# SIP Voice Solution Blueprint

Reference Architecture

Authors: Don Huovinen, Gordon Bell, et al.

Version: 1.6

Status: DRAFT

Published: 9/1/2016

GENESYS™

# Table of Contents

# Table of Figures

## Table of Tables



## Revision History

| Rev | Date Published | Author | Reason for Revision |
|---|---|---|---|
| 0.1 | 7/15/13 | Gordon Bell | Initial release |
| 0.2 | 9/26/13 | Gordon Bell | Revised based on SIP Solution PowerPoint deck |
| 0.3 | 9/30/13 | Gordon Bell | Latest draft for review |
| 0.4 | 10/25/13 | Gordon Bell | Adding input from EMEA sales training and completing missing sections. |
| 0.5 | 12/6/2013 | Gordon Bell | Incorporating last set of comments and preparing for review. |
| 0.6 | 1/28/2014 | Gordon Bell | Apply comments from SIP Architects' review. |
| 1.0 | 3/21/2014 | Gordon Bell | Final Version |
| 1.1 | 5/18/2016 | Don Huovinen | Draft 1 |
| 1.2 | 5/18/2016 | Don Huovinen | Draft 2 – Significant changes. Addition of sections and clean ups based upon review feedback.<br>Added in contributions from Brian Raynor on media gateways and SBC |

| Rev | Date Published | Author | Reason for Revision |
|---|---|---|---|
| 1.3 | 6/24/2016 | Don Huovinen | Added updates from Brian Raynor and Scott Cooke |
| 1.4 | 7/14/2016 | Don Huovinen | Added updates from Gordon Bell and Pascal |
| 1.5 | 8/4/2016 | Don Huovinen | Incorporated additional feedback from Brian Raynor and updated mandatory diagrams |
| 1.6 | 9/1/16 | Don Huovinen | Updated disclosure language. |

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS DOCUMENT ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENT ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THIS DOCUMENTATION IS BEING PROVIDED GRATUITOUSLY AND, THEREFORE GENESYS SHALL NOT BE LIABLE UNDER ANY THEORY FOR ANY DAMAGES SUFFERED BY LICENSEE OR ANY USER OF THE GENESYS DOCUMENTATION.  UNDER NO CIRCUMSTANCES, INCLUDING NEGLIGENCE, SHALL GENESYS BE LIABLE FOR ANY INCIDENTAL, SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR RELATING TO THIS DOCUMENTATION.  SOME JURISDICTIONS DO NOT ALLOW THE LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THIS LIMITATION MAY NOT APPLY TO YOU.

# 1 Introduction

The purpose of the SIP Voice Solution Blueprint document is to provide a set of design practices and guidance to ensure consistent architecture approaches are used for all SIP Voice deployments. It provides a prescriptive list of components (both Genesys and 3rd party) that should be included in the solution. It also provides deployment guidance, including sizing considerations, and addressing several system concerns such as security, high availability, disaster recovery and serviceability.

The Genesys SIP Voice Solution consists of the following core Genesys components:

- SIP Server
- Resource Manager
- Media Server (Media Control Platform)
- SIP Feature Server

Other products which may also be present in a SIP Voice deployment such as Outbound or the Genesys Voice Platform are also described this is document.

## 1.1 Document Overview

The document contains the following sections:

- Chapter 2: Definitions and Acronyms
- Chapter 3: Overall Architecture
- Chapter 4: Deployment View
- Chapter 5: Interaction View
- Chapter 6: Implementation View
- Appendix A: Common Components Summary
- Appendix B: Performance Configuration

## 1.2 Intended Audience

The Blueprint Architectures are intended to provide Genesys Solution Consultants, Professional Services and partners with information on the general architecture design and considerations for the solution. The information provided in this document should meet the needs of pre-sales and provide appropriate general guidance for professional services. This document is not intended to provide configuration level information for professional services.

Describing system and solution architectures can be difficult as there are multiple audiences each with different expectations. This document is intended for multiple audiences with various chapters being more interesting to some readers than others. It is expected that readers will already have knowledge and training on Genesys products. This document provides high-level information for completeness.

The Overall Architecture and Deployment View are likely meaningful to most audiences. However, the Interaction View and the Implementation View may be of more interest to those configuring the network and components.

# 2 Definitions, Acronyms, and Document Standards

## 2.1 Definitions

This document uses various abbreviations and acronyms that are commonly used in Genesys product documentation and the telecommunications and contact center industries. The following table defines terms that will be referenced subsequently in this document.

## 2.2 Glossary

| | |
|---|---|
| ACD | Automated Call Distribution |
| ASM | Active Switching Matrix |
| ASR | Advanced Speech Recognition |
| CIM | Customer Interaction Management |
| CME | Configuration Management Environment, another name for the Configuration Layer |
| CPA | Call Progress Analysis |
| CPD | Call Progress Detection |
| CS | Configuration Server |
| CSP | Configuration Server Proxy |
| CTI | Computer-telephony integration, the adding of computer intelligence to monitoring and control of telephone calls |
| DB | Database |
| DBMS | Database Management System |
| DBS | Database Server |
| DHCP | Dynamic Host Configuration Protocol |
| DN | Directory number |
| DNIS | Dialed number information service |
| DNS | Domain Name System |
| eSBC / E-SBC | Enterprise Session Border Controller |
| FTP | File Transfer Protocol |
| GA | Genesys Administrator |
| GAX | Genesys Administrator Extension |
| GIM | Genesys Info Mart |
| GI2 | Genesys Interactive Insights |
| GUI | Graphical User Interface |
| GVP | Genesys Voice Platform |

| | |
|---|---|
| GWS | Genesys Web Services previously known as HTCC (Hosted Telephony Contact Center) |
| HA | High Availability |
| HTTP | Hypertext Transfer Protocol |
| ICON | Interaction Concentrator |
| IIS | Internet Information Services |
| IMS | IP Multimedia Subsystem |
| IP | Internet Protocol |
| IVR | Interactive Voice Response |
| IWS | Interaction Workspace |
| IVR | interactive voice response |
| LAN | Local Area Network |
| LCA | Local Control Agent |
| LM | License Manager |
| MCP | Media Control Platform |
| MS | Message Server |
| MSML | Media Server Markup Language |
| NMS | Network Management System |
| OCS | Outbound Contact Server |
| OEM | Original Equipment Manufacturer |
| ORS | Orchestration Server |
| OS | Operating System |
| PBX | Private branch exchange |
| PSTN | Public Switched Telephone Network |
| QoS | Quality of Service |
| RDBMS | Relational Database Management System |
| RM | Resource Manager |
| RTP | Real-time Transport Protocol, the media-stream transport used with SIP |
| SBC | Session Border Controller |
| SCS | Solution Control Server |
| SCXML | State Chart XML: State Machine Notation for Control Abstraction |
| SDK | Software Development Kit |
| SIP | Session Initiation Protocol |

| | |
|---|---|
| SNMP | Simple Network Management Protocol |
| SQL | Structured Query Language |
| SSL | Secure Sockets Layer |
| TLib | TServer Library |
| TTS | Text To Speech |
| TUI | Telephony User Interface |
| UC | Unified Communications |
| UI | User Interface |
| URS | Universal Routing Server |
| VLAN | Virtual Local Area Network |
| VM | Virtual Machine |
| VoIP | Voice over IP, digitized voice segments transported in fixed packets across the IP network and re-assembled in sequence at the destination |
| WAN | Wide Area Network |

## 2.3 Document Conventions

The following documentation and naming conventions are used throughout the document:

- Code and `configuration property names & values` will appear in `console font`.
- References to other documents are bracketed ([]).

# 3 Overall Architecture

The SIP Voice Solution is designed to provide the necessary communication channels for a contact center without the need for a PBX. The solution is a pre-determined set of Genesys and 3rd party software and hardware components to fulfill the SIP communication requirements. It is intended that the solution be repeatable and easily supportable by limiting the variability of SIP deployments.

The SIP Voice Solution is targeted for enterprise deployments of varying levels of complexity where the intended goal is to support their agents and non-agents with a SIP infrastructure (vs a legacy competitive PBX). The solution blueprint is focused on the SIP/VoIP infrastructure. It is understood that there may be other Genesys components and solutions that may need to be integrated into the target deployment (e.g., E-Mail, chat, work force management, etc.), but those areas are beyond the scope of this document.

Most of the solution guidance is based on customer deployments and the lessons learned through implementing SIP within those real-world scenarios.

## 3.1 Solution Overview

This solution is based around a “stand alone” SIP Server deployment for VoIP telephony. It combines various Genesys and 3rd party components.

***Components of the solution***

**Genesys SIP Server** – Standards-based contact center software solution

**Genesys Feature Server** – Provides supplementary services for SIP Server including voicemail, dial plan services and phone provisioning/management.

**Genesys Media Server** – Delivers media services to for interactive voice response, menus, on hold treatments and call recording.

**Genesys Routing** – Industry-leading routing engine which allows to you provide flexible business driven routing to deliver great customer experience and drive operational efficiency.

**Genesys Workspace Desktop Edition (WDE)** – Agent desktop application supporting all media types

**Genesys SIP Softphone** – A Genesys provided software based SIP endpoint used by agents to provide voice communication directly through the agent’s desktop.

**Genesys Session Border Controller (SBC)** – Acts as firewall and codec for SIP. OEM of AudioCodes

**Genesys Reporting** – Real-time and Historical reporting provided by Pulse (Real-time) and ICON/Info Mart/Interactive Insights (Historical)

**Genesys Interaction Recording** – A call recording solution, screen capture, and Quality Monitoring (QM) tool utilized to store, manage, and playback recorded voice conversations and screen captures, as well as provide quality assurance.

*The SIP Voice Blueprint leverages the Common Component Blueprint for foundational elements used in orchestration, reporting and configuration/management. A summary of the Common Components is included in Appendix A.*

*Further details on Genesys Call Recording (Genesys Interaction Recording) is contained in other documents.*

*Optional components that are commonly included in an overall architecture include Session Border Controllers (SBCs) and media gateways.*

## 3.2 Logical Architecture Model

The following is a logical model of the SIP Voice Solution architecture.

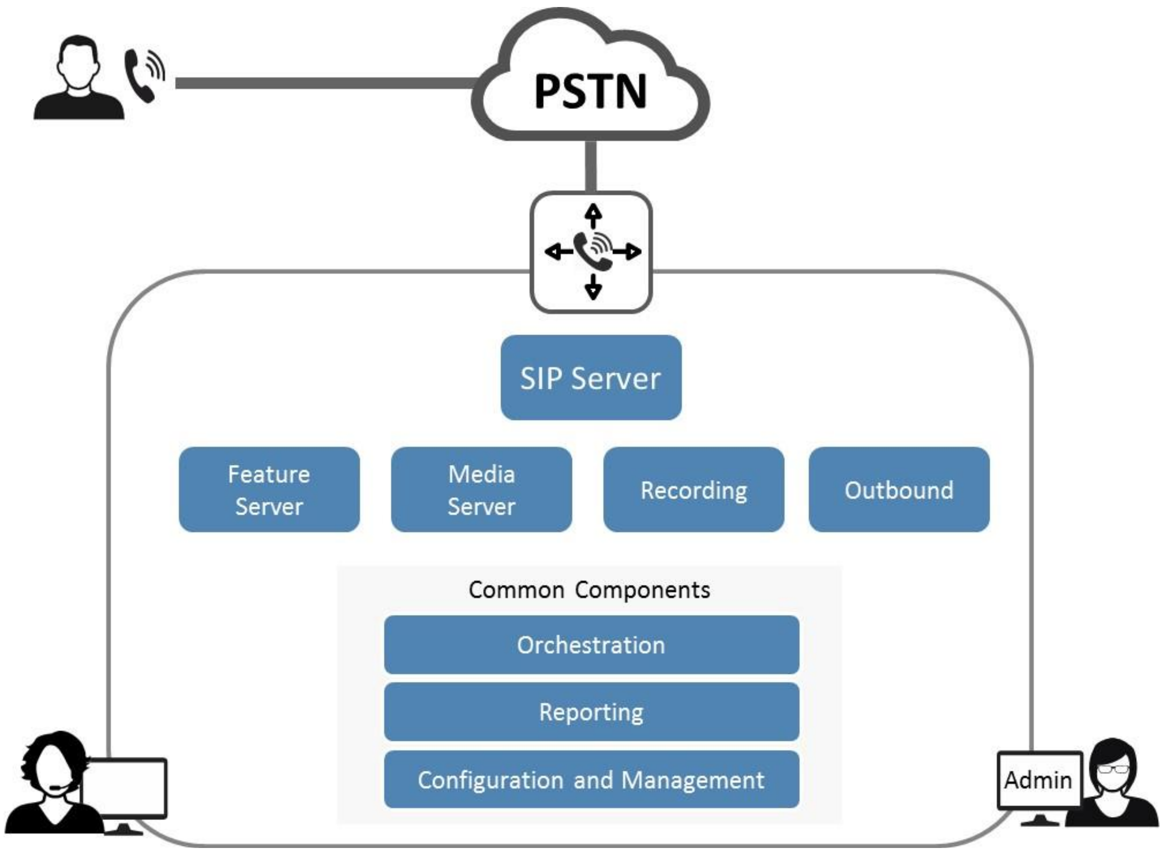



Figure 1 – SIP Voice Solution Logical Model

## 3.3 Functional View

The SIP Voice Solution can be utilized for green field contact center deployments and to replace legacy PBXs used primarily by contact center agents. It supports for both Inbound Voice and Outbound dialing scenarios. It also provides qualification and parking of inbound calls and media treatments such as announcements and IVR applications.

The functionality can be broken down into the following areas:

- Core Softswitch Functionality
- Contact Center Services

- Media Services
- Operations and Administration
- Additional Communication Services

### 3.3.1 Core Softswitch Functionality

The SIP Voice Solution may be utilized as a standalone SIP softswitch or integrated with third party softswitches. When used as a standalone softswitch the SIP Voice Solution provided full call setup and teardown for SIP endpoints.

### 3.3.2 Contact Center Services

The SIP Voice Solution supports all the services required to operate a voice contact center. These services include the following:

- Intelligent call routing based upon flexible business logic
- Agent desktop to display tasks and customer information, control the agent's environment and provides softphone controls to manage interactions.
- Supervisor functions including silent monitoring, whisper coaching and assistance call supervision.
- Outbound dialing campaigns with the ability to perform call progress detection (CPD) and answering machine detection (AMD).
- Integration to Genesys services. The SIP Voice Solution operates as a Genesys T-Server allowing for integration with Genesys components in the same manner as any other T-Server.

Some of the call controls provided to agents by the Genesys Workspace Desktop Edition (WDE) include:

- Answer Call
- Make Call
- Hold and Retrieve Call
- Release Call
- Single Site Transfer
- Two Step/Consultative Transfer
- Single Step Conference Call
- Two Step Conference Call
- Supervisor monitoring
- Start/Stop call recording

Please see section 5.1 Call Flows for representative call control interactions.

### 3.3.3 Media Services

The SIP Voice Solution provides various media services that enhance the overall contact center experience. These media services include:

- Playing announcements and greetings
- Call parking & qualification (DTMF / IVR)
- Music-on-hold
- Conferencing – serves as a Multipoint Conference Unit (MCU)
- Call Progress Detection/Answering Machine Detection (Outbound)
- Voicemail
- Call Recording
- Media Transcoding

Please see section 5.1 Call Flows for representative media services flows.

### 3.3.4 Voice Communication Services

In addition to the agent/contact center capabilities, the SIP Voice Solution can provide voice communication features to meet the basic telephony needs of non-contact center users. Genesys SIP Communication extends this platform to support enterprise users—those who need business phones but aren't contact center agents. Using this single platform simplifies communications management and frees customers from maintaining a separate PBX which directly leads to a lower total cost of ownership. SIP Communication provides:

- Standard Communication Features:
    - Make and Receive Call
    - Caller ID (CLID/COLR)
    - Call Hold, Call Waiting
    - Transfers - Single-step transfer, Two-step transfer, Call consultation/toggle
    - Call Forwarding, Do Not Disturb, Conference (1)
    - Distinctive ringing indication (1)
- Phone Capabilities – Speakerphone, Headset, Auto-answer, Speed dial, Redial, Call log, Call timer (1)
- Multi-appearance (multiple calls on same line), Multi-line (multiple dialed numbers on same endpoint)
- Hunt groups (simultaneous, linear, circular)
- Shared call appearance
- Find-me, follow-me (sequential and/or simultaneous call forwarding)
- Dial Plans
- Voicemail, Message waiting indication

- Phone/Device Management
- Call Detail Records
- Emergency Services (E-911) (2)

    (1) Requires appropriate SIP phone

    (2) Requires 911-Enable

### 3.3.5 Additional Communication Services

The SIP Voice Solution and SIP in general is a very robust standard. In addition to support for voice the SIP Solution provides support for:

- Video Services (Push Video and Video calls)
- Instant Messaging
- Presence integration with third party Unified Communications (UC) solutions

### 3.3.6 Operations and Administration

The SIP Voice Solution includes tools for operating and administrating the solution. Genesys Administrator (GA) and Genesys Administrator Extensions (GAX) are used for deploying, configuring, provisioning and monitoring the system.

For more information, please consult the Genesys Administrator documentation (http://docs.genesys.com/Documentation/GA ).

## 3.4 Component View

The following diagram illustrates the various processes in the SIP Voice Blueprint architecture. As a process view this does not address scalability or availability. For simplicity only the components directly addressed in the SIP Voice Blueprint are shown in this view.

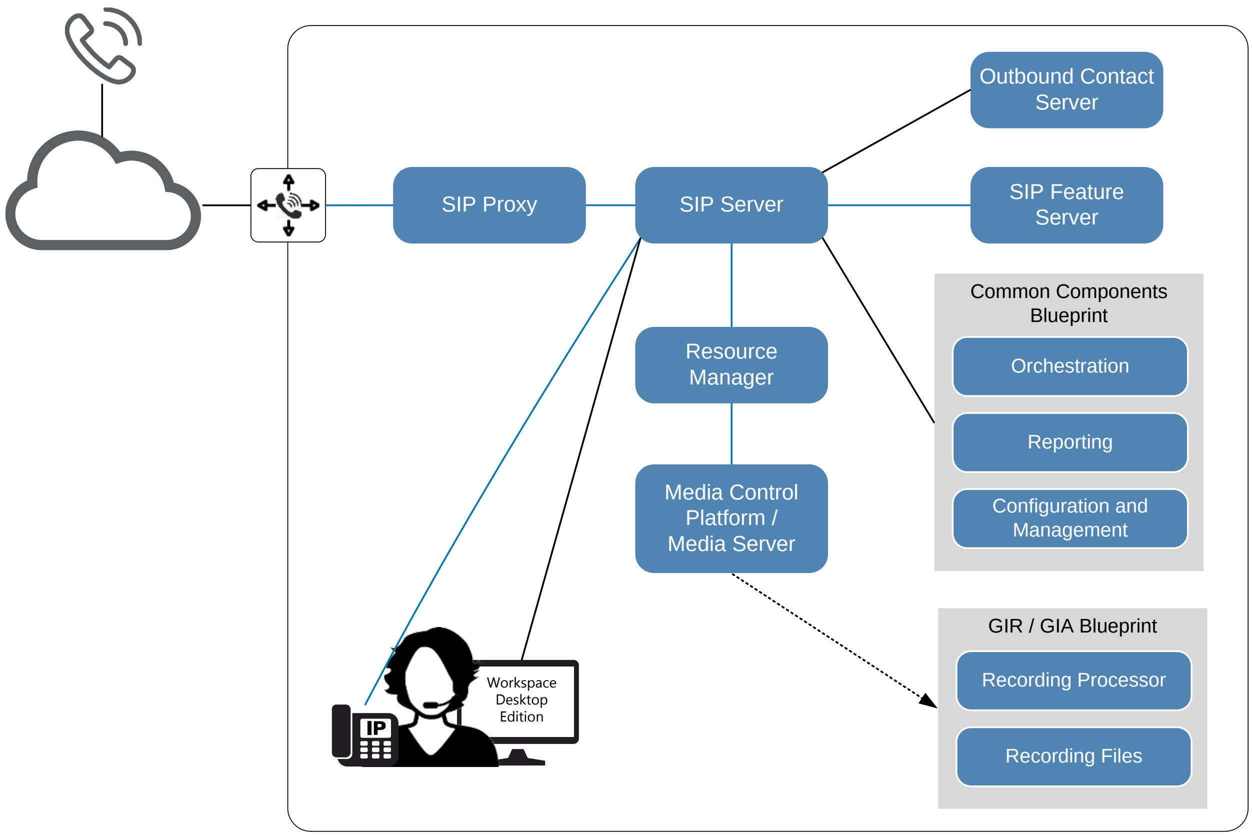



Figure 2 – SIP Voice Solution Component Overview

**SIP Proxy**

Genesys SIP Proxy provides high availability of the SIP Voice Solution without requiring the use of a virtual IP address and can insulate external SIP components from changes in the Genesys topology. SIP Proxy relies on the SIP components which it communicates with to support the use of DNS SRV records and be capable of identifying the available SIP Proxy. SIP Proxy continuously monitors the configured SIP Servers and will direct any SIP messaging to the available SIP Server instances.

**SIP Server**

Genesys SIP Server is a software-only SIP softswitch and software ACD which manages all telephony signaling in a Genesys SIP environment. SIP Server is also used for a variety of functions such as general interworking in a SIP environment, communication with other Genesys components such as Universal Routing Server (URS) / Orchestration Server (ORS) and other T-Lib clients. SIP Server acts as a SIP B2BUA (back-to-back user agent), and controls the flow of SIP requests and responses between SIP endpoints, performing the switching functions that are normally performed by the PBX or ACD. SIP Server is used in conjunction with GVP and Media Server to provide integrated self-service and call parking/queuing.

**SIP Feature Server**

SIP Feature Server provides supplementary functions which may be requested in SIP environment. The three main capabilities provided are:

- **Genesys SIP Voicemail**- Genesys SIP Voicemail provides a secure, scalable, and flexible voice messaging application specifically designed for the contact center and customer service. It allows companies to retrieve and respond to customer voice messages left in group mailboxes during peak times and after hours. This optimizes customer service continuity, since companies will no longer miss customers' inquiries, and customers will no longer have to make repeated inbound calls to engage with the company. It's capabilities include both personal voicemail and "group" voicemail, including features such as Message Waiting Indication, email notification of messages, web-based access & more. Genesys SIP Voicemail provides tight, direct integration into Genesys SIP Server. The voicemail application itself is provided by Genesys Feature Server along with the use of Genesys SIP Server and Media Server (MCP). Storage for voicemail is provided through the use of a Cassandra database.

- **Device Management** – Feature Server provides provisioning of endpoints, including configuration and firmware updates. Genesys provides provisioning of Genesys, AudioCodes, Yealink, and Polycom endpoints within Genesys Feature Server. Provisioning makes use of FTP, FTPS, HTTP, or HTTPS protocols.

- **Advanced dial plan** – including digit manipulation, PBX type features for users such as call forwarding, and trunk selection. While SIP Server itself has built in dial plan management, use of SIP Feature Server provides the ability to apply dial plans across multiple instances of SIP Server, simplifying administration for environments where multiple SIP Servers are utilized.

**Resource Manager**

The Resource Manager controls access and routing to the Media Server, Media Control Platform (MCP) and other resources. The Resource Manager receives inbound requests from SIP Server. It processes requests for services, interacts with Configuration Server to determine the resource required to deliver the service, and delivers the call to the respective resource group. The system may have separate resources groups configured to provide basic media services, VoiceXML IVR, or call recording or a single media resource group may be deploy which performs all functions. The Media Server provides basic media services while the GVP MCP provides support for VoiceXML based Interactions. The Resource Manager also manages resource high availability and call distribution including policy enforcement of call volume into specific applications and services such as gateway, the CTI Connector or Recording Server.

**Media Control Platform / Media Server**

The Media Control Platform (MCP) is provides media-centric services for both Media Server and GVP. It can be configured as a Media Server and to support general media resource functions such as announcements, conferences, call progress analysis and call recording. The Media Control Platform may also be configured to support IVR services for the Genesys Voice Platform and provides a VoiceXML browser and which is responsible for the execution of supported Voice Extensible Markup Language (VoiceXML) applications.

**Outbound Contact Server**
Genesys Outbound Server (OCS) automates customer outreach, helping your organization become more productive and cost-effective. It enables customer contact centers to proactively manage multi-channel campaigns for voice, e-mail, SMS, and blended outbound campaigns for proactive customer communications, telemarketing, and debt collections. Genesys Outbound features robust campaign management supporting predictive, progress and preview campaigns. It also operates together with Genesys Media Server to perform call progress detection (CPD) and call progress analytics (CPA) providing human answer, answering machine detection (AMD), fax detection, etc. OCS provides support for preview, predictive, and progressive dialing.

### 3.4.1 Component View – Genesys Voice Platform

Genesys Voice Platform (GVP) is standards-based software platform that enables business to provide cost-effective customer interactions 24x7. GVP is the market-leading VoiceXML platform and high capacity, operational flexibility and simplicity, and standard based development tools. GVP provides support for the VoiceXML standard, automated speech recognition (ASR), Text to Speech (TTS), and IVR application reporting. GVP is tightly integrated with the Genesys Customer Experience (CX) Platform, integrating self-service with agent-assisted service.

A GVP deployment requires additional components beyond the scope of the standard SIP Voice solution.

**Shared Components with SIP Voice Solution**

The Genesys Voice Platform shares utilizes the following components which are present in the SIP Voice Solution:

- SIP Server
- SIP Proxy
- Resource Manager
- Media Control Platform

It also relies upon the foundational components contained in the Common Component Blueprint. For an IVR only deployment on the Configuration and Management layer is mandatory.

When utilized as part of a Genesys Voice Platform deployment thee following components may take on additional functions:

- **Resource Manager** – Routes calls to appropriate Media Control Platform(s) based upon resource needs (VoiceXML). Resource Manager will both proactively poll the MCPs for availability and distribute the requests across the MCPs to manage the overall resource load. The Resource Manager also acts as an ASR/TTS proxy for MRCP v2 requests.
- **Media Control Platform** – The Media Control Platform processes VoiceXML applications. The MCP capacity is typically lower when it operates as a VoiceXML IVR than if it acts as a simple media resource function driven through MSML. If ASR and TTS is utilized the MCP will also manage connectivity through MRCP to these resources.
- **MRCP Proxy** – The MRCP proxy manages distribution of MRCP requests (MRCP v1) from the MCP to the ASR and TTS servers. It manages availability of the ASR/TTS resources and also provides event feeds for ASR/TTS usage reporting.

The Resource Manager, Media Control Platform and MRCP Proxy all send usage metrics to the GVP Reporting Server to provide real-time and historical reporting information.

**Genesys Voice Platform - Reporting Server**

Genesys Voice Platform (GVP) provides both real-time and historical platform level reports and allows business data to be added to create application level reports. Reporting Clients on the Resource Manager, Media Control Platform and MCRP Proxy send call detail records (CDRs), Metrics, and Operational Reporting (OR) statistics to the Reporting Server. The GVP Reporting Server stores and summarizes data and statistics submitted by Reporting Clients to provide near real-time reports by hour, day, week, and month. The Reporting Server also includes GVP Service Quality Reporting which provides statistics on the service quality of GVP deployments. Service quality measures the quality of voice applications from the user's perspective - such as latency in answering the call, playing prompts, collecting input, ASR/TTS responsiveness, or the application server. Service-quality measurements account for all calls to the GVP system. The platform measures the calls being handled, rather than using a *sampling* methodology where periodic test calls are made to the system. Service Quality gathers information from the platform and the applications running on the platform and prepares reports on quality at regular interval. The Reporting Server reports are accessed through Genesys Administrator Extensions. The GVP Reporting Server also provides web services interface, allowing customers easy access to GVP reporting information to incorporate into custom reports and dashboards.

**Nuance ASR and TTS**

GVP uses Nuance for Automated Speech Recognition and Text to Speech functionality. With ASR the callers audio is processed by the Nuance recognizer based upon a grammar designed to recognize what the caller is stating. The returned results are provided to GVP and the VoiceXML application in a tokenized form which can be interpreted by the application to determine the caller's needs. Nuance support grammars ranging from basic numbers to flexible user defined grammars and statistical language (or natural language) models. For text to speech the Nuance TTS engine takes text and converts the text into systhensized speech which is rendered to the caller. Numerous languages are supported for both ASR and TTS.

**Web Servers**

Web/application servers, used to serve up the actual VoiceXML, are required to support the overall application load. In order to optimize performance and reduce HTTP traffic GVP can take advantage of caching of both audio resources and VoiceXML. The web application servers may also host other components such as Nuance Dialog Modules which are pre-built building blocks containing application logic and grammars that can be used to accelerate the IVR development process.

**Additional GVP Components**

Additional GVP Components may be deployed less frequently and are not covered in the scope of this blueprint architecture. These components are:

- Policy Server
- CTI Connector
- PSTN Connector
- Call Control Platform
- Squid Caching Proxy
- Supplemental Services Gateway

If these components will be deployed then you should review the Genesys documentation for general information.

### 3.4.2 SIP Voice Components

The following table lists the Genesys components that make up the SIP Voice Solution. Optional components are noted in the table.

| Category | Component | Version | Notes |
|---|---|---|---|
| **SIP Platform** | SIP Server | 8.1.1+ | SIP platform for agent telephony and front-end to Media Services |
| | SIP Feature Server | 8.1.2+ | Dial Plan, Device Management and Voicemail |
| | SIP Proxy | 8.1.1+ | *Optional HA component* |
| | Resource Manager | 8.5.1+ | Provides HA and capacity management of MCP resources |
| **Media Server** | Media Control Platform | 8.5.1+ | Provides Media Server and GVP IVR media services |
| **Outbound** | Outbound Contact Server | 8.1.3+ | Manages outbound campaigns and campaign dialing |

Call recording is provided by Genesys Interaction Recording (GIR). A separate GIR/GIA Blueprint provides details on the requirements for GIR.

### 3.4.3 GVP Components

For a GVP only deployment the following components are utilized

| Category | Component | Version | Notes |
|---|---|---|---|
| **GVP Platform** | SIP Server | 8.1.1+ | SIP platform to front-end to GVP Media Services |
| | Resource Manager | 8.5.1+ | Provides HA and capacity management of MCP resources and MRCP v2 resources |
| | MRCP Proxy | 8.5.1+ | Provides MRCP v1 resource management |
| | Reporting Server | 8.5.1+ | Provides GVP reporting |
| **IVR Media Server** | Media Control Platform | 8.5.1+ | Used for GVP |
| **Nuance** | ASR and TTS | 10.x+, 6.x+ | Automated Speech Recognition and Text to Speech Services |
| | Dialog Modules | 6.1 | Provides pre-packaged speech building blocks containing grammars and application logic |

Note: GVP Reporting Server includes a GAX plug-in that is used to enable access to GVP reports.

### 3.4.4 Required Genesys Common Component Services

The Genesys solutions use a common set of component for configuration/management, routing and reporting. These components are detailed within the **Common Components Blueprint**.

The following is a list of the mandatory Genesys Common Components required by the SIP Voice Blueprint. This table lists any dependencies and any minimum versions required.

| Category | Component | Minimum Version | Notes |
|---|---|---|---|
| **Orchestration** | ORS, URS, Stat Server, UCS | N/A | |
| | Genesys Rules and Genesys Mobile Services are optional components which may not be activated based upon the purchased solutions | | |
| | | | |
| **Reporting** | ALL | N/A | Base versions used in Common Component blueprint are fine |
| | | | |
| **Configuration & Management** | ALL<br>(SNMP Master Agent is optional) | N/A | Base versions used in Common Component blueprint are fine |

The following desktop applications may also be deployed.

| Category | Component | Version | Notes |
|---|---|---|---|
| **Agent Application** | Workspace Desktop Edition | 8.5.1+ | |
| **Agent Endpoint** | Workspace Desktop Edition SIP Endpoint | 8.5.1+ | |
| **Script Development** | Composer | 8.1.3+ | Used for IVR & routing strategy development |

Table 1: Genesys Common Component List

### 3.4.5 Voice Network Components

This section provides information regarding voice network components that are typically deployed with the Genesys SIP Telephony infrastructure. These components include Media Gateways, Session Border Controllers (SBCs), Provisioning Systems, and Media Quality Monitoring and Management Systems.

#### 3.4.5.1 Media Gateways

Media Gateways (MGWs, MGs or GWs) provide connectivity and translation between TDM voice networks and voice over IP (VoIP) based networks.

On the TDM side, a Media Gateway may support TDM connectivity by standard digital (T1/E1, ISDN, etc) or analog (FXO / FXS) trunking. Most media gateways support either line side or trunk side connectivity.

On the VoIP side, Media Gateways may support VoIP signaling protocols such as SIP, H.323, and MGCP as well as media transport via protocols such as RTP. In today's environment, SIP is by far the most common VoIP signaling protocol, and is directly supported by the Genesys SIP Voice Solution. However, it is common to still find H.323 and MGCP in use in legacy environments.

Media Gateways make use of digital signal processors (DSPs) to convert voice media from TDM into a supported codec (coder-decoder) for transport over the network via RTP. Common codecs used include G.711, G.729, and G.722.

The diagram below shows a high level overview of a Media Gateway:

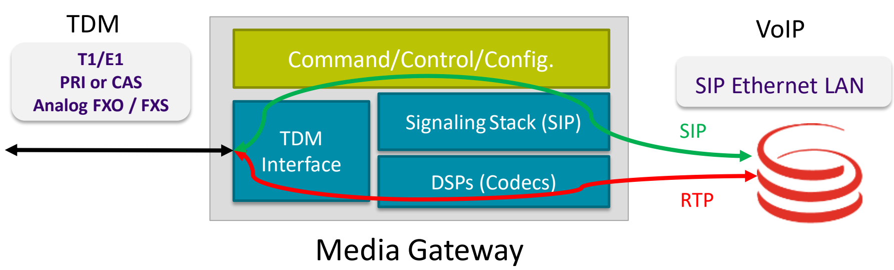



Figure 3 – Media Gateway Overview

The below diagram shows PSTN connectivity to a Genesys SIP Telephony infrastructure:

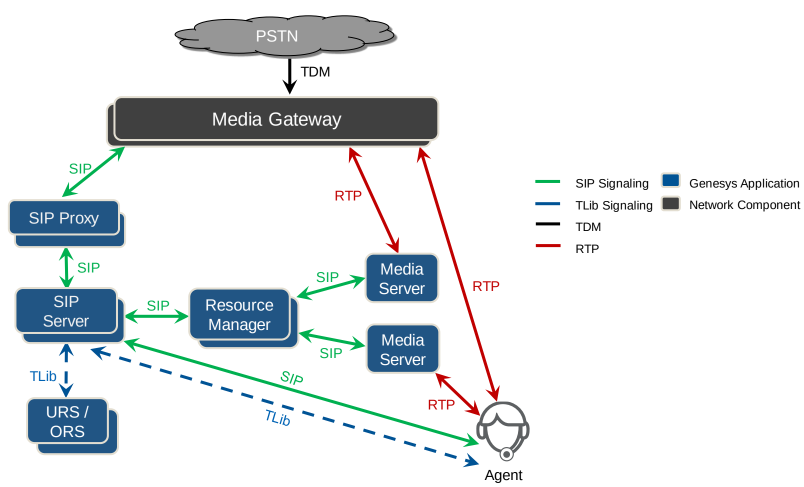



Figure 4 – Media Gateway Connectivity to Genesys SIP Telephony

It should be noted that the terms "VoIP Gateway" (for "Voice over IP Gateway") and "Media Gateway:" are often used interchangeably. In addition, while much of this section describes voice, video and other interactions are possible over SIP and RTP, and thus can be managed by an SBC as well.

### 3.4.5.2 Session Border Controllers

Session Border Controllers (SBCs) are devices or software applications that control the signaling and media streams involved in setting up, conducting, and tearing down VoIP sessions. VoIP sessions include those for voice, video, or other interactive media. SBCs are often used to protect the borders between service provider and customer networks, as well as between locations within a customer's network.

Some of the functionalities an SBC may provide include:

- **Call Flow Adaptation/Connectivity** – Translation between different signaling protocols, media, and codecs.
- **Message Manipulation** – Allows the SBC to modify the signaling between two potentially incompatible devices (such as modification of SIP messaging). This may include the ability to add, delete, or change SIP headers.
- **Security** – The SBC may provide the ability to restrict access or hide the topology of the internal network, encrypt traffic, or prevent denial of service (DDoS) attacks between trusted and untrusted networks.
- **Quality of Service (QoS) and Call Admission Control (CAC)** – Provides the ability to enforce quality of service policies within the network and manage/restrict traffic from unauthorized users and sources. Some SBCs may also be used to monitor the quality of VoIP interactions.
- **Remote Workers** – The SBC may provide support for NAT traversal and remote registration for devices and endpoints located outside of the internal network, such as over the Internet.
- **Dial Plan Management** – SBCs are often used to provide a unified dial plan for access between internal and external zones.

Not all SBCs support the above functionality, and many may support additional supplementary functions.

SBCs may provide separate zones between the external environment (such as a carrier SIP trunk), the internal SIP Voice infrastructure, and the network where the agents reside. Larger enterprises may have a mix of SIP traffic and multiple SIP based communications systems. An SBC can be used to provide a single management layer that allows for the administration of traffic between the various systems and zones.

The diagram below shows a high level overview of an SBC:

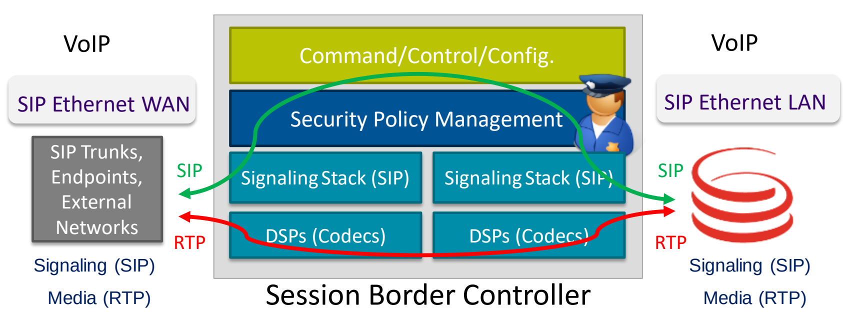



Figure 5 – Session Border Controller Overview

The below diagram shows a Session Border Controller used to provide connectivity to the PSTN via SIP/RTP carrier trunks, connectivity to remote agents (using SIP/RTP through a NAT router), and connectivity to remote sites with the Genesys SIP Telephony infrastructure:

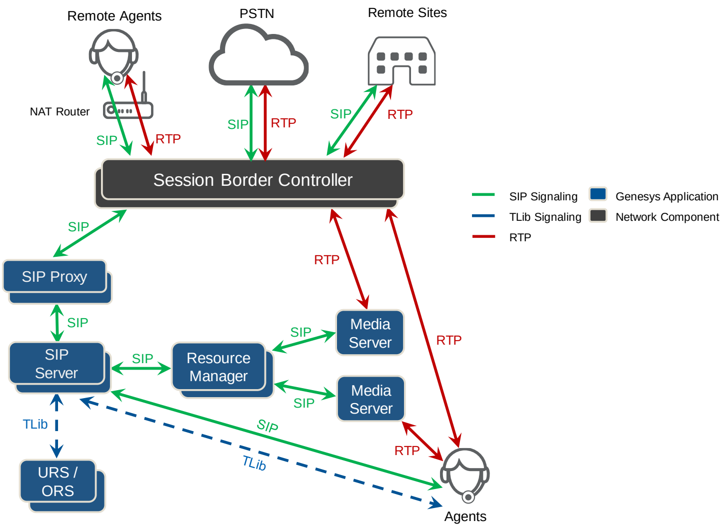



Figure 6 – Session Border Controller Connectivity to Genesys SIP Telephony

Please note that some Session Border Controllers also provide other types of connectivity to remote agents, including using WebRTC.

### 3.4.5.3 Provisioning Systems

Provisioning Systems provide the ability to configure and manage large numbers of devices, including phones, media gateways, and session border controllers; from a central location. Management of devices also includes the ability to centrally update device firmware.

Provisioning systems typically provide the following capabilities:

- **IP Address Allocation** – allowing for automatic distribution of IP addresses and default network parameters (including network gateway address, time server, DNS servers, etc) to devices. This information is typically provided by DHCP (dynamic host configuration protocol) on the core network, though some provisioning servers provide their own DHCP servers.

- **Boot Firmware and Configuration Updates** – provide the ability to update firmware in the devices as well as update configuration. This is typically delivered via HTTP/HTTP or FTP/FTPS protocols, though TFTP is also used in some devices.

- **Configuration Interface (GUI)** – allows the use of templates to define configuration by groups or individually for a large numbers of devices.

- **Centralized Logging and Management** – provides the ability to maintain and manage logs from devices and the ability to centrally force devices to update firmware, reboot, or reload configuration.

#### 3.4.5.4 Media Quality Monitoring and Management Systems

Media Quality Monitoring and Management Systems are utilized to provide information on voice and video quality between each step within a conversation. These systems can be utilized to help pinpoint call quality problems, as well as provide reports to validate delivering on SLAs.

In many systems, unique voice probes are required to be placed at key points within the VoIP network in order to monitor activity. Some systems, however, are integrated directly into the endpoints including media gateways, SBCs, and IP phones and do not require unique probes.

#### 3.4.5.5 Genesys Offered Media Gateways and Session Border Controllers

Genesys supports multiple leading vendor Media Gateways and Session Border Controllers and resells many AudioCodes Media Gateways and SBCs (as well as IP phones). AudioCodes has been a close partner with Genesys for many years and Genesys Contact Centers are a strategic focus for AudioCodes. AudioCodes has dedicated management, solution specific investment and innovations, joint labs, sales and support, and OEM product and service relationships with Genesys.

**Voice Gateways / Hybrid Session Border Controllers**

Genesys resells the following AudioCodes Mediant Hybrid SBCs, which offer both IP and TDM connectivity, and are capable of serving as both Media Gateway and Session Border Controller within the same platform (when appropriately configured):

| Product | Target Market | Max. SBC Sessions | Max. TDM Channels |
|---|---|---|---|
| Mediant 1000  | SMB/SME | 150 | 192 |
| Mediant 3000  | Large Entreprises | 1,000 | 2,016 |

Figure 7 – Genesys Offered Voice Gateways / Hybrid SBCs

**Software Based Session Border Controllers**

Genesys also resells the AudioCodes Mediant Software Enterprise Session Border Controller (E-SBC). This Session Border Controller is totally software based and can run on standard Intel-based server platforms. This is provided in two versions:

- **Server Edition (SE)** runs directly on "Bare Metal" Intel-based server platforms under its own provided hardened operating system.
- **Virtual Edition (VE)** can be run as a virtual machine under the VMWare and Hyper-V platforms.

Both versions provide the same SBC functionality, the same user interface and the same code base as the Mediant 1000 and 3000s.

The table below lists capacities of each version of the Software E-SBC, as of the time of writing of this document.

| Product | Target Market | Max. SBC Signaling Sessions | Max. SBC Media Sessions | Max. SRTP to RTP Sessions | Max. Transcoding Session | Max. Registered Users | Max. TDM Channels |
|---|---|---|---|---|---|---|---|
| Mediant Software E-SBC Virtual Edition (VE)  | Virtualized data centers | 6,000 | 6,000 | 4,000 | 350 | 30,000 | 0 (**none**), SBC Only |
| Mediant Software E-SBC Server Edition (SE)  | Large Entreprises, Service Providers | 24,000 | 24,000 | 16,000 | | 120,000 | 0 (**none**), SBC Only |

Figure 8 – Genesys Offered Software SBCs

AudioCodes and Genesys continually update the products and regularly test the Software E-SBCs against new hardware configurations. As a result, the number of sessions supported may increase in the future and is highly dependent upon the hardware utilized. Please consult the Genesys documentation site at https://docs.genesys.com/Documentation/AC for further information and full details of current capacities of the Genesys offered AudioCodes Software E-SBC.

**Benefits of Genesys provided AudioCodes Session Border Controllers and Media Gateways**

The Genesys SBCs and Media Gateways benefit from the tight product relationship that has been established between Genesys and AudioCodes. Some of the unique benefits of the Genesys/ AudioCodes SBCs for Genesys customers include:

- **Flexible Deployment and Scalability** – Ability to support TDM and SBC functionality within the same physical box with the Mediant 1000 ad 3000, ability to deploy the Software E-SBC on both barebones Intel servers or within virtual machine environments, scalability from 150 to 24,000 simultaneous sessions within the same box, flexibile high availability options, and shared code base and user interface across all SBCs.
- **REST Application API** – Provides application input and control over routing and manipulation rules, as well as configuration of the SBC through a web services API.
- **Configuration Wizards** – An SBC Configuration Wizard is provided, allowing the SBC to utilize pre-developed templates that provide tested configurations between various components and SIP trunk providers. New templates continue to be added as new integrations are tested.
- **Built in WebRTC Gateway Support** – Provides the ability for the SBC to act as a gateway from WebRTC to SIP (and vice-versa).
- **Opus Vocoder Support** – Built in support for the Opus Vocoder that is part of WebRTC. Opus was designed to handle the high packet loss and jitter inherent in the unmanged public Internet. The AudioCodes SBCs and MGWs also support Dynamic Voice Quality Adaptation which dynamically adjusts the Opus coder to optimize voice quality as network bandwidth fluctuates. The SBCs and MGWs can transcode voice from Opus to other standard codecs including G.711.
- **Voice Quality Management System Integration** – Embedded voice quality probes in the SBCs enable direct integration with AudioCodes Session Experience Manager (SEM, also resold by Genesys) for voice quality monitoring and management.

- **Genesys and AudioCodes Joint Testing, Development, and Support** – Tight integration and joint R&D, labs, testing, and support between Genesys and AudioCodes.

#### 3.4.5.6 Genesys Offered Provisioning Systems

Genesys offers two provisioning systems - Genesys Feature Server and AudioCodes Element Management System (EMS).

**Genesys Feature Server (with Device Management)**

Genesys Feature Server provides device management and provisioning capabilities for certain Genesys supported SIP phones, including Genesys, AudioCodes, Polycom, and YeaLink.

Genesys Feature Server is a software based component that runs on industry standard servers (as does the rest of the Genesys platform) and can be installed on either physical servers or virtual machines. The device management capabilities of Genesys Feature Server are included with Genesys SIP Server.

Further information on Genesys Feature Server, including more on the device management capabilities, are provides in section 4.9 of this document.

**AudioCodes Element Management System (EMS)**

AudioCodes Element Management System (EMS) provides the ability to provision AudioCodes SIP phones (including Genesys rebranded phones), media gateways, and session border controllers. EMS serves as a central control point for large numbers of AudioCodes VoIP network elements including media gateways, SBCs, and IP phones.

Like Genesys Feature Server, EMS is a software based component that can run on industry standard physical servers or in a virtual machine.

Some of the capabilities of EMS include:

- **Device Autodiscovery**
- **Zero Touch Provisioning** – allows for the automatic pushing of configuration files and firmware to devices
- **Fault Alerting and Performance & Security Management** with online graphs, activity journals, historical logging, and search capabilities
- **Bulk Provisioning Tools**
    - Ability to create and deploy per device/group of devices configuration files and firmware
    - Hierarchical templates for enterprise wide and locally specific values.
    - Ability to send a message to a single phone, group or phones or all IP phones
- **Distributed Load**
    - Provisioning activities can be paced with a "pause" between devices (such as phones) in order to eliminate load spikes

It should be noted that AudioCodes EMS is limited to provisioning of AudioCodes devices only. Genesys Feature Server would be required for provisioning or non AudioCodes phones, such as Polycom and Yealink. Even if Genesys Feature Server is used customers are still able to utilize AudioCodes EMS for provisioning of AudioCodes SBCs and Media Gateways.

**Positioning**

Both Genesys Feature Server and AudioCodes EMS provide device provisioning capabilities.

Genesys Feature Server should be positioned when:

- Customer is using phones supported by Genesys SIP Server including those from AudioCodes, Genesys, Polycom, and YeaLink, or when using a mixture of phones from these vendors.
- Customer does not require provisioning for SBCs or media gateways or is using non-AudioCodes SBCs or MGWs.
- Customer desires a provisioning solution for no additional license cost.

AudioCodes Element Management System (EMS) should be positioned when:

- Customer is deploying AudioCodes SBCs and media gateways
- Customer is using only AudioCodes (or Genesys) phones, and using AudioCodes SBCs and MGWs and desires the ability to manage all devices from the same provisioning system.

While Genesys Feature Server and AudioCodes EMS may both be used to manage devices there is no direct integration between Genesys Feature Server and AudioCodes EMS.

#### 3.4.5.7 Genesys Offered Media Quality Measurement and Monitoring

Genesys offers the **AudioCodes Session Experience Manager (SEM)** to provide the ability to monitor and manage voice quality from AudioCodes phones, SBCs, and media gateways. Since SEM makes use of the AudioCodes phones, SBCs, and media gateways, no additional network probes are required.

Some of the functionality provided by SEM include the ability to:

- **View network topology** via maps, tables, or regional views, which makes it easy to visually locate problems.
- **Watch VoIP metrics and statistics** including call success and failure rates, bandwidth utilization, and quality metrics.
- **Investigate specific calls** including enhanced call details and the ability to sort, search, and filter calls.
- **Check end user satisfaction with call quality**
- **Send alarms** when a quality issue occurs including active and historical alarms. Users can define thresholds for alarms. Notifications of alarms can be provided via email, SNMP and Syslog.
- **Receive reports** to validate performance and adherence to SLAs. Summary, trend and top user reports are provided in graphical and tabular views. Users also have options to customize reports.

In order to use SEM to manage calls end to end, AudioCodes phones, SBCs, and media gateways should be utilized. In the event the customer is using non AudioCodes phones but still using AudioCodes SBCs and media gateways, SEM can still be utilized, however it is unable to collect call quality information from non AudioCodes phones.

#### 3.4.5.8 Other Voice Network Components

Genesys also provides support for other Media Gateways and Session Border Controllers. Some of the tested and supported components include:

| Component | Recommended | Others Supported |
|---|---|---|
| **Media Gateways** | AudioCodes Mediant | Cisco |
| **Session Border Controllers** | AudioCodes Mediant or Genesys AudioCodes Software E-SBC (Server Edition or Virtual Edition) | Oracle AcmePacket, Sonus, Cisco CUBE (see note) |

Figure 9 – 3rd Party Media Gateway and SBCs

Further details on supported Media Gateways, Session Border Controllers, and other components may be found in the "Genesys Supported Media Interfaces Guide" located on the Genesys documentation site (http://docs.genesys.com).

Alternative media gateways and SBCs may potentially be utilized, although additional testing - possibly including field validation - may be required. The recommended components are encouraged due to the level of field knowledge and experience with these technologies by Genesys, our partners and customers.

**Note:** It should also be noted that while the "Genesys Supported Media Interfaces Guide" lists support for the Cisco CUBE SBC, due to limitations with the Cisco CUBE it not recommended for most deployments.

### 3.4.6 Additional 3rd Party Components

The following provides an overview of additional 3rd party components which may be utilized in the SIP Voice Solution and specific recommendations. Alternatives may be utilized, however the recommended components are encouraged due to the level of field knowledge and experience with these technologies.

**Network Management System (NMS)**

A network management system (NMS) is a set of operations and management tools deployed which allow an enterprise to monitor the health of the various components (hardware and software) connected to a network. A NMS can perform a myriad of tasks. Genesys can send alarms via SNMP to the NMS providing the enterprise visibility to specific performance metrics or events. Genesys also supports polling allowing an NMS to proactively check on the status of Genesys applications.

**HTTP Load Balancer**

An HTTP Load Balancer is commonly required to distribute HTTP requests across multiple servers and manage high availability for HTTP based components. The load balancer may manage request distribution across a server farm at a physical location or distribution and failover across multiple physical locations. The load balancer may establish affinity between the client and server if "sticky sessions" are required. A load balancer may also perform some security management tasks such as SSL offloading or client authentication via tokens or certificates thereby reducing the demand on the application tier.

| Component | Recommended | Version | Note |
|---|---|---|---|

| | | | |
|---|---|---|---|
| **Operational Management** | Zabbix | | Alternatives - HP OpenView, Nagios, Tivoli, OpenNMS |
| **Phone Sets** | Genesys 420HD | | Alternatives include Yealink, Polycom and AudioCodes |
| **SIP Soft Clients** | Genesys Softphone | | Alternatives include Counterpath Bria |
| **Database** | MSFT SQL Server 2012, Oracle 12c | | Optional: Applicable if GVP is in scope and GVP reporting server is used. |
| **Web Application Server** | Apache Tomcat 6.x | 6.x | Optional: Applicable if GVP is in scope. VoiceXML application server. Various application servers can be utilized. Java based applications need to be compliant with J2EE 5 and JSP2.1 and Servlet 2.5 |
| **Virtualization** | VMWare ESXi | 5.1+ | |

For a complete list of all 3rd party components supported by SIP Server and GVP, please consult the appropriate sections in the Supported Media Interfaces reference manual [http://docs.genesys.com/Special:Repository/g_ref_smi.pdf?id=73c96eb2-c7cb-4839-95e5-0c910861e615 ].

Note:

- Operating systems are not listed. Genesys recommends either RedHat Enterprise Linux 6.0 64-bit or Windows Server 2012 64-bit. Some components may only be supported on a specific OS. When a component is supported only on a single OS this is specifically called out.
- Databases are required as part of the Common Components Blueprints. RDBMS is often a customer preference. Genesys recommends either Microsoft SQL Server 2012 or Oracle 12c. For Business Continuity there are specific requirements on the database features utilized.

## 3.5 Limits and Constraints

The following are limits and constraints in both the scope of this document and the solution:

- The SIP Voice Blueprint is focused on ACD replacement and SIP telephony usage. SIP Server can be used in many other capacities including integration into other IP PBX and IMS architectures. These architectures are not in scope for this solution.
- SIP Feature Server uses an embedded Cassandra instance. Unlike other Genesys products is not (yet) designed to be able to take advantage of an external Cassandra database.
- Genesys ORS is used for performing all routing and treatments as specified in the Common Components Blueprint
- Media Control Platform is designed to provide in-queue treatments and music using pre-recorded music files. The MCP does support RTSP and can integrate with a streaming music source via RSTP however additional validation should be considered.

# 4 Deployment View

## 4.1 Solution Deployments

There are numerous ways the SIP Voice Solution can be architected. This blueprint focuses on the two most common deployment models.

**Centralized Deployment**

In a centralized deployment model, the components are situated in a common data center. This deployment is ideal for small and medium sized deployments (up to 2,000 agents). We consider a standard Genesys Business Continuity deployment a Centralized Deployment architecture because it is designed to provide centralized process and reflects a symmetrical replication across two data centers.

**Distributed Multi-Site Deployment**

In a distributed multi-site deployment, the majority of Genesys components may still be housed within a common data center, however, some key elements are deployed at various branch sites and are co-located with media gateways, SBCs, and agents. Multi-site deployments tend to be complex and require careful configuration, but are ideal for large deployments (10,000 to 25,000 agents) and provide additional resiliency in case a branch site loses connection to the main data center site. Unlike the a Business Continuity deployment the Distributed Multi-Site Deployment represent an asymmetrical distribution of components.

High Availability deployment of Genesys components is supported in both deployment models as is Business Continuity of the data center components.

## 4.2 Centralized Deployment

The centralized deployment assumes that the customer has a data center that is reachable by all agents and that the network has the capacity to support the traffic between solution components in the data center and the agents' desktop/endpoints.

A typical deployment will be similar to that depicted in the following diagram. Note the diagram shows a logical diagram highlighting the signaling and interaction flow. The specific components distribution across servers would vary based upon the capacity requirements and sizing.

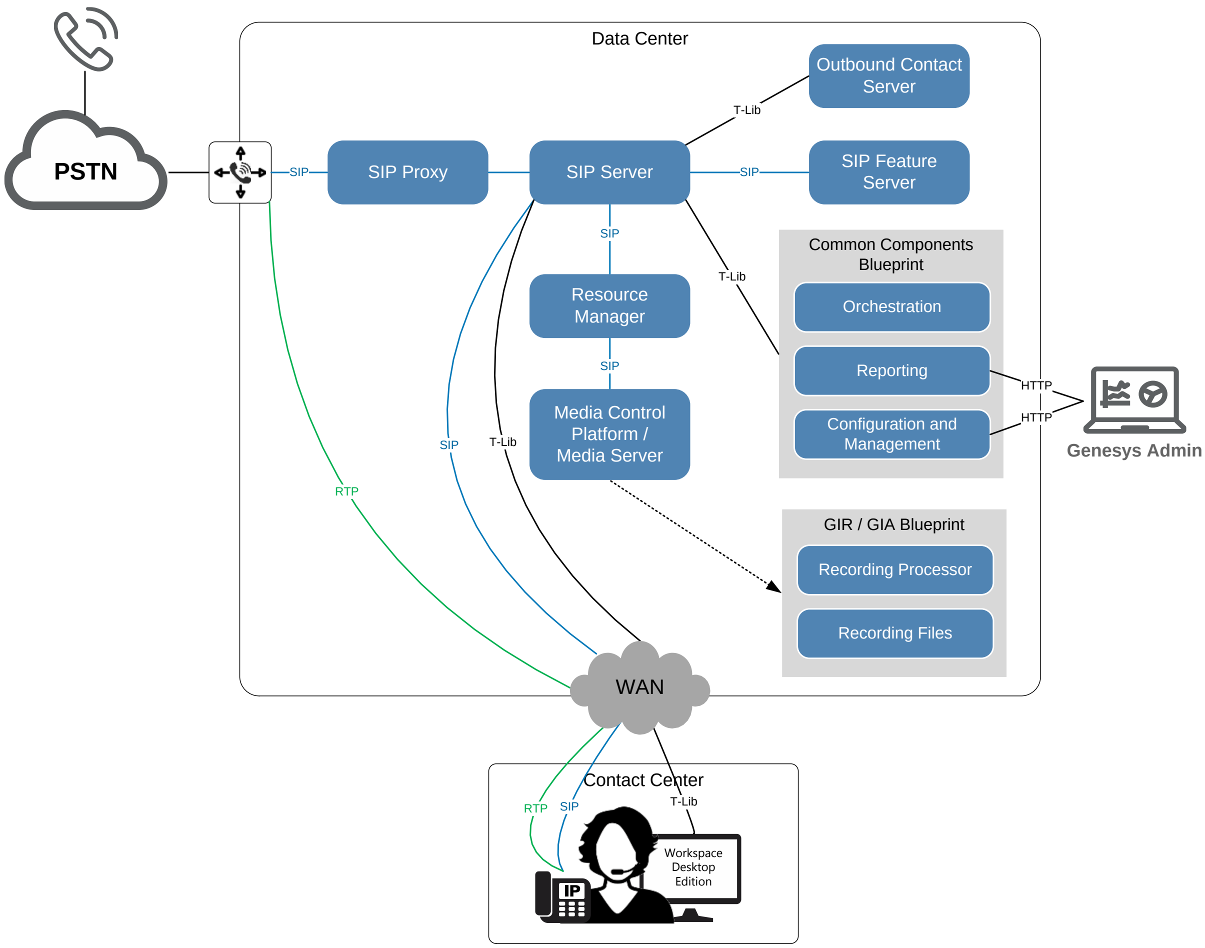



Figure 10 - Central Deployment Model

Voice traffic enters the enterprise via a SIP Trunk into the Genesys E-SBC component (media gateways and other SBCs are also supported). The initial SIP INVITE is sent to the SIP Routing node which makes a determination on how to handle the call. This decision is typically made by matching the dialed number against the internal resources and dial plan. Typically, this inbound call will map to a routing strategy on Genesys ORS/URS and SIP Server will communicate with Genesys Orchestration to obtain details on the call handling. The routing or orchestration strategy will return instructions such as commanding SIP Server to play a welcome message followed by a menu. SIP Server will direct the call to the Media Server (MCP), at which point the call will actually be answered and the RTP path will be established, and instruct the MCP to play the appropriate messages and return the results to SIP Server. These results are returned to ORS which will perform additional logic such as determining which agents are the best candidates or targets for the call and, when an agent is finally selected, informing SIP Server to transfer the call to the selected agent.

Together the SIP Routing node and MCP nodes handle the initial IVR qualification, parking and routing to the agent. When the call is delivered to the agent, Genesys call recording may also be used. If call recording is enabled, the MCP nodes will bridge the audio between the caller and agent to capture the audio and provide it downstream to the respective recording subsystem. (Note: Further information on Genesys Interaction Recording is provided in the separate GIR/GIA Blueprint).

The Outbound node handles the outbound voice campaign. It interacts with SIP Server (and MCP by extension) to make outgoing calls, perform call progress detection and then route the call to an agent. The Outbound node also performs the required campaign management such as ensuring the correct pacing, managing retries, etc.

Web based user interfaces are provided for administering the solution and providing real-time and historical reporting. The Management node provides the OAM&P functions including configuration, solution monitoring, managing high availability/failover and alarming. The Reporting node provides both real-time and historical data collection. The historical data which is captured is transformed into the data warehouse for reporting and directly accessible through a web based reporting solution which includes standard default reports. (Note: Further information on Orchestration, Management and Reporting is provided in the Common Component Blueprint).

There are also supplementary services specific to the SIP Voice solution which are provided by the SIP Feature Server. It provides voicemail, advanced dial plan management, and device/phone management including DHCP, firmware updates and device level configuration.

Note: External databases are required as part of the solution and provided typically provided by the customer

The following table lists the components that make up each of the logical nodes. The actual deployment layout may vary significantly based upon the final architecture.

| Node | Component | Comments |
|---|---|---|
| SIP Routing | SIP Server | Provides SIP ACD and telephony capabilities |
| | SIP Proxy | Recommended (Optional) - For SIP HA without virtual IP address. |
| | ICON | Captures interaction details for historical reporting |
| SIP Resource Management | Feature Server | May be included as part of SIP Routing VM |
| | Resource Manager | Manages resource distribution for media services |
| MCP | Media Control Platform | Multiple nodes can be deployed to support the required number of ports. *Note: While MCP is multi-threaded multiple process can be instantiated per node to potentially increase the total capacity.* |
| Orchestration | Orchestration Server (ORS) | |
| | Apache Tomcat | Customer web infrastructure can be used if it exists. Used for SCXML delivery |
| Routing | Universal Routing Server (URS) | |
| | Stat Server (Routing) | |
| | Outbound Contact Server | |

| | | |
|---|---|---|
| Framework | Configuration Server | |
| | Solution Control Server | |
| | Message Server | |
| | SNMP Master Agent | |
| Reporting | Info Mart | |
| | Interactive Insights | |
| Admin UI | Genesys Administrator Extensions (GAX) | With appropriate plug-ins for Feature Server, Pulse, etc. |
| | Genesys Administrator | Used for additional administration capabilities |
| | Apache Tomcat | Or supported web servers for GAX |
| Agent Support | Configuration Server Proxy (for Workspace) | |
| | Stat Server for Agents | |
| | Composer | |

Table 1 - Data Center Node Components

Please see section 6.1 Solution Sizing Guidelines for details on the sizing of each VM node.

## 4.3 Distributed Multi-Site Deployment

Voice is unique from other communication channels handled by the contact center. Not only is it generally considered the most critical channel, it is a continuous real-time channel, requires significant bandwidth for transport and may have geographic access constraints. Due to these characteristics some contact centers will elect to deploy a subset of the Genesys SIP Voice components local to the contact center agents and media gateway/SBC rather than relying solely on a centralized deployment.

The multi-site deployment model includes processing nodes distributed at various sites within the customer's enterprise. These distributed nodes are typically branch offices or regional sites and manage functions specific to signaling and media processing. Various shared components will continue to be deployed within a data center. This deployment adds complexity to the overall solution design – configurations of nodes, routing, firewalls, etc. become more cumbersome.

The advantages of deploying a multi-site topology are resiliency and scalability. By adding SIP Server and other processes to a branch site, that site can continue to function if it loses connectivity to the data center, although typically with some reduced capabilities. Adding processing nodes to the branches also increases the scalability by supporting more agents.

There are certain trade-offs that must be considered. Routing may be organizing around functional or regional groupings of agents which limit some of the global routing capabilities of Genesys. If global routing is desired a common Stat Server must be used for all regional SIP Servers and Agent-Reservation must be used.

The following diagram depicts the Multi-Site Deployment model:

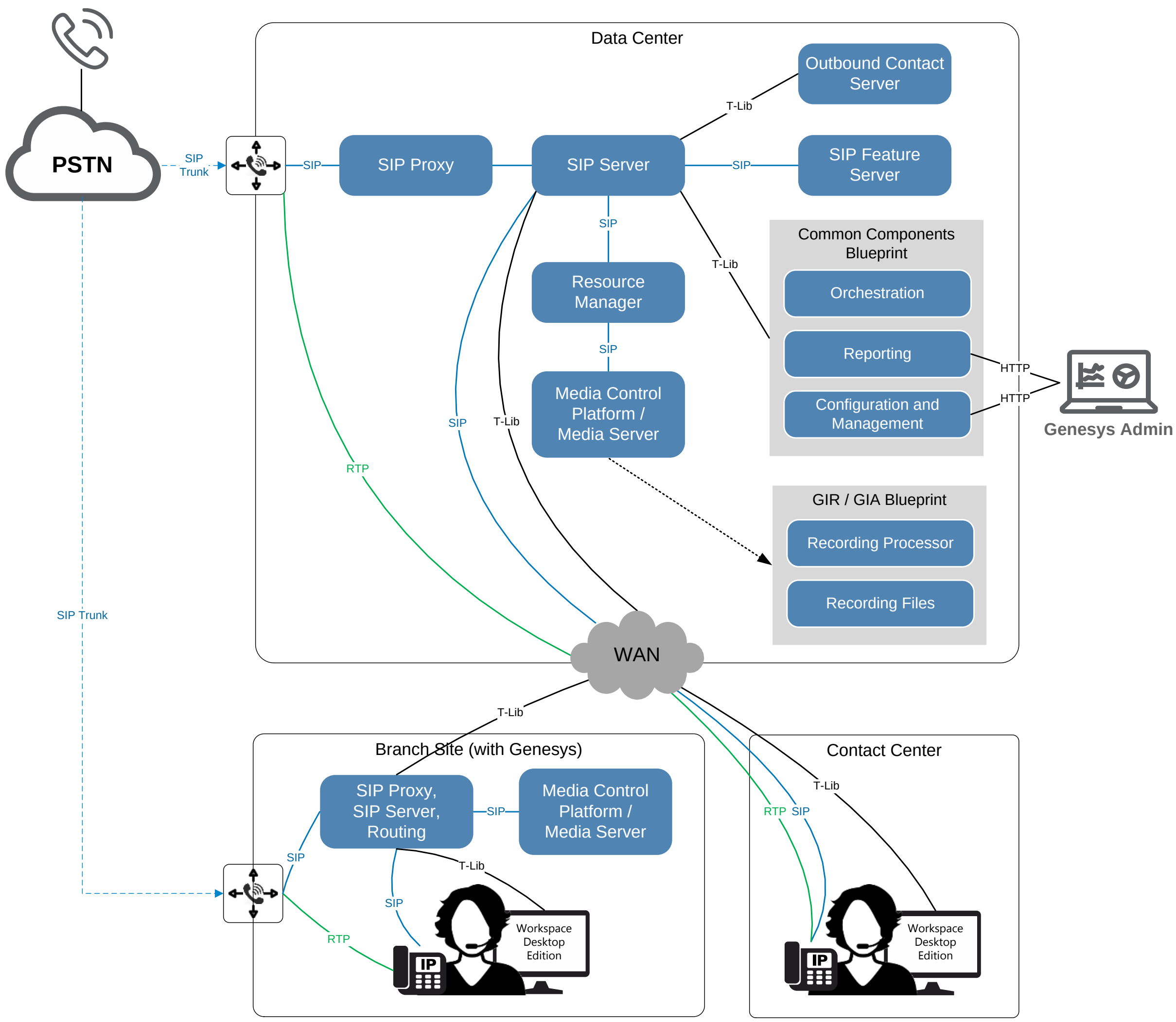



Figure 11 - Multi-Site Deployment Model

In a distributed multi-site deployment there are several options for configuring how voice traffic is handled. One important variant is whether PSTN/SIP Trunks terminate at the individual branch sites or are connected centrally and distributed internally within the customer's enterprise network. In the diagram above, there is PSTN termination both into the data center as well at the branch level. Therefore both sites would have an SBC or Media Gateway.

There are myriad possible traffic flows possible with this architecture. The traffic may arrive at the contact center by first terminating at a centralized site. If the voice traffic is then distributed out from a central site one common option is to deploy media resources (MCP nodes) to handle the initial call triage prior to routing the call to an agent. This 'triage' may be in-front IVR for self-service, provided by GVP, or menuing/call qualification before routing the, provided by Media Server. During this 'triage' phase, if self-service IVR is provided a large number of callers may be satisfied in IVR and not require any agent assistance. If the caller requires agent assistance and no agents are available, then the call may be queued (parked) while waiting an available agent. A similar approach is used for very large customers by establishing a tiered SIP Server architecture. The qualification and parking tier will perform the initial triage and routing. The routing strategy may determine that an agent in the branch is the best resource to handle the call, in which case the call can be redirected to the SIP Route Hub servicing that agent.

Traffic may also arrive at the branch site first providing localized termination and servicing of the caller followed by subsequent call routing. In general, the topology and traffic mix is specific to the call volume and characteristics. For example, in a multi-country deployment the local site may provide easy access to local intra-country telephony and initial call triage may be performed locally while voice traffic may still flow back to the centralized site for advanced IVR applications with ASR. If an enterprise is using the SIP Voice Blueprint to address both contact center and enterprise users, it is possible that most of the call traffic between the PSTN and branch is intended for enterprise users.

In a Distributed Multi-Site Deployment the nodes in the data center are the same as in the Central Deployment Model. Each branch will have local nodes to provide local voice and agent services. This approach offers a smaller localized deployment, as the orchestration, reporting and other centralized business services would be delivered from the primary data center.

The local nodes include:

- **SIP Route Hub** - The **SIP Route Hub** includes the processes for handling SIP voice services for the agent and local routing requirements.
- **MCP Hub** - The **MCP Hub** provides local media resources within the branch. The local resources would typically be used for Music on Hold and conferencing. However, there may be a need to setup IVR services on the Branch Site (e.g., survivability if the Data Center IVR capabilities are lost or if the voice traffic arrives at the branch first via a SIP trunk directly to the branch).

| Node | Component | Comments |
|---|---|---|
| SIP Route Hub | SIP Server | |
| | SIP Proxy (optional) | For SIP HA without virtual IP address. |
| | Feature Server | |
| | ICON | |
| | Distributed Solution Control Server | |
| | Logging Message Server | |
| | Resource Manager | |
| | Universal Routing Service (URS) | |
| | Orchestration Server (ORS) | |
| | Stat Server - Routing | Local Stat Server – note that Agent-Reservation needs to be setup |
| | Apache Tomcat | Or other web server for SCXML delivery |
| MCP Hub | Media Control Platform | Multiple nodes can be deployed to support the required number of ports. |

| | | |
|---|---|---|
| | | *Note: While MCP is multi-threaded multiple process can be instantiated per node to potentially increase the total capacity.* |
| Agent Support | Config Server Proxy | |
| | Stat Server for Workspace | |
| Development | Composer | Composer may be deployed locally or centrally depending upon the development and management or strategies and applications |

Table 2 - Branch Node Components

### 4.3.1 SIP Communications (Enterprise users)

Genesys SIP Communications is Genesys offering which provides standard voice services to enterprise telephony users (non-contact center agents). A SIP Communications deployment utilizes the same core architecture and solution which would be deployed for contact center users but has a set of additional considerations.

As a SIP Communications user is not an agent they do not log-in to the system, require a desktop to manage their communications or take contact center calls. All SIP Communications features are delivered with a standard SIP phone. Users may use a hard phone such as the Genesys HD420, hard phones from other supported vendors or a software based SIP endpoint such as the Genesys SIP softphone.

Access to voicemail may be performed entirely over the phone or through a web browser, allowing users to retrieve voice messages, change their greeting, or perform other administrative functions.

### 4.3.2 Large System Deployment

**SIP Server Tiers**

In very large architectures it is common practice to have multiple SIP Server tiers deployed. The number of tiers varies by the overall architecture. The most common approach is simply distributing traffic into two tiers – Self-service/Parking Tier and Agent Tier. Larger architectures may be distributed in up to 4 tiers – Network Tier, Self-Service/Queuing Tier, Routing Tier and Agent Tier.

- SIP Server Network Tier – Inbound calls are received and distributed using very simplistic routing strategies. Typically used to load balance across multiple SIP Server instances or to route the call to a particular data center. *Not to be confused with the Network SIP Server product.*

- SIP Server Self-Service and Parking Tier - Inbound calls are received and processed by the call self-service and parking tier. This layer will manage calls through self-service, call triage, and routing, including queuing if no agents are available.

- SIP Server Routing Tier – Qualified inbound calls and transferred/outbound calls are processed at this tier to determine where to route the call to. When using a Routing Tier, the Self-Service tier above will mainly handle IVR operations then forward to the Routing tier which will handling parking of the call.

- SIP Server Agent Tier – Agents are directly registered with the SIP Server Agent Tier. Callers are targeted to agents residing in this tier. These SIP Servers will also manage agent related media functions such as call recording, conference, on-hold treatments. Calls which are managed by the Agent Tier often generate more events per interaction and have more clients listening for events.

The creation of a tiered SIP Server approach provides both a staggered distribution of load and horizontal scalability. Self-service calls are handled entirely by the Call Qualification and Parking Tier thereby reducing the downstream load on the Agent Tier. This separation also makes it easy to add SIP Server Agent pairs to support large contact center deployments.

For large deployments the following options should be reviewed:

- SIP processing capacity can be increased by using a tiered SIP Server architecture.
    - A tiered SIP Server architecture can reduce the number of client connections monitoring a given SIP Server as the tiered architecture distributes objects such as Routing Points and Agents at different layers
    - When establishing a Routing Tier, call flows and strategies will need to be designed and reviewed. Optimization of ISCC Trunk usage with these strategies will be essential especially if agents will be transferring calls back to the Routing Tier.
- The number of monitoring clients impact the main T-Server thread within SIP Server. Genesys LDS can be used to proxy these monitoring clients so they only use a single connection thereby reducing the load.
    - The largest load is often due to multiple Stat Servers as they have a large set of objects which they may be monitoring.
- KVP updates will impact the performance of SIP Server. Best practice is to update numerous KVPs within a single update transaction to reduce the load on SIP Server.
    - Routing strategies should be designed to reduce the frequency of KVP updates by combining requests.
    - Adjust Workspace to combine KVP updates into fewer requests. This applies to both Workspace and custom desktop applications.
- The number of treatments of a call should be reviewed and optimized, especially treatments while the call is in queue.

## 4.4 High Availability Deployment

To provide resiliency in both deployment models, High Availability (HA) options are recommended for all components.

The standard approach to high availability supported by many of the Genesys components is to use a primary and backup process. The backup process takes over from the primary if it fails. The backups can either be setup as a cold-standby, warm-standby or hot-standby. The SIP Voice Blueprint recommends hot-standby where supported. In most cases the primary and backup components should be contained within the same data center. For cases where components are desired to be split between data centers, refer to disaster recovery and business continuity. More information on Genesys High Availability including detailed definitions is provided in the **Common Components Blueprint**.

In general, each node listed in the deployment models should have a primary and backup copy within the same data center (or physical site). The following diagram depicts the primary and backup VMs for the solution. Different components utilize different approaches for high availability including IP Takeover, Clustering and Parallel Processing.

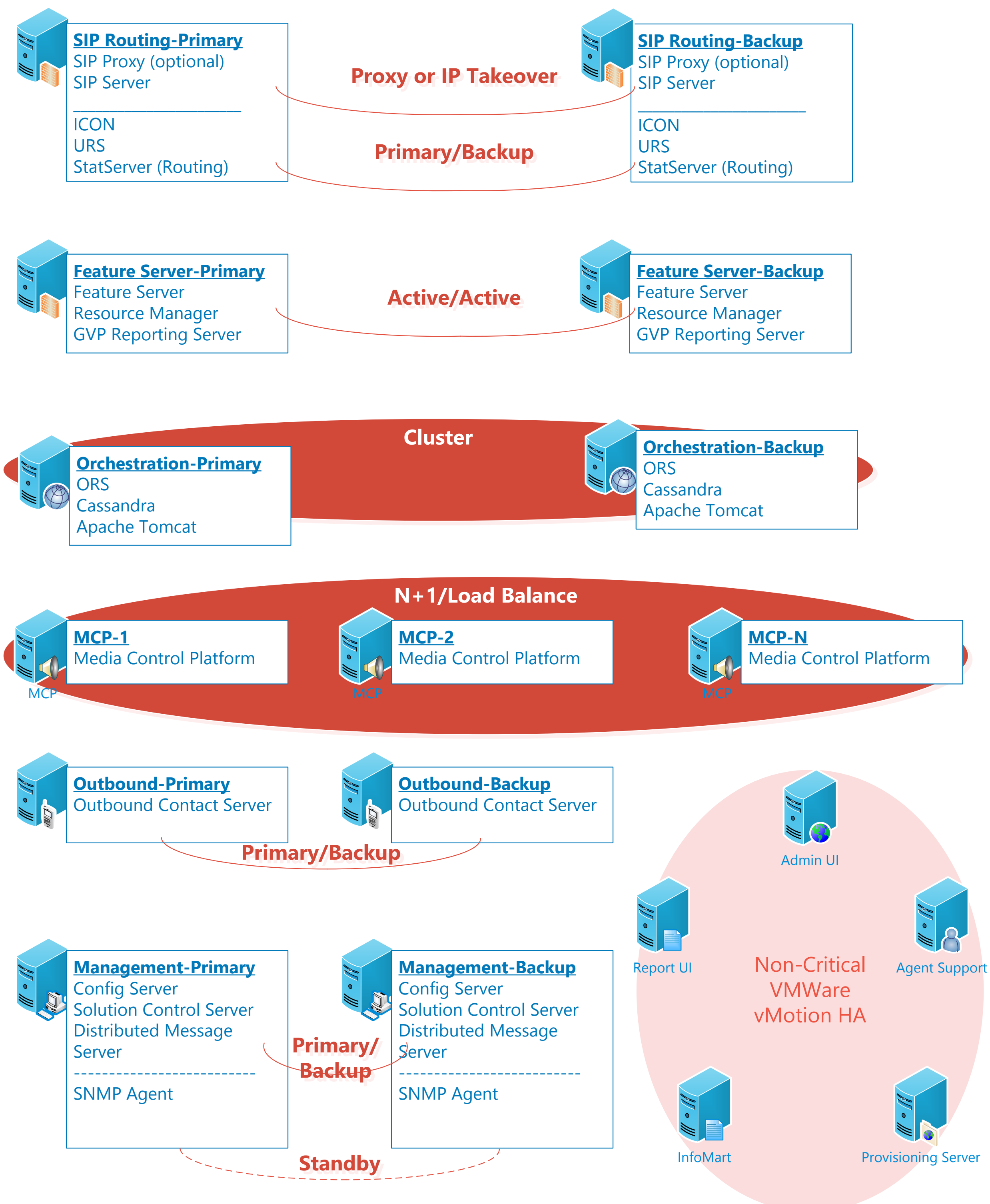



Figure 12 – SIP Voice Solution HA

The following list the high availability levels supported by the respective components:

| Genesys Component | HA Level | HA Type |
|---|---|---|
| SIP Proxy | Cluster | N+1 |
| SIP Server | Hot Standby | Primary/Backup |
| SIP Feature Server | Active/Active | 2N (Primary/Backup) |
| Resource Manager | Active/Active | 2N (Primary/Backup) |
| Media Control Platform | Cluster | N+1 |
| Outbound Contact Server | Warm Standby (With campaign sync) | Primary/Backup |
| Nuance ASR/TTS | Cluster | N+1 |
| MRCP Proxy | Warm Standby | Primary/Backup |
| GVP Reporting Server | Warm Standby | Primary/Backup |
| Application Server | Cluster | N+1 |

The following sections describe high availability to the various components of the solution.

#### 4.4.1.1 SIP Server HA

Each SIP Server may be configured to provide hot standby local availability (primary/standby). For high availability, a local pair of SIP Servers are deployed within the local site. The primary SIP Server synchronizes all call data and events with the backup SIP Server in real-time. As a result, if the primary fails, the backup SIP Server has full information about the call and can continue processing as if nothing happened (clients such as Genesys router and agent desktop applications will continue to function as if nothing had happened). To provide physical resiliency the primary and backup instances should be deployed on different physical servers. If VMWare is used the respective VMs should be deployed on separate ESX hosts.

In a hot standby HA configuration, loss of the primary SIP Server causes the standby SIP Server to immediately take over without loss of calls or call information (such as attached data, etc). While Genesys clients have intelligence to support a switch over between primary and backup components, with SIP signaling it is critical that the failover be transparent to the SIP clients. On the SIP signaling side, a method must be utilized to ensure that the endpoints, gateways, SBCs, etc. can still maintain existing calls in the event of a primary SIP Server failure (or manual failover).

SIP Server supports several methods to provide a transparent SIP failover. The recommended approaches based upon order or preference are:

1. SIP Proxy (DNS based approach)
2. Virtual IP takeover (SCS based with scripting)

**Genesys SIP Proxy** – Genesys SIP Proxy can be used in front of SIP Server in order to ensure SIP endpoints, gateways, etc are always communicating with the currently active SIP Server (ie: the current primary). Endpoints communicate with the appropriate SIP Proxy via DNS records. SIP Proxy monitors each of the SIP Server HA pairs and forwards the request to the current primary SIP Server. SIP Proxy will always know which SIP Server is currently the primary and thus can perform this function. In the event of a failover, SIP Proxy simply starts redirecting new messages to the new primary SIP Server. SIP Proxy is included as a core component of the Genesys SIP Server solution. No additional license is necessary to utilize this. ***This is Genesys preferred method as it offloads the HA management largely to Genesys and eliminates network challenges posed by the use of virtual IP addresses.***

Each SIP client/user agent must be able to connect to two (or more) SIP Proxy instances in case one goes down.

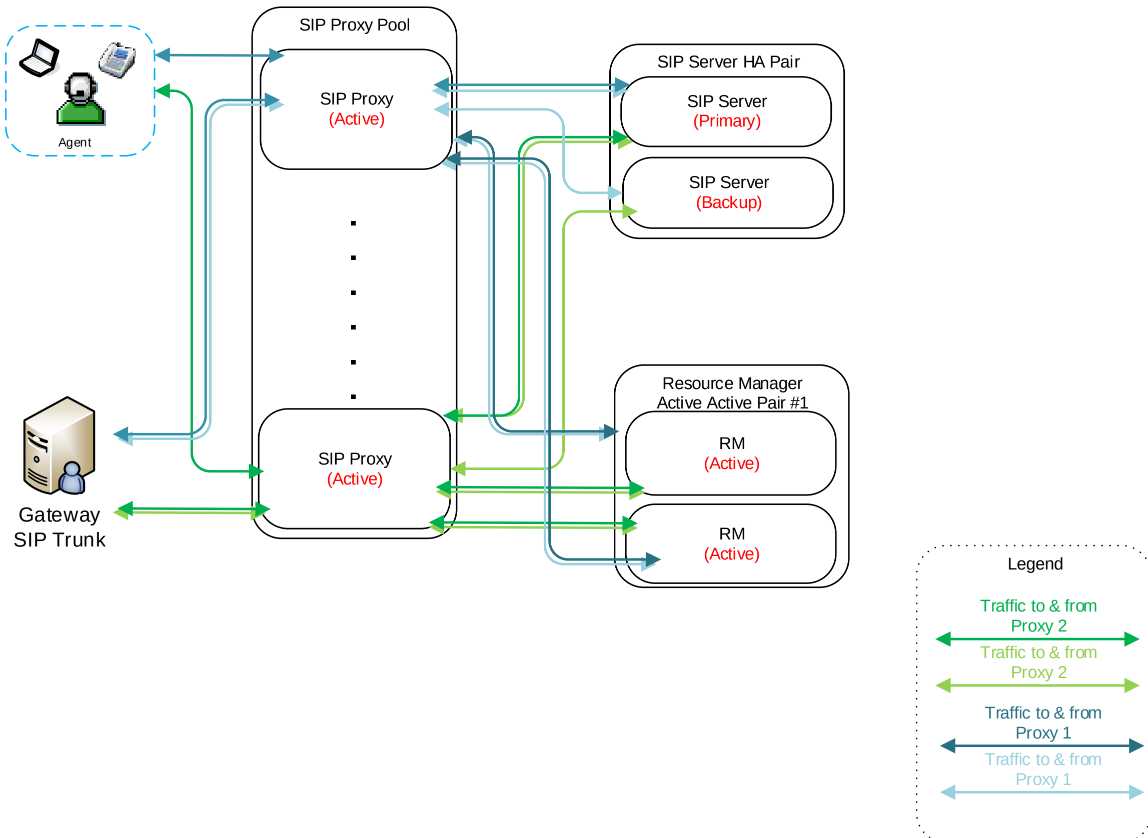



Figure 13 – SIP Proxy Deployment

For more information on IP Takeover consult the SIP Proxy HA section of the SIP Server HA Deployment Guide (Genesys)

- **Virtual IP takeover** – In this approach, the server operating system that SIP Server is running on will be configured **with both** a real IP Address and a virtual IP Address. All SIP traffic for SIP Server will be addressed to the virtual IP address. The primary node will have the virtual IP address activated while the backup node will have that same virtual IP address disabled. Note that this can be setup using one or two NIC cards in the server.

The Solution Control Server (SCS) will monitor the active SIP Server. If a problem is detected with that server, SCS will notify the backup server which will enable its virtual IP address and begin handling requests. As a hot standby, it will already have information on the existing SIP Sessions and can continue processing those calls.

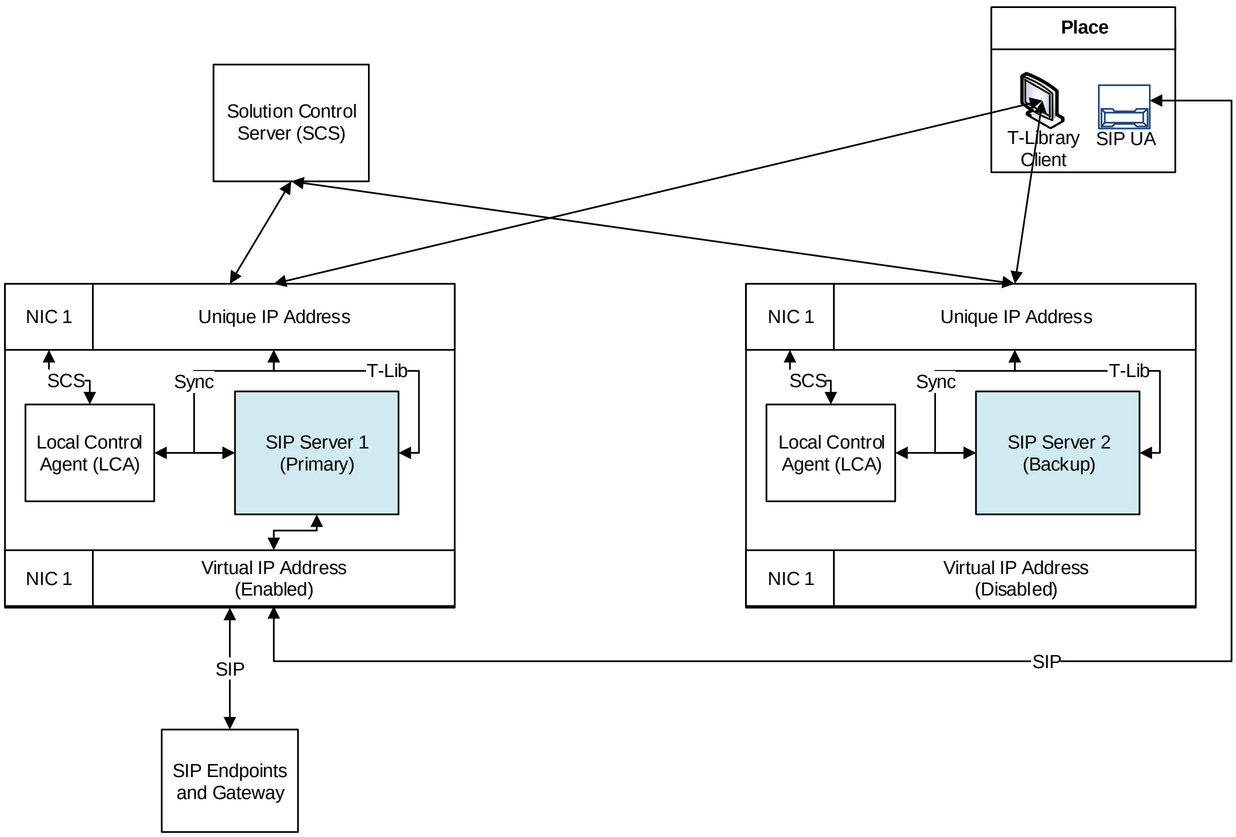



Figure 14 - Virtual IP Takeover Deployment

For more information on IP Takeover consult the SIP Server HA Deployment guide (Genesys)

Genesys also supports other approaches to configure SIP Server high availability as detailed below. While these are supported they are not recommended due to the additional interdependencies and requirements.

- **Shared IP using Microsoft Network Load Balancing** – On Windows Server platforms, Microsoft NLB may be utilized to provide a shared IP address for SIP endpoints trying to connect with SIP Server. The current primary SIP Server will “own” the shared IP address. If the primary goes down or a manual failover is initiated, the backup SIP Server will then acquire the shared IP address.

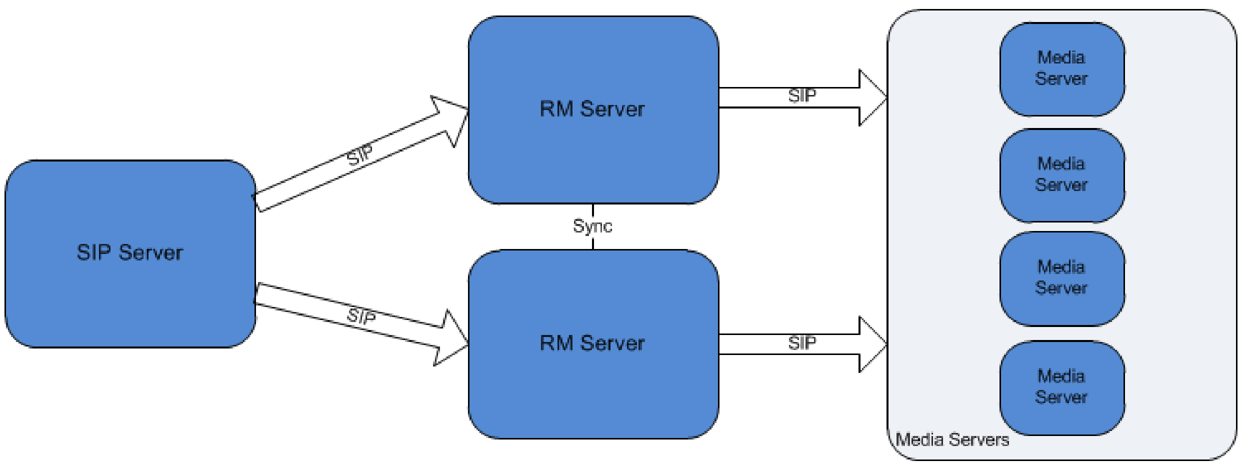
- **S-NAT approach with F5 Networks BIG IP Local Traffic Manager (LTM)** – An alternative approach to providing a shared IP managed by a host operating system is to use an F5 LTM in Static NAT (SNAT) mode to manage the IP. F5 acts as a proxy and maps the static IP provided by F5 to the real IP of the active SIP Server. All endpoints wishing to do SIP signaling with SIP Server instead will go to the F5, which will then determine which SIP Server to send it to (the correct primary), rewriting any necessary headers as required.

#### 4.4.1.2 Resource Manager and Media Control Platform

The Resource Manager and Media Control Platform are components that are used with both standard SIP Voice functionality and with GVP. Together these components establish the logical media resource pool that it used by SIP Server for all media processing functions.

The Resource Manager acts as a proxy between SIP Server and the MCP cluster.  Resource Managers are deployed in an active-active pair sharing SIP dialog port usage and conference to MCP mappings.

The SIP Server will automatically load balance traffic between the Resource Managers without requiring a third party load balancer. SIP Server uses a Contact List mechanism to perform load balancing between multiple RMs. With the contact-list mechanism, SIP Server is configured with multiple RM instances and their IP address using a contact-list parameter. Traffic to the RMs is load balanced in a round robin fashion. Additionally SIP Server proactively monitors RM availability by sending periodic OPTIONS messages to each RM instance to validate the status and include the RM in the active transport list




High Availability of Resource Managers

MCPs can be configured as a cluster of nodes providing N+1 availability. The MCPs are aware of both Resource Managers and IP address and are even designed to tolerate mid-dialog failures.

#### 4.4.1.3 GVP Reporting Server

Genesys recommends deploying the GVP Reporting server in a warm standby HA solution utilizing segregated storage. In this deployment the primary GVP Reporting Server is active and stores events in its message store. If a failure occurs, the backup GVP Reporting Server will become primary and begin collecting events in its message store. The message stores are only used for transient storage of events that have been collected but not yet processed. The collected events are batched to a common reporting database for downstream processing and aggregation.

GVP Reporting Server supports an alternate shared storage deployment however it is not typically not recommended as it requires several additional system dependencies.

#### 4.4.1.4 Nuance Automated Speech Recognition (ASR) and Text to Speech (TTS)

Multiple Nuance ASR and TTS instances can be deployed to support the overall application load. The Nuance Servers are deployed as an N+1 cluster.

Load balancing and failover of the ASR/TTS resources are managed by GVP. For MRCP v1 all requests from the MCP can be sent to the MRCP proxy to distribute requests to the ASR/TTS servers. For MRCP v2 the requests from the MCP are sent to the Resource Manager and performs ASR/TTS management and will distribute the requests to the appropriate ASR/TTS resource servers. In smaller deployments the MCP may manage the failover internally.

The respective GVP component (MRCP Proxy, Resource Manager or MCP) will proactively monitoring the resource availability of the Nuance instances and distribute requests for ASR and TTS in a round-robin fashion across the available Nuance instances.

#### 4.4.1.5 Outbound HA

Genesys Outbound utilizes a warm-standby enhanced mode. If the primary OCS fails, the backup OCS will take over the role as primary. The backup OCS has access to the status of all campaigns and campaign sequences therefore if is takes over the role of the primary the campaign processing will continue uninterrupted.

**Note:** The backup OCS does not have a real-time view of in memory records that are being processed therefore any records that were in memory at the time of a failover would eventually be marked stale and may be redialed per the established campaign rules.

#### 4.4.1.6 Web Application Server HA

The web application servers are used to serve up both SCXML applications, as described in the Common Component blueprint, and required to serve up VoiceXML applications when the Genesys Voice Platform is deployed.

The web server capacity can vary greatly based upon the application complexity. Multiple web servers can be deployed in a farm to provide high availability and scalability. HA is accomplished through an N+1 deployment.

HTTP load balancers are required to support distribution of HTTP requests from the MCPs to the VoiceXML application server farm. These load balancers do not typically need to be configured for “sticky sessions” but this requirement can vary based upon the application development paradigm that is used. The load balancer may be an external HTTP load balancer or a software based load balancer which is integrated with the web application server. For example, Apache Tomcat can be setup as a cluster using a proxy/load balancer such as Apache HTTPD with either mod_proxy or mod_jk.

*For more information see the Genesys Voice Platform 8.1 Deployment Guide or the Genesys Media Server 8.1 Deployment Guide*

#### 4.4.1.7 Media Gateway and SBC HA

The Media Gateway and/or Session Border Controller provides the connection between the external telephony network and the Genesys environment. It is critical that high availability is considered for all layers of communications.

High availability can be provided at the telephony layer by having redundant carrier connections, and ensure carrier trunking is configured to deliver calls across the telephony appliances and redirect all traffic if there is a circuit outage. Customers need to work with their telecom provider to ensure trunking is configured properly.

High availability is also required at the media gateways/SBC level.

**Media Gateway** – Multiple media gateways can be deployed at a physical location to address hardware failures. The media gateways can be deployed in an N+1 configuration with additional active circuits also provisioned by the carrier. Traffic would be distributed across all media gateway instances. In some instances customers may deploy N media gateways. In this scenario if there is a failure then the system would operate under diminished capacity until the failed component is replaced. In these scenarios customers may select hardware with internal HA, hot swappable components, utilize cold sparing, etc. to mitigate risk.

**Session Border Controller** – The session border controllers can be deployed as either a hot-standby HA pair or an N+1 approach where all instances are active. The SBCs are typically deployed as hot-standby where the primary is handling all interactions and the backup is capable of seamlessly taking over upon failure with no interruption to calls in progress. An N+1 approach may be employed where multiple SBCs are already required to handle the overall load.

#### 4.4.1.8 SIP Feature Server

Genesys SIP Feature Server provides active-active availability when two or more Feature Servers are deployed. Each Feature Server is configured to utilize a common shared Cassandra cluster, allowing for the sharing of voicemail, device management, and dial plan information. In the event one Feature Server goes down, the remaining Feature Servers can operate without loss of functionality.

Please consult section 4.9 for the overall architecture of SIP Feature Server.

##### 4.4.1.8.1 Single Site High Availability

The diagram below shows a single site deployment where each Feature Server will connect to only one SIP Server. In the event of a failure of one Feature Server, the other will continue to operate without any loss of functionality.

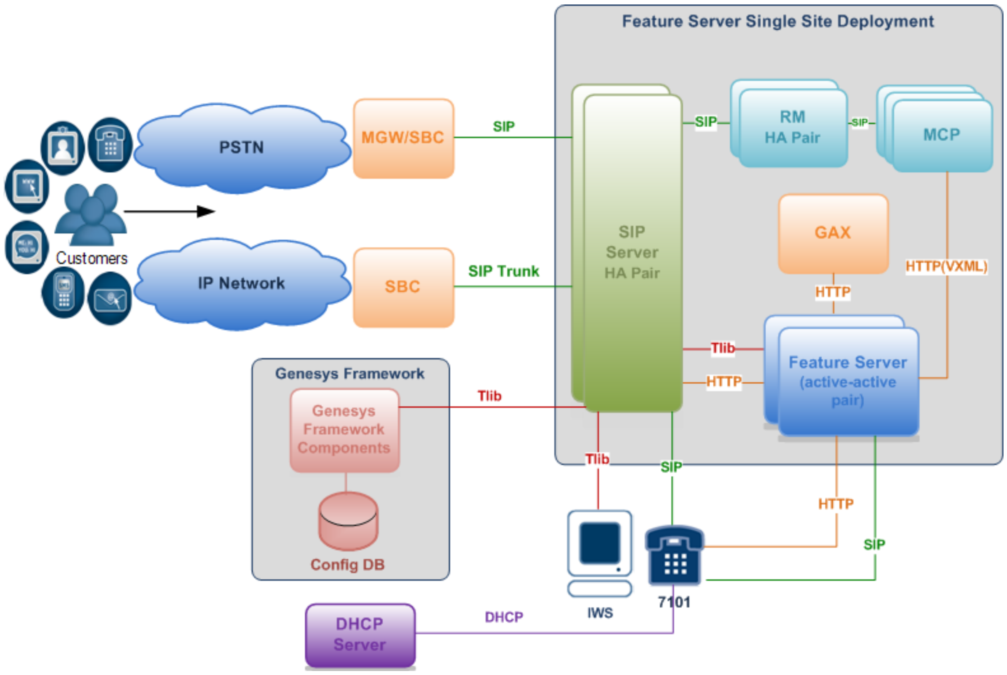



Figure 15- Single Site SIP Feature Server High Availability

### 4.4.1.8.2 Multi-Site High Availability

The diagram below shows a muti-site SIP Server deployment with SIP Feature Server:

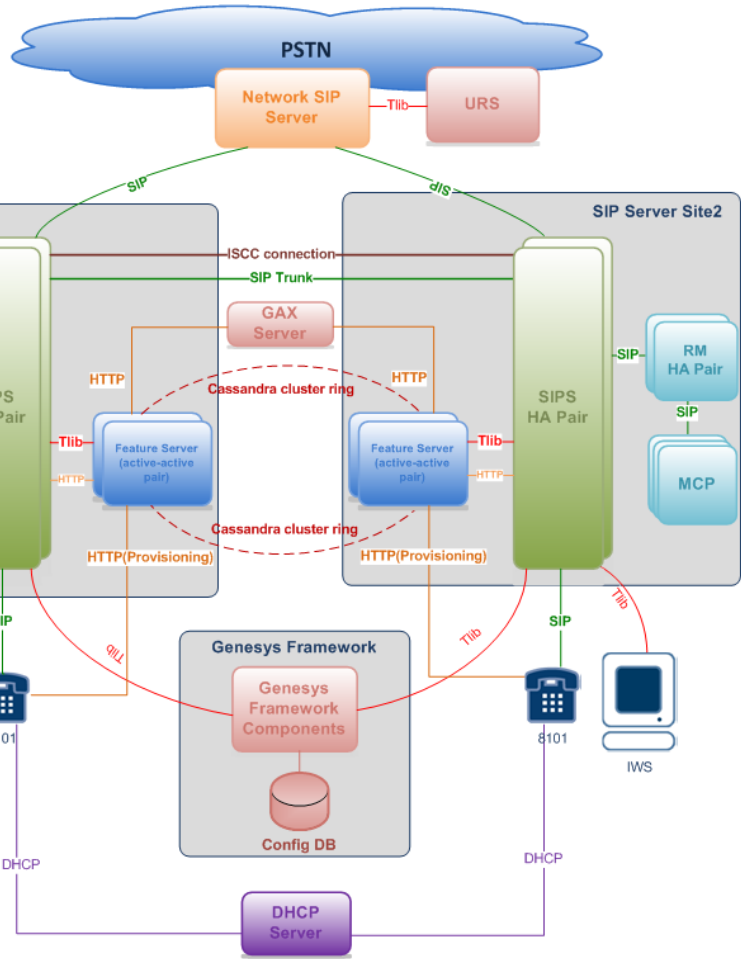



Figure 16- Multi-Site SIP Feature Server High Availability

This diagram shows the use of multiple instances of SIP Feature Server between sites. Each Feature Server utilizes a shared Cassandra cluster, allowing for full replication of data between them. This provides active-active availability between the feature servers. Feature configuration between the single-site and multi-site deployments are the same.

It should be noted that Feature Server does **not** support multi-tenant installations.

### 4.4.1.8.3 Business Continuity Support

SIP Feature Server may also be utilized within a Genesys SIP Server Business Continuity deployment. This is shown in the diagram below:

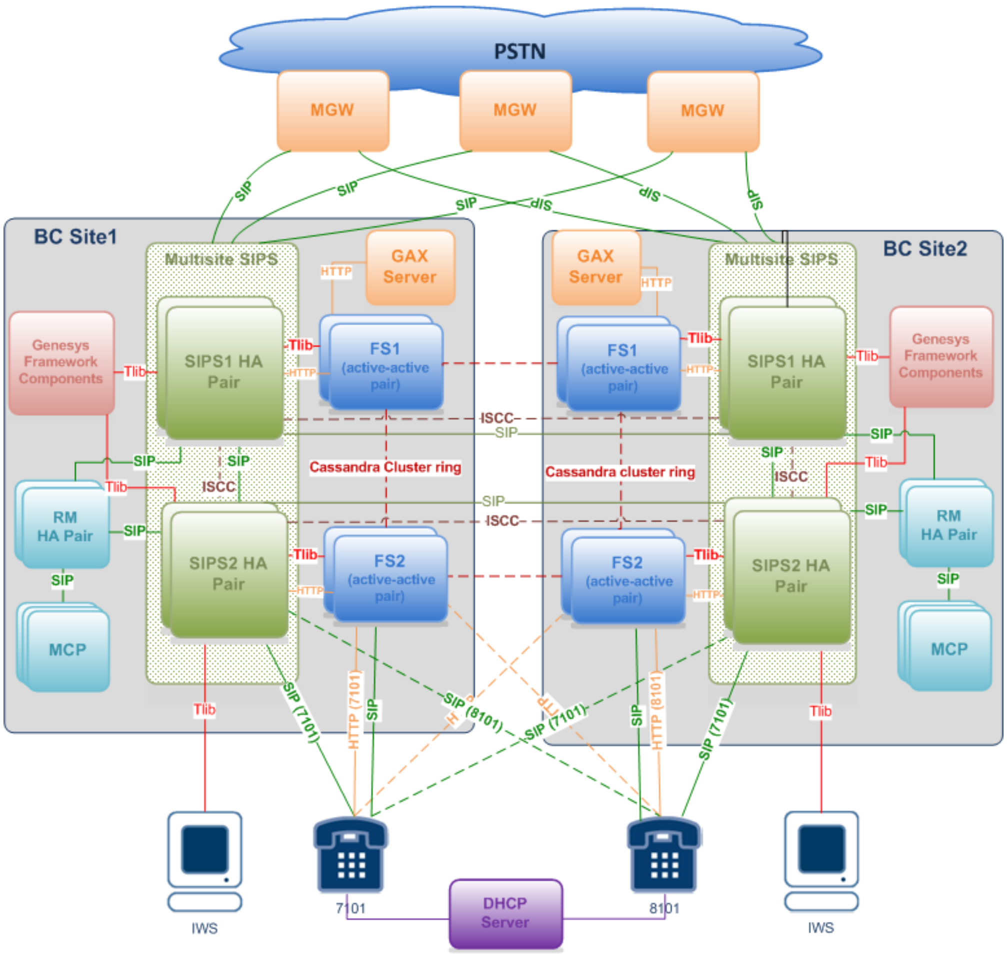


Figure 17- Business Continuity Deployment of SIP Feature Server

Configuration of Feature Server in a SIP Server Business Continuity environment follows the same approach as in the Multi-Site deployment shown previously. Feature Server is associated with the site and each site acts as the backup for the other site.

It should be noted that IVR provisioning is not supported in Business Continuity deployments.

## 4.5 Dual Data Center Deployment

Many customers require a highly survivable architecture which support geographic redundancy and will continue to provide service even in the event that a primary site become unavailable. For the SIP Voice Solution Genesys addresses this requirement through SIP Business Continuity.

Genesys Business Continuity requires that the customer have 2 major data center sites so that if one site suffers a catastrophic event, the other site has the resource to provide continued business functionality. The Business Continuity architecture is designed to provide survivability so that either site can support 100% of the projected production traffic. The overall solution is designed as an active/active architecture with centralized configuration, management and reporting. Either site can manage interactions. For some components, there is a defined primary site and an alternative back-up site while other components operate in a clustered model where the load can be arbitrarily distributed across the sites.

Specifically for SIP Server, peers are configured in the 2 sites. Each peer consists of an HA pair of SIP Servers.

SIP phones dual register with the 2 SIP Server Peer addresses so that if one is down the SIP messages can continue flowing to the second SIP Server Peer.

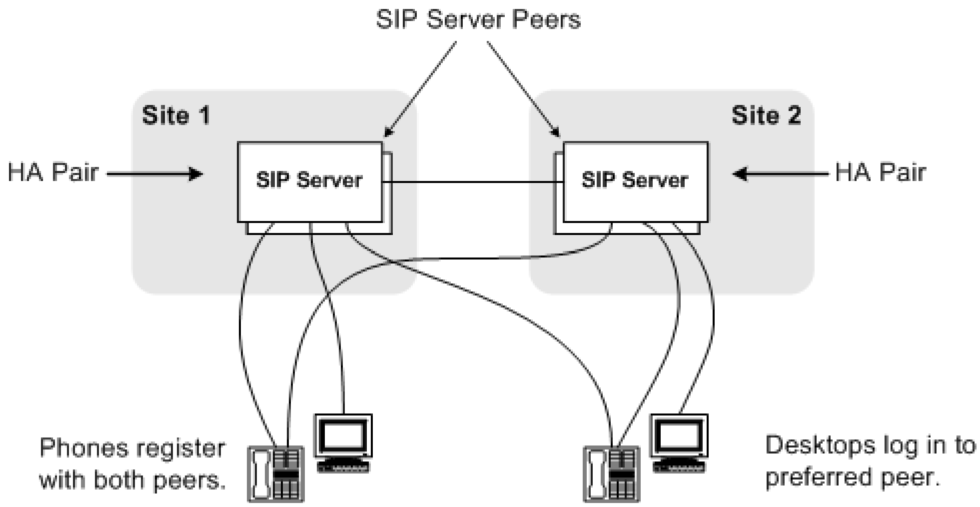



Figure 18 – SIP Business Continuity Deployment

StatServers need to be configured in each site monitoring both SIP Servers as well.

Configuration data must be replicated between sites. Additional details on Configuration replication is provided in the **Common Components Blueprint**.

A high level diagram illustrating SIP Business Continuity is shown below:

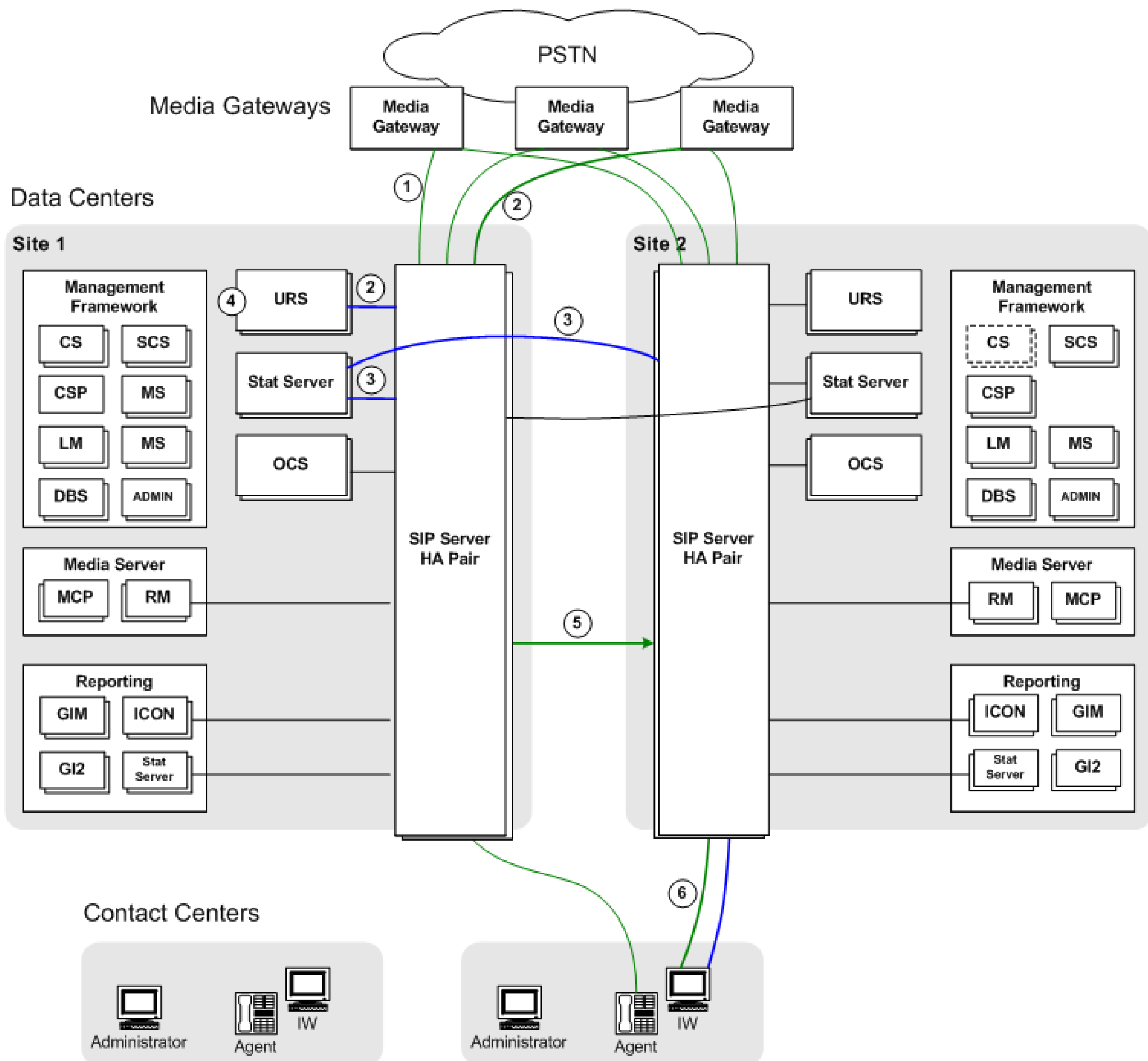



Figure 19 - Genesys Business Continuity Deployment

Business Continuity can handle several failure scenarios. The following diagram depicts a catastrophic failure in Site 1. Media Gateways would send all voice traffic to Site 2. SIP endpoints would accept messages from the Site 2 SIP Server. All necessary configuration information should have already been replicated and the Config Proxy will deliver that information as required to all components in the solution.

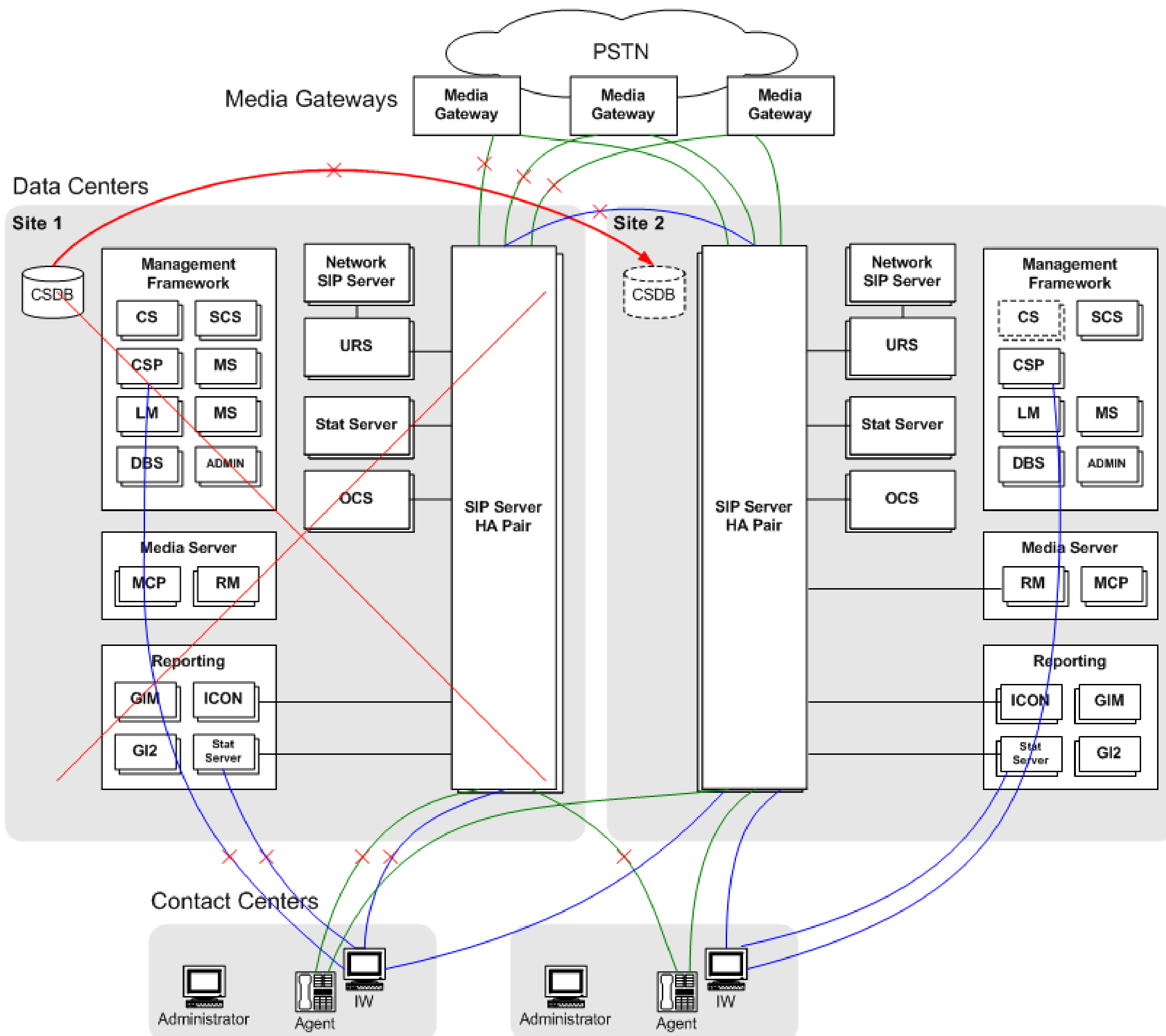



Figure 20 - Business Continuity Failover

For more information on the SIP Business Continuity architecture refer to the SIP BC Architecture documentation. Information on deploying SIP BC can be found in the Deployment Guide for SIP BC. Current limitations for Business Continuity are listed here.

### Virtual Queues

In a dual-data center environment it is important to have Virtual Queues deployed which provide the required levels of high availability and disaster recovery. There are different approaches to deploying Virtual Queues within this architecture and at this time there is not currently a formal recommendation provided by Engineering.

### Desktop Connectivity

Genesys Workspace Desktop Edition (WDE) has been designed to support SIP Business Continuity. The WDE configuration includes connectivity details for both SIP Server peers. If the preferred peer cannot be contacted, then WDE will automatically attempt to establish connectivity with the backup peer and login the agent at the backup peer. The SIP Server instance that the agent is using should be transparent to the agent desktop. Custom desktops can also be created to use the same failover/DR logic as employed by WDE.

**Telephony Connectivity**

In order to provide Business Continuity, customers should work with their carrier to ensure that inbound calls are load balanced across both active sites. This is typically done by establishing trunk groups and a call distribution which spans sites. When a call comes from the carrier it would then be delivered in a round robin fashion across the trunks. In the event of a site failure, all inbound traffic will be directed to the available site. Both sites should be designed and sized to support 100% of the planned telephony traffic.

At each data center, media gateways and/or SBCs should be deployed to support the peak hour call volumes with local high availability. This sizing needs to apply to each data center independently so that the loss of a data center does not reduce the enterprises ability to handle the peak hour production load. The Media Gateways or Session Border Controllers need to be configured to reach both SIP Server Peers so that they can send SIP traffic to the appropriate SIP Server depending on normal and business continuity scenarios. For example, if the call arrives at the SBC at Site A but for some reason the SIP Server HA pair at site A is unavailable then the SBC should direct the traffic across a WAN to the SIP peer (SIP Server HA pair at site B) for call handling. If the media gateway/SBC are co-resident with the SIP Server then this failure scenario is unlikely and a preferred approach may be to automatically busy out the site based upon media gateway/SBC capabilities.

Note that there are specific SIP handling requirements for the Media Gateways and SBCs. Please consult the Supported Media Interface (SMI) guide for Business Continuity support (see http://docs.genesys.com/Special:Repository/g_ref_smi.pdf?id=73c96eb2-c7cb-4839-95e5-0c910861e615 ).

## 4.6 Call Recording

Genesys offers a native call recording solution, Genesys Interaction Recording (GIR) and also supports integrations with various 3rd party recording vendors. The Genesys recording solution uses many of the existing components within the SIP Voice Blueprint. The Genesys call recording solution allows recording to be controlled through configuration settings, triggered dynamically through a routing strategy and controlled via a desktop such as Genesys Workspace Desktop Edition or a custom desktop using the appropriate APIs. ~~and Workspace Web using the appropriate APIs.~~

Genesys call recording performs active replication of the media stream by bridging the media through the Media Control Platform (MCP). **While detailed information is provided in the GIR/GIA Blueprint it is important to understand the impact of call recording on the voice path (RTP stream) to ensure proper network planning in a SIP Voice deployment.**

The following diagram illustrates the RTP streams when Genesys call recording is performed. When recording is performed, the RTP traffic from both the customer and agent are recorded via a Media Server and stored by Genesys Interaction Recording.

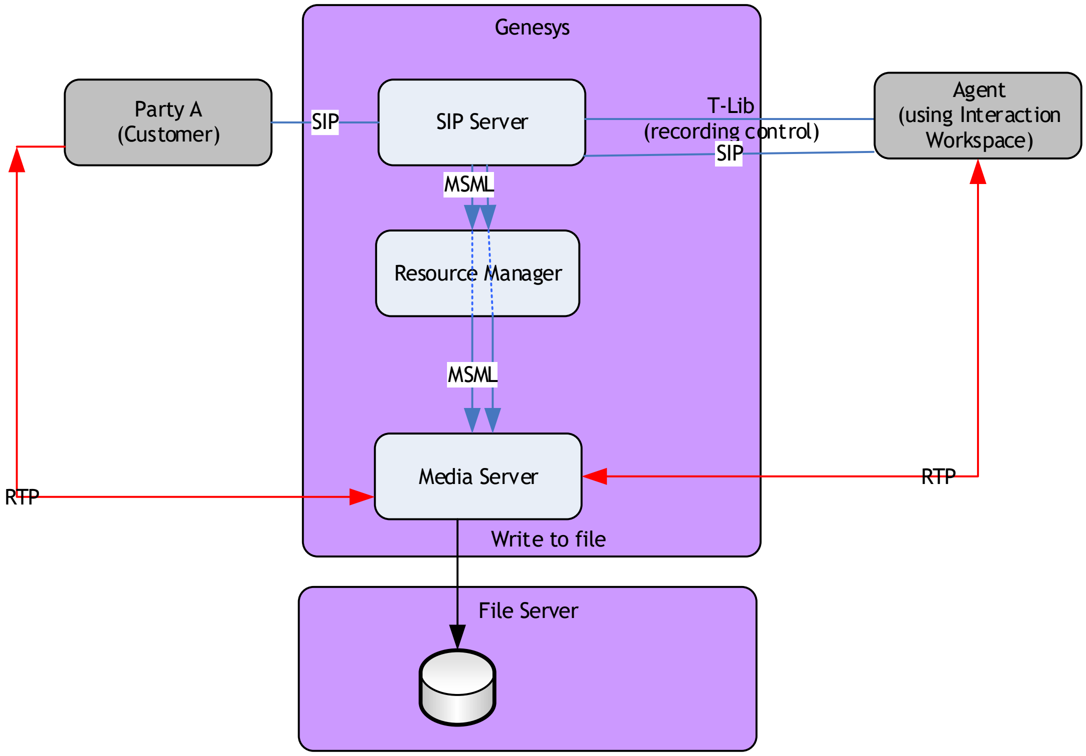



Figure 21 - Genesys Interaction Recording – RTP flow

The file server represented in the diagram is a component which is required as part of the Genesys Interaction Recording solution and detailed in the respective Blueprint.

If the calls ingress at locations different from the data centers where the Genesys software resides then the customer may elect to have call recording MCPs co-located at the ingress point to reduce bandwidth requirements. This architecture could be further extended to a Distributed Multi-Site Deployment with the addition of site level hubs.

## 4.7 Network Overview

The customer's network infrastructure is a key element for consideration when integrating SIP Server into their environment. Networks at each customer will often be different and unique to their own requirements. In most cases the network will already be in place and the solution will need to contend with its idiosyncrasies.

The following diagram does attempt to illustrate some of the typical elements in the network topology. These typical elements and topology will help provide context for the various deployment options described previously.

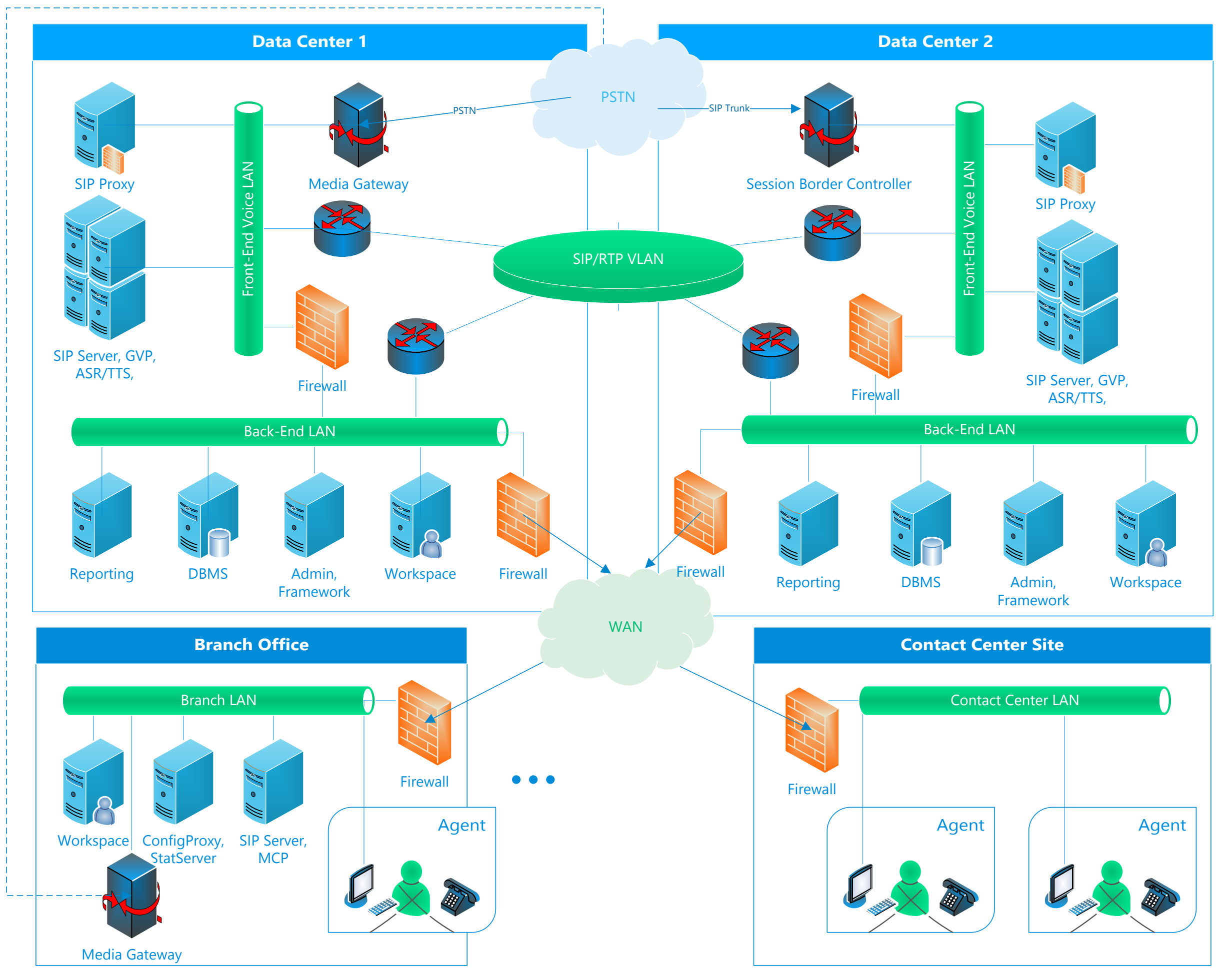



Figure 22 - Generic Network Diagram

Voice communication typically comes via the PSTN or Mobile network. Depending on the carrier, either a Media Gateway is used to convert PSTN to SIP & RTP or a SIP Trunk can supply the SIP & RTP traffic directly. A Session Border Controller is used to protect SIP & RTP traffic from unauthorized or malicious access.

Often the enterprise will have at least two Data Centers (to provide for disaster recovery). The enterprise will also have contact center sites where the agents reside. These Branch Sites are networked through WAN connections to the central Data Centers. Some deployments may have direct PSTN connectivity at the branches while other deployments may only have agents at these Branch Sites.

Local Area Network (LAN) segments will be setup with Firewalls between them to protect various elements.

VLANs are often created on the networks to isolate SIP & RTP traffic from other data traffic. Other mechanisms for isolating voice from data on IP networks is to use QoS to prioritize voice packets or to configure separate IP networks for voice and data traffic.

Several application servers/hosts will be deployed for various functions. Database (RDBMS) servers will need to be accessible for configuration data and reporting.

### 4.7.1 VoIP Quality of Service

Bandwidth, latency, and proper network configuration is critical for ensuring voice quality over IP networks.

There are multiple approaches that network architects can use to ensure that their network is ready for VoIP:

1. Separate and isolated networks
2. VLAN dedicated to SIP & RTP traffic
3. QoS (Quality of Service) settings.

Larger customers may have setup a separate network for voice traffic – in this case, the network is dedicated to voice traffic and should not be impacted by other network activities.

Configuring a VLAN to carry just voice traffic and ensuring that VLAN has an appropriate amount of bandwidth is another voice traffic isolation technique. Note that is the VLAN is still sharing the same physical network as other traffic, but if configured properly, this should not impact voice quality.

Quality of Service works by marking voice traffic packets and then giving them priority over other data packets within the network. This requires configuration of various network equipment to mark and prioritize the packets (e.g. routers). SIP Server and MCP must also be configured with the appropriate level of QoS based on the settings for the rest of the network.

*Genesys offers the Genesys Network Readiness Assessment (GNRA) service which will test the bandwidth of the network and appropriate QoS marking. We highly recommend that GNRA is performed prior to a SIP deployment.*

**VLANs**

There are typically multiple VLANs which are defined. These VLAN's provide segregation on the differing forms of communication types within the overall solution, and are required to ensure a protected and enclosed environment for the reliable, secure and expedient delivery of real-time sensitive communications traffic within the Genesys CX Platform.

The following are examples of different VLANs that may be configured:

- VoIP – Dedicated VLAN for SIP and RTP traffic. Real-time sensitive communications.
- TLib – Dedicated VLAN for Genesys application to application real-time communications (TLib, CfgLib, StatLib, http/https)
- Front-End – Interface for end user contact center access such as Genesys Administrator Extensions, Pulse, Voicemail, Genesys Administrator, Workspace Web Edition, Rules Authoring
- Mgmt – Management VLAN for maintenance activities such as backup, restore, patching updates and antivirus updates
- DMZ – Demilitarized zone for secure customer web browser or mobile http access (Not applicable for the SIP Voice solutions. However this VLAN may exist when Digital or other Genesys solutions are deployed)

**Traffic Metrics**

The following requirements exist and must be met to ensure the correct operation and performance of the Genesys CX Platform. Measurements are one-way.

| Category | Intra-Site | Across Data Centers |
|---|---|---|
| **Latency** | <20ms | <150ms* (End to End) |
| **One-way Jitter** | <2ms | <5ms |
| **Packet Loss** | <0.1% | <0.1% |

* In a multi-Data Center deployment the traffic from the ingress point to the end destination may traverse the data centers therefore end to end one latency in this model should not exceed 150ms. It is important to always consider the additional latency between data centers and to ensure planning is not based upon a 'best case' scenario.

*Note:*

- *The enterprise may want to consider the deployment of the Genesys (AudioCodes) EMS/SEM to provide VoIP network monitoring if they do not already have an existing VoIP monitoring solution in place*

**Traffic Marking**

To ensure Quality of Service is applied the traffic must be marked appropriately. The following are examples of DSCP marking based upon the traffic type.

| Traffic Type | Traffic Marking | Traffic Identification |
|---|---|---|
| **RTP** | EF | All VoIP VLAN traffic |
| **SIP** | AF31/CS3 | All VoIP VLAN traffic |
| **Call Control TLib** | AF31/CS3 | Identified server/port traffic |
| **Call Control http** | AF31/CS3 | Identified server/port traffic |
| **Agent Desktop/Web Services http** | AF21 | Identified server/port traffic |
| **CfgLib, MgmtLib** | AF11 | Identified server/port traffic |
| **DBLib** | AF11 | Identified server/port traffic |

## 4.8 Database Configuration

Databases are a customer provided component of the solution and must be provided as part of the overall solution. Details on database considerations are provided in the **Common Components Blueprint**.

Note: If Genesys Voice Platform Reporting Server is deployed it will have additional database requirements. The database used for the GVP Reporting Server should align with the database decisions already made as part of the **Common Components Blueprint**.

## 4.9 SIP Feature Server

Genesys SIP Feature Server is an optional (though included) component that provides the following functionality in a Genesys SIP Server environment:

- **Voicemail** – Genesys Feature Server is a core component of Genesys SIP Voicemail. Feature Server provides the core application server and data storage for SIP Voicemail. SIP Voicemail also makes use of the Media Control Platform (MCP) and Resource Manager (RM) components of Genesys Voice Portal (GVP) in order to execute the voicemail application and provide its media services. Genesys SIP Voicemail functionality requires purchase of Genesys voice mailbox licenses.
- **Device Management** – Genesys Feature Server is also utilized to provide endpoint provisioning / device management for Genesys supported SIP phones from AudioCodes, Genesys, Polycom, and Yealink. Device Management may also utilize the MCP and RM components from GVP in order to provide IVR provisioning of the phones. The capability to utilize SIP Feature Server for device management / provisioning is included with SIP Server.
- **Dial Plan** – While dial plans can be directly configured within SIP Server itself, for larger environments where multiple SIP Server instances are utilized, SIP Feature Server can be used to centralize those dial plans. The capability to utilize SIP Feature Server for dial plan management is included with SIP Server.

In all three use cases above, Genesys Administrator Extension (GAX) provides the user interface for voicemail, device management, and dial plan. SIP Feature Server provides GAX plugins to enable each functionality as required.

### 4.9.1 Overall Architecture

The diagram below shows the architecture of SIP Feature Server when used with a single Genesys SIP Server HA pair:

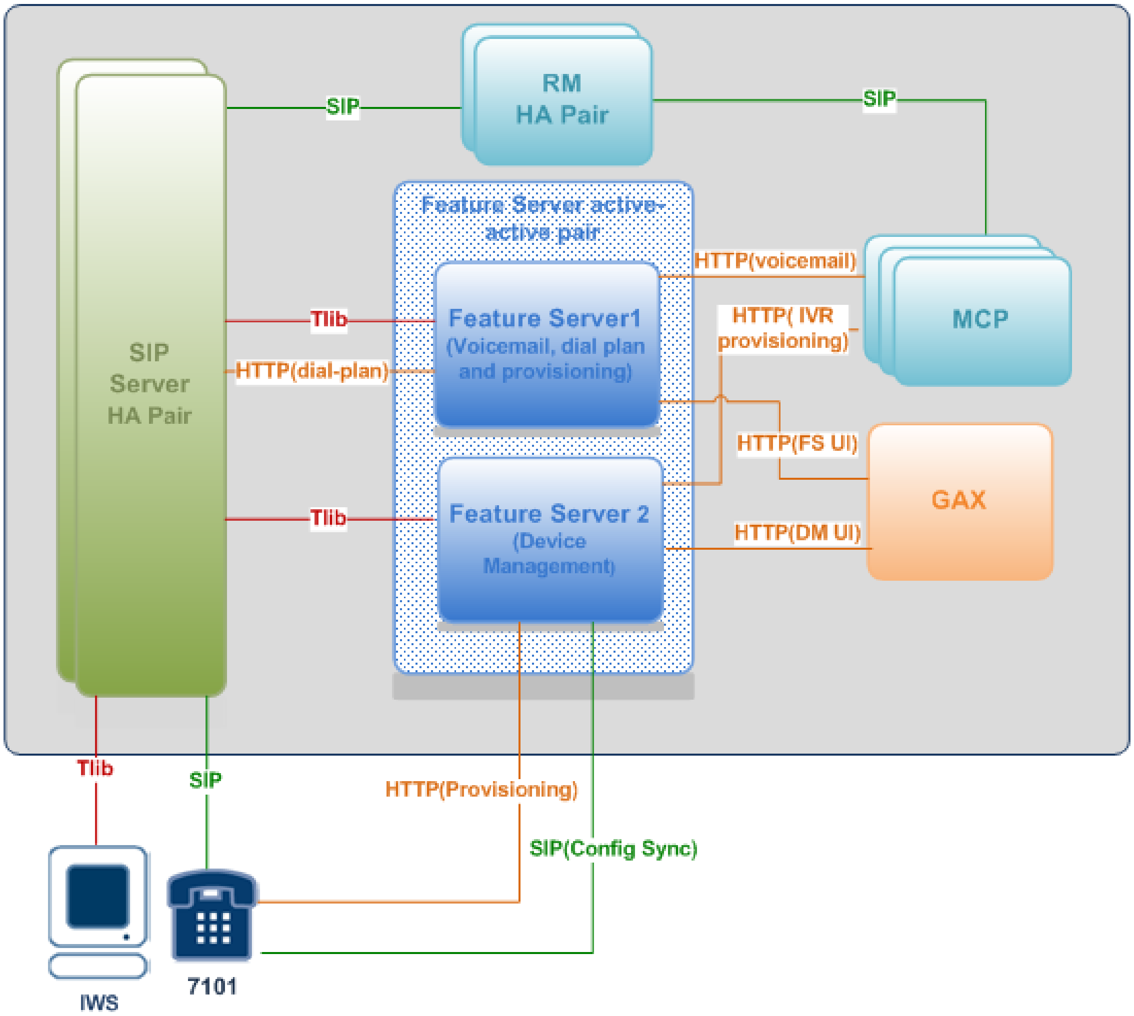



Figure 23- Genesys SIP Feature Server Architecture

A typical high availability deployment requires at least 2 SIP Feature Servers. Typically, these are configured as follows:

- One Feature Server primarily dedicated to handling voicemail, user provisioning, and dial plan functionality
- One Feature Server primarily dedicated to handling Device Management (phone provisioning)

In the event one Feature Server goes down, the other will take over its duties. It should be noted that it is not required to deploy Feature Server in all roles (ie: voicemail, dial plan, and device management) if not desired.

Further details on high availability with SIP Feature Server are provided in section

### 4.9.2 Dial Plan

In cases where Feature Server is to be utilized to provide dial plan for SIP Server, SIP Server submits an HTTP request to Feature Server to retrieve this dial plan information, when needed, for each call. Feature Server stores this information in the Cassandra cluster.

Administrators may modify the dial plan using the Genesys Administrator Extension (GAX) plugin for dial plan.

### 4.9.3 Device Management

Genesys SIP Feature Server manages device provisioning within the SIP Voice Solution. In addition to device management, the SIP Feature Server also handles voicemail services, dial-plans, class of service and monitoring functionalities for the SIP Server.

The Genesys device management solution provides the ability to automatically configure, deploy, and manage large numbers of endpoints remotely in an enterprise solution or contact center solution. It provides the following functionalities:

- Making it as seamless as possible for a new device to be connected to SIP Server, allowing for a plug-and-play type of deployment in an enterprise/contact center environment.
- Bulk provisioning of IP Phones/SIP endpoints which is very useful for large scale deployments where numerous extensions are deployed
- Allowing for remote management of devices already connected to the switch, including update of configuration and firmware upgrade.
- Supports multiple vendors

The Feature Server integrates with the Genesys Administrator Extensions (GAX), using GAX to provide the administration user interface.

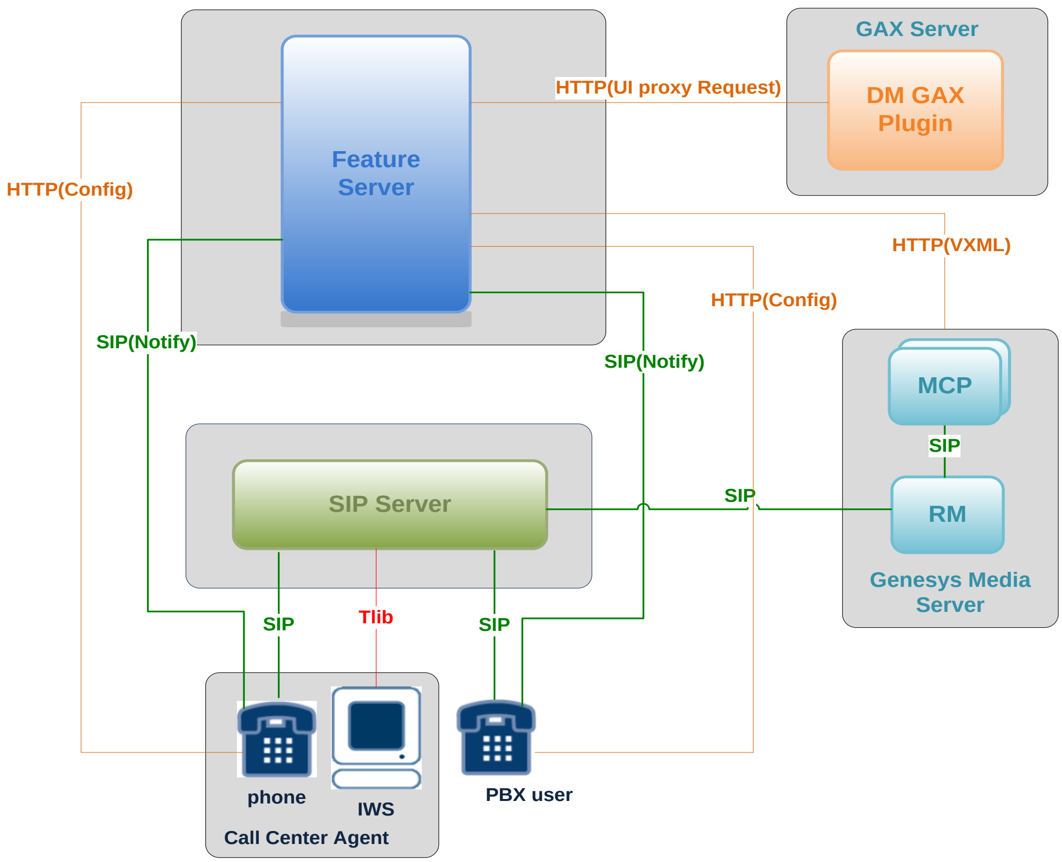



Figure 24- Device Management Architecture

The diagram above shows a high level overview of connectivity between the components when SIP Feature Server is used for Device Management.

The following should be noted in this diagram:

- **IVR Provisioning** - Genesys Media Server (MCP and RM components) are utilized in order to provide for IVR based provisioning. IVR Provisioning allows a user to plug in a brand new phone and provision the device right from the phone through the IVR by entering its extension number and password. Once this is done, Genesys Device Management in SIP Feature Server will create a profile for the device and reboot the phone, allowing for the phone to be utilized without any direct configuration by the administrator (other than initially configuring an extension profile). This will cause the phone's MAC address to be automatically associated with that extension.

- **Remote Reboot/Configuration Update** - Feature Server can send SIP NOTIFY messages to supported phones in order to command them to reboot or update their firmware and configuration. Using the Device Management plugin for Genesys Administrator Extension (GAX), an administrator can reboot or cause a configuration update for a single phone, or a large number of phones. Feature Server also can automatically ensure that devices are updated in stages so as not to overwhelm the network.

- **Phone Configuration and Firmware** – Phone configuration and firmware is stored within the Cassandra cluster.

### 4.9.4 Voicemail

Genesys SIP Voicemail is based on the overall Feature Server architecture. The high level architecture is shown below:

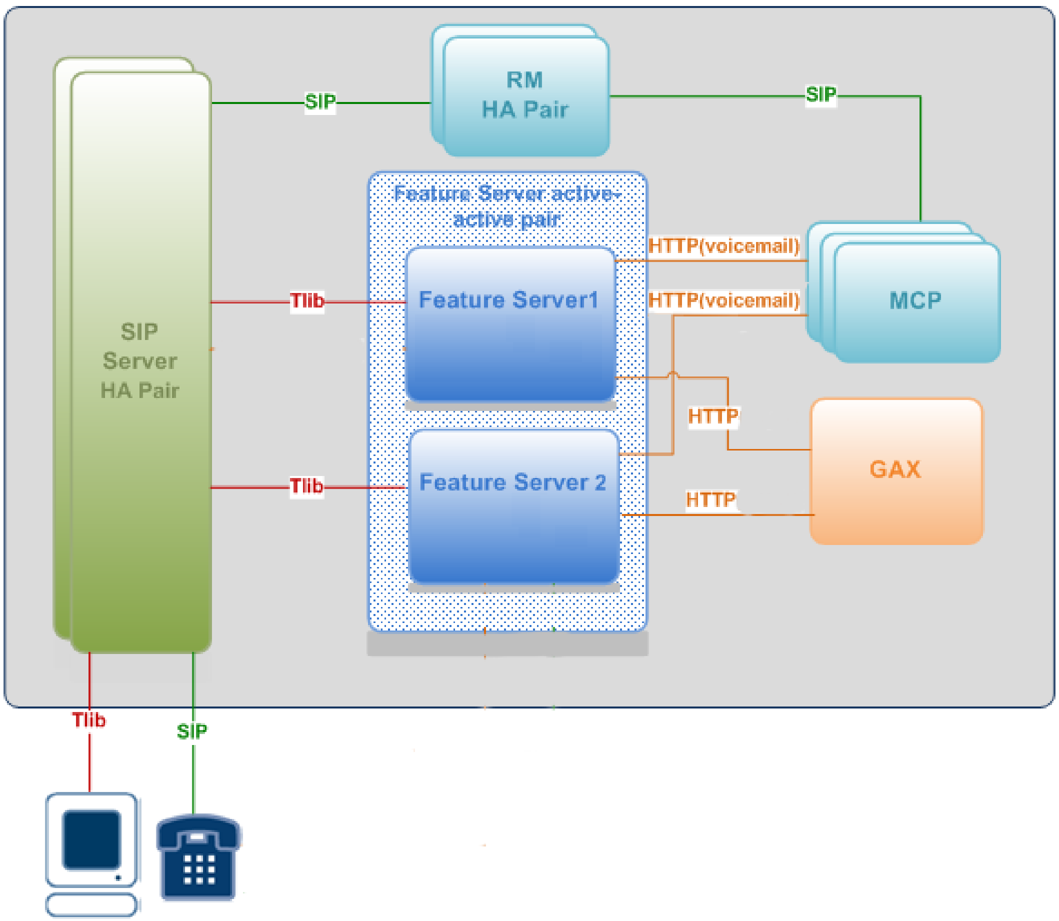



Figure 25- SIP Voicemail Architecture

SIP Voicemail makes use of Genesys SIP Feature Server. While the Cassandra cluster is not shown in the diagram, Cassandra is used as the storage for both the voicemail configuration as well as for storage of voicemail messages themselves.

SIP Voicemail makes use of components of Genesys Voice Portal (GVP) including:

- **Media Control Platform (MCP)** – which is used to provide media streaming of voicemail messages and prompts, as well as for recording of voicemail messages. In addition, MCP also executes the VXML voicemail application.
  The VXML application provides
- **Resource Manager (RM)** – provides load balancing and high availability in front of multiple MCPs.
- **Feature Server** – Provides the following functions:
  - Includes the VoiceXML application server to provide the voicemail application, as well as retrieves the configuration for the voicemail system and actual voicemails from Cassandra storage.
  - Provides the webserver interface allowing a user to retrieve his or her voice messages from within a web browser, as well as make changes to user based voicemail settings.
  - Feature Server provides SIP Server (via SIP notifications – not shown on this diagram) with information regarding the number of messages in each mailbox. SIP Server will send this information to the respective SIP endpoints via SIP NOTIFYs (MWI – Message Waiting Indicator) so that the endpoint may flash a light telling the user of new voicemails, as well as showing the number of new and old messages on the phone display. SIP Server also provides this information via TLib to Genesys desktop applications such as Genesys Workspace.
- **GAX** – provides the user interface to allow for configuration and management of the voicemail solution.

# 5 Interaction View

## 5.1 Call Flows

The following section documents the typical interactions between components in the SIP Telephony Solution. SIP messages are the main focus of this section as it can be the source of issues within a SIP/VoIP network implementation.

The call flows have been simplified – certain messages and notifications have been removed for clarity.

The other main purpose for this section is to document the typical call flows that will be used to determine the sizing of the solution components.

These typical call flows are:

- Agent/Phone Registration
- Non-Agent calling
- Customer call – qualification phase with park
- Customer call – routed to agent
- Hold & Retrieve
- Conferencing
- Transfer
- Voicemail
- Outbound Contact
- Call Recording

### 5.1.1 Agent/Phone Registration

The following figure depicts when a phone registers with SIP Server.

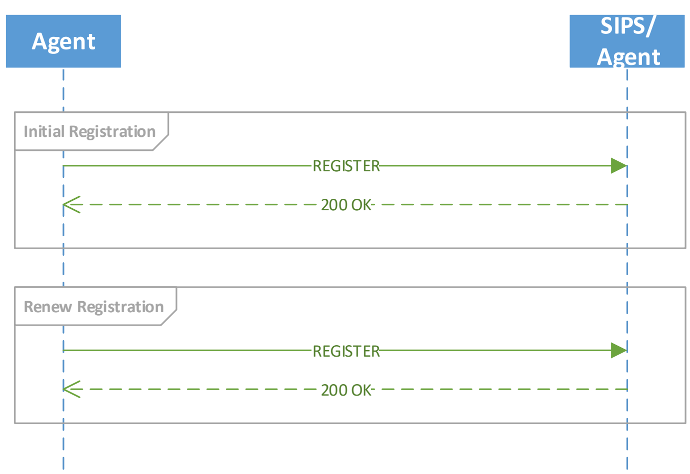



Figure 26 - Agent/Phone Registration Call Flow

Note that the phone will need to renew its registration before its previous registration times out. This is typically around 90 seconds. The phones or SIP clients can be configured with this registration refresh time.

### 5.1.2 Non-Agent calling

This section covers some of the typical call flows for a non-agent user. These may be applicable to agents if they received directed calls (as opposed to Genesys routed calls).

The first diagram describes a standard directed call. The caller can be calling from within the enterprise or externally via an SBC or Gateway. Both a successful call is shown and an abandoned call (where the caller hangs up before the user answers the call).

As the initial `INVITE` message reaches SIP Server, SIP Server requests the dial plan from the Feature Server so that it can determine which user/device to send the request to.

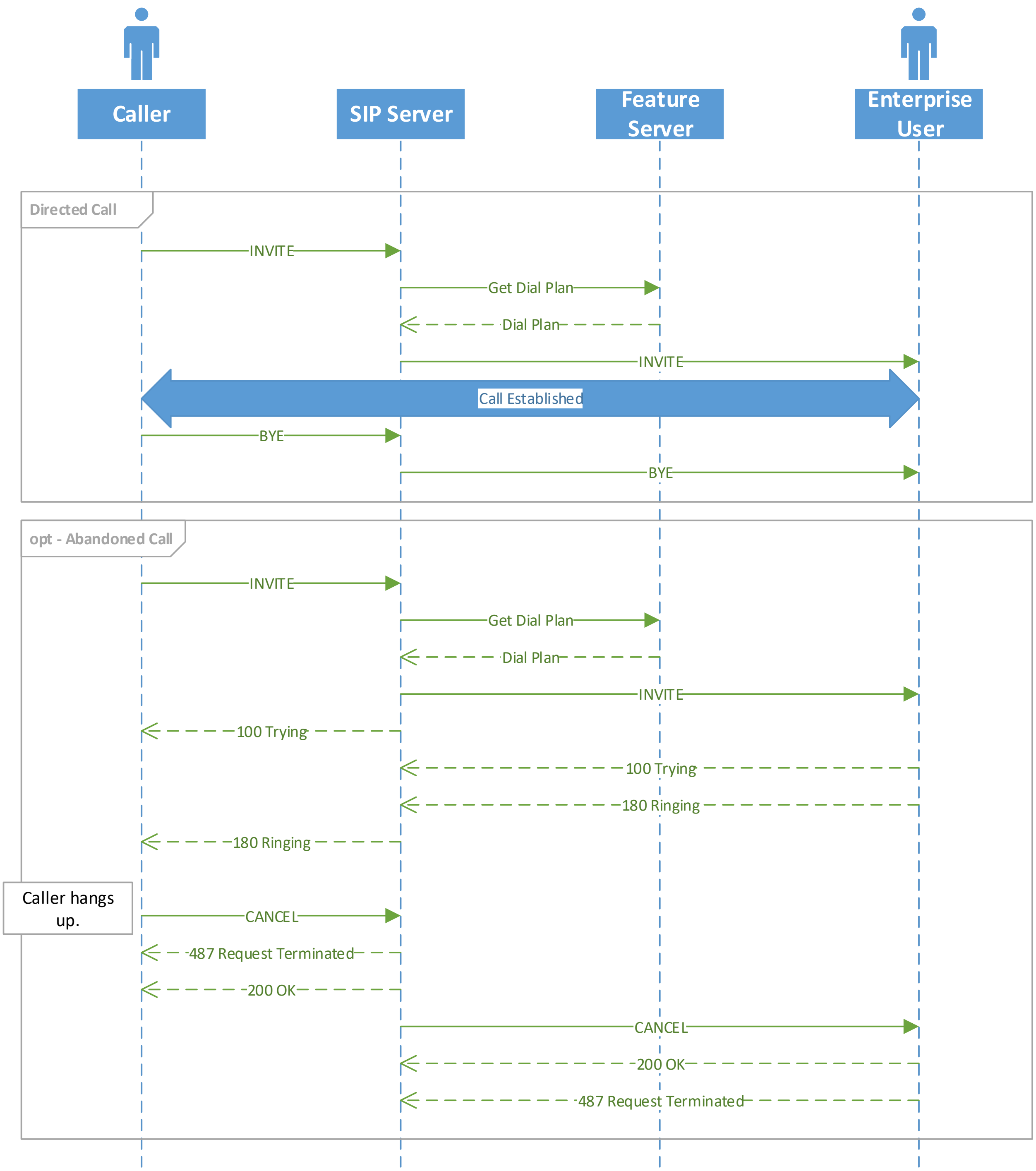



Figure 27 - Non-Agent Call Flows

Note that in the abandoned call case, the user hangs up before the call can be transferred to a voicemail system (as shown later in this document).

The next diagram shows what happens if the Enterprise user has their phone call forwarded to another user's phone (for coverage while they are out).

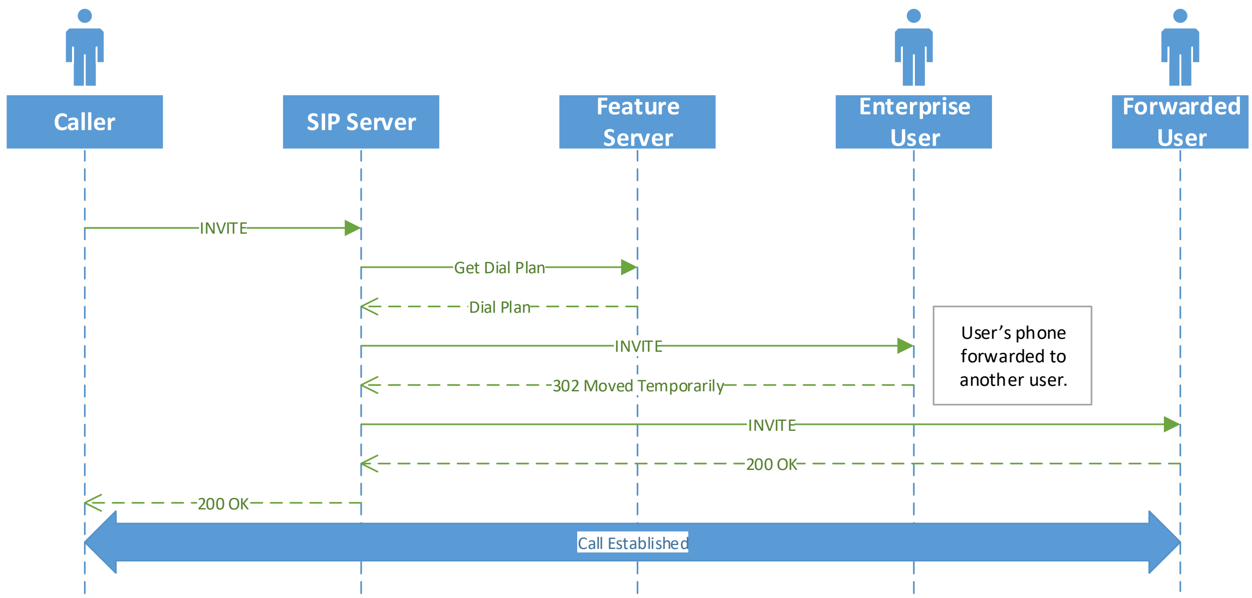



Figure 28 - Call Forwarded

### 5.1.3 Customer call – qualification phase with park

The following diagram illustrates using SIP Server and Media Server to handle qualification and parking of a call before it is delivered to an agent. For the qualification stage there are many options to choose from. The initial call qualification may be performed using Media Server (MCP) or GVP (MCP) to provide different levels of functionality to the end caller - DTMF digit collection vs ASR, playing audio vs TTS. MSML & DTMF collection has been chosen for this example. For the sake of simplicity, only the most important messages are shown.

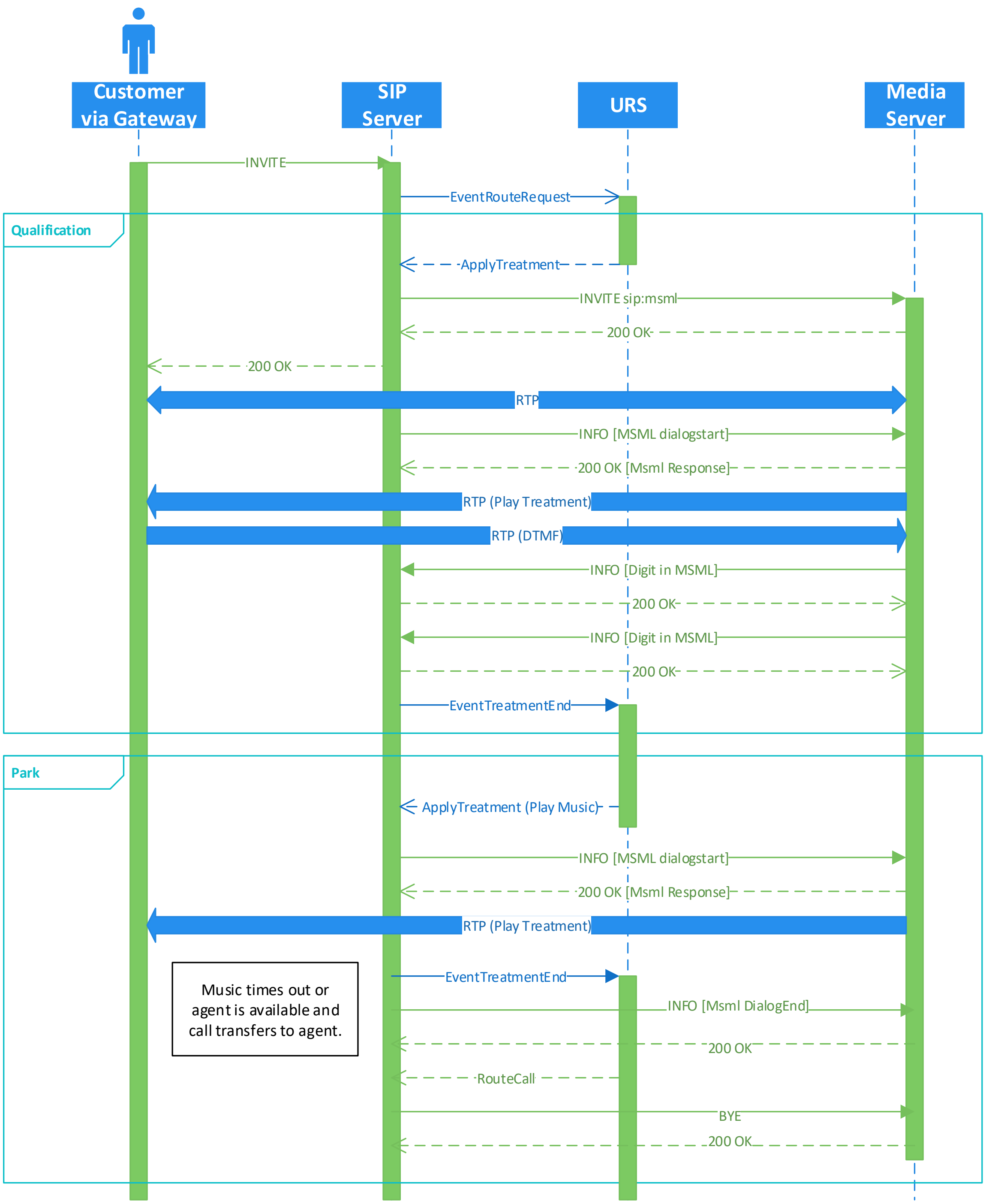



Figure 29 - Qualification & Parking

As noted, MSML is used to handle both the call qualification/triage portion and the parking (or in queue) treatment. The same SIP dialog is reused for both operations.

Once the parking phase is complete and the customer can be routed to an available agent, the Media Server is dropped from the SIP interaction with the BYE message.

### 5.1.4 Customer call – routed to agent

The following call flow assumes that a customer has already been parked as per the prior call flow, and depicts the customer being directed to an agent (presumably after an IVR qualification and parking).

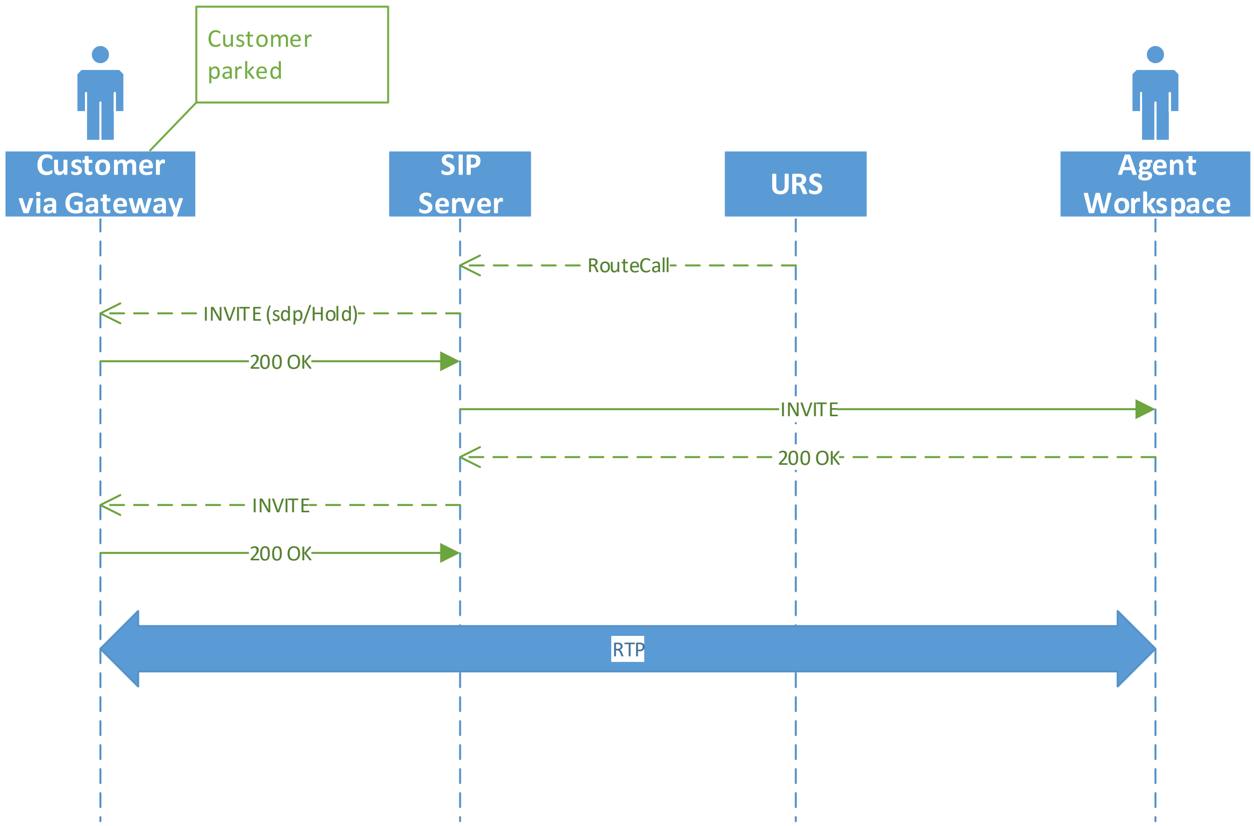



Figure 30 - Route Call to Agent

A few notes on this call flow:

- Moving the call to the agent uses a re-INVITE. To do this, SIP Server must first send an INVITE with an “On-Hold” SDP so that a dialog can be setup with the targeted agent.
- A REFER can also be configured depending on the capabilities of the SBC/Gateway the customer is calling through. This may be preferred in multi-site deployments where the SIP Server instance handling qualification and parking is separate from the instance that the agent has registered to.
- If the agent does not answer the call then the customer will likely be put back into parking/on-hold.

### 5.1.5 Hold & Retrieve

There are times when an agent must put a customer on hold to check something or a non-agent must put a colleague on hold. The following diagram depicts the SIP messaging to put someone on hold and then retrieve that call.

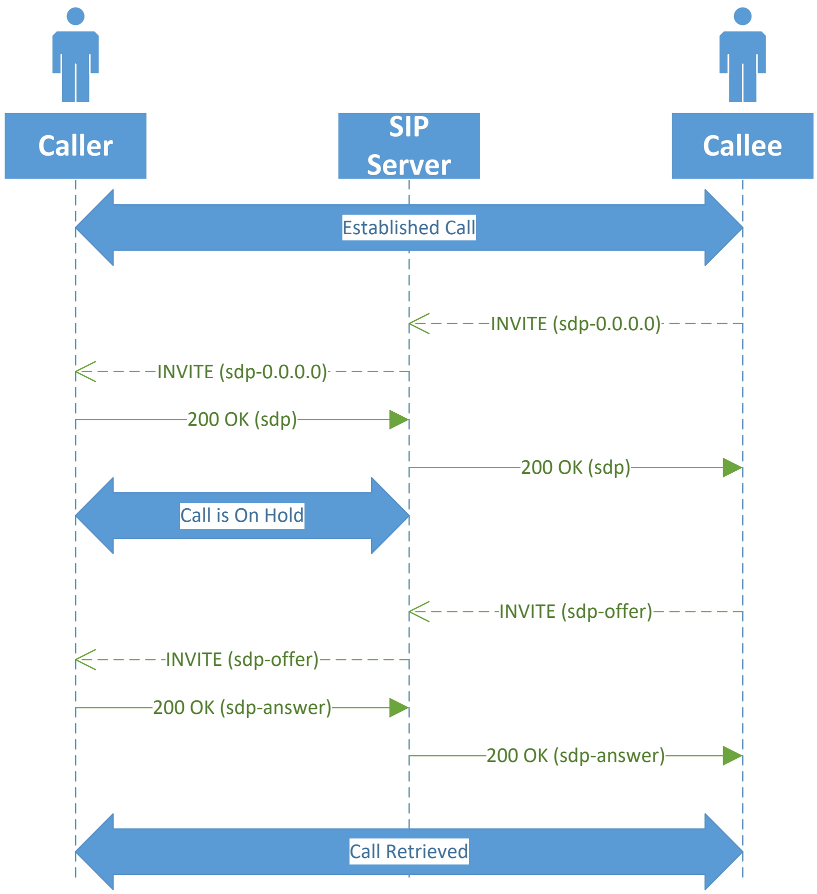



Figure 31 - Hold & Retrieve Call Flow

To put the call on hold, the Caller may be re-Invited with the appropriate settings for the `sendonly` & `recvonly` SDP attributes or with the SDP set to 0.0.0.0. The older method of setting an IP address of `0.0.0.0` in the connection field ("c=") within the SIP message is shown in the diagram above.

Note that the SIP Server configuration parameter `sip-hold-rfc3264` controls which method is used.

To use Music On Hold for the held caller, the initial steps of holding the call are required, then the caller needs to be re-Invited to a Media Server (similar to the Parking call flow in section 5.1.2).

### 5.1.6 Conferencing

There are two approaches for providing conferencing services in a SIP Voice deployment. The typical approach within a contact center deployment is to move the conference participants to a central MCU (media control unit) – Media Server – and mix the audio there. The second approach which is appropriate for enterprise users (non-contact center agents) is to use the capabilities of the SIP phone and mix the audio locally.

The use case depicted in the call flow is an agent on a call with a customer and conferencing in a second agent. The SIP flow will work as well for non-agents or internal conference calling.

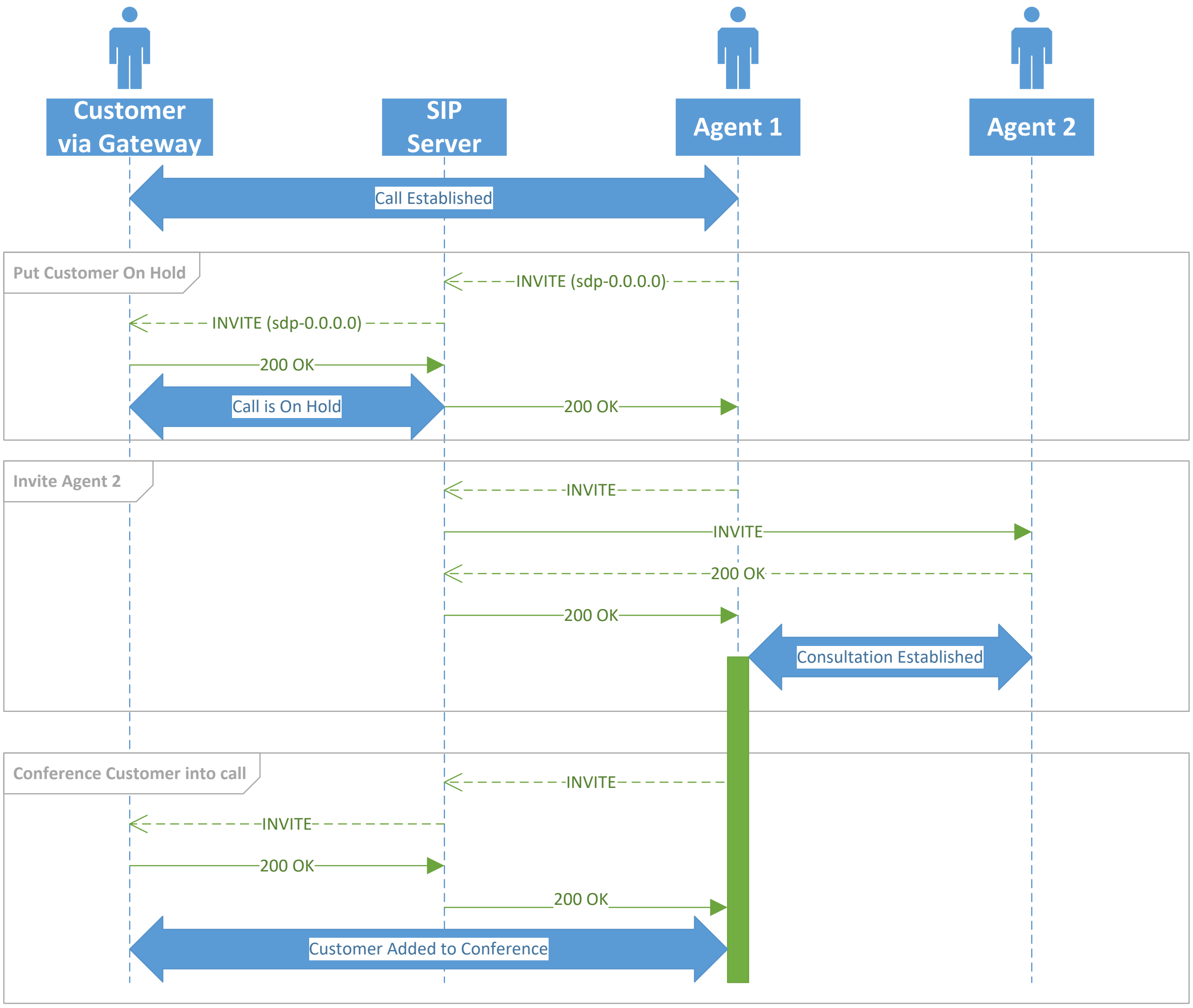



Figure 32 - Conferencing with Local Mixing

For a conference using Genesys Media Server (MCP), the initial phase is similar – the customer (in this use case) is put on hold and a call is established with the other agent. Now all callers are re-invited to the Media Server.

One interesting note – SIP Server sends an `INVITE` without SDP in order to get the Media Server to send its `SDP-Offer`. That `SDP-Offer` is then sent to the caller in the re-`INVITE` so that it can negotiate the proper codec for the conference call.

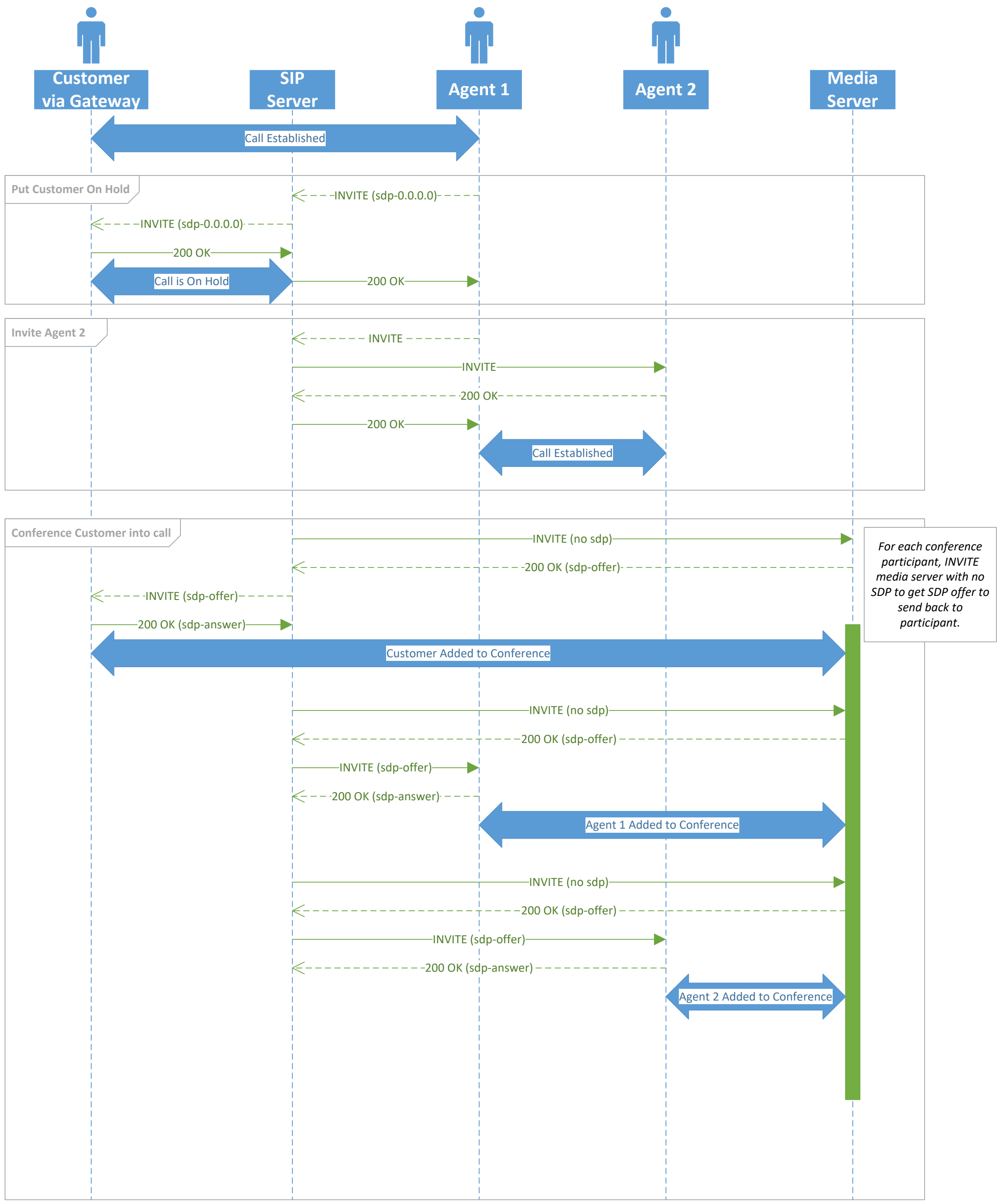



Figure 33 - Conferencing with Central Mixing

### 5.1.7 Transfer

There are a variety of call transferring scenarios and behaviors. The two most commonly supported with SIP Server are the single-step and the consult transfer.

The Single-Step Transfer involves an agent (or non-Agent) transferring the call directly to another phone. As the target phone answers, the transferor is dropped from the call. The following diagram depicts the single-step transfer.

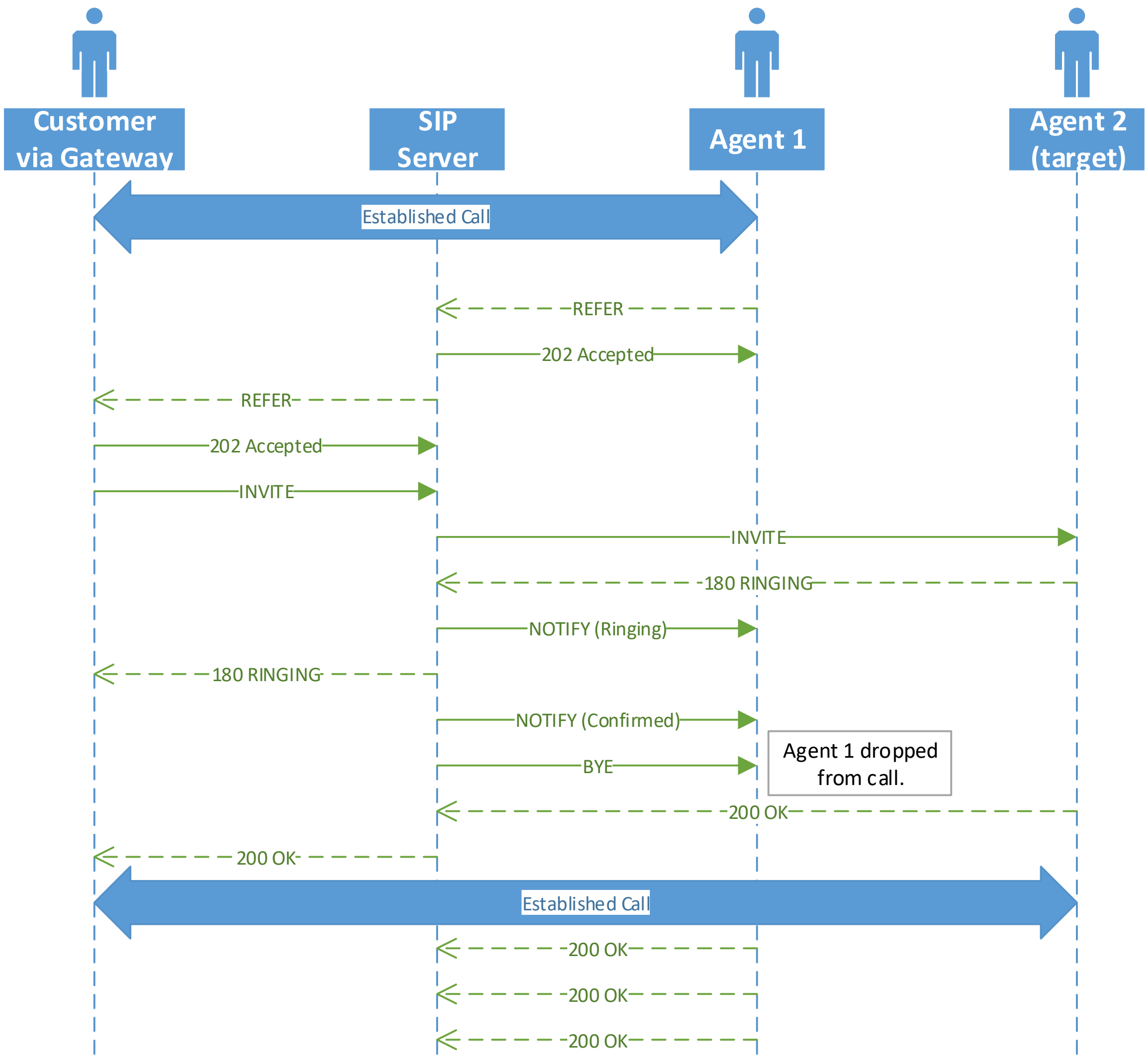



Figure 34 - Single Step Transfer

The Consult Transfer involves the agent putting the original caller on hold, initiating a call to the transfer target (another Agent). They can presumably talk before completing the transfer – at which point the agent tells SIP Server to put the original caller and the transfer target into a call and drop him/her from the call.

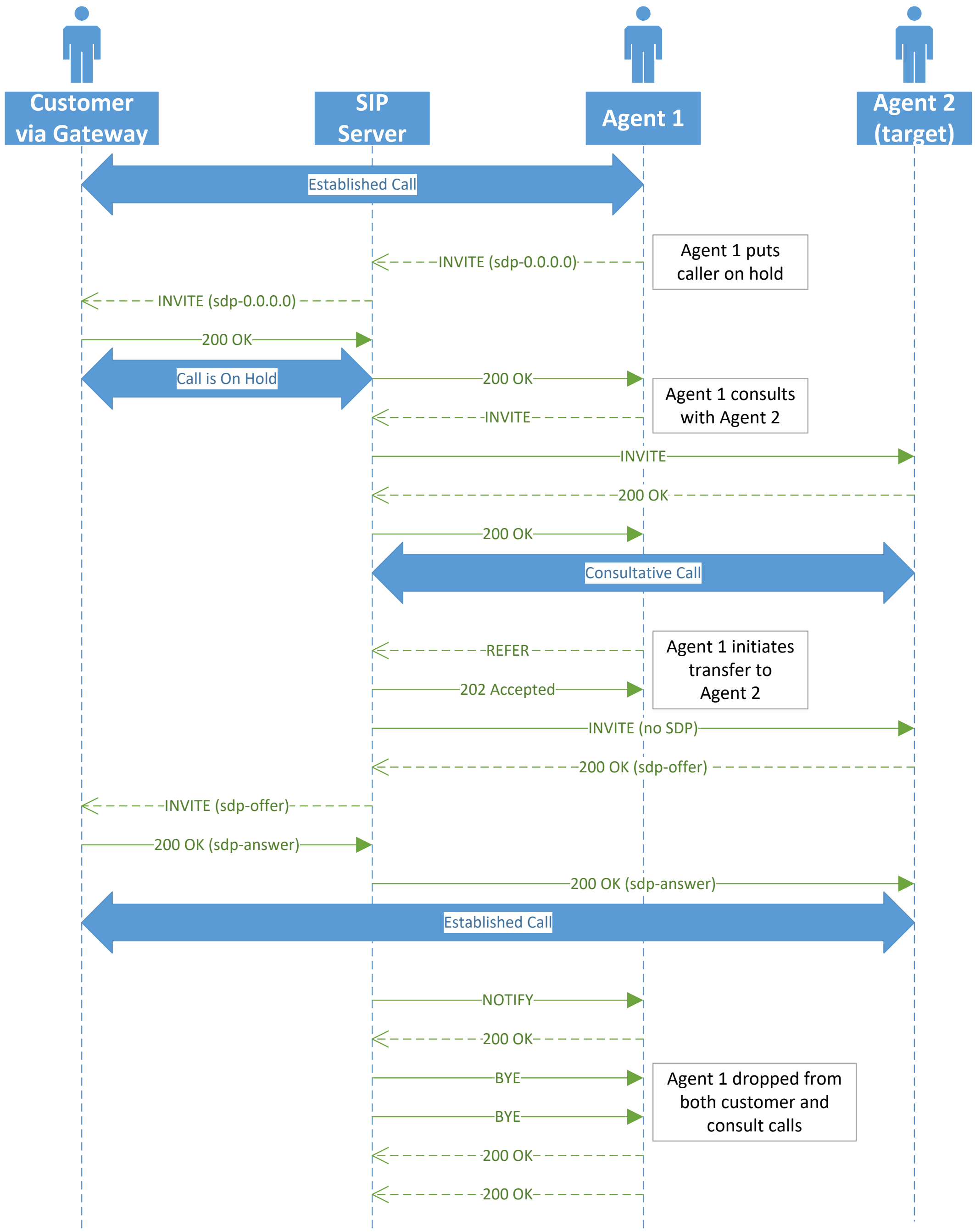



Figure 35 - Consultative Transfer

### 5.1.8 Voicemail

The following call flow depicts a caller calling either an agent or a non-agent. Feature Server provides both dial plan and voicemail management capabilities. It uses GVP (Resource Manager and MCP) to provide the TUI interaction and voice recording capabilities for voicemail.

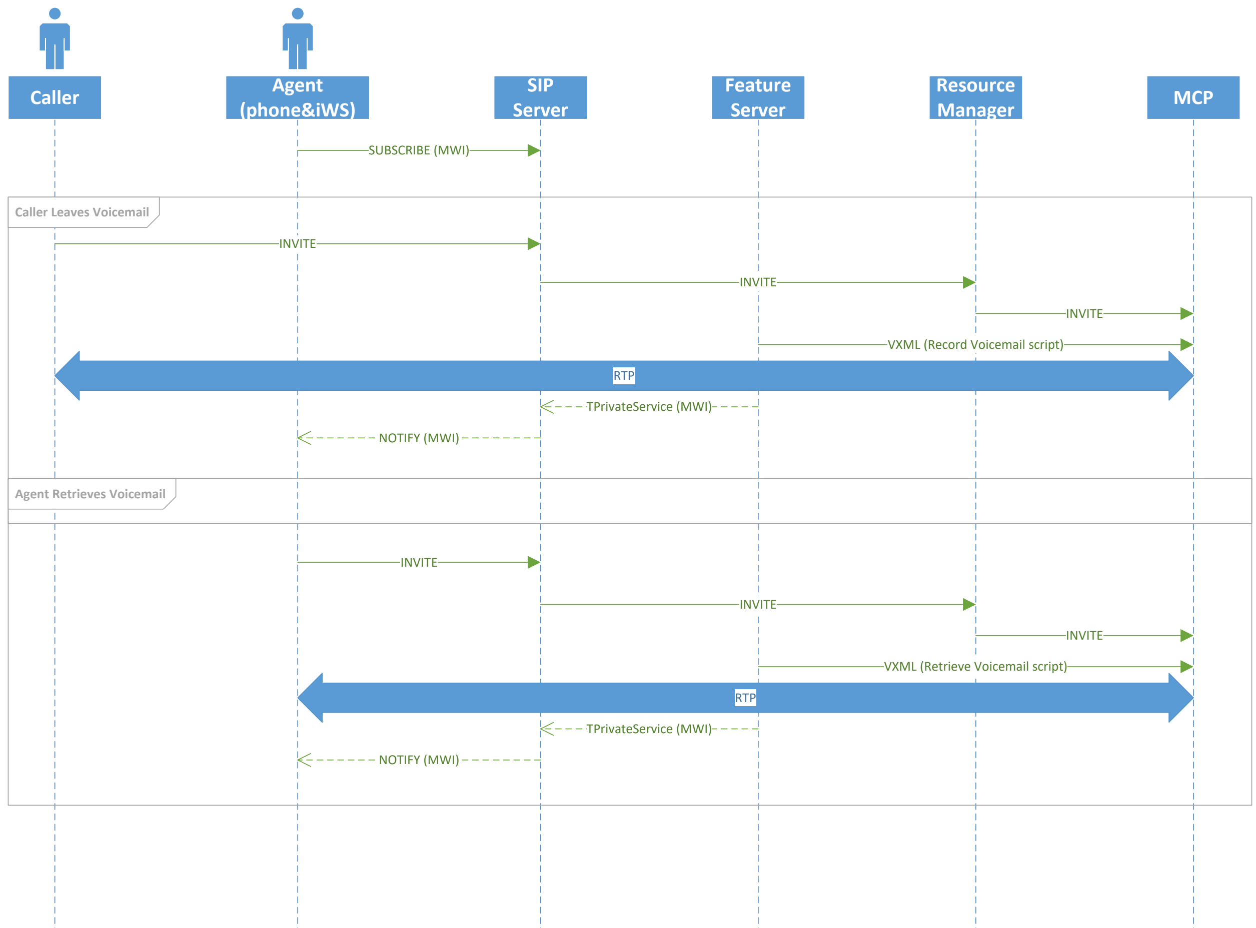



Figure 36 - Voicemail Call Flow

Note that the  user's phone will subscribe to SIP Server for notifications that voicemail is waiting (Message Waiting Indicator/MWI).  Genesys agent desktops, such as Genesys Workspace Desktop, can also receive message notification via TLib.

When the caller calls the target user (Agent in the diagram), SIP Server determines how the call should be handled. If conditions are met that this call should be handled as voicemail, then SIP Server invites Resource Manager/MCP into the call and Feature Server sends a VXML script to the MCP to control the Voicemail TUI interaction with the caller.

The VXML script will eventually record the voicemail from the caller and store it in an appropriate location for the Feature Server to access it.  Since a new message will be waiting – Feature Server informs SIP Server via SIP signaling that MWI should be set to on.  SIP Server then notifies all subscribed clients for this particular voicemail box (either via SIP or TLib messages).

When the agent decides to listen to voicemail, a very similar call flow occurs – the number that the agent dials will map through the dial plan to voicemail and the agent will be connected to the MCP with a VXML script for navigating and retrieving/listening to voicemail.

After the voicemail has been retrieved, the MWI indicator can be reset to off. Feature Server informs SIP Server and SIP Server notifies all subscribers.

### 5.1.9 Outbound Contact

The following diagram depicts the outbound calling scenario driven by OCS which uses Genesys Media Server (MCP) for Call Progress Detection (CPD) and IVR treatment.

When running Outbound in Active Switching Matrix (ASM) mode the Agent is first engaged and connected to the media server – essentially put on hold waiting for a successful customer transfer.

Genesys Media Server (MCP) is then prepared for CPD using the INVITE and INFO messages. The customer is then contacted through the gateway. At this point Media Server (MCP) determines if the call completes and there is a human answer (instead of a voicemail system). If the call is complete and there is a live answer then the customer is transferred to the agent.

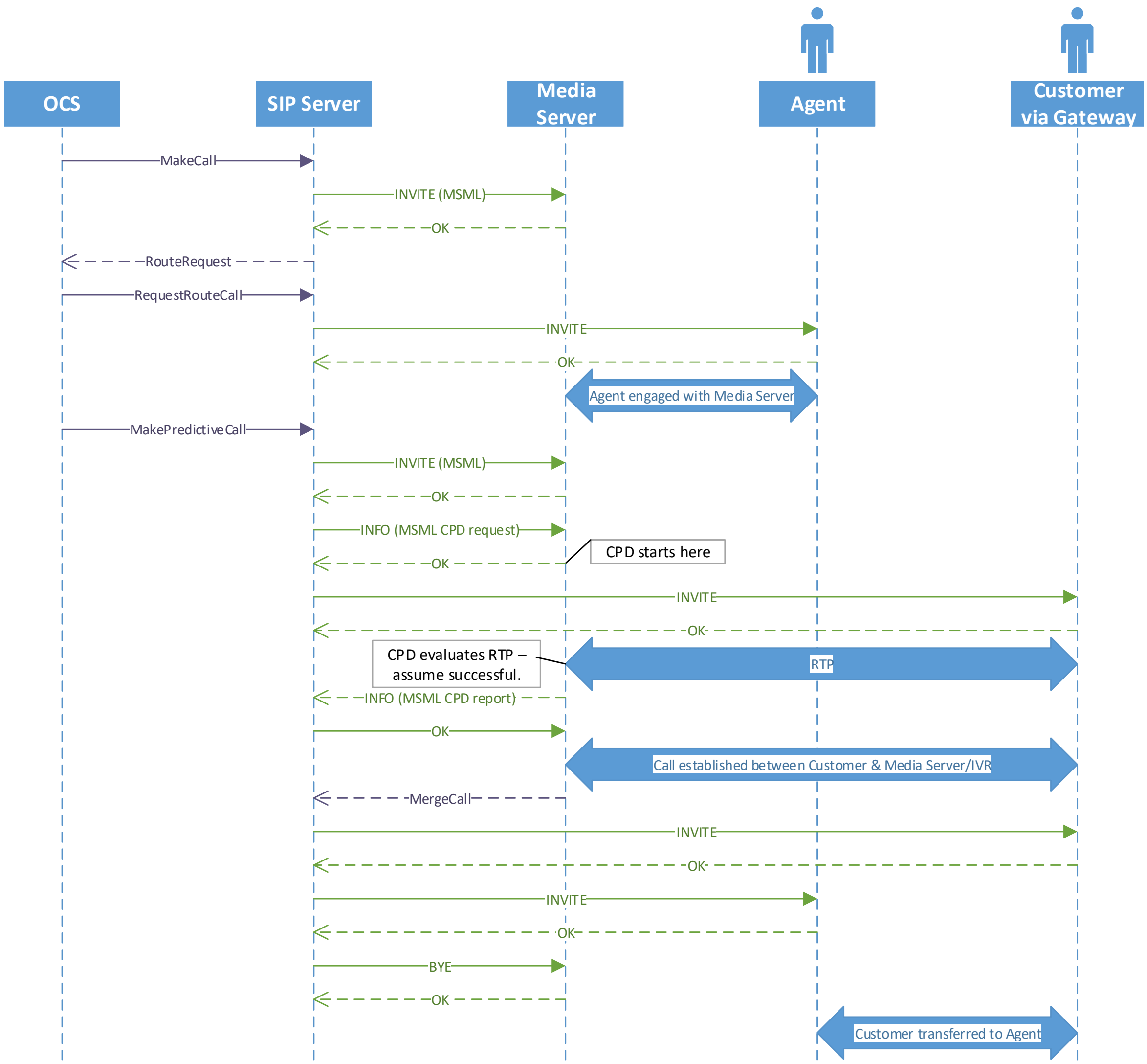



Figure 37 - OCS Call Flow

The CPD can detect issues connecting to the user and once the call is established will perform call progress analysis (CPA) by analyzing the RTP for human answer, voicemail, or fax. If CPD detects an issue, the customer/gateway is disconnected using CANCEL messages (not shown).

Genesys Media Server (MCP) may also provide a treatment if appropriate such as during a predictive campaign if a customer has been connected but no agents are currently available.

### 5.1.10 Call Recording

Call recording is based on the use of the Media Control Platform (MCP) to provide media replication. As an active recording solution, the media stream is bridged through MCP in order to record the call. This is different than a passive recording approach which requires network sniffers and SPAN/mirror ports to process all the packets in the network to determine the audio streams.

The following diagram depicts the agent initiating a recording after a call has been established with the customer.

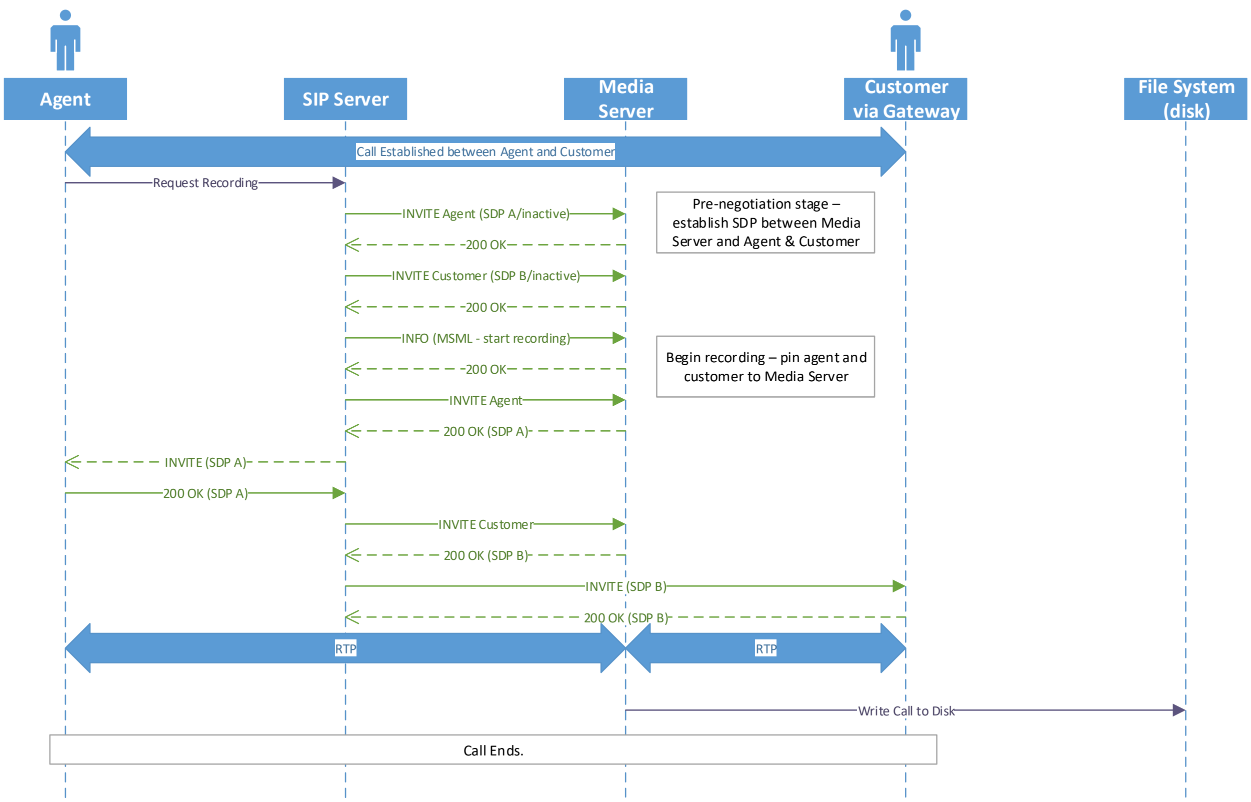



Figure 38 - Call Recording Call Flow

An important aspect of the call recording is ensuring that the Media Server is set to the proper codec/SDP. An initial pre-negotiation stage sets up the media server with the appropriate SDP.

The agent and customer legs of the call are then moved to the media server where their call continues. The media server writes the audio to disk in a streaming fashion until the call ends.

### 5.1.11 Remote Agents

Genesys provides several options for supporting remote agents using either VoIP or PSTN. The remote agent options considered for telephony are often influenced by the agent desktop and environmental requirements it needs to operate remotely.

#### Agent Desktop Support

The agent desktop may either be:

- **Thick client** – Generally requiring VPN connectivity to the enterprise to access corporate applications and the Genesys capabilities (CTI, call control, etc.)
- **Thin client** – Access may be enabled over the internet through HTTPS

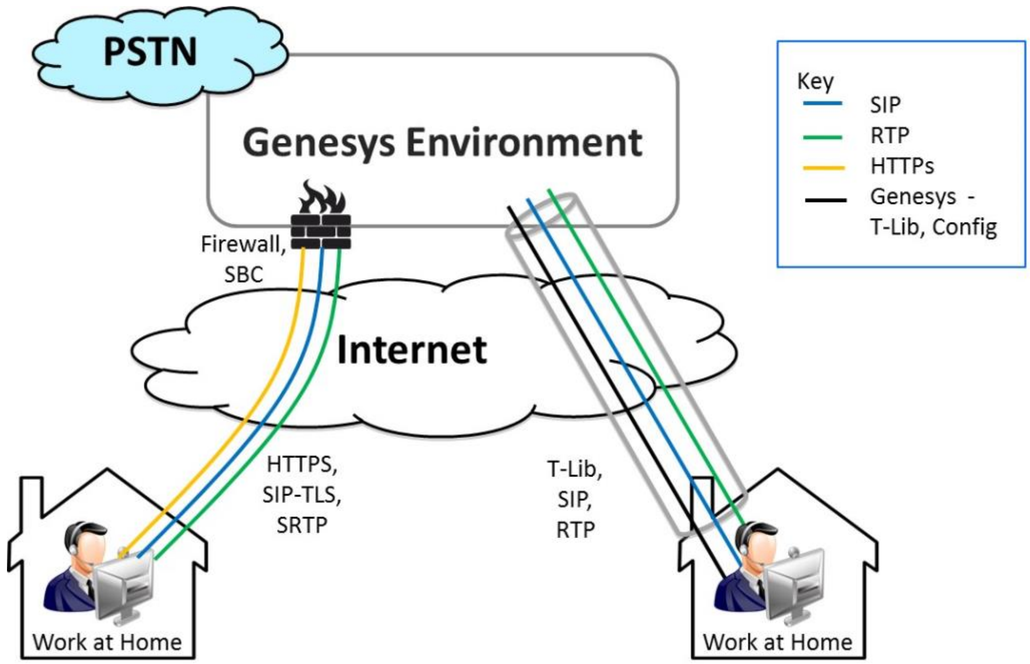
The level of effort of supporting different remote agent telephony models is often driven by the technical requirements for the remote location. Simply put if you already have a VPN in place then using VoIP for remote agents often has a small incremental effort however if remote agents do not need a VPN establish connectivity for VoIP can take considerable effort.

**IP Remote agents**

Support for IP remote agents is provided natively by Genesys. Delivering a SIP call to a remote location requires adequate network connectivity (bandwidth, latency, reliability) between the agent and the contact center with a supported software or hardware based SIP endpoint and method of NAT traversal (software or hardware based device) for SIP and RTP.

- If an agent already has a VPN connection to the enterprise, for example to support their desktop, then they may be able to use standard SIP phones for registration and call delivery through this connection.
- If a VPN connection is not in place then SIP may also be used. The SIP phones can directly register across a standard Internet connect using SIP (TLS and SRTP are used for secure signaling and encrypted audio). To provide secure connections an SSL certificate would be loaded on the endpoints and Secure SIP (SIPS)/SIP over TLS and Secure RTP (SRTP) would be utilized. An SBC such as Genesys E-SBC is recommended both to manage the connectivity to the external environment (Internet) and perform authentication.

In these deployment models the agents may be “remote” but the login, state management and call delivery is identical to agents within the contact center.




**PSTN Remote Agents**

Remote contact center agents may be configured as "SIP Server remote agents". In this model the agents do not use a SIP phone which is registered with SIP Server. Remote agents are accessed by dialing a standard DID/DDI number allowing the agent to use a standard POTS line or even reside behind a key system. Remote contact center agents may be accessed over the PSTN using either a "Dial on Demand" or "Nailed Up" configuration

- In "Dial On Demand" an agent may login through his/her agent desktop application. Once a call is routed to the agent, the contact center (via SIP Server) will place a call directly to the agent's PSTN phone. Once the agent and customer are finished with the call, the PSTN connection will be dropped.
- In "Nailed Up" a PSTN connection is established between the contact center (by SIP Server) and the agent's PSTN phone at the time the agent logs in. This PSTN connection is maintained the entire duration that the agent is logged in, and the agent should keep the phone "off hook" in order to maintain this connection. When the agent and customer finish a call, the agent still leaves the physical phone "off hook" but tells the Genesys desktop application to hangup, which will cause SIP Server to hangup from the customer and park the agent leg of the call on Genesys Media Server (streaming comfort noise) while waiting for the next customer call. It should be noted that if using PSTN agents, the "Nailed Up" method provides much faster (almost immediate) agent transfers. In order to meet regulatory requirements for outbound dialing, a "Nailed Up" connection are strongly recommended for agents actively involved in an outbound campaign.

Note: The remote agent deployment model mentioned for PSTN may also be used to deliver calls to SIP destinations. The key common characteristic of all these scenarios is the agent's phone is not being directly monitored via SIP Server.

**Future Considerations**

Enterprises may be interested in utilizing WebRTC for agent communication. WebRTC is not in scope for SIP Inbound Voice solution but it is mentioned here for completeness. We also expect it will be covered in future documents as the solution is more widely adopted. *Note: It is also possible to support WebRTC if signaling negotiation and transcoding is managed by the SBC and this capability is supported by the Genesys E-SBC.*

## 5.2 External Interfaces

This section describes the external interface for the solution. These become the integration points between solution components and the elements in the customers' premise.

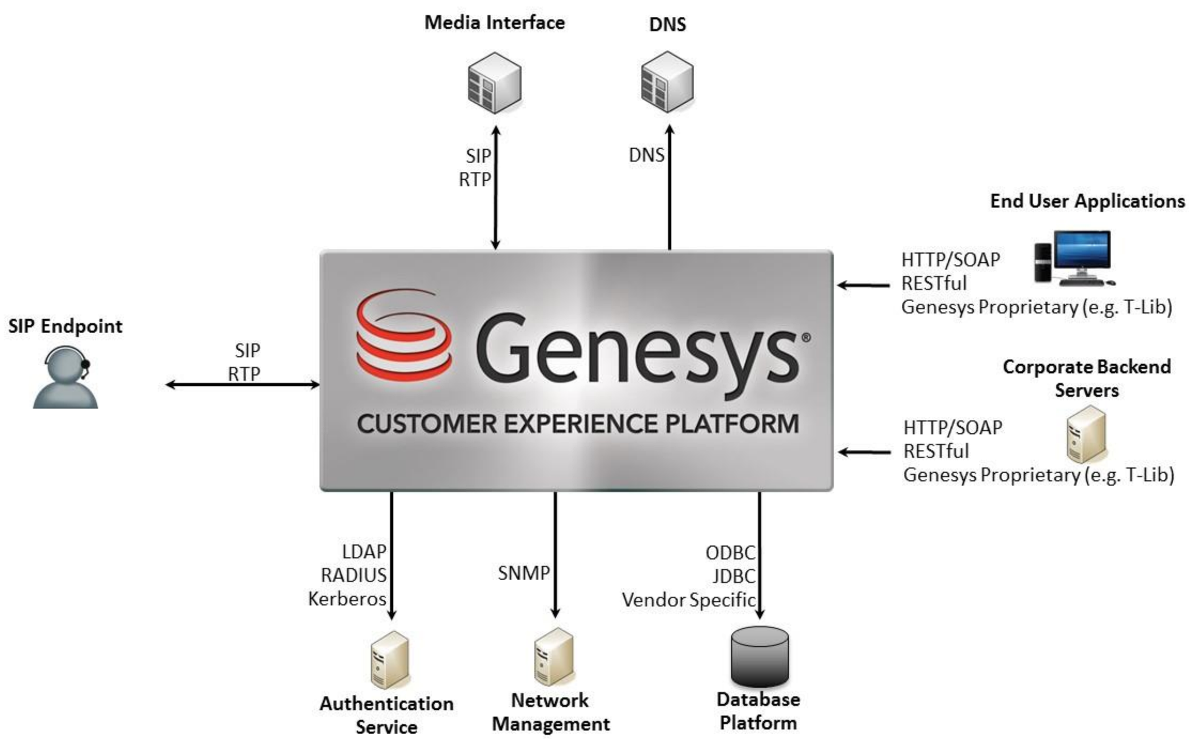



Figure 39 - SIP Voice Blueprint External Interfaces

The following table details each of the external interfaces, its protocols, the components within the solution that are impacted or connected to these external interfaces and lists the integration tasks required to setup the external interfaces.

| Interface | Protocol | Solution Components | Integration Tasks | Description |
|---|---|---|---|---|
| Media Gateway/ Session Border Controller (SBC) | SIP and RTP | SIP Proxy,<br>SIP Server,<br>Resource Manager,<br>MCP,<br>SIP Endpoints (hardphones and softphones) | Add the necessary bandwidth to the network<br>Provision the network infrastructure (e.g. DNS) for the new traffic<br>Provision the MG and SBC appropriately for the integration<br>Configure the codec list for supported codecs. | This interface is used to handle ingress and egress voice traffic from the network. |
| Phones | SIP and RTP | SIP Server (SIP signaling),<br>SIP Feature Server (Provisioning)<br>SBCs, other endpoints/phones | Add the necessary bandwidth to the network<br>Provision the network infrastructure (e.g. DNS) for the new traffic<br>Provision the phone appropriately for the integration<br>Provision the SBC appropriately | This interface is used to handle the egress voice traffic to the agent phones. |
| Phones | HTTP(s) | SIP Feature Server (Provisioning) | Provision the phone appropriately for the integration | This interface is used to provision the phone and provide firmware updates. |
| Configuration, Log, and Reporting Databases (Relational Database/RDBMS) | TCP/SQL | Genesys Info Mart, Interaction Concentrator, GVP Reporting Server, Config, Log, etc. | Provision the network infrastructure (e.g. DNS) for the new traffic<br>Run the database scripts (.sql)<br>Provision appropriate user access to required database tables | This interface is used to get configuration data about the solution and log alarms.<br>It also is used to store reporting data. |

| Interface | Protocol | Solution Components | Integration Tasks | Description |
|---|---|---|---|---|
| Feature Server Databases (Cassandra) | TCP (Apache Cassandra) | Feature Server for use with Genesys Voicemail, FS Dial Plan, and Device Management / Provisioning | Install Cassandra nodes (generally minimum of 3) as part of Feature Server installation. Configure replication.<br><br>Determine when DB is pruned. | Cassandra is the non-SQL database utilized for Genesys Feature Server. It is open source. While Genesys can utilize an embedded Cassandra, having separate external instances of Cassandra is recommended in most cases. |
| Corporate Backend Servers | HTTPS (REST or SOAP), RDMBS access methods (optional) | MCP, ORS/URS, Workspace | Provision the network infrastructure (e.g. DNS) for the new traffic<br><br>Create and provision the security information (certificates, etc.) | This interface is used to get data from the corporate systems to make decisions in solution (agent desktop, routing strategy, etc.). It can also be used to perform certain business actions. |
| Enterprise Authentication Service (Optional) | LDAP, Radius, Kerberos | Configuration Server | Provision the network infrastructure (e.g. DNS) for the new traffic<br><br>Create and provision the security information (certificates, etc.) | This interface is used to perform authentication of users using the solution. Genesys provides the option to have user passwords authenticated an external authentication service or authentication can be managed by Genesys. |
| User of Solution Applications via Load Balancers | HTTP(S)/TCP | GA, GAX, Interactive Insights, GWS, GMS | Provision the corporate load balancers and firewalls to handle the solution application traffic.<br><br>Create and provision the security information (certificates, etc.) | This interface is used for user to access the solution's applications (GA, GAX, GI2, WWE) as well as web services based APIs (GWS and GMS) |

| **Interface** | **Protocol** | **Solution Components** | **Integration Tasks** | **Description** |
|---|---|---|---|---|
| Custom Enterprise Desktop | TCP (Genesys proprietary protocols, ie: TLib, etc) | SIP Server, Stat Server, Config Server | Provision firewalls to permit the application traffic.<br>Create and provision the security information (certificates, etc.) | These interfaces are used by custom applications that integrate with Genesys using specific Genesys SDKs. |
| Corporate Network Management System<br>(Optional) | SNMP | Genesys SNMP Master Agent | Provision the network infrastructure (e.g. DNS) for the new traffic<br>Create and provision the security information (certificates, etc.) | This interface is used to integrate the solution with the Corporate network management system. |
| Domain Name Servers | DNS | SIP Proxy, SIP Server, Workspace, Interactive Insights, SIP Endpoints, etc (potentially any Genesys application). | Provision the DNS records along with appropriate weightings | This interface is used by the clients to perform the name/IP address translation. For specific cold standby components the DNS entries will be manually modified to redirect traffic in the event of a site failure. |

Table 3 - External Interfaces

Session Border Controllers and Media Gateways must be compliant with the following standard specifications:

- IETF RFC 3261 SIP: Session Initiation Protocol
- IETF RFC 3262 Reliability of Provisional Responses in SIP
- IETF RFC 3264 Offer/Answer model with SDP
- IETF RFC 3311 The Session Initiation Protocol (SIP) UPDATE Method
- IETF RFC 3960 Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)
- IETF RFC 4566 SDP: Session Description Protocol
- IETF RFC 6337 Session Initiation Protocol (SIP) Usage of the Offer/Answer Model
- IETF RFC 3323 A Privacy Mechanism for SIP
- IETF RFC 3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity
- IETF RFC 3326 Reason Header

The following standard specifications should also be supported by the SBC or Media Gateway. If the border element does not support the required standards it may be possible to configure workarounds within SIP Server for some scenarios.

For more details, please consult the SIP Server Integration Reference Manual [http://docs.genesys.com/Documentation/SIPS/8.1.1/IntegrationReferenceManual/Welcome].

## 5.3 Operational Management

Once a Genesys solution is in place, managing the solution becomes a primary concern of the customer. There are two approaches to operational management that need to be considered for the solution.

1. If Genesys components are the main focus of the operation, then using Genesys Administrator (GA) and Genesys Administrator Extensions (GAX) becomes the primary mechanism for monitoring the solution.
2. If Genesys is part of a larger operation, then integration into the customer's operational management tool becomes advisable.

In both cases, Genesys Administration and Genesys Administrator Extensions needs to be installed and configured to manage the solution.

### 5.3.1 Network Management Systems

If the customer does have a Network Management System (NMS), then Genesys components should be integrated into their NMS. This is typically done by setting up Net-SNMP to send SNMP events and info to their NMS.

Examples of supportable NMS include Zabbix, HP OpenView and OpenNMS (an open source NMS - http://www.opennms.org/).

In addition to Genesys monitoring, the following additional recommendations should be considered:

- Monitor JVM status, especially memory usage. Note that a regular saw-tooth pattern should be observed due to Java garbage collection.
- Set alarms for specific disk and CPU thresholds
- Additional SNMP traps

Consider the use of ELK (ElasticSearch, LogStash & Kibana) or Splunk to harvest logs and build alarming for specific conditions within the logs. ELK or similar technology may be a useful addition to monitoring.

### 5.3.2 Serviceability

Serviceability relates to the ability of technical support to identify issues and defects within the system. Many customers or partners will perform initial triage and analysis to determine whether Genesys Care should be engaged. If Genesys Care needs to be engaged, it is critical to retrieve the required logs and configuration information and pass this information back to Genesys Care. The following recommendations provide guidance on improving serviceability which can accelerate issues analysis and resolution.

**Logging**

Setting up logical logging locations is a best practice that makes it easier to collect logs and reduce the time to send logs to support. Configuring 3rd party components to log into the same location is ideal as well. Establishing a "log" directory in the root of the disk structure and logging there is recommended:

```
D:\GCTI\log
/log
```

Many problems can occur when trying to retrieve the log files necessary for troubleshooting. Common problems include:

- The log files for the time when the problem occurred have been overwritten or otherwise lost.
- Log files delivered are not within the event time frame.
- Log files provided were created with log levels not detailed enough for the investigation.
- The set of log files provided is inaccurate or incomplete.

The Genesys Log File Management Tool (LFMT) is an intelligent, configurable log collection utility developed by Genesys Customer Care intended to minimize these issues, and thereby reduce the time required to resolve customer problems. It is recommended to include LFMT as a standard part of every deployment.

**Log Analysis**

To assist customers with performing log analysis of SIP messaging Genesys provides the SIP Span 2 utility which can provide an understanding of the SIP call flows within a Genesys environment.

In order to understand the logs and efficiently troubleshoot SIP Server issues, it is recommended to maintain a network architecture diagram showing the IP addresses of key components (including SIP Server(s), Resource Manager(s), Media Control Platform/Media Server(s), Media Gateway(s), Session Border Controllers, etc.) and information on typical call flows. This network diagram should be maintained by customers and kept up to date to help with analysis. It is recommended to have this information readily available and, if possible, provide it to Genesys Care together with the initial problem description and logs, to help reduce overall resolution time.

**Future Tools**

*In 2H 2016 Genesys will be releasing the Genesys Care Workbench which is a suite of troubleshooting tools that can help you quickly and easily identify and resolve issues in your Genesys environment. Workbench collects data from multiple sources, analyzes it, and displays aggregate data and important data correlations in its Current and Historical dashboards as well as some specialized consoles.*

*Types of information displayed on the Workbench Dashboard include:*

- ***Configuration Server changes** – Workbench monitors Configuration Server events for all Application objects, and displays recent configuration changes in the environment*
- ***Alarms** – Workbench configures a default set of alarms in Solution Control Server and displays alarms when thresholds are triggered. If you subscribe to Remote Alarm Monitoring, additional alarms may be displayed.*
- ***Log events** – If Log File Management Tool is deployed, Workbench can monitor log files from supported Genesys applications and display important events for troubleshooting.*

*Once Genesys Care Workbench is released it is recommended that it is included as a standard part of any deployment.*

**Proactive Monitoring**

Genesys can provide proactive monitoring services which delivers the most complete servicing of a customer's environment. Genesys has the ability to perform proactive monitoring through our Premium Care offering. For details on Premium Care options consult the Genesys Account Team and Genesys Customer Care.

### 5.3.3 Monitoring Details

The following provides details on additional monitoring:

- Numerous SNMP traps can be provided by SIP Server. Ensure that these are properly configured.
- SIP Server has an HTTP interface for monitoring its health. This may provide a useful alternative monitoring approach. To enable, configure **http-port** in the **TServer** configuration section of the SIP Server application.
- SIP Server has a Stat log that can be monitored. The log filenames ends with "**-1536**".
- For larger deployments you may monitor URS response times that exceed 1 second on SIP Server. This is the time measured by SIP Server between the T-Event sent to URS/ORS and next T-Request related to the same call received from this client. If this time increases, it may indicate that SIP Server is overloaded, network latency, or that there are delays introduced on the URS/ORS side. To overcome this condition, the load on the SIP Server should be reduced. To monitor this condition, use one of the following methods:
    - Periodically monitor the HTTP interface for "URS Response 1 sec to 5 sec" and "URS Response more than 5 sec". This is a total count taken from the start of SIP Server. Differences between samples should be monitored and alarmed accordingly.
    - Harvest SIP Server's stat logs for "**URS_RESPONSE_1TO5SEC=**" and "**URS_RESPONSE+MORE5SEC=**". The differences between samples of this log should be monitored and alarmed accordingly.

  Note that the logs should not be sampled more often than the sampling period defined by SIP Server's '**operational-stat-timeout**' parameter

- Setup alarms when a SIP Server logs a message with an ID of 52031 or 52032 is recommended. These messages are logged if the transport or call manager thread is delayed.
- Monitor whether SIP Server's main thread CPU consumption is exceeding 70%. The CPU consumption statistic can be monitored using the HTTP interface or Stat log as described above.

### 5.3.4 Provisioning of Devices

Provisioning devices (such as phones, Session Border Controllers, and media gateways) keeping them updated with the latest firmware is an essential component of a telephony solution.

Provisioning provides the ability to automatically configure, deploy, and manage large numbers of devices. Full provisioning of devices typically requires:

- **IP Address Allocation** – which automatically provides IP address and default network parameters (such as network gateway, time server, DNS server, provisioning server, etc) to the device. This is typically provided via the Dynamic Host Configuration Protocol (DHCP). Devices will typically acquire the IP address and other network parameters from a DHCP server already located on the network. In many cases, the DHCP server will need to be configured to reference information specific to the SIP voice network, such as the provisioning server.
- **Boot Firmware and Configuration Updates** – when the device boots, it will look to the provisioning server for updated firmware as well as configuration. Device firmware and configuration is typically provided by FTP/FTPS or HTTP/HTTPS protocols. Some legacy devices still support TFTP as a boot/configuration mechanism, though its use is generally not recommended due to virtually non-existent security.
- **Configuration Interface** – Provides a graphical interface for configuration of individual or groups of devices (such as phones). Typically integrates with the SIP softswitch (such as Genesys SIP Server).
- **Central Logging and Management** – provides the ability for the devices to log information and errors to a centralized log, as well as the ability to manage the devices remotely in order to force them to update firmware, configuration, or force a reboot.

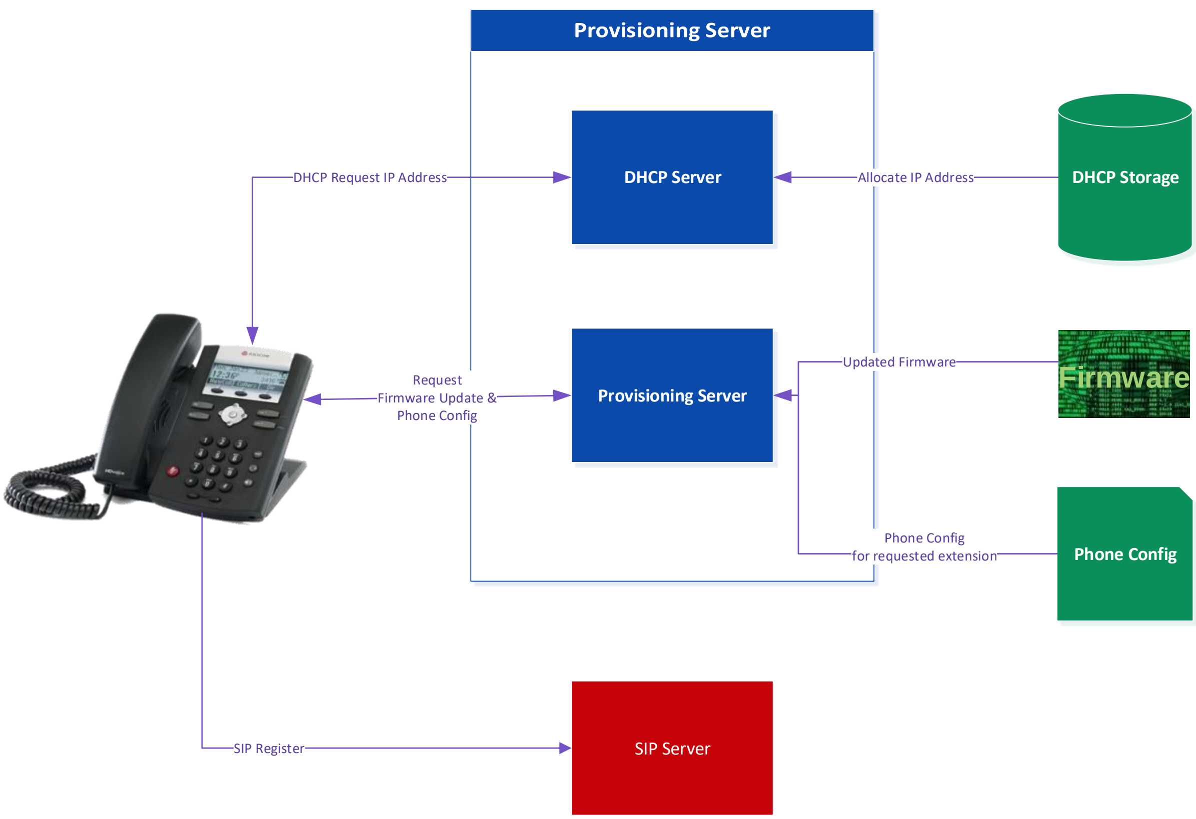



Figure 40 - Provisioning Server

The device is configured to make a DHCP request to get its IP address from the DHCP Server. The DHCP server will typically tell the device its IP address, IP gateway address, NTP server address (for updating its time), and address of the provisioning server. Once this information is obtained, the device will contact the provisioning server (typically by FTP/FTPS or HTTP/HTTPS) and request updated firmware. If updated firmware is found, it is downloaded and the phone rebooted. After checking for (and possibly updating) the firmware, the phone will request its configuration from the provisioning server. With its configuration downloaded, the device will then use that information to connect to SIP Server. For phones, the configuration will include the SIP Server extension number, SIP Server FQDN or IP address, and other parameters necessary for its configuration. At this point, phones will register with SIP Server, and become available for normal operation.

Genesys offers two solutions to provide device provisioning:

- **Genesys Device Management** is provided as part of Genesys SIP Feature Server and provides the ability to configure Genesys supported phones from AudioCodes, Genesys, Yealink, and Polycom. Genesys Device Management integrates directly with Genesys SIP Server configuration. Genesys Device Management in SIP Feature Server currently only supports provisioning of phones.
- **AudioCodes Element Management System (EMS)** that provides for provisioning of AudioCodes phones (as well as Genesys labeled phones), SBCs, and media gateways. AudioCodes EMS may be utilized when large numbers of AudioCodes devices are to be used within the network. Further information on the AudioCodes EMS solution is provided in Genesys Offered Provisioning Systems (section 3.4.5.6).

Other alternatives to device provisioning may be utilized by customers as well, including other third party provisioning systems or custom solutions that involve manual configuration of files to be served to the devices via FTP/FTPS and HTTP/HTTPS.

### 5.3.5 Dial Plan Management

There are several options which Genesys provides for dial plan management. The appropriate approach will be determined by your requirements and environment.

In a typical SIP contact center infrastructure, dial plans may exist in many places within the network. However, generally, dial plans typically provide the following functionality:

- Ability to accept or reject calls based on source, destination, digits dialed, or other criteria
- Ability to determine where the path the call will go through the network
- Ability to modify the digits dialed such as stripping off digits, adding digits, etc. In many cases this can be used for topology hiding such that the end user dialing the number does not have to be aware of the full dial string necessary in order to get the call through the network.

The following are some of the various places that dial plans typically may be configured:

- **Ingress Gateway or SBC** – Dial plans within the ingress Media Gateways or SBCs determine how calls arriving into the network from carrier trunks (or remote sites) are handled, and to where they are sent. In a Genesys SIP Server environment, this often would be directly to Genesys SIP Server (or Genesys SIP Proxy, if used within the environment) for any contact center related calls or any other calls to be handled by SIP Server.
- **Egress Gateway or SBC** – Dial plans within the egress Media Gateways or SBCs determine how calls destined to be sent through a carrier trunk or remote site are handled. In many cases, the dial plan may strip or add digits prior to sending the call on. The dial plan will also be used to determine which specific trunk(s) the call may be sent. In addition, the dial plan can allow the

SBC or media gateway to accept or reject certain calls based on many conditions (such as the source endpoint, destination, time of day, existing trunk utilization, etc).

- **SIP Endpoints** – SIP endpoints such as phones typically will have a dial plan that determines which digits are valid to be dialed from that phone. In addition in cases where the phone or endpoint may utilize multiple SIP softswitches, the phone dialplan may also determine which SIP softswitch the call will be directed to (such as Genesys SIP Server).
- **SIP softswitch / PBX** – The SIP softswitch often has its own dial plan that will determine what numbers can be dialed by each endpoint, and where to send those calls.

In a Genesys SIP Server environment, SIP Server serves as the SIP softswitch. SIP Server allows dial plans to be configured either directly within each SIP Server's configuration or, for environments with large numbers of SIP Server, within Genesys SIP Feature Server. Use of SIP Feature Server for dial plan configuration allows multiple SIP Servers to share the same dial plan, simplifying administration for larger environments.

To help determine where in the architecture the dial plan should be managed, you should begin by outlining and diagramming your dial plan needs. Examples of considerations include:

- When a call ingresses, is the SBC/MG adding any digits or characters to the ANI received (+ or 1) that will need to be stripped out by SIP Server for further processing?
- When a call egresses, is a character needed to access an outside trunk (9), or an inside trunk (8)?
- For any 4, 5, 6, 7, etc. digit dial plan, do you need to add a predefined set of digits to make it a dialable number?

Once you have your plan defined it is time to identify the tiers in your architecture that will perform each step. For small environments the dial plan could potentially be only in the SIP Server or only in the SBC. For a large environment, this could be spread across various SIP Server tiers, Feature Servers, SBCs, MGs, and so on. It is important to think about customer initiated dialing, and agent initiated dialing for internal and external calls, consults, and conferences. Consideration of what can be dialed on a SIP hardphone vs SIP softphone vs agent desktop (3pcc) should be taken into account (1pcc vs 3pcc dial is important). Some dialing rules can also be configured in Class of Service.

Even when the dial plan has been "externalized" in the SBC/MG, there are typically multiple layers of dial plans. Genesys will continue to have a dial plan to handle internal dialing within the Genesys environment. For single site deployments this is trivial as all Genesys resources reside on a single SIP Server. Multiple SIP Servers may utilize the centralized dial plan in Feature Server.

When traffic is directed outside of Genesys then it should be managed through an enterprise dial plan. This is typically accomplished by having all traffic directed to an SBC where the primary dial plan resides. The SBC is responsible for directing the traffic out the appropriate telephony trunk (SIP or TDM) or directing the traffic to other enterprise communication systems, such as a legacy PBX.

Externalizing the dial plan through an SBC or media gateway can also provide an elegant control point to manage a phased migration from a legacy contact center environment to as Genesys SIP solution. While traffic could be distributed at the carrier level managing this control through the dial plan provides for direct control.

It should be noted that in almost all cases, a dial plan will need to be configured on the SIP phones and endpoints through the provisioning server (such as Device Management in SIP Feature Server). Even if much of the dial plan management is to be done inside SIP Server configuration, at the very least, the phone dial plan will need to be configured to allow the phone to dial the correct number of digits.

#### 5.3.5.1 Outbound Call Flow

The diagram below shows an example of the dial plans invoked when a user on a SIP phone places and outbound call to the PSTN carrier:

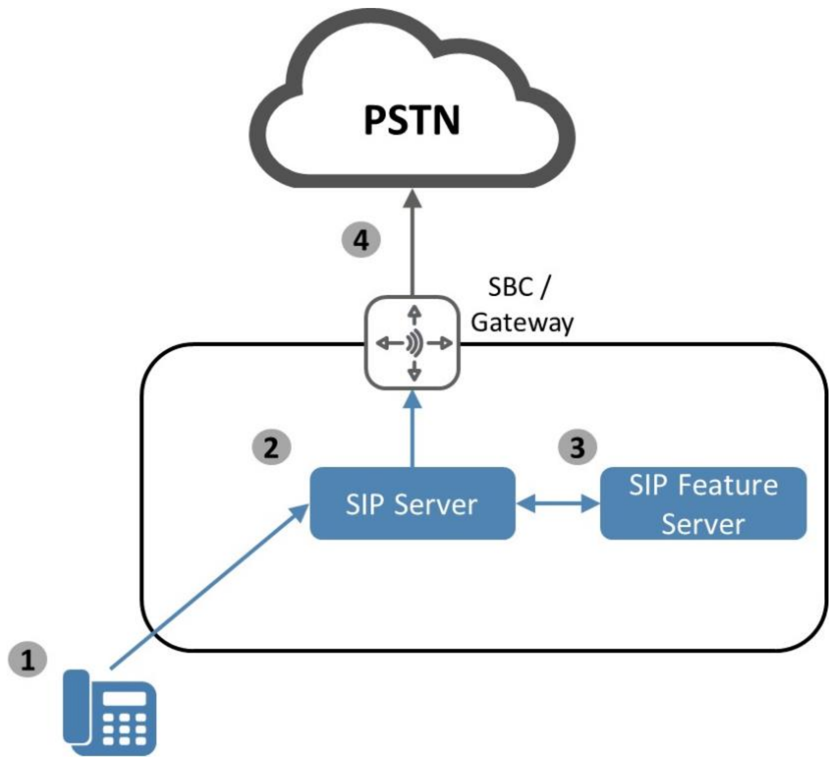



Figure 41 – Outbound Call Dial Plan Flow

The above diagram shows the following steps and places where a dial plan will be executed:

1. **Phone** – The user picks up the phone and dials a number. Here, the dial plan within the phone itself will verify that the digits and number of digits are valid and then may also use the number dialed to determine where to send the call. In some cases the phone itself may rewrite the number dialed prior to sending the call on.
   In most cases, the dial plan on the phone may be very simple and only ensure that the correct number of digits are dialed.
2. **SIP Server** – Genesys SIP Server, upon receiving the digits from the phone, will then look at its dial plan to determine whether the calls is to be accepted or rejected, whether or not to modify the digits, and where the call should be sent. In the event the call is to go through an external trunk, SIP Server will use the digits dialed in order to determine the best trunk for the call. In

the event that SIP Feature Server is used for the dial plan (see below), it may replace or supplement this functionality within this SIP Server.

3. **SIP Feature Server (Optional)** – SIP Feature Server may optionally be used to implement a dial plan across multiple SIP Servers for larger environments. In this case, SIP Server will make an HTTP request of SIP Feature Server to ask it for instructions based on the digits dialed Once this is done, the SIP Server will then use that information to determine how to handle the call.
4. **SBC or Media Gateway** – The SBC or Media Gateway typically has the final say on how the call is redirected to the carrier or to a remote site. It also will look at the digits dialed to determine if the call is to be accepted or rejected. It may also manipulate the digits and then selected the desired path to forward the call to the carrier network or remote site.

#### 5.3.5.2 Inbound Call Flow

Inbound calls arriving to the SBC or media gateway will typically follow a path similar to the one in the diagram below:

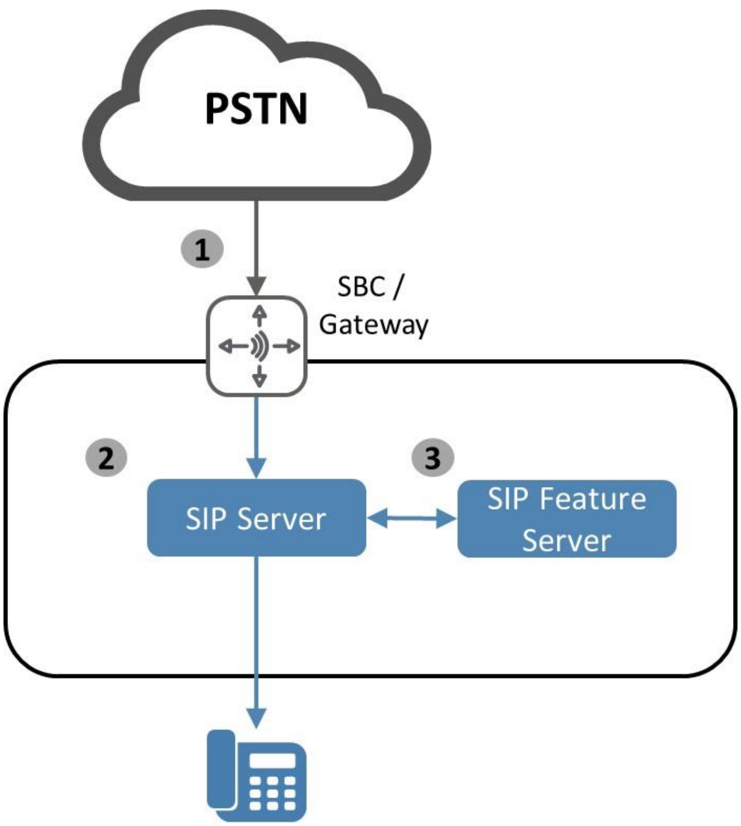



Figure 42 – Inbound Call Dial Plan Flow

The above diagram shows the following steps where a dial plan may be executed:

1. **SBC or Media Gateway** – Upon the inbound call arriving from the carrier network or remote site, the SBC or Media Gateway will look at the digits sent and other criteria to determine

whether to accept or reject the call, and how to manipulate the digits. If the call is not rejected, it will then choose where to send the call, such as to send the call to SIP Server.

2. **SIP Server** – SIP Server will receive the call from the SBC or Media Gateway and then execute a dial plan to determine where the call should go, such as (in this example) to an agent endpoint. In some cases, SIP Server may be configured to request Genesys SIP Feature Server to look at its dial plan to determine how to handle the call.
   It should be noted that if the call was destined for a Routing Point on SIP Server, that SIP Server may choose to make a route request of Genesys URS or ORS in order to determine how next to handle the call. While URS or ORS are typically not used to implement a true dial plan, they do of course determine how the call eventually gets routed.
3. **SIP Feature Server (Optional)** – In the event that SIP Feature Server is used for dial plans within the environment, SIP Feature Server will look at the information and digits provided by SIP Server and return instructions for handling the call back to SIP Server. SIP Feature Server is typically used in environments with large numbers of SIP Servers that wish to share the same dial plan.

At the end of step 2 or 3 (if SIP Feature Server is used), if the call had not been rejected, SIP Server will send the call to the destined phone or endpoint. Typically, the endpoint dial plan is not utilized at this point, though in some phones it could be, allowing for further determination of whether the call is accepted or rejected.

# 6 Implementation View

The Implementation View describes details such as sizing, security and configuration of the solution based on the previous deployment and interaction views.

## 6.1 Solution Sizing Guidelines

This section provides guidelines on sizing the SIP Voice solution to determine the server requirements as well as component distribution. When sizing the solution there are vary variables that can impact the capacity such as the number of agents, the type of call flows, peak call volumes, network bandwidth, etc. It can be challenging to perform a sizing that is both simple and accurate. Genesys has created an Integrated Sizing Calculator to assist with solution sizing.

When performing sizing the approach taken is to assume certain variables such as busy hour calls, qualification, queue & talk times and a mix of call flows (as depicted in section 5.1 Call Flows). Based on these assumptions, the CPU, memory and storage requirements are calculated.

Genesys has provided a representative sizing based on a 2,000 agent deployment. The sizing accounts for a centralized deployment (sizing for a dual-data center deployment is currently pending based upon enhancements to the sizing calculator). The sizing assumptions and architecture provided below are from the Integrated Sizing Calculator. The sizing assumes use of virtualization although specific requirements for the underlying hardware (CPU profile) are also specified. *Please treat this sizing estimate as a rule of thumb. Changes to any variable can impact the overall sizing.*

**Additional Considerations:** For detailed SIP Server sizing a separate SIP Server Sizing Tool is available. This tool can be consulted for complex, large and/or atypical architectures to help validate the overall solution sizing. The SIP Server Sizing tool can be downloaded from the Documentation site to evaluate SIP Server and SIP Proxy CPU load and network traffic. Details on the usage of this tool are beyond the scope of this document.

### 6.1.1 Solution Sizing – Centralized Deployment

This section provides the sizing for a centralized deployment supporting 2,000 agents.

#### 6.1.1.1 Sizing Assumptions

The following assumptions are made regarding the sizing of this solution.

| Input Assumptions | 2,000 Agents |
|---|---|
| Agents | 2,000 |
| Agent utilization | 80% |
| Call qualification time | 60s |
| Queue time | 120s |
| Talk time | 180s |
| Log retention | Debug 2 weeks |
| Reporting History | 2 years |

| | |
|---|---|
| Non-aggregated Reporting History | 3 months |
| ***Calculated worst case values - Inbound*** | |
| Calls / agent / hour | 16 |
| Concurrent active calls | 2000 |
| Peak CAPS | 8 |
| Busy hour calls | 28800 |
| ***Calculated worst case values - Outbound*** | |
| Calls / agent / hour | 48 |
| Total Daily Records | 50,000 |
| Total Answer Rate | 70% |
| Human Answer Rate | 30% |
| Redial Attempts | 1 |

#### 6.1.1.2 Hardware/Virtualization Assumption

The underlying hardware will impact the overall performance of any virtualization solution. To that end, the following hardware requirements were assumed when using the Integrated Sizing Calculator:

- CPU Score per Core = 30
- Hyper-threading = Off
- Number of Chips (NUMA Nodes) = 2

In addition, it is assumed that each hardware server will be running VMWare ESXi v5.4 or greater.

#### 6.1.1.3 Virtual Machine Sizing

The following table details the virtual machine sizing for CPU, RAM and disk. For further details, please see the accompanying **Integrated Sizing Calculator**.

***Note: Components specific to the SIP Voice blueprint which are not yet reflected in the Integrated Sizing Calculator include:***

- ***Genesys Feature Server***
- ***Genesys Voice Platform Reporting***
- ***MRCP Proxy***
- ***Nuance ASR and TTS***

The sizing calculator indicates that 22 VMs are required for the components which it covers. This sizing includes the SIP Voice solution as well as Genesys common components. The VMs and component distribution is:

| VM Name | vCores | Memory (GB) | Components |
|---|---|---|---|

| | | | |
|---|---|---|---|
| | | | common_cfg |
| | | | common_msg |
| | | | common_scs |
| vm_common_fw | 4 | 4 | **VM Total** |
| | | | voice_mcp |
| vm_voice_mcp | 4 | 4 | **VM Total** |
| | | | voice_mcp |
| vm_voice_mcp | 4 | 4 | **VM Total** |
| | | | voice_rm |
| vm_voice_rm | 4 | 4 | **VM Total** |
| | | | common_cfg-b |
| | | | common_msg-b |
| | | | common_scs-b |
| vm_common_fw-b | 4 | 4 | **VM Total** |
| | | | voice_mcp |
| vm_voice_mcp | 4 | 4 | **VM Total** |
| | | | voice_mcp |
| vm_voice_mcp | 4 | 4 | **VM Total** |
| | | | voice_ss |
| | | | voice_urs |
| | | | voice_ocs |
| vm_voice_stat_router_ocs | 4 | 4 | **VM Total** |
| | | | voice_db |
| | | | voice_db-cl |
| | | | voice_sql |
| vm_voice_db | 8 | 8 | **VM Total** |
| | | | voice_mcp |
| vm_voice_mcp | 4 | 4 | **VM Total** |
| | | | voice_ss-b |
| | | | voice_urs-b |
| | | | voice_ocs-b |
| vm_voice_stat_router_ocs-b | 4 | 4 | **VM Total** |
| | | | voice_sip |
| | | | voice_icon |
| | | | voice_sip_prx |
| vm_voice_sip_icon | 4 | 4 | **VM Total** |
| | | | voice_mcp |
| vm_voice_mcp | 4 | 4 | **VM Total** |
| | | | voice_mcp |
| vm_voice_mcp | 4 | 4 | **VM Total** |

| | | | |
|---|---|---|---|
| | | | voice_gim |
| | | | voice_java |
| vm_voice_gim | 4 | 4 | **VM Total** |
| | | | voice_sip-b |
| | | | voice_icon-b |
| | | | voice_sip_prx |
| vm_voice_sip_icon-b | 4 | 4 | **VM Total** |
| | | | voice_mcp |
| vm_voice_mcp | 4 | 4 | **VM Total** |
| | | | voice_ors |
| | | | voice_cas |
| vm_voice_ors_cas | 4 | 4 | **VM Total** |
| | | | voice_cfg-prx |
| | | | voice_ss-cl |
| vm_voice_cfgprx_stat | 4 | 4 | **VM Total** |
| | | | voice_mcp |
| vm_voice_mcp | 4 | 4 | **VM Total** |
| | | | voice_mcp |
| vm_voice_mcp | 4 | 4 | **VM Total** |
| | | | voice_ors-b |
| | | | voice_cas |
| vm_voice_ors_cas-b | 4 | 4 | **VM Total** |

### 6.1.2 Solutions Sizing – Dual Data Center Deployment

Awaiting updated Sizing Calculator

### 6.1.3 Database Sizing

The following table summarizes the database sizing requirements for Genesys components stored within the RDBMS. These are estimates based on the sizing assumptions and should be treated as a starting point. Other customer factors can impact the overall data requirements.

Awaiting updated Sizing Calculator

| System | 2000 agents |
|---|---|
| *Configuration Server* | _ MB |
| *Message Server* | _ MB |
| *Genesys Administrator Extension* | _ MB |
| *Universal Contact Server* | _ MB |

| | |
|---|---|
| ~~***Interaction Server***~~ | ~~_ MB~~ |
| *Outbound Contact Server* | _ MB |
| *Interaction Concentrator* | _ MB |
| *Genesys Info Mart* | _ MB |
| *Genesys Interactive Insights (GI2)* | Insignificant |
| *Pulse* | TBD |
| **Total SQL database storage** | **___ GB** |

**Cassandra DB Sizing for Genesys Feature Server (Optional)**

Awaiting updated Sizing Calculator

| System | 2000 agents |
|---|---|
| *Voicemail* | _ MB |
| *Device Management* | _ MB |
| *Dial Plan Management* | _ MB |
| **Total Cassandra database storage** | **___ GB** |

### 6.1.4 Network Sizing and Readiness

The success of a SIP Voice Blueprint deployment hinges on ensuring that the network is ready and has the appropriate bandwidth. Customer networks are varied and a Network Assessment is truly the best course of action to ensure readiness.

As guidance, the following network load has been calculated for the solution.

(Awaiting updated Network Bandwidth Sizing Calculator)

| Network Traffic | 2000 Agents |
|---|---|
| Within Data Center | |
| Between Data Centers (Business Continuity) | |
| Between Branches and Data Centers | N/A |

Table 4- Network Traffic Guidance

## 6.2 Configuration Guidelines

The following guidelines provide a high-level guide to typical settings that need to be configured within the SIP Voice Solution components. Variants in the customer's network environment may require alternate settings. See the notes section for the listed options.

- SIP Server can run as a single thread or 3 threads based on **link_type** parameter. SIP Server should be setup with the **link_type** set to **3** so that the SIP and TServer run as separate threads.
- Agent Reservation configuration is required for multi-site deployments and multiple routing Stat Servers for properly blending agents (both for media blending and distributing traffic across sites). The use of Agent Reservation may impact other settings and performance

For larger deployments the following options should be reviewed:

- SIP processing capacity can be increased by using a tiered SIP Server architecture.
    - A tiered SIP Server architecture can reduce the number of client connections monitoring a given SIP Server as the tiered architecture distributes objects such as Routing Points and Agents at different layers
    - When establishing a Routing Tier, call flows and strategies will need to be designed and reviewed. Optimization of ISCC Trunk usage with these strategies will be essential especially if agents will be transferring calls back to the Routing Tier.
- KVP updates will impact the performance of SIP Server. Best practice is to update numerous KVPs within a single update transaction to reduce the load on SIP Server.
    - Routing strategies should be designed to reduce the frequency of KVP updates by combining requests.
    - Adjust Workspace to combine KVP updates into fewer requests. This applies to both Workspace and custom desktop applications.
- The number of monitoring clients impact the main T-Server thread within SIP Server. Genesys Load Distribution Server (LDS) can be used to proxy these monitoring clients so they only use a single connection thereby reducing the load.
    - The largest load is often due to multiple Stat Servers as they have a large set of objects which they may be monitoring.
- The number of treatments of a call should be reviewed and optimized, especially treatments while the call is in queue.

Additional

- Overload controls can also be set on SIP Server using the following option: **overload-ctrl-call-rate-capacity** a discussion required to determine the appropriate value.

#### 6.2.1.1 Other Considerations

The following are not configurations specifically but other considerations for performance and reliability:

- Ensure SIP v8.1.102.01 or greater
- There should not be any high CPU consuming processes running alongside SIP Server on the same host, such as log archivers, anti-virus, 3rd-party monitoring software, etc. at the time when SIP Server handles the production traffic.

- Special attention should be paid to the SIP Server logging, aiming to minimize the number of log files kept in the logging folder. Generally it is recommended to use larger size segments (option log\'segment') with a smaller number of log segments kept in the logging folder (log\'expire').
- SIP Servers should be provisioned with logging level adequate to quick issue analysis and resolution, which usually translates into log\verbove=all.
- Avoid using console and network devices for log output
- SIP Servers are provisioned with asynchronous DNS resolution feature enabled (common\enable-async-dns=1). Refer to KB Article "SIP Server stops processing all incoming SIP traffic until restarted" (https://na12.salesforce.com/articles/SOLUTIONS/17558?popup=true)
- SIP Servers are provisioned with the Thread-Alive Monitoring feature enabled. Refer to KB Article "SIP Server stops processing all incoming SIP traffic until restarted" (https://na12.salesforce.com/articles/SOLUTIONS/17558?popup=true)

**Pre-production testing**:

- Prior to being deployed in production each SIP Voice deployment should undergo a rigorous set of tests aiming at determining its maximum sustainable call volume and fault tolerance (reliability).

**Scalability**:

- For the maximum sustainable call volume determination, the SIP Voice Solution should be put under a gradually increasing call rate, closely emulating the required production call flows. The results can be used in the overload control parameters.

**CPU Utilization:**

- In the single-threaded mode (sip-link-type=0) SIP server process must not exceed 65% of CPU usage on a single CPU core under the max load for a continuous time interval.
- In the multi-threaded mode (non-IMS deployments with sip-link-type=3 or IMS deployments with sip-link-type=4) SIP server process must not exceed 75% of CPU usage on any single core under the max load for a continuous time interval

**Change Control Process:**

- In production implement change control processes.
- Avoid making critical changes in the live environment. Make these changes only during maintenance windows.
- Keep a backup copy of your configuration database current. Make a backup copy prior each configuration change.

### 6.2.2 DN-Specific Configuration

The following table lists several instances – please refer to the diagram 999 for more details on the instance that is being configured.

| Instance | Target | Configuration Option Settings | Notes |
|---|---|---|---|

| | | | |
|---|---|---|---|
| **SIP Routing & SIP Hub** | Agent DN | `option=x` | DN created for each phone/phone number |
| **SIP Routing** | Non-Agent DN | | |
| **SIPS Routing** | SBC or Gateway DN | | |
| | SBC or Gateway DN | Userdata-map-filter="<specific userdata>" | Ensure that userdata is passed along with the call<br>NOTE: Do not use the filter on media services or RM DNs, especially with the typical filter="*" |
| | | | |

Table 5 - DN Configuration

## 6.3 Security

Protecting the customer's infrastructure should be imperative for any solution deployment. Genesys components can typically be deployed in a secure manner. Many customers have their own security procedures that our solution needs to conform to. The Genesys Security Deployment Guide provides details on security features offered by Genesys software and how these features are configured [http://docs.genesys.com/Documentation/System/8.5.x/SDG/Welcome].

The following are guidelines for some of the requirements that may be encountered or should be recommended.

### 6.3.1 Secure Connections

Connections between components, especially those external to the solution (see 5.2 External Interfaces) should be secured. Where possible use SSL or HTTPS.

Typically customers will insist on firewalls to protect HTTP traffic from the wild internet. In a similar fashion Media Gateways or Session Border Controllers need to be configured to protect VoIP traffic.

### 6.3.2 VM and OS hardening

Operating Systems are often pre-configured for ease of use and development and not necessarily security. If the O/S is being installed or is part of a set of VMs being delivered, that O/S should be hardened to ensure that typical security holes are addressed.

The following document, which provides recommendations followed with Genesys Cloud, provides an overview of processes and considerations to harden the solution VMs and the OS.

Microsoft Word 97 - 2003 Document

## 6.4 Localization and Internationalization

Localization and Internationalization are topics for numerous Genesys components, especially user interfaces and reporting. Within the SIP Voice Solution, the main components to pay particular attention are:

- Media Files such as audio files
- Administration & Operation management user interfaces
- Agent desktop software
- Reports

# Appendix A Common Components Summary

The Genesys Common Component Blueprint provides a foundational architecture which consists of elements utilized across all Blueprint architectures. The Common Components architecture is not intended as a standalone solution but should be used with other Blueprint architectures as it provides common capabilities which they utilize.

Readers are recommended to review the Common Component Blueprint for detailed information on the Common Components and the architectural considerations and recommendations. The following summary is provided as a quick reference so readers are aware of what is covered by the Common Components Blueprints.

**Common Components Scope**

Genesys Common Component Blueprint covers standard elements which are used by multiple solutions. The Common Component Blueprints is focused on 3 areas – Orchestration, Reporting and Configuration/Management.

***Genesys Orchestration***– World class routing engine which intelligently distributes interactions to the right contact center resources based contextual information and business rules and the overall state of contact center resources.

The following components are included within the Orchestration layer:

- Universal Routing Server
- Orchestration Server
- Stat Server
- Universal Contact Server
- Genesys Mobile Services (Context Services)
- Genesys Rules
- Genesys Web Services

***Genesys Reporting*** – Real-time and Historical reporting provided by Pulse (Real-time) and ICON/Info Mart/Interactive Insights (Historical)

The following components are included within Reporting layer:

- Stat Server
- Pulse (Consists of Collector, Storage and Rabbit MQ)
- Interaction Concentrator
- Info Mart
- Interactive Insights

***Genesys Configuration and Management*** – OAM&P layer enabling centralized configuration, management and alarming of the entire Genesys environment.

The following components are included within the Configuration and Management layer:

- Genesys Administrator / Genesys Administrator Extensions
- Configuration Server
- Solution Control Server
- SNMP Master Agent
- Message Server
- Local Control Agent
- DB Server (Used in prior Genesys version or for other Genesys components)

**Common Components Scope**

The following diagram shows the components included in the Common Components Blueprint.

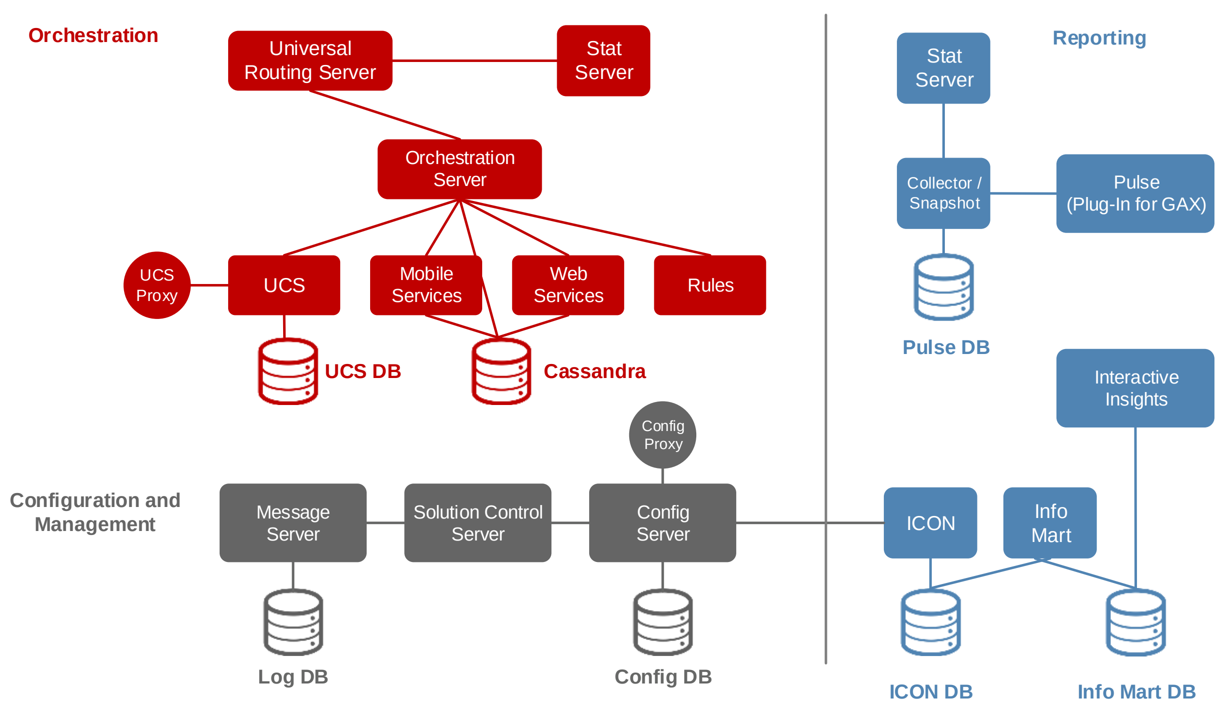



Figure 43 Common Components Blueprint - High Level

The Common Components are the foundation of any solution. The diagram is intended to provide a clear understanding of the different areas which are addressed by the Common Components Blueprint and not all components or connections are shown. The general expectation is that all elements reflected in the Common Components Blueprints will be deployed. Utilizing a standardized architecture and standard deployment strategy helps create consistency, repeatability and enables extensibility of the Genesys capabilities through the additional business scenarios without needing to install other Genesys components. For example while an Email deployment may not require Genesys Mobile Services, Web

Services or Rules these components are expected to be installed. There are some exceptions to this as those Solution Blueprints which do not directly Orchestrate interactions such as Workforce Management may not have these components installed as standard.

# Appendix B Performance Configuration

The following SIP Server related configurations relate to performance and reliability of the system in addition to other options that may require attention.

**Note:** Additional enhancements are planned for SIP Server in 2H 2016 to improve performance under overloaded conditions. These enhancements include the ability to dynamically reduce the log level under high load.

| Configuration Option | Setting | Notes |
|---|---|---|
| **[TServer]sip-link-type** | 3 | Performance improvement – TServer and sip run in different threads |
| **[Log]verbose** | standard | Valid options are none, standard, interaction, trace and debug (or all). Note that when trouble-shooting, debug is used. |
| **internal-registrar-domains** | <specific ip address or domain name> | Names are taken literally, no attempt to convert hostnames to IP address or vice-versa is made. Therefore all possible variations of domain names should explicitly be listed. |
| **internal-registrar-enabled** | yes | For most ACD solutions, this should be set to Yes on the SIP Server instance in the data center. Agents will then register their end-points to SIP Server. Some other environments may already have a SIP Registrar that SIP Server needs to integrate with (see external-registrar option) |
| **external-registrar** | <hostname: port> | Destination where to send all SIP REGISTER and SUBSCRIBE requests for domains that do not belong to SIP Server. This should typically not be set as SIP Server should be the registrar. However, the customer environment may require the use of a 3rd party registrar. |
| **internal-registrar-persistent** | false | Enables registrar persistence. If true, SIP Server will store endpoint contact information, received via REGISTER messages, in the Annex option "TServer\contact" of the DN configuration object in Configuration Server. Default value is "false". **Note: This option should only be set to true if Hot Standby HA is not used in the environment.** |
| **-nco** | Exit | Command line option ensures that process exits before restarting |

| | | |
|---|---|---|
| **Auto-Restart** | True | Set in Genesys Administrator – ensures restarting SIP Server by Management Framework. |
| **overload-ctrl-call-rate-capacity** | <max sustainable call rate> | Need to test to find the maximum sustainable call rate within the environment, then set the overload control to prevent exceeding this capacity. |
| **overload-ctrl-threshold** | overload-ctrl-call-rate-capacity/2 | Based on the previous `overload-ctrl-call-rate-capacity`. |
| **overload-ctrl-trequests-rate** | <trequest capacity rate> | Starting from SIP Server release 8.1.100.64 this option protects SIP Server from excessive T-Requests |
| **overload-ctrl-call-trequests-rate** | <trequest capacity rate> | More granular control of which T-Requests to limit and by which rate. |
| **overload-ctrl-call-tupdateuserdata-requests-rate** | <trequest capacity rate> | More granular control of which T-Requests to limit and by which rate. |
| **overload-ctrl-call-tapplytreatment-requests-rate** | <trequest capacity rate> | More granular control of which T-Requests to limit and by which rate. |

Table 6 - SIP Server Configuration

For more details, please consult the SIP Server Deployment Guide [http://docs.genesys.com/Special:Repository/81fr_dep-sip.pdf?id=2e30d00a-05d6-4c84-a539-eb7ddcbde5f4].