**Contribution**

**TITLE:** IP Interconnection Profile

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

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

**ABSTRACT**

This document provides the marked up output from the 4/30 meeting.

Additional editorial changes were made to make the document more consistent.

**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

This document was developed under a joint ATIS and SIP Forum collaboration. The document defines an IP NNI Standard with an emphasis on VoIP and other Multimedia services to be addressed in subsequent releases.

The objective of this document is to:

1. Define a reference architecture that sets forth the common functional entities necessary for CarrierCarrier to Carrier Interconnection. This reference architecture will be from the perspective of the interconnection points between carriers and will not deal with implementation details inside the networks on either side of the IP-NNI.
2. Specify the exact specifications (including IETF RFCs, 3GPP, and other existing standards) associated with these protocols that must or should be supported by each element of the reference architecture. Where required, the options that MUST or SHOULD be supported within a given standard will also be specified.
3. Specify customary methods for negotiating protocols, protocol extensions, and exchanging capability information between Carrier’s. Specify consensus methods of formulating SIP protocol messages where multiple options exist in standards.
4. Specify the exact presentations of Fully Qualified Domain Names in “From:” and “To:” fields including use of TEL URI format, including P-Asserted Identity (PAI).
5. For IP originated Calls, specify the preferred header [SHOULD] for Calling Name data [CNAM], and specify how that data is presented to the terminating proxy including format, syntax and processing of such data. Note: The expectation is that the signaling of CNAM would not survive interworking to SS7.
6. Define mandated support for underlying transport [e.g. UDP, TCP, SCTP].
7. Specify an audio codec selection strategy that minimizes the need for transcoding and a transcoding strategy that balances the workload between originating and terminating carrier.
8. Define strategies for DTMF and Fax support.
9. Specify call loop detection and avoidance methods.
10. Define common Quality of Service objectives including network overload and congestion notification and processing mechanisms.
11. Investigate issues surrounding known interoperability problems (e.g. PRACK [RFC 3262], early media, ptime, etc.).

## Purpose

IP Interconnection among service providers is significantly increasing as the Transition of the PSTN from SS7/TDM to SIP/IP networks progresses. Current deployments of SIP/IP in the core carrier networks have exposed operational and implementation differences on how IP for SIP traffic works ‘on the wire’. These differences complicate interconnection, and in some cases require ‘protocol normalization’ to achieve full interoperability. The call control protocol SIP [RFC 3261] is defined in the IETF and further refined in profiles developed by 3GPP or ATIS that reflect regional and/or national differences in implementation. There are hundreds of IETF SIP and 3GPP specifications that are open to interpretation, creating ambiguity in the detailed options that are implemented. This often requires Session Border Controllers or I-CSCF proxies to spend unnecessary processing reconciling the signaling between service providers and resolving those ambiguities. Time and effort is also required to document the differences and configure the SBC or I-CSCF proxy to implement the necessary changes to the on the wire protocol.

The purpose is to identify a baseline set of features that should be common to all IP-NNI implementations for voice service. In addition, gaps or ambiguities are identified in existing standards and request that those gaps be addressed by the responsible Standards Development Organization [SDO].

This specification defines which standards and options must be supported. They will provide Carrier’s with a precise description of the IP-NNI in the areas where the standards leave multiple options, or where the existing specifications are ambiguous.

In addition, this specification will increase requirements [i.e. MAY, SHOULD, MUST] where operational experience indicates that such enhancements are necessary to support full interoperability.

## Application

This standard is defined for North America deployments, but may be applicable for deployments outside North America..

# 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

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

## Current US Telephony PSTN Interconnect Model

The figure below depicts the current US Telephony PSTN architecture and interconnect model. This architecture is characterized by:

* One or more end office local switching systems interconnected within a Local Access and Transport Area (LATA).
* One or more Inter-exchange carrier networks providing interconnect services between these LATA based local networks.



**Figure C.1 - Current US Telephony PSTN Interconnect Model**

The end office switches within the LATA are known as Class 5 (C5) switches. Within the LATA, Class 5 switches interconnect through a Tandem switch or through direct connections between the switches. Class 5 switches connect directly to customer premises equipment such as telephones and FAX machines, and provide local telephony services to this equipment.

Interconnectivity between LATAs is provided by Inter-exchange Carrier networks. These networks are comprised of Class 4 (C4) switches that provide interconnect services between other Class 4, Class 5, and tandem switches. The inter-exchange carrier’s class 4 switch may connect to an access tandem and/or directly to the class 5 switches within a LATA.

## VoIP Interconnection Basic Configuration

VoIP in this context will coexist with SMS, MMS, Multimedia features, video calling, and other Real Time Communications features that may come available.

VoIP has been introduced into the traditional PSTN network architecture in a variety of places, forming islands of VoIP that must interconnect. For example VoIP could be used in:

* Enterprise PBX networks.
* Local networks.
* Tandem and inter-exchange networks.

The figure below illustrates one example of a bilateral carrier VoIP interconnection wherein VoIP signaling and media are exchanged between carriers. More detail relating to interconnect models is provided in section C.2 of this document.



**Figure C.2 - Bilateral Carrier VoIP Interconnections**

## Trust Model

**Security trust model**

CarrierTheCarrier functional reference architecture defines Functional Entities (FEs). However, since network security aspects depend heavily on the way that FEs are bundled together, the Carriersecurity 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.

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.

When a Carrier is connected to another Carrier, whether the other Carrier 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 Carrier service providers, or via one or more untrusted Carrier transport providers;
* Business relationships, where there may be penalty clauses in the SLA agreements, and/or a trust in the other Carrier 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, Carrier providers should view other providers as un-trusted. Figure 3 shows an example when a connected Carrier is judged un-trusted.



Figure 3 – Carrier Interconnection Trust Relationship

An “internally trusted network security zone” or “trusted zone” in short, is a zone where a Carrier provider’s network elements and systems reside and never communicate directly with customer equipment or other domains. The common characteristics of Carrier network elements in this zone are that they are under the full control of the Carrier provider are located in the Carrier 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 Carrier 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 Carrier 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 Carrier provider. The equipment may be under the control by either the customer/subscriber or the Carrier provider. In addition, the equipment may be located within or outside the Carrier 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 Carrier 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 Carrier provider in the trusted zone in order to provide the user/subscriber access to the Carrier 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 Carrier provider’s device configuration system in the trusted zone in order to configure the user’s/subscriber’s device and Carrier provider’s equipment in the outside plant.
* Operations, Administration, Maintenance, and Provisioning NBE(OAMP-NBE) that interfaces with the Carrier provider’s OAMP systems in the trusted zone in order to provide and maintain the user’s/subscriber’s device and Carrier provider’s equipment in the outside plant.
* Application Server/Web Server NBE (AS/WS-NBE) that interfaces with the Carrier 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 Carrier provider but are not located on the Carrier provider’s premises, and that may or may not be under the control of the Carrier 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 Carrier network elements, general hardening of the systems, , use of secure signaling for all signaling messages sent to Carrier 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 Carrier provider security zone outside of the related Carrier provider domain. These are connected to the Carrier provider’s border elements.. The elements in the “un-trusted zone” may not be under the control of the Carrier 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.

# General Procedures

## Extension Negotiation

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 Carrier (SIP Service Provider) network. When sending an out-of-dialog request to a peer Carrier 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 Carrier 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 Carrier network, SIP entities involved in session peering MUST identify all supported SIP requests in the Allow header field

## Public User Identities

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 Carrier 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 Carrier 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.com;user=phone |
| LNP Query - number not ported | send/receive | Above plus "npdi" parameter | sip:+13036614567;npdi@example.com;user=phone |
| LNP Query - number ported | send/receive | Above plus global "rn" parameter | sip:+13036614567;npdi,rn=+13036620000@example.com;user=phone |

North American supported formats are shown in Table 2.

### 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.

### Numbering and Addressing

Ed. Note: moved up from Section 8

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:+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 |

## IPv4/6 Interworking

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

## Fault Isolation and Recovery

### Interface Failure Detection

An Carrier 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 Carrier network fails to receive a response to an OPTIONS request, then it will consider that non-responding ingress point into the peer Carrier network to have failed, and will remove the ingress point from the available set of ingress points to the peer Carrier network. When a failure is detected, the Carrier network that detected the failure should attempt to route subsequent calls to the peer Carrier network over an available alternate route, with the final alternate route being the PSTN. In the meantime, the Carrier 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 Carrier 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

Carrier's MUST support SIP Overload Control with mandatory support of the default algorithm. Carrier's MAY optional support the Rate Based algorithm based on bilateral agreement between two carriers.

An Carrier 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 Carrier network MUST respond with a 503 (Service Unavailable) response. An Carrier network receiving a dialog-initiating request MUST limit the use of the 503 responses to reporting congestion at the ingress point. A terminating Carrier network MUST NOT send a 503 response to an originating Carrier network to report congestion or other failures that are internal to the terminating Carrier network. For example, a 503 response generated by a SIP signaling entity within a terminating Carrier network should be consumed within the terminating network, and should not be propagated across the peering interface to the originating Carrier 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 Carrier network, the receiving Carrier 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 Carrier 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 Carrier network, the receiving Carrier network MUST:

1. terminate the current transaction,
2. ignore the Retry-After header field if one is present, and
3. 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 Carrier networks SHOULD support the RTP Loopback Test procedures defined in [E-DVA]. Carrier networks that support the RTP Loopback procedures will provide a SIP URI that identifies a media endpoint within the Carrier network that performs the loopback functions. Ideally, this "loopback" media endpoint would be located near the ingress point of the peer Carrier 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 Carrier 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

The following table describes the traffic classes defined for all the interconnection configurations described above:

|  |  |
| --- | --- |
| **Traffic class** | **Traffic type** |
| Voice Media | Speech / Voice bearer. |
| Voice Signaling | Voice Control Traffic (SIP, SIP-I signaling protocols)I |
| Mobile Signaling | SMS and roaming (TCAP signaling protocol) |
| Other Customer Traffic | Internet traffic, other data traffic |

Other control/management traffic such as BGP traffic may also use the interface.

**Distinguishing traffic classes**

In order to distinguish between traffic classes, the use of the DSCP marking scheme in Behaviour Aggregation mode [9] is recommended.

Using classification based on the DSCP value, packet marking is pre-agreed by both operators. The receiving operator assumes that the sending operator has marked the packet correctly according to the pre-agreed scheme described above.

If there is a mix of Internet and VoIP traffic across the interconnection or the recommended marking cannot be guaranteed, an alternative solution is to classify packets using the Multi-Field classification method [9]. Using this scheme, ingress traffic is classified by the receiving Operator PE Router based on any field in the IP header, e.g. destination address, source address, port numbers or other IP packet header fields.

**IP Marking table**

The following table recommends the packet marking guideline for the link/network for all listed interconnection scenarios making use of the DiffServ IETF RFC and IP Precedence TOS marking scheme plus the coding scheme at the MPLS and Ethernet layers, respectively. It applies to all the traffic to be transmitted.

|  |  |  |  |
| --- | --- | --- | --- |
| **Traffic Type** | **DSCP Marking** | **IP Precedence** | **802.1Q VLAN** |
| **Voice Signaling and Media**  | for configurations 6.1, 6.2.1 DSCP 46/EF (101110). | 5 | 5 |
| for configurations 6.2.2 DSCP 46/EF (101110) or DSCP 00/DF (000000). | 5or0 | 5or0 |
| **ETS Voice Signaling and Media** | for configurations 6.1, 6.2.1 DSCP 44/VOICE-ADMIT (101100). | 5 | 5 |
| for configuration 6.2.2, DSCP 44/VOICE-ADMIT (101100). | 5 | 5 |
|  |  |  |  |
|  |  |  |
| **Other traffic** | DSCP 00/DF (000000). | 0 | 0 |

The marking for the other control/management traffic depends on the specific network implementation.

**Traffic treatment**

For interconnection configurations specified in Sections 6.2 and 6.3.1, voice media traffic leaving the sending Border Function towards the receiving Border Function should be treated according to the Expedited Forwarding Per-Hop Behavior [10], [11].

For interconnection configurations specified in Sections 6.2 and 6.3.1, ETS voice signaling and media traffic leaving the sending Border Function towards the receiving Border Function should be treated according to the VOICE-ADMIT Forwarding Per-Hop Behaviour [Reference to 5865].

For the interconnection configuration specified in Section 6.3.2, voice media traffic leaving the sending Border Function towards the sending PE router is treated either according to the Expedited Forwarding Per-Hop Behavior [10], [11] or according to Default forwarding Per-Hop Behavior [1] that is, it becomes ‘best effort‘ forwarding.

For the interconnection configuration specified in Section 6.3.2, ETS voice signaling and media traffic leaving the sending Border Function towards the sending PE router is treated according to the VOICE-ADMIT Per-Hop Behaviour [Reference to 5865].

For interconnection configurations specified in Sections 6.2 and 6.3.1, voice signaling traffic leaving the sending Border Function towards the receiving Border Function should be treated according to the Expedite Forwarding Per-Hop Behavior [10], [11], or alternatively according to the Assured Forwarding Per-Hop Behavior [12].

The industry conventionally uses both AF and EF PHB for signaling traffic. Where one carrier internally uses AF and the other interconnecting carrier internally uses EF, then bilateral agreement is required on how to configure the interconnection to re-mark the packets appropriately. Further if different DSCP markings within the AF class are used, bilateral agreement will be required regarding as to whether the different marking is maintained or traffic re-marked as described for AF / EF marking.

For the interconnection configuration specified in Section 6.3.2, signalling traffic leaving the sending Border Function towards the sending PE router is treated either according to:

* the Expedite Forwarding Per-Hop Behavior, as specified in RFC 3246 [10] and RFC 3247 [11];
* the Assured Forwarding Per-Hop Behavior as specified in RFC 2597 [12];
* the Default forwarding PHB , as specified in IETF RFC 2474 [8].

# Call Features

## Basic Call Setup

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 Carrier network SHOULD include an SDP offer in the initial INVITE. The terminating Carrier network MUST include an SDP answer in the final 200 (OK) response to an INVITE received with an SDP offer. The terminating Carrier MUST include an SDP offer in response to an INVITE received without an SDP offer.

The terminating Carrier network MAY also include an SDP body in a provisional 18x response or reliable response (e.g., PRACK). 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 Carrier network can act on this "preview" SDP to establish an early media session, as described in Section 7.1.3. The terminating Carrier 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 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 Carrier 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 Carrier network is waiting for the terminating Carrier 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 Carrier 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 Carrier 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 Carrier 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 Carrier Network MUST send a 183 (Progressing) response containing SDP that describes the terminating media endpoint to the originating Carrier 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 Carrier network performs the following action on receipt of a provisional response to a call-initiating INVITE.

* The originating Carrier network MUST apply local ringback tone if it receives a 180 (Alerting) response containing no SDP.
* The originating Carrier 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 Carrier 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 Carrier network MAY immediately remove any local ringback tone currently being applied. Alternatively, the originating Carrier 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

Carrier's MUST support P-Early-Media as defijned in RFC 5009.

### Terminating network procedures

When sending an 18x response and early media will be present, the response shall include a P-Early-Media header field, as defined in IETF RFC 5009, authorizing early media, except when

- a reliable provisional response including a P-Early-Media header field has already been sent, and

- the most recently sent P-Early-Media header field authorization matches that which would be sent.

When both-way early media is required, the 18x response shall include a P-Early-Media header field authorizing backward and forward early media (i.e., "sendrecv"), otherwise the P-Early-Media header field shall only authorize backward early media (i.e., "sendonly").

When early media will not be present, the 18x response shall include a P-Early-Media header field not authorizing early media (i.e., “inactive”).

In the event that the nature of early media changes after initially signaled in an 18x response, the new authorization may be signaled in the P-Early-Media header field of either a subsequent 18x response or an UPDATE request.

### Originating network procedures

When sending the initial INVITE request it shall include the P-Early-Media header field with the “supported” value to indicate applicability of the P-Early-Media procedures, per IETF RFC 5009.

When an initial or subsequent 18x response or UPDATE request is received containing a P-Early-Media header field, then the following through connection procedures shall occur.

* If a P-Early-Media header field is received authorizing backward early media (i.e., a value of "sendonly"), then through connection in the backward direction shall be performed, if not already done.
* If a P-Early-Media header field is received not authorizing early media (i.e., a value of "inactive"), then through connection shall not be performed or removed if already done. The originating network shall generate alerting once a 180 Ringing response has been received.
* If a P-Early-Media header field is received authorizing both backward and forward early media (i.e., a value of "sendrecv"), then through connection in both directions shall be performed. The bearer path shall be connected in both directions on completion of the bearer setup.

## Forking the INVITE

For each terminating media endpoint that requires an early media session to be established with the originating line, the terminating Carrier network MUST signal the attributes of the terminating media endpoint to the originating Carrier network within the SDP of a 183 (Progressing) response. The terminating Carrier network MUST ensure that 18x responses containing different SDP copies are not sent within the same dialog. The terminating Carrier 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 Carrier network MUST honor the most recently received 18x response to INVITE, based on the procedures defined in Section 7.1.3.

## Redirecting the INVITE

Carrier's May support redirection across the NNI, based on bilateral agreement. The redirection MAY be performed with a 3XX or REFER message.

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 Carrier 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 Carrier 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 Carrier 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 Carrier 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 Carrier 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 Carrier 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 Carrier network MUST include a Privacy header field containing the value "id" as specified in [RFC 3323] and [RFC 3325]. In addition, the originating Carrier 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 Carrier 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 Carrier network MUST provide a display of "Private" to the terminating user.

## Call Forwarding

Carrier's MUST support the History-Info Header and SHOULD support of the SIP Diversion header for a period of time in order facilitate interoperability. When both headers are sent, the sender MUST ensure that they are semantically identical.

If an Carrier offers call-forwarding services to its users, then the forwarding Carrier 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 Carrier 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 Carrier network.

## National Security/Emergency Prepardness (NS/EP)

Resource Priority Header (RPH) MUST be supported by NS/EP compliant networks, and MUST be transparently passed by non-NS/EP compliant networks.

# NNI Signaling Profile

## 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:*

*Table 6.1: Supported SIP methods*

|  |  |  |  |
| --- | --- | --- | --- |
| *Item* | *Method* | *Ref.* |  *IP-NNI* |
| *Sending* | *Receiving* |
| *1* | *ACK request* | *IETF RFC 3261 [13]* | *m* | *m* |
| *2* | *BYE request* | *IETF RFC 3261 [13]* | *m* | *m* |
| *3* | *BYE response* | *IETF RFC 3261 [13]* | *m* | *m* |
| *3* | *BYE response* | *IETF RFC 3261 [13]* | *m* | *m* |
| *4* | *CANCEL request* | *IETF RFC 3261 [13]* | *m* | *m* |
| *5* | *CANCEL response* | *IETF RFC 3261 [13]* | *m* | *m* |
| *5A* | *INFO request* | *IETF RFC 6086 [39]* | *o* | *o* |
| *5B* | *INFO response* | *IETF RFC 6086 [39]* | *o* | *o* |
| *8* | *INVITE request* | *IETF RFC 3261 [13]* | *m* | *m* |
| *9* | *INVITE response* | *IETF RFC 3261 [13]* | *m* | *m* |
| *9A* | *MESSAGE request* | *IETF RFC 3428 [19]* | *o* | *o* |
| *9B* | *MESSAGE response* | *IETF RFC 3428 [19]* | *o* | *o* |
| *10* | *NOTIFY request* | *IETF RFC 3265 [20]* | *c1* | *c1* |
| *11* | *NOTIFY response* | *IETF RFC 3265 [20]* | *c1* | *c1* |
| *12* | *OPTIONS request* | *IETF RFC 3261 [13]* | *x1* | *x1* |
| *13* | *OPTIONS response* | *IETF RFC 3261 [13]* | *x1* | *x1* |
| *14* | *PRACK request* | *IETF RFC 3262 [18]* | *m* | *m* |
| *15* | *PRACK response* | *IETF RFC 3262 [18]* | *m* | *m* |
| *15A* | *PUBLISH request* | *IETF RFC 3903 [21]* | *c1* | *c1* |
| *15B* | *PUBLISH response* | *IETF RFC 3903 [21]* | *c1* | *c1* |
| *16* | *REFER request* | *IETF RFC 3515 [22]* | *o* | *o* |
| *17* | *REFER response* | *IETF RFC 3515 [22]* | *o* | *o* |
| *18* | *REGISTER request* | *IETF RFC 3261 [13]* | *c2* | *c2* |
| *19* | *REGISTER response* | *IETF RFC 3261 [13]* | *c2* | *c2* |
| *20* | *SUBSCRIBE request* | *IETF RFC 3265 [20]* | *c1* | *c1* |
| *21* | *SUBSCRIBE response* | *IETF RFC 3265 [20]* | *c1* | *c1* |
| *22* | *UPDATE request* | *IETF RFC 3311 [23]* | *m* | *m* |
| *23* | *UPDATE response* | *IETF RFC 3311 [23]* | *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.* |

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) | *IET****F*** *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* | *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~~ |
| *9* | *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* |
| *10* | *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* |
| *11* | *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,*

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

*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

TBD

# Security

**Annex A**

(normative/informative)

# Annex A – Response Codes

This annex documents the semantics for the common response codes that appear on the peering interface so an Carrier 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 Carrier network (e.g., call routed to voice mail).

Table  - Response Codes

| Condition | Response Code | Example Action when Received |
| --- | --- | --- |
| Endpoint is unavailableUEUE powered downUE 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 QoSUE 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)