

Mediant™ 3000 E-SBC

Enterprise Session Border Controller

Session Initiated Protocol (SIP)

Configuration Note

Connecting AT&T IP Flexible Reach with Genesys®
SIP Server via AudioCodes® Mediant™ 3000 E-SBC



October 2012

Document #: LTRT-38125

Table of Contents

1	Introduction	7
1.1	Call Centers	7
1.2	PSTN Access Services	7
1.3	Role of the E-SBC.....	7
1.4	Genesys Contact Center / AT&T IP Flexible Reach / AudioCodes' E-SBC Solution	8
1.5	Document Scope.....	8
1.6	Test Scope	8
1.6.1	Feature Validation.....	9
1.6.2	Test Considerations/Exclusions	9
1.6.3	Test Facility.....	10
2	Solution Configuration	11
2.1	Solution Overview	11
3	Certification Network Configuration.....	13
3.1	Configuration Diagrams	13
4	Configuring Genesys Voice Platform.....	21
4.1	Genesys SIP Version Information	21
4.2	Genesys SIP Server Options	21
4.3	IP Phones.....	26
4.3.1	AudioCodes 320HD IP Phone	26
4.3.1.1	Firmware Version	26
4.3.1.2	Example Configuration	27
4.3.2	Polycom SoundPoint IP 650	29
4.3.2.1	Firmware version.....	29
4.3.2.2	Example Configuration	29
5	Configuring the Mediant 3000 E-SBC	31
5.1	Basic Configuration via the Web GUI.....	31
5.1.1	Configure the Multiple Interface Table.....	32
5.1.2	Configure DNS/SRV Tables	33
5.1.3	Configure Firewall Settings.....	34
5.1.4	Enable the SBC Application	36
5.1.5	Configure the Number of Media Channels	37
5.1.6	Configure the SRD Table.....	38
5.1.7	Configure Media Realm Table.....	41
5.1.8	Configure the SIP Interfaces Table	44
5.1.9	Configure the IP Groups	45
5.1.10	Configure the Proxy Sets.....	54
5.1.11	Define the Classification Rules.....	56
5.1.12	Configure SBC General Settings.....	60
5.1.13	Configure SBC Admission Control	61
5.1.14	Configure Allowed Coders Group.....	62
5.1.15	Configure IP Profiles.....	63
5.1.16	Configure SBC IP-to-IP Routing Setup.....	65
5.1.16.1	IP-to-IP Routing Row Details	69
5.2	SIP Header Manipulation	78
5.3	Mediant 3000 E-SBC User Info File	80
5.4	Mediant 3000 E-SBC Feature Key	80
5.5	Mediant 3000 E-SBC Configuration File	81

List of Figures

Figure 2-1: AT&T IP Flexible Reach with AudioCodes' E-SBC and Genesys Call Center	12
Figure 3-1: Genesys Voice Platform Layout.....	13
Figure 3-2: Network Overview	14
Figure 3-3: SRX Port layout.....	14
Figure 3-4: SRX Servers Layout	15
Figure 3-5: Inside Port Layout	16
Figure 3-6: Inside Servers Layout	17
Figure 3-7: Outside Port Layout	18
Figure 3-8: Outside Servers Layout	19
Figure 5-1: E-SBC Interfaces/Configuration.....	31
Figure 5-2: Configuring the Multiple Interface Table	33
Figure 5-3: Internal DNS Table	33
Figure 5-4: Firewall Settings.....	34
Figure 5-5: Applications Enabling.....	36
Figure 5-6: IP Media Settings	37
Figure 5-7: ATDMZ_SRD	39
Figure 5-8: RALVOX_SRD	39
Figure 5-9: RALOFFICE_SRD	40
Figure 5-10: TWCDMZ_IPP	40
Figure 5-11: Add Record Dialog Box.....	42
Figure 5-12: SIP Interface Table	42
Figure 5-13: Media Realm #0	42
Figure 5-14: Media Realm #1	43
Figure 5-15: Media Realm #2	43
Figure 5-16: Media Realm #3	43
Figure 5-17: SIP Interface Table	44
Figure 5-18: ATT IP Group 1 (SERVER).....	46
Figure 5-19: ATT Secondary IP Group 2 (SERVER)	48
Figure 5-20: Genesys Server IP Group 3.....	49
Figure 5-21: AT&T Remote Agents IP Group 7.....	50
Figure 5-22: Non-AT&T Remote Agents IP Group 8.....	51
Figure 5-23: AT&T Customer IP Group 5 (Lab Only).....	52
Figure 5-24: Non-AT&T Customers IP Group 6 (Lab only)	53
Figure 5-25: Proxy Set 1 (AT&T IP Flexible Reach SIP Trunk)	54
Figure 5-26: Proxy Set 2 (AT&T IP Flexible Reach SIP Trunk - Secondary).....	55
Figure 5-27: Proxy Set 3 (Genesys SIP Server Trunk)	55
Figure 5-28: Classification Process Overview.....	56
Figure 5-29: Classification Table ... Add Record Page.....	57
Figure 5-30: Classification Table Rule #2	57
Figure 5-31: Classification Table Rule #3	58
Figure 5-32: Classification Rule #4	58
Figure 5-33: Classification Rule #5	59
Figure 5-34: Classification Rule #6	59
Figure 5-35: Classification Rule #7	59
Figure 5-36: SBC General Settings.....	60
Figure 5-37: SBC Admission Control Table	61
Figure 5-38: Allow Coders Group.....	62
Figure 5-39: AT&T IP Flexible Reach Profile	64
Figure 5-40: IP2IP Routing Table.....	66
Figure 5-41: IP to IP Routing Table from Configuration File	67
Figure 5-42: Web Message Manipulation (SIP Header Manipulation) Table.....	78
Figure 5-43: Message Manipulations for AT&T IP Flexible Reach with Genesys SIP Server	79

Notice

This document describes how to integrate the AT&T IP Flexible Reach-MIS/PNT/AT&T Virtual Private Network (AVPN) SIP Trunk Service with Genesys Voice Platform using the AudioCodes Mediant 3000 E-SBC.

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Before consulting this document, check the corresponding Release Notes regarding feature preconditions and/or specific support in this release. In cases where there are discrepancies between this document and the Release Notes, the information in the Release Notes supersedes that in this document. Updates to this document and other documents as well as software files can be downloaded by registered customers at <http://www.audiocodes.com/downloads>.

© Copyright 2012 AudioCodes Ltd. All rights reserved.

This document is subject to change without notice.

Date Published: Oct-14-2012

Trademarks

AudioCodes, AC, AudioCoded, Ardito, CTI2, CTI², CTI Squared, HD VoIP, HD VoIP Sounds Better, InTouch, IPmedia, Mediant, MediaPack, NetCoder, Netrake, Nuera, Open Solutions Network, OSN, Stretto, TrunkPack, VMAS, VoicePacketizer, VoIPerfect, VoIPerfectHD, What's Inside Matters, Your Gateway To VoIP and 3GX are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and service are generally provided by AudioCodes' Distributors, Partners, and Resellers from whom the product was purchased. For technical support for products purchased directly from AudioCodes, or for customers subscribed to AudioCodes Customer Technical Support (ACTS), contact support@audiocodes.com.

AudioCodes Customer Support Center	Americas: +1-732-652-1085 or +1-800-735-4588 Elsewhere: 800-735-2244 Or 972-3-976-4343 http://www.crm.audiocodes.com
Corporate website	http://www.audiocodes.com
Support	http://www.audiocodes.com/support
iSupport (on-line ticket management)	https://crm.audiocodes.com/OA_HTML/jtflogin.jsp
Product Documentation and Software	http://www.audiocodes.com/downloads
Training	http://www.audiocodes.com/technical-training
Professional Services	http://www.audiocodes.com/Professional-services

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.



Note: Throughout this document, unless otherwise specified, the term *device* refers to AudioCodes' Mediant 3000 E-SBC.

Related Documentation

Manual Name
LTRT-30200 Recommended Security Guidelines Technical Note (AudioCodes)
LTRT-31620 SBC Deployment Guide (AudioCodes)
LTRT-94710 Mediant 3000 SIP Installation Manual (AudioCodes)
LTRT-89713 Mediant 3000 SIP User's Manual (AudioCodes)
Partner Certification Report – AudioCodes SBC (Genesys)
AT&T BVOIP Network SIP Trunk Specification for IP PBXs: IP Flexible Reach, Enhanced IP Flexible Reach and IP Toll Free Issue 1.33.1, May 8, 2012 (AT&T)

1 Introduction

1.1 Call Centers

Call Centers are centralized offices used for the purpose of receiving and transmitting a large volume of requests by telephone, independent of whether the request originated in the TDM or packet network. A call center is operated by a company to administer incoming product support or information inquiries from consumers. Outgoing calls for telemarketing, clientele, and debt collection are also made. In addition to a call center, collective handling of letters, faxes, and e-mails at one location is known as a **Contact Center**.

A Call Center is often operated through an extensive open workspace for call center agents, with work stations that include a computer for each agent, a telephone set/headset connected to a telecom switch, and one or more supervisor stations. It can be independently operated or networked with additional centers, often linked to a corporate computer network, including mainframes, microcomputers and LANs. The voice and data pathways into the center are linked through a set of technologies called computer telephony integration (CTI) that uses middleware to present customer data to agents. Such delivery of the voice and customer data is a complex arrangement that can be inconsistent and inefficient as the data and voice must transition different paths to arrive simultaneously at an Agent terminal.

An IP Call Center is the implementation of a Call Center using VoIP. Using the location independence of IP, the IP Call Center can be distributed, and the Call Center application server can be located anywhere in the enterprise network. The service can be provided using IP Phones, or regular phones connected to Media Gateways. The DN's for the IP phones may be local or virtual DNs, giving the appearance of a company presence in a different geographical location than the Agent's true location.

1.2 PSTN Access Services

PSTN breakout is very important in all IP Call Center implementations. It can be achieved using a centralized media gateway resource which provides PSTN connectivity to all agents. Contact Centers have historically used traditional PSTN connectivity such as T1s or analog lines to connect enterprise sites to the public voice network, but Service Providers now have means to allow enterprise customers access to the PSTN via the Service Provider's own IP networks through services that use SIP signaling and centralized IP to TDM gateways to provide on-net and off-net services. These services are giving way to significant savings in operating expenses through the unification of voice and data delivery over one network. Customer-specific data can be included in the SIP elements and can arrive at the Agent Terminal over the same network as voice in a reliable and consistent manner, opening communications with the customer through varied applications like email, chat and other multi-media applications.

1.3 Role of the E-SBC

The interworking of the Call Center Network to a Service Provider network poses some issues as it relates to voice enabled by an additional network element on the border between these two networks. This element is the Enterprise Session Border Controller (E-SBC). The role of this E-SBC can be to provide translation between the different variants of SIP (interoperability), Network Security, and remote workers connectivity.

E-SBCs are essential components of any business migration to VoIP services. E-SBCs help protect the deploying enterprise's network assets from security threats and facilitate interoperability between the enterprise network, the Service Provider network, and the enterprise's own remote workers. A core SBC helps protect the core network from security threats. Without an E-SBC at the edge of the enterprise network, any security breach at the enterprise side might expose core services to be tagged as the potential cause. An E-SBC can establish a clear and secure boundary between external SIP Trunks and the enterprise's local network elements.

In SIP-based solutions, the E-SBC can manipulate and program various fields in the SIP headers and ensure that a given SIP implementation of the Service Provider will interoperate with any specific SIP version supported by the enterprise IP-PBX.

Additionally, one of the growing trends worldwide is often called the distributed enterprise. Many employees work from home. Many others work in small offices far from the main offices and do not have a local IP-PBX. E-SBCs are the only possible means for enabling remote employees to access the enterprise's VoIP network while providing all required services.

1.4 Genesys Contact Center / AT&T IP Flexible Reach / AudioCodes' E-SBC Solution

Genesys Contact Center Solutions allow companies to manage customer requirements effectively by routing customers to appropriate resources and agents through IVR and consolidated cross-channel management of all of a customer's interactions. Sophisticated profiling, outbound voice and performance management enables companies to provide very personalized customer care and delivery.

Traditionally, Genesys software has operated in call center environments supported by TDM connections. As Genesys expands its VoIP offerings, the capabilities of the Genesys SIP server continue to increase. As the service offerings transition away from TDM services, Genesys' customers require additional network elements to mitigate needs such as connecting the Call Center to the SIP trunks provided by the ITSP, securely connecting remote agents without additional security hardware and enabling complex synchronization between non-compatible SIP components.

The **AT&T IP Flexible Reach** service is a SIP Trunk service that delivers integrated IP access for IP PBX, TDM PBX or Key System environments, providing cost benefits via consolidation of voice and data – one provider, single transport, and management options, to the PSTN. Voice and data traffic riding over the same transport drives greater bandwidth utilization and access to cost savings. This managed Voice over IP communication solution includes calling plans that support inbound and outbound calling on an enterprise's data network, allowing local, U.S. long distance and international calls to reach for the enterprise sites. The underlying transport for the AT&T IP Flexible Reach (IPFR) may be Managed Internet Service (MIS)/Private Network Transport (PNT) or AT&T Virtual Private Network (AVPN).

AudioCodes' line of E-SBCs provides these and other services associated with Session Border Control functionality. **AudioCodes' Mediant 3000 E-SBC** is a fully featured Enterprise Class Session Border Controller, providing a secure voice network (VoIP) deployment for medium and large-sized enterprises based on a Back-to-Back User Agent (B2BUA) implementation. The E-SBC provides control over SIP signaling and also the media streams involved in setting up, conducting, and tearing down calls. Additionally, the AudioCodes' Mediant 3000 E-SBC enables Contact Centers to integrate home-based agents in the public internet space securely, without requiring home users to reconfigure their home internet access devices.

1.5 Document Scope

This Configuration Note describes the network environment and configuration used to certify AudioCodes' Mediant 3000 E-SBC v6.4 interfacing with Genesys' Voice Platform v8.1 and AT&T's IP Flexible Reach MIS/PNT/AVPN SIP Trunk Service.

1.6 Test Scope

The AudioCodes E-SBC was previously Partner Certified with Genesys Voice Platform 8.1. Genesys' Voice Platform v8.1 was previously certified with AT&T's IP Flexible Reach. The certification covered in this Configuration Note was based on select cases from AT&T's Enhanced IP Flexible Reach Test Plan. The test suite is a scaled-down version of the interaction tests performed in the Genesys ODS Labs.

The objective of testing using the configuration detailed in this Note was to validate interoperability of Genesys' Voice Platform communicating with AT&T's IP Flexible Reach service, with AudioCodes' Mediant E-SBC v6.4 as the interfacing device, providing expected SBC functionality such as security, topology hiding and SIP header manipulation.

1.6.1 Feature Validation

The following features were validated as part of certification with AT&T:

- Inbound (off-net)/outbound (on-net) basic calls
- Basic International Calls
- Simultaneous Calls
- Calling Number Privacy
- Call hold & resume
- Call Conference (Intra-Site, Inter-Site)
- PBX-based Attended Call Transfer (Not based on SIP REFER)
- PBX-based Unattended Call Transfer (Not based on SIP REFER)
- PBX-based Call Forwarding (forward all, busy, no answer)
- Customer IP Trunk based Meet-Me Conference
- AT&T IP Teleconferencing (IPTC)
- Advanced Call Prompter
- 911, x11 dialing with native and virtual telephone numbers
- SIP network failover tests for CPE Equipment & AT&T IP Border Element (IPBE).
- SIP OPTIONS
- Early Media capability

1.6.2 Test Considerations/Exclusions

Note the following special considerations for the AT&T test environment:

- Fax was not tested and is not supported.
- G.729 and G711 are the only codecs certified in this solution.
- Voicemail into the Genesys platform was not tested. Per Genesys, voicemail is not applicable to the Call Center solution.
- Emergency 911/E911 Services Limitations and Restrictions:
 - Although AT&T provides 911/E911 calling capabilities, AT&T does not warrant or represent that the equipment and software (e.g., IP PBX) reviewed in this customer configuration guide will properly operate with AT&T IP Flexible Reach to complete 911/E911 calls; therefore, it is Customer's responsibility to ensure proper operation with its equipment/software vendor.
 - While AT&T IP Flexible Reach services support E911/911 calling capabilities under certain Calling Plans, there are circumstances when that E911/911 service may not be available, as stated in the Service Guide for AT&T IP Flexible Reach found at <http://new.serviceguide.att.com>. Such circumstances include, but are not limited to, relocation of the end user's CPE, use of a non-native or virtual telephone number, failure in the broadband connection, loss of electrical power, and delays that may occur in updating the customer's location in the automatic location information database. See the AT&T IP Flexible Reach Service Guide for details on limitations and restrictions.

1.6.3 Test Facility

Testing was conducted at AudioCodes' facility in Research Triangle Park, North Carolina, with support from Genesys Labs and AT&T BVoIP teams.

2 Solution Configuration

2.1 Solution Overview

The configuration scenario described in this document includes the following setup:

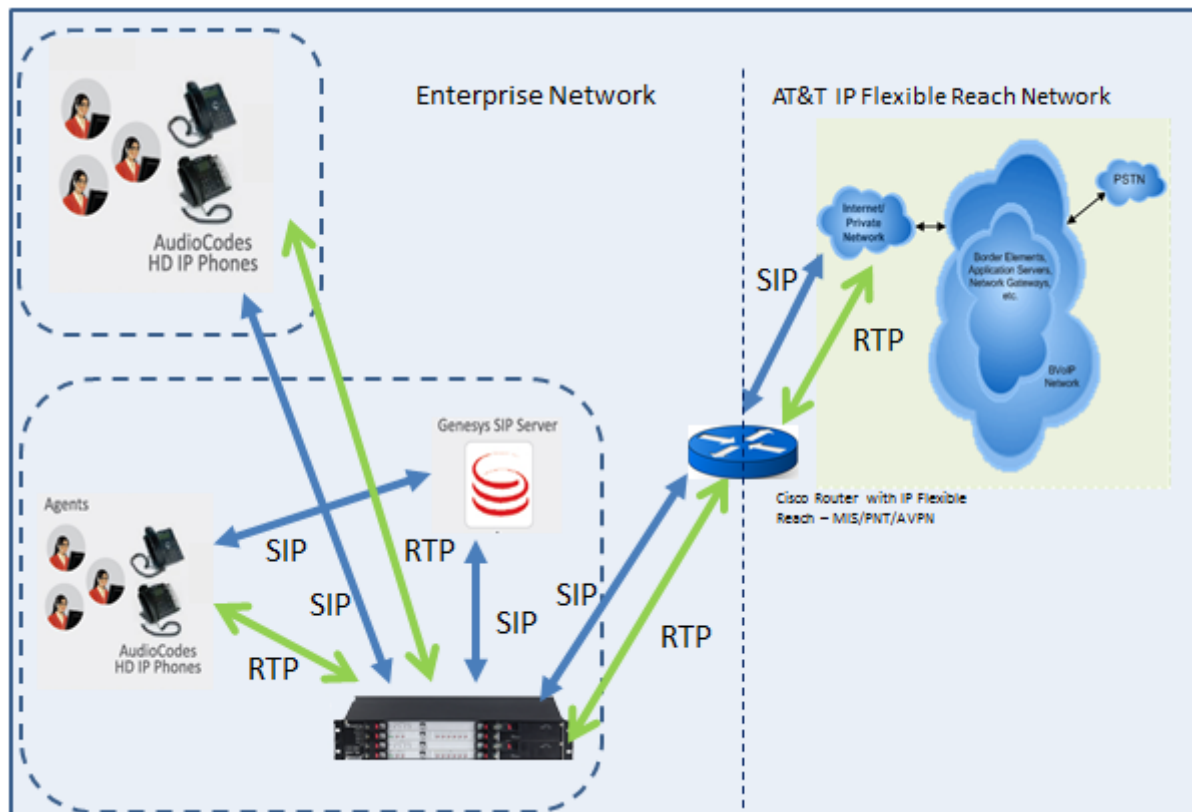
- An enterprise has a deployed Genesys Voice Platform Call Center in its private network.
- The Mediant 3000 E-SBC is connected to the LAN and WAN network interfaces such as an Edge Router/Firewall via a VLAN-aware switch, using a single physical connection. Optionally, for 1+1 (2 cables) redundancy, two physical ports may be used.
- The enterprise is connected to the PSTN network using AT&T's Flexible Reach SIP Trunk Service.
- Remote Call Agents are located in the public Internet space and registered to the Genesys SIP Server in the private network via the E-SBC.
- Local & Virtual Telephone Numbers (VTNs) are assigned to Agents

Setup requirements are:

- While Genesys' Voice Platform Call Center environment is located on the enterprise's Local Area Network (LAN), the Flexible Reach SIP Trunks are located on the Wide Area Network (WAN).
- Genesys' Voice Platform *and* the Flexible Reach SIP Trunk use SIP over UDP transport type.
- Genesys' Voice Platform *and* Flexible Reach SIP Trunk support G.729 (preferred) and G711 μ -Law coder types.
- Transcoding was not required on the Mediant 3000 E-SBC and was not used in testing to allow for future extension of the certification to the Mediant Software E-SBC which is a non-transcoding device.
- Support for early media handling.
- Support for call forwarding.
- SIP Diversion Header Manipulation for SIP compatibility and Topology hiding of the inside network.

Figure 2-1 below illustrates an overview of the certification setup.

Figure 2-1: AT&T IP Flexible Reach with AudioCodes' E-SBC and Genesys Call Center



3 Certification Network Configuration

The Mediant 3000 E-SBC in this certification has a single, redundant network interface. The traffic to the various network destinations such as AT&T network, or public internet, or the internal network, is managed through configuration of multiple IP address associated to VLANs in the LAN network.

3.1 Configuration Diagrams

Figure 3-1: Genesys Voice Platform Layout

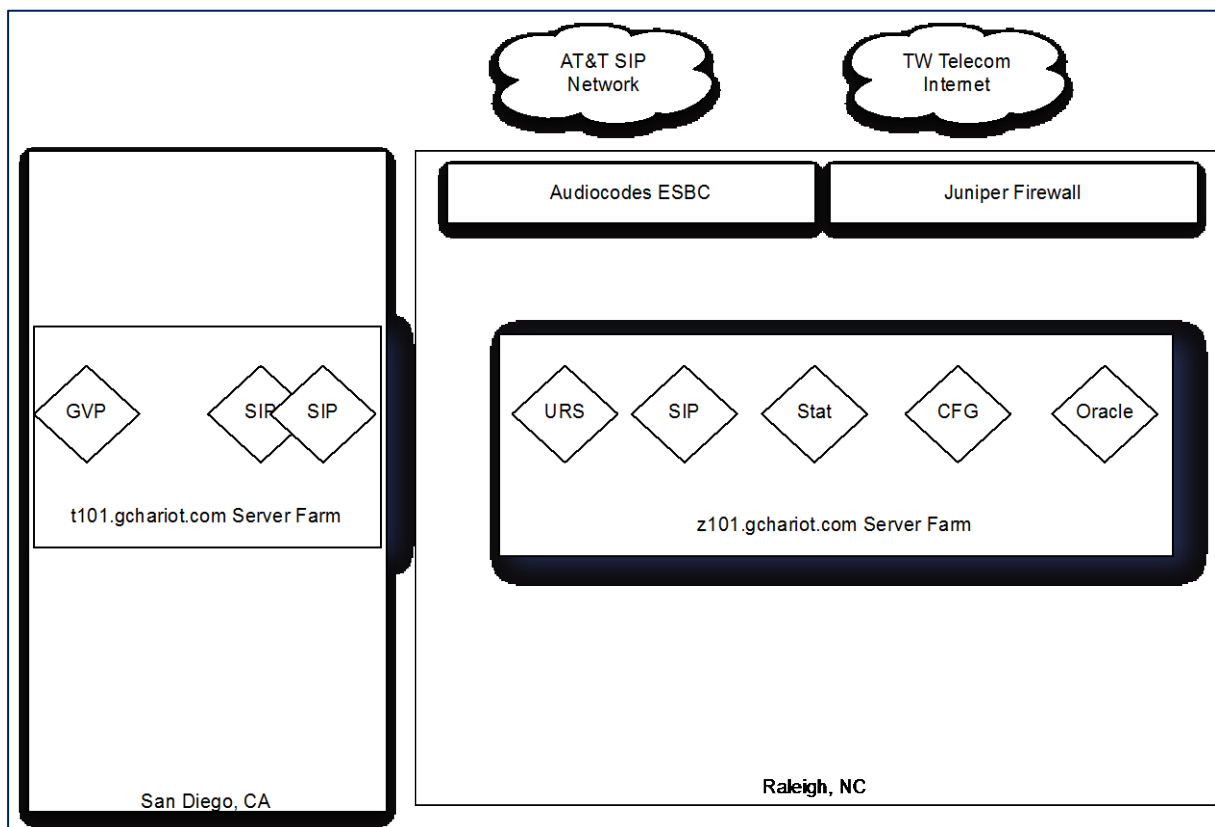


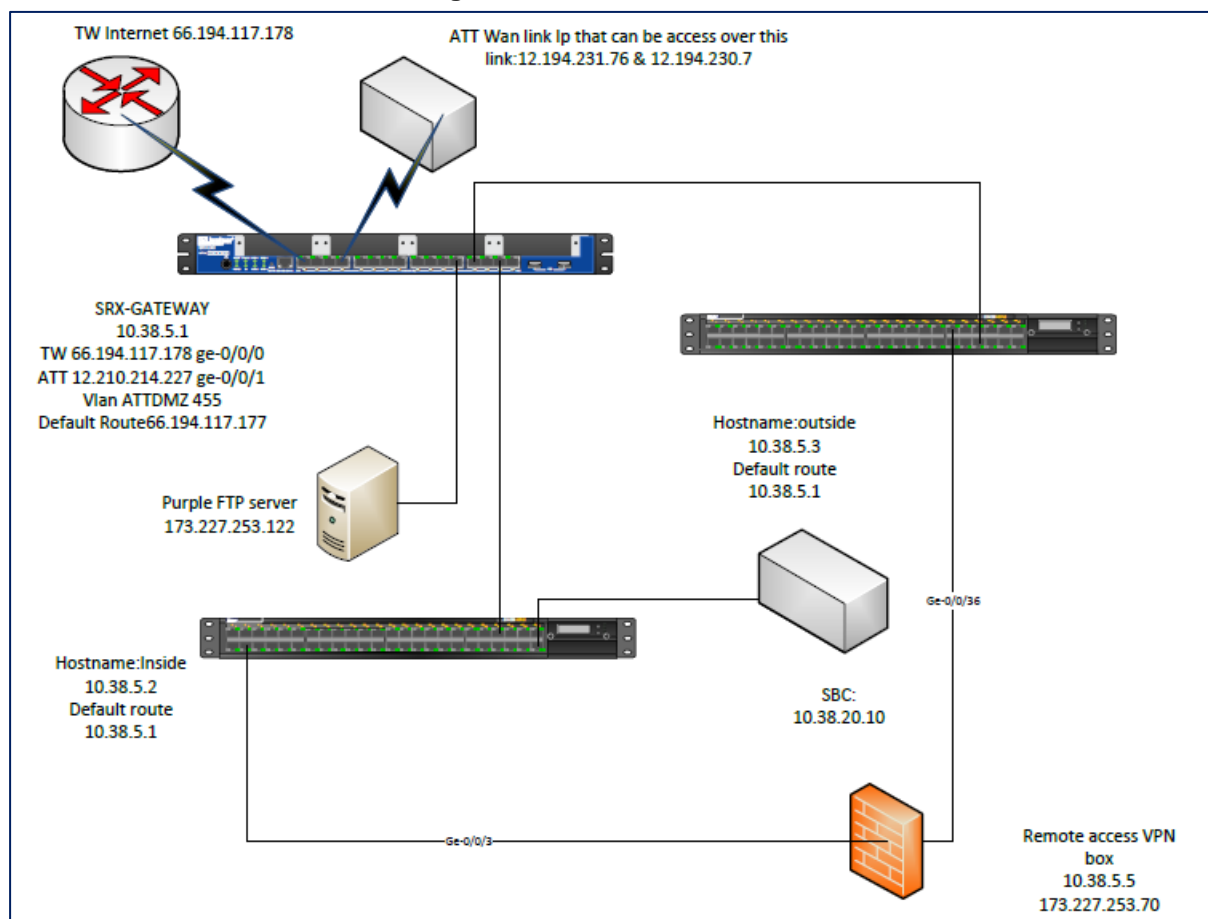
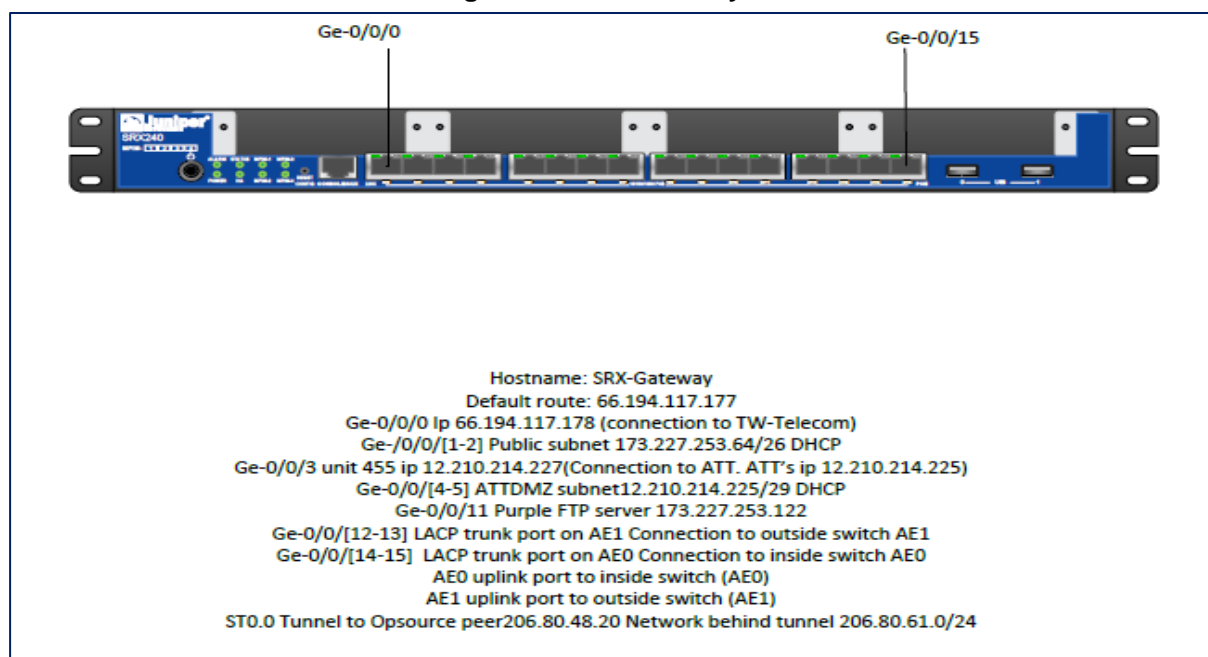
Figure 3-2: Network Overview

Figure 3-3: SRX Port layout


Figure 3-4: SRX Servers Layout

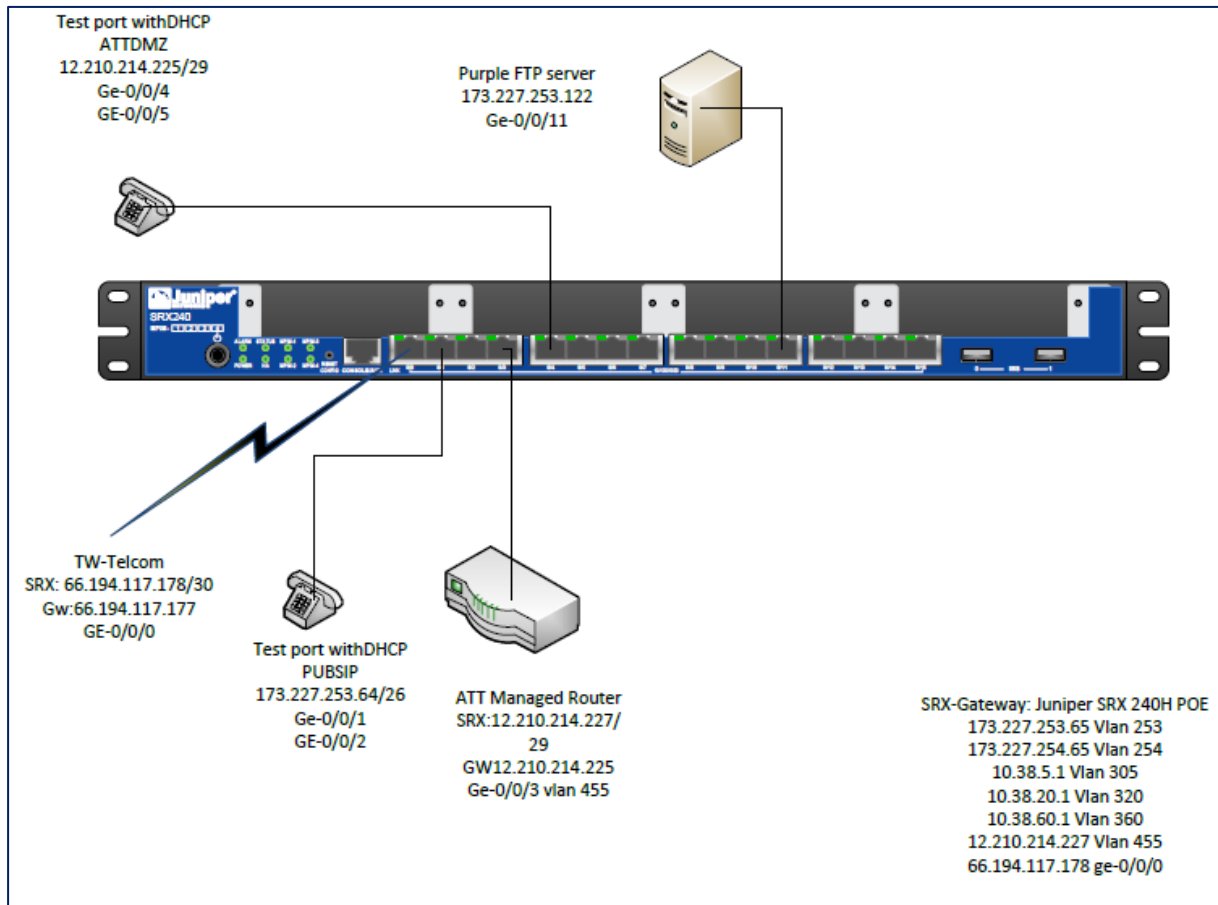


Figure 3-5: Inside Port Layout



```

Hostname: inside
Default route: 10.38.5.1
Ge-0/0/0 RALVOX addresses phone test port DHCP
Ge-0/0/1 Linksys inside wireless
Ge-0/0/3 VPN box port 1 of Pci-card 1 10.38.5.5
GE-0/0/11 Software SBC DL120
Ge-0/0/12 Server 14 Port 1 Beast 10.38.5.101
Ge-0/0/14 Server 13 Port 1 Phoenix 10.38.5.103
Ge-0/0/16 Server 12 Port 1 Storm 10.38.5.107
Ge-0/0/18Server 11 Port 1 Rogue 10.38.5.105
Ge-0/0/20 server 10 zeroshell 10.38.[5,20,60].20 (trunk)
GE-0/0/22 Mimic 10.38.5.119
Ge-0/0/24 sunfire (1) x4100 eth0
Ge-0/0/26 sunfire (2) x4100 eth0
Ge-0/0/28 sunfire (3) x4100 eth0
Ge-0/0/30 GAMBIT eth0
Ge-0/0/31 Infoblox Lan1 10.38.5.19
Ge-0/0/32 GCSRAL108-2 eth0
Ge-0/0/34 GCSRAL108-3 eth1
Ge-0/0/35 GCSRAL108-3 eth0
Ge-0/0/[40-41] LACP trunk port on AE0 Connection to SRX (AE0)
Ge-0/0/44 Printer 10.38.5.21
Ge-0/0/46 SBC connection 10.38.20.10/173.227.254.124(trunk)
Ge-0/0/47 SBC BACKUP connection 10.38.20.10/173.227.254.124(trunk)
AE0 uplink port to SRX (AE0)

```


Figure 3-6: Inside Servers Layout

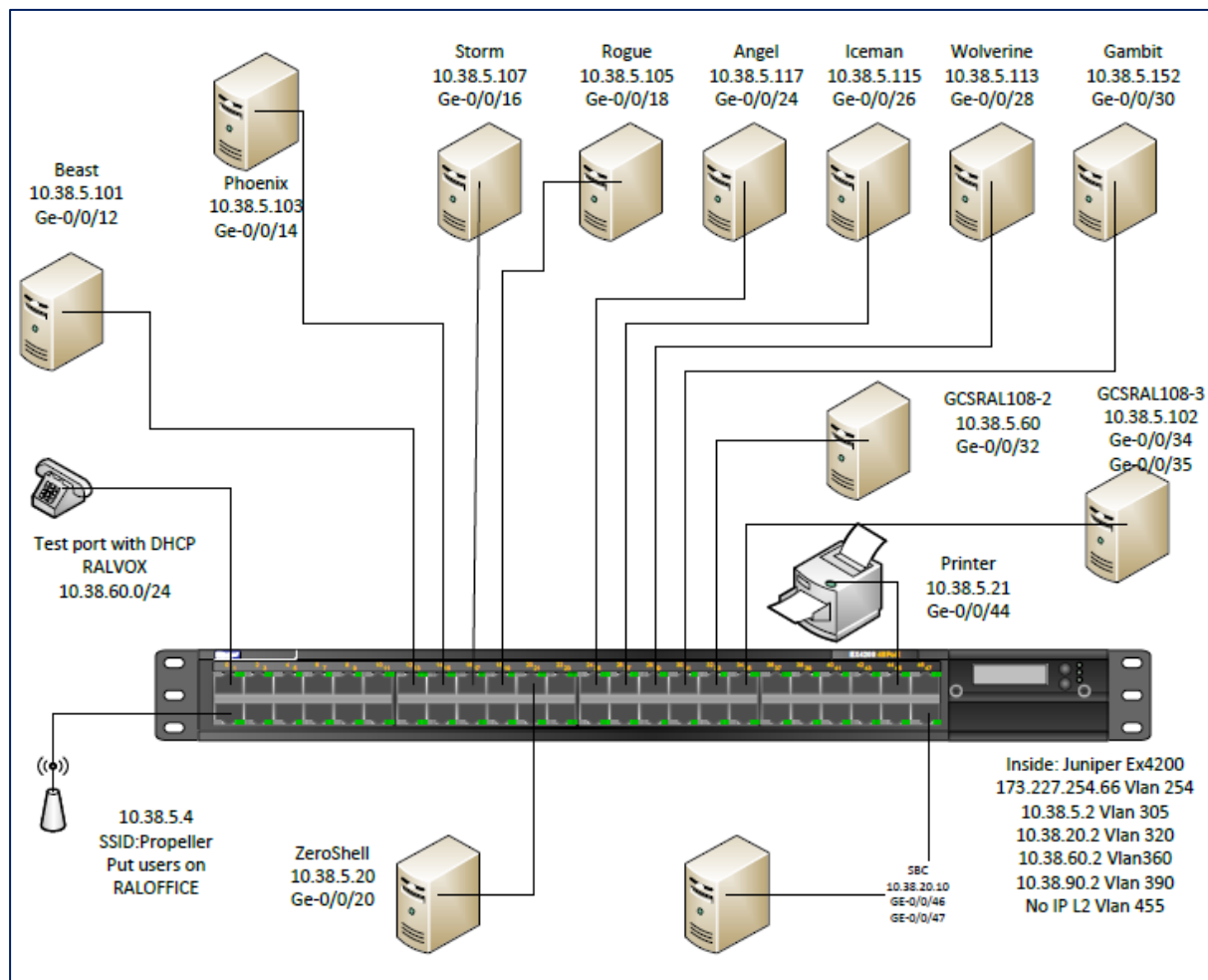


Figure 3-7: Outside Port Layout

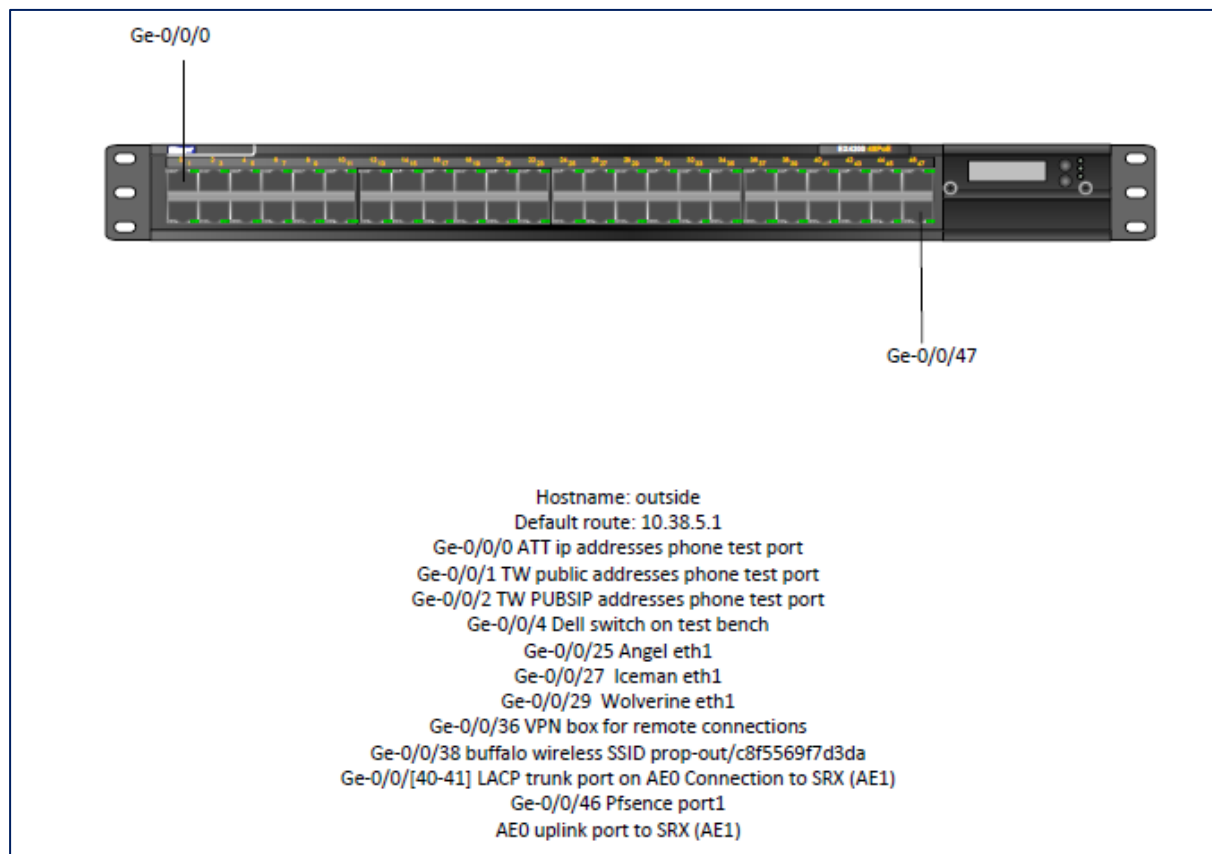
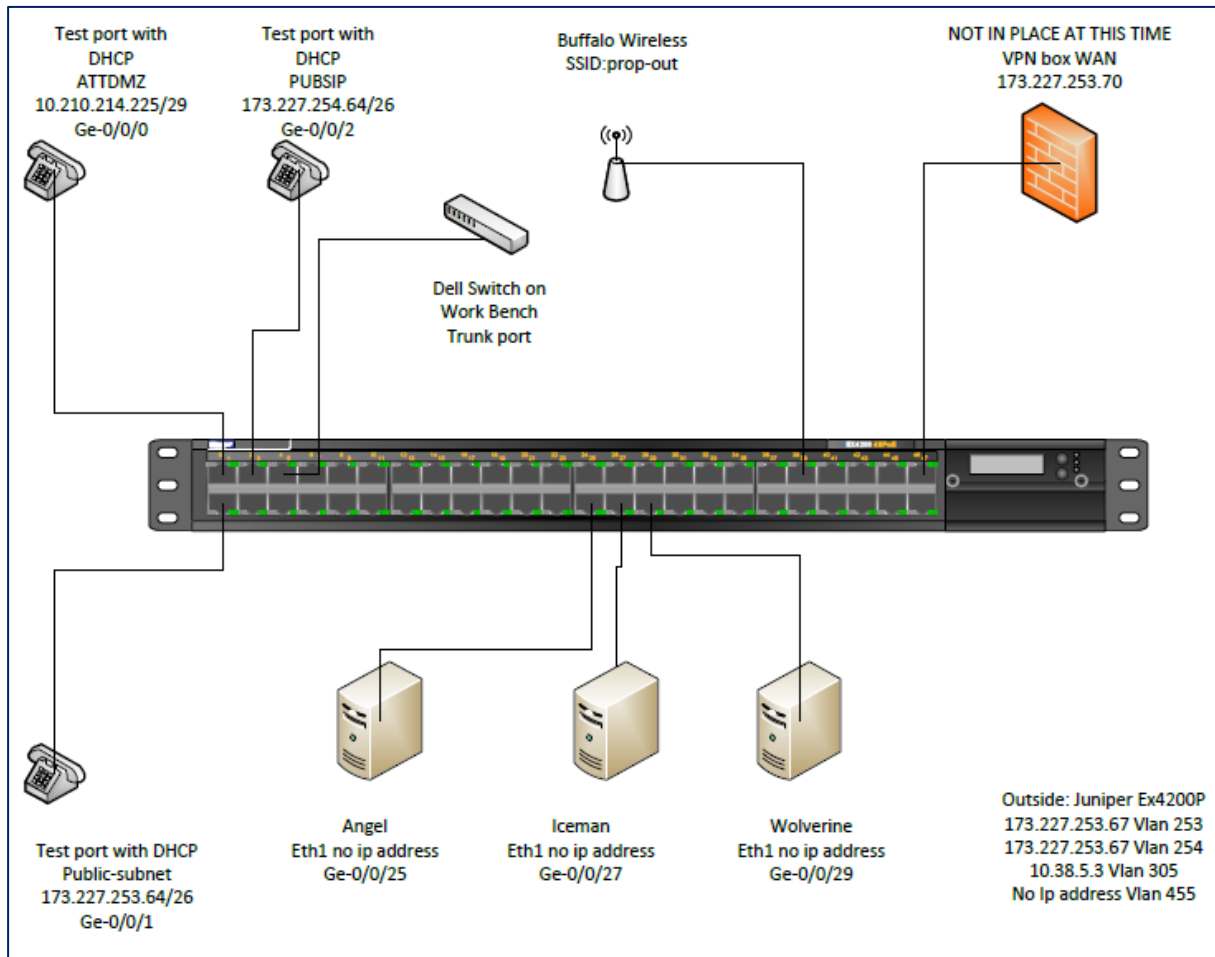


Figure 3-8: Outside Servers Layout



Reader's Notes

4 Configuring Genesys Voice Platform

4.1 Genesys SIP Version Information

```
angel.z101.gchariot.com
SIP Server, Version: 8.1.000.51 Compiled: Dec 6 2011 10:53:39
Genesys Telecommunications Laboratories, Inc., Copyright 1991 -
2008
Build with Genesys SIP Library 8.1.000.10
Build with Framework 8.1.000.09
Build with TServerCommonPart 8.1.000.25
High Availability feature: ON
ISCC feature support: ON
Genesys Common Library SE: 8.1.000.14 C2
TServer Library (TLib): 8.1.000.04 HA
    gmessage library: 8.1.000.02
    gservice library: 8.1.000.04 MT
    gthread library: 8.1.000.05
Config Server support: CfgLib 8.1.000.08
LCA support: LCalib 8.1.000.05
License support: GLMLib 8.1.000.02 MT (FLEXLm 11.9)
Message Server support: LogLib 8.1.000.09 MT
Nonstop Operation: NSOLib 8.1.001.03 try/catch
SNMP support: MngmLib 8.1.000.03
```

4.2 Genesys SIP Server Options

```
[agent-reservation]
collect-lower-priority-requests=true
reject-subsequent-request=true
request-collection-time=100 msec
reservation-time=10000 msec

[backup-sync]
addp-remote-timeout=0
addp-timeout=0
addp-trace=off
protocol=default
sync-reconnect-tout=20 sec

[call-cleanup]
cleanup-idle-tout=0
notify-idle-tout=0
periodic-check-tout=10 min
```

```
[extrouter]
cast-type=route direct-callid reroute direct-uui direct-ani
direct-notoken dnis-pool direct-digits pullback route-uui direct-
network-callid
cof-ci-defer-create=0
cof-ci-defer-delete=0
cof-ci-req-tout=500 msec
cof-ci-wait-all=false
cof-feature=false
cof-rci-tout=10 sec
compound-dn-representation=true
default-dn=
default-network-call-id-matching=
direct-digits-key=CDT_Track_Num
dn-for-unexpected-calls=
epp-tout=0 sec
event-propagation=list
match-call-once=true
network-request-timeout=20 sec
reconnect-tout=5 sec
register-attempts=5
register-tout=2 sec
report-connid-changes=false
request-tout=20 sec
resource-allocation-mode=circular
resource-load-maximum=0
route-dn=
tcs-queue=
tcs-use=never
timeout=60 sec
use-data-from=current
use-implicit-access-numbers=false
[license]
license-file=7260@storm.z101.qchariot.com
num-of-licenses=100
num-sdn-licenses=100
[link-control]
ha-sync-dly-lnk-conn=false
link-alarm-high=0
link-alarm-low=0
quiet-cleanup=false
quiet-startup=false
reg-delay=10
reg-silent=true
restart-cleanup-dly=0
restart-cleanup-limit=0
use-link-bandwidth=auto
[Log]
debug=/u01/sw/genesys/logs/rtpsip01
verbose=debug
[log-filter]
default-filter-type=copy
[log-filter-data]
<kv-pair-key>=copy
```

```
[TServer]
accept-dn-type=+extension +position +acdqueue +routedn +trunk
+routequeue
acw-in-idle-force-ready=true
after-routing-timeout=10
agent-emu-login-on-call=false
agent-group=
agent-logout-on-unreg=false
agent-logout-reassoc=false
agent-no-answer-action=none
agent-no-answer-overflow=
agent-no-answer-timeout=15
agent-only-private-calls=false
agent-strict-id=false
am-detected=drop
ani-distribution=inbound-calls-only
audio-codecs=telephone-event,PCMU,PCMA,G723,G729,GSM
auto-logout-ready=false
auto-logout-timeout=0
background-processing=true
background-timeout=60 msec
backup-mode=none
backwds-compat-acw-behavior=false
blind-transfer-enabled=false
bsns-call-dev-types=+acdq +rp +rpq +xrp
busy-tone=music/busy_5sec
busy-tone-duration=5
call-rq-gap=0
cancel-monitor-on-disconnect=true
check-tenant-profile=false
clid-withheld-name=PRIVATE
collect-tone=music/collect
consult-user-data=separate
convert-otherdn=+agentid +reserveddn +fwd
correct-rqid=false
cos=
cpd-info-timeout=3
customer-id=
default-dn=
default-dn-type=none
default-monitor-mode=mute
default-monitor-scope=call
default-music=music/on_hold
default-route-point=
default-video-file=
device-rq-gap=0
dial-plan=outbound
divert-on-ringing=true
dn-del-mode=never
dn-scope=undefined
dr-forward=off
dr-peer-trunk=
drop-nailedup-on-logout=false
dtmf-payload=101
emergency-recording-cleanup-enabled=false
emergency-recording-filename=
emulate-login=on-RP
emulated-login-state=ready
enable-ims=false
enable-unknown-gateway=false
encoding=
enforce-external-domains=
enforce-trusted=true
event-ringing-on-100trying=false
external-registrar=
extn-no-answer-overflow=
extn-no-answer-timeout=15
fast-busy-tone=music/atb_5sec
fax-detected=drop
```

```
find-trunk-by-location=false
forced-notready=true
greeting-after-merge=false
greeting-call-type-filter=-internal -consult
greeting-delay-events=none
greeting-notification=-started -complete
greeting-repeat-once-party=agent
ims-3pcc-prefix=
ims-default-icid-prefix=
ims-default-icid-suffix=
ims-default-orig-ioi=
ims-propagate-pcvector=false
ims-puid-domain=
ims-route=
ims-sip-domain=
ims-sip-params=
ims-skip-ifc=
inbound-bsns-calls=false
info-pass-through=
inherit-bsns-type=false
init-dnis-by-ruri=false
internal-bsns-calls=false
internal-registrar-domains=
internal-registrar-enabled=true
internal-registrar-persistent=false
intrusion-enabled=true
kpl-interval=10
kpl-loss-rate=10,100
kpl-tolerance=3
legal-guard-time=0
log-trace-flags+=iscc +cfg$dn -cfgserv +passwd +udata -devlink -sw
-req -callops -conn -client
logout-on-disconnect=true
logout-on-out-of-service=false
make-call-alert-info=
management-port=0
map-sip-errors=true
max-legs-per-sm=0
max-pred-req-delay=3
merged-user-data=main-only
monitor-consult-calls=false
monitor-internal-calls=true
msml-record-support=false
msml-support=false
music-in-conference-file=
music-in-queue-file=
mwi-agent-enable=false
mwi-domain=
mwi-extension-enable=false
mwi-group-enable=false
mwi-host=
mwi-implicit-notify=
mwi-mode=SUBSCRIBE
mwi-port=5060
nas-indication=none
nas-private=false
observing-routing-point=
outbound-bsns-calls=false
overload-ctrl-call-rate-capacity=200
overload-ctrl-dialog-rate-capacity=400
overload-ctrl-threshold=0
override-switch-acw=false
override-to-on-divert=false
p-asserted-identity=
parking-music=music/silence
partition-id=SipServerDefaultPartition
posn-no-answer-overflow=
posn-no-answer-timeout=15
prd-dist-call-ans-time=0
```



```
predictive-call-router-timeout=0
preview-expired=90
privacy=
propagated-call-type=false
reason-in-extension=true
recall-no-answer-timeout=15
record-after-merge=false
record-consult-calls=false
recording-filename=
refer-enabled=true
reg-interval=60
registrar-default-timeout=0
releasing-party-report=false
resolve-sip-address=false
resource-management-by-rm=true
restart-period=20
ring-tone=music/ring_back
ringing-on-route-point=true
route-failure-alarm-high-wm=10
route-failure-alarm-low-wm=1
route-failure-alarm-period=0
router-timeout=10
rq-conflict-check=true
rq-expire-tmout=0
rq-expire-tout=0
send-200-on-clear-call=true
server-id=360
server-role=0
session-refresh-interval=1800
set-notready-on-busy=false
shutdown-sip-reject-code=603
silence-detected=drop
silence-tone=music/silence
sip-491-passthrough=false
sip-address=
sip-address-srv=
sip-alert-info=
sip-alert-info-consult=
sip-alert-info-external=
sip-block-headers=
sip-call-retain-timeout=1
sip-dtmf-send-rtp=false
sip-enable-100rel=true
sip-enable-call-info=false
sip-enable-gdns=true
sip-enable-moh=false
sip-enable-rfc3263=false
sip-enable-sdp-application-filter=false
sip-enable-sdp-codec-filter=false
sip-error-conversion=
sip-from-pass-through=false
sip-hold-rfc3264=false
sip-invite-timeout=0
sip-invite-treatment-timeout=0
sip-ip-tos=256
sip-legacy-invite-retr-interval=false
sip-link-type=0
sip-max-retry-listen=15
```

```
sip-max-uui-length=256
sip-pass-check=false
sip-pass-from-parameters=
sip-pass-refer-headers=
sip-port=5060
sip-port-tls=0
sip-preserve-contact=false
sip-proxy-headers-enabled=true
sip-referxfer-bye-timeout=0
sip-replaces-mode=0
sip-respect-privacy=true
sip-retry-timeout=30
sip-ring-tone-mode=0
sip-timer-c-support=false
sip-tls-cert=
sip-tls-cert-key=
sip-tls-cipher-list=
sip-tls-crl=
sip-tls-mutual=false
sip-tls-target-name-check=
sip-tls-trusted-ca=
sip-treatment-dtmf-interruptable=false
sip-treatments-continuous=false
stranded-call-redirection-limit=4
stranded-calls-overflow=
stranded-on-arrival-calls-overflow=
subscription-delay=0
subscription-event-allowed=
subscription-timeout=180
sync-emu-agent=false
timed-acw-in-idle=true
tlib-map-replace-dn=false
unknown-bsns-calls=false
unknown-xfer-merge-udata=false
untimed-wrap-up-value=1000
use-display-name=false
user-data-limit=16000
userdata-map-all-calls=false
userdata-map-trans-prefix=
wrap-up-threshold=0
wrap-up-time=0
```

4.3 IP Phones

Polycom® SoundPoint® IP 650 phones were used during certification testing as the incumbent phone. AudioCodes 320HD phones were set up as parallel endpoints. AudioCodes' phones have achieved Genesys certification, positioning AudioCodes as a complete connectivity partner for Genesys. The configuration and software version for the phones is shown below.

4.3.1 AudioCodes 320HD IP Phone

4.3.1.1 Firmware Version

SIP = 320HD_1.6.0_build_37_4

4.3.1.2 Example Configuration

Only relevant parameters are listed.

```
;1.6.0_build_37_4
system/type=320HD
provisioning/method=STATIC
provisioning/firmware/url=tftp://192.168.4.2/320HD_1.6.0_build_37_4.img
voip/line/0/enabled=1
voip/line/0/id=9192943623
voip/line/0/description=320hd3623
voip/line/0/auth_name=9192943623
voip/line/0/auth_password=
voip/line/0/do_not_disturb/activated=0
voip/line/0/call_forward/enabled=1
voip/line/0/call_forward/timeout=6
voip/line/0/call_forward/type=NO_REPLY
voip/line/0/call_forward/destination=
voip/line/0/call_forward/active=0
voip/line/0/extension_display=
voip/line/1/enabled=0
voip/line/1/id=0
voip/line/1/description=320HD
voip/line/1/auth_name=0
voip/line/1/auth_password={'X8qWfXG895I='}
voip/line/1/do_not_disturb/activated=0
voip/line/1/call_forward/enabled=1
voip/line/1/call_forward/timeout=6
voip/line/1/call_forward/type=NO_REPLY
voip/line/1/call_forward/destination=
voip/line/1/call_forward/active=0
voip/line/1/extension_display=
voip/codec/g722_bitrate=G722_64K
voip/codec/g723_bitrate=HIGH
voip/codec/codec_info/0/enabled=1
voip/codec/codec_info/0/name=G729
voip/codec/codec_info/0/ptime=30
voip/codec/codec_info/1/enabled=1
voip/codec/codec_info/1/name=PCMU
voip/codec/codec_info/1/ptime=30
voip/codec/codec_info/2/enabled=0
voip/codec/codec_info/2/name=PCMA
voip/codec/codec_info/2/ptime=20
voip/codec/codec_info/3/enabled=0
voip/codec/codec_info/3/name=G729
voip/codec/codec_info/3/ptime=20
voip/codec/codec_info/4/enabled=0
voip/codec/codec_info/4/name=PCMU
voip/codec/codec_info/4/ptime=10
voip/signalling/sip/sdp_include_ptime=0
voip/signalling/sip/transport_protocol=UDP
voip/signalling/sip/port=5060
voip/signalling/sip/proxy_address=angel.z101.gchariot.com
voip/signalling/sip/proxy_port=5060
voip/signalling/sip/auth_retries=4
voip/signalling/sip/tls_port=5061
voip/signalling/sip/enable_sips=0
```

```
voip/signalling/sip/proxy_timeout=3600
voip/signalling/sip/registration_failed_timeout=60
voip/signalling/sip/sip_registrar/enabled=0
voip/signalling/sip/sip_registrar/port=5060
voip/signalling/sip/sip_registrar/addr=0.0.0.0
voip/signalling/sip/sip_outbound_proxy/enabled=0
voip/signalling/sip/sip_outbound_proxy/port=5060
voip/signalling/sip/sip_outbound_proxy/addr=0.0.0.0
voip/signalling/sip/redundant_outbound_proxy/enabled=0
voip/signalling/sip/redundant_outbound_proxy/port=5060
voip/signalling/sip/redundant_outbound_proxy/address=0.0.0.0
voip/signalling/sip/redundant_outbound_proxy/keepalive_period=60
voip/signalling/sip/redundant_outbound_proxy/symmetric_mode=0
voip/signalling/sip/sip_t1=500
voip/signalling/sip/sip_t2=4000
voip/signalling/sip/sip_t4=5000
voip/signalling/sip/subs_no_notify_timer=32000
voip/signalling/sip/sip_invite_timer=32000
voip/signalling/sip/session_timer=1800
voip/signalling/sip/min_session_interval=90
voip/signalling/sip/block_callerid_on_outgoing_calls=0
voip/signalling/sip/anonymous_calls_blocking=0
voip/signalling/sip/proxy_gateway=
voip/signalling/sip/digit_map=
voip/signalling/sip/number_rules=
voip/signalling/sip/use_proxy_ip_port_for_registrar=1
voip/signalling/sip/prack/enabled=1
voip/signalling/sip/rport/enabled=1
voip/signalling/sip/connect_media_on_180=0
voip/signalling/sip/keepalive_options/enabled=0
voip/signalling/sip/keepalive_options/timeout=300
voip/signalling/sip/use_proxy=1
voip/signalling/sip/tos=96
voip/signalling/sip/redundant_proxy/enabled=0
voip/signalling/sip/redundant_proxy/port=5060
voip/signalling/sip/redundant_proxy/address=0.0.0.0
voip/signalling/sip/redundant_proxy/keepalive_period=60
voip/signalling/sip/redundant_proxy/symmetric_mode=0
voip/signalling/sip/display_name_in_registration_msg/enabled=0
voip/signalling/sip/semi_transfer_with_no_cancel/enabled=0
voip/signalling/sip/registrar_ka/enabled=0
voip/signalling/sip/registrar_ka/timeout=60
```

4.3.2 Polycom SoundPoint IP 650

4.3.2.1 Firmware version

```
Bootblock = 3.0.2.0024 (12600-001)
Updater = 5.0.2.12692
SIP = 4.0.2.11307
```

4.3.2.2 Example Configuration

```
<?xml version='1.0' encoding='UTF-8' standalone='yes'?>
<!-- Application SIP Mink 4.0.2.11307 21-Mar-12 12:04 -->
<!-- Created 11-05-2012 12:48 -->
<PHONE_CONFIG>
  <ALL
    np.normal.ringing.calls.tonePattern='ringer4'
    np.normal.ringing.toneVolume.chassis='9'
    up.backlight.idleIntensity='0'
    up.backlight.timeout='15'
    voice.codecPref.G722='8'
    voice.codecPref.G729_AB='4'
    voIpProt.SIP.outboundProxy.address='10.38.5.117'
    voIpProt.SIP.outboundProxy.port='5060'
    reg.1.address='9192943620@angel.z101.gchariot.com'
    reg.1.auth.password='123456'
    reg.1.auth.userId='9192943620'
    reg.1.displayName='9192943620'
    reg.1.label='9192943620'
    voIpProt.server.1.address='angel.z101.gchariot.com'
    voIpProt.server.1.port='5060'
    voIpProt.server.1.transport='UDPOnly'
  />
</PHONE_CONFIG>
```

Reader's Notes

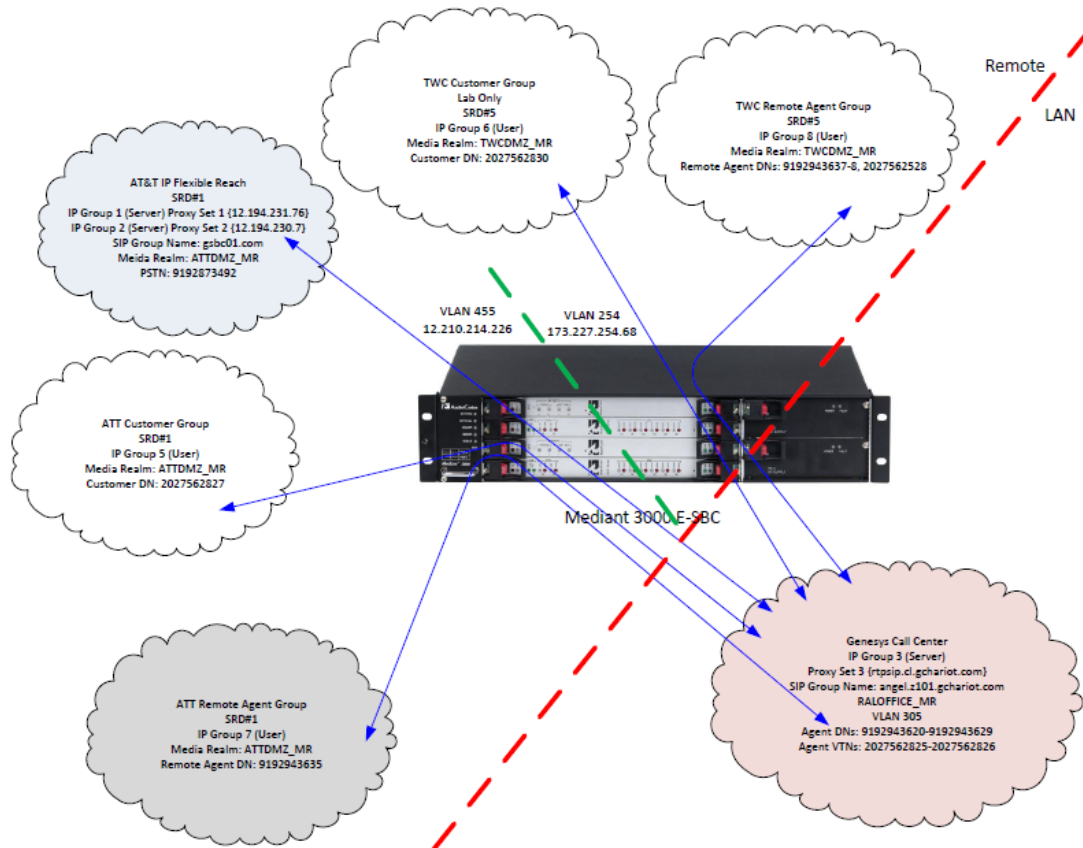
5 Configuring the Mediant 3000 E-SBC

This section describes configuration of the Mediant 3000 E-SBC for the previously defined scenario, using the Web Interface:

1. [Basic Configuration via the Web GUI](#)
2. [SIP Header Manipulation](#)
3. [Device Configuration Files](#)

For information on product specifics, see the Mediant 3000 SIP User's Manual.

Figure 5-1: E-SBC Interfaces/Configuration



5.1 Basic Configuration via the Web GUI

Take these steps to configure the Mediant 3000 E-SBC:

- Step 1: [Configure the Multiple Interface Table](#)
- Step 2: [Configure DNS/SRV Tables](#)
- Step 3: [Configure Firewall Settings](#)
- Step 4: [Enable the SBC Application](#)
- Step 5: [Configure the Number of Media Channels](#)
- Step 6: [Configure the SRD Table](#)
- Step 7: [Configure Media Realm Table](#)
- Step 8: [Configure the SIP Interfaces Table](#)
- Step 9: [Configure the IP Groups](#)
- Step 10: [Configure the Proxy Sets](#)
- Step 11: [Define the Classification Rules](#)

- Step 12: [Configure SBC General Settings](#)
- Step 13: [Configure SBC Admission Control](#)
- Step 14: [Configure Allowed Coders Group](#)
- Step 15: [Configure IP Profiles](#)
- Step 16: [Configure SBC IP-to-IP Routing Setup](#)

5.1.1 Configure the Multiple Interface Table

This section describes how to configure the Multiple Interface Table for the different logical networks used to connect to the Flexible Reach SIP Trunk, the Genesys Call Center Network and other external networks. This step assumes the Mediant has already been assigned an initial OAMP IP address (see the Mediant 3000 Installation Guide or User Manual).

The example described in this document was that of the certification environment, which used the following interfaces:

- 'NETMGMT' is the OAMP interface for all management of the E-SBC. This was VLAN 320 in the certification environment.
- 'PUBSIP' is the Media + Control interface to a public domain on which Remote Agents or Customers may exist. This was VLAN 254 in the certification environment.
- 'RALVOX' is the Media + Control interface for the Agents in the Call Center private network. This was VLAN 360 in the laboratory environment.
- 'ATTDMZ' is the Media + Control interface over which the IP Flexible Reach Services are provided. This is the IP access that leads PSTN. Customer or Remote Agents may exist in this space. This was VLAN 455 in the certification environment.
- 'RALOFFICE' is the Media + Control interface on which the Genesys Voice Platform resides. Outbound SIP messaging will route to/from the SBC over this interface. This was VLAN 305.

➤ To configure the Multiple Interface Table:

1. Open the Multiple Interface Table (**Configuration > VoIP > Network Settings > IP Settings**).
2. In the 'Add Index' field, enter the desired index number for the new interface and then click **Add Index**. The index row is added to the table.
3. Configure the Application Type {OAMP, Media, Control, OAMP + Media, OAMP + Control, Media + Control, OAMP + Media + Control}
4. Configure Interface Mode (IPv4 Manual or IPv6 Manual).
5. Assign the IP address for the interface.
6. Assign the Prefix Length (Subnet mask as a Classless Inter-Domain Routing (CIDR) style presentation).
7. Define the default gateway.
8. Define the VLAN ID assigned to the interface. Incoming traffic with this VLAN ID is routed to the corresponding interface and outgoing traffic from that interface is tagged with this VLAN ID.
9. Define the mandatory, unique interface name (up to 16 chars). This name is displayed in management interfaces (such as Web, CLI and SNMP) and the Media Realm and SIP Interface table for clarity only.
10. Configure the External DNS Servers for the solution (the certification environment did not use External DNS but Internal DNS, described in the next section).
11. Set VLAN Mode to 'Enable'.
12. Set the Native VLAN ID (this was 320 for the certification environment).
13. Click the **Apply** button; the interface is added to the table and the **Done** button

appears.

14. Click **Done** to validate the interface; if the interface is invalid, a warning message is displayed.

Figure 5-2: Configuring the Multiple Interface Table

Multiple Interface Table

Note: Select row index to modify the relevant row.

Index	Application Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name	Primary DNS Server Address	Secondary DNS Server IP Address
0	<input type="radio"/> OAMP	IPv4 Manual	10.38.20.10	24	10.38.20.1	320	NETMGMT	0.0.0.0	0.0.0.0
1	<input type="radio"/> Media + Control	IPv4 Manual	173.227.254.68	26	173.227.254.65	254	PUBSIP	0.0.0.0	0.0.0.0
2	<input type="radio"/> Media + Control	IPv4 Manual	10.38.60.10	24	10.38.60.1	360	RALVOX	0.0.0.0	0.0.0.0
3	<input type="radio"/> Media + Control	IPv4 Manual	12.210.214.226	29	12.210.214.225	455	ATTDMZ	0.0.0.0	0.0.0.0
4	<input type="radio"/> Media + Control	IPv4 Manual	10.38.5.10	24	10.38.5.1	305	RALOFFICE	0.0.0.0	0.0.0.0

VLAN Mode:

Native VLAN ID:

5.1.2 Configure DNS/SRV Tables

The Mediant 3000 E-SBC features the capability of translating domain names into IP addresses via an external, third-party Domain Name Server (DNS), as defined in the Multiple Interface Table, or by the device's embedded DNS. Two DNS types are supported on the device: an Internal DNS table and an Internal SRV table. The Internal DNS table can translate up to 20 host (domain) names into IP address. The Internal SRV Table resolves host names to DNS A-Records. Three different A-Records can be assigned to each host name. Each A-Record contains the host name, priority, weight, and port. The Internal DNS table configuration is demonstrated below. See the Mediant 3000 SIP User Manual for additional information about DNS/SRV tables.

➤ To configure the Internal DNS table:

1. Open the Internal DNS Table Page (**Configuration > VoIP > Network > DNS > Internal DNS Table**).
2. In the 'Domain Name' field, enter the host name to be translated.
3. In the 'First IP Address' field, enter the first IP address to which the hostname is translated.
4. Optionally, in the 'Second IP Address', 'Third IP Address', and 'Second IP Address' fields, enter the next IP addresses to which the host name is translated.
5. Click **Submit** to apply changes
6. Save the configuration to flash memory.

Figure 5-3: Internal DNS Table

Internal DNS Table

Internal DNS Index:

	Domain Name	First IP Address	Second IP Address	Third IP Address
1	rtpsip.cl.gchariot.com	10.38.5.117	0.0.0.0	0.0.0.0

5.1.3 Configure Firewall Settings

The Mediant 3000 E-SBC allows up to 25 ordered firewall rules for network traffic filtering. This access list provides the following rules:

- Block traffic from malicious sources
- Only allow traffic from known friendly sources, and block all others
- Mix allowed and blocked network sources
- Limit traffic to a predefined rate (blocking the excess)
- Limit traffic to specific protocols and port ranges on the device

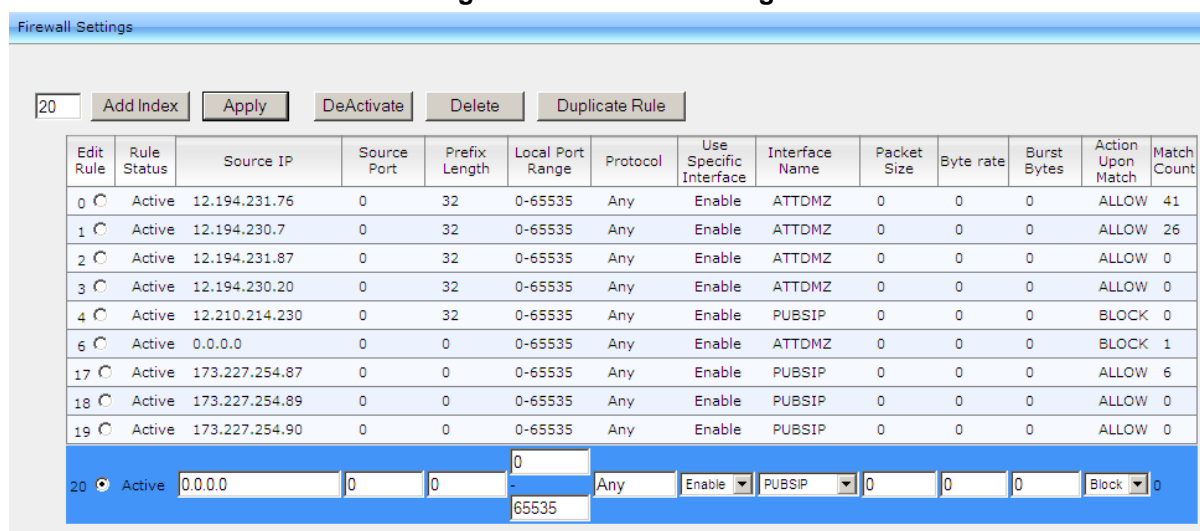
For each packet received on the network interface, the table is scanned from the top down until a matching rule is found. The rule can either deny (block) or permit (allow) the packet. Once a rule in the table is located, subsequent rules are ignored. If the end is reached without a match, the packet is accepted.

See the Mediant 3000 SIP User's Manual for more detailed description regarding configuring the firewall rules. Additionally, see the document 'Recommended Security Guidelines Technical Note' for recommendations on security settings.

➤ To add firewall rules:

1. Open the Firewall Setting Page (**Configuration > VoIP > Security > Firewall Settings**).
2. In the 'Add' field, enter the index of the access rule to be added and then click **Add**.
3. Configure the firewall rule's parameters.
4. Click **Apply** to save the new rule.
5. Select **Activate/DeActivate** as appropriate to activate or deactivate the rule.
6. Save the configuration to flash memory.

Figure 5-4: Firewall Settings



Edit Rule	Rule Status	Source IP	Source Port	Prefix Length	Local Port Range	Protocol	Use Specific Interface	Interface Name	Packet Size	Byte rate	Burst Bytes	Action Upon Match	Match Count
0	<input checked="" type="radio"/> Active	12.194.231.76	0	32	0-65535	Any	Enable	ATTDMZ	0	0	0	ALLOW	41
1	<input checked="" type="radio"/> Active	12.194.230.7	0	32	0-65535	Any	Enable	ATTDMZ	0	0	0	ALLOW	26
2	<input checked="" type="radio"/> Active	12.194.231.87	0	32	0-65535	Any	Enable	ATTDMZ	0	0	0	ALLOW	0
3	<input checked="" type="radio"/> Active	12.194.230.20	0	32	0-65535	Any	Enable	ATTDMZ	0	0	0	ALLOW	0
4	<input checked="" type="radio"/> Active	12.210.214.230	0	32	0-65535	Any	Enable	PUBSIP	0	0	0	BLOCK	0
6	<input checked="" type="radio"/> Active	0.0.0.0	0	0	0-65535	Any	Enable	ATTDMZ	0	0	0	BLOCK	1
17	<input checked="" type="radio"/> Active	173.227.254.87	0	0	0-65535	Any	Enable	PUBSIP	0	0	0	ALLOW	6
18	<input checked="" type="radio"/> Active	173.227.254.89	0	0	0-65535	Any	Enable	PUBSIP	0	0	0	ALLOW	0
19	<input checked="" type="radio"/> Active	173.227.254.90	0	0	0-65535	Any	Enable	PUBSIP	0	0	0	ALLOW	0

20	<input checked="" type="radio"/> Active	0.0.0.0	0	0	0-65535	Any	Enable	PUBSIP	0	0	0	Block	0
----	---	---------	---	---	---------	-----	--------	--------	---	---	---	-------	---

The example above shows some simple access list settings. These rules should be more stringent in a production environment by narrowing port range and specifying protocol or other known traffic characteristics to reduce the risk of unwanted traffic passing through the firewall.

- Rule #0: traffic from the host 12.194.231.76 (Primary AT&T IPBE), on any port is allowed on the ATTDMZ interface.
- Rule #1: traffic from the host 12.194.230.7 (Secondary AT&T IPBE), on any port is allowed on the ATTDMZ interface.
- Rule #2: traffic from the host 12.194.231.87 (AT&T Media Portal), on any port is allowed on the ATTDMZ interface.

- Rule #3: traffic from the host 12.194.231.20 (AT&T Media Portal), on any port is allowed on the ATTDZ interface.
- Rule #4: traffic from the host 12.210.214.230 (IP Phone in the public space), on any port is allowed on the PUBSIP interface.
- Rule #6: All traffic (0.0.0.0 with Prefix Length 0), of any protocol, on any port, of the ATT DMZ interface is blocked. (See the recommendation in the Note below).
- Rule #17-19: traffic from the specific devices in the 173.227.254.xx network is allowed on the PUBSIP interface.



Note: It is recommended to add at the end of the table a rule that blocks all traffic, and to add above it in the table firewall rules that allow traffic (with bandwidth limitations). To block all traffic, the following must be set:

- IP address to 0.0.0.0
- Prefix length of 0 (rule matches any IP address)
- Local port range 0-65535
- Protocol 'Any'
- Action Upon Match 'block'

5.1.4 Enable the SBC Application

This step describes how to enable the device's SBC application.

➤ **To enable the SBC application on the Mediant 3000 E-SBC:**

1. Open the Applications Enabling page (**Configuration > VoIP > Applications Enabling > Applications Enabling**).
2. From the relevant application drop-down list (SBC Application), select **Enable**.
3. Select the **Submit** button.
4. Save the changes to the device's flash memory with burn and reset (required).

Figure 5-5: Applications Enabling



Note:

- The page displays the application only if the device is installed with the relevant Software Upgrade Key supporting the application.
- For this parameter to take effect, a device reset is required.
- In addition to enabling this parameter, the number of maximum SBC/IP-to-IP sessions must be defined in the Software Upgrade Key.

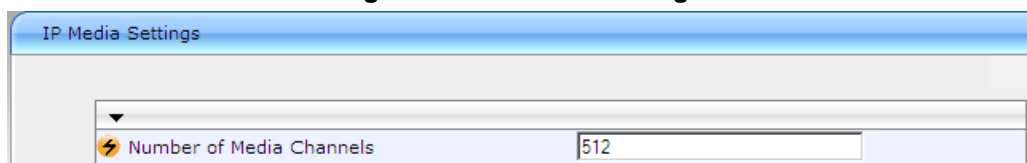
5.1.5 Configure the Number of Media Channels

DSP channels are allocated for functionality such as IP-to-IP sessions. The RTP streams for IP-to-IP calls always traverse the device and two DSP channels are allocated per IP-to-IP session. The maximum number of media channels on the Mediant 3000 E-SBC for IP-to-IP calls is therefore 2016, or 1008 IP-to-IP calls. The SBC application only requires DSP channels when media transcoding is required. No media transcoding was used in the AT&T/Genesys/AudioCodes certification testing.

➤ **To configure the number of media channels:**

1. Open the IP Media Settings page (**Configuration > VoIP > IP Media > IP Media Settings**).
2. In the 'Number of Media Channels' field, enter the required number of media channels (in the example shown below, from default 0 to 512 channels to enable 256 IP-to-IP calls).
3. Click **Submit**.
4. Save the settings to flash memory ('burn') and reset the device.

Figure 5-6: IP Media Settings



The screenshot shows a web interface titled 'IP Media Settings'. Below the title bar, there is a dropdown menu and a text input field labeled 'Number of Media Channels' with the value '512' entered. A small lightning bolt icon is visible to the left of the input field.



Note:

- For the parameter to take effect, a device reset is required.
- The SBC application does not require DSP channels when no media transcoding is required. (This was the scenario used in the certification with AT&T and Genesys Voice Platform).
- If media transcoding is required, two DSP channels are used per transcoding session.
- The maximum is also subject to the 'Feature Key' setting.

5.1.6 Configure the SRD Table

The SRD (Signaling Routing Domain) Table allows configuring up to 32 SRDs. An SRD is configured with a unique name and assigned a Media Realm (defined in the Media Realm table). In addition, other SBC attributes such as media anchoring and user registration can be configured. SRDs can be used as follows:

- Associate the SRD with a SIP Interface
- Associate the SRD with an IP Group
- Associate the SRD with a Proxy Set
- Associate the SRD with an Admission Control rule
- Define the SRD as a Classification rule for the incoming SIP request
- Use the SRD as a destination IP-to-IP routing rule

An SRD is therefore a set of definitions together creating multiple, virtual, multi-service IP gateways that may have the following characteristics:

- Multiple and different SIP signaling interfaces (SRD associated with a SIP Interface) and RTP media (associated with a Media Realm) for multiple Layer-3 networks. Due to the B2BUA nature of the SBC application, different interfaces can be assigned to each leg of the call.
- Can operate with multiple gateway customers that may reside either in the same or in different Layer-3 networks as the device. This allows separation of signaling traffic between different customers. In such a scenario, the device is configured with multiple SRDs.

Typically, one SRD is defined for each group of SIP UAs (e.g., proxies, IP phones, Application Servers, gateways, soft switches) that communicate with each other. This association provides these entities with VoIP services that reside on the same Layer-3 network (SIP UAs must be able to communicate without traversing NAT devices and must not have overlapping IP addresses). Routing from one SRD to another is possible, whereby each routing destination (IP Group or destination address) indicates the SRD to which it belongs.

The SRD Settings page also displays the IP Groups, Proxy Sets, and SIP Interfaces associated with a selected SRD index.

In the certification environment, the following four SRDs were defined and associated with a SIP interface and Media Realm:

1. 'ATTDMZ_SRD' (see [Figure 5-7](#) below)
2. 'RALVOX_SRD' (see [Figure 5-8](#) below)
3. 'RALOFFICE_SRD' (see [Figure 5-9](#) below)
4. 'TWCDMZ_IPP' (see [Figure 5-10](#) below)

➤ To configure SRDs:

1. Open the SRD Settings page (**Configuration > VoIP > Control Network > SRD Table**).
2. From the 'SRD Index' drop-down list, select an index for the SRD, and then configure the parameters.
3. Click **Submit** to apply changes.
4. Save the changes to flash memory.

Figure 5-7: ATDMZ_SRD

SRD Settings

SRD Index: 1 - ATDMZ_SRD

Common Parameters

SRD Name: ATDMZ_SRD

Media Realm: ATDMZ_MR

SBC Parameters

IP Group Status Table

Proxy Sets Status Table

Remove

SIP Interface Table

Add

Note: Select row button to modify the relevant row.

	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	Message Policy
<input checked="" type="radio"/>	ATDMZ	SBC	5060	5060	5061	None

Figure 5-8: RALVOX_SRD

SRD Settings

SRD Index: 2 - RALVOX_SRD

Common Parameters

SRD Name: RALVOX_SRD

Media Realm: RALVOX_MR

SBC Parameters

IP Group Status Table

Proxy Sets Status Table

Remove

SIP Interface Table

Add

Note: Select row button to modify the relevant row.

	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	Message Policy
<input checked="" type="radio"/>	RALVOX	SBC	5060	5060	5061	None

Figure 5-9: RALOFFICE_SRD

SRD Settings

SRD Index
3 - RALOFFICE_SRD

Common Parameters

SRD Name
RALOFFICE_SRD

Media Realm
RALOFFICE_MR

SBC Parameters

IP Group Status Table

Proxy Sets Status Table

Remove

SIP Interface Table

Add

Note: Select row button to modify the relevant row.

	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	Message Policy
<input type="radio"/>	RALOFFICE	SBC	5060	5060	5061	None

Figure 5-10: TWCDMZ_IPP

SRD Settings

SRD Index
5 - TWCDMZ_IPP

Common Parameters

SRD Name
TWCDMZ_IPP

Media Realm
TWCDMZ_MR

SBC Parameters

IP Group Status Table

Proxy Sets Status Table

Remove

SIP Interface Table

Add

Note: Select row button to modify the relevant row.

	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	Message Policy
<input type="radio"/>	PUBSIP	SBC	5060	5060	5061	None

5.1.7 Configure Media Realm Table

The Media Realm Table is used to define a pool of up to 64 SIP media interfaces, termed 'Media Realms'. Media Realms allow a Media type interface (defined in the Multiple Interface table) to be divided into several realms, where each realm is specified by a UDP port range. Additionally, the maximum number of sessions per Media Realm can be specified. Once created, Media Realms can be assigned to IP Groups (in the IP Group table) or SRDs (in the SRD), or both. Later in this provisioning, the SIP signaling interfaces will be associated with the RTP interfaces under one entity, the SRD.

**Note:**

- If different Media Realms are assigned to an IP Group and to an SRD, the IP Group's Media Realm takes precedence.
- For this setting to take effect, a device reset is required.

In this implementation, there are four Media Realms to define and associate with an interface. Though defined arbitrarily, the names are unique, and will be used later in the SRD and IP Groups table configuration.

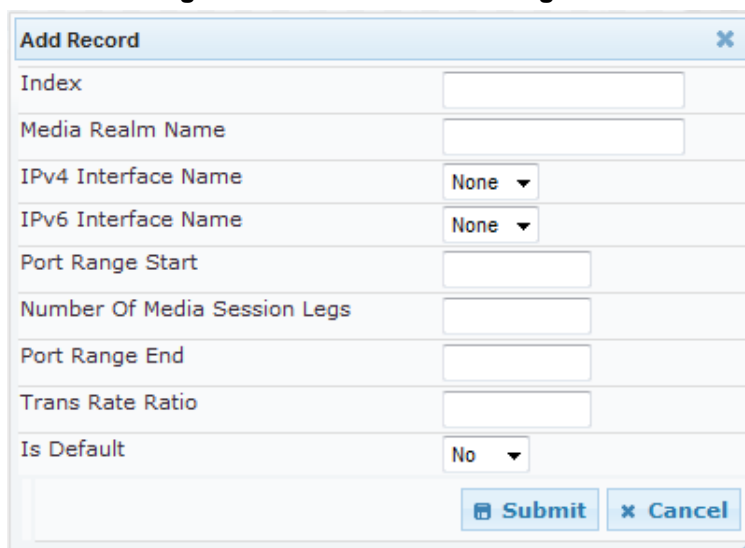
1. ATDMZ_MR - the interface out to the AT&T IPBE and eventual PSTN network (or even an IP network beyond that). Remote Agents and/or customers can be signaled through this interface.
2. RALVOX_MR – the interface to the local Call Agents in the Genesys Call Center private network.
3. RALOFFICE_MR – the interface to the Genesys SIP Server in the Genesys Call Center private network.
4. TWCDMZ_MR – this interface is a second public network for which Remote agents/Customers may exist for testing purposes.

**Note:**

- The name assigned to the IPv4/IPv6 interface is case sensitive and must be identical to the name configured in the Multiple Interface Table.
- For this setting to take effect, a device reset is required.

➤ **To define a Media Realm:**

1. Open the Media Realm Table page (**Configuration > VoIP > Media > Media Realm Configuration**).
2. Click the **Add** button; the following appears:

Figure 5-11: Add Record Dialog Box


The dialog box titled "Add Record" contains the following fields and controls:

- Index: Text input field
- Media Realm Name: Text input field
- IPv4 Interface Name: Dropdown menu with "None" selected
- IPv6 Interface Name: Dropdown menu with "None" selected
- Port Range Start: Text input field
- Number Of Media Session Legs: Text input field
- Port Range End: Text input field
- Trans Rate Ratio: Text input field
- Is Default: Dropdown menu with "No" selected
- Submit: Button with a floppy disk icon
- Cancel: Button with an "X" icon

3. Configure the parameters as required for each Media Realm.
4. Click **Submit** to apply your settings.
5. Reset the device to save the changes to flash memory

Figure 5-12: SIP Interface Table

Media Realm Table			
Add Edit Delete View/Unview			
Index	Media Realm Name	IPv4 Interface Name	IPv6 Interface Name
0	ATDMZ_MR	ATDMZ	None
1	RALVOX_MR	RALVOX	None
2	RALOFFICE_MR	RALOFFICE	None
3	TWCDMZ_MR	PUBSIP	None

Page 1 of 1 10 View 1 -

Figure 5-13: Media Realm #0

Media Realm #0 Additional Configuration

[Quality Of Experience](#)

Details of Media Realm #0

Media Realm Name = ATDMZ_MR
 IPv6 Interface Name = None
 Number Of Media Session Legs = 600
 Trans Rate Ratio = 1

IPv4 Interface Name = ATDMZ
 Port Range Start = 16390
 Port Range End = 22380
 Is Default = Yes

Figure 5-14: Media Realm #1

Media Realm #1 Additional Configuration[Quality Of Experience](#)**Details of Media Realm #1**

Media Realm Name = RALVOX_MR
IPv6 Interface Name = None
Number Of Media Session Legs = 50
Trans Rate Ratio = 1

IPv4 Interface Name = RALVOX
Port Range Start = 6000
Port Range End = 6490
Is Default = No

Figure 5-15: Media Realm #2

Media Realm #2 Additional Configuration[Quality Of Experience](#)**Details of Media Realm #2**

Media Realm Name = RALLOFFICE_MR
IPv6 Interface Name = None
Number Of Media Session Legs = 550
Trans Rate Ratio = 1

IPv4 Interface Name = RALLOFFICE
Port Range Start = 6500
Port Range End = 11990
Is Default = No

Figure 5-16: Media Realm #3

Media Realm #3 Additional Configuration[Quality Of Experience](#)**Details of Media Realm #3**

Media Realm Name = TWCDMZ_MR
IPv6 Interface Name = None
Number Of Media Session Legs = 100
Trans Rate Ratio = 0

IPv4 Interface Name = PUBSIP
Port Range Start = 12000
Port Range End = 12990
Is Default = No

5.1.8 Configure the SIP Interfaces Table

A SIP Interface consists of a combination of ports (UDP, TCP, and TLS), associated with a specific IP address (IPv4 / IPv6), and for a specific application (i.e., SAS, Gateway\IP2IP, or in this case, the SBC). Up to 32 SIP signaling interfaces are defined in the SIP Interfaces table. Later in the provisioning, the SIP signaling interfaces will be associated to the RTP interfaces under one entity called the Signaling Routing Domain (SRD).

For the certification environment, there were four SIP interfaces (pathways for which SIP signaling will travel):

1. ATDMZ - the interface out to the AT&T IPBE and eventual PSTN network (or even an IP network beyond that). Remote Agents and/or customers can be signaled through this interface.
2. RALVOX – the interface to the local Call Agents in the Genesys Call Center private network.
3. RALOFFICE – the interface to the Genesys SIP Server in the Genesys Call Center private network.
4. PUBSIP – this interface is a second public network for which Remote agents/Customers may exist for testing purposes.

➤ To configure the SIP Interface table:

1. Open the 'SIP Interface Table' page (**Configuration** tab > **VoIP** > **Control Network** > **SIP Interface Table**).
2. Add an entry for each interface listed above (see the figure below).
 - Application Type = SBC
 - UDP Port = 5060 (default)
 - TCP port = 5060 (default)
 - TLS port = 5061 (default)
 - SRD = SRD # that respective interface will belong to. This scenario used 1, 2, 3, & 5

Figure 5-17: SIP Interface Table

SIP Interface Table

Note: Select row index to modify the relevant row.

Index	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	SRD	Message Policy
1	ATDMZ	SBC	5060	5060	5061	1	None
2	RALVOX	SBC	5060	5060	5061	2	None
3	RALOFFICE	SBC	5060	5060	5061	3	None
5	PUBSIP	SBC	5060	5060	5061	5	None

5.1.9 Configure the IP Groups

The IP Group Table allows for the creation of up to 32 logical IP entities called IP Groups. An IP Group is an entity with a set of definitions such as a Proxy Set ID which represents the IP address of the IP Group.

For the SBC application, IP Groups are used to classify incoming SIP dialog-initiating requests (e.g., INVITE messages) to a source IP Group, based on Proxy Set ID (defined in the Classification Table). This occurs if the database search for a registered user is unsuccessful. The classification process locates a Proxy Set ID (associated with the SIP dialog request's IP address) in the Proxy Set table, and then locates a match with an IP Group that is associated with this Proxy Set in the IP Group table.

This section describes how to create IP groups. Each IP group represents a SIP entity in the device's network. In the certification environment, IP groups for the following entities were defined:

1. IP Group 1: AT&T IP Flexible Reach SIP trunk (relates to the IPBE)
2. IP Group 2: AT&T IP Flexible Reach SIP trunk (relates to the secondary IPBE)
3. IP Group 3: Genesys SIP Server
4. IP Group 7: AT&T Remote Agents
5. IP Group 8: Non-AT&T Remote Agents

The following groups were created in the certification environment for test call originations/terminations only. These would not be required in a production environment but are included here to enhance understanding of the full laboratory configuration.

1. IP Group 5: Customers in the AT&T network
2. IP Group 6: Customers in non-AT&T network



Note:

- When operating with multiple IP Groups, the default Proxy Server mustn't be used (i.e., the 'IsProxyUsed' parameter must be set to 0).
- If different SRDs are configured in the IP Group and Proxy Set tables, the SRD defined for the Proxy Set takes precedence.
- You cannot modify IP Group Index 0. This IP Group is set to default values and is used by the device when IP Groups are not implemented.

➤ **To configure IP Groups:**

1. Open the 'IP Group Table' page (**Configuration > VoIP > Control Network> IP Group Table**).
2. Define IP Group #1 for the AT&T IP Flexible Reach SIP Trunk as follows:
 - a. IP Group Index '1'
 - b. Type: 'SERVER' (used when the destination address (configured by the Proxy Set) of the IP Group (e.g., ITSP, Proxy, IP-PBX, etc.) is known.
 - c. Description: Arbitrary name. (e.g., 'ATT IPGroup')
 - d. Proxy Set ID: '1' (represents the IP address for communicating with this IP Group).
 - e. SIP Group Name: <ip address>. This is the SIP Request-URI host name used in INVITE and REGISTER messages sent to the IP Group, or the host name in the From header of INVITE messages received from the IP Group. For AT&T, this needs to be the IP Address of the primary IPBE.
 - f. For Servers, the SRD is provisioned in the Proxy Set configuration.

- g. SIP Group Name: the SIP Request-URI host name used in INVITE and REGISTER messages sent to the IP Group, or the host name in the From header of INVITE messages received from the IP Group. If not specified, the value of the global parameter 'Proxy Name' (configured in 'Proxy and Registration Parameters') is used instead.
- h. Media Realm: 'ATDMZ_MR' - Assigns Media Realm to the IP Group. Must be identical to the Media Realm name in the Media Realm table.
- i. IP Profile ID: '1' – the IP Profile to be assigned to this IP group.
- j. Classify By Proxy Set: 'Enable' (default). This parameter is only applicable to Server type IP Groups. When enabled, the device will resolve the incoming SIP INVITE to an IP Group according to the Proxy set. If the INVITE's IP address is defined in the IP Group's Proxy Set ID, the INVITE is assigned to this IP Group.
- k. Outbound Message Manipulation Set: '0'. This parameter designates the rule that is assigned to this IP Group for SIP message manipulation on the outbound message. The Outbound Message Manipulation rules are explained later in this document (see [SIP Header Manipulation](#)).

Figure 5-18: ATT IP Group 1 (SERVER)

IP Group Table	
Index	1
Common Parameters	
Type	SERVER
Description	ATT IPGROUP
Proxy Set ID	1
SIP Group Name	12.194.231.76
Contact User	
Domain Name in Contact	
SRD	0
Media Realm	ATDMZ_MR
IP Profile ID	1
Gateway Parameters	
Always Use Route Table	No
Routing Mode	Not Configured
SIP Re-Routing Mode	Standard
SBC Parameters	
Classify By Proxy Set	Enable
Max Number Of Registered Users	-1
Inbound Message Manipulation Set	-1
Outbound Message Manipulation Set	0
Registration Mode	User initiates registrations
Authentication Mode	User authenticates
Authentication Method List	
Enable SBC Client Forking	No

3. Define IP Group #2 for the AT&T IP Flexible Reach Secondary SIP Trunk as follows:
 - a. IP Group Index '2'
 - b. Type: 'SERVER' (used when the destination address (configured by the Proxy Set) of the IP Group (e.g. ITSP, Proxy, IP-PBX, etc) is known.
 - c. Description: arbitrary name. (e.g., 'ATT Secondary IP Group')
 - d. Proxy Set ID: '2' (represents the IP address for communicating with this IP Group).
 - e. SIP Group Name: <ip address>. This is the SIP Request-URI host name used in INVITE and REGISTER messages sent to the IP Group, or the host name in the From header of INVITE messages received from the IP Group. For AT&T, this needs to be the IP Address of the secondary IPBE.
 - f. For Servers, the SRD is provisioned in the Proxy Set configuration.
 - g. SIP Group Name: the SIP Request-URI host name used in INVITE and REGISTER messages sent to the IP Group, or the host name in the From header of INVITE messages received from the IP Group. If not specified, the value of the global parameter 'Proxy Name' (configured in 'Proxy and Registration Parameters') is used instead.
 - h. Media Realm: 'ATTDZ_MR' - Assigns Media Realm to the IP Group. Must be identical to the Media Realm name in the Media Realm table.
 - i. IP Profile ID: '1' – the IP Profile to be assigned to this IP group.
 - j. Classify By Proxy Set: 'Enable' (default). This parameter is only applicable to Server type IP Groups. When enabled, the device will resolve the incoming SIP INVITE to an IP Group according to the Proxy set. If the INVITE's IP address is defined in the IP Group's Proxy Set ID, the INVITE is assigned to this IP Group.
 - k. Outbound Message Manipulation Set: '0'. This parameter designates the rule that is assigned to this IP Group for SIP message manipulation on the outbound message. The Outbound Message Manipulation rules are explained later in this document (see [SIP Header Manipulation](#)).

Figure 5-19: ATT Secondary IP Group 2 (SERVER)

IP Group Table	
Index	2
Common Parameters	
Type	SERVER
Description	ATT IPGroup secondary
Proxy Set ID	2
SIP Group Name	12.194.230.7
Contact User	
Domain Name in Contact	
SRD	0
Media Realm	ATDMZ_MR
IP Profile ID	1
Gateway Parameters	
Always Use Route Table	No
Routing Mode	Not Configured
SIP Re-Routing Mode	Standard
SBC Parameters	
Classify By Proxy Set	Enable
Max Number Of Registered Users	-1
Inbound Message Manipulation Set	-1
Outbound Message Manipulation Set	0
Registration Mode	User initiates registrations
Authentication Mode	User authenticates
Authentication Method List	
Enable SBC Client Forking	No

4. Define IP Group #3 for the Genesys SIP Server as follows:
 - a. IP Group Index '3'
 - b. Type: 'SERVER' (used when the destination address (configured by the Proxy Set) of the IP Group (e.g. ITSP, Proxy, IP-PBX, or Application Server) is known.
 - c. Description: arbitrary name. (e.g., 'GENESYS_SRV')
 - d. Proxy Set ID: '3' (represents the IP address for communicating with this IP Group).
 - e. For Servers, the associated SRD will be in the Proxy Set configuration.
 - f. SIP Group Name: the SIP Request-URI host name used in INVITE and REGISTER messages sent to the IP Group, or the host name in the From header of INVITE messages received from the IP Group. If not specified, the value of the global parameter 'Proxy Name' (configured in 'Proxy and Registration Parameters') is used instead.
 - g. Media Realm: 'RALOFFICE_MR' - Assigns Media Realm to the IP Group. Must be identical to the Media Realm name in the Media Realm table.
 - h. IP Profile ID: '0' (default)
 - i. Classify By Proxy Set: 'Enable' (default). This parameter is only applicable to Server type IP Groups. When enabled, the E-SBC will resolve the incoming SIP INVITE to an IP Group according to the Proxy set. If the INVITE's IP address is defined in the IP Group's Proxy Set ID, the INVITE is assigned to this IP Group.

- j. Outbound Message Manipulation Set: '3'. This parameter designates the rule that is assigned to this IP Group for SIP message manipulation on the outbound message. The Outbound Message Manipulation rules are explained later in this document (see [SIP Header Manipulation](#)).

Figure 5-20: Genesys Server IP Group 3

Common Parameters	
Type	SERVER
Description	GENESYS_SRV
Proxy Set ID	3
SIP Group Name	angel.z101.gchariot.com
Contact User	
Domain Name in Contact	
SRD	0
Media Realm	RALLOFFICE_MR
IP Profile ID	0

Gateway Parameters	
Always Use Route Table	No
Routing Mode	Not Configured
SIP Re-Routing Mode	Standard

SBC Parameters	
Classify By Proxy Set	Enable
Max Number Of Registered Users	-1
Inbound Message Manipulation Set	-1
Outbound Message Manipulation Set	3
Registration Mode	User initiates registrations
Authentication Mode	User authenticates
Authentication Method List	
Enable SBC Client Forking	No

5. Define IP Group #7 for Remote Agents in the AT&T network as follows:
 - a. IP Group Index '7'
 - b. Type: 'USER' (represents a group of users (such as IP phones and softphones) where their location is dynamically obtained by the device when REGISTER requests and responses traverse (or are terminated) by the device. These users are considered remote (far-end) users.
 - c. Description: arbitrary name. (e.g., 'ATT Remote Agents')
 - d. Proxy Set ID: N/A (only applies to Type 'SERVER').
 - e. SIP Group Name: N/A - the SIP Request-URI host name used in INVITE and REGISTER messages sent to the IP Group, or the host name in the From header of INVITE messages received from the IP Group. If not specified, the value of the global parameter 'Proxy Name' (configured in 'Proxy and Registration Parameters') is used instead.
 - f. SRD: '1' – the SRD associated with this group of IP phones.
 - g. Media Realm: 'ATTDMMZ_MR' - Assigns Media Realm to the IP Group. Must be identical to the Media Realm name in the Media Realm table.
 - h. IP Profile ID: '0' (default)
 - i. Classify By Proxy Set: 'Disable'. This parameter is only applicable to Server type IP Groups. Since the IP Phone will receive its IP addresses from a DHCP server, Users will be classified by the Classification table which allows the use of a range of IP address to represent the phones. SIP messages originating from that range of IP addresses are classified to an IP group, which is then used in IP2IP routing.

- j. Outbound Message Manipulation Set: '-1' (default) No manipulations are required to the Remote Agents

Figure 5-21: AT&T Remote Agents IP Group 7

Index		7
Common Parameters		
Type	USER	
Description	ATT Remote Agents	
Proxy Set ID		
SIP Group Name		
Contact User	N/A	
Domain Name in Contact		
SRD	1	
Media Realm	ATDMZ_MR	
IP Profile ID	0	
Gateway Parameters		
Always Use Route Table	No	
Routing Mode	Not Configured	
SIP Re-Routing Mode	Standard	
SBC Parameters		
Classify By Proxy Set	Disable	
Max Number Of Registered Users	-1	
Inbound Message Manipulation Set	-1	
Outbound Message Manipulation Set	-1	
Registration Mode	User initiates registrations	
Authentication Mode	User authenticates	
Authentication Method List		
Enable SBC Client Forking	No	

6. Define IP Group #8 for Remote Agents in the non-AT&T network as follows:
 - a. IP Group Index '8'
 - b. Type: 'USER' (represents a group of users (such as IP phones and softphones) where their location is dynamically obtained by the device when REGISTER requests and responses traverse (or are terminated) by the device. These users are considered remote (far-end) users.
 - c. Description: arbitrary name. (e.g., 'TWC Remote Agents')
 - d. Proxy Set ID: N/A (only applies to Type 'SERVER').
 - e. SIP Group Name: N/A - the SIP Request-URI host name used in INVITE and REGISTER messages sent to the IP Group, or the host name in the From header of INVITE messages received from the IP Group. If not specified, the value of the global parameter 'Proxy Name' (configured in 'Proxy and Registration Parameters') is used instead.
 - f. SRD: '5' – the SRD associated with this group of IP phones
 - g. Media Realm: 'TWCDMZ_MR' - Assigns Media Realm to the IP Group. Must be identical to the Media Realm name in the Media Realm table.
 - h. IP Profile ID: '0' (default)
 - i. Classify By Proxy Set: 'Disable'. This parameter is only applicable to Server type IP Groups. Since the IP Phone will receive its IP addresses from a DHCP server, Users will be classified by the Classification table which allows the use of a range of IP address to represent the phones. SIP messages originating from that range of IP addresses are classified to an IP group, which is then used in IP2IP routing.
 - j. Outbound Message Manipulation Set: '-1' (default) No manipulations are required to the Remote Agents

Figure 5-22: Non-AT&T Remote Agents IP Group 8

Index	8
Common Parameters	
Type	USER
Description	TWC Remote Agents
Proxy Set ID	
SIP Group Name	
Contact User	N/A
Domain Name in Contact	
SRD	5
Media Realm	TWCDMZ_MR
IP Profile ID	0
Gateway Parameters	
Always Use Route Table	No
Routing Mode	Not Configured
SIP Re-Routing Mode	Standard
SBC Parameters	
Classify By Proxy Set	Disable
Max Number Of Registered Users	-1
Inbound Message Manipulation Set	-1
Outbound Message Manipulation Set	-1
Registration Mode	User initiates registrations
Authentication Mode	User authenticates
Authentication Method List	
Enable SBC Client Forking	No

7. For the simulation of end customers in the certification environment, IP Group #5 for Customers in the AT&T network was created as follows below. **This information is provided for reference only. This IP Group would not be used in a production environment.** In a production environment, the Genesys would handle Agent phone registrations and even in that case, there would be no end customer registrations.
 - a. IP Group Index '5'
 - b. Type: 'USER' (represents a group of users (such as IP phones and softphones) where their location is dynamically obtained by the device when REGISTER requests and responses traverse (or are terminated) by the device. These users are considered remote (far-end) users.
 - c. Description: arbitrary name. (e.g., 'ATT Phone')
 - d. Proxy Set ID: N/A (only applies to Type 'SERVER').
 - e. SIP Group Name: N/A - the SIP Request-URI host name used in INVITE and REGISTER messages sent to the IP Group, or the host name in the From header of INVITE messages received from the IP Group. If not specified, the value of the global parameter 'Proxy Name' (configured in 'Proxy and Registration Parameters') is used instead.
 - f. SRD: '1' – the SRD associated with this group of IP phones.
 - g. Media Realm: 'ATTDZ_MR' - Assigns Media Realm to the IP Group. This parameter is case sensitive and must be identical to the Media Realm name in the Media Realm table.
 - h. Registration Mode: 'SBC authenticates (as server)'. The device will authenticate as a server using a User Information File.
 - i. Authentication Method: 'REGISTER'. This defines the SIP methods that the device must challenge.

Figure 5-23: AT&T Customer IP Group 5 (Lab Only)

Index		5
Common Parameters		
Type	USER	
Description	ATT Phone	
Proxy Set ID		
SIP Group Name		
Contact User	N/A	
Domain Name in Contact		
SRD	1	
Media Realm	ATTDMZ_MR	
IP Profile ID	0	
Gateway Parameters		
Always Use Route Table	No	
Routing Mode	Not Configured	
SIP Re-Routing Mode	Standard	
SBC Parameters		
Classify By Proxy Set	Disable	
Max Number Of Registered Users	-1	
Inbound Message Manipulation Set	-1	
Outbound Message Manipulation Set	-1	
Registration Mode	User initiates registrations	
Authentication Mode	SBC authenticates (as server)	
Authentication Method List	REGISTER	
Enable SBC Client Forking	No	

- a. To simulate end customers in the certification environment, IP Group #6 for Customers in a non AT&T network was created as described below. **This information is provided for reference only. This IP Group would not be used in a production environment.** In a production environment, Genesys would handle Agent phone registrations and even in that case there would be no end customer registrations.
- b. IP Group Index '6'
- c. Type: 'USER' (represents a group of users (such as IP phones and softphones) where their location is dynamically obtained by the device when REGISTER requests and responses traverse (or are terminated) by the device. These users are considered remote (far-end) users.
- d. Description: Arbitrary name. (e.g., 'TWC Users')
- e. Proxy Set ID: N/A (only applies to Type 'SERVER').
- f. SIP Group Name: N/A - the SIP Request-URI host name used in INVITE and REGISTER messages sent to the IP Group, or the host name in the From header of INVITE messages received from the IP Group. If not specified, the value of the global parameter 'Proxy Name' (configured in 'Proxy and Registration Parameters') is used instead.
- g. SRD: '5' – the SRD associated with this group of IP phones.
- h. Media Realm: 'TWCMDZ_MR' - Assigns Media Realm to the IP Group. Must be identical to the Media Realm name in the Media Realm table.
- i. IP Profile ID: '0' (default)
- j. Registration Mode: 'SBC authenticates (as server)'. The device will authenticate as a server using a User Information File.
- k. Authentication Method: 'REGISTER'. This defines the SIP methods that the device must challenge.

Figure 5-24: Non-AT&T Customers IP Group 6 (Lab only)

▼	
Index	6
▼ Common Parameters	
Type	USER
Description	TWC USERS
Proxy Set ID	
SIP Group Name	
Contact User	N/A
Domain Name in Contact	
SRD	5
Media Realm	TWCDMZ_MR
IP Profile ID	0
▼ Gateway Parameters	
Always Use Route Table	No
Routing Mode	Not Configured
SIP Re-Routing Mode	Standard
▼ SBC Parameters	
Classify By Proxy Set	Disable
Max Number Of Registered Users	-1
Inbound Message Manipulation Set	-1
Outbound Message Manipulation Set	-1
Registration Mode	User initiates registrations
Authentication Mode	SBC authenticates (as server)
Authentication Method List	REGISTER
Enable SBC Client Forking	No

5.1.10 Configure the Proxy Sets

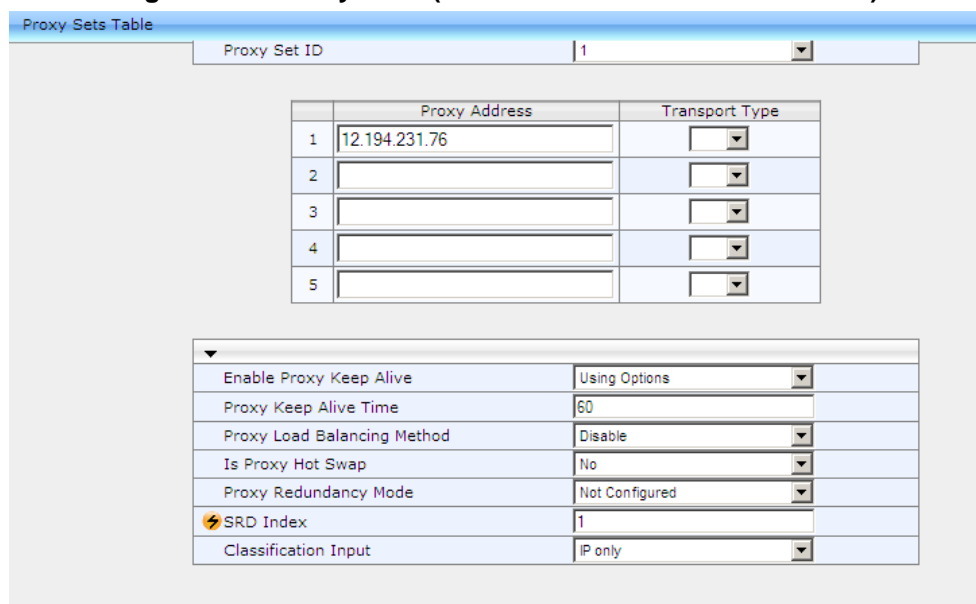
The Proxy Sets Table allows for the configuration of a Proxy set, or group of Proxy servers defined by IP address or Fully Qualified Domain Name (FQDN). Up to 32 Proxy Sets, each with a unique ID number and up to 5 Proxy Server addresses can be defined. A transport type of UDP, TCP, or TLS can be defined for each Proxy Set. Proxy load balancing and redundancy mechanisms can be applied per Proxy Set (if a Proxy Set contains more than one Proxy address).

Proxy Sets can be assigned to IP Groups of type SERVER. When the device sends an INVITE message to an IP Group, the message is sent to the IP address or domain name defined in the Proxy Set that is associated with the IP Group. The Proxy Set represents the destination of the call. Typically, for IP-to-IP call routing, at least two Proxy Sets are defined for the call destination – one for each leg (IP Group) of the call (i.e., both directions). For example, one Proxy Set for the Internet Telephony Service Provider (ITSP) interfacing with one interface of the device and another Proxy Set for the second SIP entity (e.g., IP PBX) interfacing with the other interface of the device.

➤ To configure Proxy Sets:

1. Open the Proxy Sets Table page (**Configuration > VoIP > Control Network > Proxy Sets Table**).
2. From the 'Proxy Set ID' drop-down list, select an ID for the desired group. Start with Proxy Set ID 1. For this configuration, Proxy Set ID 1 will correspond to the primary AT&T IP Flexible Reach SIP trunk. Proxy Set 2 will correspond to the secondary AT&T IP Flexible Reach SIP trunk.
3. Configure the Proxy parameters accordingly, as shown below. Note that the keep alive is set to 'use OPTIONS' and Proxy redundancy mode is set to 'Homing'. See the Mediant 3000 User Manual for parameter descriptions.

Figure 5-25: Proxy Set 1 (AT&T IP Flexible Reach SIP Trunk)



Proxy Sets Table

Proxy Set ID: 1

	Proxy Address	Transport Type
1	12.194.231.76	
2		
3		
4		
5		

☐ Enable Proxy Keep Alive: Using Options
 Proxy Keep Alive Time: 60
 Proxy Load Balancing Method: Disable
 Is Proxy Hot Swap: No
 Proxy Redundancy Mode: Not Configured
 SRD Index: 1
 Classification Input: IP only

4. Click **Submit** to apply the changes.
5. From the 'Proxy Set ID' drop-down list, select Proxy Set ID 2. For this configuration, Proxy Set 2 will correspond to the AT&T IP Flexible Reach secondary SIP Trunk.
6. Configure the Proxy parameters accordingly, as shown below. See the Mediant 3000 User Manual for parameter descriptions.

Figure 5-26: Proxy Set 2 (AT&T IP Flexible Reach SIP Trunk - Secondary)

Proxy Sets Table

Proxy Set ID: 2

	Proxy Address	Transport Type
1	12.194.230.7	
2		
3		
4		
5		

Enable Proxy Keep Alive	Using Options
Proxy Keep Alive Time	60
Proxy Load Balancing Method	Disable
Is Proxy Hot Swap	No
Proxy Redundancy Mode	Not Configured
SRD Index	1
Classification Input	IP only

7. From the 'Proxy Set ID' drop-down list, select an ID for Proxy Set ID 3. For this configuration, Proxy Set 3 will correspond to the Genesys SIP Server.
8. Configure the Proxy parameters accordingly, as shown below. See the Mediant 3000 User Manual for parameter descriptions.

Figure 5-27: Proxy Set 3 (Genesys SIP Server Trunk)

Proxy Sets Table

Proxy Set ID: 3

	Proxy Address	Transport Type
1	rtpsip.cl.gchariot.com	UDP
2		
3		
4		
5		

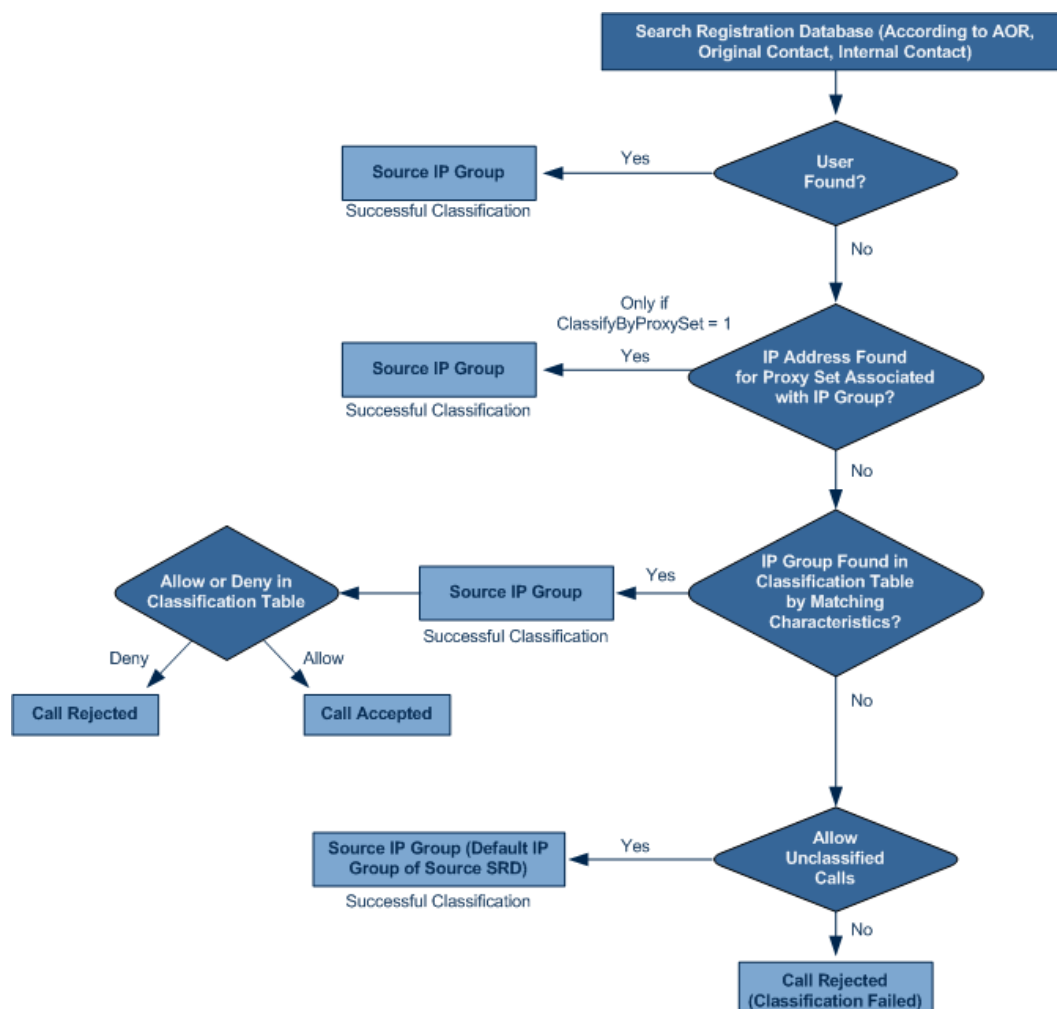
Enable Proxy Keep Alive	Using Options
Proxy Keep Alive Time	60
Proxy Load Balancing Method	Disable
Is Proxy Hot Swap	No
Proxy Redundancy Mode	Not Configured
SRD Index	3
Classification Input	IP only

9. Click **Submit** to apply the changes.

5.1.11 Define the Classification Rules

Classification rules are used to classify incoming SIP dialog-initiating requests (e.g., SIP INVITE messages) to source IP Groups where the SIP dialog request originated, which is later used in manipulation and routing processes. Classification rules also enhance security through SIP access whitelists and blacklists. The Classification table is used to classify the incoming SIP dialog request only if classification based on the device's registration database and Proxy Set fails. The figure below outlines the Classification process. See the Mediant 3000 SIP User's Manual for further information on the classification process.

Figure 5-28: Classification Process Overview



➤ **To define Classification Rules:**

1. Open the Classification Table page (**Configuration > VoIP > SBC > Routing SBC > Classification Table**).
2. Click the **Add** button; the following appears:

Figure 5-29: Classification Table ... Add Record Page

Add Record	
Index	<input type="text"/>
Source SRD ID	None
Source IP Address	<input type="text"/>
Source Port	0
Source Transport Type	<input type="text"/>
Source Username Prefix	*
Source Host Prefix	*
Destination Username Prefix	*
Destination Host Prefix	*
Message Condition	None
Source IP Group ID	None
Action Type	Allow
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

- Configure the classification rules as shown below. Apply the changes and save to flash.

Figure 5-30: Classification Table Rule #2

Classification Table								
Add	Edit	Delete	View/Unview					
Index	Source SRD ID	Source IP Address	Source Port	Source Transport Type	Source Username Prefix	Destination Username Prefix	Source IP Group ID	Action Type
2	5	173.227.254.*	0		202756282[8-9]	*	8	Allow
3	5	173.227.254.*	0		919294363[7-8]	*	8	Allow
4	5	173.227.254.*	0		2027562830	*	6	Allow
5	1	12.210.214.*	0		2027562827	*	5	Allow
6	1	12.210.214.*	0		202756282[8-9]	*	8	Allow
7	1	12.210.214.*	0		9192943635	*	7	Allow

Page 1 of 1 10 View 1 - 6 of 6

Details of Classification Table #2

Source SRD ID = 5	Source IP Address = 173.227.254.*
Source Port = 0	Source Transport Type =
Source Username Prefix = 202756282[8-9]	Source Host Prefix = *
Destination Username Prefix = *	Destination Host Prefix = *
Message Condition = None	Source IP Group ID = 8
Action Type = Allow	

Figure 5-31: Classification Table Rule #3

Classification Table								
Add	Edit	Delete	View/Unview					
Index	Source SRD ID	Source IP Address	Source Port	Source Transport Type	Source Username Prefix	Destination Username Prefix	Source IP Group ID	Action Type
2	5	173.227.254.*	0		202756282[8-9]*		8	Allow
3	5	173.227.254.*	0		919294363[7-8]*		8	Allow
4	5	173.227.254.*	0		2027562830	*	6	Allow
5	1	12.210.214.*	0		2027562827	*	5	Allow
6	1	12.210.214.*	0		202756282[8-9]*		8	Allow
7	1	12.210.214.*	0		9192943635	*	7	Allow

Page 1 of 1 View 1 - 6 of 6

Details of Classification Table #3

Source SRD ID = 5
Source Port = 0
Source Username Prefix = 919294363[7-8]
Destination Username Prefix = *
Message Condition = None
Action Type = Allow

Source IP Address = 173.227.254.*
Source Transport Type =
Source Host Prefix = *
Destination Host Prefix = *
Source IP Group ID = 8

Figure 5-32: Classification Rule #4

Classification Table								
Add	Edit	Delete	View/Unview					
Index	Source SRD ID	Source IP Address	Source Port	Source Transport Type	Source Username Prefix	Destination Username Prefix	Source IP Group ID	Action Type
2	5	173.227.254.*	0		202756282[8-9]*		8	Allow
3	5	173.227.254.*	0		919294363[7-8]*		8	Allow
4	5	173.227.254.*	0		2027562830	*	6	Allow
5	1	12.210.214.*	0		2027562827	*	5	Allow
6	1	12.210.214.*	0		202756282[8-9]*		8	Allow
7	1	12.210.214.*	0		9192943635	*	7	Allow

Page 1 of 1 View 1 - 6 of 6

Details of Classification Table #4

Source SRD ID = 5
Source Port = 0
Source Username Prefix = 2027562830
Destination Username Prefix = *
Message Condition = None
Action Type = Allow

Source IP Address = 173.227.254.*
Source Transport Type =
Source Host Prefix = *
Destination Host Prefix = *
Source IP Group ID = 6

Figure 5-33: Classification Rule #5

Classification Table									
Add	Edit	Delete	View/Unview						
Index	Source SRD ID	Source IP Address	Source Port	Source Transport Type	Source Username Prefix	Destination Username Prefix	Source IP Group ID	Action Type	
2	5	173.227.254.*	0		202756282[8-9]*		8	Allow	
3	5	173.227.254.*	0		919294363[7-8]*		8	Allow	
4	5	173.227.254.*	0		2027562830	*	6	Allow	
5	1	12.210.214.*	0		2027562827	*	5	Allow	
6	1	12.210.214.*	0		202756282[8-9]*		8	Allow	
7	1	12.210.214.*	0		9192943635	*	7	Allow	

Page 1 of 1 View 1 - 6 of 6

Details of Classification Table #5

Source SRD ID = 1
 Source Port = 0
 Source Username Prefix = 202756287
 Destination Username Prefix = *
 Message Condition = None
 Action Type = Allow

Source IP Address = 12.210.214.*
 Source Transport Type =
 Source Host Prefix = *
 Destination Host Prefix = *
 Source IP Group ID = 5

Figure 5-34: Classification Rule #6

Classification Table									
Add	Edit	Delete	View/Unview						
Index	Source SRD ID	Source IP Address	Source Port	Source Transport Type	Source Username Prefix	Destination Username Prefix	Source IP Group ID	Action Type	
2	5	173.227.254.*	0		202756282[8-9]*		8	Allow	
3	5	173.227.254.*	0		919294363[7-8]*		8	Allow	
4	5	173.227.254.*	0		2027562830	*	6	Allow	
5	1	12.210.214.*	0		2027562827	*	5	Allow	
6	1	12.210.214.*	0		202756282[8-9]*		8	Allow	
7	1	12.210.214.*	0		9192943635	*	7	Allow	

Page 1 of 1 View 1 - 6 of 6

Details of Classification Table #6

Source SRD ID = 1
 Source Port = 0
 Source Username Prefix = 202756282[8-9]
 Destination Username Prefix = *
 Message Condition = None
 Action Type = Allow

Source IP Address = 12.210.214.*
 Source Transport Type =
 Source Host Prefix = *
 Destination Host Prefix = *
 Source IP Group ID = 8

Figure 5-35: Classification Rule #7

Classification Table									
Add	Edit	Delete	View/Unview						
Index	Source SRD ID	Source IP Address	Source Port	Source Transport Type	Source Username Prefix	Destination Username Prefix	Source IP Group ID	Action Type	
2	5	173.227.254.*	0		202756282[8-9]*		8	Allow	
3	5	173.227.254.*	0		919294363[7-8]*		8	Allow	
4	5	173.227.254.*	0		2027562830	*	6	Allow	
5	1	12.210.214.*	0		2027562827	*	5	Allow	
6	1	12.210.214.*	0		202756282[8-9]*		8	Allow	
7	1	12.210.214.*	0		9192943635	*	7	Allow	

Page 1 of 1 View 1 - 6 of 6

Details of Classification Table #7

Source SRD ID = 1
 Source Port = 0
 Source Username Prefix = 9192943635
 Destination Username Prefix = *
 Message Condition = None
 Action Type = Allow

Source IP Address = 12.210.214.*
 Source Transport Type =
 Source Host Prefix = *
 Destination Host Prefix = *
 Source IP Group ID = 7

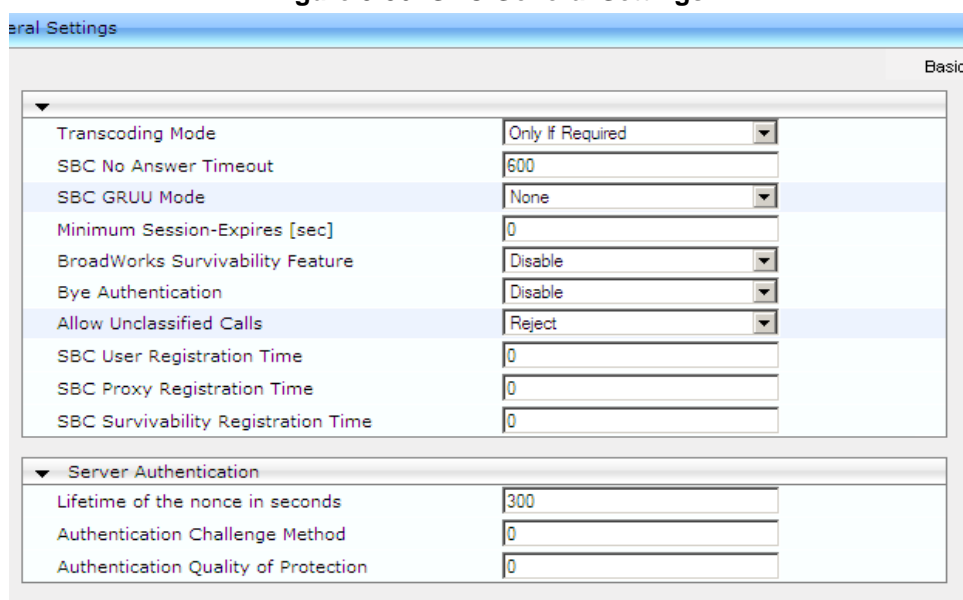
5.1.12 Configure SBC General Settings

The General Settings page is used for the configuration of general SBC parameters.

➤ **To configure SBC General Settings rules:**

1. Open the General Settings page (**Configuration > VoIP > SBC > General Settings**).
2. Change the parameter 'Allow Unclassified Calls' to 'Reject'. When set to 'reject', calls (incoming packets) that cannot be classified (i.e., classification process fails) into a Source IP Group (in the Classification table), will be rejected. If this parameter is left at 'Allow' (default), when a classification failure occurs the incoming packet is assigned to the default IP Group of the default SRD (and the call is subsequently processed).

Figure 5-36: SBC General Settings



General Settings	
Basic	
Transcoding Mode	Only if Required
SBC No Answer Timeout	600
SBC GRUU Mode	None
Minimum Session-Expires [sec]	0
BroadWorks Survivability Feature	Disable
Bye Authentication	Disable
Allow Unclassified Calls	Reject
SBC User Registration Time	0
SBC Proxy Registration Time	0
SBC Survivability Registration Time	0
Server Authentication	
Lifetime of the nonce in seconds	300
Authentication Challenge Method	0
Authentication Quality of Protection	0

3. Click the **Submit** to apply the changes.
4. Save the changes to flash memory.

5.1.13 Configure SBC Admission Control

This Admission Control table is used to enforce a configured limitation for the incoming call that is applied immediately after the Classification Process. If the call/request is rejected at this state, no routing is performed. This table allows the definitions of up to 100 rules for limiting the number of concurrent calls (SIP dialogs). These call limits can be applied per SRD, IP Group, SIP request type (e.g., INVITEs), SIP dialog direction (e.g., inbound), and/or per user (identified by its registered contact). This feature can be useful for implementing Service Level Agreements (SLA) policies. See the Mediant 3000 SIP User's manual for more information on configuring Admission Control parameters.

➤ **To configure SBC Admission Control rules:**

1. Open the General Settings table (**Configuration > VoIP > SBC > Admission Control**).
2. Add an entry and configure the parameters as required:

Figure 5-37: SBC Admission Control Table

Index	Limit Type	IP Group ID	SRD ID	Request Type	Request Direction	Limit	Limit Per User	Rate	MaxBurst
1	IP Group	-1	-1	INVITE	Inbound	1	50	0	0

3. Click the **Apply** to save the changes.
4. Save the changes to flash memory.

5.1.14 Configure Allowed Coders Group

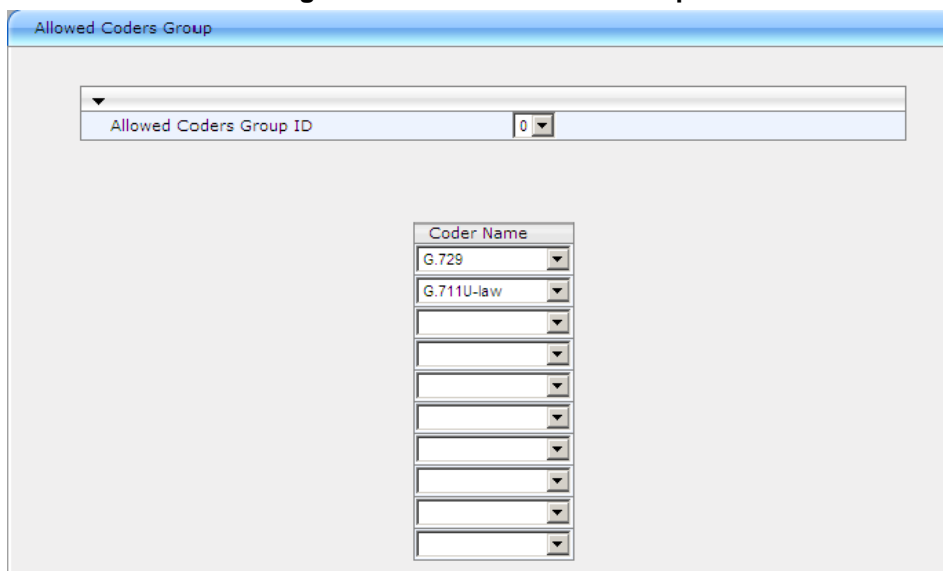
The Allowed Coders Group page allows up to five Allowed Coder Groups, each with up to 10 coders. Allowed Coder Groups determine the codes that can be used for a specific SBC leg. The device's SBC application can therefore enforce the use of specific coders while preventing the use of other coders. Coders excluded from the Allowed Coders Group are removed from the SDP offer. Only common coders between SDP offered coders and coders configured in the Allowed Coder Groups are used. Coder Priority is determined by order of appearance, with the first coder given highest priority.

For more information regarding the Allowed Coders Group, see the Mediant 3000 SIP User's Manual.

➤ **To configure Allowed Coder Groups:**

1. Open the General Settings table (**Configuration > VoIP > SBC > Allowed Coders Group**).
2. From the 'Allowed Coders Group ID' drop-down list, select an ID for the Allowed Coder Group
3. In the Coder Name table, select coders for the Allowed Coder Group. For the AT&T IP Flexible Reach solution, the required coders were G.729 & G711 U-law in this order. The Allowed Coders Group ID is associated with an IP Profile (a SIP profile for IP calls), configured in the next section. Since both the AT&T IP Flexible Reach network & the Genesys Call Center network will both use the same Coder preferences, only one Allowed Coders Group ID needs to be created.

Figure 5-38: Allow Coders Group



Allowed Coders Group	
Allowed Coders Group ID	0
Coder Name	
G.729	
G.711U-law	

4. Click the **Submit** to apply the changes.
5. Save the changes to flash memory.

5.1.15 Configure IP Profiles

The IP Profile Setting page allows up to nine SIP profiles for IP calls (referred to as an IP Profile) to be defined. Each IP Profile contains a set of parameters for configuring various behaviors, for example, used coder, echo canceller support, and jitter buffer. Different IP Profiles can be assigned to specific inbound and outbound calls.

For more information on IP Profiles, see the Mediant 3000 SIP User's Manual.

➤ **To configure IP Profiles:**

1. Open the General Settings table (**Configuration > VoIP > Coders And Profiles > IP Profile Settings**).
2. From the 'Profile ID' drop-down list, select the IP Profile index.
3. In the 'Profile Name' field, enter an arbitrary name that allows you to easily identify the IP Profile.
4. Select the priority of the IP Profile ('1' is the lowest priority)
5. Assign the Coder Group to the IP Profile.
6. Click **Submit** to apply the changes.
7. Save the changes to flash memory.

Figure 5-39: AT&T IP Flexible Reach Profile

Profile ID	1
Profile Name	ATT IP Flex

Common Parameters	
RTP IP DiffServ	46
Signaling DiffServ	40
Disconnect on Broken Connection	Yes
Media IP Version Preference	Only IPv4
Dynamic Jitter Buffer Minimum Delay [msec](*)	10
Dynamic Jitter Buffer Optimization Factor(*)	10
RTP Redundancy Depth(*)	0
Echo Canceled(*)	Enable
Input Gain (-32 to 31 dB)(*)	0
Voice Volume (-32 to 31 dB)(*)	0

Gateway Parameters	
Fax Signaling Method	No Fax
Play Ringback Tone to IP	Don't Play
Enable Early Media	Enable
Copy Destination Number to Redirect Number	Disable
Media Security Behavior	Preferable
CNG Detector Mode	Disable
Modems Transport Type	Enable Bypass
NSE Mode	Disable
Number of Calls Limit	-1
Progress Indicator to IP	Not Configured
Profile Preference	1
Coder Group	Default Coder Group
Remote RTP Base UDP Port	0
First Tx DTMF Option	RFC 2833
Second Tx DTMF Option	
Declare RFC 2833 in SDP	Yes
Add IE In SETUP	
AMD Sensitivity Parameter Suit	0
AMD Sensitivity Level	8
AMD Max Greeting Time	300
AMD Max Post Silence Greeting Time	400
Enable QSIG Tunneling	Disable
Enable Hold	Enable

SBC	
Transcoding Mode	Only if Required
Extension Coders Group ID	None
Allowed Coders Group ID	Coders Group 0
Allowed Coders Mode	Restriction and Preference
SBC Preferences Mode	Doesn't Include Extensions
Diversion Mode	Not Configured
History Info Mode	Not Configured
Media Security Behavior	As Is
RFC 2833 Behavior	As Is
Alternative DTMF Method	Don't Care
P-Assert Identity	Not Configured
SBC Fax Coders Group ID	None
SBC Fax Behavior	0
SBC Fax Offer Mode	0
SBC Fax Answer Mode	1

5.1.16 Configure SBC IP-to-IP Routing Setup

The IP2IP Routing Table enables configuring up to 120 SBC IP-to-IP routing rules. This table provides enhanced IP-to-IP call routing capabilities for routing received SIP dialog messages (e.g., INVITE) to a destination IP address. The SIP message is routed according to a routing rule in which configured input characteristics (such as the Source IP Group) match the incoming SIP message. If the characteristics of an incoming call do not match the first rule, the call characteristics are then compared to those of the second rule, and so on, until a matching rule is located. If no rule is matched, the call is rejected. For more information about IP-to-IP routing rules configuration, see the Mediant 3000 SIP User's Manual. Rows that are not applicable to a production environment are explained to facilitate understanding of routing rules and the potential use of the table.

➤ **To configure SBC IP-to-IP routing rules:**

1. Open the IP2IP Routing Table (**Configuration > VoIP > SBC > Routing SBC > IP to IP Routing Table**).
2. Click the **Add** button; the Add Record dialog box appears:
3. Add an entry per the examples below. Note that the configurations in the screenshots shown below are from the certification environment and are shown only as an example of how to achieve IP2IP routing.
4. Click the **Apply** button after each and remember to save the changes to flash memory.

Figure 5-40: IP2IP Routing Table

IP2IP Routing Table										
Add										
Index	Source IP Group ID	Destination Username Prefix	Destination Host	Request Type	Destination Type	Destination IP Group ID	Destination SRD ID	Destination Address	Destination Port	Alternative Route Options
1	5	*	*	REGISTER	IP Group	5	None		0	Route Row
3	7	*	*	All	IP Group	3	3		0	Route Row
4	8	*	*	All	IP Group	3	3		0	Route Row
5	6	*	*	REGISTER	IP Group	6	None		0	Route Row
6	1	919294	*	All	IP Group	3	3		0	Route Row
7	2	919294	*	All	IP Group	3	3		0	Alt Route Ignored
8	3	9192943635	*	All	IP Group	7	1		0	Route Row
9	3	919294363[7-8]	*	All	IP Group	8	5		0	Route Row
10	1	202756282[5-6]	*	All	IP Group	3	3		0	Route Row
11	2	202756282[5-6]	*	All	IP Group	3	3		0	Alt Route Ignored
12	1	2027562827	*	All	IP Group	5	1		0	Route Row
13	2	2027562827	*	All	IP Group	5	1		0	Alt Route Ignored
14	1	202756282[8-9]	*	All	IP Group	8	5		0	Route Row
15	2	202756282[8-9]	*	All	IP Group	8	5		0	Alt Route Ignored
16	1	2027562830	*	All	IP Group	6	5		0	Route Row
17	2	2027562830	*	All	IP Group	6	5		0	Alt Route Ignored
18	5	2027562830	*	All	IP Group	6	5		0	Route Row
19	5	91929436[00-39]	*	All	IP Group	3	3		0	Route Row
20	6	919294	*	All	IP Group	3	3		0	Route Row
21	8	919294	*	All	IP Group	3	3		0	Route Row
22	5	9192873[450-515]	*	All	IP Group	1	1		0	Route Row
23	5	9192873[450-515]	*	All	IP Group	2	1		0	Alt Route Ignored
24	5	01141583330158	*	All	IP Group	1	1		0	Route Row
25	5	01141583330158	*	All	IP Group	2	1		0	Alt Route Ignored
27	3	*	*	All	IP Group	1	1		0	Route Row
28	3	*	*	All	IP Group	2	1		0	Alt Route Ignored
29	5	18888064788	*	All	IP Group	1	1		0	Route Row
30	5	18888064788	*	All	IP Group	2	1		0	Alt Route Ignored
31	6	18888064788	*	All	IP Group	1	1		0	Route Row
32	6	18888064788	*	All	IP Group	2	1		0	Alt Route Ignored

For clarity, the figure below shows the resultant configuration stored on the device that aligns with the screenshots shown above.

Figure 5-41: IP to IP Routing Table from Configuration File

[IP2IPRouting]

Index	Src IP Group ID	Dest Username Prefix	Request Type	Dest Type	Dest IP Group ID	Dest SRDID	Dest Port	Dest Transport Type	Alt Route Options
1	5	*	2 (REGISTER)	0 (IP Group)	5		0	-1 ()	0 (Route Row)
3	7	*	0 (All)	0 (IP Group)	3	3	0	-1 ()	0 (Route Row)
4	8	*	0 (All)	0 (IP Group)	3	3	0	-1 ()	0 (Route Row)
5	6	*	2 (REGISTER)	0 (IP Group)	6		0	-1 ()	0 (Route Row)
6	1	919294	0 (All)	0 (IP Group)	3	3	0	-1 ()	0 (Route Row)
7	2	919294	0 (All)	0 (IP Group)	3	3	0	-1 ()	1 (Alt Route Ignore Inputs)
8	3	9192943635	0 (All)	0 (IP Group)	7	1	0	-1 ()	0 (Route Row)
9	3	919294363[7-8]	0 (All)	0 (IP Group)	8	5	0	-1 ()	0 (Route Row)
10	1	202756282[5-6]	0 (All)	0 (IP Group)	3	3	0	-1 ()	0 (Route Row)
11	2	202756282[5-6]	0 (All)	0 (IP Group)	3	3	0	-1 ()	1 (Alt Route Ignore Inputs)
12	1	2027562827	0 (All)	0 (IP Group)	5	1	0	-1 ()	0 (Route Row)
13	2	2027562827	0 (All)	0 (IP Group)	5	1	0	-1 ()	1 (Alt Route Ignore Inputs)
14	1	202756282[8-9]	0 (All)	0 (IP Group)	8	5	0	-1 ()	0 (Route Row)
15	2	202756282[8-9]	0 (All)	0 (IP Group)	8	5	0	-1 ()	1 (Alt Route Ignore Inputs)
16	1	2027562830	0 (All)	0 (IP Group)	6	5	0	-1 ()	0 (Route Row)
17	2	2027562830	0 (All)	0 (IP Group)	6	5	0	-1 ()	1 (Alt Route Ignore Inputs)
18	5	2027562830	0 (All)	0 (IP Group)	6	5	0	-1 ()	0 (Route Row)
19	5	91929436[00-39]	0 (All)	0 (IP Group)	3	3	0	-1 ()	0 (Route Row)
20	6	919294	0 (All)	0 (IP Group)	3	3	0	-1 ()	0 (Route Row)
21	8	919294	0 (All)	0 (IP Group)	3	3	0	-1 ()	0 (Route Row)
22	5	9192873[450-515]	0 (All)	0 (IP Group)	1	1	0	-1 ()	0 (Route Row)
23	5	9192873[450-515]	0 (All)	0 (IP Group)	2	1	0	-1 ()	1 (Alt Route Ignore)

									Inputs)
24	5	01141583330158	0 (All)	0 (IP Group)	1	1	0	-1 ()	0 (Route Row)
25	5	01141583330158	0 (All)	0 (IP Group)	2	1	0	-1 ()	1 (Alt Route Ignore Inputs)
27	3	*	0 (All)	0 (IP Group)	1	1	0	-1 ()	0 (Route Row)
28	3	*	0 (All)	0 (IP Group)	2	1	0	-1 ()	1 (Alt Route Ignore Inputs)
29	5	18888064788	0 (All)	0 (IP Group)	1	1	0	-1 ()	0 (Route Row)
30	5	18888064788	0 (All)	0 (IP Group)	2	1	0	-1 ()	1 (Alt Route Ignore Inputs)
31	6	18888064788	0 (All)	0 (IP Group)	1	1	0	-1 ()	0 (Route Row)
32	6	18888064788	0 (All)	0 (IP Group)	2	1	0	-1 ()	1 (Alt Route Ignore Inputs)

The configuration shown above is specific to the certification environment and complicated by routes that would not typically be found in a production environment to achieve test scenarios. The main concept to understand is that Genesys is the Call Control Platform for this environment and all routing from the various IP Groups (either internally by the Call Center Agents or externally over the SIP trunk) will route to the IP Group associated with the Genesys SIP Server. In this example, in the case of a remote agent in the AT&T network, routing would be from a customer coming in on IP Group 1 -> IP Group 3 -> IP Group 7 to the agent, or, from the remote agent at IP Group 7 -> IP Group 3 -> IP Group 1 (all calls transition through the Genesys SIP server).

In the AT&T Call Center production environment, the routing configuration would involve only IP Groups 1, 2, 3 and 7 as follows:

- Calls originating from IP Group 1 (AT&T IP Flexible Reach) or IP Group 2 (in the case of the AT&T IP Flexible Reach alternate SIP Trunk) would route to IP Group 3 (Genesys)
- Alternate Route rows are marked as such and the inputs are ignored as the previous row condition is met, but there would be no route to the primary SIP Server of AT&T.
- Calls originating from IP Group 3 (Genesys) could route to IP Group 1 (AT&T IP Flexible Reach), IP Group 2 (in the case of the AT&T IP Flexible Reach alternate SIP Trunk) or IP Group 7 (Remote Agents on IP Flexible Reach), depending on the destination number dialed.
- Calls originating from IP Groups 7 (Remote Agents on IP Flexible Reach) would route to IP Group 3 (Genesys).

Groups 5 and 6 are groups created to simulate end customers in the laboratory environment, so in production there's no need for these 'Customer' groups. Group 8 represents a non-AT&T network interface and was used for laboratory troubleshooting purposes.

5.1.16.1 IP-to-IP Routing Row Details

The routing rows of the test environment are discussed below to understand the certification setup and identify of those rows applicable to the AT&T IP Flexible Reach Call Center production environment.

1. **Index #1** specifies that all REGISTERS incoming on IP Group 5 (the AT&T network) will have response sent out on IP Group 5 (the same network). The originators of these REGISTERS represent customers in a production environment. These users have a termination on the device for routing only and are defined in the device's User Info file. For the certification environment, where blocks of DN's were assigned by AT&T for use in testing, this consisted of DN 2027562827. This configuration would not be necessary in a production environment as customer phones will not REGISTER to the device.

Details of IP2IP Routing Table #1

Source IP Group ID = 5	Source Username Prefix = *
Source Host = *	Destination Username Prefix = *
Destination Host = *	Request Type = REGISTER
Message Condition = None	Destination Type = IP Group
Destination IP Group ID = 5	Destination SRD ID = None
Destination Address =	Destination Port = 0
Destination Transport Type =	Alternative Route Options = Route Row
Cost Group = None	

2. **Index #2** was not used in the configuration, or once existed and was later deleted.
3. **Index #3** configuration specifies that all IP calls received from IP Group 7 (the AT&T network) will be routed to IP Group 3 (Genesys SIP Server). This entry is representative of a Remote Agent in the AT&T network that does not source from the IPBE and will be necessary in the production network only if such Remote Agents will exist.

Details of IP2IP Routing Table #3

Source IP Group ID = 7	Source Username Prefix = *
Source Host = *	Destination Username Prefix = *
Destination Host = *	Request Type = All
Message Condition = None	Destination Type = IP Group
Destination IP Group ID = 3	Destination SRD ID = 3
Destination Address =	Destination Port = 0
Destination Transport Type =	Alternative Route Options = Route Row
Cost Group = None	

4. **Index #4** configuration specifies that all IP calls received from IP Group 8 (a non-AT&T network) will be routed to IP Group 3. This entry is representative of a Remote Agent in a public IP/non-AT&T network. This entry will be required in the production network only if such agents exist.

Details of IP2IP Routing Table #4

Source IP Group ID = 8	Source Username Prefix = *
Source Host = *	Destination Username Prefix = *
Destination Host = *	Request Type = All
Message Condition = None	Destination Type = IP Group
Destination IP Group ID = 3	Destination SRD ID = 3
Destination Address =	Destination Port = 0
Destination Transport Type =	Alternative Route Options = Route Row
Cost Group = None	

5. **Index #5** specifies that all REGISTERS incoming on IP Group 6 (non AT&T network) will have responses sent out on IP Group 6 (the same network). The originators of these REGISTERS represent customers in a production environment. These users have a termination on the device for routing only and are defined in the device's User Info file. For the certification environment, where blocks of DN's were assigned by AT&T for use in testing, this consisted of DN 2027562830. This configuration will not be necessary in a production environment as user phones will not REGISTER to the device.

Details of IP2IP Routing Table #5

Source IP Group ID = 6	Source Username Prefix = *
Source Host = *	Destination Username Prefix = *
Destination Host = *	Request Type = REGISTER
Message Condition = None	Destination Type = IP Group
Destination IP Group ID = 6	Destination SRD ID = None
Destination Address =	Destination Port = 0
Destination Transport Type =	Alternative Route Options = Route Row
Cost Group = None	

6. **Index #6** specifies that all IP calls with destination prefix '919294' received from IP Group 1 (AT&T IP Flexible Reach network) will be routed to IP Group 3 (Genesys SIP Server). The destination number stipulation is to limit the DN's outside the range of what the Genesys SIP Server is configured to receive from being passed to the Genesys platform.

Details of IP2IP Routing Table #6

Source IP Group ID = 1	Source Username Prefix = *
Source Host = *	Destination Username Prefix = 919294
Destination Host = *	Request Type = All
Message Condition = None	Destination Type = IP Group
Destination IP Group ID = 3	Destination SRD ID = 3
Destination Address =	Destination Port = 0
Destination Transport Type =	Alternative Route Options = Route Row
Cost Group = None	

7. **Index #7** specifies that all IP calls with destination prefix '919294' received from IP Group 2 (AT&T IP Flexible Reach network secondary IPBE) will be routed to IP Group 3 (Genesys). The destination number stipulation is to limit DN's outside the range of what the Genesys SIP Server was configured to receive from being passed to the Genesys platform. Note that this is configured as an Alternate Route, meaning that this rule will apply if the previous rule applied but the original route was not reachable.

Details of IP2IP Routing Table #7

Source IP Group ID = 2	Source Username Prefix = *
Source Host = *	Destination Username Prefix = 919294
Destination Host = *	Request Type = All
Message Condition = None	Destination Type = IP Group
Destination IP Group ID = 3	Destination SRD ID = 3
Destination Address =	Destination Port = 0
Destination Transport Type =	Alternative Route Options = Alt Route Ignore Inputs
Cost Group = None	

8. **Index #8** specifies that all IP calls with destination prefix '9192943635' received from IP Group 3 (Genesys SIP Server) will route to SRD 1, IP Group 7. For the certification environment, this destination prefix is narrowly defined to one number. This entry represents calls that are destined for Remote Agents in the AT&T network that do not register through the IPBEs.

Details of IP2IP Routing Table #8

Source IP Group ID = 3	Source Username Prefix = *
Source Host = *	Destination Username Prefix = 9192943635
Destination Host = *	Request Type = All
Message Condition = None	Destination Type = IP Group
Destination IP Group ID = 7	Destination SRD ID = 1
Destination Address =	Destination Port = 0
Destination Transport Type =	Alternative Route Options = Route Row
Cost Group = None	

- 9. Index #9** specifies that all IP calls with destination prefix 9192943637 or 9192943638 received from IP Group 3 (Genesys) will route to SRD 5, IP Group 8 (non-AT&T network). For the certification environment, this destination prefix is narrowly defined. This represents calls that are destined for Remote Agents in a non-AT&T network that might be connected to the device.

Details of IP2IP Routing Table #9

Source IP Group ID = 3	Source Username Prefix = *
Source Host = *	Destination Username Prefix = 919294363[7-8]
Destination Host = *	Request Type = All
Message Condition = None	Destination Type = IP Group
Destination IP Group ID = 8	Destination SRD ID = 5
Destination Address =	Destination Port = 0
Destination Transport Type =	Alternative Route Options = Route Row
Cost Group = None	

- 10. Index #10** specifies that all IP calls with destination prefix 2027562825-2027562026 received from IP Group 1 (AT&T IP Flexible Reach) will route to SRD 3, IP Group 3 (Genesys). In the laboratory, this would represent calls destined for Virtual Telephone Numbers of Agents in the Call Center.

Details of IP2IP Routing Table #10

Source IP Group ID = 1	Source Username Prefix = *
Source Host = *	Destination Username Prefix = 202756282[5-6]
Destination Host = *	Request Type = All
Message Condition = None	Destination Type = IP Group
Destination IP Group ID = 3	Destination SRD ID = 3
Destination Address =	Destination Port = 0
Destination Transport Type =	Alternative Route Options = Route Row
Cost Group = None	

- 11. Index #11** specifies all IP calls with destination prefix 2027562825-2027562026 received from IP Group 2 (AT&T IP Flexible Reach secondary IPBE) will route to SRD 3, IP Group 3 (Genesys SIP Server). This represents calls that are destined for Virtual Telephone Numbers of Agents in the Call Center. Note that this entry is configured as an Alternate Route, meaning that this rule will apply if the previous rule applied but the original route is not reachable.

Details of IP2IP Routing Table #11

Source IP Group ID = 2	Source Username Prefix = *
Source Host = *	Destination Username Prefix = 202756282[5-6]
Destination Host = *	Request Type = All
Message Condition = None	Destination Type = IP Group
Destination IP Group ID = 3	Destination SRD ID = 3
Destination Address =	Destination Port = 0
Destination Transport Type =	Alternative Route Options = Alt Route Ignore Inputs
Cost Group = None	

- 12. Index #12** specifies that all IP calls with destination prefix 2027562827 received from IP Group 1 (AT&T IP Flexible Reach) will route to SRD 1, IP Group 5 (non-AT&T

network). This entry was used for testing purposes in the certification environment and would not be applicable to the production configuration. The device would not normally be used for routing calls that do not pass through the Genesys SIP Server.

Details of IP2IP Routing Table #12

Source IP Group ID = 1	Source Username Prefix = *
Source Host = *	Destination Username Prefix = 2027562827
Destination Host = *	Request Type = All
Message Condition = None	Destination Type = IP Group
Destination IP Group ID = 5	Destination SRD ID = 1
Destination Address =	Destination Port = 0
Destination Transport Type =	Alternative Route Options = Route Row
Cost Group = None	

- 13. Index #13** specifies that all IP calls with destination prefix 2027562827 received from IP Group 2 (AT&T IP Flexible Reach Secondary IPBE) will route to SRD 1, IP Group 5 (non-AT&T Customer Group). This entry was used for testing purposes in the certification environment and would not be applicable to the production configuration. Note that this is configured as an Alternate Route, meaning that this rule will apply if the previous rule applied but the route is not reachable.

Details of IP2IP Routing Table #13

Source IP Group ID = 2	Source Username Prefix = *
Source Host = *	Destination Username Prefix = 2027562827
Destination Host = *	Request Type = All
Message Condition = None	Destination Type = IP Group
Destination IP Group ID = 5	Destination SRD ID = 1
Destination Address =	Destination Port = 0
Destination Transport Type =	Alternative Route Options = Alt Route Ignore Inputs
Cost Group = None	

- 14. Index #14** specifies that IP calls with destination 2027562828-2027562829 originating on IP Group 1 (AT&T IP Flexible Reach) will be assigned to SRD 5, IP Group 8 (Remote Agent on non-AT&T network). This is part of the certification environment for troubleshooting purposes and is inapplicable to a production environment because all calls should route through the device to the Genesys SIP Server.

Details of IP2IP Routing Table #14

Source IP Group ID = 1	Source Username Prefix = *
Source Host = *	Destination Username Prefix = 202756282[8-9]
Destination Host = *	Request Type = All
Message Condition = None	Destination Type = IP Group
Destination IP Group ID = 8	Destination SRD ID = 5
Destination Address =	Destination Port = 0
Destination Transport Type =	Alternative Route Options = Route Row
Cost Group = None	

- 15. Index #15** specifies that IP calls with destination 2027562828-2027562829 originating on IP Group 2 (AT&T IP Flexible Reach Secondary IPBE) will be assigned to SRD 5, IP Group 8 (Remote Agent on non-AT&T network). This is part of the certification environment for troubleshooting purposes and is inapplicable to a production environment because all calls will route through the device to the Genesys SIP Server. Note that this is configured as an Alternate Route, meaning that this rule will apply if the previous rule applied but the route is not reachable.

Details of IP2IP Routing Table #15

Source IP Group ID = 2	Source Username Prefix = *
Source Host = *	Destination Username Prefix = 202756282[8-9]
Destination Host = *	Request Type = All
Message Condition = None	Destination Type = IP Group
Destination IP Group ID = 8	Destination SRD ID = 5
Destination Address =	Destination Port = 0
Destination Transport Type =	Alternative Route Options = Alt Route Ignore Inputs
Cost Group = None	

16. Index #16 specifies that IP calls with destination 2027562830 originating on IP Group 1 (AT&T IP Flexible Reach) will be assigned to SRD 5, IP Group 8 (Customer on non-AT&T network). This is part of the certification environment for troubleshooting purposes and is inapplicable to a production environment because all calls should route through the device to the Genesys SIP Server.

Details of IP2IP Routing Table #16

Source IP Group ID = 1	Source Username Prefix = *
Source Host = *	Destination Username Prefix = 2027562830
Destination Host = *	Request Type = All
Message Condition = None	Destination Type = IP Group
Destination IP Group ID = 6	Destination SRD ID = 5
Destination Address =	Destination Port = 0
Destination Transport Type =	Alternative Route Options = Route Row
Cost Group = None	

17. Index #17 specifies that IP calls with destination 2027562830 originating on IP Group 2 (AT&T IP Flexible Reach) will be assigned to SRD 5, IP Group 8 (Customer on non-AT&T network). This is part of the certification environment for troubleshooting purposes and is inapplicable to a production environment because all calls should route through the device to the Genesys SIP Server. Note that this is configured as an Alternate Route, meaning that this rule will apply if the previous rule applied but the route is not reachable.

Details of IP2IP Routing Table #17

Source IP Group ID = 2	Source Username Prefix = *
Source Host = *	Destination Username Prefix = 2027562830
Destination Host = *	Request Type = All
Message Condition = None	Destination Type = IP Group
Destination IP Group ID = 6	Destination SRD ID = 5
Destination Address =	Destination Port = 0
Destination Transport Type =	Alternative Route Options = Alt Route Ignore Inputs
Cost Group = None	

18. Index #18 specifies that IP calls with destination 2027562830 originating on IP Group 5 (AT&T Network) will be assigned to SRD 5, IP Group 8 (non-AT&T network). This is part of the certification environment for troubleshooting purposes and is not applicable to a production environment because all calls should route through the device to the Genesys SIP Server and customers would not communicate to each other directly through the device.

Details of IP2IP Routing Table #18

Source IP Group ID = 5	Source Username Prefix = *
Source Host = *	Destination Username Prefix = 2027562830
Destination Host = *	Request Type = All
Message Condition = None	Destination Type = IP Group
Destination IP Group ID = 6	Destination SRD ID = 5
Destination Address =	Destination Port = 0
Destination Transport Type =	Alternative Route Options = Route Row
Cost Group = None	

- 19. Index #19** specifies that all IP calls with destination 9192943600-9192943639 (the block of DNs assigned by AT&T and registered to the Genesys) arriving on IP Group 5 (AT&T network) will be routed to SRD 3, IP Group 3 (Genesys SIP Server). This routing was used as part of infrastructure in the certification environment (to simulate a customer on AT&T non-IPFR network calling to an agent) and would only apply to a production environment if there are customer terminations in the AT&T network that do not come through either IPBE.

Details of IP2IP Routing Table #19

Source IP Group ID = 5	Source Username Prefix = *
Source Host = *	Destination Username Prefix = 91929436[00-39]
Destination Host = *	Request Type = All
Message Condition = None	Destination Type = IP Group
Destination IP Group ID = 3	Destination SRD ID = 3
Destination Address =	Destination Port = 0
Destination Transport Type =	Alternative Route Options = Route Row
Cost Group = None	

- 20. Index #20** specifies that IP calls with destination 919294 originating on IP Group 6 (non-AT&T Customer Group) would be routed to SRD 3, IP Group 3 (Genesys). This configuration is for a scenario in which a customer calls the Genesys Call Center from a non-AT&T network.

Details of IP2IP Routing Table #20

Source IP Group ID = 6	Source Username Prefix = *
Source Host = *	Destination Username Prefix = 919294
Destination Host = *	Request Type = All
Message Condition = None	Destination Type = IP Group
Destination IP Group ID = 3	Destination SRD ID = 3
Destination Address =	Destination Port = 0
Destination Transport Type =	Alternative Route Options = Route Row
Cost Group = None	

- 21. Index #20** specifies that IP calls with destination 919294 originating on IP Group 8 (non-AT&T network) would be routed to SRD 3, IP Group 3 (Genesys). This configuration is for a scenario in which a Remote Agent calls the Genesys Call Center from a non-AT&T network.

Details of IP2IP Routing Table #21

Source IP Group ID = 8	Source Username Prefix = *
Source Host = *	Destination Username Prefix = 919294
Destination Host = *	Request Type = All
Message Condition = None	Destination Type = IP Group
Destination IP Group ID = 3	Destination SRD ID = 3
Destination Address =	Destination Port = 0
Destination Transport Type =	Alternative Route Options = Route Row
Cost Group = None	

- 22.** Index #22 specifies that IP calls with destination 9192873450-9192873515 originating on IP Group 5 (AT&T network) with source prefix 202 will be assigned to SRD 1, IP Group 1 (AT&T). This is part of the certification infrastructure for test purposes, representing a specific customer calling to an Agent but forcing the routing through the AT&T IP Flexible Reach network. This would not be typically configured in a production environment.

Details of IP2IP Routing Table #22

Source IP Group ID = 5	Source Username Prefix = 202
Source Host = *	Destination Username Prefix = 9192873[450-515]
Destination Host = *	Request Type = All
Message Condition = None	Destination Type = IP Group
Destination IP Group ID = 1	Destination SRD ID = 1
Destination Address =	Destination Port = 0
Destination Transport Type =	Alternative Route Options = Route Row
Cost Group = None	

- 23.** Index #23 specifies that IP calls with destination 9192873450-9192873515 originating on IP Group 5 (AT&T network) with source prefix 202 will be assigned to SRD 1, IP Group 2 (AT&T). This is part of the certification infrastructure for test purposes, representing a specific customer calling to an Agent but forcing the routing through the AT&T IP Flexible Reach network. This would not be typically configured in a production environment. Note that this is configured as an Alternate Route, meaning that this rule will apply if the previous rule applied but the route is not reachable.

Details of IP2IP Routing Table #23

Source IP Group ID = 5	Source Username Prefix = 202
Source Host = *	Destination Username Prefix = 9192873[450-515]
Destination Host = *	Request Type = All
Message Condition = None	Destination Type = IP Group
Destination IP Group ID = 2	Destination SRD ID = 1
Destination Address =	Destination Port = 0
Destination Transport Type =	Alternative Route Options = Alt Route Ignore Inputs
Cost Group = None	

- 24.** Index #24 specifies IP calls with destination 01141583330158 originating on IP Group 5 (AT&T network) will be assigned to SRD 1, IP Group 1 (AT&T). This is part of the certification infrastructure for test purposes, representing a specific customer calling to an Agent but forcing the routing through the AT&T IP Flexible Reach network. This would not be typically configured in a production environment.

Details of IP2IP Routing Table #24

Source IP Group ID = 5	Source Username Prefix = *
Source Host = *	Destination Username Prefix = 01141583330158
Destination Host = *	Request Type = All
Message Condition = None	Destination Type = IP Group
Destination IP Group ID = 1	Destination SRD ID = 1
Destination Address =	Destination Port = 0
Destination Transport Type =	Alternative Route Options = Route Row
Cost Group = None	

- 25.** Index #25 specifies IP calls with destination 01141583330158 originating on IP Group 5 (AT&T network) will be assigned to SRD 1, IP Group 2 (AT&T). This is part of the certification infrastructure for test purposes, representing a specific customer calling to an Agent but forcing the routing through the AT&T IP Flexible Reach network. This would not be typically configured in a production environment. Notice that this is configured as an Alternate Route, meaning that this rule will apply if the previous rule applied but the route is not reachable.

Details of IP2IP Routing Table #25

Source IP Group ID = 5	Source Username Prefix = *
Source Host = *	Destination Username Prefix = 01141583330158
Destination Host = *	Request Type = All
Message Condition = None	Destination Type = IP Group
Destination IP Group ID = 2	Destination SRD ID = 1
Destination Address =	Destination Port = 0
Destination Transport Type =	Alternative Route Options = Alt Route Ignore Inputs
Cost Group = None	

- 26.** Index #26 was not used in configuration, or, if it did exist, it was later deleted.
- 27.** Index #27 specifies that all IP calls originating on IP Group 3 (Genesys SIP Server) will be assigned to IP Group 1 (AT&T IP Flexible Reach). This is the default entry and would apply if all other route rows for IP calls originating from IP Group 3 (Genesys) were not a match. A similar entry will exist in a production environment.

Details of IP2IP Routing Table #27

Source IP Group ID = 3	Source Username Prefix = *
Source Host = *	Destination Username Prefix = *
Destination Host = *	Request Type = All
Message Condition = None	Destination Type = IP Group
Destination IP Group ID = 1	Destination SRD ID = 1
Destination Address =	Destination Port = 0
Destination Transport Type =	Alternative Route Options = Route Row
Cost Group = None	

- 28.** Index #28 specifies that all IP calls originating on IP Group 3 (Genesys SIP Server) will be assigned to IP Group 2 (AT&T IP Flexible Reach Secondary IPBE). This is the default entry and would apply if all other route rows for IP calls originating from IP Group 3 (Genesys) were not a match and the previous route applied but route was not available. A similar entry will exist in a production environment.

Details of IP2IP Routing Table #28

Source IP Group ID = 3	Source Username Prefix = *
Source Host = *	Destination Username Prefix = *
Destination Host = *	Request Type = All
Message Condition = None	Destination Type = IP Group
Destination IP Group ID = 2	Destination SRD ID = 1
Destination Address =	Destination Port = 0
Destination Transport Type =	Alternative Route Options = Alt Route Ignore Inputs
Cost Group = None	

- 29.** Index #29 specifies that IP calls with destination 18888064788 originating on IP Group 5 (AT&T Customer Group) will be assigned to IP Group 1 (AT&T IP Flexible Reach). This is part of the certification environment for troubleshooting and would not be configured in a production environment.

Details of IP2IP Routing Table #29

Source IP Group ID = 5	Source Username Prefix = *
Source Host = *	Destination Username Prefix = 18888064788
Destination Host = *	Request Type = All
Message Condition = None	Destination Type = IP Group
Destination IP Group ID = 1	Destination SRD ID = 1
Destination Address =	Destination Port = 0
Destination Transport Type =	Alternative Route Options = Route Row
Cost Group = None	

- 30.** Index #30 specifies that IP calls with destination 18888064788 originating on IP Group 5 (AT&T Customer Group) will be assigned to IP Group 2 (AT&T IP Flexible Reach Secondary IPBE). This alternate route is used if the previous route rule is matched but

the destination cannot be reached. This route is part of the certification environment for troubleshooting and would not be configured in a production environment.

Details of IP2IP Routing Table #30

Source IP Group ID = 5	Source Username Prefix = *
Source Host = *	Destination Username Prefix = 18888064788
Destination Host = *	Request Type = All
Message Condition = None	Destination Type = IP Group
Destination IP Group ID = 2	Destination SRD ID = 1
Destination Address =	Destination Port = 0
Destination Transport Type =	Alternative Route Options = Alt Route Ignore Inputs
Cost Group = None	

- 31.** Index #31 specifies that IP calls with destination 18888064788 originating on IP Group 6 (AT&T Customer Group) will be assigned to SRD 1, IP Group 1 (AT&T IP Flexible Reach). This was part of the certification environment for troubleshooting and would not be configured in a production environment.

Details of IP2IP Routing Table #31

Source IP Group ID = 6	Source Username Prefix = *
Source Host = *	Destination Username Prefix = 18888064788
Destination Host = *	Request Type = All
Message Condition = None	Destination Type = IP Group
Destination IP Group ID = 1	Destination SRD ID = 1
Destination Address =	Destination Port = 0
Destination Transport Type =	Alternative Route Options = Route Row
Cost Group = None	

- 32.** Index #32 specifies that IP calls with destination 18888064788 originating on IP Group 6 (AT&T Customer Group) will be assigned to IP Group 2 (AT&T IP Flexible Reach Secondary IPBE). This alternate route is used if the previous route rule is matched but the destination cannot be reached. This is part of the certification environment for troubleshooting and would not be configured in a production environment.

Details of IP2IP Routing Table #32

Source IP Group ID = 6	Source Username Prefix = *
Source Host = *	Destination Username Prefix = 18888064788
Destination Host = *	Request Type = All
Message Condition = None	Destination Type = IP Group
Destination IP Group ID = 2	Destination SRD ID = 1
Destination Address =	Destination Port = 0
Destination Transport Type =	Alternative Route Options = Alt Route Ignore Inputs
Cost Group = None	

5.2 SIP Header Manipulation

The Mediant 3000 E-SBC provides enhanced SIP header manipulation through the Message Manipulation Table. The feature enables normalization of SIP messaging fields between communication network segments such as the AT&T IP Flexible Reach SIP Trunk network and the Genesys Call Center private network. Header manipulation allows Service Providers to design their own policies on the SIP messaging fields that must be present before a SIP call enters their network. Similarly, enterprises may have policies for the information that can enter or leave their networks for policy or security reasons from a Service Provider.

SIP header manipulation supports the following features that are used in this solution:

- Addition of new headers
- Modification of header components
- Topology hiding
- Configurable identity hiding
- Multiple manipulation rules on the same SIP message

The manipulation is performed on SIP messages according to the Classification table (source/destination of username/host prefixes and source IP address). The manipulation can be performed on message type (Method, Request/Response, and Response type). Message manipulations are performed only after the classification, inbound manipulations and routing are successfully performed (i.e., manipulations are performed only in the outgoing leg). SIP Message manipulation rules can be assigned to an IP Group in the IP Group table and determined whether they must be performed for inbound or outbound messages.

Figure 5-42: Web Message Manipulation (SIP Header Manipulation) Table

Message Manipulations							
Note: Select row index to modify the relevant row.							
		<input type="text"/>	<input type="button" value="Add"/>				
Index	Manipulation Set ID	Message Type	Condition	Action Subject	Action Type	Action Value	Row Role
1	0	Invite.Request	Header.Request-uri.URL.host	Header.Request-uri.URL.host	Modify	'12.210.214.226'	Use Current Condition
2	0	Invite.Request	Header.To.url.host contains '10	Header.to.url.host	Modify	'12.210.214.226'	Use Current Condition
3	0	Invite.Request	Header.From.Url.Host contains	Header.From.Url.Host	Modify	'12.210.214.226'	Use Current Condition
4	9	Invite.Request		Header.P-Asserted-identity	Add	'Unavailable< sip:' + header.con	Use Current Condition
6	9	Invite.Request		Header.Privacy	Add	'id'	Use Current Condition
7	3			Header.Contact.url.user	Modify	'gcsbc01'	Use Current Condition
8	0	Invite.Request	Header.To.url.host contains 'ar	Header.to.url.host	Modify	'12.210.214.226'	Use Current Condition
9	0	Invite.Request	Header.P-Asserted-identity UR	Header.P-Asserted-identity UR	Modify	'12.210.214.226'	Use Current Condition
10	9	Invite.Request	Header.From contains 'AUDIO	Header.From.name	Modify	'AUDIOCODES'	Use Current Condition
12	9	Invite.Request		header.diversion	Add	'"offnet"< sip:9192943622@12	Use Current Condition
13	0	Invite.Request		header.diversion	Add	header.to.url.user + '< sip:' + he	Use Current Condition

For clarity, the table is shown again below with spacing and annotations to describe the impact of each manipulation.

Note the following regarding the entries:

- Manipulation Set '0' is the collection of rules that apply to calls on the outgoing AT&T IP Flex Reach SIP Trunk in the certification configuration (configured in the IPGroup table).
- Manipulation Set '3' is applied to calls passing to the Genesys environment. This consists of only one rule that changes the FROM header to identify the source as being from the device 'gcsbc01'
- Manipulation Set '4' was created to be an inbound (to the device) rule for calls from the Genesys to handle adding a diversion header for forwarded calls. This was not

handled in manipulation set 0 because in the IPGroup table, the SIP Name is being manipulated. This modification results in the device changing the INVITE URI and TO Header to be the same, so the comparison must be done earlier in the process.

- Some columns are not shown if these did not apply to the certification environment configuration.
- The conditions can be similar or enhanced for a production environment if the production solution does not require the rule in all cases. As an example, the below rules enforce that all Agents will have Calling Number Privacy & P-Asserted Identity added to the SIP header.
- The diversion header must be in place for forwarded calls.
- The diversion header should not be applied to non-forwarded calls, especially X11 calls, as this will result in call failure.

Figure 5-43: Message Manipulations for AT&T IP Flexible Reach with Genesys SIP Server

[MessageManipulations]

Index	Man Set ID	Message Type	Condition	Action Subject	Action Type	Action Value	Row Role
3	0	Invite.Request	Header.From.Url.Host contains angel.z101.gchariot.com	Header.From.Url.Host	2 (Modify)	12.210.214.226	0 (Use Current Condition)
4	0	Invite.Request	Header.P-Asserted-identity exists	Header.P-Asserted-identity	2 (Modify)	Unavailable	0 (Use Current Condition)
5	0	Invite.Request	Header.P-Asserted-identity !exists	Header.P-Asserted-identity	0 (Add)	Unavailable	0 (Use Current Condition)
6	0	Invite.Request		Header.Privacy	0 (Add)	id	0 (Use Current Condition)
7	3			Header.Contact.url.user	2 (Modify)	gcsbc01	0 (Use Current Condition)
9	0	Invite.Request	Header.P-Asserted-identity.URL.host contains angel.z101.gchariot.com	Header.P-Asserted-identity.URL.host	2 (Modify)	12.210.214.226	0 (Use Current Condition)
13	4	Invite.Request	Header.Request-uri.URL.user != Header.to.url.user	Header.Diversion	0 (Add)	9192943600 + <sip: + 9192943600 + @12.210.214.226 >+ ;user=phone>;user id=	0 (Use Current Condition)
16	0	Invite.Request		header.from.name	2 (Modify)	Anonymous	0 (Use Current Condition)

5.3 Mediant 3000 E-SBC User Info File



Note: The device's User Info file from the certification environment is included for reference only. This file is only necessary if an IP phone is registering to the device. For the production solution, all phones will register to Genesys.

```
[SBC]
FORMAT LOCALUSER,Username,Password,IPGroupID
2027562827,2027562827,1@A3&cD$,5
2027562830,2027562830,1@A3&cD$,6
2027562831,2027562831,1@A3&cD$,6
2027562832,2027562832,1@A3&cD$,6
2027562833,2027562833,1@A3&cD$,6
2027562834,2027562834,1@A3&cD$,6
```

5.4 Mediant 3000 E-SBC Feature Key

The feature key information is captured here for reference only, as a snapshot of the configuration used in the testing. Not all features below apply to this solution.

```
Key features:
Board Type: Mediant 3000
Channel Type: RTP DspCh=336
HA
IP Media: VXML CALEA
QOE features: VoiceQualityMonitoring
Coders: G723 G729 NETCODER GSM-FR G727 ILBC
PSTN Protocols: ISDN IUA=84 CAS V5.2
Security: IPSEC MediaEncryption StrongEncryption
EncryptControlProtocol
DSP Voice features: IpmDetector AMRPolicyManagement
PSTN STM1\SONET Interface Supported
PSTN T3 Interfaces=3
Control Protocols: MSFT MGCP MEGACO H323 SIP IP2IP=336
Default features:
Coders: G71
```


5.5 Mediant 3000 E-SBC Configuration File



Note: The Mediant 3000 E-SBC configuration file is added here for reference purposes only.

```
;*****
;** Ini File **
;*****

;Board: Mediant 3000
;M3K Board Type: TrunkPack 6310
;Serial Number: 3218534
;Slot Number: 1
;Software Version: 6.40A.037.009
;DSP Software Version: 491096AE3 => 640.25
;Board IP Address: 10.38.20.10
;Board Subnet Mask: 255.255.255.0
;Board Default Gateway: 10.38.20.1
;Private IP Address: 10.38.20.11
;Ram size: 512M   Flash size: 32M
;Num of DSP Cores: 126   Num DSP Channels: 336
;Profile: NONE
;Key features;;Board Type: Mediant 3000 ;Channel Type: RTP
DspCh=336 ;HA ;IP Media: VXML CALEA ;QOE features:
VoiceQualityMonitoring ;Coders: G723 G729 NETCODER GSM-FR G727
ILBC ;PSTN Protocols: ISDN IUA=84 CAS V5.2 ;Security: IPSEC
MediaEncryption StrongEncryption EncryptControlProtocol ;DSP Voice
features: IpmDetector AMRPolicyManagement ;PSTN STM1\SONET
Interface Supported ;PSTN T3 Interfaces=3 ;Control Protocols: MSFT
MGCP MEGACO H323 SIP IP2IP=336 ;Default features;;Coders: G711
G726;
;-----

[SYSTEM Params]

PM_VEDSPUtil = '1,302,336,15'
SyslogServerIP = 10.38.5.79
EnableSyslog = 1
NTPServerIP_abs = 66.228.35.252
NTPServerUTCOffset = -18000
ActivityListToLog = 'naa'
DayLightSavingTimeStart = '03:01:00:00'
DayLightSavingTimeEnd = '11:01:00:00'
DayLightSavingTimeEnable = 1
NTPServerIP = '66.228.35.252'

[BSP Params]

PCMLawSelect = 3
BaseUDPPort = 4000
VLANMODE = 1
VLANOAMVLANID = 320
VLANCONTROLVLANID = 254
```

```
VLANMEDIAVLANID = 254
VLANNATIVEVLANID = 320
RoutingTableHopsCountColumn = 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
VLANHEARTBEATVLANID = 320

[ControlProtocols Params]

AdminStateLockControl = 0
QOEServerIp = 10.38.20.30
QOEInformationLevel = 2

[MGCP Params]

[MEGACO Params]

EP_Num_0 = 0
EP_Num_1 = 1
EP_Num_2 = 1
EP_Num_3 = 0
EP_Num_4 = 0

[PSTN Params]

[SS7 Params]

[Voice Engine Params]

CallProgressTonesFilename = 'M2K_usa_tones.dat'
IdlePCMPattern = 85

[WEB Params]

LogoWidth = '145'
HTTPSCipherString = 'RC4:EXP'

[SIP Params]

MEDIACHANNELS = 512
AUTHENTICATIONMODE = 0
GWDEBUGLEVEL = 5
PROXYREDUNDANCYMODE = 1
ENABLEUSERINFOUSAGE = 1
USERINFOFILENAME = 'm3kuserinfo.8.22.2012.txt'
SetDefaultOnIniFileProcess = 0
ENABLESBCAPPLICATION = 1
SBCMAXFORWARDSLIMIT = 70
SBCGRUUMODE = 0
AUTHQOP = 0

[SCTP Params]

[VXML Params]
```

```

[IPsec Params]

[Audio Staging Params]

[SNMP Params]

SNMPManagerIsUsed_0 = 1
SNMPManagerIsUsed_1 = 0
SNMPManagerIsUsed_2 = 0
SNMPManagerIsUsed_3 = 0
SNMPManagerIsUsed_4 = 0
SNMPManagerTableIP_0 = 10.38.20.30
SNMPManagerTableIP_1 = 0.0.0.0
SNMPManagerTableIP_2 = 0.0.0.0
SNMPManagerTableIP_3 = 0.0.0.0
SNMPManagerTableIP_4 = 0.0.0.0

[ InterfaceTable ]

FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_VlanID, InterfaceTable_InterfaceName,
InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress;
InterfaceTable 0 = 0, 10, 10.38.20.10, 24, 10.38.20.1, 320,
NETMGMT, 0.0.0.0, 0.0.0.0;
InterfaceTable 1 = 5, 10, 173.227.254.68, 26, 173.227.254.65, 254,
PUBSIP, 0.0.0.0, 0.0.0.0;
InterfaceTable 2 = 5, 10, 10.38.60.10, 24, 10.38.60.1, 360,
RALVOX, 0.0.0.0, 0.0.0.0;
InterfaceTable 3 = 5, 10, 12.210.214.226, 29, 12.210.214.225, 455,
ATTDMZ, 0.0.0.0, 0.0.0.0;
InterfaceTable 4 = 5, 10, 10.38.5.10, 24, 10.38.5.1, 305,
RALOFFICE, 0.0.0.0, 0.0.0.0;

[ \InterfaceTable ]

[ ACCESSLIST ]

FORMAT ACCESSLIST_Index = ACCESSLIST_Source_IP,
ACCESSLIST_PrefixLen, ACCESSLIST_Start_Port, ACCESSLIST_End_Port,
ACCESSLIST_Protocol, ACCESSLIST_Use_Specific_Interface,
ACCESSLIST_Interface_ID, ACCESSLIST_Packet_Size,
ACCESSLIST_Byte_Rate, ACCESSLIST_Byte_Burst,
ACCESSLIST_Allow_Type, ACCESSLIST_Source_Port;
ACCESSLIST 0 = 12.194.231.76, 32, 0, 65535, Any, 1, ATTDMZ, 0, 0,
0, ALLOW, 0;
ACCESSLIST 1 = 12.194.230.7, 32, 0, 65535, Any, 1, ATTDMZ, 0, 0,
0, ALLOW, 0;
ACCESSLIST 2 = 12.194.231.87, 32, 0, 65535, Any, 1, ATTDMZ, 0, 0,
0, ALLOW, 0;
ACCESSLIST 3 = 12.194.230.20, 32, 0, 65535, Any, 1, ATTDMZ, 0, 0,
0, ALLOW, 0;
ACCESSLIST 4 = 12.210.214.230, 32, 0, 65535, Any, 1, PUBSIP, 0, 0,
0, BLOCK, 0;

```

```
ACCESSLIST 6 = 0.0.0.0, 0, 0, 65535, Any, 1, ATDMZ, 0, 0, 0,
BLOCK, 0;
ACCESSLIST 17 = 173.227.254.87, 0, 0, 65535, Any, 1, PUBSIP, 0, 0,
0, ALLOW, 0;
ACCESSLIST 18 = 173.227.254.89, 0, 0, 65535, Any, 1, PUBSIP, 0, 0,
0, ALLOW, 0;
ACCESSLIST 19 = 173.227.254.90, 0, 0, 65535, Any, 1, PUBSIP, 0, 0,
0, ALLOW, 0;
ACCESSLIST 20 = 0.0.0.0, 0, 0, 65535, Any, 1, PUBSIP, 0, 0, 0,
BLOCK, 0;

[ \ACCESSLIST ]

[ DspTemplates ]

FORMAT DspTemplates_Index = DspTemplates_DspTemplateName,
DspTemplates_DspResourcesPercentage;
DspTemplates 0 = 0, 100;

[ \DspTemplates ]

[ CpMediaRealm ]

FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName,
CpMediaRealm_IPv4IF, CpMediaRealm_IPv6IF,
CpMediaRealm_PortRangeStart, CpMediaRealm_MediaSessionLeg,
CpMediaRealm_PortRangeEnd, CpMediaRealm_TransRateRatio,
CpMediaRealm_IsDefault;
CpMediaRealm 0 = ATDMZ_MR, ATDMZ, , 16390, 600, 22380, 1, 1;
CpMediaRealm 1 = RALVOX_MR, RALVOX, , 6000, 50, 6490, 1, 0;
CpMediaRealm 2 = RALLOFFICE_MR, RALOFFICE, , 6500, 550, 11990, 1,
0;
CpMediaRealm 3 = TWCDMZ_MR, PUBSIP, , 12000, 100, 12990, 0, 0;

[ \CpMediaRealm ]

[ QOERules ]

FORMAT QOERules_Index = QOERules_MediaRealmIndex,
QOERules_RuleIndex, QOERules_MonitoredParam, QOERules_Profile,
QOERules_GreenYellowThreshold, QOERules_GreenYellowHysteresis,
QOERules_YellowRedThreshold, QOERules_YellowRedHysteresis;
QOERules 0 = 1, 1, 0, 2, 35, 1, 28, 1;
QOERules 1 = 2, 1, 0, 2, 35, 1, 28, 1;
QOERules 2 = 3, 1, 0, 2, 35, 1, 28, 1;
QOERules 3 = 0, 1, 0, 2, 35, 1, 28, 1;

[ \QOERules ]

[ SRD ]

FORMAT SRD_Index = SRD_Name, SRD_MediaRealm,
SRD_IntraSRDMediaAnchoring, SRD_BlockUnRegUsers,
SRD_MaxNumOfRegUsers, SRD_EnableUnAuthenticatedRegistrations;
SRD 1 = ATDMZ_SRD, ATDMZ_MR, 0, 1, -1, 0;
SRD 2 = RALVOX_SRD, RALVOX_MR, 1, 0, -1, 1;
```

```
SRD 3 = RALLOFFICE_SRD, RALLOFFICE_MR, 0, 0, -1, 1;
SRD 5 = TWCDMZ_IPP, TWCDMZ_MR, 0, 0, -1, 1;

[ \SRD ]

[ Dns2Ip ]

FORMAT Dns2Ip_Index = Dns2Ip_DomainName, Dns2Ip_FirstIpAddress,
Dns2Ip_SecondIpAddress, Dns2Ip_ThirdIpAddress,
Dns2Ip_FourthIpAddress;
Dns2Ip 0 = rtpsip.cl.gchariot.com, 10.38.5.117, 0.0.0.0, 0.0.0.0,
0.0.0.0;

[ \Dns2Ip ]

[ SBCTAlternativeRoutingReasons ]

FORMAT SBCTAlternativeRoutingReasons_Index =
SBCTAlternativeRoutingReasons_ReleaseCause;
SBCTAlternativeRoutingReasons 0 = 408;

[ \SBCTAlternativeRoutingReasons ]

[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIp_IpAddress, ProxyIp_TransportType,
ProxyIp_ProxySetId;
ProxyIp 0 = 12.194.231.76, -1, 1;
ProxyIp 1 = 173.227.254.89, -1, 8;
ProxyIp 2 = rtpsip.cl.gchariot.com, 0, 3;
ProxyIp 3 = 12.194.230.7, -1, 2;

[ \ProxyIp ]

[ IpProfile ]
```

```

FORMAT IpProfile_Index = IpProfile_ProfileName,
IpProfile_IpPreference, IpProfile_CodersGroupID,
IpProfile_IsFaxUsed, IpProfile_JitterBufMinDelay,
IpProfile_JitterBufOptFactor, IpProfile_IPDiffServ,
IpProfile_SigIPDiffServ, IpProfile_SCE,
IpProfile_RTPRedundancyDepth, IpProfile_RemoteBaseUDPPort,
IpProfile_CNMode, IpProfile_VxxTransportType, IpProfile_NSEMode,
IpProfile_IsDTMFUsed, IpProfile_PlayRBTone2IP,
IpProfile_EnableEarlyMedia, IpProfile_ProgressIndicator2IP,
IpProfile_EnableEchoCanceller, IpProfile_CopyDest2RedirectNumber,
IpProfile_MediaSecurityBehaviour, IpProfile_CallLimit,
IpProfile_DisconnectOnBrokenConnection,
IpProfile_FirstTxDtmfOption, IpProfile_SecondTxDtmfOption,
IpProfile_RxDTMFOption, IpProfile_EnableHold, IpProfile_InputGain,
IpProfile_VoiceVolume, IpProfile_AddIEInSetup,
IpProfile_SBCExtensionCodersGroupID,
IpProfile_MediaIPVersionPreference, IpProfile_TranscodingMode,
IpProfile_SBCAllowedCodersGroupID, IpProfile_SBCAllowedCodersMode,
IpProfile_SBCMediaSecurityBehaviour, IpProfile_SBCRFC2833Behavior,
IpProfile_SBCAlternativeDTMFMethod, IpProfile_SBCAssertIdentity,
IpProfile_AMDSensitivityParameterSuit,
IpProfile_AMDSensitivityLevel, IpProfile_AMDMaxGreetingTime,
IpProfile_AMDMaxPostSilenceGreetingTime,
IpProfile_SBCDiversiionMode, IpProfile_SBCHistoryInfoMode,
IpProfile_EnableQSIGTunneling, IpProfile_SBCFaxCodersGroupID,
IpProfile_SBCFaxBehavior, IpProfile_SBCFaxOfferMode,
IpProfile_SBCFaxAnswerMode, IpProfile_EnableEarly183;

IpProfile 1 = 'ATT IP Flex', 1, 0, 0, 10, 10, 46, 40, 0, 0, 0,
2, 0, 0, 0, 1, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, , -1, 0, 0,
0, 2, 0, 0, 0, -1, 0, 8, 300, 400, -1, -1, 0, -1, 0, 0, 1, 0;

[ \IpProfile ]

[ ProxySet ]

FORMAT ProxySet_Index = ProxySet_EnableProxyKeepAlive,
ProxySet_ProxyKeepAliveTime, ProxySet_ProxyLoadBalancingMethod,
ProxySet_IsProxyHotSwap, ProxySet_SRD,
ProxySet_ClassificationInput, ProxySet_ProxyRedundancyMode;

ProxySet 0 = 0, 60, 0, 0, 0, 0, -1;
ProxySet 1 = 1, 60, 0, 0, 1, 0, -1;
ProxySet 2 = 1, 60, 0, 0, 1, 0, -1;
ProxySet 3 = 1, 60, 0, 0, 3, 0, -1;
ProxySet 8 = 0, 60, 0, 0, 5, 0, -1;

[ \ProxySet ]

[ IPGroup ]

FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Description,
IPGroup_ProxySetId, IPGroup_SIPGroupName, IPGroup_ContactUser,
IPGroup_EnableSurvivability, IPGroup_ServingIPGroup,
IPGroup_SipReRoutingMode, IPGroup_AlwaysUseRouteTable,
IPGroup_RoutingMode, IPGroup_SRD, IPGroup_MediaRealm,
IPGroup_ClassifyByProxySet, IPGroup_ProfileId,
IPGroup_MaxNumOfRegUsers, IPGroup_InboundManSet,
IPGroup_OutboundManSet, IPGroup_RegistrationMode,
IPGroup_AuthenticationMode, IPGroup_MethodList,
IPGroup_EnableSBCClientForking, IPGroup_ContactName;

IPGroup 1 = 0, 'ATT IPGROUP', 1, 12.194.231.76, , 0, -1, 0, 0, -1,
1, ATTDMMZ_MR, 1, 1, -1, -1, 0, 0, 0, , 0, ;

```

```

IPGroup 2 = 0, 'ATT IPGroup secondary', 2, 12.194.230.7, , 0, -1,
0, 0, -1, 1, ATTMZ_MR, 1, 1, -1, -1, 0, 0, 0, , 0, ;
IPGroup 3 = 0, GENESYS_SRV, 3, angel.z101.gchariot.com, , 0, -1,
0, 0, -1, 3, RALLOFFICE_MR, 1, 0, -1, 4, 3, 0, 0, , 0, ;
IPGroup 4 = 1, , -1, , , 0, 2, 0, 0, -1, 0, , 1, 0, -1, -1, -1, 0,
0, , 0, ;
IPGroup 5 = 1, 'ATT Phone', -1, , , 0, -1, 0, 0, -1, 1, ATTMZ_MR,
0, 0, -1, -1, -1, 0, 2, REGISTER, 0, ;
IPGroup 6 = 1, 'TWC USERS', -1, , , 0, -1, 0, 0, -1, 5, TWCDMZ_MR,
0, 0, -1, -1, -1, 0, 2, REGISTER, 0, ;
IPGroup 7 = 1, 'ATT Remote Agents', -1, , , 0, -1, 0, 0, -1, 1,
ATTMZ_MR, 0, 0, -1, -1, -1, 0, 0, , 0, ;
IPGroup 8 = 1, 'TWC Remote Agents', -1, , , 0, -1, 0, 0, -1, 5,
TWCDMZ_MR, 0, 0, -1, -1, -1, 0, 0, , 0, ;

[ \IPGroup ]

[ IP2IPRouting ]

FORMAT IP2IPRouting_Index = IP2IPRouting_SrcIPGroupID,
IP2IPRouting_SrcUsernamePrefix, IP2IPRouting_SrcHost,
IP2IPRouting_DestUsernamePrefix, IP2IPRouting_DestHost,
IP2IPRouting_RequestType, IP2IPRouting_MessageCondition,
IP2IPRouting_DestType, IP2IPRouting_DestIPGroupID,
IP2IPRouting_DestSRDID, IP2IPRouting_DestAddress,
IP2IPRouting_DestPort, IP2IPRouting_DestTransportType,
IP2IPRouting_AltRouteOptions, IP2IPRouting_CostGroup;
IP2IPRouting 1 = 5, *, *, *, *, 2, , 0, 5, , , 0, -1, 0, ;
IP2IPRouting 3 = 7, *, *, *, *, 0, , 0, 3, 3, , 0, -1, 0, ;
IP2IPRouting 4 = 8, *, *, *, *, 0, , 0, 3, 3, , 0, -1, 0, ;
IP2IPRouting 5 = 6, *, *, *, *, 2, , 0, 6, , , 0, -1, 0, ;
IP2IPRouting 6 = 1, *, *, 919294, *, 0, , 0, 3, 3, , 0, -1, 0, ;
IP2IPRouting 7 = 2, *, *, 919294, *, 0, , 0, 3, 3, , 0, -1, 1, ;
IP2IPRouting 8 = 3, *, *, 9192943635, *, 0, , 0, 7, 1, , 0, -1, 0,
;
IP2IPRouting 9 = 3, *, *, 919294363[7-8], *, 0, , 0, 8, 5, , 0, -
1, 0, ;
IP2IPRouting 10 = 1, *, *, 202756282[5-6], *, 0, , 0, 3, 3, , 0, -
1, 0, ;
IP2IPRouting 11 = 2, *, *, 202756282[5-6], *, 0, , 0, 3, 3, , 0, -
1, 1, ;
IP2IPRouting 12 = 1, *, *, 2027562827, *, 0, , 0, 5, 1, , 0, -1,
0, ;
IP2IPRouting 13 = 2, *, *, 2027562827, *, 0, , 0, 5, 1, , 0, -1,
1, ;
IP2IPRouting 14 = 1, *, *, 202756282[8-9], *, 0, , 0, 8, 5, , 0, -
1, 0, ;
IP2IPRouting 15 = 2, *, *, 202756282[8-9], *, 0, , 0, 8, 5, , 0, -
1, 1, ;
IP2IPRouting 16 = 1, *, *, 2027562830, *, 0, , 0, 6, 5, , 0, -1,
0, ;
IP2IPRouting 17 = 2, *, *, 2027562830, *, 0, , 0, 6, 5, , 0, -1,
1, ;
IP2IPRouting 18 = 5, *, *, 2027562830, *, 0, , 0, 6, 5, , 0, -1,
0, ;
IP2IPRouting 19 = 5, *, *, 91929436[00-39], *, 0, , 0, 3, 3, , 0,
-1, 0, ;
IP2IPRouting 20 = 6, *, *, 919294, *, 0, , 0, 3, 3, , 0, -1, 0, ;
IP2IPRouting 21 = 8, *, *, 919294, *, 0, , 0, 3, 3, , 0, -1, 0, ;
IP2IPRouting 22 = 5, 202, *, 9192873[450-515], *, 0, , 0, 1, 1, ,
0, -1, 0, ;

```

```

IP2IPRouting 23 = 5, 202, *, 9192873[450-515], *, 0, , 0, 2, 1, ,
0, -1, 1, ;
IP2IPRouting 24 = 5, *, *, 01141583330158, *, 0, , 0, 1, 1, , 0, -
1, 0, ;
IP2IPRouting 25 = 5, *, *, 01141583330158, *, 0, , 0, 2, 1, , 0, -
1, 1, ;
IP2IPRouting 27 = 3, *, *, *, *, 0, , 0, 1, 1, , 0, -1, 0, ;
IP2IPRouting 28 = 3, *, *, *, *, 0, , 0, 2, 1, , 0, -1, 1, ;
IP2IPRouting 29 = 5, *, *, 18888064788, *, 0, , 0, 1, 1, , 0, -1,
0, ;
IP2IPRouting 30 = 5, *, *, 18888064788, *, 0, , 0, 2, 1, , 0, -1,
1, ;
IP2IPRouting 31 = 6, *, *, 18888064788, *, 0, , 0, 1, 1, , 0, -1,
0, ;
IP2IPRouting 32 = 6, *, *, 18888064788, *, 0, , 0, 2, 1, , 0, -1,
1, ;

[ \IP2IPRouting ]

[ Classification ]

FORMAT Classification_Index = Classification_MessageCondition,
Classification_SrcSRDID, Classification_SrcAddress,
Classification_SrcPort, Classification_SrcTransportType,
Classification_SrcUsernamePrefix, Classification_SrcHost,
Classification_DestUsernamePrefix, Classification_DestHost,
Classification_ActionType, Classification_SrcIPGroupID;
Classification 2 = , 5, 173.227.254.*, 0, -1, 202756282[8-9], *,
*, *, 1, 8;
Classification 3 = , 5, 173.227.254.*, 0, -1, 919294363[7-8], *,
*, *, 1, 8;
Classification 4 = , 5, 173.227.254.*, 0, -1, 2027562830, *, *, *,
1, 6;
Classification 5 = , 1, 12.210.214.*, 0, -1, 2027562827, *, *, *,
1, 5;
Classification 6 = , 1, 12.210.214.*, 0, -1, 202756282[8-9], *, *,
*, 1, 8;
Classification 7 = , 1, 12.210.214.*, 0, -1, 9192943635, *, *, *,
1, 7;

[ \Classification ]

[ SIPInterface ]

FORMAT SIPInterface_Index = SIPInterface_NetworkInterface,
SIPInterface_ApplicationType, SIPInterface_UDPPort,
SIPInterface_TCPPort, SIPInterface_TLSPort, SIPInterface_SRD,
SIPInterface_MessagePolicy;
SIPInterface 1 = ATDMZ, 2, 5060, 5060, 5061, 1, ;
SIPInterface 2 = RALVOX, 2, 5060, 5060, 5061, 2, ;
SIPInterface 3 = RALOFFICE, 2, 5060, 5060, 5061, 3, ;
SIPInterface 5 = PUBSIP, 2, 5060, 5060, 5061, 5, ;

[ \SIPInterface ]

[ IPInboundManipulation ]

```



```

FORMAT IPInboundManipulation_Index =
IPInboundManipulation_IsAdditionalManipulation,
IPInboundManipulation_ManipulationPurpose,
IPInboundManipulation_SrcIPGroupID,
IPInboundManipulation_SrcUsernamePrefix,
IPInboundManipulation_SrcHost,
IPInboundManipulation_DestUsernamePrefix,
IPInboundManipulation_DestHost, IPInboundManipulation_RequestType,
IPInboundManipulation_ManipulatedURI,
IPInboundManipulation_RemoveFromLeft,
IPInboundManipulation_RemoveFromRight,
IPInboundManipulation_LeaveFromRight,
IPInboundManipulation_Prefix2Add,
IPInboundManipulation_Suffix2Add;
IPInboundManipulation 0 = 0, 0, 1, , *, 29436xx, *, 0, 1, 0, 0,
255, 919, ;

[ \IPInboundManipulation ]

[ CodersGroup0 ]

FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime,
CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce;
CodersGroup0 0 = g729, 30, 0, -1, 0;
CodersGroup0 1 = g711Ulaw64k, 30, 0, -1, 0;

[ \CodersGroup0 ]

[ AllowedCodersGroup0 ]

FORMAT AllowedCodersGroup0_Index = AllowedCodersGroup0_Name;
AllowedCodersGroup0 0 = g729;
AllowedCodersGroup0 1 = g711Ulaw64k;

[ \AllowedCodersGroup0 ]

[ MessageManipulations ]

FORMAT MessageManipulations_Index = MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject,
MessageManipulations_ActionType, MessageManipulations_ActionValue,
MessageManipulations_RowRole;
MessageManipulations 3 = 0, Invite.Request, 'Header.From.Url.Host
contains 'angel.z101.gchariot.com'', Header.From.Url.Host, 2,
'12.210.214.226', 0;
MessageManipulations 4 = 0, Invite.Request, 'Header.P-Asserted-
identity exists', 'Header.P-Asserted-identity ', 2,
''Unavailable<sip:'+ header.contact.url.user+'@12.210.214.226>'',
0;
MessageManipulations 5 = 0, Invite.Request, 'Header.P-Asserted-
identity !exists', Header.P-Asserted-identity, 0,
''Unavailable<sip:'+ header.contact.url.user+'@12.210.214.226>'',
0;
MessageManipulations 6 = 0, Invite.Request, , Header.Privacy, 0,
'id', 0;
MessageManipulations 7 = 3, , , Header.Contact.url.user, 2,
'gcsbc01', 0;

```

```
MessageManipulations 9 = 0, Invite.Request, 'Header.P-Asserted-identity.URL.host contains 'angel.z101.gchariot.com'', Header.P-Asserted-identity.URL.host, 2, '12.210.214.226', 0;
MessageManipulations 13 = 4, Invite.Request, 'Header.Request-uri.URL.user != Header.to.url.user', Header.Diversion, 0, '9192943600' + '<sip:' + '9192943600' + '@12.210.214.226>' + ';user=phone>;userid=', 0;
MessageManipulations 15 = 0, Invite.Request, , header.from.url.user, 2, 'anonymous', 0;
MessageManipulations 16 = 0, Invite.Request, , header.from.name, 2, 'Anonymous', 0;

[ \MessageManipulations ]

[ RoutingRuleGroups ]

FORMAT RoutingRuleGroups_Index = RoutingRuleGroups_LCReEnable,
RoutingRuleGroups_LCRAverageCallLength,
RoutingRuleGroups_LCRDefaultCost;
RoutingRuleGroups 0 = 0, 0, 1;

[ \RoutingRuleGroups ]
```

Configuration Note