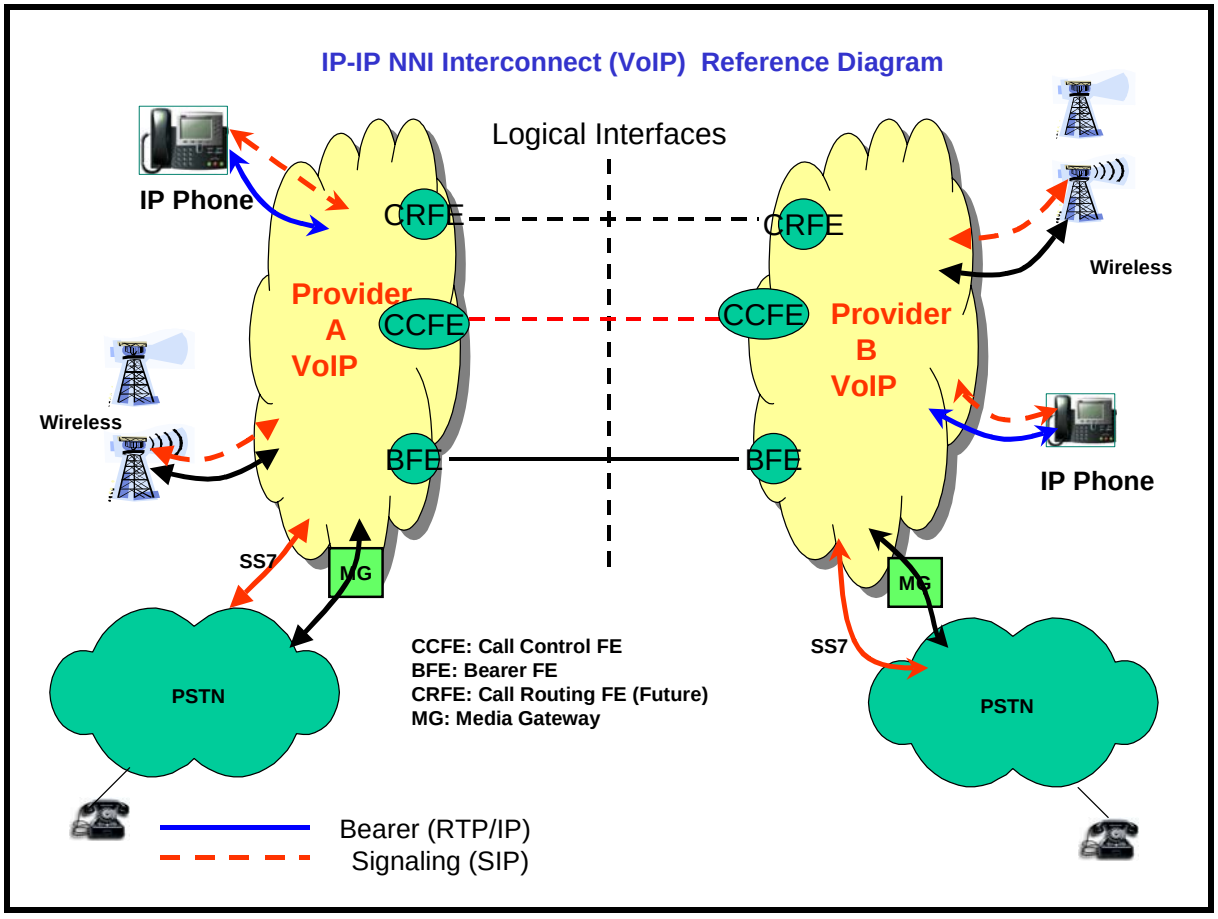


Figure 2 - VoIP Interconnection Reference Model

5.1 VoIP Interconnection Alternatives

VoIP traffic can be exchanged in several ways. It can be exchanged over existing peering interconnection used for other IP traffic, dedicated IP peering interconnections (e.g., VPNs), or via transit IP networks.

The VoIP traffic could traverse the same routers and facilities as other IP traffic (data). If VoIP traffic is exchanged over existing IP peering interconnections used for other IP traffic, there are several issues that need to be addressed:

- *Security and Availability*: VoIP traffic is being exchanged over the same routers used for exchange of Internet traffic. These routers may experience problems associated with various Internet problems and may be shut down.
- *QoS*: If VoIP traffic requires QoS different from other IP traffic, the peering arrangement must support the honoring of QoS marking across network boundaries. This may also require policing to ensure that the agreed-upon traffic profile is being honored. For example, if it is agreed that no more than 20% of the traffic is VoIP and receiving the highest QoS, then the originating peer should not exceed that level and the terminating Tier 1 peer should be able to provide the appropriate level of service.

- *Peering uses "hot-potato" routing where packets flowing in the two directions will most likely take different routes*: This happens because each side of a peering interconnection tends to hand off traffic at the point closest to its own backbone. In other words, the general rule is to get the traffic off your own network and onto the peering network as early as possible. So, for a VoIP call, packets flowing from the originating peer may be taking a different path than packets for the same call, flowing from the terminating peer. This may have performance implications.

Carriers could also choose to interconnect the VoIP traffic with each other in a VPN arrangement, over new or existing IP facilities. Using a VPN reduces the impact of the issues identified in the bullet list above.

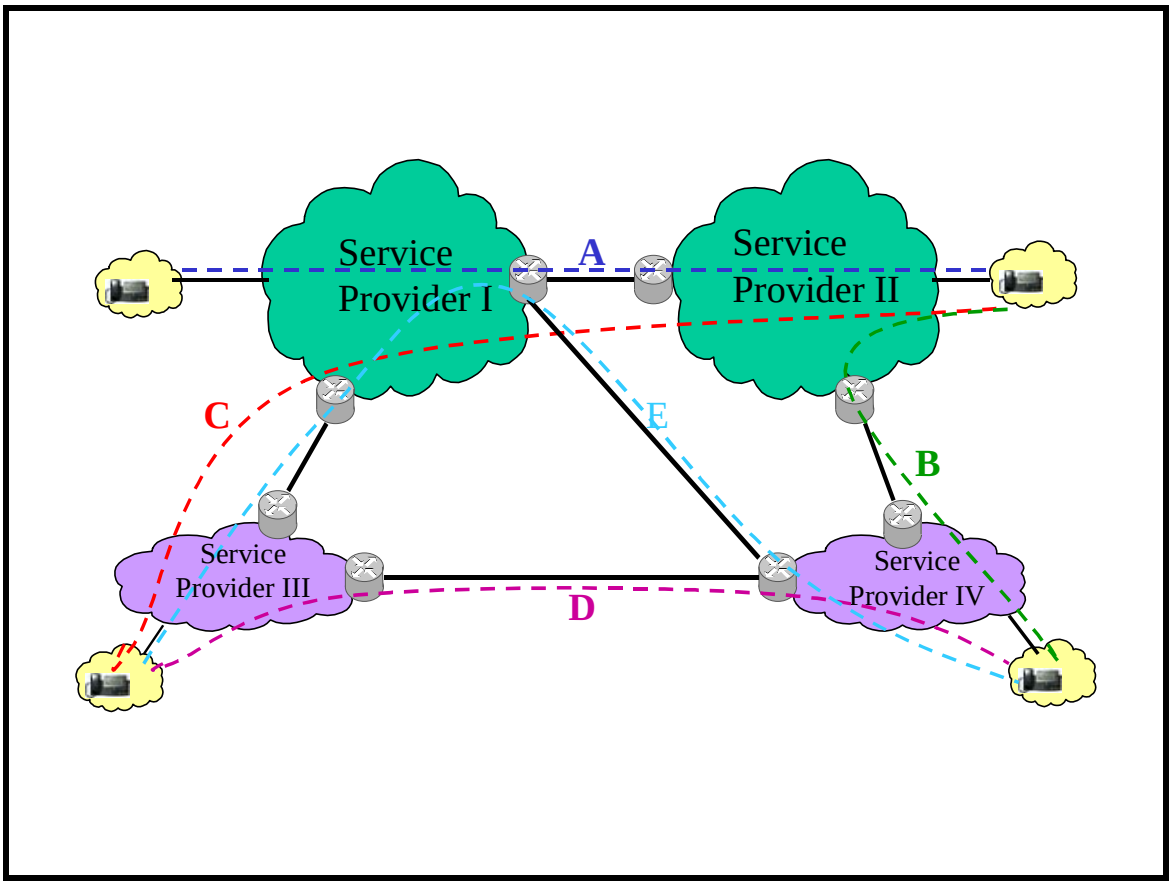


Figure 3 - VoIP Interconnection Alternatives

Figure 3 illustrates several interconnection arrangements, either with direct interconnection or via a transit IP provider:

- *Flow A* illustrates an IP-IP call where Service Provider (SP) I & SP II are both VoIP SPs and the interconnection may be via an existing IP peering interconnection or via a VPN for VoIP traffic.
- *Flow B* illustrates an IP-IP call where SP IV is a VoIP SP, and SP II maybe either a VoIP SP or an Access SP.

- *Flow C* illustrates an IP-IP call where SP III is a VoIP SP, SP I is a Transit IP SP, and SP II is either a VoIP SP or an Access SP.
- *Flow D* illustrates an IP-IP call where SP III & IV are both VoIP SPs interconnecting with dedicated facilities. These SPs access the "public internet" via SP I and/or SIP II.
- *Flow E* illustrates an IP-IP call where SP III & IV are both VoIP SPs, and SP I is either a Transit or VoIP SP.

Any of these services providers may access the PSTN either:

- Directly with their own PSTN gateways;
- Via another network acting as a VoIP; or
- Via another network acting as a Transit Network provider.

6 TRAFFIC MODEL (TYPES OF SERVICES)

Figure 4 illustrates the various traffic types that could be supported on the NNI between two carriers including:

- PSTN originating VPN, UNI, Local, International, or Inter-Exchange traffic;
- PSTN terminating VPN, UNI, Local, International, or Inter-Exchange traffic;
- IP originating VPN, UNI, Local, International, or Inter-Exchange traffic; or
- IP terminating VPN, UNI, Local, International, or Inter-Exchange traffic.

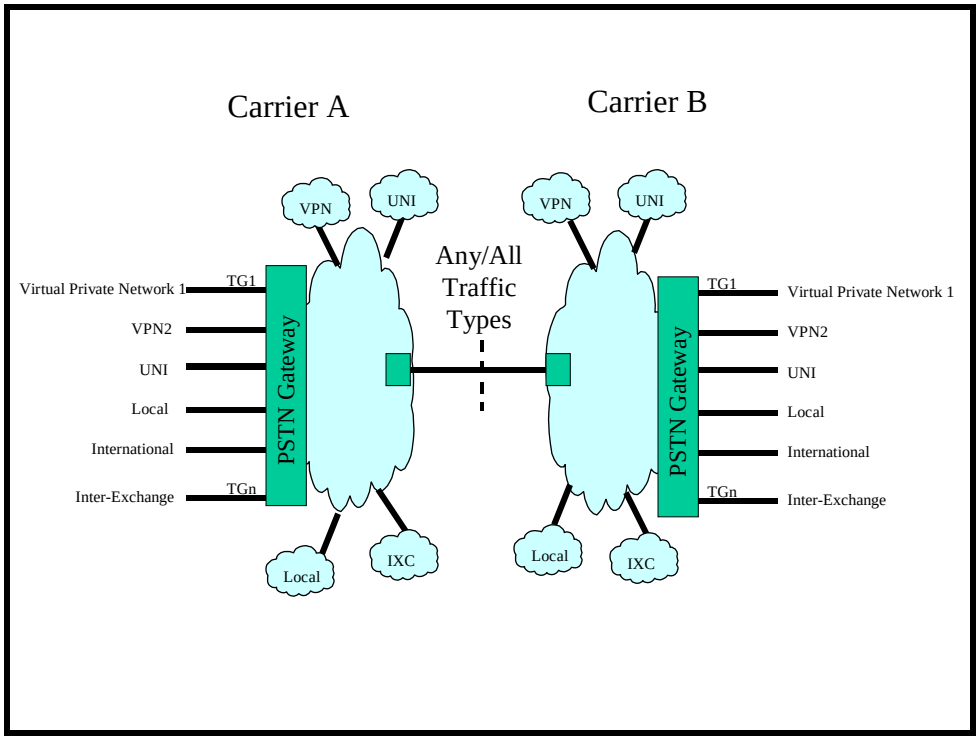


Figure 4 - Traffic Type Model

Currently in circuit-switched networks, service processing is triggered/initiated based on various variables including:

- Trunk received on and/or terminated to;
- Signaling; and
- Intelligent Network processing.

Typically, trunk groups segregate different types of service traffic, these include:

- Local;
- Inter-exchange;
- Wholesale; and
- Virtual Private Network.

As networks evolve from interconnecting with circuit-switched technology to IP technology, there will still be a need to provide interoperability of services.

In order to take advantage of the cost savings of IP technology, carriers will interconnect with larger IP "pipes" that contain mixed traffic types.

A preferred solution would relay the traffic/service type information in the SIP call control signaling.

The SIP mechanism described below can be used to represent the traffic group (e.g., VPN traffic, international traffic, etc.) for a call.

IETF draft-ietf-iptel-trunk-group-06.txt defines a SIP mechanism to convey a trunk group identifier in a sip or tel URI. This identifier is placed in the user portion of the URI. The *trunk group identifier* consists of two parameters: *trunk-group* and *trunk-context*. Both of these parameters must be present to identify a trunk group. The *trunk-group* parameter provides a trunk group label. The *trunk-context* serves a purpose analogous to the phone-context parameter of the tel URI. The trunk group identifier can be placed in the SIP Contact header (to indicate the ingress, or originating, trunk group) or in the Request-URI (to indicate the egress, or terminating, trunk group). A SIP routing entity (e.g., a proxy or a redirect server) may insert a trunk group identifier in the Request-URI to indicate to a downstream entity which egress trunk group to use when routing the call.

The trunk group identifier is applicable to both PSTN and IP call/session originations/terminations.

A UAC that initiates a call may include the trunk group identifier in the Contact header to indicate the ingress (originating) trunk group used for the call. Subsequent requests destined to that UAC must copy the trunk group information from the Contact header into the Request-URI.

To the UAS processing the request, a trunk group identifier in the Request-URI indicates that it should use the named trunk group for the outbound call.

The trunk group identifier can reveal the network topology and the routing policies used by a carrier. Therefore, the trunk group extension may be optionally supported at the IP-IP NNI.

7 MEDIA AVAILABILITY IN A SIP SESSION

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

a) The terminating-side network of the NNI must 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:

- ♦ Must pass media packets from the originating party toward the terminating party no later than on receipt of a SIP 2XX response to the INVITE.
- ♦ May pass media packets from the originating party toward the terminating party any time after receipt of the first SDP answer, which may be in a SIP 1XX or 2XX response to the INVITE. A network, as a policy, may choose to not send media packets from the originating party until the final SDP offer/answer has occurred in order to avoid theft-of-service in cases where usage-sensitive billing is employed.

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

d) The absence of media packets across the NNI in either direction over any time interval shall not be taken by either network as a reason to clear the SIP session.

8 CALL/SIGNALING FLOWS (INFORMATIVE)

This section illustrates 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 ANSI T1.679. The interworking between ISUP and SIP is shown at the diagrammatic level to illustrate interoperability. ANSI T1.679 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 IETF RFC 3261.

The following symbols (Figure 5) are used in the figures in this section:

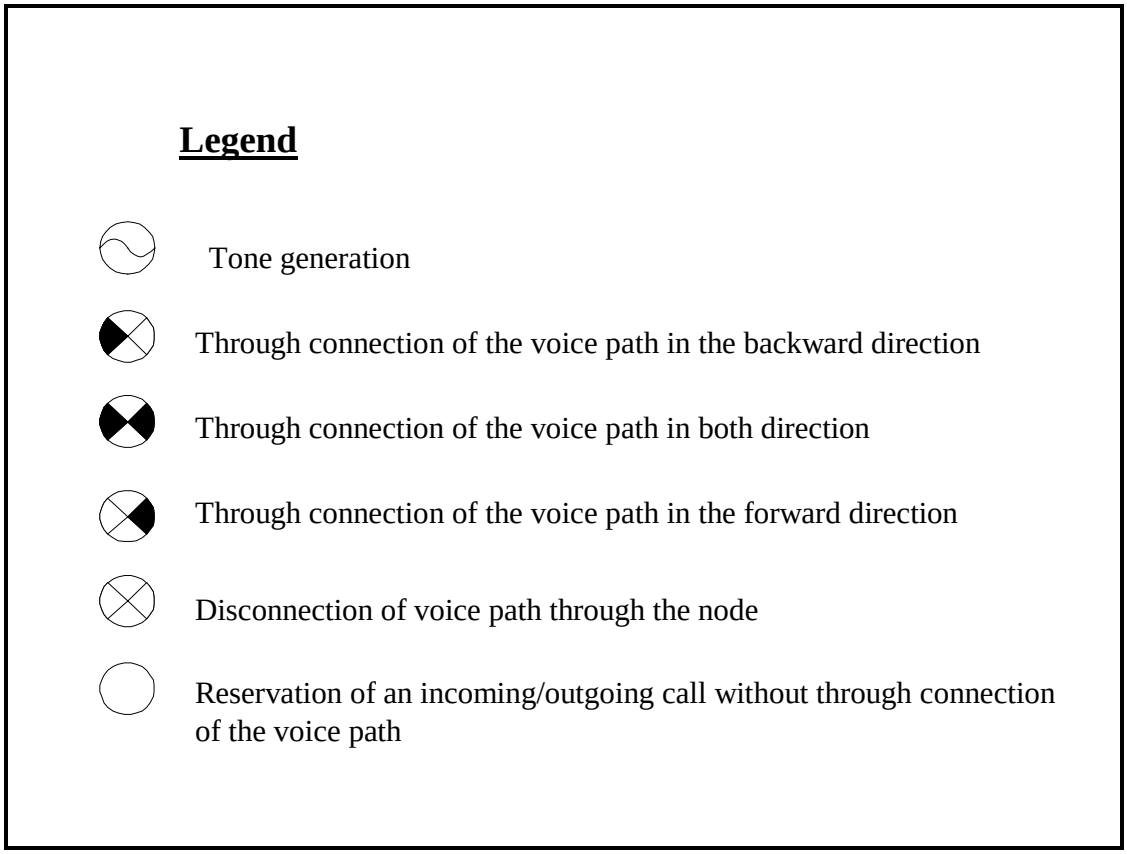


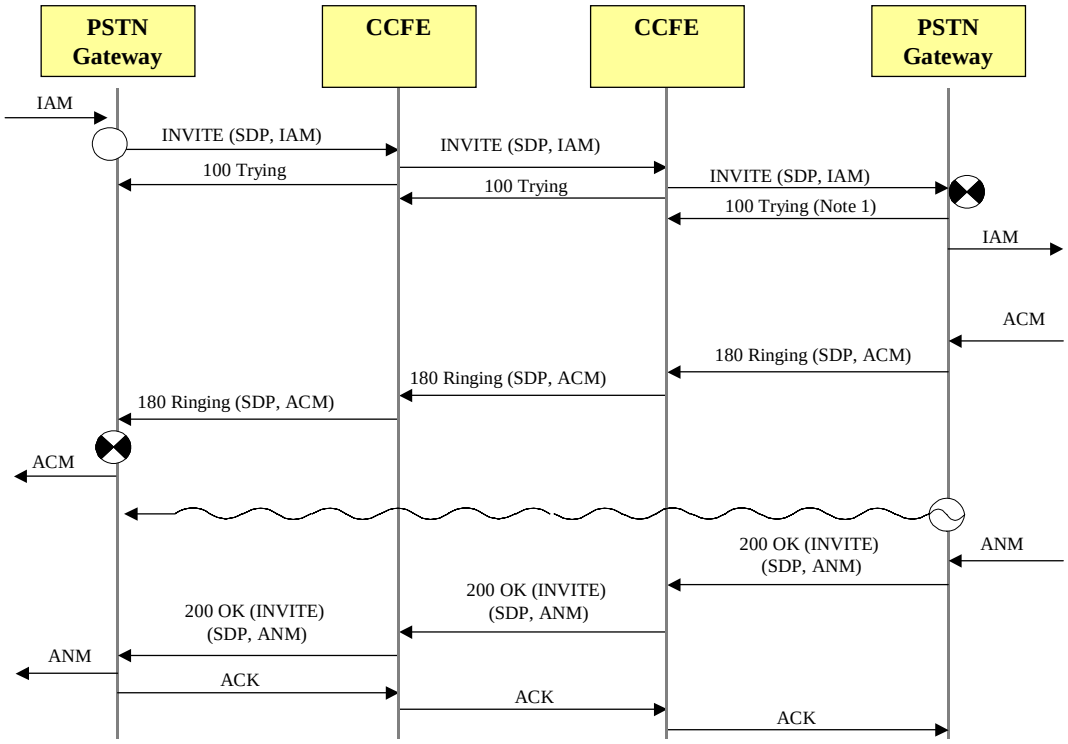
Figure 5 - Call/Signaling Flow Legend

8.1 PSTN—IP—(NNI)—IP—PSTN

This section 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.

8.1.1 Successful Call Setup (SIP Preconditions Not Used)

Figure 6 shows a typical sequence of messages for successful call setup for an incoming ISUP call over SIP-I. The PSTN Gateway performs the through-connection of the bearer path in both directions after the receipt of SDP answer in the 180 Response.



Note 1 - 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 6 - Successful Call Setup

8.1.2 Normal Call Release without Tone Provision

Figure 7 shows typical call release interworking procedures for normal call release without tone provision. A REL message is mapped and encapsulated into a BYE request to preserve ISUP signaling transparency.

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

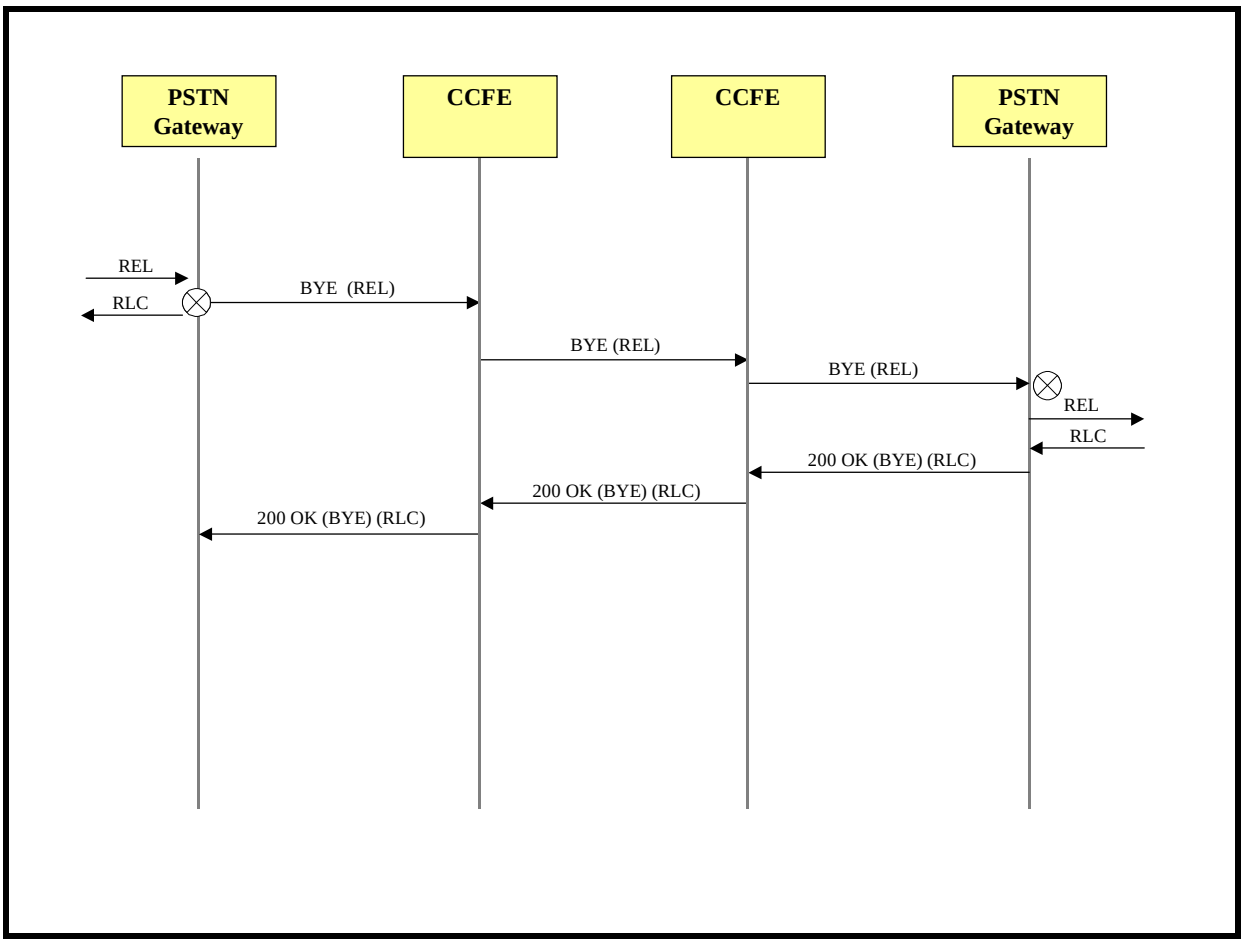


Figure 7 - Normal Call Release without Tone Provision

8.2 PSTN—IP—(NNI)—IP—IP

This section 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.

8.2.1 Successful Call Setup (SIP Preconditions Not Used)

Figure 8 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.

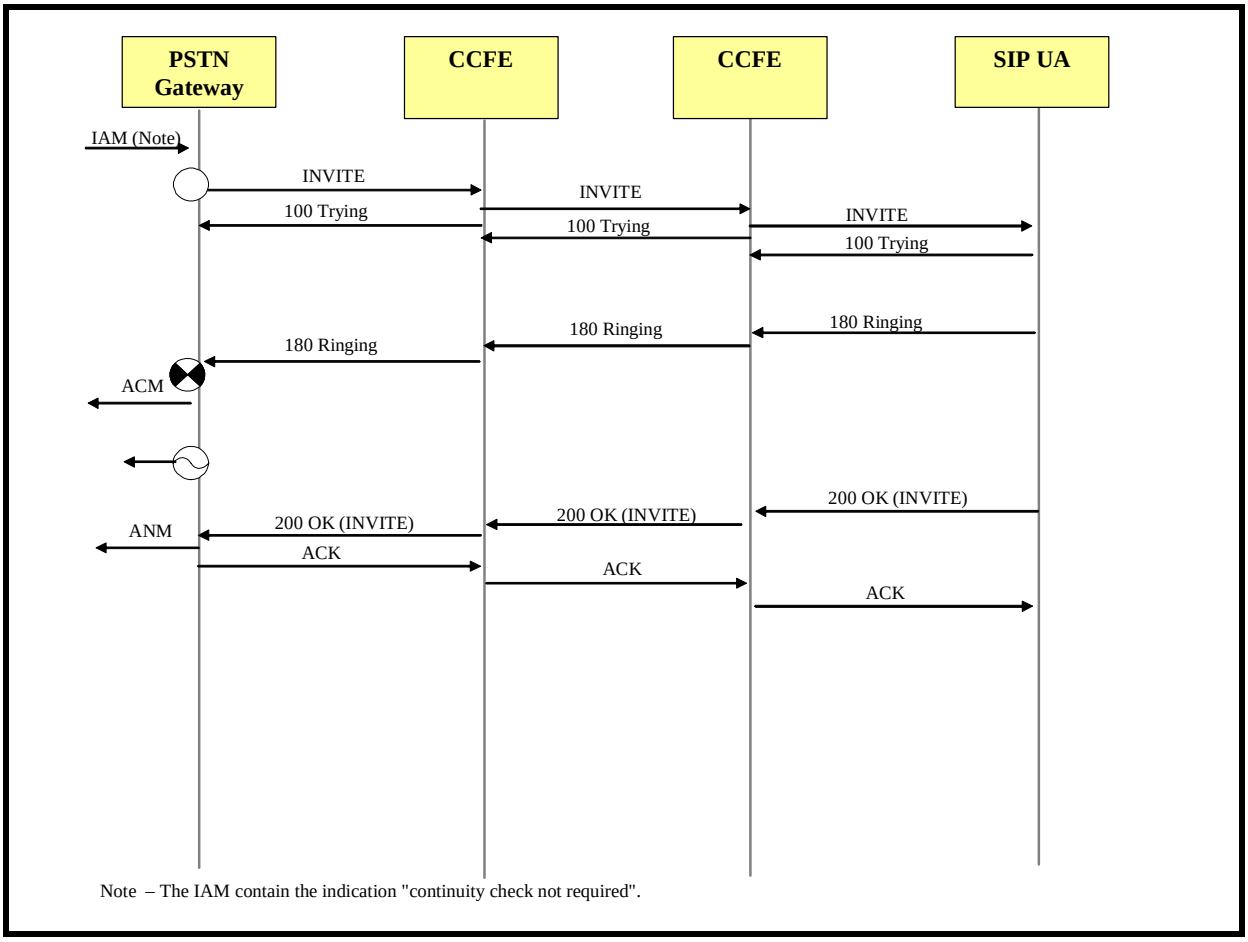


Figure 8 - Successful Call Setup from ISUP to SIP

8.2.2 Normal Call Release Initiated from the ISUP Side

Figure 9 shows a normal call release procedure initiated from the ISUP side of the call. This call flow assumes that no resource reservation teardown signaling is required on the SIP side of the call.

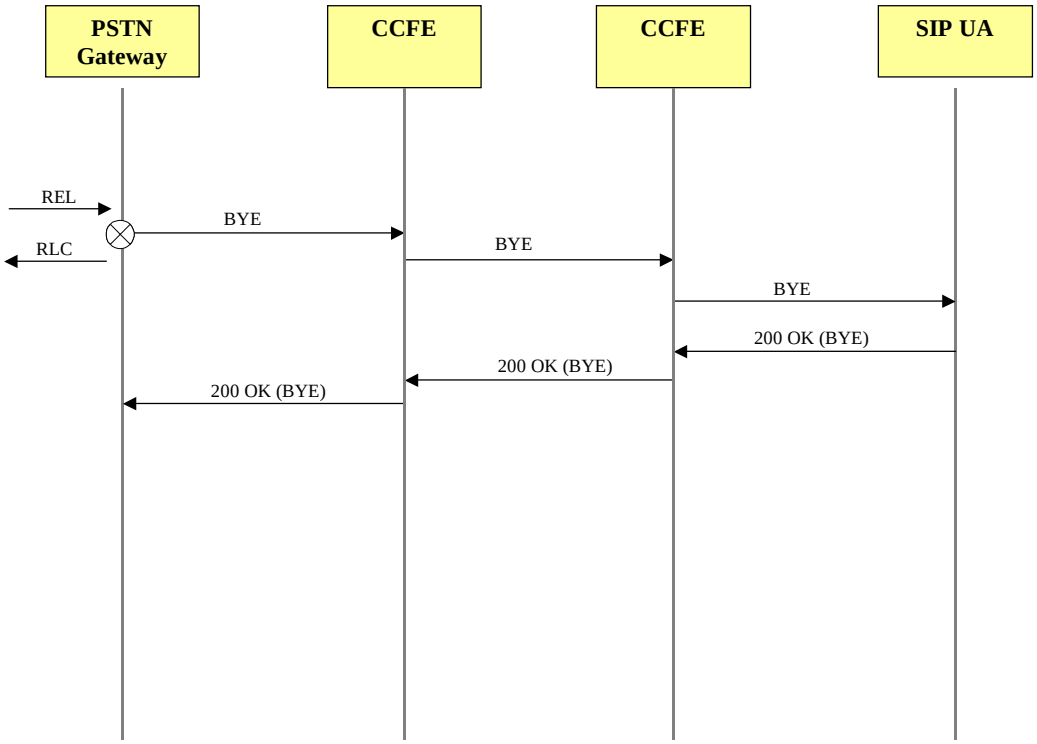


Figure 9 - Normal Call Release from ISUP to SIP

8.3 IP—IP—NNI—IP—PSTN

This section 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.

8.3.1 Successful Call Setup (SIP Preconditions Not Used)

Figure 10 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).

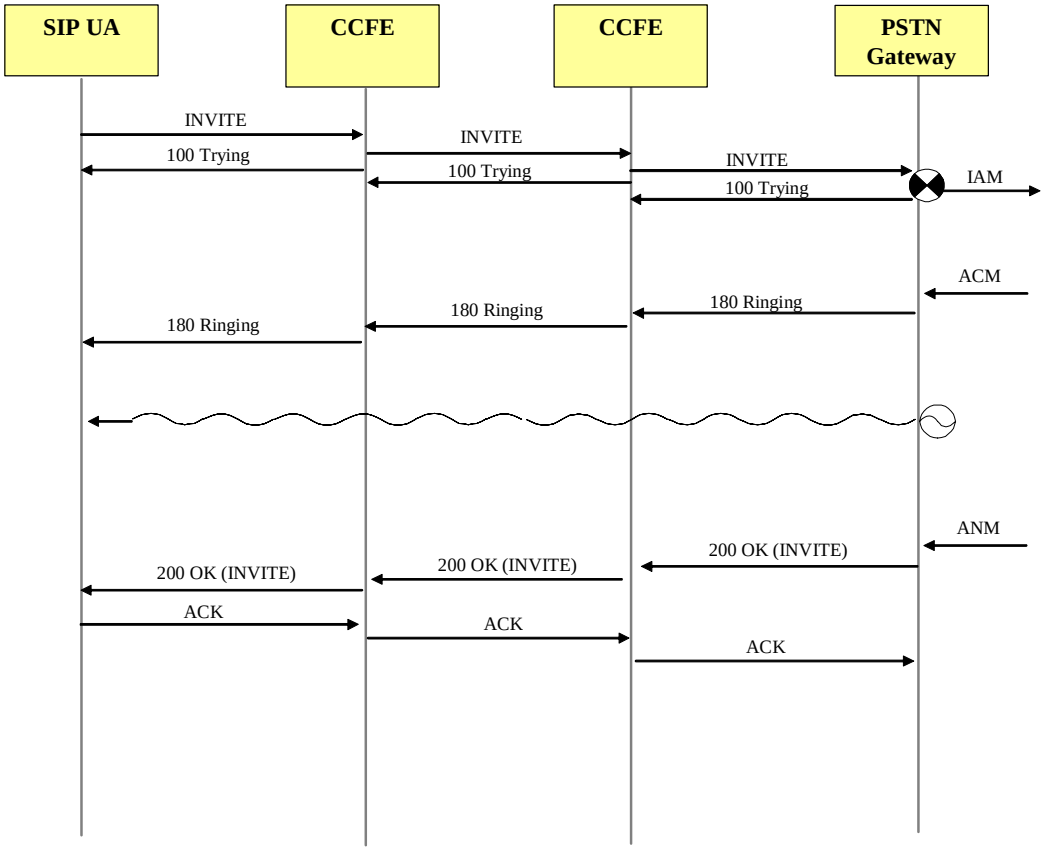


Figure 10 - Successful Call Setup from SIP to ISUP

8.3.2 Normal Call Release Procedure Initiated from the SIP Side

Figure 11 shows the sequence of messages for normal call release procedure initiated from the SIP side of the call. This call flow assumes that no resource reservation teardown signaling is required on the SIP side.

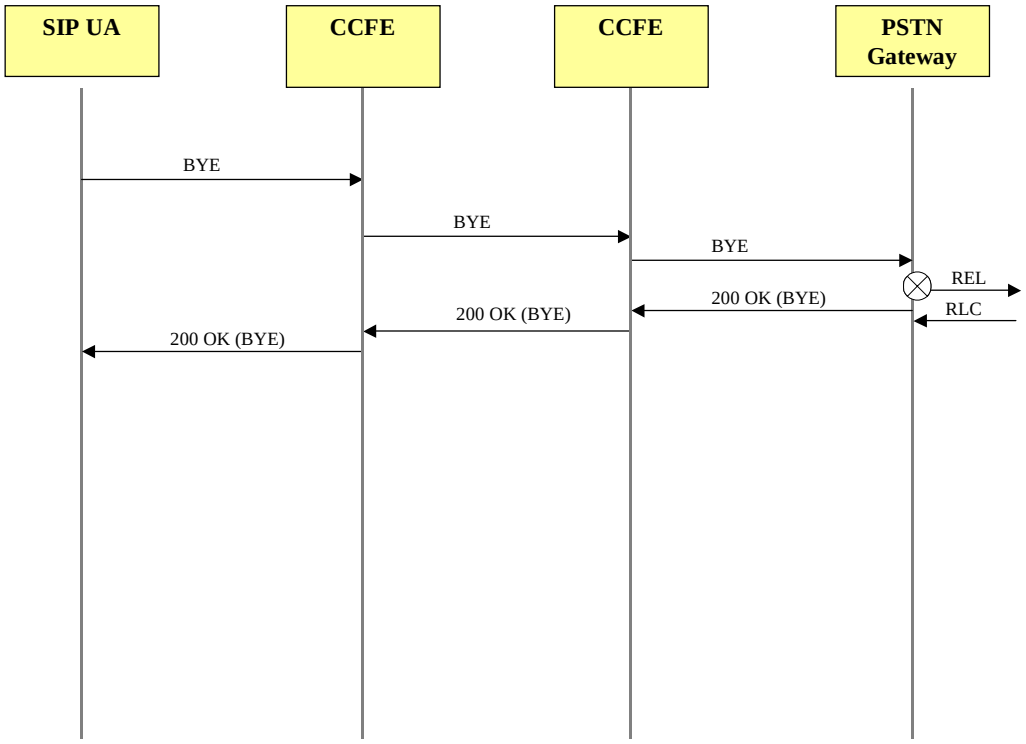


Figure 11 - Normal Call Release from SIP to ISUP

8.4 IP—IP—(NNI)—IP—IP

This section 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 an IP network without transiting a non-IP network.

8.4.1 Successful Call Setup (SIP Preconditions Not Used)

Figure 12 shows a typical sequence of messages for successful call setup for a basic call at the SIP NNI.

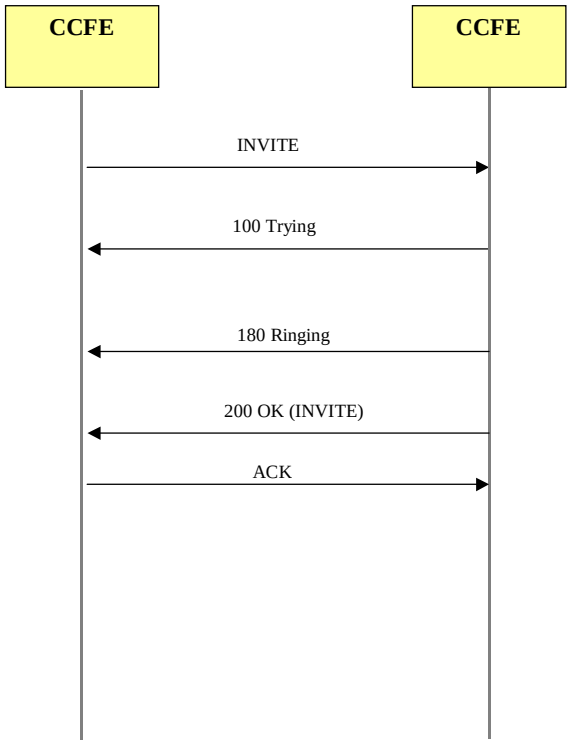


Figure 12 - Successful Call Setup at IP-IP SIP NNI

8.4.2 Normal Call Release

Figure 13 shows the sequence of messages for normal call release at the SIP NNI.

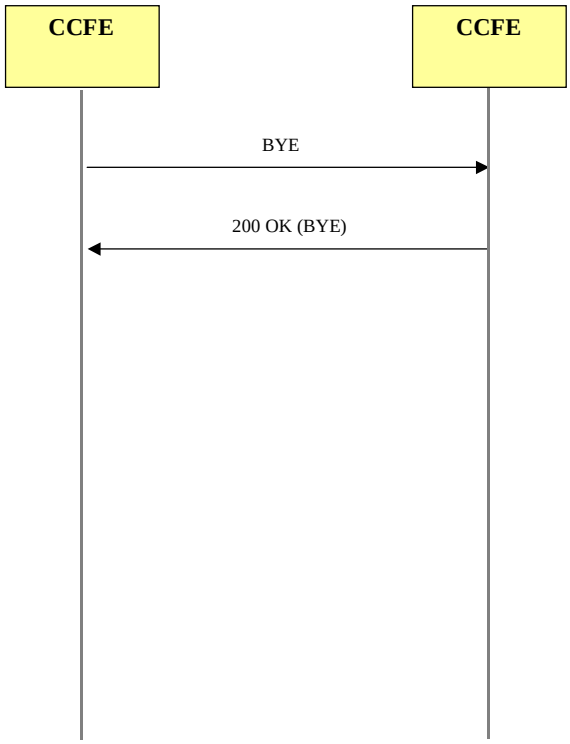
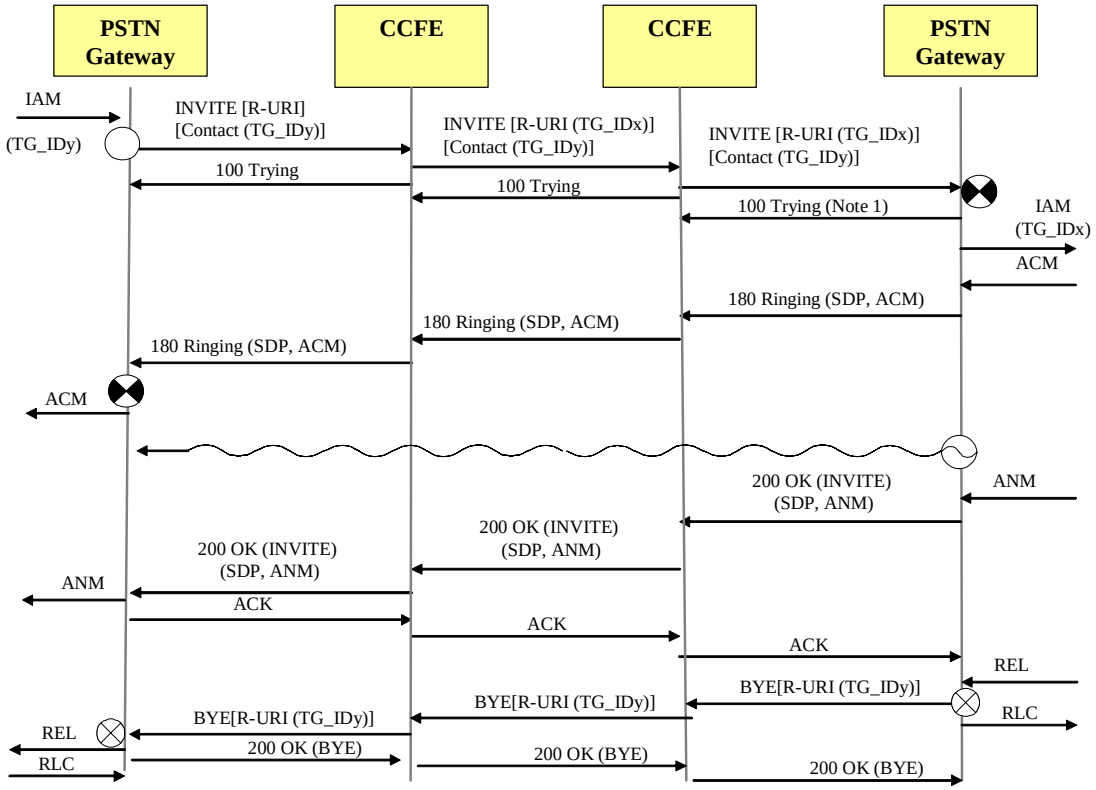


Figure 13 - Normal Call Release at IP-IP SIP NNI

8.5 Usage of Trunk Group Identifier Call Flow

Figure 14 shows the sequence of messages for a typical SIP call flows illustrating the usage of trunk group identifier.



Note 1 - 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 14 - Successful Call Setup using Trunk Group Identifier

9 QUALITY OF SERVICE

9.1 Voice Quality

9.1.1 Codec

In order to support interoperability, VoIP networks shall support G.711 and optionally support additional codecs based on bilateral agreements.

9.2 Echo Control

The degree of end user annoyance due to talker echo depends both on the amount of delay and on the level difference between the voice and echo signals. In TDM networks echo is usually controlled adequately if ITU-T Recommendation G.131, *Control of Talker Echo*, is applied. Connections requiring echo cancellers should use devices that at least meet the requirements of either ITU-T Recommendation G.165 or ITU-T Recommendation G.168.

As this NNI connection utilizes packet transmission and hence is a non-linear facility, and non-linear facilities should not exist in the tail path of an echo canceller, echo cancellation -- if required -- shall be

applied to signals prior to their crossing the NNI. If digital telephone sets are used, they shall comply with ANSI/TIA/EIA-810-A or TIA-920.

9.3 Automatic Level Control Devices

If Automatic Level Control devices are used, their use shall be compliant with ITU-T Recommendation G.136.

9.4 Transmission Plan

Networks shall follow T1.508-2003, *Loss Plans for Digital Networks*.

10 MANDATORY SIP URIS TO BE SUPPORTED

The table below describes the set of URI formats that shall be supported on the IP-NNI, and the headers in which these formats may appear. This is not intended to preclude the use of tel or sips URIs.

Table 1 – SIP URI Formats for IP-NNI

URI	`sip:+1NPANXXXXXX@host;user=phone`
Description	NANP number
Reference	IETF RFC3966
Headers	R-URI, To, From, Request Contact, 3XX Contact, PAI, Diversion
URI	`sip:+18YYXXXXXXX@host;user=phone`
Description	NANP 8YY number
Reference	IETF RFC3966
Headers	R-URI, To, 3XX Contact
URI	`sip:+1NPA5551212@host;user=phone`
Description	NANP Directory Assistance in global number format
Reference	IETF RFC3966
Headers	R-URI, To, 3XX Contact
URI	`sip:0;phone-context=+1@host;user=phone`
Description	NANP operator requested in local number format
Reference	IETF RFC3966
Headers	R-URI, To, 3XX Contact
URI	`sip:0NPANXXXXXX;phone-context=+1@host;user=phone`
Description	NANP operator requested in local number format
Reference	IETF RFC3966
Headers	R-URI, To, 3XX Contact
URI	`sip:00;phone-context=+1@host;user=phone`
Description	NANP long distance operator requested in local number format
Reference	IETF RFC3966
Headers	R-URI, To, 3XX Contact
URI	`sip:+1NPANXXXXXX;npdi@host;user=phone`
Description	NANP number with Number Portability Dip Indicator
Reference	http://www.ietf.org/internet-drafts/draft-ietf-iptel-tel-np-09.txt
Headers	R-URI, To, 3XX Contact
URI	`sip:+1NPANXXXXXX;rn=+1NPANXXXXXX;npdi@host;user=phone`
Description	NANP number with Number Portability Dip indicator and LRN
Reference	http://www.ietf.org/internet-drafts/draft-ietf-iptel-tel-np-09 .txt
Headers	R-URI, To, 3XX Contact
URI	`sip:+1NPANXXXXXX;cic=+10288@host;user=phone`
Description	NANP number with Carrier Identification Code, NPA may be an 8YY
Reference	http://www.ietf.org/internet-drafts/draft-ietf-iptel-tel-np-09.txt

Headers	R-URI, To, 3XX Contact
URI	`sip:+1NPANXXXXXX;cic=+10288;dai@host;user=phone`
Description	NANP number with Carrier Identification Code and dial around indicator; NPA may be an 8YY
Reference	http://www.ietf.org/internet-drafts/draft-ietf-iptel-tel-np-09.txt
Headers	R-URI, To, 3XX Contact
URI	`sip:+1NPANXXXXXX@host;user=phone;isup-oli=0`
Description	NANP number with OLI
Reference	IETF RFC3966
Headers	From
URI	`sip:+1NPANXXXXXX;rn=+1NPANXXXXXX@host;user=phone`
Description	NANP number with JIP (used in a From, PAI, or Diversion header)
Reference	
Headers	From, PAI, Diversion
URI	`sip:N11;phone-context=+1@host;user=phone`
Description	NANP special service code in local number format
Reference	IETF RFC3966
Headers	R-URI, To, 3XX Contact
URI	`sip:613131;phone-context=+1@host;user=phone`
Description	NANP directory assistance in local number format
Reference	IETF RFC3966
Headers	R-URI, To, 3XX Contact
URI	`sip:+CCNSN@host;user=phone`
Description	International number, CC=Country Code, NSN=National Significant Number
Reference	IETF RFC3966
Headers	R-URI, To, From, Request Contact, 3XX Contact, PAI, Diversion
URI	`sip:B;phone-context=+33@host;user=phone`
Description	Directory assistance in local number format in country with CC 33
Reference	IETF RFC3966
Headers	R-URI, To, 3XX Contact

11 SIGNALING

11.1 Call Control

11.1.1 SIP PROFILE

This section defines a SIP [RFC 3261] profile for usage in CCFE systems. This section is structured to mirror the SIP document and its section numbering. The subsections of this section are numbered such that the fourth digit tracks the SIP section numbers of the SIP specification [RFC 3261], and section titles at all header levels track the section titles of the SIP specification [RFC 3261]. In the following subsections where there are no requirements specified by this standard, the section will be left blank.

This section (11.1) and section 12.2 define the nearly complete set of enhancements and restrictions to a standard SIP implementation based on [RFC 3261]. However, not all details of the required behavior can be captured in these sections. Later sections provide details needed for certification and interoperability testing, which are generally not present in [RFC 3261].

Unless otherwise stated in this document, the CCFE shall follow the requirements given for SIP user agents in [RFC 3261] and a proxy shall follow the requirements given for SIP proxies and redirect servers in [RFC 3261].

11.1.1.1 Introduction

This section is intentionally left blank.

11.1.1.2 Overview of SIP Functionality

Section 2 of SIP [RFC 3261] is informational. .

11.1.1.3 Terminology

Section 3 of SIP [RFC 3261] is informational.

11.1.1.4 Overview of Operation

Section 4 of SIP [RFC 3261] is tutorial and therefore informational. .

11.1.1.5 Structure of the Protocol

The structure of the protocol can be found in SIP [RFC 3261], section 5. This section is informational.

11.1.1.6 Definitions

The definitions can be found in SIP [RFC 3261], section 6.

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

11.1.1.7 SIP Messages

The CCFE shall be in accordance with SIP [RFC 3261], section 7, except as noted below.

11.1.1.7.1 Requests

The CCFE shall be in accordance with SIP [RFC 3261], section 7.1, except as defined in this section.

The INVITE, ACK, CANCEL, BYE, and OPTIONS methods shall be supported. The REGISTER method *shall* be supported, depending on the policy of the peering carriers.

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 *shall* be supported.

The Request-URI in an initial INVITE for a basic telephone call[5] shall identify the called party using a tel URI or by using the telephone-subscriber syntax (i.e., the dialed phone number) in a SIP URI. When the Request-URI is a SIP URI, the host part shall identify the CCFE or 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 IPv4address or FQDN syntax, 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.

11.1.1.7.2 Responses

The CCFE shall be in accordance with SIP [RFC 3261], section 7.2.

11.1.1.7.3 Header Fields

The CCFE shall be in accordance with SIP [RFC 3261], section 7.3, and its subsections.

Furthermore, the CCFE shall be able to both generate and accept short and long form header field names as defined in [RFC 3261], section 7.3.3.

11.1.1.7.4 Bodies

The CCFE shall be in accordance with SIP [RFC 3261], section 7.4, and its subsections except as defined in this section.

11.1.1.7.4.1 Message Body Types

The CCFE shall support the message body type “application/sdp”.

The message body type "application/sdp" shall be supported with the INVITE, UPDATE, and PRACK methods as well as any non-failure response to these methods.

11.1.1.7.4.2 Message Body Length

The CCFE shall be in accordance with SIP [RFC 3261], section 7.4.2.

11.1.1.7.5 Framing SIP Messages

The CCFE shall be in accordance with SIP [RFC 3261], section 7.5.

11.1.1.8 General User Agent Behavior

Behavior of the CCFE User Agents (UA) shall be in accordance with chapter 8 of this document and with [RFC 3261], except as noted in this section.

Note that the behavior defined in this section applies only to requests and responses outside of a dialog. Behavior within a dialog is defined in [RFC 3261].

---

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

11.1.1.8.1 UAC Behavior

Support for the REGISTER method and SIPS URIs is optional, however if supported, it shall be as specified in [RFC 3261], section 8.1.

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

11.1.1.8.2 Generating the Request

The CCFE applications shall be in accordance with SIP [RFC 3261], section 8.1.1, except as noted below.

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[6]. The From and To fields in the request might contain random strings that protect the privacy of the session originator.

Refer to SIP [RFC3261] for further details of various header field values to be used.

The IETF allows option tags to be defined for their purpose only in standard-track RFCs. In addition to the standards-track RFCs' option tags, option tags from non-IETF documents should also be used, as long as they are defined in this document.

11.1.1.8.3 Sending the Request

The CCFE applications shall be in accordance with SIP [RFC 3261], section 8.1.2, and its subsections.

11.1.1.8.4 Processing Responses

The CCFE applications shall be in accordance with SIP [RFC 3261], section 8.1.3, except as noted in this section.

When receiving a 401 (Unauthorized) or 407 (Proxy Authentication Required) response, it is optional to follow the SIP authorization procedures.

When receiving a 420 (Bad Extension) response, it is optional to follow the SIP retry procedures.

11.1.1.8.5 UAS Behavior

The CCFE applications shall be in accordance with SIP [RFC 3261], section 8.2, and its subsections.

11.1.1.8.6 Redirect Servers

The ingress border CCFE 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 signaling traffic across the NNI and processing complexity associated with redirections. The Max-Forwards header field (see section 11.1.1.20.22), 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, than the CCFE applications shall be in accordance with SIP [RFC 3261], section 8.3.

3XX response codes are required to be supported at the IP NNI in order to support redirections that may take place in the interconnecting network (ingress network) or in a downstream network receiving the INVITE message.

---

[6] This can, for example, be used when forwarding to an Interactive Voice Response (IVR) system.

11.1.1.9 Canceling a Request

The CCFE applications shall be in accordance with SIP [RFC 3261], section 9, and its subsections.

11.1.1.10 Registrations

Proxies shall, and UACs *shall*, support the SIP REGISTER method in accordance with [RFC 3261], section 10. Support for registrars is optional; however if supported, it shall be as specified in [RFC 3261], section 10.

11.1.1.11 Querying for Capabilities

The CCFE applications shall be in accordance with SIP [RFC 3261], section 11, and its subsections.

11.1.1.12 Dialogs

The CCFE applications shall be in accordance with SIP [RFC 3261], section 12, and its subsections, except as noted below.

11.1.1.12.1 Creation of a Dialog

Support for SIPS URIs is optional; however if supported, it shall be as specified in [RFC 3261], section 12.1, and its subsections.

11.1.1.12.2 Requests within a Dialog

Support for SIPS URIs is optional, however if supported, it shall be as specified in [RFC 3261], section 12.2, and its subsections.

11.1.1.12.3 Termination of a Dialog

The CCFE applications shall be in accordance with SIP [RFC 3261], section 12.3.

11.1.1.13 Initiating a Session

The CCFE applications shall be in accordance with SIP [RFC 3261], section 13, and its subsections, except as noted in this section.

The UAC shall include a message body of type “application/sdp” with the initial INVITE.

To support codec selection, an SDP session description shall be included in:

- The initial INVITE request (offer); and
- The first reliable non-failure response to the INVITE (e.g., 183-Session-Progress sent reliably).

11.1.1.14 Modifying an Existing Session

The CCFE applications shall be in accordance with SIP [RFC 3261], section 14, and its subsections, except as noted in this section.

If a re-INVITE is sent, it shall include a message body of type "application/sdp" with a new offer. Furthermore, the CCFE applications shall support the procedures for modifying an existing session described in section 8.4.4.

11.1.1.15 Terminating a Session

The CCFE applications shall be in accordance with SIP [RFC 3261], section 15, and its subsections.

11.1.1.16 Proxy Behavior

The CCFE applications shall be in accordance with SIP [RFC 3261], section 16, and its subsections, except as noted in this section.

Support for multiple simultaneous media streams for a single call is optional. Since parallel forking may result in multiple simultaneous media streams for a single call, it is desirable that the CCFE implementations not use parallel forking.

11.1.1.17 Transactions

The CCFE applications shall be in accordance with SIP [RFC 3261], section 17, and its subsections except as noted in this section.

Behavior of the CCFE servers (proxies) shall be in accordance with section 8 of this document, which takes precedence over [RFC 3261], section 17, in case of any conflicts.

The CCFE User Agent Servers *shall* 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.

11.1.1.18 Transport

The CCFE applications shall be in accordance with SIP [RFC 3261], section 18, and its subsections.

11.1.1.19 Common Message Components

11.1.1.19.1 SIP and SIPS URI Component

The definition of a SIP/SIPS-URI is as given in [RFC 3261], section 19.1.1.

11.1.1.20 Header Fields

The CCFE applications shall be in accordance with SIP [RFC 3261], section 20, and its subsections, except as defined in this section.

Other SIP headers should be supported by the CCFE applications. The CCFE applications *should* transfer unsupported optional headers unchanged, if possible.

Listed below is each SIP header defined in [RFC 3261], and the requirements for supporting each in the CCFE are identified.

11.1.1.20.1 Accept

The Accept header shall be supported as specified in [RFC 3261], section 20.1.

11.1.1.20.2 Accept-Encoding

The Accept-Encoding header shall be supported as specified in [RFC 3261], section 20.2, except as noted below.

The Accept-Encoding header should be used by the CCFE implementations. The "identity" encoding value shall be supported; other encodings should be supported.

11.1.1.20.3 Accept-Language

The Accept-Language header shall be supported as specified in [RFC 3261], section 20.3, except as noted below.

The "Accept-Language" header *should* be present in requests with a value of "en" for English, which shall be supported. Other values should be supported.

11.1.1.20.4 Alert-Info

Support for the Alert-Info header is optional; however, if supported, it shall be as specified in [RFC 3261], section 20.4.

It is noted that there are security risks associated with acting on the Alert-Info header as described in [RFC 3261], section 20.4.

11.1.1.20.5 Allow

The Allow header field shall be supported as specified in [RFC 3261], section 20.5. The "Allow" header shall be present in the initial INVITE and the 200-OK response to the initial INVITE.

11.1.1.20.6 Authentication-Info

Support for the Authentication-Info is optional; however, if supported, it shall be as specified in [RFC 3261], section 20.6.

See also [RFC 3261], section 6.22.

11.1.1.20.7 Authorization

Support for the Authorization header field is optional; however, if supported, it shall be as specified in [RFC 3261], section 20.7.

See also [RFC 3261], section 6.22.

11.1.1.20.8 Call-ID

The Call-ID header shall be supported as specified in [RFC 3261], section 20.8.

11.1.1.20.9 Call-Info

Support for the Call-Info header is optional; however, if supported, it shall be as specified in [RFC 3261], section 20.9.

It is noted that there are security risks associated with acting on the Call-Info header as described in [RFC 3261], section 20.9.

11.1.1.20.10 Contact

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

The CCFE applications shall populate the Contact header field in an INVITE request, and in a 2XX response to an INVITE request, with a SIP-URI. Support for any other type of URI is optional.

The CCFE applications shall populate the Contact header field 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 section 7.1. Support for any other type of URI is optional.

11.1.1.20.11 Content-Disposition

The Content-Disposition header shall be supported as specified in [RFC 3261], section 20.11, except as noted below.

The Content-Disposition header *shall* be used by the CCFE implementations. The value "session" shall be supported; other values *shall* be supported.

Note that the default value for message bodies of 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.

11.1.1.20.12 Content-Encoding

The Content-Encoding header shall be supported as specified in [RFC 3261], section 20.12, except as noted below.

The Content-Encoding header *shall* be used by the CCFE implementations. The "identity" encoding value shall be supported; other encodings *shall* be supported.

11.1.1.20.13 Content-Language

Support for the Content-Language header is optional, however if supported, it shall be as specified in [RFC 3261], section 20.13.

11.1.1.20.14 Content-Length

This header shall be supported as specified in [RFC 3261], section 20.14.

11.1.1.20.15 Content-Type

The "Content-Type" header shall be supported as specified in [RFC 3261], section 20.15.

11.1.1.20.16 CSeq

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

11.1.1.20.17 Date

Support for the Date header is optional; however, if supported, it shall be as specified in [RFC 3261], section 20.17.

11.1.1.20.18 Error-Info

Support for the Error-Info header is optional; however, if supported, it shall be as specified in [RFC 3261], section 20.18.

It is noted that there are security risks associated with acting on the Error-Info header as described in [RFC 3261], section 20.18.

11.1.1.20.19 Expires

Support for the Expires header in the methods and responses defined in [RFC 3261] is optional[7]; however, if supported, it shall be as specified in [RFC 3261], section 20.19.

11.1.1.20.20 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 CCFE restricts the allowed contents of the SIP "From" header.

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

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

11.1.1.20.21 In-Reply-To

Support for the In-Reply-To header is optional; however, if supported, it shall be as specified in [RFC 3261], section 20.21.

Note that use of this header is subject to security considerations as described in [RFC 3261], section 20.21.

11.1.1.20.22 Max-Forwards

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

When the CCFE implementation of a back-to-back User Agent (B2BUA) forwards a request, it shall use a Max-Forwards value equal to the incoming Max-Forwards value minus one.

11.1.1.20.23 Min-Expires

Support for the Min-Expires header is optional (since support for the REGISTER method is optional); however, if supported, it shall be as specified in [RFC 3261], section 20.23.

11.1.1.20.24 MIME-Version

The MIME-Version header shall be supported as specified in [RFC 3261], section 20.24, except as noted below.

The MIME-Version header *shall* be used by the CCFE implementations. The version "1.0" value shall be supported; other values *shall* be supported.

11.1.1.20.25 Organization

Support for the Organization header is optional; however, if supported, it shall be as specified in [RFC 3261], section 20.25.

---

[7] Note that the Expires header is required for the SUBSCRIBE method.

11.1.1.20.26 Priority

Support for the Priority header is optional; however if supported, it shall be as specified in [RFC 3261], section 20.26.

There are security ramifications for entities that act on this header.

11.1.1.20.27 Proxy-Authenticate

Support for the Proxy-Authenticate header is optional; however, if supported, it shall be as specified in [RFC 3261], section 20.27.

See also [RFC 3261], section 6.22.

11.1.1.20.28 Proxy-Authorization

Support for the Proxy-Authorization header is optional; however, if supported, it shall be as specified in [RFC 3261], section 20.28.

See also [RFC 3261], section 6.22.

11.1.1.20.29 Proxy-Require

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

In addition to the standards-track RFCs' option tags, option tags from non-IETF documents *shall* also be used, as long as they are defined in this document.

11.1.1.20.30 Record-Route

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

11.1.1.20.31 Reply-To

Support for the Reply-To header is optional; however, if supported, it shall be as specified in [RFC 3261], section 20.31.

11.1.1.20.32 Require

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

In addition to the standards-track RFCs' option tags, option tags from non-IETF documents *shall* also be used, as long as they are defined in this document.

11.1.1.20.33 Retry-After

Support for the Retry-After header is optional; however, if supported, it shall be as specified in [RFC 3261], section 20.33.

11.1.1.20.34 Route

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

11.1.1.20.35 Server

Support for the Server header is optional; however, if supported, it shall be as specified [RFC 3261], section 20.35.

11.1.1.20.36 Subject

Support for the Subject header is optional, however if supported, it shall be as specified [RFC 3261], section 20.36.

11.1.1.20.37 Supported

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

In addition to the standards-track RFCs' option tags, option tags from non-IETF documents *shall* also be used, as long as they are defined in this document.

11.1.1.20.38 Timestamp

The Timestamp header shall be supported as specified in [RFC 3261], section 20.38, except as noted below.

The CCFE *shall* send the Timestamp header in requests; if received, this header shall be processed as described in [RFC 3261], section 20.38.

11.1.1.20.39 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 CCFE restricts the allowable contents of the SIP "To" header. Typically, the "To" header indicates the dialed digits in a tel-URI (see section 7.1). This information is of end-to-end significance, and might reveal information about the caller's location -- e.g., local, long-distance, PBX, or international.

When the call originator requests Privacy, the CCFE applications shall 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 dialed a telephone number, then the To: header should contain a tel-URI with the dialed digits.

11.1.1.20.40 Unsupported

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

11.1.1.20.41 User-Agent

Support for the User-Agent header is optional; however, if supported, it shall be as specified [RFC 3261], section 20.41.

11.1.1.20.42 Via

The Via header shall be supported as specified in [RFC 3261], section 20.42, except as noted below.

11.1.1.20.43 Warning

Support for the Warning header is optional; however, if supported, it shall be as specified in [RFC 3261], section 20.43.

11.1.1.20.44 WWW-Authenticate

Support for the WWW-Authenticate header is optional; however, if supported, it shall be as specified in [RFC 3261], section 20.44.

See also [RFC 3261], section 6.22.

11.1.1.21 Response Codes

The CCFE applications shall be in accordance with SIP [RFC 3261], section 21, and its subsections.

11.1.1.22 Usage of HTTP Authentication

Support of HTTP Authentication is optional; however, if used, it shall be as specified in [RFC 3261], section 22.

11.1.1.23 S/MIME

Support of S/MIME is optional; however, if used, it shall be as specified in [RFC 3261], section 23.

11.1.1.24 Examples

The examples provided in [RFC 3261], section 24, do not apply to the CCFE implementations.

11.1.1.25 Augmented BNF for the SIP Protocol

The CCFE applications shall comply with SIP [RFC 3261], section 25.

11.1.2 Header Support

In the below table, all section references are to IETF RFC 3261.

Table 2 - IETF RFC 3261 Header Fields

Header	Send	Recv	Reference and Notes
Accept	M	M	See Section 20.1
Accept-Encoding	O	M	See Section 20.2
Accept-Language	S	M	See Section 20.3
Alert-Info	O	O	See Section 20.4
Allow	M	M	See Section 20.5 The header value shall list all supported methods -- *i.e.*, at a minimum, "INVITE", "ACK", "CANCEL", "BYE", "OPTIONS", "PRACK", "UPDATE", "REFER", and "NOTIFY".
Authentication-Info	O	O	See Section 20.6
Authorization	O	O	See Section 20.7
Call-ID	M	M	See Section 20.8
Call-Info	O	O	See Section 20.9
Contact	M	M	See Section 20.10
Content-Disposition	O	M	See Section 20.11
Content-Encoding	O	M	See Section 20.12
Content-Language	O	O	See Section 20.13
Content-Length	M	M	See Section 20.14
Content-Type	M	M	See Section 20.15 The values "application/sdp", "message/sipfrag", and "application/simple-message-summary" shall be supported.
CSeq	M	M	See Section 20.16
Date	O	O	See Section 20.17
Error-Info	O	O	See Section 20.18
Expires	M	M	See Section 20.19 and Section 7.5
From	M	M	See Section 20.20
In-Reply-To	O	O	See Section 20.21
Max-Forwards	M	M	See Section 20.22
Min-Expires	O	O	See Section 20.23
MIME-Version	O	M	See Section 20.24
Organization	O	O	See Section 20.25
Priority	O	O	See Section 20.26
Proxy-Authenticate	O	O	See Section 20.27
Proxy-Authorization	O	O	See Section 20.28
Proxy-Require	M	M	See Section 20.29 The option tag "Privacy" shall be supported in accordance with Section 7.9
Record-Route	M	M	See Section 20.30
Reply-To	O	O	See Section 20.31

Header	Send	Recv	Reference and Notes
Require	M	M	See Section 20.32. The option tags “precondition”, “replaces”, and “100rel” shall be supported. Furthermore, the option tag "P-DCS" *shall* be sent and shall be supported if received as described in Section 7.7.3.
Retry-After	O	O	See Section 20.33
Route	M	M	See Section 20.34
Server	O	O	See Section 20.35
Subject	O	O	See Section 20.36
Supported	M	M	See Section 20.37 The values “precondition”, “replaces”, “100rel”, and "P-DCS" shall be supported. However, a value present in the "Require" header *should* NOT also be present in the Supported header.
Timestamp	O	M	See Section 20.38
To	M	M	See Section 20.39
Unsupported	M	M	See Section 20.40
User-Agent	O	O	See Section 20.41
Via	M	M	See Section 20.42
Warning	O	O	See Section 20.43
WWW-Authenticate	O	O	See Section 20.44

In the above table, M, O, and S have the following meanings:

Code	Code name	Sending side	Receiving side
M	Mandatory	The capability shall be supported. It is a static view of the fact that the conformance requirements related to the capability in the reference specification are mandatory requirements. This does not mean that a given behaviour shall always be observed, but that it shall be observed when the implementation is placed in conditions where the conformance requirements from this document compel it to do so. For instance, if the support for a header in a sent request or response is mandatory, it does not mean that it shall always be present, but that it shall be present according to the description of the behaviour in this document.	Same as in the sending side with the following additions: Processing should 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.

Code	Code name	Sending side	Receiving side
O	Optional	The capability may or may not be supported. It is an implementation choice.	Same as in the sending side with the following additions: If possible, perform the processing expected by the sending side. When the processing expected by the sending side cannot be performed, the received content should be ignored and processing should continue.
S	Recommended	The capability should be supported. It is an implementation choice.	Same as in the sending side with the following additions: If possible, perform the processing expected by the sending side. When the processing expected by the sending side cannot be performed, the received content should be ignored and processing should continue.

11.1.3 Mandatory SIP Extensions Supported[3]

1. IETF RFC 2046, N. Freed, N. Borenstein, *Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types*, November 1996.
2. IETF RFC 2976, S. Donovan, *The SIP INFO Method*, October 2000.
3. IETF RFC 3204, E. Zimmerer, J. Peterson, A. Vemuri, L. Ong, F. Audet, M. Watson, and M. Zonoun, *MIME media types for ISUP and QSIG Objects*, December 2001.
4. IETF RFC 3264, *An Offer/Answer Model with the Session Description Protocol (SDP)*, June 2002.
5. IETF RFC 3323, J. Peterson, *A Privacy Mechanism for the Session Initiation Protocol (SIP)*, November 2002.
6. IETF RFC 3324, M. Watson, *Short Term Requirements for Network Asserted Identity*, November 2002.
7. IETF RFC 3325, C. Jennings, J. Peterson, and M. Watson; *Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks*; November 2002.
8. IETF RFC 3326, H. Schulzrinne, D. Oran, G. Camarillo, *The Reason Header Field for the Session Initiation Protocol (SIP)*, December 2002.
9. IETF RFC 3420, R. Sparks, *Internet Media Type message/sipfrag*, November 2002.
10. IETF RFC 3428, B. Campbell, J. Rosenberg, H. Schulzrinne, C. Huitema, and D. Gurle, *Session Initiation Protocol (SIP) Extension for Instant Messaging*, December 2002.
11. IETF RFC 3515, R. Sparks, *The Session Initiation Protocol (SIP) Refer Method*, April 2003.
12. IETF RFC 3824, J. Peterson, H. Liu, J. Yu, B. Campbell, *Using E.164 numbers with the Session Initiation Protocol (SIP)*, June, 2004.
13. IETF RFC 3966, H. Schulzrinne, *The tel URI for Telephone Calls*, December 2004.
14. draft-ietf-iptel-trunk-group-03.txt, V. Gurbani and C. Jennings, *Representing Trunk Goups in tel/sip URIs*, February 2005
15. IETF RFC 3959, G. Camarillo, *The Early Session Disposition Type for the SIP*, December 2005.
16. IETF RFC 3893, J. Peterson, *SIP Authenticated Identity Body (AIB) Format*, September 2004.

17. draft-ietf-sip-content-indirect-mech-04.txt, E. Burger, *A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages*, October 2004.
18. IETF RFC 3911, R. Mahy, D. Petrie, *The Session Initiation Protocol (SIP) "Join" Header*, September 2004.
19. IETF RFC 3892, R. Sparks, *The SIP Referred-By Mechanism*, September 2004.
20. IETF RFC 3891, R. Mahy, B. Biggs, and R. Dean, *The Session Initiation Protocol (SIP) "Replaces" Header*, September 2004.
21. IETF RFC 4412, H. Schulzrinne and J. Polk, *Communications Resource Priority for the Session Initiation Protocol (SIP)*, February 2006.
22. IETF RFC 4028, S. Donnovan, *Session Timers in SIP*, February 2005.
23. draft-ietf-sipping-dialog-package-06.txt, *An INVITE Inititiated Dialog Event Package for the Session Initiation Protocol (SIP)*, April 12, 2005.
24. IETF RFC 3960, G. Camarillo, and H. Schulzrinne, *Early Media and Ringback Tone Generation in the Session Initiation Protocol*, December 2004.
25. draft-ietf-iptel-tel-np-09 .txt, J. Yu, *New Parameters for the "tel" URI to Support Number Portability*, February, 2005.
26. IETF RFC 3087, B. Campbell and R. Sparks, *Control of Service Context using SIP Request-URI*, April 2001.

11.1.4 Informational[3]

1. IETF RFC 2543, *SIP: Session Initiation Protocol, Internet Engineering Task Force*, March 1999.
2. IETF RFC 3265, A. Roach, *SIP-Specific Event Notification*, June 2002.
3. IETF RFC 3581, J. Rosenberg and H. Schulzrinne, *An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing*, August, 2003.
4. IETF RFC 3680, J. Rosenberg, *A Session Initiation Protocol (SIP) Event Package for Registrations*, March, 2004.
5. IETF RFC 3840, J. Rosenberg, H. Schulzrinne, and P. Kyzivat, *Indicating User Agent Capabilities in the Session Initiation Protocol(SIP)*, August, 2004.
6. IETF RFC 3841, J. Rosenberg, H. Schulzrinne, and P. Kyzivat, *Caller Preferences for the Session Initiation Protocol (SIP)*, August, 2004.
7. IETF RFC 3842, R. Mahy, *A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)*, August, 2004.
8. draft-ietf-simple-event-list-04.txt, A. B. Roach, J. Rosenberg, and B. Campbell, *A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists*, June 13, 2003.
9. draft-ietf-sipping-reason-header-for-preemption-01.txt, J. Polk, *Session Initiation Protocol (SIP) Reason Header and Preemption Events*, July 19, 2004.
10. IETF RFC 3319, H. Schulzrinne, and B. Volz, *DHCPv6 Options for SIP Servers*, July 2003.
11. IETF RFC 3361, H. Schulzrinne, *DHCP-for-IPv4 Option for Session Initiation Protocol (SIP) Servers*, June 2002.
12. IETF RFC 3489, *STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)*, March 2003.
13. IETF RFC 3351, *SIP Deaf Requirements*.

14. IETF RFC 3725, *Best Current Practices for Third Party Call Control (3PCC) in the Session Initiation Protocol (SIP)*, April, 2004.
15. IETF RFC 3761, P. Faltstrom and M. Mealling, *The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)*, April, 2004.
16. IETF RFC 3856, J. Rosenberg, *A Presence Event Package for the Session Initiation Protocol (SIP)*, August, 2004.
17. IETF RFC 3859, J. Peterson, *Common Profile for Presence (CPP)*, August, 2004.
18. IETF RFC 3863, H. Sugano, *Presence Information Data Format (PIDF)*, August, 2004.
19. IETF RFC 3372, A. Vemuri, and J. Peterson, *Session Initiation Protocol for Telephones (SIP-T): Context and Architectures*, September 2002.

    NOTE - T1.679-2004 takes precedence over this RFC.
20. IETF RFC 3398, G. Camarillo, A. Roach, J. Peterson, and L. Ong, *Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping*, December 2002.

11.1.5 Call Forwarding Information

Diversion may be used to relay call forwarding/referral/redirect information.

11.2 Mandatory Media-Related Protocols to Be Supported

1. IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*.[3]
2. IETF RFC 3551 (2003), *RTP Profile for Audio and Video Conferences with Minimal Control*.[3]
3. IETF RFC 2833 (2000), *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*.[3]
4. 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*.[3]
5. IETF RFC 3389 (2002), *RTP Payload for Comfort Noise*.[3]
6. IETF RFC 3611, *RTCP-XR*.[3]
7. IETF RFC 3362 (2002), *Real-time Facsimile (T.38) – image/t38 MIME Sub-type Registration*.[3]
8. IETF RFC 2327 (1998), *SDP: Session Description Protocol*.[3]
9. ITU-T Recommendation T.38 (02/00), *Procedures for real-time Group 3 facsimile communication over IP networks*.[2]

Negotiation and renegotiation of the set of available codecs during a call shall be performed as specified by RFC 3264. Use of a specific codec among the available codecs during a call shall be as specified by RFC 3550.

Internet Facsimile Protocol (IFP), as in ITU-T T.38 (fax), shall use UDPTL (Facsimile UDP Transport Layer) over UDP for transport. Alternatively or additionally, based on bilateral agreement, IFP may use:

- The TPKT (Transport Protocol Data Unit Packet) header over TCP; or
- RTP (over UDP).

11.3 Call Control Signaling Transport

The preferred SIP transport method at the NNI is TCP. However, UDP or SCTP may be used.

NOTE - A service provider may have to support multiple types of SIP Signaling Transport depending on the peering relationships.

11.4 IP Protocol Version

The following apply to the IP protocol version used:

1. Support of IPv4 is mandatory.
2. Support of IPv6 is optional based on bi-lateral agreement.
3. When IPv4 and IPv6 networks interconnect, the IPv6 shall perform addressing mapping.

12 SECURITY

For an overview of security requirements, see ATIS-PP-1000007.2006, *Generic Signaling and Control Plane Security Requirements for Evolving Networks*.

Each network administrative domain shall establish and enforce policies for Service Level Agreements (SLAs) to assure the security of its domain and the security of the network interconnection. The SLAs should specify security services, mechanisms, and practices to be implemented to protect the interconnected networks and the communications (signaling/control traffic, bearer traffic and management traffic) across the NNI.

Annex A
(informative)

A CONSIDERATIONS FOR SERVICE LEVEL AGREEMENTS (SLAS)

A.1 Introduction

The main body of this ANS and its companion TRs provide the technical specifications for the IP Network Interconnect. In practice, Network Interconnect between any pair of networks will be governed by a mutually agreed upon business agreement, generally known as a Service Level Agreement (SLA).

This annex lists some considerations that may be useful to include in a SLA for IP NI. The topics here, however, should not in be taken as a recommendation on the entire content of a SLA.

A.2 Suggested Topics to Address in the SLA

The SLA should describe what subset of the IP NNI ANS is to be supported.

When there are effectively options within the IP NNI ANS, the SLA should describe which options are to be supported.

The SLA should describe any deviations from the IP NNI ANS that the network providers mutually agree to.

The SLA should state, for SIP sessions set up across the NNI, whether the corresponding media packets must traverse the NNI (as opposed to being allowed to take some other path not across the NNI).

The SLA should contain a description of traffic types and their characteristics (volumes, patterns, priority levels, etc.), and expected QoS.

The SLA should include a description of the expected level of NNI availability/reliability.

The SLA should address security requirements for the IP NNI for VoIP.