

This document contains BroadSoft's proposed changes to the SIPconnect recommendation for the SIPconnect 1.1 recommendation. BroadSoft based these proposed changes on internal discussions and discussions with many service providers who deploy, or who want to deploy, SIP Trunking services.

BroadSoft believes that this closely reflects the needs of the SIP Trunking service providers, as evidenced by the following endorsements.

Chris MacFarland: Chief Technical Officer, Paetec – McLeod

Randy Nicklas: Chief Technical Officer, XO Communications

BroadSoft looks forward to working with the SIP Forum in the development of the SIPconnect 1.1 recommendation, and future SIPconnect work.

Mark Enstrom - BroadSoft

IP PBX / Service Provider Interoperability

*NOTE: Document file name to be added
“SIPconnect 1.1 Technical Recommendation”*

Abstract

The SIPconnect 1.0 Technical Recommendation outlined the basic requirements to enable a direct IP peering between a SIP-enabled Service Provider network and a SIP-enabled Enterprise Network for the purpose of originating and/or terminating calls from the Public Switched Telephone Network (PSTN). It specified the minimal set of IETF and ITU-T standards that must be supported, and provided guidance in areas where the standards left multiple implementation options. SIPconnect 1.0 specified a minimal set of capabilities that should be supported by the Service Provider and Enterprise networks. This Technical Recommendation builds on the foundation provided by SIPconnect 1.0 by extending it to include a number of areas of inter-working that were omitted from the first version. 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.

Deleted: s

Deleted: s

Deleted: ave

Deleted: s

NOTE: SIPconnect 1.1 effectively obsoletes SIPconnect 1.0. Where appropriate, recommendations from the first version have been left unchanged. Note however that some modifications to prior recommendations have been made based on experience and feedback gathered through adoption of SIPconnect in the industry.

Status of this Memo

NOTE: Status to be added.

Disclaimer

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

Changes

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



SIPconnect and SIPconnect Compliant are certification marks of the SIP Forum. Implementers who wish to certify their products and services as SIPconnect 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	6	Deleted: 5
2	Conventions and Terminology	8	Deleted: 7
3	Reference Architecture	8	Deleted: 7
4	Definitions	9	Deleted: 8
5	Key Assumptions and Limitations of Scope	11	Deleted: 10
6	Standards Support	12	Deleted: 11
7	Locating SIP Servers	14	Deleted: 13
7.1	Enterprise Requirements	14	Deleted: 13
7.2	Service Provider Requirements	14	Deleted: 14
8	Signaling Security	15	Deleted: 14
9	Firewall and NAT Traversal	15	Deleted: 14
10	Authentication and Accounting	16	Deleted: 15
10.1	Authentication of the Enterprise by the Service Provider	16	Deleted: 15
10.2	Authentication of the Service Provider by the Enterprise	17	Deleted: 16
11	Enterprise Public Identities	17	Deleted: 16
12	Binding Enterprise Public Identities to Enterprise Networks	18	Deleted: 17
12.1	Static Binding of the Main Public Identity	18	Deleted: 17
12.2	Dynamic Binding of the Main Public Identity	18	Deleted: 18
12.3	Implied Binding of Alternate Public Identities	19	Deleted: 18
12.4	Dynamic Binding of Alternate Public Identities	19	Deleted: 19
13	Incoming Calls from the Service Provider to the Enterprise	19	Deleted: 19
13.1	Calls to the Main Public Identity	19	Deleted: 19
	INVITE sip:+15555551212@123.123.123.1;user=phone SIP/2.0	19	Deleted: 19
	To: <sip:+15555551212@serviceprovider.net;user=phone>	20	Deleted: 19
13.2	Calls to an Alternate Public Identity	20	Deleted: 19
	INVITE sip:+15555551212@123.123.123.1;user=phone SIP/2.0	20	Deleted: 19
	To: <sip:+15555551213@serviceprovider.net;user=phone>	20	Deleted: 19
13.3	Populating the From Header	20	Deleted: 20
14	Outgoing Calls from the Enterprise to the Service Provider	20	Deleted: 20
14.1	Populating the From header for Calls from the Main Public Identity	21	Deleted: 21
	From: <sip:+15555551212@serviceprovider.net;user=phone>	21	Deleted: 21
14.2	Populating the From header for Calls from an Alternate Public Identity	22	Deleted: 21
	From: <sip:+15555551213@serviceprovider.net;user=phone>	22	Deleted: 21
14.3	Populating then Request-URI	22	Deleted: 21
14.4	Populating the To Header	22	Deleted: 21
14.5	Considerations for Emergency Services Destinations	22	Deleted: 21
14.6	Controlling the Calling Line ID and Calling Name Presentation	23	Deleted: 22
15	Quality of Service Considerations	24	Deleted: 23
16	Media Attributes and Minimum Requirements	25	Deleted: 24
16.1	Media Capability Negotiation	25	Deleted: 24
16.2	Codec Support and Media Transport	26	Deleted: 25
16.3	Transport of DTMF Tones	26	Deleted: 25
16.4	Echo Cancellation	26	Deleted: 25
16.5	Fax and Modem Calls	27	Deleted: 25
17	PSTN Interactions	27	Deleted: 26
			Deleted: 26

(Editor)

(Editor)

17.1	Call Progress Tones	27
17.2	Early Media	28
18	Retargeting Service Interactions	28
18.1	Retargeting Related Services	28
18.2	Simple 302 Redirection	28
18.3	Retargeting via In-Dialog REFER	29
18.4	Retargeting via Out-of-Dialog INVITE	30
18.5	Message Waiting Indicator	31
19	References	32
20	Changes	34
21	Contributors and Contact Information	35
22	Full Copyright Statement	35

Deleted: 26
Deleted: 27
Deleted: 27
Deleted: 27
Deleted: 27
Deleted: 27
Deleted: 28
Deleted: 29
Deleted: 30
Deleted: 31
Deleted: 33
Deleted: 34
Deleted: 34
Deleted: 1 Introduction . 4
Deleted: 3
Deleted: ¶ ... [1]
Deleted: 4
Deleted: ¶ ... [2]
Deleted: 4
Deleted: ¶ ... [3]
Deleted: 5
Deleted: ¶ ... [4]
Deleted: 6
Deleted: ¶ ... [5]
Deleted: 7
Deleted: ¶ ... [6]
Deleted: 8
Deleted: ¶ ... [7]
Deleted: 8
Deleted: ¶ ... [8]
Deleted: 8
Deleted: ¶ ... [9]
Deleted: 9
Deleted: ¶ ... [10]
Deleted: 9
Deleted: ¶ ... [11]
Deleted: 10
Deleted: ¶ ... [12]
Deleted: 10
Deleted: ¶ ... [13]
Deleted: 11
Deleted: ¶ ... [14]
Deleted: 11
Deleted: ¶ ... [15]
Deleted: 11
Deleted: ¶ ... [16]
Deleted: 11
Deleted: ¶ ... [17]
Deleted: 14
Deleted: ¶ ... [18]
Deleted: 14
Deleted: ¶ ... [19]
Deleted: 15
... [20]
... [21]
... [22]
... [23]
... [24]
... [25]

1 Introduction

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

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

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

This document restates and in some cases updates all areas of implementation guidance found in version 1.0, including:

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

Deleted: e specific

Deleted: where this document provides

Deleted: e

This document provides additional implementation guidance related to service inter-working, including:

- Voicemail Deposit

Formatted: Bullets and Numbering

(Editor)

(Editor)

- [Message Waiting Indications](#)
- [Transfer and Forwarding scenarios](#)
- [Calling Line Identity Presentation](#)

← - - - **Formatted:** Bullets and Numbering
← - - - **Formatted:** Bullets and Numbering

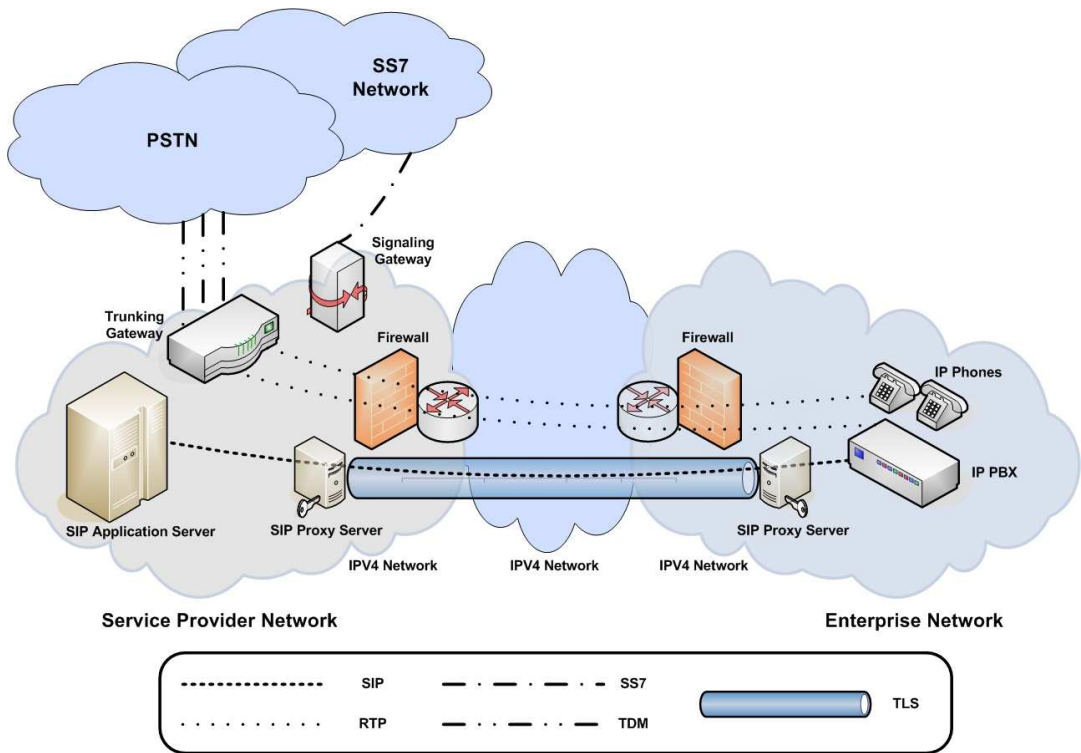
2 Conventions and Terminology

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

3 Reference Architecture

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

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



NOTE: Suggested Modification for Version 1.1 - Although it is good to have a reference architecture – in the context of the specification – I think it is difficult to impose requirements on each of the components in the diagram above – since every implementation may have a slightly different network architecture. For instance – not every Enterprise Network will have a SIP Proxy and a IP PBX – some will have just an IP-PBX managing phones – some may just have an Proxy with a bunch of IP phones – and this would need to be supported as well.

Formatted: Font: Bold

SIPConnect 1.1 should be limited in scope to defining the interface between the edge of the “Enterprise Network” and the edge of the “Service Provider Network” – and not requirements on the specific network elements in either network. All the annotations/changes I have made, and specifically anything that is normative, are based on this assumption. In this context the “blue tube” above is SIPConnect – and that’s all the specification should define.

Deleted: .

Deleted: ¶

Formatted: Bullets and Numbering

4 Definitions

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

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

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

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

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

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

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

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

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

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

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

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

5 Key Assumptions and Limitations of Scope

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

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

1. The primary service to be delivered over this interface is audio-based PSTN call origination and/or termination. The delivery of any other service (e.g. video-based services, instant messaging, etc.) is out of scope.
2. All mandatory reference architecture elements specified for the Service Provider and Enterprise Networks are in place and operational.
3. Signaling considerations between the SIP Application Server, Trunking Gateway, and Signaling Gateway is outside the scope of this document.
4. Signaling considerations between the IP PBX and other Enterprise devices (e.g. IP phones) is outside the scope of this document.
5. The Service Provider and Enterprise each operate publicly accessible DNS servers that are authoritative for one or more Internet domain(s). Alternatively, the Service Provider may delegate a sub-domain from its domain for use by the Enterprise.
6. The Enterprise network is assigned a minimum of one E.164 address, which is routed on the PSTN to the Service Provider's Signaling Gateway.
7. Emergency calling issues, for example routing to national emergency numbers such as 911, 112, 999, or 000, issues related to SIP endpoint mobility, etc. are outside the scope of this document.
8. Layer 3 network design, QoS considerations, and preconditions (e.g. RSVP) are outside of the scope of this document
9. Element management, network management, network security, and OSS considerations are outside the scope of this document.

6 Standards Support

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

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

Standard ID	Description	SAS	PBX	SPS
Rec. E.164 [2]	ITU-T Recommendation E.164: The international public telecommunication numbering plan	M	M	-
RFC 2246 [3]	The TLS Protocol Version 1.0	-	-	M
RFC 2833 [7]	RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals NOTE: Should we add "RFC 4733" here as well?	-	M	-
RFC 2782 [6]	A DNS RR for specifying the location of services (DNS SRV)	-	-	M
RFC 3261 [8]	SIP: Session Initiation Protocol	M	M	M
RFC 3262 [9]	Reliability of Provisional Responses in Session Initiation Protocol (SIP)	M	R	-
RFC 3263 [10]	Session Initiation Protocol (SIP): Locating SIP Servers	M	M	M
RFC 3264 [11]	An Offer/Answer Model with Session Description Protocol (SDP)	M	M	-
RFC 3311 [12]	The Session Initiation Protocol (SIP) UPDATE Method	M	R	-
RFC 3323 [13]	A Privacy Mechanism for the Session Initiation Protocol (SIP)	M	R	M
RFC 3324 [14]	Short Term Requirements for Network Asserted Identity	M	R	M
RFC 3325 [15]	Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks	M	R	M
RFC 3489 [16]	STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)	-	R	-
RFC 3581 [18]	An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing NOTE: Suggested Modification for Version 1.1 - Suggestion to relax this requirement for SAS to an "R" instead of the "M" requirement in 1.0. This is primarily required for "edge to edge" inter-working – which will be transparent to the SAS.	R	R	M
RFC 3725 [19]	Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)	M	R (RO)	-
RFC 4028 [21]	Session Timers in the Session Initiation Protocol (SIP)	R	R	-
RFC 4244 [22]	SIP Request History Information	M	M	-
RFC 3326 [23]	The Reason Header Field for the Session Initiation Protocol (SIP)	M	M	-
RFC 3515 [24]	The Session Initiation Protocol (SIP) Refer method	M	R	M
RFC 3842 [25]	A Message Summary and Message Waiting Indication event package	RO	RO	M

Formatted: Normal

Deleted: M

Formatted: Normal

Deleted: R

Formatted: Font: (Default) Times New Roman, 11 pt

Deleted: R

Deleted: R

	for SIP			
RFC 3265 [26]	A SIP Specific Event Notification Framework	RO	RO	M

NOTE: Suggested Modification for Version 1.1 - As suggested above, I would recommended we simplify this table to have one column for the Enterprise Network and one column for the Service Provider Network.

7 Locating SIP Servers

NOTE: Suggested Modification for Version 1.1 – I think the requirements in section 7 should be moved later in the document as they are better covered in the context of specifying the requirements for incoming and outgoing calls.

7.1 Enterprise Requirements

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

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

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

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

7.2 Service Provider Requirements

Deleted: ¶
Formatted: Bullets and Numbering

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

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

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

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

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

8 Signaling Security

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

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

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

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

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

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

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

9 Firewall and NAT Traversal

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

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

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

- Any "application/sdp" body in the message contains any "a=candidate:" lines (indicating use of the ICE extension)

- All the "c=" lines in any "application/sdp" bodies contain only public IP addresses (indicating that another element has already ensured the addresses are correct).

10 Authentication and Accounting

10.1 Authentication of the Enterprise by the Service Provider

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

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

[NOTE: Suggested Modification for Version 1.1 – Option #1 is mutual TLS - how many networks would actually meet this requirement today? Suggestion is to reverse the base requirements :](#)

- 1) [Digest Authentication – MUST](#)
- 2) [Mutual TLS - RECOMMENDED](#)

Formatted: Bullets and Numbering
Formatted: Indent: Left: 0.25"

10.1.1 [Option 1: Authentication using TLS Credentials](#)

Deleted: ¶
Formatted: Bullets and Numbering

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

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

[NOTE: Suggested Modification for Version 1.1 : Again, would suggest we modify this to specify the requirements for the respective networks -- not the network elements inside them.](#)

10.1.2 Option 2: Digest Access Authentication

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

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

1. When processing an INVITE request from an unauthenticated PBX, the SIP Application Server **MUST** challenge the message, only accepting authentication credentials that are valid within its realm.
2. When processing a REGISTER request from an unauthenticated PBX, the SIP Application Server **MUST** challenge the message, only accepting authentication credentials that are valid within its realm.
3. When challenged by the SIP Application Server, the PBX **MUST** respond with authentication credentials that are valid within the Service Provider's realm (i.e. the network account username and password supplied by the Service Provider).
4. In order to avoid unnecessary challenges, the PBX **SHOULD** include its authentication credentials using the current nonce in each request sent to the SIP Application Server.

Formatted: Indent: Left: 0",
Numbered + Level: 1 + Numbering
Style: 1, 2, 3, ... + Start at: 1 +
Alignment: Left + Aligned at: 0.25"
+ Tab after: 0.75" + Indent at:
0.75", Tabs: Not at 0.75"

Formatted: Indent: Left: 0",
Numbered + Level: 1 + Numbering
Style: 1, 2, 3, ... + Start at: 1 +
Alignment: Left + Aligned at: 0.25"
+ Tab after: 0.75" + Indent at:
0.75", Tabs: Not at 0.75"

Formatted: Indent: Left: 0",
Numbered + Level: 1 + Numbering
Style: 1, 2, 3, ... + Start at: 1 +
Alignment: Left + Aligned at: 0.25"
+ Tab after: 0.75" + Indent at:
0.75", Tabs: Not at 0.75"

Formatted: Indent: Left: 0",
Numbered + Level: 1 + Numbering
Style: 1, 2, 3, ... + Start at: 1 +
Alignment: Left + Aligned at: 0.25"
+ Tab after: 0.75" + Indent at:
0.75", Tabs: Not at 0.75"

10.2 Authentication of the Service Provider by the Enterprise

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

11 Enterprise Public Identities

For the purpose of this specification, an enterprise can have one or more "Public Identities" associated with their SIPConnect service. A public identity is simply a globally routable SIP Address-of-Record. A public identity can be represented as either a tel-uri (E.164 format) or a SIP or SIPS URI (ie. sip(s):user@host format). All public identities are owned and allocated by the corresponding Service Provider Network. An Enterprise Network is assigned one or more public identities by the Service Provider through a process outside the scope of this document.

Deleted: PSTN

Formatted: Normal

Deleted: t

In order to receive SIPConnect services, this specification requires that each Enterprise Network **MUST** have a "Main Public Identity", and **MAY** have zero or more "Alternate Public Identities". All traffic between the Service Provider Network and the Enterprise Network (ie. incoming or outgoing calls) must be associated with either the Main Public Identity or one of the Alternate Public Identities.

The "Main Public Identity" is recognized by the Service Provider Network as the default identity for the Enterprise Network. When no alternate identity is preferred (or allowed), the main public identity is used.

“Alternate Public Identities” are used in conjunction with delivering Direct Inward Dial (DID) and Direct Outward Dial services (DID) described in the sections below.

Deleted: ¶

Deleted: ¶

Formatted: Bullets and Numbering

12 Binding Enterprise Public Identities to Enterprise Networks

Formatted: Font: Bold

In order to receive an incoming call on either the main public identity (ie. the “main line”), or any of the alternate public identities (ie. a “direct line”), the Service Provider Network **MUST**, at a minimum, have a “binding” between the main public identity and the Enterprise Network. This binding is called the “Main Contact Address” – and resolves to a specific transport, port and IP address on the Enterprise Network. The “Main Contact Address” can be bound to the “Main Public Identity” statically, through provisioning in the Service Provider Network – or dynamically, through the SIP REGISTER process described in RFC 3261 [8].

Similarly, “Alternate Public Identities” can have their own respective bindings, referred to as “Alternate Contact Addresses”, that can be established statically through provisioning, or dynamically through the SIP REGISTER process described in RFC 3261 [8]. If an explicit binding is not established statically or dynamically, then the Alternate Public Identity will automatically assume an “implied binding” – which is the same as the Main Contact Address. The implied binding will be used if no explicit binding is available for the Alternate Public Identity.

Formatted: Heading 2

Formatted: Bullets and Numbering

12.1 Static Binding of the Main Public Identity

A static binding for the Main Public Identity is created by manually provisioning the contact address on the Service Provider Network. The contact address takes on the form of a SIP or SIPS URI as per RFC 3261 [8].

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

Formatted: Font: Bold

Service Provider Network **MUST** utilize DNS NAPTR and SRV queries as described in RFC 3263 [10] to resolve the IP address, transport protocol, and port number associated with the Enterprise’s domain name.

Formatted: Bullets and Numbering

12.2 Dynamic Binding of the Main Public Identity

A dynamic binding for the Main Public Identity can be established through the registration process described in RFC 3261 [8].

Formatted: Normal

If dynamic binding is used, then the Enterprise Network **MUST** support sending a REGISTER request for the Main Public Identity as per RFC 3261 [8]. The From and To header of the SIP REGISTER event **MUST** include the Main Public Identity. The Request-URI **MUST** resolve to the publicly addressable domain of the corresponding Service Provider’s SIPConnect service.

Formatted: Font: Bold

Formatted: Font: Bold

The Enterprise Network **MUST** utilize DNS NAPTR and SRV queries as described in RFC 3263 [10] to resolve the IP address, transport protocol, and port number of the associated with the Service Provider’s domain name.

The Service Provider Network **MUST** support receiving a REGISTER request from the Enterprise Network. The Service Provider Network **MAY** challenge the REGISTER request to authenticate the request. The Enterprise Network **MUST** respond to the challenge with corresponding credentials associated with the Enterprise SIPConnect account.

Formatted: Font: Bold

Formatted: Font: Bold

12.3 Implied Binding of Alternate Public Identities

An Enterprise Network may be assigned one or more alternate public identities by the Service Provider. By default, the Service Provider Network MUST consider all Alternate Public Identities to have an implied binding that is the same as the Main Contact Address.

Formatted: Heading 2

12.4 Dynamic Binding of Alternate Public Identities

A dynamic binding for the Alternate Public Identity can be established through the registration process described in RFC 3261 [8]. If a dynamic binding is established for an Alternate Public Identity – it takes precedence over the implied binding.

Formatted: Bullets and Numbering

The Enterprise Network MAY support sending a REGISTER request for one or more Alternate Public Identities as per RFC 3261 [8]. The From and To header of the SIP REGISTER event MUST include the corresponding Alternate Public Identity. The Request-URI MUST resolve to the publicly addressable domain of the corresponding Service Provider’s SIPConnect service.

Formatted: Font: Bold

The Enterprise Network MUST utilize DNS NAPTR and SRV queries as described in RFC 3263 [10] to resolve the IP address, transport protocol, and port number of the associated with the Service Provider’s domain name.

The Service Provider Network MUST support receiving a REGISTER request from the Enterprise Network on an Alternate Public Identity. The Service Provider Network MAY challenge the REGISTER request to authenticate the request. The Enterprise Network MUST respond to the challenge with credentials associated with the Enterprise SIPConnect account. Note that these credentials are typically the same credentials used to authenticate the registration of the Main Public Identity.

Formatted: Font: Bold

13 Incoming Calls from the Service Provider to the Enterprise

NOTE: Updated from original proposal – After some feedback and further research –the section below was updated to reflect using the loose routing method.

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 PBX and then transferred within the enterprise to a private extension. Calls to Alternate Public Identities are usually routed by the PBX directly to a specific user station – bypassing the attendant or operator – this is commonly referred to as “Directed Inward Dial” service.

Formatted: Normal

Formatted: Font: Italic

Formatted: Normal

Deleted: and

Formatted: Font: Bold

Deleted: <#>Calls to the Main Public Identity¶
<#>If the call is to a Main Public Identity, then the Service Provider Network MUST populate the Request-URI and To header using the rules in this section.¶

Formatted: Heading 2

Deleted: for calls to the Main Public Identity

Formatted: Font: Bold

Deleted: Main Contact Address

Deleted: for the Enterprise Network

Deleted: .

Deleted: has been dynamically registered as
"sip:+15555551212@123.123.123.1;user=phone":

Formatted: Normal

Deleted: 123.123.123.1

This specification relies on using the loose routing model for terminating calls. This section describes guidelines for populating the Request-URI, To, From and router headers for new dialog INVITE request sent from the Service Provider Network to the Enterprise Network. All other headers in the INVITE MUST comply with RFC 3261 [8]

13.1 Populating the Request-URI header

The Service Provider Network MUST populate the Request-URI of the INVITE with the actual destination identity for the call – ie the main line identity or one of the alternate identities. An example is shown below where the Main Contact Address is “sip:+15555551212@serviceprovider.net”:

INVITE sip:+15555551212@serviceprovider.net;user=phone SIP/2.0

13.2 Populating the To header

The Service Provider Network **MUST** populate the 'To:' field with the actual destination identity for the call - ie the main line identity or one of the alternate identities.

To: <sip:+15555551212@serviceprovider.net:user=phone>

13.3 Populating the Router header

The Service Provider Network **MUST** employ the loose routing model as described in RFC 3261. The Service Provider Network **MUST** populate the Router header with the corresponding contact address for the destination Enterprise Public Identity. If the destination Enterprise Public Identity is the Main Public Identity, then the "Main Contact Address" should be used. If the destination Enterprise Public Identity is an Alternate Public Identity, then the "Alternate Contact Address" should be used. If no "Alternate Contact Address" has been established (through static provisioning or dynamic registration as described in section 12), then the (implied) Main Contact Address **MUST** be used. An example is shown below where the Main Contact Address is being used:

Route 123.123.123.1

13.4 Populating the From Header

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

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

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

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

14 Outgoing Calls from the Enterprise to the Service Provider

Outgoing calls, originating from the Enterprise Network towards the Service Provider Network **MUST** assume an identity -- either the Main Public Identity or one of the Alternate Public Identities -- so the Service Provider Network can apply appropriate calling restrictions and any other origination services.

When calls are originated from extensions on the PBX that do not have an assigned public number (ie. they do not have an assigned Alternate Public Identity) then the Enterprise Network **MUST** use the Main Public Identity to originate the call.

When a call is originated from an extension on the PBX that has been assigned a public number (ie. an Alternated Public Identity), then the Enterprise Network **MAY** use the corresponding Alternate Public Identity to originate the call. This is commonly referred to as Direct Outward Dial (DOD).

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

Deleted: for calls to the Main Public Identity

Formatted: Heading 2

Deleted: th

Deleted: e

Deleted: Main Public Identity of the Enterprise Network. An example is shown below:

Deleted: Calls to an Alternate Public Identity

Formatted: Bullets and Numbering

Formatted: Font: Bold

Deleted: ¶
If the call is to an Alternate Public Identity, then the Service Provider Network **MUST** populate the Request-URI and To header using the rules in this section.¶

<#>Populating the Request-URI header for calls to an Alternate Public Identity¶

Deleted: Request-URI of the INVITE

Deleted: with

Deleted: Alternate Contact

Deleted: Address

Deleted: Enterprise Network

Deleted: .

Deleted: no explicit

Deleted: has

Formatted: Font: Bold

Deleted: INVITE

Deleted: sip:+15555551212@

Deleted: ;user=phone SIP/2.0

Deleted: <#>Populating the To header for calls to an Alternate Public Identity¶
<#>The Service Provider Network **MUST** populate the 'To:' field with the Alternate Public Identity of the Enterprise Network. An example is shown below:¶
<#>To:
<sip:+15555551213@serviceprovider.net:user=phone>¶

Formatted: Bullets and Numbering

Deleted: ¶
¶

Formatted: Bullets and Numbering

Formatted: Font: Bold

when presenting the call to the remote party – as described in RFC 3325 [15]. All other headers in the INVITE **MUST** comply with RFC 3261 [8]

14.1 Populating the From header for Calls from the Main Public Identity

If the call should be treated as a call from the Main Public Identity – meaning the Service Provider Network will apply the main line calling restrictions and origination services – then the Enterprise Network **MUST** populate the From header with the Main Public Identity:

From: <sip:+15555551212@serviceprovider.net:user=phone>

← - - - Formatted: Bullets and Numbering

← - - - Formatted: Indent: First line: 0"

← - - - Formatted: Bullets and Numbering

14.2 Populating the From header for Calls from an Alternate Public Identity

Deleted: 'To:' Field

If the call should be treated as a call from the Alternate Public Identity – meaning the Service Provider Network may apply alternate calling restrictions and origination services – then the Enterprise Network **MUST** populate the From header with the Alternate Public Identity:

From: <sip:+15555551213@serviceprovider.net;user=phone>

14.3 Populating the Request-URI

Deleted: <#>¶

Formatted: Heading 2

Formatted: Bullets and Numbering

This interface specification provides two methods of communicating the address to the Service Provider Network. The Enterprise Network **MUST** implement at least one of these options. The Service Provider Network **MUST** support both methods in order to ensure interoperability with all PBX systems.

Formatted: Bullets and Numbering

14.3.1 Option 1: SIP URI

INVITE <sip:[dialed digits] @[Service Provider Domain Name];user=phone> SIP/2.0

Formatted: Bullets and Numbering

14.3.2 Option 2: tel: URL

INVITE <tel:[E.164 Address]> SIP/2.0

Formatted: Font: Italic

Formatted: Normal, Indent: Left: 0.5"

Formatted: Heading 2

Formatted: Bullets and Numbering

14.4 Populating the To Header

The To header **MUST** adhere to the same formatting rules as that of the 'Request-URI' field described in section 14.3 above.

Formatted: Bullets and Numbering

14.5 Considerations for Emergency Services Destinations

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

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

INVITE <sip:[Country-specific emergency services address];phone-context=[Predetermined Geographic E.164 Address]@[Service Provider Domain Name];user=phone> SIP/2.0

The country-specific emergency services address is defined as the dial string used in the country of origin to request emergency services. The phone-context parameter **SHOULD** contain a valid E.164 address previously agreed upon by the Enterprise and Service Provider to represent the physical location from which the call originated. The Service Provider **SHOULD** ensure that valid location information for this E.164 address is provisioned in the ALI database.

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

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

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

14.6 Controlling the Calling Line ID and Calling Name Presentation

SIPConnect allows the Enterprise Network to control calling line ID and calling name presentation 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.

- Formatted: Heading 2
- Formatted: Bullets and Numbering
- Formatted: Normal

14.6.1 Default Calling Line ID and Calling Name Presentation

When an INVITE is sent from the Enterprise Network to the Service Provider Network, the Service Provider Network **MUST** present the Calling Line ID and Calling Name associated with the identity in the From header – 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.

- Formatted: Heading 3
- Formatted: Bullets and Numbering
- Formatted: Normal

14.6.2 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.

- Formatted: Heading 3
- Formatted: Bullets and Numbering
- Formatted: Normal
- Formatted: Font: Bold
- Formatted: Font: Bold

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 three levels of Privacy priv-values: “critical” and “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.

- Formatted: Font: Bold
- Formatted: Font: Bold

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 must have privacy enabled, the Enterprise **MUST** insert a Privacy header with a value of “id” as described in RFC 3325[15].

- Formatted: Font: Bold

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 must 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.

- Formatted: Font: Bold
- Formatted: Font: Bold

The Enterprise Network **MAY** insert a priv-value of “critical” in the Privacy header. When the Service Provider Network receives an INVITE with a Privacy header of “critical” – it **MUST** meet the requested level of privacy service. If the Service Provider Network cannot fulfill the privacy request, then it **MUST** not complete the call, but instead respond with a 500 Server Error response as required in RFC 3323 [13].

- Formatted: Font: Bold

The Enterprise Network **MAY** choose to apply local privacy policies before sending the INVITE by populating the From header with an anonymous URI in the form <anonymous@[domain name]>, in addition to requesting privacy from the privacy server in the Service Provider Network. If the From header is “anonymized” – then the Enterprise Network **MUST** provide a P-Asserted-Identity header populated with the desired originating identity for the call (either the Main Public Identity or one of the Alternate Public Identities).

Formatted: Font: Bold

14.6.3 Requesting Specific Calling Line and Calling Name Presentation

Formatted: Font: Bold

Formatted: Heading 3

Formatted: Bullets and Numbering

Formatted: Normal

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. Although, by default the calling line ID calling name **SHOULD** correspond to the acting originating identity of the call – this specification allows the Enterprise to select it. That is – the call may be originating on the Main Public Identity – but the Enterprise Network may request that the Calling Line ID and Calling Name presented to the remote party be set to one of the Alternate Public Identities. In some applications, the Enterprise Network may even request that 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 is the requirement to set the Calling Line ID and Calling Name to a free-phone service (ie. 1-800) number. Policies on the Service Provider Network dictate whether this is allowed and this is out of scope for this document.

To request a specific presentation be applied to the outgoing call, the Enterprise Network **MUST** populate the From header with the desired calling line ID and calling name, and put the preferred originating identity in either a P-Asserted-Identity or P-Preferred-Identity header as described in RFC 3325 [15].

Formatted: Font: Bold

If the Service Provider Network receives an INVITE with a P-Asserted-Identity or a P-Preferred-Identity header, it **MUST** use that header to identify the originating identity for the call. 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.

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Heading 3

Formatted: Bullets and Numbering

14.6.4 Authentication the outgoing call

Before accepting an INVITE from the Enterprise Network and originating the call, the Service Provider Network **MUST** assert the originating identity of the INVITE. This can be done in one of two ways:

- 1) Digest Authentication – as described in RFC 3261 [8]
- 2) Mutual TLS – as described in RFC 3261 [8]

Formatted: Bullets and Numbering

Digest Authentication **MUST** be supported by the Service Provider Network and the Enterprise Network.

Mutual TLS **MAY** be supported by the Service Provider Network and **MAY** be supported by the Enterprise Network.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Tab after: 0.5" + Indent at: 0.5"

15 Quality of Service Considerations

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Bullets and Numbering

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

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

Packet Type	DiffServ PHB	DSCP Value	Binary Equivalent Value
SIP Signaling Message	CS5	40	Binary = 101000

RTP Media	EF	46	Binary = 101110
-----------	----	----	-----------------

NOTE: This section seems to go against the following statement specified in section 5:

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

16 Media Attributes and Minimum Requirements

16.1 Media Capability Negotiation

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

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

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

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Tab after: 0.5" + Indent at: 0.5"

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

16.2 Codec Support and Media Transport

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

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

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

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

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

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

16.3 Transport of DTMF Tones

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

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

16.4 Echo Cancellation

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

NOTE: Not all devices that originate or terminate voice traffic need ITU-T G.168 – pure IP media servers that don't have analog interfaces cannot introduce echo – and should not be required to include echo cancellation. Can we just relax the language a bit?

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.

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Deleted: ¶

Formatted: Bullets and Numbering

16.5 Fax and Modem Calls

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

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

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

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

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

Formatted: Bullets and Numbering

17 PSTN Interactions

17.1 Call Progress Tones

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

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

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

17.2 Early Media

Formatted: Bullets and Numbering

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

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

18 Retargeting Service Interactions

Formatted: Bullets and Numbering

18.1 Retargeting Related Services

Deleted: Redirection

A number of common services can cause a call to be retargeted, 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:

Formatted: Heading 2

Formatted: Normal

- Using a 302 response to an INVITE is common for services that forward calls before answering – such as Call Forwarding and Voicemail deposit.
- 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 attended transfers.
- Transfer scenarios can be performed using multiple INVITE dialogs, using third party call control.

Deleted: -

Deleted: .

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.

Deleted:

Deleted:

Deleted:

Deleted:

18.2 Simple 302 Redirection

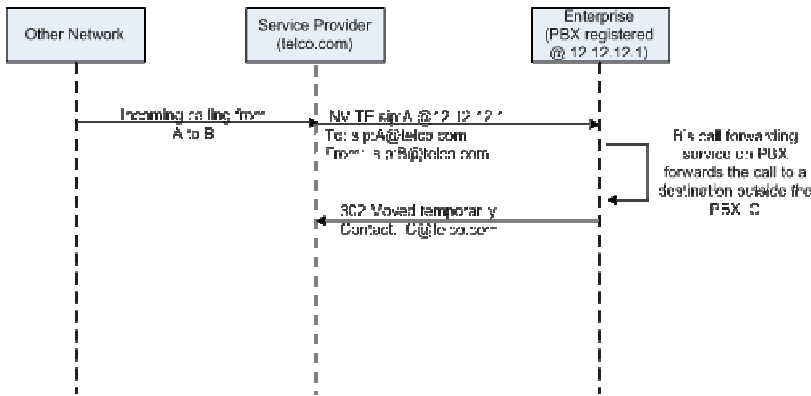
Deleted: ¶
¶
¶

A 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 the diagram below.

Formatted: Heading 2

Formatted: Bullets and Numbering

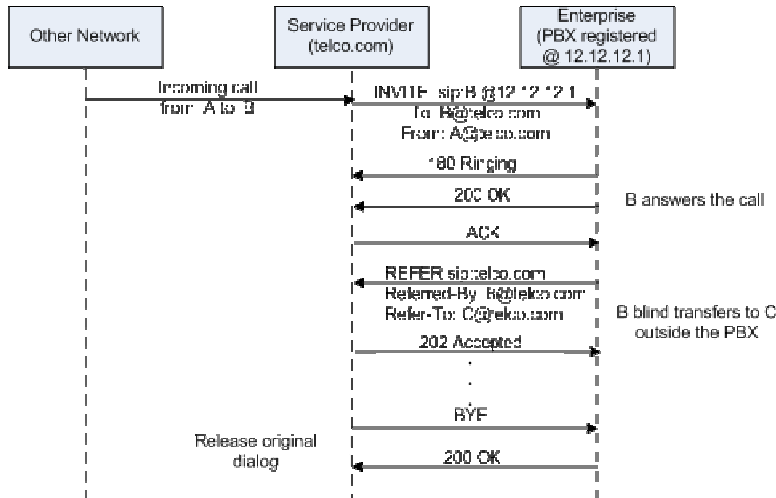
Formatted: Normal



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 [8]. The Enterprise Network **MAY** support sending a 302 redirection response back to the Service Provider Network as per RFC 3261 [8]. How the Service Provider Network handles the 302 Moved Temporarily is implementation specific and outside the scope of this document.

18.3 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 the diagram below:



Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Heading 2

Formatted: Bullets and Numbering

Formatted: Normal

Deleted: ¶

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 [24]. The Enterprise Network **MAY** support sending a REFER back to the Service Provider Network as per RFC 3515 [24]. The REFER **MUST** be sent in the context of the corresponding INVITE dialog that is being referred.

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Font: Bold

Exactly how the Enterprise Network processes the REFER is implementation specific and out of scope of this document – but it **MUST** conform to RFC 3515 [24]. It is **RECOMMENDED** that the Service Provider Network release the existing dialog with the Enterprise Network as soon as possible to free up resources over the SIP trunk. The Service Provider Network **SHOULD NOT** wait for the Enterprise Network to release the originally referred dialog.

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Font: Bold

NOTE: Out-of-dialog REFER requests **MUST NOT** be sent from the Enterprise to the Service Provider network.

Formatted: Font: Bold

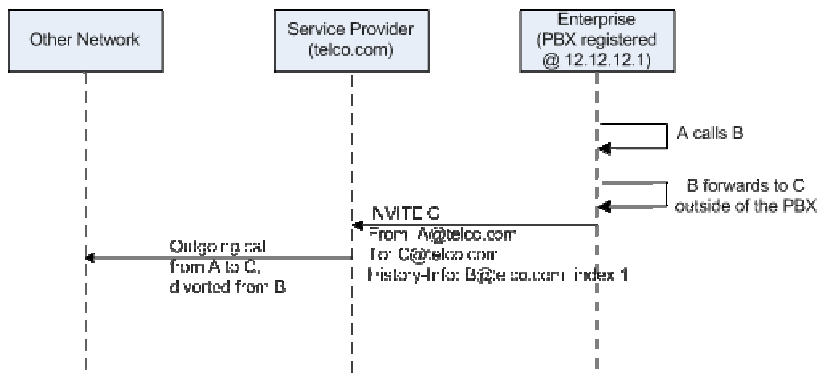
18.4 Retargeting via Out-of-Dialog INVITE

Formatted: Heading 2

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 the diagram below:

Formatted: Bullets and Numbering

Formatted: Normal



Formatted: Normal

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.

Formatted: Normal, Indent: Left: 0.5"

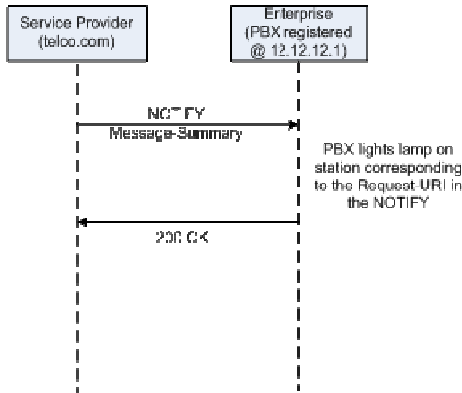
The History-Info header described in RFC 4244 [24] provides a framework for preserving request history information as a call is retargeted from one hop to the next hop. The History-Info [24] **MUST** be supported by the Service Provider Network and the Enterprise Network.

Formatted: Normal

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 [24]. 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 [24].

18.5 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 (as a standalone SAS or integrated with a general purpose SAS). 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 SAS hosting the voicemail application must be able to notify the enterprise when a new voicemail has been received. This is depicted in the diagram below using a SIP NOTIFY for message-summary.



Deleted: ¶

Formatted: Heading 2

Formatted: Bullets and Numbering

Formatted: Normal

Deleted: ¶

If voicemail is hosted on a SAS in the Service Provider network, then the Service Provider Network **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 Network **MUST** support receiving a SUBSCRIBE event for message-summary. The Service Provider Network **MAY** also support sending an unsolicited NOTIFY to the Enterprise Network (ie. implied subscription).

Deleted: ¶

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Font: Bold

If voicemail is hosted on a SAS in the Service Provider network, then the Enterprise Network **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 Enterprise Network **MUST** support sending a SUBSCRIBE event for message-summary. The Enterprise Network **MAY** also support receiving an unsolicited NOTIFY message-summary event (ie. "implied subscription").

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Font: Bold

Deleted: ¶

Formatted: Bullets and Numbering

19 References

- [1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [2] International Telecommunications Union, "Recommendation E.164: The international public telecommunication numbering plan", May 1997, <<http://www.itu.int>>.
- [3] T. Dierks, C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.
- [4] M. Handley, V. Jacobson, "SDP: Session Description Protocol", RFC 2327, April 1998.
- [5] K. Nichols, S. Blake, F. Baker, D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, December 1998.
- [6] A. Gulbrandsen, P. Vixie, L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.
- [7] H. Schulzrinne, S. Petrack, "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals", RFC 2833, May 2000.
- [8] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.
- [9] J. Rosenberg, H. Schulzrinne, "Reliability of Provisional Responses in Session Initiation Protocol (SIP)", RFC 3262, June 2002.
- [10] J. Rosenberg, H. Schulzrinne, "Session Initiation Protocol (SIP): Locating SIP Servers", RFC 3263, June 2002.
- [11] J. Rosenberg, H. Schulzrinne, "An Offer/Answer Model with Session Description Protocol (SDP)", RFC 3264, June 2002.
- [12] J. Rosenberg, "The Session Initiation Protocol (SIP) UPDATE Method", RFC 3311, October 2002.
- [13] J. Peterson, "A Privacy Mechanism for the Session Initiation Protocol (SIP)", RFC 3323, November 2002.
- [14] M. Watson, "Short Term Requirements for Network Asserted Identity", RFC 3324, November 2002.
- [15] C. Jennings, J. Peterson, M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", RFC 3325, November 2002.
- [16] J. Rosenberg, J. Weinberger, C. Huitema, R. Mahy, "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)", RFC 3489, March 2003.
- [17] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", RFC 3550, July 2003.

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

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

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

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

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

← - - - Formatted: Bullets and Numbering

20 Changes

21 Contributors and Contact Information

Formatted: Bullets and Numbering

22 Full Copyright Statement

Formatted: Bullets and Numbering

Copyright (C) SIP Forum 2006.

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 5: [1] Deleted	remlap42	7/2/2008 10:43:00 PM
2 Conventions and Terminology	6	
Page 5: [2] Deleted	remlap42	7/2/2008 10:43:00 PM
3 Reference Architecture	6	
Page 5: [3] Deleted	remlap42	7/2/2008 10:43:00 PM
4 Definitions	7	
Page 5: [4] Deleted	remlap42	7/2/2008 10:43:00 PM
5 Key Assumptions and Limitations of Scope	9	
Page 5: [5] Deleted	remlap42	7/2/2008 10:43:00 PM
6 Standards Support	10	
Page 5: [6] Deleted	remlap42	7/2/2008 10:43:00 PM
7 Locating SIP Servers	12	
Page 5: [7] Deleted	remlap42	7/2/2008 10:43:00 PM
7.1 Enterprise Requirements	12	
Page 5: [8] Deleted	remlap42	7/2/2008 10:43:00 PM
7.2 Service Provider Requirements	12	
Page 5: [9] Deleted	remlap42	7/2/2008 10:43:00 PM
8 Signaling Security	13	
Page 5: [10] Deleted	remlap42	7/2/2008 10:43:00 PM
9 Firewall and NAT Traversal	13	
Page 5: [11] Deleted	remlap42	7/2/2008 10:43:00 PM
10 Authentication and Accounting	14	
Page 5: [12] Deleted	remlap42	7/2/2008 10:43:00 PM
10.1 Authentication of the Enterprise by the Service Provider	14	
Page 5: [13] Deleted	remlap42	7/2/2008 10:43:00 PM
10.2 Authentication of the Service Provider by the Enterprise	15	
Page 5: [14] Deleted	remlap42	7/2/2008 10:43:00 PM
11 Enterprise PSTN Identities	15	
Page 5: [15] Deleted	remlap42	7/2/2008 10:43:00 PM
12 Enterprise URI Formatting and Addressing Rules	16	

Page 5: [16] Deleted remlap42 7/2/2008 10:43:00 PM

[12.1 'From:' Field](#) Error! Bookmark not defined.

Page 5: [17] Deleted remlap42 7/2/2008 10:43:00 PM

[12.2 'To:' Field – PSTN Destinations](#)Error! Bookmark not defined.

Page 5: [18] Deleted remlap42 7/2/2008 10:43:00 PM

[12.3 'To:' Field – Emergency Services Destinations](#) 20

Page 5: [19] Deleted remlap42 7/2/2008 10:43:00 PM

[12.4 'To:' Field -- Other Destinations](#)Error! Bookmark not defined.

Page 5: [20] Deleted remlap42 7/2/2008 10:43:00 PM

[12.5 Request-URI](#) Error! Bookmark not defined.

Page 5: [21] Deleted remlap42 7/2/2008 10:43:00 PM

[13 Service Provider URI Formatting and Addressing Rules](#) 18

Page 5: [22] Deleted remlap42 7/2/2008 10:43:00 PM

[13.1 'From:' Field](#) Error! Bookmark not defined.

Page 5: [23] Deleted remlap42 7/2/2008 10:43:00 PM

[13.2 'To:' Field](#) 20

Page 5: [24] Deleted remlap42 7/2/2008 10:43:00 PM

[13.3 Request-URI](#) Error! Bookmark not defined.

Page 5: [25] Deleted remlap42 7/2/2008 10:43:00 PM

[14 Quality of Service Considerations](#) 21