

SIP Enterprise Connect Requirements

Working Draft

Notice

This PacketCable™ Requirements document is a cooperative effort undertaken at the direction of Cable Television Laboratories, Inc. (CableLabs®) for the benefit of the cable industry. Neither CableLabs, nor any other entity participating in the creation of this document, is responsible for any liability of any nature whatsoever resulting from or arising out of use or reliance upon this document by any party. This document is furnished on an AS-IS basis and neither CableLabs, nor other participating entity, provides any representation or warranty, express or implied, regarding its accuracy, completeness, or fitness for a particular purpose.

PacketCable, DOCSIS and CableHome are trademarks of Cable Television Laboratories, Inc.

© Copyright 2007-2008 Cable Television Laboratories, Inc.

All rights reserved.

Document Status Sheet

Document Title: SIP Enterprise Connect Requirements

Revision History:

Date: May 28, 2008

Status: Working Draft

Distribution Restrictions: For distribution to SIPForum Members

Table of Contents

1	SERVICE AND FEATURE REQUIREMENTS.....	4
1.1	GENERAL ASSUMPTIONS.....	4
1.2	BASIC 2-WAY CALLING.....	4
1.2.1	Direct Inward and Outward Dial (DID/DOD).....	4
1.2.2	Private Network Services (Voice VPN).....	5
1.2.3	Calling Name & Number Delivery (Caller ID).....	6
1.2.4	Caller ID Blocking.....	6
1.2.5	Early Media.....	6
1.2.6	Multimedia.....	6
1.2.7	Session Limits.....	6
1.3	CALL FEATURES FOR INTER IP-PBX TO SERVICE PROVIDER CALLS.....	7
1.3.1	Hold.....	7
1.3.2	Conference.....	7
1.3.3	Transfer.....	7
1.3.4	Call Forwarding.....	7
1.3.5	Voice Mail.....	8
1.4	REGULATORY SERVICES.....	8
1.4.1	Emergency Calls.....	8
1.4.2	Operator Services.....	8
1.4.3	Equal Access Carrier Routing.....	9
2	SIP ENTERPRISE CONNECT FUNCTIONAL REQUIREMENTS.....	10
2.1	REFERENCE ARCHITECTURE.....	10
2.1.1	IP-PBX Connection to Service Provider Network.....	11
2.2	REGISTRATION.....	11
2.3	ADDRESSING IP-PBX USERS.....	12
2.4	IP-PBX START-UP PROCEDURES (SERVICE PROVIDER NETWORK DISCOVERY).....	12
2.5	BILLING AND ACCOUNTING.....	13
2.6	QUALITY OF SERVICE.....	13
2.7	SECURITY AND AUTHENTICATION.....	13
2.8	NETWORK ADDRESS TRANSLATION (NAT) AND FIREWALL TRAVERSAL.....	13
2.9	FAULT DETECTION AND ISOLATION.....	13
2.9.1	RTP Loopback Test Capability.....	13
2.9.2	VoIP Metrics.....	14

List of Figures

FIGURE 1 – FUNCTIONAL REFERENCE ARCHITECTURE.....	10
---------------------------------------------------	----

1 SERVICE AND FEATURE REQUIREMENTS

The primary application for SIP Enterprise Connect is the transport of voice sessions (media and signaling traffic) between a SIP-based IP-PBX located on the customers' premise network and the SIP elements in the Service Provider network, terminating into the PSTN or another SIP UA. This section provides additional detail on the SIP Enterprise Connect services and features that must be supported by this interface in a cable environment. Most call features work transparently over the SIP Enterprise Connect interface. The features identified in this section are only those that may place unique requirements on the interface.

1.1 General Assumptions

1. The IP-PBX is a device that is located in the customer's network. Since the IP-PBX is not in the Service Provider network, the assumption is that the IP-PBX is considered an un-trusted element by the service provider.
2. The IP-PBX may be managed by the service provider, managed by the customer, or the management may be shared between the customer and the service provider.
3. The interface between the IP-PBX and SP network carries all the signaling and bearer traffic between the IP-PBX and the global network. In general, IP-PBX users receive their features from the IP-PBX. However, certain call features may be provided to the IP-PBX users by the Service Provider network.
4. The interface will support the following types of voice calls:
 - Direct Inward Dialing (DID)
 - Direct Outward Dialing (DOD)
 - Toll Free (800) calls
 - Domestic Long Distance, International Long Distance
 - Intra-LATA, Inter-LATA calls
 - Emergency and operator assisted calls

1.2 Basic 2-way calling

This section describes requirements related to support basic 2-way calls across the SIP Enterprise Connect interface.

1.2.1 Direct Inward and Outward Dial (DID/DOD)

An IP-PBX user with DID capability can receive calls directly from users external to the IP-PBX, without requiring an IP-PBX attendant.

An IP-PBX user with DOD can originate calls directly to users external to the IP-PBX without requiring an IP-PBX attendant. The external terminating user (UAS) could be located anywhere in the global network; e.g., a user served by the home network (including a user in another IP-PBX), a user served by a peered network, or a user in the PSTN.

An IP-PBX that supports DID or DOD capability will have a unique "default" Address of Record (AOR), and one or more additional AOR's belonging to and assigned by the Service Provider network. Typically the default AOR is the main number for an Enterprise site, while each of the additional AOR's identifies a user served by the IP-PBX. For DID calls, the called address contains the AOR identifying the terminating IP-PBX

user. For DOD calls, the calling address contains the AOR identifying the originating IP-PBX user. The AOR can take the form of a SIP or Tel URI identifying a telephone number (i.e., an E.164 number) or an email style SIP URI (see section 2.3 for more details on addressing).

In order to help combat spoofing, the SP network verifies that calls originating from the IP-PBX are from valid users served by that IP-PBX with permission to originate calls into the SP network. On receiving an originating call request from the IP-PBX, the SP network asserts the identity (AOR) of the originating user using the contents of the P-Preferred-ID and P-Asserted-Identity header in the received request as a hint to which of the multiple users served by the IP-PBX is originating the call. If no hint is provided, or if the hint doesn't identify a user served by the IP-PBX, then the SP network can assert a default AOR for the IP-PBX, based on local policy. Local policy could also dictate that the SP network always assert the default AOR, for those enterprises that want to present a singular identity to the network. The default AOR could contain a special number such as an 800 number that the called user could use to contact the enterprise on a subsequent call.

AORs do not need to be assigned to IP-PBX users that don't support DID/DOD, since from the Service Provider's perspective they aren't directly addressable. These users can still originate or receive calls to/from users outside the IP-PBX. However, such calls are always routed via an IP-PBX attendant that does have DID/DOD, so that from the Service Provider's perspective, these calls are to/from the attendant.

1.2.2 Private Network Services (Voice VPN)

Private network services are traditionally supported in legacy PBXs using tie-lines facilities to directly connect two or more PBXs. This effectively creates a single virtual PBX with a uniform private numbering plan and a uniform set of intra-enterprise features that operate seamlessly across all PBXs. An example of private network services is intra-enterprise inter-PBX extension dialing, where a user in one PBX can call a user in the same enterprise but served by a different PBX by dialing the called user's private extension number.

In the case of IP-PBXs, private network services (aka "voice VPN" services) can be supported using a variety of techniques that fall into two main categories; direct exchange of private traffic between IP-PBXs (e.g., via direct IP connection, or using an IP encapsulation technology), or indirect exchange of private traffic between IP-PBXs via the SIP Enterprise Connect interface and Service Provider network.

1.2.2.1 Private Network Services via Direct Exchange

In this case, IP-PBXs support private network services by exchanging private signaling and media traffic directly over IP, or possibly using an encapsulating technology such as Layer 2 Tunneling Protocol Version 3 (L2TPV3) or Multiprotocol Label Switching (MPLS). The Service Provider network may provide the transport or encapsulation mechanism, but is otherwise transparent to the actual signaling and media traffic.

Support of private services via direct exchange of private traffic is out-of-scope for SIP Enterprise Connect.

1.2.2.2 Private Network Services using SIP Enterprise Connect

In this case, the IP-PBX sends the SIP signaling and RTP media associated with private network services over the interface to the Service Provider network, just like it does for public network services. The Service Provider can distinguish between the public and private traffic, and for private traffic it provides message routing with signaling transparency in the exchange of SIP messages between the IP-PBXs.

The only private network service required by SIP Enterprise Connect is extension dialing, which enables users in different IP-PBXs to directly call each other by dialing a local extension when the IP-PBXs serve the same enterprise. Extension dialing must also be supported between IP-PBX users and enterprise users hosted on the Service Provider network when the users belong to the same enterprise.

1.2.3 Calling Name & Number Delivery (Caller ID)

SIP Enterprise Connect must support the ability to convey calling name and number for calls originating from or terminating to the IP-PBX. Calling name and number can be delivered when the target user is idle (traditional caller ID), or busy in an existing call (caller ID with call-waiting).

Since the IP-PBX is un-trusted, the Service Provider network must validate and assert the caller ID information for calls originated by IP-PBX users. In this case, the asserted caller ID may identify the individual IP-PBX user, or some other entity representing the IP-PBX or the enterprise. The asserted caller ID identifies the calling number, and may additionally identify the calling name.

1.2.4 Caller ID Blocking

Caller ID Blocking is a service provided by the Service Provider network that enables an originating user to control whether or not his/her caller ID information is delivered to the called user. Specifically, Caller ID Blocking allows an originating IP-PBX user to control whether or not the user's calling name and number is delivered with outgoing (DOD) calls. The SIP Enterprise Connect interface must support a mechanism that enables the originating IP-PBX to indicate to the Service Provider network on a per call basis whether the originating user's calling name and number are to be delivered or blocked.

The Service Provider network must not deliver caller ID information to un-trusted entities when caller ID blocking is in effect. Specifically, when caller ID blocking is indicated, the SP network must "anonymize" the identity of the calling user in the call terminating request before sending the request to the IP-PBX.

1.2.5 Early Media

SIP Enterprise Connect must support early media, which is media exchanged before the call is answered. The early media stream may be one-way or two-way, and can be established for calls originating from or terminating to the IP-PBX.

A common use-case for 1-way early media is ring-back tone from the PSTN; i.e., IP-PBX user A calls PSTN user B, A hears ring-back tone sourced from the PSTN via early media while waiting for B to answer.

A feature that requires 2-way early media is solicitor blocking; i.e., IP-PBX user A calls hosted Service Provider user B, A is connected to an intermediary Application Server in the Service Provider network for collection of a greeting before offering the call to B. The media stream between the IP-PBX user and the Application Server is bi-directional; from the Application Server to request the greeting, and to the Application Server to record the greeting response.

In general, early media for a call can be established with a single intermediary, sequentially with a series of different intermediaries, and/or with the final called user.

1.2.6 Multimedia

SIP Enterprise Connect must support G.711 audio codecs and may support other audio codecs. The interface may support voice-band-data relay codecs such as T.38 and V.152. The interface may also support the DTMF-relay mechanism defined in RFC4733 for the DTMF digits 0-9 and * and # . The interface must be able to negotiate a common codec when the calling and called users support different but overlapping sets of codecs.

1.2.7 Session Limits

The Service Provider network must be able to limit the number of incoming, outgoing, and total calls across the IP-PBX to Service Provider network interface based on configured limits per IP-PBX. When the Service Provider network receives an originating or terminating call request from/to the IP-PBX, and establishment of

the new call would cause one of these session limits to be exceeded, the Service Provider network will reject the new-call request by sending an appropriate error response back to the originating user.

1.3 Call Features for Inter IP-PBX to Service Provider Calls

This section identifies the call features that must be supported for calls between the IP-PBX and the Service Provider network. In general, features for IP-PBX user are controlled by the IP-PBX itself, while features for users outside the IP-PBX are controlled by an entity external to the IP-PBX (say, by an Application Server in the Service Provider network). When a call spans the IP-PBX / Service Provider network interface and the user at either end of the call invokes a feature, the interface must support any interworking procedures required to make the feature work.

1.3.1 Hold

SIP Enterprise Connect must support the ability to put active DID/DOD calls on hold. For example, an IP-PBX user can put a call on hold and make a consultation call to another party. Or, a non-IP-PBX user can put an IP-PBX user on hold. When the call is put on hold, the held party may receive some kind of hold treatment such as music-on-hold (MOH). The holding party can also restore a previously held call to the previous active status. It is expected that the IP-PBX will generate its own music-on-hold across the interface to the SP network when the IP-PBX or one of its users put the call on hold. The mechanism for performing call-hold should follow the "a=sendonly", or "a=inactive", SDP attribute mechanism defined in RFC 3264.

1.3.2 Conference

SIP Enterprise Connect must support the various forms of conference (three-party, multi-party) when one or more of the conference legs is between the IP-PBX and the Service Provider network. Typically, the IP-PBX will provide the conference bridge for conferences initiated by an IP-PBX user, while the Service Provider network will provide the conference bridge for conference calls initiated outside the IP-PBX. The Service Provider network may also provide the conference bridge on behalf of the IP-PBX for meet-me style conferences.

1.3.3 Transfer

SIP Enterprise Connect must support the various forms of call transfer (consultative, blind, etc.), when the users involved in the transfer are located inside and outside the IP-PBX. The call transfer procedures must be capable of releasing the media and signaling across the interface when the transfer-to leg doesn't traverse the interface.

Note that for call-conference/transfer where one or more legs are over the SIP Enterprise Connect interface, there are no restrictions on where the user outside the IP-PBX is located; i.e., user could be in home network, peer IP network, PSTN, domestic, or international.

1.3.4 Call Forwarding

Call Forwarding features divert a call from its original target to a new, revised target, based upon the subscription data of the target party. The conditions for forwarding a call can be situational, as in the case of Call Forwarding on Busy Line (CFBL) or Call Forwarding on Don't Answer (CFDA), or the call forwarding can be unconditional, as in the case of Call Forwarding Variable (CFV). Furthermore, call forwarding can be based on user reach-ability (say user is not registered), or based on network availability (e.g., service maintenance, network outage).

SIP Enterprise Connect must support call-forwarding when either the IP-PBX destination or the destination external to the IP-PBX is retargeted. The call forwarding procedures must be capable of releasing the media and signaling across the interface when the forward-to leg doesn't traverse the interface. Call forwarding loop detection may be supported.

In general, call-forwarding services for IP-PBX users will be provided by the IP-PBX, and not by the Service Provider network. However, there are certain limited cases where the Service Provider network may need to retarget a call destined for an IP-PBX user on behalf of the IP-PBX.

Issue: how does the SP network handle the case where the IP-PBX stays in the signaling path of a forwarded call, and the forward-to INVITE from the IP-PBX contains an asserted identity for a user that doesn't belong to that IP-PBX? This can happen, say, when a DID call from the PSTN is forwarded by the IP-PBX back to PSTN, and IP-PBX stays in the signaling path because it's paying for the forwarded-to leg. In this case the SP network should just leave the PSTN user as the asserted identity, but it won't because that user isn't on its list of users served by that IP-PBX.

1.3.5 Voice Mail

The Service Provider network can provide voice mail service to IP-PBX users on behalf of the IP-PBX. This includes the recording of voice messages for IP-PBX users, providing IP-PBX user access to their voice mail recordings, and providing message-waiting indication to the IP-PBX users. (Note that voice mail service may also be provided to IP-PBX users by the IP-PBX itself.)

1.4 Regulatory Services

1.4.1 Emergency Calls

The SIP Enterprise Connect interface, together with the IP-PBX and the Service Provider network must support traditional emergency call procedures, including:

- Route call to the correct Public Safety Answering Point (PSAP) based on the network asserted identity of calling IP-PBX user
- Signal the asserted identity of calling IP-PBX user in the form of calling DN to PSAP, as key into Automatic Location Information (ALI) database
- Disable features during emergency call (e.g., IP-PBX user cannot put emergency operator on hold)
- Network hold (where IP-PBX call is not released when IP-PBX user hangs up)
- Operator ringback (where, during emergency call, the operator gets attention of emergency caller via ringing (user onhook) or ROH (user offhook))

There is no requirement for IP-PBX users to convey location information across the SIP Enterprise Connect interface.

Issue: More detail is needed on the emergency call requirements for IP-PBXs; for example, is there a requirement to assert an identity for emergency calls that is different than the identity asserted for regular calls, is support of Network hold required for emergency calls from an IP-PBX, etc.

1.4.2 Operator Services

The SIP Enterprise Connect interface must support operator-assisted 0- and 0+ DOD calls. Support of operator busy-line-verify and operator-interrupt are not required.

1.4.3 Equal Access Carrier Routing

The Service Provider network must support the ability to route DOD calls based on the pre-assigned or dialed equal access carrier and to signal the carrier to the PSTN.

2 SIP ENTERPRISE CONNECT FUNCTIONAL REQUIREMENTS

2.1 Reference Architecture

Figure 1 contains a reference architecture that shows various ways that an IP-PBX can interconnect to a Service Provider network. The diagram is meant to be sufficiently general and abstract to apply to multiple real-world architectures. The diagram shows a Home Network and a Peer Network. The Home Network contains the following logical functions:

- **Edge Proxy:** Polices the trust boundary between the user and the Home Network. Maintains a security association between itself and the user device, and asserts the identity of the authenticated users on incoming SIP messages. Ensures that incoming SIP messages conform to the protocol requirements of the Home Network. Routes incoming SIP messages between the IP-PBX and the core network.
- **Registrar:** As a SIP registrar, maintains Address of Record (AOR) to IP contact-address bindings for registered users.
- **Home Proxy:** Authenticates incoming SIP requests, and authorizes user access to services. May invoke the Application Server component to apply originating and terminating services. For originating requests, determines next-hop routing. For terminating requests, provides the Location Service for request targeting (say, by consulting the registrar database).
- **Route Proxy:** Provides intra-domain routing when the Home Network contains multiple Home Proxies.
- **Border Element:** Provides the interconnect point to external peer networks, or static trunk Enterprises. May provide functions such as topology hiding, and IPv4/6 interworking.
- **Applications:** Provides hosted network-based features and services to Service Provider users.

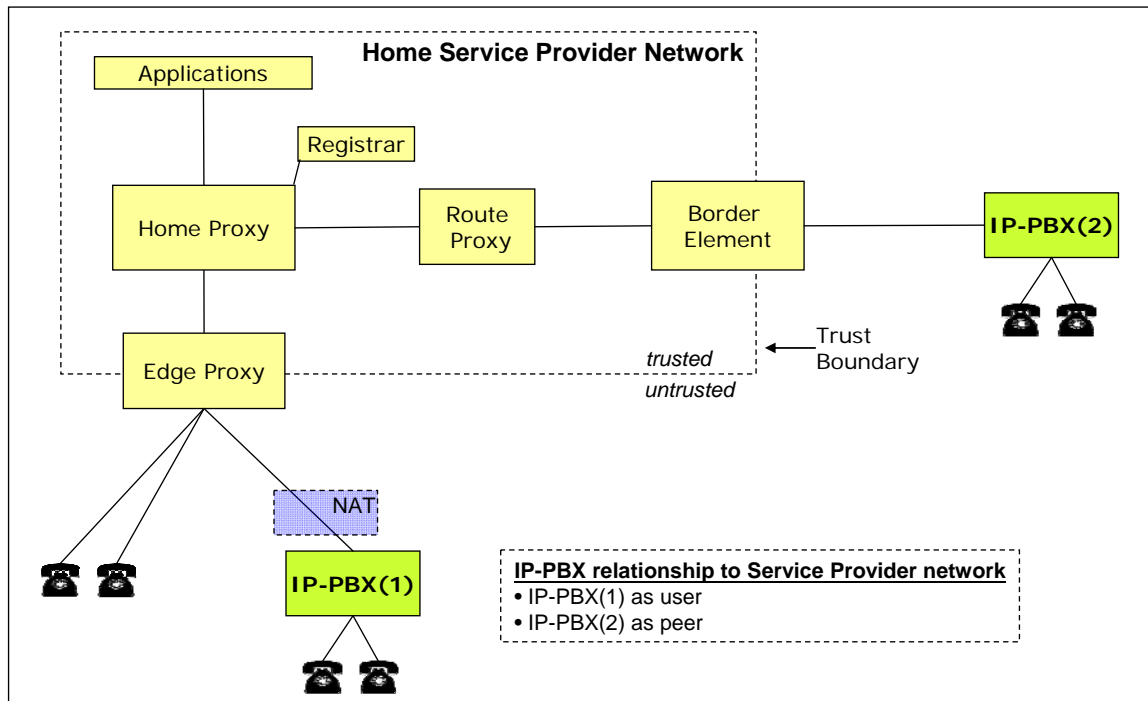


Figure 1 – Functional Reference Architecture

2.1.1 IP-PBX Connection to Service Provider Network

A globally routable contact address of an IP-PBX may not be available to the Service Provider network via DNS. In such cases, to enable communication from the Service Provider network to the IP-PBX, the IP-PBX must perform SIP Registration with the Service Provider SIP network. In addition, the Service Provider SIP network architecture may have a dependency on IP-PBX registration in order to perform authorization and authentication, and provide network services on behalf of the IP-PBX.

In this case, the IP-PBX appears as a "user" served by the Service Provider SIP Network.

SIP Enterprise Connect requires support of IP-PBX SIP registration with the Service Provider network. From a trust perspective, the IP-PBX is considered outside the trust domain of the Service Provider. A Service Provider Edge Proxy provides the entry point to the Service Provider's SIP network.

Where a globally routable contact address of an IP-PBX is available in DNS, and where the Service Provider SIP Network can provide network services without requiring registration, or such services are not required, the IP-PBX may not be treated as a user, but rather as a peer network component. In this case, a Border Element provides the entry point to the Service Provider's SIP network. Such a configuration is out of scope for SIP Enterprise Connect.

Beyond registration related requirements, the above arrangements are intended to be transparent to the IP-PBX with respect to services provided by the IP-PBX and the SIP interface requirements to the Service Provider SIP Network.

2.2 Registration

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

One method to provide IP-PBX reachability is through DNS, whereby the Enterprise provides SIP reachability information to its IP-PBX in DNS (e.g., SRV or A records), and the Service Provider 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 IP-PBX transport addressing publicly viewable in DNS, (2) it requires the Enterprise to make its IP-PBX publicly reachable even if a NAT exists between the IP-PBX and the Service Provider, (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.

The requirements for IP-PBX and Service Provider interconnection which drive the need for a Registration model are:

-
1. The IP-PBX must be reachable without requiring the Enterprise to make its IP-PBX transport addressing publicly viewable to anyone other than the Service Provider.
 2. The IP-PBX must be reachable from Service Provider edge proxies without requiring the Enterprise to open its IP-PBX to receive SIP messages from the public Internet.
 3. The Service Provider must be able to resolve the Enterprise IP-PBX transport addressing to use for SIP requests, including the path through one or more edge proxies.
 4. The Enterprise and Service Provider must be able to discover reachability failures before an active SIP request is sent; in other words before a call is attempted, or other forms of end-to-end communication are attempted. This is required to avoid excessive post-dial-delays and other user-perceived failures.

The reachability information can be statically provisioned in the Service Provider network, or dynamically discovered using a SIP Registration procedure. The IP-PBX and SP network must support an implicit registration model, where the IP-PBX registers the single AOR assigned to the IP-PBX itself, which implicitly registers all the users in that IP-PBX.

The registration procedure must be scalable to support IP-PBXs serving multiple hundreds of users, or as few as one.

2.3 Addressing IP-PBX Users

Each IP-PBX user that has DID or DOD capability must have an AOR that belongs to and is assigned by the Service Provider network. Two AOR forms must be supported:

- Global Tel URI containing an E.164 number; e.g., tel:+13035551234
- SIP URI of the telephone syntax form containing a global Tel URI; e.g., SIP:+13035551234@serviceprovider.net;user=phone

AORs in the form of an email-style SIP URI may also be supported:

- E.g.; SIP:john@pbx-1.serviceprovider.net

The IP-PBX itself may also be assigned an AOR that follows the same rules as described above for the IP-PBX users. DID calls addressed to this AOR may be routed to an IP-PBX attendant.

For DOD calls, the originating IP-PBX can identify the target called user using one of the AOR forms described above, or using a SIP URI of the form "user=dialstring":

- E.g., SIP:03035551212@serviceprovider.net;user=dialstring

In the case where the IP-PBX identifies the called user using a SIP URI "user=dialstring", the Service Provider network must convert the SIP URI "user=dialstring" to one of the valid AOR forms described above before routing the call to the terminating network.

2.4 IP-PBX Start-up Procedures (Service Provider network discovery)

Upon startup, the IP-PBX 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 Edge Proxy. It is recommended that the IP-PBX should use standard discovery procedures such as:

- No discovery (factory, manual or network-based pre-configuration of Service Provider Network Servers addressing).

-
- DHCP Option 66 for tftp provisioning server discovery.
 - RFC 3263 "Locating SIP Servers".

Upon startup, if the IP-PBX obtains its IP Address using a DHCP mechanism, the IP-PBX should immediately re-register if the IP address changes when the lease expires. Therefore, changing the IP address may cause active calls between the IP-PBX and the service provider network to be dropped.

2.5 Billing and Accounting

The Service Provider network may generate billing records for calls originating from the IP-PBX. These calls may be billed to the individual IP-PBX user or to some other entity representing the IP-PBX or the enterprise. The IP-PBX should not be 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 IP-PBX).

2.6 Quality of Service

Control of Quality of Service (QoS) over the HFC broadband access network is based on the PacketCable Multimedia (PCMM) architecture, and conforms to the network-initiated resource reservation procedures defined in PacketCable 2.0. The Service Provider network must be able to allocate QoS resources on the access network to support the session bandwidth requirements of IP-PBX calls that traverse the IP-PBX to SP network interface. The Service Provider network must also be capable of imposing provisioned limits on the overall incoming, outgoing and total bandwidth utilized by the IP-PBX, with the ability to temporarily burst beyond the provisioned limits. The IP-PBX must provide sufficient information in SDP offer/answer to enable the SP network to accurately determine the QoS resource requirements for the session.

The IP-PBX should be able to set the Differentiated Services Code Points (DSCP) values for SIP signaling and RTP/RTCP packets to conform with the Service Provider DSCP plan.

2.7 Security and Authentication

SIP Enterprise Connect requires support of Transport Layer Security (TLS) to secure SIP signaling at the IP-PBX to Service Provider network interface. In addition, the Service Provider network must be able to disable signaling security based on operator policy. The IP-PBX and Service Provider network must support SIP Digest authentication procedures for authentication of the IP-PBX by the Service Provider network.

2.8 Network Address Translation (NAT) and Firewall Traversal

Signaling and media traffic across the IP-PBX to SP network interface must be able to traverse NAT/Firewalls located in the enterprise. The NAT-traversal mechanism will vary depending on the actual deployment of the IP-PBX within the enterprise network, but when applicable will include the use of the Outbound procedures for SIP signaling NAT traversal, and ICE procedures for media NAT traversal.

2.9 Fault Detection and Isolation

2.9.1 RTP Loopback Test Capability

SIP Enterprise Connect must support a mechanism that enables the Service Provider network to initiate a test call to the IP-PBX to establish an RTP loopback session where the IP-PBX loops the incoming RTP stream received from the Service Provider network back to the Service Provider network. Two loopback modes must be supported; one where the RTP packets are looped back before decode/encode (where the IP-PBX acts as an

RTP packet reflector), and one where the IP-PBX decodes and re-encodes the received RTP payload before sending the RTP stream back to the Service Provider network.

2.9.2 VoIP Metrics

SIP Enterprise Connect requires support for the collection and reporting of the RTCP-XR VoIP metrics package specified in RFC 3611 for media streams that traverse the IP-PBX to Service Provider interface.