Mediant™ E-SBC

Enterprise Session Border Controller

Session Initiated Protocol (SIP)

Configuration Note

Connecting Genesys® SIP Server with AT&T IP Toll Free SIP Trunking Service with MIS, PNT or AT&T Virtual Private Network Transport, via Mediant E-SBC

at&t

GENESYS®

September 2013

Document #: LTRT-38127

AudioCodes

Table of Contents

List of Figures

Notice

This Configuration Note shows how to configure AudioCodes' Mediant E-SBC 6.6 with Genesys SIP Server 8.1 and AT&T IP Toll Free SIP Trunking service on MIS, PNT or AT&T Virtual Private Network transport.

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.

Date Published: Sept-09-2013

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 *AudioCodes' Mediant E-SBC* represents the Mediant 800, Mediant 1000, Mediant 3000, Mediant 4000, or the Mediant Software E-SBCs.

Note: Throughout this document, unless otherwise specified, the term *IP Toll Free* represents AT&T IP Toll Free SIP Trunking Service on MIS, PNT, or AT&T Virtual Private Network transport.

Related Documentation

Manual Name
LTRT-30202 Recommended Security Guidelines Technical Note (AudioCodes)
LTRT-31620 SBC Deployment Guide (AudioCodes)
LTRT-41501 Mediant 4000 E-SBC Hardware Installation Manual Ver 6.6 (AudioCodes)
LTRT-41531 Mediant 4000 E-SBC User's Manual Ver 6.6 (AudioCodes)
LTRT-94710 Mediant 3000 SIP Installation Manual (AudioCodes)
LTRT-89713 Mediant 3000 SIP User’s Manual (AudioCodes)
LTRT-10301 Mediant Software E-SBC Physical Server Platforms Installation Manual (AudioCodes)
LTRT-26909 SIP CPE Release Notes Ver. 6.6
LTRT-28620_SIP Message Manipulations Quick Reference Guide
LTRT-41542 Mediant Software E-SBC User's Manual Ver. 6.6
LTRT-52310 SIP CPE Product Reference Manual Ver. 6.6
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)

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our Web site at http://www.audiocodes.com/downloads.

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 Toll Free SIP / 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 it 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.

AT&T IP Toll Free Service (IPTF) is a BVoIP service offering that provides inbound only toll-free service from the PSTN to the customer premise equipment (CPE). The underlying transport for AT&T IPTF may be Managed Internet Service (MIS)/Private Network Transport (PNT) or AT&T Virtual Private Network (AVPN).

AudioCodes' family of Enterprise Session Border Controllers (**E-SBCs**) represents a key component for Service Providers and businesses looking to migrate to a Voice-over-IP based communications infrastructure. The E-SBC acts as the demarcation between the Enterprise VoIP network and the Service Providers' SIP-based services. The AudioCodes Mediant E-SBC product family includes four E-SBC hardware based platforms (**Mediant 800 E-SBC**, **Mediant 1000 E-SBC**, **Mediant 3000 E-SBC** and **Mediant 4000 E-SBC**) offering a solution that covers organizations of any size and location, from small businesses and branch offices, all the way up to very large enterprise data centers and contact center facilities. The **Mediant Software E-SBC** is a software-only version of AudioCodes' E-SBC, enabling third party and OEM vendors to integrate E-SBC functionality into their own communication solutions.

Regardless of the particular E-SBC variant, the AudioCodes 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 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 E-SBC v6.6 interfacing with Genesys' SIP Server v8.1 and AT&T's IP Toll Free SIP Trunking Service on MIS/PNT/AVPN.

1.6 Test Scope

Genesys' SIP Server 8.1 was previously Partner Certified with AT&T IP Flexible Reach SIP Trunking Service. The certification of AudioCodes' Mediant E-SBCs covered in this Configuration Note is based on select cases from the AT&T IP Flexible Reach and AT&T

IP Toll Free test plans. The test suite is a scaled-down version of the interaction tests performed in Genesys' ODS Labs.

The objective of testing using the configuration detailed in this Note was to validate interoperability of Genesys' SIP Server communicating with AT&T IP Toll Free Service (inbound only), with AudioCodes' Mediant E-SBC v6.6 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 IP Toll Free Service:

- Basic Call using G.729
- Calling Party Number Presentation and Restriction
- AT&T Legacy Transfer Connect (8YY transfer)
- PSTN Alternate Destination Routing (IP ADR)
- IP Alternate Destination Routing (IP ADR)
- Intra-site Call Transfers
- Intra-site Conference
- Incoming DNIS Translation
- DNIS based Routing
- CED based Routing
- Call Center Queuing
- Codec Negotiation

1.6.2 Test Considerations/Exclusions

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

- AT&T IP Toll Free Service is for inbound calls (to the CPE) only.
- In this certification, the AudioCodes' E-SBC serves a security and topology hiding role. SIP RE-Invites are not reported back across the Trusted/Untrusted network border. This is possible on the ESBC by disabling Remote RE-INVITE support. This implies that different call entities (SIP clients, MOH, Queues, routing based applications, etc.) in the Call Center environment are with same call characteristics (in the SDP) as was negotiated at the start of the call and there is no mid-call characteristics negotiation.
- Transcoding was not required for this solution and was not used in testing.
- Legacy Transfer Connect with inband triggers (no human input) for Contact Center and VRU configurations are not applicable to the Genesys SIP Server solution.
- Ringback Unattended Transfer was not tested for this certification and not supported on the software E-SBC. There are no DSP's on the software E-SBC to support the ringback tones.
- PSTN to CPE Faxes were not validated.
- PSTN to CPE for US, Canada, and MOW were not tested
- In IP DR testing, SIP reason code 480 was returned by SBC, but ADR feature was not invoked. Per investigation by AT&T, the issue was in the network because the response code 480 was missing from the list of codes in which to trigger ADR. The SBC performed correctly under the circumstances.

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 SIP Server in its private network.
- The Mediant 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 IP Toll Free SIP Trunking 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' SIP Server Call Center environment is located on the enterprise's Local Area Network (LAN), the AT&T IP Toll Free SIP Trunks are located on the Wide Area Network (WAN).
- Genesys' SIP Server *and* the AT&T IP Toll Free SIP Trunk use SIP over UDP transport type.
- Genesys' SIP Server *and* AT&T IP Toll Free SIP Trunk support G.729 (preferred) and G711 µ-Law coder types.
- 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: AudioCodes' E-SBC & Genesys Call Center over AT&T IP Toll Free

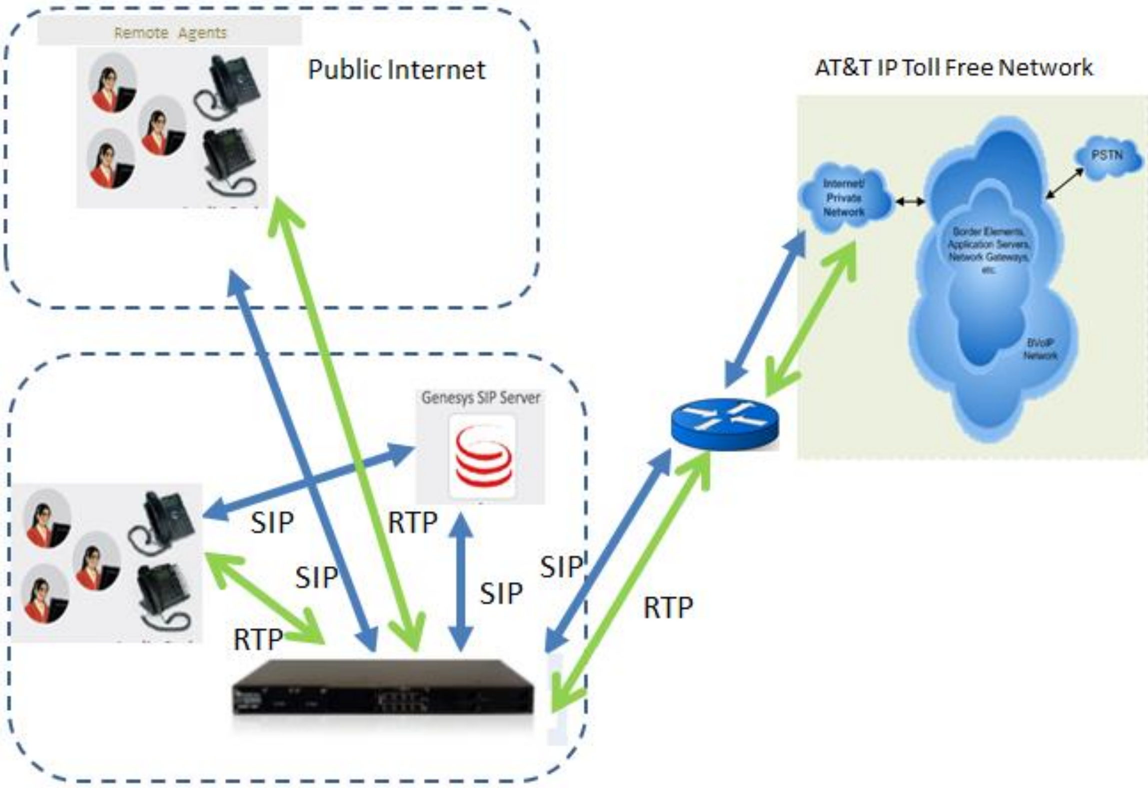
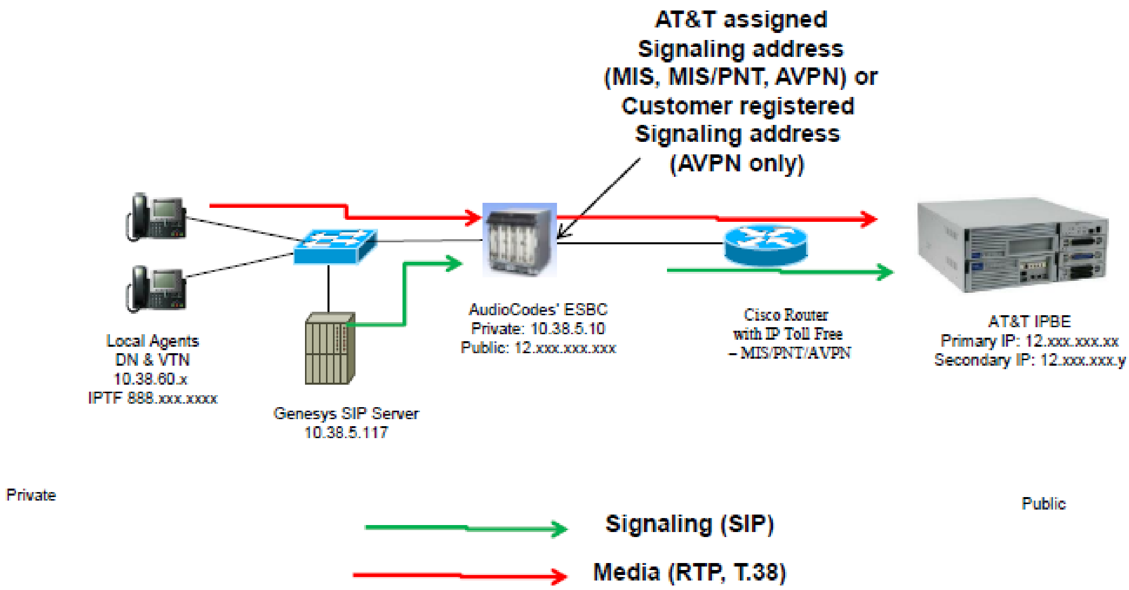


Figure 2-2: Single Combined SIP/Media Address with SBC / AT&T or Customer Registered Address on SBC



3 Configuring Genesys SIP Server

The configuration of the Genesys SIP Server used during certification is detailed in this chapter.

3.1 Genesys SIP Version Information

```
SIP Server, Version: 8.1.000.79 Compiled: Jun 1 2012 10:28:57
Genesys Telecommunications Laboratories, Inc., Copyright 1991 -
2008

Build with Genesys SIP Library 8.1.000.17

Build with Framework 8.1.000.17
Build with TServerCommonPart 8.1.001.43
High Availability feature: ON
ISCC feature support:      ON

Genesys Common Library SE: 8.1.100.09 C2
TServer Library (TLib): 8.1.000.04 HA
      gmessage library: 8.1.100.03
      gservice library: 8.1.100.05 MT
      gthread  library: 8.1.100.04

Config Server support:  CfgLib 8.1.100.08
LCA support:            LCALib 8.1.100.05
License support:        GLMLib 8.1.000.02 MT (FLEXLm 11.9)
Message Server support: LogLib 8.1.100.04 MT
Nonstop Operation:      NSOLib 8.1.001.03 try/catch
SNMP support:          MngmLib 8.1.000.03
```

3.2 Genesys SIP Server Options

```
TServer list
  list  <+M>
    dn-scope = undefined <+D>
    management-port = 0 <+D>
    license list  <+D>
      num-of-licenses = max <+D>
      num-sdn-licenses = max <+D>
    tenant-profile list  <+>
      check-tenant-profile = false <+D>
      @tenant-name = 'Resources' <+>
      @tenant-password = NULL <+D>
    server-id = 102 <+D>
    customer-id = NULL <+D>
    @location = 'rtpsip01sw' <+>
    background-processing = true <+D>
    background-timeout = '60 msec' <+D>
    req-distrib-event-support = no-check <DM>
    extrouter list  <+M>
```

```
      reconnect-tout = '5 sec' <+D>
      request-tout = '20 sec' <+D>
      timeout = '1 min' <+>
      report-connid-changes = false <+D>
      match-call-once = true <+D>
      compound-dn-representation = true <+D>
      use-data-from = current <+D>
      tcs-use = never <+D>
      tcs-queue = NULL <+D>
      cast-type = 'route direct-callid reroute direct-uui direct-
ani direct-notoken dnis-pool direct-digits pullback route-uui
direct-network-callid' <+D>
      register-tout = '2 sec' <+D>
      register-attempts = 5 <+D>
      default-dn = NULL <+D>
      route-dn = NULL <+D>
      dn-for-unexpected-calls = NULL <+D>
      use-implicit-access-numbers = false <+D>
      direct-digits-key = 'CDT_Track_Num' <+D>
      cdt-udata-key -- alias for direct-digits-key
      network-request-timeout = '20 sec' <+D>
      resource-load-maximum = 0 <+D>
      resource-allocation-mode = circular <+D>
      cof-feature = false <+D>
      cof-ci-req-tout = '500 msec' <+D>
      cof-rci-tout = '10 sec' <+D>
      cof-ci-wait-all = false <+D>
      cof-ci-defer-delete = '0' <+D>
      cof-ci-defer-create = '0' <+D>
      default-network-call-id-matching = NULL <+D>
      event-propagation = list <+D>
      epp-tout = '0' <+>
      inbound-translator-%d array
    backup-sync list  <+D>
      sync-reconnect-tout = '20 sec' <+D>
      protocol = 'default' <+D>
      addp-timeout = 0 <+D>
      addp-remote-timeout = 0 <+D>
      addp-trace = 'off' <+D>
    @server-name = 'rtpsip01' <+>
    consult-user-data = separate <+D>
    user-data-limit = 16000 <+D>
    propagated-call-type = false <+D>
    merged-user-data = main-only <+D>
    merge-consult-data -- alias for merged-user-data
    ani-distribution = inbound-calls-only <+D>
    call-cleanup list  <+D>
      notify-idle-tout = '0' <+D>
      cleanup-idle-tout = '0' <+D>
      periodic-check-tout = '10 min' <+D>
    agent-reservation list  <+>
      request-collection-time = '100 msec' <+D>
```

```
      reservation-time = '10 sec' <+>
      reject-subsequent-request = true <+D>
      collect-lower-priority-requests = true <+D>
    agent-logout-reassoc = false <+D>
    unknown-xfer-merge-udata = false <+D>
    clid-withheld-name = 'PRIVATE' <+D>
    releasing-party-report = false <+D>
    agent-group = NULL <+D>
    link-control list  <+DM>
      restart-cleanup-limit = 0 <+D>
      restart-cleanup-dly = 0 <+D>
      quiet-cleanup = false <+D>
      quiet-startup = false <+D>
      ha-sync-dly-lnk-conn = false <+D>
      reg-delay = 10 <+D>
      reg-silent = true <+D>
      use-link-bandwidth = 'auto' <+D>
      link-alarm-high = 0 <+D>
      link-alarm-low = 0 <+D>
    agent-strict-id = false <+D>
    untimed-wrap-up-value = 1000 <+D>
    wrap-up-threshold = 0 <+D>
    inbound-bsns-calls = false <+D>
    outbound-bsns-calls = false <+D>
    internal-bsns-calls = false <+D>
    unknown-bsns-calls = false <+D>
    bsns-call-dev-types = 0xF = +acdq +rp +rpq +xrp <+D>
    timed-acw-in-idle = true <+D>
    timed-cwk-in-idle -- alias for timed-acw-in-idle
    acw-in-idle-force-ready = true <+D>
    cwk-in-idle-force-ready -- alias for acw-in-idle-force-ready
    inherit-bsns-type = false <+D>
    agent-only-private-calls = false <+D>
    backwds-compat-acw-behavior = false <+D>
    override-switch-acw = false <+D>
    extn-no-answer-timeout = 15 <+D>
    posn-no-answer-timeout = 15 <+D>
    agent-no-answer-timeout = 15 <+D>
    extn-no-answer-overflow = NULL <+D>
    posn-no-answer-overflow = NULL <+D>
    agent-no-answer-overflow = NULL <+D>
    agent-no-answer-action = none <+D>
    nas-private = false <+D>
    recall-no-answer-timeout = 15 <+D>
    nas-indication = none <+D>
    prd-dist-call-ans-time = 0 <+D>
    max-pred-req-delay = 3 <+D>
    accept-dn-type = 0x11F = +extension +position +acdqueue
+routedn +trunk +routequeue <+D>
    default-dn-type = none <+D>
    dn-del-mode = 'never' <+D>
    route-failure-alarm-high-wm = '10' <+D>
```

```
    route-failure-alarm-low-wm = '1' <+D>
    route-failure-alarm-period = 0 <+D>
    emulate-login = on-RP <+D>
    emulated-login-state = ready <+D>
    wrap-up-time = '0' <+D>
    legal-guard-time = '0' <+D>
    sync-emu-agent = false <+D>
    agent-logout-on-unreg = false <+D>
    agent-emu-login-on-call = false <+D>
    rq-expire-tmout = 0 <+D>
    logout-on-out-of-service = false <+D>
    mwi-host = NULL <+D>
    mwi-domain = NULL <+D>
    sip-tls-cert = NULL <+D>
    sip-tls-cert-key = NULL <+D>
    sip-tls-trusted-ca = NULL <+D>
    sip-tls-crl = NULL <+D>
    sip-tls-cipher-list = NULL <+D>
    sip-tls-target-name-check = NULL <+D>
    make-call-alert-info = '' <+D>
    sip-alert-info = '' <+D>
    sip-alert-info-external = '' <+D>
    sip-alert-info-consult = '' <+D>
    default-music = 'music/on_hold' <+D>
    music-in-conference-file = '' <+D>
    parking-music = 'music/silence' <+D>
    ring-tone = 'music/ring_back' <+D>
    busy-tone = 'music/busy_5sec' <+D>
    fast-busy-tone = 'music/atb_5sec' <+D>
    silence-tone = 'music/silence' <+D>
    collect-tone = 'music/collect' <+D>
    music-in-queue-file = NULL <+D>
    ims-default-orig-ioi = NULL <+D>
    ims-default-icid-suffix = NULL <+D>
    ims-default-icid-prefix = NULL <+D>
    ims-route = NULL <+D>
    ims-sip-domain = NULL <+D>
    ims-sip-params = NULL <+D>
    ims-puid-domain = NULL <+D>
    p-asserted-identity = NULL <+D>
    privacy = NULL <+D>
    ims-skip-ifc = NULL <+D>
    ims-3pcc-prefix = NULL <+D>
    sip-address-srv = NULL <+D>
    userdata-map-trans-prefix = NULL <+D>
    partition-id = 'SipServerDefaultPartition' <+D>
    dial-plan = 'outbound' <+>
    cos = NULL <+D>
    info-pass-through = '' <+D>
    subscription-event-allowed = NULL <+D>
    encoding = NULL <+D>
    sip-hold-rfc3264 = 'false' <+D>
```

```
    sip-error-conversion = NULL <+D>
    sip-pass-from-parameters = NULL <+D>
    audio-codecs = 'telephone-event,PCMU,PCMA,G723,G729,GSM' <+D>
    sip-address = NULL <+D>
    internal-registrar-domains = NULL <+D>
    sip-block-headers = NULL <+D>
    enforce-external-domains = NULL <+D>
    external-registrar = NULL <+D>
    mwi-implicit-notify = NULL <+D>
    default-route-point = NULL <+D>
    sip-pass-refer-headers = NULL <+D>
    dr-peer-trunk = NULL <+D>
    sip-server-info = NULL <DM>
    sip-user-agent = NULL <DM>
    sip-enable-gdns = true <+D>
    sip-enable-moh = false <+D>
    sip-enable-100rel = true <+D>
    ringing-on-route-point = true <+D>
    divert-on-ringing = true <+D>
    sip-enable-sdp-application-filter = false <+D>
    sip-enable-sdp-codec-filter = false <+D>
    sip-treatment-dtmf-interruptable = false <+D>
    enable-ims = false <+D>
    ims-propagate-pcvector = false <+D>
    internal-registrar-enabled = true <+D>
    override-to-on-divert = false <+D>
    internal-registrar-persistent = true <+>
    mwi-extension-enable = false <+D>
    mwi-agent-enable = false <+D>
    mwi-group-enable = false <+D>
    mwi-notify-unregistered-dn = false <DM>
    find-trunk-by-location = false <+D>
    event-ringing-on-100trying = false <+D>
    emergency-recording-cleanup-enabled = false <+D>
    use-display-name = false <+D>
    init-dnis-by-ruri = false <+D>
    sip-proxy-headers-enabled = true <+D>
    sip-dtmf-send-rtp = false <+D>
    sip-enable-call-info = false <+D>
    enable-unknown-gateway = true <+>
    refer-enabled = false <+>
    sip-preserve-contact = false <+D>
    msml-support = false <+D>
    msml-record-support = false <+D>
    resource-management-by-rm = true <+D>
    record-consult-calls = false <+D>
    sip-tls-mutual = false <+D>
    sip-timer-c-support = false <+D>
    reason-in-extension = true <+D>
    sip-491-passthrough = false <+D>
    mwi-port = 5060 <+D>
    session-refresh-interval = 1800 <+D>
```

```
    sip-port = 5060 <+D>
    sip-port-tls = 0 <+D>
    dtmf-payload = 101 <+D>
    max-legs-per-sm = 0 <+D>
    server-role = 0 <+D>
    subscription-timeout = 180 <+D>
    subscription-delay = 0 <+D>
    registrar-default-timeout = 0 <+D>
    sip-invite-timeout = 0 <+D>
    sip-invite-treatment-timeout = 0 <+D>
    sip-call-retain-timeout = 1 <+D>
    cpd-info-timeout = 3 <+D>
    sip-ring-tone-mode = 0 <+D>
    sip-replaces-mode = 0 <+D>
    sip-ip-tos = 256 <+D>
    sip-retry-timeout = 30 <+D>
    busy-tone-duration = 5 <+D>
    sip-link-type = 0 <+D>
    overload-ctrl-threshold = 0 <+D>
    overload-ctrl-dialog-rate-capacity = 400 <+D>
    overload-ctrl-call-rate-capacity = 200 <+D>
    sip-max-retry-listen = 15 <+D>
    sip-pass-check = false <+D>
    enforce-trusted = true <+D>
    sip-from-pass-through = false <+D>
    mwi-mode = SUBSCRIBE <+D>
    Greetings: list  <+DM>
      greeting-repeat-once-party = agent <+D>
      greeting-delay-events = none <+D>
      greeting-call-type-filter = 0x0 = -internal -consult <+D>
      greeting-notification = 0x0 = -started -complete <+D>
      greeting-after-merge = false <+D>
    send-200-on-clear-call = true <+D>
    sip-max-uui-length = 256 <+D>
    tlib-map-replace-dn = false <+D>
    blind-transfer-enabled = false <+D>
    sip-respect-privacy = true <+D>
    resolve-sip-address = false <+D>
    record-after-merge = false <+D>
    sip-add-contact-early-dialog = false <DM>
    dr-forward = off <+D>
    sip-enable-rfc3263 = false <+D>
    shutdown-sip-reject-code = 603 <+D>
    INVITE list
      extensions-%d array
      userdata-%d array
    UPDATE list
      extensions-%d array
      userdata-%d array
    INFO list
      extensions-%d array
      userdata-%d array
```

```
    REFER list
      extensions-%d array
      userdata-%d array
    BYE list
      userdata-%d array
    userdata-map-all-calls = false <+D>
    sip-legacy-invite-retr-interval = false <+D>
    sip-referxfer-bye-timeout = 0 <+D>
    drop-nailedup-on-logout = false <+D>
    cancel-monitor-on-unpark = true <DM>
    call-observer-with-hold = false <DM>
    enable-busy-on-routed-calls = true <DM>
    observing-routing-point = NULL <+D>
    default-dn = NULL <+D>
    router-timeout = 10 <+D>
    after-routing-timeout = 10 <+D>
    set-notready-on-busy = false <+D>
    am-detected = drop <+D>
    fax-detected = drop <+D>
    silence-detected = drop <+D>
    cancel-monitor-on-disconnect = true <+D>
    logout-on-disconnect = true <+D>
    predictive-call-router-timeout = 0 <+D>
    preview-expired = 90 <+D>
    intrusion-enabled = true <+D>
    monitor-internal-calls = true <+D>
    default-monitor-scope = call <+D>
    default-monitor-mode = mute <+D>
    monitor-consult-calls = false <+D>
    use-propagated-call-type = never <DM>
    sip-treatments-continuous = false <+D>
    map-sip-errors = true <+D>
    SipErrorMap list
      sip-%d array
    stranded-calls-overflow = NULL <+D>
    stranded-on-arrival-calls-overflow = NULL <+D>
    stranded-call-redirection-limit = 4 <+D>
    forced-notready = true <+D>
    default-video-file = '' <+D>
    emergency-recording-filename = NULL <+D>
    recording-filename = NULL <+D>
    restart-period = 20 <+D>
    rq-expire-tout = 0 <+D>
    rq-expire-tmout -- alias for rq-expire-tout
    reg-interval = 60 <+D>
    kpl-interval = 10 <+D>
    kpl-tolerance = 3 <+D>
    kpl-loss-rate = '10,100' <+D>
    call-rq-gap = 0 <+D>
    device-rq-gap = 0 <+D>
    rq-conflict-check = true <+D>
    backup-mode = none <+D>
```

```
    correct-rqid = false <+D>
    convert-otherdn = 0x7 = +agentid +reserveddn +fwd <+D>
    auto-logout-timeout = 0 <+D>
    auto-logout-ready = false <+D>
    call-type-rules list
      rule-%d array
    log-trace-flags = 0x7FF0000 = +iscc +cfg$dn +cfgserv +passwd
+udata +devlink +sw +req +callops +conn +client <+>
  physical-switch array
    rtp [101] cfgtype = 72
  locally-scoped-dn array
  backup-server-%d array
  remote-server-%d array
  AgentLogin array
  DN array
    outbound [153] dn = 'outbound' type = VoIPService xtype =
Other cfgtype = 29 sstype = 1 register-flag = true
    9xxxxxxxx0 [158] dn = '9xxxxxxxx0' type = Extension xtype = DN
cfgtype = 1 sstype = 1 reg-mode = 0x21 = +force register-flag =
true
    9xxxxxxxx1 [159] dn = '9xxxxxxxx1' type = Extension xtype = DN
cfgtype = 1 sstype = 1 reg-mode = 0x21 = +force register-flag =
true
    9xxxxxxxx2 [160] dn = '9xxxxxxxx2' type = Extension xtype = DN
cfgtype = 1 sstype = 1 reg-mode = 0x21 = +force register-flag =
true
    9xxxxxxxx3 [161] dn = '9xxxxxxxx3' type = Extension xtype = DN
cfgtype = 1 sstype = 1 reg-mode = 0x21 = +force register-flag =
true
    sip-off-net [187] dn = 'sip-off-net' type = TRUNK xtype =
Trunk cfgtype = 14 sstype = 1 register-flag = true
    2xxxxxxxx5 [269] dn = '2xxxxxxxx5' type = Extension xtype = DN
cfgtype = 1 sstype = 1 reg-mode = 0x21 = +force register-flag =
true
    9xxxxxxx71 [270] dn = '9xxxxxxx71' type = Extension xtype = DN
cfgtype = 1 sstype = 1 reg-mode = 0x21 = +force register-flag =
true
  DN/EXR array
    [-1] cdn = 'direct' type = N/A reg-mode = 0x0 =
      access-list array
      linked-resources array
```

3.3 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.

3.3.1 AudioCodes 320HD IP Phone

3.3.1.1 Firmware Version

SIP = 320HD_1.6.0_build_37_4

3.3.1.2 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=9xxxxxxxxx
voip/line/0/description=320hd3623
voip/line/0/auth_name=9xxxxxxxxx
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.gch.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=xx00
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
```

3.3.2 Polycom SoundPoint IP 650

3.3.2.1 Firmware version

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

3.3.2.2 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='xxxxxxxxxx@angel.z101.gch.com'
          reg.1.auth.password='xxxxxx'
          reg.1.auth.userId='xxxxxxxxxx'
          reg.1.displayName='xxxxxxxxxx'
          reg.1.label='xxxxxxxxxx'
          voIpProt.server.1.address='angel.z101.gch.com'
          voIpProt.server.1.port='5060'
          voIpProt.server.1.transport='UDPOnly'
    />
</PHONE_CONFIG>
```

Reader's Notes

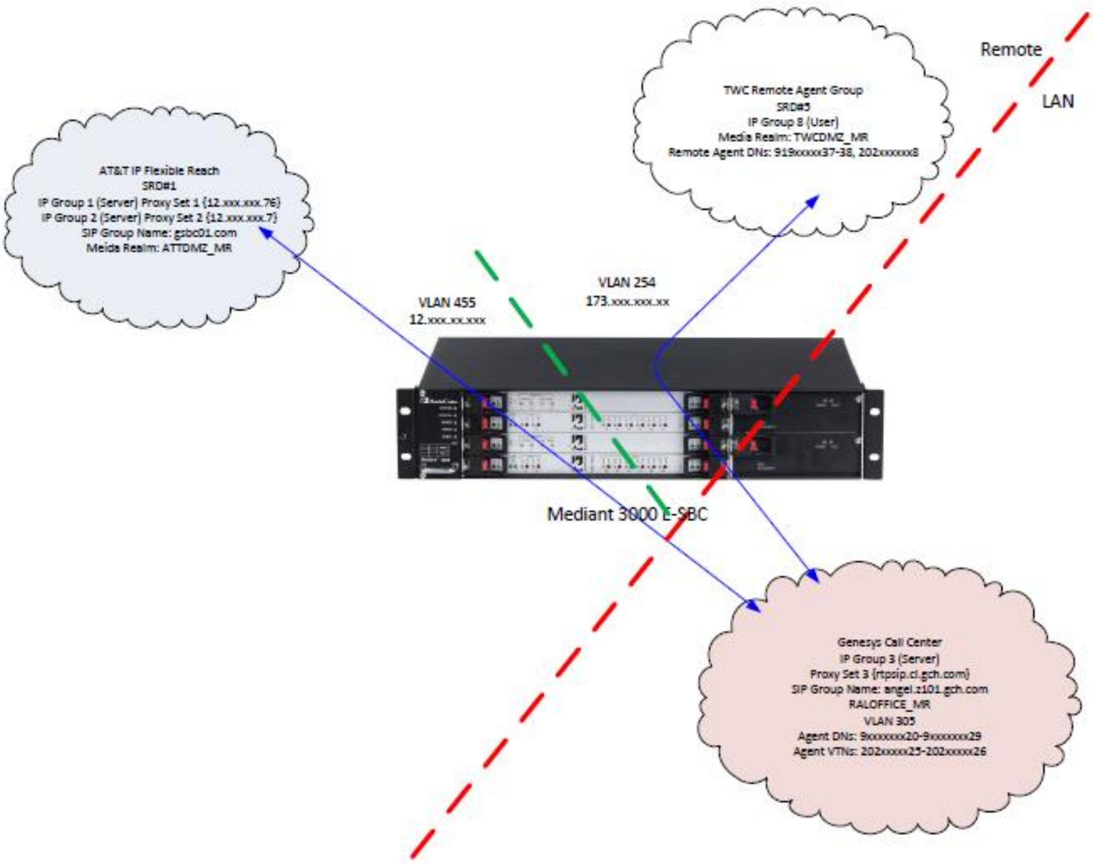
4 Configuring the Mediant E-SBC

This section describes the configuration of the Mediant 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 E-SBC SIP User's Manual*.

Figure 4-1: E-SBC Interfaces/Configuration



4.1 Basic Configuration via the Web GUI

Take these steps to configure the Mediant 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

4.1.1 Configure the Multiple Interface Table

This section describes how to configure the Multiple Interface Table for the different logical networks used to connect AT&T IP Toll Free SIP Trunking Service, 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 Installation Guide* or *User's Manual*).

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

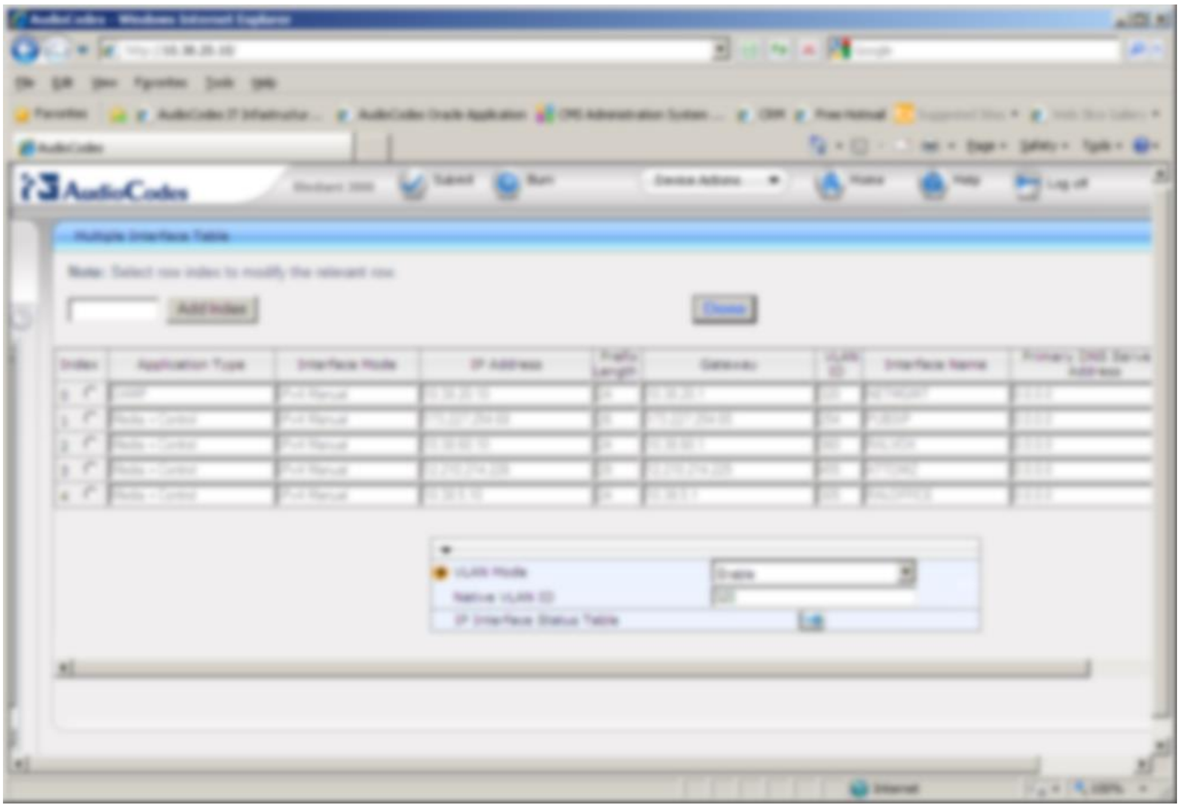
- 'NETMGMT' is the OAMP interface for all management of the E-SBC. This was VLAN 320 in the certification environment.
- 'PUBSIP' is the Media + Control interface to a public domain on which Remote Agents or Customers may exist. This was VLAN 254 in the certification environment.
- 'RALVOX' is the Media + 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 AT&T IP Toll Free 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 SIP Server resides. Outbound SIP messaging routes 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 4-2: Configuring the Multiple Interface Table



4.1.2 Configure DNS/SRV Tables

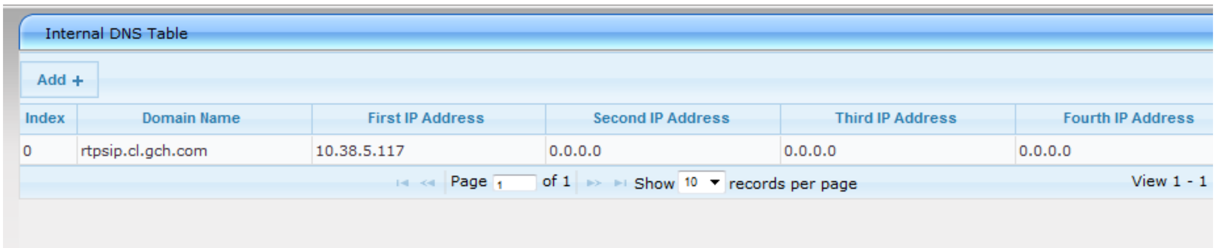
The Mediant E-SBC features the capability of translating domain names into IP addresses via an external, third-party Domain Name Server (DNS), as defined in the Multiple Interface Table, or by the device's embedded DNS. Two DNS types are supported on the device: an Internal DNS table and an Internal 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 SIP User's 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 4-3: Internal DNS Table



Internal DNS Table

Add +

Index	Domain Name	First IP Address	Second IP Address	Third IP Address	Fourth IP Address
0	rtpsip.cl.gch.com	10.38.5.117	0.0.0.0	0.0.0.0	0.0.0.0

Page 1 of 1 Show 10 records per page View 1 - 1

4.1.3 Configure Firewall Settings

The Mediant 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

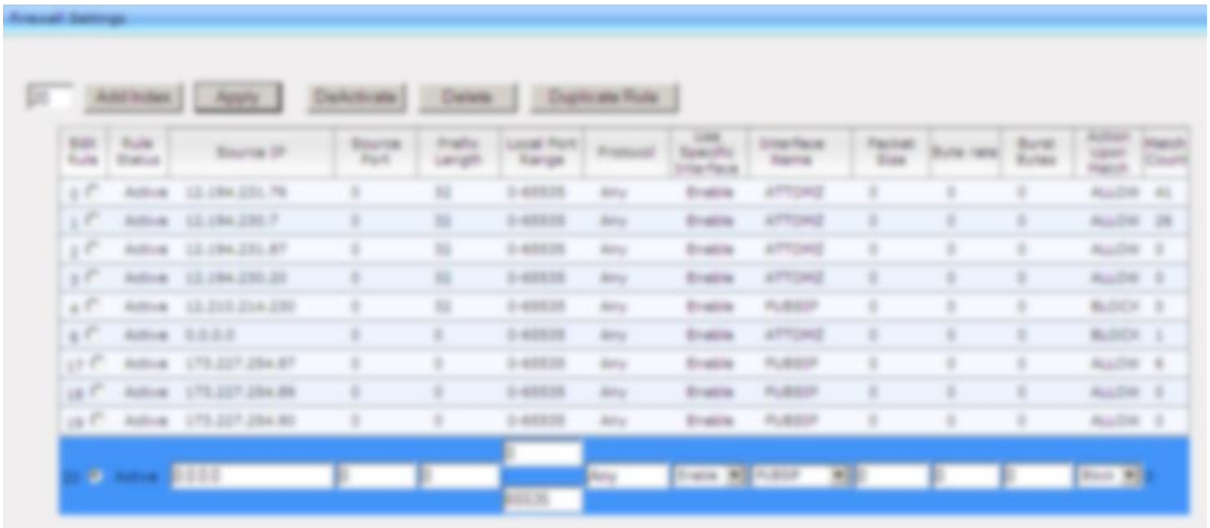
For each packet received on the network interface, the table is scanned from the top down until a matching rule is found. The rule can either deny (block) or permit (allow) the packet. Once a rule in the table is located, subsequent rules are ignored. If the end is reached without a match, the packet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

See the *Mediant 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 4-4: Firewall Settings



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.xxx.xxx.x (Primary AT&T IP Toll Free Border Element), on any port is allowed on the ATTDMZ interface.
- Rule #1: traffic from the host 12.xxx.xxx.y (Secondary AT&T IP Toll Free Border Element), on any port is allowed on the ATTDMZ interface.
- Rule #2: traffic from the host 12.xxx.xxx.z (AT&T Media Portal), on any port is allowed on the ATTDMZ interface.

- Rule #3: traffic from the host 12.xxx.xxx.a (AT&T Media Portal), on any port is allowed on the ATTDMZ interface.
- Rule #4: traffic from the host 12.xxx.xxx.b (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.xxx.xxx.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'
- Acton Upon Match 'block'

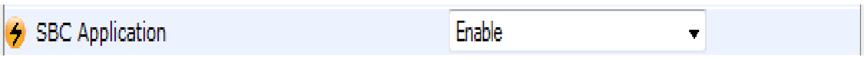
4.1.4 Enable the SBC Application

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

➢ **To enable the SBC application on the Mediant 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 4-5: 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.

4.1.5 Configure the Number of Media Channels

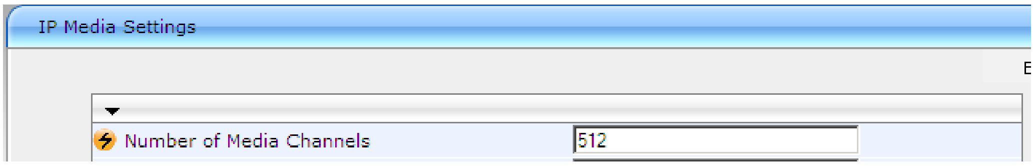
The SBC application does not require DSP channels. It only requires DSP channels if media transcoding is needed, where two DSP channels are used per transcoding session. No media transcoding was utilized in the AT&T/Genesys/AudioCodes certification testing.

Note: This step is required **only** if transcoding is required.

➢ **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 4-6: IP Media Settings



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 SIP Server).
- If media transcoding is required, two DSP channels are used per transcoding session.
- The maximum is also subject to the 'Feature Key' setting.

4.1.6 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 4-7 below)
2. 'RALVOX_SRD' (see Figure 4-8 below)
3. 'RALOFFICE_SRD' (see Figure 4-9 below)
4. 'TWCDMZ_IPP' (see Figure 4-10 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 4-7: ATTDMZ_SRD

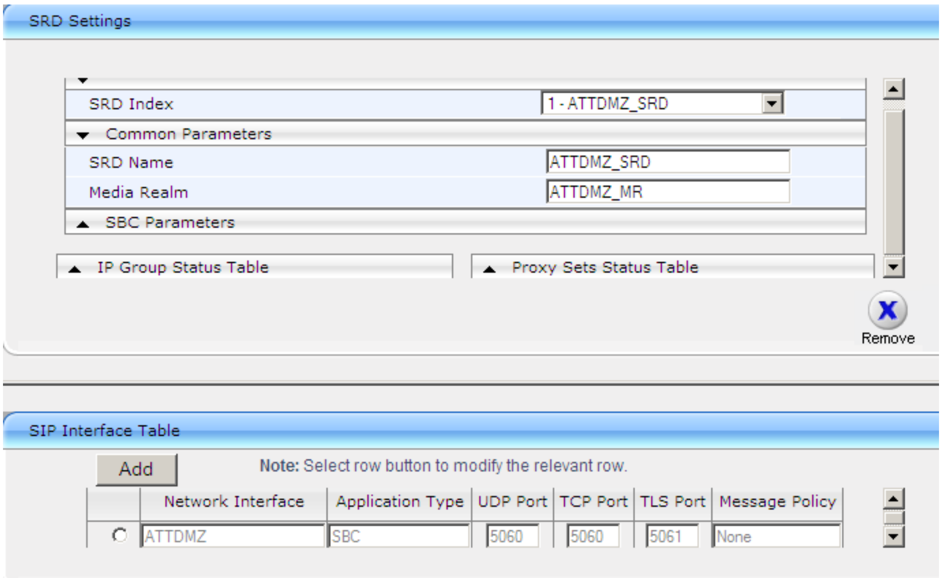


Figure 4-8: RALVOX_SRD

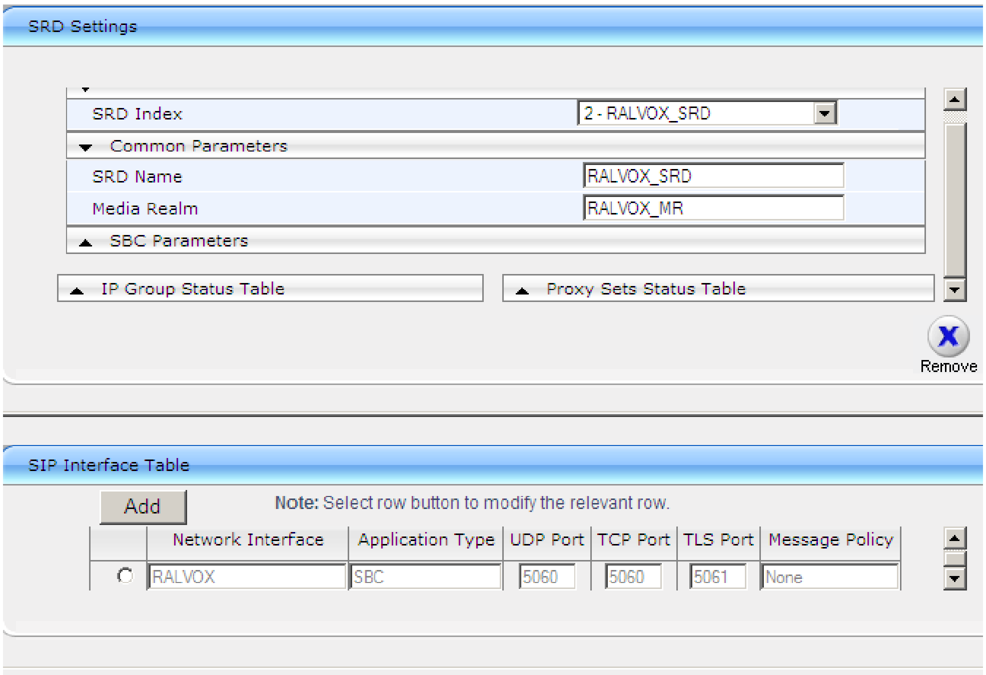


Figure 4-9: RALOFFICE_SRD

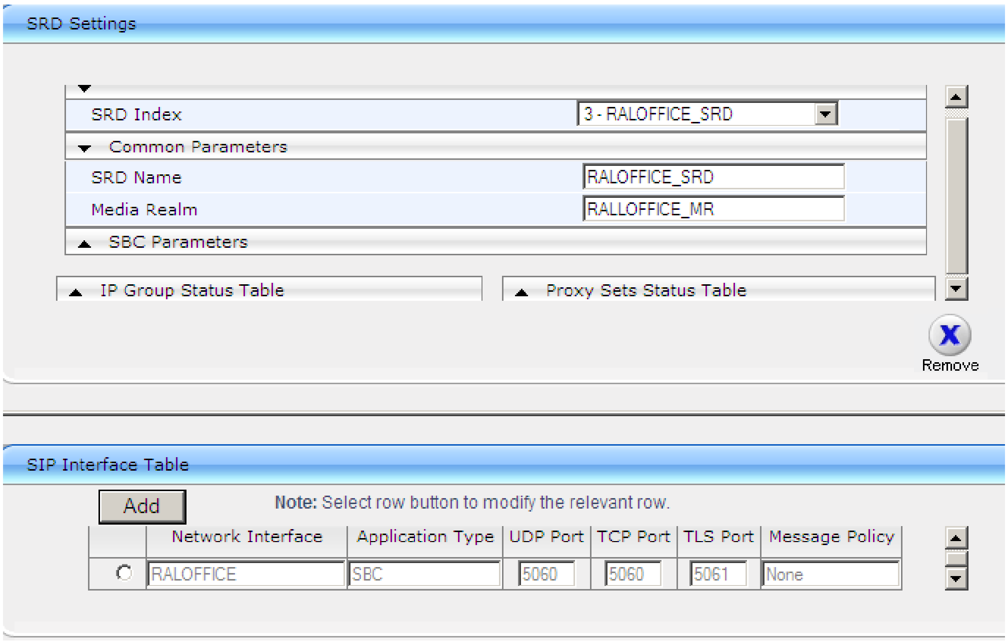
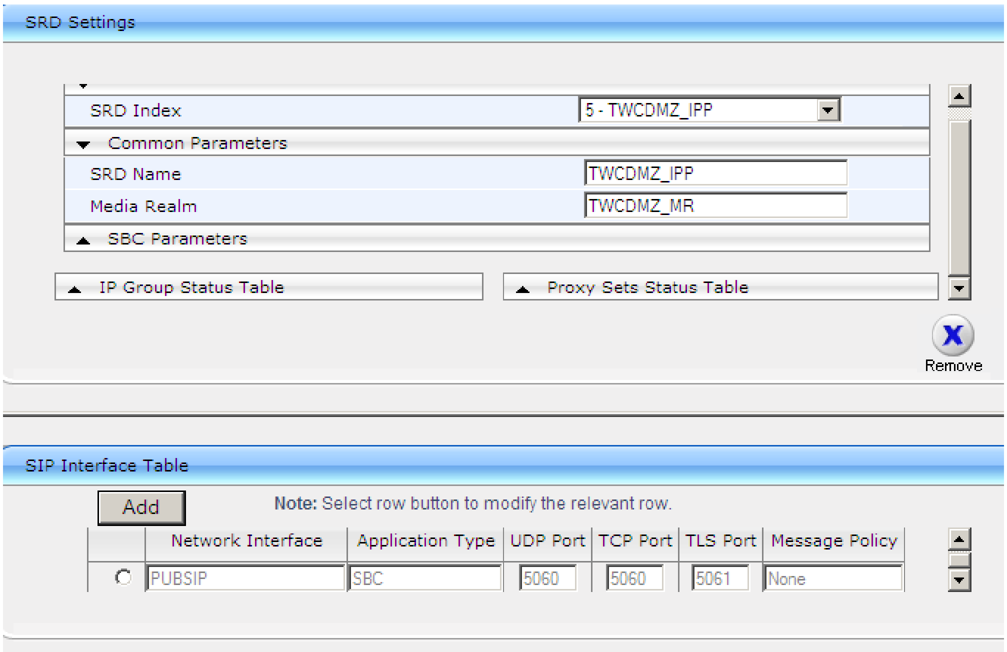


Figure 4-10: TWCDMZ_IPP



4.1.7 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 example 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. ATTDMZ_MR - the interface out to the AT&T IP Toll Free Border Element 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.

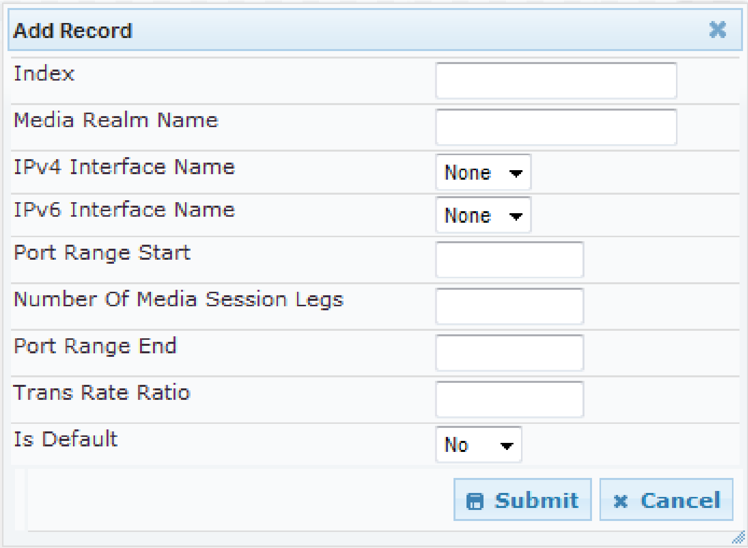
Note:

- 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:**

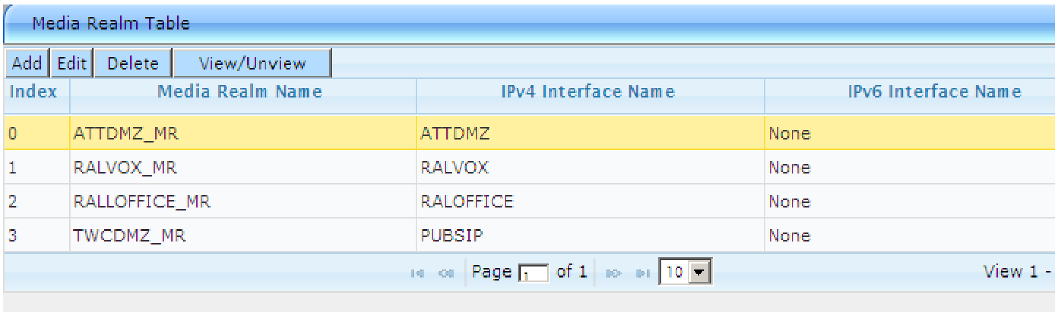
1. Open the Media Realm Table page (**Configuration** > **VoIP** > **Media** > **Media Realm Configuration**).
2. Click the **Add** button; the following appears:

Figure 4-11: Add Record Dialog Box



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 4-12: SIP Interface Table



Media Realm Table

Add | Edit | Delete | View/Unview

Index	Media Realm Name	IPv4 Interface Name	IPv6 Interface Name
0	ATTDMZ_MR	ATTDMZ	None
1	RALVOX_MR	RALVOX	None
2	RALLOFFICE_MR	RALOFFICE	None
3	TWCDMZ_MR	PUBSIP	None

Page 1 of 1 10 View 1 -

Figure 4-13: Media Realm #0

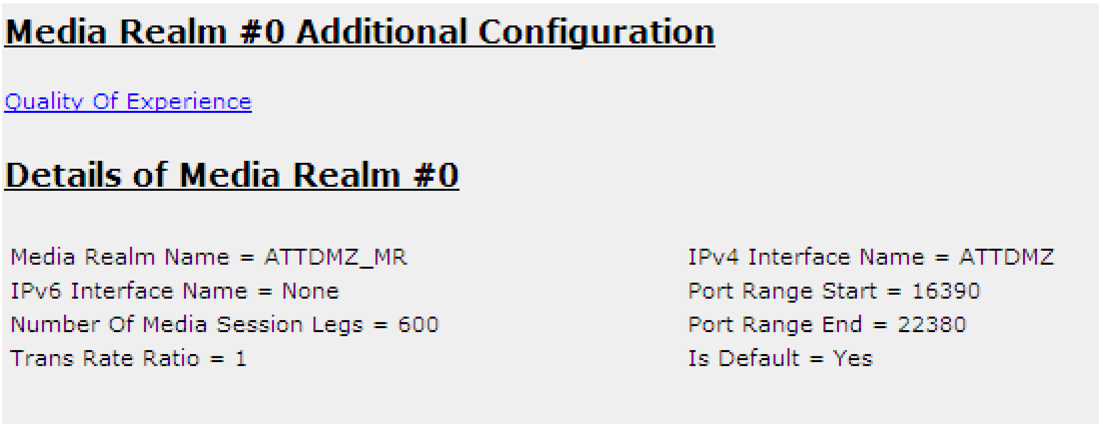


Figure 4-14: Media Realm #1

Media Realm #1 Additional Configuration

Quality Of Experience

Details of Media Realm #1

Media Realm Name = RALVOX_MR	IPv4 Interface Name = RALVOX
IPv6 Interface Name = None	Port Range Start = 6000
Number Of Media Session Legs = 50	Port Range End = 6490
Trans Rate Ratio = 1	Is Default = No

Figure 4-15: Media Realm #2

Media Realm #2 Additional Configuration

Quality Of Experience

Details of Media Realm #2

Media Realm Name = RALLOFFICE_MR	IPv4 Interface Name = RALOFFICE
IPv6 Interface Name = None	Port Range Start = 6500
Number Of Media Session Legs = 550	Port Range End = 11990
Trans Rate Ratio = 1	Is Default = No

Figure 4-16: Media Realm #3

Media Realm #3 Additional Configuration

Quality Of Experience

Details of Media Realm #3

Media Realm Name = TWCDMZ_MR	IPv4 Interface Name = PUBSIP
IPv6 Interface Name = None	Port Range Start = 12000
Number Of Media Session Legs = 100	Port Range End = 12990
Trans Rate Ratio = 0	Is Default = No

4.1.8 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).

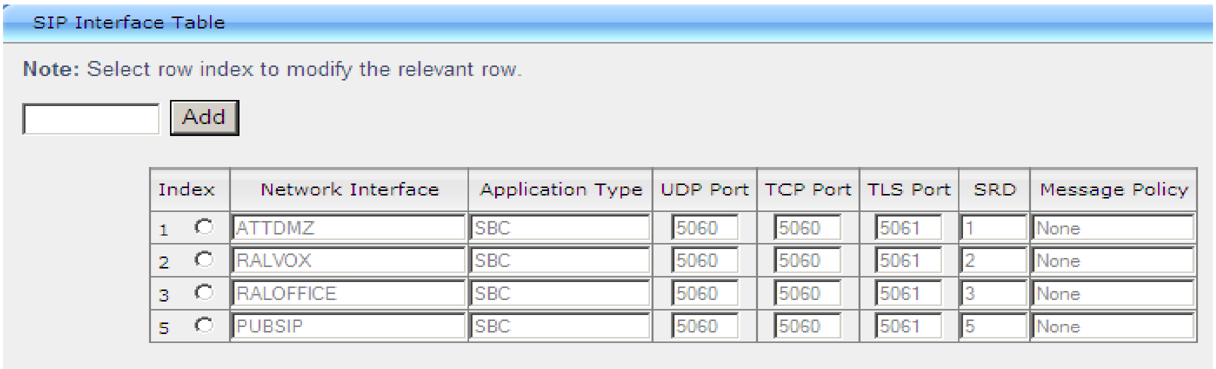
In this example configuration, there were four SIP interfaces (pathways for which SIP signaling will travel):

1. ATTDMZ - the interface out to the AT&T IP Toll Free Border Element 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 4-17: SIP Interface Table


SIP Interface Table

Note: Select row index to modify the relevant row.

Add

Index		Network Interface	Application Type	UDP Port	TCP Port	TLS Port	SRD	Message Policy
1	○	ATTDMZ	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

4.1.9 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 Toll Free Service SIP trunk (relates to the IPBE)
2. IP Group 2: AT&T IP Toll Free Service 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 must not 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 AT&T IP Toll Free Service 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.

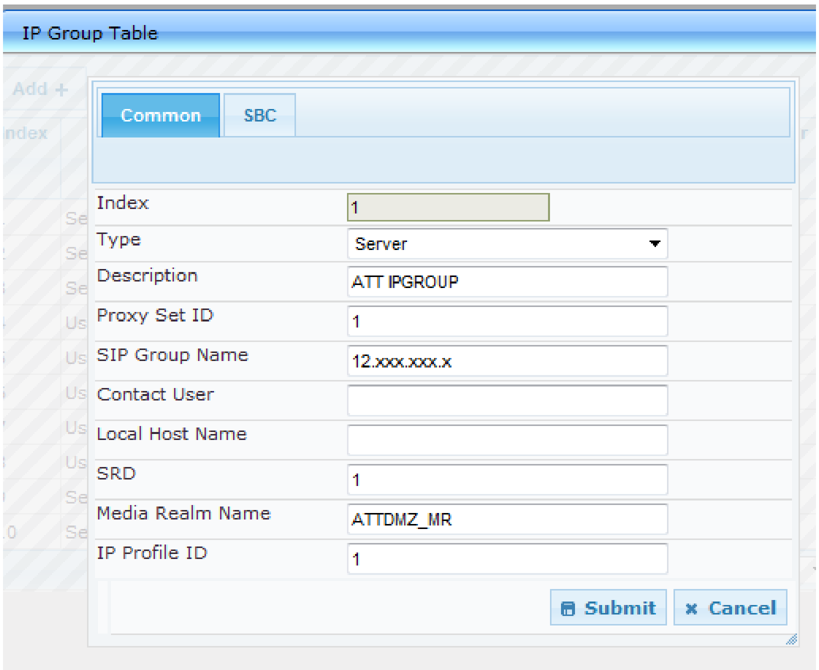
h. Media Realm: 'ATTDMZ_MR' - Assigns Media Realm to the IP Group. Must be identical to the Media Realm name in the Media Realm table.

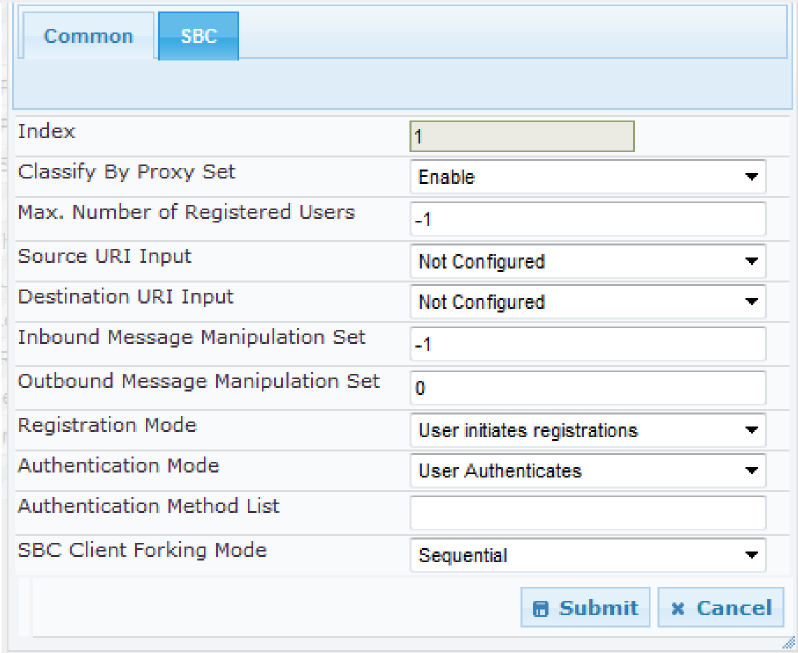
i. IP Profile ID: '1' – the IP Profile to be assigned to this IP group.

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).

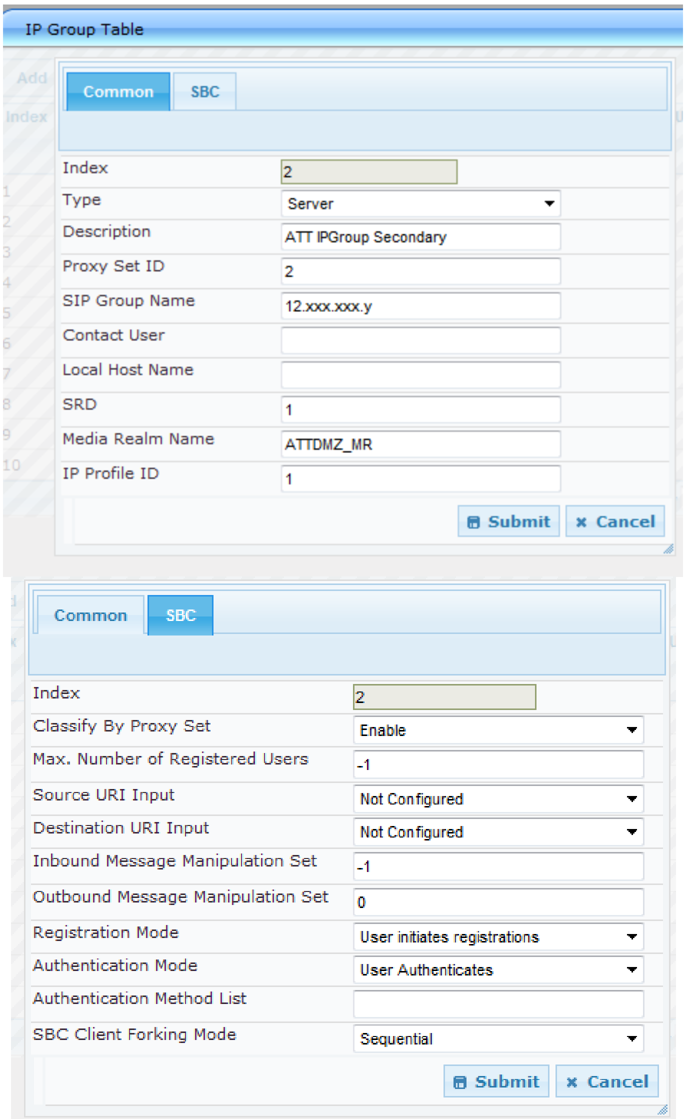
Figure 4-18: ATT IP Group 1 (SERVER)





3. Define IP Group #2 for the AT&T IP Toll Free Service’s 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: 'ATTDMZ_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 4-19: ATT Secondary IP Group 2 (SERVER)

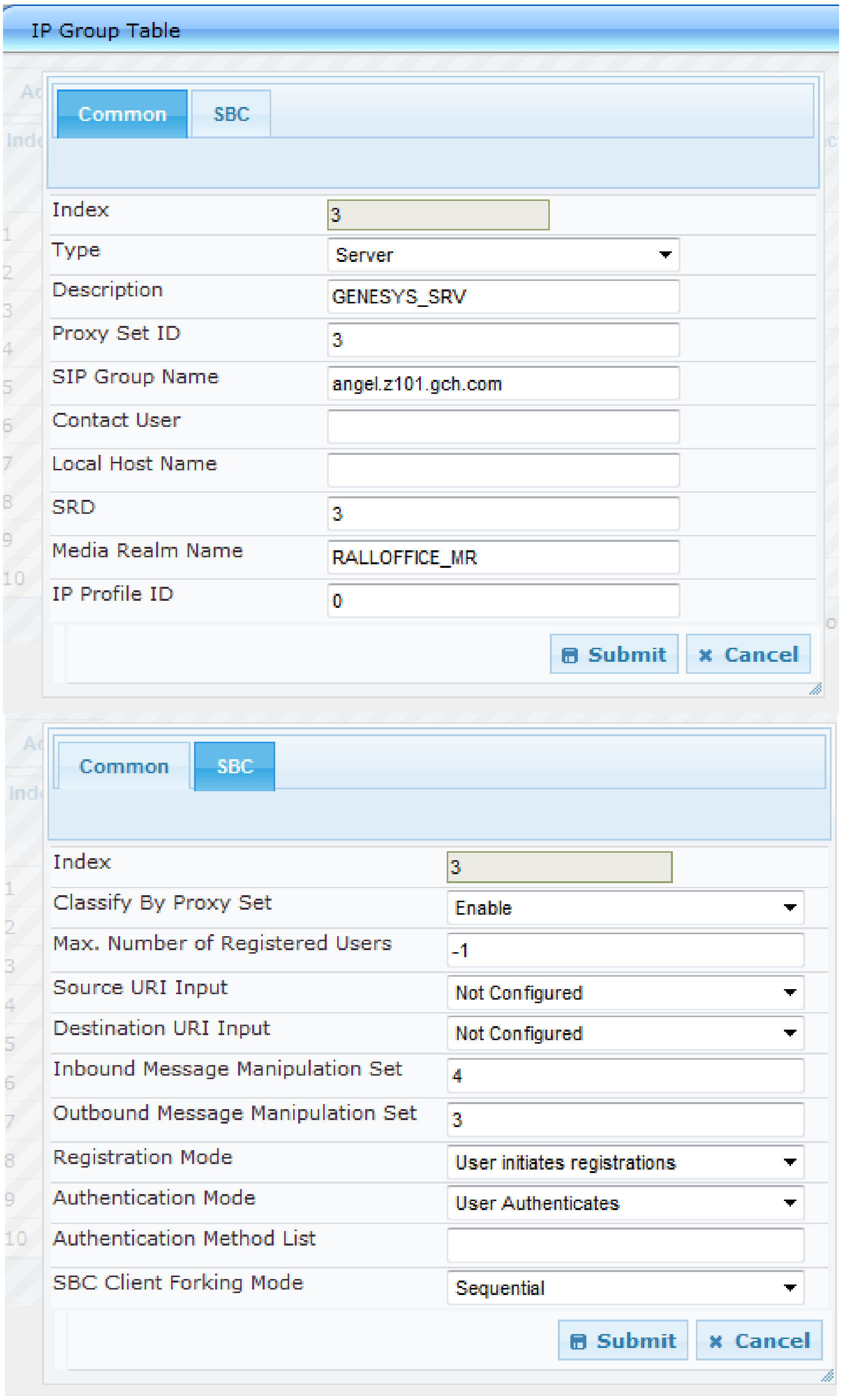


4. Define IP Group #3 for the Genesys SIP Server as follows:
   a. IP Group Index ‘3’
   b. Type: 'SERVER' (used when the destination address (configured by the Proxy Set) of the IP Group (e.g. ITSP, Proxy, IP-PBX, or Application Server) is known.
   c. Description: arbitrary name. (e.g., 'GENESYS_SRV')
   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 4-20: Genesys Server IP Group 3



5. Define IP Group #7 for Remote Agents in the AT&T network as follows:

k. IP Group Index '7'

l. 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.

m. Description: arbitrary name. (e.g., 'ATT Remote Agents')

n. Proxy Set ID: N/A (only applies to Type 'SERVER').

o. 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.

p. SRD: '1' – the SRD associated with this group of IP phones.

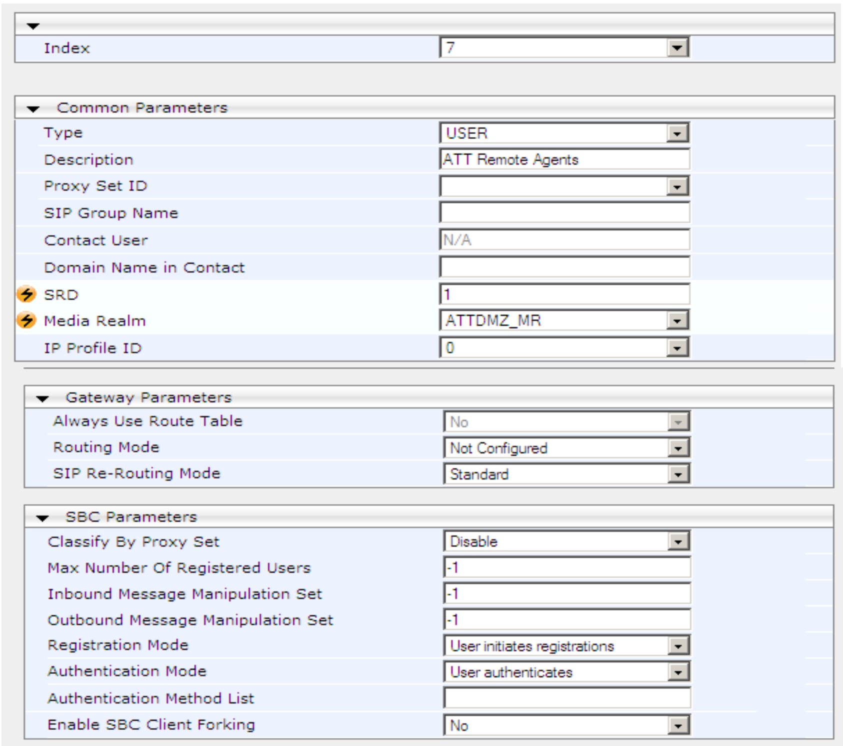
q. Media Realm: 'ATTDMZ_MR' - Assigns Media Realm to the IP Group. Must be identical to the Media Realm name in the Media Realm table.

r. IP Profile ID: '0' (default)

s. 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.

t. Outbound Message Manipulation Set: '-1' (default) No manipulations are required to the Remote Agents

Figure 4-21: AT&T Remote Agents IP Group 7



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

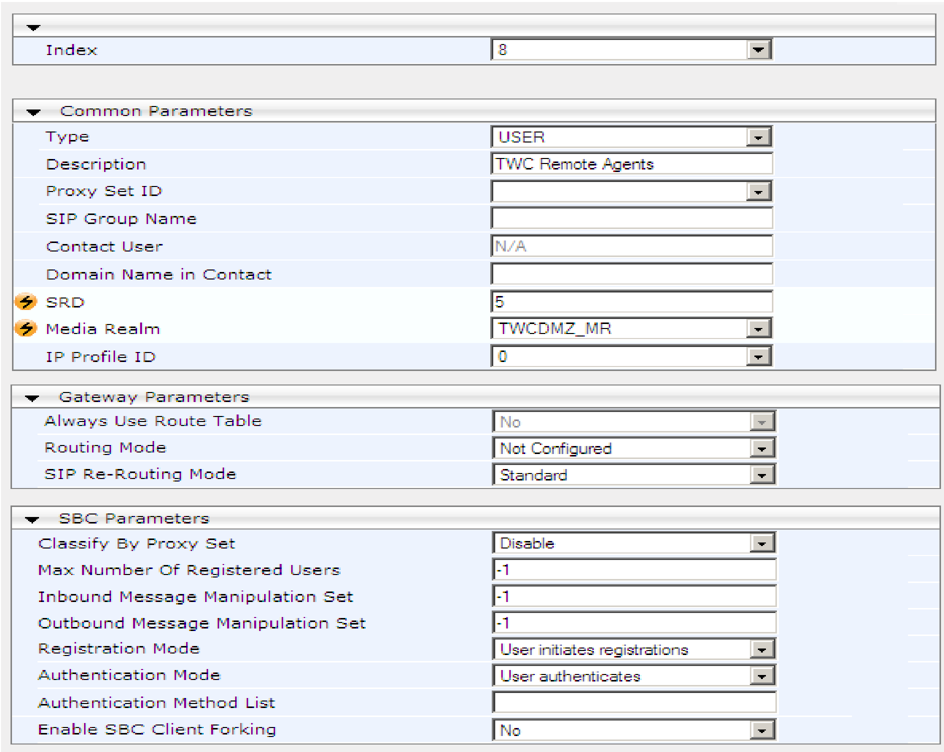
g. Media Realm: 'TWCDMZ_MR' - Assigns Media Realm to the IP Group. Must be identical to the Media Realm name in the Media Realm table.

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 4-22: Non-AT&T Remote Agents IP Group 8



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.

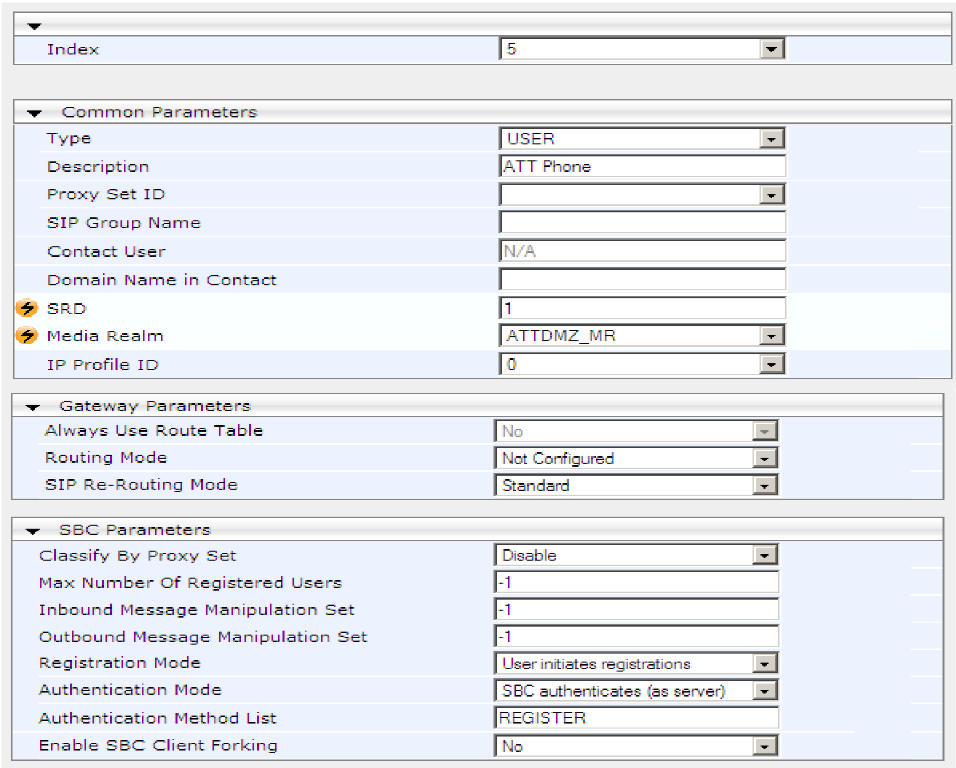
f. SRD: '1' – the SRD associated with this group of IP phones.

g. Media Realm: 'ATTDMZ_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 4-23: AT&T Customer IP Group 5 (Lab Only)



j. 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.

k. IP Group Index ‘6’

l. 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.

m. Description: Arbitrary name. (e.g., 'TWC Users')

n. Proxy Set ID: N/A (only applies to Type 'SERVER').

o. 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.

p. SRD: '5' – the SRD associated with this group of IP phones.

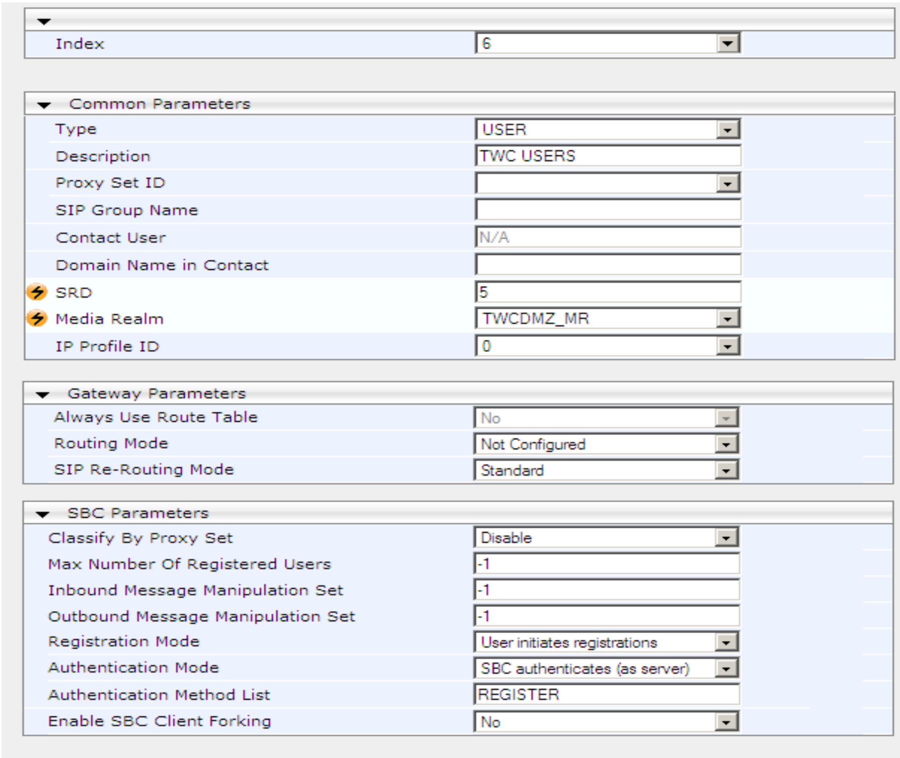
q. Media Realm: 'TWCDMZ_MR' - Assigns Media Realm to the IP Group. Must be identical to the Media Realm name in the Media Realm table.

r. IP Profile ID: '0' (default)

s. Registration Mode: ‘SBC authenticates (as server)’. The device will authenticate as a server using a User Information File.

t. Authentication Method: 'REGISTER'. This defines the SIP methods that the device must challenge.

Figure 4-24: Non-AT&T Customers IP Group 6 (Lab only)



4.1.10 Configure the Proxy Sets

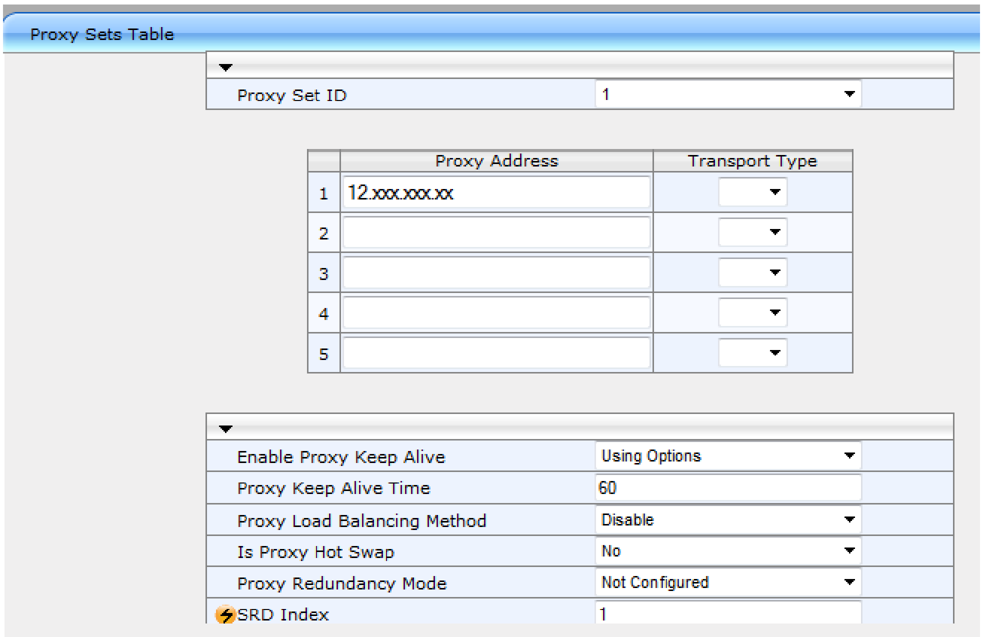
The Proxy Sets Table allows for the configuration of a Proxy set, or group of Proxy servers defined by IP address or Fully Qualified Domain Name (FQDN). Up to 32 Proxy Sets, each with a unique ID number and up to 5 Proxy Server addresses can be defined. A transport type of UDP, TCP, or TLS can be defined 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:**

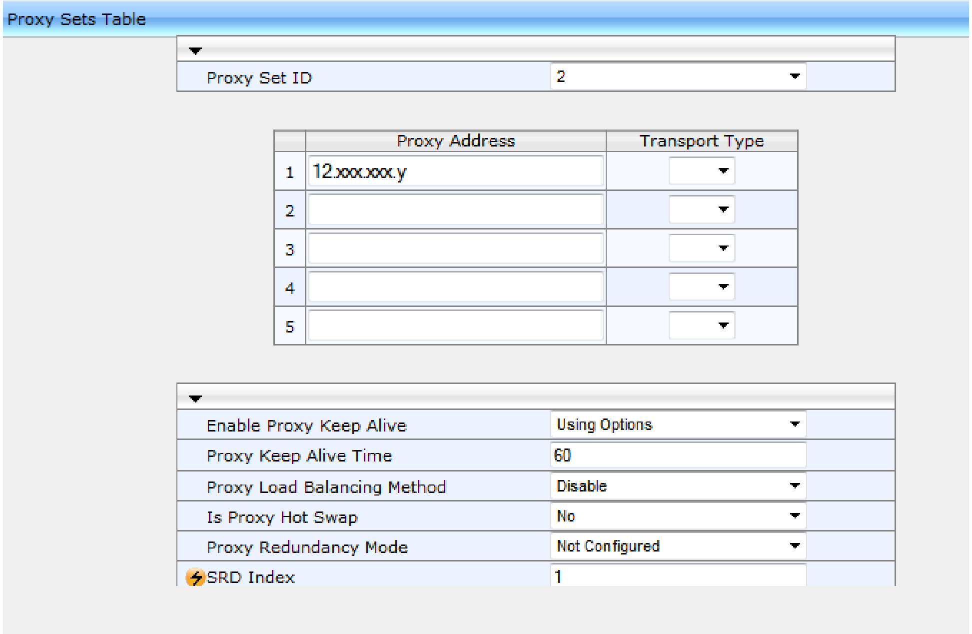
1. Open the Proxy Sets Table page (**Configuration** > **VoIP** > **Control Network** > **Proxy Sets Table**).
2. From the 'Proxy Set ID' drop-down list, select an ID for the desired group. Start with Proxy Set ID 1. For this configuration, Proxy Set ID 1 will correspond to the primary AT&T IP Toll Free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

Figure 4-25: Proxy Set 1 AT&T IP Toll Free Service SIP Trunk



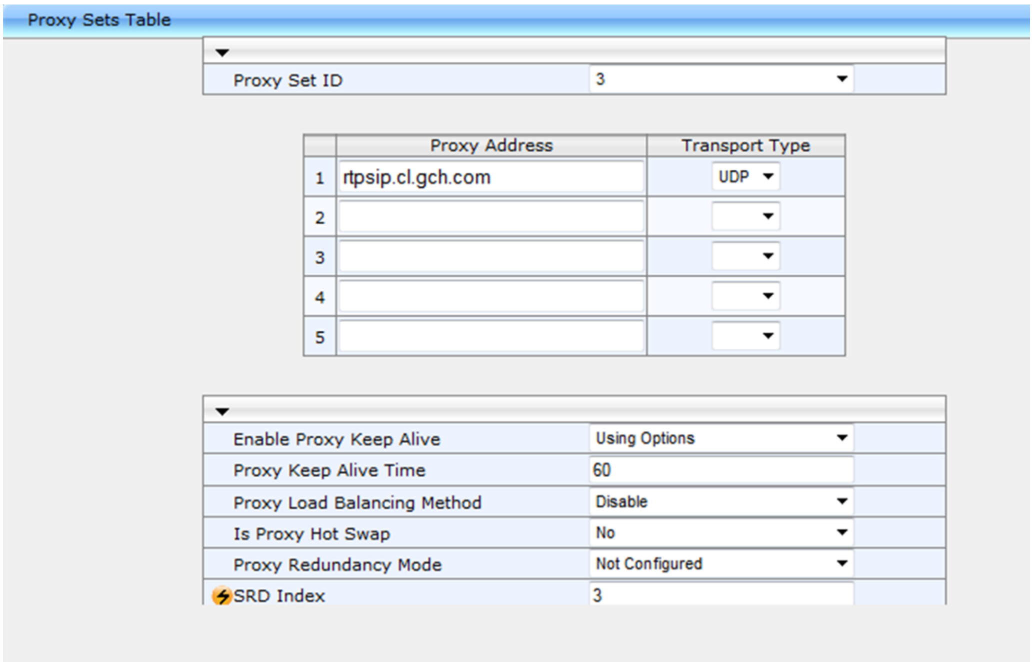
4. Click **Submit** to apply the changes.
5. From the 'Proxy Set ID' drop-down list, select Proxy Set ID 2. For this configuration, Proxy Set 2 will correspond to the secondary AT&T IP Toll Free Service's SIP Trunk.
6. Configure the Proxy parameters accordingly, as shown below. See the *Mediant User's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

Figure 4-26: Proxy Set 2 AT&T IP Toll Free Service's SIP Trunk - Secondary



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 User's Manual* for parameter descriptions.

Figure 4-27: Proxy Set 3 (Genesys SIP Server Trunk)

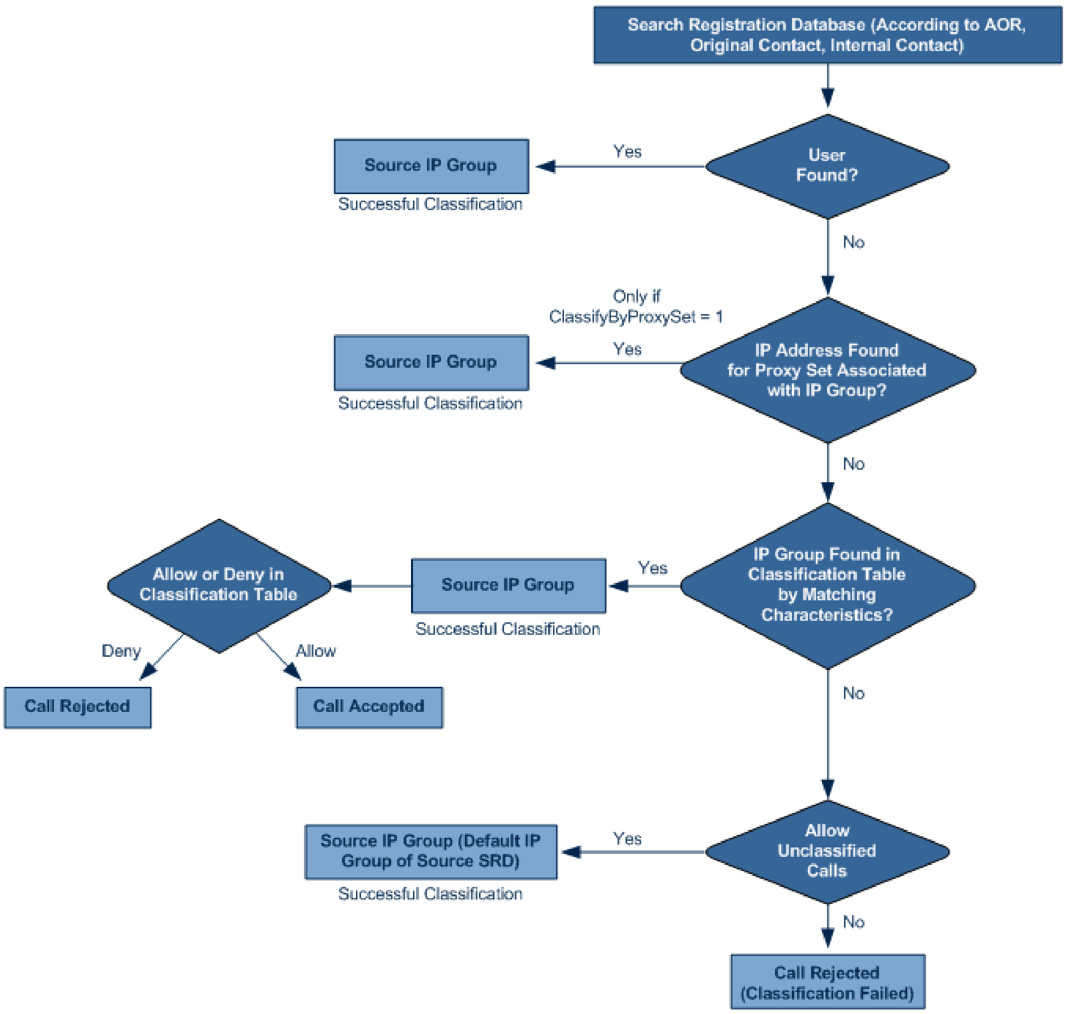


9. Click **Submit** to apply the changes.

4.1.11 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 SIP User's Manual* for further information on the classification process.

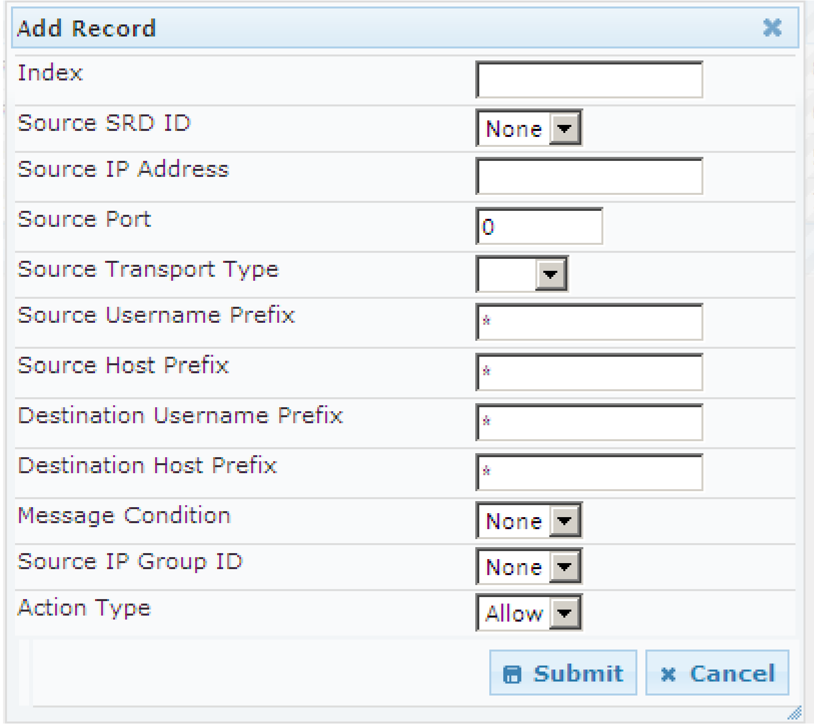
Figure 4-28: Classification Process Overview



➢ **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 4-29: Classification Table … Add Record Page



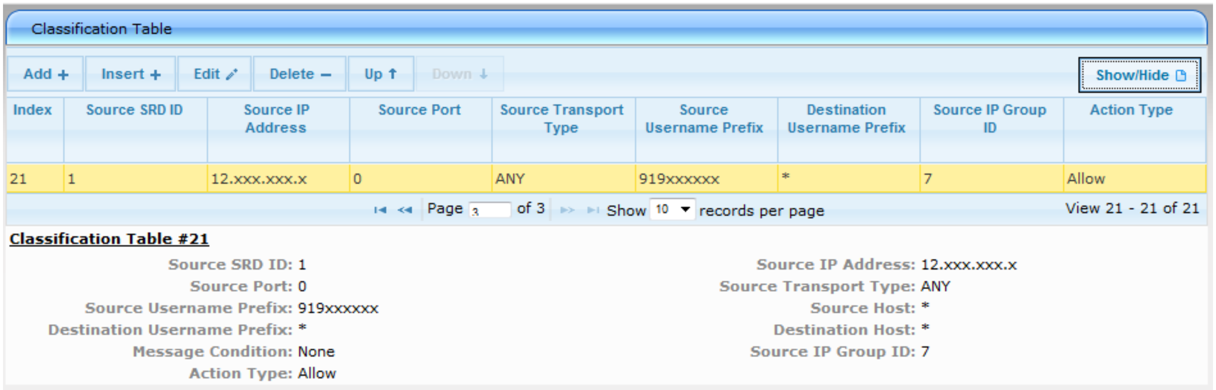
Add Record

Index	
Source SRD ID	None
Source IP Address	
Source Port	0
Source Transport Type	
Source Username Prefix	*
Source Host Prefix	*
Destination Username Prefix	*
Destination Host Prefix	*
Message Condition	None
Source IP Group ID	None
Action Type	Allow

Submit Cancel

3. Configure the classification rules as shown below. Apply the changes and save to flash. The classification below assigns Source IP Group ID 7 to a call originating on the AT&T interface, but not coming from either IPBE (a remote agent in the AT&T private network).

Figure 4-30: Classification Rule



Classification Table

Add + Insert + Edit Delete – Up Down Show/Hide

Index	Source SRD ID	Source IP Address	Source Port	Source Transport Type	Source Username Prefix	Destination Username Prefix	Source IP Group ID	Action Type
21	1	12.xxx.xxx.x	0	ANY	919xxxxxx	*	7	Allow

Page 3 of 3 Show 10 records per page View 21 - 21 of 21

Classification Table #21

Source SRD ID: 1
Source IP Address: 12.xxx.xxx.x
Source Port: 0
Source Transport Type: ANY
Source Username Prefix: 919xxxxxx
Source Host: *
Destination Username Prefix: *
Destination Host: *
Message Condition: None
Source IP Group ID: 7
Action Type: Allow

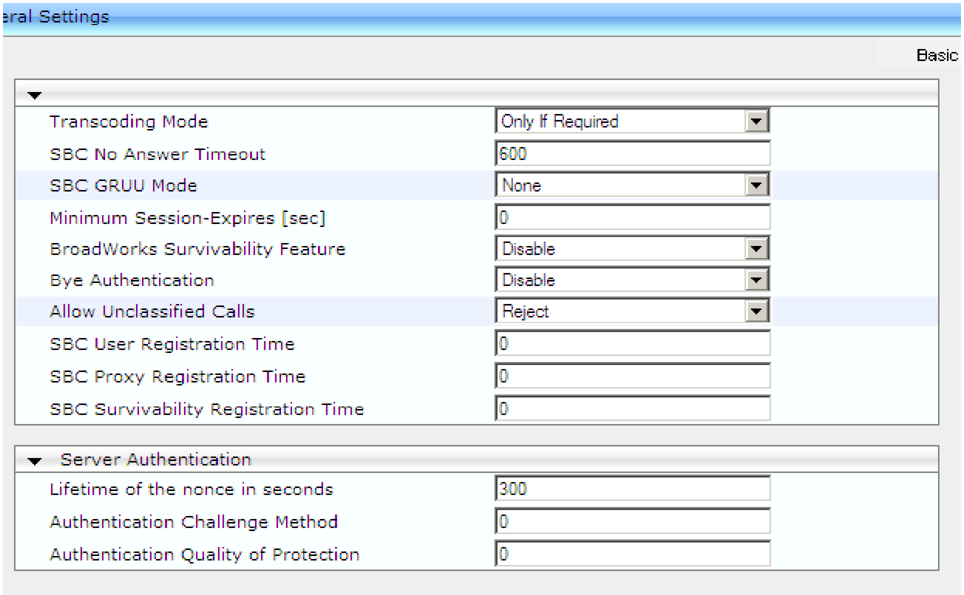
4.1.12 Configure SBC General Settings

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) and 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 4-31: SBC General Settings



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

4.1.13 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 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 4-32: SBC Admission Control Table

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

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

4.1.14 Configure Allowed Coders Group

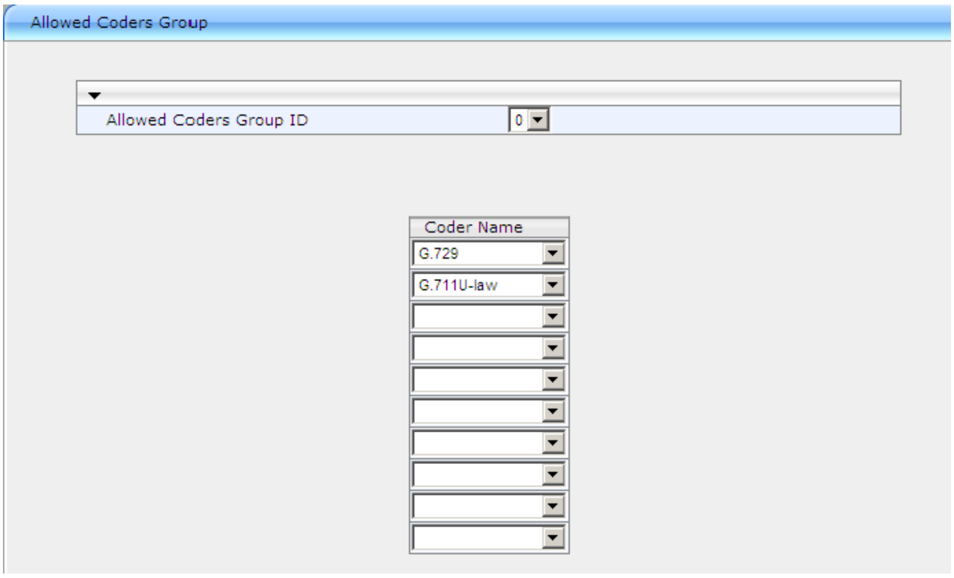
The Allowed Coders Group page allows up to five Allowed Coder Groups, each with up to 10 coders. Allowed Coder Groups determine the codes that can be used for a specific SBC leg. The device's SBC application can therefore enforce the use of specific coders while preventing the use of other coders. Coders 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 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 AT&T IP Toll Free 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 Toll Free Service network & the Genesys Call Center network will both use the same Coder preferences, only one Allowed Coders Group ID needs to be created.

Figure 4-33: Allow Coders Group



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

4.1.15 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 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. For Enh IPFR, Intra-Site call routed over AT&T Network, set the parameter 'Disconnect on Broken Connection' to **No** in the IP Profile.
7. Click **Submit** to apply the changes.
8. Save the changes to flash memory.

Figure 4-34: AT&T IP Toll Free Service 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 Canceler(*)	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	Restiction 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

4.1.16 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 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 4-35: IP2IP Routing Table

Index	Src IP Group ID	Src Username Prefix	Src Host	Dest Username Prefix	Dest IP Group ID	Dest SRDID	Dest Address	Dest Port	Dest Transport Type	Alt Route Options
3	7	"*"	"*"	"*"	3	3	""	0	-1 ()	0 (Route Row)
4	8	"*"	"*"	"*"	3	3	""	0	-1 ()	0 (Route Row)
7	1	"*"	"*"	"xxxxxx"	3	3	""	0	-1 ()	0 (Route Row)
8	2	"*"	"*"	"xxxxxx"	3	3	""	0	-1 ()	0 (Route Row)
9	3	"*"	"*"	"919xxxxxxx"	7	1	""	0	-1 ()	0 (Route Row)
10	3	"*"	"*"	"919xxxxxx[x-y]"	8	5	""	0	-1 ()	0 (Route Row)
11	1	"*"	"*"	"202xxxxxx[x-y]"	3	3	""	0	-1 ()	0 (Route Row)
12	2	"*"	"*"	"202xxxxxx[x-y]"	3	3	""	0	-1 ()	0 (Route Row)
22	8	"*"	"*"	"xxxyyy"	3	3	""	0	-1 ()	0 (Route Row)
36	3	"*"	"*"	"*"	1	1	""	0	-1 ()	0 (Route Row)
37	3	"*"	"*"	"*"	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 Toll Free) or IP Group 2 (in the case of the AT&T IP Toll Free Service's 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 is 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 Toll Free Service), IP Group 2 (in the case of AT&T IP Toll Free Service's alternate SIP Trunk) or IP Group 7 (Remote Agents on AT&T IP Toll Free Service, depending on the destination number dialed.
- Calls originating from IP Groups 7 (Remote Agents on IP Toll Free) would route to IP Group 3 (Genesys).

  Groups 5 and 6 are groups created to simulate end customers in the certification 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 certification environment troubleshooting purposes.

4.1.16.1 IP-to-IP Routing Row Details

This section exemplifies routing rows (specific to the solution instance described in this Configuration Note), similar to those required for AT&T IP Toll Free Service Call Center in the production environment.

1. **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.

2. **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 (Genesys SIP Server). 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.

3. **Index #7** specifies that all IP calls with destination prefix 'xxxxxx' received from IP Group 1 (AT&T IP Toll Free Service’s network) will be routed to IP Group 3 (Genesys SIP Server). The destination number stipulation is to limit the DNs outside the range of what the Genesys SIP Server is configured to receive from being passed to the Genesys platform.

4. **Index #8** specifies that all IP calls with destination prefix 'xxxxxx' received from IP Group 2 (AT&T IP Toll Free Service’s network secondary IPBE) will be routed to IP Group 3 (Genesys). The destination number stipulation limits DNs outside the range of what the Genesys SIP Server was configured to receive, from being passed to the Genesys platform.

5. **Index #9** specifies that all IP calls with destination prefix '919xxxxxx' received from IP Group 3 (Genesys SIP Server) will route to SRD 1, IP Group 7. In this example, this destination prefix is narrowly defined to one number. This entry represents Remote Agents in the AT&T network not originating from the IPBEs.

6. **Index #10** specifies that all IP calls with destination prefix ‘919xxxxxx’ through ‘919xxxxxy’, received from IP Group 3 (Genesys), will route to SRD 5, IP Group 8 (non-AT&T network). In this example, this destination prefix is narrowly defined. This represents calls destined for Remote Agents in a non-AT&T network.

7. **Index #11** specifies that all IP calls with destination prefix ‘202xxxxxxx’ – ‘202xxxxxxy’, received from IP Group 1 (AT&T IP Toll Free Service), will route to SRD 3, IP Group 3 (Genesys). This represents calls destined for Virtual Telephone Numbers of Agents in the Call Center.

8. **Index #12** specifies that all IP calls with destination prefix ‘202xxxxxxx’ – ‘202xxxxxxy’, received from IP Group 2 (AT&T IP Toll Free Service’s secondary IPBE), will route to SRD 3, IP Group 3 (Genesys SIP Server). This represents calls destined for Virtual Telephone Numbers of Agents in the Call Center.

9. **Index #22** specifies that IP calls with destination 'xxxyyy', originating on IP Group 8 (non-AT&T network), will 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.

10. **Index #36** specifies that all IP calls originating on IP Group 3 (Genesys SIP Server) will be assigned to IP Group 1 (AT&T IP Toll Free Service). This is the default entry and applies if all other route rows for IP calls originating from IP Group 3 (Genesys) do not match. A similar entry will exist in a production environment.

11. **Index #37** specifies that all IP calls originating on IP Group 3 (Genesys SIP Server) will be assigned to IP Group 2 (AT&T IP Toll Free Service's Secondary IPBE). This is the default entry and will apply if all other route rows for IP calls originating from IP Group 3 (Genesys) do not match and if the previous route applied but the route was not available. A similar entry will exist in a production environment.

4.2 SIP Header Manipulation

The Mediant 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 AT&T IP Toll Free SIP Trunking 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 4-36: Message Manipulations for AT&T IP Toll Free with Genesys SIP Server

Index	Man Set ID	Message Type	Condition	Action Subject	Action Type	Action Value	Row Role
3	0	"Any.Response"	"Header.To.Url.Host contains 'angel.z101.gch.com'"	"Header.To.Url.Host"	2 (Modify)	"'<sbc_ip_addr>'"	0 (Use Current Condition)
4	0	"Any.Request"	"Header.From.Url.Host contains 'angel.z101.gch.com'"	"Header.From.Url.Host"	2 (Modify)	"'<sbc_ip_addr>'"	0 (Use Current Condition)
5	0	"Invite.Request"	"Header.P-Asserted-identity exists"	'Header.P-Asserted-identity'	2 (Modify)	"'Unavailable<sip:'+ ıeader.contact.url.user+ @<sbc_ip_addr>>'"	0 (Use Current Condition)
6	0	"Invite.Request"	"Header.P-Asserted-identity !exists"	'Header.P-Asserted-identity'	0 (Add)	"Unavailable<sip:'+heac ɘr.contact.url.user+'@<s bc_ip_addr>>'"	0 (Use Current Condition)
7	0	"Invite.Request"	""	"Header.Privacy"	0 (Add)	"'id'"	0 (Use Current Condition)
9	0	"Invite.Request"	"Header.P-Asserted-identity.URL.host contains 'angel.z101.gch.com'"	"Header.P-Asserted-identity.URL.host"	2 (Modify)	"'<sbc_ip_addr>"	0 (Use Current Condition)
15	0	"Invite.Request"	""	"header.from.url.user"	2 (Modify)	"'anonymous'"	0 (Use Current Condition)
16	0	"Invite.Request"	""	"header.from.name"	2 (Modify)	"'Anonymous'"	0 (Use Current Condition)
43	0	""	"header.Refer-To exists"	"header.contact.url.user"	2 (Modify)	"header.from.url.user"	0 (Use Current Condition)
44	0	""	"Header.Refer-To exists and Header.Refer-To regex(<sip:)(.*)@(.*)"	"Header.Refer-To"	1 (Remove)	""	0 (Use Current Condition)
45	0	""	""	"Header.Refer-To"	0 (Add)	"$1+$2+$3+'<AT&T_Primary_ip_addr >'"	1 (Use Previous Condition)

Index	Man Set ID	Message Type	Condition	Action Subject	Action Type	Action Value	Row Role
8	3	""	""	"Header.Contact.url.user "	2 (Modify)	"'gcsbc01'"	0 (Use Current Condition)
13	4	"Invite.Request"	"Header.Request-uri.URL.user != Header.to.url.user"	"Header.Diversion"	0 (Add)	"'919xxxxxxx'+"+';user =phone>;userid="	0 (Use Current Condition)
41	4	""	"header.Referred-By.url.host contains 'angel.z101.gch.com'"	header.Referred-By.url.host'	2 (Modify)	"'<sbc_ip_addr>'"	0 (Use Current Condition)

Note the following regarding the entries:

- Manipulation Set '0' is the collection of rules that apply to calls on the outgoing AT&T IP Toll Free 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 particular rule in all cases. As an example, the 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.

4.3 Mediant 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
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
```

4.4 Configuration File Examples

The sections below show examples of product configuration files.

4.4.1 Mediant E-SBC

Note: Example Mediant E-SBC configuration files are added here for reference purposes only. In this Mediant 4000 E-SBC example, the IP Toll Free SIP Trunk interfaces over the PUBSIP Interface, not the ATTDMZ interface as exemplified in the document. There is a single IPBE, 207.xxx.xxx.210 in this instance. The applicable manipulation sets are 3, 4, & 18. The ATTDMZ interface exemplifies working with primary and secondary IPBE.

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

;Board: Mediant 4000
;Board Type: 70
;Serial Number: 3968219
;Slot Number: 1
;Software Version: 6.60A.035.004
;DSP Software Version: 5039AE3_R => 660.15
;Board IP Address: 10.38.20.40
;Board Subnet Mask: 255.255.255.0
;Board Default Gateway: 10.38.20.1
;Ram size: 2048M   Flash size: 252M
;Num of DSP Cores: 24  Num DSP Channels: 864
;Num of physical LAN ports: 8
;Profile: NONE
;Key features:;Board Type: Mediant 4000 ;Security: IPSEC MediaEncryption
StrongEncryption EncryptControlProtocol ;E1Trunks=0 ;T1Trunks=0 ;Channel Type:
DspCh=8000 ;HA ;IP Media: VXML ;Coders: G723 G729 GSM-FR G727 G722 ;Control
Protocols: SIP SBC=4000 MSFT CLI ;Default features:;Coders: G711 G726;

;------ M4000 HW components------
;
; Slot # : Module type : # of ports
;----------------------------------------------
;       1 : DSM         : 0
;       2 : CSM         : 0
;       3 : LSM         : 4
;       4 : DSM         : 0
;       5 : Empty
;       6 : LSM         : 4
;----------------------------------------------


[SYSTEM Params]

SyslogServerIP = 10.38.5.90
EnableSyslog = 1
NTPServerUTCOffset = -18000
ActivityListToLog = 'naa'
DebugRecordingDestIP = 10.38.5.79
;VpFileLastUpdateTime is hidden but has non-default value
DayLightSavingTimeStart = '03:01:00:00'
DayLightSavingTimeEnd = '11:01:00:00'
```

```
DayLightSavingTimeEnable = 1
SyslogFacility = 23
HARemoteAddress = 10.1.10.10
HAPriority = 7
HARevertiveEnabled = 1
HAUnitIdName = 'Device 1'
DebugRecordingStatus = 1
LDAPSEARCHDNSINPARALLEL = 0

[BSP Params]

PCMLawSelect = 3
TDMBusType = 0
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

[Analog Params]


[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

[Voice Engine Params]

IdlePCMPattern = 85

[WEB Params]

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

[SIP Params]

MEDIACHANNELS = 512
GWDEBUGLEVEL = 5
;ISPRACKREQUIRED is hidden but has non-default value
PROXYREDUNDANCYMODE = 1
ENABLEUSERINFOUSAGE = 1
SetDefaultOnIniFileProcess = 0
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
SBCMAXFORWARDSLIMIT = 70
```

```
SBCGRUUMODE = 0
AUTHQOP = 0

[IPsec Params]


[SNMP Params]

SNMPManagerIsUsed_0 = 1
SNMPManagerIsUsed_1 = 0
SNMPManagerIsUsed_2 = 0
SNMPManagerIsUsed_3 = 0
SNMPManagerIsUsed_4 = 0
SNMPManagerTableIP_0 = 10.38.20.40
SNMPManagerTableIP_1 = 0.0.0.0
SNMPManagerTableIP_2 = 0.0.0.0
SNMPManagerTableIP_3 = 0.0.0.0
SNMPManagerTableIP_4 = 0.0.0.0

[ PhysicalPortsTable ]

FORMAT PhysicalPortsTable_Index = PhysicalPortsTable_Port,
PhysicalPortsTable_Mode, PhysicalPortsTable_NativeVlan,
PhysicalPortsTable_SpeedDuplex, PhysicalPortsTable_PortDescription,
PhysicalPortsTable_GroupMember, PhysicalPortsTable_GroupStatus;
PhysicalPortsTable 0 = "GE_1", 1, 320, 4, "User Port #0", "GROUP_1", "Active";
PhysicalPortsTable 1 = "GE_2", 1, 2, 4, "User Port #1", "GROUP_2", "Redundant";
PhysicalPortsTable 2 = "GE_3", 1, 2, 4, "User Port #2", "GROUP_2", "Active";
PhysicalPortsTable 3 = "GE_4", 1, 2, 4, "User Port #3", "GROUP_2", "Redundant";
PhysicalPortsTable 4 = "GE_5", 1, 3, 4, "User Port #4", "GROUP_3", "Active";
PhysicalPortsTable 5 = "GE_6", 1, 3, 4, "User Port #5", "GROUP_3", "Redundant";
PhysicalPortsTable 6 = "GE_7", 1, 1, 4, "User Port #6", "GROUP_4", "Active";
PhysicalPortsTable 7 = "GE_8", 1, 1, 4, "User Port #7", "GROUP_4", "Redundant";

[ \PhysicalPortsTable ]


[ EtherGroupTable ]

FORMAT EtherGroupTable_Index = EtherGroupTable_Group, EtherGroupTable_Mode,
EtherGroupTable_Member1, EtherGroupTable_Member2;
EtherGroupTable 0 = "GROUP_1", 3, GE_1, ;
EtherGroupTable 1 = "GROUP_2", 3, GE_2, ;
EtherGroupTable 2 = "GROUP_3", 2, GE_5, GE_6;
EtherGroupTable 3 = "GROUP_4", 2, GE_7, GE_8;

[ \EtherGroupTable ]


[ InterfaceTable ]

FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway, InterfaceTable_VlanID,
InterfaceTable_InterfaceName, InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress, InterfaceTable_UnderlyingInterface;
InterfaceTable 0 = 0, 10, 10.38.20.40, 24, 10.38.20.1, 320, "NETMGMT", 0.0.0.0,
0.0.0.0, GROUP_1;
InterfaceTable 1 = 5, 10, 173.xxx.xxx.xx, 26, 173.xxx.xxx.65, 254, "PUBSIP",
0.0.0.0, 0.0.0.0, GROUP_3;
InterfaceTable 2 = 5, 10, 10.38.60.10, 24, 10.38.60.1, 360, "RALVOX", 0.0.0.0,
0.0.0.0, GROUP_4;
InterfaceTable 3 = 5, 10, 12.xxx.xxx.xxx, 29, 12.xxx.xxx.xxx, 455, "ATTDMZ",
0.0.0.0, 0.0.0.0, GROUP_3;
```

```
InterfaceTable 4 = 5, 10, 10.38.5.10, 24, 10.38.5.1, 305, "RALOFFICE", 0.0.0.0,
0.0.0.0, GROUP_4;

[ \InterfaceTable ]


[ ACCESSLIST ]

FORMAT ACCESSLIST_Index = ACCESSLIST_Source_IP, ACCESSLIST_Source_Port,
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 0 = "12.xxx.xxx.x", 0, 32, 0, 65535, "Any", 1, ATTDMZ, 0, 0, 0,
"ALLOW";
ACCESSLIST 1 = "12.xxx.xxx.y", 0, 32, 0, 65535, "Any", 1, ATTDMZ, 0, 0, 0,
"ALLOW";
ACCESSLIST 2 = "12.xxx.xxx.z", 0, 32, 0, 65535, "Any", 1, ATTDMZ, 0, 0, 0,
"ALLOW";
ACCESSLIST 3 = "12.xxx.xxx.a", 0, 32, 0, 65535, "Any", 1, ATTDMZ, 0, 0, 0,
"ALLOW";
ACCESSLIST 4 = "12.xxx.xxx.b", 0, 32, 0, 65535, "Any", 1, ATTDMZ, 0, 0, 0,
"ALLOW";
ACCESSLIST 5 = "0.0.0.0", 0, 0, 0, 65535, "Any", 1, ATTDMZ, 0, 0, 0, "BLOCK";
ACCESSLIST 17 = "173.xxx.xxx.a", 0, 32, 0, 65535, "Any", 1, PUBSIP, 0, 0, 0,
"Allow";
ACCESSLIST 18 = "173.xxx.xxx.b", 0, 32, 0, 65535, "Any", 1, PUBSIP, 0, 0, 0,
"Allow";
ACCESSLIST 19 = "173.xxx.xxx.c", 0, 32, 0, 65535, "Any", 1, PUBSIP, 0, 0, 0,
"Allow";
ACCESSLIST 20 = "207.xxx.xxx.xxx", 0, 32, 0, 65535, "Any", 1, PUBSIP, 0, 0, 0,
"ALLOW";
ACCESSLIST 25 = "0.0.0.0", 0, 0, 0, 65535, "Any", 1, PUBSIP, 0, 0, 0, "BLOCK";

[ \ACCESSLIST ]


[ DspTemplates ]

;
;  *** TABLE DspTemplates ***
; This table contains hidden elements and will not be exposed.
; This table exists on board and will be saved during restarts.
;

[ \DspTemplates ]


[ CpMediaRealm ]

FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName, CpMediaRealm_IPv4IF,
CpMediaRealm_IPv6IF, CpMediaRealm_PortRangeStart, CpMediaRealm_MediaSessionLeg,
CpMediaRealm_PortRangeEnd, CpMediaRealm_IsDefault;
CpMediaRealm 0 = "ATTDMZ_MR", ATTDMZ, , 16390, 600, 22380, 1;
CpMediaRealm 1 = "RALVOX_MR", RALVOX, , 6000, 50, 6490, 0;
CpMediaRealm 2 = "RALLOFFICE_MR", RALOFFICE, , 6500, 550, 11990, 0;
CpMediaRealm 3 = "TWCDMZ_MR", PUBSIP, , 16390, 100, 17380, 0;

[ \CpMediaRealm ]


[ SRD ]

FORMAT SRD_Index = SRD_Name, SRD_MediaRealm, SRD_IntraSRDMediaAnchoring,
SRD_BlockUnRegUsers, SRD_MaxNumOfRegUsers, SRD_EnableUnAuthenticatedRegistrations;
```

```
SRD 1 = "ATTDMZ_SRD", "ATTDMZ_MR", 0, 1, -1, 0;
SRD 2 = "RALVOX_SRD", "RALVOX_MR", 1, 0, -1, 1;
SRD 3 = "RALOFFICE_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.gch.com", 10.38.5.117, 0.0.0.0, 0.0.0.0, 0.0.0.0;

[ \Dns2Ip ]


[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIp_IpAddress, ProxyIp_TransportType,
ProxyIp_ProxySetId;
ProxyIp 0 = "12.xxx.xxx.x", -1, 1;
ProxyIp 1 = "173.xxx.xxx.xxx", -1, 8;
ProxyIp 2 = "rtpsip.cl.gch.com", 0, 3;
ProxyIp 3 = "12.xxx.xxx.y", -1, 2;
ProxyIp 4 = "207.xxx.xxx.x", -1, 4;

[ \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_CNGmode, 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_SBCDiversionMode, IpProfile_SBCHistoryInfoMode,
IpProfile_EnableQSIGTunneling, IpProfile_SBCFaxCodersGroupID,
IpProfile_SBCFaxBehavior, IpProfile_SBCFaxOfferMode, IpProfile_SBCFaxAnswerMode,
IpProfile_SbcPrackMode, IpProfile_SBCSessionExpiresMode,
IpProfile_SBCRemoteUpdateSupport, IpProfile_SBCRemoteReinviteSupport,
IpProfile_SBCRemoteDelayedOfferSupport, IpProfile_SBCRemoteReferBehavior,
IpProfile_SBCRemote3xxBehavior, IpProfile_SBCRemoteMultiple18xSupport,
IpProfile_SBCRemoteEarlyMediaResponseType, IpProfile_SBCRemoteEarlyMediaSupport,
IpProfile_EnableSymmetricMKI, IpProfile_MKISize, IpProfile_SBCEnforceMKISize,
IpProfile_SBCRemoteEarlyMediaRTP, IpProfile_SBCRemoteSupportsRFC3960,
IpProfile_SBCRemoteCanPlayRingback, IpProfile_EnableEarly183,
IpProfile_EarlyAnswerTimeout, IpProfile_SBC2833DTMFPayloadType,
IpProfile_SBCUserRegistrationTime, IpProfile_ResetSRTPStateUponRekey;
IpProfile 1 = "ATT IP Flex", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0, 0, -
1, 1, 0, 0, -1, 0, 4, -1, 1, 1, 0, 0, "", -1, 0, 0, 0, 2, 0, 0, 0, 0, 0, 8, 300,
400, 0, -1, 0, -1, 0, 0, 1, 3, 0, 2, 2, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 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 4 = 1, 60, 0, 0, 5, 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_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName;
IPGroup 1 = 0, "ATT IPGROUP", 1, "12.xxx.xxx.x", "", 0, -1, 0, 0, -1, 1,
"ATTDMZ_MR", 1, 1, -1, -1, 0, 0, 0, "", 0, -1, -1, "";
IPGroup 2 = 0, "ATT IPGroup Secondary", 2, "12.xxx.xxx.y", "", 0, -1, 0, 0, -1, 1,
"ATTDMZ_MR", 1, 1, -1, -1, 0, 0, 0, "", 0, -1, -1, "";
IPGroup 3 = 0, "GENESYS_SRV", 3, "angel.z101.gch.com", "", 0, -1, 0, 0, -1, 3,
"RALLOFFICE_MR", 1, 0, -1, 4, 3, 0, 0, "", 0, -1, -1, "";
IPGroup 4 = 1, "", -1, "", "", 0, 2, 0, 0, -1, 0, "", 1, 0, -1, -1, -1, 0, 0, "",
0, -1, -1, "";
IPGroup 5 = 1, "ATT Phone", -1, "", "", 0, -1, 0, 0, -1, 1, "ATTDMZ_MR", 0, 0, -1,
-1, -1, 0, 2, "REGISTER", 0, -1, -1, "";
IPGroup 6 = 1, "TWC USERS", -1, "", "", 0, -1, 0, 0, -1, 5, "TWCDMZ_MR", 0, 0, -1,
-1, -1, 0, 2, "REGISTER", 0, -1, -1, "";
IPGroup 7 = 1, "ATT Remote Agents", -1, "", "", 0, -1, 0, 0, -1, 1, "ATTDMZ_MR",
0, 0, -1, -1, -1, 0, 0, "", 0, -1, -1, "";
IPGroup 8 = 1, "TWC Remote Agents", -1, "", "", 0, -1, 0, 0, -1, 5, "TWCDMZ_MR",
0, 0, -1, -1, -1, 0, 0, "", 0, -1, -1, "";
IPGroup 9 = 0, "732 Remote Agents", 4, "207.xxx.xxx.xxx", "", 0, -1, -1, 0, -1, 5,
"TWCDMZ_MR", 1, 1, -1, 17, 18, 0, 0, "", 0, -1, -1, "";

[ \IPGroup ]


[ IP2IPRouting ]

FORMAT IP2IPRouting_Index = IP2IPRouting_SrcIPGroupID,
IP2IPRouting_SrcUsernamePrefix, IP2IPRouting_SrcHost,
IP2IPRouting_DestUsernamePrefix, IP2IPRouting_DestHost, IP2IPRouting_RequestType,
IP2IPRouting_MessageCondition, IP2IPRouting_ReRouteIPGroupID,
IP2IPRouting_Trigger, IP2IPRouting_DestType, IP2IPRouting_DestIPGroupID,
IP2IPRouting_DestSRDID, IP2IPRouting_DestAddress, IP2IPRouting_DestPort,
IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions,
IP2IPRouting_CostGroup;
IP2IPRouting 1 = 5, "*", "*", "*", "*", 2, , -1, 0, 0, 5, , "", 0, -1, 0, ;
IP2IPRouting 3 = 7, "*", "*", "*", "*", 0, , -1, 0, 0, 3, 3, "", 0, -1, 0, ;
IP2IPRouting 4 = 8, "*", "*", "*", "*", 0, , -1, 0, 0, 3, 3, "", 0, -1, 0, ;
IP2IPRouting 5 = 9, "*", "*", "*", "*", 0, , -1, 0, 0, 3, 3, "", 0, -1, 0, ;
IP2IPRouting 6 = 6, "*", "*", "*", "*", 2, , -1, 0, 0, 6, , "", 0, -1, 0, ;
IP2IPRouting 7 = 1, "*", "*", "919xxx", "*", 0, , -1, 0, 0, 3, 3, "", 0, -1, 0, ;
IP2IPRouting 8 = 2, "*", "*", "919xxx", "*", 0, , -1, 0, 0, 3, 3, "", 0, -1, 0, ;
```

```
IP2IPRouting 9 = 3, "*", "*", "919xxxxxxx", "*", 0, , -1, 0, 0, 7, 1, "", 0, -1,
0, ;
IP2IPRouting 10 = 3, "*", "*", "919xxxxxx[x-y]", "*", 0, , -1, 0, 0, 8, 5, "", 0,
-1, 0, ;
IP2IPRouting 11 = 1, "*", "*", "202xxxxxx[x-y]", "*", 0, , -1, 0, 0, 3, 3, "", 0,
-1, 0, ;
IP2IPRouting 12 = 2, "*", "*", "202xxxxxx[x-y]", "*", 0, , -1, 0, 0, 3, 3, "", 0,
-1, 0, ;
IP2IPRouting 13 = 1, "*", "*", "202xxxxxxx", "*", 0, , -1, 0, 0, 5, 1, "", 0, -1,
0, ;
IP2IPRouting 14 = 2, "*", "*", "202xxxxxxx", "*", 0, , -1, 0, 0, 5, 1, "", 0, -1,
0, ;
IP2IPRouting 15 = 1, "*", "*", "202xxxxxx[x-y]", "*", 0, , -1, 0, 0, 8, 5, "", 0,
-1, 0, ;
IP2IPRouting 16 = 2, "*", "*", "202xxxxxx[x-y]", "*", 0, , -1, 0, 0, 8, 5, "", 0,
-1, 0, ;
IP2IPRouting 17 = 1, "*", "*", "202xxxxxx", "*", 0, , -1, 0, 0, 6, 5, "", 0, -1,
0, ;
IP2IPRouting 18 = 2, "*", "*", "202xxxxxx", "*", 0, , -1, 0, 0, 6, 5, "", 0, -1,
0, ;
IP2IPRouting 19 = 5, "*", "*", "202xxxxxx", "*", 0, , -1, 0, 0, 6, 5, "", 0, -1,
0, ;
IP2IPRouting 20 = 5, "*", "*", "919xxxxx[xx-yy]", "*", 0, , -1, 0, 0, 3, 3, "", 0,
-1, 0, ;
IP2IPRouting 21 = 6, "*", "*", "919xxx", "*", 0, , -1, 0, 0, 3, 3, "", 0, -1, 0, ;
IP2IPRouting 22 = 8, "*", "*", "919xxx", "*", 0, , -1, 0, 0, 3, 3, "", 0, -1, 0, ;
IP2IPRouting 23 = 5, "202", "*", "919xxxx[450-515]", "*", 0, , -1, 0, 0, 1, 1, "",
0, -1, 0, ;
IP2IPRouting 24 = 5, "202", "*", "919xxxx[450-515]", "*", 0, , -1, 0, 0, 2, 1, "",
0, -1, 1, ;
IP2IPRouting 25 = 5, "*", "*", "011xxxxxxxxxxx", "*", 0, , -1, 0, 0, 1, 1, "", 0,
-1, 0, ;
IP2IPRouting 26 = 5, "*", "*", "011xxxxxxxxxxx", "*", 0, , -1, 0, 0, 2, 1, "", 0,
-1, 1, ;
IP2IPRouting 27 = 3, "*", "*", "[*73]", "*", 0, , -1, 0, 0, 9, 5, "", 0, -1, 0, ;
IP2IPRouting 28 = 3, "*", "*", "[*72]919xxxx[450-515]", "*", 0, , -1, 0, 0, 9, 5,
"", 0, -1, 1, ;
IP2IPRouting 29 = 3, "*", "*", "[*90]919xxxxxxx", "*", 0, , -1, 0, 0, 9, 5, "", 0,
-1, 0, ;
IP2IPRouting 30 = 3, "*", "*", "[*91]", "*", 0, , -1, 0, 0, 9, 5, "", 0, -1, 0, ;
IP2IPRouting 31 = 3, "*", "*", "[*92]919xxxxxxx", "*", 0, , -1, 0, 0, 9, 5, "", 0,
-1, 0, ;
IP2IPRouting 32 = 3, "*", "*", "[*93]", "*", 0, , -1, 0, 0, 9, 5, "", 0, -1, 0, ;
IP2IPRouting 33 = 3, "*", "*", "[*94]919xxxxxxx", "*", 0, , -1, 0, 0, 9, 5, "", 0,
-1, 0, ;
IP2IPRouting 34 = 3, "*", "*", "[*95]", "*", 0, , -1, 0, 0, 9, 5, "", 0, -1, 0, ;
IP2IPRouting 35 = 3, "*", "*", "*", "*", 0, , -1, 0, 0, 9, 5, "", 0, -1, 0, ;
IP2IPRouting 36 = 3, "*", "*", "*", "*", 0, , -1, 0, 0, 2, 1, "", 0, -1, 0, ;
IP2IPRouting 37 = 5, "*", "*", "1888xxxxxxx", "*", 0, , -1, 0, 0, 1, 1, "", 0, -1,
0, ;
IP2IPRouting 38 = 5, "*", "*", "1888xxxxxxx", "*", 0, , -1, 0, 0, 2, 1, "", 0, -1,
1, ;
IP2IPRouting 39 = 6, "*", "*", "1888xxxxxxx", "*", 0, , -1, 0, 0, 1, 1, "", 0, -1,
0, ;
IP2IPRouting 40 = 6, "*", "*", "1888xxxxxxx", "*", 0, , -1, 0, 0, 2, 1, "", 0, -1,
1, ;
IP2IPRouting 41 = 1, "*", "*", "00000888xxxxxxx", "*", 0, , -1, 0, 0, 3, 3, "", 0,
-1, 0, ;

[ \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 1 = , 5, "207.xxx.xxx.xxx", 0, -1, "*", "*", "*", "*", 1, 9;
Classification 2 = , 5, "173.xxx.xxx.*", 0, -1, "202xxxxxx[8-9]", "*", "*", "*",
1, 8;
Classification 3 = , 5, "173.xxx.xxx.*", 0, -1, "919xxxxxx[7-8]", "*", "*", "*",
1, 8;
Classification 4 = , 5, "173.xxx.xxx.*", 0, -1, "202xxxxxxx", "*", "*", "*", 1, 6;
Classification 5 = , 1, "12.xxx.xxx.*", 0, -1, "202xxxxxxx", "*", "*", "*", 1, 5;
Classification 6 = , 1, "12.xxx.xxx.*", 0, -1, "202xxxxxx[8-9]", "*", "*", "*", 1,
8;
Classification 7 = , 1, "12.xxx.xxx.*", 0, -1, "919xxxxxxx", "*", "*", "*", 1, 7;

[ \Classification ]


[ SIPInterface ]

FORMAT SIPInterface_Index = SIPInterface_NetworkInterface,
SIPInterface_ApplicationType, SIPInterface_UDPPort, SIPInterface_TCPPort,
SIPInterface_TLSPort, SIPInterface_SRD, SIPInterface_MessagePolicy,
SIPInterface_TLSMutualAuthentication, SIPInterface_TCPKeepaliveEnable,
SIPInterface_ClassificationFailureResponseType;
SIPInterface 1 = "ATTDMZ", 2, 5060, 5060, 5061, 1, , -1, 0, 500;
SIPInterface 2 = "RALVOX", 2, 5060, 5060, 5061, 2, , -1, 0, 500;
SIPInterface 3 = "RALOFFICE", 2, 5060, 5060, 5061, 3, , -1, 0, 500;
SIPInterface 5 = "PUBSIP", 2, 5060, 5060, 5061, 5, , -1, 0, 500;

[ \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, "", "*", "xxxxxxx", "*", 0, 1, 0, 0, 255,
"919", "";
IPInboundManipulation 1 = 0, 0, 1, "*", "*", "00000888xxxxxxx", "*", 0, 1, 15, 0,
255, "919xxx3620", "";
IPInboundManipulation 3 = 0, 0, 2, "*", "*", "xxxxxxx", "*", 0, 1, 0, 0, 255,
"919", "";
IPInboundManipulation 4 = 0, 0, 9, "*", "*", "732xxxxxxx", "*", 0, 1, 10, 0, 255,
"", "919xxxxxxx";
IPInboundManipulation 5 = 0, 0, 9, "*", "*", "732xxxxxxx", "*", 0, 1, 10, 0, 255,
"", "919xxxxxxx";
IPInboundManipulation 6 = 0, 0, 9, "*", "*", "732xxxxxxx", "*", 0, 1, 10, 0, 255,
"", "919xxxxxxx";

[ \IPInboundManipulation ]


[ CodersGroup0 ]

FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime,
CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce;
CodersGroup0 0 = "g729", 20, 0, -1, 0;
CodersGroup0 1 = "g711Ulaw64k", 20, 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, "Any.Response", "Header.To.Url.Host contains
'angel.z101.gch.com'", "Header.To.Url.Host", 2, "'12.xxx.xxx.xxx'", 0;
MessageManipulations 4 = 0, "Any.Request", "Header.From.Url.Host contains
'angel.z101.gch.com'", "Header.From.Url.Host", 2, "'12.xxx.xxx.xxx'", 0;
MessageManipulations 5 = 0, "Invite.Request", "Header.P-Asserted-identity exists",
"Header.P-Asserted-identity", 2, "'Unavailable<sip:'+
header.contact.url.user+'@12.xxx.xxx.xxx>'", 0;
MessageManipulations 6 = 0, "Invite.Request", "Header.P-Asserted-identity
!exists", "Header.P-Asserted-identity", 0,
"'Unavailable<sip:'+header.contact.url.user+'@12.xxx.xxx.xxx>'", 0;
MessageManipulations 7 = 0, "Invite.Request", "", "Header.Privacy", 0, "'id'", 0;
MessageManipulations 8 = 3, "", "", "Header.Contact.url.user", 2, "'gcsbc01'", 0;
MessageManipulations 9 = 0, "Invite.Request", "Header.P-Asserted-identity.URL.host
contains 'angel.z101.gch.com'", "Header.P-Asserted-identity.URL.host", 2,
"'12.xxx.xxx.xxx'", 0;
MessageManipulations 13 = 4, "Invite.Request", "Header.Request-uri.URL.user !=
Header.to.url.user", "Header.Diversion", 0, "'919xxxxx00'+'<sip:'
+'919xxxxx00'+'@12.xxx.xxx.xxx>'+';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;
;lab only
MessageManipulations 20 = 18, "Any.Request", "header.contact.URL.user ==
'919xxx3620'", "header.contact.URL.user", 2, "'732xxxxxx5'", 0;
MessageManipulations 22 = 18, "Any.Request", "header.contact.URL.user ==
'919xxx3622'", "header.contact.URL.user", 2, "'732xxxxxx6'", 0;
MessageManipulations 24 = 19, "Any.Request", "header.contact.URL.user ==
'919xxx3623'", "header.contact.URL.user", 2, " '732xxxxxx7'", 0;
;production
MessageManipulations 26 = 18, "Any.Response", "Header.To.Url.Host contains
'angel.z101.gch.com'", "header.to.url.host", 2, "'207.xxx.xxx.210'", 0;
;lab only
MessageManipulations 27 = 18, "Any.Response", "Header.contact.url.user ==
'919xxx3620'", "Header.contact.url.user", 2, "'732xxxxxx5'", 0;
;production
MessageManipulations 28 = 18, "Any.Request", "Header.From.Url.Host contains
'angel.z101.gch.com'", "Header.From.Url.Host", 2, "'173.xxx.xxx.68'", 0;
MessageManipulations 29 = 18, "Invite.Request", "", "Header.Privacy", 0, "'id'",
0;
MessageManipulations 30 = 18, "Invite.Request", "Header.P-Asserted-identity
exists", "Header.P-Asserted-identity", 2, ''"Unavailable"<sip:'+
header.contact.url.user+'@173.xxx.xxx.68>'', 0;
MessageManipulations 31 = 18, "Invite.Request", "Header.P-Asserted-identity
!exists", "Header.P-Asserted-identity", 0,
''"Unavailable"<sip:'+header.contact.url.user+'@173.xxx.xxx.68>'', 0;
MessageManipulations 33 = 18, "Invite.request", "", "header.from.url.user", 2,
"'anonymous'", 0;
```

```
MessageManipulations 34 = 18, "Invite.Request", "", "header.from.name", 2,
'"Anonymous"', 0;
MessageManipulations 35 = 18, "Invite.Request", "Header.P-Asserted-
identity.URL.host contains 'angel.z101.gch.com'", "Header.P-Asserted-
identity.URL.host", 2, "'173.xxx.xxx.68'", 0;
MessageManipulations 36 = 20, "Invite.Request", "", "header.from.url.user", 2,
"header.contact.url.user", 0;
; lab only
MessageManipulations 37 = 17, "Any.Request", "header.REQUEST-URI.url.user ==
'7323200435'", "Header.To.Url.user", 2, "'919xxx3620'", 0;
;lab only - used to discard a 180 message back to AT&T in order to generate an
error condition
MessageManipulations 38 = 13, "Invite.Request", "", "var.call.src.0", 2, "'1'", 0;
MessageManipulations 39 = 14, "Invite.Response.180", "var.call.src.0 == '1' AND
Body.sdp !exists", "header.Request-Uri.methodtype", 2, "'402'", 0;
MessageManipulations 40 = 14, "", "", "var.call.src.0", 2, "'0'", 1;
; for Network Based Blind Call Txfr using REFER
MessageManipulations 41 = 4, "", "header.Referred-By.url.host contains
'angel.z101.gch.com'", "header.Referred-By.url.host", 2, "'173.xxx.xxx.68'", 0;
MessageManipulations 42 = 4, "", "header.Referred-By.url.user == '919xxx3620'",
"header.Referred-By.url.user", 2, "'732xxxxxx5'", 0;
; production - rebuilding the Refer-To to topology hide
MessageManipulations 43 = 18, "", "header.Refer-To exists",
"header.contact.url.user", 2, "header.from.url.user", 0;
MessageManipulations 44 = 18, "", "Header.Refer-To exists and Header.Refer-To
regex(<sip:)(.*)(@)(.*)", "Header.Refer-To", 1, "", 0;
MessageManipulations 45 = 18, "", "", "Header.Refer-To", 0,
"$1+$2+$3+'207.xxx.xxx.210>'", 1;

[ \MessageManipulations ]


[ RoutingRuleGroups ]

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

[ \RoutingRuleGroups ]


[ LoggingFilters ]

FORMAT LoggingFilters_Index = LoggingFilters_FilterType, LoggingFilters_Value,
LoggingFilters_Syslog, LoggingFilters_CaptureType;
LoggingFilters 0 = 1, "", 1, 3;

[ \LoggingFilters ]


[ ResourcePriorityNetworkDomains ]

FORMAT ResourcePriorityNetworkDomains_Index = ResourcePriorityNetworkDomains_Name,
ResourcePriorityNetworkDomains_Ip2TelInterworking;
ResourcePriorityNetworkDomains 1 = "dsn", 0;
ResourcePriorityNetworkDomains 2 = "dod", 0;
ResourcePriorityNetworkDomains 3 = "drsn", 0;
ResourcePriorityNetworkDomains 5 = "uc", 1;
ResourcePriorityNetworkDomains 7 = "cuc", 0;

[ \ResourcePriorityNetworkDomains ]
```

4.4.2 Mediant Software E-SBC

Note: Example Mediant E-SBC configuration files are added here for reference purposes only. In this Mediant Software E-SBC example, the IP Toll Free SIP Trunk interfaces over the PUBSIP Interface, not the ATTDMZ interface as exemplified in document. There is a single IPBE, 207.xxx.xxx.210 in this instance. The applicable manipulation sets are 3, 4, & 18. The ATTDMZ interface exemplifies working with primary and secondary IPBE. This Mediant Software E-SBC will behave the same as the Mediant 4000 ESBC in the previous example.

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

;Board: Mediant SW
;Serial Number: 2035868
;Slot Number: 1
;Software Version: 6.60A.029.008
;DSP Software Version: 5039AE3_R => 660.15
;Board IP Address: 10.38.20.30
;Board Subnet Mask: 255.255.255.0
;Board Default Gateway: 10.38.20.1
;Ram size: 3917M   Flash size: 0M
;Num of DSP Cores: 0  Num DSP Channels: 0
;Profile: NONE
;Key features:;Board Type: Mediant SW ;Coders: G723 G729 G728 NETCODER GSM-FR GSM-
EFR AMR EVRC-QCELP G727 ILBC EVRC-B AMR-WB G722 EG711 ;Channel Type: DspCh=2000
IPMediaDspCh=2000 ;HA ;E1Trunks=0 ;T1Trunks=0 ;QOE features:
VoiceQualityMonitoring MediaEnhancement ;DSP Voice features: RTCP-XR ;Security:
IPSEC MediaEncryption StrongEncryption EncryptControlProtocol ;Control Protocols:
MGCP MEGACO SIP SASurvivability SBC=1000 ;Default features:;Coders: G711 G726;
;----------------------------------------------


[SYSTEM Params]

SyslogServerIP = 10.38.5.90
EnableSyslog = 1
NTPServerUTCOffset = -18000
ActivityListToLog = 'naa'
DebugRecordingDestIP = 10.38.5.79
DayLightSavingTimeStart = '03:01:00:00'
DayLightSavingTimeEnd = '11:01:00:00'
DayLightSavingTimeEnable = 1
SyslogFacility = 23
DebugRecordingStatus = 1
LDAPSEARCHDNSINPARALLEL = 0

[BSP Params]

PCMLawSelect = 3
TDMBusType = 0
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

[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

[Voice Engine Params]

IdlePCMPattern = 85

[WEB Params]

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

[SIP Params]

MEDIACHANNELS = 512
GWDEBUGLEVEL = 5
PROXYREDUNDANCYMODE = 1
ENABLEUSERINFOUSAGE = 1
SetDefaultOnIniFileProcess = 0
ALLOWUNCLASSIFIEDCALLS = 1
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
SBCMAXFORWARDSLIMIT = 70
SBCGRUUMODE = 0
AUTHQOP = 0

[IPsec 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

[ PhysicalPortsTable ]
```

```
FORMAT PhysicalPortsTable_Index = PhysicalPortsTable_Port,
PhysicalPortsTable_Mode, PhysicalPortsTable_NativeVlan,
PhysicalPortsTable_SpeedDuplex, PhysicalPortsTable_PortDescription,
PhysicalPortsTable_GroupMember, PhysicalPortsTable_GroupStatus;
PhysicalPortsTable 0 = "GE_1", 1, 1, 4, "User Port #0", "GROUP_1", "Active";
PhysicalPortsTable 1 = "GE_2", 1, 1, 4, "User Port #1", "GROUP_2", "Active";

[ \PhysicalPortsTable ]


[ EtherGroupTable ]

FORMAT EtherGroupTable_Index = EtherGroupTable_Group, EtherGroupTable_Mode,
EtherGroupTable_Member1, EtherGroupTable_Member2;
EtherGroupTable 0 = "GROUP_1", 3, GE_1, ;
EtherGroupTable 1 = "GROUP_2", 3, GE_2, ;

[ \EtherGroupTable ]


[ InterfaceTable ]

FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway, InterfaceTable_VlanID,
InterfaceTable_InterfaceName, InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress, InterfaceTable_UnderlyingInterface;
InterfaceTable 0 = 0, 10, 10.38.20.30, 24, 10.38.20.1, 320, "NETMGMT", 0.0.0.0,
0.0.0.0, GROUP_1;
InterfaceTable 1 = 5, 10, 173.xxx.xxx.68, 26, 173.xxx.xxx.65, 254, "PUBSIP",
0.0.0.0, 0.0.0.0, GROUP_2;
InterfaceTable 2 = 5, 10, 10.38.60.10, 24, 10.38.60.1, 360, "RALVOX", 0.0.0.0,
0.0.0.0, GROUP_1;
InterfaceTable 3 = 5, 10, 12.xxx.xxx.xxx, 29, 12.xxx.xxx.xxx, 455, "ATTDMZ",
0.0.0.0, 0.0.0.0, GROUP_2;
InterfaceTable 4 = 5, 10, 10.38.5.10, 24, 10.38.5.1, 305, "RALOFFICE", 0.0.0.0,
0.0.0.0, GROUP_1;

[ \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.xxx.xxx.x", 32, 0, 65535, "Any", 1, ATTDMZ, 0, 0, 0, "ALLOW",
0;
ACCESSLIST 1 = "12.xxx.xxx.y", 32, 0, 65535, "Any", 1, ATTDMZ, 0, 0, 0, "ALLOW",
0;
ACCESSLIST 2 = "12.xxx.xxx.z", 32, 0, 65535, "Any", 1, ATTDMZ, 0, 0, 0, "ALLOW",
0;
ACCESSLIST 3 = "12.xxx.xxx.a", 32, 0, 65535, "Any", 1, ATTDMZ, 0, 0, 0, "ALLOW",
0;
ACCESSLIST 4 = "12.xxx.xxx.230", 32, 0, 65535, "Any", 1, ATTDMZ, 0, 0, 0, "ALLOW",
0;
ACCESSLIST 5 = "0.0.0.0", 0, 0, 65535, "Any", 1, ATTDMZ, 0, 0, 0, "BLOCK", 0;
ACCESSLIST 17 = "173.xxx.xxx.87", 32, 0, 65535, "Any", 1, PUBSIP, 0, 0, 0,
"Allow", 0;
ACCESSLIST 18 = "173.xxx.xxx.89", 32, 0, 65535, "Any", 1, PUBSIP, 0, 0, 0,
"Allow", 0;
ACCESSLIST 19 = "173.xxx.xxx.90", 32, 0, 65535, "Any", 1, PUBSIP, 0, 0, 0,
"Allow", 0;
ACCESSLIST 21 = "207.xxx.xxx.210", 32, 0, 65535, "Any", 1, PUBSIP, 0, 0, 0,
"Allow", 0;
```

```
ACCESSLIST 25 = "0.0.0.0", 0, 0, 65535, "Any", 1, PUBSIP, 0, 0, 0, "BLOCK", 0;

[ \ACCESSLIST ]


[ DspTemplates ]

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

[ \DspTemplates ]

[ CpMediaRealm ]

FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName, CpMediaRealm_IPv4IF,
CpMediaRealm_IPv6IF, CpMediaRealm_PortRangeStart, CpMediaRealm_MediaSessionLeg,
CpMediaRealm_PortRangeEnd, CpMediaRealm_IsDefault;
CpMediaRealm 0 = "ATTDMZ_MR", ATTDMZ, , 16390, 600, 22380, 1;
CpMediaRealm 1 = "RALVOX_MR", RALVOX, , 6000, 50, 6490, 0;
CpMediaRealm 2 = "RALLOFFICE_MR", RALOFFICE, , 6500, 550, 11990, 0;
CpMediaRealm 3 = "TWCDMZ_MR", PUBSIP, , 16390, 100, 17380, 0;

[ \CpMediaRealm ]


[ QOERules ]

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

[ \QOERules ]


[ SRD ]

FORMAT SRD_Index = SRD_Name, SRD_MediaRealm, SRD_IntraSRDMediaAnchoring,
SRD_BlockUnRegUsers, SRD_MaxNumOfRegUsers, SRD_EnableUnAuthenticatedRegistrations;
SRD 1 = "ATTDMZ_SRD", "ATTDMZ_MR", 0, 1, -1, 0;
SRD 2 = "RALVOX_SRD", "RALVOX_MR", 1, 0, -1, 1;
SRD 3 = "RALOFFICE_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.gch.com", 10.38.5.117, 0.0.0.0, 0.0.0.0, 0.0.0.0;

[ \Dns2Ip ]


[ ProxyIp ]
```

```
FORMAT ProxyIp_Index = ProxyIp_IpAddress, ProxyIp_TransportType,
ProxyIp_ProxySetId;
ProxyIp 0 = "12.xxx.xxx.x", -1, 1;
ProxyIp 1 = "173.xxx.xxx.89", -1, 8;
ProxyIp 2 = "rtpsip.cl.gch.com", 0, 3;
ProxyIp 3 = "12.xxx.xxx.y", -1, 2;
ProxyIp 4 = "207.xxx.xxx.210", -1, 4;

[ \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_CNGmode, 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_SBCDiversionMode, IpProfile_SBCHistoryInfoMode,
IpProfile_EnableQSIGTunneling, IpProfile_SBCFaxCodersGroupID,
IpProfile_SBCFaxBehavior, IpProfile_SBCFaxOfferMode, IpProfile_SBCFaxAnswerMode,
IpProfile_SbcPrackMode, IpProfile_SBCSessionExpiresMode,
IpProfile_SBCRemoteUpdateSupport, IpProfile_SBCRemoteReinviteSupport,
IpProfile_SBCRemoteDelayedOfferSupport, IpProfile_SBCRemoteReferBehavior,
IpProfile_SBCRemote3xxBehavior, IpProfile_SBCRemoteMultiple18xSupport,
IpProfile_SBCRemoteEarlyMediaResponseType, IpProfile_SBCRemoteEarlyMediaSupport,
IpProfile_EnableSymmetricMKI, IpProfile_MKISize, IpProfile_SBCEnforceMKISize,
IpProfile_SBCRemoteEarlyMediaRTP, IpProfile_SBCRemoteSupportsRFC3960,
IpProfile_SBCRemoteCanPlayRingback, IpProfile_EnableEarly183,
IpProfile_EarlyAnswerTimeout, IpProfile_SBC2833DTMFPayloadType,
IpProfile_SBCUserRegistrationTime, IpProfile_ResetSRTPStateUponRekey;
IpProfile 1 = "ATT IP Flex", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0, 0, -
1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", -1, 0, 0, 0, 2, 0, 0, 0, 0, 0, 8, 300,
400, 0, -1, 0, -1, 0, 0, 1, 3, 0, 2, 2, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 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 4 = 1, 60, 0, 0, 5, 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_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName;
IPGroup 1 = 0, "ATT IPGROUP", 1, "12.xxx.xxx.x", "", 0, -1, 0, 0, -1, 1,
"ATTDMZ_MR", 1, 1, -1, -1, 0, 0, 0, "", 0, -1, -1, "";
IPGroup 2 = 0, "ATT IPGroup Secondary", 2, "12.xxx.xxx.y", "", 0, -1, 0, 0, -1, 1,
"ATTDMZ_MR", 1, 1, -1, -1, 0, 0, 0, "", 0, -1, -1, "";
IPGroup 3 = 0, "GENESYS_SRV", 3, "angel.z101.gch.com", "", 0, -1, 0, 0, -1, 3,
"RALLOFFICE_MR", 1, 0, -1, 4, 3, 0, 0, "", 0, -1, -1, "";
IPGroup 4 = 1, "", -1, "", "", 0, 2, 0, 0, -1, 0, "", 1, 0, -1, -1, -1, 0, 0, "",
0, -1, -1, "";
IPGroup 5 = 1, "ATT Phone", -1, "", "", 0, -1, 0, 0, -1, 1, "ATTDMZ_MR", 0, 0, -1,
-1, -1, 0, 2, "REGISTER", 0, -1, -1, "";
IPGroup 6 = 1, "TWC USERS", -1, "", "", 0, -1, 0, 0, -1, 5, "TWCDMZ_MR", 0, 0, -1,
-1, -1, 0, 2, "REGISTER", 0, -1, -1, "";
IPGroup 7 = 1, "ATT Remote Agents", -1, "", "", 0, -1, 0, 0, -1, 1, "ATTDMZ_MR",
0, 0, -1, -1, -1, 0, 0, "", 0, -1, -1, "";
IPGroup 8 = 1, "TWC Remote Agents", -1, "", "", 0, -1, 0, 0, -1, 5, "TWCDMZ_MR",
0, 0, -1, -1, -1, 0, 0, "", 0, -1, -1, "";
IPGroup 9 = 0, "732 Remote agents", 4, "207.xxx.xxx.210", "", 0, -1, -1, 0, -1, 5,
"TWCDMZ_MR", 1, 1, -1, 17, 18, 0, 0, "", 0, -1, -1, ""

[ \IPGroup ]


[ IP2IPRouting ]

FORMAT IP2IPRouting_Index = IP2IPRouting_SrcIPGroupID,
IP2IPRouting_SrcUsernamePrefix, IP2IPRouting_SrcHost,
IP2IPRouting_DestUsernamePrefix, IP2IPRouting_DestHost, IP2IPRouting_RequestType,
IP2IPRouting_MessageCondition, IP2IPRouting_ReRouteIPGroupID,
IP2IPRouting_Trigger, IP2IPRouting_DestType, IP2IPRouting_DestIPGroupID,
IP2IPRouting_DestSRDID, IP2IPRouting_DestAddress, IP2IPRouting_DestPort,
IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions,
IP2IPRouting_CostGroup;
IP2IPRouting 1 = 5, "*", "*", "*", "*", 2, , -1, 0, 0, 5, , "", 0, -1, 0, ;
IP2IPRouting 3 = 7, "*", "*", "*", "*", 0, , -1, 0, 0, 3, 3, "", 0, -1, 0, ;
IP2IPRouting 4 = 8, "*", "*", "*", "*", 0, , -1, 0, 0, 3, 3, "", 0, -1, 0, ;
IP2IPRouting 5 = 9, "*", "*", "*", "*", 0, , -1, 0, 0, 3, 3, "", 0, -1, 0, ;
IP2IPRouting 6 = 6, "*", "*", "*", "*", 2, , -1, 0, 0, 6, , "", 0, -1, 0, ;
IP2IPRouting 7 = 1, "*", "*", "919xxx", "*", 0, , -1, 0, 0, 3, 3, "", 0, -1, 0, ;
IP2IPRouting 8 = 2, "*", "*", "919xxx", "*", 0, , -1, 0, 0, 3, 3, "", 0, -1, 0, ;
IP2IPRouting 9 = 3, "*", "*", "919xxxxxx5", "*", 0, , -1, 0, 0, 7, 1, "", 0, -1,
0, ;
IP2IPRouting 10 = 3, "*", "*", "919xxxxxx[7-8]", "*", 0, , -1, 0, 0, 8, 5, "", 0,
-1, 0, ;
IP2IPRouting 11 = 1, "*", "*", "202xxxxxx[5-6]", "*", 0, , -1, 0, 0, 3, 3, "", 0,
-1, 0, ;
IP2IPRouting 12 = 2, "*", "*", "202xxxxxx[5-6]", "*", 0, , -1, 0, 0, 3, 3, "", 0,
-1, 0, ;
IP2IPRouting 13 = 1, "*", "*", "202xxxxxx7", "*", 0, , -1, 0, 0, 5, 1, "", 0, -1,
0, ;
IP2IPRouting 14 = 2, "*", "*", "202xxxxxx7", "*", 0, , -1, 0, 0, 5, 1, "", 0, -1,
0, ;
IP2IPRouting 15 = 1, "*", "*", "202xxxxxx[8-9]", "*", 0, , -1, 0, 0, 8, 5, "", 0,
-1, 0, ;
IP2IPRouting 16 = 2, "*", "*", "202xxxxxx[8-9]", "*", 0, , -1, 0, 0, 8, 5, "", 0,
-1, 0, ;
IP2IPRouting 17 = 1, "*", "*", "202xxxxxx0", "*", 0, , -1, 0, 0, 6, 5, "", 0, -1,
0, ;
```

```
IP2IPRouting 18 = 2, "*", "*", "202xxxxxx0", "*", 0, , -1, 0, 0, 6, 5, "", 0, -1,
0, ;
IP2IPRouting 19 = 5, "*", "*", "202xxxxxx0", "*", 0, , -1, 0, 0, 6, 5, "", 0, -1,
0, ;
IP2IPRouting 20 = 5, "*", "*", "919xxx36[00-39]", "*", 0, , -1, 0, 0, 3, 3, "", 0,
-1, 0, ;
IP2IPRouting 21 = 6, "*", "*", "919xxx", "*", 0, , -1, 0, 0, 3, 3, "", 0, -1, 0, ;
IP2IPRouting 22 = 8, "*", "*", "919xxx", "*", 0, , -1, 0, 0, 3, 3, "", 0, -1, 0, ;
IP2IPRouting 23 = 5, "202", "*", "919xxxx[450-515]", "*", 0, , -1, 0, 0, 1, 1, "",
0, -1, 0, ;
IP2IPRouting 24 = 5, "202", "*", "919xxxx[450-515]", "*", 0, , -1, 0, 0, 2, 1, "",
0, -1, 0, ;
IP2IPRouting 25 = 5, "*", "*", "01141583330158", "*", 0, , -1, 0, 0, 1, 1, "", 0,
-1, 0, ;
IP2IPRouting 26 = 5, "*", "*", "01141583330158", "*", 0, , -1, 0, 0, 2, 1, "", 0,
-1, 0, ;
IP2IPRouting 27 = 3, "*", "*", "[*73]", "*", 0, , -1, 0, 0, 9, 5, "", 0, -1, 0, ;
IP2IPRouting 28 = 3, "*", "*", "[*72]919xxxx[450-515]", "*", 0, , -1, 0, 0, 9, 5,
"", 0, -1, 0, ;
IP2IPRouting 29 = 3, "*", "*", "[*90]919xxxx492", "*", 0, , -1, 0, 0, 9, 5, "", 0,
-1, 0, ;
IP2IPRouting 30 = 3, "*", "*", "[*91]", "*", 0, , -1, 0, 0, 9, 5, "", 0, -1, 0, ;
IP2IPRouting 31 = 3, "*", "*", "[*92]919xxxx492", "*", 0, , -1, 0, 0, 9, 5, "", 0,
-1, 0, ;
IP2IPRouting 32 = 3, "*", "*", "[*93]", "*", 0, , -1, 0, 0, 9, 5, "", 0, -1, 0, ;
IP2IPRouting 33 = 3, "*", "*", "[*94]919xxxx492", "*", 0, , -1, 0, 0, 9, 5, "", 0,
-1, 0, ;
IP2IPRouting 34 = 3, "*", "*", "[*95]", "*", 0, , -1, 0, 0, 9, 5, "", 0, -1, 0, ;
IP2IPRouting 35 = 3, "*", "*", "*", "*", 0, , -1, 0, 0, 9, 5, "", 0, -1, 0, ;
IP2IPRouting 36 = 3, "*", "*", "*", "*", 0, , -1, 0, 0, 2, 1, "", 0, -1, 0, ;
IP2IPRouting 37 = 5, "*", "*", "18888064788", "*", 0, , -1, 0, 0, 1, 1, "", 0, -1,
0, ;
IP2IPRouting 38 = 5, "*", "*", "18888064788", "*", 0, , -1, 0, 0, 2, 1, "", 0, -1,
0, ;
IP2IPRouting 39 = 6, "*", "*", "18888064788", "*", 0, , -1, 0, 0, 2, 1, "", 0, -1,
0, ;
IP2IPRouting 40 = 6, "*", "*", "18888064788", "*", 0, , -1, 0, 0, 2, 1, "", 0, -1,
0, ;
IP2IPRouting 41 = 1, "*", "*", "000008883539397", "*", 0, , -1, 0, 0, 3, 3, "", 0,
-1, 0, ;

[ \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 1 = , 5, "207.xxx.xxx.210", 0, -1, "*", "*", "*", "*", 1, 9;
Classification 2 = , 5, "173.xxx.xxx.*", 0, -1, "202xxxxxx[8-9]", "*", "*", "*",
1, 8;
Classification 3 = , 5, "173.xxx.xxx.*", 0, -1, "919xxxxxx[7-8]", "*", "*", "*",
1, 8;
Classification 4 = , 5, "173.xxx.xxx.*", 0, -1, "2027582830", "*", "*", "*", 1, 6;
Classification 5 = , 1, "12.xxx.xxx.*", 0, -1, "202xxxxxx7", "*", "*", "*", 1, 5;
Classification 6 = , 1, "12.xxx.xxx.*", 0, -1, "202xxxxxx[8-9]", "*", "*", "*", 1,
8;
Classification 7 = , 1, "12.xxx.xxx.*", 0, -1, "919xxxxxx5", "*", "*", "*", 1, 7;

[ \Classification ]


[ SIPInterface ]
```

```
FORMAT SIPInterface_Index = SIPInterface_NetworkInterface,
SIPInterface_ApplicationType, SIPInterface_UDPPort, SIPInterface_TCPPort,
SIPInterface_TLSPort, SIPInterface_SRD, SIPInterface_MessagePolicy,
SIPInterface_TLSMutualAuthentication, SIPInterface_TCPKeepaliveEnable,
SIPInterface_ClassificationFailureResponseType;
SIPInterface 1 = "ATTDMZ", 2, 5060, 5060, 5061, 1, , -1, 0, 500;
SIPInterface 2 = "RALVOX", 2, 5060, 5060, 5061, 2, , -1, 0, 500;
SIPInterface 3 = "RALOFFICE", 2, 5060, 5060, 5061, 3, , -1, 0, 500;
SIPInterface 5 = "PUBSIP", 2, 5060, 5060, 5061, 5, , -1, 0, 500;

[ \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 1 = 0, 0, 1, "*", "*", "000008883539397", "*", 0, 1, 15, 0,
255, "919xxx3620", "";
IPInboundManipulation 3 = 0, 0, 2, "*", "*", "29436xx", "*", 0, 1, 0, 0, 255,
"919", "";
IPInboundManipulation 4 = 0, 0, 9, "*", "*", "732xxxxxx5", "*", 0, 1, 10, 0, 255,
"919xxx3620", "";
IPInboundManipulation 5 = 0, 0, 9, "*", "*", "732xxxxxx6", "*", 0, 1, 10, 0, 255,
"919xxx3622", "";
IPInboundManipulation 6 = 0, 0, 9, "*", "*", "732xxxxxx7", "*", 0, 1, 10, 0, 255,
"919xxx3623", "";

[ \IPInboundManipulation ]


[ CodersGroup0 ]

FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime,
CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce;
CodersGroup0 0 = "g729", 20, 0, -1, 0;
CodersGroup0 1 = "g711Ulaw64k", 20, 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, "Any.Response", "Header.To.Url.Host contains
'angel.z101.gch.com'", "Header.To.Url.Host", 2, "'12.xxx.xxx.xxx'", 0;
MessageManipulations 4 = 0, "Any.Request", "Header.From.Url.Host contains
'angel.z101.gch.com'", "Header.From.Url.Host", 2, "'12.xxx.xxx.xxx'", 0;
MessageManipulations 5 = 0, "Invite.Request", "Header.P-Asserted-identity exists",
"Header.P-Asserted-identity", 2, "'Unavailable<sip:'+
header.contact.url.user+'@12.xxx.xxx.xxx>'", 0;
MessageManipulations 6 = 0, "Invite.Request", "Header.P-Asserted-identity
!exists", "Header.P-Asserted-identity", 0,
"'Unavailable<sip:'+header.contact.url.user+'@12.xxx.xxx.xxx>'", 0;
MessageManipulations 7 = 0, "Invite.Request", "", "Header.Privacy", 0, "'id'", 0;
MessageManipulations 8 = 3, "", "", "Header.Contact.url.user", 2, "'gcsbc01'", 0;
MessageManipulations 9 = 0, "Invite.Request", "Header.P-Asserted-identity.URL.host
contains 'angel.z101.gch.com'", "Header.P-Asserted-identity.URL.host", 2,
"'12.xxx.xxx.xxx'", 0;
MessageManipulations 13 = 4, "Invite.Request", "Header.Request-uri.URL.user !=
Header.to.url.user", "Header.Diversion", 0, "'919xxxxx00'+'<sip:'
+'919xxxxx00'+'@12.xxx.xxx.xxx>'+';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;
;lab only
MessageManipulations 20 = 18, "Any.Request", "header.contact.URL.user ==
'919xxx3620'", "header.contact.URL.user", 2, "'732xxxxxx5'", 0;
MessageManipulations 22 = 18, "Any.Request", "header.contact.URL.user ==
'919xxx3622'", "header.contact.URL.user", 2, "'732xxxxxx6'", 0;
MessageManipulations 24 = 19, "Any.Request", "header.contact.URL.user ==
'919xxx3623'", "header.contact.URL.user", 2, " '732xxxxxx7'", 0;
;production
MessageManipulations 26 = 18, "Any.Response", "Header.To.Url.Host contains
'angel.z101.gch.com'", "header.to.url.host", 2, "'207.xxx.xxx.210'", 0;
;lab only
MessageManipulations 27 = 18, "Any.Response", "Header.contact.url.user ==
'919xxx3620'", "Header.contact.url.user", 2, "'732xxxxxx5'", 0;
;production
MessageManipulations 28 = 18, "Any.Request", "Header.From.Url.Host contains
'angel.z101.gch.com'", "Header.From.Url.Host", 2, "'173.xxx.xxx.68'", 0;
MessageManipulations 29 = 18, "Invite.Request", "", "Header.Privacy", 0, "'id'",
0;
MessageManipulations 30 = 18, "Invite.Request", "Header.P-Asserted-identity
exists", "Header.P-Asserted-identity", 2, '"Unavailable"<sip:'+
header.contact.url.user+'@173.xxx.xxx.68>'', 0;
MessageManipulations 31 = 18, "Invite.Request", "Header.P-Asserted-identity
!exists", "Header.P-Asserted-identity", 0,
'"Unavailable"<sip:'+header.contact.url.user+'@173.xxx.xxx.68>'', 0;
MessageManipulations 33 = 18, "Invite.request", "", "header.from.url.user", 2,
"'anonymous'", 0;
MessageManipulations 34 = 18, "Invite.Request", "", "header.from.name", 2,
'"Anonymous"', 0;
MessageManipulations 35 = 18, "Invite.Request", "Header.P-Asserted-
identity.URL.host contains 'angel.z101.gch.com'", "Header.P-Asserted-
identity.URL.host", 2, "'173.xxx.xxx.68'", 0;
MessageManipulations 36 = 20, "Invite.Request", "", "header.from.url.user", 2,
"header.contact.url.user", 0;
; lab only
MessageManipulations 37 = 17, "Any.Request", "header.REQUEST-URI.url.user ==
'7323200435'", "Header.To.Url.user", 2, "'919xxx3620'", 0;
;lab only - used to discard a 180 message back to AT&T in order to generate an
error condition
MessageManipulations 38 = 13, "Invite.Request", "", "var.call.src.0", 2, "'1'", 0;
MessageManipulations 39 = 14, "Invite.Response.180", "var.call.src.0 == '1' AND
Body.sdp !exists", "header.Request-Uri.methodtype", 2, "'402'", 0;
MessageManipulations 40 = 14, "", "", "var.call.src.0", 2, "'0'", 1;
; for Network Based Blind Call Txfr using REFER
MessageManipulations 41 = 4, "", "header.Referred-By.url.host contains
'angel.z101.gch.com'", "header.Referred-By.url.host", 2, "'173.xxx.xxx.68'", 0;
```

```
MessageManipulations 42 = 4, "", "header.Referred-By.url.user == '919xxx3620'",
"header.Referred-By.url.user", 2, "'732xxxxxx5'", 0;
; production - rebuilding the Refer-To to topology hide
MessageManipulations 43 = 18, "", "header.Refer-To exists",
"header.contact.url.user", 2, "header.from.url.user", 0;
MessageManipulations 44 = 18, "", "Header.Refer-To exists and Header.Refer-To
regex(<sip:)(.*)(@)(.*)", "Header.Refer-To", 1, "", 0;
MessageManipulations 45 = 18, "", "", "Header.Refer-To", 0,
"$1+$2+$3+'207.xxx.xxx.210>'", 1;

[ \MessageManipulations ]


[ RoutingRuleGroups ]

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

[ \RoutingRuleGroups ]


[ LoggingFilters ]

FORMAT LoggingFilters_Index = LoggingFilters_FilterType, LoggingFilters_Value,
LoggingFilters_Syslog, LoggingFilters_CaptureType;
LoggingFilters 0 = 1, "", 1, 3;

[ \LoggingFilters ]


[ ResourcePriorityNetworkDomains ]

FORMAT ResourcePriorityNetworkDomains_Index = ResourcePriorityNetworkDomains_Name,
ResourcePriorityNetworkDomains_Ip2TelInterworking;
ResourcePriorityNetworkDomains 1 = "dsn", 0;
ResourcePriorityNetworkDomains 2 = "dod", 0;
ResourcePriorityNetworkDomains 3 = "drsn", 0;
ResourcePriorityNetworkDomains 5 = "uc", 1;
ResourcePriorityNetworkDomains 7 = "cuc", 0;

[ \ResourcePriorityNetworkDomains ]
```

4.4.3 Mediant 3000 E-SBC

> **Note:** Example Mediant E-SBC configuration files are added here for reference purposes only. In this Mediant 3000 E-SBC example, the IP Toll Free SIP Trunk interfaces over the PUBSIP Interface, not the ATTDMZ interface, as exemplified in the document. There is a single IPBE, 207.xxx.xxx.210 in this instance. The applicable manipulation sets are 3, 4, & 18. The ATTDMZ interface exemplifies working with primary and secondary IPBE. This Mediant Software E-SBC will behave the same as the Mediant Software & Mediant 4000 ESBCs in the previous examples.

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

;Board: Mediant 3000
;M3K Board Type: TrunkPack 6310
;Serial Number: 3218534
;Slot Number: 1
;Software Version: 6.60A.029.008
;DSP Software Version: 491096AE3 => 660.31
;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]

SyslogServerIP = 10.38.5.90
EnableSyslog = 1
NTPServerUTCOffset = -18000
ActivityListToLog = 'naa'
DayLightSavingTimeStart = '03:01:00:00'
DayLightSavingTimeEnd = '11:01:00:00'
DayLightSavingTimeEnable = 1
NTPServerIP = '66.228.35.252'
LDAPSEARCHDNSINPARALLEL = 0

[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
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
SetDefaultOnIniFileProcess = 0
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
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.xxx.xxx.68, 26, 173.xxx.xxx.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.xxx.xxx.xxx, 29, 12.xxx.xxx.xxx, 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.xxx.xxx.x", 32, 0, 65535, "Any", 1, ATTDMZ, 0, 0, 0, "ALLOW",
0;
ACCESSLIST 1 = "12.xxx.xxx.y", 32, 0, 65535, "Any", 1, ATTDMZ, 0, 0, 0, "ALLOW",
0;
ACCESSLIST 2 = "12.xxx.xxx.z", 32, 0, 65535, "Any", 1, ATTDMZ, 0, 0, 0, "ALLOW",
0;
ACCESSLIST 3 = "12.xxx.xxx.20", 32, 0, 65535, "Any", 1, ATTDMZ, 0, 0, 0, "ALLOW",
0;
ACCESSLIST 4 = "12.xxx.xxx.230", 32, 0, 65535, "Any", 1, PUBSIP, 0, 0, 0, "BLOCK",
0;
ACCESSLIST 5 = "50.xxx.xxx.xx", 32, 0, 65535, "Any", 1, ATTDMZ, 0, 0, 0, "ALLOW",
0;
ACCESSLIST 6 = "0.0.0.0", 0, 0, 65535, "Any", 1, ATTDMZ, 0, 0, 0, "BLOCK", 0;
ACCESSLIST 17 = "173.xxx.xxx.87", 0, 0, 65535, "Any", 1, PUBSIP, 0, 0, 0, "ALLOW",
0;
ACCESSLIST 18 = "173.xxx.xxx.89", 0, 0, 65535, "Any", 1, PUBSIP, 0, 0, 0, "ALLOW",
0;
ACCESSLIST 19 = "173.xxx.xxx.90", 0, 0, 65535, "Any", 1, PUBSIP, 0, 0, 0, "ALLOW",
0;
ACCESSLIST 21 = "207.xxx.xxx.210", 32, 0, 65535, "Any", 1, PUBSIP, 0, 0, 0,
"Allow", 0;
ACCESSLIST 25 = "0.0.0.0", 0, 0, 65535, "Any", 1, PUBSIP, 0, 0, 0, "BLOCK", 0;

[ \ACCESSLIST ]
```

```
[ DspTemplates ]

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

[ \DspTemplates ]


[ CpMediaRealm ]

FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName, CpMediaRealm_IPv4IF,
CpMediaRealm_IPv6IF, CpMediaRealm_PortRangeStart, CpMediaRealm_MediaSessionLeg,
CpMediaRealm_PortRangeEnd, CpMediaRealm_IsDefault;
CpMediaRealm 0 = "ATTDMZ_MR", ATTDMZ, , 16390, 600, 22380, 1;
CpMediaRealm 1 = "RALVOX_MR", RALVOX, , 6000, 50, 6490, 0;
CpMediaRealm 2 = "RALLOFFICE_MR", RALOFFICE, , 6500, 550, 11990, 0;
CpMediaRealm 3 = "TWCDMZ_MR", PUBSIP, , 16390, 100, 17380, 0;

[ \CpMediaRealm ]


[ QOERules ]

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

[ \QOERules ]


[ SRD ]

FORMAT SRD_Index = SRD_Name, SRD_MediaRealm, SRD_IntraSRDMediaAnchoring,
SRD_BlockUnRegUsers, SRD_MaxNumOfRegUsers, SRD_EnableUnAuthenticatedRegistrations;
SRD 1 = "ATTDMZ_SRD", "ATTDMZ_MR", 0, 1, -1, 0;
SRD 2 = "RALVOX_SRD", "RALVOX_MR", 1, 0, -1, 1;
SRD 3 = "RALOFFICE_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.gch.com", 10.38.5.117, 0.0.0.0, 0.0.0.0, 0.0.0.0;

[ \Dns2Ip ]


[ SBCAlternativeRoutingReasons ]
```

```
FORMAT SBCAlternativeRoutingReasons_Index =
SBCAlternativeRoutingReasons_ReleaseCause;
SBCAlternativeRoutingReasons 0 = 408;

[ \SBCAlternativeRoutingReasons ]


[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIp_IpAddress, ProxyIp_TransportType,
ProxyIp_ProxySetId;
ProxyIp 0 = "12.xxx.xxx.x", -1, 1;
ProxyIp 1 = "173.xxx.xxx.89", -1, 8;
ProxyIp 2 = "rtpsip.cl.gch.com", 0, 3;
ProxyIp 3 = "12.xxx.xxx.y", -1, 2;
ProxyIp 4 = "207.xxx.xxx.z", -1, 4;

[ \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_CNGmode, 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_SBCDiversionMode, IpProfile_SBCHistoryInfoMode,
IpProfile_EnableQSIGTunneling, IpProfile_SBCFaxCodersGroupID,
IpProfile_SBCFaxBehavior, IpProfile_SBCFaxOfferMode, IpProfile_SBCFaxAnswerMode,
IpProfile_SbcPrackMode, IpProfile_SBCSessionExpiresMode,
IpProfile_SBCRemoteUpdateSupport, IpProfile_SBCRemoteReinviteSupport,
IpProfile_SBCRemoteDelayedOfferSupport, IpProfile_SBCRemoteReferBehavior,
IpProfile_SBCRemote3xxBehavior, IpProfile_SBCRemoteMultiple18xSupport,
IpProfile_SBCRemoteEarlyMediaResponseType, IpProfile_SBCRemoteEarlyMediaSupport,
IpProfile_EnableSymmetricMKI, IpProfile_MKISize, IpProfile_SBCEnforceMKISize,
IpProfile_SBCRemoteEarlyMediaRTP, IpProfile_SBCRemoteSupportsRFC3960,
IpProfile_SBCRemoteCanPlayRingback, IpProfile_EnableEarly183,
IpProfile_EarlyAnswerTimeout, IpProfile_SBC2833DTMFPayloadType,
IpProfile_SBCUserRegistrationTime, IpProfile_ResetSRTPStateUponRekey;
IpProfile 1 = "ATT IP Flex", 1, 0, 0, 10, 10, 46, 40, 0, 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, 0, 0, 8, 300,
400, 0, -1, 0, -1, 0, 0, 1, 3, 0, 2, 2, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 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 4 = 1, 60, 0, 0, 5, 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_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName;
IPGroup 1 = 0, "ATT IPGROUP", 1, "12.xxx.xxx.x", "", 0, -1, 0, 0, -1, 1,
"ATTDMZ_MR", 1, 1, -1, -1, 0, 0, 0, "", 0, -1, -1, "";
IPGroup 2 = 0, "ATT IPGroup secondary", 2, "12.xxx.xxx.y", "", 0, -1, 0, 0, -1, 1,
"ATTDMZ_MR", 1, 1, -1, -1, 0, 0, 0, "", 0, -1, -1, "";
IPGroup 3 = 0, "GENESYS_SRV", 3, "angel.z101.gch.com", "", 0, -1, 0, 0, -1, 3,
"RALLOFFICE_MR", 1, 0, -1, 4, 3, 0, 0, "", 0, -1, -1, "";
IPGroup 5 = 1, "ATT Phone", -1, "", "", 0, -1, 0, 0, -1, 1, "ATTDMZ_MR", 0, 0, -1,
-1, -1, 0, 2, "REGISTER", 0, -1, -1, "";
IPGroup 6 = 1, "TWC USERS", -1, "", "", 0, -1, 0, 0, -1, 5, "TWCDMZ_MR", 0, 0, -1,
-1, -1, 0, 2, "REGISTER", 0, -1, -1, "";
IPGroup 7 = 1, "ATT Remote Agents", -1, "", "", 0, -1, 0, 0, -1, 1, "ATTDMZ_MR",
0, 0, -1, -1, -1, 0, 0, "", 0, -1, -1, "";
IPGroup 8 = 1, "TWC Remote Agents", -1, "", "", 0, -1, 0, 0, -1, 5, "TWCDMZ_MR",
0, 1, -1, -1, 7, 0, 0, "", 0, -1, -1, "";
IPGroup 9 = 0, "732 Remote agents", 4, "207.xxx.xxx.210", "", 0, -1, -1, 0, -1, 5,
"TWCDMZ_MR", 1, 1, -1, 17, 18, 0, 0, "", 0, -1, -1, "";

[ \IPGroup ]


[ IP2IPRouting ]

FORMAT IP2IPRouting_Index = IP2IPRouting_SrcIPGroupID,
IP2IPRouting_SrcUsernamePrefix, IP2IPRouting_SrcHost,
IP2IPRouting_DestUsernamePrefix, IP2IPRouting_DestHost, IP2IPRouting_RequestType,
IP2IPRouting_MessageCondition, IP2IPRouting_ReRouteIPGroupID,
IP2IPRouting_Trigger, IP2IPRouting_DestType, IP2IPRouting_DestIPGroupID,
IP2IPRouting_DestSRDID, IP2IPRouting_DestAddress, IP2IPRouting_DestPort,
IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions,
IP2IPRouting_CostGroup;
IP2IPRouting 1 = 5, "*", "*", "*", "*", 2, , -1, 0, 0, 5, , "", 0, -1, 0, ;
IP2IPRouting 3 = 7, "*", "*", "*", "*", 0, , -1, 0, 0, 3, 3, "", 0, -1, 0, ;
IP2IPRouting 4 = 8, "*", "*", "*", "*", 0, , -1, 0, 0, 3, 3, "", 0, -1, 0, ;
IP2IPRouting 5 = 9, "*", "*", "*", "*", 0, , -1, 0, 0, 3, 3, "", 0, -1, 0, ;
IP2IPRouting 6 = 6, "*", "*", "*", "*", 2, , -1, 0, 0, 6, , "", 0, -1, 0, ;
IP2IPRouting 7 = 1, "*", "*", "919xxx", "*", 0, , -1, 0, 0, 3, 3, "", 0, -1, 0, ;
IP2IPRouting 8 = 2, "*", "*", "919xxx", "*", 0, , -1, 0, 0, 3, 3, "", 0, -1, 0, ;
IP2IPRouting 9 = 3, "*", "*", "919xxxxxx5", "*", 0, , -1, 0, 0, 7, 1, "", 0, -1,
0, ;
IP2IPRouting 10 = 3, "*", "*", "919xxxxxx[7-8]", "*", 0, , -1, 0, 0, 8, 5, "", 0,
-1, 0, ;
IP2IPRouting 11 = 1, "*", "*", "202xxxxxx[5-6]", "*", 0, , -1, 0, 0, 3, 3, "", 0,
-1, 0, ;
IP2IPRouting 12 = 2, "*", "*", "202xxxxxx[5-6]", "*", 0, , -1, 0, 0, 3, 3, "", 0,
-1, 0, ;
IP2IPRouting 13 = 1, "*", "*", "202xxxxxx7", "*", 0, , -1, 0, 0, 5, 1, "", 0, -1,
0, ;
IP2IPRouting 14 = 2, "*", "*", "202xxxxxx7", "*", 0, , -1, 0, 0, 5, 1, "", 0, -1,
0, ;
```

```
IP2IPRouting 15 = 1, "*", "*", "202xxxxxx[8-9]", "*", 0, , -1, 0, 0, 8, 5, "", 0,
-1, 0, ;
IP2IPRouting 16 = 2, "*", "*", "202xxxxxx[8-9]", "*", 0, , -1, 0, 0, 8, 5, "", 0,
-1, 0, ;
IP2IPRouting 17 = 1, "*", "*", "202xxxxxx0", "*", 0, , -1, 0, 0, 6, 5, "", 0, -1,
0, ;
IP2IPRouting 18 = 2, "*", "*", "202xxxxxx0", "*", 0, , -1, 0, 0, 6, 5, "", 0, -1,
0, ;
IP2IPRouting 19 = 5, "*", "*", "202xxxxxx0", "*", 0, , -1, 0, 0, 6, 5, "", 0, -1,
0, ;
IP2IPRouting 20 = 5, "*", "*", "919xxx36[00-39]", "*", 0, , -1, 0, 0, 3, 3, "", 0,
-1, 0, ;
IP2IPRouting 21 = 6, "*", "*", "919xxx", "*", 0, , -1, 0, 0, 3, 3, "", 0, -1, 0, ;
IP2IPRouting 22 = 8, "*", "*", "919xxx", "*", 0, , -1, 0, 0, 3, 3, "", 0, -1, 0, ;
IP2IPRouting 23 = 5, "202", "*", "919xxxx[450-515]", "*", 0, , -1, 0, 0, 1, 1, "",
0, -1, 0, ;
IP2IPRouting 24 = 5, "202", "*", "919xxxx[450-515]", "*", 0, , -1, 0, 0, 2, 1, "",
0, -1, 0, ;
IP2IPRouting 25 = 5, "*", "*", "011xxxxxxxxxxx", "*", 0, , -1, 0, 0, 1, 1, "", 0,
-1, 0, ;
IP2IPRouting 26 = 5, "*", "*", "011xxxxxxxxxxx", "*", 0, , -1, 0, 0, 2, 1, "", 0,
-1, 0, ;
IP2IPRouting 27 = 3, "*", "*", "[*73]", "*", 0, , -1, 0, 0, 9, 5, "", 0, -1, 0, ;
IP2IPRouting 28 = 3, "*", "*", "[*72]919xxxx[450-515]", "*", 0, , -1, 0, 0, 9, 5,
"", 0, -1, 0, ;
IP2IPRouting 29 = 3, "*", "*", "[*90]919xxxx492", "*", 0, , -1, 0, 0, 9, 5, "", 0,
-1, 0, ;
IP2IPRouting 30 = 3, "*", "*", "[*91]", "*", 0, , -1, 0, 0, 9, 5, "", 0, -1, 0, ;
IP2IPRouting 31 = 3, "*", "*", "[*92]919xxxx492", "*", 0, , -1, 0, 0, 9, 5, "", 0,
-1, 0, ;
IP2IPRouting 32 = 3, "*", "*", "[*93]", "*", 0, , -1, 0, 0, 9, 5, "", 0, -1, 0, ;
IP2IPRouting 33 = 3, "*", "*", "[*94]919xxxx492", "*", 0, , -1, 0, 0, 9, 5, "", 0,
-1, 0, ;
IP2IPRouting 34 = 3, "*", "*", "[*95]", "*", 0, , -1, 0, 0, 9, 5, "", 0, -1, 0, ;
IP2IPRouting 35 = 3, "*", "*", "*", "*", 0, , -1, 0, 0, 9, 5, "", 0, -1, 0, ;
IP2IPRouting 36 = 3, "*", "*", "*", "*", 0, , -1, 0, 0, 2, 1, "", 0, -1, 0, ;
IP2IPRouting 37 = 5, "*", "*", "1888xxxxxxx", "*", 0, , -1, 0, 0, 1, 1, "", 0, -1,
0, ;
IP2IPRouting 38 = 5, "*", "*", "1888xxxxxxx", "*", 0, , -1, 0, 0, 2, 1, "", 0, -1,
0, ;
IP2IPRouting 39 = 6, "*", "*", "1888xxxxxxx", "*", 0, , -1, 0, 0, 2, 1, "", 0, -1,
0, ;
IP2IPRouting 40 = 6, "*", "*", "1888xxxxxxx", "*", 0, , -1, 0, 0, 2, 1, "", 0, -1,
0, ;
IP2IPRouting 41 = 1, "*", "*", "00000888xxxxxxx", "*", 0, , -1, 0, 0, 3, 3, "", 0,
-1, 0, ;

[ \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 1 = , 5, "207.xxx.xxx.210", 0, -1, "*", "*", "*", "*", 1, 9;
Classification 2 = , 5, "173.xxx.xxx.*", 0, -1, "202xxxxxx[8-9]", "*", "*", "*",
1, 8;
Classification 3 = , 5, "173.xxx.xxx.*", 0, -1, "919xxxxxx[7-8]", "*", "*", "*",
1, 8;
Classification 4 = , 5, "173.xxx.xxx.*", 0, -1, "202xxxxxx0", "*", "*", "*", 1, 6;
Classification 5 = , 1, "12.xxx.xxx.*", 0, -1, "202xxxxxx7", "*", "*", "*", 1, 5;
Classification 6 = , 1, "12.xxx.xxx.*", 0, -1, "202xxxxxx[8-9]", "*", "*", "*", 1,
8;
Classification 7 = , 1, "12.xxx.xxx.*", 0, -1, "919xxxxxx5", "*", "*", "*", 1, 7;
```

```
[ \Classification ]


[ SIPInterface ]

FORMAT SIPInterface_Index = SIPInterface_NetworkInterface,
SIPInterface_ApplicationType, SIPInterface_UDPPort, SIPInterface_TCPPort,
SIPInterface_TLSPort, SIPInterface_SRD, SIPInterface_MessagePolicy,
SIPInterface_TLSMutualAuthentication, SIPInterface_TCPKeepaliveEnable,
SIPInterface_ClassificationFailureResponseType;
SIPInterface 1 = "ATTDMZ", 2, 5060, 5060, 5061, 1, , -1, 0, 500;
SIPInterface 2 = "RALVOX", 2, 5060, 5060, 5061, 2, , -1, 0, 500;
SIPInterface 3 = "RALOFFICE", 2, 5060, 5060, 5061, 3, , -1, 0, 500;
SIPInterface 5 = "PUBSIP", 2, 5060, 5060, 5061, 5, , -1, 0, 500;

[ \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 3 = 0, 0, 2, "*", "*", "29436xx", "*", 0, 1, 0, 0, 255,
"919", "";
IPInboundManipulation 4 = 0, 0, 9, "*", "*", "732xxxxxx5", "*", 0, 1, 10, 0, 255,
"919xxx3620", "";
IPInboundManipulation 5 = 0, 0, 9, "*", "*", "732xxxxxx6", "*", 0, 1, 10, 0, 255,
"919xxx3622", "";
IPInboundManipulation 6 = 0, 0, 9, "*", "*", "732xxxxxx7", "*", 0, 1, 10, 0, 255,
"919xxx3623", "";

[ \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, "Any.Response", "Header.To.Url.Host contains
'angel.z101.gch.com'", "Header.To.Url.Host", 2, "'12.xxx.xxx.xxx'", 0;
MessageManipulations 4 = 0, "Any.Request", "Header.From.Url.Host contains
'angel.z101.gch.com'", "Header.From.Url.Host", 2, "'12.xxx.xxx.xxx'", 0;
MessageManipulations 5 = 0, "Invite.Request", "Header.P-Asserted-identity exists",
"Header.P-Asserted-identity", 2, "'Unavailable<sip:'+
header.contact.url.user+'@12.xxx.xxx.xxx>'", 0;
MessageManipulations 6 = 0, "Invite.Request", "Header.P-Asserted-identity
!exists", "Header.P-Asserted-identity", 0,
"'Unavailable<sip:'+header.contact.url.user+'@12.xxx.xxx.xxx>'", 0;
MessageManipulations 7 = 0, "Invite.Request", "", "Header.Privacy", 0, "'id'", 0;
MessageManipulations 8 = 3, "", "", "Header.Contact.url.user", 2, "'gcsbc01'", 0;
MessageManipulations 9 = 0, "Invite.Request", "Header.P-Asserted-identity.URL.host
contains 'angel.z101.gch.com'", "Header.P-Asserted-identity.URL.host", 2,
"'12.xxx.xxx.xxx'", 0;
MessageManipulations 13 = 4, "Invite.Request", "Header.Request-uri.URL.user !=
Header.to.url.user", "Header.Diversion", 0, "'919xxxxx00'+'<sip:'
+'919xxxxx00'+'@12.xxx.xxx.xxx>'+';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;
;lab only
MessageManipulations 20 = 18, "Any.Request", "header.contact.URL.user ==
'919xxx3620'", "header.contact.URL.user", 2, "'732xxxxxx5'", 0;
MessageManipulations 22 = 18, "Any.Request", "header.contact.URL.user ==
'919xxx3622'", "header.contact.URL.user", 2, "'732xxxxxx6'", 0;
MessageManipulations 24 = 19, "Any.Request", "header.contact.URL.user ==
'919xxx3623'", "header.contact.URL.user", 2, " '732xxxxxx7'", 0;
;production
MessageManipulations 26 = 18, "Any.Response", "Header.To.Url.Host contains
'angel.z101.gch.com'", "header.to.url.host", 2, "'207.xxx.xxx.210'", 0;
;lab only
MessageManipulations 27 = 18, "Any.Response", "Header.contact.url.user ==
'919xxx3620'", "Header.contact.url.user", 2, "'732xxxxxx5'", 0;
;production
MessageManipulations 28 = 18, "Any.Request", "Header.From.Url.Host contains
'angel.z101.gch.com'", "Header.From.Url.Host", 2, "'173.xxx.xxx.68'", 0;
MessageManipulations 29 = 18, "Invite.Request", "", "Header.Privacy", 0, "'id'",
0;
MessageManipulations 30 = 18, "Invite.Request", "Header.P-Asserted-identity
exists", "Header.P-Asserted-identity", 2, '""Unavailable"<sip:'+
header.contact.url.user+'@173.xxx.xxx.68>'', 0;
MessageManipulations 31 = 18, "Invite.Request", "Header.P-Asserted-identity
!exists", "Header.P-Asserted-identity", 0,
'""Unavailable"<sip:'+header.contact.url.user+'@173.xxx.xxx.68>'', 0;
MessageManipulations 33 = 18, "Invite.request", "", "header.from.url.user", 2,
"'anonymous'", 0;
MessageManipulations 34 = 18, "Invite.Request", "", "header.from.name", 2,
'"Anonymous"'', 0;
MessageManipulations 35 = 18, "Invite.Request", "Header.P-Asserted-
identity.URL.host contains 'angel.z101.gch.com'", "Header.P-Asserted-
identity.URL.host", 2, "'173.xxx.xxx.68'", 0;
MessageManipulations 36 = 20, "Invite.Request", "", "header.from.url.user", 2,
"header.contact.url.user", 0;
; lab only
MessageManipulations 37 = 17, "Any.Request", "header.REQUEST-URI.url.user ==
'7323200435'", "Header.To.Url.user", 2, "'919xxx3620'", 0;
;lab only - used to discard a 180 message back to AT&T in order to generate an
error condition
MessageManipulations 38 = 13, "Invite.Request", "", "var.call.src.0", 2, "'1'", 0;
MessageManipulations 39 = 14, "Invite.Response.180", "var.call.src.0 == '1' AND
Body.sdp !exists", "header.Request-Uri.methodtype", 2, "'402'", 0;
MessageManipulations 40 = 14, "", "", "var.call.src.0", 2, "'0'", 1;
```

```
; for Network Based Blind Call Txfr using REFER
MessageManipulations 41 = 4, "", "header.Referred-By.url.host contains
'angel.z101.gch.com'", "header.Referred-By.url.host", 2, "'173.xxx.xxx.68'", 0;
MessageManipulations 42 = 4, "", "header.Referred-By.url.user == '919xxx3620'",
"header.Referred-By.url.user", 2, "'732xxxxxx5'", 0;
; production - rebuilding the Refer-To to topology hide
MessageManipulations 43 = 18, "", "header.Refer-To exists",
"header.contact.url.user", 2, "header.from.url.user", 0;
MessageManipulations 44 = 18, "", "Header.Refer-To exists and Header.Refer-To
regex(<sip:)(.*)(@)(.*)", "Header.Refer-To", 1, "", 0;
MessageManipulations 45 = 18, "", "", "Header.Refer-To", 0,
"$1+$2+$3+'207.xxx.xxx.210>'", 1;

[ \MessageManipulations ]


[ RoutingRuleGroups ]

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

[ \RoutingRuleGroups ]


[ ResourcePriorityNetworkDomains ]

FORMAT ResourcePriorityNetworkDomains_Index = ResourcePriorityNetworkDomains_Name,
ResourcePriorityNetworkDomains_Ip2TelInterworking;
ResourcePriorityNetworkDomains 1 = "dsn", 0;
ResourcePriorityNetworkDomains 2 = "dod", 0;
ResourcePriorityNetworkDomains 3 = "drsn", 0;
ResourcePriorityNetworkDomains 5 = "uc", 1;
ResourcePriorityNetworkDomains 7 = "cuc", 0;

[ \ResourcePriorityNetworkDomains ]
```

Reader's Notes

Configuration Note

www.audiocodes.com