

SIP-PBX / Service Provider Interoperability *(draft name goes here)*

“SIPconnect 1.1 Technical Recommendation”

Abstract

The SIPconnect 1.1 Technical Recommendation outlines an interface specification that enables direct connectivity 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.

Comment [JohnE1]: I thought we agreed to delete these words.

SIPconnect 1.1 effectively obsoletes SIPconnect 1.0. Where SIPconnect 1.0 focused primarily on basic network registration, identity/privacy management, call originations and call terminations – this version will provide additional guidance on advanced service inter-working – including, but not limited to, voicemail, call transfer, caller id, etc.

Where appropriate, recommendations from SIPconnect 1.0 have been left unchanged, although some modifications to prior recommendations have been made based on experience and feedback gathered through adoption of SIPconnect 1.0 in the industry.

Notes and Key Questions from the Editor

(Note: text in blue italics is from Spencer Dawkins, who’s acting as editor for this specification.)

Status of this Memo

Post-face-to-face-meeting draft of SIPconnect 1.1 (v01), containing restructures and section-level text submissions.

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



SIPconnect and SIPconnect Compliant are certification marks of the SIP Forum. Implementers who wish to certify their products and services as SIPconnect Compliant 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.

Table of Contents

1	Introduction	5
2	Conventions and Terminology	6
3	Reference Architecture.....	6
4	Definitions.....	8
5	Key Assumptions and Limitations of Scope	8
6	Standards Support	9
7	Modes of Operation.....	9
7.1	Registration Mode	9
7.1.1	Locating SIP Servers.....	9
7.1.2	Signaling Security	10
7.1.3	Firewall and NAT Traversal	11
7.1.4	Registration	12
7.1.5	Failover and Recovery after Registration.....	15
7.1.6	Authentication, Authorization and Accounting.....	15
7.2	Static Mode.....	16
7.2.1	Locating SIP Servers.....	16
7.2.2	Signaling Security	18
7.2.3	Firewall and NAT Traversal	18
7.2.4	Failover and Recovery	19
7.2.5	Authentication, Authorization and Accounting.....	19
8	Supported Signaling Transport Protocols.....	19
9	Enterprise Public Identities	19
10	Establishing Basic 2-Way Calls	20
10.1	Incoming Calls from the Service Provider to the Enterprise	20
10.1.1	Populating the Request-URI header.....	20
10.1.2	Populating the To header	21
10.1.3	Populating the Route header	21
10.1.4	Populating the From Header	21
10.1.5	Populating the P-Asserted-Identity Header.....	21
10.2	Outgoing Calls from the Enterprise to the Service Provider	22
10.2.1	Populating the Request-URI	22
10.2.2	Populating the To Header	23
10.2.3	Populating the P-Asserted-Identity header	23
10.2.4	Populating the P-Preferred-Identity header.....	24
10.2.5	Populating the From header	24
10.2.6	Identifying the Originating User.....	24
10.2.7	Controlling the Calling Line ID and Calling Name Presentation	25
11	Service Interactions	26
11.1	Retargeting Related Services.....	26
11.1.1	Simple 302 Redirection.....	26
11.1.2	Retargeting via In-Dialog REFER	27
11.1.3	Retargeting via Out-of-Dialog INVITE.....	28
11.2	Emergency Services	30
11.3	Session Limits.....	31
12	Section header retained for numbering	31
13	Section header retained for numbering	31
14	Media and Session Interactions	32

14.1	Media Capability Negotiation	32
14.2	Codec Support and Media Transport.....	32
14.3	Transport of DTMF Tones	33
14.4	Echo Cancellation.....	33
14.5	Fax and Modem Calls.....	33
14.6	Call Progress Tones.....	34
14.7	Ringback Tone and Early Media	34
14.8	Putting a Session on Hold.....	35
15	Section header retained for numbering	35
16	Additional Guidance	35
16.1	TLS.....	35
16.2	IPv6.....	35
16.3	UDP.....	35
17	References.....	37
18	Changes.....	40
19	Acknowledgements for SIPconnect/1.1 Initial Contributions.....	41
20	Contributors to SIPconnect/1.1 and Contact Information	41
21	Contributors to SIPconnect/1.0 and Contact Information	41
22	Full Copyright Statement	44

List of Figures

Figure 1	– Reference Architecture	6
Figure 2	– Retargeting using 302 Moved Temporarily Response	27
Figure 3	– Retargeting using REFER Request	28
Figure 4	– Retargeting using INVITE Request.....	29

1 Introduction

The Session Initiation Protocol (SIP) is fast becoming the dominant industry standard for signalling in support of VoIP or and other services. The deployment of SIP-enabled PBXs (SIP PBXs) among Enterprises of all sizes is increasing rapidly. Many new SIP-PBXs support SIP phones and SIP-based communication with other SIP-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 SIP-PBXs and SIP-enabled Service Providers.

- Deleted:** SIP-PBXs
- Deleted:** Additionally, Session Initiation Protocol, or SIP, is fast becoming the dominant industry standard.
- Deleted:** SIP routing
- Deleted:** between one or more PBXs

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 SIP-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 SIP-PBXs and SIP-enabled Service Providers. Note that this document does not preclude or discourage the negotiation of additional functionality.

Comment [JohnE2]: We should use either "SIP-enabled enterprise networks" or "SIP-PBXs" here.

SIPconnect 1.1 restates and in some cases updates all areas of implementation guidance found in SIPconnect 1.0, including:

- Specification of a reference architecture that describes the common network elements necessary for Service Provider to SIP-PBX peering for the primary purpose of 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 network elements.
- Specification of methods of formulating protocol messages where multiple legitimate implementation options exist.
- 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 compatibility.
- Specification of a basic set of guidelines for interfacing with an SIP-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 SIP-PBX.

Comment [JohnE3]: These bullets should be reviewed after the remainder of the document becomes stable.

This document provides additional implementation guidance related to service inter-working for topics added since SIPconnect/1.0, including:

- Transfer and Forwarding scenarios
- Calling Line Identity Presentation

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](#).

3 Reference Architecture

The reference architecture diagram in Figure 1 shows the common functional elements required to support the interface specification outlined by this document. The diagram shows two reference points between the Enterprise Network and the Service Provider Network; reference point (1) and reference point (2).

Reference point (1) carries SIP signaling messages to support voice services between the Enterprise Network SIP-PBX and the Service Provider network SIP Signaling Entity (SP-SSE).

Reference point (2) carries the RTP and RTCP packets between the Service Provider and enterprise Media Endpoints. An enterprise Media Endpoint could be the SIP-PBX itself, an IP-based user device (e.g., SIP phone) in the enterprise, or a media-relay device in the enterprise network. The Service Provider media endpoint could be a PSTN Gateway, an IP-based user endpoint device, a media server, or any other IP-based media-capable entity.

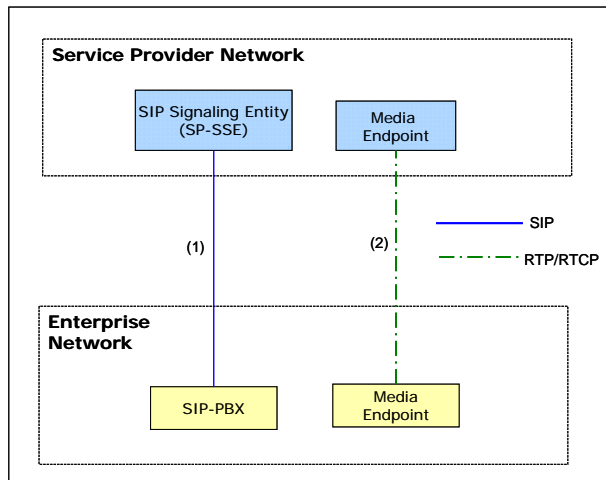


Figure 1 – Reference Architecture

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 a media endpoint with the corresponding signalling entity. For example, a manufacturer may choose to integrate the SIP-PBX, and Media Endpoint functions. Both integrated and non-integrated implementations are equally conformant as long as they fully adhere to the individual rules governing each of the defined functions.

Deleted: one or more of these functions into a single physical device

Note that many deployments will include a Network Address Translator (NAT) between the service provider network and the enterprise network. This document does not describe NATs as part of the SIPconnect/1.1 interface.

Note that a single SIP-PBX may serve media endpoints in a number of geographically-distributed locations.

4 Definitions

SIP-PBX (PBX) – The SIP-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.

Media Endpoint – Any entity that terminates an RTP/RTCP stream.

Service Provider SIP-Signaling Entity (SP-SSE) – the SP-SSE is the service provider’s point of SIP signaling interconnection with the Enterprise.

Comment [JohnE4]: I am not sure this is correct. In particular, this definition suggests that it includes media endpoint functions such as RTP. I would prefer a formulation more in line with that for SP-SSE, e.g. "The enterprise network's point of SIP signaling interconnection with the service provider. Also, do we really need "PBX" as an alias?"

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 SIP-PBX. Note that this document specifies a profile of SIP, with some media aspects. 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.) **MUST** 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 call origination and/or termination between the Enterprise and Service Provider network. The delivery of any other service (e.g. video-based services, instant messaging, etc.) is out of scope, except that service providers **MUST** accommodate unsupported (or even unrecognized) media types by passing the SDP media lines unchanged, and **SHOULD** pass unsupported (or even unrecognized) SIP headers and bodies.

Spencer: Need to move normative language into the body of the document?

2. All reference architecture elements specified for the Service Provider and Enterprise Networks are in place and operational.
3. Signaling considerations between the **SP-SSE** and other Service Provider devices (e.g. Trunking Gateway) is outside the scope of this document.
4. Signaling considerations between the SIP-PBX and other Enterprise devices (e.g. IP phones, **other SIP-enabled PBXs, non-SIP devices**) is outside the scope of this document.
5. 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.
6. Layer 3 network design, QoS considerations, and preconditions (e.g. RSVP) are outside of the scope of this document
7. Element management, network management, network security, and **OSS** considerations are outside the scope of this document.

Comment [JohnE5]: A SIP message comprises only a single header, which can contain multiple header fields. I think "header fields" is intended here. Also this is wrong elsewhere in the document (many places).

Comment [JohnE6]: Likewise I think "body parts" is intended here.

Deleted: SIP Application Server

Comment [JohnE7]: Isn't this covered elsewhere?

Comment [JohnE8]: All acronyms such as OSS, RSVP, QoS, etc. should be listed with their expansions somewhere.

6 Standards Support

This section will be filled out when the document is more mature.

7 Modes of Operation

This document describes two modes of operation for the SIP-PBX; the Registration mode and the Static mode.

In the Registration mode, the SIP-PBX plays a role similar to a subscriber endpoint device supporting multiple end-users. Unique aspects of this mode include:

- the SIP-PBX uses SIP registration procedures to obtain service from the Service Provider network,
- the SIP-PBX and Service Provider Network mutually authenticate each other using SIP Digest,
- SIP signaling between the SIP-PBX and Service Provider network is secured using TLS,
- NAT traversal is achieved using Outbound

In the Static mode, the Enterprise network appears as a peer network to the Service Provider network. Some unique aspects of this mode include:

- the Enterprise network uses DNS to advertize the SIP-PBX SIP signaling address to the Service Provider network,
- signaling security and authentication are supported using a variety of schemes based on bilateral agreement,
- NAT traversal is achieved using Connection-Reuse

The Registration mode has several advantages over the Static mode, including:

- it alleviates the Enterprise from having to make its SIP-PBX signaling address publicly viewable in DNS,
- it provides mechanisms such as Outbound that make the SIP-PBX publicly reachable even if a NAT exists between the SIP-PBX and the Service Provider network,
- it avoids having to statically provision the path from the Service Provider core to edge proxies per Enterprise, and
- it provides a direct means of discovering service outage before active request routing needs to occur.

The Static model is often used for larger Enterprises, where often the SIP-PBX does not support Registering to the Service Provider, and the size of the Enterprise warrants more explicit provisioning of connection and service information by the Service Provider. For example, large Enterprise trunks often have unique requirements for SLAs, call routing, load balancing, codec support, etc., which make explicit provisioning necessary. Service outage detection is typically performed with explicit SIP request "keep-alive", such as periodic OPTIONS requests or TCP keep-alive. As a Peering connection, digest-challenging of the SIP-PBX by the Service Provider is not often used; instead, other forms of authentication are employed or implicitly assumed, for example with a dedicated leased-line, IPSEC connection, or through Mutual-TLS.

7.1 Registration Mode

In the Registration mode, the SIP-PBX provides its SIP signaling address to the Service Provider network using the SIP registration procedure. The Service Provider network supports a location service that maintains the mapping between the registered AOR identities of the SIP-PBX users, and the location (aka transport address and proxy path) of the SIP-PBX SIP signaling interface.

7.1.1 Locating SIP Servers

7.1.1.1 Enterprise Requirements

Comment [JohnE9]: I thought we agreed that we don't need all the explanatory text.

Comment [JohnE10]: I thought we came to some conclusion on which mode(s) must be supported.

Comment [JohnE11]: Would it be more correct to say "to advertise the SIP-PBX's SIP signaling address to the Service Provider network"?

Comment [JohnE12]: This is a misleading statement. A SIP-PBX normally uses TLS to authenticate the SP-SSE.

Comment [JohnE13]: Need to say what this is, complete with reference.

Comment [JohnE14]: Connection-reuse does not give you NAT traversal. It merely improves performance and scalability. Basically static mode requires the SIP-PBX to have a publicly reachable signalling address.

Comment [JohnE15]: This seems to miss the main point, that it is useful when the SIP-PBX does not have a static IP address.

Deleted: transport addressing

Comment [JohnE16]: What does this mean - publish in DNS?

Comment [JohnE17]: But the paragraph below on static mode describes how service outage is detected.

Comment [JohnE18]: model or mode? Be consistent.

Comment [JohnE19]: We need to be clear whether we are specifying it or not. This sort of statement is not helpful.

Comment [JohnE20]: I thought we had agreed on SIP-PBX and SP-SSE as terms. There is still a mixture of terminology in the document. I have proposed some changes, but the whole document needs checking. There are some places where "Enterprise network" and "Service Provider Network" is appropriate, but in many cases we should talk specifically about the SIP-PBX or SP-SSE. References to proxy servers are wrong.

The **SIP-PBX** **MUST** provide its SIP signaling address and port to the **SP-SSE** using the SIP registration procedure described in 7.1.4.

Deleted: Enterprise network

Deleted: Service Provider network

The **SIP-PBX** **MUST** be capable of obtaining information about the **SP-SSE**, in particular, the address/port and transport protocol (i.e. UDP, TCP, SCTP, TLS) of the **SP-SSE**. To obtain this information, the **SIP-PBX** **MUST** use one of the following mechanisms:

Deleted: Enterprise SIP Proxy server (or the

Deleted: when no Enterprise SIP Proxy Server is deployed)

Deleted: Service Provider network

Deleted: Service Provider SIP Proxy Server

Deleted: Enterprise SIP Proxy Server or

Deleted: Service Provider SIP Proxy Server

Deleted: Enterprise SIP Proxy Server or

Deleted: SIP Proxy Server(s)

- No discovery:

The SIP signaling address/port of the **SP-SSE** is configured in the **SIP-PBX**.

- [RFC 3263](#) "Locating SIP Servers":

Enterprise SIP Proxy Servers utilizes DNS NAPTR and SRV queries as described in [RFC 3263](#) to determine the IP address, transport protocol, and port number of the **SP-SSE(s)** associated with the Service Provider's domain name. This option assumes that the SIP-PBX has been pre-configured with the domain name of the Service Provider network.

7.1.1.2 Service Provider Network Requirements

The Service Provider network **MUST** be publicly reachable either through a publicly-accessible DNS server that is authoritative for its domain or through a **public** static IP address. If **reachable** through DNS, the DNS server **SHOULD** support NAPTR resource records and **MUST** support SRV resource records.

Deleted: publicly addressable

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

Deleted: SIP Proxy Servers

Deleted: servers

Deleted: SIP Proxy Servers

The Service Provider network **MUST** obtain the **SIP-PBX's** SIP signaling address/port using SIP registration, as described in section 7.1.4.

Deleted: Enterprise network

7.1.2 Signaling Security

The SIP-PBX **MUST** support Transport Layer Security (TLS) as described in [RFCs 2246](#) and [RFC3261](#). The SP-SSE **MUST** support TLS if and only if the use thereof is required by the Service Provider. The SIP-PBX and the SP-SSE **MUST** support a configuration option to control whether TLS is required or disabled.

Comment [JohnE21]: I thought at the last conference call we came to a conclusion on TLS support that was different from this. I thought we said something like "SHOULD support, unless only to be deployed over managed secure connections", this applying both to the SIP-PBX and to the SP-SSE.

When TLS is required, the following rules apply:

- all SIP signaling exchanged between the SIP-PBX and the SP-SSE **MUST** be secured using TLS.
- the SIP-PBX **MUST** initiate the establishment of the TLS session.
- the SP-SSE **MUST** utilize a verifiable digital certificate to secure a TLS session.
- the SIP-PBX and SP-SSE **MUST** support the Server-provided TLS certificates model (described below)

The use of TLS certificates in subscription mode follows what may be called a 'Server-provided' model.

In this model, the Service Provider Proxy (acting as a TLS server) provides its certificate as part of the TLS establishment phase to the SIP-PBX (acting as a TLS client). Note that this is essentially the same model as secure TLS/SSL connections on the Public Internet for HTTP.

The TLS client (i.e., the SIP-PBX) has to initiate the TLS session. If there is a NAT or Firewall, the Service Provider Proxy is not in a position to establish a TCP or UDP connection to the SIP-PBX. If there is no NAT or Firewall, the Service Provider Proxy would be able to set-up a TCP connection; however, it would not be able to set-up a TLS connection because the SIP-PBX cannot take the TLS server role since it does not have a certificate. Therefore, in order to be always reachable (e.g., to receive calls or instant messages), that TLS connection MUST therefore be kept-alive.

Further, when using Server-provided TLS certificates the SIP-PBX MUST use the registration of a “main” AOR mechanism described in Section 7.1.4

In accordance with [draft-ietf-sip-domain-certs] when presenting a Certificate, it is **RECOMMENDED** that a SIP Identity be conveyed in the subjectAltName field of the certificate of type uniformResourceIdentifier. However, when receiving a certificate, an implementation MUST be able to extract the identity from the subjectCommonName (CN) if (and only if) it is not present in the subjectAltName. This is to support existing certificate signer implementations that use the CN field instead of the subjectAltName field. Furthermore, an implementation MUST be able to accept a DNS name as an identity (e.g. proxy1.example.com), instead of a URI as defined in [RFC 3986] (e.g., sip:proxy.example.com). This is to allow for supporting implementations that commonly use certificates that were created for HTTP instead of for SIP. It is also **RECOMMENDED** that implementations be able to provide either a URI or DNS name for backward compatibility.

The SIP identity of the Service Provider Proxy **SHOULD** take the form of the scheme (e.g., “sip:”) followed by the host name of the proxy (e.g., proxy1.example.net).

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.

7.1.2.1 The use of transport=tls parameter

The use of the transport=tls parameter has been deprecated in [RFC 3261] and **SHOULD NOT** be used. However, it should be accepted for backward compatibility with implementations that use this parameter.

When an SIP-PBX registers, it **SHOULD NOT** use the transport=tls parameter. The reachability through TLS is indirectly determined by the Proxy or Registrar because the registration itself is using TLS.

Is it possible to tighten transport=tls to “MUST NOT” in this specification? [Request guidance from the group on this]

7.1.2.2 The use of SIPS URI

This specification does not make use of the SIPS URI [draft-ietf-sip-sips].

Spencer: I had assumed that the service provider is allowed to pass SIPS requests across the interface, although it is not required to do so. I think the subsection should be removed.

7.1.3 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, unless the Service Provider network is providing an implicit NAT traversal function or the two are using a private VPN-style address space.

Spencer: I think (re: John’s comment) that’s what it says, UNLESS...

Comment [JohnE22]: Not if it doesn't know the IP address, which may be dynamic.

Comment [JRE23]: Further to my last but one comment, eventually we seem to get to some text that ties server authentication to the use of registration, but still leaves it open whether registration is used or not with mutual authentication, so I still think there are too many options.

In general, I think we need to do a clearer analysis of the options in this area. We have 3 degrees of freedom: TLS or not, TLS mutual or server authentication, and registration or not. This in theory gives 6 permutations. Maybe more if we consider whether or not we use sip-outbound. I think one or two of these permutations kind of get eliminated during the existing text, but I would like to see if we can eliminate more. Also it is very muddled. Once we have decided on the options, we need to document it more clearly, i.e., a top level exposition of the options (and who must support which options), then for each option, the implications (e.g., must use TLS mutual authentication). I will post a separate comment to the list on this general principle.

Comment [JRE24]: Can we refer to draft-ietf-sip-domain-certs? Unfortunately it is not an RFC yet, but it would be good to avoid duplicating material. It is mentioned in the next paragraph, but not in this paragraph.

Comment [JohnE25]: Where does this appear?

Comment [JohnE26]: I thought there was agreement to delete this.

Comment [JohnE27]: OK with me.

Comment [JRE28]: What does this mean? If an IPPBX or SP receives from elsewhere a SIPS request, is it not allowed to pass it across the interface (assuming TLS is available)?

Comment [JohnE29]: OK with me.

Comment [JRE30]: Is this really trying to say that all IP address must be within an address space agreed between enterprise and SP, which could be the public IP address space?

Comment [JohnE31]: What I had in mind was a further NAT in the SP network, so that the agreed address space between SIP-PBX and SIP-SSP is in fact private address space. I don't know whether this is likely to occur. Anyway, my formulation “an address space agreed between the enterprise and the service provider” seems to cover a multitude of sins.

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. The SIP-PBX MAY support the Outbound NAT traversal procedures defined in draft-ietf-sip-outbound-14, and the Interactive Connectivity Establishment (ICE) procedures defined in draft-ietf-mmusic-ice-19.

Spencer: I believe that the text John is commenting on can be deleted.

7.1.4 Registration

The Service Provider network **MUST** support a database that maintains the mapping between the AOR identities of the SIP-PBX users, and the location (aka transport address and proxy path) of the SIP-PBX SIP signaling interface. This is necessary to allow the Service Provider network to route SIP requests to the appropriate Enterprise SIP-PBX, and through the various SIP nodes in the path.

One method to provide SIP-PBX reachability is through DNS as described previously in section **Error! Reference source not found.**, whereby the Enterprise provides SIP reachability information to its SIP-PBX in DNS (e.g., SRV records), and the Service Provider network routes SIP requests to the Enterprise using [RFC 3263](#) procedures. Such a model has several issues, however: (1) it requires the Enterprise to make its SIP-PBX transport addressing publicly viewable in DNS, (2) it requires the Enterprise to make its SIP-PBX publicly reachable even if a NAT exists between the SIP-PBX and the Service Provider network, (3) it requires static provisioning of the path from the Service Provider core to edge proxies per Enterprise, and (4) it does not provide a direct means of discovering service outage before active request routing needs to occur.

While using DNS for the SIP-Connect trunk interface, and having static provisioning of the path to the SIP-Connect interface within the Service Provider network, **MAY** be practical for large Enterprise trunk connections, it is not pragmatic for smaller SMB-sized Enterprise SIP-PBX trunks.¹ Therefore, SIP-PBX's targeted at the SMB market, typically of the sub-100 user phones size, **MUST** support registering a "default" or "main" AoR following the procedures in [RFC 3261](#). The SP network **MUST** support an implicit registration model, where the SIP-PBX registers a single "default" AoR assigned to the SIP-PBX itself, which implicitly registers all the users in that SIP-PBX. The registration procedure **MUST** be scalable to support SIP-PBXs serving multiple hundreds of users, or as few as one.

I believe the text above can simply state SIP-PBXes that will use the Registration mode MUST support... dropping the description of when this mode should be chosen.

The SIP-PBX and Service Provider network **MUST** support the authentication mechanisms outlined in section 7.1.6 for digest authentication for the REGISTER requests, using a user name and password agreed to by both parties.

Spencer: Opinions about this comment?

All subsequent requests from the SIP-PBX to the Service Provider network **MUST** use the same top Via transport information as the successful REGISTER uses, and thus the same transport flow(s) for the SIP-Connect trunk. If the SIP-PBX is a proxy for Enterprise SIP UA's, it **MUST** insert a Record-Route in dialog-forming requests so that all in-dialog requests from the UA and Service Provider network go through the SIP-PBX. If it is a B2BUA, the Contact URI **MUST** contain the SIP-PBX's Registered host:port transport info, unless GRUU is supported and used.

¹ It is typically impractical to perform the Subscription REGISTER model for large Enterprises, due to the number of user AoR's supported in the Enterprise. Typically large Enterprises are assigned large blocks of phone numbers, and have multiple paths or SIP-PBX's available for SIP reachability.

Comment [JRE32]: This sounds like the two (ICE and sip-outbound) are coupled together, but I think they are largely independent.

In the case of outbound, this requires support on both sides, so I would agree it needs to form part of the spec. The question is whether to make it mandatory when using registration (to reduce the number of options) or whether to make it optional (thereby keeping the bar low for minimal compliant implementations). As observed above, this is all tied up with whether TLS is used and whether mutual or server authentication is used.

In the case of ICE, this too requires support on both sides, but support by the media endpoints, not the IPPBX.

Comment [JohnE33]: Yes

Comment [JohnE34]: This seems to have nothing to do with registration mode.

Comment [JRE35]: This says that DNS-based may be suitable for larger enterprises, but does not say why registration-based is not suitable for larger enterprises. All the points made in the previous paragraph suggest that registration-based has advantages. If there are no advantages to DNS-based, why specify it as an option? However, I suspect scalability can be an issue with registration-based, in which case that (and other issues, if any) should be clearly stated.

Comment [JohnE36]: Yes.

Comment [JRE37]: This seems to suggest that there is no point in using TLS mutual authentication when registration is used. Is this a correct interpretation?

Comment [JRE38]: What is the purpose of this? Is it to avoid using digest authentication on requests other than REGISTER requests? If so, I am not convinced it works (I am thinking of the recent discussions in SIPING to do with P-Asserted-Identity and whether a response received over TLS can be assumed to come from an entity previously digest-authenticated on the same TLS connection). Perhaps it (... [1])

Comment [JRE39]: Isn't this too strict? As long as the contact URI contains sufficient information to route back to the B2BUA, that should be sufficient, e.g., a GRUU would be sufficient. Also it applies only to dialog-forming and mid-dialog requests (... [2])

Comment [hsk40]: I know this is ugly, but there have been interop problems with this. We should discuss what we want to do here.

A Service Provider network **MAY** implement the P-Associated-URI header defined in [RFC 3455](#), and return the default and implicitly registered AoRs in P-Associated-URI header(s) in the 200 ok response for the REGISTER request. This header lists all the AoR's registered by the successful REGISTER transaction. The purpose for this is mainly for use inside the Service Provider network, however the SIP-PBX **MAY** record it for troubleshooting purposes, to verify the list contains the same URI's the SIP-PBX believes it supports. **Note that 3GPP/TISPAN is defining a wildcard URI mechanism for this header value, so that multiple usernames can be indicated with one URI - see 3GPP TS 23.003 section 13.5 on wildcarded PSI's.**

Comment [JRE41]: So are we endorsing that or not?

For out-of-dialog requests routed to an Enterprise SIP-PBX that has registered, the Service Provider Network **MUST** leave the request-URI unchanged (i.e., reflecting the actual called identity), and insert a loose-route Route header with the registered Contact-URI of the main AoR. **This URI MUST be the bottom-most Route header following any others used for routing the request through proxies to reach the SIP-PBX, for example those built from received Path header URIs from the Registration.** Note that the IETF is in the process of standardizing this type of behavior, with several options under discussion. The approach chosen above was selected to minimize protocol impacts until standardization occurs. Options under discussion at IETF include draft-rosenberg-sip-ua-loose-route, in which the registered Contact-URI for the main AoR contains an "lr" loose-route URI parameter, as well as options proposing a possible new header, such as a "Target" header. Previously, registered contact-URI's always replaced the request-URI of out-of-dialog requests routed to the registered UA, which cause the initial called part information to be lost. For example a request to a particular user off an SIP-PBX could not be discerned by the request-URI received at the SIP-PBX, and would instead appear in a P-Called-Party-ID header.

Comment [hsk42]: We need to decide if we're going to support the wildcarded URI, because if we do we need to mandate SIP-PBX support for it

Comment [JRE43]: I am not sure that the Route header is necessary over the interface, although it may have uses for internal routing within the SP. The IPPBX shouldn't care whether it receives a Route header or not.

Comment [hsk44]: We do need to decide if we're going to stick to this or revert to the req-uri being the registered contact. If we do that latter, do we need to support the Target or P-Called-Party-ID headers? (somehow the real called target URI needs to be identifiable by the SIP-PBX, which will not be the registered contact in all cases)

Service Provider SIP Proxy Servers **SHOULD** support the mechanism outlined in draft-ietf-sip-outbound-14.txt, and SIP-PBX's **SHOULD** support it. **[Note: this version of the draft is likely to be the one submitted for RFC status, and no significant changes have been made in several drafts]** Even if Service Provider NAT traversal is not needed, sip-outbound defines a keep-alive mechanism which is useful for SIP-Connect trunk connection liveness checks.

Comment [JRE45]: If we say "SHOULD", what are the circumstances in which either side is permitted not to support it? If we made it "MUST", we would not require any other options.

SIP-PBX's **MAY** support Subscribing for the Registration Event Package, as defined in [RFC 3680](#). The SIP-PBX **MUST** maintain only one subscription, for the main Registered AoR. Notifications for the subscription from the Service Provider network **MUST** include the implicitly registered AoR's. **[Note: this includes the wildcarded syntax URI]**

Comment [JRE46]: This effectively gives two mechanisms for obtaining the list of implicitly registered AoRs: this and P-Associated-URI. Why do we need two mechanisms? Also there seems to be no obligation on the SP to support this.

Service Provider networks and SIP-PBX's **MAY** support the Service-Route mechanism, defined in [RFC 3608](#). **If the SIP-PBX supports this, and the 200 ok for a successful REGISTER contains Service-Route header value(s), the SIP-PBX MUST create a pre-loaded list of Route Header values, containing the URI of the Service Provider Network SIP Proxy Server followed by the values from the Service-Route header, and use this list in all subsequent request to the Service Provider Network for any of its users.**

Comment [JRE47]: What is the use case for this?

Service Provider networks and SIP-PBX's **MAY** support the GRUU mechanism, as defined in draft-ietf-sip-gruu-15.txt. **[Note: this draft is in the IETF RFC Editor's queue for publication, and is therefore not expected to change]** If a GRUU is returned for the successful REGISTER request, it **MAY** be used by the SIP-PBX as the Contact-URI for subsequent requests from any of its explicitly or implicitly registered AoR's.

Comment [hsk48]: The value for this is we can't disallow it, so the statement just notes it can be used. But I agree it's odd to say this - what do you want us to do here? Just ignore it?

7.1.4.1 Registration Failures

This section details the behavior requirements for the Service Provider SIP Proxy Server and Enterprise SIP-PBX for Registration failure scenarios.

7.1.4.1.1 Failure of SIP-PBX to reach SIP Proxy Server

If the SIP-PBX fails to receive any response for a REGISTER request in Timer_F time (typically 32 seconds) or encounters a transport error when doing so, it **MUST** consider the SIP Proxy Server unreachable and try to Register with an alternate SIP Proxy Server address if it has one. If no SIP Proxy Server is reachable, or no alternates are available, it

Comment [JRE49]: As far as I can see, section 8 says an IPPBX MAY support registration (well, it says MUST, but only if it targets the smaller end of the market, so effectively it is a MAY). It also says the SP MUST support registration. It says nothing about support for DNS-based (but maybe that can be found in other sections). This all seems to underline the fact that the various optionality in this area (signalling security, mutual/server authentication, registration and outbound) is very fragmented across several sections.

MUST delay reattempting Registration for 30 seconds, and increasing this delay value by doubling it for each successive delivery failure until delivery succeeds, up to a maximum value of 960 seconds. SIP-PBX's implementing draft-ietf-sip-outbound are further restricted to comply with the backoff mechanism defined therein, for example if they already have one flow active.

Note that receiving an explicit non-2xx final response from the SIP Proxy Server does not constitute a delivery failure. Instead, behaviors for such final responses are noted in the following sections.

7.1.4.1.2 Redirection of SIP-PBX from SIP Proxy Server

The SIP Proxy Server **MAY** issue a 302 Moved Temporarily or 305 Use Proxy redirect response to a REGISTER request, to get the SIP-PBX to Register with an alternate SIP Proxy Server address identified by the Contact URI in the response. An SIP-PBX receiving such a response to a REGISTER **MUST** attempt to Register with the server in the Contact URI of the 302 or 305 response, using the received Contact URI for the new REGISTER request's request-URI for the 302 case, and using it for a target Route header for the 305 case.

Although [RFC 3261](#) defines the 302 response to only apply for a single transaction lifetime if no Expires header is present in the 302 redirect, it is common practice that for Registrations the redirected-to address be used as long as it is reachable or until another non-200 response is received from the redirected-to server. SIP Proxy Servers **SHOULD** insert an Expires header field in the 302 response, with the length of time the SIP-PBX **SHOULD** be redirected - typically 86400 seconds (1 day).

7.1.4.1.3 Unknown SIP-PBX Identity

The Service Provider network **MAY** issue a 404 Not Found response to a REGISTER request, if the AoR/Identity of the SIP-PBX is not found in its database. This response needs to be proxied by the SIP Proxy Server back to the SIP-PBX. An SIP-PBX receiving such a response to a REGISTER request **MUST** consider the Registration attempt to have failed, and notify its human user if possible through some means. The SIP-PBX **SHOULD** follow the backoff procedures defined previously in section 7.1.4.1.1.

7.1.4.1.4 Incorrect SIP-PBX Password

The Service-Provider/SIP Proxy Server **MAY** issue additional 401 Unauthorized or 407 Proxy Authentication Required responses to REGISTER requests, if the digest challenge response of the SIP-PBX in its REGISTER request is stale or invalid. Or they **MAY** issue a 403 Forbidden response, depending on policy. If an SIP-PBX receives more than three responses of 401, 407 or 403 in aggregate, without a different response other than one of those in between, then the SIP-PBX **MUST** consider the Registration attempt to have failed, and notify its human user if possible through some means. The SIP-PBX **SHOULD** follow the backoff procedures defined previously in section 7.1.4.1.1.

Note that 403 Forbidden responses produce different behavior on the SIP-PBX for non-REGISTER requests. For non-REGISTER requests, a 403 Forbidden response **SHOULD** trigger the SIP-PBX to re-Register immediately.

7.1.4.1.5 SAS unreachable from SIP Proxy Server

The SIP Proxy Server **MAY** issue a 408 Request Timeout or 480 Temporarily Unavailable response for a REGISTER request, to indicate it is unable to reach any servers within the Service Provider network. An SIP-PBX receiving such a response to a REGISTER request **SHOULD** act exactly as if delivery to the SIP Proxy Server had failed per section 7.1.4.1.1, and thus move to any alternate SIP Proxy Server's, and potentially keep retrying with increasing retry values, up to 900 seconds.

7.1.4.1.6 Other 4xx Responses

Any 4xx-class response to a REGISTER request not explicitly identified above **SHOULD** be treated in a similar manner as section 7.1.4.1.1 unless it can automatically be resolved by the SIP-PBX internally - i.e., unless it is part of an explicit negotiation mechanism or procedure. It **SHOULD** be treated as a delivery failure but with a higher maximum retry value

of 86400 seconds (1 day). Examples of 4xx responses which **SHOULD** be internally resolvable would be a 439 (First Hop Lacks Outbound Support) response based on draft-ietf-sip-outbound.

7.1.4.1.7 SIP Proxy Server Administratively Disabled or Overloaded

An SIP Proxy Server which is overloaded or administratively disabled **MAY** generate a 503 Service Unavailable response to a REGISTER request, and **SHOULD** include a Retry-After header value indicating how long before the SIP-PBX **SHOULD** re-attempt the request to the same SIP Proxy Server. An SIP-PBX receiving such a response **MUST** support the Retry-After header, and **MUST** honor the value as follows: if the value is 32 seconds or less, it **MUST** wait the requested time and retry the request to the same SIP Proxy Server; if the value is larger, it **MUST** remember the value for that SIP Proxy Server address instance, and try any alternate SIP Proxy Server addresses it can. If an alternate SIP Proxy Server can be successfully reached and Registration succeeds through the alternate, the SIP-PBX **MAY** discard the Retry-After value of the original. Otherwise, it **MUST** wait to reattempt Registration to the original SIP Proxy Server for the Retry-After value in seconds.

7.1.4.1.8 Other 5xx/6xx Responses

Any 5xx or 6xx-class response to a REGISTER request not explicitly identified above **SHOULD** be treated in a similar manner as section 7.1.4.1.1 unless it can automatically be resolved by the SIP-PBX internally - i.e., unless it is part of an explicit negotiation mechanism or procedure. It **SHOULD** be treated as a delivery failure with a maximum retry value of 960 seconds (16 minutes).

7.1.5 Failover and Recovery after Registration

In order to provide a reliable signaling interface between the Enterprise and the Service Provider network, the SIP-PBX and the SP-SSE **MUST** support the multiple connection capability described in draft-ietf-sip-outbound.

This section needs work!

This section would include discussion about dual-homing using SIP Outbound specification. TLS Connection Reuse may be discussed here or may be more appropriately discussed elsewhere in the document.

7.1.6 Authentication, Authorization and Accounting

This section needs work!

Comment [JRE50]: This section includes discussion of TLS mutual authentication as well as digest authentication. There is some overlap with what has been stated earlier.

7.1.6.1 Authentication of the Enterprise by the Service Provider

Authentication of the Enterprise by the Service Provider is performed using SIP Digest authentication mechanism.

The SIP-PBX and SP-SSE **MUST** support the digest authentication scheme as described in section 22.4 of [RFC 3261](#). 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).

The following rules apply:

1. Any SIP request may be challenged by the SP-SSE. When so challenged by the SP-SSE, the SIP-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).
2. In order to avoid unnecessary challenges, the SIP-PBX **SHOULD** include its authentication credentials using the current nonce in each request sent to the SP-SSE.

7.1.6.2 Authentication of the Service Provider by the Enterprise

Authentication of the Service Provider by the Enterprise is supported using two mechanisms: SIP Digest, and TLS server authentication.. If TLS is required (based on local configuration data), then the SIP-PBX **MUST** perform TLS server authentication using the identity conveyed in the certificate used by the Service Provider’s SP-SSE to establish the TLS connection with the Enterprise Network’s SIP-PBX.

Comment [JohnE51]: Nothing is said about how this is achieved.

7.1.6.3 Authorization of a Request by the Service Provider

It is **RECOMMENDED** that the Service Provider network authorizes initial dialog creating requests from the Enterprise. This **MAY** be done by either verifying that the identity of the request originator is a known identity associated with the Enterprise or by verification that the request conforms to an authorization policy applied by the Service Provider to requests from the Enterprise.

Comment [JRE52]: What is meant by "the identity of the request originator"? Is it the From URI, the PAI URI, the digest identity, or what?

Spencer: Suggest “the digest identity of the request originator” – comments?

7.1.6.4 Accounting

The Service Provider network **MAY** generate billing records for calls originating from the SIP-PBX. These calls may be billed to the individual SIP-PBX user or to some other entity representing the SIP-PBX or the Enterprise. The SIP-PBX is not required to signal a billing number to the SP network (i.e., the SP network will be configured with the billing number associated with incoming calls from the SIP-PBX).

7.2 Static Mode

{Describe primary characteristics of this mode...}

Spencer: need text here – the current text relies on the existence of an Enterprise SIP Proxy which is not part of the architectural model.

7.2.1 Locating SIP Servers

7.2.1.1 Enterprise Requirements

7.2.1.1.1 Providing Enterprise Address to Service Provider Network

The Enterprise network **MUST** provide its SIP signaling address and port to the Service Provider network using one of the following mechanisms:

- DNS:
The Enterprise network ensures 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.
- Static Configuration:
The mapping of the SIP-PBX SIP URI(s) to the SIP-PBX SIP signaling address and port is configured in the Service Provider network.

7.2.1.1.2 Obtaining Service Provider Network Address

The Enterprise SIP Proxy server (or the SIP-PBX when no Enterprise SIP Proxy Server is deployed) **MUST** be capable of obtaining information about the Service Provider network, in particular, the address/port and transport protocol (i.e. UDP, TCP, SCTP, TLS) of the Service Provider SIP Proxy Server. To obtain this information, the Enterprise SIP Proxy Server or SIP-PBX **MUST** use one of the following mechanisms:

- No discovery:
The SIP signaling address/port of the Service Provider SIP Proxy Server is configured in the Enterprise SIP Proxy Server or SIP-PBX.
- DHCP Option 66 for TFTP provisioning server discovery:
Once the SIP-PBX obtains the TFTP server address, it contacts the TFTP server to get its configuration data, including the SIP signaling address/port in the Service Provider SIP Proxy Server. Note, this option will work only when the DHCP server is controlled by the Service Provider, which is typically not the case when the SIP-PBX is behind a NAT.
- [RFC 3263](#) "Locating SIP Servers":
Enterprise SIP Proxy Servers utilizes DNS NAPTR and SRV queries as described in [RFC 3263](#) to determine the IP address, transport protocol, and port number of the SIP Proxy Server(s) associated with the Service Provider's domain name. This option assumes that the SIP-PBX has been pre-configured with the domain name of the Service Provider network.

7.2.1.2 Service Provider Network Requirements

7.2.1.2.1 Providing Service Provider Address to Enterprise

The Service Provider network **MUST** be publicly reachable either through a publicly-accessible DNS server that is authoritative for its domain or through a publicly addressable static IP address. If through DNS, the 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 network **MUST** utilize the mechanism outlined in [RFC 2782](#) 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.

7.2.1.2.2 Obtaining the Enterprise Network Address

The Service Provider network **MUST** support one of the following mechanisms to obtain the Enterprise network SIP signaling address/port:

- DNS:
Service Provider SIP Proxy Servers utilizes DNS NAPTR and SRV queries as described in [RFC 3263](#) to determine the IP address, transport protocol, and port number of the SIP Proxy Server(s) associated with the Enterprise network's domain name.
- Static Configuration:
The mapping of the Enterprise FQDN to the SIP-PBX signaling address/port is statically configured in the Service Provider network.

7.2.2 Signaling Security

The SIP-PBX **MUST** support Transport Layer Security (TLS) as described in [RFCs 2246](#) and [RFC3261](#). The SP-SSE **MUST** support TLS if and only if the use thereof is required by the Service Provider. The SIP-PBX and the SP-SSE **MUST** support a configuration option to control whether the use of TLS is required by the Service Provider or disabled.

When TLS is required, the following rules apply:

- all SIP signaling exchanged between the SIP-PBX and the SP-SSE **MUST** be secured using TLS.
- both SIP-PBX and SP-SSE **MUST** be able to initiate the establishment of the TLS session.
- Both SIP-PBX and SP-SSE **MUST** utilize a verifiable digital certificate to secure a TLS session.
- the SIP-PBX and SP-SSE **MUST** support the Mutual-TLS certificates model (described below)

The use of TLS certificates in peering mode follows what may be called a Mutual-TLS model. In this model, both the Server Provider Proxy and the Enterprise Proxy or SIP-PBX provide their respective certificate as part of the TLS establishment phase. In order to work, mutual TLS requires that both the Enterprise Proxy or SIP-PBX and the Service Provider Proxy be reachable directly, which prohibits the use of NATs and Firewalls (unless there is a static binding) between those elements. On the other hand, because those elements are globally reachable, there is no need to maintain a permanent nailed up connection via keep-alive.

In accordance with [draft-ietf-sip-domain-certs] when presenting a Certificate, it is **RECOMMENDED** that a SIP Identity be conveyed in the subjectAltName field of the certificate of type uniformResourceIdentifier. However, when receiving a certificate, an implementation **MUST** be able to extract the identity from the subjectCommonName (CN) if (and only if) it is not present in the subjectAltName. This is for supporting existing implementations that use the CN field instead of the subjectAltName field. Furthermore, an implementation **MUST** be able to accept a DNS name as an identity (e.g. proxy1.example.com), instead of a URI as defined in [\[RFC 3986\]](#) (e.g., sip:proxy.example.com). This is to allow for supporting implementations that commonly use certificates that were created for HTTP instead of for SIP. It is also **RECOMMENDED** that implementations be able to provide either a URI or DNS name for backward compatibility.

The SIP identity of the Service Provider Proxy and of the SIP-PBX **SHOULD** take the form of the scheme (e.g., "sip:") followed by the host name of the proxy (e.g., proxy1.example.net). Similarly, the SIP identity of the Enterprise Proxy or SIP-PBX is **RECOMMENDED** to be something like "sip:proxy-a.enterprise.com" or "sip:SIP-PBX-a.enterprise.com". [draft-ietf-sip-domain-certs] provides guidelines for using certificates for establishing a Mutual TLS connection between domains, which is the case when the Enterprise uses its own domain certificate for its SIP-PBXs or its enterprise SIP proxies. If the SIP-PBX is behind an Enterprise NAT or Firewall as opposed to being in the DMZ, its URI would resolve to a Session Border Control or other device proxying on its behalf, but globally reachable.

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 both pre-configured at the Service Provider as well as permitted by the Service Provider's local security policy. Service Provider certificates **SHOULD** be signed by a third party certification authority.

7.2.3 Firewall and NAT Traversal

Spencer: Can we refer to connection-reuse here? Or should we even discuss this topic (since it's mostly out of scope for the specification)?

7.2.4 Failover and Recovery

In order to provide a reliable signaling interface between the Enterprise and the Service Provider network, the SIP-PBX and the SP-SSE MUST support the connection reuse mechanisms described in draft-ietf-sip-connect-reuse.

7.2.5 Authentication, Authorization and Accounting

Spencer: Do we need this section given the current document structure?

8 Supported Signaling Transport Protocols

SIPconnect/1.1-compliant interfaces **MUST** implement UDP, and **MUST** implement TCP.

UDP support is mandated to accommodate legacy devices.

Comment [JohnE53]: I thought the last phone call suggested moving UDP to an appendix and not mandating it.

TCP support is mandated to accommodate large and growing SIP requests and responses, for a variety of reasons (inclusion of certificates, addition of History-Info headers, and addition of Via headers are examples).

9 Enterprise Public Identities

An Enterprise Public Identity is a SIP URI identifying an Enterprise user. Here the term “user” refers to any entity within the Enterprise that is directly addressable from the external network.

In order to receive SIPConnect services, this specification requires that each Enterprise Network have a “Main Public Identity” and zero or more “Alternate Public Identities”. All traffic between the Service Provider Network and the Enterprise Network (i.e. incoming or outgoing calls) is associated with either the Main Public Identity or one of the Alternate Public Identities.

Comment [JohnE54]: I am not sure about “alternate”, which suggests they are alternatives to the main public identity. This is not the case, for example, if a call is targeted at the main public identity, it is not generally appropriate to retarget to an alternate public identity (except where this has been explicitly requested, e.g., by setting up forwarding). How about “secondary public identity”?

The “Main Public Identity” is recognized by the Service Provider Network as the default identity for the Enterprise Network. “Alternate Public Identities” are used in conjunction with delivering Direct Inward Dial (DID) and Direct Outward Dial (DID) services described in the sections below.

Comment [JohnE55]: This is not necessarily true for forwarded calls, or for calls originating in part of the enterprise network not addressable from this SP, e.g., from another country.

The following forms of Public Identities are allowed:

- A SIP URI containing an E.164 number, the domain name of the Enterprise Network, and the “user=phone” parameter.

For example:

SIP:+16132581234@pbx1.operator.com;user=phone

Comment [JohnE56]: In fact there could be an infinite number of alternate public identities, i.e., **@enterprise.com*, although only a finite number of E.164-based alternate public identities. I think this needs to be made clear somehow.

- An “email-style” SIP URI containing a user and the domain name of the Enterprise Network.

For example:

SIP:JoeSmith@enterprise.com

or

SIP:16132581234@pbx1.operator.com

Comment [JohnE57]: Why don't we just say “incoming calls” and “outgoing calls”, as in section 10? Also why can't the main public identity be used with such services, e.g., why can't the main public identity be the target of an incoming call or the source of an outgoing call? Do we really need this second sentence?

Comment [JohnE58]: This doesn't sound like the domain name of the Enterprise Network, as stated above.

Comment [JohnE59]: As above.

Note, for a SIP-PBX operating in the Registration mode, this later form could be used during registration, where the registrar uses the canonical form of the SIP URI received in REGISTER request as the registering Public Identity.

Comment [JohnE60]: What is it about this later (latter?) form that makes it suitable for registration? Is it the numeric user part of the host part that is a sub-domain of the operator's domain? In fact I don't understand this note.

In order to route incoming calls to the Enterprise, the Service Provider network must map the Public Identity of the Enterprise user to the SIP signaling address of the IP-PBX. The mechanism to perform this mapping is based on whether the IP-PBX is deployed in a Registration or Static mode:

Spencer: the distinction following seems to depend on who is responsible for the domain, not on the mode of operation chosen.

- Registration mode: in this case the Service Provider Network is responsible for the domain of the Public Identity, and therefore queries the location service Public-Identity-to-location mapping established at registration time.
- Static mode: in this case the Enterprise Network is responsible for the domain of the Public Identity. The Service Provider network determines the IP-PBX SIP signaling address through DNS (the Enterprise must advertise the address in DNS), or via static mapping tables configured in the Service Provider Network.

Comment [JohnE61]: I think we should follow Paul Kyzivat's proposal at: <http://www.sipforum.org/pipermail/techwg/2008-October/001587.html>. Then, having decided to route to the SIP-PBX, the method of locating the SIP-PBX will depend on whether it is registration mode or static mode, although I think for static mode the enterprise network has to have its own domain name..

10 Establishing Basic 2-Way Calls

This section describes the procedures for establishing basic 2-way calls between the Enterprise and the Service Provider Network.

10.1 Incoming Calls from the Service Provider to the Enterprise

Incoming calls from the Service Provider Network to the Enterprise Network can be addressed to either the Main Public Identity or to one of the Alternate Public Identities. Typically, calls sent to the Main Public Identity are terminated by an auto attendant or front desk operator on the SIP-PBX and then transferred within the enterprise to a private extension. Calls to Alternate Public Identities are usually routed by the SIP-PBX directly to a specific user station – bypassing the attendant or operator. This latter operation is commonly referred to as “Directed Inward Dial” (DID) or “Direct Dial-In” (DDI) service.

Deleted:

This section describes guidelines for populating the Request-URI, and the P-Asserted-Identity, To, From and Route headers for new-dialog INVITE requests sent from the Service Provider Network to the Enterprise Network. The Service Provider Network MUST ensure that all other headers in the INVITE request comply with RFC 3261 [8].

Deleted: header

10.1.1 Populating the Request-URI field

The Service Provider Network MUST populate the Request-URI of the INVITE request with the identity of the actual destination for the call; i.e. either the main Enterprise Public Identity, or one of the alternate Enterprise Public Identities assigned to the SIP-PBX. The Service Provider Network MUST ensure that the form of the Request URI adheres to one of the valid Enterprise Public Identity forms, as defined in section 9.

Spencer: I'm confused here – why would the Service Provider Network choose one of the alternate Public Identities in preference to the main Enterprise Public Identity?

Comment [JohnE62]: The service provider does not choose, it is a given for a particular call. Calls not targeted at one of these and not targeted at the enterprise domain should not be routed to the SIP-PBX. In fact, I am reasonably happy with the text of the preceding paragraph.

On receiving an INVITE request where the Request URI contains a valid Enterprise Public Identity as defined in section 9, the SIP-PBX MUST identify the called user based on the contents of the Request-URI.

10.1.2 Populating the To header field

The ‘To:’ header field of a SIP request generated by the Service Provider Network is normally populated in the same format, and with the same URI, as the Request-URI, as specified in sections 10.1.1 above. However, there may be cases, such as a prior redirection, where the ‘To:’ field does not contain the desired destination. As such, the SIP-PBX **MUST NOT** rely on the contents of ‘To:’ field for routing decisions, but **MUST** use the Request-URI instead.

10.1.3 Populating the Route header

The Service Provider Network **MUST** employ the loose routing model as described in RFC 3261 when routing INVITE requests to the SIP-PBX. The Service Provider Network **MUST** populate the topmost Route header with a URI identifying the SIP signaling address of the SIP-PBX. If the SIP-PBX is operating in the Registration Mode, then the Service Provider Network **MUST** use the SIP signaling address (i.e. the contact address) that was bound to the called Enterprise Public Identity when the SIP-PBX registered, as described in section 7.1.4. If the SIP-PBX is operating in the Static Mode, then the Service Provider Network **MUST** use the SIP signaling address that was obtained using DNS as described in section 7.2.1.

John asked why “MUST populate the topmost Route header” was a MUST – would the SIP-PBX even notice if it were missing?

Comment [JohnE63]: Furthermore, for the static case we should follow RFC 3263, and that does not involve placing anything in the Route header field.

An example of the Route header is shown below:

Route: 123.123.123.1

10.1.4 Populating the From Header

For IP-based originations, there are no special restrictions on the contents of the From header, beyond the requirements specified in RFC 3261. For example, the From header could contain either a SIP or Tel URI. Typically the From header is set by the originating UAC, and either carried transparently through to the terminating UAS, or modified en-route by an originating service. For example, a network-based “anonymizing” service could update the URI contained in the From header to <SIP:anonymous@anonymous.invalid> to obscure the identity of the caller.

For calls incoming to the Service Provider Network from the PSTN, if the PSTN supplied an E.164 calling number, and the caller did not request calling number privacy, then the Service Provider Network **MUST** populate the ‘From:’ header with a SIP URI containing the E.164 calling number, the Service Provider domain name, and the “user=phone” parameter 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 did not supply an E.164 calling number, or the caller has requested calling number privacy, then the following anonymous URI **MUST** be populated in the ‘From:’ field:

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

There are no special requirements placed on the SIP-PBX in processing the From header, beyond the requirements specified in RFC 3261.

10.1.5 Populating the P-Asserted-Identity Header

If the caller requested privacy, then the Service Provider Network **MUST** remove all P-Asserted-Identity headers in the INVITE request before sending the request to the SIP-PBX. If the caller did not request privacy, then the Service Provider Network **MAY** include a P-Asserted-Identity header in the INVITE request containing a URI identifying the calling user.

Comment [JohnE64]: If the caller did request privacy, should the SP include a Privacy header field, so that the SIP-PBX knows the reason for this omission?

If the P-Asserted-Identity header is to be included, then for calls where the Service Provider Network asserts the identity of the calling user (e.g., for PSTN-based originations, or IP-based originations where the calling user belongs to the Service Provider Network) the Service Provider Network **MUST** populate the P-Asserted-Identity header with a SIP URI containing the E.164 calling number, the Service Provider domain name, and the “user=phone” parameter as shown below. The Service Provider Network **SHOULD** also include display name information in the P-Asserted-Identity header, if it is available and has not been restricted for delivery.

Comment [JohnE65]: In this particular case, will the caller ID necessarily be E.164-based?

P-Asserted-Identity: "John Smith" <Sip:+15616261234@serviceprovider.net;user=phone>

If the P-Asserted-Identity header is to be included, but the Service Provider Network did not assert the identity of the calling user (e.g. for IP-based originations where the calling user belongs to a trusted peer network), the Service Provider Network **MUST** pass the received P-Asserted-Identity header(s) to the SIP-PBX without modification. In this case there are no restrictions on the form of the URI identifying the calling user, beyond the requirements specified in RFC 3261. For example, the P-Asserted-Identity header could contain any of the following URI forms:

Comment [JohnE66]: Shouldn't this be a reference to RFC 3325?

- A SIP (or SIPS) URI containing an E.164 address, the domain of a peer service provider network, and the “user=phone” parameter:
Sip:+12126781234@peer-network.com;user=phone
- A TEL URI containing an E.164 address:
Tel:+12126781234
- An “email style” SIP (or SIPS) URI containing a user-name and the domain of a peer service provider network:
Sip:John-Smith@peer-network.com

As described in RFC-3325, the Service Provider Network **MAY** provide up to two P-Asserted-Identity headers, one in the form of a Tel URI, and one in the form of a SIP (or SIPS) URI.

On receiving an INVITE containing a valid P-Asserted-Identity header as described above, the SIP-PBX identifies the calling user based on the contents of the P-Asserted-Identity header.

Comment [JohnE67]: For From we said there were no special requirements placed on the SIP-PBX. Why a different formulation for PAI? Do we need any discussion as to which to choose? From might be more likely to reflect the origin of the call, but can also be forged.

10.2 Outgoing Calls from the Enterprise to the Service Provider

This section describes guidelines for populating the Request-URI, To and From headers for new dialog INVITE requests sent from the Enterprise Network to the Service Provider Network. It also specifies how the P-Preferred-Identity and P-Asserted-Identity can be used by the Enterprise Network to request that a specific calling line id and calling name be used when presenting the call to the remote party – as described in RFC 3325 [15]. The SIP-PBX **MUST** ensure that all other headers in the INVITE comply with RFC 3261 [8].

Comment [JohnE68]: This statement is weird. Because the domain part of a SIP URI will not be that of the enterprise network, the SIP-PBX will not be aware of whether a URI is E.164-based or not, unless it already confirms to option 1 or option2.

This section covers the case where the call is initiated by an Enterprise user served by the SIP-PBX. The case where the SIP-PBX sends an INVITE to the Service Provider Network to establish the forward-to leg of a call forwarded by an Enterprise user is covered in section **Error! Reference source not found.** Emergency calls are described in section 11.2.

Of course, there is also the case where the request is targeted only at an E.164 number (i.e., as obtained from a TEL URI or a dial string), then the SIP-PBX would need to convert it to a SIP URI (since I think we decided not to support TEL URIs), and option 1 seems to be the only possibility.

10.2.1 Populating the Request-URI

The SIP-PBX **MUST** populate the Request URI of the INVITE request with the identity of the called user. If the called user identity is based on an E.164 address, then the SIP-PBX **MUST** populate the Request-URI with a SIP URI that adheres to one of the three forms shown below. The SIP-PBX **MUST** support Option-1, and **MAY** support Options 2 and 3. The Service Provider Network **MUST** support all three options.

So I think all we can say is that if the SIP-PBX only has an E.164 number as target, and not a SIP URI, then it **MUST** construct a SIP URI using the service provider's domain name (and give an example).

Spencer: the third option is not an E.164 address – would we ever translate from an E.164 number to a dialstring?

Likewise, to cover the option 3 case, if the PBX only has a dial string meaningful to the service provider, it **MUST** construct a SIP URI using the service provider's domain name and user=dialstring (and give an example).

- **Option 1:** A SIP URI containing an E.164 address, the domain of the Service Provider Network, and the “user=phone” parameter. This is the default form used when the calling Enterprise user identifies the called user by dialing an E.164 number, and the SIP-PBX has no mechanism to determine the domain that owns that number. In this case the SIP-PBX specifies the Service Provider domain, with the expectation that the Service Provider Network will determine the target domain and route the call accordingly.

SIP:+12128901234@[Service Provider Domain Name];user=phone

- **Option 2:** A SIP URI containing an E.164 address, the domain of a peer Service Provider Network, and the “user=phone” parameter. This is the same as Option-1 except that the SIP-PBX does support a mechanism to determine the domain that owns the called E.164 number, or the SIP-PBX obtained the domain through some other means (e.g., Enterprise user originates a call to a remote user whose identity was asserted on a previous call).

SIP:+12128901234@[peer Service Provider Domain Name];user=phone

- **Option 3:** A SIP URI containing a dialed digit string, the domain of the Service Provider Network, and a “user=dialstring” parameter. This option could be used when the dialed number cannot be represented by an E.164 number (e.g., when the Enterprise user dials an equal-access carrier identity).

SIP:101066612128901234@[Service Provider Domain Name];user=dialstring

10.2.2 Populating the To Header

The To header **MUST** adhere to the same formatting rules as that of the ‘Request-URI’ field described in section 10.2.1 above. The ‘To:’ header in a SIP request generated by the SIP-PBX is normally populated in the same format, and with the same URI, as the Request-URI, as specified in section 10.2.1. However, there may be cases, such as a prior redirection, where the ‘To:’ header does not contain the desired destination. As such, the Service Provider Network **MUST NOT** rely on the contents of ‘To:’ header for routing decisions, but use the Request-URI instead.

10.2.3 Populating the P-Asserted-Identity header

The SIP-PBX **MAY** include a P-Asserted-Identity header in the INVITE request. If a P-Asserted-Identity header is included, then the SIP-PBX **MUST** populate the header with a SIP URI that adheres to one of the forms listed below:

- A SIP URI containing an E.164 address, the domain of the Enterprise Network, and the “user=phone” parameter.

For example:

SIP:+12128901234@[Enterprise Network Domain Name];user=phone

- An “email-style” SIP URI containing a user-name, and the domain of the Enterprise Network.

For example:

SIP:12128901234@[Enterprise Network Domain Name]

or

SIP:johndoe@[Enterprise Network Domain Name]

Comment [JohnE69]: This is contradicted below, where it says **MUST** if within the SP's trust domain.

Deleted: the

The SIP-PBX **MAY** also include a display name in the P-Asserted-Identity header.

For example:

P-Asserted-Identity: “John Doe” <SIP:+12128901234@[Enterprise Network Domain Name];user=phone>

See section 10.2.6 for additional guidance on the use of the P-Asserted-Identity header.

10.2.4 Populating the P-Preferred-Identity header

The SIP-PBX **MAY** include a P-Preferred-Identity header in the INVITE request. If a P-Preferred-Identity header is included, then the SIP-PBX **MUST** populate the header as specified for the P-Asserted-Identity header in section 10.2.3.

Spencer: Is anyone using the P-Preferred-Identity header now?

See section 10.2.6 for additional guidance on the use of the P-Preferred-Identity header.

Comment [JohnE70]: Furthermore, I don't think it is valid to include both, so if you include PAI you must not include PPI. I would prefer not to specify PPI at all.

10.2.5 Populating the From header

The SIP-PBX **MUST** populate the From header as specified for the P-Asserted-Identity header in section 10.2.3, unless this is an anonymous call.

See sections 10.2.6 and 10.2.7 for additional guidance on the use of the From header.

10.2.6 Identifying the Originating User

Based on bilateral agreement between the Enterprise and Service Provider, the SIP-PBX is either inside or outside the Service Provider's trust domain (using the term “trust domain” as defined in RFC 3324).

If the SIP-PBX is inside the Service Provider's trust domain, then the SIP-PBX **MUST** include a P-Asserted-Identity header in dialog-initiating INVITE requests sent to the Service Provider Network, containing the Public Identity of the originating Enterprise user. In this case the Service Provider Network uses the provided P-Asserted-Identity header as the asserted identity for the call.

Spencer: How does this work if the call arrived via retargeting, without a P-Asserted-Identity header?

If the SIP-PBX is outside the Service Provider's trust domain, then the Service Provider Network **MUST** assert the identity of the originating user by adding a P-Asserted-Identity header populated with the Public Identity of the originating user. The SIP-PBX **MAY** provide a hint of the originating user's identity to the Service Provider Network in the P-Preferred-Identity or P-Asserted-Identity header. The Service Provider Network checks if the “hint” provided matches an identity configured within the Service Provider Network for the SIP-PBX. When a match is found, the Service Provider Network asserts that identity as the identity of the originating Enterprise user. **When there is no match, or no P-Asserted-Identity or P-Preferred-Identity is provided, the Service Provider Network asserts a default public identity for the SIP PBX.** Local policy within the Service Provider Network may also allow a default identity for the SIP PBX to always be asserted even when there is a match, or allow the ‘From:’ header to be used as a hint of the originating identity when no P-Asserted-Identity or P-Preferred-Identity header is provided.

Comment [JohnE71]: I think the idea was to cover that in a later section, although I am not convinced that is the best approach.

Comment [JohnE72]: But if privacy is requested it **MUST NOT**, because it is crossing a trust domain boundary.

Comment [JohnE73]: I would prefer to limit to PAI.

Comment [JohnE74]: This could be because the call has been forwarded or has arrived from a different part of the enterprise network.

Spencer: If the SIP-PBX is not part of the Service Provider trust domain, is this in scope for SIPconnect/1.1?

Spencer: Again, is anyone using P-Preferred-Identity?

The Service Provider Network uses the asserted identity to apply the appropriate calling restrictions and other originating services to the call. The asserted identity can also be used to convey calling name and number information as described in section 10.2.7.

10.2.7 Controlling the Calling Line ID and Calling Name Presentation

SIPConnect allows the Enterprise Network to control calling line ID and calling name presentation for outgoing calls on a per call basis. This control includes both restricting the presentation for privacy reasons, as well as specifying the preferred presentation to be used for the call.

10.2.7.1 Default Calling Line ID and Calling Name Presentation

On receiving an INVITE from the SIP-PBX, the Service Provider Network **MUST** use the identity asserted in the P-Asserted-Identity header as the Calling Line ID and Calling Name (aka calling name and number) for presentation to the remote user, unless privacy or a specific Calling Line ID and Calling Name Presentation is being requested by the Enterprise Network as described in the sections that follow.

Comment [JohnE75]: This seems to be contradicted in 10.2.7.3, which allows From to be used. We do indeed need to keep the possibility of using From, because PAI will not always be the caller ID.

10.2.7.2 Managing Privacy Requests on Outgoing Calls

For calls originating from the Enterprise, the Service Provider Network can be considered trusted within its domain. For this reason, the Service Provider Network **MUST** act as a “privacy service”, and the Enterprise **SHOULD** rely on “Network-Provided Privacy” as described in 3.3 of RFC 3323[13]. Using this mechanism, whenever the Enterprise requires explicit privacy policies for a call, the Enterprise Network **MUST** insert a Privacy header in the outgoing INVITE.

The value of the Privacy header indicates the level of Privacy that should be applied. This specification requires that the privacy service in the Service Provider Network **MUST** support two levels of Privacy priv-values: “none” as described in RFC 3323 [13], and “id” as described in RFC 3325 [15]. The privacy service in the Service Provider Network **MAY** support other levels of privacy.

It is common for a SIPConnect service to have privacy “disabled” in the Service Provider Network by default – in other words, by default no restrictions will be applied to the Calling Line ID or the Calling Name when the call is presented to the remote party. Whenever an outgoing call from the Enterprise is required to have privacy enabled, the Enterprise **MUST** insert a Privacy header with a value of “id” as described in RFC 3325[15].

Although not as common, it is also possible that the default privacy policy in the network is “enabled” – and the Service Provider Network **MUST** support a way to disable the privacy policy on a per call basis. Whenever an outgoing call from the Enterprise is required to have to have privacy explicitly disabled, the Enterprise **MUST** insert a Privacy header with a priv-value of “none” as described in RFC 3323 [15]. When the Service Provider Network receives an INVITE with a Privacy header with a priv-value of “none”, it **SHOULD** disable the privacy service for that call and allow the identity of the user in all messages to be revealed to the remote party.

Comment [JohnE76]: Why not MUST? If SHOULD, what are the exceptions?

When an outgoing call from the Enterprise is required to have privacy enabled, the Enterprise Network **MUST** populate the From: header in the INVITE request with the URI SIP:<anonymous@anonymous.invalid>, in addition to requesting privacy from the privacy server in the Service Provider Network.

10.2.7.3 Requesting Specific Calling Line and Calling Name Presentation

The Enterprise Network **SHOULD** be able to request a specific calling line ID and calling name to be presented to the remote party on a per call basis. By default the Service Provider Network **SHOULD** present the calling line ID and calling name corresponding to the asserted identity contained in the P-Asserted-Identity header, However, this

Comment [JohnE77]: If the INVITE is forwarded to a SIP device or another SIP network, the service provider has no control over what is actually presented. It can only deliver information in From and PAI leave it to the UAS to decide what to display. The only case where the SP is more in control is when going to PSTN, since it can decide what is delivered as caller ID.

specification provides a mechanism that allows the Enterprise to select an identity different than the asserted identity for calling line ID and calling name display. For example, say the asserted identity is the Main Public Identity, but the Enterprise Network wants the Calling Line ID and Calling Name presented to the remote party to correspond to one of the Alternate Public Identities. Or, the Enterprise Network might want the Calling Line ID and the Calling Name presented to the remote party be set arbitrarily to an identity that does not match the Main Public Identity or any of the Alternate Identities associated with the Enterprise. A typical example application could display the Calling Line ID and Calling Name associated with a free-phone service (i.e. 1-800) number to the remote user for calls originating from the Enterprise. Policies on the Service Provider Network dictate whether this is allowed and this is out of scope for this document.

Comment [JohnE78]: I don't understand. It seems that in such cases the From URI will differ from the PAI. The only way the SP can force display of the From URI is by not forwarding the PAI. Is this the intention?

To request the presentation of a specific Calling Line ID and Calling Name that is different than the asserted identity for an outgoing call, the Enterprise Network **MUST** populate the From header with a SIP URI and display name identifying the calling line ID and calling name to be displayed. Depending on local policy, the Service Provider Network **MAY** use the contents of the From header for Calling Line ID and Calling Name presentation to the remote party.

11 Service Interactions

11.1 Retargeting and Rerouting - Related Services

A number of common services can cause a call to be retargeted or rerouted, including, but not limited to: call-forwarding, attended transfer, blind transfer and voicemail deposits. In SIP, a call can be retargeted in a variety of ways:

- Using a 302 response to an INVITE is common for services that forward calls before answering – such as Call Forwarding and Voicemail deposit.
- Formal “retargeting” – when a proxy changes the request URI.
- Using an in-dialog REFER is common for services that involve transfer scenarios, blind or attended.
- An out-of-dialog REFER can be used for services involving transfers.
- Transfer scenarios can be performed using multiple INVITE dialogs, using third party call control

Regardless of the service or the mechanism, when a call delivered from the Service Provider Network to the Enterprise Network is retargeted from within the enterprise to a destination outside of the enterprise, it is desirable to preserve the history of the original calling and called party, in order to generate accurate accounting records and apply proper calling policies for retargeted calls.

11.1.1 Simple 302 Redirection

An incoming call from the Service Provider Network can be retargeted through a simple 302 redirection response sent back from the enterprise network. This is depicted in Figure 2.

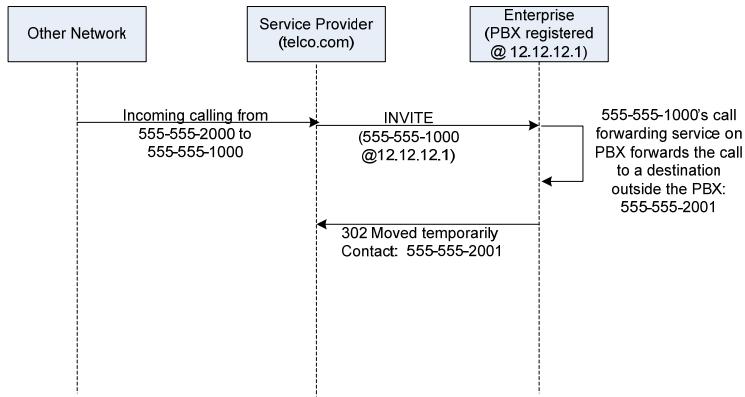


Figure 2 – Retargeting using 302 Moved Temporarily Response

Spencer: agree that we should use URIs and domain names (not numbers and IP addresses) in these figures.

This is the simplest form of retargeting – and it is common for services like call forward always and call forward to voicemail to use this mechanism. The Service Provider Network **MUST** support receiving a 302 redirection from the Enterprise Network as per RFC 3261. The Service Provider Network **MUST** support either the Tel URI or the SIP URI. It is **RECOMMENDED** that the Service Provider Network support the Tel URI; alternatively, the Service Provider Network **MAY** support the SIP URI. The Enterprise Network **MAY** support sending a 302 redirection response back to the Service Provider Network as per RFC 3261. How the Service Provider Network handles the 302 Moved Temporarily is implementation specific and outside the scope of this document.

Comment [JRE79]: Presumably this refers to the Contact header field in the 302 response.

Surely at least one of them should be a MUST. In fact, for the Request-URI of an INVITE request, a SP is mandated to support both schemes, so why not mandate both for a 302?

Spencer: We have agreed that we would use the SIP URI form, correct? So SIP URI would be MUST, correct?

11.1.2 Retargeting via In-Dialog REFER

An incoming call from the Service Provider Network can also be retargeted within the Enterprise Network through an in-dialog REFER transaction. This is depicted in Figure 3:

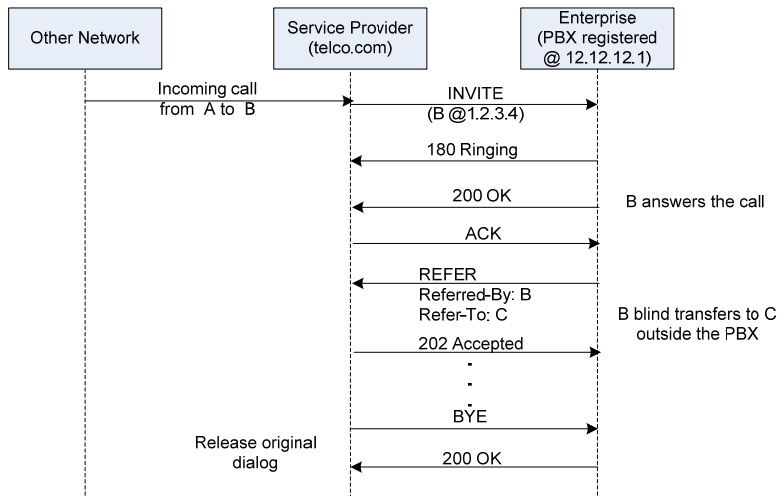


Figure 3 – Retargeting using REFER Request

This form of retargeting is common for transfer related services. It could be used to perform blind transfer or transfer with consultation services between users on the PBX and users outside of the Enterprise. The Service Provider Network **MUST** support receiving a REFER from the Enterprise Network as per [RFC 3515](#). The Enterprise Network **MAY** support sending a REFER back to the Service Provider Network as per [RFC 3515](#). The REFER **MUST** be sent in the context of the corresponding INVITE dialog that is being referred. For certain types of transfers such as transfer with consultation, the party initiating the transfer **MAY** use the Replaces header as defined [RFC 3891](#).

Exactly how the Enterprise Network initiates the REFER is implementation specific and out of scope of this document – but it **MUST** conform to [RFC 3515](#). It is **RECOMMENDED** that the party initiating the REFER release the existing dialog as soon as possible to free up resources over the SIP trunk.

Comment [JRE80]: This MAY applies to the IPPBX, but what is the requirement on the SP to support Replaces?

Comment [JRE81]: This is always the IPPBX, no?

11.1.3 Retargeting via Out-of-Dialog INVITE

The Enterprise Network may send an INVITE to the Service Provider Network as the result of a transfer or call forwarding scenario that occurs within the enterprise. This is depicted in Figure 4:

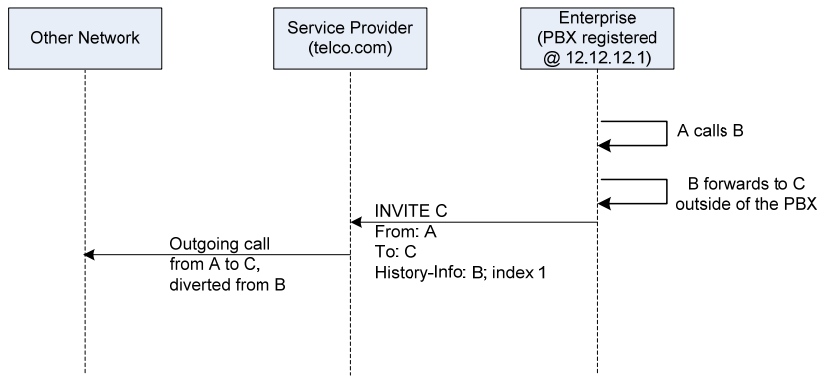


Figure 4 – Retargeting using INVITE Request

This form of retargeting is very common – it can occur whenever a station to station call within the PBX is forwarded to a PSTN number – such as a mobile number. Another common application is forwarding a call from the PBX to be deposited in a voicemail box hosted by the Service Provider network. In both cases, the INVITE looks like a new originating call dialog from the Enterprise network to the Service Provider network. However, it is important that the INVITE contain enough information so that:

- 1) In the case of call forwarding to the PSTN, proper originating call policies and accounting records can be generated,
- 2) In the case of voicemail deposit, the call is deposited into the right voicemail box.

In this scenario, the To: header **MAY** be updated to match the Forward-To user. The To: header would then contain the forward-from user id.

Comment [JRE82]: Why do we need to allow this option? It makes the meaning of the To header field ambiguous. It would be better to let it always mean the original target.

Spencer: I agree with the comment – suggest that I remove the paragraph.

The History-Info header described in [RFC 4244](#) provides a framework for preserving request history information as a call is retargeted from one hop to the next hop. **The History-Info [24] MUST be supported by the Service Provider Network and the Enterprise Network.**

Comment [JRE83]: I think MUST is too strong. For a simple scenario, the Request-URI, To and From header fields give you all the information you need. Also the IETF is considering updating 4244 to deal with some issues, and it might be worth waiting for the new version before using it in SIPconnect.

Spencer: Should we wait for the proposed revision of History-Info before making this a MUST?

When forwarding a private call from within the Enterprise Network to the Service Provider Network, the Enterprise Network **MUST** include a History-Info header indicating at least the last retargeted history information as per [RFC 4244](#). Exactly how the Service Provider Network processes the History-Info is implementation dependant and out of scope for this document, but it **MUST** conform to [RFC 4244](#).

Comment [JRE84]: What about retargeting in the opposite direction, i.e., the enterprise network receives a call from the SP that has been retargeted? Will the IPPBX receive History-Info?

11.2 Emergency Services

This text from Brian Rosen

SIP-PBXs are responsible, directly or indirectly, to provide location and call back information for emergency calls. In addition, various calling features must be disabled. Handling of emergency calls in IP connected devices is presently in flux, and SIP-PBXs must cope with changes being made in carriers, other service providers and PSAPs.

Today, PSAPs have PSTN connections for accepting calls, and limited data capabilities. Transitional mechanisms are deployed in some jurisdictions for IP connected devices sending calls to PSTN connected PSAPs. Generically, these mechanisms are termed “i2”, after a NENA 08-001 standard for North America. Various other jurisdictions are implementing variations on these concepts.

Where there are no transition mechanisms for VoIP origination, location information is provided in some off-line mechanism, and retrieval of such location is keyed on the telephone number. SIP-PBXs **MUST** insert P-Asserted-Identity/P-Preferred-Identity per Section **Error! Reference source not found.**, which also provides call back information.

Note: Where P-Preferred-Identity is provided by the SIP-PBX, the carrier **MUST** include a P-Asserted-Identity with the TN typically the same as the SIP-PBX provided number, assuming the carrier can validate that the number is assigned to the SIP-PBX.

Where there are transition mechanisms, and those mechanisms allow location to be included with the call, the SIP-PBX **SHOULD** ensure that a Geolocation header (ref draft-ietf-sip-location-conveyance) with a precise location of the caller (as specific as possible) is included on the signaling with the call.

The following calling features **MUST** be disabled for emergency calls:

1. Hold
2. Transfer
3. Conference
4. 3-Way Call

Where possible, Voice Activity Detection **SHOULD** be disabled.

Where transition to IP termination of emergency calls at the PSAP is available, SIP-PBXs **MUST** conform to draft-ietf-ecrit-phonebcf.

11.3 Message Waiting Indicator

Voicemail is a service that can be deployed either within the enterprise (often integrated with the PBX) or hosted in the service providers network. Both models have their merits and reasons for deploying one or the other are outside the scope of this document. When voicemail is hosted in the service provider network, the hosted voicemail application must be able to notify the enterprise when a new voicemail has been received.

If voicemail is hosted on the Service Provider network, then the Service Provider **MUST** support sending a message-summary NOTIFY event, acting as a message notifier, as per RFC 3842 [25] using the SIP Specific Event Notification framework as per RFC 3265 [26]. The Service Provider **MUST** support receiving a SUBSCRIBE event for message-summary.

If voicemail is hosted on the Service Provider network, then the PBX **MUST** support receiving a message-summary

NOTIFY event as per RFC 3842 [25] using the SIP Specific Event Notification Framework as per RFC 3265[26]. The PBX MUST support sending a SUBSCRIBE event for message-summary.

11.4 Session Limits

When the IP-PBX originates a session, and the Service Provider network determines that the number of sessions (originating, or the sum of both originating and terminating sessions) for this IP-PBX has reach its limit, the Service Provider network **MUST** respond with 503 Service Unavailable. The Service Provider network **MAY** include a configured Reason-Phrase in the 503, indicating that the agreed session limit has been exceeded.

If an originating session is an emergency session, then the Service Provider network **MUST** proceed with the emergency call as if there was no Session Limits.

12 Section header retained for numbering

This section was replaced.

13 Section header retained for numbering

This section was replaced.

14 Media and Session Interactions

14.1 Media Capability Exchange

Siemens asked for explicit support for re-negotiating using Re-INVITE for third-party call control applications, such as transfer, since REFER and REPLACES aren't part of SIPconnect yet.

Any device that originates and/or terminates RTP traffic **MUST** utilize the Session Description Protocol (SDP) as described in [RFC 2327](#) in conjunction with the offer/answer model described in [RFC 3264](#) 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](#) for all media streams listed in an SDP offer or answer that is generated by the device.

Comment [JRE85]: The RFC specifies that a=sendrecv is the default, so why not allow omission?

Spencer: allowing the default would make the MUST go away – why was it required in the first place?

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).

14.2 Codec Support and Media Transport

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

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. It is **RECOMMENDED** that negotiation of packetization rate during SDP offer/answer makes use of the same packetization rate for both sending and receiving.

Comment [JRE86]: It is not clear what this means in practice. There are ongoing discussions in the IETF on ptime.

Any device that originates and/or terminates voice traffic **MUST** support the [ITU-T G.711](#) u-Law and G.711 A-Law PCM codecs with a packetization rate of 20 ms, and **MUST** support ITU-T G.729 codecs.

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).

Cbeyond asked if we could drop the requirement for A-Law/u-Law transcoding. [Request guidance from the group on this]

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.

Comment [JRE87]: What does this mean?

Comment [JRE88]: Why?

Any device that originates and/or terminates RTP traffic **SHOULD** support the generation of VoIP metrics making use of RTCP XR (RTCP Extended Reports) [\[RFC3611\]](#) and [draft-ietf-sipping-rtcp-summary].

14.3 Transport of DTMF Tones

The Service Provider network **MUST** also support the ability to transport DTMF tones using the RTP telephone-event payload format as described in [RFC 4733](#) when using any codec.

Any Enterprise device that originates and/or terminates voice traffic **MUST** support [RFC 4733](#) DTMF Relay.

Any Enterprise device that supports the transport of DTMF tones **MUST** support the negotiation via an SDP offer/answer of the supported method used to transport the tones. The Enterprise device **MUST** support the ability to use any dynamic RTP payload type when negotiating the use of [RFC 4733](#).

14.4 Echo Cancellation

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

Request for clarification – we had a suggestion to drop this requirement for all-digital devices that do not introduce echo (while retaining it for other devices). Does this make sense? Should we do it? Expert guidance appreciated!

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.

14.5 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](#) or the SIP UPDATE request as described in [RFC 3311](#).

Superior performance of fax transmissions over packet networks can be achieved by utilizing the [ITU-T T.38](#) 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.

The Service Provider network **MUST** support the [ITU-T T.38](#) 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.

The Service Provider network **MAY** support [ITU-T V.152](#) for Voice Band Data, additionally Enterprise devices **MAY** support the specification.

14.6 Call Progress Tones

Media Endpoints **SHOULD** locally generate call progress tones or announcement, or other suitable indication, in response to the following subset of standard SIP response codes for INVITE requests. 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, Media Endpoints **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.

14.7 Ringback Tone and Early Media

New text provided by John Elwell

The delivery of in-band announcements and call progress tones to a caller before a call is answered is achieved through early media.

When acting as a call originator, the SIP-PBX, upon receipt of a 180 provisional response message (reliable or unreliable) **MUST** instruct the Media Endpoint to play local ringback tone to the user. Upon receipt of SDP in any 18x provisional response message (reliable or unreliable), the SIP-PBX **MUST** forward this information to the Media Endpoint.

A Media Endpoint, on receipt of an instruction to play local ringback tone, **MUST** do so until it receives valid RTP packets or is instructed by the SIP-PBX that the call has been answered. On receipt of valid RTP packets, a Media Endpoint **MUST** disable any local ringback tone and play the received media. A Media Endpoint, on receipt of information concerning received SDP, **MAY** use the information to determine whether RTP packets received are valid and **MAY** discard RTP packets arriving before that time.

14.8 Putting a Session on Hold

A 2-way session call can be put on hold by using the mechanisms described in the Media Capability Negotiation section 14.1.

When the hold initiator (which may be the SIP-PBX or Service Provider network acting transparently as Media Endpoint) provides music-on-hold (MOH) treatment:

- The MOH source in the IP-PBX or Service Provider network is based on local policy.
- The hold initiator **MUST** set the SDP directionality attribute to "a=sendonly".

If the hold initiator does not provide MOH, it **MUST** set the SDP directionality attribute to "a=inactive" or "a=sendonly". The attribute "a=inactive" is **RECOMMENDED** because it provides an indication to the held entity that MOH is not being provided by the hold initiator.

15 Section header retained for numbering

16 Additional Guidance

There are several topics that came up during discussions on SIPconnect/1.1 that we expect to be dealt with in the next version of the interface specification, but were not appropriate in version 1.1. This section is intended for network planners who expect to track the SIPconnect specification as it evolves.

16.1 TLS

Although SIPconnect/1.0 required TLS support at **MUST** strength, many commercial deployments don't use TLS. Instead, operators rely on a combination of physical security for the underlying network infrastructure and digest-based authentication to provide a minimal level of security that customers are willing to contract for.

We note that carriers who don't support hop-by-hop TLS have no choice except to refuse calls to SIPS: URIs, and callers whose calls to SIPS: URIs have only the choices of abandoning the call attempt or resubmitting the call attempt using a SIP: URI. Callers who care about security of the call outside their carrier's physical network are subject to a "bid-down" attack.

16.2 IPv6

Although we have little experience with IPv6 SIPconnect/1.0 deployments, we note that North American registrars are already denying requests for /16 IPv4 address allocations, and that IPv6 operation outside North American is becoming common.

We expect to include IPv6 recommendations in a later version of the SIPconnect specification.

16.3 UDP

Although most of our deployment experience has been with SIP over UDP as transport, we note that a number of recent developments are acting to increase the size of SIP requests and/or SIP responses. These developments include:

1. SIP History-Info,
2. including ICE candidates in SIP, and
3. Proprietary headers that increase packet sizes.

We have little deployment experience with these extensions, so we continued to allow SIP over UDP as a mode of operation, but we expect to remove SIP over UDP as a recommended mode of operation in the next version of SIPconnect. SIP over TCP is already the preferred form of operation in SIPconnect/1.1.

Even in SIPconnect/1.1, planners for deployments should carefully consider whether they expect to use these techniques, and consequently encounter larger-than-MTU SIP requests and responses.

17 References

Note that these references are for the SIPconnect/1.0 version of the specification and need to be checked carefully for the SIPconnect/1.1 version of the specification.

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

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

RFC 2246 T. Dierks, C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

RFC 2327 M. Handley, V. Jacobson, "SDP: Session Description Protocol", RFC 2327, April 1998.

RFC 2474 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

RFC 2782 A. Gulbrandsen, P. Vixie, L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.

RFC 3261 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.

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

RFC 3263 J. Rosenberg, H. Schulzrinne, "Session Initiation Protocol (SIP): Locating SIP Servers", RFC 3263, June 2002.

RFC 3264 J. Rosenberg, H. Schulzrinne, "An Offer/Answer Model with Session Description Protocol (SDP)", RFC 3264, June 2002.

RFC 3265 A. B. Roach, "Session Initiation Protocol (SIP)-Specific Event Notification. RFC 3265, June 2002

RFC 3311 J. Rosenberg, "The Session Initiation Protocol (SIP) UPDATE Method", RFC 3311, October 2002.

RFC 3323 J. Peterson, "A Privacy Mechanism for the Session Initiation Protocol (SIP)", RFC 3323, November 2002.

RFC 3324 M. Watson, "Short Term Requirements for Network Asserted Identity", RFC 3324, November 2002.

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

RFC 3455 M.Garcia-Martin, E. Henrikson, D. Mills, "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)", RFC 3455, January 2003.

RFC 3489 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.

- RFC 3515 R. Sparks, "The Session Initiation Protocol (SIP) Refer Method", RFC 3515, April 2003.
- RFC 3550 H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", RFC 3550, July 2003.
- RFC 3581 J. Rosenberg, H. Schulzrinne, "An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing", RFC 3581, August 2003.
- RFC 3608 D. Willis, B. Hoeneisen, "Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration", RFC 3608, October 2003
- RFC 3611 T. Friedman, Ed., R. Caceres, Ed., A. Clark, Ed, "RTP Control Protocol Extended Reports (RTCP XR)", RFC 3611, November 2003
- RFC 3680 J. Rosenberg, "A Session Initiation Protocol (SIP) Event Package for Registrations", RFC 3680, March 2004
- RFC 3725 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.
- RFC 3761 P. Faltstrom, M. Mealling, "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)", RFC 3761, April 2004
- RFC 3891 R. Mahy, B. Biggs, R. Dean "The Session Initiation Protocol (SIP) "Replaces" Header", RFC 3891, September 2004
- RFC 3986 T. Berners-Lee, R. Fielding, L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", RFC 3986, January 2005
- RFC 3966 H. Schulzrinne, "The tel URI for Telephone Numbers", RFC 3966, December 2004.
- RFC 4028 S. Donovan, J. Rosenberg, "Session Timers in the Session Initiation Protocol (SIP)", RFC 4028, April 2005.
- RFC 4244 M. Barnes, "An Extension to the Session Initiation Protocol (SIP) for Request History Information", RFC 4244, November 2005.
- RFC 4694 J. Yu, "Number Portability Parameters for the "tel" URI", RFC 4694, October 2006
- RFC 4733 H. Schulzrinne, T. Taylor, "RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals", RFC 4733 (Obsoletes RFC 2833), December 2006
- RFC 4967 B. Rosen, "Dial String Parameter for the Session Initiation Protocol Uniform Resource Identifier", RFC 4967, July 2007
- RFC 5031 H. Schulzrinne, "A Uniform Resource Name (URN) for Emergency and Other Well-Known Services", RFC 5031, January 2008
- ITU-T T.38 International Telecommunications Union, "Recommendation T.38: Procedures for real-time Group 3 facsimile communication over IP networks ", September 2005, <<http://www.itu.int>>.

ITU-T G.168 International Telecommunications Union, "Recommendation G.168:Digital network echo cancellers “
January 2007, <<http://www.itu.int>>.

ITU-T G.711 International Telecommunications Union, "Recommendation G.711: Pulse code modulation (PCM) of
voice frequencies “, November 1988, <<http://www.itu.int>>.

ITU-T V.152 International Telecommunications Union, "Recommendation V.152: Procedures for supporting voice-band
data over IP networks”, January 2005, <<http://www.itu.int>>.

18 Changes

19 Acknowledgements for SIPconnect/1.1 Initial Contributions

The SIP Forum Technical Working Group chairs requested contributions of suggested revisions to SIPconnect/1.0 in order to kick-start SIPconnect/1.1 work, and selected CableLabs' contribution as a starting point for SIPconnect/1.1. The editor also included text and suggestions from contributions by Avaya, Broadsoft, Cbeyond, Microsoft, and Siemens in the initial (v00) draft. The editor thanks each of these contributors for their assistance..

20 Contributors to SIPconnect/1.1 and Contact Information

21 Contributors to SIPconnect/1.0 and Contact Information

SIPconnect/1.1 is a revision of SIPconnect/1.0, not a major rewrite, so it's appropriate to thank the contributors to SIPconnect/1.0 as part of this work.

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

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

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

22 Full Copyright Statement

Copyright (C) SIP Forum 2008.

This document is subject to the rights, licenses and restrictions contained in SIP Forum Recommendation [sf-draft-admin-batson-copyrightpolicy], and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE SIP FORUM DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Page 12: [1] Comment [JRE38]

John Elwell

8/29/2008 9:14:00 AM

What is the purpose of this? Is it to avoid using digest authentication on requests other than REGISTER requests? If so, I am not convinced it works (I am thinking of the recent discussions in SIPING to do with P-Asserted-Identity and whether a response received over TLS can be assumed to come from an entity previously digest-authenticated on the same TLS connection). Perhaps it works only if TLS uses mutual authentication and the subjectAltName in the IPPBX's certificate is acceptable. We at least need more explanation here of what this is trying to achieve.

Page 12: [2] Comment [JRE39]

John Elwell

8/29/2008 9:16:00 AM

Isn't this too strict? As long as the contact URI contains sufficient information to route back to the B2BUA, that should be sufficient, e.g., a GRUU would be sufficient. Also it applies only to dialog-forming and mid-dialog requests (responses too).