1 SIP Carriers

1.1 AT&T

1.2 Introduction

This document is intended for the setup and configuration of options for the Interactive Intelligence Interaction Center (IC) server for use with the AT&T Flex Reach and Toll Free offerings. This document covers setup and configuration relative only to the IC server and the Carrier. Other configuration (stations, permissions, QoS, etc…) are outside the scope of this document. The interoperability test consisted of the following products"

AT&T Service Tested	Status
AT&T Flex Reach	Completed
AT&T Toll Free	Completed

Product Tested	Version Tested
Interaction Center (xIC)	3.0 SU-1
Dialogic HMP	3.0 SU-176
Interaction SIP Proxy	4.0
Interaction Media Server	3.0 SU-1
ACME SBC Net-Net 4250	5.0.0. Patch 13
IP Phones	
Polycom IP 560	3.0.0.0258
Cisco 7960	8.8

1.3 Product Descriptions

Interaction Center (xIC) – Interaction Center delivers an innovative pre-integrated application suite to manage all business communications on one platform. xIC's powerful contact center applications and PBX / IP PBX call processing, voicemail, fax server and unified messaging capabilities extend its reach throughout the enterprise - connecting and empowering agents, supervisors and business users, to elevate productivity, performance and customer service.

Interaction SIP Proxy – The SIP Proxy is a standalone proxy server that enables load balancing, redundancy, and protocol conversion in a simple, easy to configure application. The Interaction SIP Proxy will maintain the current status of all outbound destinations to ensure that real-time failover to a backup call path will occur. In the AT&T integration, it can be used in place of or in conjunction with the ACME SBC to facilitate real time failover to the backup xIC server and the primary/secondary AT&T IP destinations.

Interaction Media Server – A standalone server used with an xIC integration that provides a dramatic increase in IP system scalability and reliability by processing the

majority of all media RTP audio flows. The audio processing is offloaded from the xIC server to the dedicated media server or servers registered to the xIC servers.

ACME SBC – The ACME Session Border Controller is used to bridge the customer network to the AT&T IP network to support the services provided (IP Toll Free and Flex Reach). The Border Controller ensures that the session, consisting of SIP signaling and RTP, is converted, measured, and/or modified for calls to traverse both the customer and remote networks successfully.

2 Special Notes

xIC Version

The AT&T offerings were certified using Interactive Intelligence IC server 3.0. There were a few issues uncovered during the certification process, which are resolved by Interactive Intelligence in the IC server Service Update (SU) 2. If SU2 is not an available option, contact Interactive Intelligence support for the appropriate Engineering Special (ES) which will resolve any issues specific to this service.

T.38 Faxing – Requires that the call originate as a G.729 call. An inbound G.711 fax cannot be re-invited to T.38.

Remote Priority Codecs

The IC server does not accept remote priority codecs. The codec that will be selected for use is the highest one in the IC server list that matches one offered by the carrier. Please put the carrier desired codec at the top of the list to avoid any issues.

G.729 Annex B support

The IC server can use G.729 with the Annex B option, however it is not dynamically configurable per call. It is enabled on a given line (as demonstrated in the appropriate configuration section below), and is only an always on, or always off option.

G.726 support

The IC server does not support G.726 in a standalone fashion. An Interactive Intelligence Media Server can be added for G.726 support, however at the time of writing of this document, there were still some technical issues being sorted out, and G.726 was not certified.

Failover time

The IC server for a UDP line does not keep the current status of the line, meaning, when using UDP (which is the only option at the time of writing this document) it will have to fail each time a call is placed to the line. AT&T's requirement for this failover time is approximately 6 seconds, while the default IC server time is 15 seconds. This can be mitigated by using an Interactive Intelligence Interaction SIP Proxy (which does keep the current status of the line), or by adjusting options in the respective Line's Transport Menu (the adjustments are detailed in the configuration section below).

Flex Reach Phone Numbers

A customer may receive one of 2 types of DIDs from AT&T: Virtual TNs and non-virtual TNs.

A Virtual TN is one that has an NPA that is different from the NPA at the customer site to which it is being routed. For a virtual TN, AT&T will pass 10 digits to the PBX. For example, if a PBX telephone is associated with a VTN, the number received from AT&T would be 10 digits (i.e. 732-216-2700).

A non-virtual TN has an NPA that is the NPA as the customer site. For a non virtual TN, AT&T will pass the length of the phone extension plus some prefix if needed (typically a 4 digit extension

without a prefix). If a PBX telephone is associated with a non virtual TN, the number received from AT&T would be 4 digits (i.e. 2701 for a 908-216-2701 TN).

However, when originating calls to AT&T, the calling party number must be a 10 digit number regardless of the type of TN associated with the phone that is originating the call. On the PBX, a specific 10 digit AT&T TN will always be used as the calling number for PBX to AT&T calls.

3 Overview

3.1 Network Diagram

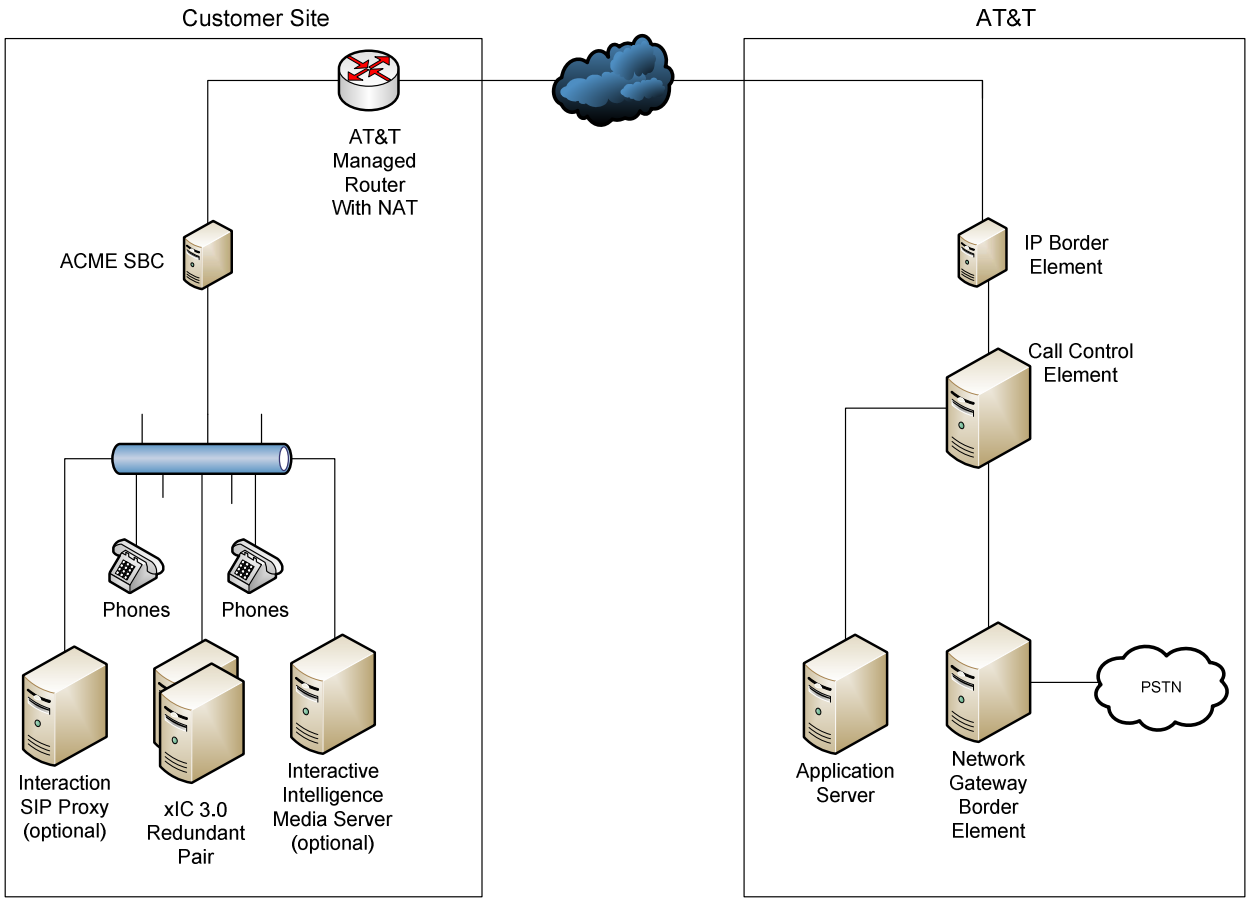

Figure 1: Diagram of General Network Setup

3.2 Proxy Description Overview

Customer Site

IC Server: The IP address entered into the Outbound Proxy will be the local side of the IP Border Element. Shown in **Figure 1** above.

Refer to section *4.1.6* for more detail.

IP Border Element: The destination Proxy address(es) of the local side of the Border Element will be directed to the primary and secondary IP addresses of the IC server redundant pair or the Interaction SIP Proxy.

The destination Proxy address(es) of the far side (AT&T Managed Router facing side) will be the primary and secondary addresses provided by AT&T during provisioning of the service. Shown in **Figure 1** above.

Refer to section *7* for more detail.

AT&T Network

AT&T will request the IP address of the customer's border element interface connected to the AT&T Managed Router. Shown in **Figure 1** above.

4 IC Configuration Guide

4.1 Line Configuration

The line page has a vast majority of the configuration options required for SIP Carrier setup. This is the section that configures the connection to the carrier's servers, any authentication or registration information, and basic configuration needs.

As stated before, two lines must be created. These lines are required, one for the AT&T connection, and one for the stations. Each portion of the lines page will be explained as it relates to the AT&T Service. For this document, the AT&T connection line will be referred to as *AT&T SIP Line*, and the station line will be referred to as *stations*. Also, any reference to a menu, while talking about the line configuration, will refer to the options on the left side of the line configuration page, and tabs will refer to the standard tab interface across the top of the line configuration page.

4.1.1 Line Menu

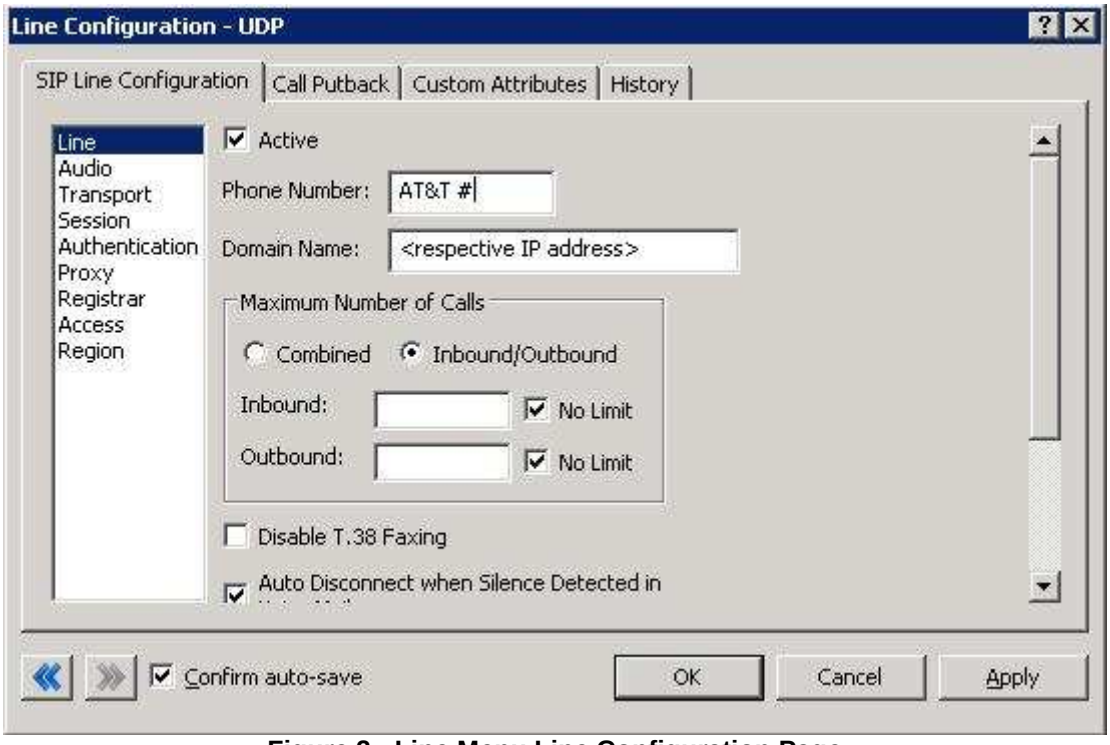

Figure 2: Line Menu Line Configuration Page

4.1.1.1 Active

The active box should be checked. This activates the line. If this box is not checked, the line will not be available for any function. This can also be affected by right

clicking on the line in Interaction Administrator, dropping to the *Set Active* menu option, and selecting *Yes*.

4.1.1.2 Phone Number

The phone number provided by the SIP Carrier should be entered into this box. The number entered is used in the "From" header in outbound SIP calls. This is very important to have correct as some AT&T validation is done one this number. Incorrect numbers can lead to some functionality (e.g. international calling, etc…) not working as expected or at all.

4.1.1.3 Domain Name

This box should contain the publicly facing IP that can reach the IC server (e.g. external IP of the element to which AT&T or the premise equipment should be sending packets). This is appended to the URL in the SIP messages.

4.1.1.4 Disable T.38 Faxing

AT&T's SIP Carrier service supports the T.38 faxing protocol by default. Leave this box unchecked if you do not have (or whish to use) an analog to SIP capable FXS type device to connect an analog fax machine to the system.

4.1.1.5 Remainder of Line Menu Options

These have no major direct impact on the SIP carrier configuration, and should be addressed according to business needs.

4.1.2 Audio Menu

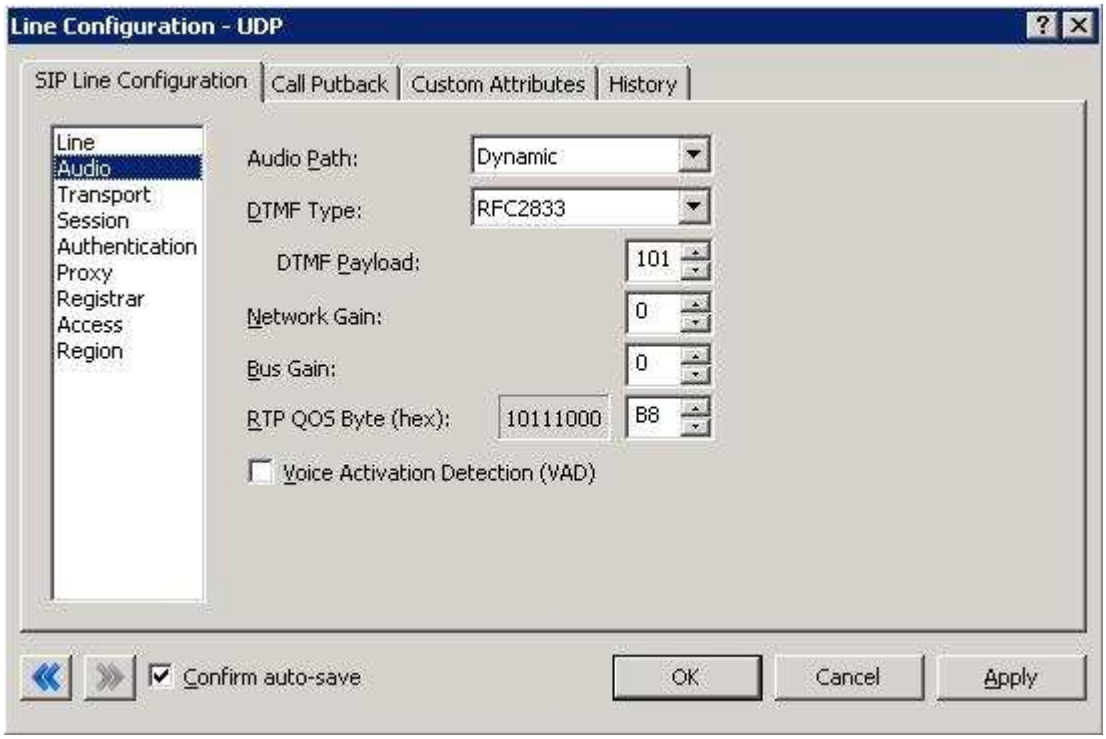

Figure 3: Audio Menu Line Configuration Page

4.1.2.1 Audio Path

This is for the most part, the choice of the client with respect to the business being done on the server. However, there are **several important caveats**.

1. *Dynamic* audio for SIP carriers has significantly less delay as compared to *Always In* audio (~100ms).
2. The audio will be brought into the IC server when set to *Dynamic Audio* for any call that is recorded (just for that call, not permanently). If using a Media Server recorded calls will not travel through the IC server.

4.1.2.2 DTMF Type

DTMF has three options, *Inband*, *RFC2833*, and *RFC2833 Only*. These are up to the discretion of the user. All three are supported with the following caveats:

AT&T requires the RFC2833 to be identified in the Invite message which requires Normal Media. To use Normal Media, the Disable Delayed Media checkbox needs to be selected (or Normal Media selected in the same location from the dropdown in a post-GA IC 3.0 server) from the session menu described later. Disabling Delayed media is the recommended method by Interactive Intelligence for all SIP Carriers.

RFC2833 – If using Delayed Media, the DTMF type will fall back to Inband.

RFC2833 Only – If using Delayed Media, the call will fail.

Inband - Delayed Media will have no effect on Inband DTMF

4.1.2.3 DTMF Payload

To use DTMF options (especially the control codes in the AT&T IP Toll Free offering) AT&T and the IC server must negotiate the same payload. The recommended way for this to happen is to upgrade the IC 3.0 server to SU1 or later, or request an ES from Interactive Intelligence that will negotiate the DTMF payload from endpoint to endpoint properly.

This can also be done manually using a packet capture to attempt to match DTMF payload being sent by AT&T, however this method is not reliable, and *not* recommended.

4.1.2.4 Voice Activation Detection (VAD)

This checkbox controls the Annex B option when using G.729. The IC server will *not* dynamically negotiate G.729 with annexb=yes. If Annex B is desired, this box must be checked, otherwise it will always use the annexb=no option. If it is required to have both another line can be set up with some differentiating factor one with Annex B enabled, and one without, then use the difference to select between the two. The reseller or an Interactive Intelligence support option can give more information on how this can be configured for the desired result.

4.1.2.5 Remainder of Audio Menu Options

These have no major direct impact on the SIP carrier configuration, and should be addressed according to business needs.

4.1.3 Transport Menu

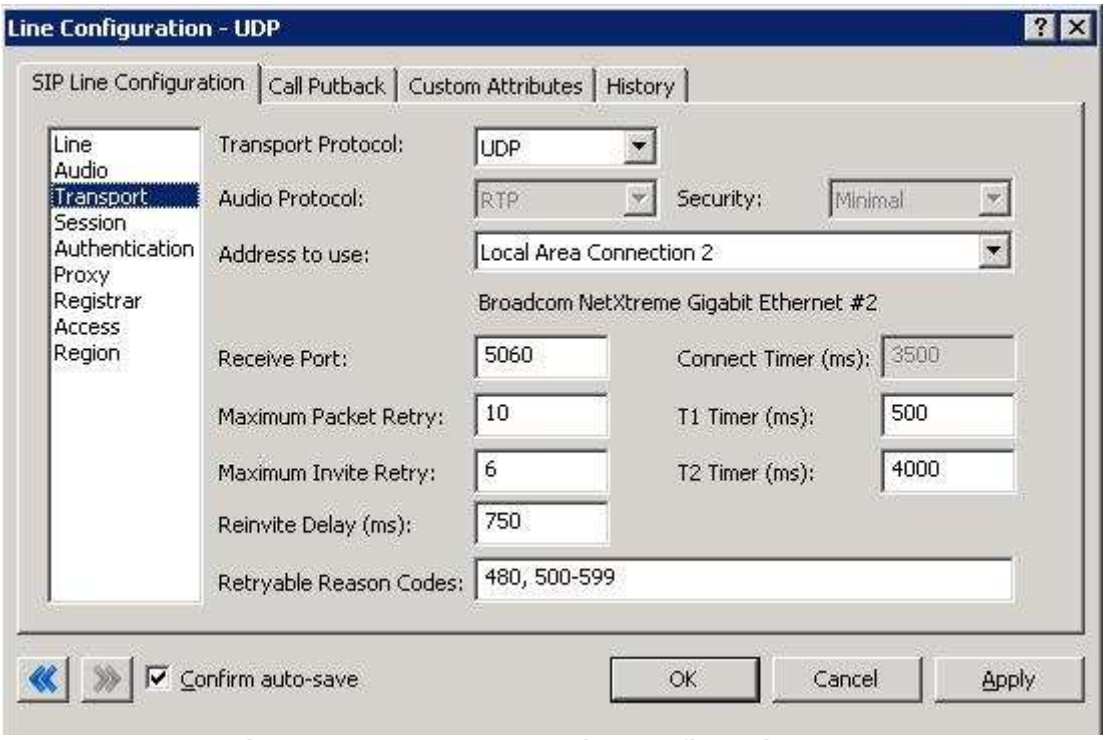

Figure 4: Transport Menu Line Configuration Page

4.1.3.1 Transport Protocol

This option should be set to UDP, unless an agreement for TCP or TLS support has been agreed upon with the SIP Carrier. As of Feb 12, 2008 AT&T has support for UDP by default. TCP and TLS are not currently supported.

4.1.3.2 Receive Port

This option should be set to 5060 (the standard SIP port), unless an agreement for an alternative port has been agreed upon with the SIP Carrier.

4.1.3.3 Configuration to Match Requested Failover Timeout Limits

The Transport Menu is also where adjustments can be made to match the timeout limitations for failover set by AT&T. At the time of writing this document, AT&T requests a 6 second or lower failover time. This can be done in one of three ways.

Option 1: Use an Interactive Intelligence SIP Proxy, which can maintain the current status of all addresses receiving SIP traffic. In this case, the failover would be instantaneous, as it would not attempt to use the line that was not available. This would be the best option if available.

Option 2: Set the Maximum Invite Retry option on this menu to be 3 rather than the default of 6. IC server INVITE message retries are sent using a growing method (e.g. the delay between each attempt grows to give the endpoint more time to recover). The default value of 6 would provide approximately 15 seconds before attempting the next proxy in the list. This would be the best option if an Interactive Intelligence SIP Proxy is not available.

Option 3: Alter the T1 and T2 timer settings. While it is possible to change these to lower the failover time, they tend to be more standard across various SIP devices and it is not recommended.

4.1.3.4 Remainder of Transport Menu Options

These have no major direct impact on the SIP carrier configuration, and should be addressed according to business needs.

4.1.4 Session Menu

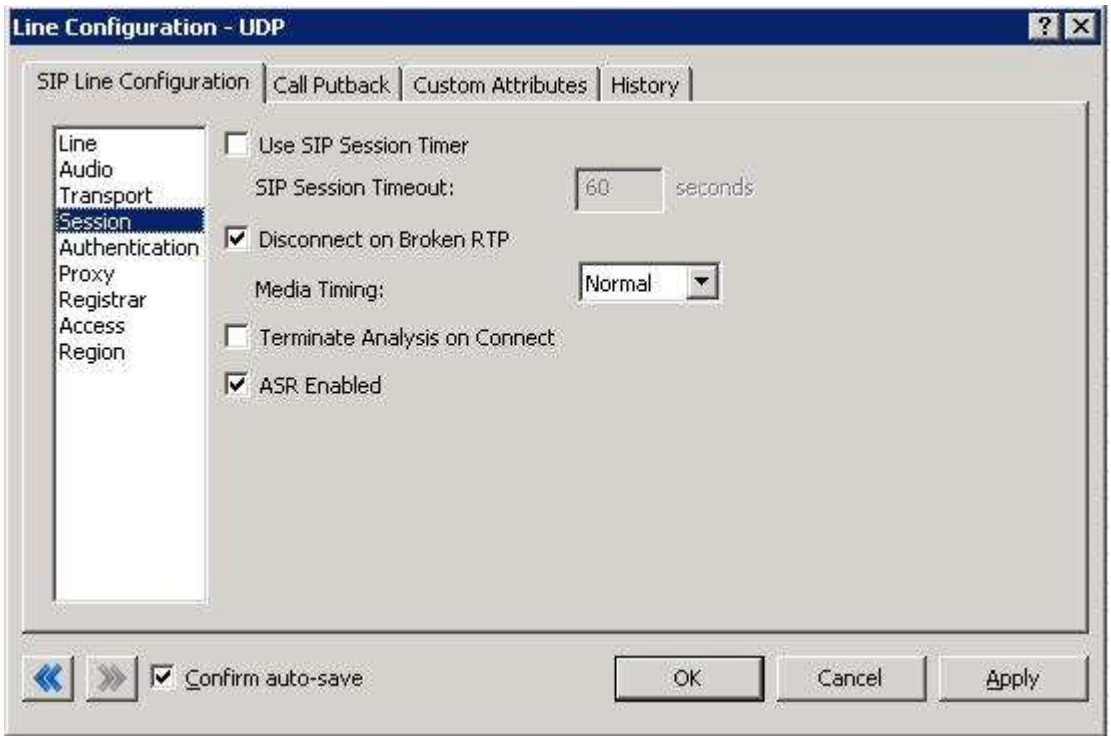

Figure 5: Session Menu Line Configuration Page

4.1.4.1 Disable Delayed Media

This checkbox controls Delayed Media support (in a post-GA IC 3.0 server, it is a dropdown that has Delayed, and Normal options). It must be checked to allow RFC2833 DTMF tones to work, as stated above (4.1.2.2 DTMF Type). Checking this box (or setting to normal) is the recommend method by Interactive Intelligence for all SIP Carriers, and is required for the AT&T service to function properly.

It is theoretically possible to have a delayed media option with AT&T, but is not part of the standard offering, would require special configuration from their side, and has not been through any kind of Interactive Intelligence/AT&T certification process.

4.1.4.2 Remainder of Session Menu Options

These have no major direct impact on the SIP carrier configuration, and should be addressed according to business needs.

4.1.5 Authentication Menu

This box must be checked to enable authentication to the SIP Carrier. At the moment, AT&T uses a static IP model with no authentication, so nothing should be done with this page. However, were they to require authentication, the *User Name* and *Password* fields should be filled out with the appropriate information provided by the SIP Carrier.

4.1.6 Proxy Menu

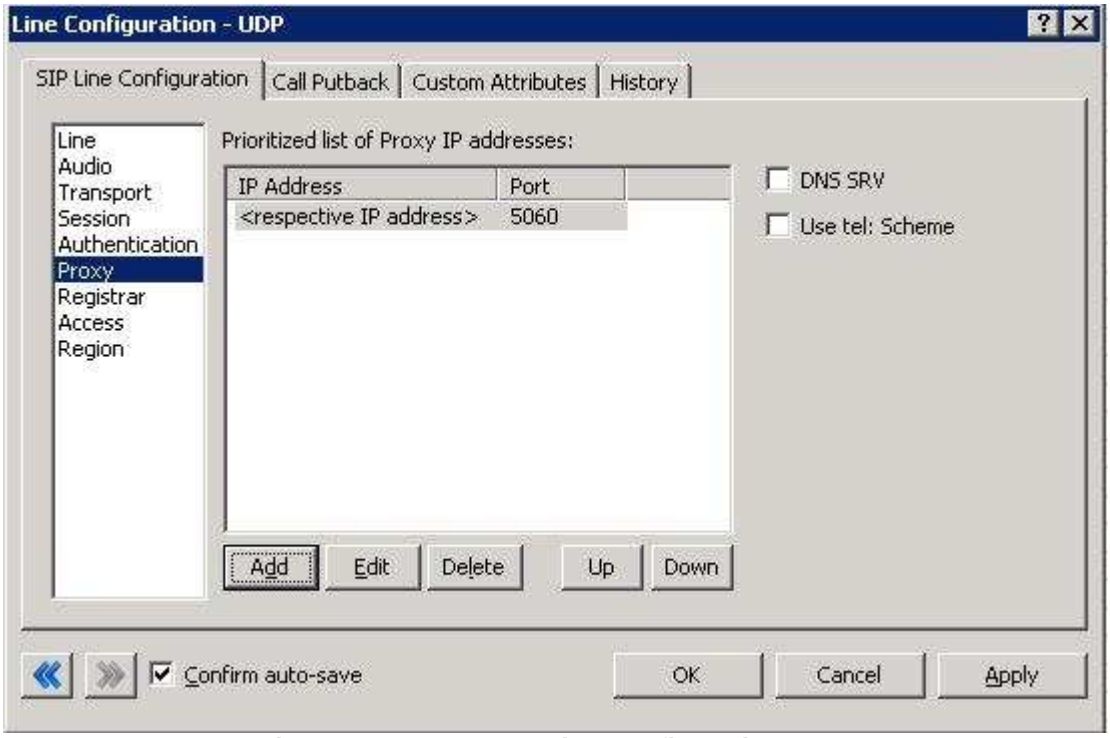

Figure 6: Proxy Menu Line Configuration Page

4.1.6.1 Prioritized list of Proxy IP addresses

This box is somewhat of a misnomer in the case of some SIP Carriers. In the case of AT&T, the proxy entry should be configured to send information directly to their network or border element. As such, the proxy address entered here should be the address of a Session Border Controller (SBC) or if not using a Session Border Controller, the address provided by AT&T in the preinstall step. The device will then forward the data and calls on to the AT&T core network.

4.1.6.2 Remainder of Proxy Menu Options

These have no major direct impact on the SIP carrier configuration, and should be addressed according to business needs.

4.1.7 Registrar Menu

4.1.7.1 External Phone Numbers

This box is not currently used by AT&T's configuration. In most cases it would be used to register multiple numbers to the same IC server. However as AT&T uses a static IP method, they do the registration/routing setup on their end and do not require the IC server to request the various numbers itself.

4.1.7.2 Prioritized list of Registrar IP addresses

This box is not used in AT&T's current configuration. The current system of providing a static IP or FQDN makes registration messages unnecessary.

4.1.8 Access Menu (Access Control lists)

If your business needs require that your endpoints (i.e. phones) use port 5060, Access Control lists are recommended. The 3.0 and higher versions of the IC server come with default station lines that are set to 8060. If using these default station lines for your endpoints, and not requiring multiple lines that are using the same protocol, and port, this section can be skipped. These lists are recommended if not using the default station lines because separate lines allow better tracking of resource utilization.

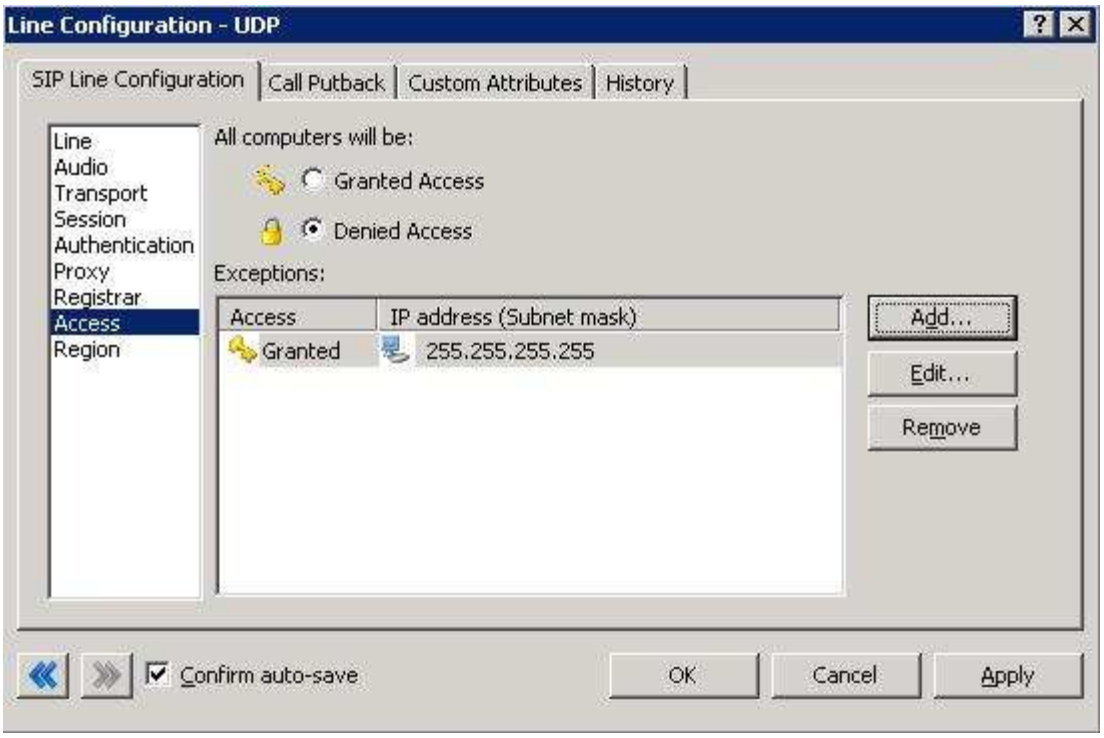

Figure 7: Access Menu Line Configuration Page (note the 255.255.255.255 address is a sample, and the actual number should be respective to the customer needs) .

4.1.8.1 AT&T SIP Line

For the access menu, the radio button should be shifted to the value:

By default, all computers will be: ***Denied Access***.

In the access list below the radio button, the resolved IP address for each proxy server **MUST** be added. The "add menu" has a DNS lookup option if the only information provided by the carrier were FQDNs. This allows the IC server to talk to all the required elements of the SIP carrier.

4.1.8.2 Stations Line

In the case of the stations line, this is up to the discretion of the user. It is possible to enter in single IP's, IP groups (using subnet masks), or allow everything. The user has several options based on business needs and security requirements. However note that only one line can be selected to "*Granted Access"* per port per IC server.

The reason why the SIP Carrier Line was selected to be ***Denied Access*** was because it has far fewer and less complicated entries than the line that will be supporting all the local endpoints.

4.1.9 Region Menu

This should be set at the user discretion, however the user should take care to assure the location supports the proper codecs supported by the SIP Carrier.

In the case of AT&T, only G.711 (mu-law and A-law), G.726 and G.729 are supported, so selecting a location that does not have any of these as an option would cause the line not to function properly. Given bandwidth and situational information, AT&T typically recommends using G.729 (this can be the default by moving it to the top of the list, if it is not supported by the other end device, then it should fall back to the second in the list and so on).

Important Note: The IC server does not by default support G.726. It should not even be included in the supported list in a 3.0 GA IC server, as it could cause issues. SU1 or later will have the ability to have G.726 in the list without an issue, but as of now, it will not be able to be used unless an Interactive Intelligence Media Server is used in conjunction with the IC server.

5 SIP Proxy Support

Note: If using a NAT/PAT type solution, a SIP Proxy can only be used in conjunction with a SIP Carrier that supports a static IP proxy (on their side, the same thing entered into the proxy menu on the lines page, not the SIP proxy). If this is not supported, the SIP Proxy can not properly pass its return address through to the carrier.

If a SIP Proxy is to be used in a NAT/PAT environment, then the externally facing IP of the **SIP Proxy** must be entered in the following places in the AT&T SIP Line configuration.

- On the proxy menu, in place of those provided by the Carrier
- On the registrar menu, in places of those provided by the Carrier

Also, the SIP Proxy (in a non NAT/PAT environment, or the NAT/PAT externally facing IP) must have the IP address provided to AT&T. Otherwise it will reject messages coming to it from an unknown IP.

The information regarding the SIP Carrier is then transferred to the appropriate places in the SIP Proxy. The SIP Proxy then feeds the required info back to the SIP Carrier. It is required to put the SIP Proxy information in the IC server. This is due to the fact that it is no longer directly talking to the SIP Carrier, and all information coming and going must be relative to the SIP Proxy.

6 Fax Caveats

AT&T supports useable and functioning T.38 faxing. However if the customer would like to use an analog fax machine connected to the network, or if T.38 faxing is not an option, the way to circumvent this problem is with an analog to SIP FXS device connecting an analog fax machine to the IP network. The FXS device will pass the SIP information on allowing for G.711 pass-through (which is the carrying of the fax signal through the voice packets on the network). This has been tested using an AudioCodes Media Pack, and a Cisco FXS card on its SIP Gateway.

Note: In the case of AT&T it may be possible to use G.729 to do the pass-through faxing, however due to the compression used by the codec, and the sensitivity of fax communications, it is not recommended (and not tested) by Interactive Intelligence.

Note: Interactive Intelligence does not support T.38 SG3 faxing at the time this document was created. It does however, support G3 faxing.

6.1 AudioCodes Media Pack Configuration

Aside from the standard configuration options that must be entered for general SIP to analog usage (e.g. proxy name, IP address, etc…) two additional features must be set to enable the Media Pack to properly pass the fax.

One is the *Fax Signaling Method*. This must be set to *G.711 Transport*, and can be found by selecting the following links from the main page of the Media Pack configuration.

- Protocol Management
    - Protocol Definition
        - General

The other required configuration setting is Fax/*Modem Bypass Coder Type*, which must be set to *G711Mulaw*. This configuration option can be found by selecting the following links from the main page of the Media Pack configuration.

- Advanced Configuration
    - Media Settings
        - Fax/Modem/CID Settings

6.2 Cisco Gateway FXS Card Configuration

To configure the Cisco Gateway FXS Card to use G.711 pass-through for an analog fax machine, the following information must be entered. The information in parenthesis at the end of the lines is not to be typed in, but provides additional information regarding the line to aid in configuration for various environments.

Also, this information must be entered under the configuration level of IOS (i.e. enable access, then configure access).

For Outbound Faxing:

dial-peer voice X voip (the X is to be respective to the given gateway)

Under the above created dial-peer, the following options must be entered.

service session
destination-pattern .T
session protocol sipv2
session target ipv4:x.x.x.x (use the IP of the IC server in place of x's)
incoming called-number pattern .T
dtmf-relay rtp-nte (This is for RFC2833 support)
codec g711ulaw
fax rate 14400

For Inbound Faxing:

dial-peer voice X pots (POTS Dial peer)
service session
destination-pattern 7777 (IC station extension)
port 0/1/1 (FXS port number)
forward-digits 0

7 Session Border Controller (SBC)

7.1 ACME SBC

The AT&T service has been tested with the ACME session border controller product. The configuration of the SBC can be difficult to understand. To help in its configuration a sample network will be provided, along with an explanation of each key SBC element required to make this setup function properly. Elements that are especially important in each configuration section will be in **bold**. There may be additional configuration for basic setup, or respective environments, however these are outside the scope of this document.

7.1.1 Sample Network

This sample network is the same as the one presented in section 3.1 of this document. However, IP addresses have been added to help follow along with the configuration steps in the SBC setup.

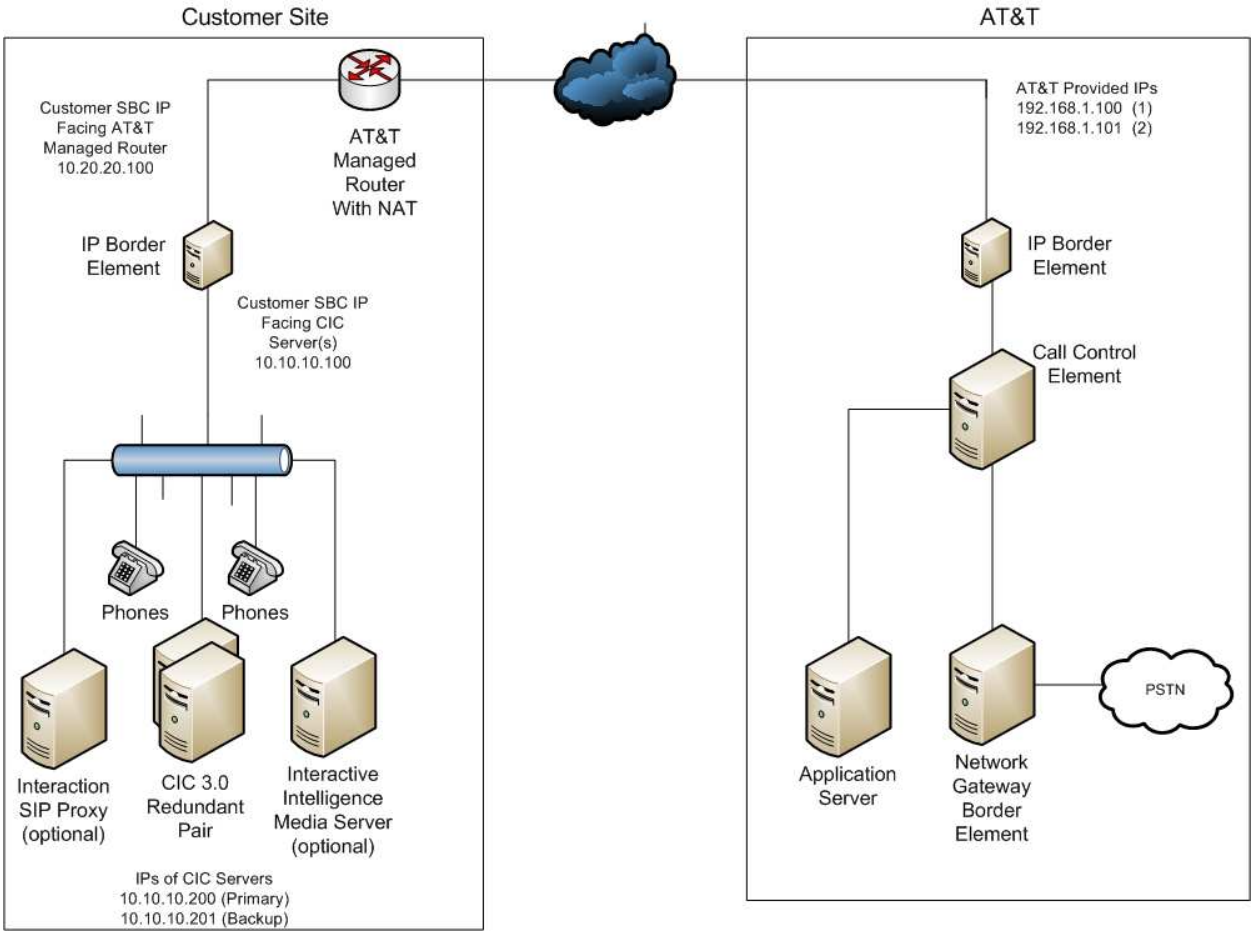

Figure 8: Sample Network with IP Addresses

7.1.2 General Interface Configuration

The actual AT&T border element IP addresses will be provided by AT&T Customer Care. Please Contact your Customer Care representative for the AT&T IP Border Element IP Addresses for your specific configuration.

7.1.2.1 SBC Interface to AT&T IP 1

This section is pretty straightforward, and is the ACME SBC description of how to get to the AT&T primary IP (as provided by AT&T). The *hostname* field identifies this particular *session-agent* entry for later steps (the IP is used to prevent the SBC from adding additional information to the INVITE headers of the SIP messages), the *ip-address* is the destination of that particular agent, and the *realm-id* groups the direction of the agents together (it will be important for later steps).

For some redundancy enabled systems there are two more important items. One is the *ping-method* which is the process the SBC will check the redundant addresses, and *ping-interval* which is the duration between checks. For the side connected to the CIC servers, an OPTIONS method will work (which sends a ping in a SIP OPTIONS message), with the interval shown being their requested default of 6 seconds. These messages are not sent while there is an active SIP session going, to prevent flooding the system with checks.

session-agent

hostname	**192.168.1.100**
ip-address	**192.168.1.100**
port	5060
state	enabled
app-protocol	SIP
app-type	
transport-method	UDP
realm-id	**core-att**
description	AT&T Session Agent Primary
carriers	
allow-next-hop-lp	enabled
constraints	disabled
max-sessions	0
max-inbound-sessions	0
max-outbound-sessions	0
max-burst-rate	0
max-inbound-burst-rate	0
max-outbound-burst-rate	0
max-sustain-rate	0
max-inbound-sustain-rate	0
max-outbound-sustain-rate	0
min-seizures	5
min-asr	0
time-to-resume	0
ttr-no-response	0
in-service-period	0
burst-rate-window	0
sustain-rate-window	0
req-uri-carrier-mode	None
proxy-mode	
redirect-action	
loose-routing	disabled
send-media-session	enabled

response-map
ping-method
ping-interval 0
ping-in-service-response-codes
out-service-response-codes
media-profiles
in-translationid
out-translationid
trust-me disabled
request-uri-headers
stop-recurse
local-response-map
ping-to-user-part
ping-from-user-part
li-trust-me disabled
in-manipulationid
out-manipulationid
p-asserted-id
trunk-group
max-register-sustain-rate 0
early-media-allow
invalidate-registrations disabled
rfc2833-mode none
rfc2833-payload 0
codec-policy

7.1.2.2 SBC Interface to AT&T IP 2

session-agent
hostname **192.168.1.101**
ip-address **192.168.1.101**
port 5060
state enabled
app-protocol SIP
app-type
transport-method UDP
realm-id **core-att**
description AT&T Session Agent Secondary
carriers
allow-next-hop-lp enabled
constraints disabled
max-sessions 0
max-inbound-sessions 0
max-outbound-sessions 0
max-burst-rate 0
max-inbound-burst-rate 0
max-outbound-burst-rate 0
max-sustain-rate 0
max-inbound-sustain-rate 0
max-outbound-sustain-rate 0
min-seizures 5
min-asr 0
time-to-resume 0
ttr-no-response 0

in-service-period 0
burst-rate-window 0
sustain-rate-window 0
req-uri-carrier-mode None
proxy-mode
redirect-action
loose-routing disabled
send-media-session enabled
response-map
ping-method
ping-interval 0
ping-in-service-response-codes
out-service-response-codes
media-profiles
in-translationid
out-translationid
trust-me disabled
request-uri-headers
stop-recurse
local-response-map
ping-to-user-part
ping-from-user-part
li-trust-me disabled
in-manipulationid
out-manipulationid
p-asserted-id
trunk-group
max-register-sustain-rate 0
early-media-allow
invalidate-registrations disabled
rfc2833-mode none
rfc2833-payload 0
codec-policy

7.1.2.3 SBC Interface to CIC Primary Server IP

Again this section is fairly straightforward, however this time the SBC interfaces pointing to the internal network CIC servers are being referenced.

session-agent
hostname **10.10.10.200**
ip-address **10.10.10.200**
port 5060
state enabled
app-protocol SIP
app-type
transport-method UDP
realm-id **peer-inin**
description ININ Session Agent Primary
carriers
allow-next-hop-lp enabled
constraints disabled
max-sessions 0
max-inbound-sessions 0
max-outbound-sessions 0

max-burst-rate 0
max-inbound-burst-rate 0
max-outbound-burst-rate 0
max-sustain-rate 0
max-inbound-sustain-rate 0
max-outbound-sustain-rate 0
min-seizures 5
min-asr 0
time-to-resume 0
ttr-no-response 0
in-service-period 0
burst-rate-window 0
sustain-rate-window 0
req-uri-carrier-mode None
proxy-mode
redirect-action
loose-routing disabled
send-media-session enabled
response-map
ping-method OPTIONS
ping-interval 6
ping-in-service-response-codes
out-service-response-codes
media-profiles
in-translationid
out-translationid
trust-me disabled
request-uri-headers
stop-recurse
local-response-map
ping-to-user-part
ping-from-user-part
li-trust-me disabled
in-manipulationid
out-manipulationid
p-asserted-id
trunk-group
max-register-sustain-rate 0
early-media-allow
invalidate-registrations disabled
rfc2833-mode none
rfc2833-payload 0
codec-policy

7.1.2.4 SBC Interface to CIC Backup Server IP

session-agent
hostname 10.10.10.201
ip-address 10.10.10.201
port 5060
state enabled
app-protocol SIP
app-type
transport-method UDP

realm-id	**peer-inin**
description	ININ Session Agent Secondary
carriers	
allow-next-hop-lp	enabled
constraints	disabled
max-sessions	0
max-inbound-sessions	0
max-outbound-sessions	0
max-burst-rate	0
max-inbound-burst-rate	0
max-outbound-burst-rate	0
max-sustain-rate	0
max-inbound-sustain-rate	0
max-outbound-sustain-rate	0
min-seizures	5
min-asr	0
time-to-resume	0
ttr-no-response	0
in-service-period	0
burst-rate-window	0
sustain-rate-window	0
req-uri-carrier-mode	None
proxy-mode	
redirect-action	
loose-routing	disabled
send-media-session	enabled
response-map	
ping-method	**OPTIONS**
ping-interval	6
ping-in-service-response-codes	
out-service-response-codes	
media-profiles	
in-translationid	
out-translationid	
trust-me	disabled
request-uri-headers	
stop-recurse	
local-response-map	
ping-to-user-part	
ping-from-user-part	
li-trust-me	disabled
in-manipulationid	
out-manipulationid	
p-asserted-id	
trunk-group	
max-register-sustain-rate	0
early-media-allow	
invalidate-registrations	disabled
rfc2833-mode	none
rfc2833-payload	0
codec-policy	

7.1.2.5 SBC Session Grouping For CIC Servers

The ACME SBC uses a *session-group* entry to tie the above *session-agent* entries together. The *group-name* and *description* fields are of course discretionary (but will become important to know in a later step), however the **dest** entries, must match the *session-agent* hostnames to be properly grouped.

It is recommended that grouping and *local-policy* (as described later) be used on the CIC side even if there is only one address being referenced. This allows for future expansions with a minimum of configuration changes. It is required for the AT&T side as they provide two IP addresses for redundancy and the SBC must be aware of both.

session-group

group-name	**ININ-SA**
description	ININ Session Agents
state	enabled
app-protocol	SIP
strategy	Hunt
dest	
	10.10.10.200
	10.10.10.201
trunk-group	
sag-recursion	disabled
stop-sag-recurse	401,407

7.1.2.6 SBC Session Grouping For AT&T

The ACME SBC uses a *session-group* entry to tie the above *session-agent* entries together. The *group-name* and *description* fields are of course discretionary (but will become important to know in a later step), however the **dest** entries, must match the *session-agent* hostnames to be properly grouped.

session-group

group-name	**ATT-SA**
description	AT&T Session Agents
state	enabled
app-protocol	SIP
strategy	Hunt
dest	
	192.168.1.100
	192.168.1.101
trunk-group	
sag-recursion	disabled
stop-sag-recurse	401,407

7.1.2.7 SBC Local Policy For AT&T

The Local Policy is used by the ACME SBC for routing in a grouped environment. It is used when the *route-home-proxy* is set to disabled in the next section (which will be explained in more detail there. The key terms in this section are the *source-realm* which describes where the packet came from (in this case from one of the CIC servers), the *next-hop* which describes where (in this case what *session-group* as defined above, which is going to AT&T) the packet should head, and *realm* which is

the area in which the packet is headed (which is referenced in the *session-agent* entry).

```
local-policy
    from-address
                                *
    to-address
                                *
    source-realm
                                peer-inin
    activate-time               N/A
    deactivate-time             N/A
    state                       enabled
    policy-priority             none
    policy-attribute
        next-hop                SAG:ATT-SA
        realm                   core-att
        action                  none
        terminate-recursion     disabled
        carrier
        start-time              0000
        end-time                2400
        days-of-week            U-S
        cost                    0
        app-protocol            SIP
        state                   enabled
        media-profiles
```

7.1.2.8 SBC Local Policy For CIC Servers

This is section the inverse of the one above, for traffic going in the other direction.

```
local-policy
    from-address
                                *
    to-address
                                *
    source-realm
                                core-att
    activate-time               N/A
    deactivate-time             N/A
    state                       enabled
    policy-priority             none
    policy-attribute
        next-hop                SAG:ININ-SA
        realm                   peer-inin
        action                  none
        terminate-recursion     disabled
        carrier
        start-time              0000
        end-time                2400
        days-of-week            U-S
        cost                    0
        app-protocol            SIP
        state                   enabled
```

media-profiles

7.1.2.9 SBC SIP NAT for AT&T

The *sip-nat* section is one of the more difficult to understand sections of the SBC configuration. This is especially true when multiple IPs or grouping is involved. The *realm-id* identifies the realm grouping as entered in the *session-agent* configuration.

The *ext-proxy-address* would normally be the destination of packets headed to the configured *realm-id* (in this case the AT&T provided IP), however using local policies and session groups changes this somewhat. Instead of going directly to that address, it searches the group that address is in for all possible addresses. A name cannot be used in that entry, just an address in that group.

The *ext-address* is the IP of the SBC interface connected to the line that has a logical connection to the *ext-proxy-address*. Essentially it is the IP of the SBC that connects to the AT&T Managed Router at the customer site.

The *route-home-proxy* setting is also required for group routing. When it is set to *disabled* the SBC then uses the local policy to route, completing the rest of the required grouping elements.

Finally, the *home-address*, and *home-proxy-address* fields are used in conjunction with the *sip-nat* entry that respective to packet flows in the other direction. Notice that the CIC *sip-nat* section has the same addresses in inverse. This is to allow the SBC to know the other interface side, and complete the NAT process. Essentially it's an internal map to the other interface, which is based on the direction of the packet flow.

```
sip-nat
    realm-id                core-att
    domain-suffix           .core-att.acme.com
    ext-proxy-address               192.168.1.100
    ext-proxy-port          5060
    ext-address                     10.20.20.100
    home-address            127.0.0.100
    home-proxy-address              127.0.0.101
    home-proxy-port         5060
    route-home-proxy        disabled
    address-prefix          *
    tunnel-redirect         disabled
    use-url-parameter       none
    parameter-name
    user-nat-tag                    -core-
    host-nat-tag                    CORE-
    headers                 Call-ID Contact f From i Join m r
                            Record-Route Refer-To Replaces Reply-To
                            Route t To v Via
```

7.1.2.10 SBC SIP NAT for CIC Servers

The second *sip-nat* section is, like the local policy, a relative inverse for packet flows in the opposite direction. The key differences here are the *realm-id* obviously, the *ext-proxy-address*, and the *ext-address*. Also note that the *home-address*, and the *home-proxy-address* are inverted from the previous example.

```
sip-nat
    realm-id                peer-inin
```

domain-suffix	.peer-inin.acme.com
ext-proxy-address	**10.10.10.200**
ext-proxy-port	5060
ext-address	**10.10.10.100**
home-address	**127.0.0.101**
home-proxy-address	**127.0.0.100**
home-proxy-port	5060
route-home-proxy	**disabled**
address-prefix	*
tunnel-redirect	disabled
use-url-parameter	none
parameter-name	
user-nat-tag	-peer-
host-nat-tag	PEER-
headers	Call-ID Contact f From i Join m r Record-Route Refer-To Replaces Reply-To Route t To v Via

8 E911 Support

AT&T currently supports E911 support via linking provided phone numbers to internal databases. This allows for dynamic updates, and accurate routing of emergency calls based on originating location. Essentially, it is how a standard phone line would be expected to function.