**Contribution**

**TITLE:** IP Interconnection Outline

**SOURCE\*:** Martin Dolly, AT&T, Lead Member Technical Staff

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**ABSTRACT**

This document provides a draft outline for the IP-NNI specification. Preliminary text has been added into a number of sections, with the source of the content identified. The text has **not** yet been accepted by the group as baseline text, but is merely provided as a starting point to facilitate further contributions.

**NOTICE**

This is a draft document and thus, is dynamic in nature. It does not reflect a consensus of the ATIS-SIP Forum IP-NNI Task Force and it may be changed or modified. Neither ATIS nor the SIP Forum makes any representation or warranty, express or implied, with respect to the sufficiency, accuracy or utility of the information or opinion contained or reflected in the material utilized. ATIS and the SIP Forum further expressly advise that any use of or reliance upon the material in question is at your risk and neither ATIS nor the SIP Forum shall be liable for any damage or injury, of whatever nature, incurred by any person arising out of any utilization of the material. It is possible that this material will at some future date be included in a copyrighted work by ATIS or the SIP Forum.

\* CONTACT: Martin Dolly; email: md3135@att.com; Tel: +1-609-903-3360

**ATIS-0x0000x.YYYY**

American National Standard for Telecommunications

**IP Interconnection**

**Alliance for Telecommunications Industry Solutions**

Approved Month DD, YYYY

**American National Standards Institute, Inc.**

**Abstract**

Abstract text here.

**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 Telecommunications Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The [**COMMITTEE NAME**] Committee [**INSERT MISSION**]. [**INSERT SCOPE**].

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, [**COMMITTEE NAME**], 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, [**COMMITTEE NAME**], which was responsible for its development, had the following leadership:

[**LEADERSHIP LIST**]

The **[SUBCOMMITTEE NAME]** Subcommittee was responsible for the development of this document.

**Table of Contents**

[INSERT]

**Table of Figures**

[INSERT]

**Table of Tables**

[INSERT]

# Scope, Purpose, & Application

## Scope

xxx

## Purpose

xxx

## Application

xxx

# Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

ATIS-0x0000x, *Technical Report*.

ATIS-0x0000x.201x, *American National Standard*.

# Definitions, Acronyms, & Abbreviations

For a list of common communications terms and definitions, please visit the *ATIS Telecom Glossary*, which is located at < <http://www.atis.org/glossary> >.

## Definitions

**AAA**: xxxx.

**Bbbb**: xxxx.

## Acronyms & Abbreviations [i3 Forum]

3GPP 3rd Generation Partnership Project

ALG Application Level Gateway

ATCF Access Transfer Control Function

B2BUA Back to Back user agent

BGCF Border Gateway Control Function

CSCF Call Session Control Function

IBCF Interconnection Border Control Function

I-BGF Interconnection Border Gateway Function

I-CSCF Interrogating-Call Session Control Function

ICSS IMS Centralized Services

II-NNI Inter-IMS Network to Network Interface

IM-CN IP Multimedia Core Networks

IMS IP Multimedia Subsystem

IMS-ALG Multimedia Subsystem Application Level Gateway

IP Internet Protocol

IPSec IP Security

IPv4 Internet Protocol Version 4

IPv6 Internet Protocol Version 6

MGCF Media Gateway Control Function

MGF Media Gateway Function

MIME Multipurpose Internet Mail Extensions

MSC Mobile Switching Center

NAT Network Address Translation

NAT-PT Network Address Translation—Protocol Translation

NNI Network to Network Interface

P-CSCF Proxy Call Session Control Function

RTP Real-Time Protocol

SBC Session Border Controller

S-CSCF Serving-Call Session Control Function

SCTP Stream Control Transmission Protocol

SDP Session Description Protocol

SGF Signalling Gateway Function

SIP Session Initiation Protocol

SIP URI SIP protocol Uniform Resource Identifier

SIP-I SIP with encapsulated ISUP

SIP-T SIP for Telephones

SLA Service Level Agreement

SRVCC Single Radio Voice Call Continuity

TCP Transmission Control Protocol

tel-URI Telephone Uniform Resource Identifier

TRF Transit and Roaming Function

TrGw Transition Gateway

TLS Transport Layer Security

UA User Agent

UDP User Datagram Protocol

URI Uniform Resource Identifier

VoIP Voice over IP

# Reference Model for Interconnection

## General

[ATIS-1000009.2006, IP NETWORK-TO-NETWORK INTERFACE (NNI) STANDARD FOR VOIP]

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 - VoIP Interconnection Reference Model

For the purpose of the present document clause 5.1 TS 29.165 v11.5.0 (2012-12) with the following additions applies as follows:

[i3 Forum]

*Figure 5.1.1 illustrates the architecture diagram given in 3GPP TS 23.228 [4] showing the Inter-IMS Network to Network Interface (II-NNI) between two IM CN subsystem networks*

**

*NOTE: The TRF can reside in a stand-alone entity or can be combined with another functional entity.*

***Figure 5.1.1: Inter-IMS Network to Network Interface between two IM CN subsystem networks***

Figure 5.1.2 illustrates the i3 Forum Interconnection & Roaming IMS Network to Network Interface, where there are IBCF/TrGw’s on either side of the interface. The internal carrier’s network environment is out of scope.



**Figure 5.1.2: i3 Forum Interconnection & Roaming IMS Network to Network Interface**

*The protocols over the two reference points Ici and Izi make up the Inter-IMS Network to Network Interface.*

*The Ici reference point allows IBCFs to communicate with each other in order to provide the communication and forwarding of SIP signalling messaging between IM CN subsystem networks. The Izi reference point allows TrGWs to forward media streams between IM CN subsystem networks.*

*IMS roaming performed by using II-NNI is considered, when the IBCFs are inserted at the network borders. The applicability of roaming scenario by using II-NNI is based on agreement between the operators.*

*Whenever the Inter-IMS Network to Network Interface is used to interconnect two IM CN subsystem networks belonging to different security domains, security procedures apply as described in 3GPP TS 33.210 [10].*

## Functionalities performed by entities at the edge of the network

### Interconnection Border Control Function (IBCF)

For the purpose of the present document clause 5.2.1 of [161] TS 29.165 v11.5.0 (2012-12) applies as follows:

*An IBCF provides application specific functions at the SIP/SDP protocol layer in order to perform interconnection between IM CN subsystem networks by using Ici reference point. According to 3GPP TS 23.228 [4], IBCF can act both as an entry point and as an exit point for a network.*

*The functionalities of IBCF are indicated in the 3GPP TS 23.228 [4] and specified in 3GPP TS 24.229 [5]. They include:*

*• network topology hiding;*

*• application level gateway (for instance enabling communication between IPv6 and IPv4 SIP applications, or between a SIP application in a private IP address space and a SIP application outside this address space);*

*• controlling transport plane functions;*

*• controlling media plane adaptations;*

*• screening of SIP signalling information;*

*• selecting the appropriate signalling interconnect;*

*• generation of charging data records;*

*• privacy protection; and*

*• inclusion of a transit IOI when acting as an entry point for a transit network.*

*Based on local configuration, the IBCF performs transit routing functions as specified in 3GPP TS 24.229 [5].*

*The IBCF acts as a B2BUA when it performs IMS-ALG functionality.*

### Transition Gateway (TrGW)

For the purpose of the present document clause 5.2.1 of [161] TS 29.165 v11.5.0 (2012-12) applies as follows:

*According to 3GPP TS 23.002 [3], the TrGW is located at the network borders within the media path and is controlled by an IBCF. Forwarding of media streams between IM CN subsystem networks is applied over Izi reference point.*

*The TrGW provides within the media path functions like network address/port translation and IPv4/IPv6 protocol translation. NAT-PT binds addresses in IPv6 network with addresses in IPv4 network and vice versa to provide transparent routing between the two IP domains without requiring any changes to end points. NA(P)T-PT provides additional translation of transport identifier (TCP and UDP port numbers). The approach is similar to that one described also in 3GPP TS 29.162 [8].*

*Further details are described in 3GPP TS 23.228 [4].*

*[PKT-SP-IGS-C01-130930, PacketCable Interconnect Guidelines Specification]*

Figure 1 shows the peering relationship between two SSP (SIP Service Provider) networks; Cable MSO-A and Cable MSO-B. The two peering MSO networks may be any combination of PacketCable 1.5 and PacketCable 2.0. The Signaling Path Border Element (SBE) serves as the egress/ingress point for SIP signaling into each peer network. The SBE may act as a proxy or a Back-to-Back User Agent (B2BUA). The optional Data Path Border Element (DBE) serves as a media relay at the peering interface for media interworking, topology hiding, and IPv4/6 interworking. When the DBE is not deployed, media are exchanged directly with the E-MTA (Embedded Media Terminal Adapter) or E-DVA (Embedded Digital Voice Adapter).



***Figure 1 - Peering Architecture***

As shown in Figure 1, this specification defines two reference points at the peering interface; pkt-igs-1 and pkt-igs-2. Pkt-igs-1 carries the SIP (Session Initiation Protocol) and SDP (Session Description Protocol) signaling between the peering networks, while pkt-igs-2 carries the media RTP (Real-Time Transport Protocol) and RTCP (RTP Control Protocol) packets between the peering networks.

Even though the pkt-igs-1 reference point terminates at the SBE of each peering SSP network, the responsibility for supporting this interface does not rest solely with the SBE. The reason for this is that the SBE can play the role of a firewall or a SIP Proxy that is largely transparent to the SIP signaling exchanged between the two networks. In reality, the responsibility for supporting the pkt-igs-1 belongs to the set of SIP entities in the SIP signaling chain, including the SBE plus the SIP proxies and UAs inside the SSP network. Therefore, normative statements in this document that define SIP and SDP requirements should be interpreted as applying to the set of SIP entities in the SIP signaling chain within the SSP network that can affect the peering interface pkt-igs-1. This document does not identify which specific entities within the SIP signaling chain are responsible for meeting the normative requirements.

As shown in Figure 1, pkt-igs-2 terminates at a Media Endpoint in the SSP network. However, the location of the Media Endpoint varies based on how the network is engineered. If a DBE is deployed and configured to perform media encode/decode, then pkt-igs-2 terminates at a Media Endpoint in the DBE. If the DBE is not deployed, or is configured to be transparent to RTP/RTCP (i.e., no encode/decode), then the pkt-igs-2 terminates at a Media Endpoint somewhere within the SP network; e.g., in the E-MTA or E-DVA (as shown in Figure 1) or in a Media Server.

## Trust Model

**Security trust model**

This clause defines the NGN security trust model.

The NGN functional reference architecture defines Functional Entities (FEs). However, since network security aspects depend heavily on the way that FEs are bundled together, the NGN security architecture is based on physical Network Elements (NEs), i.e., tangible boxes that contain one or more FEs. The way these FEs are bundled into NEs will vary, depending on the vendor.

**Single network trust model**

This sub-clause defines three security zones;

1. Trusted,
2. Trusted but vulnerable,
3. Un-trusted,

These security zones are dependent on operational control, location, and connectivity to other device/network elements. The three zones are illustrated in the security trust model shown in Figure 3.



**Figure 3 - Security trust model**

An “internally trusted network security zone” or “trusted zone” in short, is a zone where a NGN provider’s network elements and systems reside and never communicate directly with customer equipment or other domains. The common characteristics of NGN network elements in this zone are that they are under the full control of the NGN provider are located in the NGN provider domain, and they communicate only with elements in the “trusted” zone and with elements in the “trusted-but-vulnerable” zone. It should not be assumed that because it is in a trusted zone it is secure per se.

The “trusted zone” will be protected by a combination of various methods. Some examples are physical security of the NGN network elements, general hardening of the systems, , use of secure signaling, security for OAMP messages separate VPN within the (MPLS/)IP network for communication within the “trusted” zone and with NGN network elements in the “trusted-but-vulnerable” zone. See clause 8 for more details.

A “trusted but vulnerable network security zone”, or “trusted but vulnerable zone” in short, is a zone where the network elements/devices are operated (provisioned and maintained) by the NGN provider. The equipment may be under the control by either the customer/subscriber or the NGN provider. In addition, the equipment may be located within or outside the NGN provider’s premises. They communicate with elements both in the trusted zone and with elements in the un-trusted zone, which is why they are “vulnerable”. Their major security function is to protect the NEs in the trusted zone from the security attacks originated in the un-trusted zone.

Elements that are located on the NGN provider’s domain with connectivity to elements outside the trusted zone are referred to as Network Border Elements (NBEs). Examples of these are the:

* Network Border Elements (NBE), which provide the User-Network Interface service control or transport elements of the NGN provider in the trusted zone in order to provide the user/subscriber access to the NGN provider’s network for services and/or transport.
* Domain Border Element (DBE) that is the same kind of equipment with network border element except that it resides on the border between domains.
* Device configuration & bootstrap NBE (DCB-NBE) that interface with the NGN provider’s device configuration system in the trusted zone in order to configure the user’s/subscriber’s device and NGN provider’s equipment in the outside plant.
* Operations, Administration, Maintenance, and Provisioning NBE(OAMP-NBE) that interfaces with the NGN provider’s OAMP systems in the trusted zone in order to provide and maintain the user’s/subscriber’s device and NGN provider’s equipment in the outside plant.
* Application Server/Web Server NBE (AS/WS-NBE) that interfaces with the NGN provider’s AS/WS-NBE in the trusted zone to provide the user/subscriber access to web based services.

.

Examples of devices and systems that are operated by an NGN provider but are not located on the NGN provider’s premises, and that may or may not be under the control of the NGN provider (and, therefore, may or may not be part of the trusted zone), are:

* Outside plant equipment in the access network/technology;
* Base Station Router (BSR), a wireless network element that integrates the base station, radio network controller and router functionalities;[[1]](#footnote-1)
* Optical Units (ONUs) within a user/subscriber’s residence.

The “trusted-but-vulnerable” zone will be protected by a combination of methods. Some examples are physical security of the NGN network elements, general hardening of the systems, , use of secure signaling for all signaling messages sent to NGN network elements in the “trusted” zone, security for OAMP messages, and packet filters and firewalls as appropriate. See clause 8 for more details.

An “un-trusted zone” includes all network elements and systems of a customer network, peer network, or other NGN provider security zone outside of the related NGN provider domain. These are connected to the NGN provider’s border elements.. The elements in the “un-trusted zone” may not be under the control of the NGN providers and it is effectively impossible to enforce the provider’s security policy on the user. Still it is desirable to apply some security measures, and to that end, it is recommended that signaling, media, and OAM&P be secured and that the Terminal Equipment Border Element (TE-BE) located in the “un-trusted zone”, is hardened. However, due to the lack of physical security, these measures cannot be considered absolutely safe. See clause 8 for more details.

**Peering network trust model**

When an NGN is connected to another network, whether the other network is trusted depends on:

* Physical interconnection, where the interconnection can range from a direct connection in a secure building to via shared facilities;
* The peering model, whether the traffic is exchanged directly between the two NGN service providers, or via one or more untrusted NGN transport providers;
* Business relationships, where there may be penalty clauses in the SLA agreements, and/or a trust in the other NGN provider’s security policy. The relationship must specify contractual terms stating the obligations each party to the contract agrees to and should also specify any specific security mechanisms, information and procedures also agreed to by the parties.

In general, NGN providers should view other providers as un-trusted.

Figure 4 shows an example when a connected network is judged un-trusted.

****

**Figure 4 – Peering trust model**

# General Procedures

## Extension Negotiation

*[PKT-SP-IGS-C01-130930, PacketCable Interconnect Guidelines Specification]*

SIP entities involved in session peering SHOULD be configured in such a way that they do not require any SIP extensions to be supported by the peer SSP (SIP Service Provider) network. When sending an out-of-dialog request to a peer SSP network, SIP entities involved in session peering SHOULD include a Supported header field identifying all the extensions supported by the sending network.

SIP entities involved in session peering MAY support configuration controls to disable certain extensions based on bilateral agreement between peer SSP networks. For example, a SIP entity involved in session peering could be configured to remove '100rel' from the Supported header in order to disable the use of reliable provisionable response (PRACK).

Note: Policies that limit or block the use of SIP extensions should be applied with care, since their application tends to disable SIP's native extension negotiation mechanism, and therefore inhibit the deployment of new services.

When sending a dialog-initiating request to a peer SSP network, SIP entities involved in session peering MUST identify all supported SIP requests in the Allow header field

## Public User Identities

*[PKT-SP-IGS-C01-130930, PacketCable Interconnect Guidelines Specification]*

Users are identified at the peering interface by their Public User Identity. A SIP entity involved in session peering MUST encode Public User Identities as a SIP URI of the telephone-subscriber syntax form of a Tel URI as indicated by the "user=phone" parameter (see [RFC 3261] section 19.1.6), where the user part of the SIP URI contains a global Tel URI as defined in [RFC 3966].

Example:

sip:+13035551212@example.operator.com;user=phone

### Identifying the Called User

When sending a dialog-initiating request to a peer SSP network, SIP entities involved in session peering MUST:

identify the called user in the Request-URI of the request, and

identify the called user using the telephone-subscriber syntax form of the SIP URI as described above in Section 6.2.

In addition, if Local Number Portability (LNP) information for the called number was obtained, then SIP entities involved in session peering MUST:

include the LNP data in SIP URI in the Request-URI using the Tel URI "npdi" and "rn" parameters as defined in [RFC 4694], and

if the called number is ported, then identify the routing number using the global form of the "rn" parameter, which is indicated by a leading "+" character followed by the country-code followed by the national number (e.g., "rn=+16132220000").

On receiving a dialog-initiating request from a peer SSP network, SIP entities involved in session peering MUST:

identify the called user based on the contents in the Request-URI, where the Request-URI contains a SIP URI as described above in Section 6.2;

obtain the LNP data for the called number based on the presence and contents of the "npdi" and "rn" Tel URI parameters contained in the SIP URI in the Request-URI as defined in [RFC 4694].

Table 1 summarizes the allowed forms for the called Public User Identity at the peering interface.

Table  - Called Public User Identities

| Use Case | Direction | Valid Form | Example |
| --- | --- | --- | --- |
| No LNP query | send/receive | SIP URI containing global Tel URI | sip:+13036614567@example.mso-a.com;user=phone |
| LNP Query - number not ported | send/receive | Above plus "npdi" parameter | sip:+13036614567;npdi@example.mso-a.com;user=phone |
| LNP Query - number ported | send/receive | Above plus global "rn" parameter | sip:+13036614567;npdi,rn=+13036620000@example.mso-a.com;user=phone |

### Identifying the Calling User

When sending or receiving a dialog-initiating request, SIP entities involved in session peering MUST identify the calling user in the P-Asserted-Identity header field using the telephone-subscriber syntax form of the SIP URI as described above in Section 6.2. When sending or receiving a dialog-initiating request, SIP entities involved in session peering SHOULD identify the calling name display information in the display-name component of the P-Asserted-Identity header field as described in Section 7.2.

## IPv4/6 Interworking

*[PKT-SP-IGS-C01-130930, PacketCable Interconnect Guidelines Specification]*

It is the responsibility of the IPv6 SSP network to perform the IPv4/IPv6 interworking function when interworking with an IPv4 SSP network.

## Fault Isolation and Recovery

[PKT-SP-IGS-C01-130930, PacketCable Interconnect Guidelines Specification]

### Interface Failure Detection

An SSP network MAY periodically send an OPTIONS request containing a Max-Forwards header field set to a value of '0' to detect the availability of a peer’s ingress point. The ping rate is based on bi-lateral agreement (typically every 5 seconds). If the sending SSP network fails to receive a response to an OPTIONS request, then it will consider that non-responding ingress point into the peer SSP network to have failed, and will remove the ingress point from the available set of ingress points to the peer SSP network. When a failure is detected, the SSP network that detected the failure should attempt to route subsequent calls to the peer SSP network over an available alternate route, with the final alternate route being the PSTN. In the meantime, the SSP network that detected the failure will continue to send periodic OPTIONS pings to the failed ingress point, in order to detect when it has been restored and is available for service.

**Note:**  A possible enhancement to the OPTIONS ping is to declare a well-known SIP URI in the registry that could be used to test the health of each ingress point in a peer SSP network. For example, SIP INVITE (with no SDP) to SIP:999999999@mso-a.com would respond with a 200OK (again no SDP), followed by a BYE/200OK.

### Congestion Control

SIP does not currently provide an explicit congestion control mechanism. However, an SSP network MAY impose limits on the number of simultaneous calls, and the incoming rate at which it will accept calls, from a peer. On receiving a dialog-initiating request that exceeds such limits, the receiving SSP network MUST respond with a 503 (Service Unavailable) response. An SSP network receiving a dialog-initiating request MUST limit the use of the 503 responses to reporting congestion at the ingress point. A terminating SSP network MUST NOT send a 503 response to an originating SSP network to report congestion or other failures that are internal to the terminating SSP network. For example, a 503 response generated by a SIP signaling entity within a terminating SSP network should be consumed within the terminating network, and should not be propagated across the peering interface to the originating SSP network (i.e., avoid sending a 503 response to an originating peer if the same failure is likely to be encountered when the call is retried via an alternate route).

On receiving a 503 (Service Unavailable) response from a peer SSP network, the receiving SSP network MUST limit the scope of the response to the call on which it was received (i.e., a 503 response has no affect on the routing of subsequent calls to the peer). Also, the receiving SSP network MUST attempt to consume the 503 response from a peer as close to the egress signaling point as possible, and avoid propagating the response back toward the originating CMS or E-DVA. Specifically, on receiving a 503 response to a dialog-initiating request that was sent to a peer SSP network, the receiving SSP network MUST:

terminate the current transaction,

ignore the Retry-After header field if one is present, and

attempt to route the call via an alternate peering interface (i.e., do not attempt to route the call via the same peering interface since it may encounter and aggravate the same overload condition).

### Session Timer

SIP entities involved in session peering SHOULD support Session Timer as defined in [RFC 4028].

### RTP Loopback Test

Peer SSP networks SHOULD support the RTP Loopback Test procedures defined in [E-DVA]. SSP networks that support the RTP Loopback procedures will provide a SIP URI that identifies a media endpoint within the SSP network that performs the loopback functions. Ideally, this "loopback" media endpoint would be located near the ingress point of the peer SSP network.

## Media

SIP entities involved in session peering MUST support the G.711 PCMU audio codec at a packetization interval of 20 msec as defined in [RFC 3551].

SIP entities involved in session peering MAY support voice-band-data relay mechanisms such as the following:

T.38 fax relay as specified in [T.38]

V.152 as specified in [V.152]

DTMF-relay for digits 0-9 and \* and # as defined in [RFC 4733]

A SIP entity involved in session peering that supports one or more of these voice-band-data relay mechanisms MUST revert to G.711 pass-though when interworking with a peer SSP network that does not support the same voice-band-date relay mechanism.

### RTP

### Codecs

### *Codec/packetization period use and transcoding guidelines*

## IP Routing and IP Addressing

## IP Packet marking

# Call Features

## Basic Call Setup

*[PKT-SP-IGS-C01-130930, PacketCable Interconnect Guidelines Specification]*

*NOTE: Initial INVITES will not always include an SDP offer*

This section describes the procedures at the peering interface required to establish a 2-way session for a basic voice call. In this case it is assumed that no originating or terminating features are applied (no call blocking, forwarding, etc), and that the called line is available to accept the call. Also, this section describes the session establishment procedures when the call is initiated by the originating SIP User Agent itself, and not via a 3rd party in support of features like click-to-call. Two-way call establishment using 3rd Party Call Control (3PCC) procedures is covered in Section 7.1.5.

SIP entities involved in session peering MUST support the SDP offer/answer procedures specified in [RFC 3264]. The originating SSP network MUST include an SDP offer in the initial INVITE. The terminating SSP network MUST include an SDP answer in the final 200 (OK) response to INVITE. The terminating SSP network MAY also include an SDP body in a provisional 18x response to INVITE. The SDP contained in an 18x provisional response can be considered a "preview" of the actual SDP answer to be sent in the 200 (OK) to INVITE. The originating SSP network can act on this "preview" SDP to establish an early media session, as described in Section 7.1.3. The terminating SSP network MUST ensure that the "preview" SDP matches the actual SDP answer contained in the 200 (OK) response to INVITE.

**Note**: An SDP offer/answer exchange occurs within the context of a single dialog. Therefore, the requirement for matching SDPs in the provisional and final responses to INVITE applies only when the provisional and final response are in the same dialog. If the provisional and final response are on different dialogs (say, when the INVITE is forked), the requirement for matching SDPs does not apply.

SIP entities involved in session peering MUST always set the SDP mode attribute in the initial offer/answer to "a=sendrecv".

**Note**: Setting the mode to "a=sendrecv" on the initial SDP offer/answer exchange avoids an additional SDP offer/answer exchange to update the mode to send-receive after the call is answered. This should help mitigate the problem of voice-clipping on answer.

SIP entities involved in session peering that advertise support for different but overlapping sets of codecs in the SDP offer/answer exchange for a given call MUST negotiate a common codec for the call.

### SDP Requirements

SIP entities involved in session peering MUST support the SDP requirements defined in [RFC 4566]. A SIP entity involved in session peering MUST include only one media (m=) descriptor per desired media stream in an SDP offer to a peer SSP network.

If a SIP entity involved in session peering receives an SDP offer containing multiple media descriptors, it MUST act on the media descriptors and include all of them in the same order in the response, including non-zero ports and zero ports for the offered media according to its capabilities as specified in [RFC 3264], an Offer/Answer Model with SDP. A SIP entity involved in session peering MUST NOT reject an offered session because it offers more media than the SIP entity can handle.

## Ringback Tone vs. Early Media

During the call setup phase, while the originating SSP network is waiting for the terminating SSP network to answer the call, the originating line is either playing local ringback tone to the calling user, or is connected to a receive-only or bi-directional early-media session with the terminating SSP network. For example, early media can be supplied by the terminating endpoint (e.g., custom ringback tone) while waiting for answer.

SIP entities involved in session peering must use the following procedures to control whether the originating line applies local ringback tone or establishes an early media session while waiting for the call to be answered.

1. The terminating SSP network controls the application of local ringback tone at the originating line or the establishment of an early media session by sending the following provisional response to a call-initiating INVITE.

The terminating SSP Network MUST send a 180 (Alerting) response containing no SDP to the originating SP network, if the call scenario requires the application of local ringback tone at the originating line.

The terminating SSP Network MUST send a 183 (Progressing) response containing SDP that describes the terminating media endpoint to the originating SSP network, if the call scenario requires an early media session.

The provisional response sent for other call scenarios is not be specified, as long as the response is not one of those described above.

2. The originating SSP network performs the following action on receipt of a provisional response to a call-initiating INVITE.

The originating SSP network MUST apply local ringback tone if it receives a 180 (Alerting) response containing no SDP.

The originating SSP network MUST establish an early media session with the media endpoint described by the SDP when it receives a 18x response containing SDP.

The originating SSP Network MUST do nothing (e.g., continue to apply local ringback tone if it was already being applied when the response was received) if it receives a 18x response other than 180 (Alerting), and the response contains no SDP.

When establishing an early media session, the originating SSP network MAY immediately remove any local ringback tone currently being applied. Alternatively, the originating SSP network MAY wait for receipt of RTP that matches the received SDP, and apply other checks/policies to validate the received RTP, before removing any locally applied ringback tone.

## Early-Media with Multiple Terminating Endpoints

There are some call scenarios that require media sessions to be established (serially) between the originating line and one or more intermediate media endpoints before the call is connected to the final target called party. For example, the terminating SSP network can insert a media server in the call to interact with the calling user in some way (e.g., to collect a blocking-override PIN) before offering the call to the called user. Another case occurs when the called user fails to answer within an allotted time and the call is redirected to voice-mail, or forwarded to another user via Call Forwarding Don’t Answer (CFDA). These different cases can be combined in the same call.

For each terminating media endpoint that is associated with a call before the call is answered, the terminating SSP network must decide whether to establish an early media session, or apply ringback tone at the originating line. For example, consider the case where the called user has call blocking with PIN override, and CFDA. First, an early-media session is established with the call-blocking server to collect the PIN. Next, the originating line in instructed to play local ring-back tone while waiting for the called user to answer, and finally an early media session is established with the forward-to party to play custom ringback tone.

[RFC 3261] mandates that the SDP included in provisional 18x responses to INVITE within the context of a dialog must match the SDP-answer included in the final 200 (OK) response to INVITE. The following sections describe two different mechanisms for supporting multiple terminating media endpoints before answer, within the confines of this requirement.

## Forking the INVITE

For each terminating media endpoint that requires an early media session to be established with the originating line, the terminating SSP network MUST signal the attributes of the terminating media endpoint to the originating SSP network within the SDP of a 183 (Progressing) response. The terminating SSP network MUST ensure that 18x responses containing different SDP copies are not sent within the same dialog. The terminating SSP network does this by specifying a different tag parameter in the To header field for each provisional response that contains a unique SDP, as if the INVITE had been sequentially forked.

The originating SSP network MUST honor the most recently received 18x response to INVITE, based on the procedures defined in Section 7.1.3.

## Redirecting the INVITE

As an alternative to sequentially forking the INVITE, the terminating entity can redirect the originating entity to the next endpoint in the series by sending a 302 (Moved Temporarily) response containing a Contact header field that identifies the next endpoint. The resulting INVITE from the originating SSP network is sent as a dialog-initiating request, and can therefore establish a new early-media session with the next endpoint in the series. The use of this procedure is based on bilateral agreement between peering operators.

On receiving a 302 (Moved Temporarily) response to an INVITE request, and if this mechanism is enabled based on local policy, the originating SSP network MUST send a new dialog-initiating INVITE with a Request-URI set to the value returned in the Contact header field of the 302 (Moved Temporarily) response, as described in [RFC 3261].

## Establishing calls using 3PCC

Section 7.1.2 describes the procedures that are used to establish basic two-way call when the call is initiated directly by the originating user's endpoint. However, an SSP may support features such as click-to-call, where the call is initiated by a 3rd party such as an Application Server on behalf of the originating user. To support such features, SIP entities involved in session peering MUST support the 3PCC procedures described in [RFC 3725].

## Call Hold

A SIP entity involved in session peering that wishes to place a media stream "on hold" MUST offer an updated SDP to its peer SSP network with an attribute of "a=inactive" or "a=sendonly" in the media description block. A SIP entity involved in session peering that wishes to place a media stream "on hold" MUST NOT set the connection information of the SDP to a null IP address. For example, the SIP entity involved in session peering MUST NOT set the 'c=' connection line to c=IN IP4 0.0.0.0. A SIP entity involved in session peering that wants to place a media stream "on hold" SHOULD locally mute the media stream.

A SIP entity involved in session peering that receives an SDP offer with an attribute of "a=inactive" in the media block MUST place the media stream "on hold" and send an SDP answer containing a media attribute of "a=inactive". A SIP entity involved in session peering that receives an SDP offer with an attribute of "a=inactive" in the media block MUST NOT set the connection data of the answer SDP to c=0.0.0.0. A SIP entity involved in session peering operating in IPv4 that receives an SDP offer with no directionality attributes but connection data set to c=IN IP4 0.0.0.0 SHOULD place the media stream "on hold".

## Calling Number and Name Delivery

The originating SSP network MUST provide the calling number of the originating user in the P-Asserted-Identity header field of dialog-initiating requests. Subject to local policies/agreements, the originating SSP network SHOULD provide the calling name of the originating user in the P-Asserted-Identity header field of dialog-initiating requests. (The mechanism for obtaining the calling name is outside the scope of this document.) The calling number is contained in the telephone-subscriber syntax form of the SIP URI, containing an E.164 number [E.164] as described in Section 6.2. The calling name is contained in the display-name component of the P-Asserted-Identity header field.

If the originating user wants to remain anonymous, the originating SSP network MUST include a Privacy header field containing the value "id" as specified in [RFC 3323] and [RFC 3325]. In addition, the originating SSP network SHOULD obscure the identity of the originating user in other header fields as follows:

Set the identity information in the From header field to "Anonymous <sip:anonymous@anonymous.invalid>"

Set the display-name in the To header field to "Anonymous" (since the To display-name selected by the originating user could provide a hint to the originating user’s identity)

Obscure any information from the Call-ID and Contact header fields, such as the originating FQDN, that could provide a hint to the originating user’s identity

The terminating SSP network MUST obtain the calling name and number for caller-ID display from the contents of the P-Asserted-Identity header field contained in dialog-initiating requests. If the INVITE request contains a Privacy header with the value "id", the terminating SSP network MUST provide a display of "Private" to the terminating user.

## Call Forwarding

If an SSP offers call-forwarding services to its users, then the forwarding SSP network MAY remain in the signaling path of the forwarded call in order to support separate billing for forward-from and forward-to legs. An SSP network that is required to remain in the signaling path of a forwarded call based on local policy MUST do so using one of the following procedures:

1. forward the INVITE to the forward-to-user while remaining in the signaling path as a SIP Proxy or B2BUA, or

2. respond to the initial INVITE with a 302 (Moved Temporarily) response with a Contact header field containing a private URI that points back to the forwarding SSP network.

## Call Transfer

A user in a peered call can perform the various forms of call-transfer (e.g., consultative transfer, blind transfer). Call-transfer can be supported in one of two ways; either using the REFER request and Replaces header, or by manipulating the call legs using 3rd Party Call Control (3PCC) techniques. SIP entities involved in session peering that support call transfer MUST support the 3PCC option, and MAY support the REFER/Replaces option. If an SSP network supports both options, then the option that is used when interworking with a specific peer is based on locally configured data that indicates the capabilities of that peer.

### Call Transfer using REFER/Replaces

SIP entities involved in session peering that support call-transfer using the procedures described in the section MUST support the SIP REFER extension described in [RFC 3515], and the SIP Replaces extension described in [RFC 3891]. Furthermore, [RFC 3515] requires support of the SIP Event Notification extension described in [RFC 3265].

To describe the basic transfer call-flow, consider the case where user-A in SSP network-A is in an active call with user-B in peered SSP network-B, and user-A decides to transfer user-B to user-C. User-C could be located anywhere in the global network; for example in network-A, network-B, another peered SSP network, a non-peering IP network, or the PSTN. Here are the basic steps to complete the transfer using REFER/Replaces:

1. User-A puts user-B on hold (sends re-INVITE with SDP "a=inactive" as described in Section 7.1.6).

2. User-A initiates a basic 2-way call to user-C.

3. User-A sends an in-dialog REFER to user-B containing a Refer-To header field. The Refer-To header field instructs user-B to send an INVITE to user-C with an imbedded Replaces header field identifying the A-to-C dialog.

- If SSP network-A is not required to remain in the signaling path of the transferred call, then it identifies user-C directly in the Refer-To header field,

- If SSP network-A is required to remain in the signaling path of the transferred call (say to generate events for proper billing of the call), then it identifies a private URL pointing to itself in the Refer-To header field, as described in [RFC 3603].

4. User-B sends an INVITE containing the Replaces header field specified in step 3 to the address contained in the Refer-To header field (i.e., the INVITE is routed to user-C either directly from SSP network-B, or indirectly via SSP network-A using the private URL).

5. User-B sends NOTIFY requests within the original A-to-B dialog, informing user-A of the progress of the B-to-C call.

6. At some point user-A drops out of both dialogs (e.g., drops out of A-to-C dialog on receiving BYE from user-C). At this point users B and C are active in a 2-way call.

SIP entities involved in session peering SHOULD support receiving a Globally Routable User Agent URI (GRUU) as defined in [RFC 5627] in the Refer-To header.

### Call Transfer Using 3PCC

SIP entities involved in session peering that support call-transfer using 3PCC techniques MUST act as a B2BUA, and manipulate the call legs using INVITE and re-INVITE requests. It is recommended that such techniques follow the guidance presented in [RFC 3725].

## Conferencing

The media mixing for 3-way conference calls may be performed by the E-MTA or E-DVA endpoint of the conference control party, or by a conference bridge server in the peer SSP network serving the conference control party. When mixing is done by the E-MTA or E-DVA endpoint, there are no specific requirements placed on the peering interface other than the support of media hold as described in Section 7.1.6. When conference mixing is performed by a network-based server, users are added to the conference using procedures similar to those described for call transfer in Section 7.4.

## Auto Recall/Callback

When a user invokes Auto-Callback, (AC) or Auto-Recall, (AR) and the user targeted by the recall/callback feature belongs to a peer SSP network, the originating SSP network first attempts to establish a basic 2-way call with the target user. If the call completes normally (e.g., the target user answers) then the feature is complete. If the terminating SSP network responds with an indication that the target user is busy, then the originating SSP network subscribes to the dialog-event package as defined in [RFC 4235] of the target user, as a mechanism to detect when the target user becomes available. When the terminating SSP network subsequently notifies the originating SSP network that the target user is available, the originating SSP network re-attempts to establish a 2-way call to the target user.

### Originating SSP Network Sends INVITE to Target

When a user invokes an AR or AC call, the originating SSP network MUST follow the procedures given for a basic call as described in Section 7.1.2, and attempt to establish a 2-way call with the target user. In addition, the originating SSP network MUST add a Call-Info header field to the INVITE with a purpose of "answer\_if\_not\_busy".

If the originating SSP network receives a 200-OK response to INVITE, then the AC/AR feature is considered complete, and the remainder of the call is handled like a normal 2-way call. If the originating SSP network receives a 486-Busy-Here or 600-Busy-Everywhere response to the INVITE, then it MUST follow the AC/AR procedures as defined below. If the terminating SSP network receives an inbound INVITE with a Call-Info header field declaring purpose=answer\_if\_not\_busy, then the terminating SSP network MUST ignore any active Call-Forwarding-Busy-Line (CFBL) service for the target user, not forward the call if the target is busy, and instead handle the call as if CFBL was not active (e.g., offer the call using the call-waiting feature).

### Originating SSP Network Sends SUBSCRIBE to Target

On receiving a 486-Busy-Here or 600-Busy-Everywhere response to an AC/AR INVITE request, the originating SSP network MUST establish a subscription to the dialog event package of the target endpoint, by sending a SUBSCRIBE request containing an Event header field set to "dialog" to the terminating SSP network. The originating SSP network MUST populate the SUBSCRIBE Request-URI with the URI returned in the Contact header field of the INVITE response, if that URI is a Globally Routable User Agent URI (GRUU), as defined in [RFC 5627]. Otherwise, the originating SSP network MUST populate the Request-URI with the Public User Identity of the target callback/recall user.

### Target Sends NOTIFY to Originating SSP Network

On receiving the SUBSCRIBE to the dialog event package, the terminating SSP network MUST notify the originating SSP network of the dialog state of the target user endpoint as described in [RFC 4235]. Upon receiving a NOTIFY message of "target is idle", the originating SSP network MUST first cancel the dialog-event subscription by sending a SUBSCRIBE message with an Expires header field containing the value "0".

Once the subscription is cancelled, the originating SSP network MUST send a new INVITE request to establish a call with the target user. If the originating SSP network receives a 486-Busy-Here or 600-Busy-Everywhere response to the INVITE, then it MUST automatically re-subscribe to the dialog event package of the target user.

**Note**: A "busy" response could be returned in this case as a result of a race condition, where the target endpoint sends a NOTIFY of "target is idle", and then becomes busy in a new call before the subsequent INVITE is received).

## Other stuff ( the PC Martin)???

# NNI Signaling Profile

[i3 Forum]

## SIP Methods and Header Fields

Notations of the codes

For the purpose of the present document clause 6.1.1.4 TS 29.165 v11.5.0 (2012-12) applies as follows:

*In the table 6.3 the status codes "m", "o", "c" and "n/a" have the following meanings:*

*Table 6.3: Key to notation codes for SIP messages*

|  |  |  |  |
| --- | --- | --- | --- |
| *Notation code* | *Notation name* | *Sending side* | *Receiving side* |
| *m* | *mandatory* | *The message shall be supported at II-NNI.**Supporting sending a SIP message at the II-NNI means that this message shall be sent over the II-NNI if received from the serving network. It does not imply that network elements inside the serving network or user equipment connected to this network shall support this message.* | *Supporting receiving a SIP message at the II-NNI means that this message shall be forwarded to the serving network. It does not imply that network elements inside the served network or user equipment connected to this network are supporting this message.* |
| *o* | *optional* | *The message may or may not be supported at II-NNI. The support of the method is provided based on bilateral agreement between the operators.* | *Same as for sending side.* |
| *n/a* | *not applicable* | *It is impossible to use/support the message.* | *It is impossible to use/support the message. This message will be discarded by the IBCF.* |
| *c <integer>* | *conditional* | *The requirement on the message ("m", "o" or "n/a") depends on the support of other optional or conditional items. <integer> is the identifier of the conditional expression.* | *Same as for sending side.* |

### SIP Methods

For the purpose of the present document clause 6.1.1.2 TS 29.165 v11.5.0 (2012-12) with the following changes applies.

*3GPP TS 24.229 [5] defines the methods allowing an IBCF to interconnect to an IBCF placed in another IM CN subsystem.*

*The following SIP methods are supported on the II-NNI as defined in table 6.1.*

*The following table is based on table A.5 and table A.163 of 3GPP TS 24.229 [5] and endorsed for this document:*

*Editor's Note: Roaming is not included in the initial scope of this document.*

*Table 6.1: Supported SIP methods*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| *Item* | *Method* | *Ref.* | *II-NNI* | I3Forum II-NNI(non roaming) | **I3Forum II-NNI****(roaming)** |
| *Sending* | *Receiving* | Sending | Receiving | Sending | Receiving |
| *1* | *ACK request* | *IETF RFC 3261 [13]* | *m* | *m* | m | m | m | m |
| *2* | *BYE request* | *IETF RFC 3261 [13]* | *m* | *m* | m | m | m | m |
| *3* | *BYE response* | *IETF RFC 3261 [13]* | *m* | *m* | m | m | m | m |
| *3* | *BYE response* | *IETF RFC 3261 [13]* | *m* | *m* | m | m | m | m |
| *4* | *CANCEL request* | *IETF RFC 3261 [13]* | *m* | *m* | m | m | m | m |
| *5* | *CANCEL response* | *IETF RFC 3261 [13]* | *m* | *m* | m | m | m | m |
| *5A* | *INFO request* | *IETF RFC 6086 [39]* | *o* | *o* | o | o | o | o |
| *5B* | *INFO response* | *IETF RFC 6086 [39]* | *o* | *o* | o | o | o | o |
| *8* | *INVITE request* | *IETF RFC 3261 [13]* | *m* | *m* | m | m | m | m |
| *9* | *INVITE response* | *IETF RFC 3261 [13]* | *m* | *m* | m | m | m | m |
| *9A* | *MESSAGE request* | *IETF RFC 3428 [19]* | *o* | *o* | ~~O~~ | ~~O~~ | o | o |
| *9B* | *MESSAGE response* | *IETF RFC 3428 [19]* | *o* | *o* | ~~O~~  | ~~O~~  | o | o |
| *10* | *NOTIFY request* | *IETF RFC 3265 [20]* | *c1* | *c1* | ~~c1~~  | ~~c1~~  | ~~c1~~ m | ~~c1~~ m |
| *11* | *NOTIFY response* | *IETF RFC 3265 [20]* | *c1* | *c1* | ~~c1~~  | ~~c1~~  | ~~c1~~ m | ~~c1~~ m |
| *12* | *OPTIONS request* | *IETF RFC 3261 [13]* | *m* | *m* | ~~m~~ x1 | ~~m~~ x1 | ~~m~~ x1 | ~~m~~ x1 |
| *13* | *OPTIONS response* | *IETF RFC 3261 [13]* | *m* | *m* | ~~m~~ x1 | ~~m~~ x1 | ~~m~~ x1 | ~~m~~ x1 |
| *14* | *PRACK request* | *IETF RFC 3262 [18]* | *m* | *m* | m | m | m | m |
| *15* | *PRACK response* | *IETF RFC 3262 [18]* | *m* | *m* | m | m | m | m |
| *15A* | *PUBLISH request* | *IETF RFC 3903 [21]* | *c1* | *c1* | ~~c1~~  | ~~c1~~  | ~~c1~~  | ~~c1~~ |
| *15B* | *PUBLISH response* | *IETF RFC 3903 [21]* | *c1* | *c1* | ~~c1~~  | ~~c1~~  | ~~c1~~  | ~~c1~~  |
| *16* | *REFER request* | *IETF RFC 3515 [22]* | *o* | *o* | ~~o~~ | ~~o~~ | ~~o~~ x2 | ~~o~~ x2 |
| *17* | *REFER response* | *IETF RFC 3515 [22]* | *o* | *o* | ~~o~~ | ~~o~~ | ~~o~~ x2 | ~~o~~ x2 |
| *18* | *REGISTER request* | *IETF RFC 3261 [13]* | *c2* | *c2* | ~~c2~~  | ~~c2~~  | ~~c2~~ m | ~~c2~~ m |
| *19* | *REGISTER response* | *IETF RFC 3261 [13]* | *c2* | *c2* | ~~c2~~  | ~~c2~~  | ~~c2~~ m | ~~c2~~ m |
| *20* | *SUBSCRIBE request* | *IETF RFC 3265 [20]* | *c1* | *c1* | ~~c1~~  | ~~c1~~  | ~~c1~~ m | ~~c1~~ m |
| *21* | *SUBSCRIBE response* | *IETF RFC 3265 [20]* | *c1* | *c1* | ~~c1~~  | ~~c1~~  | ~~c1~~ m | ~~c1~~ m |
| *22* | *UPDATE request* | *IETF RFC 3311 [23]* | *m* | *m* | m | m | m | m |
| *23* | *UPDATE response* | *IETF RFC 3311 [23]* | *m* | *m* | m | m | m | m |
| * *c1: In case of roaming scenario, the support of the method is m, else o.*
* *c2: In case of roaming scenario, the support of the method is m, else n/a.*
* *NOTE: In the above table, m, o and c and n/a have the meanings indicated in table 6.3*
* x1: Support of OPTIONS in a SIP dialog is mandatory, where support of OPTIONS out of a SIP dialog is optional. Use of OPTIONS outside the dialogue may be used as a keepalive mechanism only based on bilateral agreement.
* x2: Needed to support CONF service as specified within TS 24.147 [106] Section 5.3.1.5.3
 |

Items stroke out in the table above are not in scope of this i3 Forum Release, and items underlined are modifications or additions

Services supporting the following SIP Methods via interconnection II-NNI are out of scope:

* MESSAGE;
* NOTIFY;
* PUBLISH;
* REFER;
* REGISTER; and
* SUBSCRIBE.

Services supporting the following SIP Methods via Roaming II-NNI are out of scope:

* PUBLISH

### SIP Header Fields

##### General

For the purpose of the present document clause 6.1.1.3.0 of TS 29.165 v11.5.0 (2012-12) applies as follows:

*The IBCF shall provide the capabilities to manage and modify SIP header fields according to subclause 5.10 and Annex A of 3GPP TS 24.229 [5] with modifications as described in the following subclauses.*

##### Trust and no trust relationship

For the purpose of the present document clause 6.1.1.3.1 of TS 29.165 v11.5.0 (2012-12) applies with the following changes of Table 6.2 as follows:

*The IBCF acting as exit point applies the procedures described in clause 5.10.2 of 3GPP TS 24.229 [5] before forwarding the SIP signalling to the IBCF acting as entry point. The IBCF acting as entry point applies the procedures described in clause 5.10.3 of 3GPP TS 24.229 [5].*

*Additionally, in case there is no trust relationship between the two IM CN subsystems connected by II-NNI, the IBCF acting as exit point applies the procedures described in clause 4.4 of 3GPP TS 24.229 [5], before forwarding the SIP signalling.*

*These procedures may be utilized on a per header field basis to realize overall trust as well as per service level screening of header fields. Trust relationships and trust domains may be defined by inter-operator agreements for individual services and/or individual SIP header fields.*

*The management of the SIP header fields (if present) over II-NNI in case of a presence or not of a trust relationship between the two interconnected IM CN subsystems is wrapped up in the following table.*

*Table 6.2: Management of SIP header fields over II-NNI in presence or not of a trust relationship*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Item* | *Header field* | *Reference* | *Trust relationship* | *Not trust relationship* |
| *1* | *P-Asserted-Identity*  | *IETF RFC 3325 [44]* | *As specified in 3GPP TS 24.229 [5], clause 4.4**(NOTE 5)* | *As specified in 3GPP TS 24.229 [5], clause 4.4**(NOTE 5)* |
| *2* | *P-Access-Network-Info* (NOTE 2) | *IETF RFC 3455 [24]* | *As specified in 3GPP TS 24.229 [5], clause 4.4* | *As specified in 3GPP TS 24.229 [5], clause 4.4* |
| ~~3~~ | ~~Resource-Priority~~  | ~~IETF RFC 4412 [78]~~ | ~~As specified in 3GPP TS 24.229 [5], clause 4.4~~ | ~~As specified in 3GPP TS 24.229 [5], clause 4.4~~ |
| *4* | *History-Info*(NOTE 2) | *IETF RFC 4244 [25]* | *As specified in 3GPP TS 24.229 [5], clause 4.4* | *As specified in clause 4.3.3 of RFC 4244 [25] and in 3GPP TS 24.229 [5], clause 4.4* |
| *5* | *P-Asserted-Service*(NOTE 2) | *IETF RFC 6050 [26]* | *As specified in 3GPP TS 24.229 [5], clause 4.4**(NOTE 3)* | *As specified in 3GPP TS 24.229 [5], clause 4.4* *(NOTE 3)* |
| *6* | *P-Charging-Vector*  | *IETF RFC 3455 [24]* | *As specified in 3GPP TS 24.229 [5], clause 5.10* | *As specified in 3GPP TS 24.229 [5], clause 5.10* |
| *7* | *P-Charging-Function-Addresses**(NOTE 4)* | *IETF RFC 3455 [24]* | *As specified in 3GPP TS 24.229 [5], clause 5.10* | *As specified in 3GPP TS 24.229 [5], clause 5.10* |
| *8* | *P-Profile-Key (NOTE 2)* | *IETF RFC 5002 [64]* | *As specified in 3GPP TS 24.229 [5], clause 4.4* | *As specified in 3GPP TS 24.229 [5], clause 4.4* |
| ~~9~~ | ~~P-Private-Network-Indication(NOTE 1)~~ | ~~draft-vanelburg-dispatch-private-network-ind [84]~~ | ~~As specified in 3GPP TS 24.229 [5], clause 4.4~~ | ~~As specified in 3GPP TS 24.229 [5], clause 4.4~~ |
| *10* | *P-Served-User**(NOTE 1, NOTE 2)* | *IETF RFC 5502 [85]* | *As specified in 3GPP TS 24.229 [5], clause 4.4* | *As specified in 3GPP TS 24.229 [5], clause 4.4* |
| *11* | *Reason (in a response)*  | *IETF RFC 6432 [49]* | *As specified in 3GPP TS 24.229 [5], clause 4.4* | *As specified in 3GPP TS 24.229 [5], clause 4.4* |
| *12* | *P-Early-Media* | *IETF RFC 5009 [74]* | *As specified in 3GPP TS 24.229 [5], clause 4.4* | *As specified in 3GPP TS 24.229 [5], clause 4.4* |
| * *NOTE 1: For a roaming II-NNI, a trust relationship with respect to this header field is required.*
* *NOTE 2: This header field is only applicable on a roaming II-NNI* whereas for the interconnect NNI it is left unspecified.
* *NOTE 3: In addition, value-dependent operator policies may be applied.*
* *NOTE 4: This header field is not applicable at II-NNI.*
* *NOTE 5: The handling of the URI parameters "cpc" and "oli", defined in 3GPP TS 24.229 [5] subclause 7.2A.12, is specified in 3GPP TS 24.229 [5], clause 4.4.*
 |

Items stroke out in the table above are not in scope of this i3 Forum Release, and items underlined are modifications or additions.

##### Derivation of applicable SIP header fields from 3GPP TS 24.229 [5]

For the purpose of the present document clause 6.1.1.3.2 of TS 29.165 v11.5.0 (2012-12) applies as follows:

*For any method in table 6.1, the SIP header fields applicable on the II-NNI are detailed in the corresponding method tables for the UA role and proxy role sending behavior in Annex A of 3GPP TS 24.229 [5]. Unless other information is specified in the normative part of the present specification, the applicability of header fields at the II-NNI can be derived for each method from the corresponding tables in annex A of 3GPP TS 24.229 [5] as follows:*

*- All header fields not present in the corresponding tables in Annex A of 3GPP TS 24.229 or marked as "n/a" in both the "RFC status" and "profile status" columns for the UA role and proxy role sending behaviour of that tables are not applicable at the II-NNI.*

*NOTE 1: Operators could choose to apply header fields for other SIP extensions on an II-NNI based on bilateral agreements, but this is outside the scope of the present specification.*

*- All header fields which are marked as "o" in at least one of the "RFC status" or the "profile status" profile columns for the sending behaviour in the corresponding UA role and proxy role tables in annex A of 3GPP TS 24.229 [5] and as "n/a" or "o" in the other such columns are applicable at II-NNI based on bilateral agreement between operators.*

*- All header fields which are marked as "m" in at least one of the "RFC status" or the "profile status" columns for the sending behaviour in the corresponding UA role or proxy role table in annex A of 3GPP TS 24.229 [5] and as "n/a", "o", or "m" in the other such columns are applicable at the II-NNI.*

*- If conditions are specified, they are also applicable at the II-NNI and the above rules are applicable to the "n/a", "o" and "m" values within the conditions.*

*NOTE 2: In the above rules, the RFC profile columns are taken into account in order to enable interworking with non-3GPP networks,*

*An informative summary of SIP header fields to be used over the II-NNI is proposed in annex A.*

##### Applicability of SIP header fields on a roaming II-NNI

For the purpose of the present document clause 6.1.1.3.3 of TS 29.165 v11.5.0 (2012-12) applies as follows:

*The following SIP header fields are only applicable on a roaming II-NNI:*

*- Authentication-Info*

*- Authorization*

*- P-Associated-URI*

*- P-Called-Party-ID*

*- P-Preferred-Service*

*- P-Profile-Key*

*- P-Served-User*

*- P-Visited-Network-ID*

*- Path*

*- Proxy-Authenticate*

*- Proxy-Authorization*

*- Service-Route*

*- WWW-Authenticate*

##### Applicability of SIP header fields on a non-roaming II-NNI

For the purpose of the present document clause 6.1.1.5 of TS 29.165 v11.5.0 (2012-12) applies as follows:

*The following SIP header fields are only applicable on a non-roaming II-NNI or for the loopback traversal scenario:*

*- P-Refused-URI-List*

#### Notations of the codes

Moved to Section 7.1.1.1.

#### Modes of signalling

For the purpose of the present document clause 6.1.1.5 of TS 29.165 v11.5.0 (2012-12) applies applies as follows:

*Overlap signalling may be used if agreement exists between operators to use overlap and which method to be used, otherwise enbloc shall be used at the II-NNI.*

### SDP Protocol

#### General

For the purpose of the present document clause 6.1.2.1 of TS 29.165 v11.5.0 (2012-12) applies as follows:

*The functional entity closest to the border of an II-NNI (see reference model in Clause 5) shall provide the capabilities specified for that network element in Annex A.3 of 3GPP TS 24.229 [5].*

*The SDP bodies shall be encoded as described in IETF RFC 3261 [13] and in IETF RFC 4566 [147]. The offer/answer model with the SDP as defined in IETF RFC 3264 [146] shall be applied.*

### Major Capabilities

For the purpose of the present document clause 6.1.3 of TS 29.165 v11.5.0 (2012-12) applies with the following changes in Table 6.1.3.1 and Table 6.1.3.2. as follows:

*This subclause contains the major capabilities to be supported over the II-NNI.*

*The table 6.1.3.1 specifies which capabilities are applicable for II-NNI. The profile status codes within table 6.1.3.1 are defined in table 6.1.3.2. For the "Basic SIP" capabilities part of table 6.1.3.1, the last column "Profile status over II-NNI" specifies the general status of applicability of the IETF RFC 3261 [13] main mechanisms described in the 2nd column "Capability over the Ici".*

*For the "Extensions to basic SIP" capabilities part, the last column "Profile status over II-NNI" specifies the general status of applicability of the RFC referenced in the 2nd column "Capability over the Ici". If necessary, the applicability of RFCs at the II-NNI level is further detailed in the present Technical Specification.*

*The columns "Reference item in 3GPP TS 24.229 [5] for the profile status" provide informative references for comparison purposes into the UA and Proxy role major capabilities tables in 3GPP TS 24.229 [5], where the capabilities are defined via additional references.*

*Table 6.1.3.1: Major capabilities over II-NNI*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| *Item* | *Capability over the Ici* | *Reference item in 3GPP TS 24.229 [5] for the profile status* | *Profile status over II-NNI* | I3Forum Profile status over II-NNI (non-roaming) | I3Forum Profile status over II-NNI (Roaming) |
|  | *UA Role (NOTE 1)* | *Proxy role (NOTE 2)* |
|  | ***Basic SIP (IETF RFC 3261 [13])*** |  |  |  |  |  |
| *1* | *registrations* | *1, 2, 2A* | *-* | *c2* | ~~c2~~ n/a | ~~c2~~ m |
| *2* | *initiating a session* | *2B, 2C, 3, 4* | *-* | *m* | m | m |
| *3* | *terminating a session* | *5* | *3* | *m* | m | m |
| *4* | *General proxy behaviour* | *-* | *4, 5, 14, 15, 19F* | *n/a* | n/a | n/a |
| *5* | *Managing several responses due to forking* | *9,10* | *6* | *m* | m | m |
| *6* | *support of indication of TLS connections in the Record-Route header* | *-* | *7, 8* | *n/a* | n/a | n/a  |
| *7* | *Support of authentication* | *7, 8, 8A* | *8A* | *c2* | ~~c2~~ n/a | ~~c2~~ m |
| *8* | *Timestamped requests (Timestamp header field)* | *6* | *-* | *m* | m | m |
| *9* | *Presence of date in requests and responses (Date header field)* | *11* | *9* | *m* | ~~m~~ oNOTE i3F-2 | ~~m~~ oNOTE i3F-2 |
| *10* | *Presence of alerting information data (Alert-info header field)* | *12* | *10* | *o* | o | o |
| *11* | *Support and handling of the Require header field for REGISTER and other requests or responses for methods other than REGISTER* | *-* | *11, 12, 13* | *m* | m  | m |
| *12* | *Support and reading of the Supported and Unsupported header fields* | *-* | *16, 17, 18* | *m* | m | m |
| *13* | *Support of the Error-Info header field in 3xx - 6xx responses* | *-* | *19* | *o* | o | o |
| *14* | *Support and handling of the Organization header field* | *-* | *19A, 19B* | *m* | m | m |
| *15* | *Support and handling of the Call-Info header field* | *-* | *19C, 19D* | *m* | m  | m |
| *16* | *Support of the Contact header field in 3xx response* | *-* | *19E* | *m* | m | m |
| *16A* | *Proxy reading the contents of a body or including a body in a request or response* |  | *19F* | *n/a* | n/a | n/a |
|  | ***Extensions to basic SIP*** |  |  |  |  |  |
| *16B* | *3GPP TS 24.237 [131]: proxy modifying the content of a body* | *n/a* | *19G* | *n/a* | n/a | n/a |
| *17* | *IETF RFC 6086[39]: SIP INFO method and package framework* | *13* | *20* | *o* | o | o |
| *17A* | *IETF RFC 6086 [39]: legacy INFO usage* | *13A* | *20A* | *o* | o | o |
| *18* | *IETF RFC 3262 [18]: reliability of provisional responses in SIP (PRACK method)* | *14* | *21* | *m* | m | m |
| *19* | *IETF RFC 3515 [22]: the SIP REFER method* | *15* | *22* | *o* | ~~o~~ | o NOTE i3F-1 |
| *20* | *IETF RFC 3312 [40] and RFC 4032 [41]: integration of resource management and SIP (Preconditions framework)* | *16* | *23* | *o* | o | o |
| *21* | *IETF RFC 3311 [23]: the SIP UPDATE method* | *17* | *24* | *m* | m | m |
| *22* | *IETF RFC 3313 [42]: SIP extensions for media authorization (P-Media-Authorization header field)* | *19* | *26* | *n/a* | n/a | n/a |
| *23* | *IETF RFC 3265 [20]: SIP specific event notification (SUBSCRIBE/NOTIFY methods)* | *20, 21, 22, 23* | *27, 28* | *c1* | ~~c1~~ o | ~~c1~~ m |
| *24* | *IETF RFC 3327 [43]: session initiation protocol extension header field for registering non-adjacent contacts (Path header field)* | *24* | *29* | *c2* | ~~c2~~ n/a | ~~c2~~ m |
| *25* | *IETF RFC 3325 [44]: private extensions to the Session Initiation Protocol (SIP) for network asserted identity within trusted networks* | *25* | *30*  | *c4* | c4 | c4 |
| *26* | *IETF RFC 3325 [44]: the P-Preferred-Identity header field extension* | *-* | *-* | *n/a* | n/a | n/a |
| *27* | *IETF RFC 3325 [44]: the P-Asserted-Identity header field extension* | *-* | *-* | *c4* | c4 | c4 |
| *28* | *IETF RFC 3323 [34]: a privacy mechanism for the Session Initiation Protocol (SIP) (Privacy header field)* | *26, 26A, 26B, 26C, 26D, 26E, 26F, 26G, 26H* | *31, 31A, 31B, 31C, 31D, 31E, 31F, 31G, 31H* | *m* | m | m |
| *29* | *IETF RFC 3428 [19]: a messaging mechanism for the Session Initiation Protocol (SIP) (MESSAGE method)* | *27* | *33* | *o* | ~~o~~ | o |
| *30* | *IETF RFC 3608 [45]: session initiation protocol extension header field for service route discovery during registration (Service-Route header field)* | *28* | *32* | *c2* | ~~c2~~ n/a | m |
| *31* | *IETF RFC 3486 [46]: compressing the session initiation protocol* | *29* | *34* | *n/a* | n/a | n/a |
| *32* | *IETF RFC 3455 [24]: private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP)*  | *30* | *35* | *o* | o  | o |
| *32A* | *IETF RFC 3325 [44]: act as first entity within the trust domain for asserted identity* | *30A* | *30A* | *n/a* | n/a | n/a |
| *32B* | *IETF RFC 3325 [44]: act as entity within trust network that can route outside the trust network* | *30B* | *30B* | *n/a* | n/a | n/a |
| *32C* | *IETF RFC 3325: act as entity passing on identity transparently independent of trust domain* | *30C* | *30C* | *n/a* | n/a | n/a |
| *33* | *IETF RFC 3455 [24]: the P-Associated-URI header field extension* | *31* | *36* | *c2* | ~~c2~~ n/a | ~~c2~~ m |
| *34* | *IETF RFC 3455 [24]: the P-Called-Party-ID header field extension* | *32* | *37* | *c2* | ~~c2~~ n/a | ~~c2~~ m |
| *35* | *IETF RFC 3455 [24]: the P-Visited-Network-ID header field extension* | *33* | *38, 39* | *c2* | ~~c2~~ n/a | ~~c2~~ m |
| *36* | *IETF RFC 3455 [24]: the P-Access-Network-Info header field extension* | *34* | *41, 42, 43* | *c4* | ~~c4~~ n/a | ~~c4~~ o NOTE i3F-2 |
| *37* | *IETF RFC 3455 [24]: the P-Charging-Function-Addresses header field extension* | *35* | *44, 44A* | *n/a* | n/a | n/a |
| *38* | *IETF RFC 3455 [24]: the P-Charging-Vector header field extension* | *36* | *45, 46* | *c1* | ~~c1~~ o | ~~c1~~ m |
| *39* | *IETF RFC 3329 [47]: security mechanism agreement for the session initiation protocol* | *37* | *47* | *n/a* | n/a | n/a |
| *39A* | *draft-dawes-dispatch-mediasec-parameter-03 [137]: Capability Exchange for Media Plane Security* | *37A* | *47A* | *n/a* | n/a | n/a |
| *40* | *IETF RFC 3326 [48]: the Reason header field for the session initiation protocol* | *38* | *48* | *o* | o | o |
| *41* | *IETF RFC 6432  [49]: carrying Q.850 codes in reason header fields in SIP (Session Initiation Protocol) responses* | *38A* | *48A* | *c4* | c4 | c4 |
| *42* | *IETF RFC 3581 [50]: an extension to the session initiation protocol for symmetric response routeing* | *39* | *49* | *o* | o | o |
| *43* | *IETF RFC 3841 [51]: caller preferences for the session initiation protocol (Accept-Contact, Reject-Contact and Request-Disposition header fields)* | *40, 40A, 40B, 40C, 40D, 40E, 40F*  | *50, 50A, 50B, 50C, 50D, 50E, 50F* | *m* | m | m |
| *44* | *IETF RFC 3903 [21]: an event state publication extension to the session initiation protocol (PUBLISH method)* | *41* | *51* | *c1* | ~~c1~~  | o NOTE i3F-2 |
| *45* | *IETF RFC 4028 [52]: SIP session timer (Session-Expires and Min-SE headers)* | *42* | *52* | *m* | ~~m~~oNOTE i3F-2 | ~~m~~oNOTE i3F-2 |
| *46* | *IETF RFC 3892 [53]: the SIP Referred-By mechanism* | *43* | *53* | *m* | ~~m~~ | m NOTE i3F-1 |
| *47* | *IETF RFC 3891 [54]: the Session Initiation Protocol (SIP) "Replaces" header* | *44* | *54* | *o* | ~~o~~ | o NOTE i3F-1 |
| *48* | *IETF RFC 3911 [55]: the Session Initiation Protocol (SIP) "Join" header* | *45* | *55* | *o* | ~~o~~ | o NOTE i3F-1 |
| *49* | *IETF RFC 3840 [56]: the callee capabilities* | *46* | *56* | *o* | ~~o~~ | ~~o~~ |
| *50* | *IETF RFC 4244 [25]: an extension to the session initiation protocol for request history information (History-Info header field)* | *47* | *57* | *o* | o | o |
| *51* | *IETF RFC 5079 [57]: Rejecting anonymous requests in the session initiation protocol* | *48* | *58* | *o* | o | o |
| *52* | *IETF RFC 4458 [58]: session initiation protocol URIs for applications such as voicemail and interactive voice response (NOTE 3)* | *49* | *59* | *o* | o | o |
| *53* | *IETF RFC 4320 [59]: Session Initiation Protocol's (SIP) non-INVITE transactions* | *50* | *61* | *m* | m | m |
| *54* | *IETF RFC 4457 [60]: the P-User-Database private header field extension* | *51* | *60* | *n/a* | n/a | n/a |
| *55* | *IETF RFC 5031 [61]: a uniform resource name for services* | *52* | *62* | *n/a* | n/a | n/a |
| *56* | *IETF RFC 5627 [62]: obtaining and using GRUUs in the Session Initiation Protocol (SIP)* | *53* | *63* | *c1* | ~~c1~~o | ~~c1~~ m |
|  | *Void* |  |  |  |  |  |
| *58* | *IETF RFC 4168 [27]: the Stream Control Transmission Protocol (SCTP) as a Transport for the Session Initiation Protocol (SIP)* | *55* | *65* | *o* | o | o |
| *59* | *IETF RFC 5002 [64]: the SIP P-Profile-Key private header field extension* | *56* | *66, 66A, 66B* | *c3* | ~~c3~~ n/a | ~~c3~~ o |
| *60* | *IETF RFC 5626 [65]: managing client initiated connections in SIP* | *57* | *67* | *c1* | ~~c1~~o | ~~c1~~ m |
| *61* | *IETF RFC 5768 [66]: indicating support for interactive connectivity establishment in SIP* | *58* | *68* | *n/a* | n/a | n/a |
| *62* | *IETF RFC 5365 [67]: multiple-recipient MESSAGE requests in the session initiation protocol* | *59* | *69* | *o if 29, else n/a* | o if 29, else n/a | o if 29, else n/a |
| *63* | *draft-ietf-sipcore-location-conveyance-08 [68]: SIP location conveyance (Geolocation header)* | *60* | *70, 70A, 70B* | *m* | ~~m~~ | ~~m~~ |
| *64* | *IETF RFC 5368 [69]: referring to multiple resources in the session initiation protocol* | *61* | *71* | *o if 19, else n/a* | o if 19, else n/a | o if 19, else n/a |
| *65* | *IETF RFC 5366 [70]: conference establishment using request-contained lists in the session initiation protocol* | *62* | *72* | *o* | o  | o |
| *66* | *IETF RFC 5367 [71]: subscriptions to request-contained resource lists in the session initiation protocol* | *63* | *73* | *o if 23, else n/a* | o if 23, else n/a | o if 23, else n/a |
| *67* | *IETF RFC 4967 [72]: dialstring parameter for the session initiation protocol uniform resource identifier* | *64* | *74* | *c2* | ~~c2~~ n/a | ~~c2~~ m |
| *68* | *IETF RFC 4964 [73]: the P-Answer-State header extension to the session initiation protocol for the open mobile alliance push to talk over cellular* | *65* | *75* | *o* | o | o |
| *69* | *IETF RFC 5009 [74]: the SIP P-Early-Media private header field extension for authorization of early media* | *66* | *76* | *c4* | c4 | c4 |
| *70* | *IETF RFC 4694 [75]: number portability parameters for the ‘tel’ URI* | *67, 67A, 67B* | *77, 77A, 77B* | *o* | o | o |
| *72* | *IETF RFC 4411 [77]: extending the session initiation protocol Reason header for preemption events* | *69* | *79* | *o* | ~~o~~ | ~~o~~ |
| *73* | *IETF RFC 4412 [78]: communications resource priority for the session initiation protocol? (Resource-Priority header field)* | *70, 70A, 70B*  | *80, 80A, 80B* | *o* | ~~o~~ | ~~o~~ |
| *74* | *IETF RFC 5393 [79]: addressing an amplification vulnerability in session initiation protocol forking proxies* | *71* | *81* | *m* | m | m |
| *75* | *IETF RFC 5049 [80]: the remote application identification of applying signalling compression to SIP* | *72* | *82* | *n/a* | n/a | n/a |
| *76* | *IETF RFC 5688 [81]: a session initiation protocol media feature tag for MIME application sub-types* | *73* | *83* | *c1* | ~~c1~~ o | ~~c1~~ m |
| *77* | *IETF RFC 6050 [26]: Identification of communication services in the session initiation protocol* | *74* | *84, 84A* | *o* | ~~o~~ | ~~o~~ |
| *78* | *IETF RFC 5360 [82]: a framework for consent-based communications in SIP?* | *75, 75A, 75B* | *85* | *o* | ~~o~~ | ~~o~~ |
| *79* | *draft-johnston-sipping-cc-uui-09 [83]: transporting user to user information for call centers using SIP?* | *76* | *86* | *c1* | ~~c1~~ o | ~~c1~~ m |
| *79A* | *draft-ietf-cuss-sip-uui-isdn [83A]: Interworking ISDN Call Control User Information with SIP* | *76A* | *n/a* | *c1* | ~~c1~~ o | ~~c1~~ m  |
| *80* | *draft-vanelburg-dispatch-private-network-ind-01 [84]: The SIP P-Private-Network-Indication private-header (P-Header)* | *77* | *87* | *c1* | ~~c1~~ | ~~c1~~ |
| *81* | *IETF RFC 5502 [85]: the SIP P-Served-User private header* | *78* | *88* | *c2* | ~~c2~~ n/a | ~~c2~~ m |
| *83* | *draft-dawes-sipping-debug-04 [87]: the P-Debug-ID header extension* | *80* | *90* | *o* | ~~o~~ | ~~o~~ |
| *84* | *IETF RFC 6228 [88]: the 199 (Early Dialog Terminated) response code* | *81* | *91* | *m* | m | m |
| *85* | *IETF RFC 5621 [89]: message body handling in SIP* | *82* | *92* | *m* | m | m |
| *86* | *IETF RFC 6223 [90]: indication of support for keep-alive* | *83* | *93* | *o* | ~~o~~ | ~~o~~  |
| *87* | *IETF RFC 5552 [91]: SIP Interface to VoiceXML Media Services* | *84* | *94* | *n/a* | n/a | n/a |
| *88* | *IETF RFC 3862 [92]: common presence and instant messaging (CPIM): message format* | *85* | *95* | *o* | ~~o~~ | o |
| *89* | *IETF RFC 5438 [93]: instant message disposition notification* | *86* | *96* | *o* | ~~o~~ | o |
| *90* | *IETF RFC 5373 [94]: requesting answering modes for SIP (Answer-Mode and Priv-Answer-Mode header fields)* | *87* | *97, 97A* | *o* | ~~o~~ | ~~o~~ |
|  | *Void* |  |  |  |  |  |
| *92* | *IETF RFC 3959 [96]: the early session disposition type for SIP* | *89* | *99* | *o* | ~~o~~ | o |
| *93* | *IETF RFC 4244 [97]: delivery of Request-URI targets to user agents* | *90* | *100* | *n/a* | n/a | n/a |
| *94* | *draft-kaplan-dispatch-session-id-00 [124]: The Session-ID header* | *91* | *101* | *o* | o | o |
| *95* | *IETF RFC 6026 [125]: correct transaction handling for 200 responses to Session Initiation Protocol INVITE requests* | *92* | *102* | *m* | m | m |
| *96* | *IETF RFC 5658 [126]: addressing Record-Route issues in the Session Initiation Protocol (SIP)* | *93* | *103* | *o* | o | o |
| *97* | *IETF RFC 5954 [127]: essential correction for IPv6 ABNF and URI comparison in IETF RFC 3261 [13]* | *94* | *104* | *m* | m | m |
| *98* | *IETF RFC 4488 [135]: suppression of session initiation protocol REFER method implicit subscription* | *95* | *105* | *m if 19, else n/a* | m if 19, else n/a  | m if 19, else n/a |
| *99* | *draft-ietf-salud-alert-info-urns [136]: Alert-Info URNs for the Session Initiation Protocol* | *96* | *106* | *o* | ~~o~~ | o |
| *100* | *Subclause 3.1 of 3GPP TS 24.229: multiple registrations* | *97* | *107* | *c2* | ~~c2~~ n/a | ~~c2~~ m |
| *101* | *IETF RFC 5318 [141]: the SIP P-Refused-URI-List private-header* | *98* | *108* | *c5* | c5 | ~~c5~~ n/a |
| *102* | *IETF RFC 4538 [140]: request authorization through dialog Identification in the session initiation protocol (Target-Dialog header field)* | *99* | *109* | *o* | o | o |
| *103* | *draft-holmberg-sipcore-proxy-feature [143]: indication of features supported by proxy* | *100* | *110* | *o* | o | o |
| *104* | *IETF RFC 6140: registration of bulk number contacts* | *101* | *111* | *c2* | ~~c2~~ n/a | ~~c2~~ m |
| *105* | *IETF RFC 6230: media control channel framework* | *102* | *112* | *o* | o | o |
| *105A* | *3GPP TS 24.229 [5]: S-CSCF restoration procedures* | *103* | *113* | *c3* | ~~c3~~ n/a | ~~c3~~ o |
| *106* | *RFC 6357 [164] SIP overload control* | *104* | *114* | *o* | o | o |
| *107* | *draft-ietf-soc-overload-control [165] feedback control* | *104A* | *114A* | *o* | o | o |
| *c1: m in case of roaming II-NNI, else o**c2: m in case of roaming II-NNI, else n/a**c3: o in case of roaming II-NNI, else n/a**c4: m in case of trust relationship between the interconnected networks, else n/a**c5: o in case of non-roaming II-NNI and loopback traversal scenario, else n/a** *NOTE 1: The item numbering corresponds to the one provided in table A.4 in [5].*
* *NOTE 2: The item numbering corresponds to the one provided in table A.162 in [5].*
* *NOTE 3: A common URI namespace is required to apply this feature on the II-NNI.*
* NOTE i3F-1: Needed to support CONF service as specified within TS 24.147 [106] Section 5.3.1.5.3

NOTE i3F-2:. Item 9: Date header is of no use for basic voice service, which is the scope of the document, as it is globally considered less reliable with regards to locally registered timestamp. Furthermore it's not commonly used for any post-processing (charging, reporting, …) so it's more appropriate to leave it as an optional item.Item 36; this capability is optional due to possible unsecure relationship via public Internet, Item: 44: as shown is Sec. 6.1.1.2.the PUBLISH method is out-of-scope at Interconnection II-NNIItem 45: SIP Session Timer as specified in RFC 4028 is meant to be an end-to-end per-session keepalive mechanism which can result meaningless if there is any node (B2BUA, ASs,...) in the chain, re-generating SIP signalling so interrupting the signalling transparency, as it is common in real environments. It’s more appropriate not to mandate it.  |

Items stroke out in the table above are not in scope of this i3 Forum Release, and items underlined are modifications or additions.

*Table 6.1.3.2: Key to notation codes for major capabilities*

|  |  |  |
| --- | --- | --- |
| *Notation code* | *Notation name* | *Explanation* |
| *M* | *mandatory* | *The capability shall be supported at II-NNI.**SIP message relating to this capability shall be sent over the II-NNI if received from the serving network, unless they also make use of other unsupported capabilities.**SIP headers or other information elements relating to this capability shall be passed over the II-NNI if received from the sending side.**This does not imply that network elements inside the serving network or served network or user equipment connected to these networks shall support this capability.* |
| *O* | *optional* | *The capability may or may not be supported at II-NNI. The support of the capability is provided based on bilateral agreement between the operators (*i.e. Service Provider and/or carriers according to i3Forum terminology). |
| *n/a* | *not applicable* | *It is impossible to use/support the capability at the II-NNI.* |
| *c <integer>* | *conditional* | *The support of the capability ("m", "o" or "n/a") depends on the support of other optional or conditional items. <integer> is the identifier of the conditional expression.* |

## Control Plane Transport

### General

For the purpose of the present document clause 6.2.1 of TS 29.165 v11.5.0 (2012-12) applies as follows:

*The control plane transport of the II-NNI shall comply with clause 4.2A of 3GPP TS 24.229 [5].Support of SCTP as specified in IETF RFC 4168 [27] is optional for an IBCF connected by II-NNI. Nevertheless this option is favourable if the operators would like to improve reliability over the Ici.*

## SIP Timers

# Numbering and Addressing

[ATIS-1000009.2006, IP NETWORK-TO-NETWORK INTERFACE (NNI) STANDARD FOR VOIP]

The table below describes the set of URI formats that MUST 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.

|  |  |
| --- | --- |
| 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 Codeand 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 SignificantNumber |
| 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 |

# Security

**Annex A**

(normative/informative)

# Annex A – Response Codes

*[PKT-SP-IGS-C01-130930, PacketCable Interconnect Guidelines Specification]*

This annex documents the semantics for the common response codes that appear on the peering interface so an SSP network that receives a response code from a peer will take the correct action.

Table 2 lists response codes for some of the common call failures. For many of the 4xx error cases, the response code would only be generated for the stated condition if the call wasn’t handled in some manner by the terminating SSP network (e.g., call routed to voice mail).

Table  - Response Codes

| Condition | Response Code | Example Action when Received |
| --- | --- | --- |
| Endpoint is unavailableMTA powered downMTA removed from service by OSLine in lockout | 480 Temporarily Unavailable | Reorder tone, or announcement "Your call cannot be completed at this time. Please hang up and try again later."  |
| Line is "busy"Line doesn’t have call waiting and is busy in a call Line has call waiting, but is already busy with two calls, busy in an emergency call, is in a transient state with another call (ringing, origination glare, etc)  | 486 Busy Here | Busy tone |
| Call times out waiting for user actionRinging timeout waiting for answerTimeout waiting to accept call-waiting callTimeout waiting for caller to enter digits after solicitor-call-blocking prompt  | 480 Temporarily Unavailable | Reorder tone, or announcement "Your call cannot be completed at this time. Please hang up and try again later." |
| Call blocked by a featureTerminating call blockingDo not disturb | 403 Forbidden | Announcement: "Due to network difficulties, your call cannot be completed at this time. Please try your call again later." |
| Call blocked because called user not authorized to receive callsTemporarily disconnected due to late paymentRecently deleted  | 404 Not Found | Announcement: "Your call cannot be completed as dialed. Please check the number and try again." |
| Call blocked due to resource limitationNo QoSMTA resource exhaustion (e.g., no DSP resources) | 480 Temporarily Unavailable | Reorder tone, or announcement "Your call cannot be completed at this time. Please hang up and try again later." |
| Call Forward loop detected | Depends on type of call forwarding:CFBL: 486 Busy HereCFDA, CFV, SCF: 480 Temporary Failure | Reorder tone, or announcement "Your call cannot be completed at this time. Please hang up and try again later." |
| During call-transfer, transfer-to user agent can’t find dialog identified in Replaces header | 481 Call/Transaction Doesn’t Exist | Application dependent |
| Called endpoint can not support SDP offerDoes not support IP version in SDP c= lineDoes not support any offered codecNot authorized for authored media | 488 Not Acceptable Here | Reorder, or announcement  |
| Called address does not existTarget routing number not owned by this networkCalled user does not exist in this network | 404 Not Found | Announcement: "Your call cannot be completed as dialed. Please check the number and try again." |
| Congestion encountered at the peering interface | 503 Service Unavailable | Retry call via PSTN (see Section 6.5.2 for more details). |

1. This is not CPE. [↑](#footnote-ref-1)