C. Sibley (Editor)
Cbeyond
C. Gatch (Editor)
Cbeyond

IP PBX / Service Provider Interoperability

sf-adopted-twg-IP_PBX_SP_Interop-sibley-sipconnect

"SIPconnect 1.0 Technical Recommendation"

Abstract

This document outlines an interface specification that enables direct IP peering between a SIP-enabled Service Provider network and a SIP-enabled Enterprise Network for the purpose of originating and/or terminating calls from the Public Switched Telephone Network (PSTN). It specifies the minimal set of IETF and ITU-T standards that must be supported, provides precise guidance in the areas where the standards leave multiple implementation options, and specifies a minimal set of capabilities that should be supported by the Service Provider and Enterprise networks.

Status of this Memo

This Recommendation was promoted to Adopted status by the SIP Forum Board of Directors on January 23, 2008.

Disclaimer

The SIP Forum takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the SIP Forum's procedures with respect to rights in SIP Forum Recommendations, both drafts and final versions, or other similar documentation can be found in the SIP Forum's current adopted intellectual property right Recommendation. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the SIP Forum.

Changes

Prior to final presentation of this document to the SIP Forum Board of Directors, the Working Group Chair submitted one change that, while minor, he viewed as necessary to maintain compatibility with initiatives in the IETF that have emerged since this document entered Proposed Recommendation status. Details of this change can be found in Section 18 of this document

SIPconnect and SIPconnect Compliant are certification marks of the SIP Forum. Implementers who wish to certify their products and services as SIPconnect Complaint may do so under the SIPconnect Compliant program of the SIP Forum. To learn more about this opportunity and obtain other useful information about SIPconnect, please visit www.sipforum.org/sipconnect.

C. Sibley (Editor)
Cbeyond
C. Gatch (Editor)
Cbeyond

Table of Contents

C. Sibley (Editor)
Cbeyond
C. Gatch (Editor)
Cbeyond

1 Introduction

The deployment of IP PBXs among Enterprises of all sizes is increasing rapidly. Additionally, SIP, or Session Initiation Protocol, is fast becoming the dominant industry standard. Many new IP PBXs support SIP phones and SIP routing between one or more PBXs. Deployment of SIP infrastructure by Service Providers is also increasing, driven by the demand for commercial VoIP offerings. The result of these parallel deployments is a present need for direct IP peering between SIP-enabled IP PBXs and SIP-enabled Service Providers.

Currently published ITU-T Recommendations and IETF RFCs offer a comprehensive set of building blocks that can be used to achieve direct IP peering between SIP-enabled IP PBX systems and a Service Provider's SIP-enabled network. However, due to the sheer number of these standards documents, Service Providers and equipment manufacturers have no clear "master reference" that outlines which standards they must specifically support in order to ensure success. This has led to a number of interoperability problems and has unnecessarily slowed the migration to SIP as replacement for traditional TDM connections.

This SIP Forum document aims to address this issue. In short, this document defines the protocol support, implementation rules, and features required for a predictable interoperable scenario between SIP-enabled IP PBXs and SIP-enabled Service Providers. Note that this document does not preclude or discourage the negotiation of additional functionality.

The specific areas where this document provides implementation guidance include:

- Specification of a reference architecture that describes the common network elements necessary for Service Provider to IP PBX peering for the primary purpose of PSTN call origination and termination.
- Specification of the basic protocols (and protocol extensions) that must be supported by each element of the reference architecture.
- Specification of the exact standards associated with these protocols that must or should be supported by each element of the reference architecture.
- Specification of standard methods for negotiating protocols, protocol extensions, and exchanging capability information between endpoints.
- Specification of methods of formulating protocol messages where multiple legitimate implementation options exist.
- Definition of an authentication scheme that provides user security and billing traceability to a single Enterprise.
- Specification of minimum requirements and consensus methods for codec support, packetization intervals, and capability negotiation.
- Specification of a consensus method for handling fax and modem transmissions.
- Specification of minimum requirements and consensus methods for handling echo cancellation.
- Specification of a consensus method for transporting DTMF tones.
- Specification of a consensus method for conveying traffic priority to the Service Provider in order to enable proper QoS delivery.
- Specification of a basic set of guidelines for interfacing with an IP PBX when Network Address Translation and/or packet filtering devices are utilized in the communications path.
- Definition of a basic security model based on existing standards to authenticate and authorize utilization of the Service Provider's resources by an IP PBX.

C. Sibley (Editor)
Cbeyond
C. Gatch (Editor)
Cbeyond

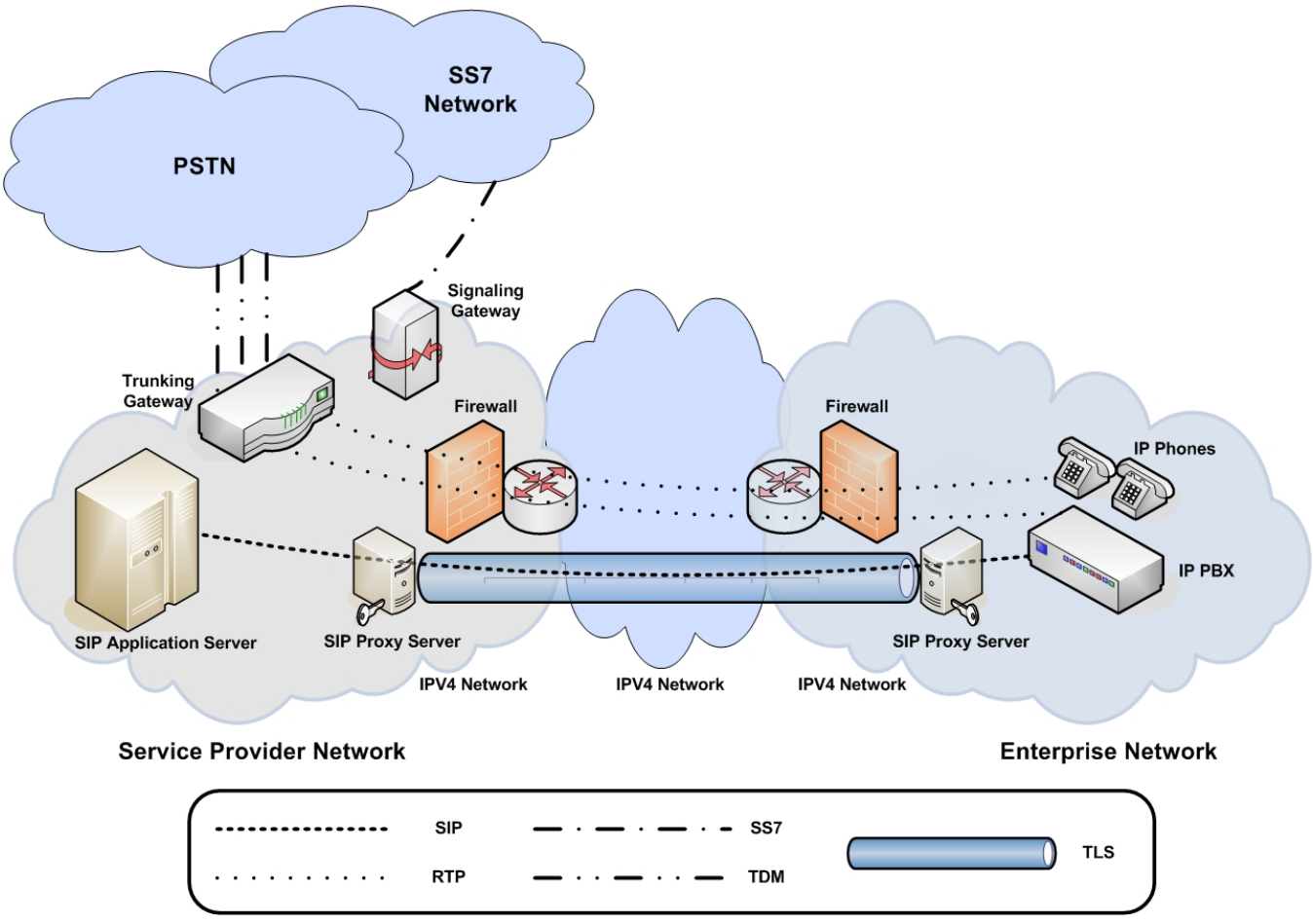
2 Conventions and Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [1].

3 Reference Architecture

The following reference diagram outlines the common functional elements required to support the interface specification outlined by this document. It is important to note that this specification treats these elements as separate physical components for the purposes of illustration only. It is perfectly acceptable for an equipment manufacturer to combine one or more of these functions into a single physical device.

For example, a manufacturer may choose to integrate the SIP Proxy Server function with the IP PBX function whereas another manufacturer may choose to integrate the SIP Proxy Server, IP PBX, and Firewall functions. Both implementations (as well as other combinations thereof) are equally conformant as long as they fully adhere to the individual rules governing each of the integrated functions.



C. Sibley (Editor)
Cbeyond
C. Gatch (Editor)
Cbeyond

4 Definitions

IP PBX (PBX) – The IP PBX constitutes an Enterprise's collection of network elements that provides packetized voice call origination and termination services using SIP for signaling and RTP for media traffic. The definition of an IP PBX for the purposes of this specification includes any "hard wired" (physically connected) phones as well as any IP Phones under the IP PBX System's control (see "IP Phones" below).

IP Phones – IP Phones are devices that are capable of originating and terminating packetized voice calls using the Enterprise's IP PBX. For the purposes of this specification, IP Phones are considered part of the IP PBX System itself and are therefore subject to the same overall requirements.

SIP Application Server (SAS) - The SIP Application Server is a server or group of servers within the Service Provider's network that provides PSTN call origination / termination services to Enterprises using SIP.

SIP Proxy Server (SPS) - The SIP Proxy Server is a server or group of servers that provides SIP message routing and TLS termination services at the Service Provider and Enterprise network edges.

Signaling Gateway (SGW) – The Signaling Gateway performs translation of SIP signaling to SS7 signaling.

Trunking Gateway (TGW) – The Trunking Gateway interfaces with PSTN switches and converts packetized voice samples to TDM voice samples.

Firewall – The Firewall provides packet filtering and general security services at the Service Provider and Enterprise network edges.

Interactive Connectivity Establishment (ICE) – ICE provides a mechanism for NAT traversal using various techniques such as STUN and TURN. In particular, it is used to allow SIP-based VoIP clients to successfully traverse the variety of NAT types that may exist between a remote user and a network.

Simple Traversal of UDP over NATs (STUN) – STUN allows clients behind NAT (or multiple NATs) to determine its public address, the type of NAT it is behind and the Internet-side port associated by the NAT with a particular local port.

Traversal using Relay NAT (TURN) – TURN allows clients behind NAT (or multiple NATs) to receive incoming data over TCP or UDP connections. It is most commonly used for elements behind symmetric NATs or firewalls that wish to be on the receiving end of a connection to a single peer.

Application Layer Gateway (ALG) – An Application Layer Gateway (ALG) modifies IP addresses and port numbers inside the payload of IP packets even when the corresponding IP packets are not addressed to the ALG. SIP ALGs do not follow the rules necessary to conform to any SIP role, for example, most SIP ALGs do not insert a 'Via:' header.

IPv4 Network – The IPv4 network constitutes a combination of the physical and logical elements (i.e. circuits, routers, switches, etc.) required to route and/or switch IPv4 packets between the Service Provider and Enterprise network edges.

C. Sibley (Editor)
Cbeyond
C. Gatch (Editor)
Cbeyond

5 Key Assumptions and Limitations of Scope

This recommendation lists a number of IETF and ITU-T specifications that should be utilized to meet the requirements for interconnection between a Service Provider and an Enterprise IP PBX. Note that it is not a profile of SIP. Users of this recommendation **MUST NOT** assume that a particular feature or option listed as mandatory in this document is supported by another user. Instead, all normal SIP extension and negotiation mechanisms (e.g. Supported, Require, Allow, etc.) M**UST** continue to be used. Failure to do this will lead to interoperability problems.

The following key assumptions have been made with regards to this interface specification:

1. The primary service to be delivered over this interface is audio-based PSTN call origination and/or termination. The delivery of any other service (e.g. video-based services, instant messaging, etc.) is out of scope.

2. All mandatory reference architecture elements specified for the Service Provider and Enterprise Networks are in place and operational.

3. Signaling considerations between the SIP Application Server, Trunking Gateway, and Signaling Gateway is outside the scope of this document.

4. Signaling considerations between the IP PBX and other Enterprise devices (e.g. IP phones) is outside the scope of this document.

5. The Service Provider and Enterprise each operate publicly accessible DNS servers that are authoritative for one or more Internet domain(s). Alternatively, the Service Provider may delegate a sub-domain from its domain for use by the Enterprise.

6. The Enterprise network is assigned a minimum of one E.164 address, which is routed on the PSTN to the Service Provider's Signaling Gateway.

7. Emergency calling issues, for example routing to national emergency numbers such as 911, 112, 999, or 000, issues related to SIP endpoint mobility, etc. are outside the scope of this document.

8. Layer 3 network design, QoS considerations, and preconditions (e.g. RSVP) are outside of the scope of this document

9. Element management, network management, network security, and OSS considerations are outside the scope of this document.

C. Sibley (Editor)
Cbeyond
C. Gatch (Editor)
Cbeyond

6 Standards Support

The interface specification described by this document requires network element support (as outlined below) of the functionality detailed in the following standards documents:

LEGEND	
M	MANDATORY (Send and Receive)
R	RECOMMENDED (Send and Receive)
R(RO)	RECOMMENDED (at minimum to Receive)
-	NOT REQUIRED / NOT APPLICABLE

Standard ID	Description	SAS	PBX	SPS
Rec. E.164 [2]	ITU-T Recommendation E.164: The international public telecommunication numbering plan	M	M	-
RFC 2246 [3]	The TLS Protocol Version 1.0	-	-	M
RFC 2833 [7]	RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals	-	M	-
RFC 2782 [6]	A DNS RR for specifying the location of services (DNS SRV)	-	-	M
RFC 3261 [8]	SIP: Session Initiation Protocol	M	M	M
RFC 3262 [9]	Reliability of Provisional Responses in Session Initiation Protocol (SIP)	M	R	-
RFC 3263 [10]	Session Initiation Protocol (SIP): Locating SIP Servers	M	M	M
RFC 3264 [11]	An Offer/Answer Model with Session Description Protocol (SDP)	M	M	-
RFC 3311 [12]	The Session Initiation Protocol (SIP) UPDATE Method	M	R	-
RFC 3323 [13]	A Privacy Mechanism for the Session Initiation Protocol (SIP)	M	R	M
RFC 3324 [14]	Short Term Requirements for Network Asserted Identity	M	R	M
RFC 3325 [15]	Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks	M	R	M
RFC 3489 [16]	STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)	-	R	-
RFC 3581 [18]	An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing	M	R	M
RFC 3725 [19]	Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)	M	R (RO)	-
RFC 4028 [21]	Session Timers in the Session Initiation Protocol (SIP)	R	R	-

C. Sibley (Editor)
Cbeyond
C. Gatch (Editor)
Cbeyond

7 Locating SIP Servers

7.1 Enterprise Requirements

The Enterprise **MUST** ensure the existence of a publicly-accessible DNS server that is authoritative for its domain (or a sub-domain delegated by the Service Provider for use by the Enterprise). This DNS server **SHOULD** support NAPTR resource records and **MUST** support SRV resource records.

Calls that are to be routed to the Service Provider's network for termination **MUST** be sent to the Enterprise SIP Proxy Server.

Enterprise SIP Proxy Servers **MUST** utilize DNS NAPTR and SRV queries as described in RFC 3263 [10] to determine the IP address, transport protocol, and port number of the SIP Proxy Server(s) associated with the Service Provider's domain name.

The PBX **MAY** register a contact address against one or more or more SIP URIs with the Service Provider's SIP Application Server. These URIs **MUST** be associated with the Service Provider's domain/realm.

7.2 Service Provider Requirements

The Service Provider **MUST** operate a publicly-accessible DNS server that is authoritative for its domain. This DNS server **SHOULD** support NAPTR resource records and **MUST** support SRV resource records.

Though not required, it is **RECOMMENDED** that Service Providers deploy redundant SIP Proxy Servers to service customer traffic. If redundant servers are deployed, the Service Provider **MUST** utilize the mechanism outlined in RFC 2782 [6] to return a prioritized list of contact information for the SIP Proxy Servers in DNS SRV resource records associated with the Service Provider's domain name.

Calls that are to be routed to the Enterprise's network for termination **MUST** be sent to the Service Provider's SIP Proxy Server.

Service Provider SIP Proxy Servers **MUST** utilize DNS NAPTR and SRV queries as described in RFC 3263 [10] to determine the IP address, transport protocol, and port number of the SIP Proxy Server(s) associated with the Enterprise network's domain name.

SIP Application Servers **MUST** be prepared to accept (but **MUST NOT** require) registrations for any valid URI that the Service Provider has assigned to an Enterprise. This interface specification does not define any specific action that is triggered by a successful registration; however one possible use of this information might be to update a DNS entry associated with the PBX in a DNS zone managed by the Service Provider.

C. Sibley (Editor)
Cbeyond
C. Gatch (Editor)
Cbeyond

8 Signaling Security

SIP Proxy Servers **MUST** support Transport Layer Security (TLS) as described in RFCs 2246 [3] and 3261 [8].

All SIP signaling exchanged between the Service Provider and Enterprise SIP Proxy Servers **MUST** be secured using TLS.

The TLS connection **MUST** be able to be established by both the Service Provider's and Enterprise's SIP Proxy Server.

SIP Proxy Servers **MUST** utilize a verifiable digital certificate to secure the TLS session.

SIP Proxy Servers **MUST** use canonical hostnames in any 'Via:' and/or 'Route:' SIP header field that it inserts in the SIP message.

Certificates used to establish a TLS connection **MUST** be verified and **MAY** be validated. Verification steps include verifying that the certificate has not expired, that the issuing certification authority is one the SIP Proxy Server trusts, and finally that the subject of the certificate matches the host portion of the target URI. Validation steps include checking the status of the certificate as well as the status of all the certificates in the certificate chain using CRLs or other mechanisms such as OCSP.

Enterprise certificates that are not signed by a trusted third party certification authority (i.e. self-signed certificates) **MAY** be used if permitted by the Service Provider's local security policy. Service Provider certificates **SHOULD** be signed by a third party certification authority.

9 Firewall and NAT Traversal

Any IP address contained within the headers and message bodies (e.g. SDP) of SIP messages exchanged between the Service Provider and Enterprise networks **MUST** be a publicly routable address.

This requirement implies that any "fix up" functions required for NAT traversal have already been performed either by the device originating the message (e.g. using STUN/TURN/ICE, static configuration, etc.) or by another network element (e.g. SIP-aware firewall, Session Border Controller, etc.) before the message is permitted to exit the Service Provider / Enterprise network edge.

SIP intermediaries **MUST NOT** modify IP addresses or port numbers in the body or Contact header of any message if any of the following are true:

- Any "application/sdp" body in the message contains any "a=candidate:" lines (indicating use of the ICE extension)
- All the "c=" lines in any "application/sdp" bodies contain only public IP addresses (indicating that another element has already ensured the addresses are correct).

C. Sibley (Editor)
Cbeyond
C. Gatch (Editor)
Cbeyond

10 Authentication and Accounting

10.1 Authentication of the Enterprise by the Service Provider

Authentication of the Enterprise by the Service Provider can be performed in one of two ways. PBX systems **MUST** implement Option 1 and **MAY** implement Option 2.

SIP Application Servers **MUST** support both Option 1 and Option 2 in order to ensure interoperability with all PBX systems.

10.1.1 Option 1: Authentication using TLS Credentials

The first method relies on authorization of the identity asserted by the Enterprise's verified certificate used to establish the TLS connection with the Service Provider's SIP Proxy Server.

This model requires that the Service Provider's SIP Proxy Server and SIP Application Server be capable of exchanging authorization, accounting, and usage information on a per-call basis in order to ensure complete billing traceability through the network. When this model is utilized, information identifying the Enterprise is extracted from the Enterprise's certificate (for example, domain name) by the SIP Proxy Server and conveyed to the "downstream" device as necessary. (It is out of the scope of this interface specification to specify the actual mechanism used to convey this information within the Service Provider's Network.)

10.1.2 Option 2: Digest Access Authentication

The second method of authenticating an Enterprise utilizes the digest authentication scheme as described in section 22.4 of RFC 3261 [8]. In this model the Service Provider assigns the Enterprise Network a username and password (referred to as a "Network Account" hereafter) that is valid within the Service Provider's domain (realm). It is important to note that if the digest authentication scheme is employed, it does not eliminate the requirement to utilize TLS between the Service Provider and Enterprise Network SIP Proxy Servers.

When this model is employed, the following rules must be observed:

1. When processing an INVITE request from an unauthenticated PBX, the SIP Application Server **MUST** challenge the message, only accepting authentication credentials that are valid within its realm.

2. When processing a REGISTER request from an unauthenticated PBX, the SIP Application Server **MUST** challenge the message, only accepting authentication credentials that are valid within its realm.

3. When challenged by the SIP Application Server, the PBX **MUST** respond with authentication credentials that are valid within the Service Provider's realm (i.e. the network account username and password supplied by the Service Provider).

4. In order to avoid unnecessary challenges, the PBX **SHOULD** include its authentication credentials using the current nonce in each request sent to the SIP Application Server.

10.2 Authentication of the Service Provider by the Enterprise

Authentication of the Service Provider by the Enterprise is not explicitly required by this interface specification, however it is **RECOMMENDED**. If the Enterprise chooses to do so, it **MUST** be performed using the identity conveyed in the certificate used by the Service Provider's SIP Proxy Server to establish the TLS connection with the Enterprise Network's SIP Proxy Server.

11 Enterprise PSTN Identities

This specification considers a single E.164 address equivalent to a single "PSTN identity." Accordingly, a PBX with 100 assigned telephone numbers would have 100 associated PSTN identities.

The PBX **MUST** choose which of its valid PSTN identities to use on a per-call basis. For example, on a call from a user without a dedicated telephone number (i.e. DID number) the PBX might choose to assert its "main" identity (e.g. the company's main business number), while a call from a user with a dedicated DID number would use the identity of that user's specific telephone number.

Obviously at some point a translation between an E.164 address on the PSTN and an Enterprise's SIP URI will need to be performed. This requirement implies that the SIP Application Server **MUST** maintain an E.164 address ←→ Enterprise domain mapping table that is used to perform routing decisions for calls received from the PSTN.

While not required by this interface specification, it is important to note that a SIP Application Server **MAY** support a more granular mapping scheme as well (e.g. E.164 address ←→ specific Enterprise URI). It should also be noted that this mapping function does not necessarily need to be collocated on or a function of the SIP Application Server; for example, an external ENUM database (RFC 3761 [20]) could perform this function.

12 Enterprise URI Formatting and Addressing Rules

Any device that handles signaling **MUST** support addressing for closed (fixed length) and open (variable length) numbering plans.

12.1 'From:' Field

This interface specification provides two methods of communicating the PBX's desired PSTN identity to the Service Provider's SIP Application Server.

PBX systems **MUST** implement Option 2 and **SHOULD** implement Option 1. Option 1 is the preferred method and **SHOULD** be utilized if the PBX supports it.

SIP Application Servers **MUST** support both Option 1 and Option 2 in order to ensure interoperability with all PBX systems.

12.1.1 Option 1: Utilizing the 'From:' and 'P-Asserted-Identity:' SIP Header Fields

The first method for communicating PSTN identity information utilizes the 'From:' field in conjunction with the 'P-Asserted-Identity:' field as described in RFC 3325 [15]. This method allows the Enterprise to deliver a "public" and "private" PSTN identity to the Service Provider per call. The public identity represents the identity that the Enterprise wants to deliver to the PSTN for a given call. The private identity represents the identity that the Enterprise wants to deliver to the Service Provider for a given call.

When this method is used, the 'From:' field is populated with the Enterprise's desired public identity (e.g. the company or department's main business number) or an anonymous URI as described in RFC 3323 [13]. The caller's private identity information is provided to the Service Provider by utilizing the 'P-Asserted-Identity:' and 'Privacy:' SIP header fields as described in RFC 3325 [15]. It is important to note that SIP Application Servers **MUST ONLY** use any provided private identity information to provide services and/or features that the Enterprise has subscribed to for that identity.

For the purposes of this specification, the Enterprise SIP Proxy Server is considered part of the Service Provider's "Trust Domain", as defined in RFC 3325 [15]. When the SIP Application Server routes the call to any network element in the Service Provider's network that does not support RFC 3325 [15], it **MUST** consider the network element to be outside of its Trust Domain. Per RFC 3325 [15], this means that the SIP Application Server **MUST NOT** disclose or otherwise pass any information contained in the 'P-Asserted-Identity:' header field to that network element. In addition, the SIP Application Server **MUST** remove any 'P-Asserted-Identity:' SIP header fields and the SIP header field requesting privacy.

When this method is used, the PBX **MUST** format all INVITES sent to the Service Provider according to the following rules:

1. The PBX **MUST** populate the 'From:' field with the URI that is associated with its desired public PSTN identity or an anonymous URI in the form <anonymous@[domain name]>. The PBX **SHOULD** also provide any applicable display name information (e.g. "Acme Rockets Sales Department").

2. The PBX **MUST** include a SIP 'Privacy:' header field that requests "id" privacy as defined in RFC 3325 [15].

3. The PBX **MUST** populate the 'P-Asserted-Identity:' SIP header field with one of the options below (listed in order of preference):

    a. The PBX caller's telephone number in ITU-T E.164 format [2] + Enterprise domain name and (optional) desired display name information.

    For example:

    INVITE sip:+17705551211@serviceprovider.net;user=phone SIP/2.0
    Via: SIP/2.0/UDP useragent.acmerockets.com:5060;branch=z9hG4bKl54j1
    From: "Acme Rockets Sales" <sip:+16789901234@acmerockets.com;user=phone>;tag=1648468
    To: <sip:+17705551211@serviceprovider.net;user=phone>
    Call-ID: 502848105829482738
    CSeq: 1 INVITE
    Max-Forwards: 70
    Privacy: id
    P-Asserted-Identity: "John Doe" <sip:+16789902000@acmerockets.com;user=phone>

b. Other RFC-3261-compliant [8] URI format agreed upon by the Service Provider and customer.

For example:

INVITE sip:+17705551211@serviceprovider.net;user=phone SIP/2.0
Via: SIP/2.0/UDP useragent.acmerockets.com:5060;branch=z9hG4bK9kj2b
From: "Acme Rockets Sales" <sip:sales@acmerockets.com>;tag=0323873
To: <sip:+17705551211@serviceprovider.net;user=phone>
Call-ID: 830284710729349284
CSeq: 1 INVITE
Max-Forwards: 70
Privacy: id
P-Asserted-Identity: "John Doe" <sip:johndoe@acmerockets.com>

12.1.2 Option 2: Utilizing the 'From:' SIP Header Field only

The second method for passing Enterprise PSTN identity information uses the 'From:' field described in RFC 3261 [8]. This method provides less overall flexibility due to the fact that it allows only one identity to be conveyed to the Service Provider on a given call. When this method is used, the single identity is used by the Service Provider as both the "public" and "private" PSTN identities for the call.

When using this method, the following requirements **MUST** be observed:

1. The 'From:' field **MUST** contain a SIP URI containing the PBX's desired PSTN identity for the PBX caller. In the event the PBX caller does not have its own PSTN identity, the main PSTN identity of the PBX **SHOULD** be used to populate the 'From:' field. If available, the PBX **SHOULD** also provide any applicable display name information (e.g. "John Doe", "Acme Rockets").

2. The format of the 'From:' field **MUST** be expressed as one of the following two options (listed in order of preference):

   a. ITU-T E.164 format [2] + Enterprise domain name.

   For example:

   INVITE sip:+17705551211@serviceprovider.net;user=phone SIP/2.0
   Via: SIP/2.0/UDP useragent.acmerockets.com:5060;branch=z9hG4bK-a111
   From: "John Doe" <sip:+16789905555@acmerockets.com;user=phone>;tag=9802748
   To: <sip:+17705551211@serviceprovider.net;user=phone>
   Call-ID: 245780247857024504
   CSeq: 1 INVITE
   Max-Forwards: 70

b. Other RFC-3261-compliant [8] URI format agreed upon by the Service Provider and Enterprise.

For example:

INVITE sip:+17705551211@serviceprovider.net;user=phone SIP/2.0
Via: SIP/2.0/UDP useragent.acmerockets.com:5060;branch=z9hG4bKk3s12
From: "John Doe" <sip:johndoe@acmerockets.com>;tag=9315428
To: <sip:+17705551211@serviceprovider.net;user=phone>
Call-ID: 096398618493230967
CSeq: 1 INVITE
Max-Forwards: 70

12.2 'To:' Field – PSTN Destinations

This interface specification provides two methods of communicating the PBX's destination (dialed) E.164 address to the Service Provider's SIP Application Server. PBX systems **MUST** implement at least one of these options. SIP Application Servers **MUST** support both methods in order to ensure interoperability with all PBX systems.

12.2.1 Option 1: SIP URI

*To: <sip:+**[E.164 Address] @[Service Provider Domain Name]**;user=phone>*

12.2.2 Option 2: tel: URL

*To: <tel:+**[E.164 Address]** >*

12.3 'To:' Field – Emergency Services Destinations

While not explicitly required by this interface specification, it is **RECOMMENDED** that the Service Provider support the termination of emergency services calls for one or more fixed physical locations serviced by the Enterprise PBX. For each such physical location, the Enterprise and Service Provider **SHOULD** mutually agree upon an E.164 address that will be used when an emergency services call is made from that location. This E.164 address **SHOULD** be used for routing the call to the appropriate Public Safety Answering Point (PSAP) as well as for providing any required emergency location information to the PSAP.

The PBX **SHOULD** format the 'To:' field as follows when an emergency services call is made:

*To: <sip:**[Country-specific emergency services address]**;phone-context=**[Predetermined Geographic E.164 Address]@[Service Provider Domain Name]** ;user=phone>*

The country-specific emergency services address is defined as the dial string used in the country of origin to request emergency services. The phone-context parameter **SHOULD** contain a valid E.164 address previously agreed upon by the

Enterprise and Service Provider to represent the physical location from which the call originated. The Service Provider **SHOULD** ensure that valid location information for this E.164 address is provisioned in the ALI database.

For example, an emergency services call originating in the United States with a Geographic E.164 address of +16789901234 would be formatted as follows:

*To: <sip:**911**;phone-context=**+16789901234@serviceprovider.net**;user=phone>*

It is important to note that this interface specification defines no particular behavior that should be taken by the Service Provider in the event a valid E.164 address is not supplied. Accordingly, the Enterprise **SHOULD** ensure that no emergency services calls are sent to the Service Provider without a valid geographic E.164 address.

12.4 'To:' Field -- Other Destinations

While this interface specification defines no particular call handling behavior for URI formats other than those described above, the SIP Proxy Server and SIP Application Server **SHOULD** support any URI format that conforms to RFC 3261[8].

12.5 Request-URI

The initial Request-URI of any SIP message generated by an IP PBX system **MUST** adhere to the same formatting rules as that of the 'To:' field described in sections 12.2, 12.3, and 12.4 above.

13 Service Provider URI Formatting and Addressing Rules

13.1 'From:' Field

If the PSTN caller has supplied their E.164 address and did not request calling number privacy, SIP Application Servers **MUST** populate the 'From:' field with the E.164 address of the PSTN caller + Service Provider domain name as shown below. If any display name information is available and has not been restricted for delivery, it **SHOULD** also be provided.

From: "Acme Rockets" <sip:+15616261234@serviceprovider.net;user=phone>;*tag=5320917*

If the PSTN caller has not supplied their E.164 address or has requested calling number privacy, the following anonymous URI **MUST** be populated in the 'From:' field:

From: "Anonymous" <anonymous@[domain name]> ;*tag=0728361*

13.2 'To:' Field

The SIP Application Server **MUST** populate the 'To:' field with the Enterprise PSTN identity associated with the dialed E.164 address + Enterprise domain name as shown below:

To: <sip:+16789901234@acmerockets.com;user=phone>

13.3 Request-URI

The initial Request-URI of any SIP message generated by a SIP Application Server **MUST** adhere to the same formatting rules as that of the 'To:' field described in section 13.2 above.

14 Quality of Service Considerations

IP Packets containing SIP signaling messages or RTP voice samples **MUST** be marked with a predefined value in the packet header before being sent to the peer's network. This provides the Service Provider and Enterprise with a standard mechanism for identifying and prioritizing voice-related packets at the edge and in the core of their packet networks.

In order to accomplish this goal, the interface specification outlined by this document requires the use of the Differentiated Services Field as specified in RFC 2474 [5]. The following IP packet marking values are **RECOMMENDED** for use between the Enterprise and Service Provider network edges.

Packet Type	DiffServ PHB	DSCP Value	Binary Equivalent Value
SIP Signaling Message	CS5	40	Binary = 101000
RTP Media	EF	46	Binary = 101110

15 Media Attributes and Minimum Requirements

15.1 Media Capability Negotiation

Any device that originates and/or terminates RTP traffic **MUST** utilize the Session Description Protocol (SDP) as described in RFC 2327 [4] in conjunction with the offer/answer model described in RFC 3264 [11] to exchange session information (IP address, port number, media type, send/receive mode, codec, DTMF mode, etc).

Any device that originates and/or terminates RTP traffic **MUST** include an attribute specifying the device's desired directionality (i.e. a=inactive/sendonly/recvonly/sendrecv) as described in RFC 3264 [11] for all media streams listed in an SDP offer or answer that is generated by the device.

Any device that originates and/or terminates RTP traffic **MUST** support the ability to receive SDP session descriptions that have the 'c=' field set to all zeros (0.0.0.0).

15.2 Codec Support and Media Transport

Voice samples **MUST** be transported using the real-time transport protocol (RTP) as described in RFC 3550 [17].

Any device that originates and/or terminates RTP traffic over UDP **MUST** use the same UDP port for sending and receiving session media (i.e. symmetric RTP.)

Any device that originates and/or terminates RTP traffic **SHOULD** be capable of processing RTP packets with different packetization rate than the one used for sending.

Any device that originates and/or terminates voice traffic **MUST** minimally support the ITU-T G.711 u-Law and G.711 A-Law PCM codecs with a packetization rate of 20 ms.

Any device that originates and/or terminates voice traffic **MUST** support the ability to convert between G.711 A-Law to G.711 u-Law (by the u-Law end).

Voice Activity Detection (VAD) and any other techniques that require mutual modification (e.g. comfort noise generation) of media content **SHOULD** be avoided where possible.

15.3 Transport of DTMF Tones

Trunking Gateways **MUST** support the ability to transport DTMF tones in-band when using the G.711 codec. Trunking Gateways **MUST** also support the ability to transport DTMF tones using the RTP telephone-event payload format as described in RFC 2833 [7] when using any codec.

Any Enterprise device that originates and/or terminates voice traffic **MUST** support at least one of the above two methods for transporting DTMF tones (with RFC 2833 [7] DTMF Relay being the preferred method).

15.4 Echo Cancellation

Any device that originates and/or terminates voice traffic **MUST** provide ITU-T G.168 compliant echo cancellation.

Any device that supports fax and/or modem transmissions **MUST** recognize in-band 2100 Hz tones (+/- 15 Hz) in conjunction with phase reversals at 450 ms intervals (+/- 25 ms). Upon detection of this tone, echo cancellation **MUST** be disabled and remain disabled for the duration of the call or until one of the following events occurs:

1. No single-frequency sinusoid is present as defined in Section 7 of G.168.
2. The end of the call is detected.
3. The end of data transmission is detected by the lack of modem or fax tones on the channel.

15.5 Fax and Modem Calls

When performing in-band transport of fax or modem calls, any device that supports fax and/or modem transmissions **MUST** upon recognition of a 2100 Hz tone (+/- 15 Hz) tone:

1. Switch the active codec in use on the call to G.711 (if a codec other than G.711 was previously in use).
2. Disable the high pass filter.
3. Disable voice activity detection (VAD) and comfort noise generation (CNG).
4. Switch from any adaptive/dynamic jitter buffer in use to a fixed-length jitter buffer. (A **RECOMMENDED** depth of 200-ms is suggested when switching to a fixed-length jitter buffer.)

Renegotiation of the session media attributes **MUST** be performed using the SIP reINVITE request as described in RFC 3261 [8] or the SIP UPDATE request as described in RFC 3311 [12].

Superior performance of fax transmissions over packet networks can be achieved by utilizing the ITU-T T.38 [22] fax relay specification (as opposed to in-band transport). In-band fax transmissions are especially problematic over packet networks, especially for calls that traverse the public Internet or other network that doesn't offer adequate QOS. Accordingly, it is **RECOMMENDED** that Enterprise devices utilize T.38 fax relay when possible.

Trunking Gateways **MUST** support the ITU-T T.38 [22] specification and Enterprise devices **SHOULD** support the specification. It is important to note that steps 1-4 outlined above for in-band transport of fax/modem calls do not apply, to fax calls only, for implementations utilizing T.38 fax relay.

16 PSTN Interactions

16.1 Call Progress Tones

PBX systems **MUST** locally generate call progress tones in response to the following subset of standard SIP response codes. Selection of the particular tone is left to the equipment manufacturer's discretion.

SIP Response Code
180 Ringing
400 Bad Request
403 Forbidden
404 Not Found
408 Request Timeout
480 Temporarily Unavailable
482 Loop Detected
483 Too Many Hops
486 Busy Here
500 Server Internal Error
503 Service Unavailable
504 Server Time-out
600 Busy Everywhere
604 Does Not Exist Anywhere

In addition to the response codes outlined above, PBX systems **SHOULD** generate some form of call progress tone for the remaining set of standard SIP response codes (where a call progress tone is applicable). Selection of the particular tone is left to the equipment manufacturer's discretion.

16.2 Early Media

In order to support delivery of in-band announcements and call progress tones, upon receipt of SDP information in any '183 Session Progress', '200 OK', or '202 Accepted' message the PBX **MUST** immediately disable any locally generated call progress tones and cut-through the early media to the end-user as described in RFC 3261 [8].

After sending an SDP offer, the IP PBX **MUST** be prepared to receive media on all offered "recvonly" or "sendrecv" transport protocol / transport port / codec (media stream) combinations. Upon receipt of media on any such media stream, the PBX **MUST** immediately disable any locally generated call progress tones and cut-through the early media to the end-user as described in RFC 3261 [8].

17 References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[2] International Telecommunications Union, "Recommendation E.164: The international public telecommunication numbering plan", May 1997, <http://www.itu.int>.

[3] T. Dierks, C. Allen, “The TLS Protocol Version 1.0”, RFC 2246, January 1999.

[4] M. Handley, V. Jacobson, “SDP: Session Description Protocol”, RFC 2327, April 1998.

[5] K. Nichols, S. Blake, F. Baker, D. Black, “Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers”, RFC 2474, December 1998.

[6] A. Gulbrandsen, P. Vixie, L. Esibov, “A DNS RR for specifying the location of services (DNS SRV)”, RFC 2782, February 2000.

[7] H. Schulzrinne, S. Petrack, “RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals”, RFC 2833, May 2000.

[8] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[9] J. Rosenberg, H. Schulzrinne, “Reliability of Provisional Responses in Session Initiation Protocol (SIP), RFC 3262, June 2002.

[10] J. Rosenberg, H. Schulzrinne, “Session Initiation Protocol (SIP): Locating SIP Servers”, RFC 3263, June 2002.

[11] J. Rosenberg, H. Schulzrinne, “An Offer/Answer Model with Session Description Protocol (SDP)”, RFC 3264, June 2002.

[12] J. Rosenberg, “The Session Initiation Protocol (SIP) UPDATE Method”, RFC 3311, October 2002.

[13] J. Peterson, “A Privacy Mechanism for the Session Initiation Protocol (SIP)”, RFC 3323, November 2002.

[14] M. Watson, “Short Term Requirements for Network Asserted Identity”, RFC 3324, November 2002.

[15] C. Jennings, J. Peterson, M. Watson, “Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks”, RFC 3325, November 2002.

[16] J. Rosenberg, J. Weinberger, C. Huitema, R. Mahy, “STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)”, RFC 3489, March 2003.

[17] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, “RTP: A Transport Protocol for Real-Time Applications”, RFC 3550, July 2003.

[18] J. Rosenberg, H. Schulzrinne, “An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing”, RFC 3581, August 2003.

[19] J. Rosenberg, J. Peterson, H. Schulzrinne, G. Camarillo, “Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)”, RFC 3725, April 2004.

[20] P. Faltstrom, M. Mealling, “The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)”, RFC 3761, April 2004.

[21] S. Donovan, J. Rosenberg, “Session Timers in the Session Initiation Protocol (SIP)”, RFC 4028, April 2005.

[22] International Telecommunications Union, "Recommendation T.38: Procedures for real-time Group 3 facsimile communication over IP networks ", September 2005, <http://www.itu.int>.

C. Sibley (Editor)
Cbeyond
C. Gatch (Editor)
Cbeyond

18 Changes

In Section 12.1.1, 2nd paragraph, “or an anonymous URI as described in RFC 3261 [8].” was replaced with “or an anonymous URI as described in RFC 3323 [13]
.
In Section 12.1.1 “The PBX MUST populate the ‘From:’ field with the URI that is associated with its desired public PSTN identity or an anonymous URI. The PBX SHOULD also provide any applicable display name information (e.g. “Acme Rockets Sales Department”).” was replaced with ”The PBX MUST populate the ‘From:’ field with the URI that is associated with its desired public PSTN identity or an anonymous URI in the form <anonymous@[domain name]>. The PBX SHOULD also provide any applicable display name information (e.g. “Acme Rockets Sales Department”).”

In Section 13.1 “If the PSTN caller has not supplied their E.164 address or has requested calling number privacy, one of the following two anonymous URIs MUST be populated in the ‘From:’ field:

From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=0728361

From: "Anonymous" <anonymous@[domain name]> ;tag=0728361”

was replaced with “If the PSTN caller has not supplied their E.164 address or has requested calling number privacy, the following anonymous URI MUST be populated in the ‘From:’ field:

From: "Anonymous" <anonymous@[domain name]> ;tag=0728361”

19 Contributors and Contact Information

Chris Sibley (editor)
Cbeyond
320 Interstate N Pkwy
Atlanta, GA 30339
USA
tel:+1-678-424-2693
sip:csibley@engsip.cbeyond.net
mailto: chris.sibley@cbeyond.net

Chris Gatch (editor)
Cbeyond
320 Interstate N Pkwy
Atlanta, GA 30339
USA
tel:+1-678-424-2406
mailto: chris.gatch@cbeyond.net

François Audet
Nortel Networks
4655 Great America Parkway
Santa Clara, CA 95054
USA
mailto:audet@nortel.com

Jay Batson
SIP Forum
mailto: batsonjay@sipforum.org

Rob Brown
Talkswitch
1545 Carling Avenue Suite 510
Ottawa, Ontario
Canada K1Z 8P9
mailto: rbrown@talkswitch.com

Vikas Butaney
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134
USA
mailto: vbutaney@cisco.com

Yuan Cai
Cisco Systems, Inc.
170 West Tasman Dr.

San Jose, CA 95134
USA
mailto: yuanca@cisco.com

Klaus Darilion
enum.at
mailto: klaus.darilion@enum.at

Jim Davies
Mitel Networks
350 Legget Drive
P.O. Box 13089
Kanata, ON
Canada K2K 2W7
mailto: jim_davies@mitel.com

Alex Doyle
BroadSoft, Inc.
220 Perry Parkway
Gaithersburg, MD 20877
USA
mailto: alex@broadsoft.com

John Elwell
Siemens AG
mailto: john.elwell@siemens.com

Sonya Fullarton
Mitel Networks
350 Legget Drive
P.O. Box 13089
Kanata, ON
Canada K2K 2W7
mailto: sonya_fullarton@mitel.com

Scott Hoffpauir
BroadSoft, Inc.
220 Perry Parkway
Gaithersburg, MD 20877
USA
mailto: scott@broadsoft.com

Ernst Horvath
Siemens AG
mailto: ernst.horvath@siemens.com

Alan Johnston
Avaya, Inc.

mailto: ajohnston@tello.com

Paul Kyzivat
Cisco Systems, Inc.
mailto: pkyzivat@cisco.com

Matthew Lazaro
Avaya, Inc.
211 Mt. Airy Road
Basking Ridge, NJ 07920
USA
mailto: mlazaro@avaya.com

Rohan Mahy
SIP Edge LLC
mailto: rohan@ekabal.com

Joanne McMillen
Avaya, Inc.
mailto: joanne@avaya.com

Francois Menard
Xit Telecom
mailto: fmenard@xittelecom.com

David R. Oran
Cisco Systems, Inc.
mailto: oran@cisco.com

Rick Ringel
Inter-Tel, Inc.
mailto: Rick_Ringel@inter-tel.com

Richard Shockey
NeuStar, Inc.
mailto: Rich.Shockey@neustar.biz

Henry Sinnreich
Pulver.com
mailto: henry@pulver.com

David Sauerhaft
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134
USA
mailto: dsauerha@cisco.com

C. Sibley (Editor)
Cbeyond
C. Gatch (Editor)
Cbeyond

20 Full Copyright Statement