Framework 8.0

SIP Server

Integration Reference Manual

About Genesys

Genesys Telecommunications Laboratories, Inc., a subsidiary of Alcatel-Lucent, is 100% focused on software for contact centers. Genesys recognizes that better interactions drive better business and build company reputations. Customer service solutions from Genesys deliver on this promise for Global 2000 enterprises, government organizations, and telecommunications service providers across 80 countries, directing more than 100 million customer interactions every day. Sophisticated routing and reporting across voice, e-mail, and Web channels ensure that customers are quickly connected to the best available resource—the first time. Genesys offers solutions for customer service, help desks, order desks, collections, outbound telesales and service, and workforce management. Visit www.genesyslab.com for more information.

Each product has its own documentation for online viewing at the Genesys Technical Support website or on the Documentation Library DVD, which is available from Genesys upon request. For more information, contact your sales representative.

Notice

Although reasonable effort is made to ensure that the information in this document is complete and accurate at the time of release, Genesys Telecommunications Laboratories, Inc., cannot assume responsibility for any existing errors. Changes and/or corrections to the information contained in this document may be incorporated in future versions.

Your Responsibility for Your System's Security

You are responsible for the security of your system. Product administration to prevent unauthorized use is your responsibility. Your system administrator should read all documents provided with this product to fully understand the features available that reduce your risk of incurring charges for unlicensed use of Genesys products.

Trademarks

Genesys, the Genesys logo, and T-Server are registered trademarks of Genesys Telecommunications Laboratories, Inc. All other trademarks and trade names referred to in this document are the property of other companies. The Crystal monospace font is used by permission of Software Renovation Corporation, www.SoftwareRenovation.com.

Technical Support from VARs

If you have purchased support from a value-added reseller (VAR), please contact the VAR for technical support.

Technical Support from Genesys

If you have purchased support directly from Genesys, please contact Genesys Technical Support at the regional numbers provided on page 11. For complete contact information and procedures, refer to the ***Genesys Technical Support Guide***.

Ordering and Licensing Information

Complete information on ordering and licensing Genesys products can be found in the ***Genesys Licensing Guide.***

Released by

Genesys Telecommunications Laboratories, Inc. www.genesyslab.com

Document Version: 80fr_ref-sip_06-2010_v8.0.001.00

Table of Contents

List of Procedures

Preface

Welcome to the *Framework 8.0 SIP Server Integration Reference Manual*. This document introduces you to the concepts, terminology, and procedures related to integrating SIP Server with SIP softswitches and gateways. The reference information includes, but is not limited to, configuration options, limitations, and switch-specific functionality. This document is designed to be used along with the *Framework 8.0 SIP Server Deployment Guide*.

This document is valid only for the 8.0 release of this product.

Note: For versions of this document created for other releases of this product, visit the Genesys Technical Support website, or request the Documentation Library DVD, which you can order by e-mail from Genesys Order Management at `orderman@genesyslab.com`.

This preface contains the following sections:

For information about related resources and about the conventions that are used in this document, see the supplementary material starting on page 179.

About SIP Server

SIP Server is the Genesys software component that provides an interface between your telephony hardware and the rest of the Genesys software components in your enterprise. It translates and keeps track of events and requests that come from, and are sent to the telephony device. SIP Server is a TCP/IP-based server that can also act as a messaging interface between SIP Server clients. It is the critical point in allowing your Genesys solution to facilitate and track the contacts that flow through your enterprise.

Intended Audience

This guide is intended primarily for system administrators, certified technicians, those who are new to SIP Server and those who are familiar with it. Based on your specific contact center environment and your responsibilities in it, you may need to be familiar with a much wider range of issues as you deploy SIP Server.

In general, this document assumes that you have a basic understanding of, and familiarity with:

- Computer-telephony integration (CTI) concepts, processes, terminology, and applications.
- Network design and operation.
- Your own network configurations.
- Your telephony hardware and software.
- Genesys Framework architecture and functions.
- Configuration Manager interface and object management operations.

In particular, this document assumes that you are trained and certified on the products this guide is written for. For more information, see product-specific documentation.

The SIP Server integration solutions described in this document are not the only methods that will work; rather, they are the ones that have been tested and approved by Genesys, and that are supported by Genesys Customer Support.

Reading Prerequisites

You must read the *Framework 8.0 Deployment Guide* and *Framework 8.0 SIP Server Deployment Guide* before using this *SIP Server Integration Reference Manual.*

Making Comments on This Document

If you especially like or dislike anything about this document, feel free to e-mail your comments to `Techpubs.webadmin@genesyslab.com`.

You can comment on what you regard as specific errors or omissions, and on the accuracy, organization, subject matter, or completeness of this document. Please limit your comments to the scope of this document only and to the way in which the information is presented. Contact your Genesys Account Representative or Genesys Technical Support if you have suggestions about the product itself.

When you send us comments, you grant Genesys a nonexclusive right to use or distribute your comments in any way it believes appropriate, without incurring any obligation to you.

Contacting Genesys Technical Support

If you have purchased support directly from Genesys, contact Genesys Technical Support at the following regional numbers:

Region	Telephone	E-Mail
North America and Latin America	+888-369-5555 (toll-free) +506-674-6767	support@genesyslab.com
Europe, Middle East, and Africa	+44-(0)-1276-45-7002	support@genesyslab.co.uk
Asia Pacific	+61-7-3368-6868	support@genesyslab.com.au
Malaysia	1-800-814-472 (toll-free) +61-7-3368-6868	support@genesyslab.com.au
India	000-800-100-7136 (toll-free) +91-(022)-3918-0537	support@genesyslab.com.au
Japan	+81-3-6361-8950	support@genesyslab.co.jp
Before contacting technical support, refer to the *Genesys Technical Support Guide* for complete contact information and procedures.		

Chapter

1

SIP Server Integration with Siemens OpenScape Voice

This chapter describes how to integrate SIP Server with the Siemens OpenScape Voice switch (hereafter referred to as *OpenScape Voice*). It contains the following sections:

Note: The instructions in this chapter assume that OpenScape Voice is fully functional and routing calls before Genesys products are installed. They also assume that SIP Server has already been configured to function properly in Stand-alone mode, and that configuration between SIP Server and Universal Routing Server (URS) has already been completed.

Overview

The SIP Server and OpenScape Voice integration solution described in this chapter is not the only method that will work. Although there are other methods, this is the only one that has been tested and approved by Genesys, and that is supported by Genesys Customer Support. This chapter contains best practice guidelines determined by both Genesys and Siemens Engineering departments. Deviating from the solution described in this chapter can have unexpected consequences.

Although this chapter provides steps to log in to OpenScape Voice, login credentials are site-specific and should be different for each installation, due to the nature of the equipment.

Note: The OpenScape Voice screen captures in this chapter were taken from the HiPath Assistant 3.0R0.0.0 Build 860. Depending on your on-site version, the on-screen output may differ.

Assumptions

The integration solution described in this chapter makes the following assumptions about the desired call flow:

- Agent endpoints (SIP Phones) register directly with OpenScape Voice. Genesys SIP Server does not signal these endpoints directly; instead, it always goes through OpenScape Voice.
- A single instance of SIP Server is configured behind OpenScape Voice.
- Stream Manager, if it is used for treatments, music on hold, MCU (Multipoint Conference Unit) recording, and supervisor functionality, is signaled only by SIP Server. No direct SIP signaling occurs between OpenScape Voice and Stream Manager. For information about configuring SIP Server to use Stream Manager, see the *Framework 8.0 SIP Server Deployment Guide*.

In the event that these assumptions are not valid for the required deployment, you can still configure SIP Server for integration with OpenScape Voice; however, you may need to modify the configuration described in this chapter.

To configure multiple instances of SIP Server to work with OpenScape Voice, create a unique Numbering Plan for each SIP Server and each group of agents associated with it, and related switch entities as described in Table 2 on page 16. For example, to configure two SIP Servers, create two unique SIP Server Numbering Plans, two Agent Numbering Plans, and all related switch entities as required for each Numbering Plan.

For GVP integration with SIP Server, the configuration must be performed on the SIP Server side, not on the OpenScape Voice side.

Supported Hardware

Currently, only Siemens optiPoint phones and Siemens OpenStage phones have been tested and approved. If you have any questions about device compatibility, see the *Genesys Supported Media Interfaces* document or ask your Sales Representative.

The Click-to-Answer feature requires OpenScape Voice version 2.2, Patchset 14 or later.

Deployment Architecture

A successful implementation requires that Genesys SIP Server be in the communications path for every call in the contact center—both internal and external (see Figure 1). This can be done efficiently and effectively by using multiple Numbering Plans. Note, however, that gateways should not be put into the Global Numbering Plan. Doing so can cause complications by routing gateway calls directly to the agents, bypassing SIP Server.

In the General Numbering Plan (the Numbering Plan that contains the gateways), the contact center is given a range of numbers for agents (assuming that the agents have direct lines) and Routing Points. Those numbers route directly to SIP Server, which then routes the calls accordingly.

SIP Server must have its own Numbering Plan, because it will make calls on behalf of the agents. These calls are sent to the E.164 Numbering Plan (to reach internal phones), or, if necessary, to available gateways.

The Agent Numbering Plan is simple; all calls go to SIP Server. The configuration of SIP Server will determine how the calls should be routed.

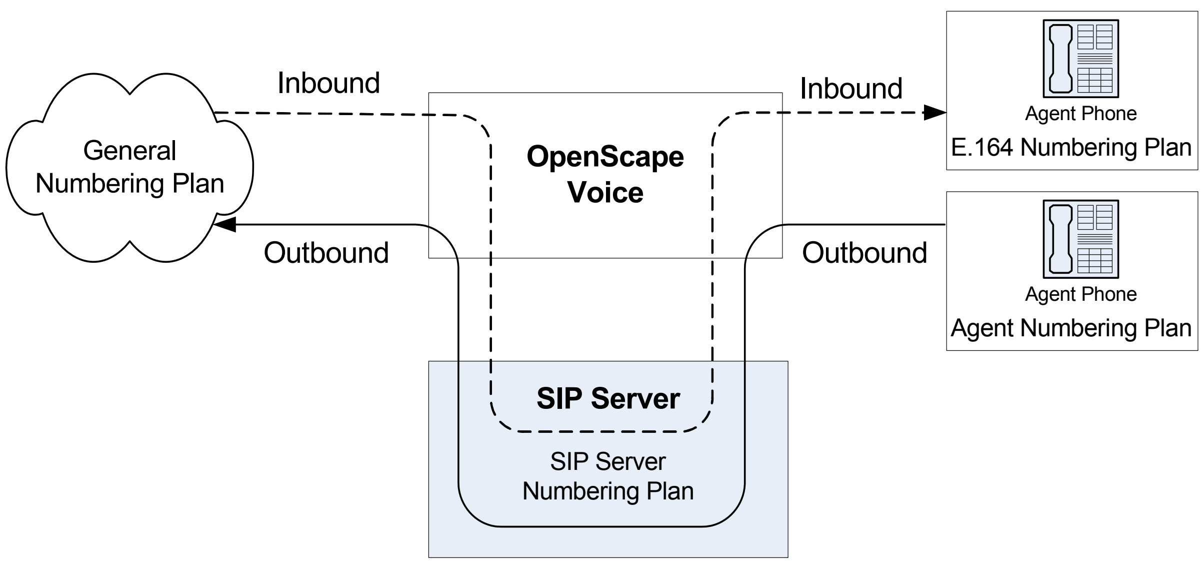

Figure 1: SIP Server - OpenScape Voice Deployment Architecture

Integration Task Summary

Table 1 summarizes the steps that are required in order to integrate SIP Server with OpenScape Voice.

Table 1: Task Summary—Integrating SIP Server with OpenScape Voice

Objective	Related Procedures and Actions
1. Configure OpenScape Voice.	See Table 2.
2. Configure OpenScape Voice DN objects in the Configuration Layer.	See Table 3 on page 48.

Configuring OpenScape Voice

Table 2 provides an overview of the main steps that are required in order to configure OpenScape Voice. Complete all steps in the order in which they are listed.

Table 2: Task Flow—Configuring OpenScape Voice

Objective	Related Procedures and Actions
1. Confirm that OpenScape Voice is functional and routing calls appropriately.	The procedures in this chapter assume that OpenScape Voice is functional and routing calls appropriately. There should already be at least one Numbering Plan that has gateways and non-agent subscribers in it. For more information, see Siemens OpenScape Voice–specific documentation.
2. Configure the Numbering Plans.	Complete the following procedure: • Procedure: Configuring Numbering Plans, on page 18
3. Configure a SIP Server Endpoint Profile.	Complete the following procedure: • Procedure: Configuring a SIP Server Endpoint Profile, on page 20
4. Configure a SIP Server Endpoint.	Complete the following procedure: • Procedure: Configuring a SIP Server Endpoint, on page 22
5. Configure SIP Server Destinations for Gateways.	Complete the following procedure: • Procedure: Configuring SIP Server Destinations for Gateways, on page 25
6. Configure SIP Server Prefix Access Codes.	Complete the following procedure: • Procedure: Configuring SIP Server Prefix Access Codes, on page 29

Table 2: Task Flow—Configuring OpenScape Voice (Continued)

Objective	Related Procedures and Actions
7. Configure SIP Server Destination Codes.	Complete the following procedure: • Procedure: Configuring SIP Server Destination Codes, on page 32
8. Configure Agent Destinations for SIP Server.	Complete the following procedure: • Procedure: Configuring an Agent Destination for SIP Server, on page 34
9. Configure Agent Prefix Access Codes and Destination Codes.	Complete the following procedure: • Procedure: Configuring Agent Prefix Access Codes and Destination Codes, on page 37
10. Configure Click-to-Answer.	Complete the following procedure: • Procedure: Configuring Click-to-Answer, on page 40
11. (Optional) Configure emergency call routing.	Complete the following procedure: • Procedure: Configuring emergency call routing, on page 42

Procedures

This section provides detailed procedures for configuring the various elements required for the OpenScape Voice-SIP Server integration.

Accessing the Configuration Tools of OpenScape Voice

HiPath Assistant

The HiPath Assistant is a thin, Web-based application that runs within a browser to provide a common user experience. It is primarily intended for use as a Service Management Center that provides administrators of communications networks with provisioning information and control over their subscribers' voice services. Its purpose is to provide enterprises with a cost-effective, IP-based system that works seamlessly with OpenScape Voice.

For enterprises with more than 5000 lines, the HiPath Assistant can be installed on an external server as a stand-alone (off-board) installation, separated from the OpenScape Voice switch.

To access the HiPath Assistant, simply enter the following URL in the `Address` text box of Microsoft Internet Explorer:

`https://<IP Address>/.`

Command-Line Interface

OpenScape Voice also has an SSL (Secure Sockets Layer) command-line interface that you can access. SSL is the same as Telnet, except that it is encrypted to provide more security. There are many SSL client applications available on the Web for free, in addition to commercial applications. A common application for SSL is PuTTY. You can download PuTTY from the following web page:

`http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html.`

After you have your SSL application, configure it to connect to the management IP address of OpenScape Voice.

Procedure: Configuring Numbering Plans

Summary

The instructions in this chapter assume that OpenScape Voice is functional and routing calls appropriately. There should already be at least one Numbering Plan with configured gateways and non-agent subscribers.

Purpose: To create the Numbering Plans that will contain the Agents and SIP Server.

Start of procedure

1. Log in to the HiPath Assistant, and navigate to the Business Group of the contact center that you want to configure—for example, `GenesysLab` (see Figure 2).

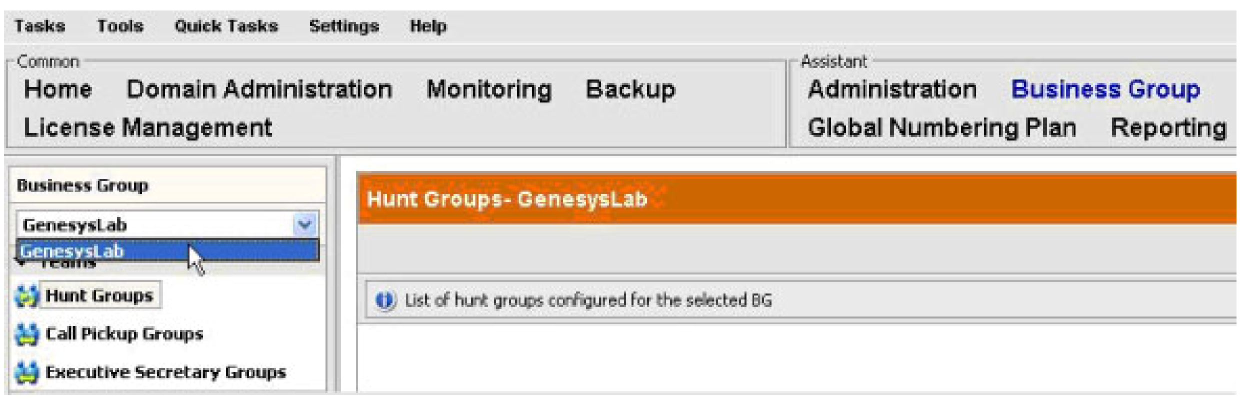

Figure 2: Selecting the Business Group

2. Click `Resources` (see Figure 3).

Figure 3: Selecting Resources

3. Click `Private Numbering Plans` (see Figure 4).

Figure 4: Selecting Private Numbering Plans

4. In the `Private Numbering Plans` dialog box, click `Add`.
5. Add two new Private Numbering Plans: one for your agents and one for SIP Server itself—for example, `AgentNumPlan` and `SIPServerNumPlan` respectively.

   When you are finished, the dialog box shown in Figure 5 appears.

Figure 5: Created Private Numbering Plans

End of procedure

Next Steps

- Procedure: Configuring a SIP Server Endpoint Profile

Procedure:
Configuring a SIP Server Endpoint Profile

Prerequisites

- Procedure: Configuring Numbering Plans, on page 18

Start of procedure

1. Log in to the HiPath Assistant, and navigate to the Business Group of the contact center that you want to configure—for example, `GenesysLab`.
2. Click `Private Numbering Plan`, and then click the SIP Server Numbering Plan—for example, `SIPServerNumPlan` (see Figure 6).

Figure 6: Selecting the Numbering Plan

3. Click `Endpoint Profiles`, and then click `Add` (see Figure 7).

Figure 7: Selecting Endpoint Profiles

4. In the `Endpoint Profile: <Business Group>` dialog box, enter a name for this configured Endpoint Profile in the `Name` text box. This will associate the endpoint that uses it, with the Numbering Plan the Endpoint Profile was created in.
5. (Optional) If there are existing dialing rules and conventions that require the use of Class of Service and Routing Areas, enter that information. As a general rule, give this Endpoint Profile the same calling access as you would give to your agents (see Figure 8).

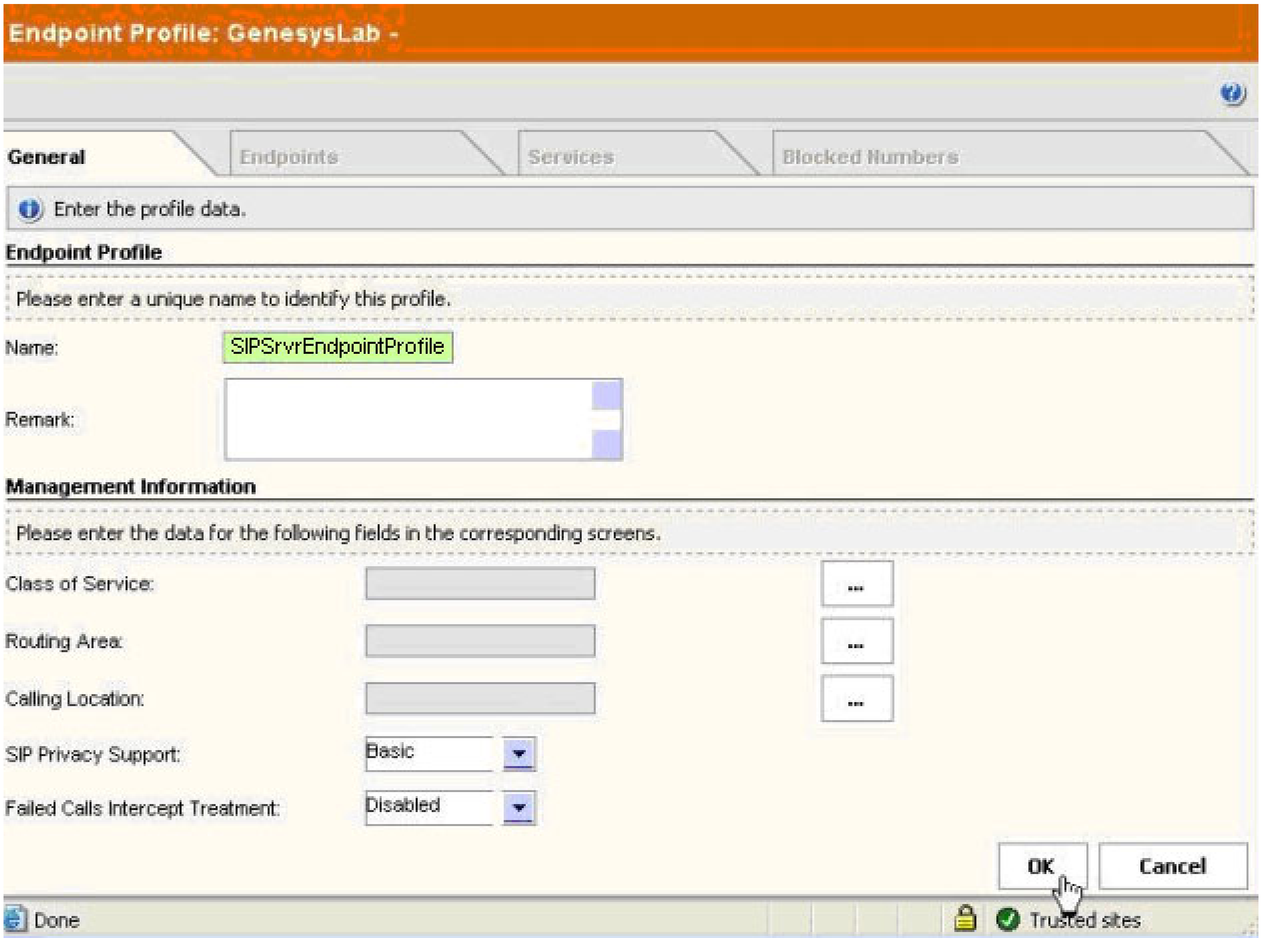

Figure 8: Configuring an Endpoint Profile

6. When you are finished, click `OK`.

End of procedure

Next Steps

- Procedure: Configuring a SIP Server Endpoint

Procedure: Configuring a SIP Server Endpoint

Prerequisites

1. Procedure: Configuring Numbering Plans, on page 18
2. Procedure: Configuring a SIP Server Endpoint Profile, on page 20

Start of procedure

1. Log in to the HiPath Assistant, and navigate to the Business Group of the contact center that you want to configure—for example, `GenesysLab`.
2. Click `Private Numbering Plan`, and then click the SIP Server Numbering Plan—for example, `SIPServerNumPlan`.
3. Click `Endpoints`, and then click `Add` (see Figure 9).

Figure 9: Selecting Endpoints

4. In the `Endpoint: <Business Group>` dialog box, click the `General` tab, and do the following (see Figure 10):
   a. In the `Name` text box, enter a unique name for this configured Endpoint.
   b. Make sure that the `Type` text box is set to `Static`, and that the `Registered` check box is selected.
   c. Set the `Profile` text box to the Endpoint Profile that you created for SIP Server, by clicking the browse (...) button.
   d. In the `Signaling Primary` text box, enter the IP address of SIP Server.
   e. From the `Transport protocol` drop-down box, select `UDP`.
   f. In the `Max. no of sessions` text box, enter `2000`.

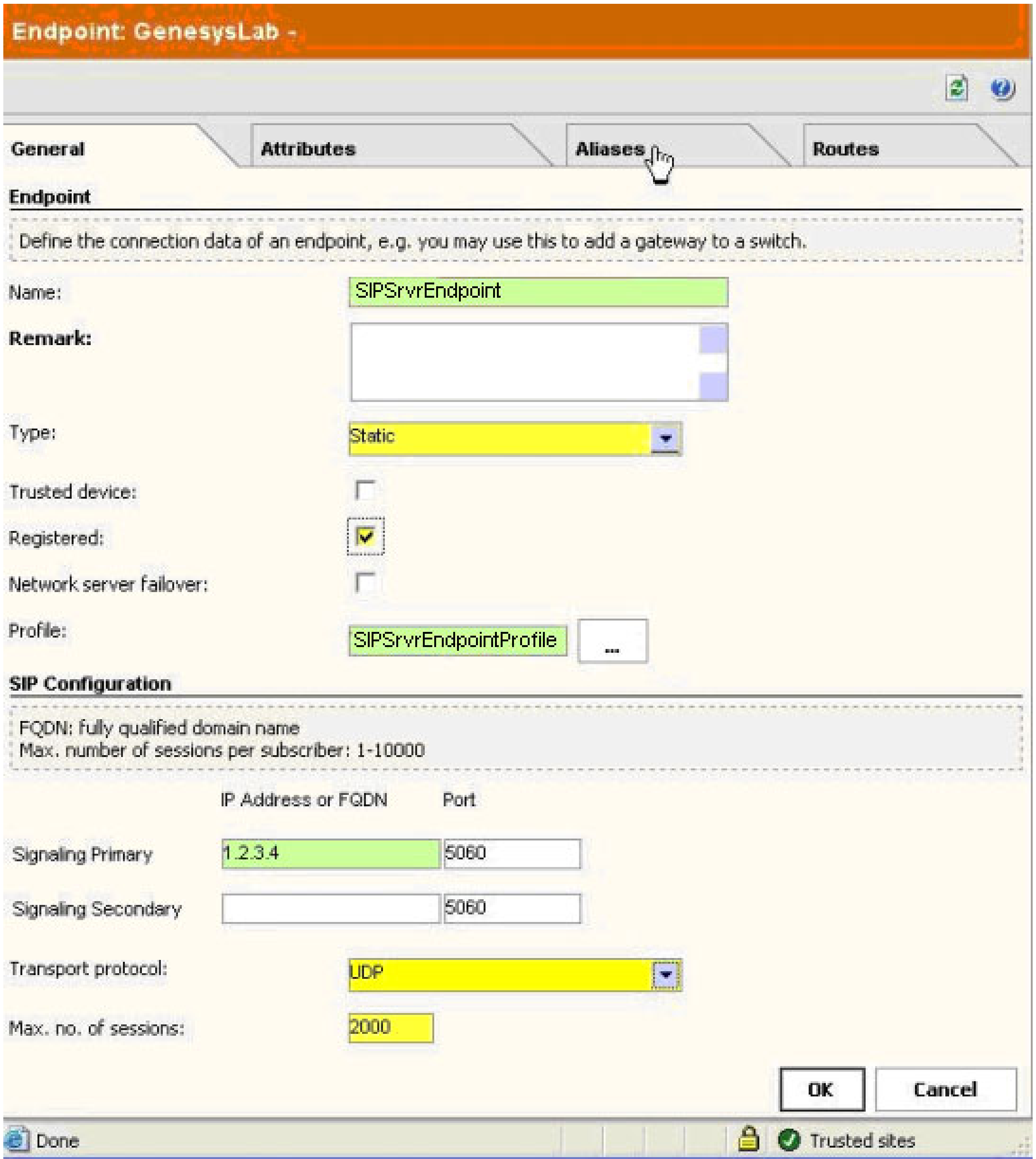

Figure 10: Configuring Endpoints: General Tab

5. Click the `Aliases` tab, and then click `Add`.
6. In the `Alias` dialog box, do the following (see Figure 11):
   a. In the `Name` text box, enter the IP address that you entered in the `Signaling Primary` text box in Step 4.
   b. Set the `Type` text box to `SIP URL`.
   c. Click `OK`.

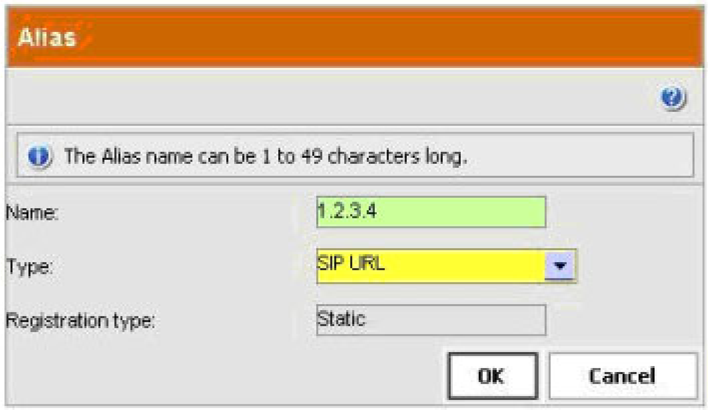

Figure 11: Configuring Endpoints: Aliases Tab

7. In the Endpoint dialog box, click `OK`.
8. When the confirmation message box appears, informing you that the Endpoint was created successfully, click `Close`.

End of procedure

Next Steps

- Procedure: Configuring SIP Server Destinations for Gateways

Procedure:
Configuring SIP Server Destinations for Gateways

Purpose: To create Gateway Destinations for SIP Server to route calls. The Endpoints of such Gateway Destinations must already be configured in OpenScape Voice. SIP Server routes calls to Gateways and to phones. Since calls to the phones are routed via the E.164 Numbering Plan, no Destinations need to be configured for them.

Prerequisites

1. Procedure: Configuring Numbering Plans, on page 18
2. Procedure: Configuring a SIP Server Endpoint Profile, on page 20
3. Procedure: Configuring a SIP Server Endpoint, on page 22

Start of procedure

1. Log in to the HiPath Assistant, and navigate to the Business Group of the contact center that you want to configure—for example, `GenesysLab`.
2. Click `Private Numbering Plan`, and then click the SIP Server Numbering Plan—for example, `SIPServerNumPlan`.

3. Click `Destinations`, and then click `Add` (see Figure 12).

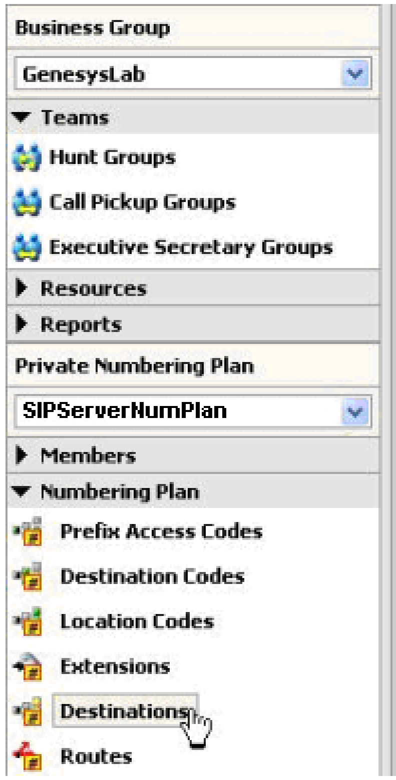

Figure 12: Selecting Destinations

4. In the `Destination` dialog box, on the `General` tab, do the following (see Figure 13):
   a. In the `Name` text box, enter a unique name for the Destination—for example, `Gateway`. The name must be unique within the switch configuration database.
   b. Make sure that all check boxes are cleared.
   c. When you are finished, click `OK`.

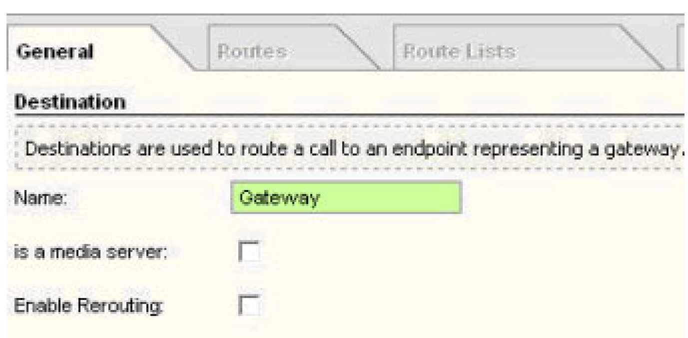

Figure 13: Configuring a Gateway Destination

5. In the `Destination - <Business Group>` dialog box, click the Destination that you just created (see Figure 14).

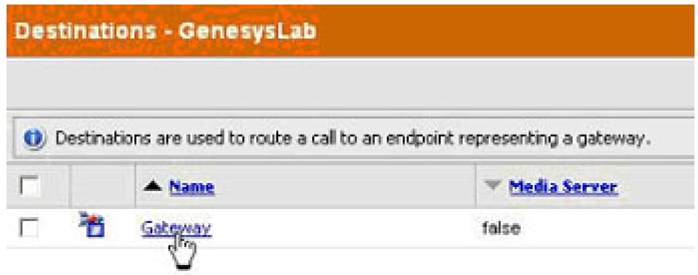

Figure 14: Selecting a Gateway Destination

6. Click the `Routes` tab, and then click `Add`.
7. In the `Route` dialog box, do the following (see Figure 15):
   a. In the `ID` text box, enter `1` for this particular route.
   b. Set the `Type` text box to `SIP Endpoint`.
   c. Set the `SIP Endpoint` text box to the Endpoint that you created in "Configuring a SIP Server Endpoint" on page 22—for example, `SIPSrvrEndpoint`—by clicking the browse (...) button.
   d. (Optional) Modify the dialed digits for the gateway, if necessary. Ideally, you should not need to further modify the digit string for calls being routed from SIP Server. All modifications to the digit string should be completed before the calls arrive to SIP Server.

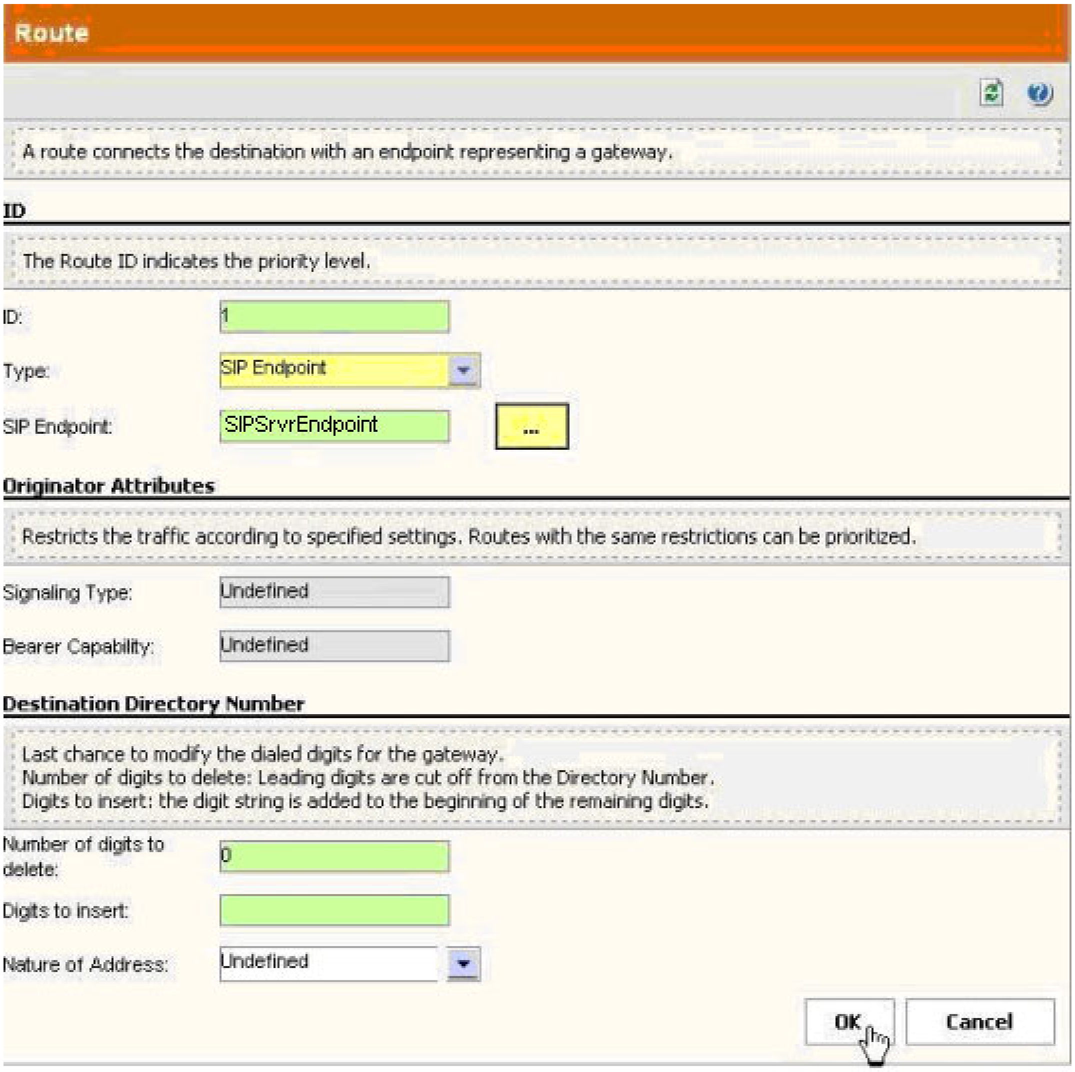

Figure 15: Configuring a Route for a Gateway Destination

8. When you are finished, click `OK`.
9. When the confirmation message box appears, informing you that the Route was added successfully, click `Close`.
10. In the `Destination` dialog box, click `OK`. You will now be able to view the Route that you just created in the `Routes` dialog box.
11. Repeat Steps 3–10 to create other gateway Destinations for SIP Server as necessary.

End of procedure

Next Steps

- Procedure: Configuring SIP Server Prefix Access Codes

Procedure: Configuring SIP Server Prefix Access Codes

Purpose: To configure Prefix Access Codes that SIP Server will dial to reach Subscribers and Gateways.

Start of procedure

1. Log in to the HiPath Assistant, and navigate to the Business Group of the contact center that you want to configure—for example, `GenesysLab`.
2. Click `Private Numbering Plan`, and then click the SIP Server Numbering Plan—for example, `SIPServerNumPlan`.
3. Click `Prefix Access Codes`, and then click `Add` (see Figure 16).

Figure 16: Selecting Prefix Access Codes

4. For calls to be routed to Subscribers: In the `Prefix Access Code: <Business Group>` dialog box, do the following (see Figure 17):
   a. In the `Prefix Access Code` text box, enter the digits you want to use to route calls to Subscribers.

Note: For the SIP Server Numbering Plan, minimal modifications should be required. Dialed numbers should be modified before they reach SIP Server. This convention should be followed at all sites, to simplify the solution as much as possible.

b. Set the `Prefix Type` text box to `Off-net Access`.

c. Set the `Nature of Address` text box to `Unknown`.

d. Set the `Destination Type` text box to `E164 Destination`.

e. Click `OK`.

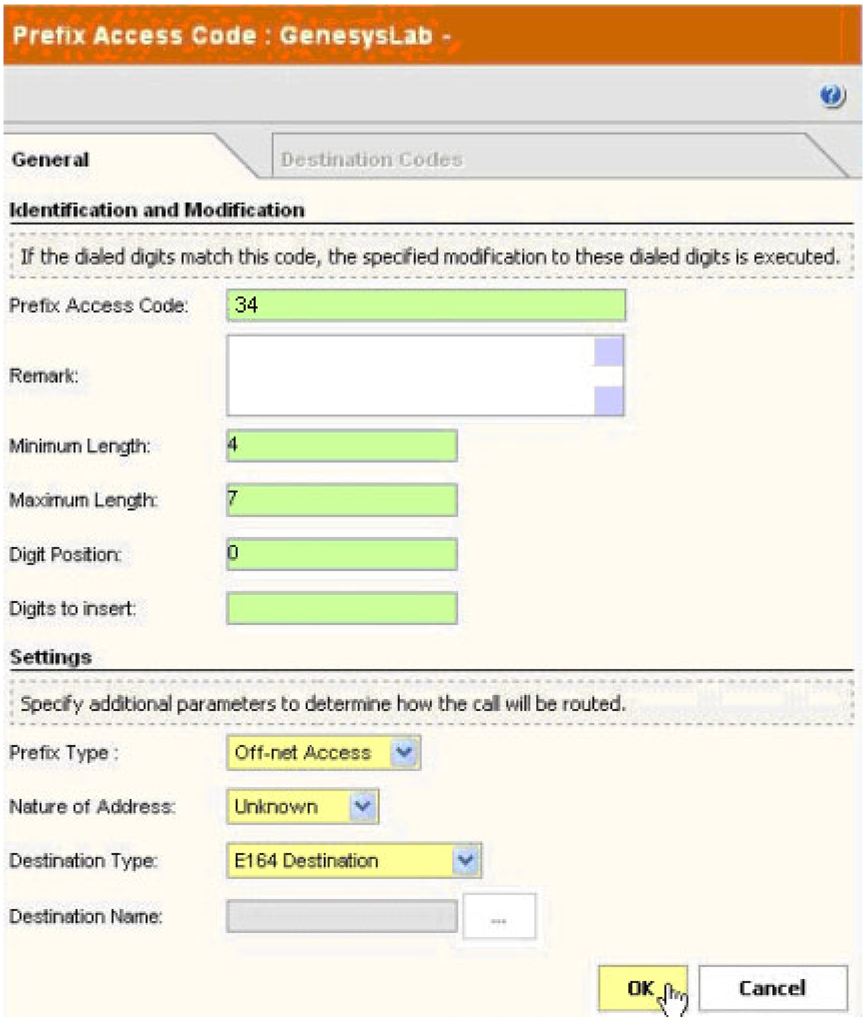

Figure 17: Configuring a Prefix Access Code for Calls Routed to Subscribers

5. When the confirmation message box appears, informing you that the Prefix Access Code was created successfully, click `Close`.

6. In the `Prefix Access Code` dialog box, click `Add`.

7. For calls to be routed to Gateways: In the `Prefix Access Code` dialog box, do the following (see Figure 18):
   a. In the `Prefix Access Code` text box, enter the digits that you want to use to route calls to Gateways. The matched digits will be site-specific, and there should be minimal modification of the digit string.
   b. Set the `Prefix Type` text box to `Off-net Access`.
   c. Set the `Nature of Address` text box to `Unknown`.
   d. Set the `Destination Type` text box to `None`.
   e. Click `OK`.

Note: Some contact centers do not allow their agents to make external calls. If this is true, skip this step.

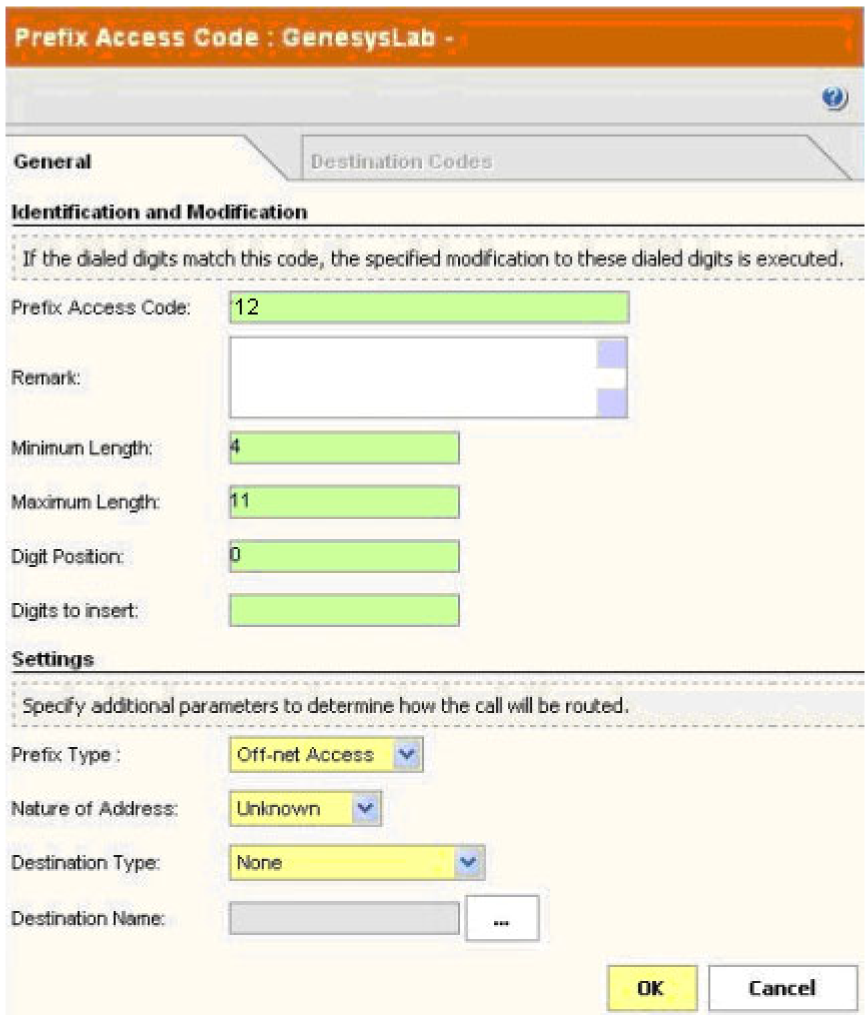

Figure 18: Configuring a Prefix Access Code for Calls Routed to Gateways

8. When the confirmation message box appears, informing you that the Prefix Access Code was created successfully, click `Close`.

End of procedure

Next Steps

Continue with the following procedure, unless calls are routed only to Subscribers:

- Procedure: Configuring SIP Server Destination Codes

Procedure: Configuring SIP Server Destination Codes

Purpose: To configure SIP Server Destination Codes to route calls to non-Subscriber devices.

Start of procedure

1. Log in to the HiPath Assistant, and navigate to the Business Group of the contact center that you want to configure—for example, `GenesysLab`.
2. Click `Private Numbering Plan`, and then click the SIP Server Numbering Plan—for example, `SIPServerNumPlan`.
3. Click `Prefix Access Codes`.
4. Click the Prefix Access Code that you created for non-Subscriber devices (see Figure 19).

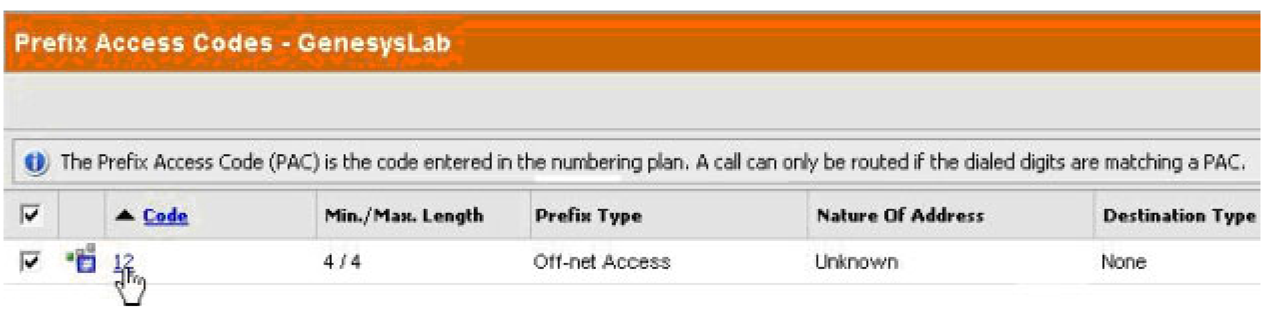

Figure 19: Selecting a Destination Code

5. In the `Prefix Access Code` dialog box, click the `Destination Codes` tab (see Figure 20).

Figure 20: Selecting the Destination Codes Tab

6. In the `Destination Code` dialog box, do the following (see Figure 21):
   a. Set the `Destination Type` text box to `Destination`.
   b. Set the `Destination Name` text box to the Destination that you created for SIP Server in "Configuring SIP Server Destinations for Gateways" on page 25—for example, `Gateway`—by clicking the browse (...) button.
   c. Click `OK`.

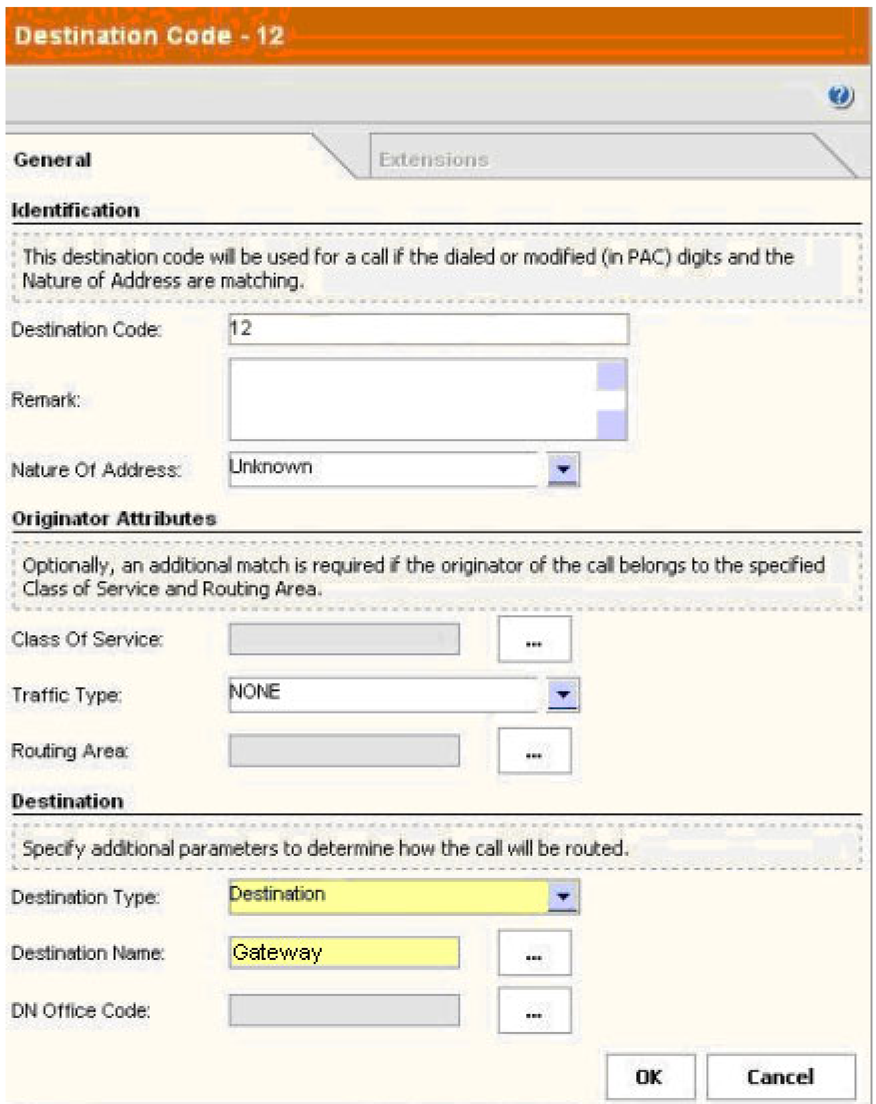

Figure 21: Configuring a Destination Code

7. When the confirmation message box appears, informing you that the Destination Code was created successfully, click `Close`.

End of procedure

Next Steps

- Procedure: Configuring an Agent Destination for SIP Server

Procedure: Configuring an Agent Destination for SIP Server

Purpose: To configure a Destination for the Agent Numbering Plan for SIP Server.

Prerequisites

1. Procedure: Configuring Numbering Plans, on page 18
2. Procedure: Configuring a SIP Server Endpoint Profile, on page 20
3. Procedure: Configuring a SIP Server Endpoint, on page 22

Start of procedure

1. Log in to the HiPath Assistant, and navigate to the Business Group of the contact center that you want to configure—for example, `GenesysLab`.
2. Click `Private Numbering Plan`, and then click the Agent Numbering plan—for example, `AgentNumPlan`.
3. Click `Destinations`, and then click `Add` (see Figure 22).

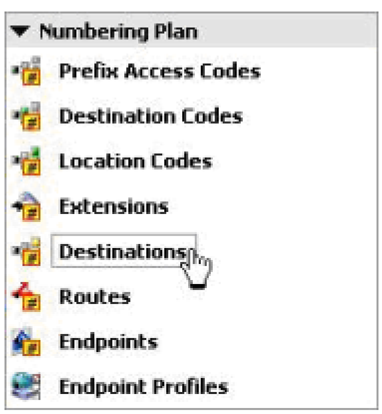

Figure 22: Selecting Destinations

4. In the `Destination - <Agent Numbering Plan>` dialog box, click the `General` tab, and then do the following (see Figure 23):
   a. In the `Name` text box, enter a unique name for the Destination—for example, `SIPServer`.

Note: Destinations must be unique within the switch configuration database, not just within the Numbering Plan and Business Group.

   b. Make sure that all check boxes are cleared.
   c. When you are finished, click `OK`, and then close the dialog box.

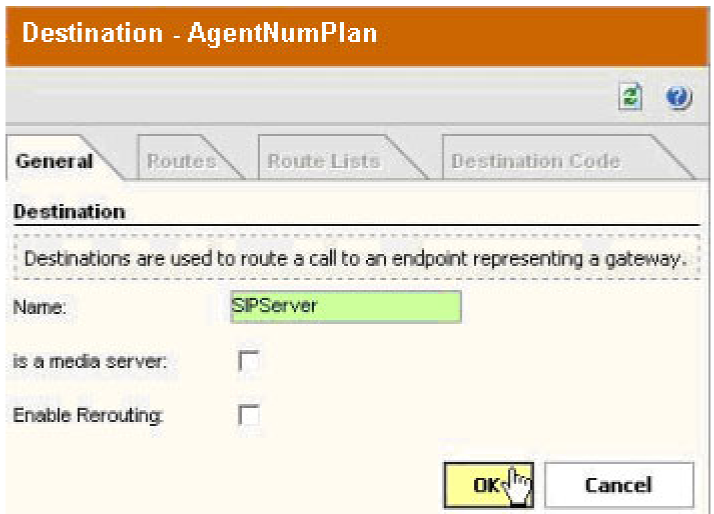

Figure 23: Configuring a SIP Server Destination in the Agent Numbering Plan

5. Click the Destination you just created—for example, `SIPServer`.
6. Click the `Routes` tab, and then click `Add`.
7. In the `Route` dialog box, do the following (see Figure 24):
   a. In the `ID` text box, enter `1`.

Note: The ID of the first Route must always be `1`.

   b. Set the `Type` text box to `SIP Endpoint`.
   c. Set the `SIP Endpoint` text box to the Endpoint that you created for SIP Server in "Configuring a SIP Server Endpoint" on page 22—for example, `SIPSrvrEndpoint`—by clicking the browse (...) button.
   d. When you are finished, click `OK`.

Note: Genesys recommends that you not modify the dialed-digit string that is passed on to SIP Server at this point.

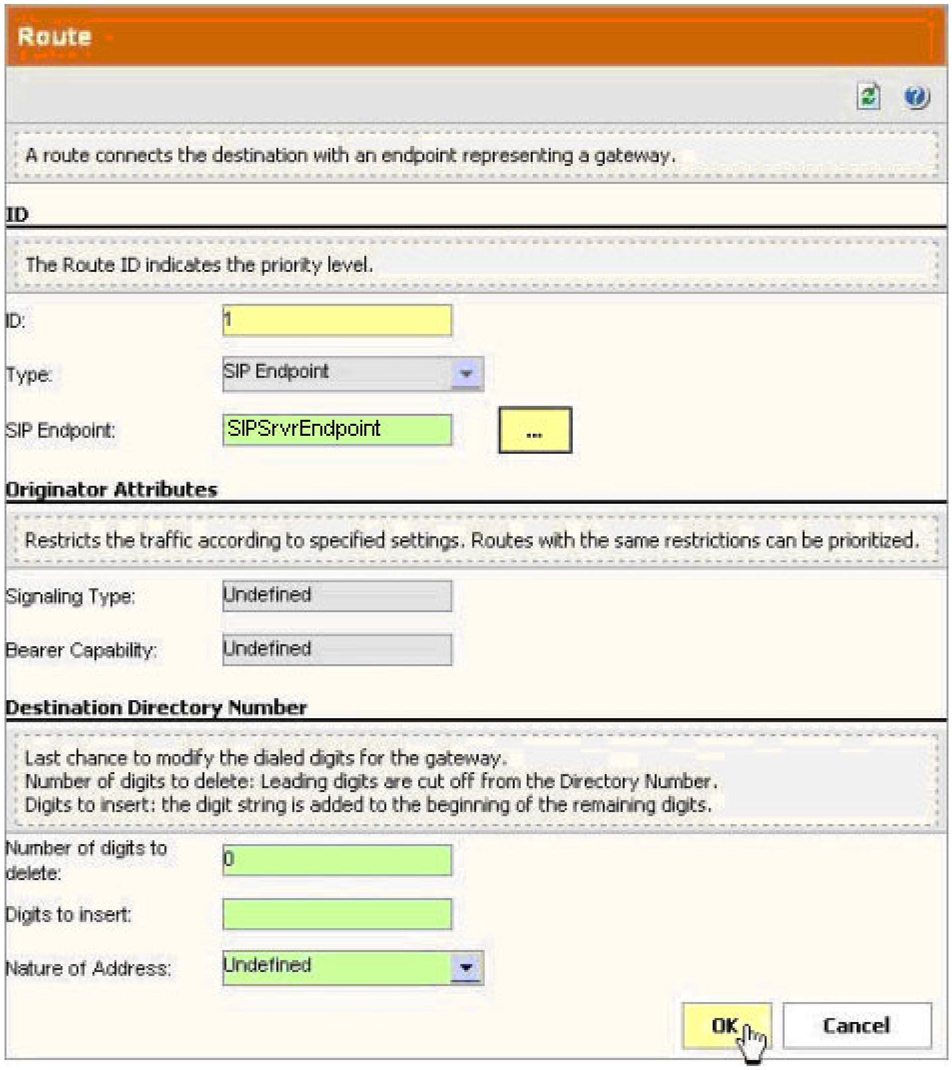

Figure 24: Configuring a Route for SIP Server in the Agent Numbering Plan

8. When the confirmation message box appears, informing you that the Route was added successfully, click `Close`.

End of procedure

Next Steps

- Procedure: Configuring Agent Prefix Access Codes and Destination Codes

Procedure: Configuring Agent Prefix Access Codes and Destination Codes

Summary

In this section, you configure dialing patterns for the Agents. Every number that the agent dials must be configured. If an agent dials a four-digit extension, the Prefix Access Code should be configured to convert the dialed-digit string to the full E.164 code that OpenScape Voice expects. If the agent dials a number that needs to be routed to an external gateway, make sure that the dialed-digit string is correct for that gateway before it reaches SIP Server.

As mentioned earlier, all calls must go to SIP Server first; otherwise, the calls will not be visible to SIP Server. In the Private Numbering Plan for agents, every Prefix Access Code must route the call to a Destination Code that points the call to SIP Server. It is best to copy the non-agent Prefix Access Codes from the General Numbering Plan; however, make sure that the destination is always SIP Server.

Prerequisites

- Procedure: Configuring an Agent Destination for SIP Server, on page 34

Start of procedure

1. Log in to the HiPath Assistant, and navigate to the Business Group of the contact center that you want to configure—for example, `GenesysLab`.
2. Click `Private Numbering Plan`, and then click the Agent Numbering Plan—for example, `AgentNumPlan`.
3. Click `Prefix Access Codes`, and then click `Add`.
4. In the `Prefix Access Code` dialog box, do the following (see Figure 25):
   a. In the `Prefix Access Code` text box, enter the digits you that want to use for routing, and any modifications that OpenScape Voice will need to make in order to route the call properly.
   b. Set the `Prefix Type` text box to `Off-net Access`.
   c. Set the `Nature of Address` text box to `Unknown`.
   d. Set the `Destination Type` text box to `None`.
   e. Click `OK`, and close the dialog box.

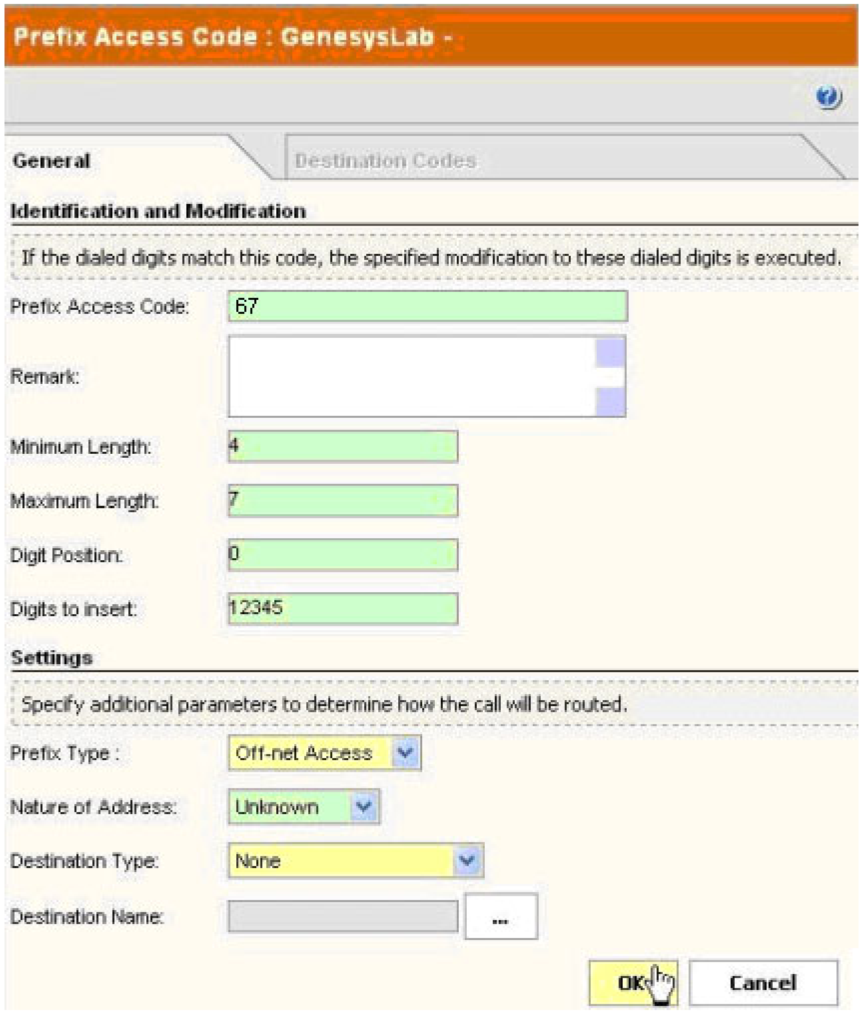

Figure 25: Configuring a Prefix Access Code for the Agent Numbering Plan

5. In the `Prefix Access Code` dialog box, click the Prefix Access Code that you just created, and then click the `Destination Codes` tab (see Figure 26).

Figure 26: Selecting the Destination Codes Tab

6. In the `Destination Code` dialog box, click the `General` tab, and then do the following (see Figure 27):
   a. Do not modify the `Destination Code` text box.
   b. Make sure that the `Nature of Address` text box is set to `Unknown`.

c. Make sure that the `Destination Type` text box is set to `Destination`.

d. Set the `Destination Name` text box to the Destination that you created for SIP Server in "Configuring an Agent Destination for SIP Server" on page 34—for example, `SIPServer`—by clicking the browse (...) button.

e. When you are finished, click `OK`.

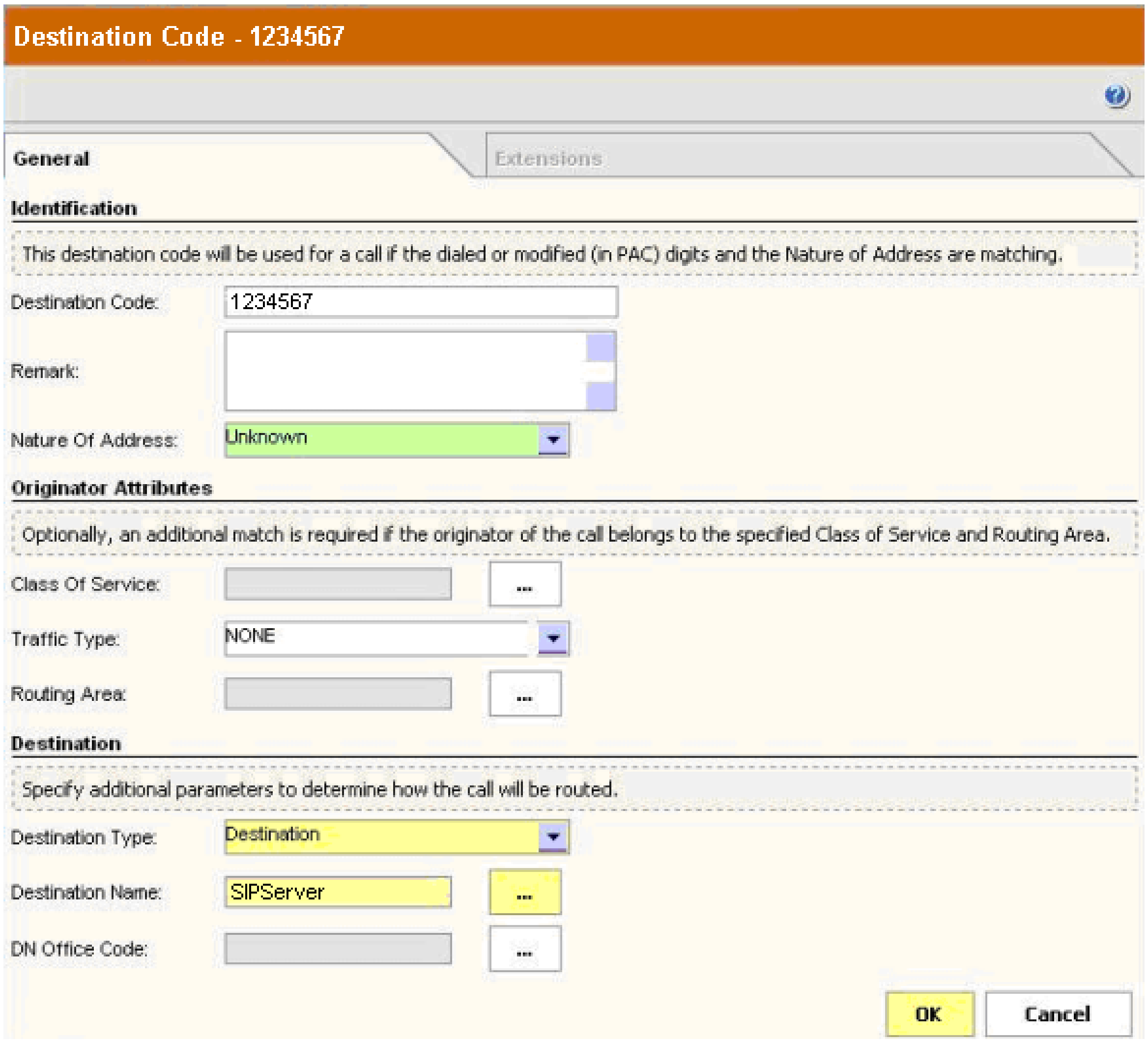

Figure 27: Configuring a Destination Code for the Agent Destination

7. When the confirmation message box appears, informing you that the Destination Code was created successfully, click `Close`.

8. Repeat Steps 3–7 to create other Prefix Access Codes and Destination Codes as necessary.

End of procedure

Next Steps

- Procedure: Configuring Click-to-Answer

Procedure: Configuring Click-to-Answer

Summary

The Click-to-Answer feature enables agents to click within Genesys Agent Desktop to answer the phone.

Notes: The current procedure has been tested only with optiPoint 410 advance, 420 advance, and 410 standard phones running software version 6.0.54. OptiClient “phones” are not supported at this time.

The Click-to-Answer feature requires OpenScape Voice version 2.2, Patchset 14 or later.

Start of procedure

1. Log in to the SSL command-line interface (see “Command-Line Interface” on page 18).
2. Enter `startCli`.
3. Enter `1` to select `Configuration Management`.
4. Enter `1` to select `Configuration Parameters`.
5. Enter `2` to select `getParameterInfo`.
6. At the `name (default: )` prompt, enter the following:

   `Srx/Sip/Profile_validate_based_on_contact`

   You should see the following:

   ```
   name             : Srx/Sip/Profile_validate_based_on_contact
   value            : NO
   type             : PARM_STRING
   usage            : PARM_USAGE_CUSTOMER
   lastUpdateMillis : 19.Sep.2006 14:18:31h (000 msec)
   changeId         : 0
   descriptionString:
   ```

   If you see `value: NO,` as above, continue with the Step 7. If you see `value: Yes,` continue with Step 12.
7. Enter `3` to select `modifyParameter`.
8. At the `name` prompt, enter the following:

```
Srx/Sip/Profile_validate_based_on_contact
```

You should see:

```
invariant settings:
    name               : Srx/Sip/Profile_validate_based_on_contact
    type               : PARM_STRING
    usage              : PARM_USAGE_CUSTOMER
    lastUpdateMillis   : 19.Sep.2006 14:18:31h (000 msec)
    changeId           : 0
    descriptionString:
modifying variable parameters:
    current value: NO
    value <max length: 2047>:
```

9. At the `value <max length: 2047>` prompt, enter `YES`.
10. At the `Do you want to execute this action? (default: yes)` prompt, either enter `yes` or just press `Enter`.
11. Repeat Steps 5 and 6 to verify the configuration parameter value has been changed from `NO` to `YES`.

    Configuration of OpenScape Voice is now complete. You must now configure the phones to enable Click-to-Answer.
12. Go to the `Administrator` menu of the phone you need to configure, and then click `SIP features` (see Figure 28).

Figure 28: Selecting SIP Features on the optiPoint Phone

13. Select the `Auto answer` check box (see Figure 29).

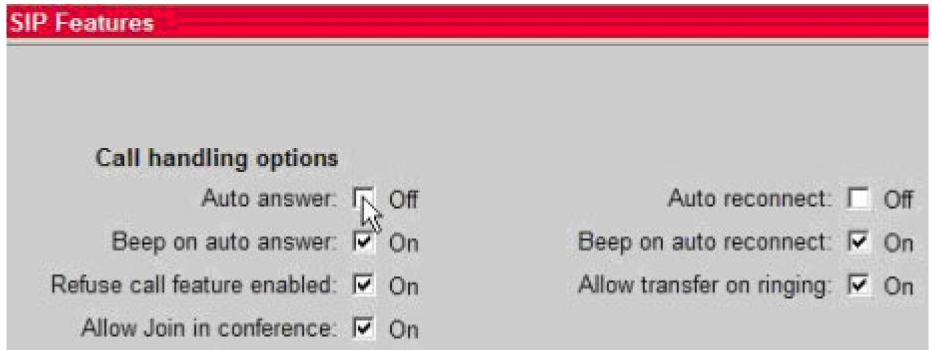

Figure 29: Configuring SIP Features on the optiPoint Phone

14. In the browser window, click `Submit` (see Figure 30).

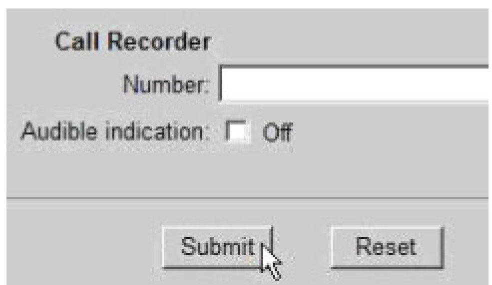

Figure 30: Submitting SIP Features on the optiPoint Phone

15. Repeat Steps 12–14 for every agent phone on the switch.

End of procedure

Procedure: Configuring emergency call routing

Summary

The emergency call routing feature provides alternate call routing in case when SIP Server is unavailable, or if your local emergency (or 911) laws require some form of alternate routing for agents.

During the first 30 seconds after the emergency calling support is activated, calls will fail to route. After that, OpenScape Voice will route calls via the alternate route that you configure and the calls will work.

Start of procedure

1. Log in to the HiPath Assistant, and navigate to the Business Group of the contact center that you want to configure—for example, `GenesysLab`.
2. Click `Private Numbering Plan`, and then click the Agent Numbering Plan—for example, `AgentNumPlan`.
3. Click `Destinations`, and then click `Add`.
4. In the `Destination` dialog box, do the following (see Figure 31):
   a. In the `Name` text box, enter a new destination for the gateway that you want emergency calls to go through—for example, `EmergencyBypass`.
   b. Make sure that all check boxes are cleared.
   c. Click `OK`.

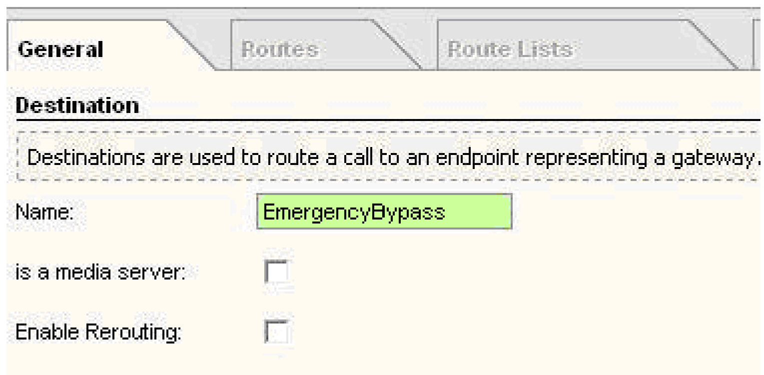

Figure 31: Configuring a Destination for Emergency Call Routing

5. Click the Destination you just created—for example, `EmergencyBypass`.
6. Click the `Routes` tab, and then click `Add`. In this step you are adding a route that goes to SIP Server. This is necessary in order to prevent calls from bypassing SIP Server while it is working.
7. In the `Route` dialog box, do the following (see Figure 32):
   a. In the `ID` text box, enter `1` for this particular route.
   b. Set the `Type` text box to `SIP Endpoint`.
   c. Set the `SIP Endpoint` text box to the Endpoint that you created in "Configuring a SIP Server Endpoint" on page 22—for example, `SIPSrvrEndpoint`.

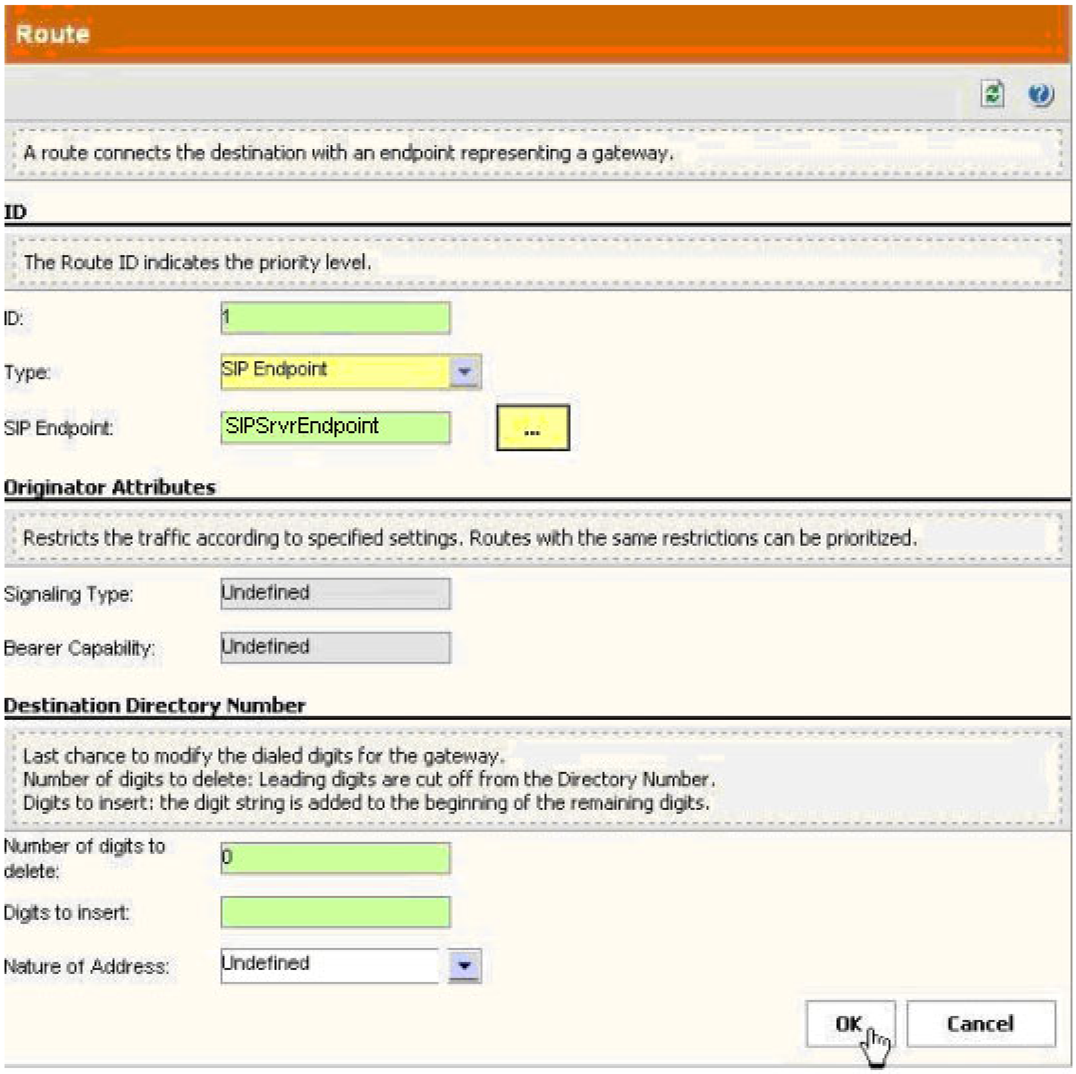

Figure 32: Configuring a Route for a SIP Server Destination

8. When you are finished, click `OK`.
9. Click the Destination you just created—for example, `EmergencyBypass`.
10. Click the `Routes` tab, and then click `Add` again.
11. In the `Route` dialog box, do the following (see Figure 33):
    a. In the `ID` text box, enter `2`.
    b. Set the `Type` text box to `SIP Endpoint`.
    c. Set the `SIP Endpoint` text box to the Gateway that you created in "Configuring SIP Server Destinations for Gateways" on page 25—for example, `Gateway`.
    d. When you are finished, click `OK`.

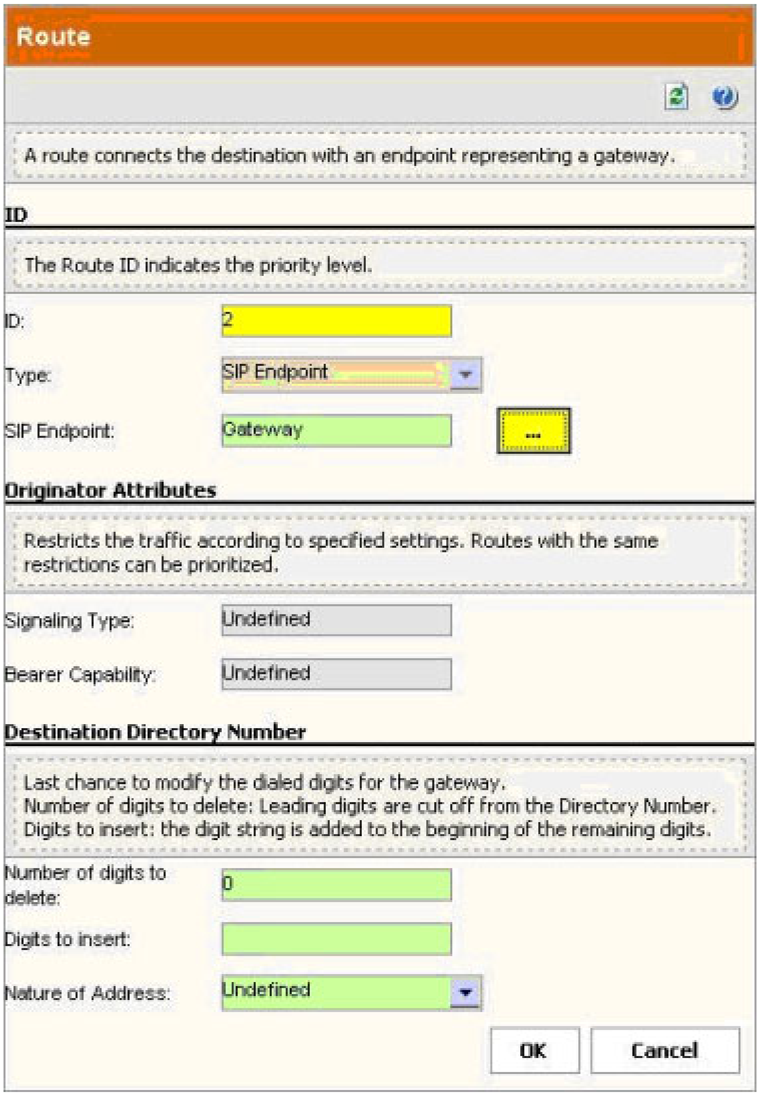

Figure 33: Configuring a Route for Emergency Call Routing

12. Click `Prefix Access Codes`, and then click `Add`.
13. In the `Prefix Access Code` dialog box, do the following (see Figure 34):
    a. In the `Prefix Access Code` text box, enter the digits for your emergency number.
    b. Set the `Prefix Type` text box to `Off-net Access`.
    c. Set the `Nature of Address` text box to `Unknown`.
    d. Set the `Destination Type` text box to `None`.
    e. Click `OK`, and close the dialog box.

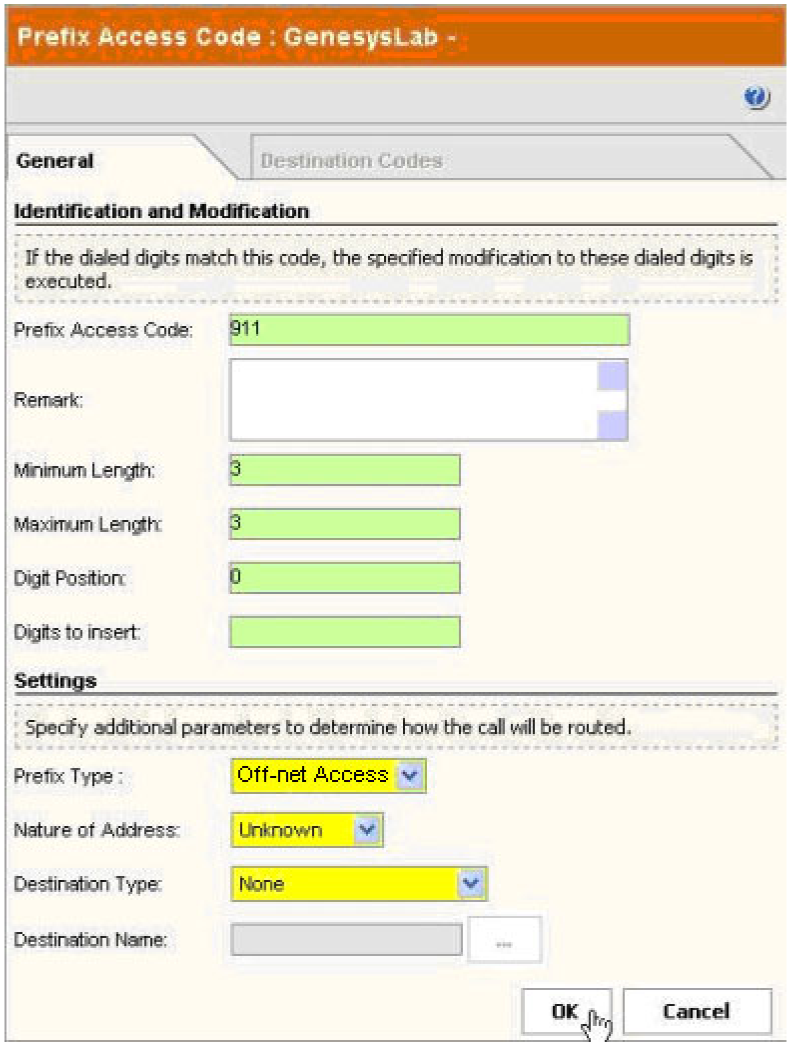

Figure 34: Configuring a Prefix Access Code for Emergency Call Routing

14. In the `Prefix Access Code` dialog box, click the `Destination Codes` tab.

15. On the `General` tab, do the following (see Figure 35):

a. Make sure that the `Destination Type` text box is set to `Destination`.

b. Set the `Destination Name` text box to the Destination that you created in Step 4—for example, `EmergencyBypass`—by clicking the browse (...) button.

c. When you are finished, click `OK`.

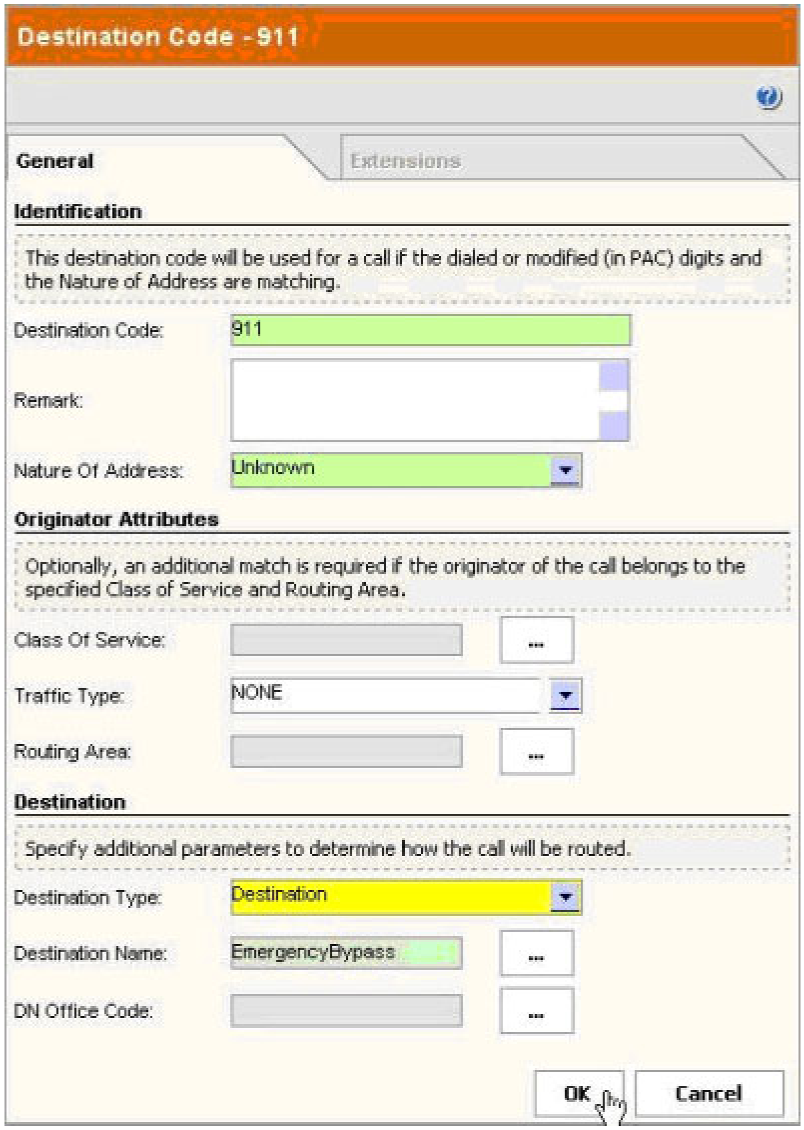

Figure 35: Configuring a Destination Code for Emergency Call Routing

End of procedure

Configuring OpenScape Voice DN Objects

Table 3 provides an overview of the main steps to configure DNs under the OpenScape Voice `Switch` object in the Configuration Layer.

Table 3: Task Flow—Configuring DNs for the OpenScape Voice Switch Object

Objective	Related Procedures and Actions
1. Configure a `Voice over IP Service` DN.	Complete the following procedure: • Procedure: Configuring a Voice over IP Service DN for OpenScape Voice, on page 48
2. Configure a `Trunk` DN.	Complete the following procedure: • Procedure: Configuring a Trunk DN for OpenScape Voice, on page 51
3. Configure `Extension` DNs.	Complete the following procedure: • Procedure: Configuring Extension DNs for OpenScape Voice, on page 53
4. Configure `Routing Point` DNs.	Complete the following procedure: • Procedure: Configuring Routing Point DNs for OpenScape Voice, on page 55

Procedures

You configure DNs for the OpenScape Voice `Switch` object that is assigned to the appropriate SIP Server.

Procedure: Configuring a Voice over IP Service DN for OpenScape Voice

Purpose: To configure a DN of type `Voice over IP Service` that specifies the connection and options for OpenScape Voice communication with a SIP Server running in Application Server (B2BUA) mode.

Start of procedure

1. In Configuration Manager, under a configured `Switch` object, select the `DNs` folder. From the `File` menu, select `New > DN` to create a new `DN` object.
2. In the `New DN Properties` dialog box, click the `General` tab, and then specify the following properties (see Figure 36):
   a. `Number:` Enter the softswitch name—for example, `OpenScape Voice`. Although this name is currently not used for any messaging, it must still be unique.
   b. `Type:` Select `Voice over IP Service` from the drop-down box.

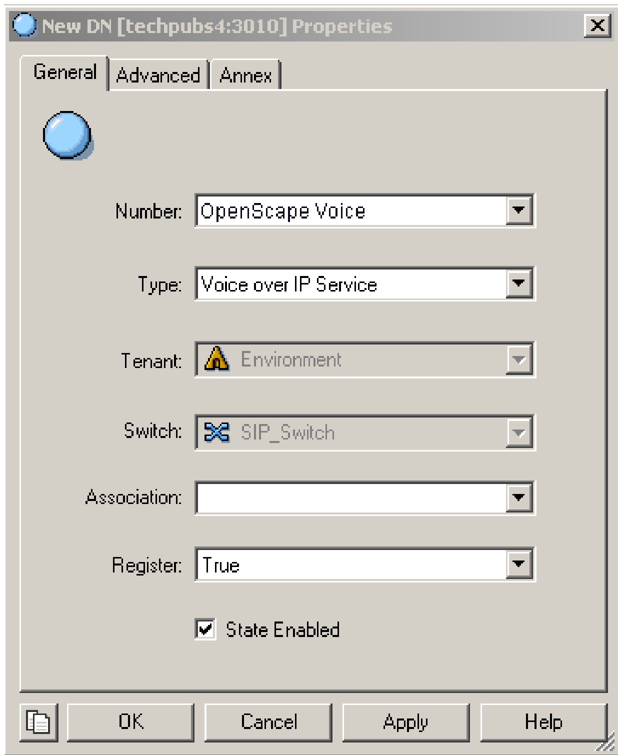

Figure 36: Creating a Voice Over IP Service DN for OpenScape Voice: Sample Configuration

3. Click the `Annex` tab.
4. Create a section named `TServer`. In the `TServer` section, create options as specified in Table 4 (see Figure 37).

Table 4: Configuring a Voice over IP Service DN

Option Name	Option Value	Description
contact	<ipaddress>:<SIP port>	Specifies the contact URI that SIP Server uses for communication with the softswitch, where <ipaddress> is the IP address of the softswitch and <SIP port> is the SIP port number of the softswitch.
dual-dialog-enabled	false	Set this option to false if Siemens optiPoint phones are used in re-INVITE mode for third-party call control (3pcc) operations.
makecall-subst-uname	1, or none	For OpenScape Voice version 2.1, set this option to 1. For OpenScape Voice version 2.2 and later, do not configure this option. When makecall-subst-uname is set to 1, SIP Server sets the From header to the same value as the To header in the INVITE request, to work around issues with pre-2.2 versions of OpenScape Voice.
refer-enabled	false	Set this option to false for SIP Server to use a re-INVITE request method when contacting the softswitch. This is the only method supported in the OpenScape Voice configuration.
service-type	softswitch	Set this option to softswitch.
sip-cti-control	talk	Specifies whether the SIP endpoints support the Broadsoft SIP Extension Event Package. When sip-cti-control is set to talk, SIP Server instructs the endpoint to go off-hook by sending a SIP NOTIFY message with the header Event: talk. This enables a TAnswerCall request to be sent to SIP Server. SIP Server then sends the NOTIFY message to the switch. Setting this option to talk sets the default for all endpoints configured with this softswitch. The value talk is supported only on OpenScape Voice version 2.2 Patchset 14 or later. In addition, Siemens optiPoint hardphones must be version 6.0.54 or later. **Note:** You must also configure OpenScape Voice to support this functionality. See "Configuring Click-to-Answer" on page 40.

5. When you are finished, click Apply (see Figure 37).

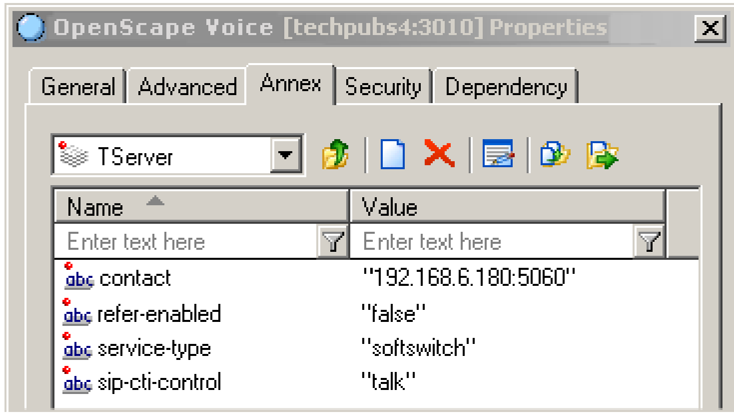

Figure 37: Setting Options for a Voice Over IP Service DN: Sample Configuration

End of procedure

Next Steps

- Procedure: Configuring a Trunk DN for OpenScape Voice

Procedure: Configuring a Trunk DN for OpenScape Voice

Purpose: To configure a DN of type `Trunk` that specifies how SIP Server handles outbound calls. It is also used for configuration of gateways, SIP proxies (including connections to other instances of SIP Server), and other SIP-based applications. From the SIP Server perspective, OpenScape Voice in Application Server (B2BUA) mode is considered a gateway or SIP proxy.

Start of procedure

1. Under a configured `Switch` object, select the `DNs` folder. From the `File` menu, select `New > DN` to create a new `DN` object.
2. In the `New DN Properties` dialog box, click the `General` tab, and then specify the following properties (see Figure 38):
   a. `Number:` Enter a name for the `Trunk` DN. This name can be any unique value, and it can be a combination of letters and numbers.
   b. `Type:` Select `Trunk` from the drop-down box.

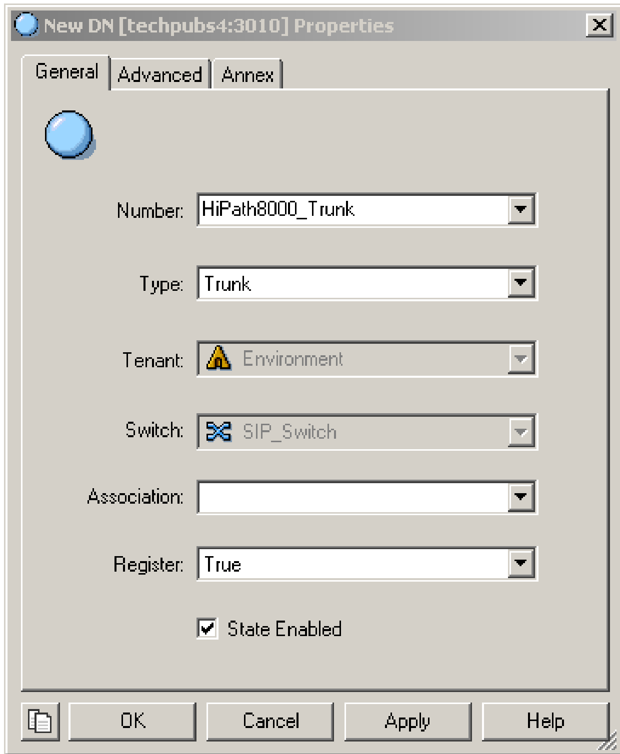

Figure 38: Creating a Trunk DN for OpenScape Voice: Sample Configuration

3. Click the `Annex` tab.
4. Create a section named `TServer`. In the `TServer` section, create options as specified in Table 5 (see Figure 39).

Table 5: Configuring a Trunk DN

Option Name	Option Value	Description
contact	`<ipaddress>:` `<SIP port>`	Specifies the contact URI that SIP Server uses for communication with the softswitch, where `<ipaddress>` is the IP address of the softswitch and `<SIP port>` is the SIP port number of the softswitch.
prefix	Any numerical string	Specifies the initial digits of the number that SIP Server matches to determine whether this trunk should be used for outbound calls. For example, if `prefix` is set to `78`, dialing a number starting with 78 will cause SIP Server to consider this trunk a gateway or SIP proxy. If multiple `Trunk` objects match the prefix, SIP Server will select the one with the longest prefix that matches.

Table 5: Configuring a Trunk DN (Continued)

Option Name	Option Value	Description
refer-enabled	`false`	Set this option to `false` for SIP Server to use a `re-INVITE` request method when contacting the softswitch. This is the only method supported in the OpenScape Voice configuration.
replace-prefix	Any numerical string	Specifies (if necessary) the digits that replace the prefix in the DN. For example, if `prefix` is set to `78`, and `replace-prefix` is set to `8`, the number `786505551212` will be replaced with `86505551212` before it is sent to the gateway or SIP proxy (here, OpenScape Voice).

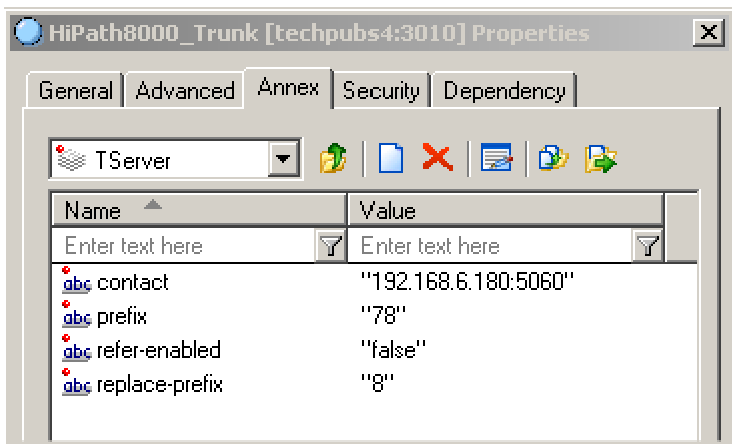

Figure 39: Setting Options for a Trunk DN: Sample Configuration

5. When you are finished, click `Apply`.

End of procedure

Next Steps

- Procedure: Configuring Extension DNs for OpenScape Voice

Procedure: Configuring Extension DNs for OpenScape Voice

Purpose: To configure DNs of type `Extension` that represent agent phone extensions and register directly with the softswitch.

Summary

When you configure an extension where the phone registers directly with SIP Server, you must configure options in the `TServer` section on the `Annex` tab. However, if you are using a softswitch in Application Server (B2BUA) mode, SIP Server takes the `Extension` DN name together with the value of the `contact` option in the softswitch object configuration (not the `Extension` object) to access the phone. This procedure describes the configuration for phones that are registered directly with OpenScape Voice and not with SIP Server. As a result, SIP Server sends the request to OpenScape Voice to communicate with the phone

Start of procedure

1. Under a configured `Switch` object, select the `DNs` folder. From the `File` menu, select `New > DN` to create a new `DN` object.
2. In the `New DN Properties` dialog box, click the `General` tab, and then specify the following properties (see Figure 40):
   a. `Number:` Enter a name for the `Extension` DN. In general, this should be the 10-digit phone number of the extension. You must not use the @ symbol or a computer name. The name of this DN must map to the SIP user name of the extension in OpenScape Voice.
   b. `Type:` Select `Extension` from the drop-down box.

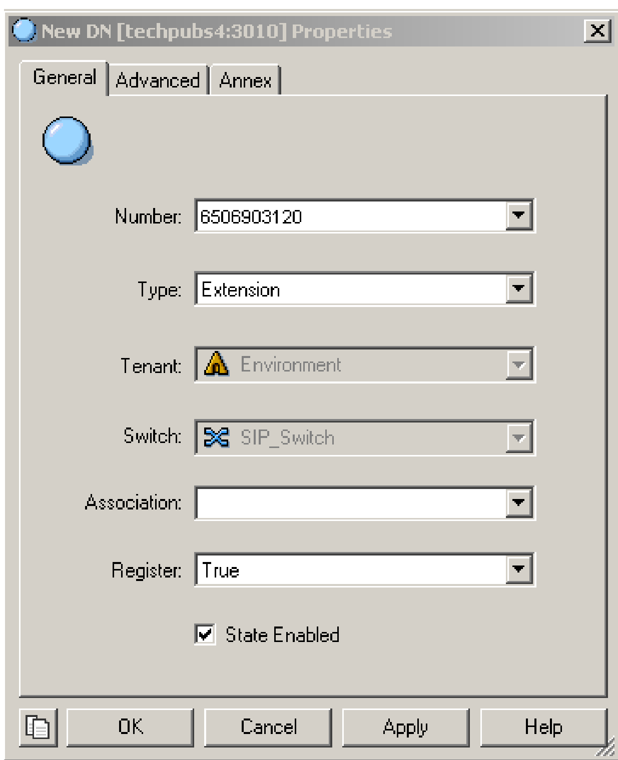

Figure 40: Creating an Extension DN for OpenScape Voice: Sample Configuration

3. When you are finished, click `Apply`.

   No configuration options are required for the `Extension` DN. Adding configuration options, such as `contact`, `password`, `refer-enabled`, and others may cause unexpected results.

End of procedure

Next Steps

- Procedure: Configuring Routing Point DNs for OpenScape Voice

Procedure: Configuring Routing Point DNs for OpenScape Voice

Purpose: To configure a DN of type `Routing Point` that is used to execute a routing strategy with Genesys URS. When SIP Server receives an `INVITE` request on a DN that is configured as a Routing Point, it sends an `EventRouteRequest` message to URS.

Start of procedure

1. Under a configured `Switch` object, select the `DNs` folder. From the `File` menu, select `New` > `DN` to create a new `DN` object.
2. In the `New DN Properties` dialog box, click the `General` tab, and then specify the following properties (see Figure 41):
   a. `Number`: Enter a number for the `Routing Point` DN. This number must be configured on OpenScape Voice.
   b. `Type`: Select `Routing Point` from the drop-down box.

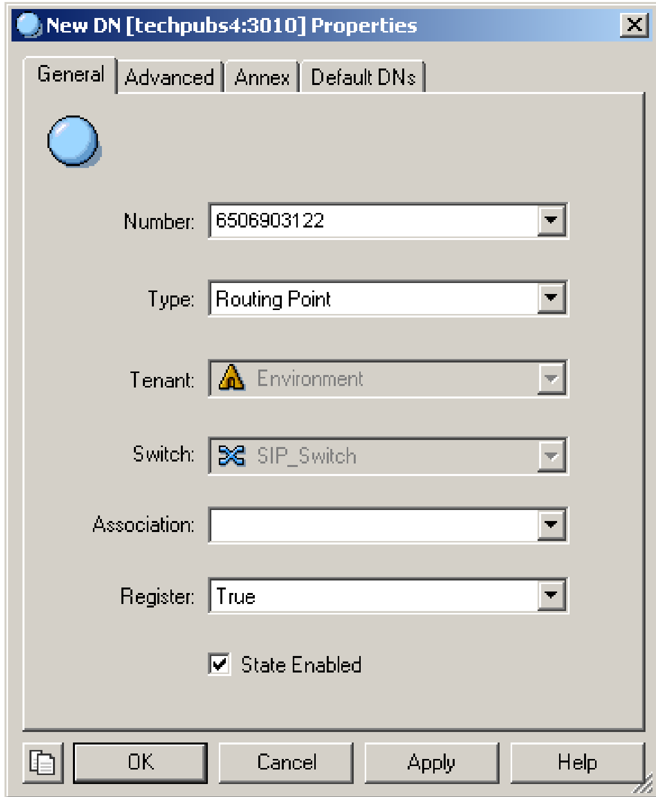

Figure 41: Creating a Routing Point for OpenScape Voice: Sample Configuration

3. When you are finished, click `Apply`.

   Although no configuration options are required for the Routing Point, URS does look at options to determine how to handle the Routing Point and what strategy is currently loaded. For details about these options, see the *Genesys 8.0 Universal Routing Server Reference Guide*.

End of procedure

Chapter

2 SIP Server Integration with Asterisk

This chapter describes how to integrate SIP Server with the Asterisk switch. It contains the following sections:

Note: The instructions in this chapter assume that both Asterisk and SIP Server are fully functional as stand-alone products. The instructions only highlight modifications to the existing configuration to make these products work as an integrated solution.

Overview

Asterisk integrated with SIP Server can function in three different roles:

- As a PBX with a business call routing capability.

  Asterisk is configured to send business calls to SIP Server to engage a Genesys routing solution. SIP Server uses the routing results to forward the call to the selected agent.

- As a voice mail server.

  SIP Server uses Asterisk as a voice mail server. Unanswered calls are forwarded to Asterisk to record the voice messages. Contact center agents receive indication on their T-Library agent desktops about new voice messages waiting in their voice mail box. Agents can access and manage their voice mail boxes hosted on Asterisk.

- As a media server.

SIP Server uses Asterisk as a Media Server. Asterisk is engaged in the call to perform one of the following functions:

- Call recording
- Announcement or music playing
- DTMF digits collection
- Conferences

Asterisk with a Business Call Routing Capability

Figure 42 depicts a sample deployment architecture of SIP Server with Asterisk, in which:

- Asterisk is connected to the network via a SIP gateway.
- The agent endpoint is registered on Asterisk.
- The agent endpoint is associated with a T-Library desktop application.

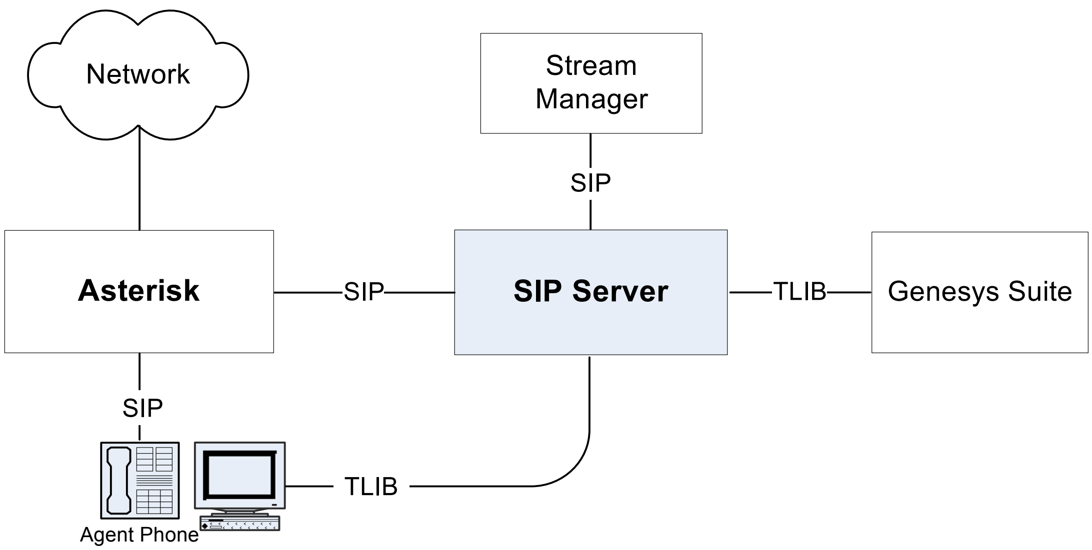

Figure 42: SIP Server - Asterisk Deployment Architecture

Integration with the Asterisk switch relies on the SIP presence subscription from SIP Server. For any call handled by the agent endpoint, Asterisk is requested to provide a notification about the status change for that endpoint. SIP Server uses those notifications to synchronize an agent state visible to all Genesys T-Library clients with the actual state of this agent. The business call routing solution that is built on these integration principles involves SIP Server to handle the business calls only. Private calls are processed locally on Asterisk. Agent statuses are reported to SIP Server for all call types, because they are used to identify the agents' availability for the Genesys Routing Solution.

All figures in this chapter depicting Stream Manager refer to the Genesys Stream Manager. This component, when working together with SIP Server, provides different kinds of media services, such as ring-back, music-on-hold, DTMF digit collection, and others. You can also configure Asterisk to work as a media server for SIP Server. For information about architectural and configuration details of this solution, see “Asterisk as a Media Server” on page 92.

Private Calls

An Asterisk dialing plan can be set up in such a way that private calls (direct calls to an agent, for example) are not forwarded to SIP Server. Instead, only the notification about the busy status of the endpoint is passed to SIP Server. SIP Server uses this status change notification to set the endpoint DN to a busy state (`EventAgentNotReady`), so that the rest of the Genesys suite will not consider that DN available for the routing of contact center calls.

Figure 43 illustrates the processing of private calls.

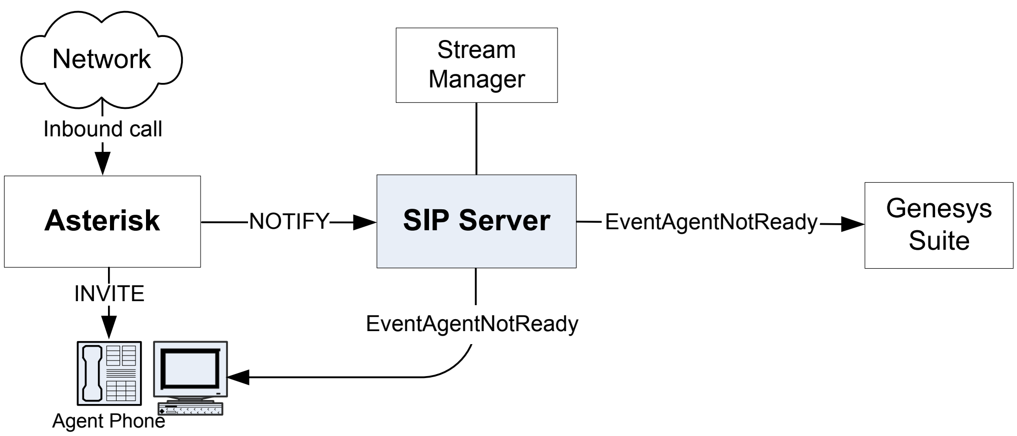

Figure 43: Private Call Processing

Contact Center Calls

In the same way that you can set up an Asterisk dialing plan to bypass SIP Server for private calls, you can write rules so that Asterisk connects contact center calls (typically, calls to the service number of the company) to SIP Server. After that, SIP Server triggers a strategy for Universal Routing Server (URS) to process this type of call. Eventually, an agent DN is selected to handle the customer call and SIP Server initiates a new dialog to Asterisk for the selected endpoint. Finally, Asterisk delivers the call to the agent endpoint.

This mechanism creates a signaling loop inside SIP Server, which is then in charge of maintaining the inbound leg from Asterisk (customer leg) with the outbound leg to Asterisk (agent leg).

Note: From the Asterisk perspective, the two legs are two completely separate calls. Correlation is performed at the SIP Server level.

By staying in the signaling path, SIP Server detects any change in call status, and can therefore produce call-related events (EventRinging, EventEstablished, EventReleased, and so on).

Any call control operation from the agent must be performed using a third-party call control (3pcc) procedure. In other words, the agent desktop must be used for any call control operation (besides the answer call operation). This includes, but is not limited to, hold, transfer, and conference requests.

Figure 44 illustrates the processing of contact center calls.

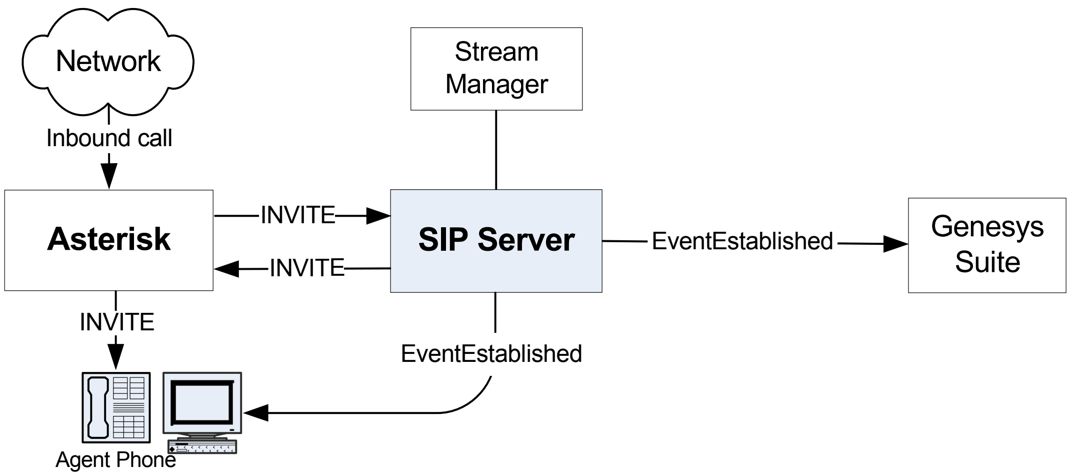

Figure 44: Contact Center Call Processing

Call Flows

Subscription

At startup, SIP Server sends SUBSCRIBE messages to the Asterisk switch, which notifies about changes in the endpoints' status. The Asterisk switch sends NOTIFY messages to SIP Server to report the endpoints' status. See Figure 45.

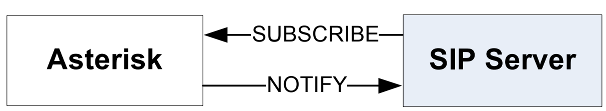

Figure 45: Presence Subscription from SIP Server

If an endpoint is not yet registered, the Asterisk switch reports its status as closed. As soon as the endpoint registers, Asterisk sends a NOTIFY message to SIP Server, reporting the status open. See Figure 46.

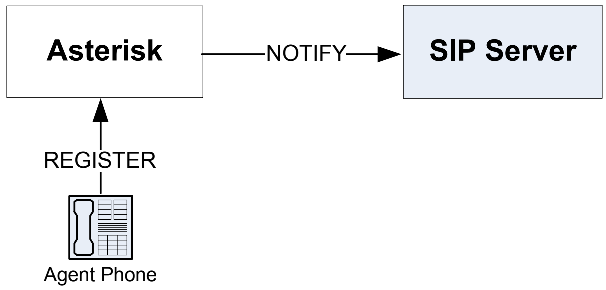

Figure 46: Presence Notification to SIP Server

Private Calls

For private calls, the Asterisk dialing plan is set up in such a way that the call is sent directly to the endpoint. Asterisk notifies SIP Server about the call activity on that particular endpoint. In this case, SIP Server generates `EventAgentNotReady`, which reports the overall agent status as unavailable for contact center calls. (See Figure 43 on page 59.)

SIP Server generates only agent-related TEvents for the private Asterisk calls—for example, `EventAgentReady` and `EventAgentNotReady`. Call-related events—such as `EventRinging`, `EventEstablished`, and so on—are not generated for private calls, because SIP Server is not involved in the processing of private calls.

As soon as the call is released at the endpoint, Asterisk notifies SIP Server, which then generates an `EventAgentReady` message. The agent is then considered available for contact center calls.

Note: The mechanism for private outbound call processing is exactly the same. SIP Server receives the `NOTIFY` messages sent by Asterisk.

Contact Center Calls

Inbound Calls to SIP Server

Inbound contact center calls are programmed within the Asterisk dialing plan to be directed to SIP Server. In this case, the call arrives at a Routing Point, and URS is triggered. You can request a call treatment (using the `TApplyTreatment` request) to play announcement or music. If Stream Manager is configured to provide a treatment functionality, SIP Server connects a caller to Stream Manager to listen to the treatment while waiting for an agent to become available. See Figure 47.

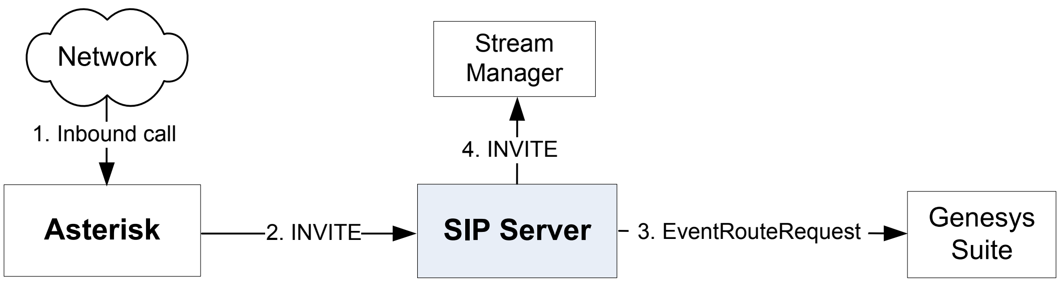

Figure 47: Handling Contact Center Calls

Whenever the agent becomes ready, SIP Server receives a `TRouteCall` request to the targeted agent endpoint. Because this endpoint is configured to point to Asterisk, SIP Server then initiates a new dialog with Asterisk to engage the agent. Asterisk forwards the call to the specified endpoint and reports to SIP Server the call activity on that endpoint with a `NOTIFY` message (`EventAgentNotReady`). When the call is answered, Stream Manager is disconnected, and the original SIP dialog is renegotiated between SIP Sever and Asterisk.

Because SIP Server is in the signaling path for contact center calls, it generates all call-related events (`EventRinging`, `EventEstablished`, and so on) for the agent's DN. See Figure 48.

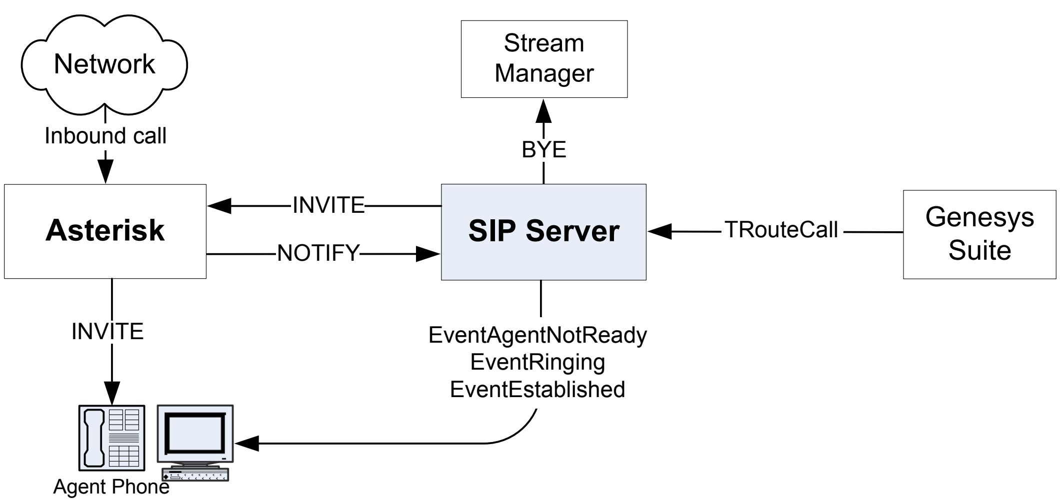

Figure 48: Delivering the Call to the Agent

Furthermore, when the call is released, SIP Server also generates `EventReleased`, and Asterisk notifies SIP Server with a `NOTIFY` message (`EventAgentReady`). See Figure 49.

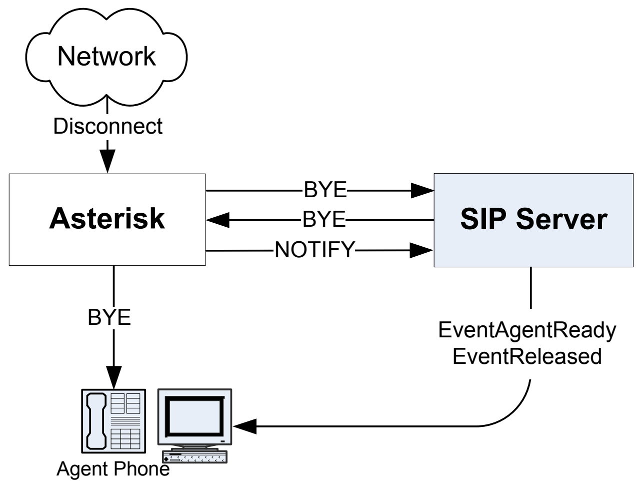

Figure 49: Contact Center Call Disconnection

Inbound Calls to Extensions

Inbound contact center calls, and manual internal first-party call control (1pcc) calls that are directed to extensions, are not visible to SIP Server; as a result, you cannot make third-party call control (3pcc) calls for them. Only inbound calls that are directed to Routing Points on SIP Server, and manual internal calls, which go via Routing Points can be seen by SIP Server; as a result, 3pcc calls can be made for them.

Outbound Calls

An outbound call that is contact-center-related (for example, a call back to a customer) must be performed using 3pcc operations. This ensures that SIP Server creates and controls the SIP dialogs on behalf of the agent endpoint. SIP Server uses the call flow 1 described in RFC 3725 to create a call initiated from the agent's T-Library client using the `TMakeCall` request.

An agent initiates the outbound call by sending the `TMakeCall` request from the T-Library client to SIP Server. SIP Server attempts to engage the agent by sending the `INVITE` message to this agent endpoint (via Asterisk).

Note: If the phone is not configured with auto-answer, the agent must manually answer the call. This is the only manual action that is required for contact center calls.

If Stream Manager is configured to provide treatments, then SIP Server connects the agent to Stream Manager to listen to a ringback tone while establishing a connection to the outbound call destination. See Figure 50.

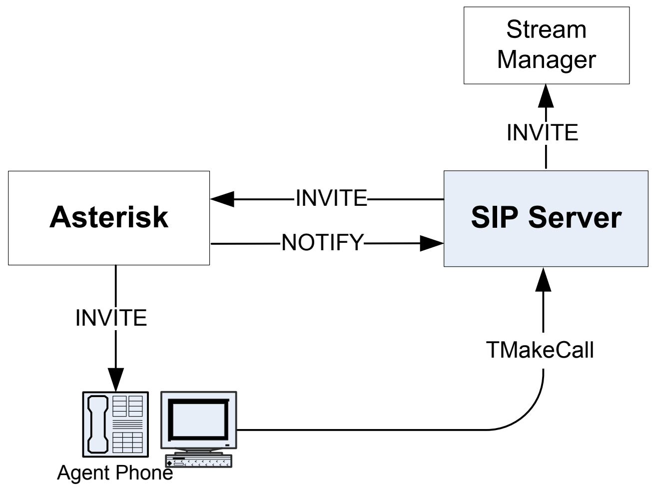

Figure 50: Engaging the Agent Endpoint for an Outbound Call

SIP Server contacts the requested destination number. After the destination answers the call, SIP Server discontinues the ringback tone (by sending the `BYE` message to Stream Manager) and renegotiates with the agent endpoint (via Asterisk), so that the media stream is connected between the agent and the customer. See Figures 51.

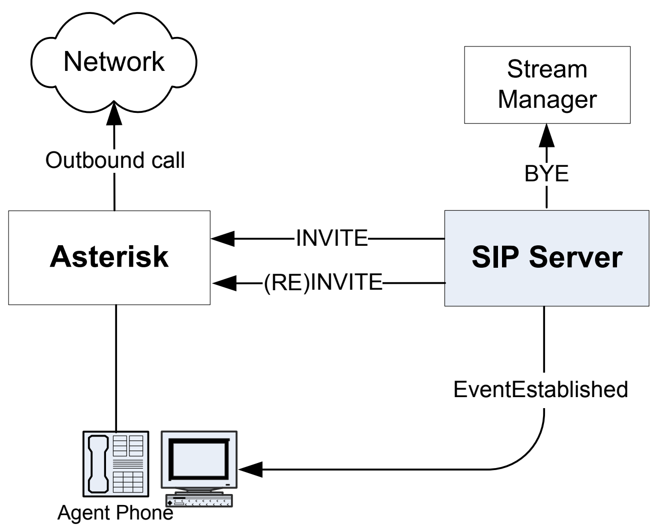

Figure 51: Connecting to the Customer

Although disconnection would work if it were initiated directly from the agent endpoint, it is good practice to always use a desktop application to perform any actions related to contact center calls. Therefore, the disconnection is requested by sending the `TReleaseCall` request to SIP Server.

SIP Server manages two dialogs: one for the agent and another for the customer. It sends the `BYE` message to both of them, and the call is eventually disconnected. See Figures 52.

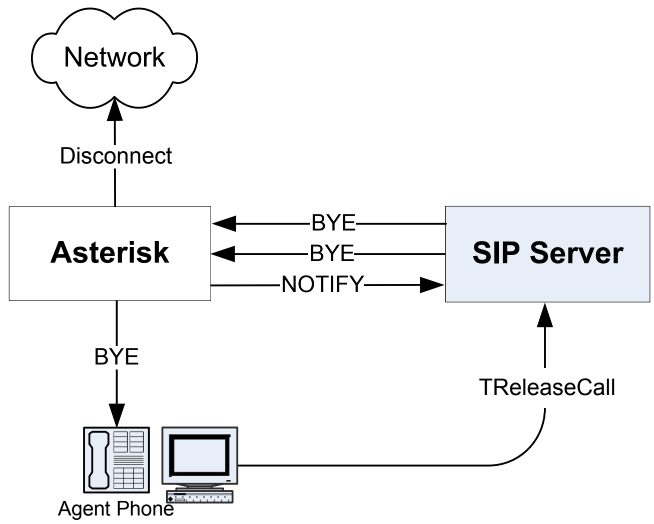

Figure 52: Outbound Call Disconnection

Asterisk as a Voice Mail Server

Asterisk can provide the voice mail server functionality. A stand-alone Asterisk solution allows all agents registered on Asterisk to use multiple voice mail boxes. SIP Server integration with Asterisk adds several new voice-mail-related features to the standard Asterisk set:

1. Agents registered on SIP Server (an agent VOIP phone sends the SIP `REGISTER` message to SIP Server) can use voice mail boxes hosted on Asterisk.
2. All agents (registered on Asterisk or on SIP Server) can receive voice mail notifications on their T-Library client desktops.
3. Voice mail boxes can be associated with extensions, agent logins, and agent groups.

Voice Mail Boxes For Agents Registered on SIP Server

One or multiple voice mail boxes can be created on Asterisk for the agents registered on SIP Server. All voice mail features configured on Asterisk become available for SIP Server agents. Unanswered calls can be forwarded to the corresponding voice mail box allowing callers to leave a voice message. SIP Server agents can call their voice mail boxes from their VOIP phones to listen to the voice messages and to manage the voice mail box.

Voice Mail Notifications Sent to SIP Server T-Library Clients

Genesys contact center agents use T-Library client desktops. If Asterisk is configured as a voice mail server for SIP Server, agents can receive notifications about the new voice messages left in their voice mail boxes on their T-Library client desktops. These notifications also provide information about the number of old and new messages stored in the voice mail box.

Voice Mail Boxes Associated with Extensions, Agent Logins, or Agent Groups

SIP Server associates each voice mail box it controls on Asterisk with one of the following configuration objects in the Configuration Layer: `Extension`, `Agent Login`, or `Agent Group`. The voice mail box associated with a corresponding object defines a group of SIP Server T-Library clients to receive voice mail status notifications for a particular voice mail box. Voice mail notifications described in this section are transmitted using the T-Library interface. SIP Server sends messages to its T-Library clients.

If the voice mail box is associated with an extension, then notifications are sent to an agent whose T-Library client is registered to this extension. If the voice mail box is associated with the agent login, then SIP Server sends voice mail notifications to this agent T-Library client. In this case, it does not matter what DN this agent used to log in.

It is also possible to associate a voice mail box with the agent group. If a new voice message is left in such a voice mail box, then all logged in agents associated with this agent group will receive a notification about this message.

Call flows

Figure 53 illustrates a general integration schema representing Asterisk configured as a voice mail server for SIP Server.

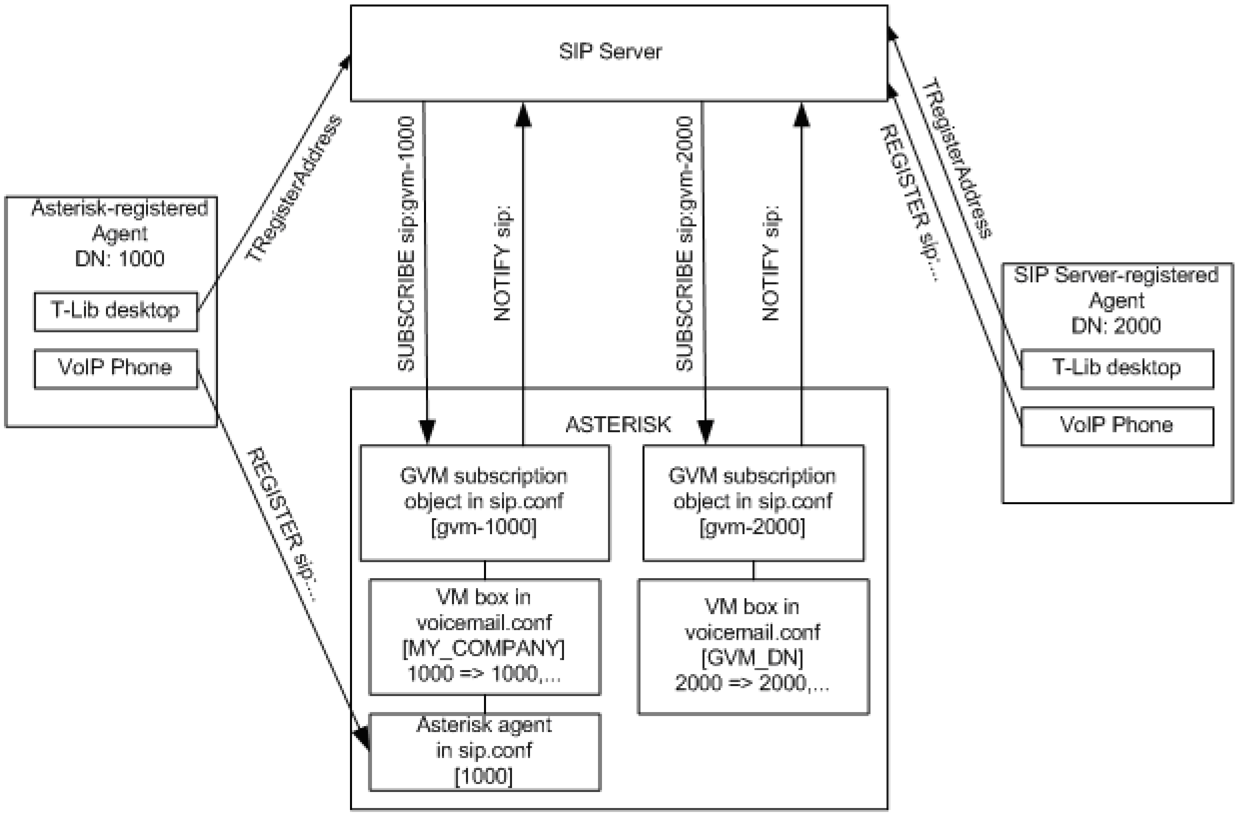

Figure 53: Asterisk Configuration as a Voice Mail Server

Figure 53 shows how voice mail services can be provided for two agents: Agent DN 1000 and Agent DN 2000. Both agents use T-Library desktops connected to SIP Server via the T-Library protocol. Agent DN 1000 has the VOIP phone that is registered on Asterisk. Agent DN 2000 has the VOIP phone that is registered on SIP Server.

Asterisk is configured to fully support all calls made from and to DN 1000. For this purpose, it has a SIP entity `[1000]` configured in the `sip.conf` file to represent the agent's phone. It also has a voice mail box configured in some private context `[MY_COMPANY]` in the Asterisk `voicemail.conf` configuration file.

SIP Server integration with Asterisk requires adding a new object to the Asterisk configuration to provide the voice mail functionality for the SIP Server agent at DN 2000. A new voice mail box for this agent is created in the `[GVM_DN]` context of the Asterisk `voicemail.conf` configuration file.

The Asterisk Message Waiting Indicator (MWI) interface is used to integrate Asterisk as a voice mail server with SIP Server. The MWI interface utilizes the SIP subscription schema. SIP Server subscribes to the `message-summary` event at Asterisk using the SIP `SUBSCRIBE` request method:

```
SUBSCRIBE sip:gvm-1000@192.168.0.300 SIP/2.0
From: sip:gvm-1000@192.168.0.300;tag=7C217D88
```

```
To: sip:gvm-1000@192.168.0.300;tag=as050e992c
Call-ID: 1CD815F7-1@192.168.0.300
CSeq: 1103 SUBSCRIBE
Content-Length: 0
Via: SIP/2.0/UDP 192.168.0.200:5060;branch=z9hG4bK3B
Event: message-summary
Accept: application/simple-message-summary
Contact: <sip:gsipmwi@192.168.0.200:5060;mb=1000;dn=1000;tp=1>
Expires: 600
```

Asterisk sends notifications to SIP Server about the voice mail box status using the SIP `NOTIFY` message:

```
NOTIFY sip:gsipmwi@192.168.0.200:5060;mb=1000;dn=1000;tp=2 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.200:5070;branch=z9hG4bK219f391e
From: "asterisk" <sip:asterisk@192.168.0.200:5070>;tag=as13d3077a
To: <sip:gsipmwi@192.168.0.200:5060;mb=1000;dn=1000;tp=2>
Contact: <sip:asterisk@192.168.0.200:5070>
Call-ID: 1CD815F7-1@192.168.0.300
CSeq: 102 NOTIFY
User-Agent: Asterisk PBX
Event: message-summary
Content-Type: application/simple-message-summary
Content-Length: 43
Messages-Waiting: yes
Voice-Message: 1/0
```

SIP Server generates the `EventUserEvent` message based on this notification and sends it to the T-Library client registered on a DN associated with a particular voice mail box. This is an example of such a T-Library event:

```
EventUserEvent
AttributeUserData[120] 00 01 03 00..
       'gsipmwi'(list) 'Mailbox''1000'
                      'Messages-Waiting'   'true'
                      'Voice-Message'      '1/0'
                      'NewMessages'        1
                      'OldMessages'        0
AttributeUserEvent[1001]
AttributeThisDN'1000'
```

Dedicated SIP objects are created in the `sip.conf` Asterisk configuration file to support the MWI subscription. These objects are `gvm-1000` and `gvm-2000` in Figure 53 on page 67. The GVM acronym in the object name stands for Genesys Voice Mail. These objects are created in Asterisk for MWI subscription purposes only, and no SIP clients are registered on these objects. Both objects have a parameter pointing to a specific Asterisk voice mail box:

```
[gvm-1000]
        mailbox=1000@MY_COMPANY
[gvm-2000]
        mailbox=2000@GVM_DN
```

SIP Server activates one SIP subscription per voice mail box it needs to monitor. The above configuration guarantees that SIP Server will receive notification on a correct voice mail box when it subscribes to a corresponding GVM object.

MWI Subscription Scope

SIP Server activates one or multiple MWI subscriptions for each voice mail box it needs to monitor. Individual voice mail boxes created for Extensions or Agent Logins are monitored by a single MWI subscription per box. The number of MWI subscriptions activated per Agent Group voice mail box is equal to the number of agents currently logged in to this Agent Group.

SIP Server is designed in the assumption that all extensions have voice mail boxes. So, if MWI monitoring is enabled for the extensions (`mwi-extension-enable` is set to `true`), SIP Server at start up attempts to activate MWI subscriptions for all extensions configured in the Configuration Layer. Subscriptions for the Extension-related voice mail boxes are deactivated when SIP Server shuts down.

MWI subscription for Agent Login is when an agent with the corresponding agent ID logs in to SIP Server. SIP Server keeps this subscription active while the agent is logged in and stops it when the agent logs out.

The same MWI subscription logic is applied to the monitoring of voice mail boxes created for the Agent Groups. SIP Server activates MWI subscription for the group when the first agent associated with this group logs in. SIP Server stops the subscription when the last agent of this group logs out.

If, for some reason, a subscription request for any voice mail box type is rejected or times out, SIP Server attempts to activate this subscription again in one minute.

Building a Voice Mail Solution

The Voice Mail functionality in SIP Server and Asterisk allows you to build multiple Voice Mail solutions with different complexity to address different business needs. This section provides examples that show how to build Voice

Mail solutions. It outlines general architectural ideas that refer to some configuration options only for clarification purposes. For configuration procedures, see the *Framework 8.0 SIP Server Deployment Guide*.

The easiest approach to a Voice Mail solution is to have calls, which are not answered on a DN during a specified timeout, forwarded to the voice mail box associated with this DN (extension). This solution requires that you associate an Asterisk-hosted voice mail box with the DN. A `DN` object in Configuration Manager should be configured with the following options:

- `no-answer-overflow`
- `no-answer-timeout`

The `no-answer-timeout` option specifies the time during which the call must be answered. When the `no-answer-timeout` timer expires and the call is not answered, SIP Server uses the value of option `no-answer-overflow` to decide how to process the call. If this option contains the name of the voice mail box associated with this DN, then SIP Server sends the call to this voice mail box.

A similar solution can be configured for agents. SIP Server can apply the same algorithm that is used for process unanswered calls for an agent who ignores the DN where the agent logs in. In this case, the Asterisk-hosted voice mail box should be associated with the Agent Login (and not the extension). Also, the `no-answer-timeout` and `no-answer-overflow` options should be specified in the `Agent Login` configuration object.

SIP Server also allows you to use voice mail boxes in business call routing. Usually in those scenarios, calls are controlled by the URS strategy, which attempts to find an appropriate agent to forward the call to. There are many ways to write a URS strategy to utilize a Voice Mail solution. For example, if a call is routed to an agent group that does not have any currently available agents, URS can send a call to the voice mail box associated with the Agent Group. In this case, all logged in members of this group will receive a notification about the new message left in the group voice mail box.

SIP Server can also redirect unanswered calls to the voice mail box based on the options configured for the SIP Server `Application` configuration object. There are two groups of options, which define how SIP Server processes unanswered calls for extensions and for agents:

- `extn-no-answer-XXX`
- `agent-no-answer-XXX`

See the *Framework 8.0 SIP Server Deployment Guide* for more information about the options.

Asterisk as a Media Server

You can configure Asterisk as a media server for SIP Server. SIP Server can utilize the following services provided by Asterisk:

- Play announcements.

- Collect DTMF digits.
- Organize conferences.
- Recording calls.

Communication between two servers is mainly based on RFC 4240; an exception is the recording service, which is not described in this RFC.

Asterisk for Business Calls Routing

Integration Task Summary

Table 6 summarizes the steps to integrate SIP Server with Asterisk to support business calls routing.

Table 6: Task Summary—Integrating SIP Server with Asterisk

Objective	Related Procedures and Actions
1. Configure Asterisk to support business call routing.	See Table 7 on page 72.
2. Configure DNs for the Asterisk `Switch` object in the Configuration Layer.	See Table 8 on page 75.

Configuring Asterisk

This section describes the procedures for configuring Asterisk in the following environment (see Figure 54):

- Asterisk is connected to the network via a SIP gateway.
- Two SIP endpoints, 2001 and 2002, are registered on Asterisk.
- Each endpoint is associated with a T-Library desktop application.

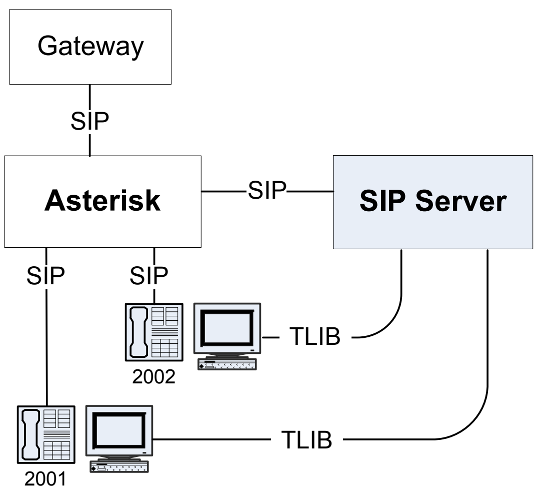

Figure 54: Asterisk Sample Configuration

Table 7 provides an overview of the main steps to integrate SIP Server with Asterisk.

Table 7: Task Flow—Configuring Asterisk

Objective	Related Procedures and Actions
1. Confirm that Asterisk is functional and handling calls appropriately.	The procedures in this chapter assume that Asterisk is functional and handling calls appropriately. For more information, see Asterisk documentation.
2. Configure the `sip.conf` file.	Complete the following procedure: • Procedure: Configuring the sip.conf file
3. Configure the `extensions.conf` file.	Complete the following procedure: • Procedure: Configuring the extensions.conf file, on page 74

Procedures

This section describes the configuration that you must perform on the Asterisk side.

Procedure: Configuring the sip.conf file

Purpose: To configure the `sip.conf` file.

Start of procedure

1. Configure two peers, one describing the gateway access, and the other describing SIP Server access—for example:

```
[gwsim]
type=peer
host=10.0.0.1
port=5066
context=default
canreinvite=no
[gsip]
type=peer
username=gsip
host=10.0.0.1
context=default
canreinvite=no
```

2. Configure the endpoints. The user name of the endpoint must match the `Extension` DN configured on the SIP Server side—for example:

```
[2001]
type=friend
username=2001
host=dynamic
context=default
notifyringing=yes
canreinvite=no
[2002]
type=friend
username=2002
host=dynamic
context=default
notifyringing=yes
canreinvite=no
```

Note: SIP Server does not support receiving authentication challenges. For this reason, Asterisk users must not be configured with the `secret` option; otherwise, Asterisk would challenge `INVITE` messages that SIP Server issues on behalf of the user, and SIP Server would fail to respond to the challenge.

3. When you are finished, save your configuration.

End of procedure

Next Steps

- Procedure: Configuring the extensions.conf file

Procedure: Configuring the extensions.conf file

Purpose: To configure the `extensions.conf` file.

Start of procedure

1. For each endpoint that SIP Server monitors, configure a *hint* entry to ensure that Asterisk will accept a presence subscription (from SIP Server, in this case) for those endpoints—for example:

```
exten => 2001,hint,SIP/2001
exten => 2001,1,Dial(SIP/2001,60)
exten => 2002,hint,SIP/2002
exten => 2002,1,Dial(SIP/2002,60)
```

2. Configure a basic dialing plan for contact center calls.

   In this example, extension 2400 is used as a company's service number, so all business calls should arrive to this extension. Those calls are routed to SIP Server. If a call is not answered within 30 seconds, it will be dropped. The "`r`" flag tells Asterisk to generate a ringback tone for the caller while the call is being routed.

```
; Inbound call to routing point 2400 -> contact SIP Server
exten => 2400,1,Dial(SIP/${EXTEN}@gsip,30,r)
exten => 2400,2,Hangup()
```

3. Configure a basic dialing plan for calls to external numbers—for example:

```
; Any number with prefix '0' -> contact gateway (with remaining
digits only)
exten => _0.,1,Dial(SIP/${EXTEN:1}@gwsim,60)
```

4. When you are finished, save your configuration.

End of procedure

Configuring Asterisk DN Objects

Table 8 provides an overview of the main steps to configure different DNs under the Asterisk Switch object in the Configuration Layer.

Table 8: Task Flow—Configuring DNs for the Asterisk Switch Object

Objective	Related Procedures and Actions
1. Configure a Trunk DN.	Complete the following procedure: • Procedure: Configuring a Trunk DN for Asterisk
2. Configure an Extension DN.	Complete the following procedure: • Procedure: Configuring Extension DNs for Asterisk, on page 77

Procedures

If you integrate SIP Server with Asterisk in order to support the business routing capability, you do not need to set any configuration options in the SIP Server Application object. Instead, you configure DNs for the Asterisk Switch object that is assigned to the appropriate SIP Server.

Procedure:
Configuring a Trunk DN for Asterisk

Purpose: To configure a DN of type Trunk to support the presence SUBSCRIBE/NOTIFY functionality and to configure external access through Asterisk.

Start of procedure

1. Under a configured Switch object, select the DNs folder. From the File menu, select New > DN to create a new DN object.
2. In the New DN Properties dialog box, click the General tab, and then specify the following properties (see Figure 55):
   a. Number: Enter a name for the Trunk DN. This name can be any unique value, and it can be a combination of letters and numbers.
   b. Type: Select Trunk from the drop-down box.

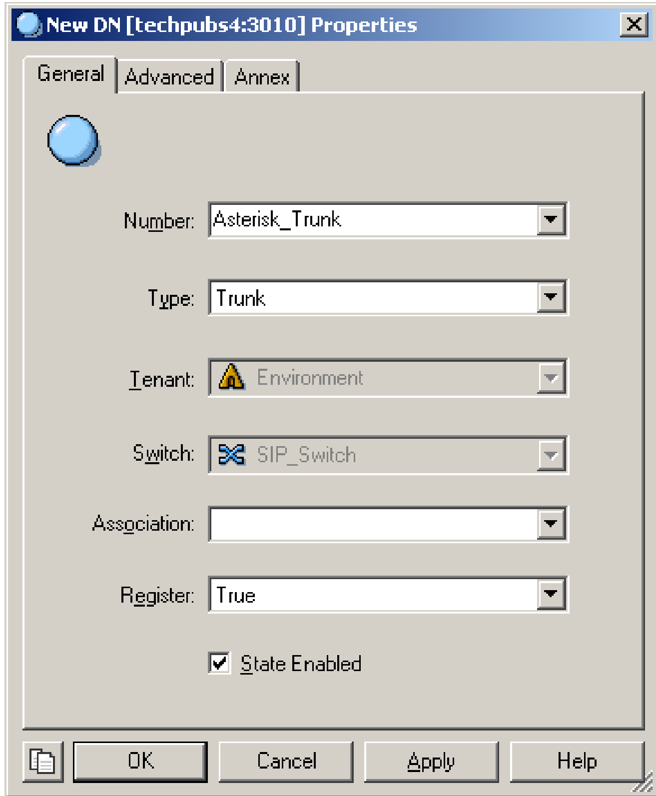

Figure 55: Creating a Trunk DN for Asterisk: Sample Configuration

3. Click the `Annex` tab.
4. Create a section named `TServer`. In the `TServer` section, create options as specified in Table 9 (see Figure 56).

Table 9: Configuring a Trunk DN

Option Name	Option Value	Description
contact	SIP URI	Specifies the contact URI to which SIP Server sends the `SUBSCRIBE` message.
subscribe-presence-domain	A string	Specifies the subscription domain information for the `Trunk` DN. This option value will be used with the DN name to form the `SUBSCRIBE` request URI and the `To:` header.
subscribe-presence-expire	Any positive integer	Specifies the subscription renewal interval (in seconds).
subscribe-presence-from	SIP URI	Specifies the subscription endpoint information. This option value will be used to form the `From:` header in the `SUBSCRIBE` request.

Table 9: Configuring a Trunk DN (Continued)

Option Name	Option Value	Description
prefix	Any positive integer	Specifies the initial digits of the number used to direct to Asterisk any call that SIP Server does not recognize as an internal DN.
refer-enabled	`false`	Set this option to `false` for SIP Server to use a `re-INVITE` request method when contacting Asterisk.

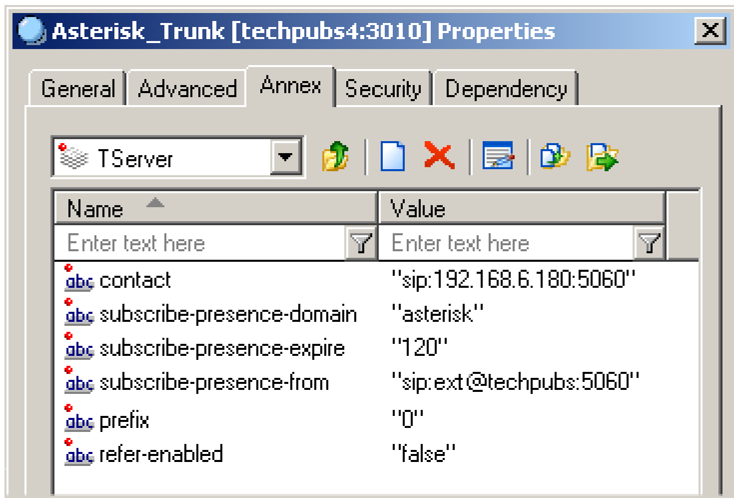

Figure 56: Setting Options for the Trunk DN: Sample Configuration

5. When you are finished, click `Apply`.

End of procedure

Procedure: Configuring Extension DNs for Asterisk

Purpose: To configure Asterisk endpoints that SIP Server will monitor and control.

Start of procedure

1. Under a configured `Switch` object, select the `DNs` folder. From the `File` menu, select `New > DN` to create a new `DN` object.
2. In the `New DN Properties` dialog box, click the `General` tab, and then specify the following properties (see Figure 57):
   a. `Number`: Enter a name for the `Extension` DN. In general, this should be the phone number of the extension. You must not use the @ symbol or a computer name.

b. `Type`: Select `Extension` from the drop-down box.

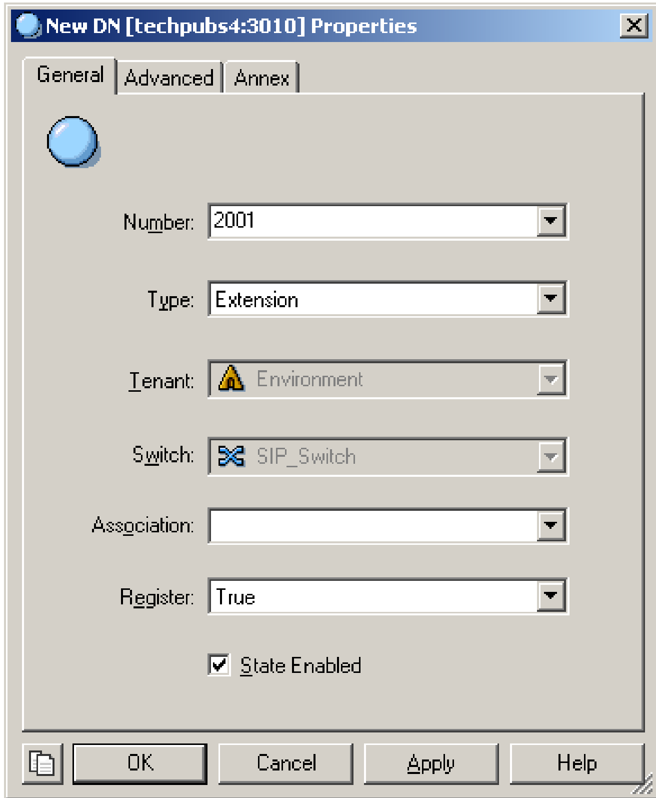

Figure 57: Creating an Extension DN for Asterisk: Sample Configuration

3. Click the `Annex` tab.
4. Create a section named `TServer`. In the `TServer` section, create options as specified in Table 10 (see Figure 58).

Table 10: Configuring an Extension DN for Asterisk

Option Name	Option Value	Description
contact	SIP URI	Specifies the contact URI to which SIP Server sends the `SUBSCRIBE` message.
dual-dialog-enabled	`false`	Set this option to `false` so that consultation calls are handled using the same SIP dialog that is sent to Asterisk.
make-call-rfc3725-flow	1	Set this option to `1`, so that 3pcc call flow will be used according to RFC3725.
refer-enabled	`false`	Set this option to `false` if you are using the RFC3725 flow.

Table 10: Configuring an Extension DN for Asterisk (Continued)

Option Name	Option Value	Description
sip-hold-rfc3264	`false`	Set this option to `false` so that RTP stream hold is performed in a manner compliant with RFC2543.
subscribe-presence	A string	Specifies the name of the `Trunk` DN that is configured for the presence subscription messages to be sent to Asterisk.

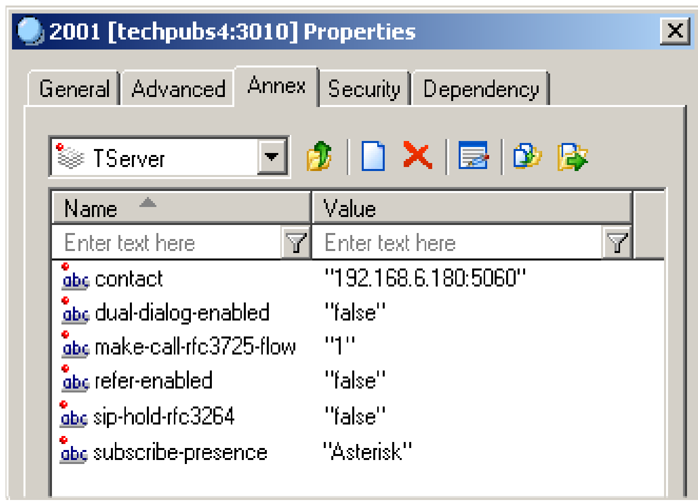

Figure 58: Setting Options for the Extension DN: Sample Configuration

5. When you are finished, click `Apply`.

End of procedure

Asterisk as a Voice Mail Server

Integration Task Summary

Table 11 summarizes the steps to integrate SIP Server with Asterisk to support the Voice Mail solution.

Table 11: Task Summary—Integrating SIP Server with Asterisk to Support the Voice Mail Solution

Objective	Related Procedures and Actions
1. Configure the SIP Server `Application` configuration object.	Complete the following procedure: • Procedure: Configuring a SIP Server Application object.
2. Configure DNs, Agent Logins, and Agent Groups in the SIP Server `Switch` object to use voice mail boxes.	Complete the following procedure: • Procedure: Configuring Configuration Layer Objects.
3. Configure Asterisk using the GVMA utility.	The GVMA utility is used to collect all GVM-options from the `Switch` objects in the Configuration Layer and propagate these options into the Asterisk configuration. Some manual Asterisk configuration may be required. See "Configuring Asterisk" on page 85.

Configuring a SIP Server Application object

The following section describes configuration procedures to integrate SIP Server with Asterisk to support the Voice Mail solution.

Procedure: Configuring a SIP Server Application object

Start of procedure

1. Set the MWI mode:

   In the SIP Server `Application` object, set the `mwi-mode` option to `REGISTER` or `SUBSCRIBE`. This is the SIP method that SIP Server uses to utilize the MWI interface.

- With a value of SUBSCRIBE (default), SIP Server activates SIP subscriptions for all voice mail box owners as configured by other mwi-<xxx> options.
- With a value of REGISTER, SIP Server activates MWI functionality using the REGISTER SIP message.

Note: It is recommended that you use SUBSCRIBE for SIP Server release 7.6 and later. The SUBSCRIBE-based method works both for agents registered on Asterisk and for agents registered on SIP Server, whereas the REGISTER-based method does not work for agents registered on Asterisk.

Set the mwi-domain option to the domain name, which SIP Server should send to Asterisk in the MWI REGISTER or SUBSCRIBE requests. This option must be synchronized with the Asterisk settings. But in the basic configuration it can be set to the Asterisk hostname or IP address.

2. Configure SIP Server access to Asterisk:

   In the SIP Server Application object, set the following configuration options:

   - mwi-host: Enter the host name or IP address where Asterisk runs.
   - mwi-port: Enter the port on Asterisk to listen to the SIP messages.

   SIP Server sends MWI-related REGISTER and SUBSCRIBE requests to the address specified by these two options.

3. Select the types of voice mail boxes to use:

   In the SIP Server Application object, set the parameters corresponding to the voice mail box types to be used in the system to true to activate a support of the voice mail boxes of this type. Multiple voice mail box types can be enabled simultaneously.

   - mwi-extension-enable—For a voice mail box of type Extension
   - mwi-agent-enable—For a voice mail box of type Agent
   - mwi-group-enable—For a voice mail box of type Agent Group

End of procedure

Configuring Configuration Layer Objects

Genesys provides the Genesys Voice Mail Adapter (GVMA) utility, which reads the configuration related to the Voice Mail solution from the Configuration Layer. The GVMA utility uses this information to modify the Asterisk configuration accordingly. All Configuration Layer objects that you will associate with the Asterisk-hosted voice mail boxes must be supplied with the GVM options, which provide necessary information for the GVMA utility.

There are three types of configuration objects that can be associated with the voice mail boxes:

- `DN`
- `Agent Login`
- `Agent Groups`

A `DN` object can be associated only with the `Extension` voice mail box.

An `Agent Login` object can be associated with two types of voice mail boxes at the same time:

- `Agent` voice mail box
- `Agent Group` voice mail box

An `Agent Groups` object can be associated with the Agent Group voice mail box only.

GVM Configuration Options

You specify GVM configuration options in the `TServer` section on the `Annex` tab of the following three configuration objects:

- `DN`
- `Agent Login`
- `Agent Group`

You can use all GVM options in all objects with one exception the `gvm_group_mailbox` option, which can appear only in the `Agent Login` object. A full set of GVM options, which you can use to configure objects, is provided below:

- `gvm_mailbox`: This option is used in two ways:
  - The GVMA utility uses this option as the name of the voice mail box it creates on Asterisk for the `DN`, `Agent Login`, and `Agent Group` objects.
  - SIP Server uses the value of this option to activate the MWI subscription for a voice mail box created for the `DN` and `Agent Login` objects. SIP Server compiles an object name for the MWI subscription as shown it below:

Table 12: Example of Compiled Object Names for the MWI Subscription

Configuration Layer Objects	gvm_mailbox Value	MWI Subscription Name
DN	1000	gvm-1000
Agent Login	1000	gvm-a-1000

The MWI subscription name is sent in the SIP `SUBSCRIBE` message to Asterisk to activate the MWI subscription. See more information about this option in "Configuring the Voice Mail Boxes for Agent Groups".

- `gvm_group_mailbox`: This option can be specified only in `Agent Login` objects. SIP Server uses the value of this option to compile the MWI subscription name for the `Agent Group` voice mail box. For example, if this option is set to `1000`, then SIP Server sends a `SUBSCRIBE` message to Asterisk to activate the MWI subscription to the object `gvm-g-1000`. See more information about this option in "Configuring the Voice Mail Boxes for Agent Groups".
- `gvm_mailbox_context`: This option is defined only if the voice mail box already exists for this configuration object and a new one must not be created. In this case, the option contains the name of the Voice Mail context in the `voicemail.conf` file where the voice mail box resides.
- `gvm_name`: This option specifies the owner's name associated with the voice mail box.
- `gvm_password`: This option specifies the voice mail box password.
- `gvm_email`: This option specifies the e-mail associated with the voice mail box. Asterisk can be configured to send Voice Mail notifications to this e-mail address.
- `gvm_pager_email`: This option specifies the pager e-mail associated with the voice mail box.
- `gvm_options`: This option specifies a list of voice mail box options separated by a pipe (`|`) symbol. For more information, see Asterisk documentation.

Voice Mail Boxes Created by the GVMA Utility

The GVMA utility scans the following objects to decide if it should create new voice mail boxes for them in the Asterisk configuration:

- All DNs for a switch specified in the GVMA configuration file.
- All Agent Logins for a switch specified in the GVMA configuration file.
- All Agent Groups for a tenant specified in the configuration file.

A new voice mail box, which does not have the GVM option `gvm_mailbox_context` specified, is created for all DNs. The voice mail box name is set to the value of the `gvm_mailbox` option if it is specified for this DN. If this option is undefined, then the voice mail box is created with the name of the DN. The DN name is also used as the default value of the `gvm_password` and `gvm_name` options.

A new voice mail box is created for the `Agent Login` or `Agent Group` object only if the `gvm_mailbox` option is specified for this object in the Configuration Layer. If there is no such option, a voice mail box is not created.

Configuring the Voice Mail Boxes for Agent Groups

The voice mail box configuration for an Agent Group should be provided in the `TServer` section on the `Annex` tab of the corresponding `Agent Group` object. This information is used by the GVMA utility, which creates a MWI subscription object for SIP Server in the Asterisk configuration. The GVMA utility monitors either the existing voice mail box or the one specifically created for the Agent Group.

SIP Server does not read information about Agent Groups from the Configuration Layer. So, the configuration information specified in the `Agent Group` objects is not available for SIP Server. It also means that SIP Server does not have information about how agents are organized into the Agent Groups.

SIP Server uses the GVM option `gvm_group_mailbox` specified in the `TServer` section on the `Annex` tab of the `Agent Login` object to associate an agent with the Agent Group.

SIP Server analyzes two GVM options specified for an agent when this agent logs in:

- `gvm_mailbox`
- `gvm_group_mailbox`

If the `gvm_mailbox` is specified, SIP Server activates the MWI subscription to a voice mail box for this agent. If the `gvm_group_mailbox` is defined for this agent, SIP Server initiates the MWI subscription to the Agent Group voice mail box. In this scenario, one agent has multiple MWI subscriptions active. This agent will receive Voice Mail-related notifications for both personal Agent voice mail boxes and Agent Group voice mail boxes.

Configuring Agents Registered on Asterisk or on SIP Server

There are two possible scenarios to configure GVM options for a corresponding configuration object:

- A voice mail box is already created for this object.
- A new voice mail box should be created for this object.

The first scenario occurs when SIP Server is added to the existing Asterisk installation in which agents register directly on Asterisk and already have the voice mail boxes configured for them. In this case, it is only required for SIP Server to monitor existing voice mail boxes to provide appropriate notifications to the T-Library clients.

The second scenario takes place when Asterisk is added to the SIP Server installation. All agents register on SIP Server and all of them need new voice mail boxes created. It is also possible to build a system with both types of agents.

The GVMA utility uses the gvm_mailbox_context option to differentiate these two scenarios. If this option is not specified in the corresponding object, then GVMA creates a new mail box in one of the GVMA default contexts (GVMA_DN / GVMA_AGENT / GVMA_AGENTGROUP). If this option is specified, then GVMA does not create a new voice mail box for this configuration object, and it uses the specified context in the voice mail box option of the sip.conf file.

Configuring Access to Voice Mail Boxes for the Agents Registered on SIP Server

SIP Server supports three types of voice mail boxes:

- Extension
- Agent Login
- Agent Group

The GVMA utility used for the Asterisk configuration creates voice mail boxes in three different contexts in the voicemail.conf Asterisk configuration file:

- GVMA_DN: The voice mail boxes are associated with Extensions.
- GVMA_AGENT: The voice mail boxes are associated with Agent Logins.
- GVMA_AGENTGROUP: The voice mail boxes are associated with Agent Groups.

Correspondingly, three different prefixes (wild cards) are configured in the extensions.conf configuration file to reach voice mail boxes in three contexts. To utilize this configuration on the Asterisk side there should be one or several trunks configured in the SIP Server Switch configuration object to send all voice mail calls to Asterisk. Prefixes defined for these trunks should match the wild cards used on Asterisk to reach different voice mail contexts. Configured prefixes will be supplied as options for the GVMA utility later.

To access a voice mail box with this configuration, agents need to dial a prefix corresponding to a voice mail box type, followed by the voice mail box number.

Configuring Asterisk

The Genesys Voice Mail Adapter (GVMA) utility is provided by Genesys to propagate the Voice Mail configuration from the Configuration Layer to the Asterisk configuration files. GVMA performs the following steps:

1. GVMA starts.
2. GVMA connects to Configuration Server using the SOAP protocol.
3. GVMA makes a backup copy of the Asterisk configuration.

4. GVMA loads the Voice Mail configuration from the following configuration objects:
   - `DNs`
   - `Agent Logins`
   - `Agent Groups`
5. GVMA updates Asterisk configuration files with the information retrieved from the Configuration Layer during Step 4.
6. GVMA instructs Asterisk to reload configuration files.
7. GVMA exits.

GVMA can be run manually or scheduled for periodic execution using the OS scheduling tools, such as cron on Linux systems.

Table 13 provides an overview of the main steps to integrate SIP Server with Asterisk to support the Voice Mail solution.

Table 13: Task Flow—Configuring Asterisk

Objective	Related Procedures and Actions
1. Define all required parameters in the GVMA configuration file.	See the following sections: • "Prerequisites" • "GVMA Location" • "Configure the GVMA Configuration File" on page 88
2. Run the GVMA utility on the Asterisk host to configure Asterisk.	Run the GVMA utility by executing the `gvma_asterisk76.pl` script.

Prerequisites

Back Up the Asterisk Configuration

The GVMA utility modifies the following Asterisk configuration files: `extensions.conf`, `sip.conf`, and `voicemail.conf`. To save the original Asterisk configuration, create backup copies of all Asterisk configuration files before using the GVMA utility.

Perl Interpreter

You must install the Perl interpreter on the Asterisk host to run the GVMA utility, which is written as a perl script. Install these additional perl packages that are required to run GVMA:

- SOAP-Lite
- Net-Telnet

Enable the Asterisk Manager Interface

Enable the Asterisk Manager Interface (AMI) by setting the following parameters in the `manager.conf` Asterisk configuration file:

```
[general]
enabled = yes
port = 5038
bindaddr = 0.0.0.0
```

Enable the GVMA Utility to Change the Asterisk Configuration

Enable the GVMA utility to change the Asterisk configuration by adding the following section in the `manager.conf` Asterisk configuration file:

```
[gvma]
secret = genesys1
deny=0.0.0.0/0.0.0.0
permit=127.0.0.1/255.255.255.0
read = system,call,log,verbose,command,agent,user
write = system,call,log,verbose,command,agent,user
```

GVMA Location

The GVMA utility is located in the `tools` folder of the SIP Server installation utility. Files in the tools directory include:

- `gvma_asterisk76.cfg`—The GVMA utility for 7.6 SIP Server.
- `gvma_asterisk76.pl`—The GVMA utility configuration file for 7.6 SIP Server.
- `gvma_asterisk.cfg`—The GVMA utility for 7.5 SIP Server.
- `gvma_asterisk.pl`—The GVMA utility configuration file for 7.5 SIP Server.

Depending on the `mwi-mode` option value set in the SIP Server `Application` object, you choose which configuration file and script to run. If the `mwi-mode` option is set to `SUBSCRIBE`, use the following files:

- `gvma_asterisk76.cfg`
- `gvma_asterisk76.pl`

If the `mwi-mode` option is set to `REGISTER`, use the following files:

- `gvma_asterisk.cfg`
- `gvma_asterisk.pl`

The `REGISTER` value of the `mwi-mode` option is for backward compatibility with 7.5 releases of SIP Server.

Configure the GVMA Configuration File

Configure the following sections in the GVMA configuration file before using the utility:

- cfgserver
- gvma_settings

Section *cfgserver*

Parameters in the cfgserver section define how GVMA connects to Configuration Manager and what information GVMA reads from it.

Note that option port refers to the SOAP port of Configuration Server and not to the port where Configuration Manager is connected. The Configuration Server SOAP port is specified in the Configuration Server configuration file as a port option in the [soap] section.

```
[cfgserver]

host=<config server hostname or IP>

port=<config server SOAP port>

username = <config server username>

password = <config server password>
```

The second part of the cfgserver section provides several examples about how to define a query to allow for the GVMA utility to collect information about DNs, Agent Logins, and Agent Groups from the Configuration Layer. One query should be chosen for each of these three object types. The following placeholders in the selected queries should be replaced with the information from the Configuration Layer:

- <Switch DBID>
- <tenant DBID>
- <tenant name>
- <Switch Name>

```
#Query examples using DBIDs:
#dnquery = CfgDN[(@ownerDBID=<Switch DBID>) and (@type=1)]
#agentquery = CfgAgentLogin[@ownerDBID=<Switch DBID>]
#agentgroupquery = CfgAgentGroup[@tenantDBID=<tenant DBID>]

#Query examples using switch and tenant names:
dnquery = CfgTenant[@name='<tenant
Name>']/switches/CfgSwitch[@name='<swith name>']/DNs/CfgDN[@type='1']
agentquery = CfgSwitch[@name='<Switch name>']/agentLogins/CfgAgentLogin
agentgroupquery = CfgTenant[@name='<tenant
name>']/agentGroups/CfgAgentGroup
```

Section *gvma_settings*

The first group of parameters in the `gvma_settings` section specifies the location of Asterisk configuration files and what files you have to change:

- `asterisk_cfg_path=/etc/asterisk`
- `asterisk_cfg_file_sip=sip.conf`
- `asterisk_cfg_file_vm=voicemail.conf`
- `asterisk_cfg_file_exten=extensions.conf`

The following parameters define the comments, which GVMA puts as a boundaries around the parts it inserts into the Asterisk configuration files.

- `asterisk_cfg_gvma_begin=;$---GVMA-BEGIN-GVMA---$`
- `asterisk_cfg_gvma_end=;$---GVMA-END-GVMA---$`

GVMA creates backup copies of the configuration files to be modified in the location defined by the `backup_path` parameter:

- `backup_path=./gvma_backup`

GVMA uses the Asterisk Manager Interface port to connect to Asterisk:

- `asterisk_cm_port=5038`

On the Asterisk side, this port is defined in the `manager.conf` file.

Use the `siptserver_host` and `siptserver_port` parameters to specify the host and port, respectively, in the GVM subscription objects created in the `sip.conf` file.

- `siptserver_host=<SIP Server hostname or IP>`
- `siptserver_port=<SIP Server Port>`

Finally, the `gvma_settings` section has a group of parameters specifying how to access different types of voice mail boxes from the agent VOIP phones:

- `vm_dn_ext_prefix=37`
- `vm_agt_ext_prefix=38`
- `vm_grp_ext_prefix=39`
- `vm_voicemail_main_ext=9500`

GVMA Modifications to Asterisk Configuration Files

You can easily find all modifications the GVMA utility makes to the Asterisk configuration files by searching for the beginning and end key specified in the GVMA configuration file in the parameters `asterisk_cfg_gvma_begin` and `asterisk_cfg_gvma_end`.

File extensions.conf

GVMA creates a new context called `[GVMA]` in the Asterisk dialing plan. This context includes six wildcards. The following wildcard is created to provide access to the agent voice mail boxes from the agent VOIP phones:

```
exten => _37X.,1,Wait(1)
exten => _37X.,2,Set(GVM_DEST=${EXTEN:2})
exten => _37X.,3,GotoIf($["${CALLERID(num)}" = "${GVM_DEST}"]?4:6)
exten => _37X.,4,VoicemailMain(${GVM_DEST}@GVMA_DN)
exten => _37X.,5,Hangup
exten => _37X.,6,GotoIf($["${GVM_DEST}" = "9500"]?7:9)
exten => _37X.,7,VoicemailMain(@GVMA_DN)
exten => _37X.,8,Hangup
exten => _37X.,9,Voicemail(${GVM_DEST}@GVMA_DN,u)
exten => _37X.,10,Hangup
```

Three wildcards of this type are created to provide access to three different types of voice mail boxes: `Extensions`, `Agent Logins`, and `Agent Groups`. Prefixes used in these wildcards are taken from the following GVMA configuration file parameters:

- `vm_dn_ext_prefix`
- `vm_agt_ext_prefix`
- `vm_grp_ext_prefix`

Another three wildcards that are created in the GVMA context are:

- `_gvm-X`
- `_gvm-a-X`
- `_gvm-g-X`

These wildcards are not supposed to be dialed directly, but they are required for the MWI subscription to function properly.

Note: You must manually include a new GVMA context into the existing dialing plan context that is used to process agent calls on Asterisk. If there is no special context created for this purpose, you must include the GVMA context into the default dialing plan context. Include the following parameters:

```
[default]
include => GVMA
```

File *sip.conf*

The GVMA utility creates a block of new GVM SIP entities in the `sip.conf` file. Each SIP entity is associated with one voice mail box. SIP Server activates one MWI subscription for each GVM SIP entity.

```
;$---GVMA-BEGIN-GVMA---$
; Generated by Genesys VoiceMail Configuration Adapter for Asterisk.
; Content generated at Tue Jan 15 20:36:50 2008
```

```
[gvm-1111]
type=friend
host=192.168.0.200
port=5060
mailbox=1111@GVMA_DN
vmexten=1111
...
;$---GVMA-END-GVMA---$
```

The GVMA utility creates multiple `gvm-*` objects in the `sip.conf` configuration file. If Asterisk is also integrated with SIP Server to perform a business call routing, then the `sip.conf` file also contains an object representing a SIP Server. The `host` and `port` parameters specified for the SIP Server object are the same as the ones defined for the `gvm-*` entities in the `sip.conf` file. This configuration can cause a problem if the Asterisk dialing plan uses the `host:port` format in the `Dial()` function to send calls to SIP Server. For example:

```
SIP-SERVER_HOST = 10.10.10.1
SIP-SERVER_PORT = 5060
exten => 2400,1,Dial(SIP/${EXTEN}@${SIP-SERVER_HOST}:${SIP-
SERVER_PORT},30,r)
```

Asterisk can select any `gvm-*` object to send calls, instead of the SIP Server object. In this case, a call is delivered to the correct destination but the call processing depends on the `sip.conf` object parameters, which are different for SIP Server and `gvm-*` objects.

To avoid this problem, Genesys recommends using the dial plan `Dial()` function with reference to the object name defined in the `sip.conf` file instead of using the `host:port` format. For example:

```
extensions.conf:
       exten => 2400,1,Dial(SIP/${EXTEN}@genesys-sip-server,30,r)
sip.conf:
       [genesys-sip-server]
       host=10.10.10.1
       port=10.10.10.1
```

File *voicemail.conf*

The GVMA utility creates three new Voice Mail contexts in the `voicemail.conf` Asterisk configuration file: `GVMA_DN`, `GVMA_AGENT`, and `GVMA_AGENTGROUP`. Those contexts contain voice mail boxes created for `Extensions`, `Agent Logins`, and `Agent Groups`, respectively. GVMA takes all parameters that are specified for the GVM voice mail boxes from the configuration of the corresponding the Configuration Layer objects.

```
;$---GVMA-BEGIN-GVMA---$
; Generated by Genesys VoiceMail Configuration Adapter for Asterisk.
; Content generated at Tue Jan 15 20:36:50 2008
; ######## Voice Mail Boxes for the Extensions #######
[GVMA_DN]
1111 => 1111,1111,,,
; ######## Voice Mail Boxes for the Agents #######
[GVMA_AGENT]
2222 => 2222, 2222, 2222@192.168.0.200,
2222@192.168.0.200,operator=yes
; ######## Voice Mail Boxes for the Agent Groups #######
[GVMA_AGENTGROUP]
3333 => 3333, 3333, 3333@192.168.0.200,
3333@192.168.0.200,operator=yes
;$---GVMA-END-GVMA---$
```

Asterisk as a Media Server

In order for Asterisk to work as a media server integrated with SIP Server, you must enhanced the Asterisk dialing plan with several Genesys macros and global variables as described in this section.

Configuring Asterisk

Dialing Plan Global Variables

You must add the following list of global variables to the `[globals]` section of the Asterisk dialing plan.

```
SIP_PREFIX=.*sip:.*@.*:[0-9]+.*
DIG_PRMT_REGEX=silence/1?[0-9]
FIND_CLT_REGEX=${SIP_PREFIX}play=[ ]*(music/collect).*
FIND_PLY_REGEX=${SIP_PREFIX}play=[ ]*([^>\;]*)[>\;].*
FIND_REP_REGEX=${SIP_PREFIX}repeat=[ ]*([^>\;]*)[>\;].*
FIND_REC_REGEX=${SIP_PREFIX}record=[ ]*([^>\;]*)[>\;].*
FIND_COF_REGEX=.*sip:conf=(.*)@.*:[0-9]+.*
DEFAULT_FILE_TO_PLAY= /var/lib/asterisk/moh/fpm-calm-river
```

Variable `DEFAULT_FILE_TO_PLAY` points to the default music file that is played for the Genesys treatments. In the example, above it refers to the voice file, which comes with Asterisk (if Asterisk is installed in the standard directory). You can change this reference to any other file in the actual deployment.

Dialing Plan Macro to Perform Genesys Treatments

You must add this treatment to the Asterisk dialing plan to perform Genesys treatments.

```
[macro-treatment]
;
; ${ARG1} - SIP_HEADER(To)
;
; IF treatment == CollectDigits
;
exten => s, 1, Answer
exten => s, 2, Set(collect=$["${ARG1}":"${FIND_PLY_REGEX}"])
exten => s, 3, GotoIf($[$["${collect}"="music/collect"] |
$["${collect}"="music/silence"]] ? 15 : 20)
exten => s, 15, macro(get-digits,${collect})
exten => s, 16, Goto(s,99)
;
; ELSE IF treatment == record
;
exten => s, 20, Set(rec_file=$["${ARG1}":"${FIND_REC_REGEX}"])
exten => s, 21, Set(ply_file=$["${ARG1}":"${FIND_PLY_REGEX}"])
exten => s, 22, GotoIf($[${LEN(${rec_file})} != 0] ? 30 : 40)
;
;           Recording Treatment
exten => s, 30, GotoIf($[${LEN(${ply_file})} = 0] ? 32 : 31)
exten => s, 31, Playback(${ply_file}) ;
exten => s, 32, Record(genesys-rec-${rec_file}.wav) ;can't
detect|report dtmf
exten => s, 33, Goto(s,98)
;
; ELSE
;           Play treatment
exten => s, 40, GotoIf($[${LEN(${ply_file})} = 0] ? 41 : 43)
exten => s, 41, Set(ply_file=${DEFAULT_FILE_TO_PLAY})
exten => s, 42, Goto(s,44)
exten => s, 43, Set(ply_count=$["${ARG1}":"${FIND_REP_REGEX}"])
exten => s, 44, GotoIf($[$[${LEN(${ply_count})} = 0] | $["$ply_count" =
"forever"]]? 50 : 60)
; Playback forever
exten => s, 50, Playback(${ply_file})
exten => s, 51, GotoIf($[${PLAYBACKSTATUS}=FAILED] ? 52 : 50) ;Goto(s,
50)
exten => s, 52, Goto(s, 99)
; Counted playback
; here probably possible to use background()
exten => s, 60, Playback(${ply_file}) ; Playback
exten => s, 61, Set(ply_count=$[${ply_count} - 1])
```

```
exten => s, 62, GotoIf($[$[${ply_count} > 0] & $[${PLAYBACKSTATUS} =
SUCCESS]] ? 61 : 98)

exten => s, 98, Hangup
exten => s, 99, NoOp(end-withot-hagup)
```

Dialing Plan Macro to Collect DTMF Digits

You must add this treatment to the Asterisk dialing plan to collect DTMF digits. Replace `<COLLECT-MESSAGE-PLACEHOLDER>` in the macros below with the name of the file to play to announce digit collection.

```
[macro-get-digits]
exten => s,1, GotoIf($[$[${ARG1}=music/collect] |
$[${ARG1}=music/silence]] ? 2 : 3)
exten => s,2, Set(ARG1=silence/2)
exten => s,3,Read(dncdigits,<COLLECT-MESSAGE-PLACEHOLDER>,1,s)
exten => s,4,SendText(Signal=${dncdigits})
exten => s,5, Goto(macro-get-digits,s,3)
```

Dialing Plan Macro to Create a Conference

You must add this treatment to the Asterisk dialing plan to organize a conference using the Asterisk MeetMe application.

```
[macro-conf]
exten => s, 1, Set(conf_id=$["${ARG1}":"${FIND_COF_REGEX}"])
exten => s, 2, NoOp(${ARG1})
exten => s, 3, GotoIf($[${LEN(${conf_id})} != 0] ? 4 : 20)
exten => s, 4, Set(rec_file=$["${ARG1}":"${FIND_REC_REGEX}"])
exten => s, 5, GotoIf($[${LEN(${rec_file})} != 0] ? 6 : 8)
exten => s, 6, MeetMe(${conf_id},drq)
exten => s, 7, Goto(s,20)
exten => s, 8, MeetMe(${conf_id},dq)
exten => s, 20, NoOp()
```

Integrating Genesys Macros into the Dialing Plan

The Asterisk dialing plan all macros provided above. This section suggests one possible way to do that. Add the following macro in the dialing plan:

```
[moh_conf_treatment]
include => macro-treatment
exten => annc, 1, macro(treatment,${SIP_HEADER(To)})
exten => _co[n]f=., 1, macro(conf,${SIP_HEADER(To)})
```

You must include this macro into the context used to process agent calls. If there is no special context created for this purpose, you must include macro into the default dialing plan context.

```
[default]
include => moh_conf_treatment
```

Media Files

Media files used for the Genesys treatments should be placed into the standard Asterisk `sounds` directory. The default location of this directory is:

`/var/lib/asterisk/sounds`

Call recordings created by Asterisk are also stored in this directory. There are two types of recordings, which can be activated by SIP Server:

- Regular (proxy mode)
- Emergency

By default, names of the recordings made in `regular` mode are prefixed with `genesys-rec.` Names of the emergency recordings start with the `meetme-conf-rec` prefix. In both cases, the name prefix is followed by a conference ID.

Configuring Asterisk DN Objects

SIP Server utilizes media services through the DNs of type `Voice over IP Service` configured under the `Switch` object. The `Voice over IP Service` DNs have a `service-type` configuration option, which defines the kind of service this DN can provide. SIP Server selects an appropriate DN when the client application requests a media service.

When you use Asterisk as a media server for SIP Server, you should configure the `Voice over IP Service` DNs with the following `service-type` values in the SIP Server `Switch` object:

- `mcu`
- `treatment`
- `recorder`
- `music`

For information about configuring DNs for different types of services, see the “SIP Device Configuration” chapter of the *Framework 8.0 SIP Server Deployment Guide.*

Chapter

3 SIP Server Integration with BroadWorks

This chapter describes how to integrate SIP Server with the BroadSoft's BroadWorks application software (hereafter referred to as *BroadWorks*), the VOIP platform. It contains the following sections:

Note: The instructions in this chapter assume that BroadWorks is fully functional, and routing calls before Genesys products are installed. They also assume that SIP Server has already been configured to function properly.

Overview

The SIP Server and BroadWorks integration solution described in this chapter is not the only method that will work. Although there are other methods, this is the only one that has been tested and approved by Genesys, and that is supported by Genesys Customer Support.

Assumptions

The integration solution described in this chapter makes the following assumptions about the desired call flow:

- Agent endpoints (SIP phones) are registered on BroadWorks only. They are not registered on SIP Server.

- The agent desktop is required to maintain agent status (logged in, logged out, ready, not ready) toward SIP Server.
- The agent desktop is also required for the agent to control (hold, transfer, conference, and so on) SIP Server calls.
- Media Gateway can be located behind BroadWorks or SIP Server. Media Gateway can also be connected to both BroadWorks and SIP Server.

In the event that these assumptions are not valid for the required deployment, you can still configure SIP Server for integration with BroadWorks; however, you may need to modify the configuration described in this chapter.

Deployment Architecture

Figure 59 depicts a sample deployment architecture of SIP Server with BroadWorks, in which:

- BroadWorks is connected to the network via a SIP gateway.
- The SIP endpoint is registered on BroadWorks.
- The SIP endpoint is associated with a T-Library desktop application.

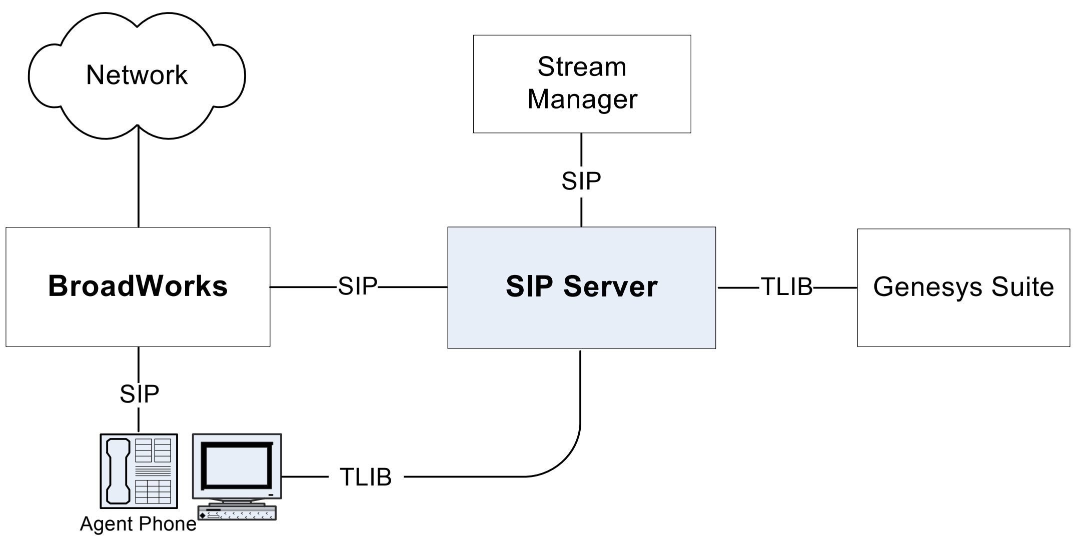

Figure 59: SIP Server - BroadWorks Deployment Architecture

Genesys SIP Server integration with BroadWorks relies on the Busy Lamp Feature (BLF) in BroadWorks. SIP Server subscribes for the BLF list, and then BroadWorks provides notifications about the status change of all endpoints that are part of the BLF list. SIP Server does not need to be in signaling path of every call.

Private Calls

A BroadWorks dialing plan can be set up in such a way that private calls (direct calls to an agent, for example) are not forwarded to SIP Server. Instead, only the notification about the busy status of the endpoint is passed to SIP Server. SIP Server uses this status change notification to set the endpoint DN to a busy state (`EventAgentNotReady`), so that the rest of the Genesys suite will not consider that DN available for the routing of contact center calls.

Figure 60 illustrates the processing of private calls. When an agent is busy on a private call, a business call is not routed to that agent.

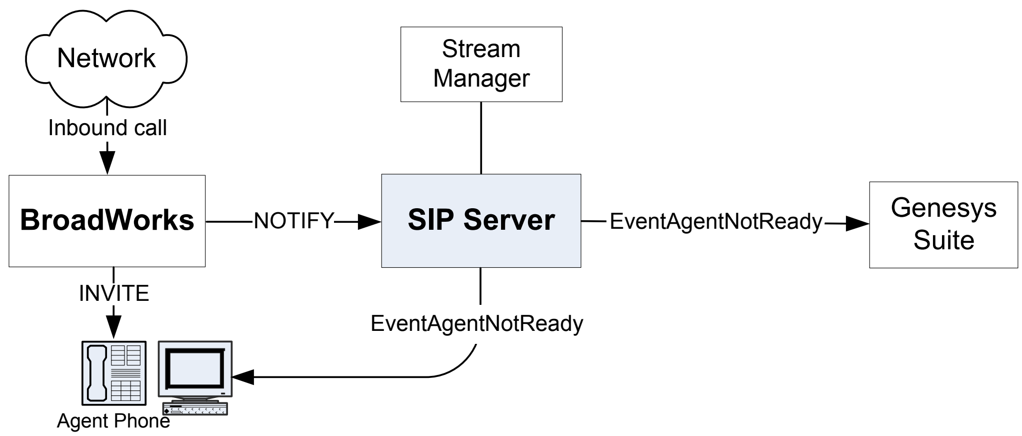

Figure 60: Private Call Processing

Contact Center Calls

In the same way that a BroadWorks dialing plan can be set up to bypass SIP Server for private calls, rules can be written so that BroadWorks forwards contact center calls (typically, calls to the service number of the company) to SIP Server. After that, SIP Server triggers a strategy for Universal Routing Server (URS) to process this type of call. Eventually, an agent DN is selected to handle the customer call, and SIP Server initiates a new dialog with BroadWorks for the selected endpoint. BroadWorks finally delivers the call to the agent endpoint.

This mechanism creates a signaling “loop” inside SIP Server, which is then in charge of maintaining the inbound leg from BroadWorks (customer leg) with the outbound leg to BroadWorks (agent leg).

By staying in the signaling path, SIP Server detects any change in call status, and can therefore produce call-related events (`EventRinging`, `EventEstablished`, `EventReleased`, and so on).

Any call control operation from the agent must be performed using a third-party call control (3pcc) procedure. In other words, the agent desktop must be used for any call control operation (besides the answer call operation). This includes, but is not limited to, hold, transfer, and conference requests.

Figure 61 illustrates the processing of contact center calls.

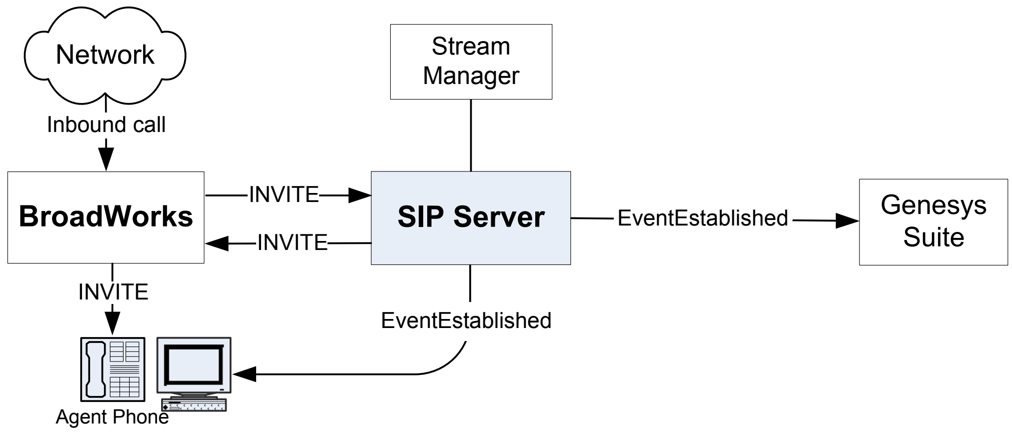

Figure 61: Contact Center Call Processing

If a network/media gateway is directly connected to SIP Server, contact center calls are first received by SIP Server. The call flow for routing the call is very similar to the flow described in the preceding paragraphs, except only there is only one call leg in BroadWorks.

Call Flows

Subscription

At startup, SIP Server sends `SUBSCRIBE` messages for the BLF list, so that is can be notified about changes in the endpoints status. BroadWorks sends `NOTIFY` messages to SIP Server to report the endpoints status. See Figure 62.

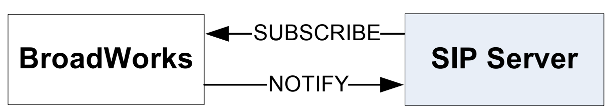

Figure 62: Presence Subscription from SIP Server

As soon as an endpoint registers on BroadWorks, BroadWorks sends a `NOTIFY` message to SIP Server, reporting the status as active. See Figure 63.

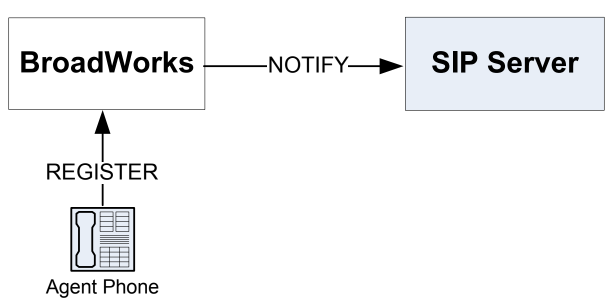

Figure 63: Presence Notification to SIP Server

Private Calls

For private calls, the BroadWorks dialing plan is set up to send private calls directly to the endpoint. BroadWorks notifies SIP Server about the call activity on that particular endpoint. In this case, SIP Server generates the `EventAgentNotReady` message, so that the overall agent status is reported as unavailable for contact center calls. The `EventAgentNotReady` and `EventAgentReady` messages are reported for the endpoints where an agent is logged in. (See Figure 60 on page 99.)

As soon as the call is released at the endpoint, BroadWorks notifies SIP Server, which then generates `EventAgentReady`. The agent is then considered available for contact center calls.

Note: The mechanism for private outbound call processing is exactly the same. SIP Server receives the `NOTIFY` messages sent by BroadWorks.

Contact Center Calls

Inbound Calls

Inbound contact center calls are programmed within the BroadWorks dialing plan to be directed to SIP Server. In this case, the call arrives at a Routing Point, and URS is triggered. A call treatment can be requested (using the `TApplyTreatment` request), and SIP Server initiates the dialog to Stream Manager. See Figure 64.

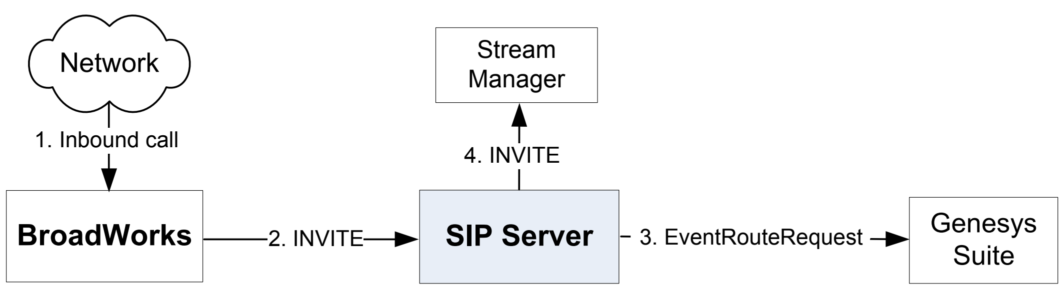

Figure 64: Handling Contact Center Calls

Whenever the agent becomes ready, SIP Server receives a `TRouteCall` request. Because this endpoint is configured to point to BroadWorks, SIP Server then initiates a new dialog with BroadWorks. BroadWorks forwards the call to the specified endpoint. When, the call is answered, Stream Manager is disconnected, and the original SIP dialog is renegotiated between SIP Sever and BroadWorks.

Because SIP Server is in the signaling path for contact center calls, it generates all call-related events (`EventRinging`, `EventEstablished`, and so on). See Figure 65.

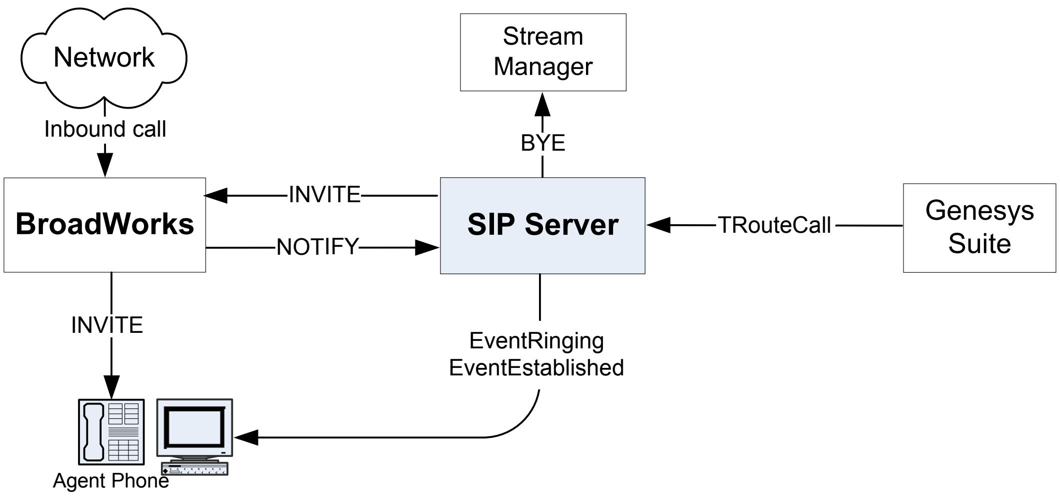

Figure 65: Delivering the Call to the Agent

Furthermore, because SIP Server is in the signaling path for the call, it also generates `EventReleased`. See Figure 66.

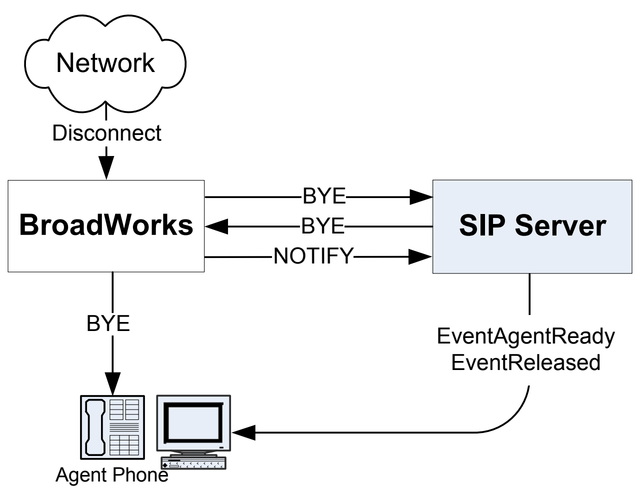

Figure 66: Contact Center Call Disconnection

Outbound Calls

An outbound call that is contact center-related (for example, a call back to a customer) must be performed using 3pcc operations. This ensures that SIP Server creates and controls the SIP dialogs on behalf of the agent endpoint.

An agent initiates the outbound call with the `TMakeCall` request. SIP Server sends the `INVITE` message to an agent endpoint (via BroadWorks). SIP Server then uses Stream Manager resources to produce a ringback tone to the agent. See Figure 67.

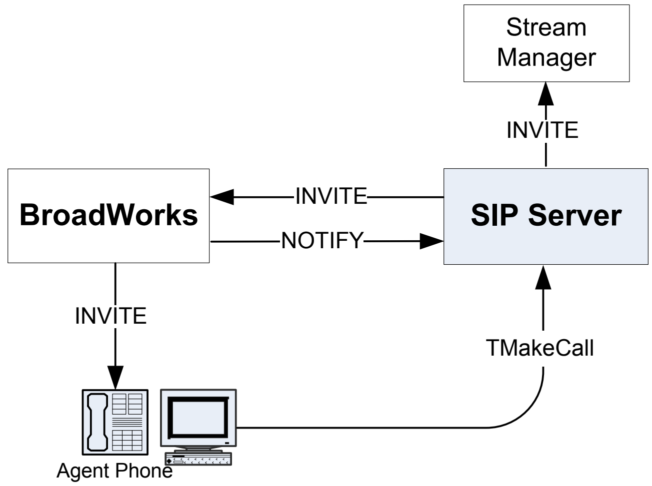

Figure 67: Engaging the Agent Endpoint for Outbound Call

SIP Server contacts the requested destination number. For external numbers, a rule should be configured within SIP Server to dial out via BroadWorks again (see "Configuring a Trunk DN for external access through BroadWorks" on page 117).

After the destination answers the call, SIP Server discontinues the ringback tone (by sending the `BYE` message to Stream Manager) and renegotiates with the agent endpoint (via BroadWorks), so that the media stream is connected between the agent and the customer. See Figure 68.

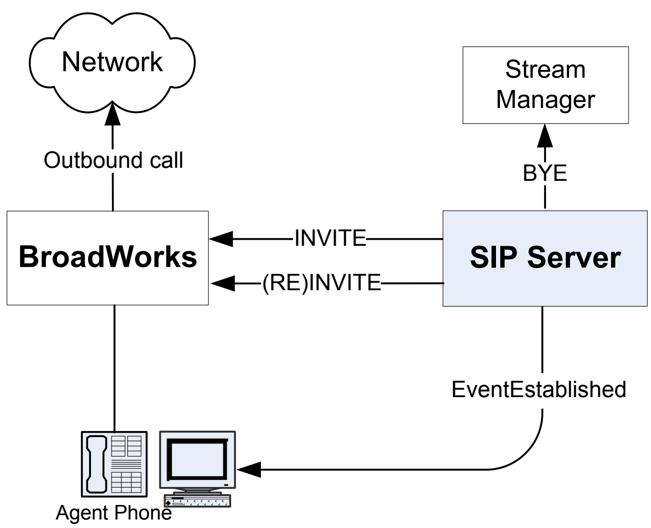

Figure 68: Connecting to the Customer

Although disconnection would work if it were initiated directly from the agent endpoint, it is a good practice to always use a desktop application to perform any action related to contact center calls. Therefore, the disconnection is requested by sending the `TReleaseCall` request to SIP Server.

SIP Server manages the two dialogs: one for the agent and another for the customer. It sends the `BYE` message to both of them, and the call is eventually disconnected. See Figure 69.

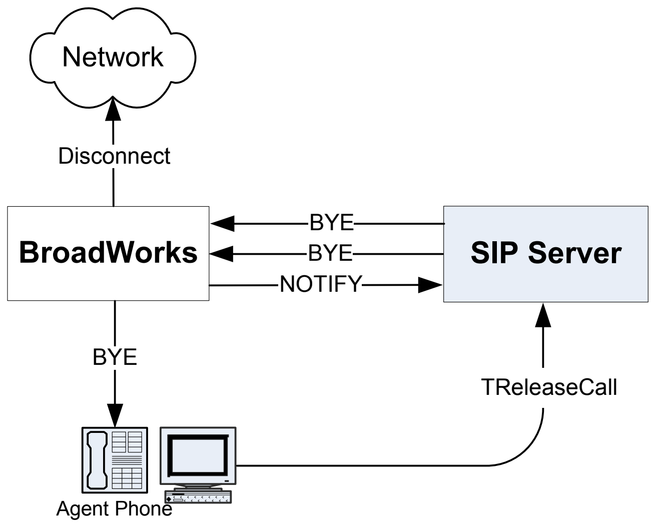

Figure 69: Outbound Call Disconnection

Conferences

SIP Server supports conferences for agents on BroadWorks. Conferences must be initiated by a T-Library client (for example, Genesys Agent Desktop). SIP Server can be configured to use either Stream Manager or other third-party MCUs to provide the conferencing feature. For details about the conference functionality, see the *Framework 8.0 SIP Server Deployment Guide*.

Supervisor Features

Supervisor features such as Silent Monitoring and Barge In are also supported for the SIP Server integration with BroadWorks. Supervisor functionality is supported via the T-Library interface. SIP Server includes a supervisor on calls between a customer and an agent (conferences), and signals the MCU to keep the Supervisor media leg open for either two-way media (`sendrecv`) or one-way media (for Silent Monitoring).

Integration Task Summary

Table 14 summarizes the steps that are required in order to integrate SIP Server with BroadWorks.

Table 14: Task Summary—Integrating SIP Server with BroadWorks

Objective	Related Procedures and Actions
1. Configure BroadWorks.	See Table 15.
2. Configure BroadWorks 8000 `DN` objects in the Configuration Layer.	See Table 16 on page 112.

Configuring BroadWorks

This section describes procedures for configuring BroadWorks in the following environment (see Figure 70):

- BroadWorks is connected to the network via a SIP gateway.
- Two SIP endpoints, 8032 and 8034, are registered with BroadWorks.
- Each endpoint is associated with a T-Library desktop application.

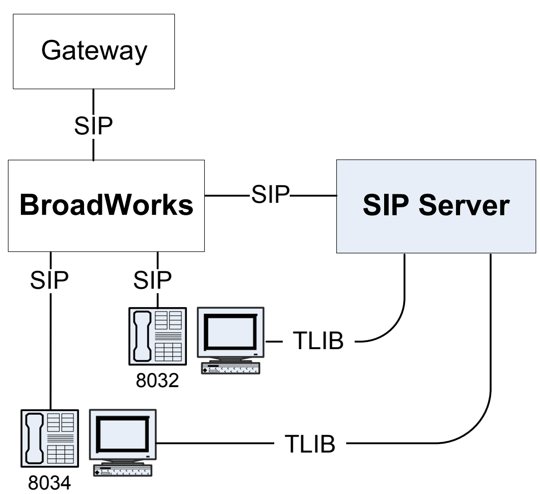

Figure 70: BroadWorks Sample Configuration

Table 15 provides an overview of the main steps that are requires to configure BroadWorks.

Table 15: Task Flow—Configuring BroadWorks

Objective	Related Procedures and Actions
1. Confirm that BroadWorks is functional and handling calls appropriately.	The procedures in this chapter assume that BroadWorks is functional and handling calls appropriately. For more information, see BroadWorks-specific documentation.
2. Configure BroadWorks phone users.	Complete the following procedure: • Procedure: Configuring BroadWorks phone users, on page 106
3. Configure a BroadWorks endpoint for a SIP Server host.	Complete the following procedure: • Procedure: Configuring a BroadWorks endpoint for a SIP Server host, on page 108
4. Configure BroadWorks BLF.	Complete the following procedure: • Procedure: Configuring BroadWorks BLF, on page 110

Procedures

This section describes important configuration steps that you must perform on the BroadWorks side.

Procedure:
Configuring BroadWorks phone users

Purpose: To configure SIP endpoints (phone users) to be registered with BroadWorks.

Start of procedure

1. Create a phone user profile (see Figure 71).

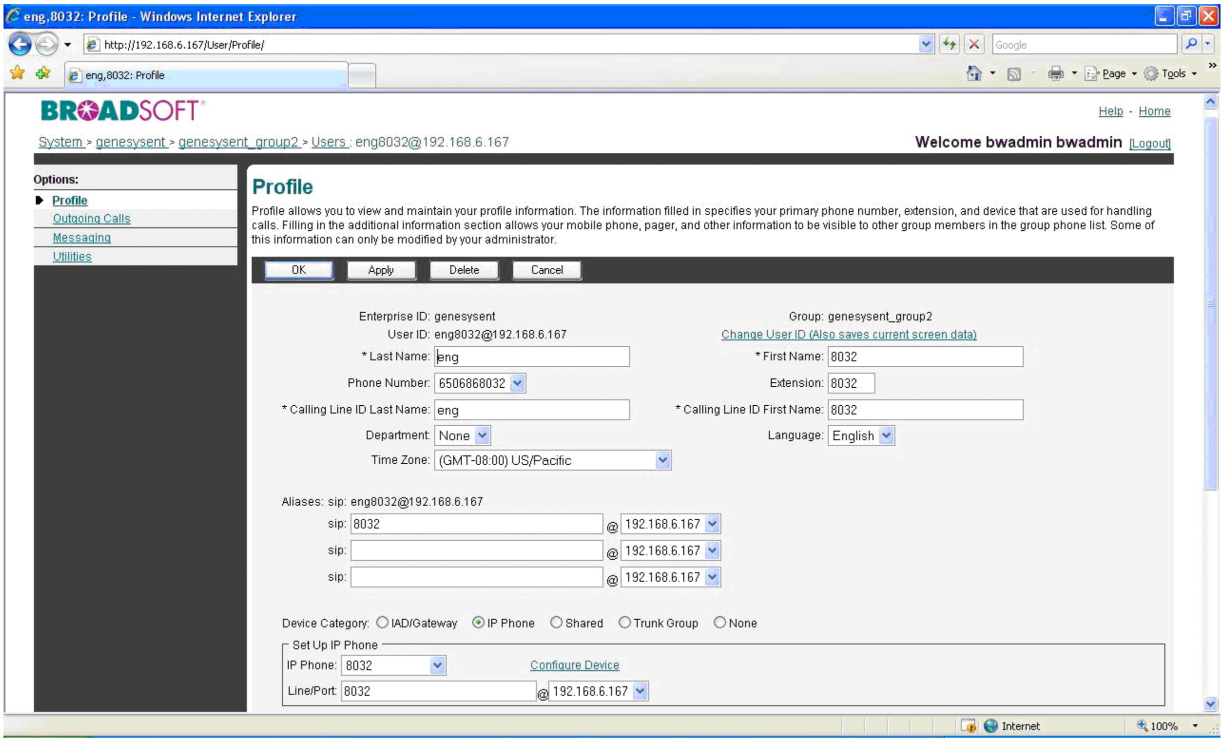

Figure 71: Creating the 8032 Phone User Profile: Sample Configuration

2. Configure a device for the phone user (see Figures 72–73).

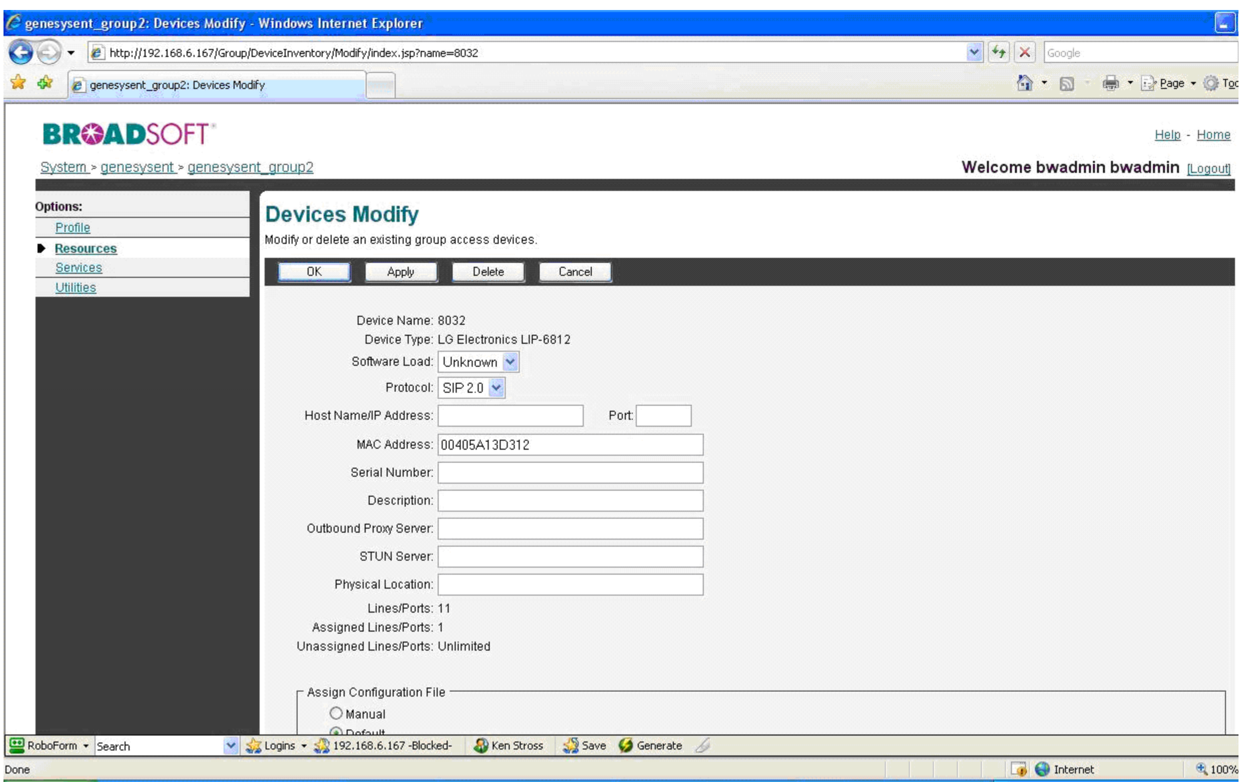

Figure 72: Configuring the 8032 Phone User Device (Screen 1): Sample Configuration

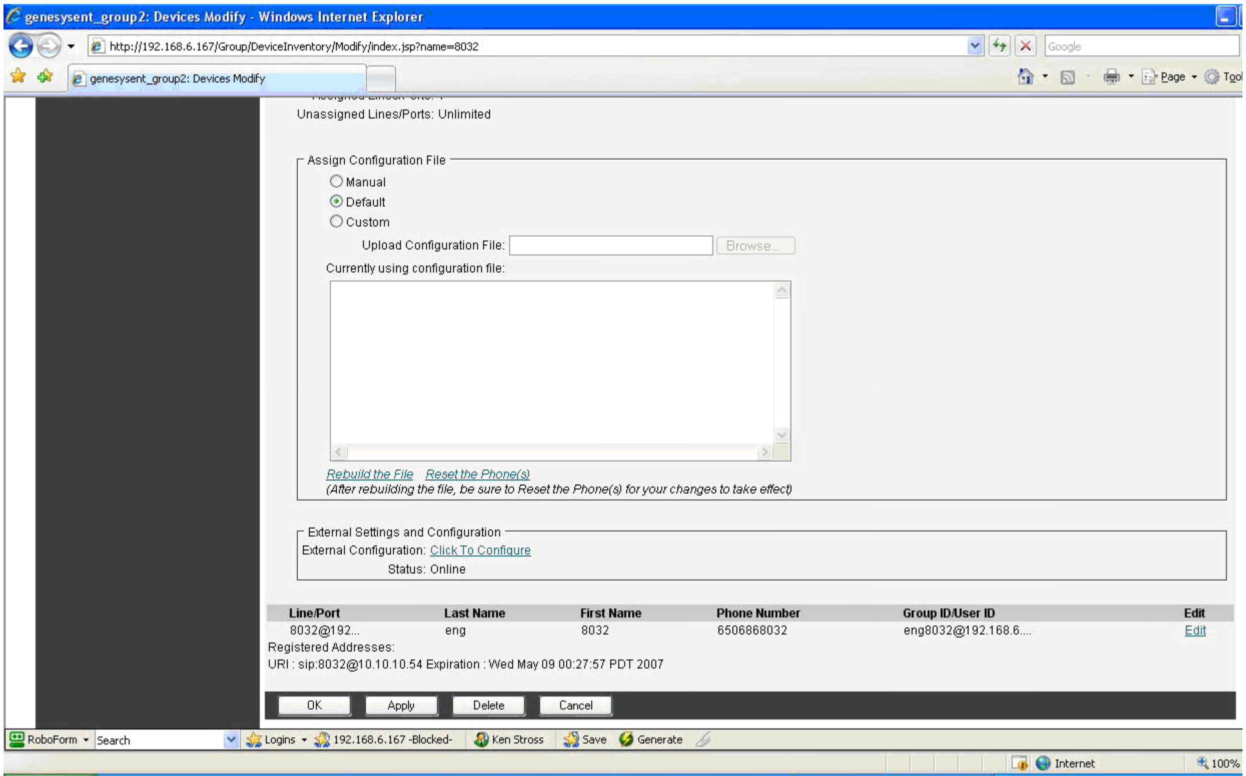

Figure 73: Configuring the 8032 Phone User Device (Screen 2): Sample Configuration

3. When you are finished, click `OK`.

End of procedure

Next Steps

- Procedure: Configuring a BroadWorks endpoint for a SIP Server host

Procedure: Configuring a BroadWorks endpoint for a SIP Server host

Purpose: To configure an endpoint that connects to SIP Server. This step is required only on the BroadWorks side; it helps set up routing in BroadWorks, so that is can route inbound calls to SIP Server.

Start of procedure

1. Configure an endpoint for a SIP Server host (see Figure 74).

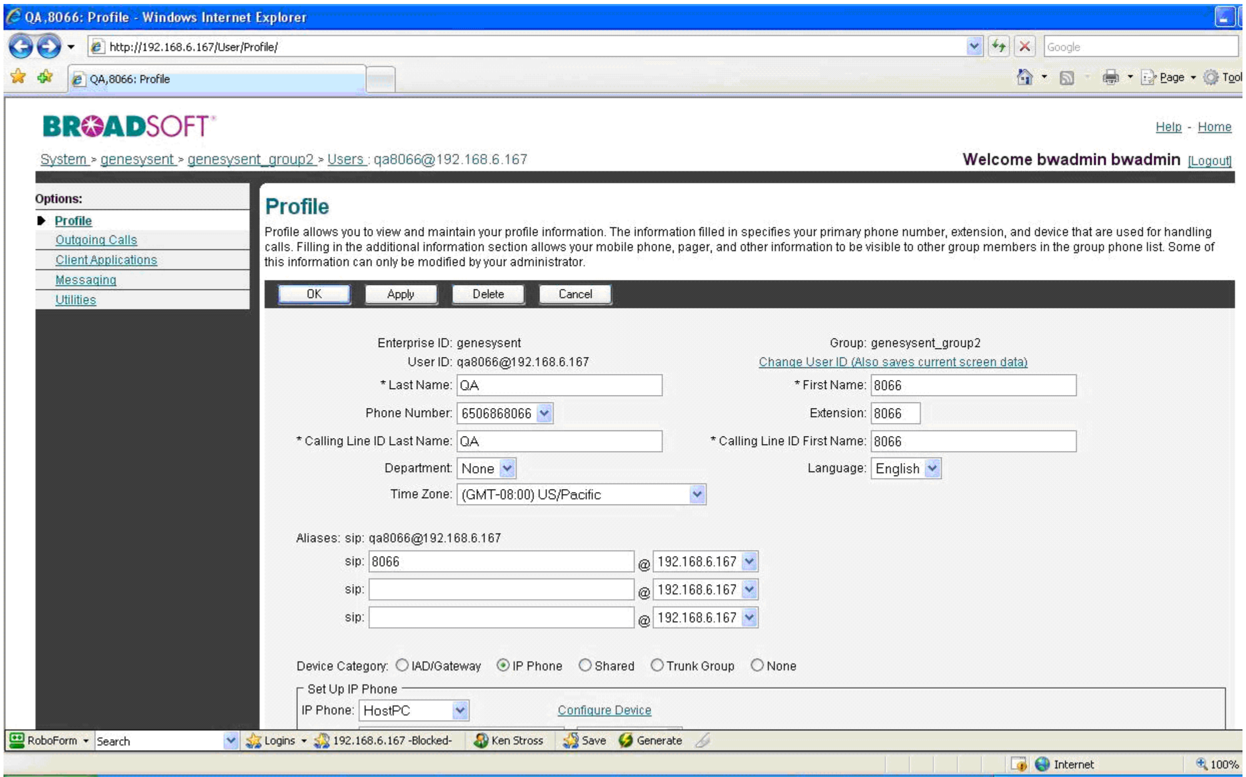

Figure 74: Configuring Endpoint 8066 for a SIP Server Host: Sample Configuration

2. When you are finished, click `OK`.
3. Modify a device for the endpoint (see Figure 75).

   Note that the `HostPC` device contains the SIP Server IP address as the host name. Also note that the setting does not have a corresponding setting in the SIP Server configuration.

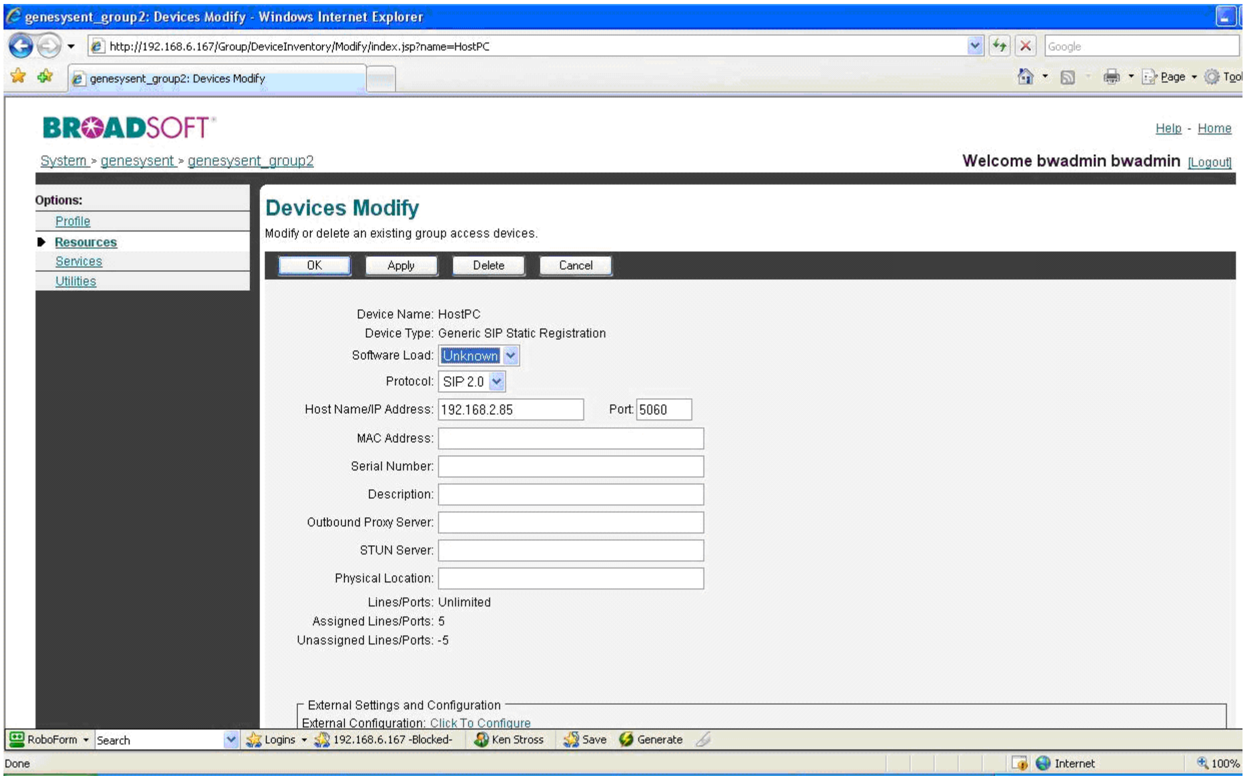

Figure 75: Modifying a Device for Endpoint 8066: Sample Configuration

4. When you are finished, click `OK`.

End of procedure

Next Steps

- Procedure: Configuring BroadWorks BLF

Procedure: Configuring BroadWorks BLF

Purpose: To create a user with an assigned Client Application BLF. In this sample configuration, the phone user number is `8026` and the access URI is `8866@192.168.6.167`. This BLF monitors multiple phone users, one of which is the agent 8032.

Start of procedure

1. Configure a user with an assigned Client Application BLF (see Figure 76).

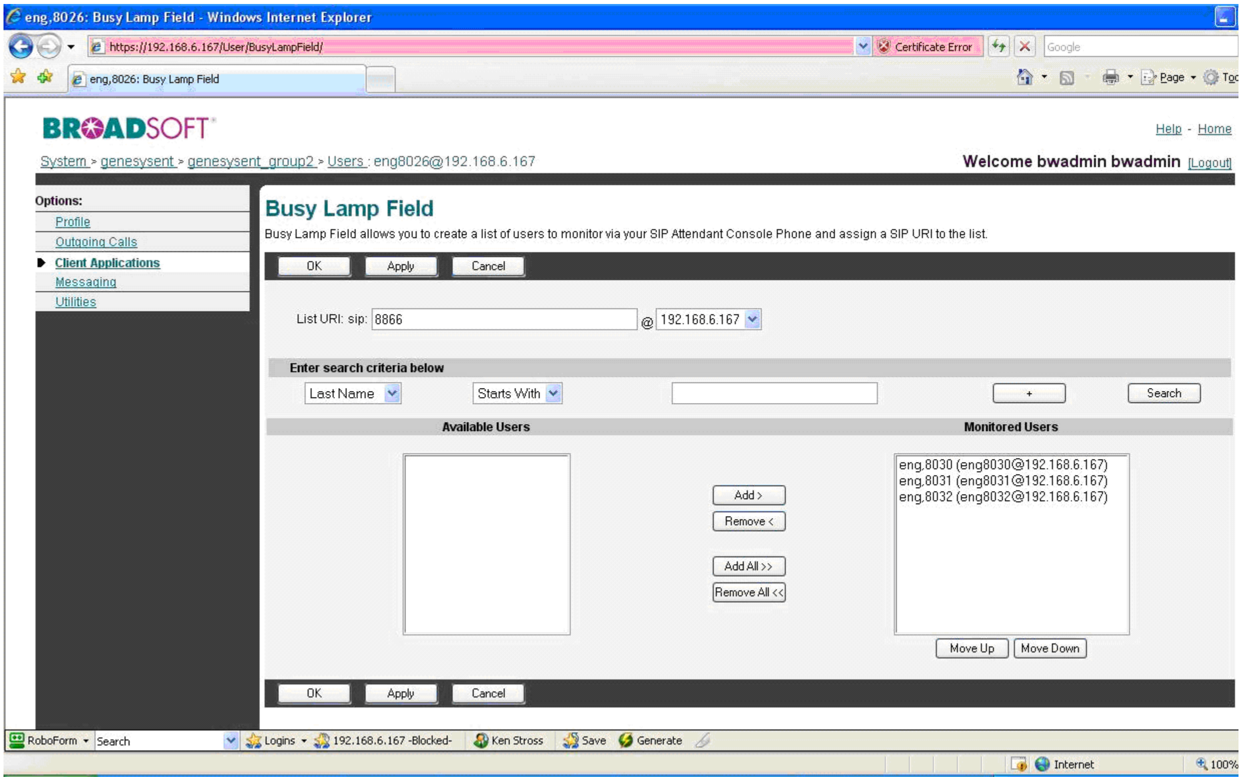

Figure 76: Configuring User 8026 Client Application BLF: Sample Configuration

The BroadWorks system is currently limited to a maximum of 50 users (endpoints) per BLF URI. This BLF URI is configured as a value of the `request-uri` configuration option (see page 113) for a DN of type `Voice Over IP Service`. Multiple BLF entries can be configured in BroadWorks, and SIP Server can be configured to subscribe to multiple BLFs.

In other words, if there are 50 BroadWorks endpoints (50 DNs of type `Extension` in the SIP Server configuration), it is possible for all of them to be part of one BLF entry. In this case, you configure one DN of type `Voice Over IP Service` (see "Configuring a Voice over IP Service DN" on page 112), SIP Server sets `Subscription` for that BLF, and BroadWorks will notify (by sending `NOTIFY` messages) SIP Server about the status of all 50 endpoints that are part of that BLF entry. If there are more than 50 endpoints, you must configure more than one BLF entry in BroadWorks.

For more information about this configuration or routing configuration, see your BroadWorks Application Server documentation.

2. When you are finished, click `OK`.

End of procedure

Configuring BroadWorks DN Objects

Table 16 provides an overview of the main steps to configure DNs under the BroadWorks `Switch` object in the Configuration Layer.

Table 16: Task Flow—Configuring DNs for the BroadWorks Switch Object

Objective	Related Procedures and Actions
1. Configure a `Voice over IP Service` DN.	Complete the following procedure: • Procedure: Configuring a Voice over IP Service DN, on page 112
2. Configure `Extension` DNs.	Complete the following procedure: • Procedure: Configuring Extension DNs, on page 115
3. Configure a `Trunk` DN.	Complete the following procedure: • Procedure: Configuring a Trunk DN for external access through BroadWorks, on page 117

Procedures

There are no particular configuration options related to BroadWorks integration at the SIP Server application level. Instead, you configure DNs for the BroadWorks `Switch` object that is assigned to the appropriate SIP Server.

Procedure:
Configuring a Voice over IP Service DN

Purpose: To configure a DN of type `Voice over IP Service` that supports the presence `SUBSCRIBE/NOTIFY` feature.

Start of procedure

1. Under a configured `Switch` object, select the `DNs` folder. From the `File` menu, select `New > DN` to create a new `DN` object.
2. In the `New DN Properties` dialog box, click the `General` tab, and then specify the following properties (see Figure 77):
   a. `Number:` Enter a name for this DN—for example, `8026`. This name must be unique within the configuration. The name of this DN does not need to correspond to any configuration on BroadWorks.

b. `Type:` Select `Voice over IP Service` from the drop-down box.

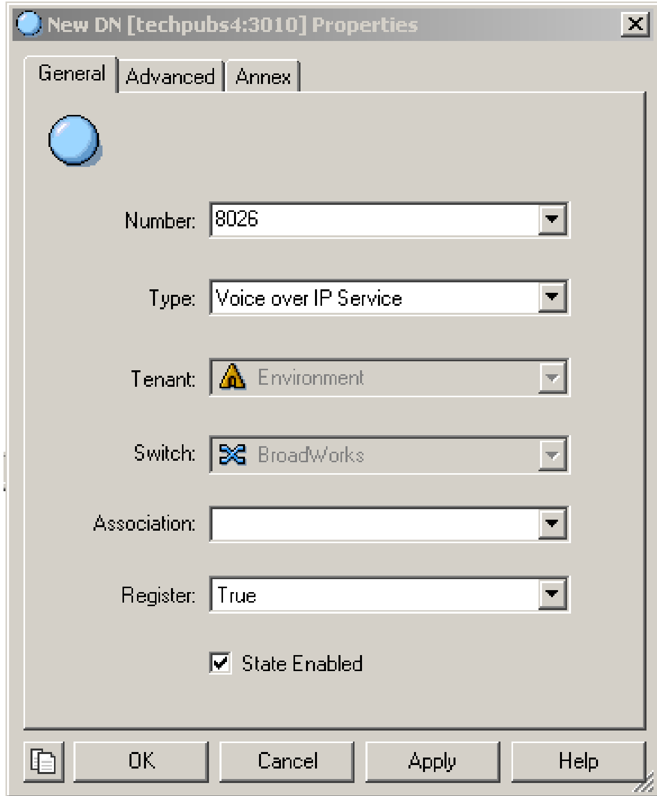

Figure 77: Creating a Voice over IP Service DN for BroadWorks: Sample Configuration

3. Click the `Annex` tab.
4. Create a section named `TServer`. In the `TServer` section, create options as specified in Table 17 (see Figure 78).

Table 17: Configuring a Voice over IP Service DN

Option Name	Option Value	Description
contact	SIP URI	Specifies the host and SIP port to which SIP Server sends the `SUBSCRIBE` message—in this case, the BroadWorks contact.
request-uri	SIP URI	Specifies the access URI for the BLF. **Note:** The request URI must be the same as the URI in the BroadWorks configuration. See “Configuring BroadWorks BLF” on page 110.
service-type	`blf`	Set this option to `blf`.

Table 17: Configuring a Voice over IP Service DN (Continued)

Option Name	Option Value	Description
subscribe-presence-from	SIP URI	Specifies the subscription endpoint information. This option value will be used to form the `From:` header in the `SUBSCRIBE` request to the softswitch.
subscribe-presence-expire	Any positive integer	Specifies the subscription renewal interval (in seconds).

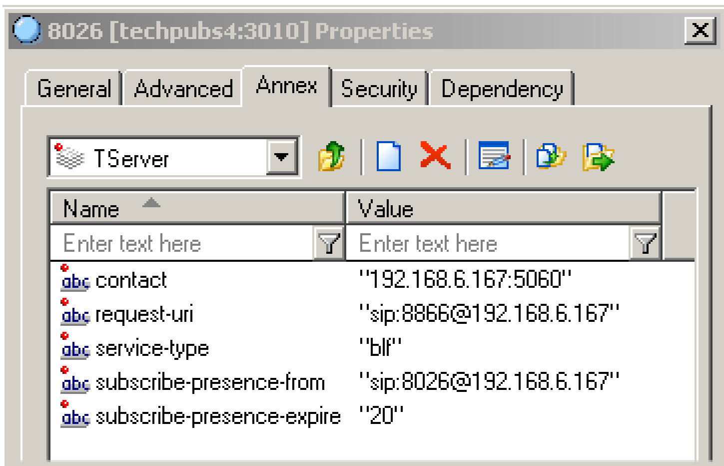

Figure 78: Setting Options for the Voice over IP Service DN: Sample Configuration

5. When you are finished, click `Apply`.

   The following is an example of the subscription message that SIP Server sends:

```
SUBSCRIBE sip:8866@192.168.6.167 SIP/2.0
From: <sip:8026@192.168.6.167>;tag=49943F92-B5F2-41DE-8AB0-
A9AEDA6A58B6-1
To: <sip:8866@192.168.6.167>
Call-ID: 16AECC4F-C7E4-49BF-974A-A1CE8F838494-1@192.168.14.109
CSeq: 1 SUBSCRIBE
Content-Length: 0
Via: SIP/2.0/UDP 192.168.14.109:5060;branch=z9hG4bKD77D63AD-10A2-
4E75-A345-
5D6E65E0EAD0-1
Event: dialog
```

```
Accept: application/dialog-info+xml, application/rlmi+xml,
multipart/related
Supported: eventlist
Max-Forwards: 70
Contact: <sip:192.168.14.109:5060>
Expires: 1800
```

End of procedure

Next Steps

- Procedure: Configuring Extension DNs

Procedure: Configuring Extension DNs

Purpose: To configure each BroadWorks endpoint that needs to be monitored and controlled by SIP Server.

Start of procedure

1. Under a configured `Switch` object, select the `DNs` folder. From the `File` menu, select `New > DN` to create a new `DN` object.
2. In the `New DN Properties` dialog box, click the `General` tab, and then specify the following properties (see Figure 79):
   a. `Number:` Enter a name for the `Extension` DN. In general, this should be the phone number of the extension. You must not use the @ symbol or a computer name.
   b. `Type:` Select `Extension` from the drop-down box.

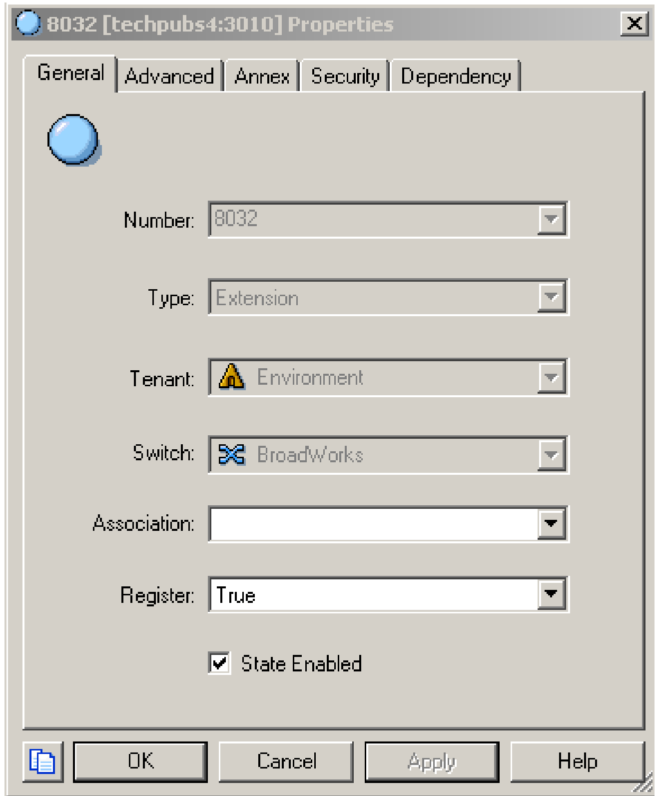

Figure 79: Creating an Extension DN: Sample Configuration

3. Click the `Annex` tab.
4. Create a section named `TServer`. In the `TServer` section, create options as specified in Table 18 (see Figure 80).

Table 18: Configuring an Extension DN

Option Name	Option Value	Description
contact	SIP URI	Specifies the contact URI to which SIP Server sends the `INVITE` message.
refer-enabled	`false`	Set this option to `false` for SIP Server to use a `re-INVITE` request method when contacting BroadWorks.

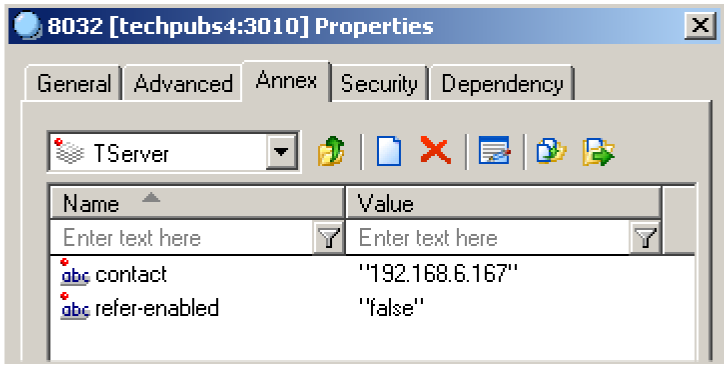

Figure 80: Setting Options for the Extension DN: Sample Configuration

5. When you are finished, click `Apply`.

End of procedure

Procedure: Configuring a Trunk DN for external access through BroadWorks

Purpose: To configure a DN f type `Trunk` for external access through BroadWorks.

Summary

In order for SIP Server to contact external numbers by going through BroadWorks, you can configure one or several `Trunk` DNs with the `contact` option set to the BroadWorks address and port.

You can define multiple rules. This part of the configuration is identical to the configuration when SIP Server is deployed in Stand-alone mode, except that access to gateways is replaced with access to BroadWorks in this procedure.

Start of procedure

1. Under a configured `Switch` object, select the `DNs` folder. From the `File` menu, select `New` > `DN` to create a new `DN` object.
2. In the `New DN Properties` dialog box, click the `General` tab, and then specify the following properties:
   a. `Number`: Enter a name for the external access DN. This name can be any unique value, and it can be a combination of letters and numbers.
   b. `Type`: Select `Trunk` from the drop-down box.
3. Click the `Annex` tab.

4. Create a section named `TServer`. In the `TServer` section, create options as specified in Table 19 (see Figure 81).

Table 19: Configuring a Trunk DN for External Access

Option Name	Option Value	Description
contact	SIP URI	Specifies the contact URI to which SIP Server sends the `SUBSCRIBE` message.
prefix	Any positive integer	Specifies the initial digits of the number used to direct to BroadWorks any call that SIP Server does not recognize as an internal DN.
refer-enabled	`false`	Set this option to `false` for SIP Server to use a `re-INVITE` request method when contacting BroadWorks.

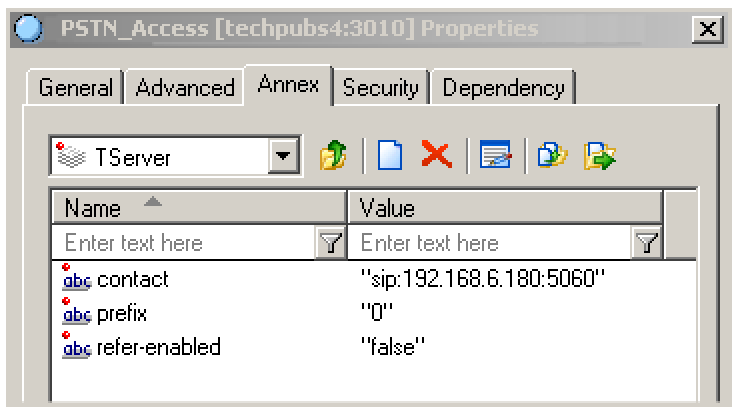

Figure 81: Setting Options for a Trunk DN for External Access: Sample Configuration

5. When you are finished, click `Apply`.

End of procedure

Chapter

4 SIP Server Integration with the Cisco Media Gateway

This chapter describes how to integrate SIP Server with the Cisco Media Gateway Controller (MGC). It contains the following sections:

Note: The instructions in this chapter assume that the Cisco Media Gateway is fully functional and routing calls before Genesys products are installed. They also assume that SIP Server has already been configured to function properly in Stand-alone mode.

Overview

The SIP Server and Cisco Media Gateway integration solution described in this chapter is not the only method that will work. Although there are other methods, this is the only one that has been tested and approved by Genesys, and that is supported by Genesys Customer Support.

The following Cisco IOS Software versions were tested:

- 2800 Series
- 3700 Series
- 3800 Series
- 5300 Series
- 5400 Series

Note: For confirmation of the supported Cisco IOS Software versions, contact Genesys Technical Support. For more information about Cisco IOS Software, go to the Cisco web site at `http://www.cisco.com/`.

Deployment Architecture

Figures 82 depicts a sample deployment architecture of SIP Server with Cisco Media Gateway.

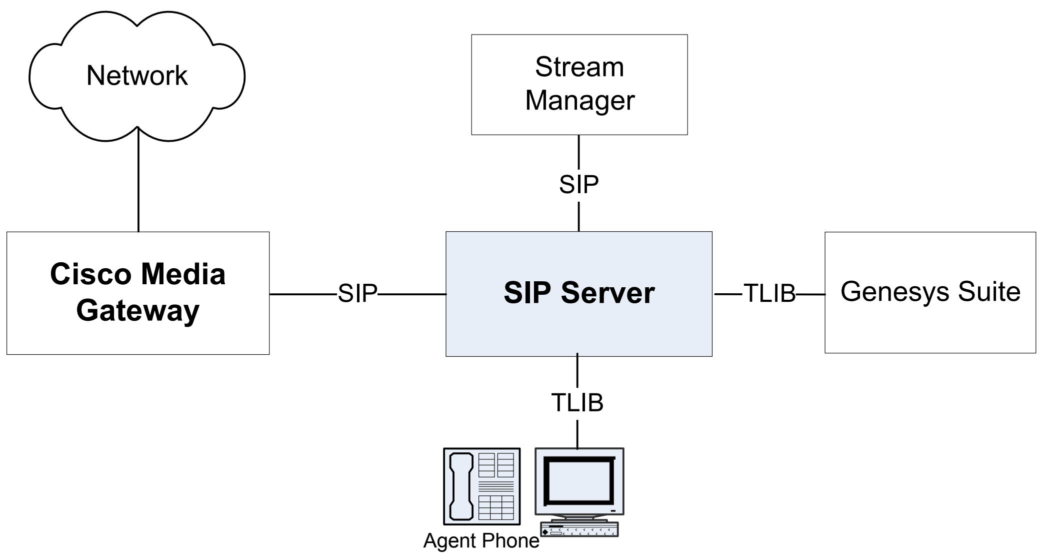

Figure 82: SIP Server - Cisco Media Gateway Deployment Architecture

Integration Task Summary

Table 20 summarizes the steps that are required in order to integrate SIP Server with Cisco Media Gateway.

Table 20: Task Summary—Integrating SIP Server with Cisco Media Gateway

Objective	Related Procedures and Actions
1. Configure Cisco Media Gateway.	See Table 21 on page 121.
2. Configure a Cisco Media Gateway object in the Configuration Layer.	See Table 22 on page 127.

Configuring Cisco Media Gateway

Table 21 provides an overview of the main steps that are required in order to configure Cisco Media Gateway.

Table 21: Task Flow—Configuring Cisco Media Gateway

Objective	Related Procedures and Actions
1. Confirm that Cisco Media Gateway is functional and handling calls appropriately.	The procedures in this chapter assume that Cisco Media Gateway is functional and handling calls appropriately. For more information, see Cisco Media Gateway-specific documentation.
2. Configure an E1 environment.	Complete the following procedure: • Procedure: Configuring an E1 environment, on page 121
3. Configure a T1 CAS environment.	Complete the following procedure: • Procedure: Configuring a T1 CAS environment, on page 123
4. Configure a T1 PRI environment.	Complete the following procedure: • Procedure: Configuring a T1 PRI environment, on page 124
5. Configure an E1 PRI environment.	Complete the following procedure: • Procedure: Configuring an E1 PRI environment, on page 126
6. Configure a SIP User Agent.	Complete the following procedure: • Procedure: Configuring a SIP User Agent, on page 127

Procedures

The following section describes configuration to be performed on the Cisco Media Gateway side.

Procedure: Configuring an E1 environment

Purpose: To configure an E1 environment. This section provides an example of an E1 configuration.

Start of procedure

1. Configure a controller:

```
controller E1 0/2/0
   framing NO-CRC4
   ds0-group 0 timeslots 1 type fxo-loop-start
   ds0-group 1 timeslots 2 type fxo-loop-start
   ds0-group 2 timeslots 3 type fxo-loop-start
```

2. Configure voice ports:

```
voice-port 0/2/0:0
   output attenuation 0
   station-id name 2300090
voice-port 0/2/0:1
   output attenuation 0
   station-id name 2300091
voice-port 0/2/0:2
   output attenuation 0
   station-id name 2300092
```

3. Configure dial peers:

```
dial-peer voice 2300090 pots
   destination-pattern 6...
   supplementary-service pass-through
   port 0/2/0:0
   forward-digits all
dial-peer voice 2300091 pots
   destination-pattern 6...
   supplementary-service pass-through
   port 0/2/0:1
   forward-digits all
dial-peer voice 2300092 pots
   destination-pattern 6...
   supplementary-service pass-through
   port 0/2/0:2
   forward-digits all
dial-peer voice 8800 voip
service session
destination-pattern 8800
voice-class codec 4
```

```
session protocol sipv2
session target ipv4:192.168.50.137
dtmf-relay rtp-nte
supplementary-service pass-through
```

End of procedure

Next Steps

- Procedure: Configuring a T1 CAS environment

Procedure: Configuring a T1 CAS environment

Purpose: To configure a T1 CAS environment. This section provides an example of a T1 CAS configuration.

Start of procedure

1. Configure a controller:

```
controller T1 1/0/1
   framing sf
   clock source internal
   linecode ami
   ds0-group 0 timeslots 1 type e&m-immediate-start
   ds0-group 1 timeslots 2 type e&m-immediate-start
   ds0-group 2 timeslots 3 type e&m-immediate-start
```

2. Configure voice ports:

```
voice-port 0/2/0:0
   output attenuation 0
   station-id name 2300090
voice-port 0/2/0:1
   output attenuation 0
   station-id name 2300091
voice-port 0/2/0:2
   output attenuation 0
   station-id name 2300092
```

3. Configure dial peers:

```
dial-peer voice 2300090 pots
   destination-pattern 6...
   supplementary-service pass-through
   port 0/2/0:0
   forward-digits all
dial-peer voice 2300091 pots
   destination-pattern 6...
   supplementary-service pass-through
   port 0/2/0:1
   forward-digits all
dial-peer voice 2300092 pots
   destination-pattern 6...
   supplementary-service pass-through
   port 0/2/0:2
   forward-digits all
dial-peer voice 8800 voip
   service session
   destination-pattern 8800
   voice-class codec 4
   session protocol sipv2
   session target ipv4:192.168.50.137
   dtmf-relay rtp-nte
   supplementary-service pass-through
```

End of procedure

Next Steps

- Procedure: Configuring a T1 PRI environment

Procedure: Configuring a T1 PRI environment

Purpose: To configure a T1 PRI environment. This section provides an example of a T1 PRI configuration.

Start of procedure

1. Configure a controller:

```
controller T1 0/0/0
    framing esf
    linecode b8zs
    pri-group timeslots 1-24
```

2. Configure an interface serial:

```
interface Serial0/0/0:23
    no ip address
    encapsulation hdlc
    isdn switch-type primary-ni
    isdn incoming-voice voice
    no cdp enable
```

3. Configure a voice port:

```
voice-port 0/0/0:23
```

4. Configuring dial peers:

```
dial-peer voice 9 pots
    destination-pattern 9T
    incoming called-number 9...
    port 0/0/0:23
dial-peer voice 8800 voip
    service session
    destination-pattern 8800
    voice-class codec 4
    session protocol sipv2
    session target ipv4:192.168.50.137
    dtmf-relay rtp-nte
    supplementary-service pass-through
```

End of procedure

Next Steps

- Procedure: Configuring an E1 PRI environment

Procedure: Configuring an E1 PRI environment

Purpose: To configure an E1 PRI environment. This section provides an example of an E1 PRI configuration.

Start of procedure

1. Configure a controller:

```
controller E1 0/2/1
   framing NO-CRC4
   pri-group timeslots 1-31
```

2. Configure an interface serial:

```
interface Serial0/2/1:15
   no ip address
   encapsulation hdlc
   isdn switch-type primary-net5
   isdn protocol-emulate network
   isdn incoming-voice voice
   no cdp enable
```

3. Configure a voice port:

```
voice-port 0/2/1:15
```

4. Configure dial peers:

```
dial-peer voice 130 pots
   destination-pattern 130T
   direct-inward-dial
   port 0/2/1:15
dial-peer voice 8800 voip
   service session
   destination-pattern 8800
   voice-class codec 4
   session protocol sipv2
   session target ipv4:192.168.50.137
   dtmf-relay rtp-nte
   supplementary-service pass-through
```

End of procedure

Next Steps

- Procedure: Configuring a SIP User Agent

Procedure: Configuring a SIP User Agent

Purpose: To configure a SIP User Agent. This section provides an example of a SIP User Agent configuration.

Start of procedure

- Configure a SIP User Agent: enter global configuration "configure terminal":

```
sip-ua
    timers notify 400
    sip-server dns:host.genesyslab.com
```

End of procedure

Configuring Cisco Media Gateway DN Objects

Table 22 provides an overview of the main step to configure a `Trunk` DN for Cisco Media Gateway under the `Switch` object associated with SIP Server in the Configuration Layer.

Table 22: Task Flow—Configuring a Trunk DN for Cisco Media Gateway

Objective	Related Procedures and Actions
Configure a `Trunk` DN.	Complete the following procedure: • Procedure: Configuring a Trunk DN for Cisco Media Gateway, on page 128

Procedure

Procedure: Configuring a Trunk DN for Cisco Media Gateway

Purpose: To configure a DN of type `Trunk` for Cisco Media Gateway.

Start of procedure

1. Under a configured `Switch` object, select the `DNs` folder. From the `File` menu, select `New > DN` to create a new `DN` object.
2. In the `New DN Properties` dialog box, click the `General` tab, and then specify the following properties (see Figure 83):
   a. `Number:` Enter the gateway name.
   b. `Type:` Select `Trunk` from the drop-down box.

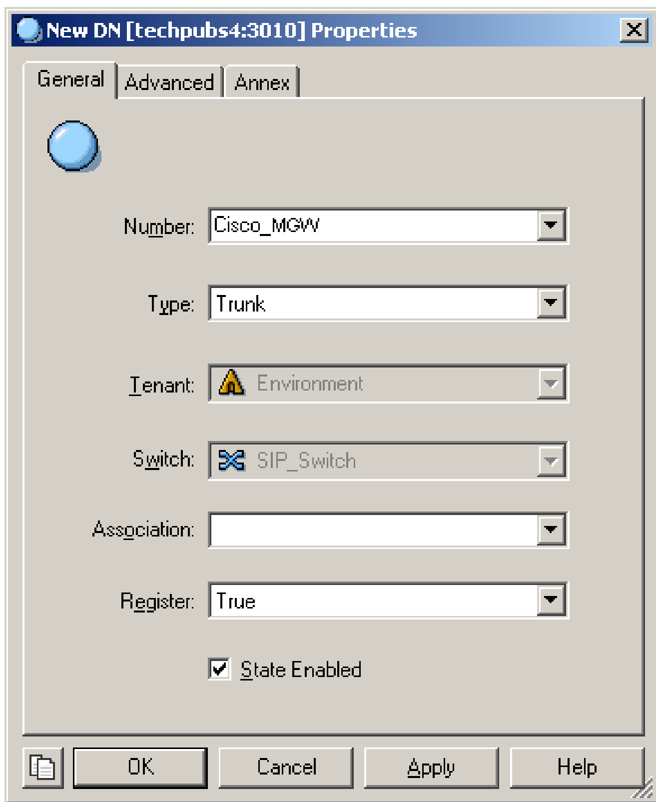

Figure 83: Creating a Trunk DN for Cisco Media Gateway: Sample Configuration

3. Click the `Annex` tab.

4. Create a section named `TServer`. In the `TServer` section, create options as specified in Table 23.

Table 23: Configuring a Trunk DN

Option Name	Option Value	Description
contact	`<ipaddress>:` `<SIP port>`	Specifies the contact URI that SIP Server uses for communication with the gateway, where `<ipaddress>` is the IP address of the gateway and `<SIP port>` is the SIP port number of the gateway.
oos-check	0-300	Specifies how often (in seconds) SIP Server checks a DN for out-of-service status.
oos-force	0-30	Specifies how long (in seconds) SIP Server waits before placing a DN out-of-service.
prefix	Any numerical string	Specifies the initial digits of the number that SIP Server matches to determine whether this trunk should be used for outbound calls. For example, if `prefix` is set to `78`, dialing a number starting with 78 will cause SIP Server to consider this trunk a gateway or SIP proxy. If multiple `Trunk` objects match the prefix, SIP Server will select the one with the longest prefix that matches.
priority	Any non-negative integer	Specifies a gateway priority that SIP Server uses to decide a route. A smaller number designates higher priority. If more than one gateway with the same prefix is selected, the gateway with highest priority is normally selected. This `priority` option is used to control primary-backup gateway switchover, and to provide lowest-cost routing.
refer-enabled	`false`	Set this option to `false` for SIP Server to use a `re-INVITE` request method when contacting the gateway. This is the only method supported in the Cisco Media Gateway configuration.
recovery-timeout	`0–86400`	Specifies whether a gateway is taken out of service when an error is encountered, and how long (in seconds) it is out of service.
replace-prefix	Any numerical string	Specifies the digits that replace the prefix in the DN. For example, if `prefix` is set to `78`, and `replace-prefix` is set to `8`, the number `786505551212` will be replaced with `86505551212` before it is sent to the gateway or SIP proxy (here, Cisco Media Gateway).

5. When you are finished, click `Apply`.

End of procedure

Chapter

5 SIP Server Integration with the AudioCodes Gateway

This chapter describes how to integrate SIP Server with the AudioCodes Gateway. It contains the following sections:

Note: The instructions in this chapter assume that the AudioCodes Gateway is fully functional and connected to the corresponding PBX.

Overview

The SIP Server and AudioCodes integration solution described in this chapter is not the only method that will work. Although there are other methods, this is the only one that has been tested and approved by Genesys, and that is supported by Genesys Customer Support.

In the configuration example, the AudioCodes IPMedia 2000 Gateway is used. The same configuration procedures are also applicable to the AudioCodes Mediant 2000 and the TP (or TrunkPack) gateways.

Deployment Architecture

Figures 84 depicts a sample deployment architecture of SIP Server with the AudioCodes Gateway.

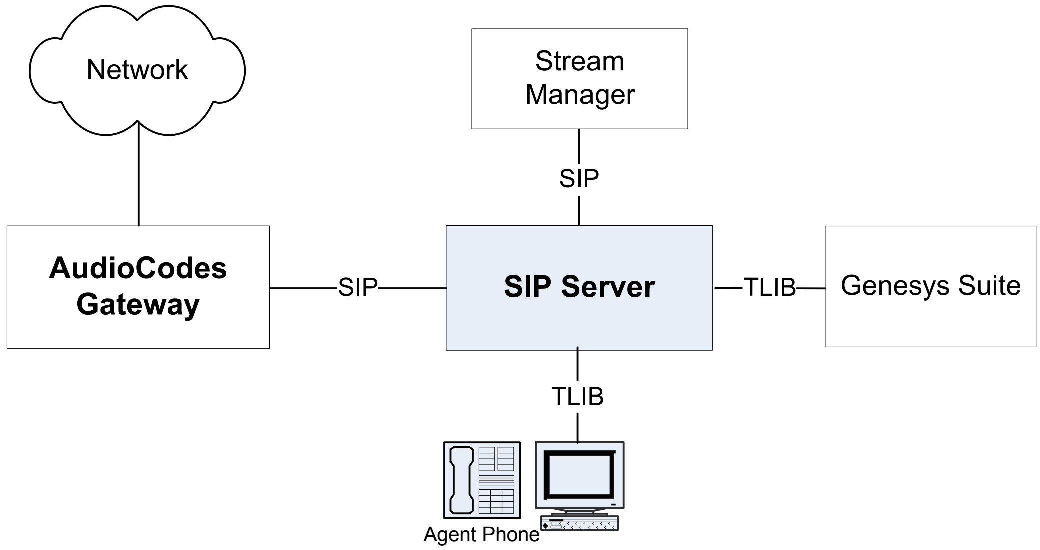

Figure 84: SIP Server - AudioCodes Gateway Deployment Architecture

Integration Task Summary

Table 24 summarizes the steps that are required in order to integrate SIP Server with the AudioCodes Gateway.

Table 24: Task Summary—Integrating SIP Server with the AudioCodes Gateway

Objective	Related Procedures and Actions
1. Configure the AudioCodes Gateway.	See Table 25 on page 133.
2. Configure an AudioCodes Gateway object in the Configuration Layer.	See Table 26 on page 134.

Configuring the AudioCodes Gateway

Table 25 provides an overview of the main steps that are required in order to configure the AudioCodes Gateway.

Table 25: Task Flow—Configuring the AudioCodes Gateway

Objective	Related Procedures and Actions
1. Confirm that AudioCodes Gateway is functional and handling calls appropriately.	The procedures in this chapter assume that AudioCodes Gateway is functional and handling calls appropriately. For more information, see AudioCodes Gateway-specific documentation.
2. Configure the AudioCodes Gateway.	Complete the following procedure: • Procedure: Configuring the AudioCodes Gateway

Procedure

The following section important configuration steps that you must perform on the AudioCodes Gateway side.

Procedure: Configuring the AudioCodes Gateway

Purpose: To configure the AudioCodes Gateway to support integration with SIP Server.

Start of procedure

1. Log in to the AudioCodes web administrative interface (see Figure 85).
2. From the left pane menu, select `Protocol Management`.
3. Navigate to the `Routing Tables` tab, and select `Tel to IP Routing` from the drop-down menu.
4. In the `Dest. Phone Prefix` text box, enter the DNs that you will be routing through the gateway.
5. In the `Source Phone Prefix` text box, enter an asterisk (*) to accept any source phone number.
6. In the `Dest. IP Address` text box, enter the SIP Server IP address and port. Note that port is only required if other than default port `5060` is used.

   In the example configuration (see Figure 85), line 14 demonstrates that the range of DNs `4030` through `4039` is passed through the AudioCodes Gateway to SIP Server at the address `192.168.22.63, port 6060`.

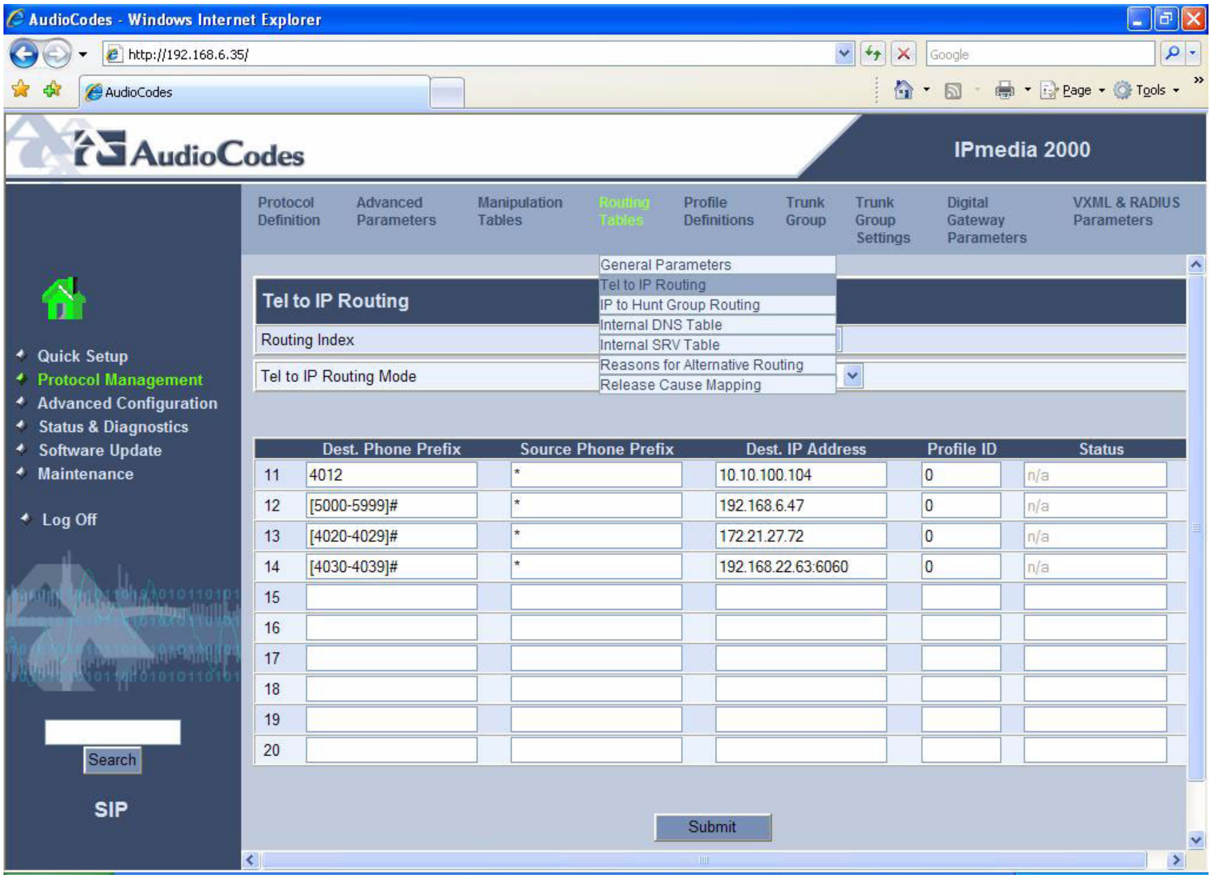

Figure 85: Configuring the AudioCodes Gateway: Sample Configuration

End of procedure

Configuring AudioCodes Gateway DN Objects

Table 26 provides an overview of the main step to configure a `Trunk` DN for the AudioCodes Gateway under the `Switch` object associated with SIP Server in the Configuration Layer.

Table 26: Task Flow—Configuring a Trunk DN for the AudioCodes Gateway

Objective	Related Procedures and Actions
Configure a `Trunk` DN.	Complete the following procedure: • Procedure: Configuring a Trunk DN for the AudioCodes Gateway

Procedure

Procedure: Configuring a Trunk DN for the AudioCodes Gateway

Purpose: To configure a DN of type `Trunk` for the AudioCodes Gateway.

Start of procedure

1. Under a configured `Switch` object, select the `DNs` folder. From the `File` menu, select `New > DN` to create a new `DN` object.
2. In the `New DN Properties` dialog box, click the `General` tab, and then specify the following properties (see Figure 86):
   a. `Number:` Enter the gateway name.
   b. `Type:` Select `Trunk` from the drop-down box.

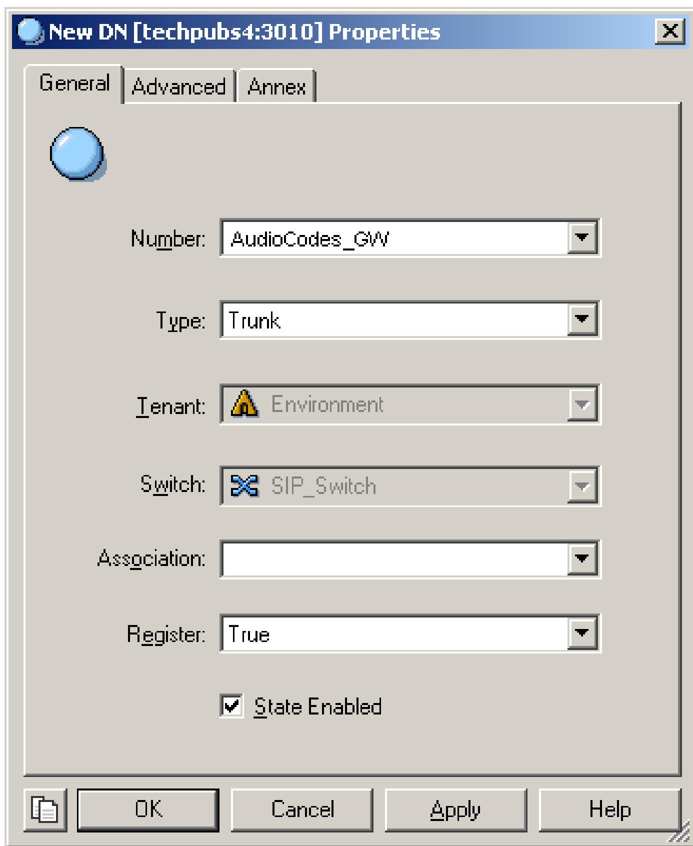

Figure 86: Creating a Trunk DN for the AudioCodes Gateway: Sample Configuration

3. Click the `Annex` tab.

4. Create a section named `TServer`. In the `TServer` section, create options as specified in Table 27.

Table 27: Configuring a Trunk DN

Option Name	Option Value	Description
contact	`<ipaddress>:<SIP port>`	Specifies the contact URI that SIP Server uses for communication with the gateway, where `<ipaddress>` is the IP address of the gateway and `<SIP port>` is the SIP port number of the gateway.
oos-check	0-300	Specifies how often (in seconds) SIP Server checks a DN for out-of-service status.
oos-force	0-30	Specifies how long (in seconds) SIP Server waits before placing a DN out-of-service.
prefix	Any numerical string	Specifies the initial digits of the number that SIP Server matches to determine whether this trunk should be used for outbound calls. For example, if `prefix` is set to `78`, dialing a number starting with 78 will cause SIP Server to consider this trunk a gateway or SIP proxy. If multiple `Trunk` objects match the prefix, SIP Server will select the one with the longest prefix that matches.
priority	Any non-negative integer	Specifies a gateway priority that SIP Server uses to decide a route. A smaller number designates higher priority. If more than one gateway with the same prefix is selected, the gateway with highest priority is normally selected. This `priority` option is used to control primary-backup gateway switchover, and to provide lowest-cost routing.
refer-enabled	`true`, `false`	Specifies whether the `REFER` method is sent to an endpoint. When set to `false`, SIP Server uses the `re-INVITE` method instead.
recovery-timeout	`0–86400`	Specifies whether a gateway is taken out of service when an error is encountered, and how long (in seconds) it is out of service.
replace-prefix	Any numerical string	Specifies the digits that replace the prefix in the DN. For example, if `prefix` is set to `78`, and `replace-prefix` is set to `8`, the number `786505551212` will be replaced with `86505551212` before it is sent to the gateway or SIP proxy (here, AudioCodes Gateway).

5. When you are finished, click `Apply`.

End of procedure

Chapter

6 SIP Server Integration with the F5 Networks BIG-IP Local Traffic Manager

This chapter describes how to integrate SIP Server with the F5 Networks BIG-IP Local Traffic Manager (hereafter referred to as *BIG-IP LTM*) to support SIP Server `hot standby` high-availability (HA) mode. It contains the following sections:

Note: The instructions in this chapter assume that BIG-IP LTM is fully functional. They also assume that Genesys SIP Server has already been installed and configured to function properly.

Overview

The SIP Server and BIG-IP LTM integration solution described in this chapter enables you to preserve SIP sessions between SIP Server and other SIP-enabled devices that are involved in contact center operations, in switchover scenarios.

In this integration solution, one Virtual Server configured on the BIG-IP LTM is associated with a single IP address (referred to as *Virtual IP address*), and it represents one HA pair of SIP Servers configured as members of one server pool that is associated with the Virtual Server. It is possible to have more than one HA pair running behind a single BIG-IP LTM. This requires configuring additional Virtual Servers and server pools for each HA pair in the way that the one unique Virtual IP address is used for each HA pair.

Integration Solution Notes

- Up-front load balancing via Network SIP Server or other device could be implemented, but is not described in this chapter.
- BIG-IP LTM supports an active/hot-standby HA mode itself; configuration of the LTM in HA mode is not described in this chapter and has not been validated with SIP Server.
- Either UDP or TCP can be used as the transport for SIP signaling. Use of TLS for encrypted SIP signaling has not been validated, and configuration of TLS is not described in this chapter.
- BIG-IP LTM can be configured in a more complex load-balancing role. This is beyond the scope of this chapter.

Deployment Architecture

Figure 87 depicts a sample deployment architecture of primary and backup SIP Servers with the BIG-IP LTM, in which:

- BIG-IP LTM is positioned as a network switch between a SIP Server HA pair and other network entities.
- BIG-IP LTM is configured to apply SNAT (Secure Network Address Translation) to all outbound packets, with the exception of destinations that are defined in the SNAT exclusion group.

Deployment Requirements

There are four different communication groups of devices that interact with SIP Server (see Figure 87). Each group has its own requirements that must be considered when configuring the BIG-IP LTM.

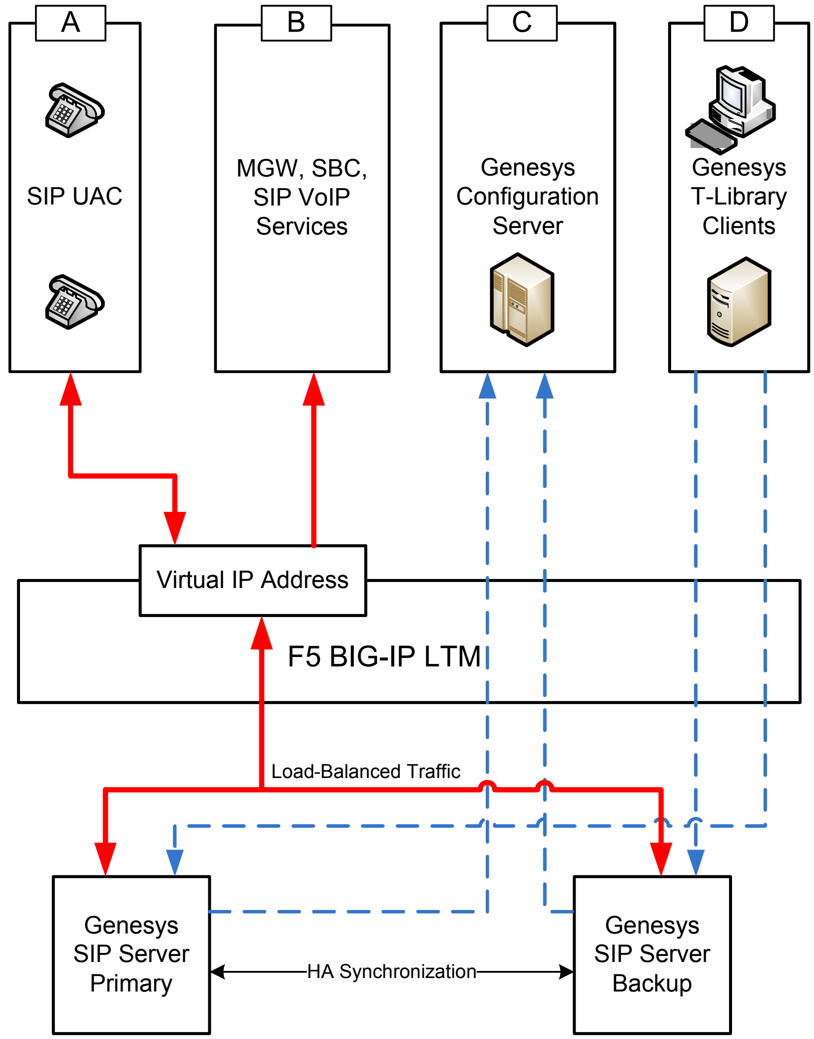

Figure 87: Device Communication Groups

SIP Phones Group

The SIP Phones group (group A in Figure 87) includes SIP phones that are used by agents.

Initially, devices of this group use the `REGISTER` method to notify SIP Server of the current `Contact` URI (IP address). SIP Server uses the `Contact` information for further communication with the device.

By default, SIP Server uses the UDP to communicate with devices of the group. Devices send requests to and receive responses from the BIG-IP LTM Virtual IP address.

This group requires that:

- Any inbound packets received at the BIG-IP LTM Virtual IP address are directed to the primary SIP Server.

- SNAT is applied to any outbound packets that are sent to devices of the group, which means that a source IP address of the outbound packet is translated from a SIP Server physical IP address to the BIG-IP LTM Virtual IP address.

SIP Service Devices Group

The SIP Service Devices group (group B in Figure 87) includes media gateways, softswitches, Session Border Controllers (SBC), and SIP-based VoIP Service devices such as Genesys Stream Manager. These devices do not register with SIP Server; their contact information is known in advance and it remains consistent.

By default, SIP Server uses the UDP to communicate with devices of the group. Devices receive requests from the BIG-IP LTM Virtual IP address.

This group requires that:

- Any inbound packets received at the BIG-IP LTM Virtual IP address are directed to the primary SIP Server.
- SNAT is applied to any outbound packets that are sent to devices of the group.

Genesys Configuration Server

SIP Server maintains permanent TCP/IP connection with Genesys Configuration Server (group C in Figure 87). Requests to Configuration Server are sent from a SIP Server physical IP address. Responses from Configuration Server are directed to the SIP Server physical IP address.

This group requires that:

- No SNAT is applied to outbound packets sent to Configuration Server.
- The primary or backup SIP Server is accessible via its physical IP address.

Genesys T-Library Clients Group

All Genesys T-Library clients (group D in Figure 87) that implement Genesys T-Library functionality maintain permanent TCP/IP connection with SIP Server. Devices send requests to and receive responses from a SIP Server (primary or backup) physical IP address.

This group requires that:

- No SNAT is applied to outbound packets sent to devices of the group.
- The primary or backup SIP Server is accessible via its physical IP address.

Note: In this deployment architecture, the HA synchronization traffic between primary and backup SIP Servers does not pass through the BIG-IP LTM, that is why it is excluded from applying SNAT.

Integration Task Summary

Table 28 summarizes the steps that are required in order to integrate SIP Server with the BIG-IP LTM.

Table 28: Task Summary—Integrating SIP Server with BIG-IP LTM

Objective	Related Procedures and Actions
1. Configure the BIG-IP LTM.	See Table 29.
2. Configure SIP Server HA.	See Table 30 on page 172.

Configuring the BIG-IP LTM

Table 29 provides an overview of the main steps that are required in order to configure the BIG-IP LTM. Complete all steps in the order in which they are listed.

Table 29: Task Flow—Configuring the BIG-IP LTM

Objective	Related Procedures and Actions
1. Confirm that the BIG-IP LTM is functional.	The procedures in this chapter assume that the BIG-IP LTM is properly licensed and fully functional, with login and password access configured. For more information, see BIG-IP LTM–specific documentation.
2. Configure VLANs.	Complete the following procedure: • Procedure: Configuring VLANs, on page 143
3. Configure Self IP addresses.	Complete the following procedure: • Procedure: Configuring Self IP addresses, on page 145
4. Configure the Default IP route.	Complete the following procedure: • Procedure: Configuring the Default IP route, on page 147
5. Configure SIP Server nodes.	Complete the following procedure: • Procedure: Configuring SIP Server nodes, on page 148

Table 29: Task Flow—Configuring the BIG-IP LTM (Continued)

Objective	Related Procedures and Actions
6. Modify the `sip_info` Persistence Profile.	Complete the following procedure: • Procedure: Modifying the sip_info Persistence Profile, on page 150
7. Configure a health monitor.	Complete the following procedure: • Procedure: Configuring a health monitor, on page 151
8. Configure a server pool.	Complete the following procedure: • Procedure: Configuring a server pool, on page 153
9. Add server pool members.	Complete the following procedure: • Procedure: Adding server pool members, on page 155
10. Configure data groups.	Complete the following procedure: • Procedure: Configuring data groups, on page 158
11. Configure a SNAT pool.	Complete the following procedure: • Procedure: Configuring a SNAT pool, on page 160
12. Configure an iRule.	Complete the following procedure: • Procedure: Configuring an iRule, on page 162
13. Configure a Virtual Server for outbound traffic.	Complete the following procedure: • Procedure: Configuring a Virtual Server for outbound traffic, on page 163
14. Configure a Virtual Server for inbound traffic.	Complete the following procedure: • Procedure: Configuring a Virtual Server for inbound traffic, on page 166
15. Configure Virtual Servers for UDP and TCP SIP communications.	Complete the following procedure: • Procedure: Configuring Virtual Servers for UDP and TCP SIP communications, on page 168

Procedures

This section provides detailed procedures for configuring the various elements that are required for the BIG-IP LTM—SIP Server integration.

Note: Any fields that are not mentioned in the configuration must be left at their default values.

Procedure:
Configuring VLANs

Purpose: To configure two VLANs (Virtual Local Area Networks): one VLAN for the external interface (physical interface 1.3) and one VLAN for the internal (SIP Server side) interface (physical interface 1.1). VLANs are used to logically associate Self IP interfaces with physical interfaces on the BIG-IP LTM.

Prerequisites

- You are logged in to the BIG-IP LTM web interface.

Start of procedure

1. Go to `Network > VLANs > VLAN List`.
2. Click `Create`.
3. In the dialog box that appears, specify the following properties (see Figure 88):
   a. `Name:` Enter the VLAN name for the external interface—for example, `vlanSipExternal`.
   b. `Tag: 503` (it is set automatically).
   c. `Resources > Interfaces > Untagged:` Select `1.3` in the `Available` section and click the left-pointing arrow button to move it into the `Untagged` section.
4. Click `Finished`.

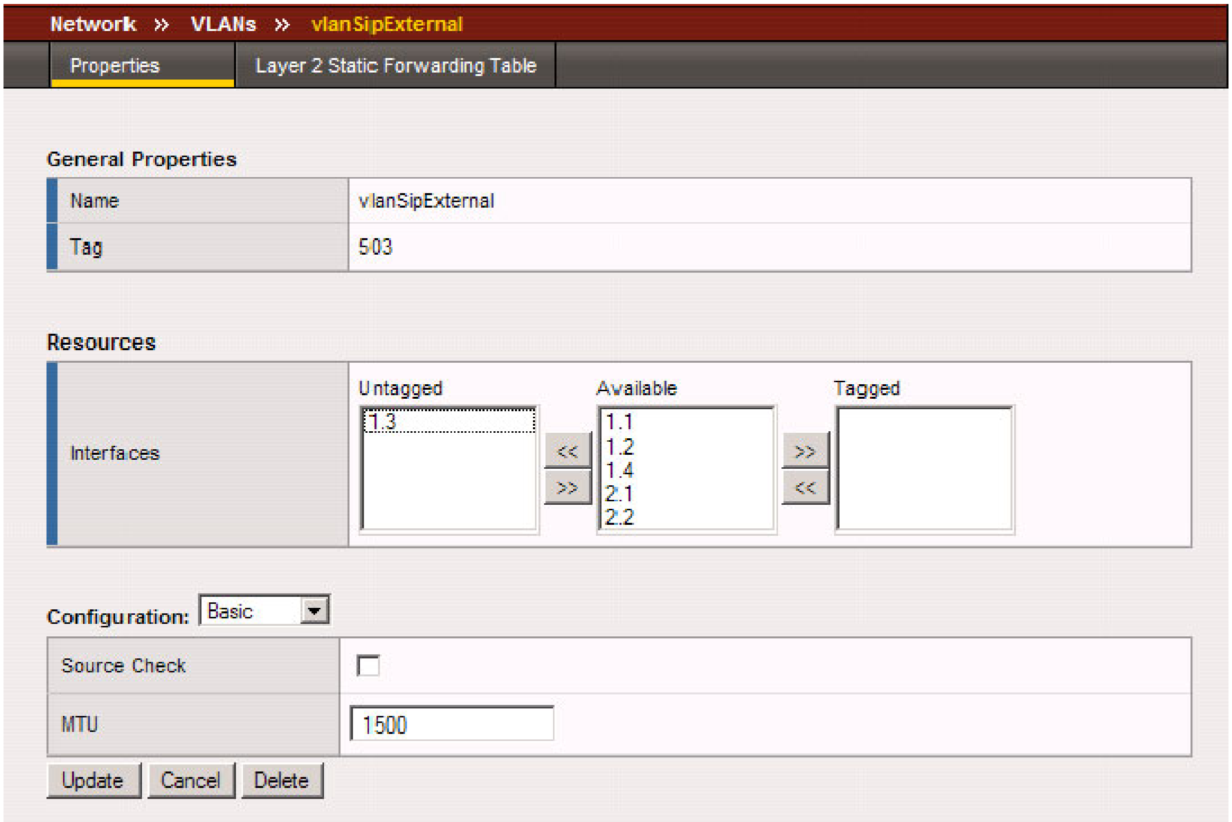

Figure 88: Configuring a VLAN for the External Interface

5. Click `Create`.
6. In the dialog box that appears, specify the following properties (see Figure 89):
   a. `Name`: Enter the VLAN name for the internal interface—for example, `vlanSipInternal`.
   b. `Tag`: `103` (it is set automatically).
   c. `Resources > Interfaces > Untagged`: Select `1.1` in the `Available` section and click the left-pointing arrow button to move it into the `Untagged` section.
7. Click `Finished`.

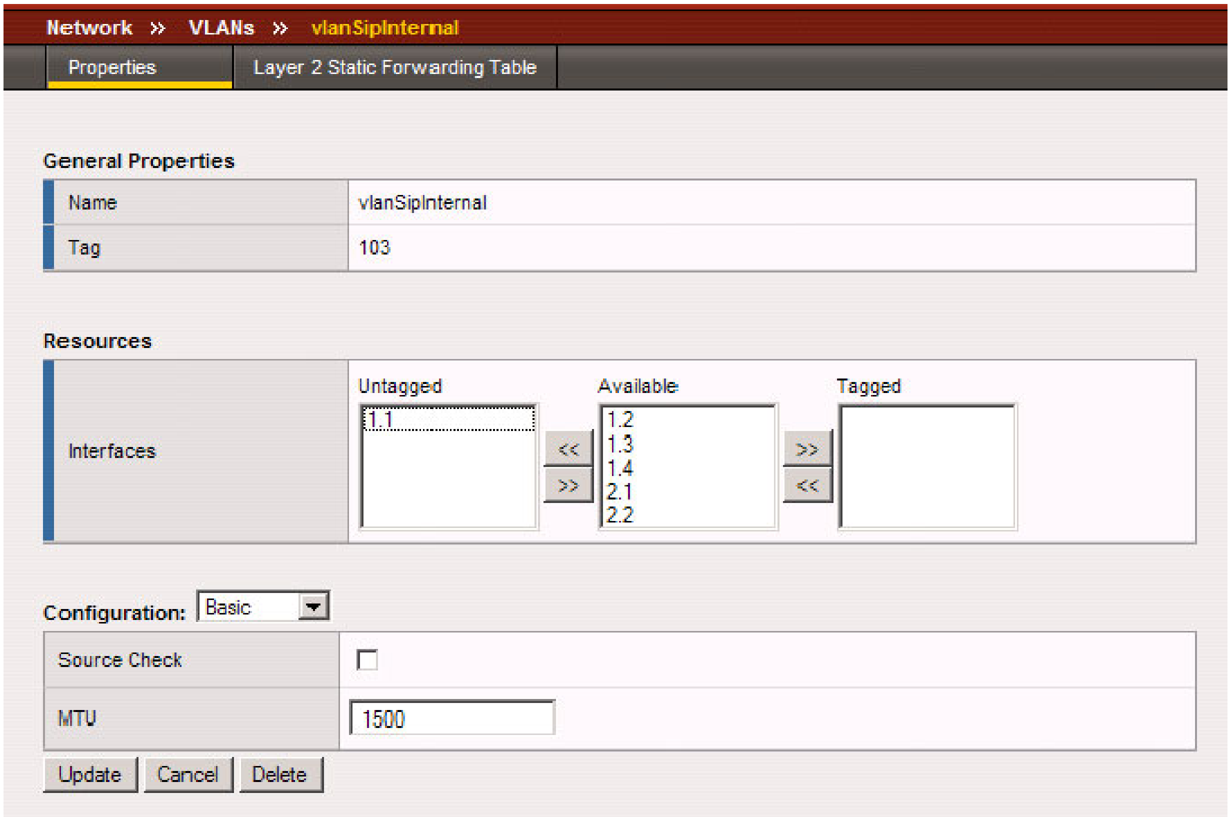

Figure 89: Configuring a VLAN for the Internal Interface

End of procedure

Next Steps

- Procedure: Configuring Self IP addresses, on page 145

Procedure:
Configuring Self IP addresses

Purpose: To configure two Self IP addresses—one for the external interface and one for the internal interface—and associate them with the VLANs, to access hosts in those VLANs.

Prerequisites

- Procedure: Configuring VLANs, on page 143

Start of procedure

1. Go to `Network > Self IPs`.
2. Click `Create`.
3. In the dialog box that appears, specify the following properties (see Figure 90):
   a. `IP Address`: Enter the IP address for the internal interface—for example, `192.168.63.1`.
   b. `Netmask`: Enter the netmask—for example, `255.255.255.240`.
   c. `VLAN`: Select the name of the VLAN to which you want to assign the self IP address—for example, `vlanSipInternal`.
4. Click `Finished`.

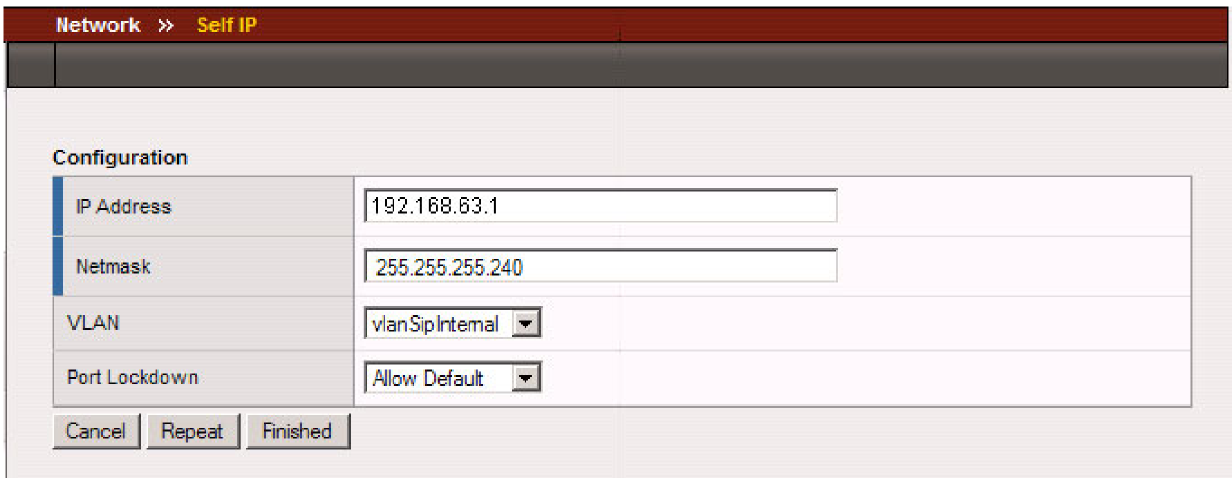

Figure 90: Configuring a Self IP Address for the Internal Interface

5. Click `Create`.
6. In the dialog box that appears, specify the following properties (see Figure 91):
   a. `IP Address`: Enter the IP address for the external interface—for example, `192.168.203.67`.
   b. `Netmask`: Enter the netmask—for example, `255.255.255.0`.
   c. `VLAN`: Select the name of the VLAN to which you want to assign the self IP address—for example, `vlanSipExternal`.
   d. Click `Finished` (see Figure 91).

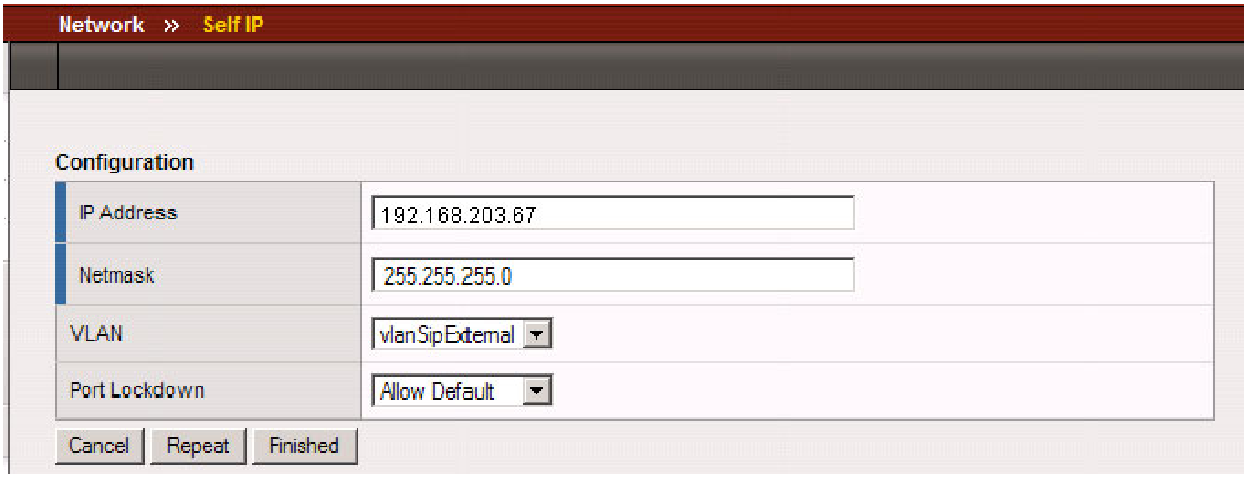

Figure 91: Configuring a Self IP Address for the External Interface

End of procedure

Next Steps

- Procedure: Configuring the Default IP route, on page 147

Procedure: Configuring the Default IP route

Purpose: To configure the default IP route.

Prerequisites

- Procedure: Configuring Self IP addresses, on page 145

Start of procedure

1. Go to `Network > Routes`.
2. Click `Add`.
3. In the dialog box that appears, specify the following properties (see Figure 92):
   a. `Type:` Select `Default Gateway`.
   b. `Resource > Use Gateway:` Enter the IP address for this default IP route—for example, `192.168.203.1`.
4. Click `Finished`.

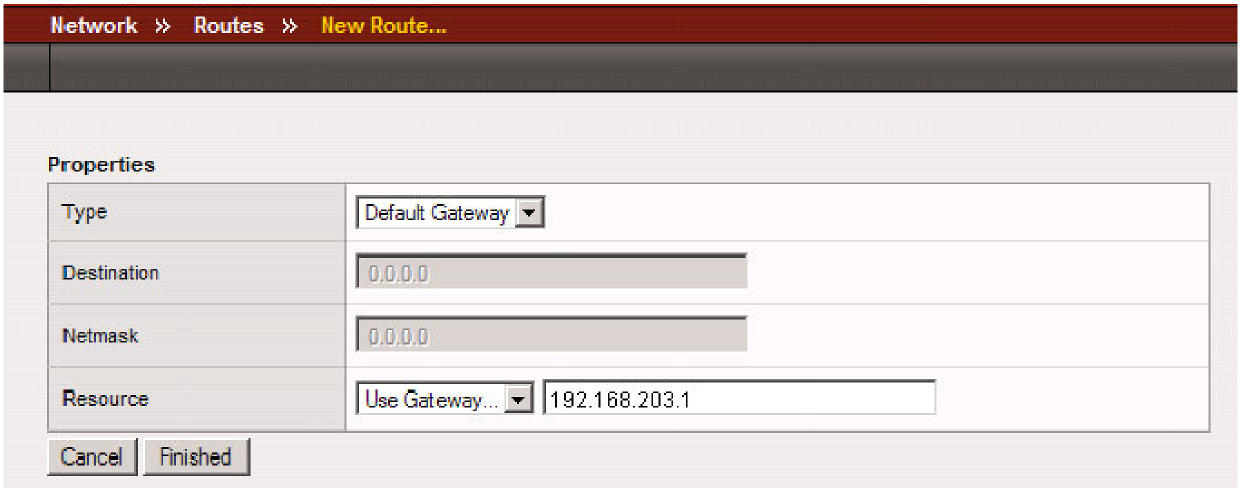

Figure 92: Configuring Default IP Route

End of procedure

Next Steps

- Procedure: Configuring SIP Server nodes, on page 148

Procedure:
Configuring SIP Server nodes

Purpose: To configure two SIP Server nodes, primary and backup.

Prerequisites

- Procedure: Configuring the Default IP route, on page 147

Start of procedure

1. Go to `Local Traffic > Nodes`.
2. Click `Create`.
3. In the dialog box that appears, specify the following properties (see Figure 93):
   a. `Address`: Enter the IP address for the primary SIP Server node—for example, `192.168.63.201`.
   b. `Name`: Enter the node name—for example, `nodeHa01Primary`.
   c. `Health Monitors`: Select `Node Specific`.
   d. `Select Monitors > Active`: Select `icmp`.
4. Click `Finished`.

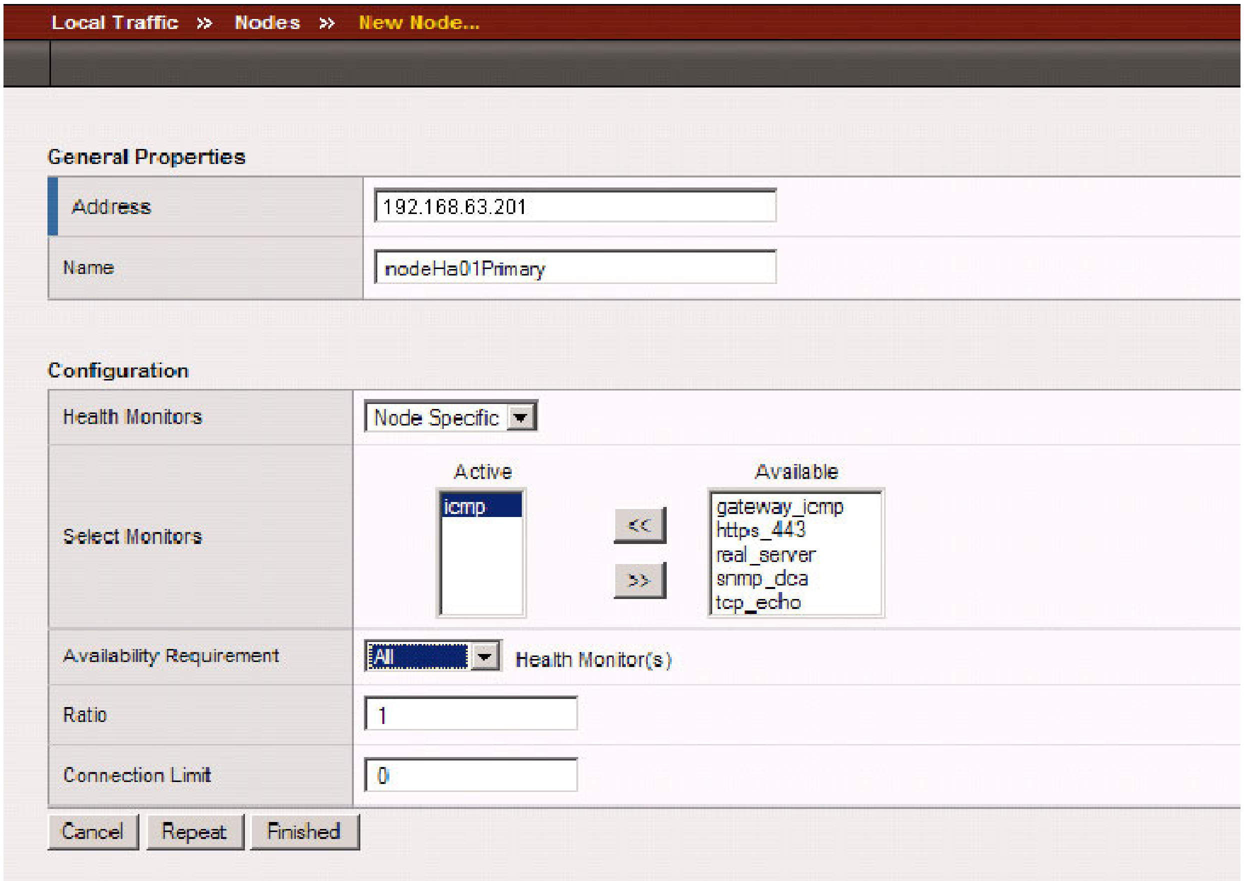

Figure 93: Configuring a Primary SIP Server Node

5. Click `Create`.
6. In the dialog box that appears, specify the following properties (see Figure 94):
   a. `Address`: Enter the IP address for the backup SIP Server node—for example, `192.168.63.203`.
   b. `Name`: Enter the node name—for example, `nodeHa01Backup`.
   c. `Health Monitors`: Select `Node Specific`.
   d. `Select Monitors > Active`: Select `icmp`.
7. Click `Finished`.

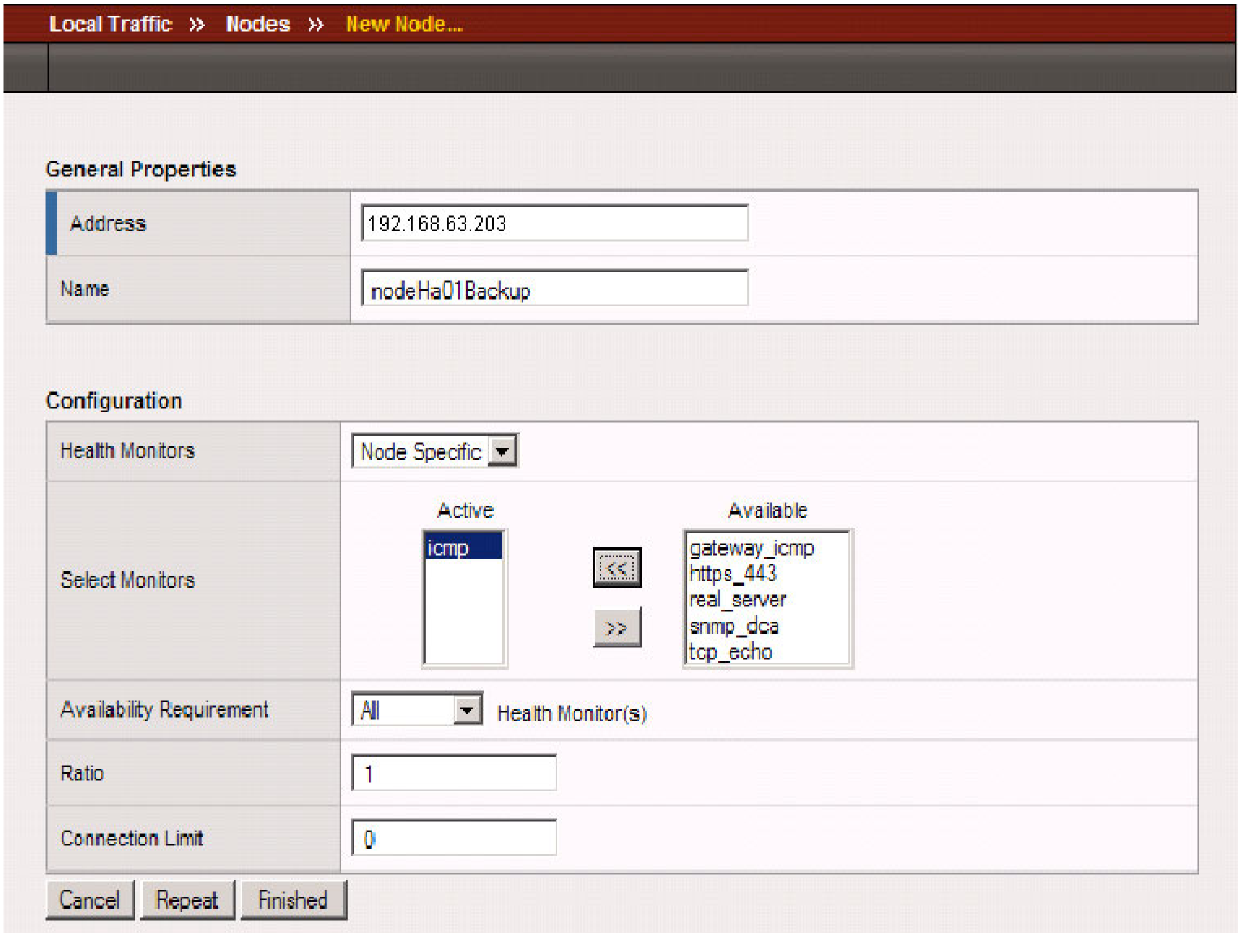

Figure 94: Configuring a Backup SIP Server Node

End of procedure

Next Steps

- Procedure: Modifying the sip_info Persistence Profile, on page 150

Procedure:
Modifying the sip_info Persistence Profile

Prerequisites

- Procedure: Configuring SIP Server nodes, on page 148

Start of procedure

1. Go to `Local Traffic > Profiles > Persistence`.
2. Select `sip_info`.

3. In the dialog box that appears, specify the following properties (see Figure 95):
   a. Select the `Match Across Services` check box.
   b. `SIP Info`: Select `Call-ID`.
4. Click `Update`.

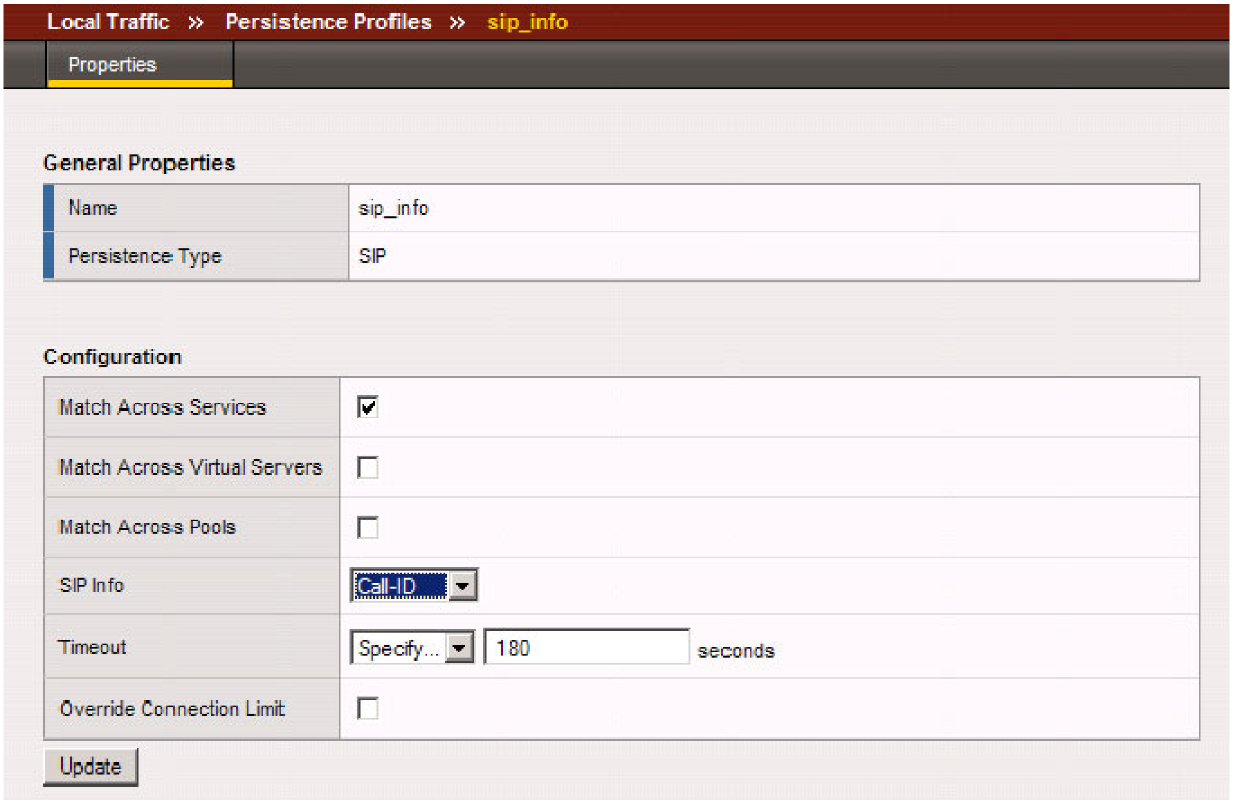

Figure 95: Modifying the sip_info Persistence Profile

End of procedure

Next Steps

- Procedure: Configuring a health monitor, on page 151

Procedure: Configuring a health monitor

Overview

In general, the BIG-IP LTM uses health monitors to determine whether a server to which messages can be routed is operational (active). Servers that are flagged as not operational (inactive) will cause the BIG-IP LTM to route messages to another server if one is present in the same server pool. However, primary and backup SIP Servers must be configured as the only members of the same server pool—one member active (primary) and one member inactive (backup).

In this procedure, the BIG-IP LTM is configured to use the health monitor of SIP type in UDP mode. This means that the `OPTIONS` request method will be sent to both primary and backup SIP Servers. Any response to `OPTIONS` is configured as `Accepted Status Code`.

SIP Server always starts in backup mode, establishes a permanent connection with the Genesys Management Layer, and changes its role to primary only if a trigger from the Management Layer is received. Such trigger is only generated if no other primary SIP Server is currently running. After switching to primary mode, SIP Server responds to UDP packets received on the SIP port specified by the `sip-port` configuration option. Therefore, after receiving the `OPTIONS` request from the BIG-IP LTM, SIP Server responds to the health check, and the BIG-IP LTM marks SIP Server as active.

When running in backup mode, SIP Server ignores UDP messages. Since the BIG-IP LTM does not receive any response to the `OPTIONS` request, it marks the backup SIP Server as inactive. If SIP Server does not respond because of network latency or other reasons, the BIG-IP LTM will mark SIP Server as inactive, and continue sending ping messages periodically.

The `Interval` setting (see Figure 96) defines how often pool members (primary and backup) are checked for presence. The `Timeout` setting defines the waiting time before an unresponsive member of the pool is marked as inactive. Regardless of the member's status (or SIP Server status), the BIG-IP LTM will always check servers for presence. When an inactive member responds to the health check, it is marked as active. In this configuration, the `Interval` parameter is set to one second and `Timeout` to four seconds in order to minimize a possible delay that might result from a switchover.

Prerequisites

- Procedure: Modifying the sip_info Persistence Profile, on page 150

Start of procedure

1. Go to `Local Traffic > Monitors`.
2. Click `Create`.
3. In the dialog box that appears, specify the following properties (see Figure 96):
   a. `Name`: Enter the name for this health monitor—for example, `monSipUdp`.
   b. `Type`: Select `SIP`.
   c. `Configuration`: Select `Basic`.
   d. `Interval`: Enter `1`.
   e. `Timeout`: Enter `4`.
   f. `Mode`: Select `UDP`.

g. `Additional Accepted Status Codes`: Select `Any`.

4. Click `Finished`.

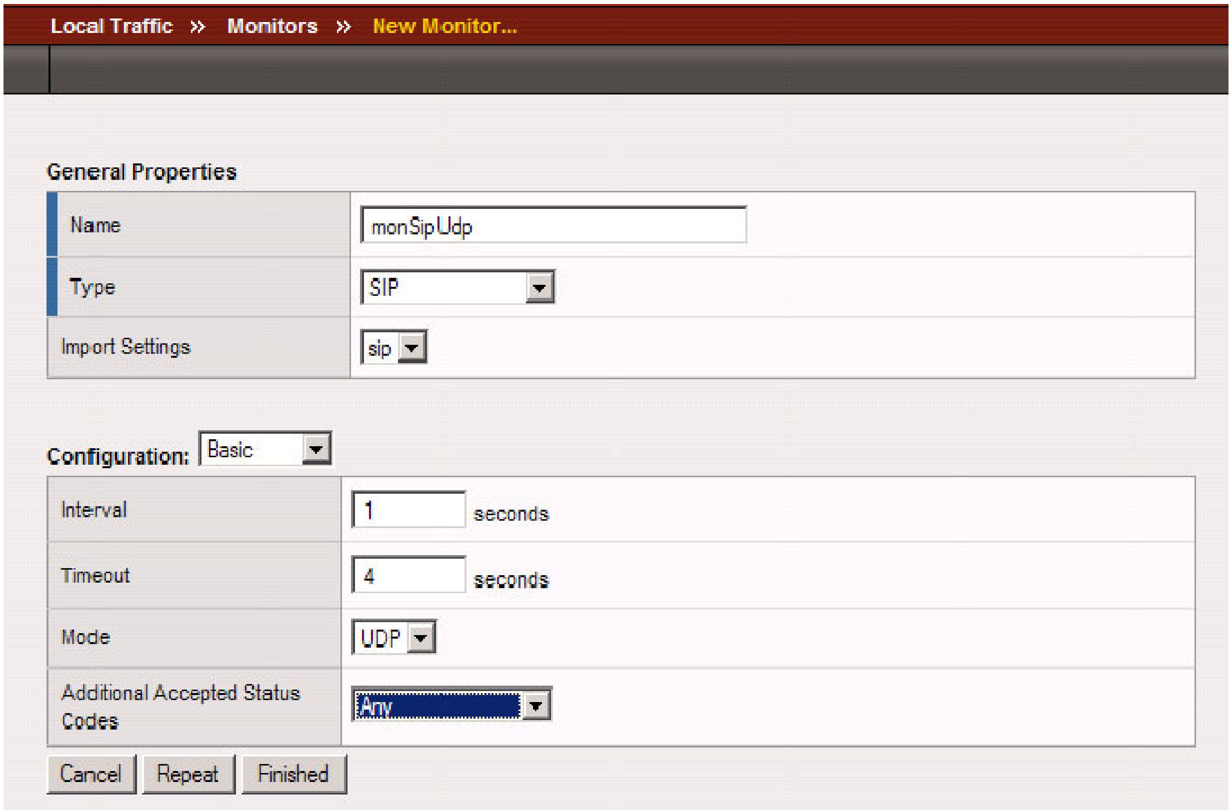

Figure 96: Configuring a Health Monitor

End of procedure

Next Steps

- Procedure: Configuring a server pool, on page 153

Procedure:
Configuring a server pool

Purpose: To configure a server pool with which the BIG-IP LTM will communicate.

Prerequisites

- Procedure: Configuring a health monitor, on page 151

Start of procedure

1. Go to `Local Traffic > Pools`.
2. Click `Create`.
3. In the dialog box that appears, specify the following properties (see Figure 97):
   a. `Configuration:` Select `Basic`.
   b. `Name:` Enter the name for this server pool—for example, the `poolHa01`.
   c. `Health Monitors > Active:` Select `monSipUdp`.
   d. `Load Balancing Method:` Select `Round Robin`.
   e. `Priority Group Activation:` Select `Disabled`.
4. Click `Finished`.

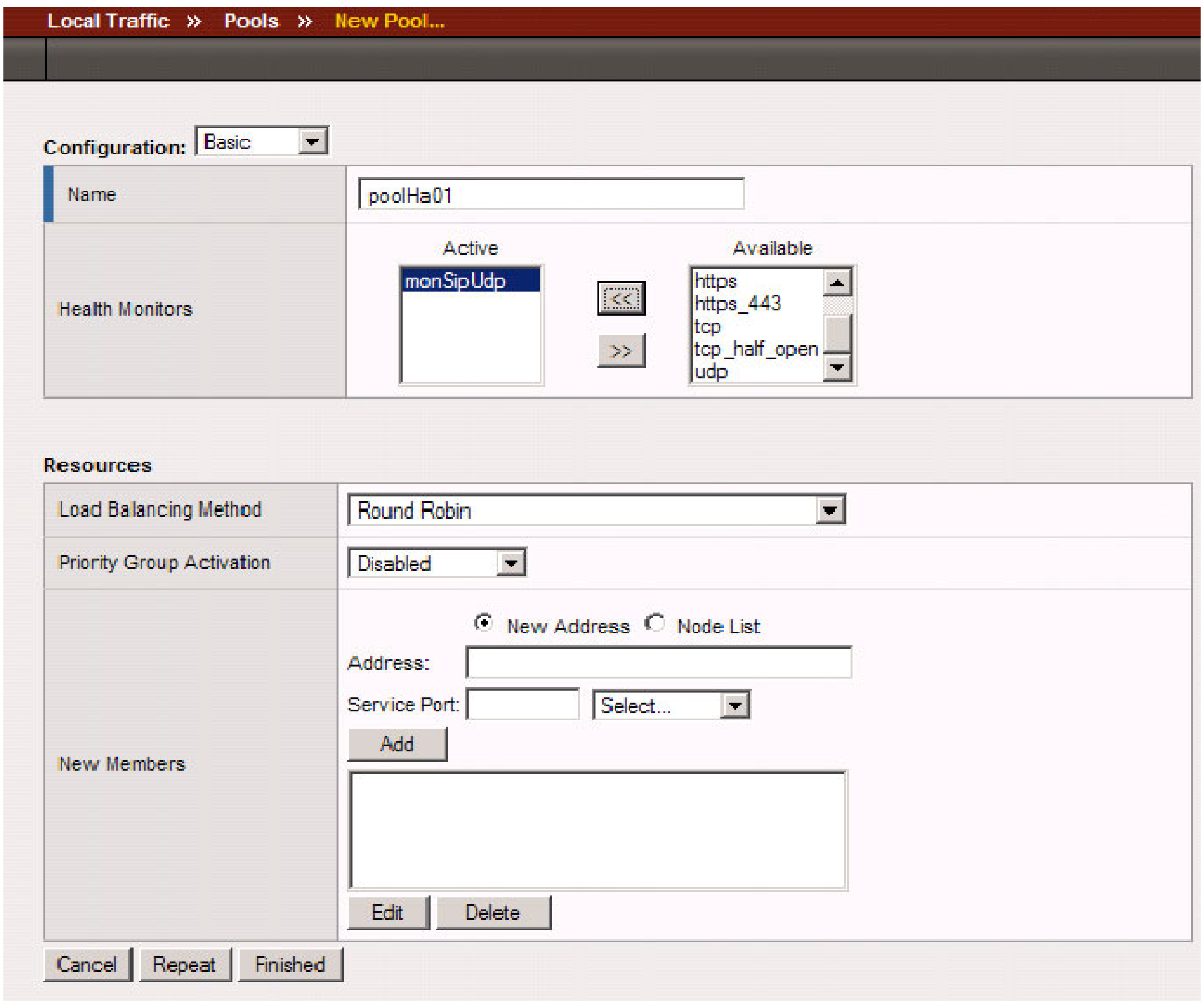

Figure 97: Configuring a Server Pool

End of procedure

Next Steps

- Procedure: Adding server pool members, on page 155

Procedure: Adding server pool members

Purpose: To add primary and backup SIP Servers to the server pool. Note that they must be the only members of this server pool.

Prerequisites

- Procedure: Configuring a server pool, on page 153

Start of procedure

1. Go to `Local Traffic > Pools > poolHa01 > Members`.
2. Click `Add`.
3. In the dialog box that appears, specify the following properties (see Figure 98):
   a. `Address > Node List`: Select the primary server node you created in Procedure: Configuring SIP Server nodes, on page 148. In our example, it would be `192.168.63.201 (nodeHa01Primary)`.
   b. `Service Port`: Enter `5060`.
4. Click `Finished`.

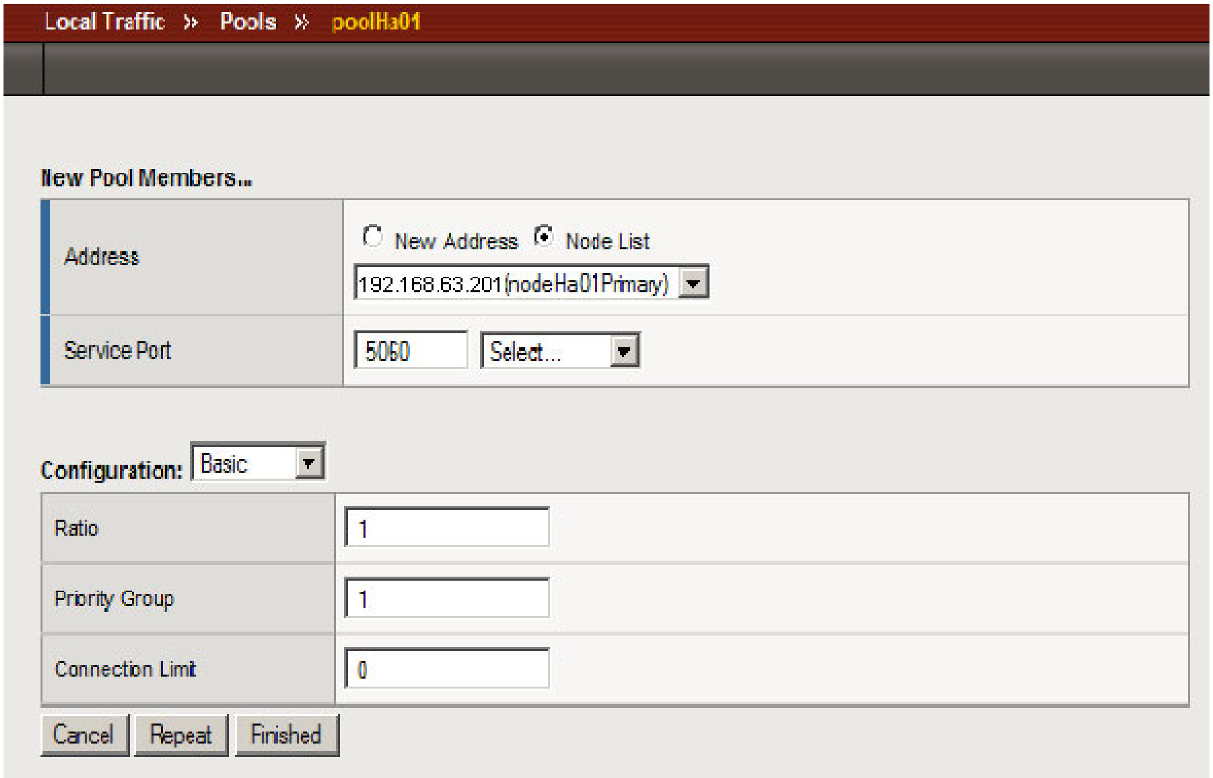

Figure 98: Adding the Primary SIP Server to the Server Pool

5. Click `Add`.
6. In the dialog box that appears, specify the following properties (see Figure 99):
   a. `Address > Node List`: Select the backup server node you created in Procedure: Configuring SIP Server nodes, on page 148. In our example, it would be `192.168.63.203 (nodeHa01Backup)`.
   b. `Service Port`: Enter `5060`.

7. Click `Finished`.

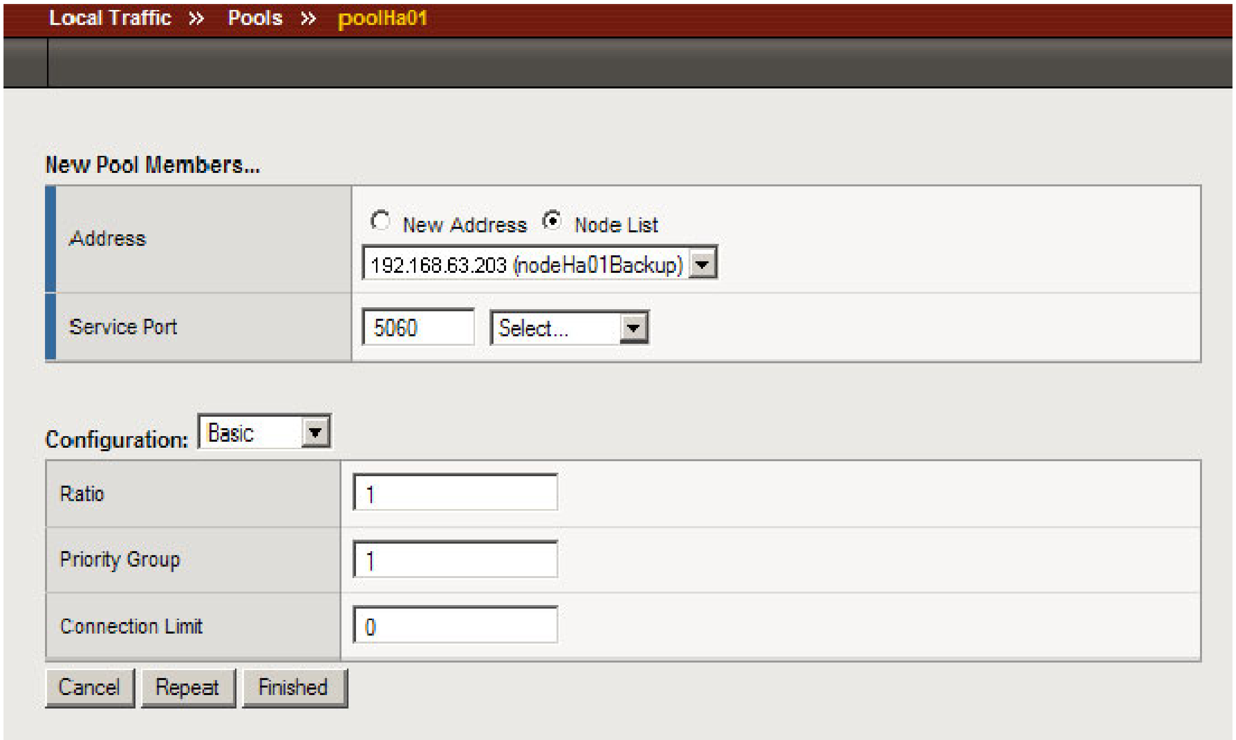

Figure 99: Adding the Backup SIP Server to the Server Pool

8. Go to `Local Traffic > Pools`. The status of the `poolHa01` server pool displays as available (green) (see Figure 100).

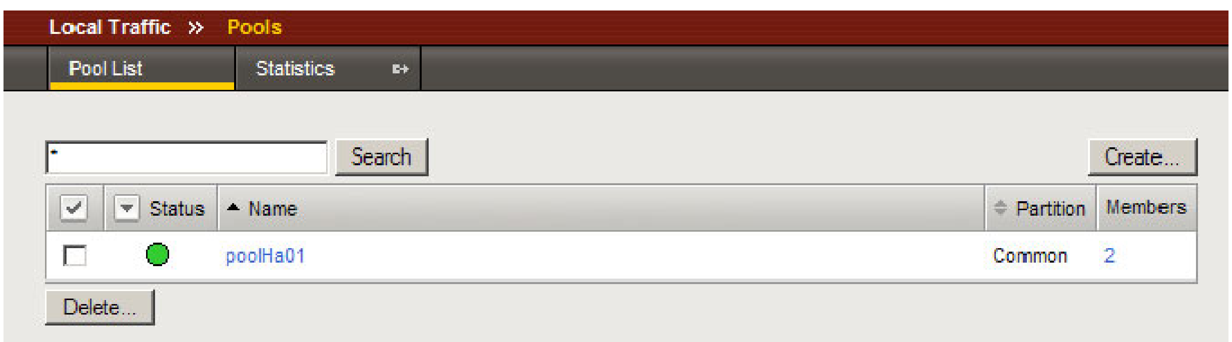

Figure 100: The Server Pool of Two Members

End of procedure

Next Steps

- Procedure: Configuring data groups, on page 158

Procedure: Configuring data groups

Purpose: To configure data groups that will be used by the iRule. One data group (`dataGroupHa`) contains physical IP addresses of primary and backup SIP Server nodes. The second data group (`dataGroupSnatExcluded`) contains IP addresses of the groups that will be excluded from applying SNAT, such as the Genesys Configuration Server group and Genesys T-Library Clients group (see Figure 87 on page 139).

Prerequisites

- Procedure: Adding server pool members, on page 155

Start of procedure

1. Go to `Local Traffic > iRules > Data Group List`.
2. Click `Create`.
3. In the dialog box that appears, specify the following properties (see Figure 101):
   a. `Name`: Enter the name for this data group—for example, `dataGroupSnatHa`.
   b. `Type`: Select `Address`.
   c. `Address Records > Type Host > Address`: Enter the host IP address of the primary server node—for example, `192.168.63.201`. Click `Add`.
   d. `Address Records > Type Host > Address`: Enter the host IP address of the backup server node—for example, `192.168.63.203`. Click `Add`.
4. Click `Finished`.

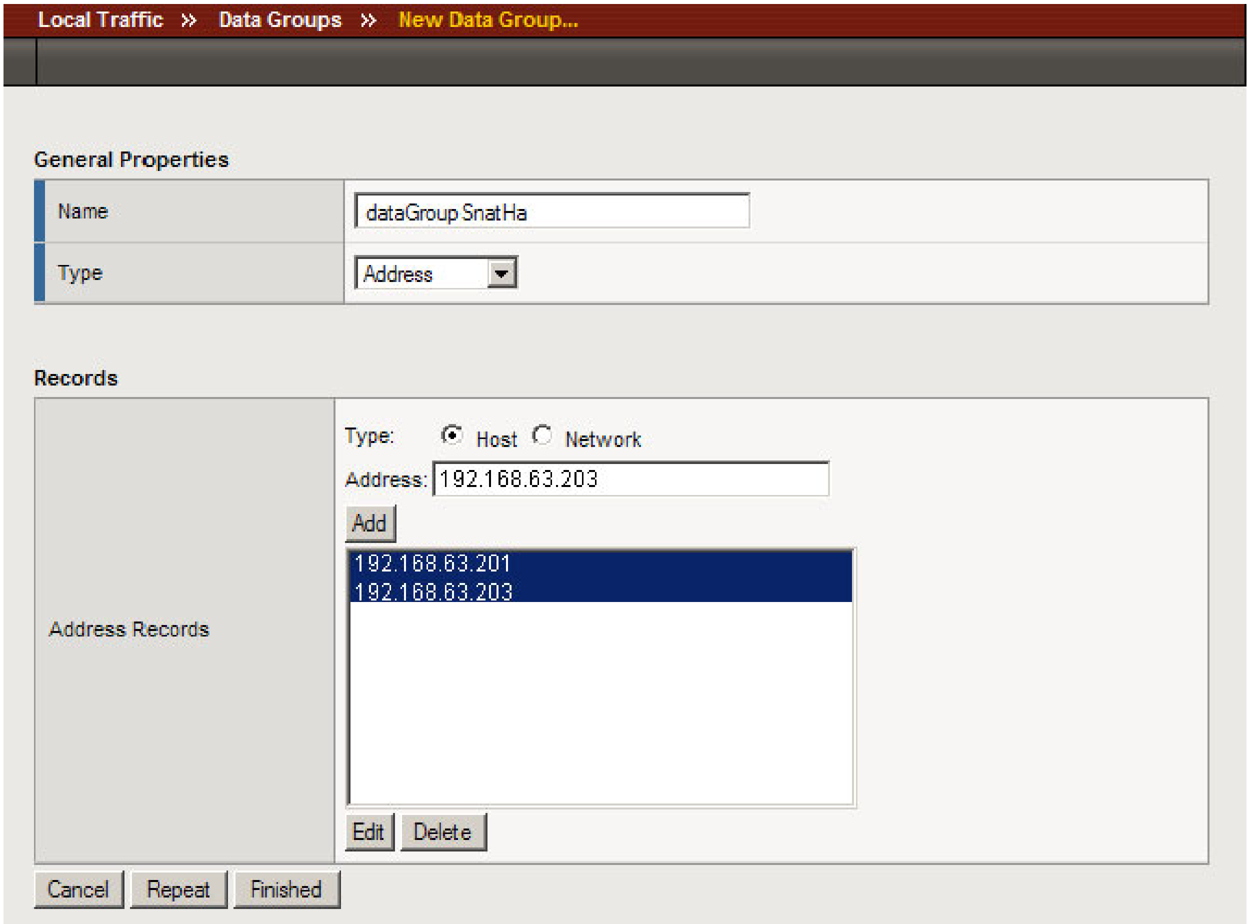

Figure 101: Configuring a Data Group for SNAT

5. Click `Create`.
6. In the dialog box that appears, specify the following properties (see Figure 102):
   a. `Name`: Enter the name for this data group—for example, `dataGroupSnatExcluded`.
   b. `Type`: Select `Address`.
   c. `Address Records > Type Host > Address`: Enter the host IP address of Genesys Configuration Server—for example, `172.21.226.73`. Click `Add`.
   d. `Address Records > Type Network > Address`: Enter the IP address and net mask—for example, `192.168.89.0/255.255.255.0`. Click `Add`.
7. Click `Finished`.

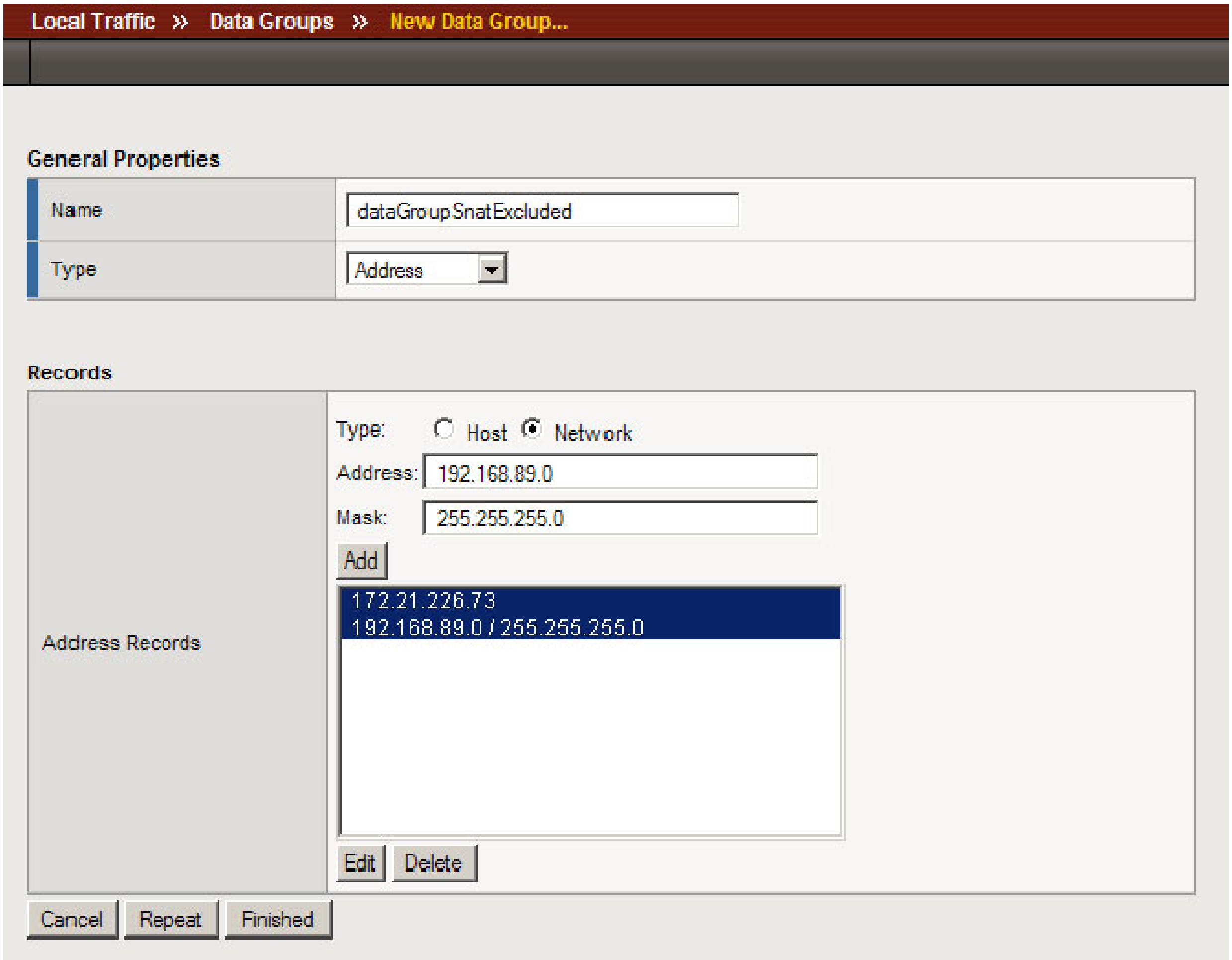

Figure 102: Configuring a Data Group for SNAT Exclusions

End of procedure

Next Steps

- Procedure: Configuring a SNAT pool, on page 160

Procedure: Configuring a SNAT pool

Purpose: To configure a SNAT pool that specifies the Virtual IP address to be used as a source IP address for any packet that originates from the primary or backup SIP Server to which SNAT is applied (with the exception of the devices specified in the `dataGroupSnatExcluded` data group). SNAT is the mapping of one or more original IP addresses to a translation address.

Prerequisites

- Procedure: Configuring data groups, on page 158

Start of procedure

1. Go to `Local Traffic > SNAT Pools`.
2. Click `Create`.
3. In the dialog box that appears, specify the following properties (see Figure 103):
   a. `Name`: Enter the name for this SNAT pool—for example, `snatPoolVip`.
   b. `Configuration > Members List > IP Address`: Enter the IP address to be used as a source IP address—for example, `192.168.203.164`.
4. Click `Finished`.

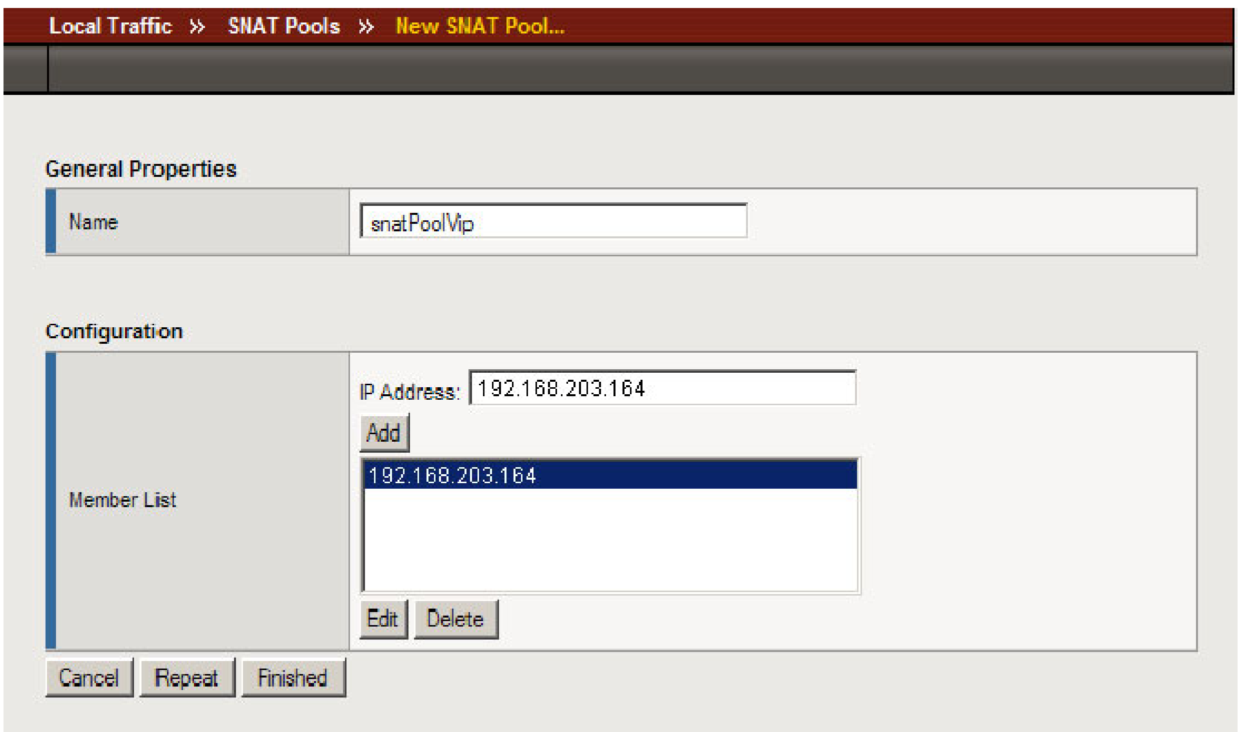

Figure 103: Configuring a SNAT Pool

End of procedure

Next Steps

- Procedure: Configuring an iRule, on page 162

Procedure: Configuring an iRule

Purpose: To configure an iRule that is used to perform SNAT to the Virtual IP address to any packets that originate from the primary or backup SIP Server (with the exception of the packets addressed to Configuration Server and the Genesys T-Library Clients group). This iRule will then be associated with a Virtual Server for the outbound traffic, `vsWildCardOutbound`. In this deployment architecture, the HA synchronization traffic between primary and backup SIP Servers does not pass through the BIG-IP LTM, that is why it is excluded from applying SNAT.

Purpose:

- Procedure: Configuring a SNAT pool, on page 160

Start of procedure

1. Go to `Local Traffic > iRules`.
2. Click `Create`.
3. In the dialog box that appears, specify the following properties (see Figure 104):
   a. `Name`: Enter the name for this iRule—for example, `iRuleSnatOutbound`.
   b. `Definition`: Enter the following text:

```
#=======================================================#
# Apply SNAT as specified in snatPoolVip for all
# packets originated from dataGroupSnatHa members.
# Exclude packets addressed to members of
# dataGroupSnatExcluded.
#=======================================================#
when CLIENT_ACCEPTED {
  if { [matchclass [IP::remote_addr] equals $::dataGroupSnatHa] }
  {
    if { [matchclass [IP::local_addr] equals $::dataGroupSnatExcluded] }
    {
    }
    else
    {
      snatpool snatPoolVip
    }
  }
}
```

4. Click `Finished`.

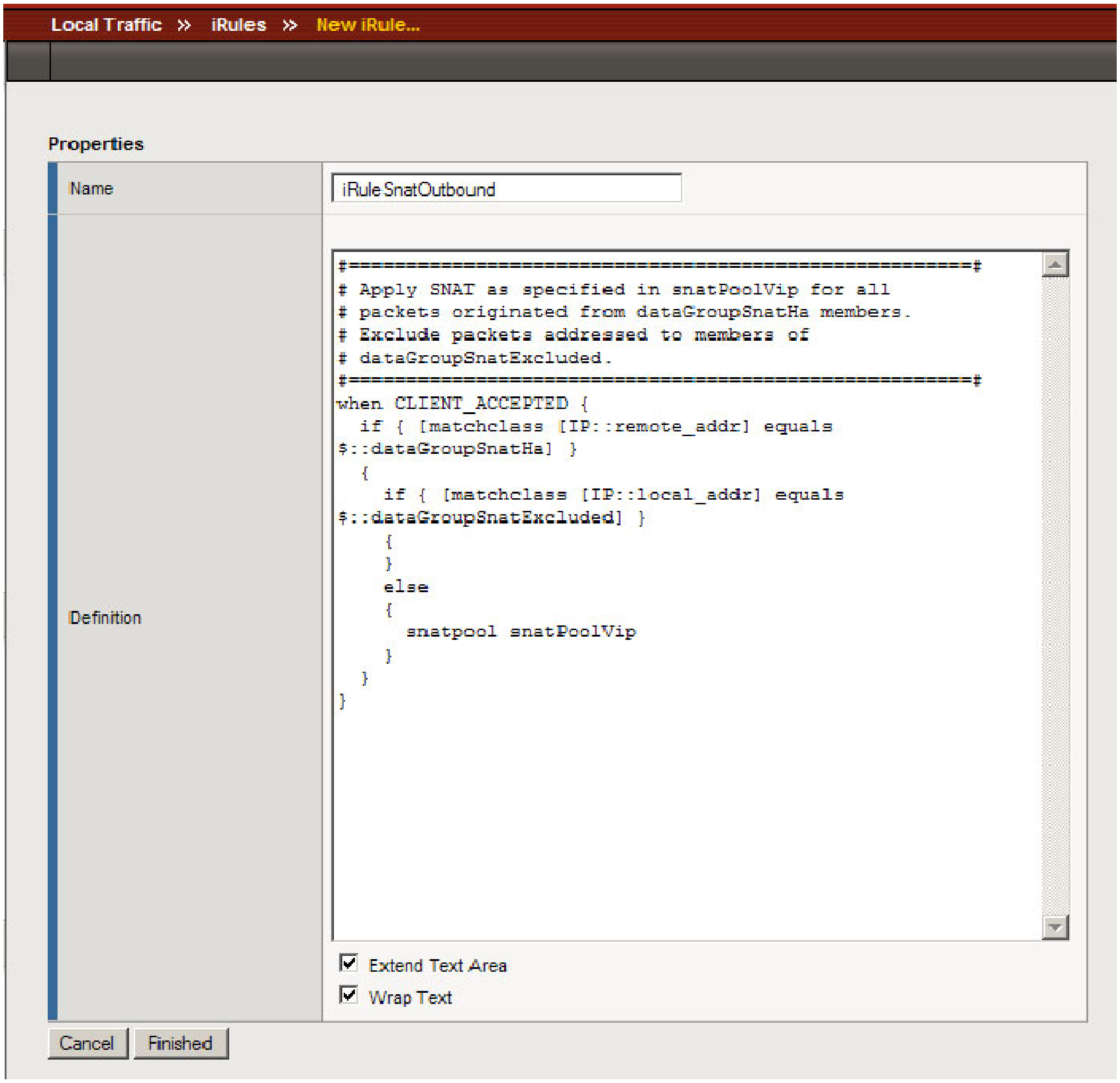

Figure 104: Configuring an iRule

End of procedure

Next Steps

- Procedure: Configuring a Virtual Server for outbound traffic, on page 163

Procedure: Configuring a Virtual Server for outbound traffic

Purpose: To configure a Virtual Server to be used for outbound traffic. It is associated with a VLAN that is configured for the internal interface (see

Procedure: Configuring VLANs, on page 143) and it has iRule assigned to Resources, which applies SNAT to all packets (except for packets addressed to Configuration Server).

Prerequisites

- Procedure: Configuring an iRule, on page 162

Start of procedure

1. Go to `Local Traffic > Virtual Servers`.
2. Click `Create`.
3. In the dialog box that appears, specify the following properties (see Figure 105):
   a. `Name`: Enter the name for this Virtual Server—for example, `vsWildCardOutbound`.
   b. `Destination > Type`: Select `Network`.
   c. `Destination > Address`: Enter `0.0.0.0`.
   d. `Destination > Mask`: Enter `0.0.0.0`.
   e. `Service Port`: Enter `*` (asterisk).
   f. `Configuration`: Select `Basic`.
   g. `Type`: Select `Forwarding (IP)`.
   h. `Protocol`: Select `All Protocols`.
   i. `VLAN Traffic`: Select `Enabled on...`.
   j. `VLAN List Selected`: Select `vlanSipInternal`.
   k. `Resources > iRules > Enabled`: Select `iRuleSnatOutbound`.
4. Click `Finished`.

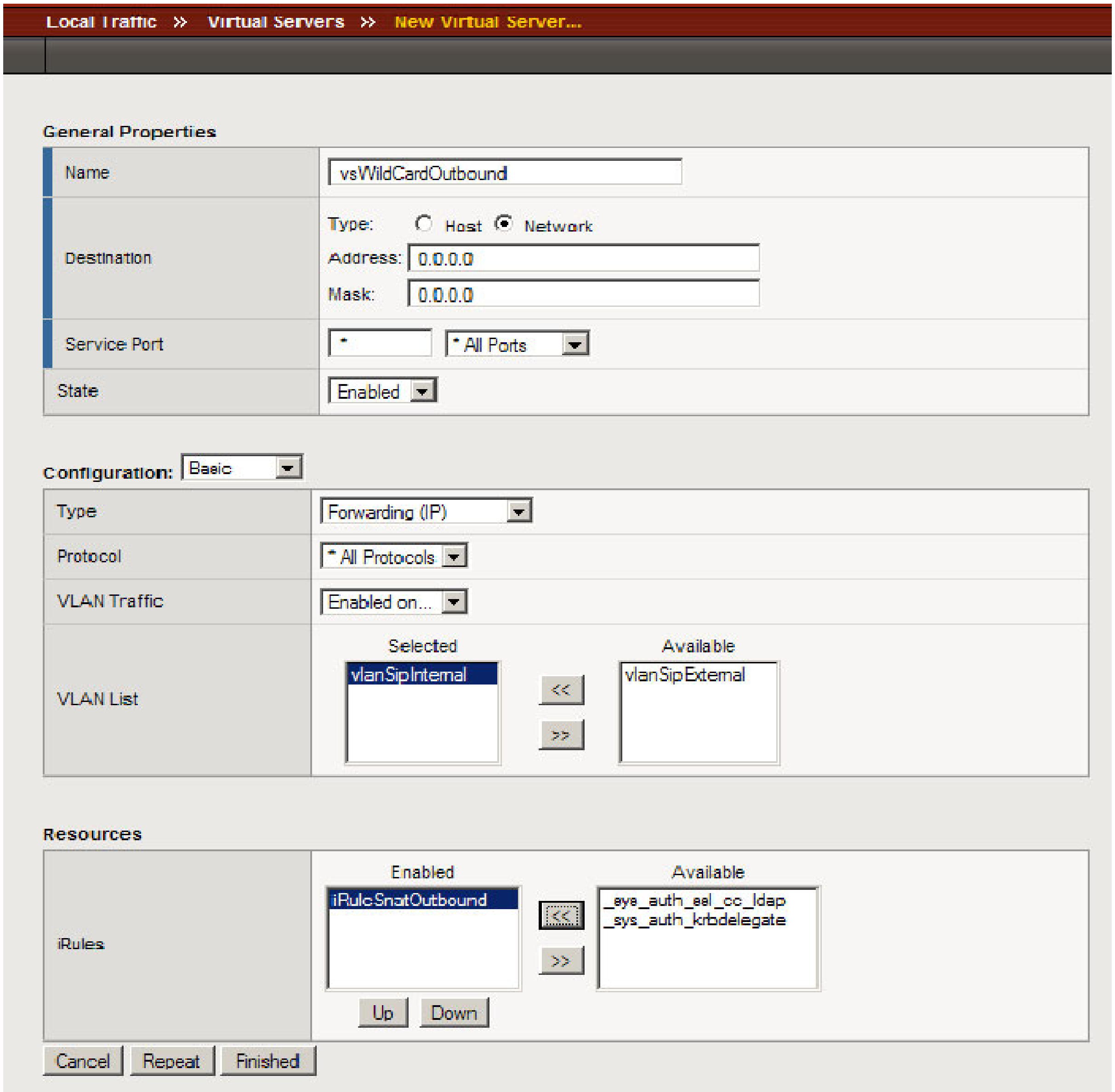

Figure 105: Configuring a Wildcard Virtual Server for Outbound Traffic

End of procedure

Next Steps

- Procedure: Configuring a Virtual Server for inbound traffic, on page 166

Procedure: Configuring a Virtual Server for inbound traffic

Purpose: To configure a Virtual Server for inbound traffic. In Layer 3/Routing configuration mode, the BIG-IP LTM passes through only those packets that have a destination matching a virtual server. Having the Virtual Server for inbound traffic allows packets with a destination that matches the physical IP address of the primary or backup SIP Server to pass through.

Prerequisites

- Procedure: Configuring a Virtual Server for outbound traffic, on page 163

Start of procedure

1. Go to `Local Traffic > Virtual Servers`.
2. Click `Create`.
3. In the dialog box that appears, specify the following properties (see Figure 106):
   a. `Name`: Enter the name for this Virtual Server—for example, `vsWildCardInbound`.
   b. `Destination > Type`: Select `Network`.
   c. `Destination > Address`: Enter `0.0.0.0`.
   d. `Destination > Mask`: Enter `0.0.0.0`.
   e. `Service Port`: Enter `*` (asterisk).
   f. `Configuration`: Select `Basic`.
   g. `Type`: Select `Forwarding (IP)`.
   h. `Protocol`: Select `All Protocols`.
   i. `VLAN Traffic`: Select `Enabled on...`.
   j. `VLAN List Selected`: Select `vlanSipExternal`.
4. Click `Finished`.

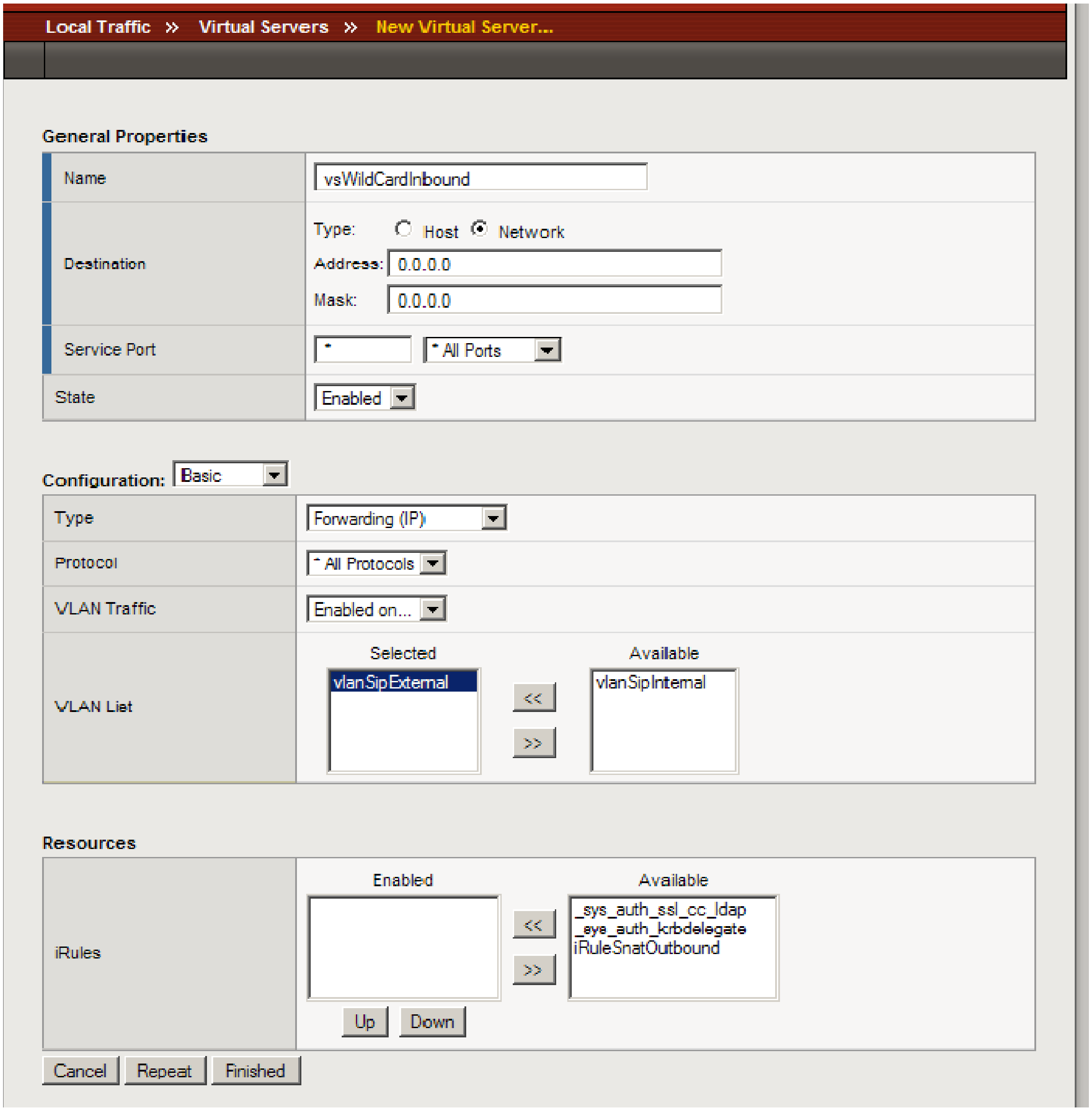

Figure 106: Configuring a Wildcard Virtual Server for Inbound Traffic

End of procedure

Next Steps

- Procedure: Configuring Virtual Servers for UDP and TCP SIP communications, on page 168

Procedure:
Configuring Virtual Servers for UDP and TCP SIP communications

Purpose: To configure two virtual servers to handle traffic directed to a Virtual IP address: one virtual server for SIP communications using the UDP as a transport protocol and one virtual server for SIP communications using the TCP as a transport protocol. The Virtual IP address is used by SIP clients to contact SIP Server. In other words, the Virtual IP address hides two physical IP addresses (used by the primary and backup servers) and presents the SIP Server HA pair as a single entity for all SIP-based communications.

Prerequisites

- Procedure: Configuring a Virtual Server for inbound traffic, on page 166

Start of procedure

1. Go to `Local Traffic > Virtual Servers`.
2. Click `Create`.
3. In the dialog box that appears, specify the following properties (see Figure 107):
   a. `Name:` Enter the name for this Virtual Server—for example, `vsVip`.
   b. `Destination > Type:` Select `Host`.
   c. `Destination > Address:` Enter the IP address for this Virtual Server—for example, `192.168.203.164`.
   d. `Service Port:` Enter `5060` and select `Other`.
   e. `State:` Select `Enabled`.
   f. `Configuration:` Select `Basic`.
   g. `Type:` Select `Standard`.
   h. `Protocol:` Select `UDP`.
   i. `SMTP Profile:` Select `None`.
   j. `SIP Profile:` Select `sip`.
   k. `VLAN Traffic:` Select `Enabled on...`.
   l. `VLAN List Selected:` Select `vlanSipExternal`.
   m. `Resources > Default Pool >` Select `poolHa01`.
4. Click `Finished`.

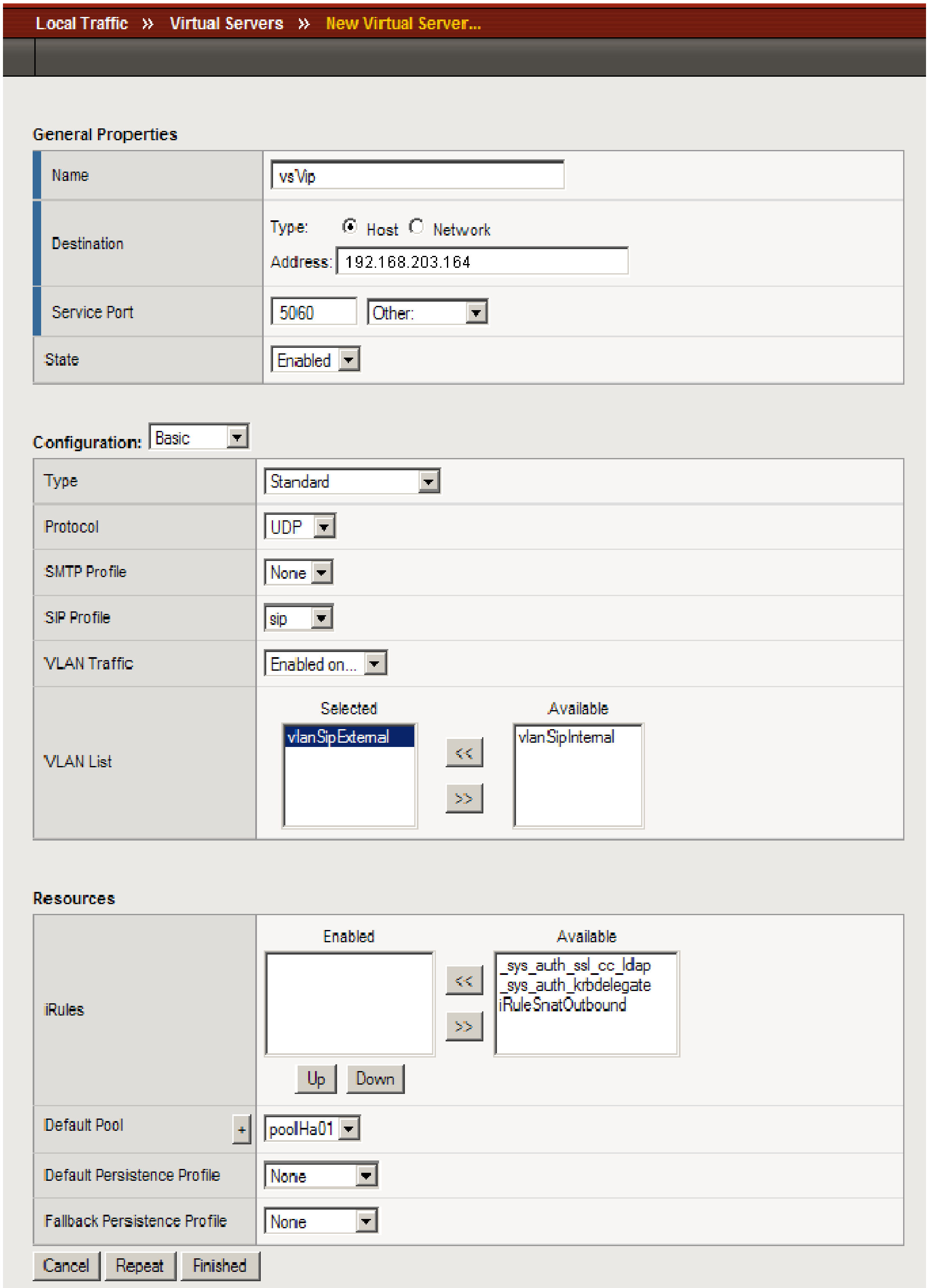

Figure 107: Configuring a Virtual Server for UDP-Based Communications

5. Click `Create`.

6. In the dialog box that appears, specify the following properties (see Figure 108):
   a. `Name:` Enter the name for this Virtual Server—for example, `vip_tcp`.
   b. `Destination > Type:` Select `Host`.
   c. `Destination > Address:` Enter the IP address for this Virtual Server—for example, `192.168.203.164`.
   d. `Service Port:` Enter `5060` and select `Other`.
   e. `State:` Select `Enabled`.
   f. `Configuration:` Select `Basic`.
   g. `Type:` Select `Standard`.
   h. `Protocol:` Select `TCP`.
   i. `SMTP Profile:` Select `None`.
   j. `SIP Profile:` Select `sip`.
   k. `VLAN Traffic:` Select `Enabled on...`.
   l. `VLAN List Selected:` Select `vlanSipExternal`.
   m. `Resources > Default Pool >` Select `poolHa01`.
7. Click `Finished`.

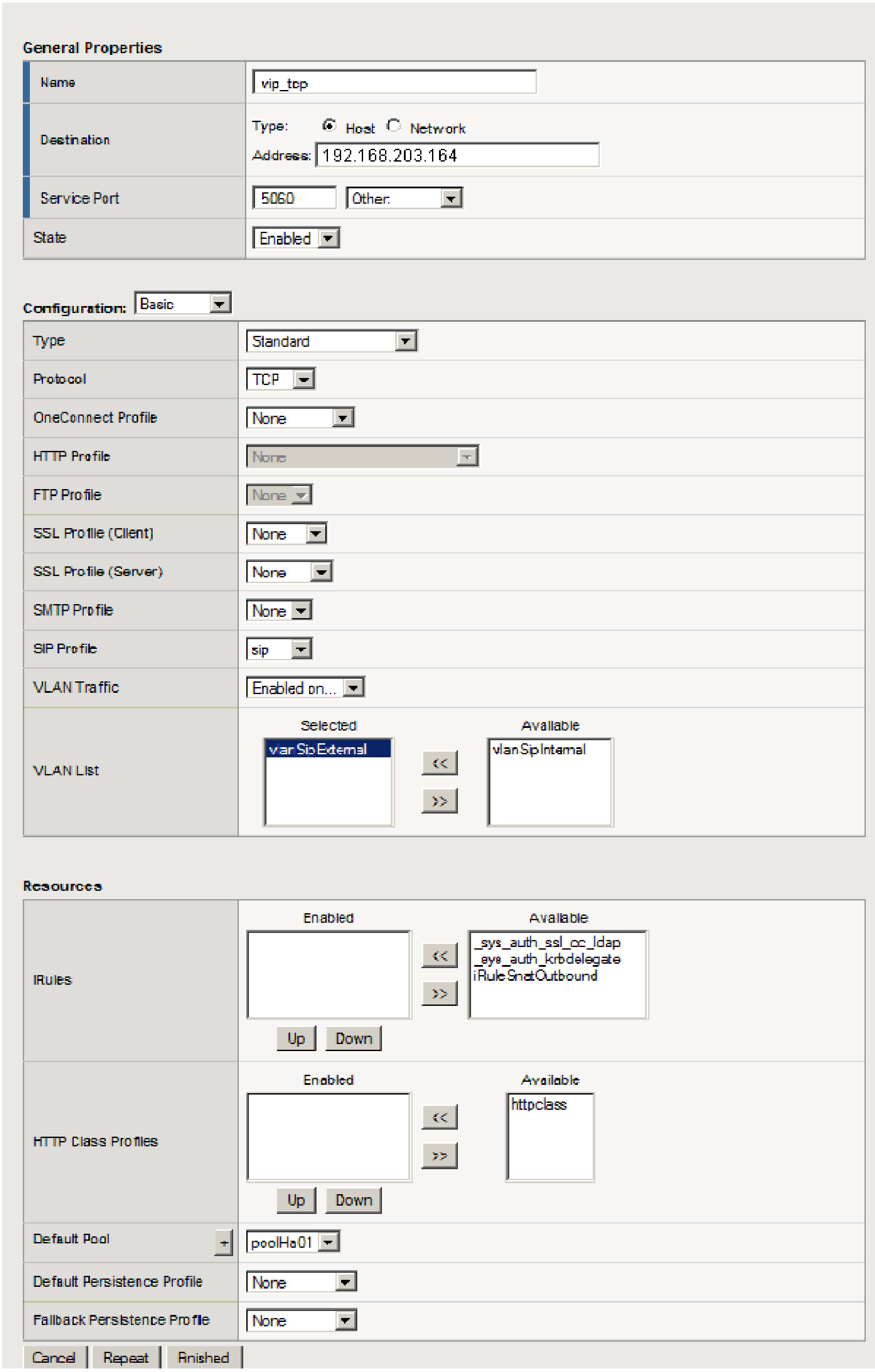

Figure 108: Creating a Virtual Server for TCP-Based Communications

End of procedure

Configuring SIP Server HA

Table 30 provides an overview of the main steps that are required in order to configure SIP Server HA in the Configuration Layer.

Table 30: Task Flow—Configuring SIP Server Applications

Objective	Related Procedures and Actions
1. Configure `Host` objects for primary and backup SIP Server applications.	Complete the following procedure: • Procedure: Configuring Host objects, on page 172
2. Configure primary and backup SIP Server applications.	Complete the following procedure: • Procedure: Configuring primary and backup SIP Server applications, on page 174

Procedures

Procedure: Configuring Host objects

Purpose: To configure a `Host` object for the computer on which a primary SIP Server application runs and to configure a `Host` object for the computer on which a backup SIP Server application runs.

Start of procedure

1. In Configuration Manager, right-click the `Environment > Hosts` folder and select `New > Host`.
2. On the `General` tab (see Figure 109):
   a. Enter the name of the host for the primary SIP Server application—for example, `192.168.63.201`.
   b. Enter the IP address of the host—for example, `192.168.63.201`.
   c. Select the type of operating system from the `OS Type` drop-down list, and enter its version, if known.
   d. Enter the LCA port number or accept the default (`4999`) to be used by the Management Layer to control applications running on this host.

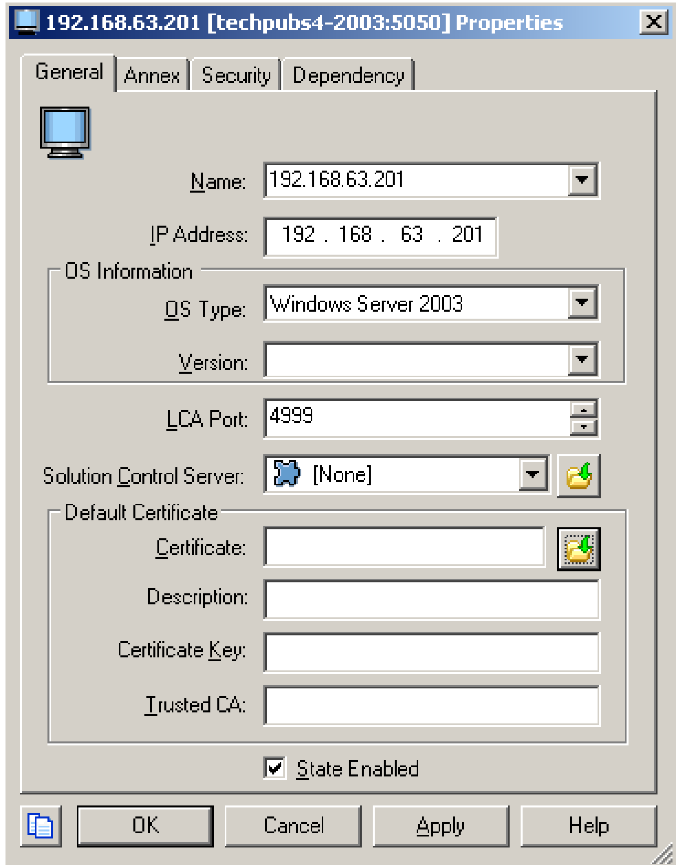

Figure 109: Configuring a Host Object for a Primary SIP Server Application: Sample Configuration

3. Click `OK`.
4. Right-click the `Environment > Hosts` folder and select `New > Host`.
5. On the `General` tab (see Figure 110):
   a. Enter the name of the host for the backup SIP Server application—for example, `192.168.63.203`.
   b. Enter the IP address of the host—for example, `192.168.63.203`.
   c. Select the type of operating system from the `OS Type` drop-down list, and enter its version, if known.
   d. Enter the LCA port number or accept the default (`4999`) to be used by the Management Layer to control applications running on this host.

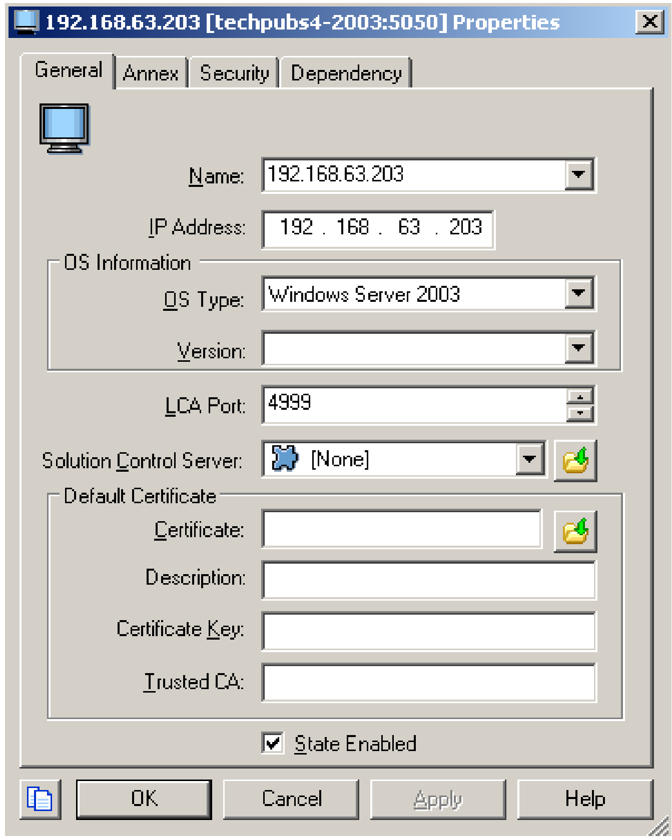

Figure 110: Configuring a Host Object for a Backup SIP Server Application: Sample Configuration

6. Click `OK`.

End of procedure

Next Steps

- Procedure: Configuring primary and backup SIP Server applications, on page 174

Procedure: Configuring primary and backup SIP Server applications

Purpose: To configure primary and backup SIP Server applications.

Start of procedure

1. Open the primary SIP Server application.
2. Click the `Server Info` tab, and then specify the `Host` you created for the primary SIP Server application (see Figure 111).

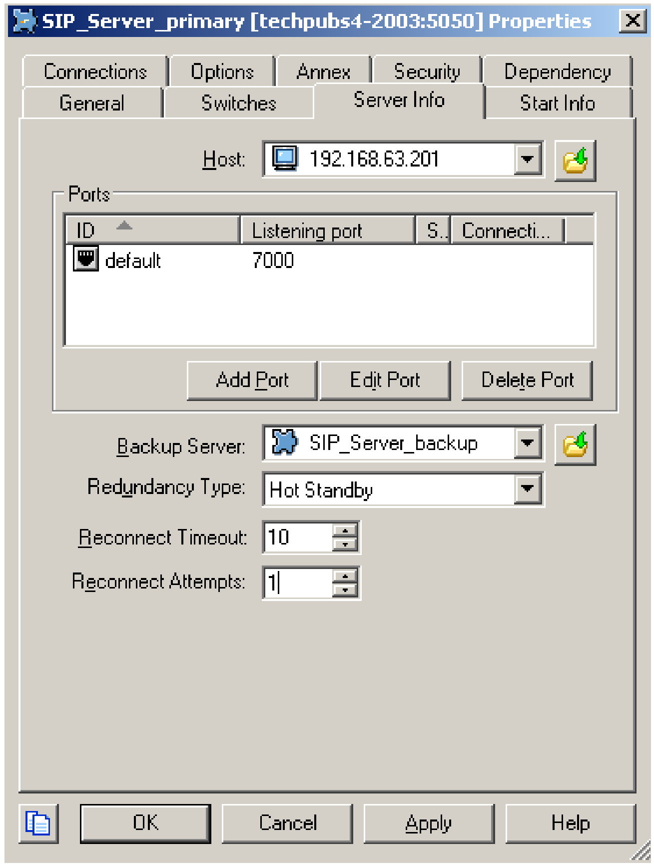

Figure 111: Configuring a Primary SIP Server Application: Sample Configuration

3. Click the `Options` tab. In the `TServer` section, set options as specified in Table 31.

Table 31: Configuration Options for a Primary SIP Server Application

Option Name	Option Value	Description
sip-address	String	Set this option to the value of the BIG-IP LTM Virtual IP address, which is the destination address for all incoming SIP messages. In our example, this would be `192.168.203.164`.
sip-port	`5060`	Specifies the port on which SIP Server listens to incoming SIP requests. The same port number is used for both TCP and UDP transports.
sip-interface	String	Set this option to the value of a host physical IP address where the primary SIP Server runs. In our example, this would be `192.168.63.201`.
internal-registrar-enabled	`true, false`	Set this option to `true`.
internal-registrar-persistent	`true, false`	Set this option to `true`.
sip-hold-rfc3264	`true, false`	Set this option to `true`.

4. When you are finished, click `OK`.
5. Open the backup SIP Server application.
6. Click the `Server Info` tab, and then specify the `Host` you created for the backup SIP Server application (see Figure 112).

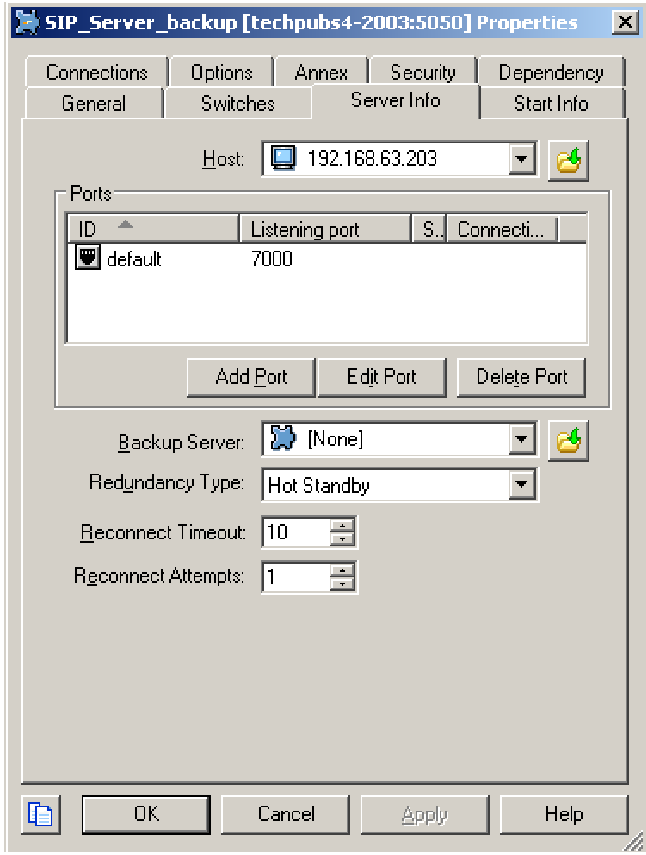

Figure 112: Configuring a Backup SIP Server Application: Sample Configuration

7. Click the `Options` tab. In the `TServer` section, set options as specified in Table 32.

Table 32: Configuration options for a Backup SIP Server Application

Option Name	Option Value	Description
sip-address	String	Set this option to the value of the BIG-IP LTM Virtual IP address, which is the destination address for all incoming SIP messages. In our example, this would be `192.168.203.164`.
sip-port	`5060`	Specifies the port on which SIP Server listens to incoming SIP requests. The same port number is used for both TCP and UDP transports.

Table 32: Configuration options for a Backup SIP Server Application (Continued)

Option Name	Option Value	Description
sip-interface	String	Set this option to the value of a host physical IP address where the backup SIP Server runs. In our example, this would be `192.168.63.203`.
internal-registrar-enabled	`true, false`	Set this option to `true`.
internal-registrar-persistent	`true, false`	Set this option to `true`.
sip-hold-rfc3264	`true, false`	Set this option to `true`.

8. When you are finished, click `OK`.

End of procedure

Supplements

Related Documentation Resources

The following resources provide additional information that is relevant to this software. Consult these additional resources as necessary.

Management Framework

- The *Framework 8.0 SIP Server Deployment Guide*, which contains detailed reference information for the Genesys Framework 7.6 SIP Server, including configuration options and specific functionality.
- The *Framework 8.0 Deployment Guide*, which will help you configure, install, start, and stop Framework components.

Genesys

- *Genesys Technical Publications Glossary,* which ships on the Genesys Documentation Library DVD and which provides a comprehensive list of the Genesys and computer-telephony integration (CTI) terminology and acronyms used in this document.
- *Genesys Migration Guide*, which ships on the Genesys Documentation Library DVD, and which provides documented migration strategies for Genesys product releases. Contact Genesys Technical Support for more information.
- Release Notes and Product Advisories for this product, which are available on the Genesys Technical Support website at `http://genesyslab.com/support`.

Information about supported hardware and third-party software is available on the Genesys Technical Support website in the following documents:

- *Genesys Supported Operating Environment Reference Manual*
- *Genesys Supported Media Interfaces Reference Manual*

Consult these additional resources as necessary:

- *Genesys Hardware Sizing Guide,* which provides information about Genesys hardware sizing guidelines for the Genesys 7.x/8.x releases.
- *Genesys Interoperability Guide,* which provides information on the compatibility of Genesys products with various Configuration Layer Environments; Interoperability of Reporting Templates and Solutions; and Gplus Adapters Interoperability.
- *Genesys Licensing Guide,* which introduces you to the concepts, terminology, and procedures relevant to the Genesys licensing system.
- *Genesys Database Sizing Estimator 7.6 Worksheets,* which provides a range of expected database sizes for various Genesys products.

For additional system-wide planning tools and information, see the release-specific listings of System Level Documents on the Genesys Technical Support website, accessible from the `system level documents by release` tab in the Knowledge Base `Browse Documents` Section.

Genesys product documentation is available on the:

- Genesys Technical Support website at `http://genesyslab.com/support`.
- Genesys Documentation Library DVD, which you can order by e-mail from Genesys Order Management at `orderman@genesyslab.com`.

Document Conventions

This document uses certain stylistic and typographical conventions—introduced here—that serve as shorthands for particular kinds of information.

Document Version Number

A version number appears at the bottom of the inside front cover of this document. Version numbers change as new information is added to this document. Here is a sample version number:

80fr_ref_06-2008_v8.0.001.00

You will need this number when you are talking with Genesys Technical Support about this product.

Screen Captures Used in This Document

Screen captures from the product graphical user interface (GUI), as used in this document, may sometimes contain minor spelling, capitalization, or grammatical errors. The text accompanying and explaining the screen captures corrects such errors *except* when such a correction would prevent you from installing, configuring, or successfully using the product. For example, if the name of an option contains a usage error, the name would be presented exactly as it appears in the product GUI; the error would not be corrected in any accompanying text.

Type Styles

Table 33 describes and illustrates the type conventions that are used in this document.

Table 33: Type Styles

Type Style	Used For	Examples
Italic	• Document titles • Emphasis • Definitions of (or first references to) unfamiliar terms • Mathematical variables Also used to indicate placeholder text within code samples or commands, in the special case where angle brackets are a required part of the syntax (see the note about angle brackets on page 182).	Please consult the *Genesys Migration Guide* for more information. Do *not* use this value for this option. A *customary and usual* practice is one that is widely accepted and used within a particular industry or profession. The formula, $x + 1 = 7$ where x stands for . . .

Table 33: Type Styles (Continued)

Type Style	Used For	Examples
Monospace font (Looks like `teletype` or `typewriter text`)	All programming identifiers and GUI elements. This convention includes: • The *names* of directories, files, folders, configuration objects, paths, scripts, dialog boxes, options, fields, text and list boxes, operational modes, all buttons (including radio buttons), check boxes, commands, tabs, CTI events, and error messages. • The values of options. • Logical arguments and command syntax. • Code samples. Also used for any text that users must manually enter during a configuration or installation procedure, or on a command line.	Select the `Show variables on screen` check box. In the `Operand` text box, enter your formula. Click `OK` to exit the `Properties` dialog box. T-Server distributes the error messages in `EventError` events. If you select `true` for the `inbound-bsns-calls` option, all established inbound calls on a local agent are considered business calls. Enter `exit` on the command line.
Square brackets ([ ])	A particular parameter or value that is optional within a logical argument, a command, or some programming syntax. That is, the presence of the parameter or value is not required to resolve the argument, command, or block of code. The user decides whether to include this optional information.	`smcp_server -host [/flags]`
Angle brackets (< >)	A placeholder for a value that the user must specify. This might be a DN or a port number specific to your enterprise. **Note:** In some cases, angle brackets are required characters in code syntax (for example, in XML schemas). In these cases, italic text is used for placeholder values.	`smcp_server -host <confighost>`

Index

Symbols

A

B

C