A MITEL PRODUCT GUIDE

Unify OpenScape Voice

Design and Planning Manual, SIP Network Planning

Design and Planning Manual, SIP Network Planning

Planning Guide
07/2024

A31003-H80A0-P100-01-76A9

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos, and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively "Unify") or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

Contents

History of Changes

Issue	Date	Changes
1	10/2019	Initial release for V10

1 Overview and Unify OpenScape Voice Terminology

This chapter gives an overview of the Unify OpenScape Voice product family and defines terms frequently used and newly introduced in this book.

1.1 Unify OpenScape Voice Networking Overview

Unify OpenScape Voice is a carrier-class softswitch that is scalable from 300 to 100,000 users per system. When networked, the number of subscribers are virtually limitless. The system runs on highly reliable, fault-tolerant servers using SuSe Linux Enterprise Server Operating System from Novell. The core protocol of Unify OpenScape Voice is IETF Session Initiation Protocol (SIP). For an overview of the SIP protocol, see Appendix E, “SIP Overview”.

In addition to industry-standard SIP, Unify OpenScape Voice supports SIP-Q (QSIG over SIP) for interfacing to legacy PBX systems—for example, OpenScape 4000.

Unify OpenScape Voice supports a number of terminal or endpoint devices (see Figure 1, "Unify OpenScape Voice Main Components"):

Hard Phones

- OpenStage telephones (Models 15, 20, 20E, 40, 60, and 80)
- Limited support for SIP-compliant third-party devices

Soft Clients

- optiClient 130 S
- OpenScape Desktop Client Personal Edition

Analog Adapters

- Mediatrix 4102 – 2 ports
- Mediatrix 4104 – 4 ports
- Mediatrix 4108 – 8 ports
- Mediatrix 4116 – 16 ports
- Mediatrix 4124 – 24 ports
- HiPath AP 1120 – 2 ports (Does not support SRTP)

SIP Gateways—for Access to the PSTN and other TDM networks

- **Unify Gateways:**
  - RG 8300
  - RG 8700 product family:
    - RG 8702 (200 users)
    - RG 8708 (1000 users)
    - RG 8716 (2000 users)
  - HiPath 3000
  - OpenScape 4000
- **Mediatrix Gateways**
  - Mediatrix 1204
  - Mediatrix 4402
  - Mediatrix 4404
  - Mediatrix 3600

Other Network Devices

- OpenScape Branch solution (50 to 6000 users)
- Session border controllers:
  - OpenScape SBC (1,200 to 4,000 simultaneous sessions)
  - Acme Packet SBCs

Note: Because the OpenScape Branch product includes integrated SBC, it does not require the use of an external SBC.

- OpenScape Media Server

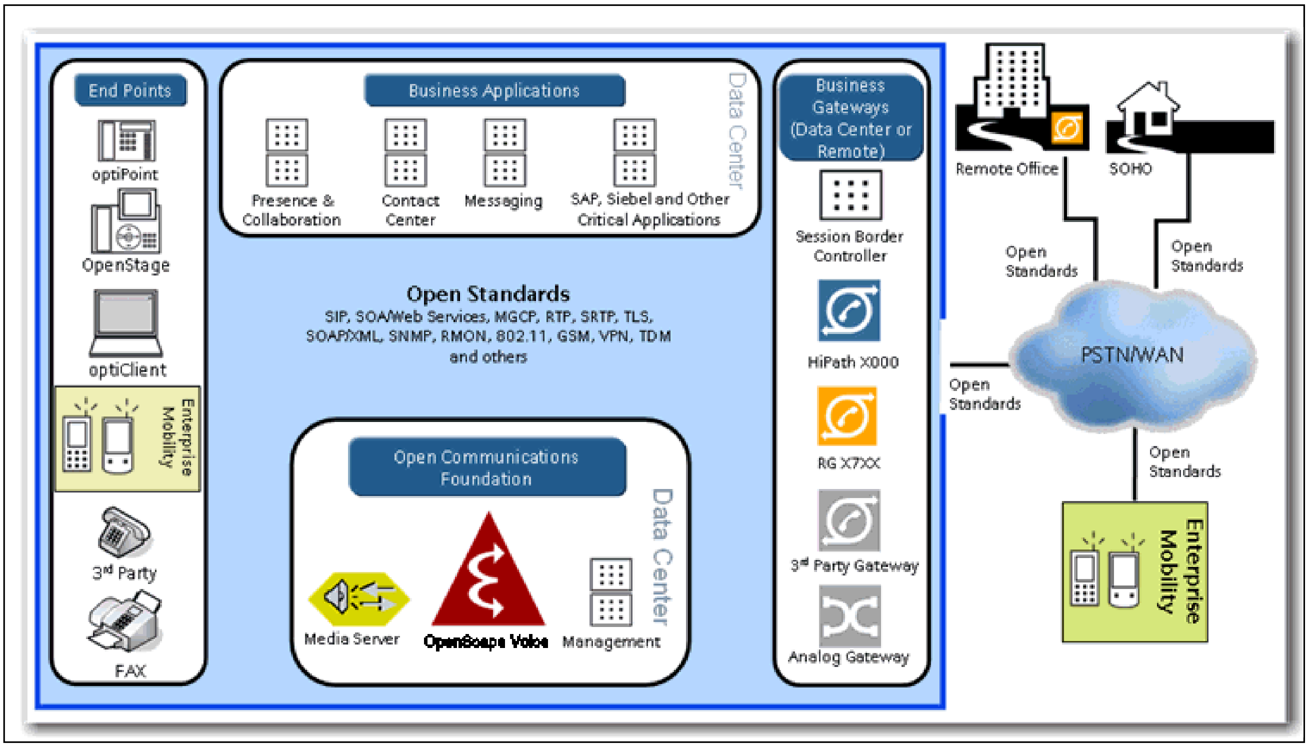


Figure 1 *Unify OpenScape Voice Main*

1.2 Unify OpenScape Voice Configuration Options

1.2.1 Deployment Models Overview

A set of common configurations are shown on the next several pages and are designed to meet the requirements of the customer in the most efficient way. The customer has the choice of using a single server or a dual-node (redundant) installation for “5 nines” reliability, integrated or functionally distributed architectures, single site, or geographically separated installations. This section does not describe every valid configuration but illustrates, at a high level, the most common configurations.

1.2.1.1 Integrated Simplex

In the integrated simplex deployment model (Figure 2, "Unify OpenScape Voice—Integrated Simplex Configuration"), the Unify OpenScape Voice Assistant administration application, OpenScape Media Server, deployment service (DLS), HiPath license management (HLM) tool, Common Management Platform (CMP), and OpenScape UC Application are all installed on a single server.

- Table 1 shows the measured mix of users for the supported hardware platforms when the OpenScape UC Application is activated. The formula assumptions (footnoted in Table 1) are:
  - BHCA per user is 5 CCS.

    Note: CCS are units of 100 seconds of usage per hour (for details, refer to Section 4.1.1, "Traffic Measurement Units").

  - CSTA originated calling (ringback tone) is 18 seconds.
  - Call duration (time the average call is connected) is 180 seconds.

Platform	UC Users	Voice-Only Users	Overall Users
IBM x3550 M2 - (Not available for new orders)	0	5000	5000
	500	500	1000
FSC RX330 S1 * - (Not available for new orders)	0	5000	5000
	500	500	1000
IBM x3550 M3	1250	5000	5000
FSC RX200 S6	1250	5000	5000
IBM x3550 M4	1250	5000	5000
FSC RX200 S7	1250	5000	5000

Table 1 Integrated Simplex - Maximum Users on Each HW Platform

* The maximum number of OpenScape UC users in the RX330 platform is 500. The gradations can be calculated by the formula: 5000 - (9 X number of UC Users).

- The customer has the option of installing the Unify OpenScape Voice Integrated Simplex software image on a Virtual Machine.
- The customer has the option of installing CLM/HLM/DLS on separate Windows servers.
- As a simplex (nonredundant) system, this configuration does not provide "5 nines" reliability, but can be suitable for some small enterprises with limited budgets.

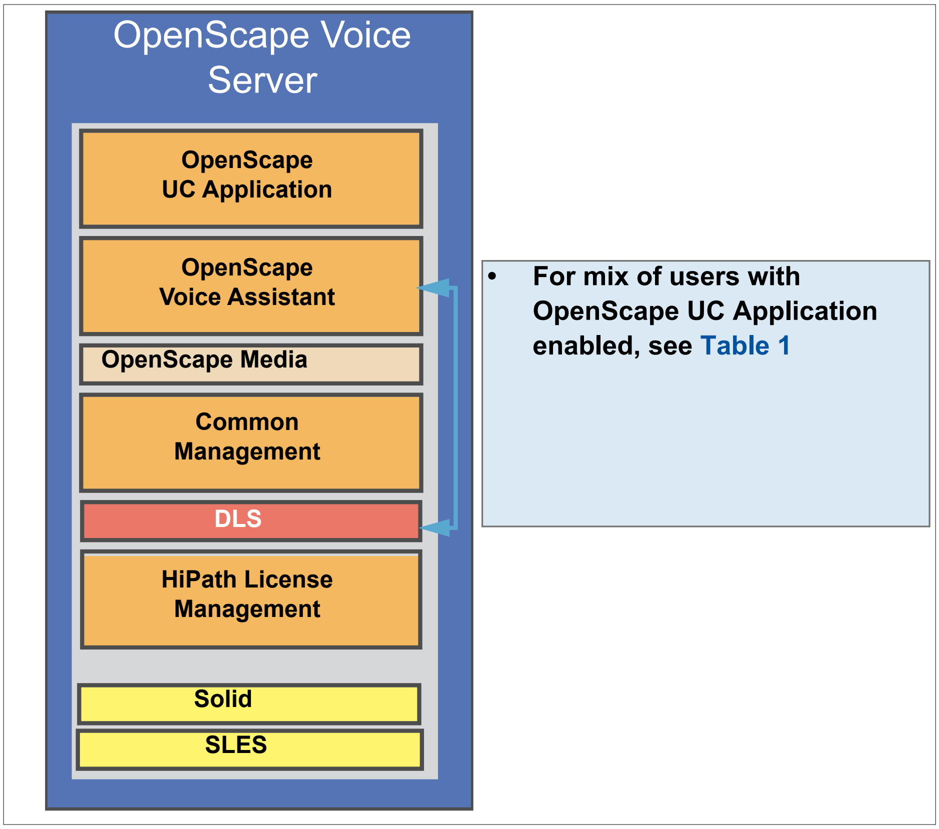
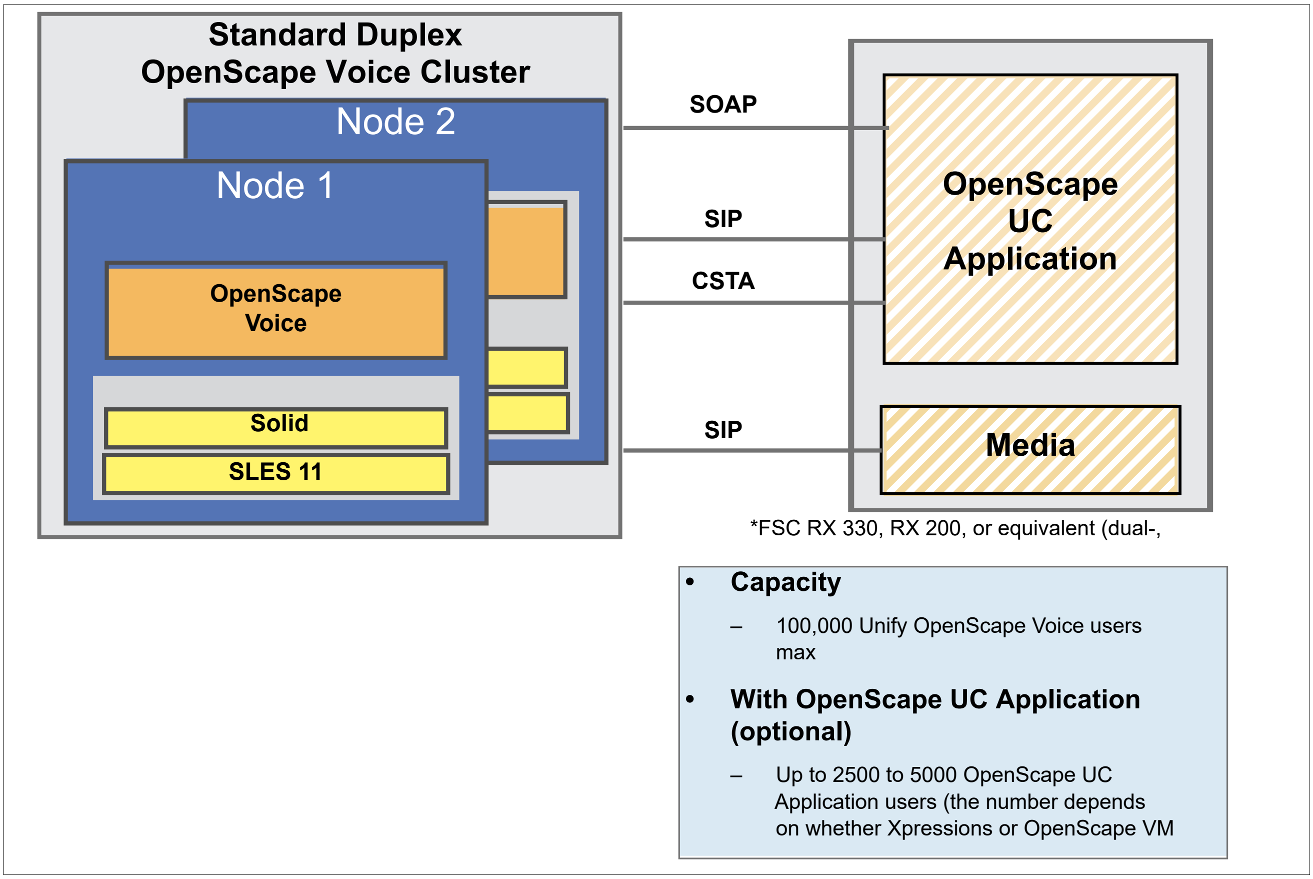

OpenScape Voice Server
OpenScape UC Application
OpenScape Voice Assistant
OpenScape Media
Common Management
DLS
HiPath License Management
Solid
SLES
• For mix of users with OpenScape UC Application enabled, see Table 1

Figure 2 Unify OpenScape Voice—Integrated Simplex Configuration

1.2.1.2 Standard Duplex

In the standard duplex deployment model (Figure 3, "Unify OpenScape Voice—Standard Duplex Configuration"), the Unify OpenScape Voice system runs on two servers. The two Unify OpenScape Voice nodes can be co-located or geographically separated. All the supporting applications (HLM, CMP, Assistant, Media Server, and DLS) are installed on external servers.

The Hardware Platforms supported by the Standard Duplex deployment model (see Table 99, "Unify OpenScape Voice Hardware Platforms") are the same as those supported by the Integrated Simplex (see Section 1.2.1.1, “Integrated Simplex”). However, the Standard Duplex configuration can support up to 100,000 subscribers under certain traffic and feature configurations, irrespective of the Hardware Platform used.



- **Capacity**
  - 100,000 Unify OpenScape Voice users max
- **With OpenScape UC Application (optional)**
  - Up to 2500 to 5000 OpenScape UC Application users (the number depends on whether Xpressions or OpenScape VM

Figure 3 Unify OpenScape Voice—Standard Duplex Configuration

The overall capacity of the system can scale upwards by installing multiple application servers of each type. An overview of application server performance limits are shown in Table 2. Numerous configuration options exist for each of these applications. Refer to product-specific documents for more detailed and up-to-date product limits.

Application	Server Type	Example	Performance Limit
OpenScape UC Application	2 quad-core	FSC RX 300 S3	5000 subscribers
CMP / Unify OpenScape Voice Assistant	1 dual-core	FSC TX 150 S5	20,000 subscribers
	2 quad-core	FSC RX 300 S3	100,000 subscribers

Table 2 Application Server Performance Limits (Seite 1 von 2)

Application	Server Type	Example	Performance Limit
OpenScape Media Server	1 dual-core	FSC RX 300 S3	150 channels (G.711) or 52 channels (G.729)
	2 quad-core	FSC RX 330 S1	500 channels (G.711) or 175 channels (G.729)
Xpressions	1 dual-core	FSC TX 150 S5	4000 subscribers 60 voice mail channels (G.711)

Table 2 Application Server Performance Limits (Seite 2 von 2)

1.2.2 Other Configuration Options

1.2.2.1 Node-Separated Configurations

Refer to Chapter 13, “Redundancy and Node Separation”, for information about deployments in various node-separated configurations.

1.2.2.2 Common Management Platform (CMP)

The Common Management Platform is a browser-based application that gives the administrator network status and administrative access to many of the components of the of the Unify OpenScape Voice solution. It provides access to the following components:

- **Unify OpenScape Voice Assistant:** A unified graphical administration tool, Unify OpenScape Voice Assistant runs under (as part of) the CMP and provides for the administration of Unify OpenScape Voice using a standard web browser. The Assistant software is installed and runs on the Unify OpenScape Voice server itself, on the integrated system, or can be installed as a standalone application on a Linux server, for any system configuration.

  On the integrated system, Unify OpenScape Voice Assistant operates in a single-node environment or in a cluster. In a cluster environment, the Assistant runs active-active, with instances on both nodes of the duplex system. The active instances of Unify OpenScape Voice Assistant maintain database synchronization of administration updates to the master Unify OpenScape Voice database.

- **OpenScape Media Server:** The OpenScape Media Server can be installed on a separate Linux server or on Unify OpenScape Voice itself (integrated systems under 5000 lines only). Note that the actual number of users a single OpenScape Media Server can support depends upon the installation type (internal or external) and the feature usage options chosen by the customer.

- **OpenScape Deployment Service (DLS):** The DLS is a Java-based application with a browser-based user interface that is used to configure and manage Unify SIP telephones connected to the Unify OpenScape Voice system. It can run on the Unify OpenScape Voice system or on a standalone Windows server. See Section 6.4, “OpenScape Deployment Service (DLS)” for more information.
- **OpenScape UC Application** : OpenScape UC Application is an advanced unified communication application which can provide voice mail, conferencing, mobility, and presence service for Unify OpenScape Voice subscribers. It runs on Unify OpenScape Voice in the integrated simplex configuration, and can also be installed on one or more external Linux servers in other configurations. See Section 6.6, “OpenScape UC Application”, on page 119 for more information.

1.2.2.3 OpenScape Xpressions

OpenScape Xpressions, is an external unified message application which can process voice and fax mail, and deliver messages directly to the user’s Outlook or Notes E-mail box. See Section 6.2, “Messaging Servers” for more information about Xpressions.

1.3 Terminology for Switching Systems

The following switching systems are referred to frequently in this document:

- **Unify OpenScape Voice**: Scalable enterprise softswitch that can support up to 100,000 subscribers.
- **OpenScape 4000:** Unify’ advanced hybrid TDM/VoIP switching system, that can support up to 12,000 subscribers.
- **HiPath 3000:** Unify’ highly flexible hybrid TDM/VoIP switching system for customers with smaller line size requirements.

1.4 Terminology Used with the Private Numbering Plans

There are certain terms that the reader will encounter in the discussion of private numbering plans. A few are listed here.

closed numbering plan

This term commonly applies to numbering plans in which the number dialed to reach a given party is always the same, regardless of where in the network the caller is located. In the enterprise environment, the extension dialing plans used within a single switch or in a small private networks are examples of closed numbering plans. In the public network, there are a few very small countries that still maintain closed numbering plans.

Note: Some sources use the term *closed dialing plan* instead of *closed numbering plan*, and reserve the term *closed numbering plan* to signify networks where the fully defined subscriber numbers are all the same length.

complete number

A number sufficient to route the call to its final destination—for example, a private network number that consists of the on-net access code, a location code, and an extension number.

device

An instrument which can be dialed, such as a telephone or a fax machine.

equipped quantities and wired-for quantities

Equipped quantities refers to the number of devices actually connected to the network and activated within the PBX or softswitch. *Wired-for* is an obsolete term in the VoIP environment. A more appropriate term is *licensed for* or *authorized for*, because the addition of additional devices—for example, phones—does not require any new hardware or cabling in the switchroom or softswitch cabinet.

extension dialing plan

A dialing scheme in which each device within the network can be accessed by its extension number. Extension dialing plans are also known as *closed numbering plans* or *single domains.*

extension number

A short form of the subscriber number dialable within the business group or location.

local site/remote site

These terms refer to the user’s point of view. The geographical site in the network in which the user is currently located is the local site, and all other geographical sites in the same network are remote sites.

location code

A portion of a private network number that identifies a particular PBX or softswitch, physical or logical location, or organization within the network, to which a group of subscribers will be assigned, and a call may be routed. In large networks, each company location will typically have one (or more) location codes assigned.

location dialing plan

A dialing scheme in which the caller must dial the location code plus the extension number. Typically, location dialing includes the dialing of the on-net access code as well. Location dialing plans are also known as *open numbering plans* or *multi-domain networks.*

multi-domain network

See *location dialing plan.*

off-net

A term indicating a process, location, or equipment (for example, a central office) that is *not* considered to be part of a customer's private network.

off-net access code

A prefix access code to permit access to remote destinations using facilities provided by the PSTN or a third-part service provider.

off-net destination

An addressable location or device *not* within a customer's private network. In the case of VoIP, the term off-net applies to equipment connected and reachable through the public switched telephone network (PSTN) gateway or SIP Trunking. It can also apply to equipment connected behind an SIP proxy, where the equipment is addressed and reached using a separate numbering plan.

off-net routing

Routing a call to a next hop destination which is reached via the PSTN or through a public VoIP proxy.

on-net

A term indicating a process, location, or equipment (for example, a private branch exchange [PBX]) that is considered to be part of a customer's private network.

on-net access code

A prefix access code to permit access to remote destinations using the customer’s private network, which may include TDM trunking, LAN, and WAN facilities.

on-net destination

An addressable location or device within a customer's private network. In the case of VoIP, the term on-net applies to equipment connected and reachable via the corporate LAN/WAN utilizing the corporate numbering plan.

on-net routing

Routing a call to a next hop via the customer’s private network, which may include private facilities and LAN/WAN facilities.

open numbering plan

This term commonly refers to a numbering plan in which the number dialed to reach the desired party may be different, depending on the location of the caller. Most national networks and large private networks fall into this category. In the US public network, for example, the caller is usually not required to dial the area code when dialing a local number, but will be required to dial the area code to reach the same party, when calling from a distant location.

Private networks that use extension dialing within a location, and require location codes to enable dialing between locations, are open numbering plans.

Note: Some sources use the term *open dialing plan* instead of *open numbering plan*, and reserve the term *open numbering plan* to signify networks where the fully defined subscriber numbers are not all the same length.

private network

A network owned or leased by a business or corporation, with its own numbering plan and subscribers.

public network

A network owned by a public carrier. It may be a traditional TDM network, an IP network, or a combination of the two.

routing

Process of selecting a next hop destination for a call.

single-domain network

See *extension dialing plan.*

station

A telephone.

wired-for quantities

This term is obsolete in a VoIP network. See *equipped quantities and wired-for quantities.*

2 The Network Design Team and Its Tasks

This chapter describes the network design team, the goals of a good design, and the issues to consider while developing the network design.

2.1 The Network Design Team

The purpose of the network design team is to provide or coordinate the information and expertise required to design a network that meets customer requirements. The core of the design team is the sales account team from Unify, which consists of a sales representative and an Unify OpenScape Voice Regional Expert assigned to the account. Any of the following people or entities are included as needed:

- The customer
- Systems engineers in the same or another sales office
- Unify OpenScape Voice Pursuit Team
- Other sales personnel who have experience with similar applications
- Voice and data network designers
- National Support Center (NSC)
- Customer engineers or installation specialists

If other expertise is needed, the network design team can also include individuals from the following organizations:

Call Center Engineering

This group specializes in call centers handling more than 100 agents and cases where integrated services digital network (ISDN) or other computer-telephone interfaces are involved. It is especially helpful where systems integration and consulting are required.

Network Systems Group (NSG)

This group provides complete network solutions with expertise in voice and data network design, systems integration, and support.

2.2 Goals of Network Design

The goal of designing a network is to fulfill the site-specific needs and expectations using a customer-driven balance between cost and performance.

Cost considerations include the following:

- Design
- Installation
- Maintenance and administration over the life of the network
  - Repairs
  - Traffic metering
  - Moves and changes
  - Adding capacity to accommodate growth
- Evolution of the network over time

Performance considerations include the following:

- Transmission quality—how quickly the call is established, voice quality, data throughput, and so forth
- Availability—the degree of traffic congestion in the network
- Reliability—the mean time between failures (MTBF) and routing options to prevent congestion
- Survivability—the response of the network to power outages, failed private branch exchanges (softswitches or PBXs), and other problems
- Optimal routing through the network without loops
- Conservation of trunks

How well a network performs is largely determined by the network design team's planning. For example, call routing plans, switch configuration, and network topology all influence network availability. System redundancy, such as having two power supplies, multiple paths, or two processors, affects reliability. Customer call-flow priorities and routing plans affect survivability. Network delays caused by poor routing plans can noticeably affect quality and speed.

Although each organization values these considerations differently, it is up to the network design team to meet the performance goals and still remain within the customer's budget and Unify' capabilities.

2.3 Steps in Designing a Network

Designing a network usually requires several iterations and includes the following steps:

1. Defining the cost and performance goals
2. Gathering information on the existing telecommunications environment and traffic patterns
3. Defining the desired network topology, including alternate routes, disaster recovery scenarios, and future expansion
4. Designing the individual switch configurations
5. Designing the network using Unify configuration tools
6. Validating the configuration with the customer

2.3.1 Defining the Customer’s Goals

Defining the customer’s goals is an important step. You should obtain answers to the following questions:

Note: Depending on the data load and type, it may be advisable to segregate VoIP traffic onto a separate Virtual LAN to ensure good voice quality (Quality of service [QoS]).

- What level of reliability and voice quality do the users expect of the network?
- What features are required?
- What is the dialing plan or numbering plan?
- What applications need to run on the network?
- What types of data must the network carry?
- What is the present and future mix of voice, video, and data?
- What are the call detail recording (CDR) requirements?
- What are the present and future PSTN trunking needs and plans?
- What present and future applications require high bandwidth?
- Are there future organizational goals that could affect the network?
- What future growth is expected for the network and for each site?

- Are the goals economically and operationally feasible?
- What type of network management is needed?
- Does the network interface with an international network?
- What are the E911/emergency calling requirements of the customer?
- Does the customer have regulatory CALEA/lawful wiretap requirements?

2.3.2 Gathering Information

After defining the goals, the next step is to gather detailed information about the customer’s current telecommunications environment.

Include the following information:

- Equipment types and locations for both equipped and planned quantities
- Current communications links
- Numbering plan
- Traffic load and patterns
- Routing plan, including alternate routing
- Synchronization plan
- IP network details, including IP addresses and subnet plan, and the location of DHCP and DNS servers
- For network IP planning it should be considered, that there should not be more than 500 devices in the same physical IP subnet in which the OpenScape Voice server resides. It it recommended that the devices reside in a different IP subnet than the OpenScape server.

A network diagram is useful for viewing the interrelationships between components, particularly if the network diagram is accompanied with an equipment table lists showing the “planned” or “equipped” capacity.

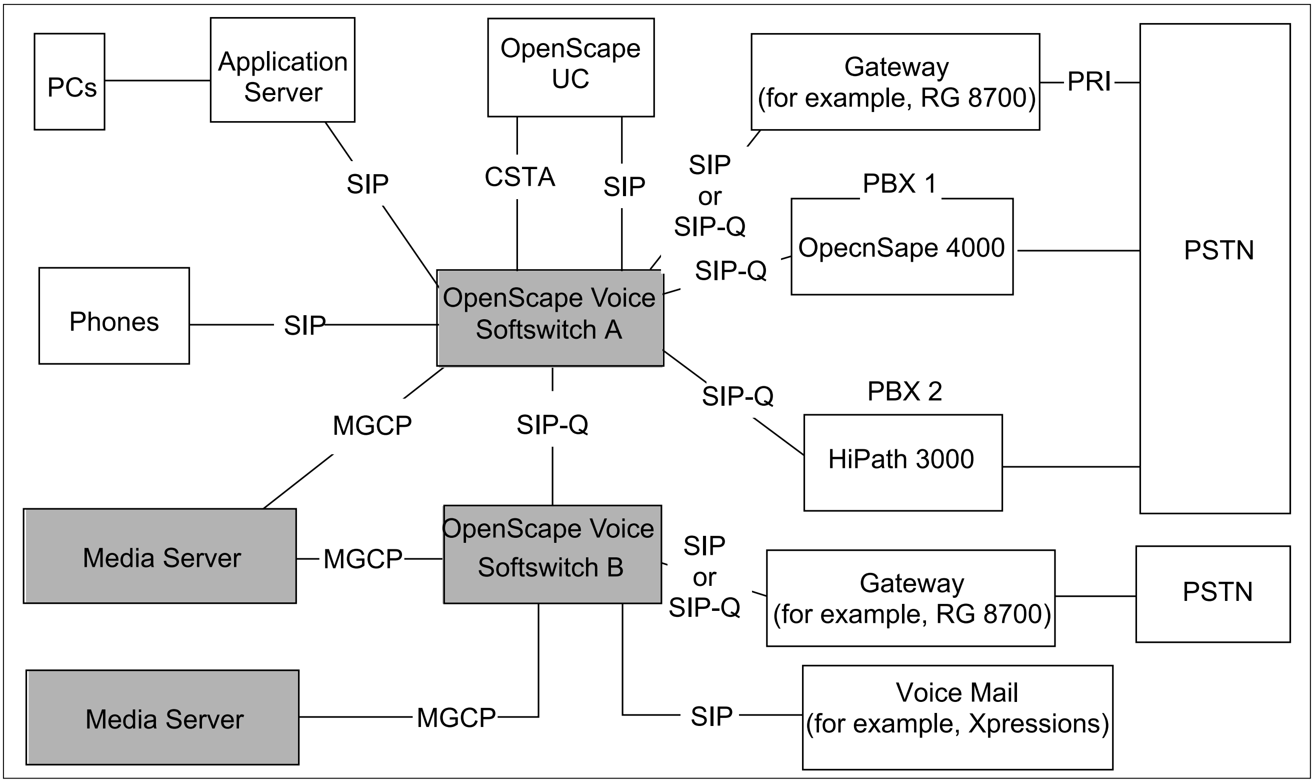


Figure 4 Example of an Network Containing Unify OpenScape Voice Softswitches

In the traditional PBX world, the term *wired-for* was used to described the maximum number of interfaces that can be physically installed in a PBX. Another related term, *equipped-for*, was used to described the number of interfaces actually installed in a PBX. However, for the softswitch, the wired-for quantity is an obsolete term, since no additional hardware is normally required to add additional subscribers or endpoints. The user only needs to ensure the system is licensed and configured for the new quantities. A more important number is *maximum quantity*, the quantity at which the system can no longer be expanded just by software means, and new hardware may be required.

Wired-for or equipped capacity can be an issue for PSTN gateways and media servers (voice mail servers and conference servers).

2.3.3 Routing Plan

The routing plan defines:

- All possible routes among the PBXs or softswitches within a network
- Access to the public network

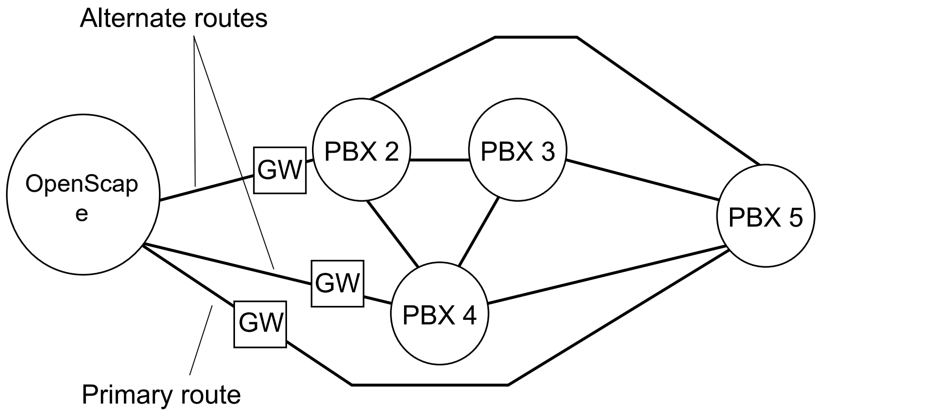
The routing plan in a VoIP network is different from traditional routing plans in three important ways:

- Control signaling and the resulting voice channels may take different paths through the network. There is no longer a tight bond between control signaling and the resulting voice channel between two endpoints.
- In a VoIP network, path selection and routing is handled by the underlying IP data network, its routers and switches. Therefore, it is more customary to configure the voice network as a full-mesh network, with each softswitch having a direct logical route to each other softswitch.

  A star-based routing architecture or partial meshed network were historically used to optimize trunk and channel bandwidth utilization on the links among the PBXs. In the VoIP network, this is generally not necessary, because the underlying router network allows the voice streams between the endpoints to find the optimal paths, regardless of the path chosen for the call signaling. In a VoIP network, a star-based routing architecture may be useful when the number of softswitches is very large, as a means for simplifying network administration, but it is generally not needed for optimizing call flows or bandwidth between the softswitches.
- The placement of media servers and gateways becomes very important because the softswitch relies on these servers for many important functions. It is customary, but not mandatory to co-locate the media server and gateways with the softswitch(es).

When a call is made, an administrable routing database in each switch determines the most efficient way to route the signaling connection of the call.

The routing plan defines the relationship between the physical connections (the path the call takes through the actual network) and the logical connections (the various paths, consisting of the primary route and all alternate routes possible between PBXs or softswitches). This is illustrated in Figure 5, "Comparison of Physical and Logical Transmission Facilities". A call between a user on Unify OpenScape Voice and a user on PBX 5 can use the primary route or an alternate route. The route used determines the physical connections that make the call possible. In other words, a single logical connection can have many possible physical paths.



A logical connection from OpenScape Voice to PBX 5 can have many physical routes.

Figure 5 Comparison of Physical and Logical Transmission Facilities

In a mixed TDM/VoIP network, it is important to avoid unnecessary conversions from VoIP to TDM and vice versa, since gateways can add delay to the connection and reduce voice quality. The goal should be that a call never passes through more than two gateways (although there can be exceptions).

When designing a routing plan, ensure that you consider routing of calls to public network trunks when all available private network trunks are busy.

2.3.4 Traffic Plan

A traffic plan defines the traffic conditions for each softswitch or PBX in the network, and between any two PBXs or softswitches in the network. It balances the number of calls going through each softswitch or PBX in the network, which optimizes performance and cost. The traffic plan defines grade of service goals within the individual softswitch or PBX and across the entire network. (The grade of service specifies the proportion of calls that are not completed because of unavailable resources.)

The traffic plan must consider the following topics:

- Primary route traffic and attributes (such as gateway trunk type)
- Alternate route traffic (between PBXs only)
- Busy hours
- Call center traffic

- PSTN and IP carrier rates
- Communications mix (voice, data, fax, and video)
- Load balancing issues and constraints
- Network traffic (calls to, from, and through the PBX involving other PBXs)
- Bandwidth available between the softswitches
- Number and location of attendant positions
- Number of routes
- PBX-to-PBX traffic
- Voice mail server location
- Planned grade of service or busy hour call attempts (BHCA)
- Priority of routes
- Private network traffic
- Inbound/outbound public traffic
- Traffic to and from application servers on remote nodes

If traffic information is not available, the type and capacity of current transmission facilities can help determine the level of traffic between switches.

Chapter 4, “Calculating Network Traffic, Bandwidth Requirements, and Gateway Sizing” describes traffic in detail.

2.3.5 Synchronization Plan

Synchronization is not required for softswitches because the links between softswitches are not synchronous. VoIP gateways are normally time-synchronized to the PSTN through one or more digital channels. Unify OpenScape Voice can be time-synchronized to a network time server (NTP). SIP phones are normally synchronized to an IP network time server (typically the same one used by Unify OpenScape Voice).

2.3.6 Loss Plan

Like the ISDN network, the VoIP network provides completely separate full-duplex transmit and receive paths, thereby reducing or eliminating the need for a complex loss plan. The loss plan for IP gateways is covered in the TIA standard TIA 912. One function of the gateway, and the TDM network behind it, is to normalize voice levels arriving from the various trunk and line types, and to present a common loudness rating to the VoIP network. The RG 8700 gateway, for example, allows a separate attenuation level to be set for each trunk group.

Attenuation levels between digital (ISDN) trunking and the VoIP network are normally set at 0 dB (no attenuation).

2.4 Defining the Desired Network

Using the customer’s cost and performance requirements and the information gathered from the current telecommunications environment, Unify personnel assist the customer in writing a description of the desired network. The description should encompass all the elements of the network plan as described in Section 2.3.2, “Gathering Information”.

When developing a new network plan, include any constraints that currently exist. For example, an existing numbering plan can use blocks of numbers allocated by the central office for direct inward dialing. Additionally, existing feature access codes, location codes, or extension numbers can place constraints on the new network, unless the customer is willing to implement a new numbering plan. The location of existing voice network facilities, data network facilities, and voice PBXs may also constrain the design of the network.

2.5 Creating the Network Configuration

Create the network configuration as follows:

1. Determine the number of gateways and softswitches required, in addition to the type and location of legacy PBXs.
2. Establish the type and number of required station equipment at each location.
3. Determine the number and type of PSTN trunks required on the gateways and/or legacy PBXs.
4. Assign applications by location.
5. Identify the locations of shared resources, such as the Xpressions messaging system and IVRs.

There are typically two constraints on the softswitch:

- Call handling capacity (busy hour call attempts rating)
- Subscriber capacity (maximum number of subscribers permitted in the softswitch database)

To satisfy the customer’s needs and budget, the network design team may need to develop several switch designs to determine the optimal design. The team might:

- Initially propose one switch design, then modify it as warranted.

  -or-

- Prepare several switch designs and permit the customer to choose the design most suited to the needs of the organization.

2.6 Private Communications Networks

Private networks provide communication services to specific organizations. They can route voice, video, fax, and data. Typically, they include:

- Two or more PBXs and/or softswitches
- A combination of analog, digital, and IP technology
- Access to public switched communication networks for both incoming and outgoing calls

Some private networks also support computer connections for local area networks (LANs) and wide area networks (WANs).

The benefits of a private network are:

- Increased efficiency
- Reduced cost
- Features not available in public networks, such as feature transparency
- Increased communications security
- Control over the structure and quality of the network
- Control over features provided to the users
- Shared resources such as Xpressions and long distance service
- Network monitoring for optimum use of network resources

Refer to Section 9.2, “Private Network Interfaces” for detailed information about private networking.

2.7 Traditional Trunking vs. IP Networks

Voice over the IP network provides several advantages in comparison to traditional trunking, in environments where the customer is already paying to maintain an IP data network:

- **Facilities cost**: There is a substantial cost to installing and maintaining a dedicated TDM network for voice communication. When voice and data are combined on a unified data network, maintenance costs usually go down.
- **Flexibility**: Because dedicated TDM voice network facilities can be expensive to install and lease, they need to be carefully engineered and sized for full utilization, and during periods of heavy call load, call blockages may occur.

  Because voice channels must be terminated at the PBXs that control them, traffic patterns dictate, to a great extent, the location and quantity of PBXs.

  In contrast, because the voice channels of VoIP calls typically go directly from phone (device) to phone (device), and need not go through the softswitch, there are fewer restrictions on the location and number of softswitches required in the network. Finally, because voice and data share a common physical network, bandwidth can be shared between the two applications, and some capacity restrictions can be reduced.

3 Planning Network Equipment, Topology, and Routing

This chapter describes how to plan network equipment, network topologies, network requirements diagrams, and routing tables. It includes an example to illustrate most of the topics.

3.1 Defining Usage and Equipment in Multiple-Switch Configurations

The number and the location of softswitches in a network depends on:

- The number of users
- The number and location of sites
- Topology, reliability, and type of existing data facilities.
- Location and type of existing legacy voice facilities and PBXs

After these factors are reviewed, the placement of softswitches in a network can be performed.

3.1.1 Allocating Extensions

Before allocating extensions to a specific softswitch, the network designers should evaluate available traffic information between sites.

Determine which user groups receive large numbers of incoming calls or place large numbers of outgoing calls. The placement of these user groups on a particular softswitch affects the allocation of gateways and the operation of features related to the groups. For instance, although many features can work across multiple softswitches, members of the following community-of-interest groups must reside in a single softswitch:

- Pickup and hunt groups
- Executive/assistant groups
- Keyset groups sharing multiple lines

Note: Network-wide pickup groups are supported. This support is limited to SIP-Q private network members belonging to the same business group—that is, SIP-Q endpoints need to belong to the same business group as the subscribers. SIP-Q members are restricted to

OpenScape 4000 users and remote Unify OpenScape Voice subscribers.

Unify OpenScape Voice does not provide an internal implementation of ACD. The hunt group feature can be used to create simple call distribution arrangements with announcement. When a full ACD solution is required, Unify OpenScape Voice can be integrated with OpenScape Contact Center and Genesys ACD systems to provide such a solution.

3.1.2 Allocating Trunks

In an Unify OpenScape Voice network, the PSTN trunks are connected to and terminated on a hardware unit known as a *gateway*.

Table 3 lists the gateway types that are supported in Unify OpenScape Voice networks. The selection of a gateway or gateways depends on many factors, including the placement of the trunk facilities.

PBX or Gateway Type	T1/ E1	DS 0	Analo g	Notes
OpenScape 4000	•	•	•	A good option if the customer already has a OpenScape 4000 PBX.
HiPath 3000	•	•	•	A good option if the customer already has a HiPath 3000 PBX.
RG 8700 family	•			Standalone gateway. T1 and E1 spans only.
RG 8300	•			A SIP gateway that enables IP connections with SIP-Q to Unify OpenScape Voice and ISDN T1/E1 PRI connections to PSTN or to the OpenScape 4000.
OpenScape Branch 50i	•	•	•	Provides integrated Analog Adapter and PSTN Gateway connectivity.
Mediatrix (various models)	•	•	•	For small systems. Maximum size is two T1/E1 spans.

Table 3 Gateway Types Supported in Unify OpenScape Voice Networks

In deciding placement of trunks, cost and reliability are the primary consideration.

- What area or city code, and what office code, does the customer want to present to callers? If a customer wants a New York City area code, he typically needs to place the gateway in that location.

- Where are the employees located? Overall costs of trunking tend to be cheaper if the gateway is close to the employees that will use it.
- What is the availability and location of existing equipment.
- What is the availability and location of facilities between the company locations (LAN and WAN facilities or legacy trunking facilities)?
- Are there economies of scale? One large trunk group typically costs less and can be used more efficiently than many smaller groups.
- What is the reliability of the trunks? If a network facility (gateway, WAN link, or trunk span) is temporarily out of service, can the employees still make urgent calls to the public network?

3.1.2.1 Distributing the Trunks Among Sites

In a company that has multiple sites, the advantage of distributing the gateways among the various sites are:

- Each site can have a local listed directory number and/or DID number block.
- In the event of an outage on the corporate LAN and WAN, the customers at each site can still have incoming and outgoing telephone service.
- The load of inbound and outbound calling on the corporate LAN and WAN is minimized.

The advantages of centralizing all trunks at a single location usually are:

- Easier physical maintenance (all the gateways are at one site)
- Lower cost of facilities from the local and long distance companies
- Simpler routing arrangement

3.1.2.2 Using IP Trunking

A small but growing number of local and long distance carriers provide IP trunking. This eliminates the need for gateways, which are IP-to-TDM converters. Instead, a digital trunk span from the carrier is connected through a firewall server to the customer LAN/WAN, which enables Unify OpenScape Voice to route calls directly between the customer telephones and the carrier IP network using the SIP protocol. See also Section 6.9.3, “SIP Trunking”.

3.1.3 Assigning Attendant Positions

Unify OpenScape Voice supports multiple business groups, which can be viewed as separate organizations within the enterprise, or separate enterprises sharing a softswitch (VoIP tenant service). Because many feature restrictions exist on calls between business groups, Unify generally recommends that all subscribers within an enterprise belong to a common business group. It is common for each business group to have its own attendant and answering arrangement.

- If the trunks are on an Unify OpenScape Voice gateway (such as the RG 8700 gateway), the attendant positions are probably best located on Unify OpenScape Voice, and OpenScape Branch during normal and survivable modes.
- If the trunks are on a PBX gateway (such as the HiPath 3000 or OpenScape 4000), placing the attendants on the PBX is a good option, particularly if a substantial number of subscribers remain connected to the PBX rather than to Unify OpenScape Voice.

It is particularly important to avoid call flows that create *hairpin* (or *trombone*) connections at the gateway between a legacy PBX and Unify OpenScape Voice. If a trunk call arriving on the switch A is routed over a gateway to an attendant on switch B, and must then be transferred and extended by to a subscriber on switch A, a trombone connection may result, which consumes resources (two channels) on the gateway between the PBX and Unify OpenScape Voice for the duration of the call. This results in inefficient gateway channel utilization, and should be avoided by proper placement of the attendants.

Trombone connections are not a problem in homogeneous SIP networks (where, for example, switch A and B are both Unify OpenScape Voice softswitches), or in homogeneous CorNet NQ networks (where, for example, switch A and B are both OpenScape 4000 PBXs), but in mixed networks they can occur.

In general, the attendant position is best placed close to the trunks that require attendant service.

Note: Unify OpenScape Voice does not support DID recall to the attendant if the DID destination fails to answer. Therefore, Unify recommends that all subscribers be configured with no answer forwarding to voice mail or to a must-answer destination (which could be the attendant position).

3.1.3.1 Attendant Answering Positions

Unify OpenScape Voice currently does not support a specialized attendant console. However, it does support attendant groups consisting of SIP keyset telephones and/or SIP keyset soft clients—for example, the optiClient 130 S soft client.

These phones are configured within a hunt group that provides call queuing and uniform distribution to the attendant group members. Each phone or client is provisioned with a Make Busy key, which is used to indicate that the attendant is away or not able to receive calls. When all members of the attendant group have activated the Make Busy feature, the system is considered to be in night mode.

Separate hunt groups may be configured for arriving external calls and internal “dial-operator” calls. The attendant answering positions (SIP keysets) can be configured with separate line keys representing these two call types and their respective call queues.

Unify OpenScape Voice supports OpenScape Contact Center Attendant Console, which combines a soft client PC application and a specially configured SIP telephone to provide an enhanced attendant capability. The attendant console application monitors and controls the incoming traffic using the Unify OpenScape Voice industry-standard CSTA CTI interface.

3.1.3.2 CallTicket Attendant Application

CallTicket is a feature-rich and flexible PC-based attendant application. When integrated as a core component in a telephony solution, it monitors the status of every station, receives incoming calls, and allows designated attendants to transfer calls to the right employees quickly and efficiently.

CallTicket is designed as a centralized application that can host multiple attendants. Full-featured attendants can be located anywhere within the globally distributed enterprise.

CallTicket is designed for use as an enterprise attendant application, to service customers for the best possible business results. Its inherent flexibility allows customers to create call-handling solutions that are fully customized to their operation.

CallTicket delivers all the functions needed for attendant activities. Using tools integrated in the graphical user interface (GUI), the attendant is able to quickly identify the caller’s destination and transfer calls reliably and efficiently. Flexible search options and clear display of call information combine with real-time views of queue workloads to ensure fast and efficient communication.

3.1.3.3 Night Answer Arrangements

It is possible to configure an attendant group with an night answer arrangement. This may be:

- A single phone
- Separate hunt group consisting of alternate SIP phones and clients
- Analog phones connected via SIP adapter modules (Mediatrix AP device)
- Auto-attendant applications
- Recorded announcement devices

3.1.3.4 Auto Attendant

The OpenScape Xpressions Unified Messaging Server provides an automated attendant function. Xpressions connects to Unify OpenScape Voice via a standard SIP interface.

OpenScape Branch provides Auto Attendant functionality during normal and survivable modes.

In normal mode, the incoming call is sent by OpenScape Branch to Unify OpenScape Voice as usual. By deriving that the destination defined in the Request URI is configured as Auto-Attendant, Unify OpenScape Voice routes the call to the corresponding OpenScape Branch. The OpenScape Branch then checks whether the destination DN/FQDN is configured to be served by the Auto-Attendant function. If so, a menu will be selected according to the time of the day and day of the week or according to the menu which was manually activated by a subscriber.

In survivability mode, when the incoming call is received in the OpenScape Branch, it checks if the DN/FQDN is configured to be served by the Auto-Attendant function. If so, a menu will be selected according to the time of the day and day of the week or according to the menu which was manually activated by a subscriber.

Note: This feature cannot be activated on OpenScape Branch together with Backup Automatic Call Distribution (ACD).

3.1.4 Allocating Application Resources

The following are the applications to be considered:

- OpenScape Contact Center
- Xpressions Unified Messaging Server
- OpenScape UC Application (collaboration/conferencing/call screening/mobility services)
- Other CSTA applications (for example, CAP)
- Media Server/IVR

The location and sizing of these servers is important to the layout of the network because they tend to generate and focus large amounts of traffic, in comparison to individual phones and endpoints.

If applications are considered mission-critical, special care must be taken to ensure reliability. Not all applications offer fully redundant operation.

3.2 Estimating the Number and Type of Required PBXs

After determining the number of users at each site, you can estimate the number and type of PBXs required to support the network.

PBX/Switch Type	Number of Subscribers	Notes
HiPath 3000	Up to 500	
OpenScape 4000	200 – 5760	
OpenScape 4000 IPDA	Up to 12,000	Up to 83 remote shelves
Unify OpenScape Voice	300 – 100,000	

Table 4 Planned-For Subscribers in Unify PBXs

If the customer wants a pure VoIP solution based on SIP, Unify OpenScape Voice is the proper solution. If the customer wants a hybrid (mixed TDM/VoIP) solution, or specific features supported only by the legacy PBXs, a HiPath 3000 or OpenScape 4000 PBX may be a valid choice.

3.3 Defining a Network Topology

A network topology describes the arrangement of softswitches, PBXs, and links in a network. The basic network topologies for traditional TDM (telephony) networks are star, ring, and meshed. Most private networks use a combination of these topologies.

In a VoIP network, the physical topology is defined by the underlying broadband data network, and is often less important than in a TDM network. The following factors can impact network design in a VoIP environment:

- In a converged voice and data network, often the data network traffic is significantly higher (in bandwidth requirements) than the voice network traffic and is the primary factor in defining the physical network topology.
- In VoIP networks, the voice network topology is usually a logical and virtual topology placed on top of the physical data network. The voice network may be a logical mesh even though the physical data network has a star or backbone topology.
- In a VoIP network, the path taken by the call signaling messages between the switches and gateways can be completely different from the path taken by the higher-bandwidth voice packets between the two connected endpoints.
- VoIP breaks the wiring and distance barriers between the switch and the phones it serves. A single Unify OpenScape Voice system can serve subscribers in multiple locations and even in multiple time zones, provided that reliable broadband data connections exist.
- Remote users can be connected to Unify OpenScape Voice via the public Internet, providing that adequate security measures are taken.
- Users located in branch offices can be connected to Unify OpenScape Voice via the public Internet, provided that adequate security measures are taken or via a WAN.

Note: Security measures for the above may require security appliances such as firewalls in addition to Session Border Controllers be used in the VoIP signaling path. Any use of SIP Application-Level Gateway’s (SIP ALG) in the VoIP signaling path must be avoided. A centralized or branch office Session Border Controller should be used to address special SIP handling procedures between networks. Attempting to use a SIP ALG will likely lead to some type of VoIP service breakdown. A SIP ALG applied to an enterprise network is at most a partial solution and may work adequately in some simple deployments. In most enterprise networks, a SIP ALG is unable to adequately address all VoIP requirements or requires complex configurations which are difficult to manage.

3.4 Creating a Network Requirements Diagram

A network requirements diagram is a map that denotes the number of users and equipment of the desired network. It constitutes the basis for configuring a new network or updating an existing network.

The following factors are among those that must be considered for a network requirements diagram:

- Required number of subscribers (equipped and planned-for) at each location.
- Number of trunks and digital spans to the public network.
- Number and location of existing private TDM facilities, especially in campus environments where wiring may already be in the ground and paid for.
- The amount of attendant traffic (calls to an answering position).
- Traffic flow between locations.
- Inbound and outbound PSTN traffic patterns and loads, which will be a factor in the location of the gateways.
- The reliability, bandwidth, quality, and topology of the underlying broadband data network.
- Criticality of voice communication to specific sites and organizations.

  If an distributed enterprise site has a small number of users and relatively little external customer contact, it may be possible for it to operate without a local gateway or switch, and rely on one or more broadband data links to a central location where Unify OpenScape Voice and the PSTN gateways are located.
- Location of existing PBXs and application servers.

3.5 Defining Call Routing

3.5.1 Introduction to Routing

Call routing in VoIP is the process of selecting a signaling path for a call. Such a path will always go through at least one Unify OpenScape Voice, and can be:

- From endpoint to endpoint (dialable devices connected to the same soft switch)

- From endpoint to gateway, and vice versa
- From gateway to gateway or to another softswitch (a VoIP tandem connection)

The private IP network may consist of physically-owned data facilities (especially in a campus environment where the enterprise is free to put cable in the ground) or facilities leased from a public carrier. In many cases the private data network will transit public data facilities as a secure virtual private data network (VPN).

The call control signaling between two endpoints, or between an endpoint and a gateway, will go through one or more Unify OpenScape Voice switches. However, the final voice path, taken by the voice packets, will be routed by the underlying data network, and will pass directly between the two endpoints, and not through Unify OpenScape Voice, even though the Unify OpenScape Voice softswitch remains in complete control of the call.

3.5.2 Routing to and from the Public Switched Network

Calls are routed to and from the public switched network through IP gateways.

As a general rule, each gateway should be controlled by a single Unify OpenScape Voice in the network. The gateway is effectively owned by that Unify OpenScape Voice, which serves as a gatekeeper and admission control point to the gateway. All calls to the gateway are signalled through the owning Unify OpenScape Voice, and all calls from the gateway are signaling to the owning Unify OpenScape Voice for further call routing. This simplifies network routing and control. In traditional telephony terminology, one would say that each gateway is associated with a specific Unify OpenScape Voice softswitch.

OpenScape 4000 can support multiple gateway interface cards, each of which is a separate gateway and can be associated with a different Unify OpenScape Voice softswitch, if desired. The HiPath 3000 supports one gateway card (HG 1500).

In a network with multiple gateways and a single Unify OpenScape Voice softswitch, Unify OpenScape Voice uses its routing database to select the most appropriate gateway for an outbound call.

In a network with multiple Unify OpenScape Voice switches, with each Unify OpenScape Voice managing one or more gateways, routing of outbound calls is somewhat more complicated.

The originating Unify OpenScape Voice (where the calling endpoint is registered) may determine, from its routing database, that the best route to the destination is through gateway which is owned by a different Unify OpenScape Voice in the network.

In this case, the originating switch will route the call to the intermediate Unify OpenScape Voice, and that Unify OpenScape Voice will select an appropriate gateway for the call. This type of routing is sometimes called *tail-end hop off* (TEHO). The call is routed through the private network to a PSTN access point (gateway or SIP Trunking) closest to the destination, usually because that is cheapest. Unify OpenScape Voice supports this type of routing.

3.5.3 On-Net and Off-Net Routing

Routing paths and methods have been historically categorized as *on-net* and *off-net*. In the VoIP environment of Unify OpenScape Voice, these terms pertain too SIP signaling:

- A call that remains on the Unify OpenScape Voice SIP signaling network is an on-net call.
- A call that exits the Unify OpenScape Voice SIP signaling network is an off-net call.

3.5.3.1 Attributes Common to Both Routing Methods

Unify OpenScape Voice supports routing of voice, video, digital data, modem data, and fax calls. It uses customer-defined routing tables that provide *incremental routing*, which means that routing is performed at each tandem softswitch along the routing path.

The routing tables are flexible, so that calls to an on-net destination can be routed off-net if necessary (but with a reduction of feature capabilities). Likewise, calls to an off-net destination can be routed on-net, to a remote gateway.

3.5.3.2 Attributes Specific to On-Net Routing

On-net routing has the following attributes:

- On-net routing is routing within the SIP network.
- It supports voice, video, digital data, modem data, and fax calls.

- It allows the endpoints to negotiate the type of media coding and bandwidth required. Calls are not limited to a 64 Kbps channel or multiple 64 Kbps channels.
- It routes calls over the underlying broadband data network, which can include permanent or semi-permanent paths through the TDM network, depending on the capabilities and configuration of the data routers in the network.
- It supports the concept of multiple business groups within a single Unify OpenScape Voice switch and between Unify OpenScape Voice switches, and allows each business group to be associated with a separate numbering plan and private network location code.
- In the event that a call reaches a busy destination, the call is immediately rejected, and the caller given an appropriate busy tone. Queueing (on-hook and off-hook) for an busy destination is generally not provided. However:
  - Most SIP endpoints support multiple simultaneous calls and call waiting, so endpoint-to-endpoint calls encounter a busy condition relatively infrequently.
  - Unify OpenScape Voice supports call back on busy (CCBS) for calls within a business group.
  - If queuing is only needed for special BGLs, the hunt group feature with only one BGL can be used.
  - In the event of temporary WAN congestion or failure, off-net routing is an option (see Section 10.3, “Subscriber Rerouting”).
- Unify OpenScape Voice requires the configuration of a minimum of one business group per switch. The numbering plan for the business group is defined via Unify OpenScape Voice Assistant. Network routing is also configured using Unify OpenScape Voice Assistant.

3.5.3.3 Attributes Specific to Off-Net Routing

Off-net routing has the following attributes:

- Off-net routing is also SIP-based routing, and uses the same data tables and administrative tools as on-net routing.
- Off-net routing terminates at a gateway or border controller (firewall), where the call leaves the customer SIP network. The signaling from Unify OpenScape Voice to the gateway can be:
  - Pure SIP (same protocol used for SIP endpoints)

  - SIP-Q (CorNet-NQ transported over SIP) – available for gateways on a OpenScape 4000 or HiPath 3000 PBX

- Queuing (on-hook and off-hook) for a busy facility—for example, when all TDM trunks are busy—is not provided.
- Incoming trunk calls may queue for a busy endpoint or hunt group, if the endpoint supports call waiting or the hunt group is configured for queueing.
- In the event of gateway or WAN congestion or failure, alternate routing to another gateway is possible (see Section 10.2, “Gateway Rerouting”.

3.5.4 Constructing Routing Tables

The PSTN numbering plan for Unify OpenScape Voice is managed via Unify OpenScape Voice Assistant. Using this interface, the PSTN numbers assigned to this softswitch, and the gateways used for PSTN calling, are defined.

The numbering plan for business group subscribers is defined via Unify OpenScape Voice Assistant.

The following are the factors that can be used to control the path selected to the destination:

- Business group/number plan ID of the caller
- Routing class of service of the caller
- Routing area (location) of the caller
- Time of day and day of week
- The dialed digits

3.5.5 Important Considerations for Routing Tables

The following factors are important when constructing routing tables:

- Direct paths are generally preferable to paths through tandem switches. However, this is subject to the rule regarding gateway ownership (above), and it should be noted (again) that the cost of a tandem connection is less in the IP world than in the traditional telephony world. Even if the signaling path tandems through an intermediate switch, the voice path will be direct between the IP endpoints, and not through the tandem switch.

- Long-distance alternate routes between on-net endpoints should generally be avoided for obvious cost reasons. However, based on the COS of the caller, some calls might be given access to such expensive routes. They may also be used when the intervening IP WAN network is congested or out of service, if a suitable TDM ingress gateway exists near the destination (more on that later).
- It is the administrator’s responsibility to avoid routing loops (see Figure 6).

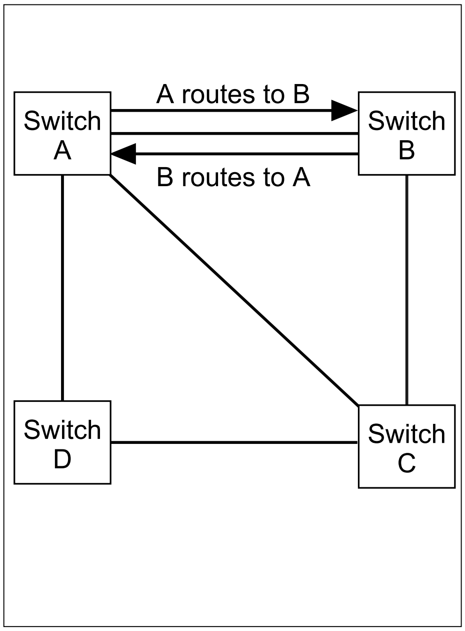


Figure 6 Sample Routing Loop

Referring to Figure 6, assume:

- The primary (direct) route from Switch A to Switch C is not available. The first alternate route goes over to Switch B.
- The primary (direct) route from Switch B to Switch C is not available. The first alternate route goes back over to Switch A, creating a loop.

For this situation, if both primary routes remain unavailable and the routing tables are not configured correctly, the call is routed between Switch A and Switch B

The consequence of routing loops is failed calls and needless load on the softswitch, which can result in network congestion. No trunks are falsely seized in a pure VoIP network. However, in a mixed network of softswitches and traditional PBXs, routing loops can lead to falsely seized trunks.

To help prevent endless routing loops, there is a hop counter associated with every signaling message, which counts consecutive tandem hops the message has taken. If the hop count is exceeded, the following takes place depending on the hop counter exceeded:

- **Internal hop counter:** The last party that was attempted will begin alerting.
- **External hop counter:** The message will go no further and the call is cleared (disconnected).

3.5.6 Trunks Used for Routing

Unlike traditional PBXs, Unify OpenScape Voice does not route calls to specific trunks. It routes calls to specific endpoints (for example, phones and soft clients) and to specific gateways. The selection of the specific trunk, span, or B-channel is handled by the gateway.

The signaling protocols supported depend on the capabilities of the selected gateway.

The RG 8700 gateway can be partitioned into trunk groups. Each group is seen by Unify OpenScape Voice as a separate logical gateway, with a different FQDN (server name), but sharing a common IP address. This permits Unify OpenScape Voice to route calls to a specific trunk group (set of trunks on the gateway) based on the dialed digits, and so on.

3.6 The LoCal Corporation—an Example

The following sections, as well as Chapter 4, “Calculating Network Traffic, Bandwidth Requirements, and Gateway Sizing” use a fictitious company called LoCal Corporation as an example.

LoCal has three sites: Los Angeles, Hollywood, and Anaheim. LoCal’s desired equipment for each site is listed in Table 5.

Site	Phones with Xpressions (Equipped/Planned-For)	Answering Positions (Equipped/ Planned-For)	CSTA Application Server?
Los Angeles	3500/7000	500/1000	Yes
Hollywood	1200/2400	none	No
Anaheim	1500/3000	50/100	No

Table 5 LoCal’s Desired Network Features

LoCal Corporation wants all incoming calls to enter the Los Angeles site with DID trunks. Incoming calls for Hollywood or Anaheim are then routed through the private network to their destination. Each site has its own outbound trunks.

Figure 7 shows a first iteration of a network requirements diagram for the LoCal Corporation. Section 3.4, “Creating a Network Requirements Diagram” describes network requirements diagrams.

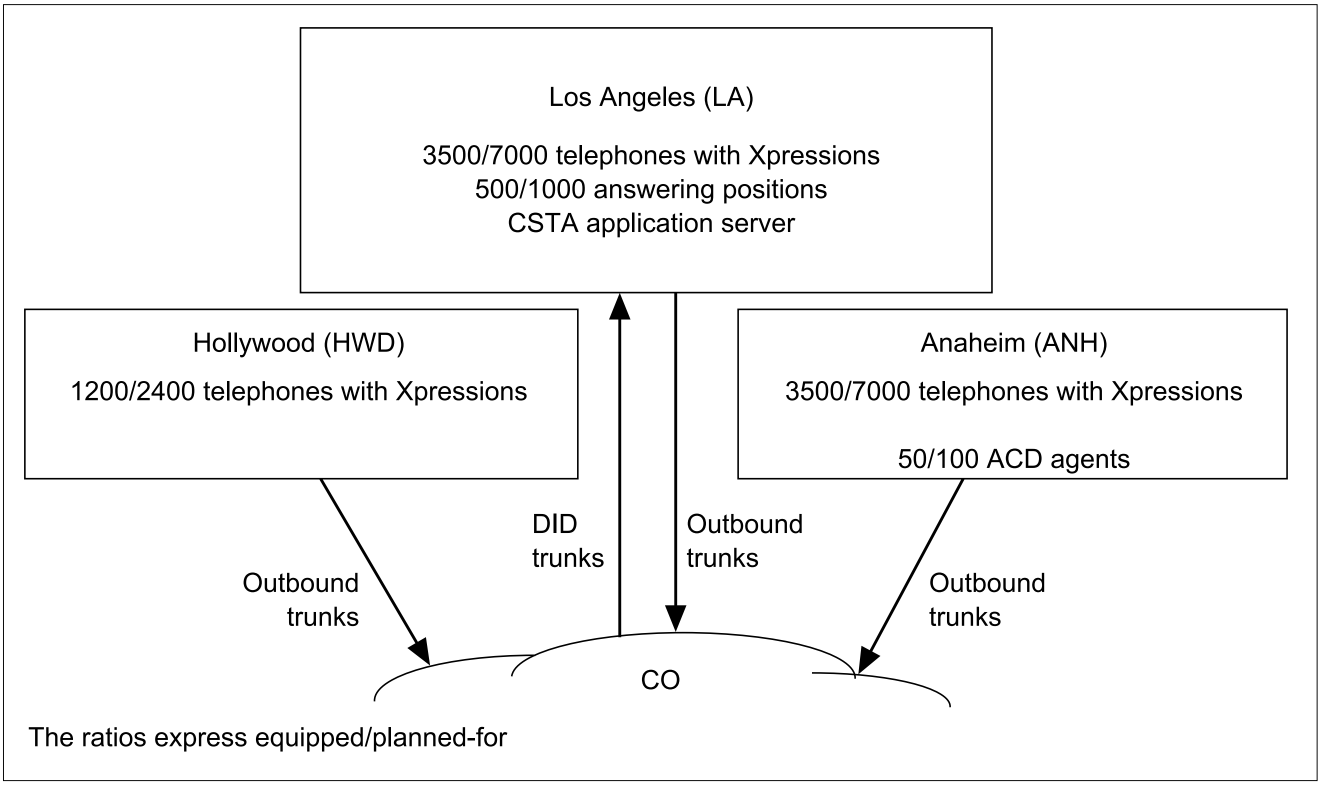

Los Angeles (LA)
3500/7000 telephones with Xpressions
500/1000 answering positions
CSTA application server
Hollywood (HWD)
1200/2400 telephones with Xpressions
Anaheim (ANH)
3500/7000 telephones with Xpressions
50/100 ACD agents
DID trunks
Outbound trunks
Outbound trunks
Outbound trunks
CO
The ratios express equipped/planned-for

Figure 7 Network Requirements Diagram for the LoCal Corporation—First Iteration

3.6.1 Estimating the Required PBXs for the LoCal Application

While this customer configuration would typically require several traditional PBXs, it is well within the capacity of a single Unify OpenScape Voice softswitch. Therefore, as a starting point, we will assume a single Unify OpenScape Voice softswitch for this customer.

The LoCal network requires that all incoming trunks come into the Los Angeles site. That means a significant amount of IP bandwidth must be provided to the other sites to handle the inbound traffic.

3.6.2 Network Topology and Reliability

In the traditional telephony world, network topology refers the configuration of trunks between PBXs. In the converged data and VoIP network, the network topology refers primarily to the configuration of the underlying data switches and routers. It is a data network topology.

The VoIP topology is a virtual topology overlaid on the data network. In the case of LoCal corporation, VoIP topology is simple: we have a single switch in LA. But the data links between main site in LA and the branch locations in Anaheim and Hollywood will be critical to the success of the installation.

Chapter 4, “Calculating Network Traffic, Bandwidth Requirements, and Gateway Sizing” provides guidelines for estimating the bandwidth required for these links. That is one factor in defining the topology. A second factor is reliability. Since all DID traffic for LoCal is arriving at the LA office, an outage of the link to Hollywood or Anaheim would block incoming traffic to these sites.

In the topology shown in Figure 8, "Local Data Network Topology", all the critical backbone components are duplicated, to prevent a single component outage from causing a loss of communication to the branch offices. Even the leased WAN facilities are duplicated, and they should be engineered so that a single external event will *not* cause a loss of both links. They should not, for example, travel in the same fiber-optic cable, such that a single errant backhoe digging along a roadside could tear up both links.

Note: Section 3.6.2.3, “Survivable Gateways” and Section 10.3, “Subscriber Rerouting” describe survivability and subscriber rerouting, which provide an alternate mechanism for maintaining DID service to the branches in the event of a data network failure. This mechanism uses the PSTN, rather than redundant data facilities, to provide additional reliability.

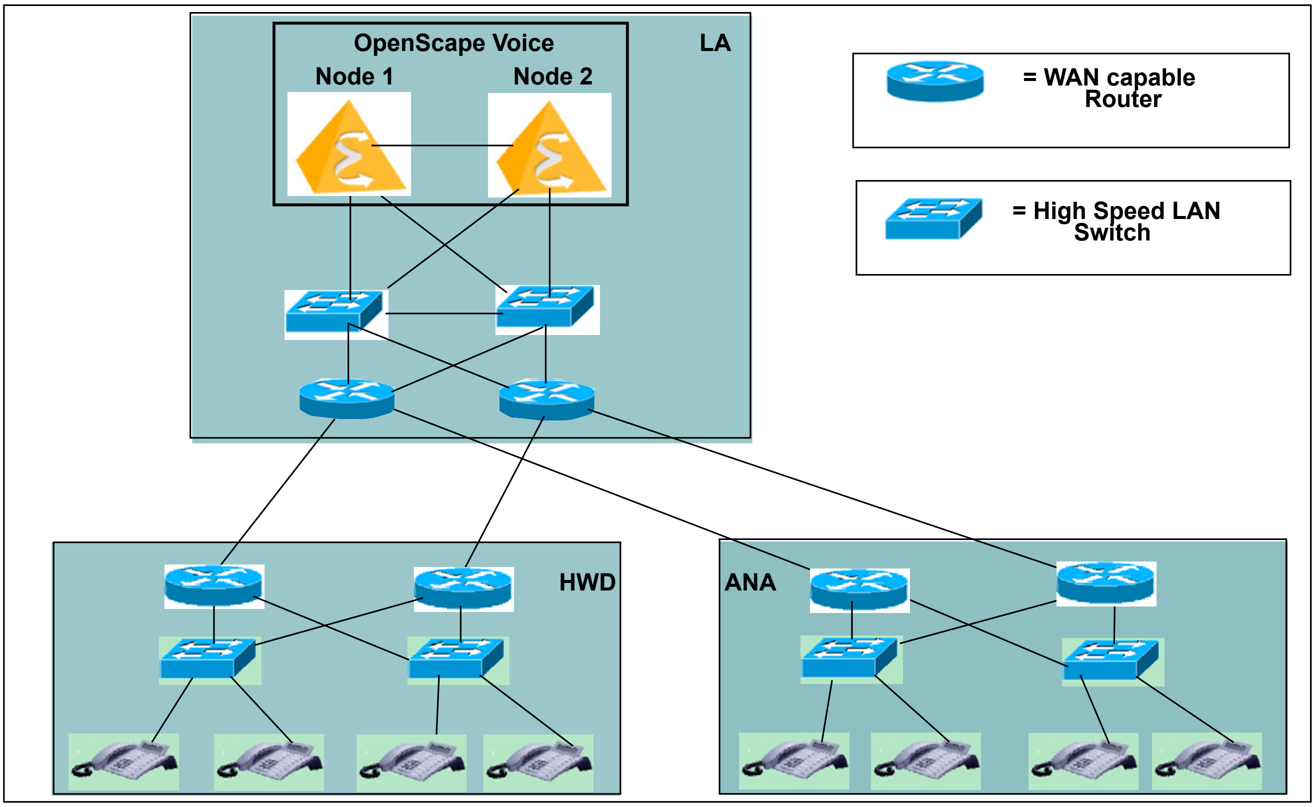


Figure 8 Local Data Network Topology

3.6.2.1 Outbound Gateways

The LoCal company requires gateways at the Hollywood and Anaheim for outgoing calls to the PSTN, as shown in Figure 7, "Network Requirements Diagram for the LoCal Corporation—First Iteration".

By assigning the phones in Anaheim a specific routing area (call it ANA), and the phones in Hollywood to a different routing area (call it HWD), the administrator can ensure that the local gateways will be the first-choice outbound routes to the PSTN for the respective locations.

Alternately, the administrator can assign specific prefix access codes to each gateway, so the caller can select the gateway to use for the outbound call.

With the implementation of gateway rerouting (see Section 10.2, “Gateway Rerouting”), if all trunks are busy at the local gateway, the outbound call can overflow (be redirected) to a gateway at the main office or at another location.

3.6.2.2 Redundant Gateways

Many common gateways, especially the smaller models, are simplex (nonredundant) devices, so hardware failure can result in a complete gateway outage. When such gateways are employed, the network plan must rely on multiple gateways to provide a measure of redundancy, in order to prevent a complete loss of PSTN connectivity in the event of a gateway hardware failure.

The basic single-box RG 8700 is a simplex gateway. A dual-box duplex configuration is also available.

3.6.2.3 Survivable Gateways

The survivable gateway (also known as *survivable media gateway ([SMG]*) is a gateway that has the additional ability to act as an alternate switching server, in the event that communication with the central Unify OpenScape Voice is lost. The RG 8700 gateway is an example of a gateway that has this capability.

In many cases, the presence of a survivable gateway will permit a remote location to operate without redundant WAN links to Unify OpenScape Voice, because the SMG will permit basic calling functions to continue in the event of a WAN failure.

The RG 8700 solution works as follows:

1. The SIP phones at the remote location are programmed with the IP addresses of both Unify OpenScape Voice and the emergency server (in this example, the RG 8700). The phones register with both servers but initially send all calls to the primary server (Unify OpenScape Voice).

2. The RG 8700 switches into survivability mode when it detects that communication to the central Unify OpenScape Voice has been lost. In this mode, it will provide basic telephone service. It becomes, effectively, a softswitch.

3. When the phone detects that it can no longer communicate with Unify OpenScape Voice, due to a WAN outage, the phone automatically uses the backup server (the RG 8700), for basic communication service. In this emergency operation mode, only basic service is provided. Services like keyset operation, hunt group, and pickup group operation are not provided during the outage period. Calls to phones at other locations must be made via the PSTN, in failure mode, because the WAN is down.

4. When the WAN link is restored, the phones will re-register with Unify OpenScape Voice, and normal service and features will be restored.

It is not clear that an SMG is a valuable feature for the LoCal corporation example, because the customer has chosen to route all inbound traffic through the central location (LA). A WAN outage with SMG backup would preserve internal and outbound calling at the isolated site, but all inbound traffic through LA to the isolated site would be blocked by the WAN outage.

3.7 Estimating Network Bandwidth

Several factors will have an influence on the amount of IP bandwidth required:

- Number of simultaneous calls
- Choice of audio codec used on the IP network
- Packetization interval
- Use of silence suppression (not usually recommended)

These will all be discussed in some detail later. The choice of voice encoding options available to the customer depends on the capabilities of the endpoints, clients, gateways, and media servers. G.711 is the most common codec choice; it provides the best voice quality and requires the most bandwidth.

Note: OpenStage telephones, as well as newer versions of the optiPoint 410 S/420 S, support the G.722 codec, which provides voice quality better than G.711 at approximately the same bandwidth. For network planning purposes, G.722 can be treated as G.711.

If G.711 voice encoding is used, each voice connection generally requires 75 Kbps to 95 Kbps of IP bandwidth in each direction on the IP (WAN) link, depending on the packetization interval. G.711 with packet loss concealment (PLC) provides the best voice quality, comparable to ISDN voice quality.

The G.729A/B encoding requires around 40 kbps of bandwidth in each direction, a considerable improvement, but with somewhat less voice quality. Unlike G.711, G.729A/B cannot support fax and low-speed modem data calls.

Because voice quality is critical in a business environment, the LoCal example assumes G.711 encoding, and uses 100 kbps as the bandwidth required in each direction for a voice call, a very conservative number that is easy to work with.

Treating the 100 kbps increment of bandwidth as a virtual VoIP trunk, you can use the Erlang tables in Appendix A, “Erlang B Carried Traffic Capacity Table” to get a rough idea of the bandwidth required for a remote site.

Chapter 4, “Calculating Network Traffic, Bandwidth Requirements, and Gateway Sizing” discusses bandwidth sizing in detail. As a quick calculation, consider the following. The Hollywood site has 1200 subscribers. Assume each subscriber is involved in (originates or answers) 5 calls in a typical busy hour (5 BHCA from the subscriber view). Assume 20% incoming traffic from the DID trunks in the LA office, and an average holding time of 3 minutes. That equates to 0.05 Erlangs of WAN usage per subscriber in the busy hour, or 60 Erlangs total.

The Erlang table predicts that LoCal will need approximately 90 trunks to handle this amount of inbound traffic, with a 0.01 blocking factor (0.01% of calls encounter congestion during the busy hour). In this example, a “trunk” is 100 kbps increment of bandwidth, so we need an available bandwidth of 9 Mbps (megabits per second) full duplex (in each direction) for the VoIP traffic in the busy hour.

In addition to this bandwidth, the engineer must add bandwidth for on-net calling between LA and Hollywood, and for data traffic, if voice and data share the same WAN IP facility.

The alternate design shown in Figure 9, "Alternate Topology Design" also provides full redundancy, but with one less external WAN link. It is interesting to note that these two topologies look identical to Unify OpenScape Voice and its VoIP call routing tables. The differences are only visible in the underlying data network routing tables. These tables may be manually configured and/or automatically compiled, and maintained using network discovery and routing protocols such as Intermediate System to Intermediate System (IS-IS) and Open Shortest Path First (OSPF).

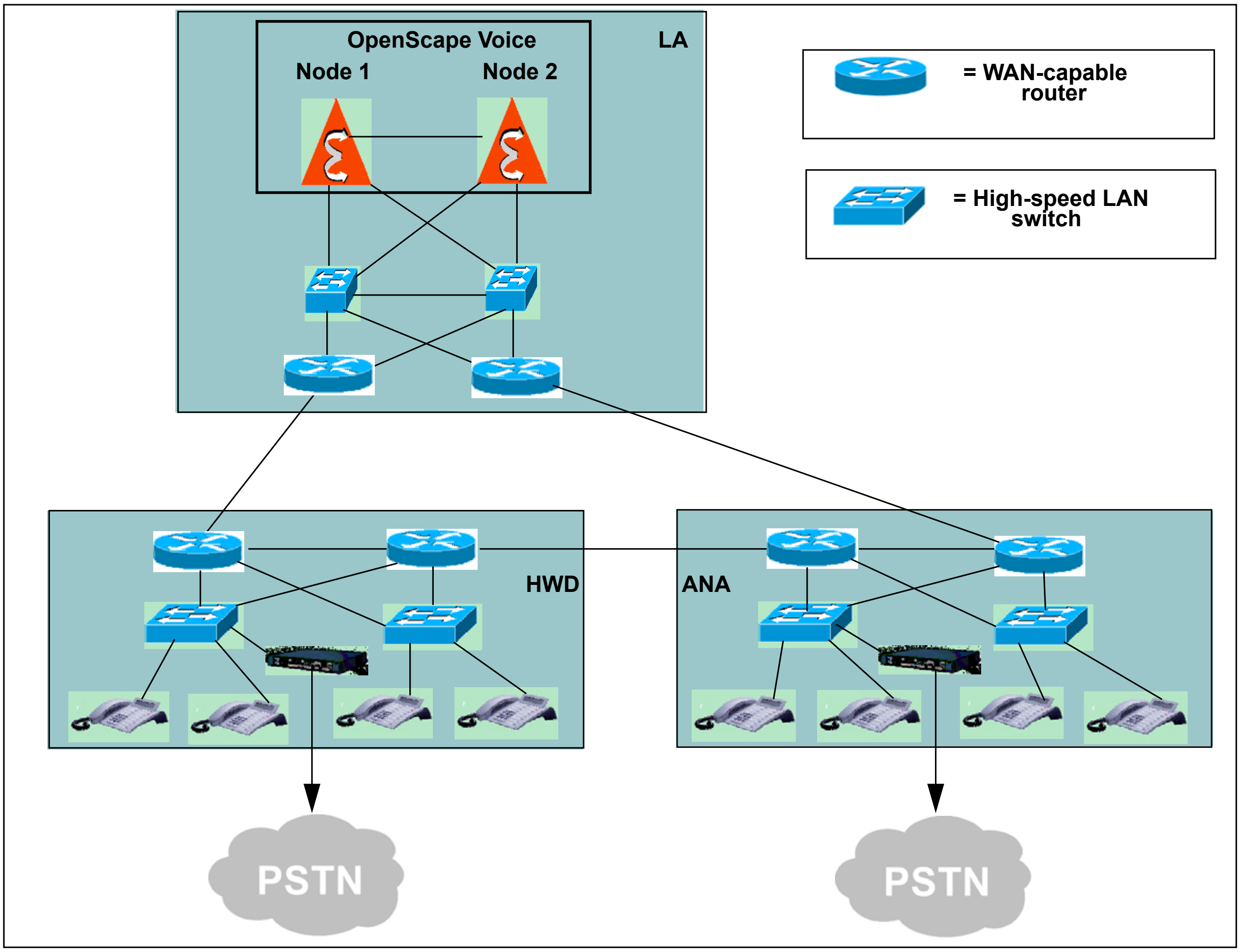


Figure 9 Alternate Topology Design

4 Calculating Network Traffic, Bandwidth Requirements, and Gateway Sizing

This chapter describes how to calculate network traffic and the number of trunks required to support that traffic. It also describes how to calculate the correct amount of bandwidth needed on the data network for the voice over IP traffic. All calculations are based on the example of the LoCal Corporation introduced in Section 4.5, “Calculating the Traffic for the LoCal Corporation”.

The information in this chapter is intended to explain the thought process. The results will only be as good as the data supplied to whatever tool is used.

4.1 Traffic Calculation Basics

This section discusses the following fundamentals of traffic calculations:

- Traffic measurement units
- Grade of service
- Erlang tables

4.1.1 Traffic Measurement Units

Voice traffic in the United States is usually specified in terms of hundred (or centum) call seconds (CCS) per line (CCS/line). CCS are units of 100 seconds of usage. A telephone with 6 CCS per hour is off-hook 600 seconds per hour. Another common unit of traffic is the Erlang. One Erlang is one hour of usage during an hour period. One Erlang is equal to 36 CCS per hour.

Note: In general, CCS is used to specify traffic on an individual telephone or within a private branch exchange (PBX), and Erlangs are used to correlate PBX traffic requirements with trunks.

Where voice traffic consists of incoming, outgoing, and on-net calls, the values for CCS are calculated as follows:

Incoming + Outgoing + Station + Station = Telephony CCS

Incoming + Outgoing + Station = Switched CCS

Telephony values represent traffic as seen from the subscriber viewpoint, whereas switched values represent traffic as it relates to PBX or softswitch capacity. For example, where there is one incoming call, one outgoing call, and one on-net call taking place, there are four telephones being used from the customer or endpoint. But for PBX configuration considerations, there are only three connection paths being used, one incoming path, one outgoing path, and one on-net path. Therefore, switched values for CCS are approximately 25 percent less than the values for telephony. The switched values represent the CCS/line capacity that has to be designed into the PBX to support the customer or endpoint level of usage.

Many years ago, AT&T did extensive research on enterprise customer telephone usage, which enabled them to construct traffic tables that provide usable values for light-, medium-, and heavy-traffic PBXs. A light-traffic PBX is defined as being in the 10th percentile, meaning that nine out of ten PBXs have heavier traffic. Similarly, a medium-traffic PBX is in the 50th percentile, and a heavy-traffic PBX is in the 90th percentile. Table 6 lists the CCS values for these three levels of traffic for both switched and telephony traffic.

Traffic Level	**CCS/Line**	
	Telephony	**Switched**
Light traffic	1.9	1.4
Medium traffic	3.8	2.9
Heavy traffic	7	5.3

Table 6 AT&T Traffic Values

In the enterprise environment, Unify has found that, in the absence of traffic data or estimates from the customer, a useful rule of thumb is an Erlang value of 0.15 erl. per digital user (= 5.4 CCS), with a call split of 1/3 incoming, 1/3 outgoing, and 1/3 internal. In a network configuration, a rule of thumb for call distribution is on-site (could be a building or campus) 50%, on-network 25%, and PSTN 25%. From the viewpoint of call load and call split, this is virtually identical to the AT&T model.

If nothing is known about a network’s traffic levels, it is generally safe to use the heavy-traffic value of 5.3 CCS/line for the lines not used for automatic call distribution (ACD). For example, the voice traffic at a single PBX with 2000 lines can be estimated using the heavy-traffic value as follows:

2000 lines x 5.3 CCS/line = 10,600 CCS

10,600 CCS/(36 CCS/Erlang) = 294.4 Erlangs

In most cases, non-ACD voice traffic is equally divided among incoming, outgoing, and on-net calls. This means that at any given moment, about one-third of the calls going through a PBX are incoming calls, one-third are outgoing calls, and one-third are on-net calls. Therefore, to obtain the Erlangs for each direction of traffic, divide the total Erlangs by 3 as follows:

294.4 Erlangs/3 = 98.1 Erlangs

Incoming, outgoing, and on-net traffic each needs 98.1 Erlangs.

4.1.2 Grade of Service

The grade of service specifies the proportion of calls that are not completed (blocked) because of unavailable resources. A grade of service of 0.01, for example, means that no more than one call in 100 attempts fails because of blocking. This equates to 1-percent blockage. The number of trunks (or amount of bandwidth) required to carry a given amount of traffic depends upon the grade of service that is required.

Grade of service is frequently discussed in terms of blockage levels. Blockage levels are always given in percentages. To convert a grade of service to a blockage level, multiply the value for the grade of service by 100.

4.1.3 Erlang Tables

Erlang tables provide a way to correlate the total traffic needs of a network with the number of trunks required. There are different types of Erlang tables in use throughout the world, including Erlang A, Erlang B, Erlang C, and Erlang D tables. Each of these tables uses different criteria to correlate the traffic needs with the number of trunks.

Erlang B tables assume no queuing for trunks and resources. The model on which the tables are based takes the simplistic approach that there is (a) no queuing, and (b) failed callers go away and do not reattempt for an extended period of time. These tables are most commonly used to estimate the number of trunks needed in a network.

Erlang C revises the Erlang B formula above to assume that (a) queueing is available in the network, and (b) people will wait (indefinitely) for an idle trunk or resource. As a result, the trunks can achieve a higher actual CCS utilization and handle more traffic. In reality, of course, a caller will not wait indefinitely. These tables were traditionally used to estimate the number of attendants and operators needed in the PSTN.

The Erlang B Carried Traffic Capacity Table is the most widely used in the United States. Appendix A, “Erlang B Carried Traffic Capacity Table” contains this table and instructions to use it.

4.2 Measuring Network Traffic

The fundamental task of network planning involves the following steps:

1. Breaking the enterprise down into logical groups of common interest and common location, then estimating who they call, how often they are called, who calls them and how often.
2. Converting these estimates into call rates and holding times (Erlangs) within each switch, between switches, and on the trunk groups which provide the interface to the public telephone network.
3. Using the traffic tables (Appendix A, “Erlang B Carried Traffic Capacity Table”) to convert the call rate and erlang values into the numbers of trunks and amount of bandwidth required.

Estimating the traffic patterns and load that will be generated by the enterprise is often very difficult. If the planner is replacing or upgrading an existing network, traffic reports from the switches in the existing network may be able to provide an accurate measurement of network traffic.

4.2.1 Measurements from Existing Networks

If the customer has an existing network with a OpenScape 4000 PBX, a Traffic Metering and Statistics application is available as a standard Unixware-based application on the OpenScape 4000 Administrative Data Processor. This application analyzes system performance and generates tabular data for evaluating and optimizing system resources. It can provide valuable data for evaluating and sizing the new network.

In addition, in existing networks containing OpenScape 4000, the OpenScape 4000 Manager system may be available. The System Management application includes a Collection Agent which allows the customer to collect a wide variety of traffic data, including trunk group and attendant usage data within the network. The HiPath Manager Report Generator allows the user to create customized reports.

OpenScape 4000 Manager also provides a Performance Management (PM) application, which allows you to run various reports on metered data that has been collected from CDR records, the Collecting Agent, and other sources.

OpenScape 4000 permits call detail recording for all calls (internal and external). This data, when processed by a downstream application, can provide valuable data on call flows between organizations and sites.

4.2.2 Tromboning

In networks where there will be a mix of equipment on traditional PBXs and on IP softswitches, tromboning may occur when calls are transferred or forwarded across the boundary between the TDM and IP networks.

In a pure VoIP network, tromboning does not occur. However, most networks will have some TDM equipment, in the form of legacy PBX equipment, or PSTN gateway equipment, so the effects of tromboning must be considered. The following examples reference the network shown in Figure 10:

- A call arrives from the PSTN through a OpenScape 4000 PBX which serves as a gateway into the IP network. The call is routed to subscriber A on Unify OpenScape Voice. The Unify OpenScape Voice subscriber then transfers the call to subscriber B on the OpenScape 4000. This will result in a trombone connection within the gateway. Two TDM channels on the gateway will be occupied by this call, for the duration of the call.

- A call arrives from the PSTN through a OpenScape 4000 PBX. The call is routed to subscriber A, but A does not answer and the call is forwarded on no answer to the voice mail system, which is also on the OpenScape 4000. This will result in a trombone connection within the gateway. Two TDM channels on the gateway will be occupied by this call, for the duration of the call. The dotted line in Figure 10 represents the resulting trombone connection.

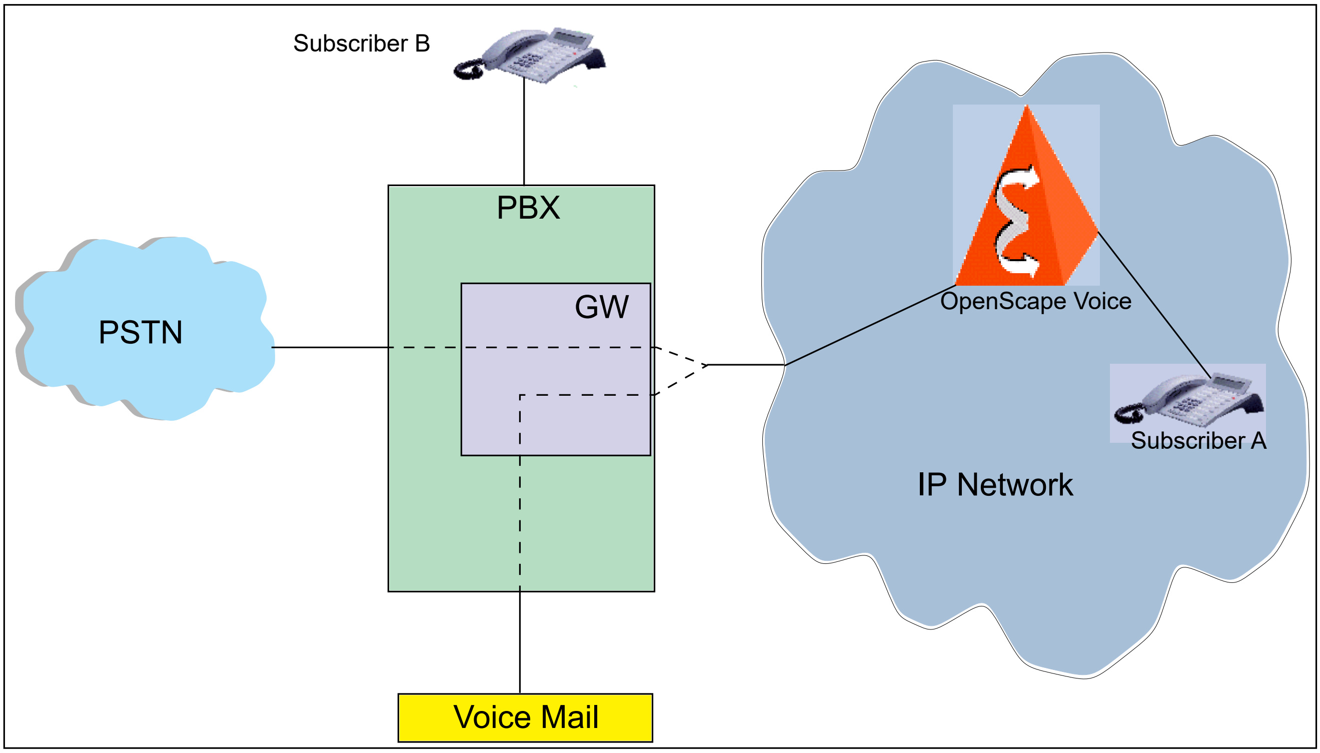


Figure 10 Tromboning

Trombone connections at the IP gateway resulting from these scenarios can be eliminated for gateways that support the SIP-Q protocol (QSIG over SIP), as long as proper provisioning is performed. These gateways include:

- RG 8700 (depending on QSIG implementation behind the gateway)
- HG 1500 – gateway card of the HiPath 3000
- HG 3500 – SIP-Q gateway card of the OpenScape 4000

4.3 Traffic in Simple Networks

Every Unify OpenScape Voice installation is, in effect, a network because there are at least three IP switching components present:

- Unify OpenScape Voice itself
- The media server used for tones, station-controlled conferences, and IVR functions
- One or more PSTN gateways

Even in a simple network, the network engineer must ensure that the proper number of gateway ports (trunks) and media server channels are provisioned, and that adequate IP LAN bandwidth is provided between the components and on the LAN switches where the phones will be connected.

A simple network is one in which all components are co-located within a single LAN, so that more than adequate bandwidth can easily be provided.

4.4 Traffic in Complex Networks

A network can be considered moderately complex if it involves any of the following:

- Multiple softswitches (and therefore tandem traffic)
- Multiple locations (and therefore WAN links that may need special consideration)
- Special business-critical call flows (for example 800-call answering groups)
- Special call reliability requirements

4.5 Calculating the Traffic for the LoCal Corporation

The fictitious LoCal Corporation was introduced in Section 3.6, “The LoCal Corporation—an Example”. We continue with this example.

4.5.1 Number of Planned Lines at All Sites

Referring to Table 5, "LoCal’s Desired Network Features", note the number of planned-for lines for each PBX and the total number of lines denoted in Table 7.

Subscribers			ACD Agents*		
Site	**Equipped**	**Planned**	**Equipped**	**Planned**	**CSTA**
Los Angeles	3500	7000	1000	1000	Yes
Hollywood	1200	2400	0	0	No
Anaheim	1500	3000	50	100	No
Total	6200	12400	1050	1100	

Table 7 Planned Lines at All Sites

* True ACD operation can be provided using the OpenScape Contact Center ACD system, which connects to Unify OpenScape Voice via SIP and CSTA.

4.5.2 Traffic Calculation Method

The traffic for the LoCal Corporation is calculated as follows:

1. All calculations are based on the equipped values for each site as noted in Table 7 above.
2. All calculations are based on the assumption of heavy traffic (5.3 CCS/line switched) as defined in Section 4.1.1, “Traffic Measurement Units”.
3. In the absence of traffic flow details from Section 4.2.1, “Measurements from Existing Networks”, all calculations are based on the assumption that traffic is equally distributed between incoming, outgoing, and on-net traffic. This means that incoming, outgoing, and on-net traffic each are 1.8 CCS/line. Recall that 1.8 CCS equals 180 seconds of usage.

4.5.3 Public Network Traffic

For the purposes of this section, outgoing traffic is defined as traffic that terminates in the public network. Outgoing trunks to the CO are supplied at each location in the LoCal corporate network. Therefore, the outgoing traffic matrix only has values in the CO column. Outgoing calls use the WAN links only when all outgoing CO trunks at the originating location are in use and alternate routing to another location is enabled.

Table 8 shows the outgoing traffic in each location, calculated as follows:

Outgoing traffic (Erlangs) = (Number of lines at the site *x* (1.8 CCS per line))/(36 CCS per line).

The same formula works for incoming (DID) traffic because of assumption number 3 in Section 4.5.2, “Traffic Calculation Method”.

Destination	**CO LA**	**CO ANA**	**CO HWD**	**MS LA**	**VM LA**	**LA**	**ANA**	**HWD**	**Total**
Source ↓									
DID LA						175	75	60	310
Los Angeles	175								175
Anaheim		75							75

Table 8 Public Network Traffic

Destination	CO LA	CO ANA	CO HWD	MS LA	VM LA	LA	ANA	HWD	Total
Hollywood			60					60	120
Total	175	75	60			175	75	120	680

Table 8 Public Network Traffic

4.5.4 On-Net Traffic

For the purposes of this section, on-net traffic is traffic that originates and terminates within the VoIP network. In the absence of solid traffic flow data, we assume that on-net traffic is uniformly distributed among the stations. Based on this assumption, tandem calling over the WAN between sites can be estimated as follows.

The WAN traffic between sites A and B can be computed as follows. Let NA, NB, and NTOTAL be the number of subscribers (lines) at A and B and in the total network, respectively. Then, using the factor of 36 CCS per Erlang, the traffic specifically between stations on A and B will be (assuming the uniform distribution of calls):

> Erlangs between A and B = (1.8 CCS per line) * NA * NB / (NTOTAL*36)

The on-net traffic between stations at LA and HWD will be:

> 1.8 * 3500 * 1200 / (6200 * 36) = 33.9 erlangs (about 17 in each direction)

Between ANA and HWD:

> 1.8 * 1200 * 1500 / (6200 * 36) = 14.5 erlangs (about 7.3 in each direction)

Between LA and ANA:

> 1.8 * 3500 * 1500 / (6200 * 36) = 42.3 erlangs (about 21.2 in each direction)

Inserting these new values in the traffic matrix, we now have the values shown in Table 9.

Destination	CO LA	CO ANA	CO HWD	MS LA	VM LA	LA	ANA	HWD	Total
Source ↓									
DID LA						175	75	60	310
Los Angeles	175					175	21.2	17	388.2
Anaheim		75				21.2	75	7.3	178.5
Hollywood			60			17	7.3	60	144.3
Total	175	75	60			388.2	178.5	144.3	1021

Table 9 Public Network and On-Net Traffic

Note: Table 9 only shows traffic based on communities of interest and does not reflect a particular network topology.

4.5.5 Voice Mail Traffic

There are two reasons for computing the voice mail (VM) traffic.

- To size the VM system itself
- To determine the network impact of the VM traffic

In our LoCal example, we have made very general assumptions regarding traffic flow, so it is doubtful whether the VM traffic impact is already included in the assumption of 5.3 CCS per line evenly distributed. For the purpose of this example, we assume that the VM traffic is in addition to these numbers.

In the network we have proposed for LoCal corporation, the VM system is centralized at the LA site. To compute the additional network traffic resulting from this decision, we need an estimate of the number of VM calls each user will receive and then retrieve, during a typical busy hour. If we assume that the user receives two VM messages and listens to them during a typical busy hour, we can compute a traffic number. In this computation, we assume that the VM calls are shorter than normal calls (45 seconds in duration). We also assume that half the messages come from internal parties and half from external trunk parties.

In order to do this computation, recall that forwarding in the VoIP network is forwarding with path optimization. This means that if a subscriber in ANA calls a subscriber in HWD, and is forwarded on busy (or no answer) to the VM system in LA, no bandwidth between LA and HWD will be used in this case.

So the VM traffic between ANA and LA will be the sum of two numbers:

(a) calls from ANA subscribers that are forwarded to VM in LA, to leave a message.

(b) calls from ANA subscribers to retrieve their VM messages.

Using the uniform distribution assumption from Section 4.5.2, “Traffic Calculation Method” item (a) can be computed as follows, assuming 2 messages left per hour, where NA is the number of subscribers at the site:

(a) Traffic due to subscribers leaving messages (a) = 1 * NA * (.45 CCS / 36)

(b) Traffic due to subscribers retrieving messages (b) = 2 * NA * (.45 CCS / 36)

So for Anaheim the numbers compute as follows

(a) = 1 * 1500 * (.45 / 36) = 18.75

(b) = 2 * 1500 * (.45 / 36) = 37.5 (for a total of 56.25 Erlangs VM traffic)

Repeating this computation for HWD the additional traffic is 45 Erlangs.

For the DID VM traffic, the formula will be (since we assumed above 1 incoming VM call per subscriber per hour):

1* (number of subscribers in NW) * (.45 /36) = 77.5 Erlang

The VM traffic from LA subscribers does not impact the network traffic, but it does impact the sizing of the VM system. Using formulas (a) and (b) above, we compute 131.25 Erlangs for internal VM traffic resulting from the subscribers in LA (Table 10).

Destination	CO LA	CO ANA	CO HWD	MS LA	VM LA	LA	ANA	HWD	Total
Source ↓									
DID LA					77.5	175	75	60	387.5
Los Angeles	175				131.25	175	21.2	17	519.45
Anaheim		75			56.25	21.2	75	7.3	234.75
Hollywood			60		45	17	7.3	60	189.3
Total	175	75	60		310	388.2	178.5	144.3	1331

Table 10 Voice Mail Traffic Sizing

Some additional points to be considered are:

- We have not taken into account the mechanism by which the VM system controls the LEDs on the SIP phones at the various locations. This is generally handled via signaling-only calls of very short duration – they have no impact significant on Erlang computation.
- Many voice mail systems today can be configured to deliver the voice mail message to the subscriber’s E-mail application—for example, Microsoft Outlook. In this case, the subscriber does not have to call the VM system to retrieve messages. If this mode of operation is universally adopted, it will reduce the VM traffic by 50%.

4.5.6 Media Server Traffic and Load

Every Unify OpenScape Voice installation includes a media server, which is used for tones, integrated voice response (IVR), and station-controlled conferences. The planner needs to consider the network impact of centralizing the media server at a specific location.

The basic call processing tones (ringback tone, busy tone, reorder tone) are generated within the SIP telephones themselves, so these tones do not require the media server. However, tones and announcements associated with feature activation and deactivation are provided by the media server. These tones will normally have negligible impact on the network, but not always.

The SIP phone is capable of originating and managing a three-party conference internally, without using the media server, so this also has negligible impact on the network. For conferences of more than three parties, however, the Unify OpenScape Voice station-controlled conference feature must be employed; a media server conferencing application is also an option. If a subscriber endpoint is configured to permit conferences larger than three parties, all conferences originated by the endpoint use the media server.

Some feature that may have a non-negligible impact on the network and the media server, depending on usage, are:

- Station-controlled conferencing
- CSTA make call
- ACD and hunt group queue music and announcements
- Dialed authorization codes for outgoing calls
- Centralized music on hold

- Other miscellaneous features

Each of these items is discussed below. It is important that they considered because their impacts may be non-intuitive for those familiar with traditional PBXs.

4.5.6.1 Station-Controlled Conferencing

The media server can be used to create station-controlled conference scenarios of 8 or more parties. These conferences are usually rare, but if they are used frequently, the impact may need to be calculated separately. Each leg of the conference is equivalent to a separate call, so an 8-party conference is equivalent to 8 individual calls to or from the media server.

4.5.6.2 CSTA Make Call

The CSTA Make Call, which is used by click-to-dial functions provided by such applications as OpenScape UC Application, uses the media server to provide ringback tone in many cases. This implies an average 18 seconds of media server usage per call originated via CSTA.

If the call is an outbound call to a TDM gateway that provides early media (early cut-through), the media server is not engaged. Likewise, if a SIP phone provides early media (ringback) when called, as some do, the media server will not be engaged. But most SIP phones do not provide early media, so most internal calls originated via CSTA require the media server for ringback tone.

If ringback tone from the media server is required, it is engaged even if the source and destination are in the same node, creating a non-intuitive network impact. For example, if subscriber A in Anaheim calls subscriber B in Anaheim, using CSTA, the ringback tone to A will come from the media server in LA, creating a short interval of network traffic.

4.5.6.3 ACD and Hunt Group Queue Music and Announcements

If the network has an ACD-like answering group, with a music or an announcement sequence, a substantial number of calls may occupy channels on the media server. Again, this may occur even if the media server is in a remote location.

Assume, for example, that each of the 1050 ACD agents at LoCal processes 20 calls per hour, where on average each call receives 30 seconds of music and announcements prior to answer. This translates to 630,000 seconds of usage for announcements or 175 Erlangs of traffic to the media server.

Note that the agents can be at any of the three sites. Because the incoming DID trunks and media server are all centralized, this media server usage has no impact on the links to the branch site.

4.5.6.4 Authorization Codes for Outgoing Calls

If the system is configured to prompt the user for an authorization code prior to permitting an outgoing call on certain routes or trunk groups, this invokes the IVR functionality of media server for prompting and digit collection, even if the media server is at a remote location. This can add 12 to 18 seconds of media server usage to each affected call.

For example, if an outbound call from a subscriber at Anaheim to a gateway at Anaheim requires a post-dial authorization code, a link to the media server in LA will be established for the IVR functionality. If this is a common occurrence, the network and media server impact may need to be estimated.

4.5.6.5 Centralized Music on Hold

The SIP phones are capable of providing an internally generated music clip (a *jingle*) when a call is placed on hold by the far end. However, the customer may also choose to have one or more business-friendly centralized music sources, to provide a more pleasing customer experience. This centralized music function can create a non-trivial load on the media server.

a) Assume that 20% of all calls receive music on hold at some point, for an average duration of 30 seconds. Assuming a switched call rate of 3 BHCA per line, the impact of music on hold is = 0.2 * 3 * (number of subscribers) * 30 / 3600. For the LoCal network, this would compute to a non-significant number:

   .2 * 3 * 6200 *.3 / 36 = 31 Erlangs (load on the media server)

b) The value above estimates the Media Server impact of music on hold, but it does not quantify the network impact. The impact is difficult to determine in general terms because it depends on traffic flow, network topology, and location of the media server.

As a first order computation we estimate the network effect of music on hold for internal calls at remote locations. Consider a station-to-station or station-to-CO-trunk call in a remote location (say Anaheim). Placing this call on hold will cause a network load as the held party is connected to the media server in LA. Based on the selected traffic model, the network impact would be a = (% of calls held) * (internal calls per subscriber) * (number of subscribers) * (seconds per hold) / 3600.

c) Running these calculations for the LoCal remote sites, we get the following:

ANA = 0.2 * 1 * 1500 * 30 / 3600 = 2.5 Erlangs

HWD = 0.2 * 1 * 1200 * 30 / 3600 = 2.0 Erlangs

4.5.6.6 Other Features

Miscellaneous features – for all the other features that might occasionally be used and require the media server, we assume in the busy hour 30 seconds of media server usage per subscriber. Other = 6200 * 30 / 3600 = 51.66 Erlangs

4.5.6.7 Usage Summary

Media server usage is summarized in Table 11, from the example above.

Media Server Usage	Affected Calls	Calls per Subscriber	Subscribers	Seconds per Call	Total Usage Seconds	Erlangs
Conference						Negligible
Make call	10%	2	6200	18	22320	6
ACD announcements	100%	20	1050	30	630000	175
Authorization codes						Not Used
Music on hold	20%	3	6200	30	111600	31
Other					186000	52
Total						264

Table 11 Media Server Usage

The traffic matrix in Table 12 estimates the WAN impact of the media server traffic by allocating the total Erlang load for each media server feature based on the number of subscribers at each site. The exception is ACD where all the announcement traffic is at LA, where the DID trunks are exist.

Erlangs	ANA	HWD	LA	Total
Make call	1.45	1.16	3.39	6
ACD announcements	0	0	175	175
Music on hold	7.5	6.00	17.50	31
Other	12.58	10.06	29.36	52
Total	21.53	17.22	225.25	264

Table 12 WAN impact of the Media Server Traffic Matrix

In Table 13, the network load caused by the media server features has been added.

Destinatio n	CO LA	CO ANA	CO HWD	MS LA	VM LA	LA	ANA	HWD	Total
Source ↓									
DID LA					77.5	175	75	60	387.5
Los Angeles	175			225	131.25	175	21.2	17	744.45
Anaheim		75		21.5	56.25	21.2	75	7.3	256.25
Hollywood			60	17.2	45	17	7.3	60	206.5
Total	175	75	60	263.7	310	388.2	178.5	144.3	1594.7

Table 13 Network Load Due to Media Server Usage

4.5.7 ACD (Hunt Group) Traffic Impact

We have ignored the impact of the ACD traffic on the network so far. The 1050 answering agents are part of the 6200 total subscribers. We assume, because it is not specified, that they process a very heavy traffic load:

- 20 calls per station in the busy hour
- Average holding time of 90 seconds
- In addition to the normal non-ACD related traffic load
- All hunt group traffic is external, arriving via DID trunks

This results in 1800 seconds of usage per agent, or 0.5 Erlang. This results in 1050 * 0.5 = 525 Erlangs of traffic on the incoming DID trunk group. Of that number, 500 Erlangs will terminate in LA, where 1000 agents reside.

The hunt group also has 50 agents that are located in Anaheim. The traffic on the Anaheim link will be increased by 50 * 20* 90 / 3600 = 25 Erlangs of traffic. The ACD traffic numbers have been added in the traffic matrix below.

4.5.8 Total Resource Usage

The ACD numbers have been added into the traffic matrix of Table 14, with some of the results totaled. All units are in Erlangs.

Destination →	CO LA	CO ANA	CO HWD	MS LA	VM LA	LA	ANA	HWD	TOTAL
Source									
DID LA					77.5	675	100	60	912.5
Los Angeles	175			225	131.25	x	21.2	17	394.45
Anaheim		75		21.5	56.25	21.2	x	7.3	106.25
Hollywood			60	17.2	45	17	7.3	x	86.5
Total	175	75	60	263.7	310	713.2	128.5	84.3	1499.7

Table 14 Total Resource Usage

The internal traffic numbers within each site have been removed to make the totals more useful for this step.

From the number in traffic matrix, a topological diagram can be drawn as shown in Figure 11, illustrating the traffic flow more clearly.

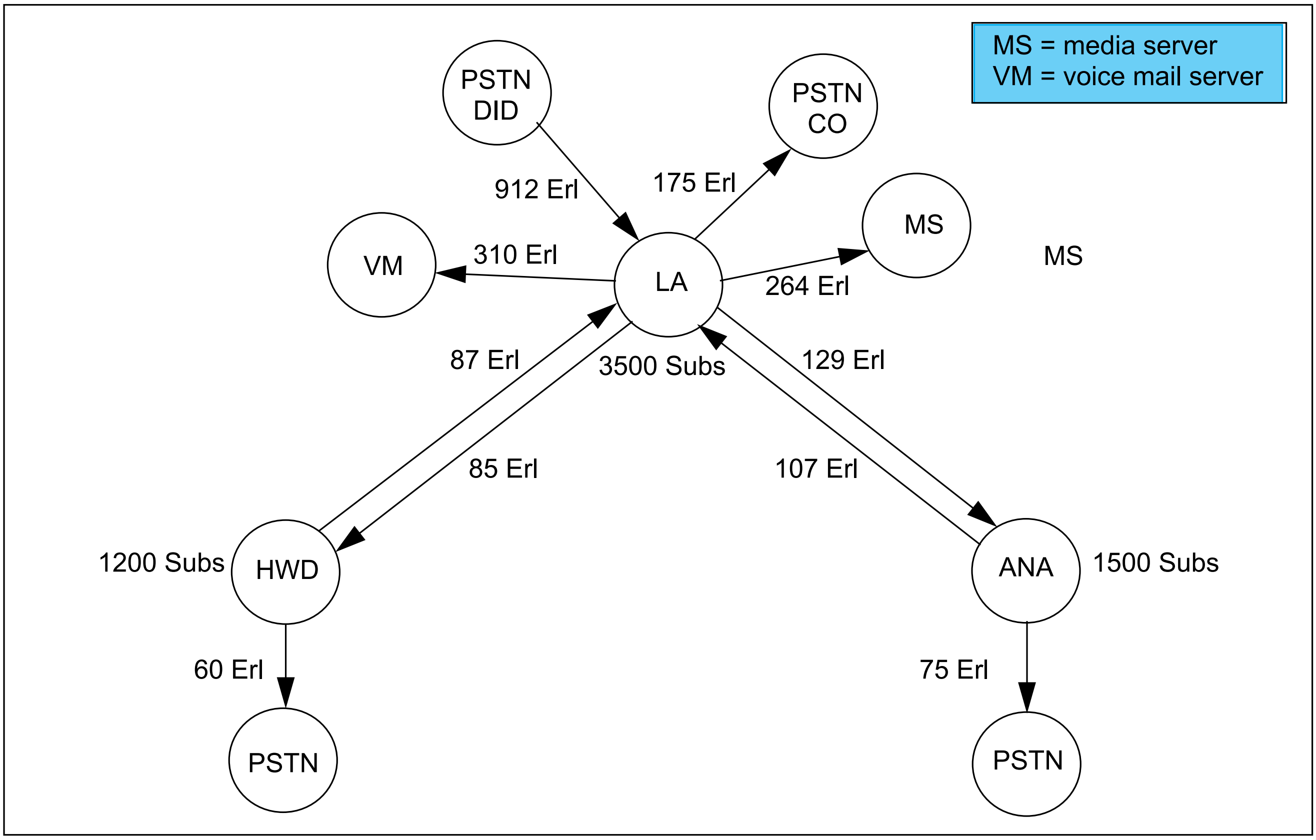


Figure 11 *Topological Diagram of the Traffic Matrix*

4.5.9 Trunks, Channels, and Bandwidth

From the traffic summary above, the planner can now start estimating the critical resource requirements, using the Erlang table B of Appendix A, “Erlang B Carried Traffic Capacity Table”. The planner selects the blocking factor on the various resources.

Trunk Groups	ERL	P (B)	Trunks
DID LA	912	0.01	1007
CO LA	175	0.05	214
CO HWD	60	0.05	85
CO ANA	75	0.05	102
Total			1408

Table 15 *Traffic Summary*

The media server capacity is measured in maximum number of IP channels, which are logically equivalent to trunks. An example of this is shown in Table 16. Because a missing tone or announcement will typically cause an incorrectly processed call, a low blocking factor is advisable. Assuming a SIP-based voice mail system, the same concept applies: Logical channels instead of trunks.

Channels	ERL	P (B)	Channels
Media Server	264	0.01	310
Voice Mail	310	0.01	360

Table 16 Media Server Channel Capacity

Bandwidth on the WAN comes next, and the goal is to estimate the bandwidth required for the voice traffic (Table 17). As described earlier, this calculation depends on the primary codec chosen for the network. Assuming G.711 is the codec of choice and rounding up, you can view each logical channel as 100 KBps of bandwidth (full duplex).

WAN Links	ERL	P (B)	Channels	Kbps / Channel	Bandwidth
LA – ANA	236	.01	289	100	30 Mbps
LA – HWD	172	.01	218	100	22 Mbps

Table 17 WAN Bandwidth

In almost all cases, the voice packets will share the WAN links with data activity of equal or greater quantity, so the voice bandwidth requirement is just one factor in sizing the WAN links.

4.5.10 Signaling Bandwidth

Signaling bandwidth required to operate a SIP telephone is less than 1 Kbps (full duplex), even under heavy load and when keyset operation and an associated OpenScape UC Application are included. Because the bandwidth to operate 1000 phones at a remote location is less than 1 Mbps, bandwidth is rounded up in Table 17. Therefore, the bandwidth required for signaling can be ignored.

4.5.11 Performance Considerations

When operating in a tandem switching environment, Unify OpenScape Voice’s SIP call handling rate varies depending on the server platform, as follows:

- **IBM x3550 M3**: 280 calls per second
- **IBM x3550 M4**: 280 calls per second

- **IBM x3250:** Five calls per second
- **FSC RX 330 S1:** 240 calls per second
- **FSC RX 200 S6:** 280 calls per second
- **FSC RX 200 S7:** 280 calls per second

However, when keyset operation, CSTA, and other features are configured, these numbers can be reduced to a value as low as 40 calls per second.

For this reason, an Unify OpenScape Voice Performance Planning Tool is available which allows the planner to supply the selected configuration, call rate, and feature usage variables, to determine if the actual capacity of a single system is sufficient for the configuration.

The BHCA requirement for the LoCal network is approximately 3 BHCA per normal line and 20 BCHA per ACD/Hunt Group phone:

BHCA (LoCal) = 3 *6200 + 20*1050 = 39,600 busy hour calls

This is within the Unify OpenScape Voice performance limits even when features are taken into account. When the network expands to its planned-for size, the BHCA rate will increase:

BHCA (LoCal) = 3*12400 + 20*1100 = 59,200 busy hour calls

This is well within the capacity of a single Unify OpenScape Voice system, even with a very aggressive feature configuration.

4.5.12 Selecting the Equipment

The final step is usually selecting associated equipment – gateways, media server, and voice mail server. Chapter 6, “Network Features and Applications” provides a list of product options and some sizing information that may assist in the selection process.

In the LoCal example, if Unify OpenScape Voice is replacing existing OpenScape 4000 and/or HiPath 3000s, the possibility of leaving these in place and using them as gateways may exist. If this is a green-field installation, new gateways are obviously required, and the Unify RG 87xx gateway family is the preferred choice.

5 OpenScape Branch Solution

This chapter describes OpenScape Branch, a SIP-based branch office solution that provides superior survivability operation during the loss or degradation of service between the remote branch and headquarters Unify OpenScape Voice.

5.1 Solution Overview

The OpenScape Branch solution, available for Unify OpenScape Voice provides the following functionality:

- Feature-rich set of survivability capabilities at remote branch locations
- PSTN gateway support
- TLS/TCP/UDP connections (default setting is TCP for new installations)
- A local OpenScape Media Server for tones, announcements, and conferencing, which minimizes the WAN bandwidth to the host Unify OpenScape Voice when in normal mode; it also permits the branch to have access to media server capabilities when it is operating in survivability mode.
- Full integration in Unify OpenScape Voice management. In addition, a local GUI, which can be used for most tasks, continues to be available when the headquarters Unify OpenScape Voice Assistant is not. Refer also to Section 8.2, “OpenScape Branch Assistant”.
- SBC functionality.
- Security functions, such as firewall and virtual private network (VPN).
- Additional billing/CDR capabilities in survivability mode.
- Improved serviceability for installation, upgrades, and configuration.

The OpenScape Branch is supported on various platforms and can be divided into two groups:

1. Without Integrated Gateway and Analog Adapters

   - **OpenScape Branch 50/250** – supported by Advantech SYS-2USM02-6M01E server without any Gateway and Analog Adapter interfaces. This server supports up to 250 registered lines.

   - **OpenScape Branch 1000** – (IBM x3250 M3 servers) for up to 1,000 registered lines.

     Note: OpenScape Branch 1000 on the IBM x 3250 M2 platform is no longer offered. However, support for installed servers shall continue.

   - **OpenScape Branch 6000** – (IBM x3550 M4 or Fujitsu Primergy RX200 S7 servers) for up to 6000 registered lines.

     Note: OpenScape Branch 6000 on the IBM x 3550 M2 or the Fujitsu RX330 S1 platforms are no longer offered. However, support for installed servers shall continue.

2. With Integrated Gateway and Analog Adapters

   - **OpenScape Branch 50i** – (Advantech SYS-2USM02-6M01E server) for up to 80 registered lines with Integrated Gateway and Analog Adapter interfaces and currently available in four flavors:

     – OpenScape Branch 50i **A84** (Analog - 8 FXO ports + 4 FXS ports)

     – OpenScape Branch 50i **D44** (Digital - 4 BRI ports + 4 FXS ports)

     – OpenScape Branch 50i **DP14E** (Digital - 1 PRI E1 port + 4 FXS ports)

     – OpenScape Branch 50i **DP14T** (Digital -1 PRI T1 port + 4 FXS ports)

   - **OpenScape Branch 50i** – (Advantech SYS-2USM01-6M01E server) for up to 24 or 48 registered lines with Integrated Analog Adapter interfaces currently available in two flavors:

     – OpenScape Branch 50i **A024** (Analog - 0 FXO ports + 24 FXS ports)

  - OpenScape Branch 50i **A048** (Analog - 0 FXO ports + 48 FXS ports)

- **OpenScape Branch 500i** – (Advantech SYS-2USM03-6M01E server) for up to 500 registered lines with Integrated Gateway available in two flavors:
  - OpenScape Branch 500i **DP4** (Digital - 4 PRI E1/T1 ports)
  - OpenScape Branch 500i **DP8** (Digital - 8 PRI E1/T1 ports)

5.2 Configuration Options

The OpenScape Branch solution supports two main deployment scenarios:

- Proxy deployment
- SBC deployment

Figure 12 shows the OpenScape Branch proxy deployment scenario.

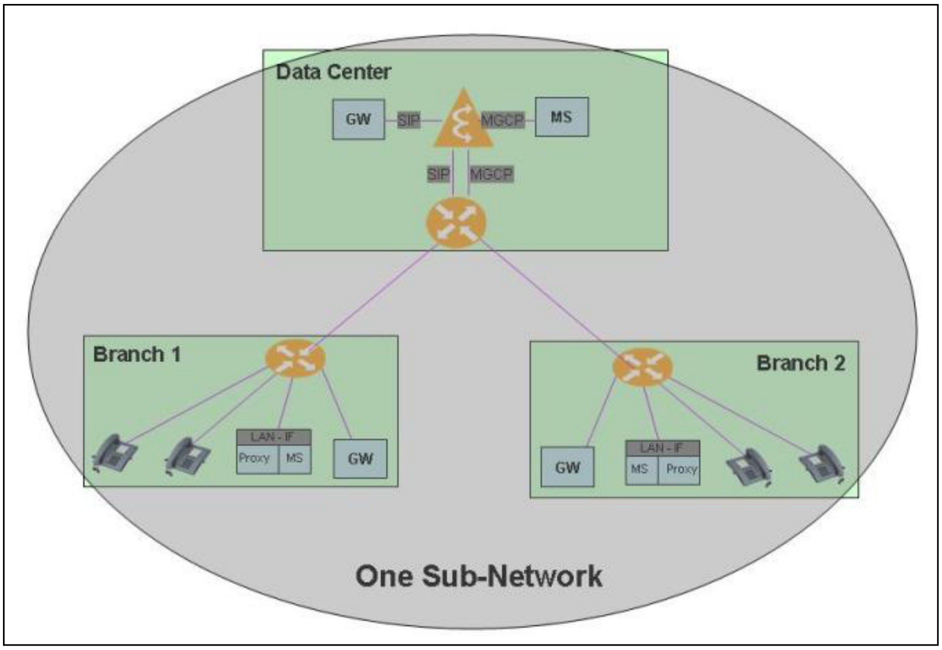


Figure 12 OpenScape Branch Proxy Deployment Scenario

Figure 13, "OpenScape Branch SBC Deployment Scenario" shows the OpenScape Branch SBC deployment scenario.

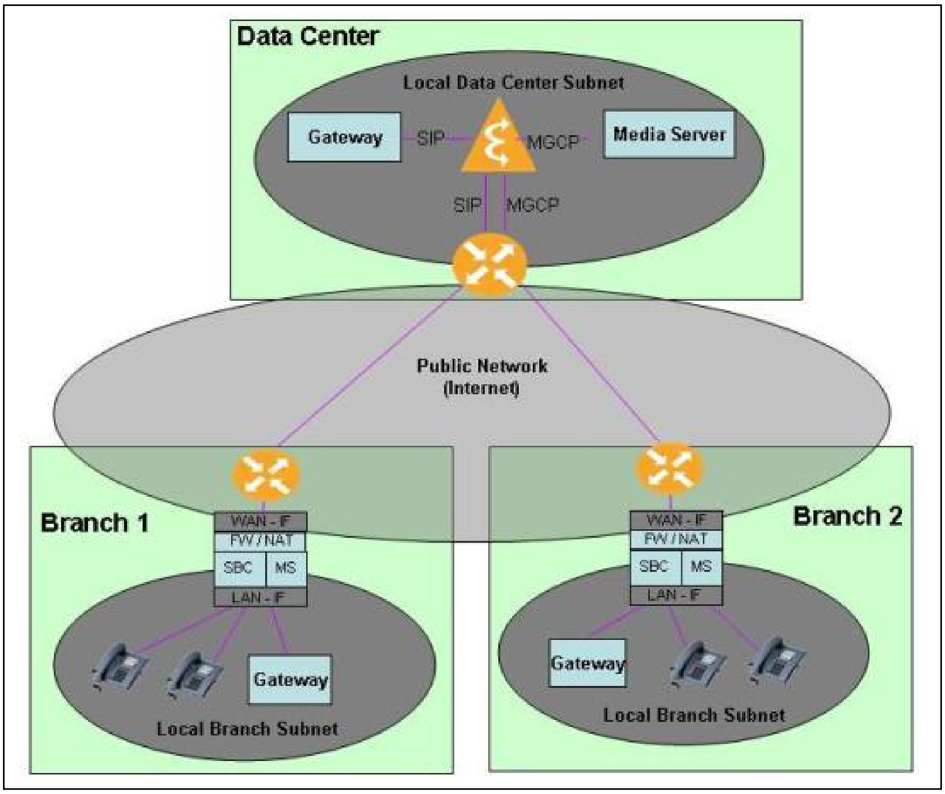


Figure 13 OpenScape Branch SBC Deployment Scenario

5.3 Normal Operation—Headquarters to Branch

In normal mode, the full functionality of Unify OpenScape Voice is available to all the phones in the branch.

5.4 Survivability Mode—Headquarters to Branch

If the WAN or Unify OpenScape Voice is not operable, OpenScape Branch enters the survivability mode of operation as shown in Figure 14, "OpenScape Branch Survivability Mode". In this figure, Subscriber B receives incoming calls from the PSTN, including calls from Subscriber A received via subscriber rerouting.

During survivability mode, phones within the branch office will be able to call each other, make outgoing calls to the PSTN, and receive incoming calls from the PSTN. OpenScape Branch generates CDRs for calls that were initiated or terminated during survivability mode.

Unify OpenScape Voice synchronizes the digest authentication credentials towards the OpenScape Branch, in order for the branch to be able to challenge registering subscribers during survivable mode. This prevents security intrusions in these branches during survivability mode, since nobody can register a phone without the proper credentials and make phone calls to external, possibly expensive destinations.

OpenScape Branch also supports several features on the B-side of the call—for example, forking the calls to multiple registered contacts, calling a hunt group, transporting a LIN to the PSAP when dialing 911, and forwarding calls.

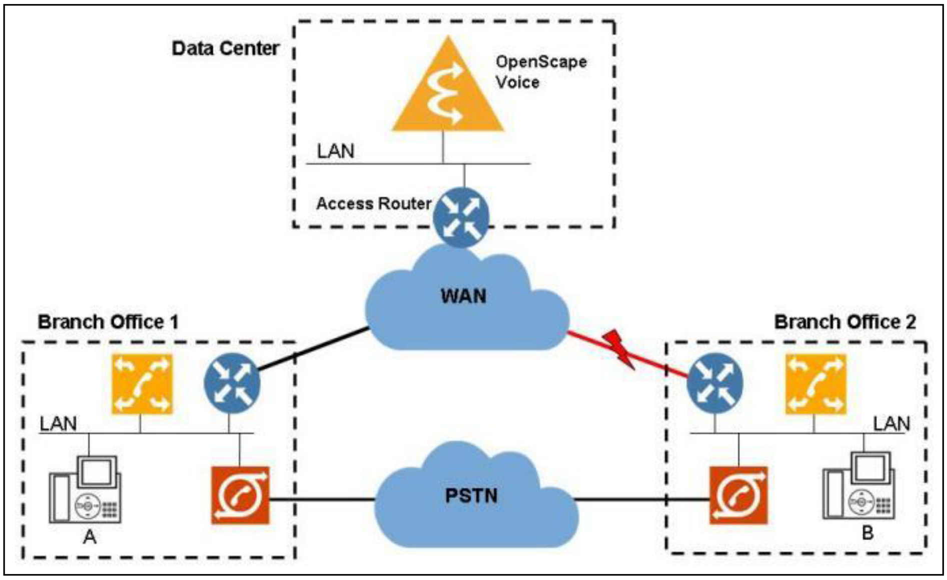


Figure 14 OpenScape Branch Survivability Mode

6 Network Features and Applications

This section describes servers and applications that may optionally be equipped within an Unify OpenScape Voice network.

6.1 Media Servers

Every Unify OpenScape Voice installation requires at least one media server for tones, announcements, and optionally conferencing.

For an Unify OpenScape Voice integrated installation:

- An onboard 100-channel media server is already provided as part of Unify OpenScape Voice itself.
- If the integrated Unify OpenScape Voice system is a redundant system (two nodes), the onboard media server is also redundant.
- If the OpenScape UC Application is in use on an Unify OpenScape Voice integrated simplex system, it will, by default, include an additional 100 media server channels dedicated to the OpenScape UC Application.
- The planner must estimate total media server channel usage for all functions, to determine if the user community requirement exceeds the capacity of the on-board (integrated) OpenScape Media Server. If it does, an additional external media server (or servers) will be required.

In the higher-capacity Unify OpenScape Voice standard duplex system configuration, the media server cannot be onboard Unify OpenScape Voice, so an external media server is required. The planner must then determine the size, number, and location(s) of the external media servers. The OpenScape UC Application will normally have its own dedicated media server, separate from the one used by Unify OpenScape Voice for general telephony and conference functions.

Section 4.5.6, “Media Server Traffic and Load” gives a fairly detailed description of how media server channel usage can be estimated. At a high level, the following aspects need to be considered.

- Media server channel capacities are normally quoted assuming that G.711 voice coding is used in the network. If the network will be using a compressed codec, such as G.729, the capacity of any given media server will be reduced by a significant factor, and this must also be considered.

- Media server usage per user varies greatly depending on the customer feature options and usage patterns. In heavy conference use environments, the need for media server channels may reach or exceed one channel for every 10 subscribers.

If the network is geographically distributed, the planner can consider scattering several smaller media servers at the various sites, rather than placing one media server at the headquarters. The following are the options to do so:

- **By branch:** Up to eight media servers, each of which provides support of tones, announcements, and conferencing, can provide all necessary support to a particular branch. Doing so minimizes the WAN bandwidth to the host Unify OpenScape Voice when in normal mode; it also permits the branch to have access to media server capabilities when it is operating in survivability mode.
- **By routing area**: If a media server is not associated with a specific branch as described above, the subscriber's routing area can be used to determine which media server he or she is directed to when one is required.
- **By function**: If a media server is not associated with a specific branch as described above, different treatments (tones, announcements, feature functions) can be assigned to specific media servers. For example, one media server can be dedicated to (used exclusively for) music on hold.

Up to 3000 media servers can be assigned.

Media servers can be configured in a primary/alternate configuration for reliability. If the primary media server is not reachable, the switch will route the user to the alternate media server.

If the primary (centralized) media server fails, Unify OpenScape Voice routes the user to a backup media server to ensure that the required media server functionality is still available to users.

6.1.1 OpenScape Media Server

The OpenScape Media Server is Unify’ software-only media server offering. It is included and runs on the Unify OpenScape Voice server in the integrated deployment model. For the Unify OpenScape Voice standard configuration, it must be installed on a separate standard Linux server, as described below.

Note: The OpenScape Branch solution also uses the OpenScape Media Server, but it is scaled differently depending on whether the branch is small or large.

Unify provides minimum hardware requirements for low- and high-end performance levels and cost points. The enterprise is responsible to provide the hardware that is capable of delivering the required performance level; Unify provides the OpenScape Media Server on the Unified Communication (UC) DVD that is provided with all Unify OpenScape Voice and OpenScape UC Application orders.

Table 18 lists the hardware specifications for the external OpenScape Media Server.

Performance Level	Usage Range	Specifications (see note)
Low end	Up to 7,500 users	• One IA32/EM64T (x86-64) • One dual-core CPU 2.4 GHz • 4 GB RAM • Two 160GB SATA hard disks in RAID 1 configuration • DVD-ROM drive • Ethernet interfaces as required
High end	Up to 25,000 users	• Two quad-core CPUs (Intel Xeon 5345 CPU/ QuadCore/2.33Ghz or higher, or AMD Opteron 2350 2Ghz Quad Core–Barcelona) • 8 GB RAM • Two 146GB SAS hard disks in RAID 1 configuration • DVD-ROM drive • Ethernet interfaces as required
Note: 1. All servers must be certified for SUSE SLES 11.		

Table 18 External OpenScape Media Server Hardware Specifications

Table 19 lists the capacities associated with the external OpenScape Media Server by performance level.

Characteristic	Low-End Capacity	High-End Capacity
Estimated users	7500	25,000
G.711 ports (see note)	150	500
G.729 ports (see note)	52	175
Busy hour call attempts	6000	20,000
Note: If SRTP is used, port capacity decreases by approximately 15%.		

Table 19 External OpenScape Media Server—Capacities by Performance Level

6.2 Messaging Servers

6.2.1 OpenScape Xpressions

For larger installations, OpenScape Xpressions is the preferred voice mail system for an Unify OpenScape Voice network. OpenScape Xpressions offers a direct LAN interface for voice mail recording and retrieval, as well as message waiting LED status updates to the phones. The interface utilizes the SIP signaling protocol and is compatible with Unify OpenScape Voice.

OpenScape Xpressions is a Windows-based server application running on an FSC TX 150 S5 server platform. A single server can support 4000 voice mail boxes (4000 subscribers) or 2000 unified messaging mailboxes (UMS includes voice, fax, e-mail replication, and SMS delivery). Refer also to Section 6.7.3, “Xpressions Conferencing” for information about Xpressions conferencing capabilities.

Up to eight OpenScape Xpressions servers can be configured in a cluster to support up to 20,000 subscribers with voice mail.

OpenScape Xpressions supports G.711 (a-law and u-law) and G.729 codecs.

System capacity is summarized in Table 20.

Codec Connections	Single Server	Cluster / Distributed System
Simultaneous G.711 connections	60	300
Simultaneous G.729 connections	40	280

Table 20 OpenScape Xpressions System Capacities

6.2.1.1 Multiple OpenScape Xpressions Systems

If a customer wishes to deploy multiple OpenScape Xpressions system in a network and have it supported by a single Unify OpenScape Voice system, it is possible to do so.

6.2.1.2 OpenScape Xpressions Connected to HiPath 3000 or OpenScape 4000

If the network contains HiPath 3000 or OpenScape 4000 switches that are serving as gateways to the PSTN, OpenScape Xpressions may be to used as the voice mail system for the VoIP subscribers connected to Unify OpenScape Voice.

Using the HG 3500 gateway card as interface between Unify OpenScape Voice and OpenScape 4000:

- The OpenScape Xpressions system on the OpenScape 4000 can control message waiting LEDs on the Unify OpenScape Voice SIP phones.
- Calls forwarded to OpenScape Xpressions from Unify OpenScape Voice will be delivered to the proper mailbox belonging to the Unify OpenScape Voice subscriber.

6.2.2 Other Messaging Server Options

Unify OpenScape Voice customers have the following additional voice mail options:

- For smaller installations, the OpenScape UC Voice Portal can provide basic voice mail service, delivering messages into the subscribers e-mail box as part of the UC (unified communication) function.
- Unify OpenScape Voice provides a compatible SIP interface to the Microsoft Exchange UC messaging system.

6.3 HiPath License Management (HLM)

The Unify OpenScape Voice installation allows the following types of licenses to be purchased:

- **Dynamic user licenses:** Each phone or soft client that registers on the system consumes one dynamic license, then returns that license to the free pool when it deregisters or powers off. Previously Unify OpenScape Voice was licensed based on the number of subscriber directory numbers (DNs) equipped in the database. Now the license quantity is not based on the number of DNs, but on the number of registered phones and clients.
  - If many subscribers will have two phones, and both will be connected to Unify OpenScape Voice simultaneously, the number of dynamic licenses required might be substantially higher than the number of actual subscribers. However, a subscriber can also register multiple phones with the same DN (this is called multiple contacts) and in that case only one dynamic license is required.
  - If, on the other hand, many subscribers only use SIP soft clients, running on PCs which are powered down or disconnected from the corporate IP network much of the time, then the number of dynamic licenses required might actually be less than the total number of subscribers.
  - Keyset phantom lines (DNs that only appear as secondary lines on keysets) do not require licenses.
- **Trunking session licenses:** These licenses permit calls between non-subscriber endpoints. These are what historically are called *tandem calls*. For example, the following types of calls require a trunking session license:
  - A call routed from one SIP gateway to another SIP gateway
  - An incoming public network call routed directly to OpenScape Xpressions or the OpenScape UC Application Voice Mail
  - An incoming PSTN call routed directly through Unify OpenScape Voice to a different Unify OpenScape Voice system
- **Client access licenses**: These licenses control the maximum users that can be provisioned with both the CSTA service and one number service inbound/outbound (ONS-I/O). Sometimes used in conjunction with trunking session licenses, they provide the ability to charge for the B2BUA capabilities provided by the Unify OpenScape Voice/OpenScape bundled packages—for example, the OpenScape UC Application.

- **OpenScape Mobile licenses**: The handling of this license type closely follows the current behavior of dynamic licenses except that its count is managed separately. OpenScape Mobile licenses control the number of concurrent registered clients, each reserving a single license for its DN.

  Note: If the license file does not contain an entry for OpenScape Mobile then OpenScape Voice considers OpenScape Mobile licensing as not being activated. License usage will operate as before (i.e., the dynamic license pool will be used to serve OpenScape Mobile users).

- **Encryption licenses**: This license type controls the number of subscribers in OpenScape Voice which are configured to allow SRTP and for which at least one contact is registered using the TLS transport type.

  Encryption licenses are handled similar to dynamic licenses meaning similar counters, enforcement at registration time, support for Subscription based licensing, support for Regular License files.

  As long as the Encryption license enforcement is not active, all devices shall be allowed to register even when exceeding the system's Encryption licenses.

  Note: If Dynamic Licensing enforcement or OpenScape Mobile licensing enforcement is active the Registration Request may be rejected because of the enforcement for those licenses. OpenScape Voice keeps track of violations and generate alarms to notify the System Administrator about the violations.

  A registration which requires a new encryption license will be rejected if encryption license enforcement is active and all encryption licenses are used.

  Note: As soon as enforcement becomes active, devices which require but don't possess an encryption license will lose their registration on the next re-registration. This results in a complete loss of calling capabilities including emergency calls from the device.

The network planner will need to estimate the proper quantity of each license type, based on knowledge of the customer and network traffic flow.

6.4 OpenScape Deployment Service (DLS)

SIP telephones are highly functional devices and require a significant number of configuration parameters to be set correctly for proper operation, including IP parameters, feature options, and key and button layouts. In addition, software updates for the endpoints are required from time to time. While these phone parameters and software updates can be handled manually, on a phone-by-phone basis, this can result in time-consuming installation and maintenance tasks in a large network.

Unify SIP phones offer another option, a centralized download server, or DLS, which can be used to set the configuration of each phone automatically. DLS is a Java-based application with a web-based user interface. It currently runs on the Windows 2000 or 2003 Server OS. The DLS supports Unify OpenStage, optiPoint 410 S/420 S, WL 2 Professional S, and the optiClient 130 S SIP client.

One of the most important feature of DLS is the “plug-and-play” feature, which permits phones and clients, when they are connected to the network and powered up, to automatically discover the DLS and download the proper software and configuration data. In order for the “plug and play” feature to work, a DHCP server must be configured and available in the domain. You can only use the plug-and-play functionality if there is a DHCP/DNS infrastructure in the network and it has been configured for working with the DLS, by adding Unify specific tag values to the DHCP server response message format.

Operation of the DLS requires the presence of the HiPath License Management solution to count and dispense endpoint licenses as phones are installed and brought into service. Refer to Section 6.3, “HiPath License Management (HLM)”.

A single DLS can support multiple Unify OpenScape Voice systems. However, there should not be any overlaps in the phone numbers between the various systems; in other words, the phone numbers should be unique across the whole system.

For plug-and-play operation, only one DLS, DHCP, CLA, and FTP server is allowed per domain at the customer facility.

The DHCP server provides the phone with an IP address and the address of the DLS server. The DLS needs the address of the CLA and FTP servers to complete the software update and configuration of the phones. The FTP server is used to download software and configuration data to the endpoints.

In addition to providing a convenient mechanism to install and upgrade phones, DLS also provides, in cooperation with Unify OpenScape Voice, an advanced DLS mobility feature that permits an authorized user to logon to any authorized phone. The DLS automatically configures the phone to the key settings and preferences of the user. When DLS mobility is in use, the capacity of the DLS server (the number of phones that can be supported) is reduced.

When the DLS is integrated in the Unify OpenScape Voice server, its capacity is as listed in Table 21, "DLS Specifications When Integrated Into Unify OpenScape Voice Server".

Scenario	**Maximum of**	**Users or Sessions**
SIP	SIP Devices	5000
DLS Mobility	Mobile Users (30k data)	1000
DLS Mobility	Logon/logoff of Mobile Users per hour (30k data)	250

Table 21 DLS Specifications When Integrated Into Unify OpenScape Voice Server

When the DLS application is installed on a standalone server, its capacity will depend on the server type and application configuration options. The application utilizes (and comes standard with) Microsoft SQL Express Edition. On a dual Xeon server with 2 GB of RAM and adequate disk space (equivalent to a Fujitsu Siemens Econel 200 S2), the approximate capacity is as listed in Table 22.

Scenario	**Maximum of**	**Users or Sessions**
SIP only	SIP devices	40,000
DLS Mobility	Mobile users (30k data)	20,000
	Mobile users (200k data)	5,000
	Logon/logoff of mobile users per hour (30k data)	10,000

Table 22 DLS Specifications—Express Edition

Capacity can be expanded by switching to Microsoft SQL Enterprise edition, which can be installed on the same server or on a separate server. On a Xeon Quad CPU server with 8 GB of RAM (equivalent Fujitsu-Siemens PRIMERGY RX300 S3) the approximate capacity is listed in Table 23.

Scenario	**Maximum of**	**Users or Sessions**
SIP only	SIP devices + mobile users	100,000
DLS Mobility		

Table 23 DLS Specifications—Enterprise Edition (Seite 1 von 2)

Scenario	Maximum of	Users or Sessions
DLS Mobility	Logon/logoff of mobile users per hour (30k data)	20,000
DLS Mobility	Logon/logoff of mobile users per hour (200k data)	10,000

Table 23 DLS Specifications—Enterprise Edition (Seite 2 von 2)

6.5 Enhanced Emergency Calling Service

Enhanced emergency service (E9-1-1) is a challenge for IP telephone systems because IP endpoints are inherently mobile. A subscriber can often disconnect the phone, walk to another location, and plug the phone into any available LAN plug, at which point the phone will usually return to service.

Therefore, the traditional database which maps phone numbers to locations is not a reliable mechanism for identifying the location of the emergency call originator. This is particularly true for VoIP soft clients, which are often installed on laptop computers and are intended to be mobile. Because of this, Unify OpenScape Voice provides an optional alternate mechanism for locating the originator of the emergency call. This mechanism can be used where emergency call routing and location identification be based on the IP address or Fully Qualified Domain Name (FQDN) of the caller, rather than their telephone number.

The administrator may subdivide the corporate network into logical subnets (e.g. geographically grouped), each having a range of IP addresses it serves, each having a route and ELIN (emergency location identifier number) assigned. The ELIN is a digit string that represents a physical location. In a network where the phones are not portable and the IP addresses are static (permanent), the ELIN can sometimes be configured the same as the phone number.

In an IP environment where phones frequently move, the phone number can no longer be reliably used to identify a location, so ELINs based on subnets are used for this purpose. Using subnets, the ELIN can represent an area as general as the building address, or as specific as a particular office or row of cubicles.

Proper ELIN reporting requires the network planner to do the following:

1. Divide the enterprise work area (campus, building, floor, work room) into areas of appropriate size, each served by a specific LAN switch or switch port.
2. Assign a suitable IP address range to the area.
3. Use the DHCP server(s) to assign IP addresses in accordance with this network plan.

The auto-discovery mechanism maintains and provides the proper ELIN reporting.

The LIN is assigned based on the emergency caller's URI (host part) identification which can be one of the following:

- IPv4 IP Address or subnet information

- IPv6 IP Address or subnet information
- FQDN or location domain name

Source-based routing, based on the emergency caller's IP address assigned via DHCP, is used to route the call to the proper Gateway and PSAP where the caller is located.

FQDNs are supported in the host part of the calling party URI. A DNS is required (in conjunction with DHCP server(s)) and is typically provided by a Service Provider. This enables subscribers that are located behind an SBC and/or Service Provider to be provisioned as part of the Unify OpenScape Voice Emergency Calling application.

6.5.1 DHCP Auto-Discovery Mechanism

The Dynamic Host Configuration Protocol (DHCP) Auto-Discovery mechanism of Unify OpenScape Voice provides the correct LIN and callback number assignments for emergency calls from nomadic subscribers on the corporate network. DHCP option 82 and/or 120 must be used at the Relay Agent and DHCP server.

The purpose of the Relay Agent is to obtain an IP address for the endpoint when the endpoint does not have a static IP address or has moved location. The Relay Agent forwards the endpoint’s request for an IP address to a DHCP server. The Relay Agent notes the port to which the endpoint is connected and, then forwards this information (including the LAN switch ID) to the designated DHCP server. The DHCP server uses the port number and switch ID to correlate it with a work area and assigns an IP address in the appropriate range to the requesting device.

Note: The Layer 2 (L2) switch only adds the switch ID and port number (Option 82) to the DHCP request. It is the network administrator’s task to understand the wire-map of the building and create subnet scopes that correspond to the floor plan layout. The correct scope can then be assigned by programming the DHCP server accordingly.

The DHCP server sends the relay agent the IP address for the endpoint along with Option 82 information. The relay agent removes the Option 82 information, then forwards the IP address to the requesting endpoint.

When subscribers are not all within the same IP Network, Session Border Controller’s (SBCs) are generally required and an Internet Service Provider (ISP) interface may be used to provide SIP interconnection to subscribers in other branches of the same Enterprise or in other Enterprises. The Network Address Translation (NAT) and firewall functions deployed in these networks change the IP addresses of SIP calls. In this case, the use of Fully Qualified Domain Names (FQDN), configured via DHCP Option 120, must be employed. The FQDNs are passed transparently to Unify OpenScape Voice in the URI host part of the To header of a REGISTER request (as part of the contact data). When an emergency call is made, the FQDN is included in the From header of an INVITE method which identifies the subscriber's domain name (URI user part identifies the specific subscriber).

6.5.1.1 DHCP Option 82 Address Assignment - Registration

Figure 15, "DHCP Option 82 Address Assignment and SIP Registration" illustrates the process by which an endpoint, in this case a phone, receives an IP address and registers with Unify OpenScape Voice. This occurs in two phases: first, obtaining an IP address; second, registering with Unify OpenScape Voice.

DHCP Option 82 Address Assignment by DHCP Server

1. The phone sends a DHCP broadcast to obtain an IP address.
2. The DHCP relay agent (L2 switch) relays the request to the DHCP server along with the port information (Option 82) indicating the port to which the phone is connected.
3. The DHCP server responds with an IP address, including Option 82 information.
4. The DHCP relay agent strips off the Option 82 information and passes the IP address to the phone.

Registration to Unify OpenScape Voice with the obtained IP Address

5. The phone registers with Unify OpenScape Voice using the newly obtained IP address.
6. Unify OpenScape Voice correlates the IP address with the location information (LIN) and stores the association (phone/IP address/ LIN) in the location database.

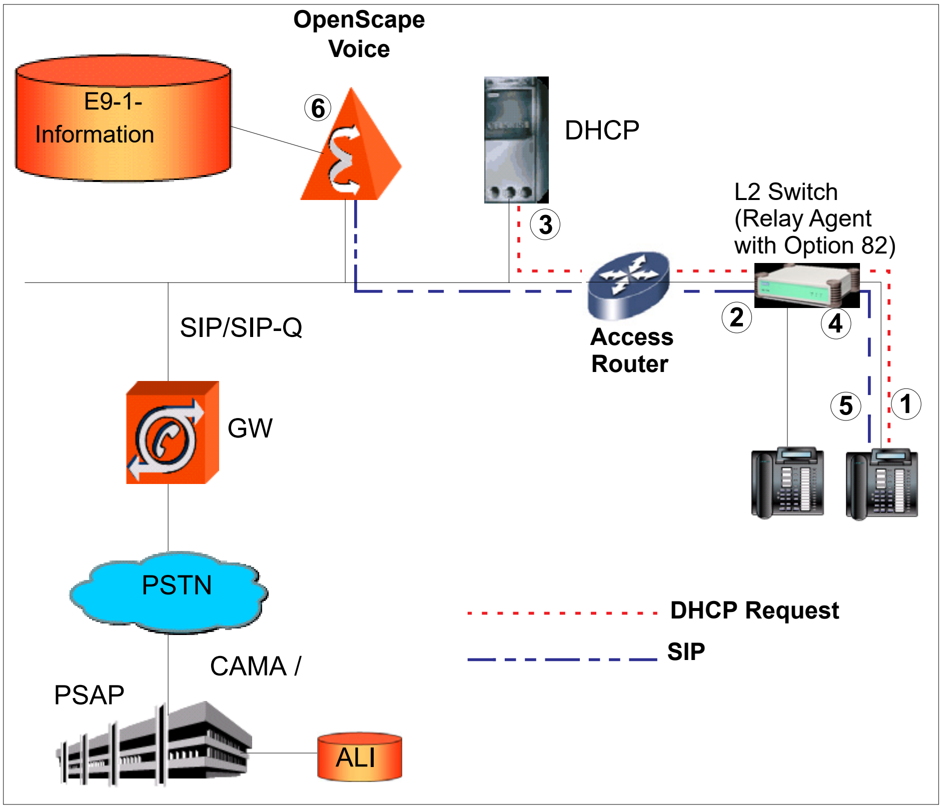


Figure 15 DHCP Option 82 Address Assignment and SIP

6.5.1.2 DHCP Option 120 Address Assignment - Registration

The domain name provided by the DHCP Option 120 can be passed through the SBC transparently so that it can be used by Unify OpenScape Voice to determine the appropriate emergency call LIN/ Route to be used. The system administrator must configure the DHCP servers to provide an Option 120 domain name that identifies the geographic location of the device. Within Unify OpenScape Voice administration, this is referred to as the ‘location domain’. The DNS servers must also be configured so that all these ‘location domains’ resolve to the address of the SIP Registration/Location Server (i.e. Unify OpenScape Voice or central SBC). In other words, all the ‘location domains’ are aliases for the ‘real’ SIP Registration/Location Server domain.

When using DHCP Option 120 for subscribers behind a SBC, the process by which an endpoint device, receives a FQDN and registers with Unify OpenScape Voice occurs in two phases: first, obtaining the FQDN that identifies the geographical location of the device; second, registering with Unify OpenScape Voice.

DHCP Option 120 FQDN by DHCP Server

1. The phone sends a DHCP Broadcast to obtain a FQDN.
2. The DHCP relay agent (L2 switch) relays the DHCP Broadcast request to the DHCP server.
3. The DHCP server responds with an FQDN, including Option 120 information.
4. The DHCP relay agent strips off the Option 120 information and passes the FQDN to the endpoint device.

Registration to Unify OpenScape Voice with the obtained IP Address

5. The endpoint device sends the FQDN as host part of the To header field in the SIP Register request
6. The SBC does not change the FQDN when relaying the SIP Register to Unify OpenScape Voice.
7. Unify OpenScape Voice retrieves the location information (LIN=FQDN) and saves it in the location database.

6.5.2 Emergency Call Processing

When an emergency call arrives at Unify OpenScape Voice, it uses the subscriber’s DN, or IP address and/or FQDN to look up and retrieve from the Emergency Calling table its assigned LIN and route. Emergency Departments, or Subnets and/or FQDNs are defined and routes are assigned using Unify OpenScape Voice Assistant for each Unify OpenScape Voice business group in the Emergency Calling table. This mechanism can work for any emergency call, regardless of the digits that are dialed to signal the emergency.

The so-called route is actually a digit suffix logically identifying the public safety answering point (PSAP). This digit string is appended to the emergency number (normally 911) and the resulting number—for example, 911-88—is retranslated. This new number must route to the appropriate gateway to reach the PSAP.

Delivery of the LIN and other 911 parameters to the appropriate PSAP is by way of the PSTN gateway, using SIP or SIP-Q. Caller ID is also delivered to the gateway. The system provides an option to deliver the LIN as the caller ID, rather than in addition to the caller ID for those central offices which do not recognize a separate LIN parameter. An administrable flag controls whether Unify OpenScape Voice sends LIN information:

- As the user part of the From header URI or (when not present) in the body in the clear
- As the calling party number digits to the appropriate PSAP

This option permits the support of scenarios where the PSAP requires the LIN without supporting an emergency call specific-interface—for example, PRI instead of CAMA.

The PSTN interface utilized by the PSAP is traditionally an analog centralized automatic message accounting (CAMA) trunk, although some PSAPs now use an ISDN PRI interface.

When emergency calling service is provided, it is expected that one or two dedicated trunks or ISDN B-channels will be reserved for this purpose. Unify OpenScape Voice does not provide preemption or priority override for emergency calls, so if all available trunks are in use, the emergency call is blocked.

The selected gateway must support the appropriate interface. Table 24 lists gateway options that support the necessary signaling.

Gateway	Protocol Used	Comments
OpenScape 4000 HG 3500	SIP-Q	OpenScape 4000 relays call and ELIN to the PSAP via ISDN or CAMA trunk configuration

Table 24 E9-1-1 Gateway Options

Figure 16, "Emergency Call Flow" illustrates the following steps in the emergency call flow:

1. A caller places an emergency call by sending an INVITE to Unify OpenScape Voice.
2. Unify OpenScape Voice, via translation, identifies an emergency number and uses the subscriber’s DN, or IP address subnet mask and/or FQDN to look up and retrieve an appropriate LIN from the Emergency Calling table.
3. The route number leads the call to a particular gateway (GW) in the geographical location that is served by the public network’s E9-1-1 tandem office. It can then route the call to the proper PSAP jurisdiction serving the caller.

The survivable media gateway RG 8700 provides CAMA/MF signaling to the
E9-1-1 AT. In normal mode, Unify OpenScape Voice sends a LIN and this is signaled as ANI. In survivability mode, the LIN is derived from local administration information that is configured in the gateway itself. This ensures E9-1-1 compliance in survivability mode.

If an emergency call cannot be routed to a PSAP operator, the call can be optionally routed to an E9-1-1 Default Emergency Number (Directory Number format) as an added precaution.

If a PSAP operator needs to return a call placed to the emergency center, Unify OpenScape Voice provides the capabilities to do so; however, this capability requires additional administration. Refer to Section 6.5.3, “Administration”.

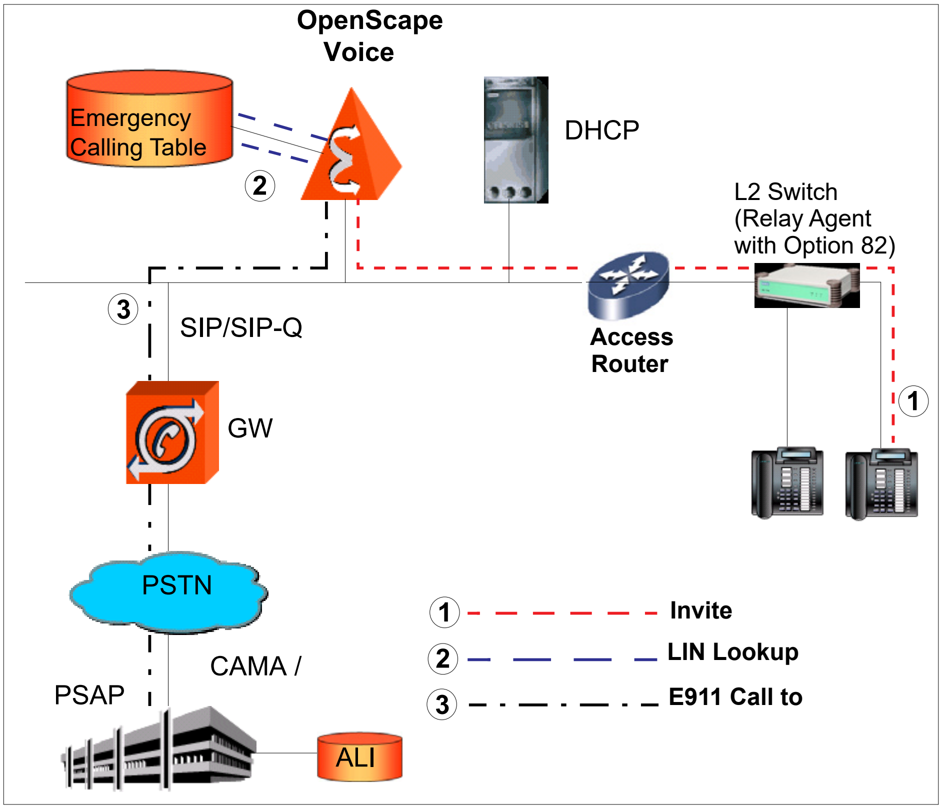


Figure 16 Emergency Call Flow

If an Unify OpenScape Voice system is serving multiple geographic locations, and
E9-1-1 service is a requirement, links (and routes) to each responsible PSAP will be required.

6.5.3 Administration

To support the Emergency Service capability, Unify OpenScape Voice contains an Emergency Calling table. This table consists of Emergency Departments, or IP address/subnet and/or Location Domain (i.e. FQDN) entries populated with the emergency location identifier number (ELIN) and, additional digits that can be appended to the called number to determine via translation the associated route, to ensure that the Emergency Call is sent to the correct gateway connected to the PSAP.

Each Business Group contains an Emergency Calling table. The administrator can enter in the table a list of Emergency Departments or, IP subnets and/or a Location Domain, an ELIN, Digits to append to determine the route, as well as other information—for example, database IDs, passcodes for admins, and descriptions.

The Emergency Calling table also contains information associated with each LIN that permits calls to be placed from the PSAP directly to the device which placed the emergency call, or alternately to a designated static number. Examples of this information are as follows:

- The AoR of the endpoint that placed the emergency call
- Callback DID number known by PSAP
- A default callback destination
- A flag to indicate if the last user should be called back

Note: GNF format—for example, +15615551234, must not be used in North America since a 10-digit national numbering format LIN is required in the US and Canada.

Unify OpenScape Voice also provides a SOAP export mechanism to generate, on demand, output files containing E9-1-1 table data currently existing on Unify OpenScape Voice.

6.5.4 Integration with RedSky E911Network Services

Unify OpenScape Voice and OpenScape Voice Assistant support the integration with RedSky E911 Manager and RedSky E911 Anywhere Network Services (Emergency Call Services provider).

Note: It is an emergency subscription service for North America only.

The RedSky E911 Network Services provide location information to Public Safety Access Points (PSAPs) that has finer granularity then the Unify OpenScape Voice subnet-based solution. It consists of the following two network components:

- RedSky E911 Manager

- RedSky E911 Anywhere

Attention: In order for Unify OpenScape Voice to interoperate with RedSky E911 Manager and RedSky E911 Anywhere, Unify OpenScape Voice must be configured appropriately by OpenScape Voice Assistant to retrieve the ELINs from the RedSky E911 Manager and route Emergency Service Calls to RedSky E911 Anywhere.

The RedSky E911 Manager can be simplex or redundant (active/ standby mode). Unify OpenScape Voice shall support both options. Unify OpenScape Voice shall send the signaling only to the active RedSky node. When the active RedSky node does not respond, Unify OpenScape Voice shall switch to the redundant node. The signaling transport type between Unify OpenScape Voice and RedSky E911 Manager shall be either TCP or TLS.

RedSky E911 Anywhere is an optional subscription service for routing emergency calls in North America only. It acts as a SIP Service Provider for emergency calls and distributes E911 calls to their respective Local PSAP. Unify OpenScape Voice shall connect to RedSky Anywhere Network Service via an SBC.

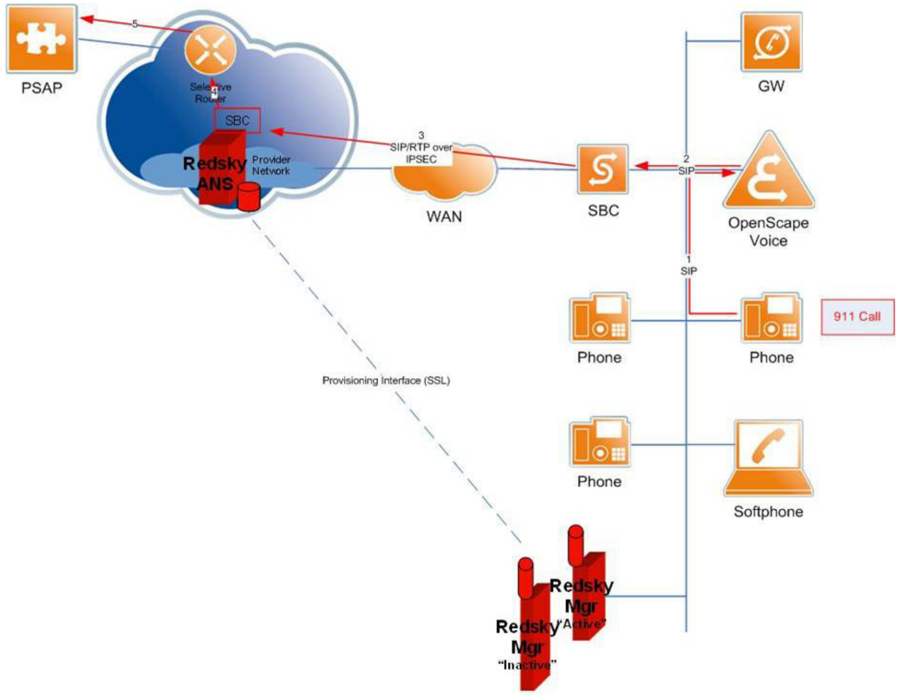


Figure 17 Using RedSky E911 Manager & RedSky E911 Anywhere

Unify OpenScape Voice informs RedSky E911 Manager (via SIP PUBLISH messages) about any registration changes of its subscribers' contacts. RedSky E911 Manager performs a network discovery for each registered contact in order to find the Emergency Response Location associated with it, and returns to Unify OpenScape Voice the corresponding ELIN. Unify OpenScape Voice receives the ELINs (via SIP PUBLISH messages) and stores them locally.

Note: RedSky E911 Manager can be provisioned with an ELIN per IP range. When provisioned, it shall respond with an ELIN to Unify OpenScape Voice even if the network discovery fails.

Note: Remote users registered behind an SBC shall not be supported. If any of such users originates an E911 call, the IP of the SBC shall be sent to the RedSky E911 Manager, and the discovery shall either fail or return the ELIN associated with the SBC.

During emergency calls, Unify OpenScape Voice uses the ELIN discovered for the calling device's contact and transports it as the calling party number. The emergency calls are routed to the Redsky Anywhere Network Services server for further routing to the proper PSAP authority. The routing is based on digits appended to the dialed emergency number.

Unify OpenScape Voice can be connected with the RedSky Anywhere either with SIP trunking (via SBCs on the network boundaries) or through PSTN (via SIP GWs).

Emergency callbacks are identified by the ELIN as the called party number. For this purpose all the known ELINs must be provisioned in Unify OpenScape Voice to route to the emergency callback service. The emergency callback service uses the ELIN in order to find the latest contact that used the ELIN in the emergency call, and routes the call back to this contact.

Survivable mode

Currently there is no integration between OpenScape Branch and RedSky. In case a WAN failure isolates a branch office from the data center hosting OpenScape Voice, OpenScape Branch shall provide local emergency calling service to users located in the Branch.

Note: RedSky E911 Manager shall not be connected or integrated with OpenScape Branch. OpenScape Branch shall use its existing Emergency Calling service when in survivability mode.

6.5.4.1 Device Registration and Publish to RedSky E911 Manager

RedSky E911 Manager must be notified of the SIP subscribers registrations. When a SIP subscriber registers successfully, or is unregistered, Unify OpenScape Voice shall send a PUBLISH message to the active RedSky E911 Manager when:

- the maximum threshold of registrations per PUBLISH message is reached (configurable, default is 50), or
- the configurable periodic publish timer (default is 60 seconds) expires since receiving the response to the last message.

Unify OpenScape Voice supports two Registration and Publishing mechanisms with the RedSky E911 Manager:

1. Devices that do not support sending their MAC address (Generic mechanism): RedSky E911 Manager must query the L3 switch (router) in order to obtain the devices's MAC address and then perform a Network Discovery on the L2 switch.
2. Devices that support sending their MAC address: Since the MAC address is provided, it eliminates the need for RedSky E911 Manager to access the L3 switch and it can perform a Network Discovery directly on the L2 switch.

The PUBLISH shall contain registrations that have been identified as “new” registrations or un-registrations by Unify OpenScape Voice. Each registration contains the registration information (Contact-URI), a unique identifier and the registration status (registered or unregistered). Refresh registrations that have already been published shall not be published again.

For every PUBLISH message that Unify OpenScape Voice sends, it shall wait for a 200 OK before sending the next message.

RedSky E911 Manager asynchronously sends a PUBLISH message back to Unify OpenScape Voice for every new association of a registered device, containing the received contact information, the unique identifier of the contact, and the ELIN assigned to the contact. Unify OpenScape Voice updates its database with the ELINs.

Devices that do not support sending their MAC address (Generic mechanism)

When a SIP subscriber registers successfully, Unify OpenScape Voice sends a PUBLISH message to the RedSky E911 Manager providing the IP address of the device. Since the PUBLISH message does not contain a MAC address, the RedSky E911 Manager server must dynamically determine the MAC address based on the IP Address using the ARP tables on the appropriate network L3 switch(es).

Note: Redsky E911 Manager supports IPv4 addresses but not IPv6. Contacts with IPv6 addresses will not be published to RedSky E911 Manager.

After the RedSky E911 Manager sends an SNMP ARP query to the L3 switch to resolve the IP address to the device's MAC address, it queries the L2 switch with the MAC address to find the physical switchport location of the device, and based on RedSky E911 Manager's configured DB obtains the device's ELIN. The device's ELIN is sent to Unify OpenScape Voice and RedSky E911 Anywhere using a PUBLISH message.

Note: There are risks with the SNMP ARP queries and many customers do not allow them on their L3 switches (routers).

If an ELIN for a contact is changed, RedSky E911 Manager shall send a new PUBLISH to Unify OpenScape Voice with the new ELIN. Unify OpenScape Voice shall replace the previous ELIN with the new one.

If a contact is registered using an FQDN, then RedSky E911 Manager must be able to resolve the FQDN. If RedSky E911 Manager cannot resolve the FQDN, then it will not send an ELIN for this contact and Unify OpenScape Voice shall fallback and use the Emergency Calling table in order to retrieve a provisioned LIN (refer to Section 6.5.3, “Administration”).

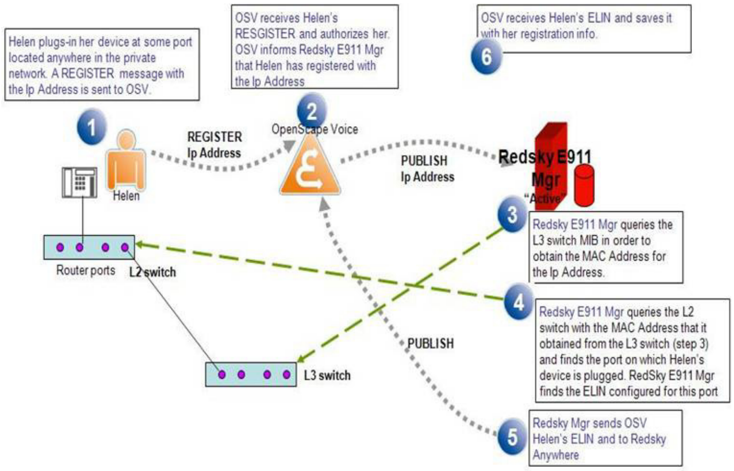

Helen plugs-in her device at some port located anywhere in the private network. A REGISTER message with the Ip Address is sent to OSV.
OSV receives Helen's RESGISTER and authorizes her. OSV informs Redsky E911 Mgr that Helen has registered with the Ip Address
OSV receives Helen's ELIN and saves it with her registration info.
6
1
2
OpenScape Voice
REGISTER Ip Address
Helen
PUBLISH Ip Address
Redsky E911 Mgr
"Active"
3
Redsky E911 Mgr queries the L3 switch MIB in order to obtain the MAC Address for the Ip Address.
Router ports
L2 switch
4
Redsky E911 Mgr queries the L2 switch with the MAC Address that it obtained from the L3 switch (step 3) and finds the port on which Helen's device is plugged. RedSky E911 Mgr finds the ELIN configured for this port
PUBLISH
L3 switch
5
Redsky Mgr sends OSV Helen's ELIN and to Redsky Anywhere

Figure 18 Devices that do not support sending their MAC address

Devices that support sending their MAC address

The Unify OpenStage and OptiPoints devices as well as the OpenScape Desktop Client Personal Edition soft client (Section 1.1, "Unify OpenScape Voice Networking Overview") support sending their MAC address during registration.

Unify OpenScape Voice provides the MAC address of its registered devices to RedSky E911 Manager. RedSky E911 Manager can therefore go directly to the L2 switch, eliminating the step of SNMP ARP queries to the L3 switches. In order to facilitate this procedure, the devices have been requested to provide their MAC addresses in their REGISTER requests. Unify OpenScape Voice parses the MAC address from the REGISTER requests and publish them to RedSky E911 Manager.

For devices that do not support providing their MAC address in REGISTER requests, Unify OpenScape Voice shall publish their IP address to RedSky E911 Manager. The RedSky E911 Manager shall perform SNMP ARP queries to L3 switches (refer to: Devices that do not support sending their MAC address (Generic mechanism)).

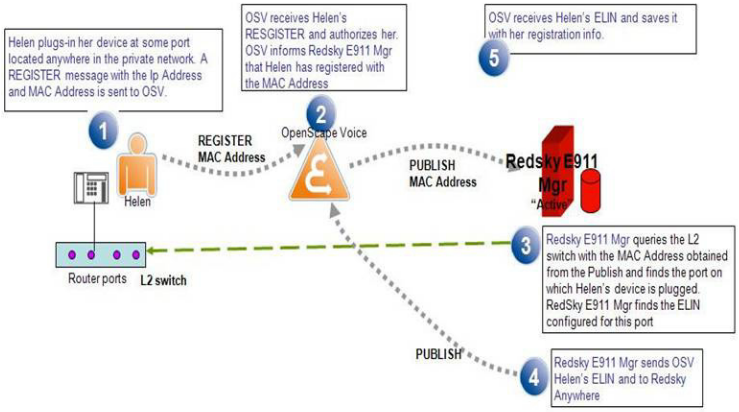

Helen plugs-in her device at some port located anywhere in the private network. A REGISTER message with the Ip Address and MAC Address is sent to OSV.
1
OSV receives Helen's RESGISTER and authorizes her. OSV informs Redsky E911 Mgr that Helen has registered with the MAC Address
2
OSV receives Helen's ELIN and saves it with her registration info.
5
Helen
REGISTER
MAC Address
OpenScape Voice
PUBLISH
MAC Address
Redsky E911
Mgr
"Active"
Router ports
L2 switch
3
Redsky E911 Mgr queries the L2 switch with the MAC Address obtained from the Publish and finds the port on which Helen's device is plugged. RedSky E911 Mgr finds the ELIN configured for this port
PUBLISH
4
Redsky E911 Mgr sends OSV Helen's ELIN and to Redsky Anywhere

Figure 19 Devices that support sending their MAC address

6.5.4.2 Emergency Calls using the RedSky E911 Services

When an Unify OpenScape Voice subscriber makes an emergency 911 call that is subscribed to use RedSky E911, the following takes place:

1. Unify OpenScape Voice finds the entry in the database based on the contact information, retrieves the stored ELIN, and updates the entry with the timestamp
2. Unify OpenScape Voice adds the ELIN in the outgoing SIP INVITE and routes the call to RedSky E911 Anywhere Service
3. The RedSky E911 Anywhere Service routes the call to the corresponding PSAP based on the ELIN

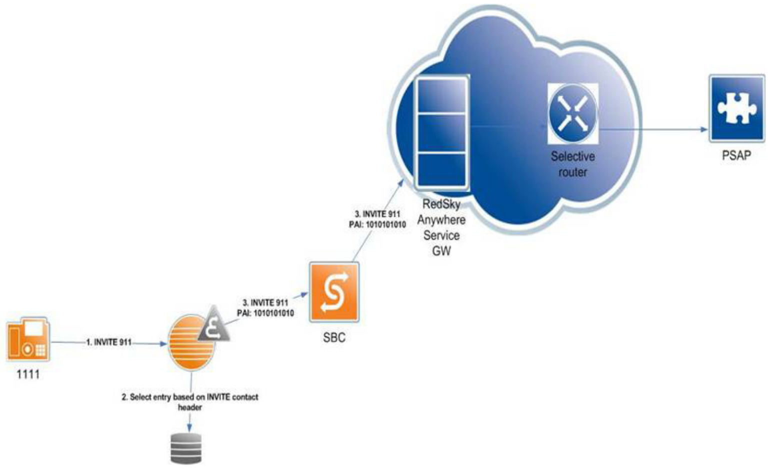


Figure 20 Emergency service call using RedSky E911 Network Services

When an emergency call is originated by an Unify OpenScape Voice subscriber, the emergency call service has the following logic:

When integration with RedSky is enabled:

- If an ELIN is found, insert the ELIN in the CPN and PAI headers and route the call to the provisioned route for the RedSky Anywhere service
- If an ELIN is not found, search under the Emergency Calling table entries in order to find the subnet
  - If a subnet is found, route the call to the provisioned destination
  - If no subnet is found, route the call to the default emergency destination

When integration with RedSky is not enabled

- Search under the Emergency Calling table entries in order to find the subnet
  - If a subnet is found, route the call to the provisioned destination
  - If no subnet is found, route the call to the default emergency destination

6.5.4.3 Emergency Callback using the RedSky E911 Services

When the PSAP calls back, the ELIN that it received is used as the Emergency Callback Number:

1. Unify OpenScape Voice finds the entry with ELIN and selects the one with the latest timestamp (i.e., last registered device that made the emergency call with the given ELIN).
2. Unify OpenScape Voice routes the call to the contact stored in the corresponding entry

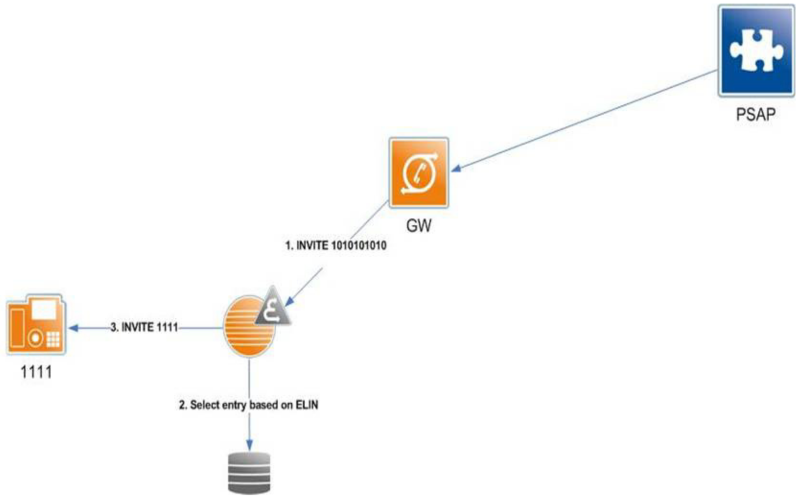


Figure 21 Emergency Callback using RedSky E911 Services

When Unify OpenScape Voice receives an emergency callback, the emergency callback service shall have the following logic:

When “Integration with RedSky” is enabled, Unify OpenScape Voice searches the DB to find entries which have the ELIN received in the callback

- If match is found:
  - And configured to “Use default Call Back Destination”, then route the call to the Default Callback Destination
  - Otherwise, route the call to the contact stored in the entry
- If no match is found, use the Callback number to search for the entry in the Emergency Calling table:

  - If match is found and configured to “Use default Call Back Destination”, then route the call to the Default Callback Destination,
  - If match is found and not configured to “Use default Call Back Destination”, then route the call to the contact stored in the entry
  - If no match is found, then route to the Default Callback Destination

If integration with RedSky is not enabled, use the Callback number to search for the entry in the Emergency Calling table

- If match is found:
  - And configured to “Use default Call Back Destination”, then route the call to the Default Callback Destination
  - Otherwise, route the call to the contact stored in the entry
- If no match is found, then route to the Default Callback Destination

6.5.5 Emergency calls using the subscribers’ DN

Unify OpenScape Voice supports emergency sub-grouping entities under a Business Group defined as Emergency Departments, where subscribers are assigned as members to one of the subgroups. This service facilitates emergency call routing logic based on the calling user's identity (ie phone number).

Each Emergency Department shall be configured with a route and a LIN.

When Unify OpenScape Voice handles an emergency call it shall check whether the originating user belongs to an Emergency Department, and if so, it shall route the call according to the group’s routing configuration and use the LIN provisioned under the group.

Attention: It shall be the responsibility of the company's administrator to ensure that the database is updated any time a user is moved to a different location in the company (e.g. different room, floor, building, site).

6.5.6 Emergency calls using OpenScape Xpert

An OpenScape Xpert Communication solution consists mainly of the following components:

- OpenScape Xpert Multi-Line Controller (MLC)
- OpenScape Xpert System Manager
- OpenScape Xpert terminals (turrets)
  - OpenStage Xpert 6010p Terminal with Touch Screen
  - OpenScape Xpert Client Terminal (PC with Softclient)
- Unify OpenScape Voice (SIP Server)
- Gateways

The MLC is the heart of the OpenScape Xpert Communication Solution. It serves as a softswitch that provides the resources, features and IP interfaces to all other OpenScape Xpert components and acts as multiple SIP subscribers (lines) towards Unify OpenScape Voice.

The MLC explicitly passes the terminal's IP in the X-Siemens-Location header field. If Unify OpenScape Voice, on processing the emergency call, identifies an IP in the X-Siemens-Location header field, it shall use that IP in order to find a matching IP subnet in its provisioned Emergency Calling table. This way Unify OpenScape Voice shall provide emergency location discovery based on the turret's IP and not that of the MLC.

When the Unify OpenScape Voice identifies the X-Siemens-Location header field in the incoming Invite request of an emergency call, then the following shall apply:

1. If an IP address is provided (in the IP parameter) and it matches a provisioned emergency IP subnet, then the IP address is used.

   Note: Unify OpenScape Voice shall provide emergency location discovery based on the turret's IP and not that of the MLC.

2. If a location domain is provided and it matches a location domain in the provisioned emergency subnets, then the location domain is used.
3. Otherwise, the contact’s IP is used to find a matching emergency IP subnet.

During an emergency call, on processing a location domain with an explicit IP, if an emergency IP subnet is found for this IP, Unify OpenScape Voice shall store the location domain string as it was received on the X-Siemens-Location header field (e.g. IP=10.10.10.10;802MAC=0123456789AB). During an emergency callback, Unify OpenScape Voice shall retrieve the string that was stored and shall insert it in the X-Siemens-Target field of the outgoing INVITE request that is sent to the MLC. The MLC on processing the emergency callback INVITE shall be able to process the X-Siemens-Target field and present the callback to the specific turret identified by the IP.

6.5.7 Emergency Call Attribute settings for SIP to ISDN interworking

Users making emergency calls that are routed to the PSAP via a SIP to ISDN interworking Gateway, ie. OpenScape Branch, must be configured properly in order to send the LIN or alternatively, for different scenarios, the Subscriber’s Calling Identity (Home DN).

The **Emergency Calling** table contains the **Send LIN instead of CPN** attribute which defines whether to send the LIN or CPN to the PSAP. When this attribute is enabled/checked, the intention should be to send the provisioned LIN which has to be interworked SIP to ISDN by the Gateway and sent to the PSAP. When this attribute is disabled/unchecked, a number of Endpoint attribute settings shall designate the CPN identity and the SIP headers used for delivery. Endpoints with proper attribute settings must be created to provide the means for the desired SIP to ISDN interworking outcome at the Gateway to the PSAP. Therefore, the provisioning suggestions outlined below should be followed for each case:

1. **Send LIN instead of CPN** attribute is enabled/checked:
   - In order to send LIN to the Gateway the Endpoint attribute **Use Subscriber Home DN as Authentication Number** under OpenScape Voice configuration must not be set.
2. **Send LIN instead of CPN** attribute is disabled/unchecked
   - If the Application Populated Caller ID (APCID) or the Subscriber Provided Calling Identity (SPCID) is active, then the APCID or SPCID shall be sent to the PSAP. If this is not desired, then the **Use Subscriber Home DN as Authentication Number** Endpoint attribute under Unify OpenScape Voice configuration for the Gateway must be enabled/checked in addition to one or more of the following:

- **Send Authentication Number in P-Asserted-Identity header** - when this attribute is set, the U**se PAI/PPI as ISDN Calling Party Number** attribute under the OpenScape Branch configuration must be enabled/checked.
- **Send Authentication Number in Diversion Header**
- **Send Authentication Number in From Header**

6.5.8 Emergency Call SNMP Trap (Alarm)

When an Emergency Call is initiated, the Unify OpenScape Voice Emergency Service reads the RTP parameter emergency_SNMP_event to check whether an alarm must be sent. The default setting for this RTP parameter is ‘disabled’. When enabled, an SNMP emergency event shall be sent to a Network Operations Center (NOC) with severity level (4)) ‘warning’ for the emergency call. The NOC can be any device with an SNMP interface that supports displaying the emergency event. An application at the NOC is responsible to interpret the event fields and present them in a meaningful arrangement.

After retrieving all emergency related information and if an alarm must be issued, the SNMP event is built and sent. The data retrieved and sent with the SNMP event at the time of an emergency call includes only the relevant fields that were appropriated for the call. Fields that have not been provisioned shall not be sent. Likewise, fields that are provisioned but not used for the emergency call shall not be included in the data sent in the emergency event. The emergency data shall comprise of the fields in the Table 25, with the exceptions noted.

Data Field Description	Data in Emergency Event	Comment / Example
Calling Party Number	CPN=	Public #, else Private # of caller CPN=561333444
Business Group Name	BG=	BG=Eon23
Default Emergency Number	DefEmNum	DefEmNum=5613338000
Subnet IP or Subnet IPv6	IP	172.25.35.45 (IPv4) 172.25.35.1/45 (IPv4 subnet) fe80::200:f8ff:fe21:67cf (IPv6)
Location Domain	LD=	LD=EonSouth.com
Route Number	RT=	RT=77
LINLIST_E911LIN	LIN=	LIN=5613334444
LINLIST_CBN	CBN=	CBN=5619990000
LINLIST_DCBN	DCBN=	DCBN=5619998888
Address of Record	AoR=	Only if LIN pool is employed with more that one LIN entry. AoR=3
Subscriber IP address	SubIP=	SubIP=172.25.35.63
Subscriber Port	SubPort=	SubPort=5060

Table 25 Emergency data in the Emergency Event

Note: If the emergency call failed to reach the PSAP, then the word “Unsuccessful” is included in the emergency text.

6.6 OpenScape UC Application

Unify OpenScape Voice brings Unified Communications (UC) into an open services-oriented architectural (SOA) solution for managing communications. Optimized for business process integration, OpenScape UC is a unified, real-time, modular UC application suite providing opportunities for a seamless modular upgrade path.

OpenScape UC Application fits into an enterprise’s existing voice and data infrastructure and ties together phones, voice mail, E-mail, text-messaging, calendaring, instant messaging, and conferencing services. It provides an interface to manage online presence and communication and collaboration services.

OpenScape UC Application makes it easier for users—in the office, at home, or on the road—to access the people and the information they need. For example:

- A user can set his preferences for various communications media, specify which people he will take calls from and how they can reach him. For example, if he’s out of the office for the afternoon, he can have all incoming calls between noon and 5:00 p.m. routed to his assistant.
- With a glance at the contact list, a user can see how a particular contact has set his status (for example, in the office, in a meeting) and determine the best way to reach him (voice, instant messaging, E-mail).
- With a single click, a user can initiate a voice conference with his team members and share documents. He can also launch a web conference.

Specific capabilities include:

- IBM groupware integration and Microsoft groupware integration
- Harmonized presence with IBM Lotus Sametime

  Unify OpenScape Voice supports a variety of deployment scenarios for multiple IT and telephony domains across IBM systems, including a tight integration into IBM SameTime 7.5 for a harmonized native user experience.

  The native IBM user experience is also enhanced by having voice mail provided as E-mail in the user's inbox, having real-time communication facilities such as voice calling associated with Livename tags, and the ability to move seamlessly from one contact medium to another as demanded by a collaboration session.
- Linux server and Windows Vista support

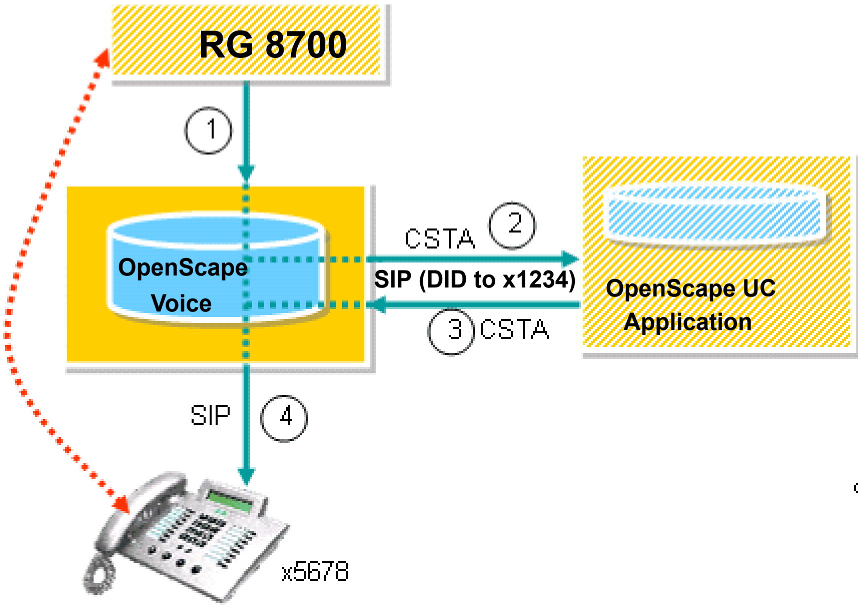
- OpenSOA (Services-oriented Architecture)
- Mobility support via mobile client and device handover
- OpenScape UC Application's real-time communications features allow users to set up and be reached on a single published number, with call routing to actual physical devices controlled by a user configurable set of rules.

In addition, access to specific features is constrained by the license type that is assigned to an OpenScape UC Application user. Unify OpenScape Voice is shipped with a number of OpenScape Personal Edition licenses. This permits a user to originate and answer calls using OpenScape UC, but does not provide presence-related features.

Examples of OpenScape UC Application call handling are illustrated in the following figures:

- Figure 22, "OpenScape UC Application: Inbound Call Handling".
- Figure 23, "OpenScape UC Application: Outbound Call Handling" (i.e. call origination).

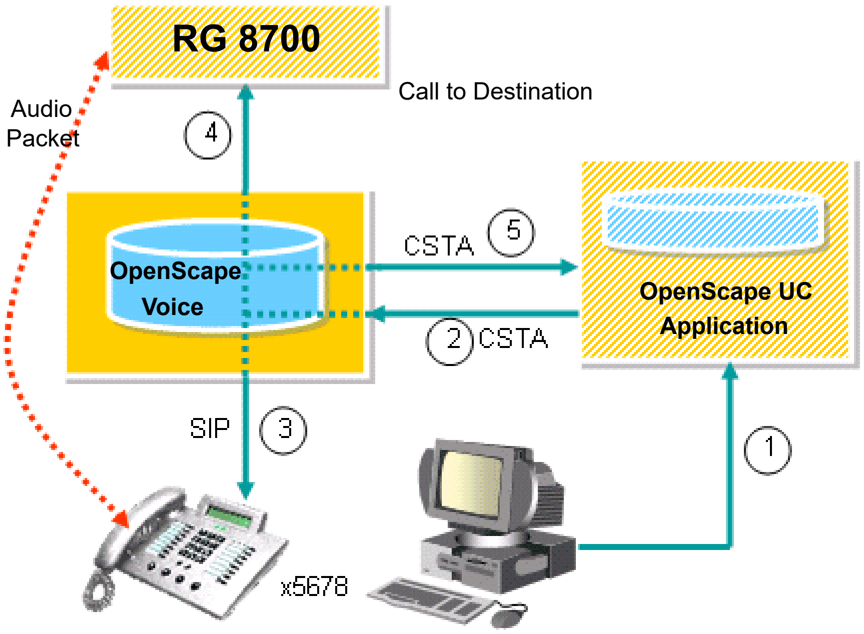
OpenScape UC Application – Inbound Call



1. Incoming SIP call for OpenScape UC Application subscriber x1234.
2. Unify OpenScape Voice delays the call and uses CSTA to ask the OpenScape UC Application how to route this call.
3. OpenScape UC Application orders Unify OpenScape Voice to route the call to the current preferred device – x5678.
4. Preferred device rings.
5. Only one SIP call is processed by Unify OpenScape Voice.

Figure 22 OpenScape UC Application: Inbound Call Handling

OpenScape UC Application – Outbound Call



1. User initiates a call via OpenScape UC Application Web Portal.
2. OpenScape UC Application issues CSTA Make Call request to Unify OpenScape Voice.
3. Unify OpenScape Voice calls the preferred device of the requestor.
4. After requestor answers, Unify OpenScape Voice calls the desired destination.

Figure 23 OpenScape UC Application: Outbound Call Handling

6.7 Conferencing Solutions

SIP telephones have the internal ability to support three-party audio conferences. Some SIP soft clients may support conferences larger than three parties, utilizing the processing power of the host PC. But in general, an alternative is required for larger conferences.

A branch telephone that is optioned for internal three-party conferencing will be able to originate conferences even when the branch is operating in survival mode—for example, when communication with Unify OpenScape Voice and central media server are interrupted.

6.7.1 Unify OpenScape Voice Station-Controlled Conferencing Service

The Unify OpenScape Voice server supports an internal conferencing service, utilizing the OpenScape Media Server as a conference bridge. Ad-hoc conferences of up to 16 parties per conference are supported, without any additional server.

Each Unify SIP phone or soft client is provisioned to:

- Use its own internal conference capability, which limits the user to creating three-party conferences

  -or-

- Use the station-controlled conferencing service of HiPath, in which it uses that service for all conferences the user creates (including three-party conferences).

The network planner needs to be aware that additional ports need to be provisioned on the media server if the station-controlled conferencing option is widely provisioned.

6.7.2 OpenScape UC Application Media Conferencing Unit

If the customer has the OpenScape UC Application, the OpenScape UC Media Conference Unit (MCU) provides an instant conferencing capability and a meet-me (dial-in) conference service. Only OpenScape UC users are permitted to organize or originate a conference, but any Unify OpenScape Voice subscriber (including those without an OpenScape UC license) or PSTN party can be invited to an OpenScape UC controlled conference.

OpenScape UC MCU (which is an instance of the OpenScape Media Server) must be sized accordingly. In rough terms, assuming a standard OpenScape UC traffic model, one media server channel is required for approximately every 10 to 15 subscribers.

6.7.3 Xpressions Conferencing

OpenScape Xpressions provides the ability to establish ad-hoc and meet-me conferences through a web interface with the same look and feel of the OpenScape UC Application client.

The following are the number of channels supported:

- 300 channels with G.711
- 280 channels with G.729 and SRTP

6.8 Video Communication and Video Conferencing

Like most VoIP soft switches, Unify OpenScape Voice is capable of supporting video clients. The Unify optiClient 130 S SIP soft client, when used in conjunction with a desktop PC video camera, can transmit and receive video. It is capable of displaying two video connections simultaneously, but does not provide any video mixing or conferencing capability. The OpenScape Desktop Client Personal Edition also supports video.

Because Unify OpenScape Voice implements the SDP transparency feature concept, it can potentially support a wide variety of IP video apparatus that utilize the SIP protocol for wideband video call setup. The actual negotiation of video codec and bandwidth is done between the endpoints, as is the flow of video information.

Note: Unify OpenScape Voice provides specific video service support and allows video calls to be identified and handled separately when required. In addition, the administrator has the ability to enable and disable video capabilities on a per-subscriber endpoint basis.

At this time, there is no supported VoIP gateway that offers video conversion between the IP environment and the ISDN video environment.

Video conferencing with more than two parties, in which each party sees all others, requires a video conferencing server with video mixing capability.

Therefore, a high use of video calls could potentially affect the voice quality of voice calls. To prevent this, the CAC thresholds need to be manually adjusted to reserve adequate bandwidth for the expected video calling load. See Chapter 14, “Call Admission Control” for CAC calculations and decision making.

OpenScape Video conference bridges and video endpoints support H.264 and the older H.263 video compression, and high resolution audio codecs such as H.722.1 and MPEG AAC.

As Table 26 indicates, video requires significant bandwidth. Keep in mind the conference bridge will require *n*BW* where *n* is the number of video conferees, and *BW* is the bandwidth required for one connection to the bridge.

Quality	Pixel Resolution	Data Rate (kilobits per second)
Webcam / VCR	400*244	128 kbps

Table 26 Video Bandwidth Matrix (Seite 1 von 2)

Quality	Pixel Resolution	Data Rate (kilobits per second)
Cable TV	768*432	384 kbps
DVD	848*480	512 kbps
High Definition TV (720p)Z	1280*720	at least 1 mbps

Table 26 Video Bandwidth Matrix (Seite 2 von 2)

6.9 Session Border Controllers

A session border controller (SBC) enables voice, video, and multimedia communication across IP borders. They also allow SIP-based applications to be extended beyond the Enterprise network boundaries—for example, when the SIP clients of an Unify OpenScape Voice system reside in different IP networks.

SBCs perform the necessary interoperability, security, management, and control capabilities to support SIP trunking applications. They also support the SIP endpoint registration services that are necessary to support remote user and branch office applications. SBCs that are certified for use with Unify OpenScape Voice perform SIP deep-packet inspection specifically tailored for the Unify OpenScape Voice environment to provide proper mediation between IP networks, such as the mapping of IP addresses within SIP signaling and RTP/SRTP media packets that allows for NAT traversal. Media anchoring can be configured to the extent required by media control policies, or set to allow direct media connections between clients.

An SBC enhances customer-network security by providing SIP-aware policy enforcement and security functions such as dynamic RTP/SRTP pin-holing, stateful SIP protocol validation, DoS mitigation, and network topology hiding. SBCs can also provide TLS encryption on both the core- and access-side SIP signaling interfaces as well as SRTP/MIKEY0 media encryption transparent relay. Some SBCs are also capable of SRTP/MIKEY0 termination which allows for media interworking scenarios.

The following are the scenarios in which SBCs can be used:

- **Remote user:** SIP clients behind a NAT registered to Unify OpenScape Voice.
- **Branch office:** SIP clients behind a proxy (OpenScape Branch) register to Unify OpenScape Voice.
- **SIP trunking:** Unify OpenScape Voice routes calls to and from a SIP trunk service provider.

The following sections briefly describe these scenarios. Refer to the *OpenScape Voice, Configuration, Administrator Documentation* for detailed information.

6.9.1 Remote User

Remote users may connect to the main office over the public Internet. When the remote user is a soft client, there is a possibility to use a virtual private network (VPN) to connect to the main office as well as to the Unify OpenScape Voice server; this option is described in Section 6.10, “VPN Access for Remote Users”.

However, when the remote user is a hard phone there is generally no support for a VPN connection at the phone; therefore, it is necessary to use an SBC to allow connection to the Unify OpenScape Voice server. Even when use of VPNs is possible, it is advantageous to use the SBC solution for remote users so that the difficulties of supporting and managing large numbers of VPNs are avoided.

The SBC in the main office data center is given a publicly accessible URL and IP address, and the home workers use this as the address of their SIP Registrar and SIP Server for their SIP phones or SIP soft clients. The SBC also has a second IP address and a separate LAN connection in the corporate LAN, to communicate with the Unify OpenScape Voice server.

6.9.2 Branch Office

The SBC allows the data center to have its own addressing scheme, independent of the addressing schemes of the branch offices. The choice of using a central SBC in the data center or SBCs in each branch office depends on several factors, including the need for any of the following:

- Media relay function via an SBC in the data center. The enterprise policies may require RTP media to pass through the data center rather than allowing direct media connections between the branches.
- Media transcoding at a central media relay SBC—for example, between Secure RTP and RTP or between different payload types (codecs).
- The enhanced security/firewall capabilities of a central SBC.
- Fast recovery from Unify OpenScape Voice node failover, particularly in a geographically separated data center configuration. All other effects being equal, the branch SBC can provide faster recovery times. However, if the branches are connected to the data center via the public Internet and VPNs are used, the advantage of the branch SBC is lost.

If a branch office includes a PSTN gateway, there are two possibilities:

- The gateway is only used for PSTN access when the branch is in survivability mode
- The gateway is used for PSTN access during normal mode (as well as in survivability mode).

The configuration of a central SBC must take account of the second possibility and provide the capability to route SIP signaling between the branch gateway and Unify OpenScape Voice via the SBC.

6.9.3 SIP Trunking

The Unify OpenScape Voice server is located in the main office data center; the connection to the SIP Service Provider is achieved using the Internet or the Service Provider WAN. There is no direct connection between Unify OpenScape Voice and the Service Provider's SIP Server. An SBC is used to secure and interwork the connection. The Service Provider uses an SBC and provides a public IP address on the outside of their SBC for the Enterprise to connect to. Use of an SBC on the enterprise side of the SIP trunk is, therefore, not essential to provide connectivity to the Service Provider, but in practice most enterprises consider an SBC indispensable to secure their network. The enterprise SBC also provides the opportunity to configure SIP message header manipulations that may be necessary to satisfy Service Provider specific requirements. A PSTN call would always be:

Subscriber - Unify OpenScape Voice - SBC - Provider - PSTN (or vice versa)

Refer also to the following:

- *Unify OpenScape Voice Interface Manual: Volume 7, SIP Service Providers Interface*
- Section 9.4, “SIP Trunking”

6.9.4 SBC Options

Figure 24, "SBC Deployment Options" shows the SBC deployment options in the enterprise network. Table 27, "SBCs Approved for Use with Unify OpenScape Voice" lists the SBCs that can be used with Unify OpenScape Voice and the scenarios for which each can be used.

In addition to the SBCs listed, the OpenScape Branch provides an integrated SBC, which can be used for SIP trunking:

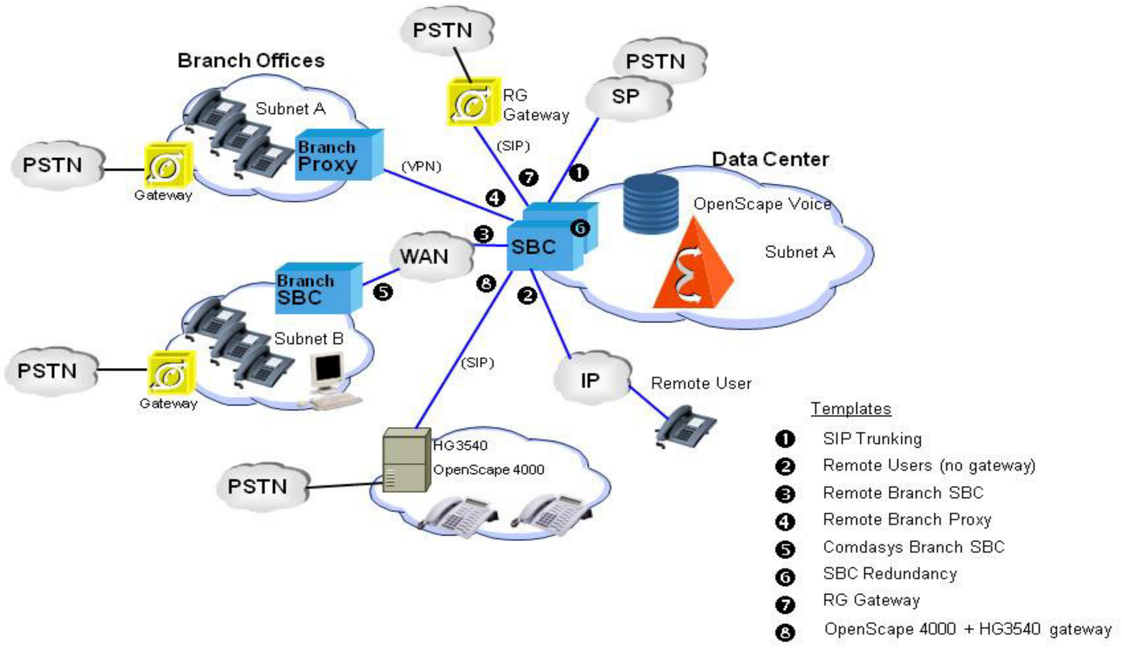


Figure 24 SBC Deployment Options

SBC	Approved Usage				PSR Required ?
	Centralized SBC			Branc h SBC	
	Remote User	Branch Office	SIP Trunking		
OpenScape SBC	•	•	•		No
OpenScape Branch				•	No
Acme Packet Net-Net 3820/4500	•	•	•		Yes

Table 27 SBCs Approved for Use with Unify OpenScape Voice

6.10 VPN Access for Remote Users

VPN access is suitable for remote VoIP access using a SIP soft client, provided that:

- The user has a broadband internet connection.
- The PC has the horsepower to handle the demands of encrypting both signaling and voice packets without significant jitter or delay.
- The VPN gateway (at the customer premises) likewise has the horsepower and capacity to handle the high encrypted packet rate from multiple voice connections, without introducing significant packet loss, jitter, or delay.

Note: Use of an SBC for remote users can be preferable for several reasons. Refer to Section 6.9.1, “Remote User”.

Most SIP telephones do not support VPN access, so this approach tends to limit the customer to soft clients. However, small router boxes—for example, from Linksys—which provide VPN access to the corporate network are now affordable (under $200), and will enable standard SIP phones to connect via VPN to Unify OpenScape Voice.

A VPN router at the branch office can also be used to provide a secure link to an Unify OpenScape Voice system in the main office, as illustrated by Figure 25, "VPN Router at the Branch Office".

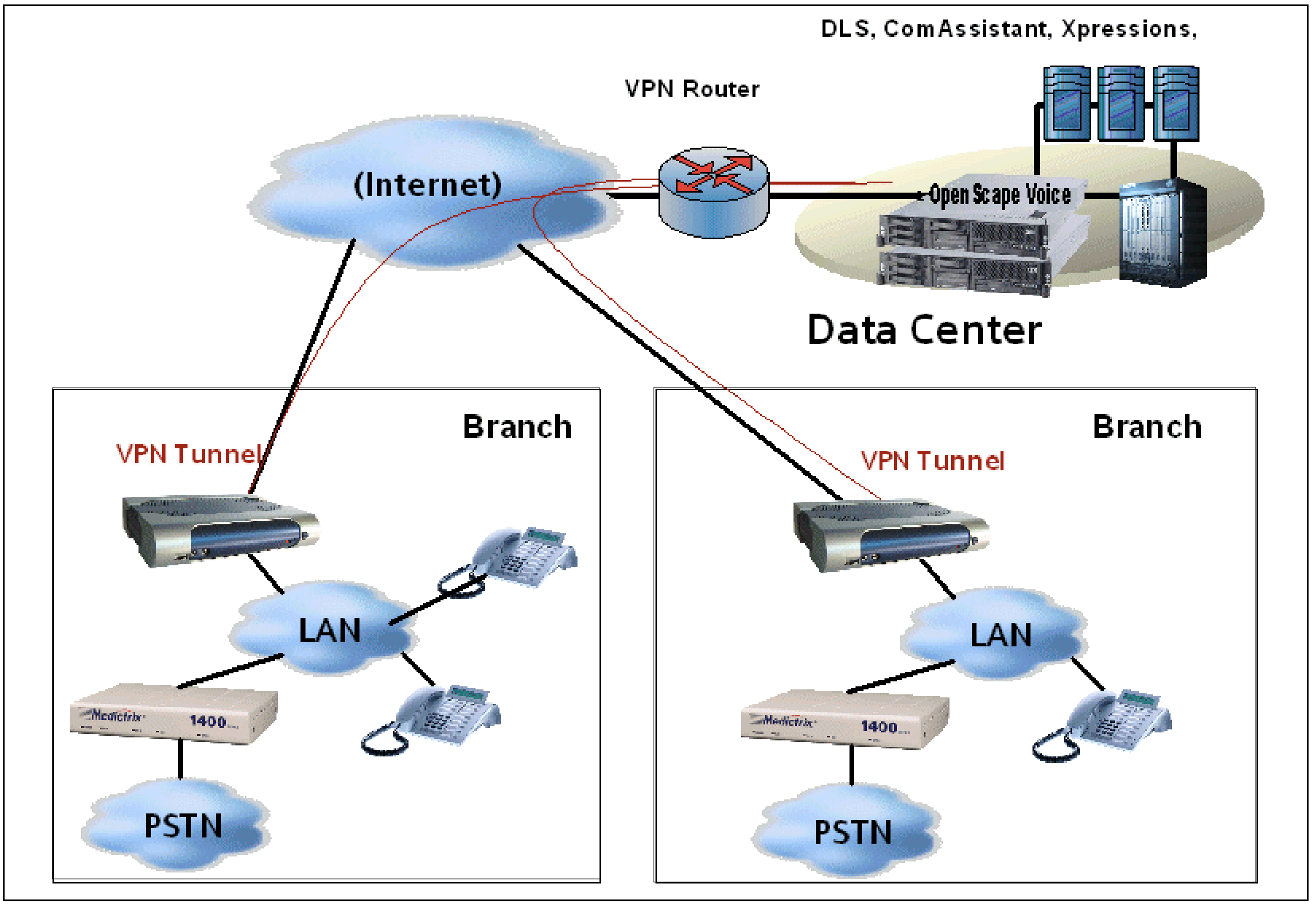


Figure 25 VPN Router at the Branch Office

6.11 External ACD Solutions

Unify OpenScape Voice supports both OpenScape Contact Center and Genesys as external ACD solutions. Because ACD operations typically generate high traffic loads, care must be taken in planning the location of the ACD servers and their respective trunks and agents.

These servers typically use CSTA, SIP, or both to provide announcements and control call flows in Unify OpenScape Voice.

6.11.1 OpenScape Contact Center

The OpenScape Contact Center Integration has the configuration shown in Figure 26. The SIP interface is provided by a Mediatrix gateway. It uses both CSTA and SIP to provide call center services. The

ACD operation makes use of the OpenScape Media Server, as well as special-purpose media server (Interalia in the picture) for ACD-specific announcements.

The OpenScape Contact Center Enterprise Edition can support up to 1500 active agents. The smaller Agile Version supports up to 150 active agents. ProCenter Agile is not currently offered with Unify OpenScape Voice.

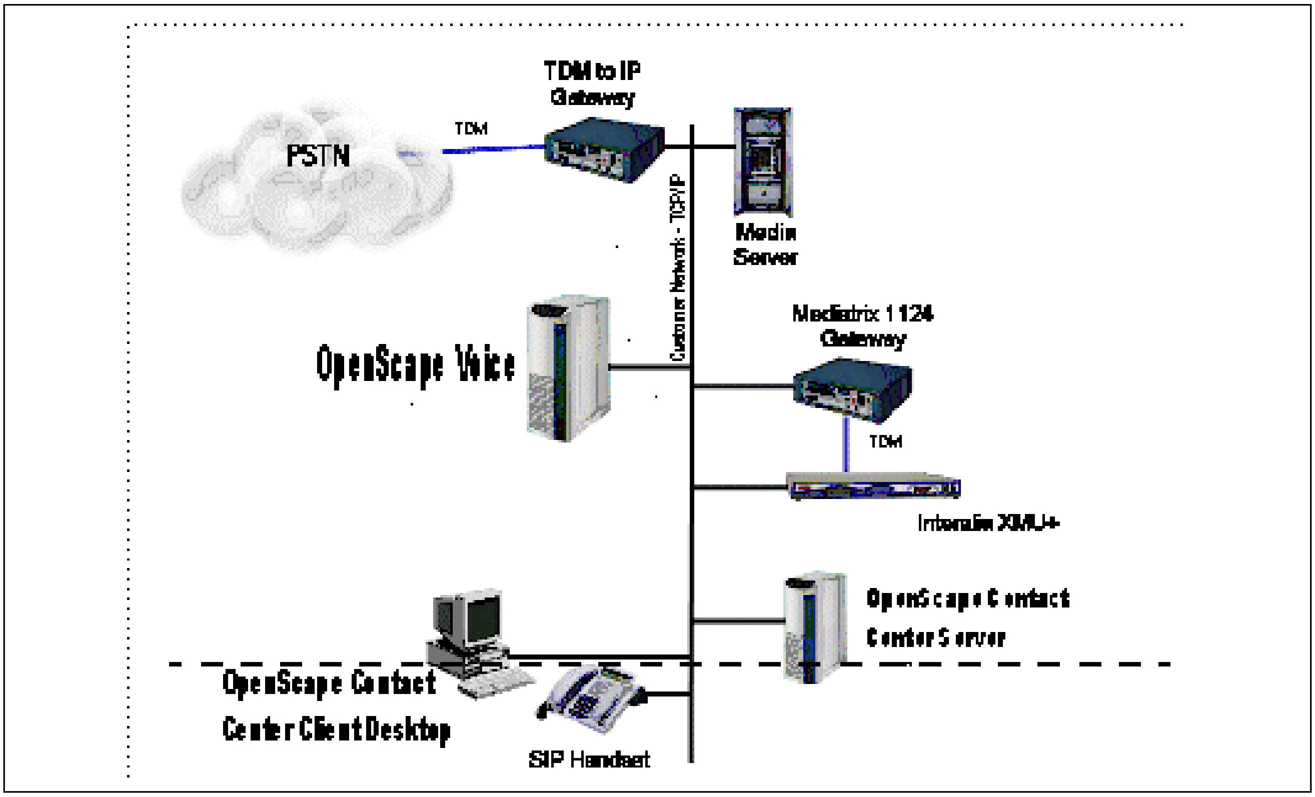


Figure 26 *OpenScape Contact Center External ACD Solution*

The Interalia server provides voice processing services and customized announcements for OpenScape Contact Center. The Mediatrix gateway provides a SIP-to-TDM interface to the Interalia unit, since that unit does not currently support a SIP interface.

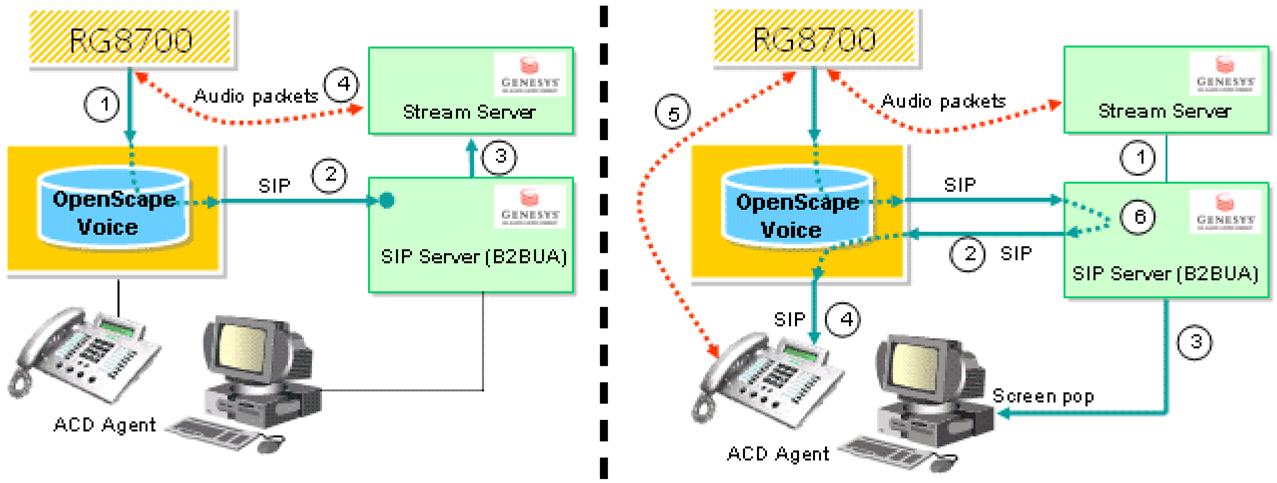
Special care must be taken in computing the resources needed for ACD, since the call rate for each agent is typically much higher than for a typical enterprise users. A call rate of 10 to 20 calls per hour is typical.

6.11.2 Genesys Call Center

The Genesys implementation uses only a SIP interface, as illustrated in Figure 27. In its largest configuration, it can support up to 30,000 agents. However, given the call rate associated with the typical ACD agent, and the manner in which Genesys integrates with Unify OpenScape Voice, the maximum supported configuration will likely be much smaller than this number. Note that if the number of active agents is expected to be greater than 5,000, Unify Engineering should be consulted for a detailed call flow analysis.

Inbound Call – waiting for an

Inbound Call – routed to agent



1. Incoming ACD call is routed to Genesys SIP Server.
2. Genesys SIP server answers the call.
3. SIP server instructs Genesys Stream Server to play an appropriate tone and / or collect digits from caller.
4. Stream Server plays tones / announcements and / or collects digits (e.g. pin number).
5. Call remains in this state until agent is

1. When idle agent is available, SIP Server instructs the stream to give ringback to caller.
2. SIP Server originates second call to the agent.
3. SIP Server sends “screen pop” to agent PC.
4. Agent answers call.
5. Audio connection completed from GW to agent.
6. SIP server remains in the call to monitor status.

Figure 27 Genesys Call Center Architecture

6.12 Other Network Components

6.12.1 Virus Protection

Customers seeking VoIP communication solutions are rightfully concerned about server virus protection and intrusion detection and prevention.

Unify’ software delivery process protects the integrity of software running on the Unify OpenScape Voice server to defend against known viruses, worms, or Trojans. This protection includes incorporation of standard security procedures to be applied during the production, delivery, and installation of Unify OpenScape Voice software, including:

- Scanning of the software package for known viruses
- Digitally signing the scanned software package
- Delivering the scanned software package via trusted channels

Additionally, Unify respects the right of its customers to protect and monitor their networks through the installation and use of third-party application software packages designed to perform such functions. However, Unify' server-based products are designed to meet specific criteria and performance requirements that can be impacted by the installation of such software packages.

Because of this, Unify assumes no responsibility or liability for the performance of the third-party software, nor for any negative impacts caused to Unify network elements specifically or the to network in general.

Refer to the *Unify OpenScape Voice Security Checklist* for more information about virus protection as it applies to Unify OpenScape Voice and its associated servers and gateways. Also, be aware of the *Unify Security Advisory and Security Note Page* https://unify.com/en/support/security-advisories

6.12.2 DHCP Servers

Most large networks use DHCP servers to distribute IP addresses down to desktop clients, such as PCs and laptop computers. It is also a common practice to assign static (permanent) IP addresses to critical servers in the network, which are expected to be in continuous operation.

The advantage of using DHCP are several:

- More efficient use of IP addresses. A computer that is only used part-time only gets an IP address when it is in use, and returns it into a common address pool when it is disconnected or turned off.
- Less manual configuration of each desktop device is required because the DHCP server will automatically configure the device when it is powered up, with critical parameters such as the IP address, net mask, default router address, and DNS server addresses.
- Easier inventory control because it is not necessary to keep track of which IP address was permanently assigned to any specific desktop device. A device that is removed from inventory does not take its IP address with it.

The primary disadvantages of DHCP are:

- The DHCP server is another component that needs to be configured and monitored.
- The server itself is potentially a critical point of network failure. IP addresses are handed out for a period of time (a *lease duration*), and the desktop device must periodically renew the lease. The duration is typically a few hours to a few days. This means that if the DHCP server fails, and the failure is not detected, devices on the network will, one-by-one, stop functioning.

The Unify OpenScape Voice solution does not, in general, require the use of DHCP. Phones and servers can be manually configured and will work properly without the presence of DHCP servers. However, the following features are available only when DHCP is in use:

- The plug-and-play phone installation process, which allows a new SIP phone to be connected to the network and automatically brought into service, requires the use of DHCP. Without DHCP, a portion of the telephone configuration must be done manually via the telephone keys before the phone can be brought into service.
- The E911 auto-location process, which determines the caller’s location based on IP address assignment, and automatically adapts if the phone is moved, requires the use of dynamically assigned IP addresses, and therefore DHCP.

Therefore, the decision to use or not use DHCP for phones and soft clients is part of the architectural design of the VoIP network, and should be based on the customer requirements and existing IP infrastructure design and policies.

6.12.2.1 DHCP Redundancy

If DHCP will be used, the number and placement of DHCP servers must be determined.

If the IP network is already in place, this issue may already have been resolved. However, the designer must keep in mind that when DHCP is being used to supply IP addresses to the telephones, an outage of the DHCP server can spread eventually to the phones themselves and interrupt critical telephone service, if not promptly corrected.

There are several mechanisms for installing resilient DHCP servers.

- **Scope splitting**: The range of IP addresses to be handed out or split in two, with each half being given to a different DHCP server. Since the DHCP request from the client is a broadcast request, both servers will see the request and respond. The first responder will assign an address. The problem with this solution is that it tends to require more IP address space, because each DHCP server needs enough addresses to service the entire DHCP domain.
- **Clustering**: Using a clustering service, such as Windows Advanced Server, the DHCP server can be operated on a server in a way that automatically permits failover to a backup server. The primary issue with this solution is cost.
- **Resilient DHCP service**: The Internet System Consortium offers a DHCP service that automatically communicates with a partner DHCP service, such that each instance can take over for the other. This comes at a cost of additional system configurations.

The standard DHCP lease time must also be determined as part of the design. A longer lease time—for example, one week—puts less load on the DHCP server and gives the system administrator more time to deal with a DHCP server failure, should it occur. But a long lease time means that if a device is abruptly disconnected from the network, its IP address will remain leased, and therefore unavailable for others to use until the lease expires or the device is reconnected again.

Unify SIP phones are designed to begin requesting a lease renewal when the lease is 50% expired, and will continue to request a renewal until one of the following occurs:

- The request is successful.
- The renewal is explicitly rejected by the DHCP server.
- The lease is fully expired.

6.12.2.2 DHCP Location

In many cases the number and location of the DHCP servers will have been determined before the voice network planning begins, but the designer must consider the added impact of an extended DHCP outage. The DHCP service is often collocated with the DNS and (where applicable) WINS services.

DHCP request messages are broadcast messages, so they will not pass through routers unless special provisions are made. There are basically two options:

- Install a DHCP server (or server pair) in each broadcast domain.
- Centralize the DHCP server (or pair) and configure the intervening routers with the DHCP relay service so an endpoint can communicate with a DHCP server on the other side of the routers.

In a distributed deployment of Unify OpenScape Voice, where Unify OpenScape Voice is serving multiple remote locations (branches), the network planner must place a DHCP server (or pair) at each branch, or accept the possibility that an extended WAN outage between the branch and the central DHCP server could result in a telephony outage as well.

6.12.2.3 DHCP Configuration

In addition to the standard configuration parameters that the DHCP server provides, the service can also be configured to provide:

- VLAN ID for the SIP telephones (voice connectivity)
- IP address of the DLS server to enable plug-and-play phone configuration
- Scope definitions to allow emergency caller location based on current location rather than just caller phone number

7 Numbering Plans and Digit Translation

This chapter describes numbering plans and digit translation used within Unify OpenScape Voice.

The numbering plans within Unify OpenScape Voice are based on business groups (BGs). Each subscriber within the Unify OpenScape Voice system is assigned to a BG. Each subscriber is also assigned a unique subscriber ID, which is typically the public DID number of the subscriber if the subscriber is reachable via DID. However, the subscriber ID need not be a number that is dialable from the PSTN.

7.1 Overview

Unify OpenScape Voice is designed to support IP Centrex and multi-tenant service. As such, Unify OpenScape Voice supports multiple BGs, which are similar to closed user groups—a group of users permitted to communicate with each other but can be prevented from calling users outside the group—and multiple numbering plans.

Each business group can be assigned one or more unique numbering plans. In addition, there is a shared global E.164 numbering plan which can be used for access to and from resources—for example, gateways or peer servers in the network—that may be shared by multiple BGs.

All numbering plans and feature assignments are managed by Unify OpenScape Voice Assistant. With Unify OpenScape Voice Assistant, the administrator defines:

- PSTN number blocks that will be serviced by this Unify OpenScape Voice server (these are the subscriber IDs defined and used within this Unify OpenScape Voice switch)
- Gateways and routes to the PSTN
- The mapping of PSTN numbers to BGs and BG subscribers.
- Routes to shared resources like the media server, or peer switches in the VoIP network
- BGs and BG numbering plans
- Individual subscriber endpoints (SIP phones)
- Feature access codes
- Feature authorizations for each subscriber
- Hunt groups, pickup groups, and keyset arrangements

All BGs, features, and numbering plans can also be managed by the Unify OpenScape Voice command line interface (CLI), which is a console based text-mode interface. It includes an expert mode which allows command line input from a predefined batch (text) file, for quick input of large amounts of data.

7.2 Numbering Plan Types

A **closed numbering plan** is one in which the number dialed to reach a given party is always the same, regardless of where in the network the caller is located. In the enterprise environment, the extension dialing plans used within a single switch or in a small private network consisting of several switches are examples of closed numbering plans.

An **open numbering plan** is one in which the number dialed to reach the desired party may be different, depending on the location of the caller. In the enterprise environment, private networks typically use location codes to implement an open numbering plan.

Unify OpenScape Voice supports both closed and open numbering plans.

An **implicit numbering network** is one in which the type of number (private, public, local, national, international) passed between the servers must be *deduced* entirely from the digit string itself. In an implicit numbering network, the number type is often signaled in the form of prefix digits (for example, 9 for local, 91 for national, 9011 for international, 8 for private). The signaling between originating phone and the originating switch and server is always “implicit.”

An **explicit numbering network** is one in which the type of number (private, public, local, national, international) is passed explicitly between the servers in the form of separate signaling parameters. In an explicit numbering network, the call setup message typically carries NPI (numbering plan identifier) and TON (type of number) parameters, which guide the receiving switch in interpreting the dialed digit string. In the administration interfaces, the administrator will see NPI and TON referred to as NOA (nature of address).

Unify OpenScape Voice supports both implicit and explicit numbering. However, the SIP protocol used in most switch-to-switch communication currently does not support explicit numbering (it does not support passing of the NPI and TON parameters). SIP-Q does support explicit numbering, and is the required signaling protocol for IP connections of Unify OpenScape Voice to the OpenScape 4000 and to other Unify OpenScape Voice systems.

Block dialing is a variation of dialing where the originating endpoint transmits all of the digits for the destination at one time, in single message or command, to the originating switch. The alternative is digit-by-digit dialing, which is customary in most public wireline networks. In digit-by-digit operation, each digit is transmitted to the originating switch as the user dials it. DTMF and rotary phones operate in this fashion. Newer networks, such as the public cellular networks and VoIP networks use block dialing.

Historically, in an open numbering plan and open dialing plan arrangement, the originating switch (where the caller is connected) might not know how many digits are needed to reach a given destination, so the system may rely on interdigit timeouts or use of a terminator digit (#) to detect the end of dialing by the caller. Unify OpenScape Voice and its endpoints support interdigit timing and the use of a terminating digit, but because SIP endpoints are block dialing devices, use of these special mechanisms is not required in most cases.

Overlapped sending is the practice by which one switch begins sending digits to the next switch before the user has completed dialing. SIP does not support overlapped sending. Likewise, Unify OpenScape Voice does not support overlapped sending.

7.3 Business Group Creation

The following is a broad overview of the steps required to create a business group and its necessary elements using the Unify OpenScape Voice Assistant tool:

1. The administrator defines one or more blocks of E.164 numbers for use by subscribers. A given subscriber may or may not be reachable from the PSTN via a personal DID number. Regardless, every subscriber must have a number within the E.164 numbering plan. E.164 is the ITU-T document which defines the international public telecommunication numbering plan used in the PSTN.

2. After the E.164 number blocks are defined, the administrator defines at least one BG. Every subscriber line must be assigned to one (and only one) BG.

3. The administrator assigns each BG a default (common) numbering plan. The number plan must be given a name before the BG is defined, so that the assignment of the numbering plan can be made as the BG is created. Whereas the global E.164 numbering plan can be used by any number of BGs, a BG-specific numbering plan cannot be shared between BGs.

4. If desired, the administrator can define additional unique numbering plans for the group. A single BG can utilize multiple numbering plans.

5. The administrator defines at least one feature profile, which contains the set of default features that each subscriber will be given.

6. After the BG, its associated numbering plan(s), and its associated feature profile(s) have been defined and selected, subscribers (formerly called business group lines [BGLs]) can be created.

All of the steps above can be executed in a single operation using the Create New BG wizard of Unify OpenScape Voice Assistant (on the Quick Tasks menu).

Each subscriber BGL is given a subscriber ID, which is the E.164 number assigned to this endpoint. In the US, this is typically the 10 or 11-digit PSTN number of the endpoint (for example 15619231001). Even if it is not callable from the public network, it must have such a service or subscriber ID. If a BGL is not callable from the public network, it will be marked in such a way that its subscriber ID will not be reported to the public network as a caller ID, since it is not a valid caller ID. Instead, a substitute number, such as departmental main number, will be transmitted, or the caller ID can be signaled as unavailable.

The network designer has the option of defining subscriber IDs with or without the country code:

- If the country code is included in the subscriber ID—for example, 15619231000— the number type is by definition “international.”
- If the country code is not included in the subscriber ID—for example, 5619231000— the number type is “national.”

If an Unify OpenScape Voice system is serving subscribers in a single country, inclusion of the country code is optional. If the Unify OpenScape Voice system is serving subscribers in more than one country, including the country code eliminates potential number ambiguities.

Unify recommends defining subscriber identities in the international form, with the country code as part of the subscriber ID (for example, 1-561-923-1234). In a private network involving multiple switches, the subscriber numbering plan needs to be consistent network-wide.

Through the subsequent numbering plan configuration steps, the administrator can make it possible to reach this endpoint through any of the standard dialing forms:

- Extension number (31001)

- Location code plus extension number (923-1001 or abc-1001)
- Private network barrier code plus location code plus extension number (8-abc-1001)
- Full PSTN number (with or without the country code)

However, the identity of the subscriber is defined by the Subscriber ID (also known as the *Service ID* [E.164 number]), and that identity must be unique within the system. Two subscribers (in different BGs) may have the same extension number without any confusion, but two subscribers cannot have the same Service ID (E.164 number) even if they are in different BGs or on different Unify OpenScape Voice switches.

Unify OpenScape Voice supports the concept of subscriber groups (within a business group) being physically scattered in locations (sites) that are physically remote from the Unify OpenScape Voice system, in different time zones, or even across national borders. For this reason, a BG can have more than one numbering plan.

Each subscriber within a BG may be assigned to a specific numbering plan, which overrides the default (common) numbering plan assigned to the BG itself. This provides the preferred mechanism for the definition of site-specific dialing routing, when all the subscribers at multiple sites are within one BG.

If the administrator decides that a BG should have only one numbering and routing plan, the unique routing requirements of a specific site can also be accomplished by using routing area and class of service assignments.

7.4 Extension Numbers

As most readers know, extension numbers are short numbers used for calling within a BG. In most networks, extension numbers are 2 to 7 digits long, and are typically (but not always) a right-most subset of the public number of the phone in question.

Unify OpenScape Voice supports extension numbers up to 7 digits in length. Through proper setup of the BG numbering plans and the E.164 numbering plan, extension dialing can be provided:

- Within a BG
- Between BGs

- Between BGs on different Unify OpenScape Voice switches

Note: This type of extension dialing is not commonly used.

The form of number displayed as caller ID or connected party ID is controlled by a number of configurable options and by the number modification feature described in Section 7.10.3, “Number Modification”.

7.5 Location Codes and Private Numbering Plans

As soon as an extension number is assigned to a subscriber, the administrator has begun the process of creating a private numbering (and dialing) plan. The most basic form of a private numbering plan (PNP) is *extension dialing*. A subscriber with an extension number usually has two identities:

- A public identity (the subscriber ID, which is usually a public DID number)
- A private identity (the extension number) that can be dialed within the business group

Note: A subscriber can also be created as private only, which means that the subscriber is not reachable from public network destinations. This type of subscriber is created by ensuring that the External DN flag is unchecked.

Unify OpenScape Voice also supports the concept of Level 0, 1, and 2 private numbering plans, including location codes. Just as public numbers have multiple forms (with or without the country code, with or without the city code/area code, and so on), private numbers also have multiple forms.

An L0 (level 0) private number is the private network equivalent of a local subscriber number in the public network; in the US, this is a 7-digit number. An L1 private number is the private network equivalent of a national number in the public network. An L2 private number is the private network equivalent of an international number in the public network.

Using Unify OpenScape Voice Assistant, the administrator can create an L0, L1, or L2 private number by assigning a location code to each local BG numbering plan, and repeating the process for each Unify OpenScape Voice switch in the private network.

Unify OpenScape Voice Assistant allows the administrator to define the L0, L1, and L2 forms of the PNP location code digits. For a given BG numbering plan, Unify OpenScape Voice Assistant allows the administrator to define the:

- Location code digit string (up to 14 digits)
- Number of digits in the L2 part of the location code
- Number of digits in the L1 part of the location code
- Number of digits in the L0 part of the location code

- Number of skip digits (number of digits in the location code which must be deleted to reach the first digit of the PNP extension number)

The network designer must decide whether the network requires the use of location codes, and if so, how many levels. Few networks require more than L0 location codes.

An example location code definition for a Level 3 PNP network might look like the one shown in Table 28.

Parameter	Value	Comment/Note
Location code digit string	1408492	This is a level 3 PNP location code.
L0 length	3	492
L1 length	3	408
L2 length	1	1
Digits to skip	6	The 2 in 492 is part of the extension number.

Table 28 Location Code—Level 3 Example

An example location code definition for a L0 PNP network might look like the one shown in Table 29.

Parameter	Valu e	Comment/Note
Location code digit string	994	This is a level 1 PNP location code.
L0 length	3	994
L1 length	0	No level 1 digits.
L2 length	0	No level 2 digits.
Digits to skip	2	The 4 in 994 is part of the extension number.

Table 29 Location Code—L0 Example

A network designer needs to know when to define and use location codes. There are two basic instances:

- To resolve numbering conflicts between sites. If two sites within the network want to call each other, but both have extension numbers in the 1xxx block, the location code provides a way to remove the ambiguity between the numbers. Both groups can keep their extension numbers and still call each other.

- In large networks, to provide additional subscriber numbering capacity without forcing subscribers to dial 5, 6, or 7 digits on every internal call.

When a BG numbering plan is assigned a location code, other BG numbering plans can route calls to that location code as a destination (destination type “home location” in Assistant).

Location codes are defined and assigned at the BG numbering plan level. This means that each BG numbering plan can have one or more unique location codes.

Creating a location code does not put it fully into use. After the location code is defined, it must be assigned to one or more extension number blocks, using the Assistant BG “Extensions” screen. The location code definition instructs the translation logic how to parse an L1, L2, or L3 private number to determine the private extension number. The extension block definition then links the location code and extension number block (for example, 1xxx) to the appropriate subscriber IDs, giving the system the ability to translate a subscriber ID into a private number, and vice versa.

It is worth noting that the main function of the location code definitions and extension block definitions is *not* call routing; complex multilevel private dialing plans can be created without using these tables. The number type of the dialed destination number is determined and set in the prefix access code tables of the appropriate numbering plan. The primary function of the location and extension tables is to permit proper handling and display of caller ID information.

The number modification tables (Section 7.10.3, “Number Modification”) are used to send a caller ID in proper format (E.164 or private network format) to a SIP destination, such as a SIP phone or SIP gateway, and will use the location code information as appropriate, when the caller is a BG subscriber.

Over SIP-Q, both the fully qualified public and private number are transmitted as caller ID. The receiving switch or gateway determines which number to display or forward.

7.6 Overlapping Location Code and Extension Digits

The location code definition tables, as described in the previous section, permit the designer to create networks in which location code digits and extension number may overlap. This may be of use if the designer wants to impose a standard-length location code on all locations, including some larger locations.

For example, in the number 492-1001, the 2 may be the leading digit of the extension number dialed within the BG, and also the last digit of the Level 0 location code, which is dialed by callers in a different BG.

7.7 On-Net Versus Off-Net Traffic

On-net traffic consists of calls where the source, destination, and call path are on the private SIP network, both within a BG (intra-group) and between BGs (inter-group).

Off-net traffic consists of calls where either the source, destination, or transmission facility is outside the private corporate network.

7.8 Simple Numbering Plan Setup with Unify OpenScape Voice Assistant

This section describes the basic setup of a single node numbering plan utilizing Unify OpenScape Voice Assistant. Note that all of the steps described here can also be accomplished using the Unify OpenScape Voice CLI and batch file interface.

The Unify OpenScape Voice Assistant graphical user interface (GUI) has a navigation bar near the top with five options or activity categories:

- **General:** Displays switch status and provides access to available downloads
- **Administration:** Displays various data tables on the left side of the display, so they can be selected, viewed, and modified if necessary.
- **Business Group**: Displays tables associated with specific business groups, so that they can be selected, viewed, and modified if necessary.
- **Global Translation and Routing:** Displays tables associated with the global (E.164) numbering plan, which may be used by all business groups, so that they can be selected, viewed, and modified if necessary.
- **Maintenance:** Displays various alarm, fault, and activity logs so that they can be selected, viewed, and cleared.

7.8.1 Home Directory Numbers

The first logical step is the definition of the base E.164 numbering ranges used by the system, effectively defining the public number blocks which will be used to reach the subscribers on the system. These are sometimes referred to as *home DNs*. This step consists of the following tasks:

1. The central office codes of the public switches which provide trunks to Unify OpenScape Voice need to be defined. For example, an Unify OpenScape Voice system may have public DID numbers in the ranges 408-492-xxxx and 561-923-xxxx. The central office codes 408492 and 561923 would be defined in this case.
2. Next, the range of endpoint numbers (DID number blocks) which belong to Unify OpenScape Voice, within each office code, need to be defined. For example, the number block 1000-2999 within the office code 561923 may be used by Unify OpenScape Voice subscribers. These number blocks are traditionally called DID number blocks.
3. Some endpoints on Unify OpenScape Voice may not have publicly dialable DID numbers. Regardless, they must be defined before they can be configured. This can be done by defining a fictitious office code or number block for these endpoints.
4. When defining the office codes, the administrator has the option of including (or not) the country code as part of the office code. However, all office codes should be defined in a consistent manner (with or without the country code) and all are subject to the number length constraints.

These tasks can be done at one time using the Quick Add Business Group wizard (under the Business Group option of Unify OpenScape Voice Assistant), or by using the Office Codes screen (under Global Translation and Routing).

7.8.2 Routing Area and Classes of Service Definition

Use of routing area (RA) and class of service (COS) definitions are optional. Both parameters are used in the call routing process, along with the dialed digits, and both are defined under Administration on the Unify OpenScape Voice Assistant navigation bar. Routing areas are some times referred to as *rate areas*, a term commonly used in the public network.

Each subscriber endpoint can be assigned a class of service and routing area. The routing area is normally used indicate the physical location of the endpoint, especially within installations where Unify OpenScape Voice subscribers are located at multiple geographic sites.

Class of service can be used to indicate the endpoint device type—for example, a fax-only device, an emergency phone, or a terminate-only device—or to indicate the department, priority, or importance of the caller.

By using these two values, it is possible to create location-specific (source-based) routing configurations, department-specific, and/or prioritized call routing arrangements within a single Unify OpenScape Voice switch.

Routing areas and classes of service are just user-defined readable category names which can be used in the routing process. The string name is only used for ease of administration and viewing. Caller class of service and routing area, along with the translated digits, are three parameters taken into account during the call routing, destination, and gateway selection process.

7.8.3 Making the Home Directory Numbers Accessible from the Global Numbering Plan

In a configuration with multiple business groups, shared resources—for example, shared PSTN gateways and application servers—are commonly assigned to the global numbering plan. In order for these resources to call members of the defined business group(s), appropriate entries must be made in the global numbering plan prefix access code table and E.164 code table.

The global prefix access code table and E.164 code table will normally be configured automatically by the Quick Add Business Group wizard.

7.8.4 Global Numbering Prefix Access Code Table

In order for a dialed number from the global numbering plan to be routed, it must have a matching entry in the prefix access code (PAC) table controlled via Unify OpenScape Voice Assistant. If Unify OpenScape Voice has subscribers in the public number block 1-561-923-xxxx, an appropriate entry needs to be made in the PAC table. This will normally be done by the Quick Add Business Group wizard, but in some cases it may need to be done manually.

Within Unify OpenScape Voice Assistant, the administrator must make an appropriate entry in the PAC table. For this example, assume that home DN subscribers are defined in international form (including the country code – 1561923xxxx) and that the numbers supplied by gateway are in form (561923xxxx). The appropriate entry in the PAC table consists of the following items:

- **Prefix Access Code:** As many digits as appropriate to define the dialed number block (for example, 561923).

- **Directory Number minimum and maximum length:** Dialed number length limits (both 10 in this example).
- **Digit Position:** number of prefix digits to delete before proceeding to the next translation step (in the example, 0).
- **Digits to Insert:** Enter prefix digits to add to the dialed number before proceeding to the next translation step. These digits are added after the delete operation specified by the digit position is executed. In this example, the digit 1 must be added to translate the number supplied by the gateway into the form used internally.
- **Nature of Address:** Indicates the type of the resulting number (after the delete and insert steps are completed). Possible values include (national, international, PNP level 0, and so on. In this example, home DN numbers are in international form, so the correct selection is “international.”
- **Destination Type:** Select “none” to indicate the resulting digit string will be passed to the E.164 code table for further analysis.
- **Destination Name:** Left blank in this case, since destination type is none.

It is possible (even common) that different gateways will present dialed numbers differently, so there may be a PAC table entry for (in this example) 1561923, 561923, and 8923 – all of which lead to the same entry in the E.164 code table (Section 7.8.4.1, “E.164 Code Table Entries”) through the PAC digit translation mechanism described above.

Generally SIP gateways do not supply a destination number “type,” such as national or international, in an incoming call seizure. For that reason, the PAC table is used to evaluate the number and (usually) assign a valid type before the number is forwarded to the E.164 code table for routing. SIP-Q gateways may supply a number type in addition to the number itself. If the incoming number type is supplied, and it is any valid value other than “unknown”, the number does not be passed through the PAC table, and instead goes directly to the E.164 code table for routing.

7.8.4.1 E.164 Code Table Entries

By selecting “none” in the destination type field of the PAC access code table entry (Section 7.8.4, “Global Numbering Prefix Access Code Table”), the administrator is indicating that the number should be passed to the E.164 code table for the next routing step. Therefore, an appropriate entry is required in this table as well.

Normally, the necessary entries in this table will be set up by the Quick Add Business Group wizard, but occasionally it may need to be done manually.

This table provides the primary routing mechanism for the global numbering plan, by defining E.164 number blocks and the “destinations” to which they should be routed.

To add this entry, the administrator goes to the E.164 codes folder under Global Translation and Routing, and inputs the appropriate values, as follows:

- **Destination Code**: These are the leading digits of an E.164 number (1561923 would be appropriate for the example of the previous section).
- **Nature of Address**: Must match the nature of address specified in the PAC table entry (previous section). If the PAC table translates the dialed number into an “international” number form, then the correct choice here is “international.” If the office code consists of 6 digits containing only area code and office code, the number type should be set to NATIONAL, which means area code and office code without the country code. If the office code includes the country code (for example, 1561923) then the number type should be INTERNATIONAL.
- **Traffic Type**: Some calls may need to be marked as traffic of a special type (for example, emergency call). The type is normally set to NONE, which means this entry applies to all traffic types. If a value other than NONE is selected here, the call is assigned that traffic type, which can affect later routing decisions.
- **Class of Service**: Normally left blank for entries related to inbound calls. If the table entry were being used to define outbound routing for a particular subscriber class of service, it would be entered here. A blank in this field means this entry applies to all classes of service.
- **Routing Area**: Normally left blank for entries related to inbound calls. If the table entry were being used to define outbound routing for a particular routing area, it would be entered here. A blank in this field means this entry applies to all routing areas.
- **Destination Type:** For an entry related to inbound calls, this will usually be “Home DN”, meaning this number terminates on an Unify OpenScape Voice subscriber, rather than being routed to another switch via a gateway.
- **Destination Name**: Select from the list of options the appropriate home DN number office code as defined in Section 7.8.3, “Making the Home Directory Numbers Accessible from the Global Numbering Plan”. If the

destination type is set to “Home DN” the destination name must match one of the home DN office codes previously defined.

Note: Each home DN office code is a named destination in the system. Internally, the destination is a table containing all the endpoints of this office code that have been defined within this switch, using Unify OpenScape Voice Assistant.

7.8.5 Creating A Business Group and BG Numbering Plan

Before subscriber lines (endpoints) can be created, the administrator must define at least one BG, and a BG must have a numbering plan. So the next logical step is the definition of a BG numbering plan.

The Quick Add Business Group wizard will take care of this automatically. If for some reason the administrator needs to create a business group manually, this can be done from the Business Group selection on the navigation bar.

When a BG is created, a BG numbering plan is automatically created and assigned by Unify OpenScape Voice Assistant. If the BG is named XYZ, the corresponding numbering plan will be named NP_XYZ. After the BG numbering plan is defined (or at least named), the BG itself can be created:

- A name string – for example BG1 or “sales force.” Maximum 16 characters and may contain spaces.
- A remark – a text description of the group.
- Display number – a number that is displayed as caller ID when a BG endpoint which does not have a dialable public number makes an off-net (public network) call. This is typically the attendant or must-answer number for the group.
- Default Office Code – the global number block from which subscribers in this BG will be assigned by default.

7.8.6 Creating A Feature Profile

When a BG is created via the wizard, Unify OpenScape Voice Assistant also creates a default feature profile for members of the group. If the BG is named *xyz*, the feature profile will be named *FP_xyz*. The administrator can create additional feature profiles for the BG if needed.

A feature profile is a named set of feature permissions which can be conveniently assigned to a subscriber. It is similar in concept to a OpenScape 4000 feature class of service.

7.8.7 Creating Subscribers

Now that a BG, BG numbering plan, and feature profile have been created, either manually or using the wizard, the first subscibers can be created. Under the Business Group category on the Unify OpenScape Voice Assistant navigation bar, select the Members → Subscribers tab on the left. There the administrator can see a list of existing subscribers, then click the Add button to a add new subscriber (BGL).

7.8.7.1 General Tab

On the General tab, the fields which must be filled in to define the BGL in Unify OpenScape Voice Assistant include the following:

- The numbering plan assigned to this BGL. The default numbering plan of the BG will be displayed here, but the administrator can override this value with another numbering plan ID assigned to the BG.
- A remark (text) which is provided for the convenience of the administrator.
- Office code – this will be one of the home DN office codes defined earlier as part of the global numbering plan.
- Extension number – this will be a number in the range defined for the home DN code as part of the global numbering plan. The administrator can select from a drop down list of available extension numbers, by clicking the ellipses (…) button. The office code + extension number make up the subscriber ID, which is the unique system wide number by which the BGL is identified.
- Internal name – the name displayed as caller name when the subscriber makes a call within the BG.

- External name – the name displayed as caller name when the subscriber makes a call outside the BG (to another BG or to the PSTN, for example).
- Pickup group membership – optional. The administrator can add the new BGL to an already defined pickup group.
- Class of service, routing area, and calling location – all optional. In each case the administrator can chose from the list of already defined values. Calling location is used in some environments (mainly in Europe) for emergency calling processing.

7.8.7.2 Other Tabs

There are a number of tabs on the BGL definition screen. On most of these tabs, the default values are sufficient for a basic BGL definition.

- **User tab:** The administrator can indicate which Unify OpenScape Voice Assistant users can administer this BGL in the future.
- **Attributes tabs:** The administrator can specify various attributes necessary to certain Unify OpenScape Voice feature operation—for example, whether SRTP support is enabled for this subscriber.
- **SIP tab**: The administrator can set the device registration options, SIP signalling transport type, security, and survivability options. For registration:
  - Name – this is the value by which the phone registers with the switch. It is normally set to the subscriber ID (that is – the phone number).
  - Type – static (permanent) or dynamic registration. Phones normally use dynamic registration.
  - Transport protocol – for new installations, TCP.
  - SIP phone—among other tasks, the administrator can configure executive/assistant group information.
  - Security—if SIP authentication has been enabled, these fields are mandatory.
- **Advanced tab:** The administrator can define parameters such as department membership, time zone in which the phone resides, and PIN (authorization) code. On this tab the administrator indicates whether the BGL is an actual SIP phone, or a virtual number (profile only – a number without a physical device), and whether the BGL number is an external directory number (dialable

from the PSTN via DID service). A profile only BGL can be used, for example, as the pilot number for a hunt group, or as a permanently forwarded line.

- **Hunt Groups tab:** The administrator can add the new BGL to an already defined hunt group.
- **Keyset tab:** The administrator can define whether this BGL will be a standard phone (keyset type NONE) or a keyset (keyset type PRIMARY) or a phantom line.
- **Services tab:** The administrator can select the feature profile for the BGL and customize the feature settings.

7.8.8 Configuring the Business Group Numbering Plan

In order permit extension number calling between members of a BG, the BG numbering plan should be configured with the appropriate:

- Prefix access code(s)
- New destination code table entries
- Extension table entries

In the basic scenario where there is only one customer location (site), the common BG numbering plan defined above (for example, using the Quick Add Business Group wizard) will suffice as the one and only BG numbering plan.

If there are multiple locations, and the planner has decided to accommodate site specific routing by providing multiple numbering plans for the BG, the common BG numbering plan has a reduced function. It is typically used as follows, in this case:

- To define the numerous feature access codes (* and # codes) that will be common to all sites
- To provide access to common resources within the BG, such as PSTN gateways that can be accessed by all sites for long distance calls

The scenario described here assumes a single BG numbering plan is sufficient.

7.8.8.1 Business Group Prefix Access Code Table

Each numbering plan has an associated prefix access code table. This is a table of leading digit patterns, where for each digit leading pattern (prefix) the administrator sets a minimum and maximum number of digits required with this prefix, prior to the next step in the translation process. No feature or destination can be dialed by a BG member without an entry in a prefix access code table. For each new entry in the prefix code table, the administrator must enter the following:

- One or more prefix digits
- A minimum and maximum number length. The same prefix digits may show up twice in the table, with different non-overlapping minimum and maximum lengths.
- Digit position – the number of prefix digits to delete prior to the next translation step.
- Digits to insert – a string of 0 or more digits to be inserted. These digits are added after the delete operation specified by the digit position is executed.
- Trailing digit position – Any digits beyond this position are deleted.
- Prefix type – the type of the resulting digit string, from a drop-down list. Common choices are:
  - Vertical service: indicating a feature access code. If this option is selected, the destination type (below) cannot be NONE.
  - Extension dialing: internal extension number prefix
  - On-net access prefix – for calls within the private network
  - Off-net access prefix– for calls to the PSTN
  - Attendant: attendant access code
  - Speed calling prefix.
  - Invalid code – a digit prefix that must be blocked.
- Nature of address – indicates the NOA value to be associated with the resulting number, after digit deletion and insertion is complete. The assigned NOA value can be used as a factor in subsequent routing and translation steps. Values selectable from a drop-down list depend on the prefix type selection:
  - If the prefix type is “vertical service”, “invalid code”, or “speed calling” this field is unused and set to Unknown.
  - If the prefix type is “extension dialing”, the options are Unknown and PNP Extension (PNP extension being the normal case).

  - If the prefix type is “on-net” or “off-net”, all options are valid (Unknown, Subscriber, National, International, PNP level 0, level1, or level 2).

- Destination type. Options include:
  - E.164 destination – output of translation is fed to the E.164 translation tables defined via Global Numbering Plan section of Unify OpenScape Voice Assistant
  - Service – output goes to a “service destination” which is one of the predefined system features (like call forward activation). The service destination must be named below
  - Destination – call is routed directly to a named destination, which must have been defined already in the routing database. A named destination is typically a gateway.
  - None – destination cannot be determined yet. The results from the prefix access code translation are passed to the destination table of this numbering plan.
- Destination name – is the name string of a service (feature), an announcement name (in the case of an invalid code), or a gateway (or other destination) that has already been defined.

All digit analysis and routing for BG lines starts with the BG prefix access code table. To allow BG lines to call each other using the E.164 dialing—for example, by dialing the full subscriber ID— an entry must be added to the PAC table. One or more separate entries are required to allow BG lines to call each other by dialing extension numbers.

Assume, as before, that subscriber IDs are defined in international number format (with country code), and the home DN block for the BG is 1561923xxxx, and the BG has 5-digit extension numbers in the range 31xxx. To allow subscribers to call each other by their 11-digit E.164 number, the fields are filled in as shown in Table 30.

Field	Input Value	Comment
Digits	1561923	
Minimum length	11	
Maximum length	11	
Digit Position	6	Delete 6 digits
Digits to Insert		Leave blank
Prefix Type	Extension Dialing	
Nature of Address	PNP Extension	Only valid choice
Destination Type	None	Go to BG destination code table

Table 30 Prefix Access Code Table Entries Permitting E.164 Dialing

To allow the BG lines to call each other by their extension numbers, the administrator must create a second PAC table entry. The fields are filled in as shown in Table 31.

Field	Input Value	Comment
Digits	31	
Minimum length	5	
Maximum length	5	
Digit Position	0	No digits deleted
Digits to Insert		Leave blank
Prefix Type	Extension Dialing	
Nature of Address	PNP Extension	Only valid choice
Destination Type	None	Go to BG destination code table

Table 31 Prefix Access Code Table Entries Permitting Extension Dialing

At this point, the administrator has created two prefix access codes to allow intra-BG calling (31xxx and 1561923xxxx). Both prefix access codes are translated to the same result = 31xxx with nature of address = PNP extension. The resulting numbers are forwarded to the BG destination code table for further analysis.

In systems where there will be multiple business group numbering plans, it is advisable, wherever possible, to organize the numbers so that as many as possible can be handled in a common numbering plan (either the global e.164 numbering plan or the BG common numbering plan as defined in Section 7.11, “Branch Office Numbering Plan Administration”). This conserves both system translation memory, which is a limited resource, and administrative effort.

7.8.8.2 Business Group Destination Code Table

After the prefix access code table analyzes and translates the digits, the destination code table actually routes the call. Continuing the same example above, the administrator should add the entry shown in Table 32 to the destination code table.

Field	Input Value	Comment
Destination Code	31	
Nature of Address	PNP Extension	
Class of Service		leave blank
Traffic Type	None	Do not assign a traffic type
Routing Area		Leave blank
DN Office Code		Leave blank

Table 32 Destination Code Table Entries(Seite 1 von 2)

Field	Input Value	Comment
Destination Type	Home Extension	Go to the Extension table for routing
Destination Name	None	

Table 32 Destination Code Table Entries(Seite 2 von 2)

Repeating, in the destination code table, the destination codes are unique based on:

- Digits
- Nature of address (NOA – note the prefix access code table assigns a NOA to the number)
- Originating routing area (blank means “any”)
- Originating class of service (blank means “any”)

So 31 with NOA= “PNP extension” is distinct from 31 with NOA = subscriber, and so on.

In the destination code table, the destination types are:

- Home Extension – The next translation step uses the BG Extensions table described Section 7.8.8.3, “Business Group Extension Number Table” below.
- Service – The destination is a feature (also known as service destination).
- Destination – The destination is a named destination in the E.164 routing data or the BG routing data.

7.8.8.3 Business Group Extension Number Table

The next step is to add an entry in the BG extensions table. This table has nothing directly to do with defining subscribers. Rather, it is used to define rules that permit Unify OpenScape Voice to convert between extension numbers and fully qualified subscriber IDs. The extension number may be dialed, but the device, identified by its fully qualified subscriber ID, must be located. In Unify OpenScape Voice Assistant, the administrator can go directly from the Destination Code table (previous section) to the Extensions table by clicking the table name on the left, or the Extensions tab near the top right of the display.

To add a range of extensions, the administrator selects the tabs NEW EXT/CREATE EXT to activate the new extension panel. To complete the example started above, a new entry is created with the fields filled in as shown in Table 33.

Field	**Input Value**	**Comment**
Prefix	31	The extension prefix digits
Length	5	length of the extension digits 31xxx
Location Code		Leave blank. Used to assign a PNP location code to this extension block
E.164 prefix	156192 31	Digits to convert extension to subscriber ID (it includes the prefix digits)
Destination Type	Home DN	Destination is in a home DN table
Office Code	156192 3	Pick from the list of home office codes

Table 33 BG Extensions Table Entries

- Extension prefix – this is a leading digit (or digits) that will identify the extension number (range). For example, if all numbers beginning with 31 are extension numbers, then 31 goes in this field. An entry in this table can indicate a single extension or a range of extensions. If the prefix is 4 digits long, and the extension length (next field) is also 4, then this entry is defining a single extension.

- Extension length – must be at least as many digits as the prefix. If extension numbers are beginning with 31 are all 5 digits long, then 5 goes in this field.

- Location code – the PNP location code to which this block of extension numbers belongs, if location codes are in use. Left blank in this example.

- E.164 Prefix – if this table entry is defining a single extension, this is filled in with the E.164 number (subscriber ID) of the endpoint. If this entry is defining a range, this field specifies the prefix digits for the range, including the extension prefix digits of (a), needed to convert the extension number to an E.164 number and subscriber ID recognizable by the home DN table. In this example, for extensions with prefix = 31, the E164 prefix should be 15619231 (yes, it includes the extension prefix).

- Destination type – when defining an extension range, the type is always homeDN (no other option is shown).

- The destination name is a valid entry in the destination table, and is required. In this example it indicates the home DN table associated with this block of extensions (1561923).

Note that although extension numbers are used for routing, in this example, the endpoints are not identified nor are they are directly addressable by their extension numbers. They are defined by their E.164 number (subscriber ID).

At this point, phones should be able to register and make basic intra-BG calls using both the 11-digit public number and the 5-digit extension number forms of dialing.

7.8.8.4 Business Group Location Codes

If the configuration will support location code dialing, this is an appropriate time to define the location code(s) for the BG numbering plan, as discussed in Section 7.5, “Location Codes and Private Numbering Plans”.

7.8.9 Routing Calls to the PSTN

The next logical step is to consider outbound and external routing. The general steps (not necessarily in this order) are:

1. Define destinations – these are places the subscriber wants to reach using this numbering plan. Destinations can be logical or physical, general or very specific (for example, Chicago or Gateway3, International or Germany, US or Florida or Jacksonville).
2. Define the server endpoints (gatekeepers, gateways, media servers, SIP endpoints) that the system will route calls to in order to, reach these destinations.
3. Create routes to these endpoints.
4. Define the numbering plan entries to allow the destinations to be dialable.

7.8.9.1 Defining A SIP Gateway to the PSTN

There are a minimum of two steps to defining a SIP gateway to the PSTN.

1. Create a SIP endpoint profile.
2. Create the SIP gateway endpoint (server).

Creating An Endpoint Profile

A SIP gateway is an endpoint. In order to create a SIP endpoint, it must be assigned an existing endpoint profile. An endpoint profile is created under a specific numbering plan, and belongs to that numbering plan. The administrator can create an endpoint profile under the global numbering plan, or under a numbering plan of a business group that has been created solely to contain the gateways to the PSTN, and that does not include any users.

The profile is then assigned to one or more specific gateway endpoints, and will determine which numbering plan is used to evaluated the digits on inbound calls from those gateways.

The administrator will find the Endpoint Profile list on the left side of the Unify OpenScape Voice Assistant window, when either of the following paths are selected from the navigation bar at the top:

- Global Translation and Routing → Endpoint Management → Endpoint Profiles
- Business Group → Profiles

When initially created, the only parameter required for an endpoint profile is the profile name. Everything else can be defaulted, in the normal case.

Creating the SIP Gateway Endpoint

SIP entities in the network are categorized as either subscribers or endpoints. A SIP subscriber has a subscriber ID (phone number) and requires a subscriber license. A SIP endpoint has a name, rather than a phone number, and does not require a license. Endpoints are typically gateways or peer SIP servers in the network. Subscriber features are generally not provided to SIP endpoints.

Comparable to the endpoint profile, the administrator can create an endpoint under the global numbering plan, or under a numbering plan of a business group that has been created solely to contain the gateways to the PSTN, and that does not include any users.

The administrator will find the Endpoint list on the left side of the Unify OpenScape Voice Assistant window, when either of the following paths are selected from the navigation bar at the top:

- Global Translation and Routing → Endpoint Management → Endpoints
- Business Group → Members → Endpoints

By clicking this, the administrator can view the list of existing endpoints, and add new endpoints.

The endpoint definition must have:

- A name (an alphanumeric string).
- Type, which indicates whether the device will be statically or dynamically registered. Most gateways and peer servers are statically registered (they do not send REGISTER messages to Unify OpenScape Voice).
- An IP address or FQDN (for example, server31.companyx.com), if the device is to be statically registered.

Note: If dynamic registration is selected, the user cannot enter an IP address or FQDN. These values will be determined when the device registers.

- Authorization type (by endpoint or by subscriber). The former is most common for gateways, meaning that the endpoint is pre authorized to make and receive calls. If the endpoint option is selected, the user must identify an endpoint profile, which was previously created.
- Endpoint profile name (see above) selected from the list of already defined profiles.
- On the SIP tab, an indication (in the SIP Private Networking or SIP-Q Private networking attributes) if this SIP interface is a SIP private networking or SIP-Q private networking interface.
- On the Attributes tab, the Public/Offnet flag, which is only relevant to SIP trunking interfaces. It indicates whether Unify OpenScape Voice should assume that the caller is a public/offnet party rather than an internal (private network) party.
- On the Aliases tab, the name or alias for the gateway. The alias is the name string by which the gateway will register with Unify OpenScape Voice (if it is dynamically registered) and the name by which the gateway will be known in the SIP registrar database.

Note: A SIP gateway has completely different feature capabilities from a SIP subscriber endpoint. However, it is possible to use a SIP telephone or soft client as a gateway simulator, to test routing results, before the real gateway is installed and available. A SIP gateway (typically) behaves much like a featureless SIP phone with an unusually high call handling capacity.

A endpoint defined with an endpoint profile cannot have subscriber features (such as CSTA or call forwarding) provisioned.

7.8.9.2 Creating the Destinations for the SIP Gateway

The SIP gateway configured in the previous section is not used for outbound traffic yet. For outbound traffic “destinations” are created in the private numbering plan of the users, the common numbering plan of a business group, or in the global numbering plan.

Defining A Destination

To create a destination, the administrator must go to the Destinations table that is either in the numbering plan of the user making the outbound call, in the user’s business group’s common numbering plan, or in the global numbering plan, depending on how the prefix access codes and destination/E164 codes tables have been set up in the numbering plan of the user.

The destination name can be logical or physical (for example, CHICAGO or GATEWAY21) according to the wishes of the network designer. The only parameter that must be entered initially is the destination name string (for example, BOCA_GW1 or CHICAGO or 15619231501, if the gateway itself has a phone number.

Note: This is a name string, not a number. Defining an endpoint or destination with name 15619231000 does not affect the home DN table or prohibit the definition of a subscriber with that number.

Defining A Route

To use the destination, the administrator must add routes to the destination. A route links a destination to a specific endpoint/gateway. This is also done in the Destinations table of Unify OpenScape Voice Assistant. The user selects a defined destination, which opens a window with the destination parameters. On the Routes tab, the administrator can select Add to add a new route. To define a route, the following parameters must be defined:

- A route ID – actually the priority of the route. If there are multiple routes to a destination, the route with the lowest numbered route ID has the highest priority, and will be selected first.

- Endpoint name – selected from the list of already defined endpoints. These endpoints may have been defined in any numbering plan of the Unify OpenScape Voice system.
- Originating signaling type (normally left as undefined – which means “any”). By selecting a specific signaling type, the administrator can give special routing based on the protocol of the originating device.
- Originating bearer capability (normally left as undefined – which means “any”). The bearer cap field make it possible to give special routing to selected bearer types (speech, audio, unrestricted 56kb data, unrestricted 64 kbps data). Certain gateways might be suitable for voice (speech) but not for modem data (audio), for example.
- Digits to delete and insert can be specified. This permits limited manipulation of the destination digits prior sending the outgoing setup/invite.
- The address type (NOA) of the resulting number can be specified (national, international, and so on). Some endpoints/gateways ignore this and others consider it important.
  - SIP protocol does not care the NOA information so this setting is meaningless if the destination is a SIP gateway.
  - SIP-Q protocol does carry the NOA information so it is important that it be set correctly if the destination is a SIP-Q gateway such as the HG3540. In this context, “correctly” means in accordance with what the receiving gateway expects.

Creating the Prefix Access Codes for PSTN Access

At this point, the destination, gateway endpoint, and route have been defined. In order to dial a number and reach the newly created destination, the administrator must put entries in the user’s numbering plan’s prefix access code table. Every digit analysis starts with the dialing user’s PAC table, and stops there if a matching entry cannot be found. To create a new entry, here are some typical values:

- The prefix digits. In as simple routing arrangement, only a few PSTN prefix digits may need to be defined (for example, for the US, 9 for local calls, 91 for national calls, and 9011 for international calls).
- The minimum and maximum number of digits that must be dialed for this prefix, if the entry is to be matched. Note the same prefix digits can appear in the table twice, but with different, non-ambiguous, minimum and maximum lengths. For the examples of

(a) the minimum and maximum for prefix 9 will be 8, for prefix 91 the minimum and maximum will be 11. For prefix 9011 the minimum and maximum would be a range.

- Prefix type – for normal PSTN call routing, this is typically set to off-net access.
- Digit position – indicates how many leading digits to delete before inserting the digits below.
- Digits to insert – used to add prefix digits, for example to normalize the number before passing it to the e164 code table. In a simple prefix based PSTN routing scheme there is probably no need to modify the digit string at this point.
- Nature of address – used to indicate the NOA (for example, international) of the resulting digit string. The e164 code table can select a destination based not only on dialed digits, but NOA, routing area, and class of service. So the value selected here can influence the final routing decision.
- Destination type – for the prefix type off-net access can be BG Common Destination, E164 Destination, or none. None means the resulting digits will be processed in the user’s numbering plan’s destination codes table (below). BG Common Destination means that the resulting digits after modification will be offered to the user’s business group’s common numbering plan and E164 Destination means that the resulting digits after modification will be offered to the E164 numbering plan.

Creating the Destination Codes Table Entries for PSTN Access

The destination codes table defines the destination for a number range, which can be a previously defined destination, or a home DN table (in the case of a subscriber). The parameters of a destination codes table entry include the following:

1. The prefix digits which define the block of numbers. These are selected from the list of prefix access codes defined in the previous section.
2. The remark field can be left empty (a field for future use).
3. The NOA (for example, unknown, international, and so on). Note that the destination codes table differentiates based on the NOA type. So the administrator can have the same prefix digits in the table multiple times, with different NOA values. In order for the entry to be “selected” the NOA of the dialed digits (coming out of the prefix access code table) must match the NOA of the entry. Also note, “unknown” is not a wild card. There is no “wild card” value for this parameter. This value is automatically set when the prefix digits are selected in Step 1.

4. Routing Area and Class of service are normally left blank, unless the administrator wants to control routing based on these values. If they are filled in, only calls with the appropriate routing area and class of service will match on this code table entry. This permits unique routing based on calling location and user class of service.

5. Traffic type – normally set to none (meaning no specific traffic type).

6. Destination type – indicates how to route the call.

The above created destination can only be selected when this option is set to Destination.

Entries in the destination codes table do not specify a number length. Length is not a factor in the entry matching process. However, entries in this table can be overlapping, in the sense that there can be an entry 9 and an entry 91 and an entry 91407, and so on.

When several code table entries all potentially match the dialed digits as modified by the PAC table, the longest matching code table entry will be selected, and that call will be routed to the “destination” named in that code table entry.

7.8.10 Calling Between Business Groups

Calls between BGs can be enabled by inserting the appropriate entries in the BG prefix access code table. The PAC table can be configured to permit inter-BG dialing by dialing:

- The fully qualified E.164 number of the destination in another BG
- A location code and extension number
- A barrier code (for example, 8), followed by a location code and extension number.
- An extension number (provided that the extension numbers of the BGs are not overlapping)

For example if subscribers in BG2 (with number range 1408492xxxx) want to dial subscribers in BG1 (with number range 1561923xxxx), this can be accomplished by creating a PAC in BG2 with the values listed in Table 34, which routes the translation through the E.164 number tables: This permits dialing from BG2 to BG1 with extension number 3xxx, via 8-923-xxxx, and the PSTN dialing forms of the number (with or without the prefix 9).

Prefix Digits	Min length	Max length	Digit Pos	Insert	NOA	Dest Type
3	5	5	0	156192	Unknown	E.164 Dest
8923	8	8	1	1561	Unknown	E.164 Dest
1561	11	11	0		Unknown	E.164 Dest
91	12	12	1		Unknown	E.164 Dest

Table 34 Example of BG Dialing: BG2 Dials BG1

7.8.11 Using PNP Location Codes

As noted above, the network designer can set up a private numbering plan with location code-like dialing, without ever making an entry in the location code table.

The location code table is not primarily used for routing. It is used to properly manage and present the nature of address (NOA/TON) of the calling party to the network, on a call from the BG. As such, the only entries in this table should be for location codes that are within this BG. Most commonly there will be only one entry.

The location code entry instructs the system how to parse the service ID and calling party number into fields, so that the signaling logic can properly set NPI and TON on an outbound call.

The parameters input to create a location code entry include the following:

- The location code – this may be the office code part of the BGL service Ids (for example 1561923) or a completely unrelated value.
- L0 length – the length of PNP Level 0 prefix digits within the location code. The L0 prefix is the PNP equivalent of the PSTN office code. In the example 1561923, the length would typically be 3.
- L1 length – the length of the PNP equivalent of the PSTN city code/area code part of the location code (in the example above, that would probably also be 3 – the digits 561).
- L2 length – the PNP equivalent of the PSTN country code part of the location code (1 in the example)
- Digits to skip (the number of digits to be deleted from location code to get the first digit of the extension number (in the example, this would be 6 if the BG is using 5 digit extension numbers).

The network designer has the option of choosing a network with no location codes, level 0, level 1, or level 2 location codes. Few networks use more than Level 0 location codes. If the network is using L0 location codes, L1 and L2 lengths above will be 0, and the location code itself is 923.

On outbound calls (to a gateway or peer switch in the network), the system normally sends the subscriber ID of the caller (the E.164 number assigned to the subscriber endpoint). There is a system option flag (rarely used) which, when set, causes Unify OpenScape Voice to send the private number as caller ID, that number being constructed from the PNP location code and the extension number. This option applies to all outbound calls, systemwide.

The location code information also can also play a role in determining how the caller ID is displayed on the Unify OpenScape Voice subscriber endpoints and call logs. On calls between subscribers belonging to different numbering plans, the display number modification logic (Section 7.10.3, “Number Modification”) can be configured to display the appropriate PNP number of the other party number, rather than public number.

7.8.12 Viewing Number Translation

After creating the numbering plan, the network designer might want to verify how a given number translates. This can be for either of the following reasons:

- To verify that translation provisioning has resulted in the correct configuration
- To respond to concerns that certain call scenarios are not working as desired

In either case, the manager accesses the Translation Viewer on Unify OpenScape Voice Assistant via the path Unify OpenScape Voice → Maintenance → Tools → **Simulated Dial**, then enters the applicable translation criteria and observes the resulting translation results. After viewing the results, the E.164 translation and routing data can be updated and the tool run again, until the results are satisfactory.

7.9 Networking Unify OpenScape Voice Systems

Unify OpenScape Voice is designed to support distributed enterprises, and can therefore support subscriber groups in multiple geographic locations. This type of configuration is covered in other sections of this document.

Some customers may prefer to install multiple independent Unify OpenScape Voice systems, rather than placing all subscribers under the control of a single Unify OpenScape Voice system. This may be for any of the following reasons:

- **Capacity:** The total number of subscribers exceeds the capacity of a single Unify OpenScape Voice system. Unify OpenScape Voice has a nominal capacity of 20,000-plus subscribers with normal call rates and feature mixes. Depending on the call rate and feature mix, actual capacity may vary from 10,000 to 40,000 plus subscribers. Unify Engineering has an Unify OpenScape Voice Performance Tool that assists the planner in estimating actual system capacity based on the customers' traffic and feature requirements.
- **Reliability:** When subscribers are geographically distributed, the reliability of the intervening WAN links must be considered, and some form of survivability option may be needed for the remote site. One tried-and-true survivability option is a separate, completely independent soft switch.
- **Separate organizational domains:** Different divisions of the company may want or insist on complete administrative control of their own communication facilities. Although Unify OpenScape Voice Assistant provides some functional separation of administrative control at the business group level, often the preferred way to ensure independent administration is through the installation of separate systems.

The deployment strategy for multiple Unify OpenScape Voice systems in a private network is as follows:

- If the customer network requires any SIP-Q interfaces—for example, if interworking is required with a HiPath 3000, OpenScape 4000, or RG 8700 using SIP-Q protocol—the networking between the Unify OpenScape Voice systems *must* be via the SIP-Q private networking interface.
- If the customer network has no requirement for SIP-Q interfaces, the networking between the Unify OpenScape Voice systems *must* be via the SIP private networking interface.

Refer also to Section 9.2, "Private Network Interfaces".

7.10 Setting Up a Network with Geographically Separated Subscribers

Utilizing the basic concepts of the previous section, this section describes two ways to set up a single Unify OpenScape Voice that has subscribers in two physically separated locations. In this example, there are multiple gateways (3) and they are also physically separated, creating the need for location-based routing. Local PSTN calls from the subscribers should be routed to the co-located gateway when possible. The destinations are configured to permit overflow (alternate routing) among the gateways. In the examples, one Unify OpenScape Voice server is located in Boca Raton, Florida, with a secondary location in San Jose, California.

For both of these examples, the provision of one or more survivable gateways at the remote site is recommended to ensure continued operation in the event of a complete WAN failure that prevents access from the remote site to Unify OpenScape Voice.

7.10.1 Using a Single Business Group

The advantage of having all PBX subscribers in a single BG is that full feature functionality is provided between all subscribers. Unify strongly recommends this configuration if feature transparency is needed for calls between the sites. Site-specific routing is accomplished through the use of routing areas, classes of service, or separate numbering plans for the sites. Members of a BG are not required to share the same numbering/routing plan.

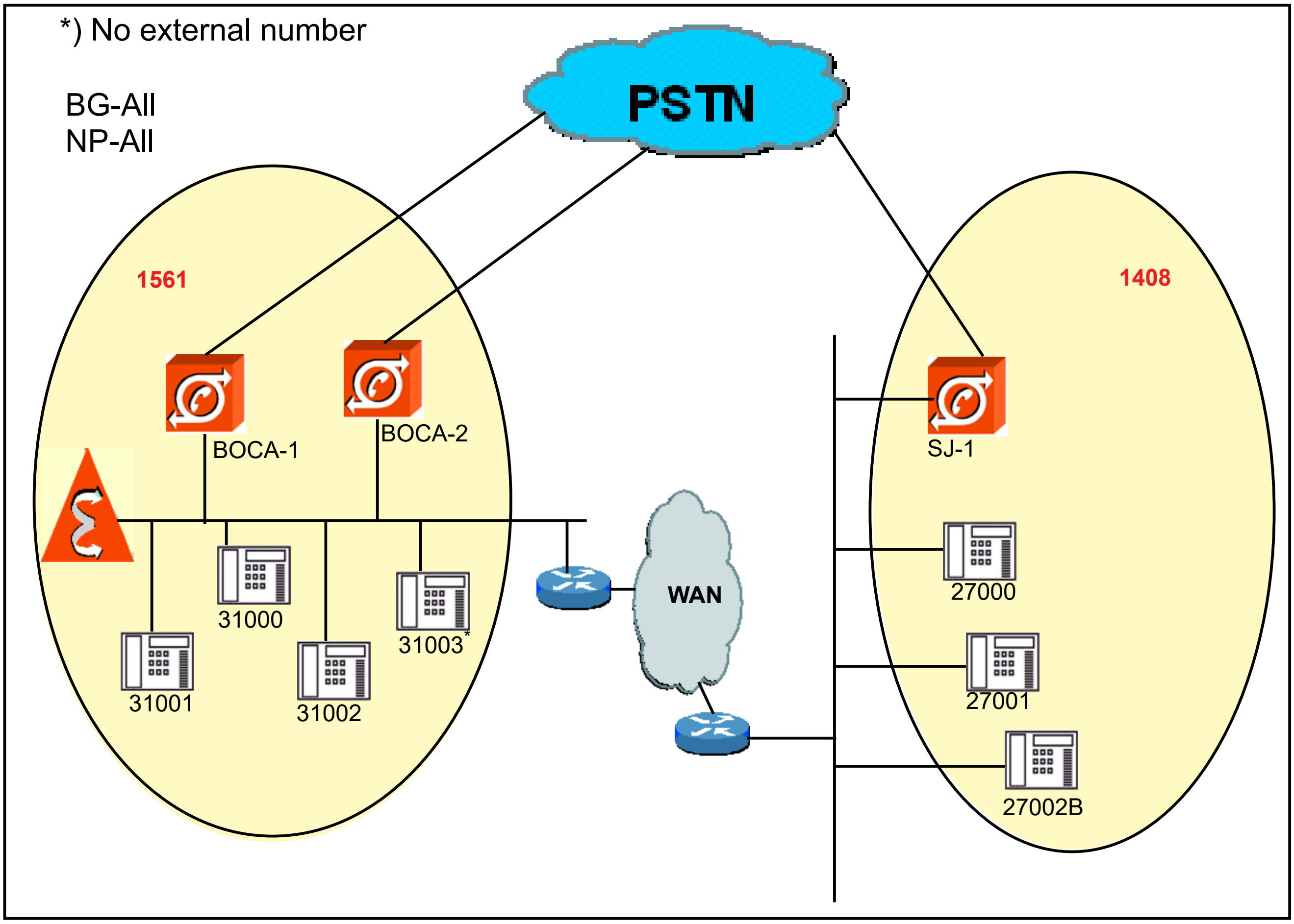


Figure 27 Single Business Group Model

All subscribers can dial each other. In this example, subscriber “31003” does not have an external DN and can therefore not be reached from the PSTN. Unify OpenScape Voice physically resides in Boca Raton, Florida.

The routing and numbering plan provisioning for this reference model would be done as follows:

1. Create office codes for each branch. The example in Table 35 illustrates that Unify OpenScape Voice can connect to central offices in different area codes and time zones.

Location	Office Code Name	Country Code Length	Country Code Length
Boca Raton	1561923	1	3
San Jose	1408492	1	3

Table 35 Branch Office Code Creation

2. Create vacant Home DNs for all subscribers. Normally these blocks are at least 100 or 1000 subscribers long, but Table 36 shows how precisely the home DN number blocks can be tuned. These steps (1 and 2) can be executed on the Global Translation and Routing → Directory Numbers → Home Directory Numbers panel.

Location	Office Code Name	Starting Subscriber Number	Ending Subscriber Number
Boca Raton	1561923	1000	1003
San Jose	1408492	7000	7002

Table 36 Home Directory Number Blocks

3. Create routing areas for each branch office (Table 37). These will enable location-based (also called source-based) routing. Although the routing areas are numeric in this example, they are just text strings, and could just as easily be named BOCA and SANJOSE.

Location	Routing Area Name	Routing Area ID
Boca Raton	1561	1
San Jose	1408	2

Table 37 Routing Areas

4. Create E.164 Codes for all subscribers via Global Translation and Routing → Translation → E.164 Codes (Table 38) It is important *not* to enter routing areas for these E.164 codes; doing so would prevent calling between branch offices.

Location	E164 Code Number	Nature of Address	Traffic Type	Destination Type	Destination Name
Boca Raton	1561923	International	None	Home DN	1561923
San Jose	1408492	International	None	Home DN	1408492

Table 38 E.164 Codes

5. Create private numbering plan for extension dialing via Business Group → Resources → Private Numbering Plans (Table 39).

Location	Numbering Plan Name	Numbering Plan ID
All	NP-All	2

Table 39 Private Numbering Plan for Extension Dialing

6. Create the business group via Administration → General → Business Groups (Table 40).

Location	Name	Display Number	Numbering Plan Name
All	BG-All	15619231000	NP-All

Table 40 Business Group

7. Create an endpoint profile for each gateway via the Administration → Profiles → Endpoint Profiles panel (Table 41). The endpoint profiles contain the correct routing areas. Note that in this example, the gateways will be using the BG numbering plan, rather than the E.164 numbering plan, as illustrated in the previous section. Because there is only one BG in this system, this is perfectly acceptable.

Location	Endpoint Name	BG Name	Routing Area
Boca Raton	EP-Boca	BG-All	1561
San Jose	EP-SJ	BG-All	1408

Table 41 Endpoint Profile for Each Gateway

8. Configure the SIP endpoints for each gateway (Table 42).

Location	Endpoint Name	Registration Type/Registered	IP Address: Port	Account Auth and Service	Endpoint Profile	Transport Protocol
Boca Raton	Boca-1	Static/Yes	x.x.x.x:5060	Based on Endpoint	EP-Boca	TCP
	Boca-2	Static/Yes	x.x.x.x:5060	Based on Endpoint	EP-Boca	TCP
San Jose	SJ-1	Static/Yes	x.x.x.x:5060	Based on Endpoint	EP-SJ	TCP

Table 42 SIP Endpoints for Gateways

9. Configure the logical destinations for each group of gateways (Table 43).

<table>
<tr><th colspan="2">Destination Name</th><th>Numbering Plan Name</th><th colspan="4">Description</th></tr>
<tr><td colspan="2"><b>Boca-Local</b></td><td><b>NP-All</b></td><td colspan="4"><b>The call destination is Boca (see note below).</b></td></tr>
<tr><td></td><th>Route ID</th><th>Route Type</th><th>Route Name</th><th>Number of Digits to Delete</th><th>Digits to Insert</th><th>Nature of Address</th></tr>
<tr><td></td><td>1</td><td>SIP Endpoint</td><td>Boca-1</td><td>1</td><td></td><td>Subscriber</td></tr>
<tr><td></td><td>2</td><td>SIP Endpoint</td><td>Boca-2</td><td>1</td><td></td><td>Subscriber</td></tr>
<tr><td></td><td>3</td><td>SIP Endpoint</td><td>SJ-1</td><td>1</td><td>561</td><td>National</td></tr>
</table>

Table 43 Logical Destinations for Gateways—Boca-Local

Note: The destination in Table 43 receives a dialed number of form 9-xxx-xxxx. If the call is passed through one of the Boca gateways, the destination number will be transmitted in 7-digit subscriber form. If the call is rerouted through the SJ gateway, 561 is prefixed to the number to put it in national number form.

Destination Name	Numbering Plan Name	Description			
SJ-Local	**NP-All**	**The call destination is SJ (see note below).**			
Route ID	**Route Type**	**Route Name**	**Number of digits to delete**	**Digits to insert**	**Nature of Address**
1	SIP Endpoint	SJ-1	1		Subscriber
2	SIP Endpoint	Boca-1	1	408	National
3	SIP Endpoint	Boca-2	1	408	National

Table 44 Logical Destinations for Gateways—SJ Local

The destination in Table 44 receives a dialed number of form 9-xxx-xxxx. If the call is passed through the SJ gateway, the destination number will be transmitted in 7-digit subscriber form. If the call is rerouted through the Boca, 408 is prefixed to the number to put it in national number form.

Destination Name	Numbering Plan Name	Description			
Boca-LD	**NP-All**	**Long distance number dialed by a Boca Subscriber**			
Route ID	**Route Type**	**Route Name**	**Number of digits to delete**	**Digits to insert**	**Nature of Address**
1	SIP Endpoint	Boca-1	2		National
2	SIP Endpoint	Boca-2	2		National
3	SIP Endpoint	SJ-1	2		National

Table 45 Logical Destinations for Gateways—Boca-LD

The destination in Table 45 receives a dialed number of form 91-xxx-xxx-xxxx. If the call is passed through one of the Boca gateways, the destination number will be transmitted in 10-digit national (the 91 is deleted). The same is true if the call is alternate routed to the SJ gateway. The SJ gateway is the last choice in the list, for Boca callers.

Destination Name	Numbering Plan Name	Description
SJ-LD	**NP-All**	**Long distance number dialed by a San Jose Subscriber**

Table 46 Logical Destinations for Gateways—SJ-LD (Seite 1 von 2)

Route ID	Route Type	Route Name	Number of digits to delete	Digits to insert	Nature of Address
1	SIP Endpoint	SJ-1	2		National
2	SIP Endpoint	Boca-1	2		National
3	SIP Endpoint	Boca-2	2		National

Table 46 Logical Destinations for Gateways—SJ-LD (Seite 2 von 2)

The destination in Table 46 receives a dialed number of form 91-xxx-xxx-xxxx. If the call is passed through one of the Boca gateways, the destination number will be transmitted in 10-digit national (the 91 is deleted). The same is true if the call is alternate routed to the Boca Gateways. The SJ gateway is the first choice gateway for SJ callers.

Destination Name	Numbering Plan Name	Description			
Boca-LD-SJ	**NP-All**	**Boca subscriber dials 9-1-408-xxx-xxxx destination. This arrangement permits tail-end-hop-off.**			
Route ID	**Route Type**	**Route Name**	**Number of digits to delete**	**Digits to insert**	**Nature of Address**
1	SIP Endpoint	SJ-1	5		Subscriber
2	SIP Endpoint	Boca-1	2		National
3	SIP Endpoint	Boca-2	2		National

Table 47 Logical Destinations for Gateways—Boca-LD-SJ

The first choice gateway in this case (Table 47) is the San Jose gateway. The number is transmitted to the PSTN as a 7-digit subscriber number, in this case. Second choice routes are the Boca gateways, where the number is transmitted and outpulsed as a 10-digit national number.

Destination Name	Numbering Plan Name	Description
SJ-LD-Boca	**NP-All**	**SJ subscriber dials 9-1-561-xxx-xxxx destination. This arrangement permits tail-end-hop-off.**

Table 48 Logical Destinations for Gateways—SJ-LD-Boca (Seite 1 von 2)

Route ID	Route Type	Route Name	Number of digits to delete	Digits to insert	Nature of Address
1	SIP Endpoint	Boca-1	5		Subscriber
2	SIP Endpoint	Boca-2	5		Subscriber
3	SIP Endpoint	SJ-1	2		National

Table 48 Logical Destinations for Gateways—SJ-LD-Boca (Seite 2 von 2)

The first choice gateway in this case (Table 48) is the Boca-1 gateway. The number is transmitted to the PSTN as a 7-digit subscriber number, in this case. Second choice routes are the Boca gateways, where the number is transmitted and outpulsed as a 10-digit national number.

Destination Name	Numbering Plan Name	Description			
Boca-Int-Local	**NP-All**	**Allows a subscriber that is local in Boca Raton to select the local gateways only for international calls.**			
Route ID	**Route Type**	**Route Name**	**Number of digits to delete**	**Digits to insert**	**Nature of Address**
1	SIP Endpoint	Boca-1	4		International
2	SIP Endpoint	Boca-2	4		International

Table 49 Logical Destinations for Gateways—Boca-Int-Local

Destination Name	Numbering Plan Name	Description

Table 50 Logical Destinations for Gateways—SJ-Int (Seite 1 von 2)

	SJ-Int	**NP-All**	**Allows a subscriber that is local in SJ to select the local gateway for international calls with overflow to a Boca gateway.**			
	Route ID	**Route Type**	**Route Name**	**Number of digits to delete**	**Digits to insert**	**Nature of Address**
	1	SIP Endpoint	SJ-1	4		International
	2	SIP Endpoint	Boca-2	4		International

Table 50 Logical Destinations for Gateways—SJ-Int (Seite 2 von 2)

10. Create the necessary prefix access codes for the NP-All Private Numbering Plan via Unify OpenScape Voice Assistant as shown in Table 51:

Digits	DN Min Length	DN Max Length	Prefix Type	Digit Position	Digits to Insert	Nature of Address	Dest Type	Dest Name
31	5	5	Extension Dialing	0		PNP Extension	None	
27	5	5	Extension Dialing	0		PNP Extension	None	
9	8	8	Off-net Access	0		Unknown(1)	None	
91	12	12	Off-net Access	0		National	None	
9011	10	30	Off-net Access	0		International	None	
Prefixes for Tail-end hop-off								
91561	12	12	Off-net Access	0		Unknown	None	
91408	12	12	Off-net Access	0		Unknown	None	

Table 51 Prefix Access Codes

Note: Cannot use “subscriber” here because that automatically prefixes the area code (npa) which must be specified.

11. Table 52 shows the creation of destination codes for NP-All Private Numbering Plan via Unify OpenScape Voice Assistant:

#	Code	Nature of Address	Routing Area	NPA	Dest Type	Destination Name
1	9	Unknown	1561		Destination	Boca-Local
2	9	Unknown	1408		Destination	SJ-Local
3	91	National	1561		Destination	Boca-LD
4	91	National	1408		Destination	SJ-LD
5	9011	International	1561		Destination	Boca-Int-Local
6	9011	International	1408		Destination	SJ-Int
	Tail End Hop off code points:					
7	91408	Unknown	1561		Destination	Boca-LD-SJ
8	91561	Unknown	1408		Destination	SJ-LD-Boca
	Code points for extension dialing					
	31	PNP Extension			Home Ext	
	27	PNP Extension			Home Ext	

Table 52 Destination Codes for NP-All

12. Table 53 shows the entries in setting up the Extension Code Table for extension dialing.

Extension Prefix	Length	Location Code	E.164 Prefix	Destination Type	Destination Name
27	5		5619231	Home DN	1408492
31	5		408492	Home DN	1561923

Table 53 Extension Code Table Entries

Because this system consists of one BG with extension dialing, there is no need to assign the subscribers to a location code.

13. All that remains to be done is the definition of the subscriber endpoints with appropriate phone numbers and routing area assignments.

7.10.2 Using a Business Group Per Branch

The steps below illustrate the configuration of another network with two sites (physical locations) but using a single Unify OpenScape Voice switch. Refer to Figure 28, "Business Groups at Each Sites". In this case, each site is defined as a BG. This has the advantage that Unify OpenScape Voice Assistant permits each BG to have its own administrator, with appropriate access rules enforced. However, the network planner must keep in mind that some features will not work between the branches. Features such as calling party name and connected party name are blocked or restricted on calls between BGs.

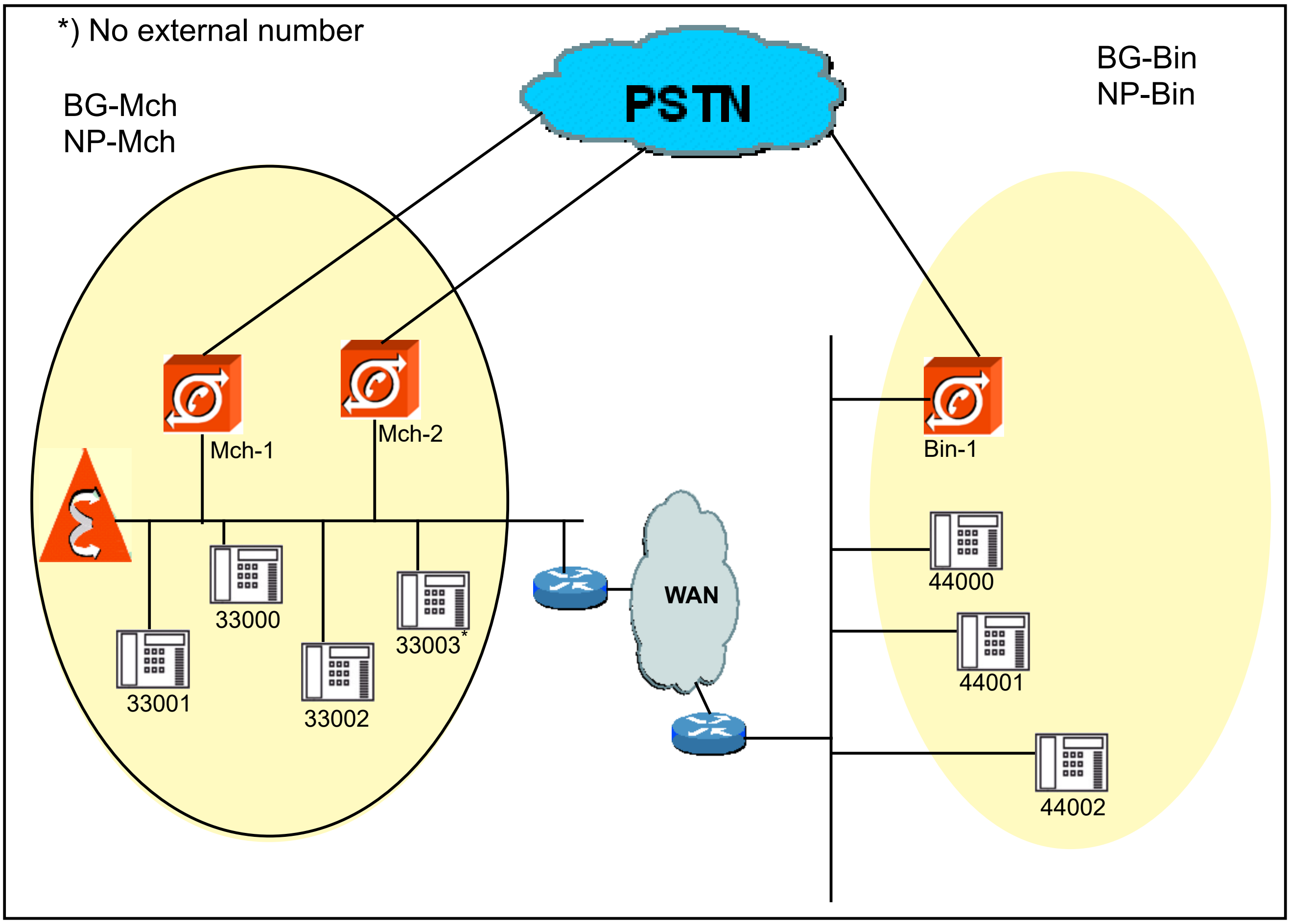


Figure 28 *Business Groups at Each Sites*

In this case, there is no need to work with routing areas to separate out the geographical location of the gateways. The routing and numbering plan provisioning for this reference model would be done as follows:

1. Table 54 illustrates the configuration of office codes for each branch office.

Location	Office Code Name	Country Code Length	Area Code Length
Munich	49897223	2	2
Berlin	49303864	2	2

Table 54 *Office Code Creation for Each Branch Office*

2. Table 55 provides an example of the configuration of Home DNs for all subscribers.

Location	Office Code Name	Starting Subscriber Number	Ending Subscriber Number
Munich	49897223	3000	3003
Berlin	49303864	4000	4002

Table 55 Vacant Home Directory Numbers for All Subscribers

3. Table 56 provides an example of the configuration of E.164 Codes for all subscribers.

Location	E164 Code Number	Nature of Address	Traffic Type	Dest Type	Dest Name
Munich	49897223	International	None	Home DN	49897223
Berlin	49303864	International	None	Home DN	49303864

Table 56 E.164 Codes for All Subscribers

4. Table 57 provides an example of the configuration of the E.164 prefix access code table entries to enable the code table entries above.

Digits	DN Min Len	DN Max Len	Prefix Type	Digit Position	Digits to Insert	Nature of Address	Dest Type	Dest Name
49	6	20	no prefix	0		international	None	

Table 57 Example of E.164 Prefix Access Code Table Entries

5. Table 58 provides an example configuration of Private Numbering Plans for extension dialing.

Location	Numbering Plan Name	Numbering Plan ID
Munich	NP-Mch	10
Berlin	NP-Bln	11

Table 58 Private Numbering Plan for Extension Dialing

6. Table 59 shows the entries for Business Group via Unify OpenScape Voice Assistant:

Location	Name	Display Number	Numbering Plan Name
Munich	BG-Mch	498972233000	NP-Mch
Berlin	BG-Bln	493038644000	NP-Bln

Table 59 Business Groups

7. Table 60, "Endpoint Profile Creation" provides example entries for gateway endpoint profiles.

Location	Endpoint Name	BG Name	Routing Area
Munich	EP-Mch	BG-Mch	
Berlin	EP-Bln	BG-Bln	

Table 60 Endpoint Profile Creation

8. Table 61 provides example entries of SIP endpoints for each gateway.

Location	Endpoint Name	Registration Type/ Registered	IP Address: Port	Account Auth and Service	Endpoint Profile	Transport Protocol
Munich	Mch-1	Static/Yes	x.x.x.x:5060	Based on Endpoint	EP-Mch	TCP
	Mch-2	Static/Yes	x.x.x.x:5060	Based on Endpoint	EP-Mch	TCP
Berlin	Bln-1	Static/Yes	x.x.x.x:5060	Based on Endpoint	EP-Bln	TCP

Table 61 SIP Endpoints for Each Gateway

9. Table 61 through Table 71 provides example entries of destinations for each group of gateways.

Destination Name	Numbering Plan Name	Description
Mch-Local	**NP-Mch**	**Allows a local call to go to the gateway as if dialed by a subscriber that is local in Munich. (local calls). Numbers are presented to this route as a local number (no city code) prefixed by a 0 (barrier code).**

Route ID	Route Type	Route Name	Number of digits to delete	Digits to insert	Nature of Address
1	SIP Endpoint	Mch-1	1		Subscriber
2	SIP Endpoint	Mch-2	1		Subscriber
3	SIP Endpoint	Bln-1	1	89	National

Table 62 Destinations for Each Group of Gateways—Mch-Local

<table>
<tr><th colspan="2">Destination Name</th><th>Numbering Plan Name</th><th colspan="4">Description</th></tr>
<tr><td colspan="2"><b>Bln-Local</b></td><td><b>NP-Bln</b></td><td colspan="4"><b>Allows a local call to go to the gateway as if dialed by a subscriber that is local in Berlin. (local calls). Numbers are presented to this route as a local number (no city code) prefixed by a 0 (barrier code).</b></td></tr>
<tr><td></td><td><b>Route ID</b></td><td><b>Route Type</b></td><td><b>Route Name</b></td><td><b>Number of digits to delete</b></td><td><b>Digits to insert</b></td><td><b>Nature of Address</b></td></tr>
<tr><td></td><td>1</td><td>SIP Endpoint</td><td>Bln-1</td><td>1</td><td></td><td>Subscriber</td></tr>
<tr><td></td><td>2</td><td>SIP Endpoint</td><td>Mch-1</td><td>1</td><td>30</td><td>National</td></tr>
<tr><td></td><td>3</td><td>SIP Endpoint</td><td>Mch-2</td><td>1</td><td>30</td><td>National</td></tr>
</table>

Table 63 Destinations for Each Group of Gateways—Bin-Local

<table>
<tr><th colspan="2">Destination Name</th><th>Numbering Plan Name</th><th colspan="4">Description</th></tr>
<tr><td colspan="2"><b>Mch-LD</b></td><td><b>NP-Mch</b></td><td colspan="4"><b>Allows a long distance call to go to the gateway as if dialed by a subscriber that is local in Munich. (long distance calls). Numbers are presented to this route in national number form (no country code) but with a 00 barrier code still present.</b></td></tr>
<tr><td></td><td><b>Route ID</b></td><td><b>Route Type</b></td><td><b>Route Name</b></td><td><b>Number of digits to delete</b></td><td><b>Digits to insert</b></td><td><b>Nature of Address</b></td></tr>
<tr><td></td><td>1</td><td>SIP Endpoint</td><td>Mch-1</td><td>2</td><td></td><td>National</td></tr>
<tr><td></td><td>2</td><td>SIP Endpoint</td><td>Mch-2</td><td>2</td><td></td><td>National</td></tr>
<tr><td></td><td>3</td><td>SIP Endpoint</td><td>Bln-1</td><td>2</td><td></td><td>National</td></tr>
</table>

Table 64 Destinations for Each Group of Gateways—Mch-LD

The barrier code is deleted and the national form of the number is transmitted.

Destination Name	Numbering Plan Name	Description

Table 65 Destinations for Each Group of Gateways—Bln-LD (Seite 1 von 2)(Seite 1 von 2)

Bln -LD	NP- Bln	Allows a long distance call to go to the gateway as if dialed by a subscriber that is local in San Jose. (long distance calls). Numbers are presented to this route in national number form (no country code) but with a 00 barrier code still present. The barrier code 00 is deleted here.				
	Route ID	**Route Type**	**Route Name**	**Number of digits to delete**	**Digits to insert**	**Nature of Address**
	1	SIP Endpoint	Bln-1	2		National
	2	SIP Endpoint	Mch-1	2		National
	3	SIP Endpoint	Mch-2	2		National

Table 65 Destinations for Each Group of Gateways—Bln-LD (Seite 2 von 2)(Seite 2 von 2)

Destination Name	Numbering Plan Name	Description				
Mch-LD-Bln	**NP-Mch**	**Allows a subscriber that is local in Munich to make a local call in Berlin. (Tail-end hop-off). The number is still in dialed form 0030-xxxxxx.**				
	Route ID	**Route Type**	**Route Name**	**Number of digits to delete**	**Digits to insert**	**Nature of Address**
	1	SIP Endpoint	Bln-1	4		Subscriber
	2	SIP Endpoint	Mch-1	2		National
	3	SIP Endpoint	Mch-2	2		National

Table 66 Destinations for Each Group of Gateways—Mch-LD-Bln

Destination Name	Numbering Plan Name	Description				
Bln-LD-Mch	**NP-Mch**	**Allows a subscriber that is local in Berlin to make a local call in Munich. (Tail-end hop-off)**				
	Route ID	**Route Type**	**Route Name**	**Number of digits to delete**	**Digits to insert**	**Nature of Address**
	1	SIP Endpoint	Mch-1	4		Subscriber
	2	SIP Endpoint	Mch-2	4		Subscriber
	3	SIP Endpoint	Bln-1	2		National

Table 67 Destinations for Each Group of Gateways—Bln-LD-Mch

<table>
<tr><th colspan="2">Destination Name</th><th>Numbering Plan Name</th><th colspan="4">Description</th></tr>
<tr><td colspan="2"><b>Mch-LD-Local</b></td><td><b>NP-Mch</b></td><td colspan="4"><b>Allows a subscriber that is local in Munich to select the local gateways only for national calls. (Local only). The number is presented in national form with the barrier code (prefix digits) 80 still present. The 80 are deleted by the route.</b></td></tr>
<tr><td></td><th>Route ID</th><th>Route Type</th><th>Route Name</th><th>Number of digits to delete</th><th>Digits to insert</th><th>Nature of Address</th></tr>
<tr><td></td><td>1</td><td>SIP Endpoint</td><td>Mch-1</td><td>2</td><td></td><td>National</td></tr>
<tr><td></td><td>2</td><td>SIP Endpoint</td><td>Mch-2</td><td>2</td><td></td><td>National</td></tr>
</table>

Table 68 Destinations for Each Group of Gateways—Mch-LD-Local

Destination Name	Numbering Plan Name	Description
Mch-Int-Local	**NP-Mch**	**Allows a subscriber that is local in Munich to select the local gateways only for international calls. (Local only). The dialed digits are presented to this route in international form (including country code) but with the 000 prefix still attached. It will be deleted by the route.**

Route ID	Route Type	Route Name	Number of digits to delete	Digits to insert	Nature of Address
1	SIP Endpoint	Mch-1	3		International
2	SIP Endpoint	Mch-2	3		International

Table 69 Destinations for Each Group of Gateways—Mch-Int-Local

Destination Name	Numbering Plan Name	Description
Bln-LD-Local	**NP-Bln**	**Allows a subscriber that is local in Berlin to select the local gateway only for national calls (Local only). Number is presented in national number form with the 80 prefix digits still present. The prefix digits are deleted by the route.**

Route ID	Route Type	Route Name	Number of digits to delete	Digits to insert	Nature of Address
1	SIP Endpoint	Bln-1	2		National

Table 70 Destinations for Each Group of Gateways—Bln-LD-Local

Destination Name	Numbering Plan Name	Description

Table 71 Destinations for Each Group of Gateways—Bln-int-Local (Seite 1 von 2)

Bln-Int-Local		NP-Bln	Allows a subscriber that is local in Berlin to select the local gateway only for International (Local only). The dialed digits are presented to this route in international form (including country code) but with the 000 prefix still attached. It will be deleted by the route.			
	Route ID	**Route Type**	**Route Name**	**Number of digits to delete**	**Digits to insert**	**Nature of Address**
	1	SIP Endpoint	Bln-1	3		International

Table 71 Destinations for Each Group of Gateways—Bln-int-Local (Seite 2 von 2)

10. Table 72 shows the creation of Prefix Access Codes for the NP-Mch Private Numbering Plan via Unify OpenScape Voice Assistant.

Digits	DN Min Len	DN Max Len	Prefix Type	Digit Position	Digits to Insert	Nature of Address	Dest Type	Dest Name
33	5	5	Extension Dialing	0	4930386	Unknown	E.164 Destination	E164NANP
44	5	5	Extension Dialing	0	4989722	Unknown	E.164 Destination	E164NANP
0	4	30	Off-net Access	0		Unknown(1)	None	
00	8	30	Off-net Access	0		National	None	
000	10	30	Off-net Access	0		International	None	
Tail-end hop-off								
0030	8	30	Off-net Access	0		Unknown(1)	None	

Table 72 Prefix Access Codes for the NP-Mch PNP

In Table 72, extension dialing is handled by appending the E.164 prefix and processing the number through the E.164 (Global Numbering Plan) digit tables configured. This requires that appropriate entries be made in both the E.164 prefix access code table and the E.164 destination access code table (above).

Note: This entry is matched for local calls, where the remaining digits are a local subscriber number. NOA = subscriber cannot be used here because the resulting destination code entry will automatically prefix the city code, in front of the local access code (barrier code) 0.

11. Table 73 shows the creation of prefix access codes for the NP-Bln Private Numbering Plan via Unify OpenScape Voice Assistant.

Digits	DN Min Len	DN Max Len	Prefix Type	Digit Positio n	Digits to Insert	Nature of Address	Destination Type	Destination Name
33	5	5	Extension Dialing	0	4930386	Unknown	E.164 Destination	E164NANP
44	5	5	Extension Dialing	0	4989722	Unknown	E.164 Destination	E164NANP
0	4	30	Off-net Access	0		Unknown (2)	None	
00	8	30	Off-net Access	0		National	None	
000	10	30	Off-net Access	0		Inter national	None	
Tail-end hop-off								
0089	8	30	Off-net Access	0		Subscriber	None	

Table 73 Prefix Access Codes for the NP-Bln PNP

Note: This entry is matched for local calls, where the remaining digits are a local subscriber number. NOA = subscriber cannot be used here because the resulting destination code entry will automatically prefix the city code, in front of the local access code (barrier code) 0.

12. Table 74 shows the configuration of destination codes for NP-Mch Private Numbering Plan.

Code	Nature of Address	Routing Area	NPA	Destination Type	Destination Name
0	Unknown			Destination	Mch-Local
00	National			Destination	Mch-LD
000	International			Destination	Mch-Int-Local
80	National			Destination	Mch-LD-Local
Tail-end hop-off					
0030	Unknown			Destination	Mch-LD-Bln

Table 74 Destination Codes for NP-Mch PNP

13. Table 75 shows the configuration of destination codes for NP-Bln Private Numbering Plan via Unify OpenScape Voice Assistant.

Code	Nature of Address	Routing Area	NPA	Destination Type	Destination Name
0	Unknown			Destination	Bln-Local
00	National			Destination	Bln-LD
000	International			Destination	Bln-Int-Local
80	National			Destination	Bln-LD-Local
Tail-end hop-off					
0030	Unknown			Destination	Bln-LD-Mch

Table 75 Destination Codes for NP-Bln PNP

14. Finally, create all subscribers via Unify OpenScape Voice Assistant.

7.10.3 Number Modification

This section describes the administrative tools that have been provided to ensure that the display number that appears in the display of the endpoint (for example, of the calling party, called party, or connected party) is the preferred format of the number that can be used to dial back the calling party. Ideally, this would be the shortest possible dialable number: national number, international number, and so on.

7.10.3.1 Background

Without the number modification feature, the call parties see the display numbers differently depending on the call scenario. For example, if a call is between two endpoints in different BGs, the calling party’s number will appear as the number with which it was provisioned in the system and without prefixes of any kind. If the calling and called numbers are in the same BG, the display will show the extension number only. This is not what a user is typically used to seeing on their display using conventional TDM systems.

For example, if the A-Party was provisioned in the system using an International number format of, for example, 1-561-923-1008 and had the extension field set to 31008 in their profile, the B-Party would see 31008 as the calling party number—if they are within the same BG. Because a BG may have members scattered in different cities, states, or even in different nations, the extension number is not necessarily a dialable number. If they are in a different BG, the calling number would appear as 15619231008 in the display. Number modification allows the administrator to control the number display format, based on the numbering plan assignments of the two parties.

Similarly, gateways have certain requirements regarding numbers that are delivered to them. An example would be an outgoing call from an A-Party in Boca which is going out through a PSTN gateway in Boca to the PSTN. It will need to have the A-Party number transmitted in the call setup message as a national number. However, when the same party makes an outbound call through a gateway located in Munich, the gateway would require all numbers to be sent in international format. Currently number modification logic has no influence on numbers (such as caller ID/connected party number) transmitted over SIP-Q links.

7.10.3.2 Functions and Capabilities

Note: The number modification feature is not just limited to the calling party number but also the called party number and the connected party number—that is, it is every number that can appear in a user’s phone as the call progresses through each state transition.

The number modification feature allows the administrator to configure number displays so that the B-party always sees a display number that can be used to call back the A-party. For example:

- Parties in different numbering plans and different companies, but in the same country will see the **national** number when calling each other.
- Parties in different numbering plans that are in the same company want to see the shortest unambiguous **private** number, which could be just an extension or a location code with or without an access code.
- Incoming PSTN call from a gateway that is providing a **national** number format may have to be mapped to an **international** number format.
- Calls between two residential customers in a carrier scenario usually wish to see the shortest number based on their area code location.
- The function that derives the correct number will also insert the correct prefix or access codes in addition to the shortest component of the number [for example, **national**, international and private/ public number access code (PNAC) prefix].

The display number is correct even in more complex redirection call scenarios—for example, call forwarding, simultaneous ringing, call pickup, hunt group, and so on.

7.10.3.3 Number Modification Rules

Number modification rules are defined via Unify OpenScape Voice Assistant for each private numbering plan. The administrator selects the Administration/Display Number option in Unify OpenScape Voice Assistant to access the associated data structures.

There are options under this tab:

- The Number Definition option tab allows the administrator to define, for each numbering plan, how the subscriber IDs for each number using this number plan are subdivided into country code, area or city code, office code, and extension numbers, and so on. Where private numbers are being exchanged, the table also enables the system to subdivide the private number into the appropriate L2, L1, and L0 number fields.
- The Number Modification tab allows the administrator user to define how numbers should be modified for appropriate display, when calls passing between endpoints belonging to separate numbering plans. Separate rules are possible for each source and destination numbering plan ID pair modified into a calling party number, when displayed to subscribers members of each other numbering plan.
- The Number Prefixes tab allows the administrator to define, for each number type, the prefix digits that must be added prior to display, to put the number in a dialable format. A switch frequently is presented with a number that is marked as “national” or “local” or “international” and this table is used to determine what digit prefix the user must dial in order to complete a call to this destination.

Refer to the *OpenScape Voice, Configuration, Administrator Documentation* for more information about how these tables should be configured.

7.10.3.4 Planning Considerations

Prior to implementation of the display number modification feature, the number display rules were relatively fixed, and governed by the BG membership of the two parties in the call.

Going forward, Unify envisions that all members of an enterprise will be normally be members of the same BG, even if they are geographically distributed in multiple locations, even multiple countries, because this configuration provides the best feature transparency among all users.

Consistent with this concept, a single BG can have multiple number plans.

Within a single large BG, the planner can use class of service assignments, routing area assignments, or numbering plan assignments to provide location specific routing. If the dialing rules among and between the locations are simple (for example, extension dialing throughout the network) then any of these options works equally well.

If there are different and complex dialing rules among and between the locations (for example location codes, barrier codes, or special prefixes) then the use of separate number plans and the number modification tables described here provide the best mechanism to ensure optimal dialable numbers are displayed to both the calling and called parties.

For calls outside of the business group (BG), users must normally dial a prefix string before the number of destination party. Sometimes this is required between numbering plans as well. When the system displays a caller ID number to the user, on the phone display or in a call log, the customer will want the proper prefix code shown as part of the number display, so the number should be shown in the actual dialable form. The number modification tables make this possible. The number modification tables can also shorten a calling party to the abbreviated dialable (optimized) form.

To access the number modification tables via Unify OpenScape Voice Assistant, select **Display Number,** under the topic **Administration**, on the left column. There are three subfolders – **Definitions**, **Prefixes**, and **Modifications**.

7.10.3.5 Prefixes

In the prefixes table, you can define the prefix string for each number type. The prefix digits are divided into two parts:

- The prefix number access code (PNAC) (usually a single digit)
- A prefix string (which depends on the type of number)

For each numbering plan, you can define the prefix strings for public number forms (international, national, and local) and private network numbers (L2, L1, and L0). Table 76 is a typical example:

public (e.164)	local	9	(none)
public	national	9	1
public	international	9	011
private	level 0 (L0)	8	

Table 76 Prefix Number Access Code Plan – Example

private	L1	not normally defined	
private	L2	not normally defined	

Table 76 Prefix Number Access Code Plan – Example

When a caller ID is to be displayed to a subscriber within the business group, the system will evaluate the Numbering Plan Identifier/Type of Number (NPI/TON) of the caller ID, then add the appropriate prefix digits before displaying the number.

To evaluate the caller ID, the system uses the **Definitions** Table described in Section 7.10.3.6, "Definition Table", which evaluates the leading digits of the caller ID to establish the type of number.

7.10.3.6 Definition Table

1. When the caller is behind a SIP gateway, the calling party number does not carry any NPI/TON information, which limits what "number modification" logic can do with the caller ID before it is displayed at the destination. The definition table is used to parse the caller ID, assign it an appropriate number type (national, international, or the like), and (in some cases) divide the number into appropriate parts (country code, area code, office code, and so on.)

2. The minimum set for calls within a number plan (where subscribers and SIP gateways share the NP) is shown in Table 77 below. In this example, the subscribers are in the 1561923xxxx range.

NP1	1	–	–	–	–	–	–	–	–	*
NP1	1	561	923	2	–	–	–	–	–	**
NP1	49	–	–	–	–	–	–	–	–	***
NP1	–	40	–	–	–	–	–	–	–	****

Table 77 Definition Table Example

* A rule is needed to tell Number Modification (NM) logic that all numbers starting with 1 are international.

** A rule is also needed to allow NM logic to parse subscriber numbers within the BG so that extension numbers can be displayed. Note, this rule can override the extension number length defined when the subscriber is created. A subscriber may be created with displayed extension number 1001, but this rule will cause internal calls to display a 5-digit number (31001).

*** A rule is needed to indicate country code (49) that should be displayed as a dialable international number (801149…). The number of entries of this type will depend on the complexity of caller IDs coming in from the gateways. Generally, it should not be necessary to put an entry in the table for each country code. If all caller IDs are in international form, then a single entry of "4" will cover all country codes beginning with 4.

****If national numbers are sent in without the prefix 1, you would need one or more rules like this to mark these as national numbers. This rule is not needed if all caller IDs are supplied in international format. Note that the longest match wins in the analysis of the caller ID. The rules above will interpret 49 as international but 41 as national.

3. If Unify OpenScape Voice can identify the NPI/TON of the calling party number from this table, it will follow the rules of the modification table and append the appropriate access code string before displaying the caller ID.

4. On intraswitch calls (subscriber to subscriber) the operation of number modification takes a bit of explanation.

   a) The default behavior between subscribers within a BG is to display extension numbers. This operation predates the number modification feature. The displayed extension numbers are explicitly defined when the subscriber created via Unify OpenScape Voice Assistant. Between BGs, the full subscriber IDs are exchanged/displayed by default.

   b) As soon as the number modification feature is enabled by defining the prefix access codes for a number plan, the default behavior changes. The full subscriber ID of the partner will be displayed, with an access code. This display is generally not correct, as described below.

   c) If the caller ID number is a US number with prefix 1, and this is properly categorized as “international”, the default behavior will prefix the international access digits (for example, 8011) so you get a possibly inappropriate display (for example, 801115619231003).

   d) If the caller ID type cannot be identified from the definition table, the default behavior is to display the number unchanged on the called device, with no modification.

5. To correct the problem noted in 4c above, additional setup is required, in the Modification Table.

7.10.3.7 Modifications

To restore extension number displays with the BG, you need to create a basic rule for intra-BG calling.The rule shown in Table 78 below will restore extension number displays for subscriber to subscriber calls within the BG. If you do not check **Optimize**, the displays will be the full subscriber ID of the partner party.

NP1	NP1	ANY	ANY	transparent	yes

Table 78 Modification Rule Restoring Extension Numbers for Subscriber to Subscriber Calls

However, the rule shown in Table 78 will not prefix the necessary access codes for external caller IDs coming in from a gateway. To get both proper extension number displays, and external caller IDs with appropriate access codes, a small modification to the rule is required, as shown in Table 79 below.

NP1	NP1	ANY	ANYpre	transparent	yes

Table 79 Modification Table Rule Using ANYpre

- The *ANYpre* instructs Unify OpenScape Voice to find the most appropriate access code and add it to the displayed number.
- The **Optimize** flag is essential. If not set, calls between stations in the BG will be shown in complete international form, including the 8011 prefix.
- The **Optimize** flag has another important benefit. If an international caller ID has the same country code as the BG, the number is optimized into a national number, and the national prefix digits are applied. So 12125551234 becomes 812125551234 rather than 801112125551234 (a general international dialing form).
- Unfortunately, a rule like this applies to both phones and gateways within the BG, so this rule also adjusts the caller ID sent to the gateway. So caller IDs sent to the gateway will have form 81561aaabbbb.
  - This is one reason the manuals suggest putting the gateway in a separate numbering plan. A separate numbering plan allows you to define non-symmetric rules. You can prefix the access code on calls within the subscriber number plan, but leave the prefix off on calls to the gateway.
  - An alternative, with the newer RG software, is to adjust the caller ID in the gateway itself via DSUB rules. A DSUB rule can be used to remove the prefix 8 (in our example) from caller IDs going to the PSTN. This allows the gateway to remain within a common numbering plan with its subscribers.

7.10.3.8 Calls Between Numbering Plans (Same Business Group)

Given that NP1 has been configured for number modification as described above, but NP2 has not been set up in the number modification tables, the default behavior on station to station calls between the two numbering plans (same BG) is that extension numbers are displayed. Assuming that NP2 calls NP1:

- The calling extension number displayed on the NP1 phone will be the extension number defined in the subscriber data when the line was created. This may or may not be a dialable number in the direction NP1 to NP2. If extension dialing is provided throughout the BG, then displayed number will be dialable, but in general it will not.
- The connected extension number displayed at NP2 will be the extension number as defined by the number modification tables defined for NP1. Again, this may or may not be a dialable number in the direction NP2 to NP1.

Since every modification rule has a “from” and “to” number plan, the operation for displays can be non-symmetric. The directionality refers not to the directionality of the call, but the directionality of the display information. If NP1 calls NP2:

- The definition rules for parsing of the caller ID is found in NP1.
- The modification rule governing display of calling party on the destination is the calling party, for example, NP1 to NP2 rule.
- The modification rule governing display of called number on the calling party display is the NP2 to NP1 rule.

As soon as the prefix strings are defined for NP2, the behavior changes. When NP2 calls NP1:

- The calling party number on NP1 will still be the extension number of calling device. NM does not (apparently) have enough information to override the default behavior of the system (which is not correct).
- The ringing/connected party on NP2 will be the full international number in international format. If the international prefix string is 9011 and the called party is 15619231001, the displayed number will be 901115619231001 (which is not correct).

The next step: number pattern definition for NP2. Assuming NP2 has area/office code 408/492, the appropriate starting definition for NP2 would be:

NP2	1	408	492	2	–	–	–	–	–	–

Table 80 Number Pattern Definition for NP2

When the rule above (Table 80) is in place, behavior changes again. When NP2 calls NP1:

- The calling party number on NP1 will now be in (incorrect) international form (80111408492xxxx). NM has taken the subscriber ID, which is in international form (includes country code) and prefixed the defined international prefix string 8011.
- The ringing/connected party on NP2 is unchanged, in the full international number, in international format. If the international prefix string is 9011 and the called party is 15619231001, the displayed number will be 901115619231001.

To provide dialable (public) number displays between two NPs, the following modification rules need to be inserted. As a destination number plan, you can specify the specific number plan, or use the ANY destination, if the system behavior is generally consistent among all number plans.

NP1	NP2 or ANY	ANY	ANYpre	transparent	yes
NP2	NP1 or ANY	ANY	ANYpre	transparent	yes

Table 81 Displaying Private Numbers with Location Codes

If some subscribers can dial between numbering plans using a private location code, then the user will want to see the private form of the caller ID on the phone. This can be overlaid on the solution shown in Table 81 above.

Assume NP2 calls NP1 in the example above (Table 81), and that NP1 can call NP2 using the private network location code 492. Then the following change should be made to the definition table entry for NP2, to define the relationship between public and private number (see Table 82).

NP2	1	408	492	2	492	3	–	–	2	

Table 82 Relationship between Public and Private Numbering Plan Defined

Next, a number modification rule must be added for the NP2 to NP1 direction, as shown in Table 83 below. Note that the specific rule for NP2 to NP1 overrides the general rule for NP2 to ANY number plan.

NP2	NP1	International	Private Lev 0	transparent	yes
NP2	ANY	ANY	ANYpre	transparent	yes

Table 83 Modification Rule for the NP2 to NP1 Direction

7.11 Branch Office Numbering Plan Administration

When a customer has many branches, it is fairly common for each branch to have its own local PSTN gateway. This means each branch has branch-specific call routing requirements for a few selected numbers (usually the local PSTN office codes), while the routing for most numbers (on-net numbers, national, and international numbers) is frequently often common among all branches.

Prior to the implementation of this feature, it was customary to handle the unique routing aspects of each branch within a BG numbering plan, and handle common routing using the E.164 (global) numbering plan. The BG numbering plan logic has always provided the ability to direct selected prefix codes to the global numbering plan, by setting the destination type for the prefix as “E164 numbering plan”. We say the BG numbering plan permits selected prefix codes to “escape” to the common, global numbering plan.

When Unify OpenScape Voice is supporting multiple enterprises, in a multi-tenant or hosted (shared) configuration, it may not be appropriate to route calls from multiple businesses to the global E.164 routing and numbering plan.

Branch office numbering plan administration provides an option to solve that problem, by permitting each enterprise, defined as a business group, to have its own BG common numbering plan in addition to the location-specific BG numbering plans.

As a result, each branch can have its own location-specific BG numbering plan, for handling site specific requirements (such as local number routing and emergency rerouting in the case of a WAN outage) and can “escape” to the common BG numbering plan for routing functions common to all branches within the business group.

Within a BG numbering plan, it is possible to route selected prefix codes to either the common BG numbering plan or the global E.164 routing plan. This provides additional flexibility to the network designer and BG administrator.

Consider the example in Figure 29.

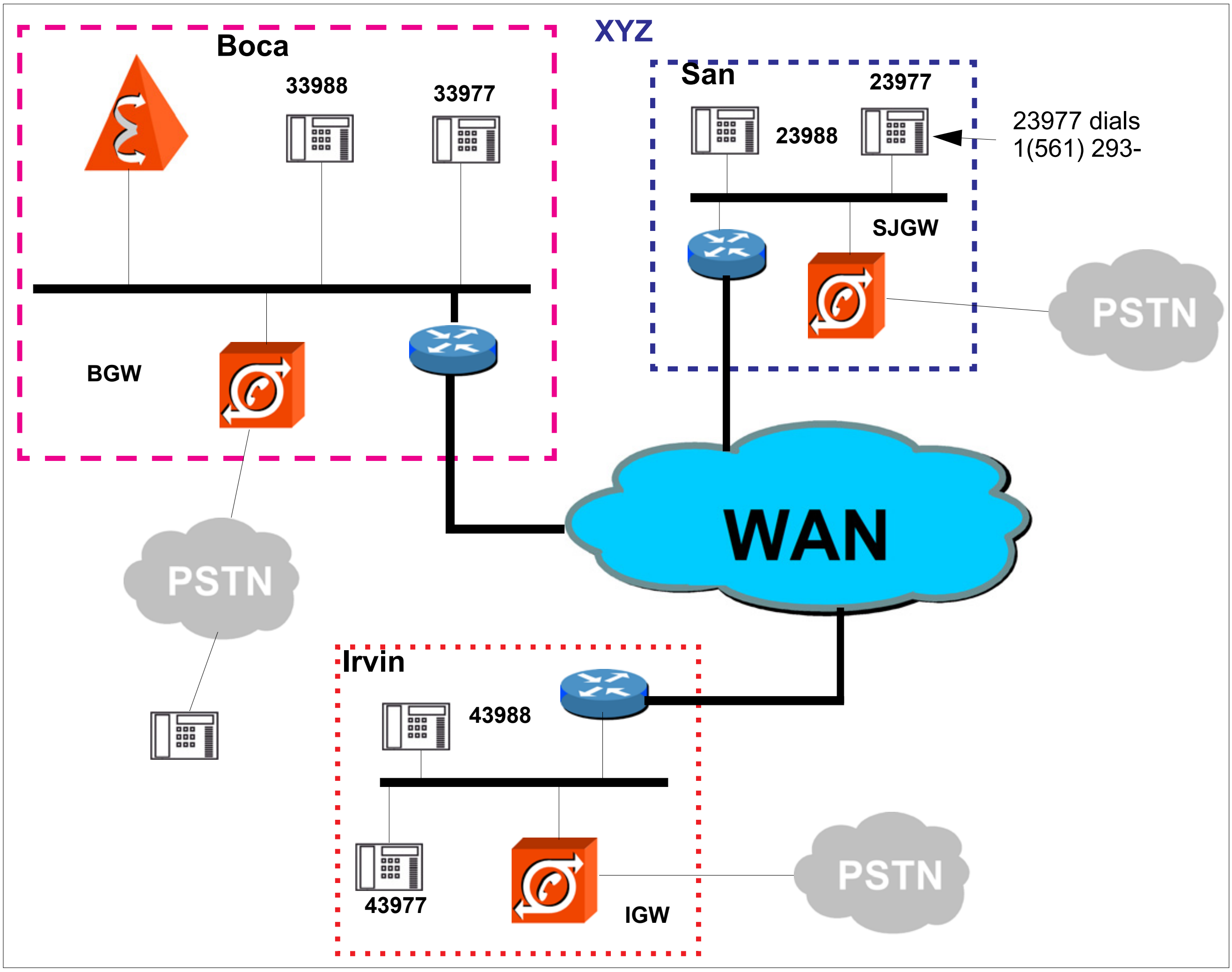


Figure 29 *Branch Office Numbering Plan Administration Example*

In Figure 29, the headquarters of the XYZ corporation is located in Boca Raton, with branches in San Jose, and Irving. The XYZ corporation has just added a branch in Irving. This branch, like all the others, has been placed in the same BG. Having the branches and the headquarters in the same BG allow the system features to be available to all subscribers. The BG has a default numbering plan assigned to it which is used to assigned a numbering plan to a BGL when the BGL is created if the craftperson doesn't enter a numbering plan for the BGL. All of the subscribers (BGLs) in the headquarters and the branches have a numbering plan assigned. Each subscriber on the network must have a unique E.164 number (either public or private) assigned to it.

A branch subscriber (San Jose or Irving) wishing to place a call to a public subscriber in Boca dials the public Boca number, which must be translatable within the calling party's BGL numbering plan so the call hops off at the Boca gateway (BGW). Without the branch office numbering plan administration feature, each branch must have a numbering plan with Boca as a destination so that the dialed Boca number can be translated by Unify OpenScape Voice, leading to the BGW gateway as a route off-net in Boca. As branches are added, the Boca destination must be configured in the new branch's numbering plan.

Instead of having to add this routing information for each branch, the branch office numbering plan administration feature makes it possible to have a common BG numbering plan.

- In the common BG numbering plan, the Boca routing information is added. Only one common numbering plan is allowed per BG and it is optional.
- The numbering plan escape capability allows a BGL private numbering plan to escape (move up) to a BG common numbering plan, in addition to the system default numbering plan. Only upward escapes are allowed; lateral escapes are not. For example, the BGL numbering plan escapes to the BG common numbering plan, and the BG common numbering plan escapes to the system default numbering plan.
- The far-end hop off gateways shared among different branches is supported via the BG common numbering plan.
- The head-end hop off is supported via reroute with the BGL's local numbering plan.

In the example in Figure 29, "Branch Office Numbering Plan Administration Example", San Jose user 23977 dials 1(561) 293-3432. Unify OpenScape Voice initially attempts to translate this number in the calling party's BGL numbering plan, which is provisioned such that all numbers that start with 1561 escape to the BG common numbering plan. For example, 1561 is provisioned in the calling party's NP as a prefix access code with a prefix type that specifies retranslation in the BG common numbering plan.

Unify OpenScape Voice then re-translates this number based on the BG common numbering plan, resulting in one or more routes leading to a Boca gateway (BGW). If all attempts to route the call via the Boca gateways fail—for example, due to WAN failure—Unify OpenScape Voice will "fallback" by retranslating the dialed digits again using the calling party's BGL numbering plan and ignoring the escape prefix to the BG common numbering plan. When provisioned properly in the calling party's numbering plan, this results in one or more routes leading to the local gateway (SJGW) in San Jose. Refer also to Chapter 10, "Gateway and Subscriber Rerouting".

7.12 Telephony Number Mapping (ENUM)

The abbreviation ENUM is derived from t*E*lephony *NU*mber *M*apping. The DNS ENUM system can be used to convert telephone numbers into service-specific uniform resource identifiers (URI). The ENUM feature provides support for the domain name service (DNS)-based architecture and protocol for mapping an E.164-compliant number into a service-specific URI.

Unify OpenScape Voice can be configured to consult an ENUM server during the call routing process. In such a configuration, the ENUM server converts the translated destination number into a SIP address, the address to which the call is to be routed. The destination may be any of the following:

- SIP or SIP-Q gateway to the PSTN
- Peer switch or server
- Subscriber local to (registered on) Unify OpenScape Voice
- Public internet service provider that supports SIP interconnect service

The ENUM server is basically a database with the E.164 numbers correlated to the SIP-URIs.

An ENUM query is launched when one of the following takes place:

- An E.164 route marked as an ENUM route is reached.
- The office classmark indicates that Unify OpenScape Voice must perform ENUM queries on all calls to non-hosted subscribers.

The query resolves the number into a sorted list of URIs (SIP addresses).

7.12.1 Sample Call Flow with ENUM Query

The scenario in Figure 30, "Simple SIP Call Flow with ENUM Query" showing a simple call flow may help to clarify the call processing.

In this scenario, an enterprise might own two Unify OpenScape Voices with on-net subscribers on each, and has set up the office classmark to perform ENUM queries on all calls. Whenever a subscriber dials a telephone number that is not on the same Unify OpenScape Voice, Unify OpenScape Voice performs an ENUM query to determine if the call can be routed via an IP network—in this case, to a subscriber on the other Unify OpenScape Voice—or if it has to be delivered to the PSTN.

In the simple SIP call flow that includes an ENUM query, the following occurs:

1. User A dials user B, who is not located on the same Unify OpenScape Voice hosting user A.
2. Unify OpenScape Voice queries the ENUM server to determine the location of user B.
3. The ENUM server returns the naming authority pointer (NAPTR) record(s) containing the location of user B or how to route the call to user B.

   For best performance, the ENUM server should return the IP address of the destination gateway or endpoint. If a domain name is returned (for example *boca.companyx.com*) this may trigger a subsequent DNS SRV query, plus subsequent queries, on a per-call basis, to resolve this domain name into an IP address. This can slow call setup and impact system performance.
4. Unify OpenScape Voice determines whether it can route the call on-net or whether the call must be sent to the PSTN. If it is on-net, an INVITE is sent to the proxy (likely another Unify OpenScape Voice) for user B.
5. The far-end switch (most likely another Unify OpenScape Voice) presents the call to user B.

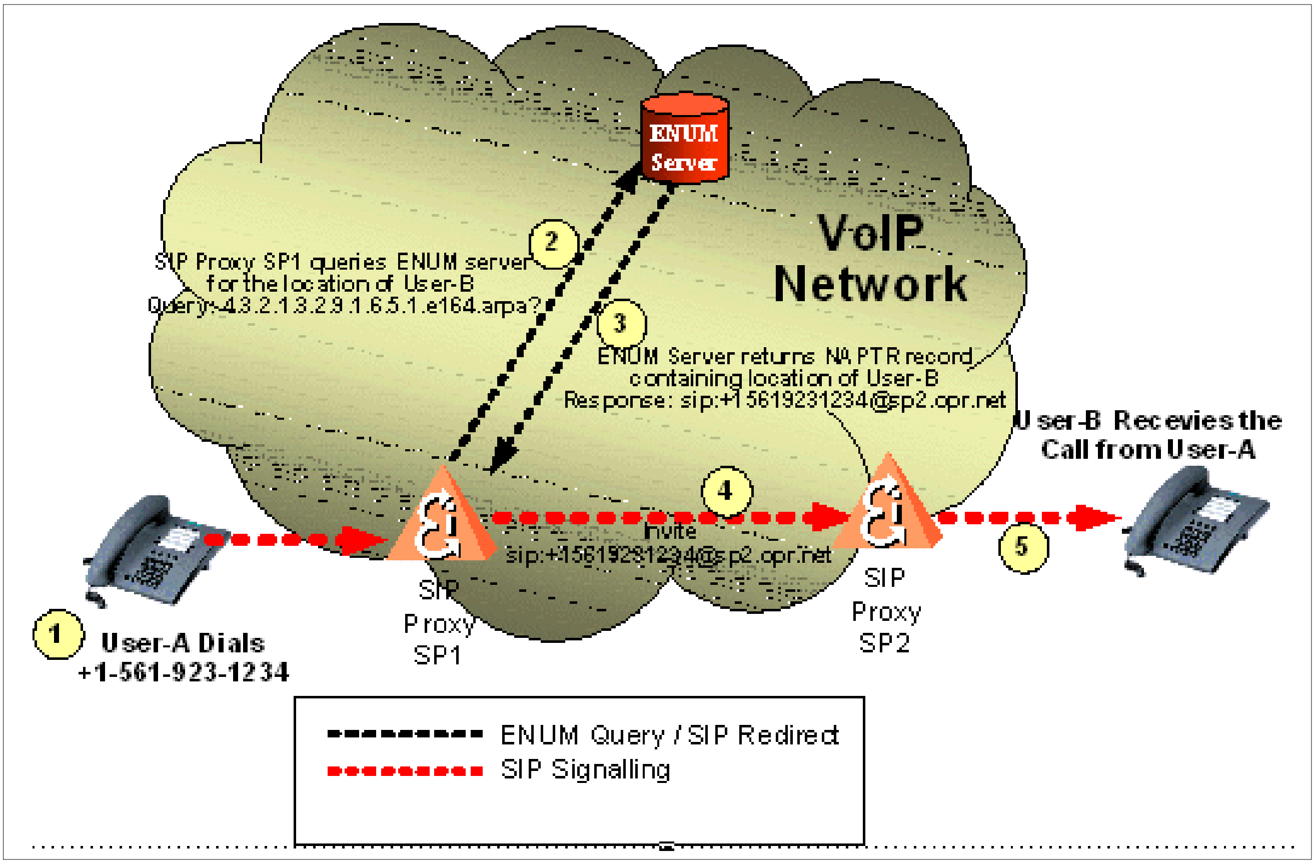

ENUM Server
VoIP Network
2
SIP Proxy SP1 queries ENUM server for the location of User-B
Query: 4.3.2.1.3.2.9.1.6.5.1.e164.arpa?
3
ENUM Server returns NAPTR record containing location of User-B
Response: sip:+15619231234@sp2.opr.net
User-B Recevies the Call from User-A
4
Invite sip:+15619231234@sp2.opr.net
5
1
User-A Dials +1-561-923-1234
SIP Proxy SP1
SIP Proxy SP2
ENUM Query / SIP Redirect
SIP Signalling

Figure 30 Simple SIP Call Flow with ENUM Query

For calls involving ENUM server transactions, additional time, in the order of milliseconds, will be consumed for each ENUM server transaction, thereby increasing the call processing time.

Unify does not supply an ENUM server product. If the network designer elects to use the ENUM feature, the designer must ensure that a DNS ENUM server is available with adequate capacity and fast enough response time. Round-trip delay, from query to response, should be under 50 milliseconds. Longer response times can result in call setup delay and lost calls. The designer should also define the Unify OpenScape Voice routing database in a way that ensures that outbound calls can continue to be routed if an ENUM server fails.

7.12.2 Provisioning

In Unify OpenScape Voice Assistant, ENUM is provisioned via the Global Translation and Routing path.

The ENUM Server table is located at the path Global Translation and Routing → ENUM → ENUM Servers. It allows up to six ENUM servers to be configured, each with:

- Server name (string)
- Primary IP address of the server
- Optional secondary IP address of the server
- Cache size (in megabytes)

  The cache is a record of recent queries and responses. If the same destination address is called repeatedly, the cache provides a means to reduce the traffic on the ENUM server.

The administrator then defines the destination if necessary. When setting up the call routing plan, as described in Section 7.8.9, “Routing Calls to the PSTN”, calls are routed to destinations, and destinations point to one or more prioritized routes (alternate paths to the destination). Most routes point to gateways or peer servers where the call should be directed. The administrator can add an entry in the route list with destination type “ENUM”. When destination type ENUM is specified, the administrator must subsequently specify an ENUM route, as described below.

Note: If the ENUM server fails to respond with a valid destination for the call, Unify OpenScape Voice will select an alternate route, if one is available, based on the prioritized route list associated with the destination.

Finally, the administrator defines the ENUM route, which points to an ENUM server that will be queried. This route requires the following information fields:

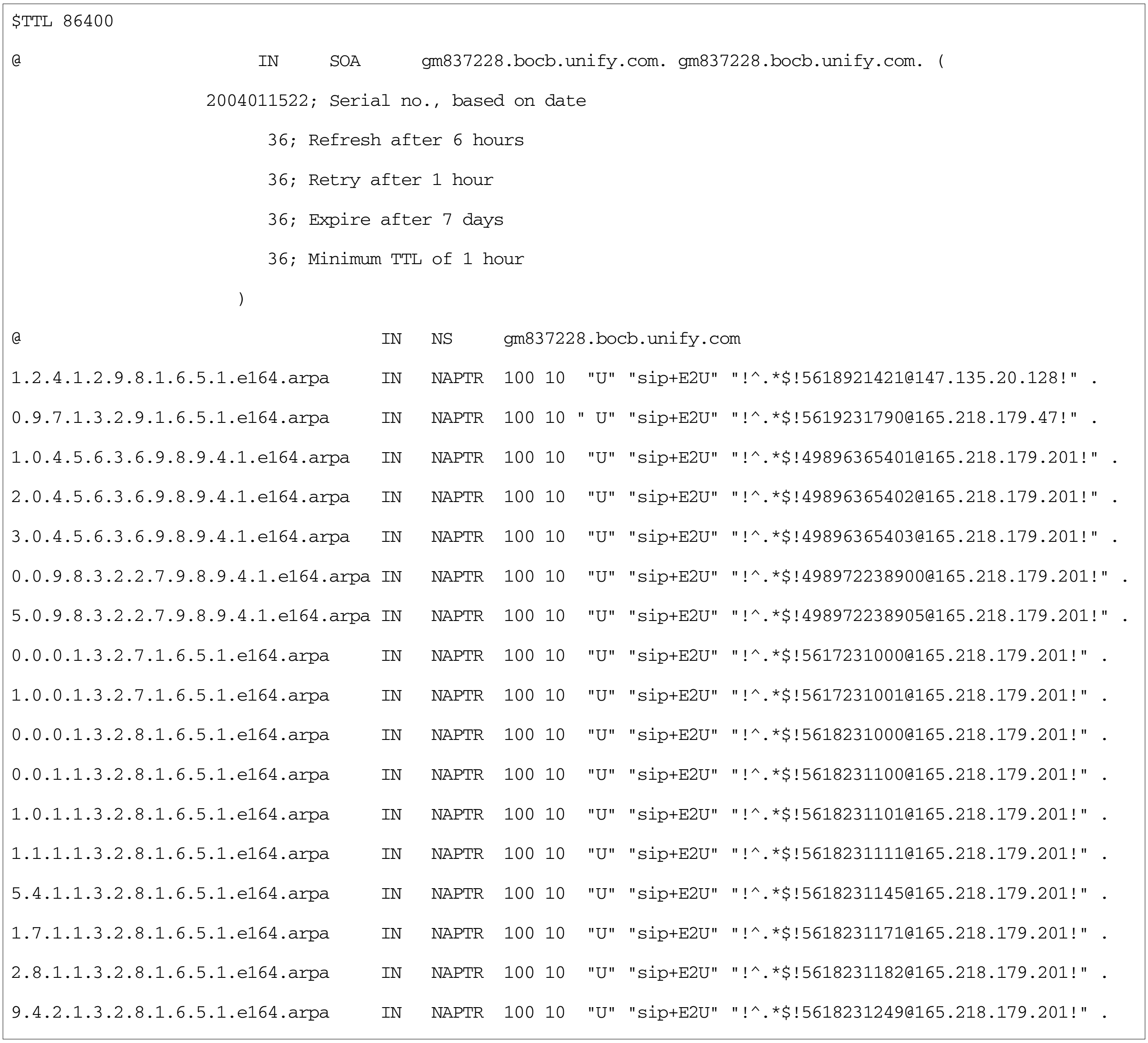
- A route name (string)
- The name of the ENUM server used for this route
- The tier 0 zone string used for this route (most commonly “e164.arpa”)

  The most common tier 0 zone string (and the only one formally supported by the ENUM standards document) is e164.arpa. However, in the enterprise environment, other customer-defined strings are possible (for example, companyx.com or usa.companyx.com). Using different domain strings, a single DNS server can in principle provide number translation service for more than one numbering plan.

  The tier 0 zone string is appended to the number in the query to the ENUM server, as a way to clearly define the number type.

When a user dials a number, the number is represented in reverse so that, for example, the number `5618921421` would be represented by `1.2.4.1.2.9.8.1.6.5.1` or a wild car entry can be just a portion of that, so any `954*` number would be represented by `.4.5.9`.

Figure 31 shows a printout of a small portion of a typical DNS ENUM server database.



```
$TTL 86400
@                      IN     SOA      gm837228.bocb.unify.com. gm837228.bocb.unify.com. (
                   2004011522; Serial no., based on date
                         36; Refresh after 6 hours
                         36; Retry after 1 hour
                         36; Expire after 7 days
                         36; Minimum TTL of 1 hour
                      )
@                                  IN   NS     gm837228.bocb.unify.com
1.2.4.1.2.9.8.1.6.5.1.e164.arpa     IN   NAPTR  100 10  "U" "sip+E2U" "!^.*$!5618921421@147.135.20.128!" .
0.9.7.1.3.2.9.1.6.5.1.e164.arpa     IN   NAPTR  100 10 " U" "sip+E2U" "!^.*$!5619231790@165.218.179.47!" .
1.0.4.5.6.3.6.9.8.9.4.1.e164.arpa   IN   NAPTR  100 10  "U" "sip+E2U" "!^.*$!49896365401@165.218.179.201!" .
2.0.4.5.6.3.6.9.8.9.4.1.e164.arpa   IN   NAPTR  100 10  "U" "sip+E2U" "!^.*$!49896365402@165.218.179.201!" .
3.0.4.5.6.3.6.9.8.9.4.1.e164.arpa   IN   NAPTR  100 10  "U" "sip+E2U" "!^.*$!49896365403@165.218.179.201!" .
0.0.9.8.3.2.2.7.9.8.9.4.1.e164.arpa IN   NAPTR  100 10  "U" "sip+E2U" "!^.*$!498972238900@165.218.179.201!" .
5.0.9.8.3.2.2.7.9.8.9.4.1.e164.arpa IN   NAPTR  100 10  "U" "sip+E2U" "!^.*$!498972238905@165.218.179.201!" .
0.0.0.1.3.2.7.1.6.5.1.e164.arpa     IN   NAPTR  100 10  "U" "sip+E2U" "!^.*$!5617231000@165.218.179.201!" .
1.0.0.1.3.2.7.1.6.5.1.e164.arpa     IN   NAPTR  100 10  "U" "sip+E2U" "!^.*$!5617231001@165.218.179.201!" .
0.0.0.1.3.2.8.1.6.5.1.e164.arpa     IN   NAPTR  100 10  "U" "sip+E2U" "!^.*$!5618231000@165.218.179.201!" .
0.0.1.1.3.2.8.1.6.5.1.e164.arpa     IN   NAPTR  100 10  "U" "sip+E2U" "!^.*$!5618231100@165.218.179.201!" .
1.0.1.1.3.2.8.1.6.5.1.e164.arpa     IN   NAPTR  100 10  "U" "sip+E2U" "!^.*$!5618231101@165.218.179.201!" .
1.1.1.1.3.2.8.1.6.5.1.e164.arpa     IN   NAPTR  100 10  "U" "sip+E2U" "!^.*$!5618231111@165.218.179.201!" .
5.4.1.1.3.2.8.1.6.5.1.e164.arpa     IN   NAPTR  100 10  "U" "sip+E2U" "!^.*$!5618231145@165.218.179.201!" .
1.7.1.1.3.2.8.1.6.5.1.e164.arpa     IN   NAPTR  100 10  "U" "sip+E2U" "!^.*$!5618231171@165.218.179.201!" .
2.8.1.1.3.2.8.1.6.5.1.e164.arpa     IN   NAPTR  100 10  "U" "sip+E2U" "!^.*$!5618231182@165.218.179.201!" .
9.4.2.1.3.2.8.1.6.5.1.e164.arpa     IN   NAPTR  100 10  "U" "sip+E2U" "!^.*$!5618231249@165.218.179.201!" .
```

Figure 31 Typical ENUM Records

Attention: It is the customer’s responsibility to keep all ENUM servers up-to-date and populated correctly. Unify OpenScape Voice accesses the data on a read-only basis; if a matching entry is incorrect, the call will be routed incorrectly. Unify does not assume responsibility for the contents of the ENUM server.

8 Network Element Management

This chapter describes the network administration tools used to provision and maintain the Unify OpenScape Voice system. These tools provide for:

- Provisioning and viewing network topology data used by the softswitch
- Configuring the switch for its operational environment
- Analyzing measurements and operational statistics
- Monitoring alarms, alerts, and traps

The administration interfaces supported by Unify OpenScape Voice are:

- Unify OpenScape Voice Assistant, which provides a web browser-based GUI for administration and management of the system
- OpenScape Branch Assistant, which provides a web-based GUI for administration and management of functions specific to the OpenScape Branch platform
- The command line interface (CLI), whose basis is provided by RTP (Fujitsu Unify Real-time Telecommunications Platform software) and is extended by Unify with softswitch-specific commands

8.1 Unify OpenScape Voice Assistant

Unify OpenScape Voice Assistant brings the administration of Unify OpenScape Voice together into one web-based tool. It is accessible from any PC with a suitable web browser and connectivity to Unify OpenScape Voice. It can reside on Unify OpenScape Voice itself (for installations with fewer than 5000 subscribers), or on a separate server for larger installations.

The Unify OpenScape Voice Assistant application, even though its average bandwidth requirement is very low, requires a minimum of 2 Mbps of available bandwidth to both nodes of a duplex cluster for adequate performance during administrative tasks.

Unify OpenScape Voice Assistant provides the following:

- Single web-based tool for administration and maintenance
- Dashboard for status visibility and access to all system components (Unify OpenScape Voice, OpenScape Media Server, phones, and gateways)

- Web-based GUI for subscriber, dial plan, OpenScape Media Server configuration
- Role-based access to specific administration functions
- Support of Unify phones via integration with DLS phone deployment server
  - Software download
  - QoS configuration
- Integration into HiPath Management Landscape:
  - HiPath Accounting Management
  - HiPath Fault Management
  - HiPath User Management

Refer to the *OpenScape Voice, Configuration, Administrator Documentation* for additional information.

8.2 OpenScape Branch Assistant

Open Branch Assistant is a tool to manage functions specific to the OpenScape Branch platform. It is accessible via a tab on the Common Management Platform (CMP). In addition to providing a dashboard view of all branches, it provides access to the following:

- Alarms
- Media server
- Security
- Survivability features
- Utilities, such as import and export

Note: OpenScape Branch also has its own local GUI that is used for certain tasks. Most of these tasks can also be performed via the OpenScape Branch Assistant tab; however, this GUI continues to be available when the headquarters is not.

The alarms generated by the OpenScape Branch platform are integrated into the CMP, so that a consolidated view of the alarms can be provided.

8.3 Command Line Interface (CLI)

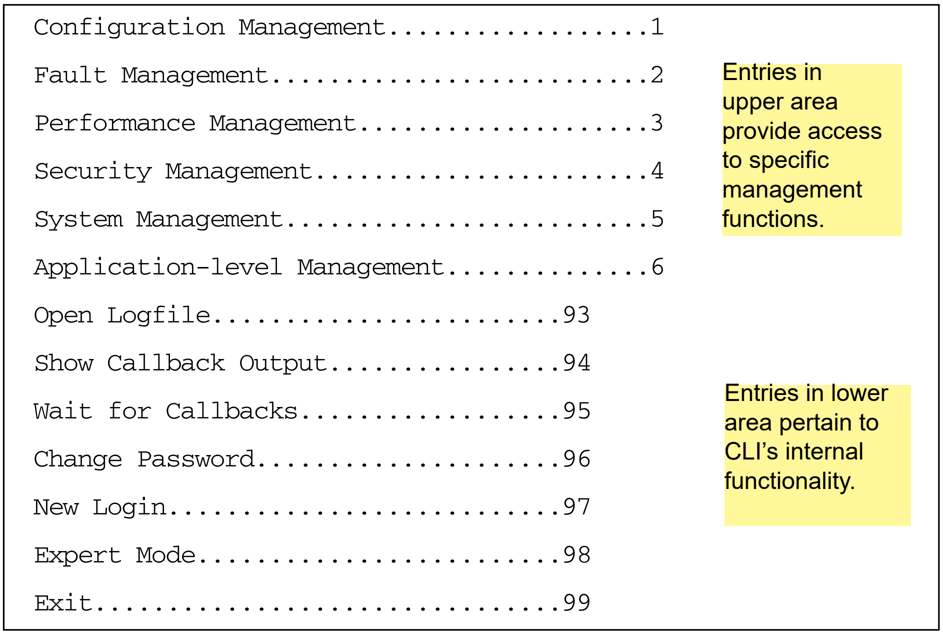
The CLI is a traditional command-line application that interfaces with and manages Unify OpenScape Voice. It is appropriate for tasks that cannot be performed using Unify OpenScape Voice Assistant.

It is accessible either locally— that is, by using a local console—or remotely using the SSH Secure Shell. There are two modes of operation for the CLI:

- **CLI menu mode (default mode):** Has a text-based user interface which has a menu using numbers to select the various tasks.
- **CLI expert mode:**
  - Assumes the user has advance knowledge of the commands and required syntax.
  - Assumes the user has some experience with other command line interfaces, for example UNIX shells.
  - Used for mass provisioning.

To access the Linux operating system, users must have a client that can do Secure Shell (SSH). Unify OpenScape Voice does not let users do a simple Telnet or FTP session due to the security implemented during installation.

Figure 32 shows the CLI main menu.



```
Configuration Management..................1
Fault Management..........................2
Performance Management....................3
Security Management.......................4
System Management.........................5
Application-level Management..............6
Open Logfile.......................93
Show Callback Output...............94
Wait for Callbacks.................95
Change Password....................96
New Login..........................97
Expert Mode........................98
Exit...............................99
```

Entries in upper area provide access to specific management functions.

Entries in lower area pertain to CLI's internal functionality.

Figure 32 CLI Main Menu

9 Selecting Network Interfaces

This chapter describes the Unify interfaces for making connections within a private network, or between a private network and the public network. Several gateway and proxy devices enable the customer to connect to the public network and between private network nodes. These include:

- RG 8700 ISDN gateway family from Unify:
  - RG 8716
  - RG 8708
  - RG 8702
- HG 3500 SIP-Q gateway that resides on the OpenScape 4000
- HG 1500 SIP-Q gateway that resides on the HiPath 3000
- Third-party SIP gateways from Mediatrix
- RG 8300

  The SIP gateway RG 8300 enables IP connections with SIP-Q to Unify OpenScape Voice and ISDN T1 or E1 PRI connections to PSTN or to the OpenScape 4000. It is based on the hardware and software of OpenScape 4000.

9.1 RG 8700

The RG 8700 is a compact low- to mid-capacity gateway family designed for enterprise networking. It is suitable for use in both headquarters and remote locations.

The RG 8700 supports both SIP (for interworking with the public ISDN network) and SIP-Q (only for interworking with QSIG-compatible PBXs such as the OpenScape 4000 and HiPath 3000).

Table 84 lists the available RG 8700 models.

Model	Number of PRI Spans	Number of Users in Survivability Mode
RG 8716	16	2000
RG 8708	8	1000
RG 8702	2	200

Table 84 RG 8700 Models

For voice processing, the RG 8700 delivers the following base functionality:

- Multiple codec types:
  - G.711 (A-law and μ-law)
  - G.723.1
  - G.726
  - G.729A
  - Clear mode (for passing digital data without codec or echo canceller corruption)
- Echo cancellers (up to 128 ms)
- Silence suppression
- DTMF tone detection and generation
- Comfort noise generation (CNG)
- Packet loss concealment (PLC)
- Jitter buffers (Adaptive up 150 ms)
- Transparent fax/modem transmission over IP

The RG 8700 provides up to 16 directly connected T1/E1 lines for PSTN interfaces and one 10/100 Ethernet interfaces for IP network connections.

As a survivability media gateway (SMG), the RG 8700 can operate in two modes: normal and survivability.

The phones have to support dual registration and will reregister at the RG 8700 in case of WAN failure.

9.1.1 Normal Mode—Headquarters to Branch

In normal mode of operation shown in Figure 33, "RG 8700 Normal Mode Operation—Headquarters to Branch":

- Users have to be configured in the headquarters Unify OpenScape Voice and in the RG 8700s.

  Note: Lower-priority phones that do not require operation in survivability mode need not be configured in the RG 8700 or configured for dual registration.

- All endpoints, at the headquarters and the branch, must register with Unify OpenScape Voice as their primary (first choice) registrar and SIP server. Branch endpoints that must continue to operate when Unify OpenScape Voice is unreachable must also be configured to register with the RG 8700, as a secondary registrar and SIP server.

  Unify SIP endpoints dual-register, meaning they are registered with both the RG 8700 and Unify OpenScape Voice at the same time, and can, in principle, receive calls directly from either source. However, while in normal operation, the RG 8700 sends all inbound calls to Unify OpenScape Voice.

- Call setup and teardown are performed by Unify OpenScape Voice.

During normal operation, the RG 8700 acts as a pure trunking gateway and can support any number of subscribers in the network as a PSTN access point, subject only to the number of T1/E1 spans that are configured and the call blocking factor the customer is willing to tolerate.

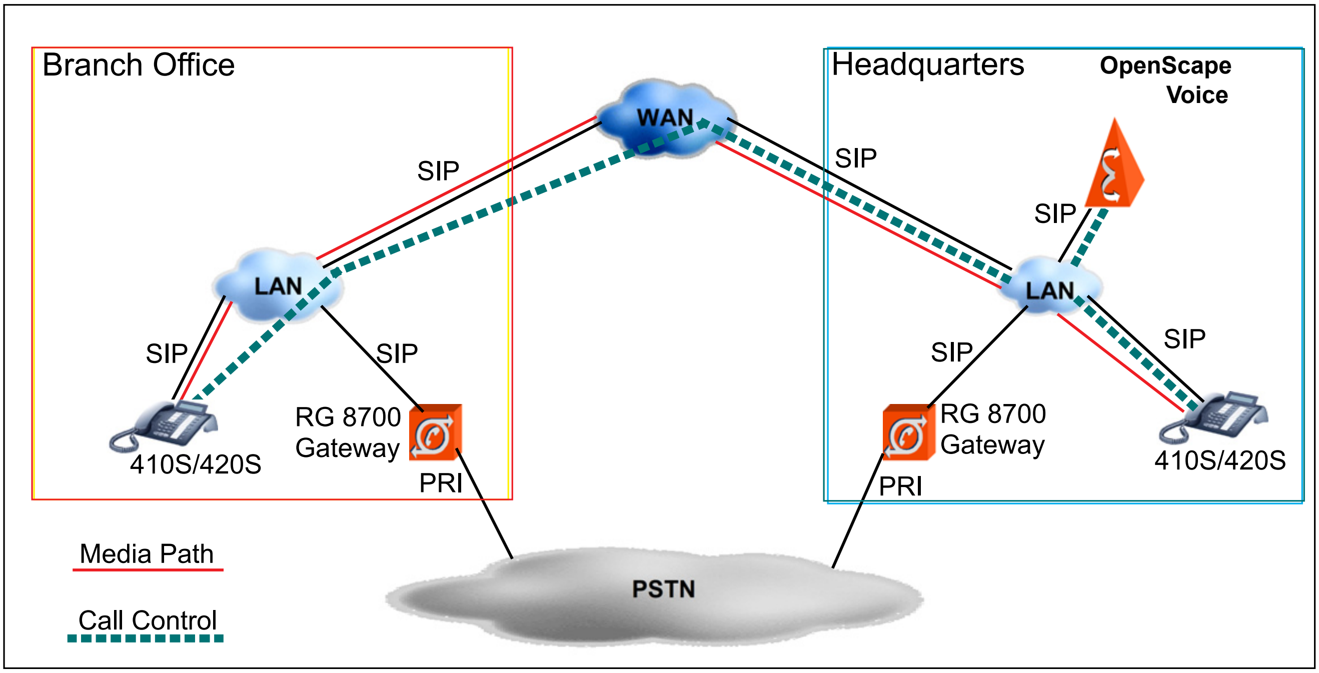


Figure 33 RG 8700 Normal Mode Operation—Headquarters to Branch

9.1.2 Survivability Mode—Headquarters to Branch

If the WAN or Unify OpenScape Voice is not operable, the RG 8700 enters the survivability mode of operation as shown in Figure 34, "RG 8700 Survivability Mode Operation—Headquarters to Branch".

- Survivable endpoints remain registered on the RG 8700. Endpoints not registered on the RG 8700 do not function until connectivity to Unify OpenScape Voice is restored.
- When the RG 8700 detects loss of connection to Unify OpenScape Voice, it switches to survivability mode and begins routing inbound calls directly to the local phones (or to a PSTN destination) based on its own internal database.
- When the phones determine that Unify OpenScape Voice cannot service a call request, they route their outbound call requests directly to the local RG 8700 gateway. However, the ability of those subscribers to make and receive calls from the PSTN during the outage will be governed by the number of trunks available on the local gateway, because other gateways will be inaccessible during the outage period.
- Features provided by the central Unify OpenScape Voice, such as keyset line status and hunt group operation, will not be available.
- Calls from the branch office to headquarters are routed via the PSTN.
- Calls from headquarters to the branch office are rerouted via the PSTN.

The 2000-subscriber limit in survivability mode is a hard limit, based on memory available in the gateway, and cannot be exceeded. The ability of those subscribers to make and receive calls from the PSTN during the outage will be governed by the number of trunks available on the local gateway, because other gateways will be inaccessible during the outage period.

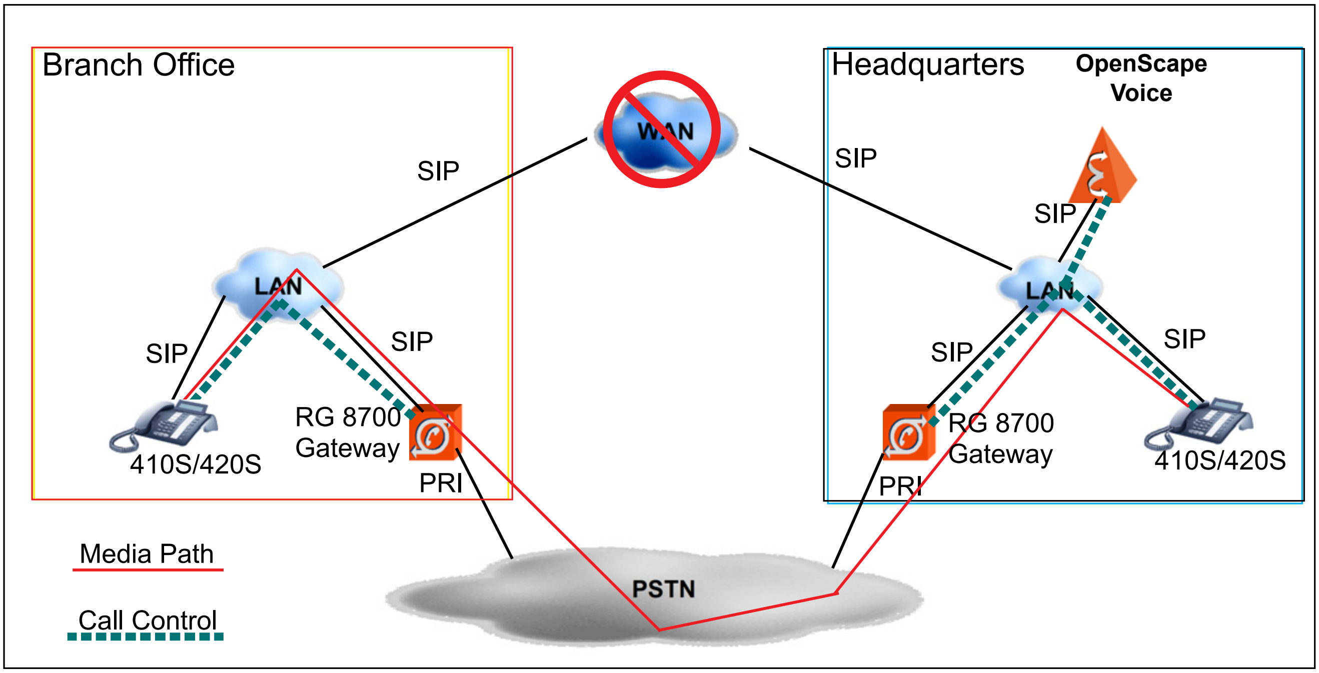


Figure 34 RG 8700 Survivability Mode Operation—Headquarters to Branch

9.1.2.1 SIP Features Available in Survivability Mode

Generally, local SIP phone and SIP client features will still function. Table 85 lists SIP features available in survivable mode.

Available SIP Features		
SIP-to-SIP calls	SIP-to-gateway calls	Gateway-to-SIP calls
Only prime line can be used	Abbreviated dialing list	Local ID shown in idle menu
Digest authentication of client	Ringer on/off function	Directed call pickup
Local three-party conference calls	Tone generation	Hold
Message waiting displayed in idle menu	Local (unsynchronized) display of time of day clock	Attended and unattended transfer
Local forwarding	Call duration time display	Consultation and alternate
Music on hold and call park (only if local functions)	Repertory dialing (assuming number is reachable)	Display of customer's logo and name
Headset operation: open listening, speakerphone, and mute		Do not disturb

Table 85 SIP Features Available in Survivable Mode (Seite 1 von 2)

Available SIP Features		
Missed call list	Drop call key	Inband DTMF generation
Repeat dial list		

Table 85 SIP Features Available in Survivable Mode (Seite 2 von 2)

9.1.2.2 Additional Features Available in Survivability Mode

- Support for basic ISDN calls in survivability mode
- Emergency services (for example, E9-1-1) supported via channel bank to CAMA trunk
- Basic CDR records preserved on the RG 8700
- Advice of charge (AOC) during call only (International Market only)
- Hunt groups within single RG 8700, no overflows possible
- Trunk group access code (for example: 0-9) is stripped before relaying to PSTN
- Full subscriber number dialing required between extensions in different business groups

9.1.3 Planning

There are several things a planner should consider. In sizing the gateway for the appropriate number of T1/S1 or E1/S2 spans, the planner must consider:

- The amount of traffic that will pass through the gateway in normal operation
- The blocking factor that will be tolerated due to an all-channels-busy condition
- The number of subscribers that will use the gateway in survivability mode
- The level of service that is acceptable in survivability mode

The users must be informed that in the survivability mode, the features supported are significantly reduced.

9.2 Private Network Interfaces

Unify OpenScape Voice supports two separate private network protocols and networked features: SIP-Q (QSIG protocol over SIP) and SIP (native trunking).

Note: A SIP private network is a project-specific release.

A customer network may deploy either a SIP-Q or SIP private network. They are mutually exclusive and may not coexist, with the following exceptions:

- A SIP-Q private network and SIP Trunking to SBCs/Service Providers (refer to Section 6.9.3, “SIP Trunking”) may coexist. Feature interoperability between the two networks is provided where possible, but is not guaranteed.
- In hosted environments, although one customer network (business group) must not deploy coexisting SIP and SIP-Q private networks, each separate customer network hosted on Unify OpenScape Voice may employ either SIP private networking or SIP-Q private networking—that is, the network coexistence limitation only applies at the business group level, not at the system level.
- A customer with legacy CorNet-NQ/QSIG servers in the network should deploy a SIP-Q private network. Customers with no legacy products should deploy a SIP private network.

9.2.1 SIP-Q Private Networking Overview and Features

In this section:

- *QSIG* is a signaling protocol that permits the interconnection of other vendors’ QSIG-compliant PBXs (*QSIG PBXs*) to Unify PBXs. It also provides for IP network connectivity.
- *CorNet-NQ* is a Unify proprietary QSIG-based signaling protocol for interconnecting Unify OpenScape Voice systems to one or more QSIG PBX systems. It is a superset of the QSIG-defined Q.931/Q.932 protocol extensions.

The SIP-Q protocol—which refers to SIP signaling with QSIG protocol, with Unify CorNet-NQ extensions, embedded as a MIME for call control and supplementary service interoperability according to ECMA 339—is used for the following:

- Interworking between Unify OpenScape Voice systems when legacy servers are present in the network.
- Interworking between Unify OpenScape Voice and other systems that support the SIP-Q procedures—for example, the OpenScape 4000.
- Interworking between the Unify OpenScape Voice system and other systems that support QSIG procedures—for example, an Avaya PBX. In this configuration:
  - SIP-Q is used between Unify OpenScape Voice and a SIP-Q compatible gateway, such as the RG 8700.
  - A QSIG TDM trunk is used between the RG 8700 and the other system.

For a complete discussion of all CorNet variations, refer to the following documents:

- *CorNet Reference Manual*, A31003-H3140-T100-1-7618

9.2.1.1 Feature Availability

Table 86 lists feature availability over SIP-Q.

Feature	**SIP-Q Feature Support**		
	OSV to OS4K	**OSV to OSV**	**OSV to HiPath 3000**
Basic Call	Yes	Yes	Yes
E 911 Location Identification Number (LIN)	Yes	Yes	Yes
Call Waiting (CW)	Yes	Yes	Yes
Calling Line Identification Presentation (CLIP)	Yes	Yes	Yes
Calling Line Identification Restriction (CLIR)	Yes	Yes	Yes
Connected Line Identification Presentation (COLP)	Yes	Yes	Yes
Connected Line Identification Restriction (COLR)	Yes	Yes	Yes
Calling/Connected Name Identification Presentation (CNIP)	Yes	Yes	Yes
Calling/Connected Name Identification Restriction (CNIR)	Yes	Yes	Yes
Do Not Disturb (DND) (see note 1)	Yes	Yes	Yes
Do Not Disturb Override (DNDO)	No	No	No
Call Deflection (CD) (per call/user invoked)	Yes	Yes	Yes

Table 86 QSIG/CorNet-NQ Feature Support via SIP-Q (Seite 1 von 2)

Feature	SIP-Q Feature Support		
	OSV to OS4K	OSV to OSV	OSV to HiPath 3000
Call Offer (CO) (see note 1)	No	No	No
Call Intrusion (CI) (override) (see note 1)	Yes	Yes	Yes
Recall (RE) (transfer security)	Yes	Yes	Yes
Malicious Call Identification (see note 1)	Yes	Yes	Yes
Call Hold/Retrieve (CH)	Yes	Yes	Yes
Advice of Charge (AOC)	No	No	No
Three Way Conference (see note 1)	Yes	Yes	Yes
Call Diversion (CFSD)	Yes	Yes	Yes
Call Forwarding Unconditional (CFU)	Yes	Yes	Yes
Call Forwarding Busy (CFB)	Yes	Yes	Yes
Call Forwarding No Reply (CFNR)	Yes	Yes	Yes
Path Replacement (ANF-CR)	Yes	Yes	No
Call Transfer (by Join) (CT)	Yes	Yes	Yes
Explicit Call Transfer (by Join)	Yes	Yes	Yes
Call Completion to Busy Subscriber (CCBS)	Yes	Yes	Yes
Call Completion on No Reply (CCNR)	Yes	Yes	Yes
Message waiting indication (MWI) for voice mail	Yes	Yes	Yes
Single Step Call Transfer (reroute) (SSCT)	No	No	No
Call Park (PARK)	No	No	No
Call Pickup (PICKUP) (see note 2)	Yes	Yes	Yes
Notes: 1. Local function only. 2. Local function only; however, pickup across networksare supported.			

Table 86 QSIG/CorNet-NQ Feature Support via SIP-Q (Seite 2 von 2)

9.2.1.2 OpenScape 4000 Networked Feature Availability

Table 87 lists QSIG/CorNet-NQ networked features between Unify OpenScape Voice and the OpenScape 4000; it does *not* consider Unify OpenScape Voice local feature interworking with the OpenScape 4000—for example, DND and call waiting terminating (CWT). Many of these networked features are subject to limitations (such as display issues) and/or had enhancements to enhance the functionality after it was initially introduced.

Unify OpenScape Voice Networked Feature	OpenScape 4000
Basic call and generic functions	•
CLIP CLIR	•
COLP COLR	•
Hold/retrieve	•
Call transfer	•
Transfer security/recall	•
Path replacement	•
Call forward	•
CCBS/NR/automatic callback	•
CCBS/NR path reservation	•
Message waiting	•
IOC (CDR global identifier/thread identifier)	•
Network call pickup	•
SPE	•
E9-1-1 LIN	

Table 87 OpenScape 4000 Networked Feature Availability

9.2.2 SIP Private Networking Overview and Features

Unify OpenScape Voice's SIP private network uses a native SIP protocol that includes support for IETF "SIP Service Examples" in RFC 5359 and many other features using IETF RFC SIP building blocks. Unify OpenScape Voice is a B2BUA (Back-to-Back User Agent) and interoperates with many other SIP network entities such as:

- SIP proxy/registrars
- SBCs
- SIP/PSTN gateways
- SIP media servers
- SIP Service Provider (may be represented by a SIP proxy or SBC as a single point of entry)
- DNS server
- ENUM server
- Clients (phones and soft clients)

The following URI schemas are supported for incoming and outgoing requests:

- SIP
- SIPS
- TEL (see RFC 3966)

Table 88 lists IETF RFC SIP compliance support for SIP network services.

SIP Method	Reference	Compliance (see note)	Remarks
ACK	RFC 3261	C	
BYE	RFC 3261	C	
CANCEL	RFC 3261	C	
INFO	RFC 3261	PC	• INFO messages may be passed transparently based on Content-Type and OSV configuration options. • INFO message are sent/received for tunneling QSIG in the SDP body.
INVITE	RFC 3261	C	• With or without SDP supported. • With or without M-lines supported.
MESSAGE	RFC 3428	PC	Not currently supported for NNI interfaces.
NOTIFY	RFC 3265	PC	Supported for call forwarding, message waiting indication, and CCBS/NR.
OPTIONS	RFC 3261	PC	Only supported as keep-alive or audit mechanism.
PRACK	RFC 3262	C	
PUBLISH	RFC 3903	PC	Tandem transmittal only.

Table 88 IETF RFC SIP compliance support for SIP Network Services (Seite 1 von 2)

SIP Method	Reference	Compliance (see note)	Remarks
REFER	RFC 3515	C	• Unify OpenScape Voice supports the SIP REFER method when received from an Xpressions server connected via SIP interface to initiate a single-step call transfer. Unify OpenScape Voice performs the call reconfiguration itself, and sends re-INVITEs to the other party in the call. Therefore, Unify OpenScape Voice does not send a REFER message over network. • Unify OpenScape Voice may be configured to proxy (pass transparently) SIP REFER requests (and the responses) within a dialogue instead of performing the call reconfiguration itself.
REGISTER	RFC 3261	C	Third-party registrations are allowed—for example, for HiPath 3000 and OpenScape 4000 gateways—but not required.
SUBSCRIBE	RFC 3265	PC	Unify OpenScape Voice supports receiving SUBSCRIBE for the following event packages: • ccbs • ccnr
UPDATE	RFC 3311	PC	Unify OpenScape Voice supports the use of UPDATE for SDP negotiation during session setup. After a dialog is established, Unify OpenScape Voice sends and receives UPDATE for session timer refresh.
Unknown methods	RFC 3261		Tandemed transparently.
Note: Compliance is classified as follows: • C: fully compliant • PC: partially compliant • NC: noncompliant or not supported • Blank: not applicable to the particular service			

Table 88 IETF RFC SIP compliance support for SIP Network Services (Seite 2 von 2)

9.2.3 SIP-Q Private Networking to OpenScape 4000

Unify OpenScape Voice is connected to the OpenScape 4000 through using the SIP-Q protocol:

The OpenScape 4000 uses the HG 3500 gateway cards. These cards come in two models with different capacities; the smaller model supports 60 simultaneous SIP-Q connections, and the larger model supports up to 120 simultaneous SIP-Q connections.

9.2.3.1 Normal Mode—Headquarters to Branch

In order to provide continued operation in WAN failure scenarios, the applicable gateway card is logically connected to Unify OpenScape Voice through OpenScape Branch proxy located in the branch. This means the gateway registers with the proxy, and the proxy relays the registration to Unify OpenScape Voice. The phones that require continued operation during a failure must also register with the proxy.

During normal operation, all SIP-Q signaling between Unify OpenScape Voice and the gateway, and all SIP signaling between Unify OpenScape Voice and the survivable branch phones, passes through the proxy. The proxy operates transparently, but learns about the configuration of the branch by examining the SIP signaling as it passes through.

In normal mode, Figure 35, "Unify OpenScape Voice to OpenScape 4000 — Normal Mode", the full functionality of Unify OpenScape Voice is available to all the phones in the branch.

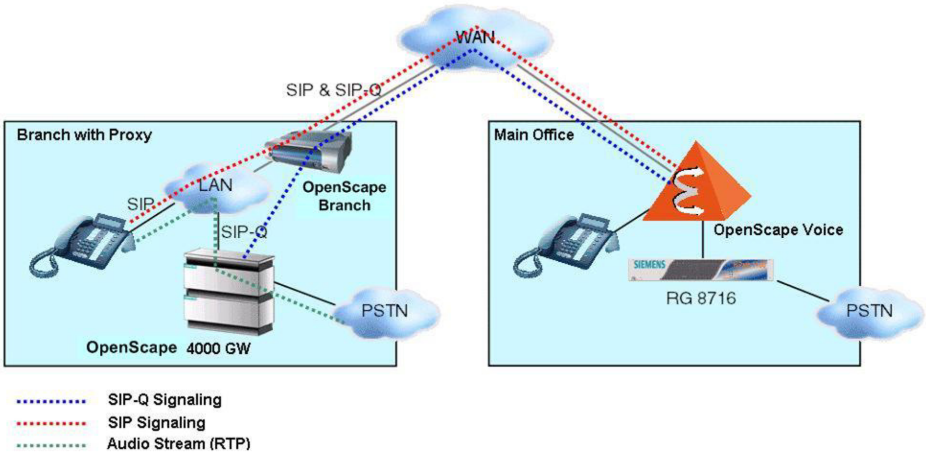


Figure 35 Unify OpenScape Voice to OpenScape 4000 — Normal Mode

9.2.3.2 Survivability Mode—Headquarters to Branch

The proxy maintains a SIP heartbeat signal with Unify OpenScape Voice so it can detect a WAN outage. When an outage is detected, the proxy takes over, ctivates its SIP switching function, and provides basic calling functionality during the outage.

Via SIP, the phones are passed an indication that the system has entered emergency (also known as survivability) mode, Figure 36, "Unify OpenScape Voice to OpenScape 4000 - Survivability Mode". Because the phones are already registered on the proxy, they are not otherwise aware of the failure and continue to function normally.

Basic functions like internal calling, calls to and from the local gateway, hold, consultation, transfer, local forwarding, local conference, calling and called party name and number, and E911 can continue to function. Features provided from Unify OpenScape Voice, such as keyset line indications and hunt group operation, are not available during the WAN outage interval.

To guard against the possibility of a proxy outage, the phones should also be configured to register directly with Unify OpenScape Voice as a second choice registrar/server. If the proxy fails, Unify OpenScape Voice begins signaling directly to the phone and gateway, and likewise the phone and gateway signal directly to Unify OpenScape Voice, bypassing the failed proxy. Therefore, a proxy failure results in no noticeable change of operation to the end user. All Unify OpenScape Voice features will still be available.

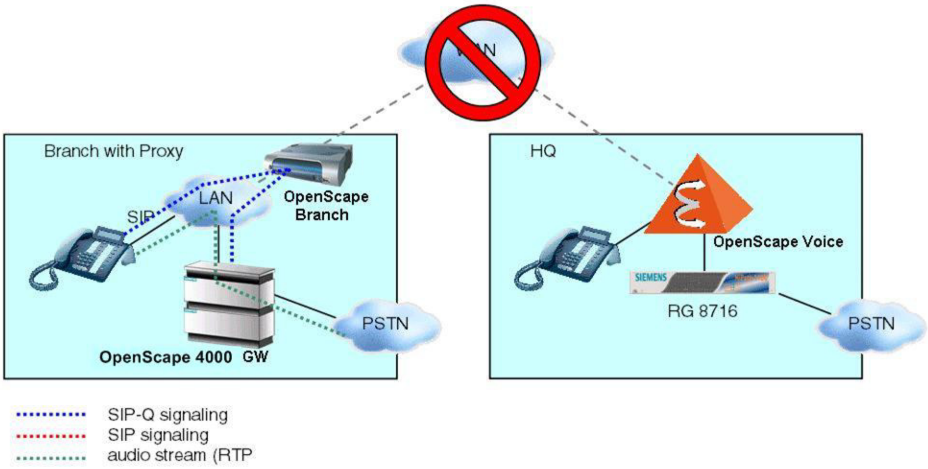


Figure 36 Unify OpenScape Voice to OpenScape 4000 - Survivability Mode

9.2.4 SIP-Q Private Networking to HiPath 3000

Unify OpenScape Voice is connected to the HiPath 3000 through the HG 1500 gateway card. Depending on the model, the following interfaces are provided:

- **HiPath 3800**: Up to five T1 or four E1 interfaces; up to 120 analog interfaces
- **HiPath 3500**: One T1/E1 interfaces; up to 16 analog interfaces

The following are the supported scenarios:

Note: These capabilities are only available on a PSR basis.

- HiPath 3000 as an exchange gateway for Unify OpenScape Voice for digital exchange lines (ISDN, CAS, T1) with no terminals connected to the HiPath 3000 gateway
- Single HiPath 3000 system as an exchange gateway for digital exchange lines (ISDN, CAS, T1) for Unify OpenScape Voice with TDM (digital, analog, DECT) subscribers connected to the HiPath 3000 gateway
- Several HiPath 3000 systems as exchange gateways for digital exchange lines (ISDN, CAS, T1) for Unify OpenScape Voice with TDM (digital, analog, DECT) subscribers connected to the H3K gateways

Figure 37 shows operation in normal mode.

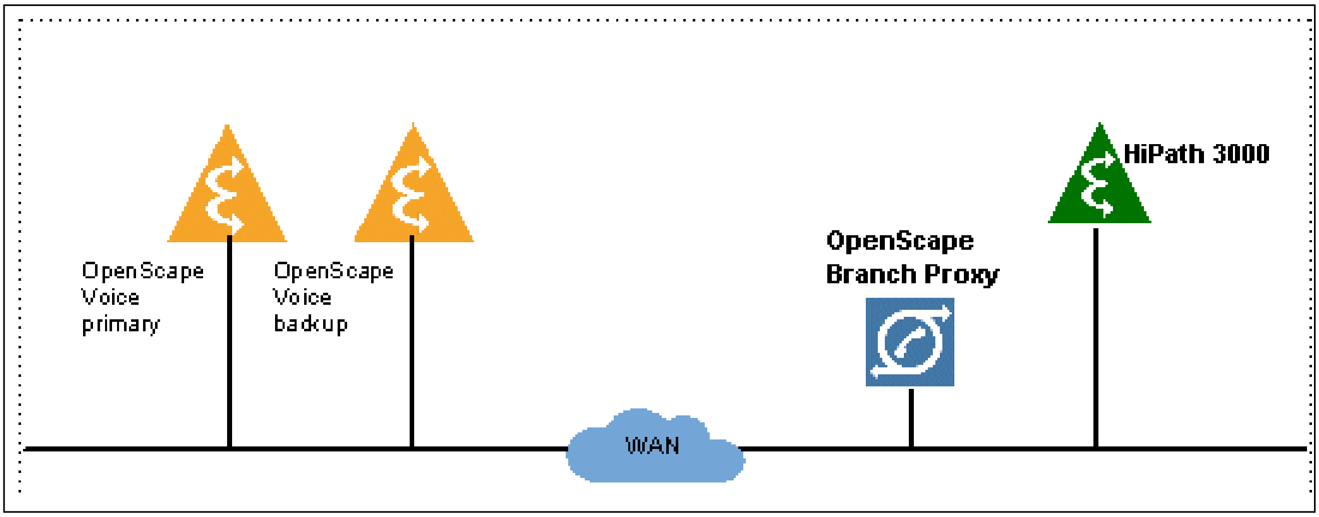


Figure 37 Unify OpenScape Voice to HiPath 3000—Normal Mode

9.2.5 SIP-Q Private Networking Between Unify OpenScape Voice Systems

Figure 38, "Two Unify OpenScape Voice Systems in Simple SIP-Q Network—Physical Connectivity" shows the physical connectivity for a simple network of two Unify OpenScape Voice systems in a network; each is a duplex system consisting of two processing nodes.

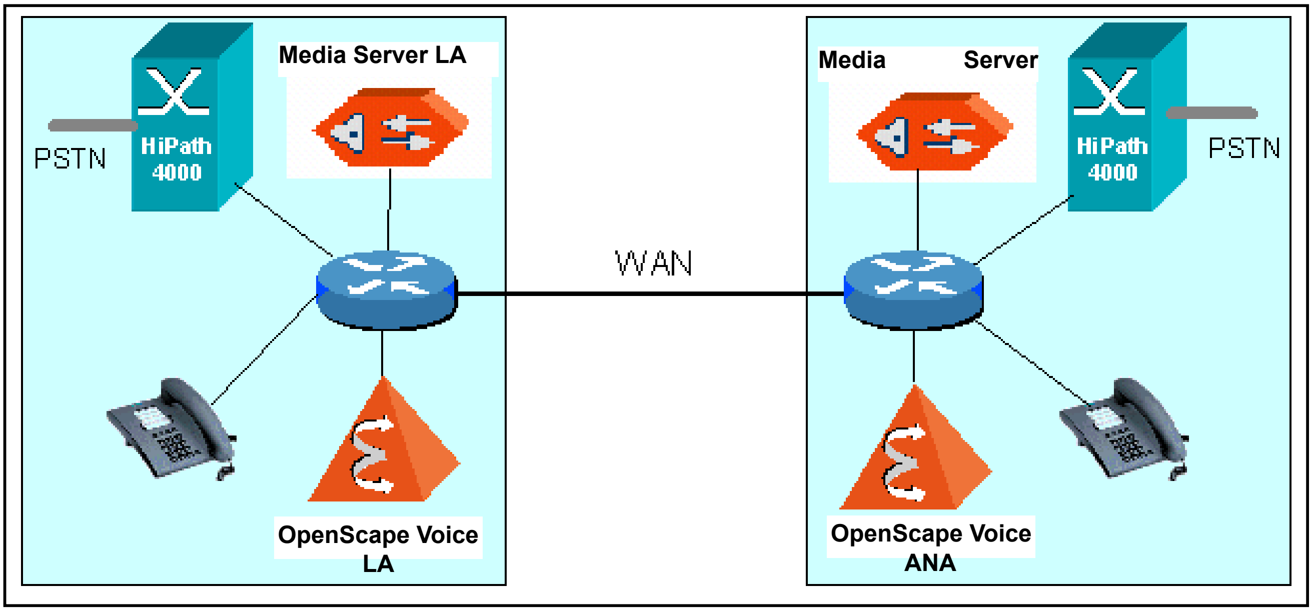


Figure 38 Two Unify OpenScape Voice Systems in Simple SIP-Q Network—Physical Connectivity

The logical connectivity among the boxes (Figure 39) may look quite different from the physical connectivity shown in Figure 38.

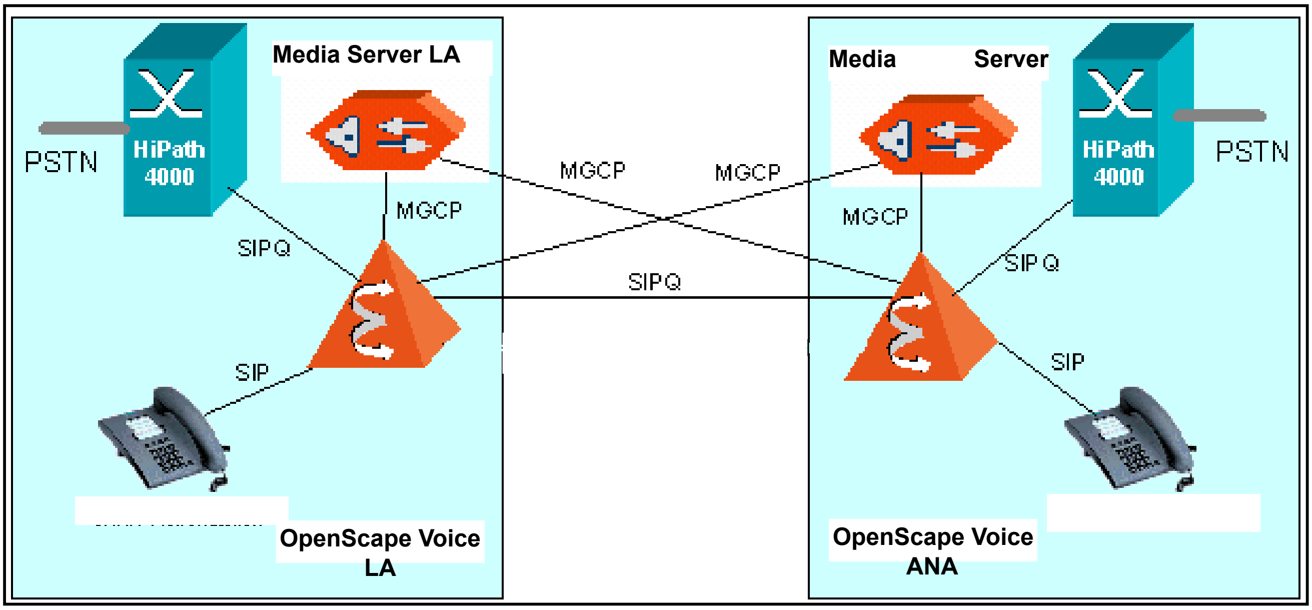


Figure 39 *Two Unify OpenScape Voice Systems in Simple SIP-Q Network—Logical Connectivity*

In Figure 39:

- The OpenScape 4000 switches, each equipped with one or more HG 3500 gateway cards, provide the PSTN interface. Because of the larger message sizes resulting from the QSIG additions to SIP, the signaling link between Unify OpenScape Voice and HG 3540 must be TCP (UDP and TLS are not options).

  The gateways are defined in the Unify OpenScape Voice database as SIP endpoints. Unify OpenScape Voice supports multiple gateways, each defined as an endpoint. In addition to the normal configuration, the SIP-Q option flag must be checked during the configuration of the endpoint. The maximum number of sessions (calls) value should be set to a value that is compatible with the gateway capacity.

- Each HG 3540 or HG 3500 supports only one Unify OpenScape Voice system. This means that it accepts SIP-Q signaling from only one Unify OpenScape Voice, and routes all inbound PSTN calls to that Unify OpenScape Voice system. Therefore, if traffic from the LA gateway is destined for a subscriber in ANA, the signaling will “tandem” through the LA Unify OpenScape Voice (and the ANA Unify OpenScape Voice) even though the audio stream takes a direct path from the gateway to the SIP subscriber.

Routing can be arranged so that tandem SIP-Q traffic from one OpenScape 4000 gateway can flow through the two Unify OpenScape Voice softswitches as SIP-Q tandem traffic, and out to a gateway on the other OpenScape 4000 system. In this manner, CorNet-NQ calls from the TDM domain can utilize the Unify OpenScape Voice network as a virtual CorNet-NQ link to the other OpenScape 4000 system, with no loss of CorNet-NQ features. To accomplish this:

- Within each Unify OpenScape Voice, the partner Unify OpenScape Voice is defined as a permanently registered SIP endpoint, with authentication by endpoint, and with the SIP-Q option flag set. The maximum number of sessions (calls) value for the endpoint should be set to a value that is compatible with the expected tandem traffic level.

- After the endpoints are defined, the appropriate destinations, routes, and numbering plan entries need to be made in each Unify OpenScape Voice to permit the tandem calls.

- The endpoints (gateways and peer Unify OpenScape Voice systems) should most probably be marked as trusted endpoints, to prevent unwanted SIP digest authentication challenges on these links.

Note: In order for SIP-Q features such as CCBS to work, the gateway endpoint must be given an endpoint profile which is assigned to the same BG as the Unify OpenScape Voice subscriber who is the originator or target of the call.

Figure 39 also illustrates that the media server can be shared by multiple Unify OpenScape Voice systems, and the Unify OpenScape Voice system can utilize multiple media servers. However, if the media server is located remotely, the customer impact of a WAN outage need to be considered since the remote media server would be unreachable during the outage.

- Basic calling, incoming, outbound, and internal, are not blocked by a media server outage, and many features will continue to function (click to dial, pickup groups, hunt groups, keyset groups, forwarding, and so on). However, some features require audible prompting, and those features would not be usable during the WAN outage. If the media server provides voice mail service, voice mail would not be accessible from the remote location during the outage period.
- Unify OpenScape Voice supports multiple media servers for specialized functions and for geographic distribution of subscribers. Multiple media servers can be configured in a primary/secondary configuration so that in the event that one media server is unreachable, the alternate media server can be utilized.

Extension dialing between the Unify OpenScape Voice systems, and between the Unify OpenScape Voice systems and the OpenScape 4000 subscribers, can be configured. However, there are numerous feature restrictions when calls go between Unify OpenScape Voice switches, or between Unify OpenScape Voice and a OpenScape 4000 subscriber. Refer to the SIP-Q feature support list in Section 9.2.1.1, “Feature Availability”.

9.2.6 SIP Private Networking Between Unify OpenScape Voice Systems

Figure 40, "Two Unify OpenScape Voice Systems in SIP Private Network" shows a a simple network of two Unify OpenScape Voice systems in a network. SIP protocol is used from end to end, and there are no legacy systems present.

An Unify OpenScape Voice SIP private network is based on open standards, including the publications of ISO/IEC, JTC1, ITU-T, ETSI, ECMA, IETF (RFCs and draft RFCs), and other national/international standardization bodies.

The private network allows Unify OpenScape Voice registered user agents/clients to communicate with other users/resources in the private network. The users are connected directly via the LAN/WAN using SIP protocol.

The SIP private network interface is generally used only for the following:

- Calls between Unify OpenScape Voice users on two separate Unify OpenScape Voice systems.
- Calls between Unify OpenScape Voice users on separate systems placed through an Unify OpenScape Voice tandem system. This usage is not common.

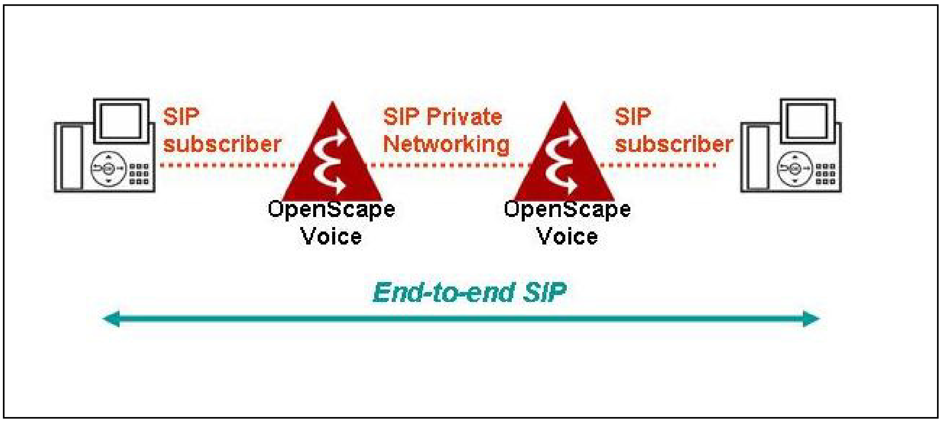


Figure 40 Two Unify OpenScape Voice Systems in SIP Private Network

In this scenario, the following features and services are supported:

- CDR information transport
- Call completion (CCBS/NR)
- Identification services

  This includes support for Additional Party Number (APN), which permits the calling party's public number (for sending to PRI) and private number (for billing purposes) to be sent to a gateway.
- Message waiting indication
- Name identification services
- Emergency services (E9-1-1)

- Call diversion/forwarding
- Hold/toggle/consultation
- Call transfer (blind, semi-attended and consultation)
- Private numbering plan
- Carrier Services: Carrier Identification

However, no path replacement or throwback is supported.

The following are important attributes when defining SIP private networking endpoints:

- SIP Private Networking: When selected, this attribute, located on the endpoint’s SIP tab, identifies a SIP interface as a SIP private networking interface.
- Public/Offnet Traffic: This attribute, located on the endpoint’s Attributes tab, is only applicable to SIP Trunking. For that reason, it must *not* be selected.

9.3 Small Gateways

Sometimes in a branch solution, a small gateway is used to facilitate communication to the central office (CO) as well as to provide survivability in case of WAN or Unify OpenScape Voice failure.

The column labeled **Users Supported** in Table 89 only applies to survivability mode, and even then it is only a typical or suggested number. Because OpenScape Branch proxy provides the call control intelligence in survivability mode, this gateway imposes no fixed limit on the number of users that can be supported in this mode.

Gateway Model	SIP Proxy Server Options*	Users Supported	Interfaces
Mediatrix 1204 (US)	• OpenScape Branch	16 users	4-port analog
Mediatrix 4402 Advanced (IM)	• OpenScape Branch	16 users	2-port S0
Mediatrix 4404 Advanced (IM)	• OpenScape Branch	50 users	4-port S0

Table 89 Survivable Media Gateway Solutions for Small Branches and Offices(Seite 1 von 2)

Gateway Model	SIP Proxy Server Options[*]	Users Supporte d	Interfaces
Mediatrix 3600 (US/IM)	• OpenScape Branch	150 users	1T1/1E1
RG 8702	Not required	200 users	1 or 2 T1/E1 spans (PRI)

Table 89 Survivable Media Gateway Solutions for Small Branches and Offices(Seite 2 von 2)

[*] These servers are only needed if the Survivability option is purchased.

The Mediatrix gateways listed in Table 89 have the following characteristics:

- Phones are registered directly at the proxy server.
- The proxy server forwards all signaling of the phones and gateway to the central Unify OpenScape Voice.
- When the link to Unify OpenScape Voice is broken, the proxy provides the emergency switching and routing function as described in Section 9.2.3.2, “Survivability Mode—Headquarters to Branch”.

Refer to Section 9.1, “RG 8700” for description of the RG 8702.

9.3.1 Normal Mode

Figure 41 shows the Mediatrix branch solution operating in normal mode.

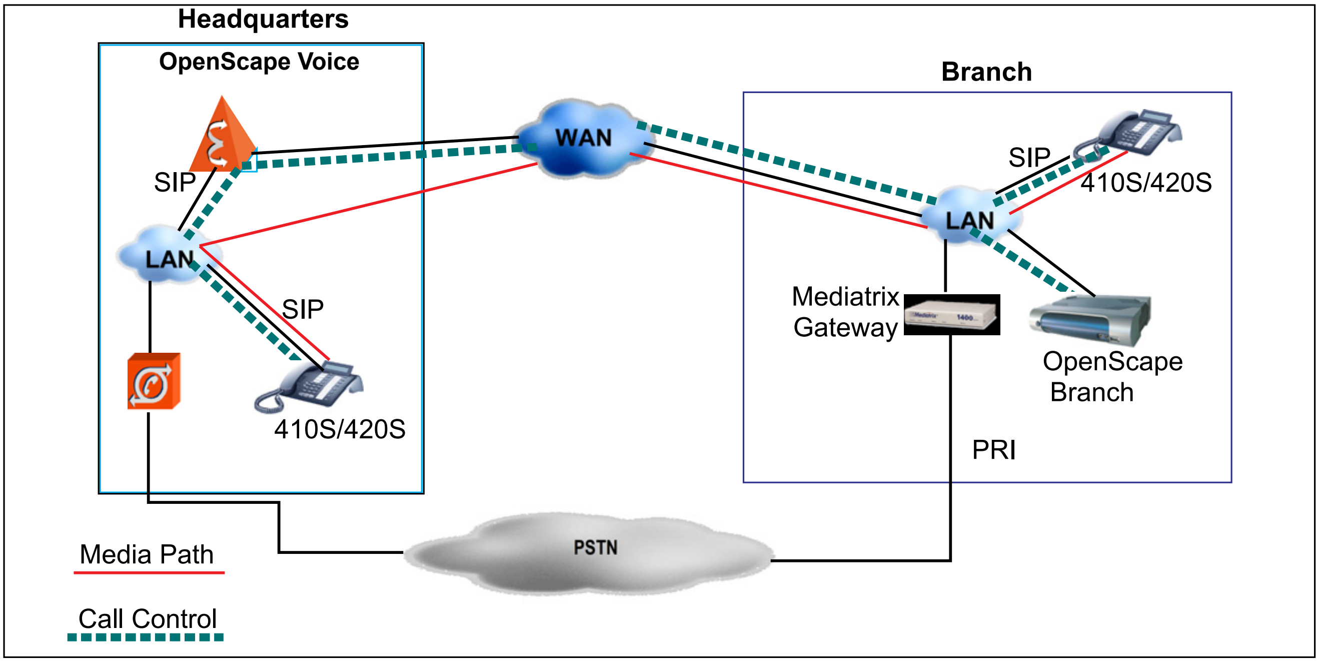


Figure 41 Mediatrix Branch Solution—Normal Mode

9.3.2 Survivability Mode

Figure 42, "Mediatrix Branch Solution—Survivability Mode" shows the call control and media paths in case of WAN failure.

- Dual registration support is not needed by branch endpoints.
- OpenScape Branch proxy will forward the branch’s external calls via the Mediatrix gateway to the target destination.
- A limited feature set is available for all branch office users.
- The centrally configured Unify OpenScape Voice features are not available.
- Calls from the branch office to headquarters are routed via the PSTN.
- Calls from the headquarters to the branch office are rerouted via the PSTN.

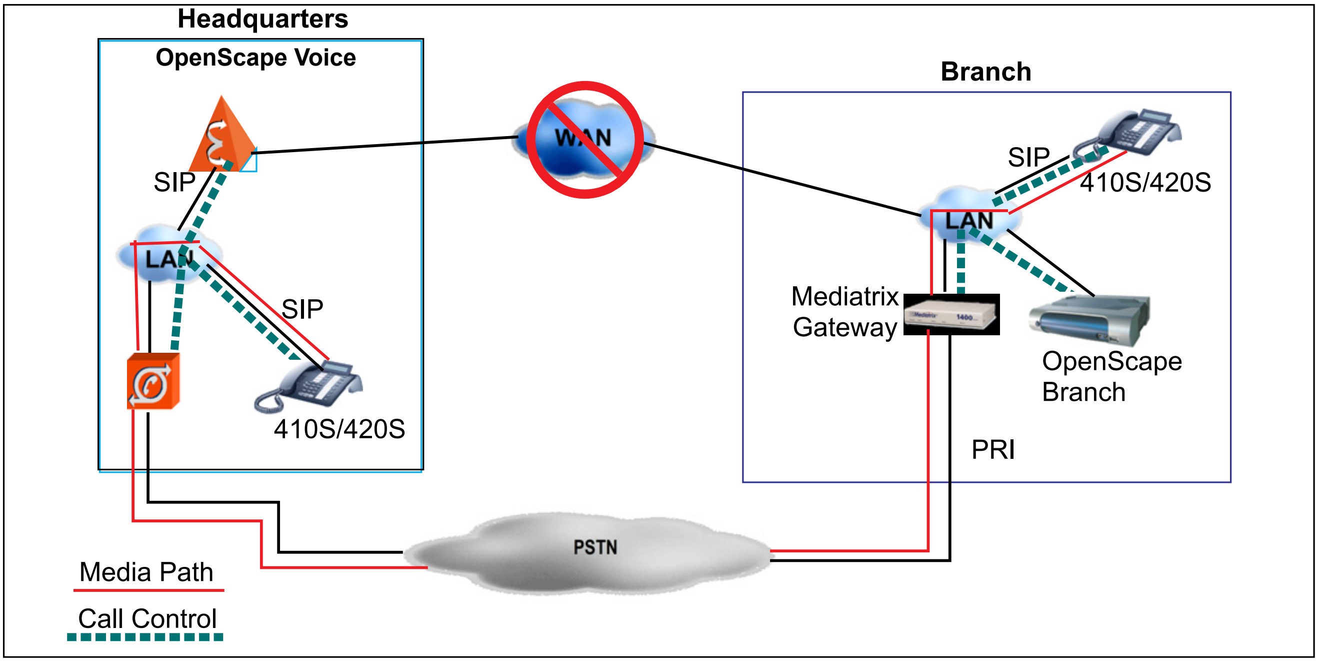


Figure 42 *Mediatrix Branch Solution—Survivability Mode*

9.4 SIP Trunking

Many enterprises are already using VoIP; however, many are only using it for communication on the enterprise LAN. In this scenario, VoIP is only being used as a one-to-one replacement for traditional wireline telephony. For all calls made to the outside of the LAN, a PSTN gateway on the enterprise edge is used. These businesses realize a solid return on investment (ROI) just by lowering administrative costs and the costs associated with calls made within the company.

With SIP trunking, the potential for ROI is far greater because SIP trunking takes the idea of VoIP a step beyond this LAN application. The full potential for IP communications can be realized only when the communication is taken outside of the corporate LAN.

SIP trunking delivers several benefits, such as the following:

- It eliminates costly ISDN BRIs and PRIs.
- There is no need to invest in PSTN gateways and additional line cards as the enterprise grows.
- Edge devices offer a low-investment path in adding new lines because they are less expensive per line than the corresponding PSTN gateway.

- It permits optimal utilization of bandwidth by delivering both data and voice in the same connection.
- It gives maximum flexibility in dimensioning and usage of lines because capacity is not purchased in bundles of 23 (T1) or 30 (E1) lines.
- It provides flexible termination of calls to preferred providers; calls to anywhere worldwide can be made for the cost of a local one.
- Redundancy with multiple service providers and links is available.

Interface requirements currently differ significantly between SIP service providers, although progress is being made to standardize the enterprise/SIP service provider interface in standards bodies such as the SIP Forum.

The Unify OpenScape Voice SIP trunking interface to SIP service providers is described in the *Unify OpenScape Voice Interface Manual: Volume 6, SIP Service Providers Interface*.

Typically, an SBC is used at the enterprise side of the SIP trunk to secure the enterprise from the SIP service providers network. Refer also to Section 6.9.3, “SIP Trunking”. However, if the enterprise customer is satisfied with the security level provided by the SIP service provider—for example, when the SIP trunk is connected via a VPN connection and/or a SBC at the service provider side of the trunk—use of a SBC for SIP trunking is not essential.

The SIP trunking interface provides the following customization options when sending SIP requests:

- The ability to send the P-Preferred-Identity (PPI) SIP Header field, rather than the P-Asserted-Identity (PAI) SIP header field.
- The ability to send the domain name, rather than the IP address, in the host part of the SIP From Header field.
- The ability to send the domain name of "anonymous.invalid", rather than the IP address, if the caller has Calling Line Identity Presentation Restricted (CLIR) active.
- The ability to send the SIP From and PPI header fields with the identity of the transferring/forwarding party, rather than the calling party, when a call is transferred or forwarded.
- The ability to always send SIP reINVITE requests with SDP.

These options are primarily relevant for SIP trunking to service providers that use a non-standard SIP interface—for example, Italtel. Each can be enabled and disabled via Unify OpenScape Voice Assistant or the CLI. Unify OpenScape Voice Assistant also provides the ability to use endpoint templates that automatically assign these SIP attributes to SIP trunking endpoints without having to manually assign each attribute individually.

Unify OpenScape Voice has successfully interoperated with SIP Service Providers including Verizon (USA and Europe), Level3, Cbeyond, Italtel, Arcor, T-Systems, BT, and Entel.

9.5 Analog Adapters

In some cases a customer may wish to connect fax machines or other analog equipment to Unify OpenScape Voice. In these cases, an analog adapter is required. An analog adapter is very similar to an analog gateway, except that the analog circuits are conditioned for connection to a telephone (or analog modem or fax machine) rather than an analog central office trunk circuit.

The following analog adapters can be used with Unify OpenScape Voice:

- **Mediatrix 4102**: Two ports
- **Mediatrix 4104:** Four ports
- **Mediatrix 4124:** 24 ports

All are available in Europe, the United States, and the United Kingdom.

Note: These adapters support SRTP, permitting support of encryption of the connection between the adapter and SIP endpoints that also support this encryption type. Refer also to Section 15.1, “Media Encryption”.

The HiPath AP 1120 analog adapters have two foreign exchange station (FXS) ports and two 10/100 Base-T Ethernet ports that can be used with Unify OpenScape Voice.

Note: Purchase orders of the HiPath AP 1120 for new installations are no longer availabe. In addition, these analog adapters do not support SRTP. Therefore, it should be replaced by the Mediatrix 4102, particularly when secure media is required.

9.5.1 Voice Call Operation

The analog adapter configured for voice calling looks to Unify OpenScape Voice as a standard SIP telephone which can make and receive calls. The adapter provides the ringing voltage needed to ring the telephone when a call arrives.

Call origination is via enbloc dialing – the adapter collects all the digits, and the originates the call to Unify OpenScape Voice via standard SIP protocol (an INVITE message). Rotary dial phones are not supported.

If the analog phone has a flash or consultation key, or can support a hook flash, then features such as consultation, transfer, alternating, and three-party conference are possible. Most adapters must be configured to support either alternating or three-party conference, not both.

Some adapters support caller ID presentation to the phone, if the phone supports the analog PSTN-style caller ID functionality. The adapter provides the necessary translation between the SIP messaging and the caller ID protocol to the phone.

9.5.2 Fax Call Operation

The following are guidelines to manage fax call traffic:

- It is possible to segregate fax traffic (for example, sending it to a different gateway or trunk group) using endpoint class of service. Class of service is one of the variables that Unify OpenScape Voice takes into account during the routing process.
- T.38 is the normally the preferred transmission mechanism over the IP network. If the analog adapter and destination SIP endpoint (in this case the SIP gateway to the PSTN) both support T.38, T.38 transmission will be used. This is sometimes referred to as *fax relay*.
- If either the analog adapter or the egress gateway does not support T.38, or T.38 has been disabled via configuration, the fax modem signal will normally be transmitted using the G.711 voice encoding. This is referred to as *transparent mode*. When the originating device is operating in transparent (G.711) mode, the destination device (usually a SIP gateway to the PSTN) will be unaware that the call is a fax call. In that case, the T.30 tones are exchanged transparently end-to-end, from the source fax machine to the ultimate destination fax machine.
- Fax transmission in the PSTN is governed by the ITUT T.30-related standards. The egress gateway is responsible for the conversion from T.38 to T.30 transmission at the PSTN interface.

The call flow as depicted in Figure 43, "Analog Adapter Fax Call flow" shows a fax machine and an analog telephone connected to an analog adapter. In the scenario that is illustrated here, an assumption is that the fax machine places the call. A typical sequence would follow similar to this:

1. The fax machine goes off-hook and dials.
2. When dialing is complete, the adapter initiates a SIP call to Unify OpenScape Voice by sending a SIP INVITE with the complete destination number. The analog adapter may be configured to include a fax indication in the SDP of the INVITE message. Alternately, a call may start as a normal voice call and transition into FAX mode when the T.30 tones are detected, as described below.
3. The destination device (in the PSTN) signals that it is a fax device by sending called party tone (aka fax answer tone) then starts the modem speed negotiation process in-band.   This triggers the start of the T.38 session. If the fax call was originated using a standard telephone handset for supervision, this tone is also a signal to the caller, to switch into fax send mode by pushing the appropriate button and replacing the handset.
4. The sending fax machine typically sends a periodic calling party tone, indicating its desire to deliver a FAX, during the call setup phase. This allows a dual-mode (voice/fax) device at the destination to be switched (manually or automatically) into fax receive mode.

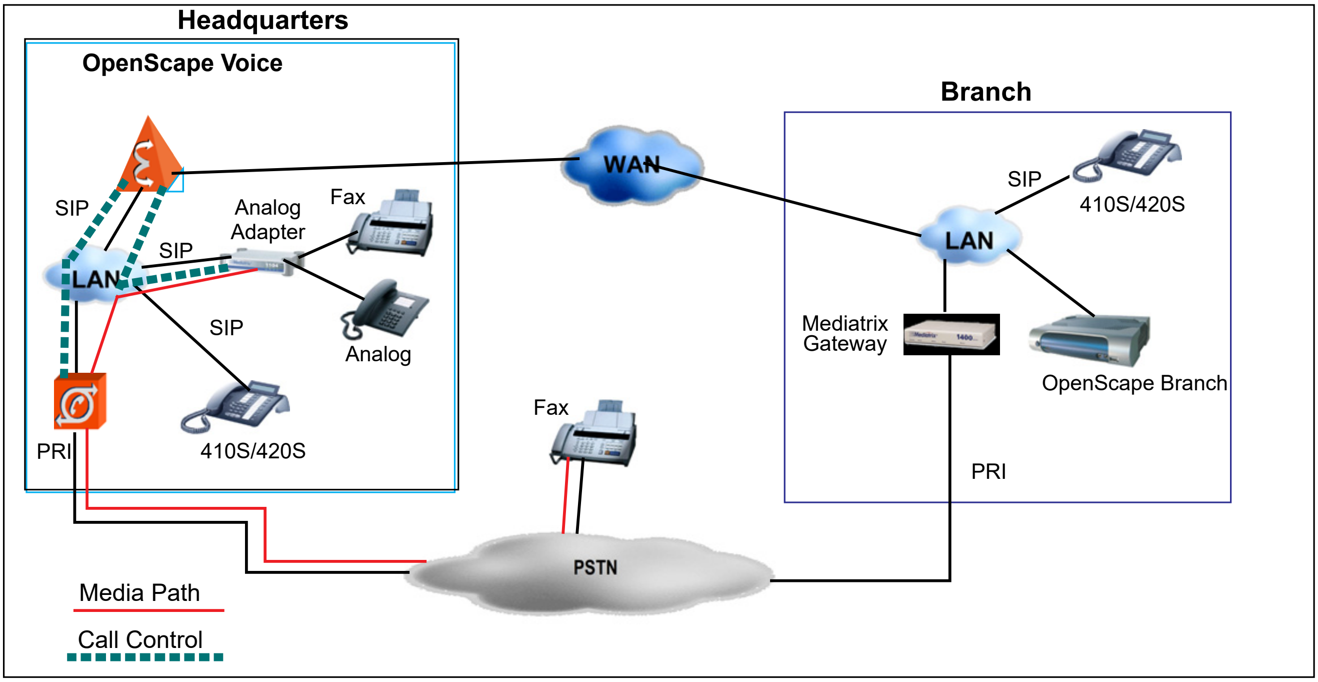


Figure 43   Analog Adapter Fax Call flow

9.5.3 Modem Data Call Operation

Modem data calls are handled the same as transparent mode fax calls, using the G.711 codec. Silence suppression must be disabled in the adapter settings. Due to the jitter present in all IP networks, analog modem speed is generally limited to 19 kbps or less.

The survivability scenario is the same as other previously described scenarios in which Unify OpenScape Voice or the WAN became disabled; the gateway handles the communications.

9.6 Final Considerations

The network planner must consider the following:

- Number of users
- Calling patterns
- Which users can use the gateways
- Percentage of blockage that can be tolerated
- Erlangs at each location
- Number of gateways needed
- Number of analog adapters needed

10 Gateway and Subscriber Rerouting

This chapter describes two related but separate features: gateway rerouting and subscriber rerouting.

- *Gateway rerouting* may be triggered when a call destined for a gateway or peer server—for example, another softswitch in the network—cannot be completed because this destination is unreachable as a result of a malfunction, congestion, or LAN/WAN link outage.

- *Subscriber rerouting* may be triggered when a call destined for a remote subscriber—for example, in a branch office—is blocked by congestion or outage of the LAN/WAN link. When subscriber rerouting occurs, it may or may not lead to gateway rerouting.Subscriber rerouting accommodates the needs of customers that need access to certain Unify OpenScape Voice features—for example, group features that are needed by subscribers in a branch.

These features provide rerouting of SIP calls if a gateway cannot accept an outbound call (connection request). The calls can be off-net (to the PSTN via a SIP gateway) or on-net (to another SIP network, such as OpenScape UC Application). The SIP response codes upon which rerouting is attempted are provisioned in the system, to provide flexibility when dealing with various third-party gateway and server types.

In addition, a rerouting timer provides rerouting to handle the case when no response is received from the remote SIP gateway or SIP server after an INVITE has been sent.

These features can also be configured to provide for the rerouting of SIP calls between SIP subscribers through the PSTN, in case of WAN failure between the two subscribers, or after receipt of a SIP response code indicating bandwidth congestion on the WAN link.

These features monitor the gateway so that a more intelligent routing can take place. Subsequent calls are immediately sent to the next available route, and polling begins on the unreachable gateway to determine when the problem or congestion is resolved. Call routing automatically switches back to the gateway when the polling mechanism indicates the problem or congestion is resolved.

10.1 Terminology Used with Gateway and Subscriber Rerouting

Before describing scenarios and other relevant concepts, a few terms are offered with definitions to provide clarity.

SIP endpoint

SIP endpoint administered in Unify OpenScape Voice using an endpoint profile. These endpoints are typically statically registered SIP gateways and other SIP servers.

SIP subscriber

SIP endpoint administered in Unify OpenScape Voice using a subscriber profile.

SIP proxy

SIP endpoint administered in Unify OpenScape Voice with the SIP Proxy attribute set. This endpoint is usually administered without endpoint or subscriber profile (preauthorized, no services).

SIP proxy subscriber

A SIP subscriber registered through a SIP proxy.

Survivable SIP proxy

A SIP endpoint with the SIP proxy and Survivable attributes set. A survivable SIP proxy can handle calls between registered SIP subscribers if Unify OpenScape Voice is not accessible for call control. The SIP proxy also needs to have an associated SIP gateway that allows incoming traffic from the PSTN.

Survivable SIP proxy subscriber

IP subscribers registered through a survivable SIP proxy.

Survivable branch office

The combination of a survivable SIP Proxy and its associated SIP gateway. The branch office is survivable because if Unify OpenScape Voice is not reachable from the branch office, basic telephony is still possible between:

- The SIP subscribers of the branch office
- SIP subscribers outside the branch office to SIP subscribers in the branch office through the SIP gateway
- SIP subscribers in the branch office to SIP subscribers outside the branch office through the SIP gateway

10.2 Gateway Rerouting

Note: Refer to Chapter 9, “Selecting Network Interfaces” for information about the gateways and SIP proxies that may be used with Unify OpenScape Voice.

When a call is being directed by Unify OpenScape Voice to a SIP gateway for routing into the PSTN, the most common reason for a call rejection is congestion at the PSTN interface (all trunks busy). However, calls may also be rejected due to the following:

- Processor overload conditions in the gateway
- Partial gateway system failures
- WAN congestion
- Other maintenance problems

A rerouting option is provided in the case where the first choice gateway rejects the outgoing call request for any reason.

When gateways reject offered SIP phone calls, they do so by returning a SIP response code (an error code in the range 1xx – 6xx) indicating the reason for the rejection. Unfortunately, there are many possible response codes, and little consistency on their use among the many third-party SIP gateways that may interface to a softswitch such as Unify OpenScape Voice.

Therefore, the list of response codes that can be used to trigger a call rerouting action can be configured for special customer configurations. The initial (default) list of actionable codes is defined in the resilient telco platform (RTP) parameter file *SrxSip.parm*. Changes to the lists in this file are possible via CLI or by direct editing of the file, but should only be attempted by system experts, following standard MOP procedures. The response codes listed in Table 90 will, by default, cause a gateway to attempt rerouting.

Numbe r	Name	Numbe r	Name
400	Bad Request	483	Too Many Hops
402	Payment Required	485	Ambiguous
403	Forbidden	488	Not Acceptable Here
405	Method Not Allowed	493	Undecipherable
406	Not Acceptable	500	Server Internal Error
408	Request Timeout	501	Not Implemented

Table 90 SIP Response Codes That Cause Rerouting (Seite 1 von 2)

Number	Name	Number	Name
413	Request Entity Too Large	502	Bad Gateway
414	Request-URI Too Long	503	Service Unavailable
416	Unsupported URI Scheme	504	Server Time-out
420	Bad Extension	505	Version Not Supported
423	Interval Too Brief	513	Message Too Large
480	Temporarily Unavailable	580	Precondition Failure
481	Call/Transaction Does Not Exist	606	Not Acceptable
482	Loop Detected		

Table 90 SIP Response Codes That Cause Rerouting (Seite 2 von 2)

In addition, if a SIP gateway is detected to have become unresponsive because an outgoing call to it timed out, the gateway is marked as inaccessible and no calls are routed to it anymore. Prior to the gateway becoming active again, calls will be offered to the next provisioned route. An audit of the defective gateway is started in order to detect the gateway becoming active again. When the audit is successful, calls can then be routed to the gateway again.

In order for intelligent gateway rerouting to occur, the following SIP features must be enabled system wide:

- Rerouting for SIP endpoints
- Registration renewal

After a provisionable audit interval time is set, audits are regularly scheduled to all unresponsive gateways.

A detected unresponsive route is also selected for outgoing calls again after an incoming call of the route and a subsequent immediate audit.

The following sections provide examples of common uses for gateway rerouting.

10.2.1 Scenario 1: Multiple Routes (Gateways) to A Destination

Sometimes the amount of traffic going to a specific destination, or to the PSTN in general, may be more than can be handled by a single gateway. Alternately, the customer may wish to have multiple gateways for improved reliability. Figure 44, "Gateway Rerouting Example—Multiple Routes to a Destination" illustrates this configuration.

Using Unify OpenScape Voice Assistant, the destination (called Boca Local) can be defined with three routes, each representing one of the gateways (GwyBoc1-3).

Keeping in mind that Unify OpenScape Voice does not manage individual PSTN trunks or track the status of individual trunks:

- The gateways may be assigned priorities. For example, all outbound calls may first be routed to GwyBoc1 first, then overflow to GwyBoc2 if GwyBoc1 rejects the call due to all trunks busy (ATB).
- The gateways may be assigned without priority, in which case the gateway will be selected via a round-robin technique (more or less randomly). Again, if the first choice gateway rejects the call due to ATB, the call will overflow to another of the three gateways.

A given call will alternate routes up to two times, so the maximum number of egress gateways that will be checked for a given call is three.

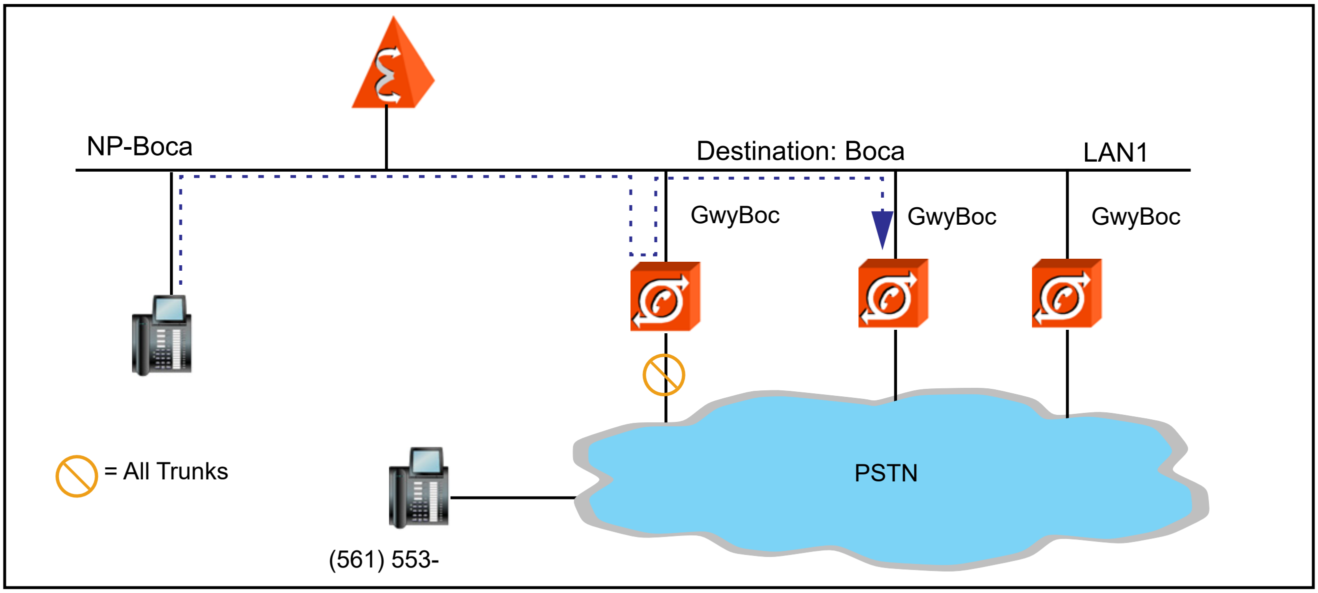


Figure 44 Gateway Rerouting Example—Multiple Routes to a Destination

10.2.2 Scenario 2: Overflow to a Remote Gateway

Another typical configuration is one in which gateways exist both in the main office and in one or more branch offices. When a main office subscriber (Boca in the example shown in Figure 45, "Gateway Rerouting Example—Overflow to Remote Gateway") makes a local call to the PSTN, the call is normally routed to a Boca gateway. If the Boca gateway is busy or out of service, the call can be rerouted via the WAN to a branch office gateway for egress into the PSTN, with appropriate dialed digit prefix modification, using the existing destination/route definition technique in Unify OpenScape Voice Assistant. In this example, the call will be routed to destination “Boca Local” and this destination will contain a second priority route entry for gateway “GwySJ1.”

This gateway configuration can also support tail-end hop-off or breakout. If the Boca subscriber calls a San Jose PSTN destination, the call can be routed as a local call through the San Jose gateway, with the appropriate prefix digit deletion. If the San Jose gateway is congested or out of service, the call can overflow back to the Boca gateway for routing to the PSTN as a long-distance call. Again, this can be configured using the existing destination/route definition technique in Unify OpenScape Voice Assistant. In this example, the dialed call would be routed to destination “SJ Local” and this destination will contain a second priority route entry for “GwyBoc1.” Overflow will be automatic if multiple route entries are defined for the destination.

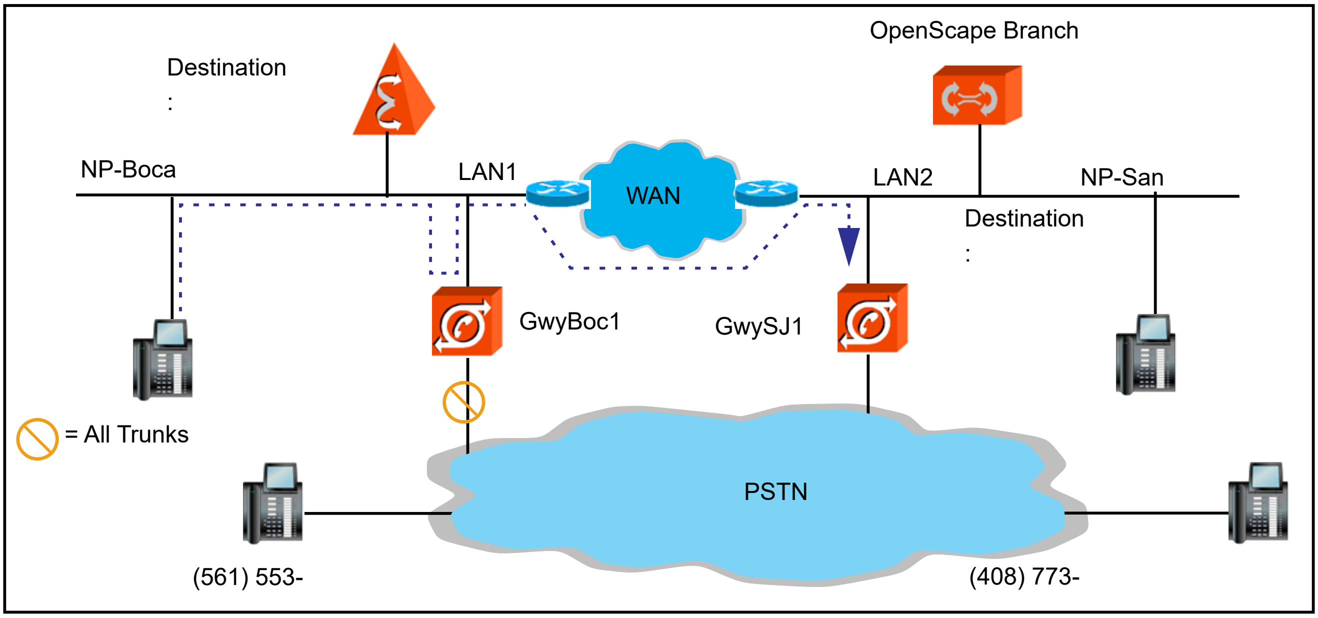


Figure 45 Gateway Rerouting Example—Overflow to Remote Gateway

10.2.3 Scenario 3: Other SIP Server

This is an application of gateway rerouting, as described in Section 10.2, “Gateway Rerouting”.

If the WAN that connects two SIP servers (for example, Unify OpenScape Voice with OpenScape UC Application, as shown in Figure 46, "Other SIP Server") encounters problems, Unify OpenScape Voice can reroute the calls through the local SIP gateway and the PSTN to the other SIP server. In this scenario, none of the SIP phones that are connected to the OpenScape UC Application server are known in Unify OpenScape Voice.

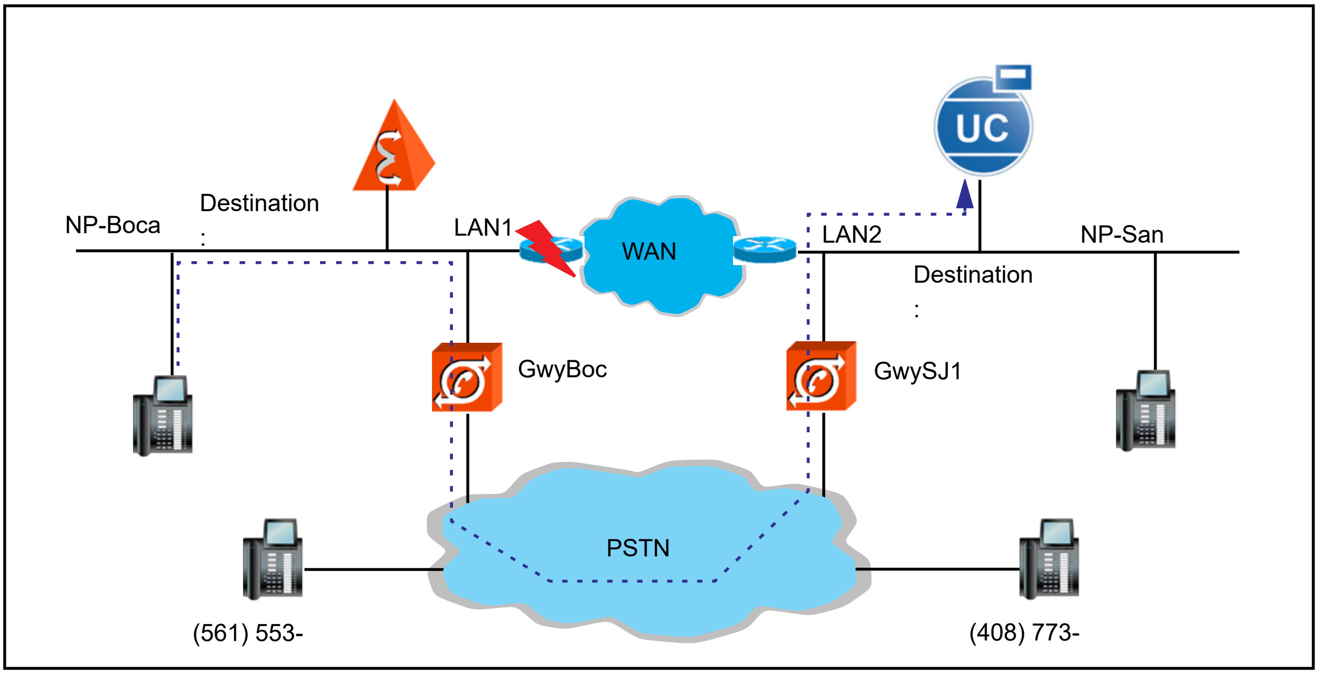


Figure 46 Other SIP Server

10.3 Subscriber Rerouting

When a single Unify OpenScape Voice system supports subscribers that are geographically distributed, most subscribers are typically co-located with Unify OpenScape Voice. However, many may be located remotely, connected to the main location via a WAN link or network. In that case, subscriber-to-subscriber calls between the locations will typically transit over the WAN link between the sites.

Subscriber rerouting is a feature that can provide additional reliability for remote subscribers connected to Unify OpenScape Voice by a WAN link which has restricted bandwidth or less-than-desired reliability. A typical configuration of such a network is illustrated in Figure 47, "Subscriber Rerouting Example".

If the WAN link between the sites goes down or is blocked due to bandwidth restrictions, calls to the remote subscriber which normally go over the WAN can be automatically rerouted via the PSTN. In the example of Figure 47, subscriber 31002 (in Florida) dials subscriber 21001 (in San Jose). Because the WAN link is down or congested, Unify

OpenScape Voice instead routes the call through the PSTN to the destination. This routing can be accomplished in either of the following modes:

- In survivable mode, the survivable branch office proxy or gateway does not retain communication with Unify OpenScape Voice via the PSTN.
- In backup mode, the survivable branch office proxy or gateway can continue to communicate with Unify OpenScape Voice via a backup link through the PSTN. This option requires appropriate provisioning of the applicable CAC groups; refer to Section 14.3.1, “CAC Groups”.

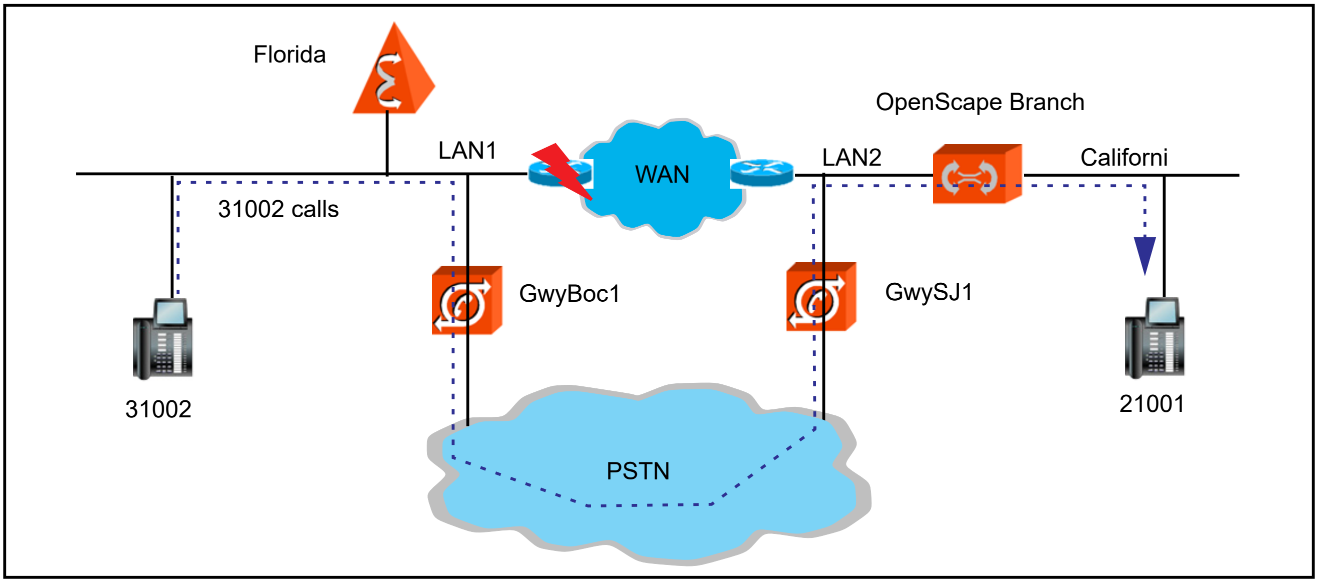


Figure 47 Subscriber Rerouting Example

This feature is also available when the RG 8700 is used as the survivability solution (without the proxy).

This feature is extended to permit its use:

- If the calling party is not a subscriber registered on Unify OpenScape Voice
- If the called party is a member of a hunt group arrangement
- If the called party is a mobile subscriber or private subscriber
- In all possible call forwarding scenarios

The operation of this feature relies on the availability of a survivable proxy at the remote site. The proxy function may be:

- Provided by a separate box—for example, the OpenScape Branch box in Figure 47

- Built into the remote PSTN gateway, as in the case of the RG 8700.

SIP signaling to the associated phones passes through the proxy, which is basically transparent during normal operation, but is capable of providing basic SIP-to-SIP softswitch functionality when a WAN outage is detected.

The RG 8700 is technically not a proxy, since registrations and signaling messages are not proxied through the RG 8700. Instead, the phones register with both the RG 8700 and Unify OpenScape Voice (dual registration), and SIP Call Processing messages are handled by the RG 8700 only in survival/failure mode. Refer also to Section 9.1, “RG 8700”.

To enable the subscriber rerouting feature, the following hardware configuration and database parameters need to be configured:

- The SIP phones in the branch must be configured with the IP address of the proxy, and the proxy must be configured with the IP address of Unify OpenScape Voice. The phones then register with the proxy, which relays the registration message to Unify OpenScape Voice after adding a second VIA-header.
- When the RG 8700 provides the survivability solution, the phone is configured with the IP address of both Unify OpenScape Voice and the RG 8700.
- In Unify OpenScape Voice Assistant:
  - Each branch subscriber that is served by the proxy must be identified, by filling in the Associated Endpoint field with the IP address (or name) of the serving proxy. This field must match the address of the proxy or RG 8700 survivable gateway in order for the feature to be activated.
  - The SIP endpoint definition of the proxy or RG 8700 must always be marked with the Survivable Endpoint attribute.
  - The SIP endpoint definition of the proxy or RG 8700 must, as applicable, have the following additional attributes selected:
    - **Enhanced Subscriber Rerouting**: Select this attribute to enable *enhanced subscriber routing*, which pertains to the ability for Unify OpenScape Voice to perform enhanced subscriber rerouting on calls to this endpoint. Note that this type of rerouting is only applicable if a CAC restriction is present.
    - **Reroute Forwarded Calls:** Select this attribute to allow subscriber rerouting of incoming calls through the SIP endpoint that are forwarded to a survivable SIP subscriber.

   - **Reroute Incoming Calls**: Select this attribute to allow subscriber rerouting of incoming calls through the SIP endpoint (that are not forwarded). This attribute is not commonly used, and should *not* be selected for gateway endpoints.

   None of these attributes is applicable to subscriber endpoints.

- If applicable, hunt groups must have the Enable Rerouting advanced attribute selected.
- For enhanced subscriber rerouting, the DID pool of a branch office must be appropriately provisioned in order to enable the correlation of calls. This correlation is required in order to provide correct displays and call forwarding features when calls are rerouted.

As in the case of gateway rerouting, when the feature is enabled, alternate routing is triggered if the remote location fails to respond to the call request, or sends back a 606 response code from the proxy, which typically indicates network congestion.

When rerouting is required, the dialed digits are prefixed by an appropriate access code created specifically for this feature, then sent through translation again, to select the appropriate egress gateway.

The prefix digit strings for international, national, and local rerouting are defined. The system chooses which of these three prefix access codes to use, based on analysis of the fully qualified calling and called party numbers (subscriber IDs) and not based on the dialed digits.

The administrator must provision a subscriber rerouting prefix access code for rerouting. These access code digits are prepended to the E.164 number of the DN that is being rerouted; in the case of forwarded or hunt group calls, this is not necessarily the called party number.

Note: If the subscriber rerouting prefix access code is not provisioned, the appropriate international, national, or local prefix access code is used in the translation process; however, this is *not* recommended.

The administrator must set up appropriate entries in the prefix access code table of the caller’s numbering plan, to route calls using these prefix digits to the appropriate egress gateways.

In addition, the survivable proxy must be configured to handle the inbound PSTN calls to the isolated subscribers, without the assistance of Unify OpenScape Voice, to handle the case of a total WAN outage (lack of even signaling connectivity).

10.3.1 Registration Renewal During WAN Outage

SIP phones must periodically register with Unify OpenScape Voice to receive service. The registration interval is typically 60 minutes, but is configurable, and can sometimes be as short as 15 minutes. If a SIP phone fails to re-register before the registration interval expires, the phone is “aged-out” of the Unify OpenScape Voice registrar database and will no longer be callable.

As described in the previous section, during a WAN outage, the endpoints at a branch location may lose SIP connectivity for a period of time. However, as a result of subscriber rerouting, they may still be reachable through PSTN rerouting.

To ensure that these SIP endpoints remain reachable during the WAN outage, registrations for these endpoints are set to the Suspended state. As long as a SIP endpoint is in this state, the call is routed directly to the PSTN gateway. The time a SIP endpoint remains in this state before its registration is removed can be provisioned with Unify OpenScape Voice Assistant.

When the WAN outage is resolved, the registration of the SIP endpoint will be renewed again.

Unify OpenScape Voice determines the WAN status by testing SIP connectivity to both the SIP endpoint itself and the associated endpoint, which is either the OpenScape Branch proxy or RG 8700 survivable gateway. If connectivity is lost to both devices, the WAN link is assumed to be down, activating the registration renewal feature.

10.4 SIP Survivability Models for Phones

Unify OpenScape Voice supports the following models for survivability for the phones:

- Proxy registration model
- Dual registration model

The proxy registration model is the preferred solution for survivable branches on Unify OpenScape Voice.

10.4.1 Proxy Registration Model

In this model, Figure 48, "Proxy Registration Model", the phones are configured with Unify OpenScape Voice as their primary SIP server/SIP registrar.

However, the phones are configured with the domain name of the Unify OpenScape Voice server (for example, *openscape01.yourcompany.com*) rather than the IP address of the server, and use a network Domain Name System (DNS) server to obtain the IP address of the server. The DNS response, in the form of DNS Service (SRV) records, will provide a prioritized list of IP addresses by which the Unify OpenScape Voice server can be reached. In this configuration, the first-choice IP address will be the IP address of the proxy. The second-choice IP address will be the true IP address of the Unify OpenScape Voice server.

With the use of the DNS SRV record, the communication layer would send all outbound messages directly to Unify OpenScape Voice in case of a SIP proxy outage.

For a survivable branch office, the SIP proxy must offer the survivability, meaning that it must offer limited SIP server capabilities when it detects that Unify OpenScape Voice is unreachable. The proxy detects survivability mode within a configurable amount of time (default: 1 minute) of the WAN or Unify OpenScape Voice outage. It may also detect the survivability mode when it is not able to forward a request from a phone or endpoint to Unify OpenScape Voice.

Examples of survivable SIP proxies are OpenScape Branch, and RG 8700.

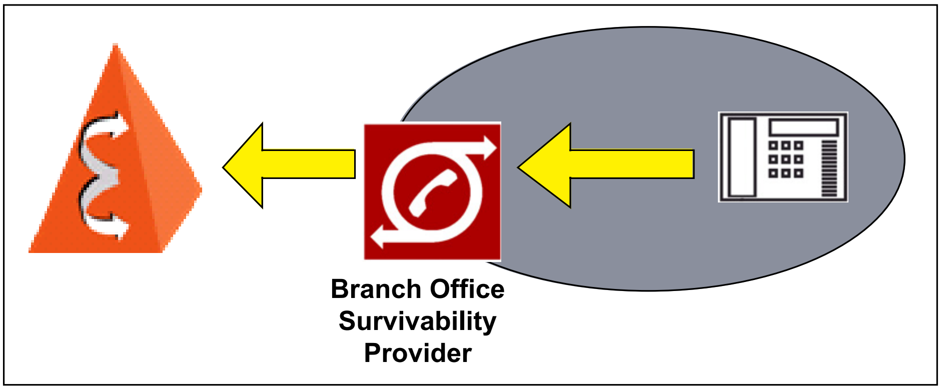


Figure 48 Proxy Registration Model

Other Characteristics

The proxy registration model is a far cleaner survivability solution than the dual registration model because all phones in the branch office will be treated the same in an outage condition (display "Temporary Limited Mode" and act as non-keyset phones) and have virtually no noticeable service interruption in this case. In detail, the proxy registration model has the following advantages when compared to the dual registration model:

- The phone is notified of the survivability mode condition and it displays "Temporary Limited Mode". All phones in the branch office remain registered with the proxy. There is no service interruption.
- The proxy detects normal mode within 1 minute of the restoration of the WAN or OpenScape Voice. All phones in the branch office are notified of the normal mode condition.

As a disadvantage an outage of the proxy will lead to a service interruption until the proxy is considered down and is bypassed.

10.4.2 Dual Registration Model

In this model, Figure 49, "Dual Registration Model", the phones are configured with Unify OpenScape Voice as their primary SIP server/SIP registrar, and a secondary SIP server as their backup SIP server. In this case, the communication layer of the phone will send registration requests directly to Unify OpenScape Voice and to the backup SIP server (for example, OpenScape Branch) at the same time. The phone will be simultaneously registered on both devices, but will always send calls to the first-choice server (the Unify OpenScape Voice server), unless it fails to respond. The backup SIP server must offer a limited set of SIP server capabilities for those instances where it receives call requests and the primary server is down.

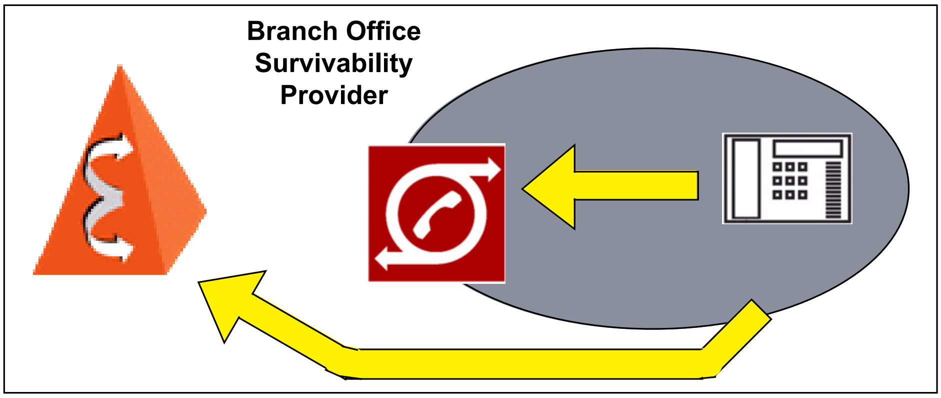


Figure 49 Dual Registration Model

11 Network Quality of Service

11.1 Codec Selection

Selection of the preferred codec for voice calls is an important factor in the perceived quality of service within the VoIP network, and also has a significant impact on the required bandwidth.

Several standards have evolved for rating codecs under varying conditions. ITU-T standard P.800 rates codecs using a Mean Opinion Score (MOS) rating in the range 0 to 5, generated by live test subjects. Values 4 and above are excellent, values 3 to 4 are considered good, and values 0 to 1 are completely unacceptable. Some typical values:

- G.729A…………….3.95 (8 kbps)
- G.723.1…………..…3.88
- G.726……………....3.85

ITU-T standard G.107 describes a so-called E-model, which generates an “R” rating on the following scale:

100-90	Users Are “Very Satisfied” (R of 94 MOS of 4.4)
90-80	Users Are “Satisfied” (R of 80 MOS of 4.0)
80-70	Some Users “Dissatisfied” (R of 70 MOS of 3.6)
70-60	Many Users “Dissatisfied
60-50	Nearly All Users “Dissatisfied

E-model allows you to enter the transmission characteristics of network and terminal equipment in order to calculate the expected speech quality using that setup. E-model takes into account many parameters, such as the effects of room noise, quantizing distortion, delay, codec impairments and impairments due to packet-loss.

Statistically, the R value is related to the old MOS values, but the methodology is more rigorous. As a set of reference values, they use the performance of G.711 in the presence of known delay (shown below). The value 94.5 is the highest attainable value for narrowband telephony (300-3400Hz). For R-scores at different delay values, see Table 91.

Delay	0 ms	50 ms	100 ms	150 ms	200 ms	250 ms
G.711 with TELR= 65dB	94	93	92	90	87	80

Table 91 R-Scores for G.711

Table 92 provides a “satisfaction” comparison with other common codecs. The talker echo loudness rating (TELR) is a measure of echo loudness. As echo becomes louder (lower TELR value) the tolerance of delay becomes less. ITUT standard G.131 contains a curve that shows a more or less linear relationship between delay and echo, with 5 msec delay being the tolerable limit when TELR is 20, and 300 Msec being tolerable when TELR is 55.

Dela y	G.711 w/ TELR = 55dB	G.72 9	G.723.1 @6.3 kbps	G.729A + VAD + 2% loss	GSM – EFR	G.729A + VAD +4% loss
50	93	83	xx	74	xx	67
100	90	82	77	73	87	66
150	87	80	75	71	85	64
200	80	77	72	68	82	61
250		70	65			

Table 92 R-Scores for Various Codecs at Given Values of Delay

VAD is voice activity detection (also known as silence suppression). VAD can significantly reduced bandwidth required for a given codec, by reducing the packet rate during periods of silence. However, VAD is hard to tune properly, and can lead to speech clipping particularly in environments where speaker-phones are in use. As a result, user satisfaction usually goes down when VAD is being used.

Note that 4% packet loss has traditionally been typical on the public internet, but loss in well managed private IP networks is usually much lower.

The choice of codecs is obviously constrained by the capabilities of the endpoints. Unify optiPoint 410 S/420 S phones, for example, only offer G.711 and G.729 codec options.

Finally, it should be noted that virtually all codecs, with the exception of G.711, are “vocoders” in that they are not suitable for even slow-speed modem data.

11.2 Base Network Requirements

The measures of a network as related to VoIP are:

- Packet loss
- Latency (delay)
- End-to-end packet jitter
- Available bandwidth

- Reliability (uptime)

11.2.1 Packet Loss

11.2.1.1 Description

Packet loss leads to voice drop-outs. Some codecs attempt to hide drop-outs using sophisticated algorithms. Many G.711 codecs, for example, support an algorithm referred to as PLC (packet loss concealment). Regardless, the result of packet loss is always a perceived speech quality reduction.

	R-Scores at 100 Msec Delay	
% Packet Loss	**G.711**	**G.711 with PLC**
0	92	92
1	67	87
2	57	85
3		82
5		76

Table 93 R-Scores at Different Percentages of Packet Loss

Table 94 shows customer dissatisfaction percentages with different percentages of packet loss.

% Packet Loss	G.729B% Unhappy	G.723.1A% Unhappy
0	13	15
0.5	15	17
1	17	19
1.5	19	22
2	21	24
3	25	27
4	28	32
8	38	41
16	51	55

Table 94 Customer Dissatisfaction Percentages at Different Percentages of Packet Loss

Overall packet loss must be well below 1% for acceptable voice quality (from the Telephone Industries Association [TIA]). An average packet loss of 1% might be acceptable, if the packet loss was truly uniform (constant) over time, but packet loss tends to be bursty, not uniform, so an average measurement does not disclose very much information.

Voice quality is particularly susceptible to bursty packet loss (two or more consecutive packets lost). Given an overall error rate well below 1%, a more accurate predictor of perceived voice quality will be "% errored seconds", where an errored second is one with error percentage greater than a specified threshold (for example, 5%). This is a simplified view of the bursty error measures of IETF standard RFC 3611, which describes in detail the concepts of burst duration, gap duration, and burst density.

A network should exhibit less than 1% errored seconds where an errored second is one with greater than 4% packet loss. Applying this rule to a G.711 codec with a 20 msec packet interval, an errored second is one with more than 2 packets lost (2 out of 50).

11.2.1.2 Packet Size Considerations

A maximum transmission unit (MTU) is the largest size packet or frame, specified in octets or eight-bit bytes, that can be sent over an Internet protocol (IP) link. MTU is specified on a link by link basis, based on the equipment type and configuration of the link endpoints.

If a user data message exceeds the MTU value for the outbound link, the sending device will typically segment the user data message into separate IP packets, each smaller than the MTU value, and send them individually. The far end is then responsible for reassembling the IP packets into a complete message.

A potential problem with the MTU concept is that messages will typically transit several links before it reaches its destination, and each link can have a different MTU value. Packet segmentation and reassembly is a time consuming function, and some routers may elect to simply discard packets that are too large, rather than segmenting them. The router will typically send an Internet Control Message Protocol (ICMP) message back to the sender, indicating that the message could not be delivered.

Most computer operating systems provide a default MTU value that is suitable for most users. This MTU default is 1500 units. But there may be cases where an intermediate link has a smaller MTU value.

As an example, If the customer's branch offices are connected to the data center through a VPN or an IP security (IPsec) tunnel, the routers facilitating this connection may require a MTU lower than the 1500 unit default.

Many SIP call control messages are quite large, and approach or exceed the typical MTU limit and require segmentation, and are sensitive to the MTU limit.

For this reason, Unify OpenScape Voice is configured to support the Path MTU discovery algorithm (see IETF standard RFC-1191) which uses ICMP messages to determine the path MTU.

Note: When using cross channel to interconnect two Unify OpenScape Voice nodes, PMTU is not supported and the MTU size is set to 1400 (Refer to: Section 13.1.3.1, "Cluster Interconnect Requirements")

11.2.2 Latency (Delay)

It is well known that end-to-end delay (also called *latency*) reduces customer satisfaction, because it amplifies the effect of acoustic and electrical echo, and also because it makes interactive conversation more difficult. The tables on voice quality above make it clear why total end-to-end delay of less than 100 milliseconds is highly desirable, if not required.

Delay in a network is a sum of the hardware processing delays of two endpoints in the connection, plus all of the IP switches and routers along the voice path, plus the jitter buffers in the endpoints. Table 95 illustrates the delays inherent in some common codecs.

	A	**B**	**C**	**D**	**E**	**F**	**G**
	Frame Size (ms)	**Frames per Packet**	**Queueing Delay**	**Multiple packet delay**	**Look Ahead**	**Jitter**	**Total Delay**
Codec			**3 x A (ms)**	**(B-1) x A (ms)**	**(ms)**	**2 x A (ms)**	**C + D + E + F (ms)**
G.711	5	1	15	0	0	10	25
G.711	5	2	15	5	0	10	30
G.711	5	4	15	15	0	10	40
G.711	10	1	30	0	0	20	50

Table 95 Inherent Delays with Common Codecs

	A	B	C	D	E	F	G
	Frame Size (ms)	**Frames per Packet**	**Queueing Delay**	**Multiple packet delay**	**Look Ahead**	**Jitter**	**Total Delay**
Codec			**3 x A (ms)**	**(B-1) x A (ms)**	**(ms)**	**2 x A (ms)**	**C + D + E + F (ms)**
G.711	10	2	30	10	0	20	60
G.729A	10	1	30	0	5	20	55
G.729A	10	2	30	10	5	20	65
G.723.1 (6.3 kbps)	30	1	90	0	8	60	158

Table 95 Inherent Delays with Common Codecs

The delay numbers in Table 95 do not include the switching delay of the intermediate routers and LAN switches. In addition, when long distances are involved, the transmission delay may be non-negligible (5 microsecond per kilometer or about 8 Milliseconds per 1000 miles).

11.2.3 Jitter

Jitter is one of the factors that impacts subjective voice quality perception, but only indirectly. Jitter occurs when the network is not able to deliver each voice packet exactly on schedule, due to random occurrences and delays in the network. All networks have jitter, and to compensate for that fact, all VoIP endpoints employ jitter buffers, and some have adaptive jitter buffers, meaning the depth of the buffer (measured in milliseconds of delay) may automatically adjust during use, to accommodate observed network behavior. The higher the jitter in the network, the “deeper” the jitter buffers must be to avoid speech drop-outs. In other words, high jitter leads ultimately to high delay in the network.

Another factor in effective delay is the packetization rate. Jitter buffer depth is measured in the number of voice samples (RTP voice packets) held in queue at the receiving end, as a cushion against late arrival of the next packet. G.711 typically send packets at a 10 msec or 20 msec rate, meaning the jitter buffer can be “tuned” in increments as small as 10 msecs. G.723, in contrast, sends packets at 30 msec rate, so the jitter buffer must be a minimum of 30 msec, and typically 60 or even 90 msec deep. So the choice of codecs will have an influence on the amount of perceived end-to-end delay. This is illustrated in the table above.

11.2.4 Bandwidth Requirements

Bandwidth requirements for voice were discussed at a high level in Chapter 4, “Calculating Network Traffic, Bandwidth Requirements, and Gateway Sizing”. Table 96 illustrates the impact of packet rate and frames per packet on the actual bandwidth required on the IP link, when the Ethernet and IP message headers are factored into the mix. In order to get a desirable latency value, the designer must accept a fairly inefficient packet overhead.

Codec	Frame Size Bytes	Frames /Packet	Packets / Sec	Payload Size Bytes	Audio Bits / Sec	Packet Size Bytes*	Line Bits / Sec	% Optimal	Latency (ms)
G723.1	24	1	33.33	24	6400	64	17067	267%	30.00
G723.1	24	2	16.67	48	6400	88	11733	183%	60.00
G723.1	24	3	11.11	72	6400	112	9956	156%	90.00
G.711	80	1	100	80	64000	120	96000	150%	10.00
G.711	240	1	33.33	240	64000	280	74667	117%	30.00

Table 96 Bandwidth Factors on G723.1 and G.711 Codecs

* Packet Size Bytes includes all applicable headers: RTP, UDP, and IP headers.

11.2.4.1 Voice Bandwidth

Table 97 and Table 98 list the bandwidth requirements for audio codecs without and with payload encryption, respectively.

These tables show the number of concurrent calls that can be transported over various link speeds. The calculations assume a default RTCP overhead of 4%. The required bandwidth and the link speed values shown in the tables are for unidirectional traffic.

It should be understood that use of codecs that provide compression introduces a trade-off of speech quality against additional capacity.

These tables are provided for reference and planning purposes.

Table 97 shows the effective bandwidth for the most popular codecs not using payload encryption for any of the calls.

Codec – Voice Bandwidth	Codec Bit Rate (Kbps)	Packet duration (ms)	Required Bandwidth* (Kbps)	Number of Calls Possible at a Given Link Speed		
				300 Kbps	1 Mbps	2 Mbps
G.711 or G.722	64	10	99.84	3	10	20
		20	83.20	3	12	24
		30	77.65	3	12	25
G.723.1	6.4	30	17.75	16	56	112
		60	12.20	24	81	163
G.726-16 or G.728	16	10	49.92	6	20	40
		20	33.28	9	30	60
		30	27.73	10	36	72
G.726-24	24	10	58.24	5	17	34
		20	41.60	7	24	48
		30	36.05	8	27	55
G.726-32	32	10	66.56	4	15	30
		20	49.92	6	20	40
		30	44.37	6	22	45
G.726-40	40	10	74.88	4	13	26
		20	58.24	5	17	34
		30	52.69	5	18	37
G.729 (including its Annexes A and B)	8	10	41.60	7	24	48
		20	24.96	12	40	80
		30	19.41	15	51	103
iLBC	15.2	20	32.45	9	30	61
		30	26.90	11	37	74
AMR	12.2	20	29.33	10	34	68
AMR-WB	23.85	20	41.44	7	24	48

Table 97 Bandwidth Requirements — No Calls Using Payload Encryption

* Line bandwidth includes all applicable headers: RTP, UDP, IP, and Ethernet headers.

Table 98 shows the effective bandwidth for the most popular codecs using payload encryption for all calls.

Codec – Voice Bandwidth	Codec Bit Rate (Kbps)	Packet duration (ms)	Required Bandwidth* (Kbps)	Number of Calls Possible at a Given Link Speed		
				300 Kbps	1 Mbps	2 Mbps
G.711 or G.722	64	10	108.16	2	9	18
		20	87.36	3	11	22
		30	80.43	3	12	24
G.723.1	6.4	30	20.52	14	48	97
		60	13.59	22	73	147
G.726-16 or G.728	16	10	58.24	5	17	34
		20	37.44	8	26	53
		30	30.51	9	32	65
G.726-24	24	10	66.56	4	15	30
		20	45.76	6	21	43
		30	38.83	7	25	51
G.726-32	32	10	74.88	4	13	26
		20	54.08	5	18	36
		30	47.15	6	21	42
G.726-40	40	10	83.20	3	12	24
		20	62.40	4	16	32
		30	55.47	5	18	36
G.729 (including its Annexes A and B)	8	10	49.92	6	20	40
		20	29.12	10	34	68
		30	22.19	13	45	90
iLBC	15.2	20	36.61	8	27	54
		30	29.67	10	33	67
AMR	12.2	20	33.49	8	29	59
AMR-WB	23.85	20	45.60	6	21	43

Table 98 Bandwidth Requirements — All Calls Using Payload Encryption (Worst Case)

* Line bandwidth includes all applicable headers: SRTP, UDP, IP, and Ethernet headers.

11.2.4.2 Signaling Bandwidth

The bandwidth required for SIP signaling to the endpoints is small in comparison to the bandwidth required for audio transmission (RTP audio packets), so in environments where voice and signaling travel over the same network path, the bandwidth for signaling is basically negligible.

In cases where signaling and voice are each segregated onto separate network paths, and the path used by signaling is restricted, the bandwidth requirements for signaling may be an issue which must be considered. The bandwidth required for signaling to an endpoint (SIP telephone) will not exceed 1 Kbps (average) even under heavy load (5 BHCA).

Attention: To avoid undesirable signaling latency, the minimum recommended bandwidth on a link used only for signaling is 64 kbps, with 256 kbps being strongly recommended (especially for scenarios causing higher signaling load, for example when using features like MLHG, keysets etc.).

Refer to other documents for a more detailed analysis of this topic.

11.2.5 Voice Traffic Segregation

In converged voice/data IP networks, one common source of voice quality problems is data traffic peaks that consume too much of the available bandwidth, resulting in voice packet loss, or unacceptable packet delays. There are three common approaches to minimize this problem, all of which involve (to one extent or another) the logical segregation of the voice and data IP traffic. The three approaches are:

1. Layer 2 QoS: IEEE 802.1p Ethernet-level packet class of service
2. Virtual LAN (VLAN) configuration
3. Layer 3 QoS: IP Packet class of service configuration (the Type of Service or TOS bits)

Methods 1 and 2 impact the format of the Ethernet frames on the network, by adding additional octets for VLAN and Priority indicators IEEE 802.1Q/P add 32 bits = 4 octets for VLAN and Priority. Method 3 uses the QoS fields in the IP message header to establish a prioritized packet delivery system.

The Unify SIP telephones (for example) and many SIP gateways can be configured to support any or all of these traffic segregation mechanisms. However, they all require compatible support with the network switches and routers.

11.2.6 Summary of Base Network Requirements

The following text is adapted from the recommendations of the Unify OpenScape Voice Implementation Guidelines document. It outlines the minimum network requirements for a VoIP installation. It is strongly recommended that a full network analysis be performed to assess the IP infrastructures.

1. Category 5 or higher cabling (tested, watch for home-made patch cables).
2. Edge and Core routers of adequate capacity.
3. Managed LAN switches with:
   a) SNMP support for alarms and status.

   b) IEEE 802.1p – layer 2 (Ethernet) QoS of service control (up to 8 priorities)

   c) Spanning tree protocol support – for efficient path selection and error recovery in multipath networks

   d) VLAN tagging – enables segregation of voice traffic, signaling traffic, and normal traffic onto separate virtual lans.

   e) HSRP/VRRP support for layer-3 switches – HSRP (Hot Standby Router Protocol) enables one router to assume the role of another, in the event of a failure. VRRP (Virtual Router Redundancy Protocol) is the IETF standards-based equivalent. The goal of both is improved network availability (up-time).

   f) VLAN trunking – permits easier and consistent centralized administration of multiple VLANs across multiple switches and routers using VTP (VLAN trunking protocol).

   g) DiffServ – IP packet class over service differentiation (layer 3 QoS)

   h) Port mirroring – enables easier analysis of traffic and errors by enabling traffic on any switch port to be replicated to a second port for analysis (sniffing) without interrupting the traffic flow.

   i) Multicast suppression – to prevent broadcast/multicast packet storms.

4. Keep broadcast domains to a minimum size (suggested 100 devices if possible).
5. End-to-end LAN latency less than 10 ms.
6. End-to-end WAN latency less than 100 ms.
7. End-to-end WAN jitter less than 30 ms peak.
8. End-to-end LAN jitter less than 10 ms peak.
9. Broadcast/multicast traffic less than 10%.
10. Packet loss less than 1% peak over 5-minute period.
11. Peak link usage on the gateway ports less than 75%.
12. Peak link usage on the WAN less than 75%.
13. UPS for all LAN/MAN/WAN devices used to transport the VoIP traffic recommended.
14. Network management (NMS, Sniffer, capacity planning).
15. Trouble Ticket/Help Desk with reporting.
16. Remote access for Unify VoIP support (modem, RAS).

11.3 Call Admission Control

Unify OpenScape Voice supports an internal CAC solution. This solution is described in detail in Chapter 14, “Call Admission Control”.

12 OpenScape User Management Overview

OpenScape User Management (OS UM) represents a new functionality in Common Management Platform (CMP), that allows assignment of communications equipment (resources) to the users of this equipment.

OS UM supports assignment, modification and deletion of the following resource types:

- OpenScape Voice resource and OpenScape Voice Softphone resource
- OpenScape 4000 resource
- OpenScape Xpressions
- Unified Communications
- External

In general, the OS UM application is composed of two parts:

- Administration
- Provisioning

It is very important, at the beginning, to distinguish between three different types of Users that may appear within the OS UM. These Users are:

- UM User (described in details, in the chapters that follow)
- UC User (Unified Communication (Web Client) Account)
- CMP Admin User.

Note: A User can become an Administrator if one or more administrator profiles have been assigned to him.

Besides the Users that belong to the selected domain, it is also possible to create Foreign Users. The Foreign Users are external Users, or administrators from another domain, that have specific rights in the selected domain. It is possible to assign the profiles from the selected domain, but the profiles from other domains cannot be assigned. Assigning the resources to the Foreign Users is not allowed.

Note: OpenScape Voice can currently only be operated with one domain – the predefined system domain System. Therefore, no Foreign Users are currently supported.

13 Redundancy and Node Separation

This chapter describes a solution for Unify OpenScape Voice redundancy and geographic separation of the two cluster nodes. Unify OpenScape Voice node redundancy can be deployed in the following ways:

- Geographically co-located cluster nodes
- Geographically separated with the cluster nodes in the same VLANs/subnets where the two locations are connected by a layer-2 connection
- Geographically separated with the cluster nodes in different subnets where the interconnect link is a routed (layer-3) connection

13.1 Redundancy Concepts

Reliability for the Unify OpenScape Voice solution means ensuring that its functionality is maintained through unforeseen failures of the hardware or software of its components. One of the methods to provide reliability is by adding redundancy to critical components of the Unify OpenScape Voice solution.

There are many components in the Unify OpenScape Voice solution. This section discusses redundancy for each of the following components:

- Unify OpenScape Voice
- Networking components (such as LAN switches, routers, and L2 bridges)

Unify OpenScape Voice provides redundancy for hardware and software. In the following sections, the Unify OpenScape Voice redundancy concept is shown within a typical Unify OpenScape Voice solution network environment. The two servers of the Unify OpenScape Voice system are referred to as *node 1* and *node 2*.

13.1.1 Active-Active and Active-Standby Configurations

Unify OpenScape Voice is capable of operating in both an active-active configuration and active-standby configuration, as follows:

- In the active-active configuration, the phones should be administered such that half register to one node and the other half to the second node during normal operation. This is controlled by setting the appropriate registrar address within each phone.

Note: Any ratio of phones registering on Node-1 and Node-2 is possible.

- In the active-standby configuration, all phones are registered to one node, during normal operation.

Note: In the event of a node failure, for either configuration, the surviving node shall assume control of all phones.
Since registration are stored on both nodes, it does not matter to which node a phone registers. The phone may send requests to either node and must accept call requests from either node.

13.1.2 Hardware Redundancy

To ensure quality of hardware, the Unify OpenScape Voice software is run on Unify certified platforms that are selected for their reliability. Table 99 list the hardware platforms that are certified to run the Unify OpenScape Voice software in a redundant configuration.

Hardware Vendor	Hardware Platform	Available for new installations (Yes/No)
IBM	IBM x3550 M2	No
FSC	PRIMERGY RX 330 S1	No
IBM	IBM x3550 M3	Yes
FSC	PRIMERGY RX 200 S6	Yes
IBM	IBM x3550 M4	Yes
FSC	PRIMERGY RX 200 S7	Yes

Table 99 Unify OpenScape Voice Hardware Platforms

13.1.2.1 Cluster Interconnect

The two Unify OpenScape Voice nodes are interconnected by a redundant pair of data links, which are direct Ethernet connections in the co-located cluster case not using the LAN switches.

The system uses this one pair of links for cluster, database, and call data synchronization.

13.1.2.2 Remote Access

A terminal server is not needed for remote access to the console ports of the Unify OpenScape Voice nodes. During normal operation a console port can be opened via secure shell (SSH) using an application like PUTTY. In the event of a system failure, a remote system console can be accessed via the IP addresses assigned to the maintenance controller. Depending on the hardware platform, this is:

- **FSC RX 330 S1**: Integrated remote management controller (iRMC)
- **IBM x3550 M3:** Intel management module (IMM)
- **IBM x3550 M4:** Intel Management Module II (IMM2)
- **FSC RX 200 S6**: Integrated remote management controller (iRMC)
- **FSC RX 200 S7**: Integrated remote management controller (iRMC)

13.1.2.3 Network Redundancy and Traffic Separation

Each node is connected to the network through redundant Ethernet ports to two LAN switches. Each of the three functions—call processing, OAM&P, and billing— has its own pair of Ethernet interfaces for security and traffic separation.

IP failover from one cable to the partner cable is controlled by the Linux bonding driver. This mechanism compensates for faults of the Ethernet card, Ethernet port, the cable, and the LAN switch.

13.1.2.4 Node Redundancy

Each node is the redundant backup for its partner. In the co-located node configuration, switchover is done by moving all signaling IP addresses to the partner. The system informs the network about the relocated IP addresses by issuing a gratuitous address resolution protocol (ARP) message.

For software simplicity and robustness, the Unify OpenScape Voice redundancy concept clearly distinguishes between node and network failures. Node failures are handled by node failover within the cluster. Most network failures (not all) are handled by Ethernet port failover within the node.

13.1.2.5 Disk Redundancy

The disks of each node are duplicated using either a software or a hardware RAID-1 controller; therefore, a single disk failure does not impact Unify OpenScape Voice operation. A double disk fault is considered a node failure and leads to a node failover.

13.1.2.6 Fan Redundancy

The set of fans in a single Unify OpenScape Voice node handle the cooling required for a fully loaded platform. Normally they run at a reduced speed setting; if a fan fails, all the other fans speed up to compensate for the failure.

13.1.2.7 Power Redundancy

Each node has two power supply units. A failure of one power supply does not impact Unify OpenScape Voice operation at all. That way, a single UPS failure will not trigger a node failure.

Dual UPSs are recommended, powering the power supply units within the nodes, so that the failure of a single UPS does not cause a node failure or a system outage.

In a configuration with co-located nodes, a double UPS power failure normally results in a complete system outage, unless the customer elects to install a third UPS system at the site. In a geographically separated configuration, a double power failure at one site causes a node failover, with the remaining node assuming all call processing responsibilities.

13.1.3 Redundant Cluster Interconnect

Each Unify OpenScape Voice node has eight 10/100/1000 BaseT Ethernet links. As an option, but configured by default, two of these Ethernet links are dedicated to a private cluster interconnection, with one port being the active cluster interconnect and the other port being a standby. Refer also to Section 13.1.4, “Other Redundant Ethernet Links”.

When the two nodes are co-located, these two links are directly connected to the other node using two Ethernet cross-over cables, one for each port. The private interconnect is used to transmit heartbeat and clocking information between cluster nodes. It is crucial for maintaining cluster synchronization and availability which is controlled by Unify OpenScape Voice Cluster. This interconnect is also used to maintain data synchronization between the two nodes. In some configurations, this interconnect is also used to pass signaling information between the parties of a call, when the A and B parties are controlled on different nodes.

13.1.3.1 Cluster Interconnect Requirements

Unify OpenScape Voice Cluster imposes the following requirements on the cluster interconnect links, regardless of whether the two nodes are co-located or geographically separated.

- **Reliability:** A cluster uses its interconnect connection on a full time basis—24/7. As a result, a routine maintenance operation that would normally go unnoticed in a typical user network can result in cluster recovery actions that cause the temporary shutdown in a redundant Unify OpenScape Voice node. As such, the cluster interconnect link between two geographically separated nodes must be a highly reliable connection. Using the default settings, if the redundant interconnect links become unavailable for 15 seconds, the Unify OpenScape Voice Cluster software assumes a potential node failure and will initiate recovery actions, which can effect features and call processing.
- **Bandwidth:** The equipment serving the cluster interconnect must provide sufficient bandwidth to carry traffic for:
  - Unify OpenScape Voice Cluster and resilient telco platform (RTP) middleware traffic
  - Database replication
  - Shared memory updates
  - Context saving
  - Half of the signaling and Operation, Administration, Maintenance, and Provisioning (OAM&P) traffic (in failure cases)

  The bandwidth required for the internode links depends on call rates on the system and call flows between the sites. In a co-located configuration, cluster interconnect links are typically direct Ethernet connections operated at 1 Gigabit per second or 100 Mbit per second links. In geographically separated clusters, the bandwidth requirements are stated below.

  The bandwidth required for the cluster interconnect links depends on call rates on the system and call flows between the sites.

  For very small systems, with up to 3 calls per second, an x-channel bandwidth of 1.5 Mbit/sec is sufficient. But in general, if the overall load on the system is less than 25 calls per second, then duplicated

10 mbps (guaranteed available bandwidth) full duplex links are sufficient. If the overall load on the system is less than 50 calls per second, then duplicated 20 mbps full duplex links are sufficient. If the call rate is expected to be higher than 50 calls per second, then consult Unify Engineering for an analysis.

In geographically separated configurations, bandwidth usage on the cluster interconnect links should be routinely monitored. If occupancy consistently exceeds 70%, additional bandwidth may be required.

- **Latency:** Tests indicate roundtrip latency should be less than 100 msec. Longer delays may impede SIP signaling, resulting in feature malfunctions, or result in unwanted alarms and recovery actions.
- **Security:** Exchanged information, over the cluster interconnect links, is encrypted with pre-configured keys using IPSEC in transport mode.
- **MTU Size:** The Unify OpenScape Voice IPSEC implementation does not support PMTU that allows for auto-configuration of MTU size. Therefore, the Unify OpenScape Voice Maximum Transmission Unit (MTU) size of X-Channel packets is configurable with a default of 1500.

Note: See the Unify OpenScape Voice Installation and Upgrade Guide (IUG), especially if the X-channels traffic runs over a customer VPN, which may not support a 1500 byte MTU size.

- **Packet Loss:** The Unify OpenScape Voice X-Channel supports an IP network with 1% Packet Loss, i.e., the network requirements regarding Packet Loss for node interconnection links cannot exceed 1%.

Note: Since most of the X-Channel-traffic is via transmission control protocol (TCP), a packet loss increases the round trip delay. With too much delay there is an increased risk of call data not being replicated to the partner node, which may lead to call irregularities after a node failover.

No impact to stable calls is expected if the Packet Loss limit is not exceeded.

13.1.4 Other Redundant Ethernet Links

In a standard configuration, each node has six Ethernet links that are paired and bonded to support the following three redundant connections from each node, in addition to the cluster connection:

- OAM&P (management)
- Signaling
- Billing/CDR

Specific Ethernet port assignments for the bonded interfaces depend on the server type. Refer to the *OpenScape Voice, Installation and Upgrades, Installation Guide* for detailed information.

The Linux bonding driver in each node provides an Ethernet port switchover function for each pair whereby one port is active and the other is in standby. Proper alarms for link failure of the bonded pairs are indicated.

The Unify OpenScape Voice system normally reserves a block of 64 contiguous IP addresses (*aa.bb.cc.00 – aa.bb.cc.63*) spread over 4 different IP subnets. Both nodes share this address range, except for the L3 Geographic Separation case.

Each of the bonded Ethernet pairs supports multiple IP addresses in this range, related to its primary function. A more detailed description of the standard configuration is shown in Appendix C, “Cluster Addressing Scheme”. Addresses with final octet 64 and above are currently not used in this configuration.

Each of the three bonded Ethernet pairs is required to be assigned to a separate IP subnet (collision domain) within the reserved address range, to minimize unnecessary broadcast traffic between the interfaces. The split mode upgrade procedure will fail if this requirement is not met. The equivalent interfaces on the two nodes share a common subnet, except for the L3 Geographic Separation case.

Typical examples of subnetting and cluster addressing are found in Appendix B, “Subnetting Scheme” and Appendix C, “Cluster Addressing Scheme”.

13.1.5 Maintenance Controller Internode Connection

The maintenance controller provides an additional independent supervisory connection between the two nodes of the cluster.

The maintenance controller boards are intended to run separately. However, in the event that the boards fail simultaneously with the associated node, due to a massive power outage or building failure, the nodes consult the Survival Authority, which determines the node that should continue running, and the node that should shut down.

13.1.6 Survival Authority

The Survival Authority is a software program that can be installed on a third server—either on the same server as the external Unify OpenScape Voice Assistant or on a standalone server. Normally, it is co-located with the external Unify OpenScape Voice Assistant administration server; it can also be installed on a standalone server. At any rate, the SA must be located at a point on the IP network where it can communicate with both Unify OpenScape Voice nodes. Unify recommends that the SA be physically located at a separate location, remote from both nodes of the cluster. There can only be one SA (If there were two, there would be a need for a third survival authority to avoid a split brain of the two SAs).

The SA is mandatory for the Unify OpenScape Voice cluster.

In the event of a communication failure between the two Unify OpenScape Voice nodes, the SA determines which node should stay active and which node must shut down to avoid a split-brain situation.

Attention: When communication between the Unify OpenScape Voice nodes is lost, the two nodes cannot continue to operate normally because they can no longer coordinate their call routing and handling decisions, nor can they maintain a consistent database of user and feature status. Therefore, one node must shut down while the other continues to operate. This is called *split-brain avoidance*.

The SA is not a single point of failure because it is not needed for Unify OpenScape Voice operation. It is only needed when the two nodes cannot communicate over the redundant cross-channel and, in addition, none of the nodes can reach the maintenance controller of the partner node.

The communication between each Unify OpenScape Voice node and the SA is tested every 5 minutes and a failure is alarmed. So in order to have a problem with the SA, three events need to happen:

- A communication failure takes place between Unify OpenScape Voice and the SA.
- Alarms are being ignored.

- A node or network failure results in failures of both cross-channels and both connections to the partner maintenance controller.

13.1.7 Standalone Service

If the standalone service option is enabled, the node that does *not* get the permission to take over from the Survival Authority stays active. Standalone service is only useful in geographically separated configurations.

The following sections provide information about the limitations of standalone secondary mode. For this reason, it is advisable to consider both the benefits and drawbacks of enabling standalone service.

The main restriction of Standalone Service is that the node doesn’t activate the virtual partner IP.

13.1.7.1 Provisioning Impacts

Feature provisioning is blocked in standalone secondary mode. This is necessary because the database of the standalone secondary node is overwritten with the database of the primary node when the cluster is re-established. All provisioning requests from the CMP/Assistant (SOAP interface) or from the command line interface (CLI) are rejected.

13.1.7.2 Subscriber Feature Impacts

Feature activation and deactivation, as well as subscriber-controlled input is blocked in standalone secondary mode for the same reason described in the previous section. If the media server is available to provide announcements, subscribers will hear an announcement indicating, "Your request cannot be processed at this time. Please try later."

Activation and deactivation of the following services are blocked:

- Anonymous call rejection
- Selective call rejection
- Selective call acceptance
- Selective call forwarding list editing
- Hot desking
- Simultaneous ringing, including remote activation and list editing

- Unify OpenScape Voice-based call forwarding features, including remote activation
- Unify OpenScape Voice-based do not disturb
- Hunt group features (activate, make busy, stop hunt, toggle)
- Personal identification number (PIN) validation
- Call completion services (CCBS/CCNR)

Note: If a callback is activated before standalone secondary service begins, but is executed after it begins, the standalone primary node does not know the callback has happened. Consequently, the callback may execute a second time when the cluster is re-established and standalone service ends.

However, features or activities that do not require database writes are still functional—for example:

- Call hold
- Consultation
- Call transfer
- Conference
- Call pickup

13.1.7.3 Impacts to Other Network Elements

Standalone mode is caused by network failures, which most likely affect other equipment and functions. The following are examples of the potential impacts:

- **Media servers:** No announcements, music on hold, or station-controlled conferences
- **OpenScape UC Application, CSTA applications:** No presence, one number service (ONS), OpenScape-controlled conferences, or click to dial
- **PSTN gateways**: No calls to and from the PSTN
- **SIP phones, proxies:** Unavailable subscribers, dropped calls
- **Voice mail servers**: No voice mail or voice mail indications
- **Domain name servers:** Failed call attempts

- **Network Time Protocol (NTP) servers:** Incorrect time of day, RTP impacts
- **OAM&P servers:** No alarms or performance monitoring

13.1.8 Preferred Node to take over

In case the two Unify OpenScape Voice nodes cannot communicate with each other via the x-channel, one of the nodes either needs to deactivate itself or transition to the operation mode StandAloneSecondary.

Note: Please see the Unify OpenScape Voice Installation and Upgrade guide (IUG) on how to configure which node should be preferred to survive this scenario.

It is recommended to select the node, which is closer to the other OpenScape applications (such as UC, XPR, CC) as the preferred node to takeover.

13.2 Cluster Redundancy with Co-Located Nodes

This section describes the interconnections for Unify OpenScape Voice when the nodes are co-located (Figure 50, "Geographically Co-Located Redundant System"). This is the usual way of deploying Unify OpenScape Voice. In the collocated cluster deployment:

- Unify OpenScape Voice is connected to two LAN switches.
- The Unify OpenScape Voice subnet is connected to the WAN/LAN via a redundant pair of routers.
- Survival Authority guards against situations where a normal node failover would not occur due to multiple failures impacting both the node and its maintenance controller, but not the partner node.

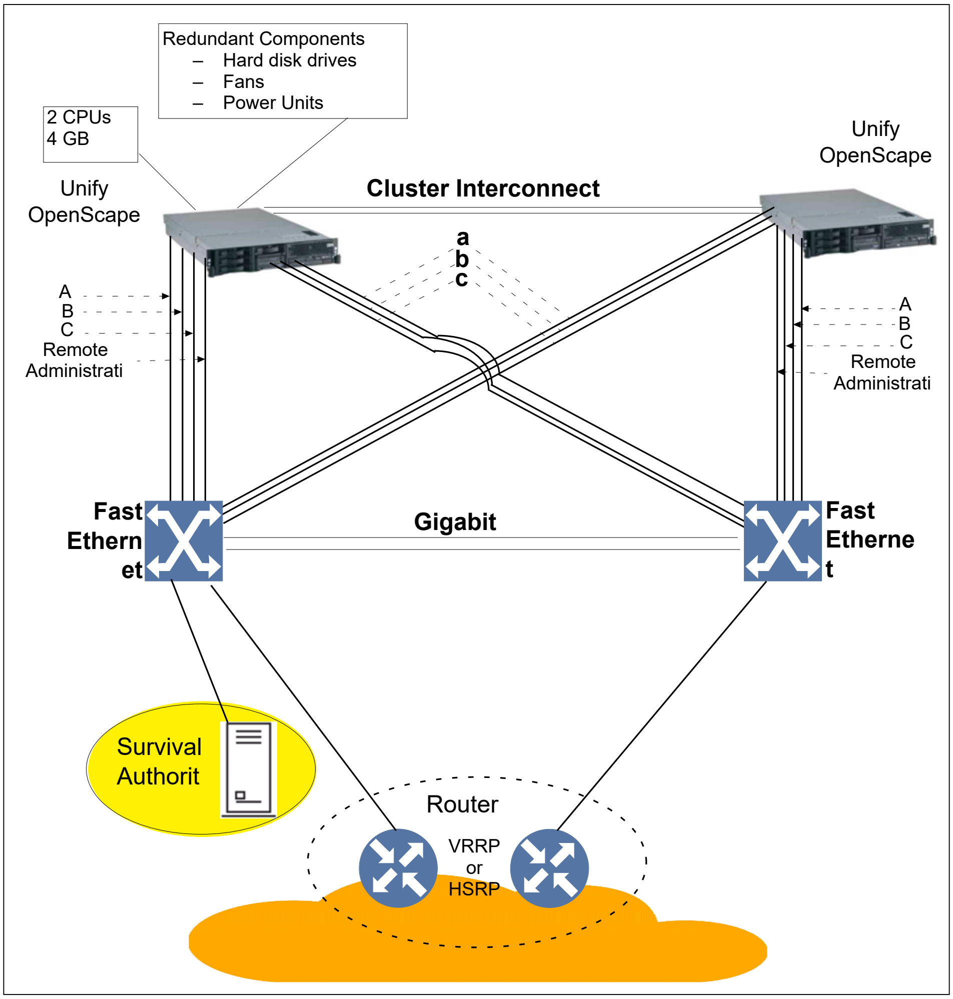


Figure 50 Geographically Co-Located Redundant

13.3 Geographic Separation

This section describes the interconnections for Unify OpenScape Voice when the nodes are geographically separated.

Unify OpenScape Voice supports two distinct Geographic Separation configuration deployment scenarios:

- Layer-2 Geographic Separation ("L2 geo separation"), presented in Section 13.3.1, "L2 Geographic Separation - Same Subnets".
  - Nodes share the same networks (IP subnets)
- Layer-3 Geographic Separation ("L3 geo separation"), presented in Section 13.3.2, "L3 Geographic Separation - Different Subnets".
  - Nodes are on different networks (separate IP subnets)

If Unify OpenScape Voice is installed together with OpenScape applications such as OpenScape UC Application or OpenScape Xpressions, L2-geo separation is recommended (Chapter 13, "Geographic Separation—Nodes in Same Subnet").

The most important difference between L2 and L3 geo separation is that moving virtual IP addresses from one node to the partner node is not possible in L3 geo separation, and therefore disabled.

In L3 separation, all network elements that communicate with the Unify OpenScape Voice cluster must support two IP addresses to continue communication in case of a node failure or, a network failure disabling the node communication. Therefore, the guideline recommendation is that these network elements use DNS-SRV.

Although such a configuration is not necessary in L2-geo separation (since the Unify OpenScape Voice IP address moves to the partner after a node failure), DNS-SRV is still recommended.

Note: The Unify OpenScape Voice cluster is installed with a time zone that is used for time-of-day routing and other time-related features. In addition, for support of endpoint-specific features requiring time of day, subscribers default to the Unify OpenScape Voice server's time zone, with the ability to be provisioned as a different time zone.
This implementation does not change with geographic redundancy via node separation. One time zone is picked for the cluster even if one node of the two nodes is physically located in another time zone. If special handling is required for all endpoints at that second location, all

these endpoints need to be provisioned with a ‘none-default’ time zone (default meaning the Unify OpenScape Voice server’s cluster time zone).

13.3.1 L2 Geographic Separation - Same Subnets

Unify OpenScape Voice can be installed in a geographically separated configuration by connecting the two nodes via LAN bridges. The functionality is the same as the co-located configuration, including the support of virtual IP addresses. For example, this means that after a node failure, signaling traffic travels over the LAN bridge to the surviving node. The following are some characteristics of this configuration:

- All logical IP subnets (VLANs) are spanned between two 2 remote sets.
- For redundancy reasons, there are redundant LAN switches and routers at each site. The L2 bridge is also a redundant pair of L2 only links between the 2 sites – usually fiber connections are used for this link.
- The router of Data Center 1 is the default router for all IP addresses and virtual IP addresses that are active on Unify OpenScape Voice.
- The network is set up to route traffic for clients or servers that intend to reach one of the Unify OpenScape Voice nodes. The network is also set up to reroute this traffic to the other data center if the routers of a particular data center are unavailable.
- In order to protect against a network failure that disables node-to-node communication, the Survival Authority is mandatory for this and all geographically separated installations.

13.3.1.1 Configuration Requirements

Both Unify OpenScape Voice nodes are in the same IP subnets and connected via layer-2 as shown in Figure 51.

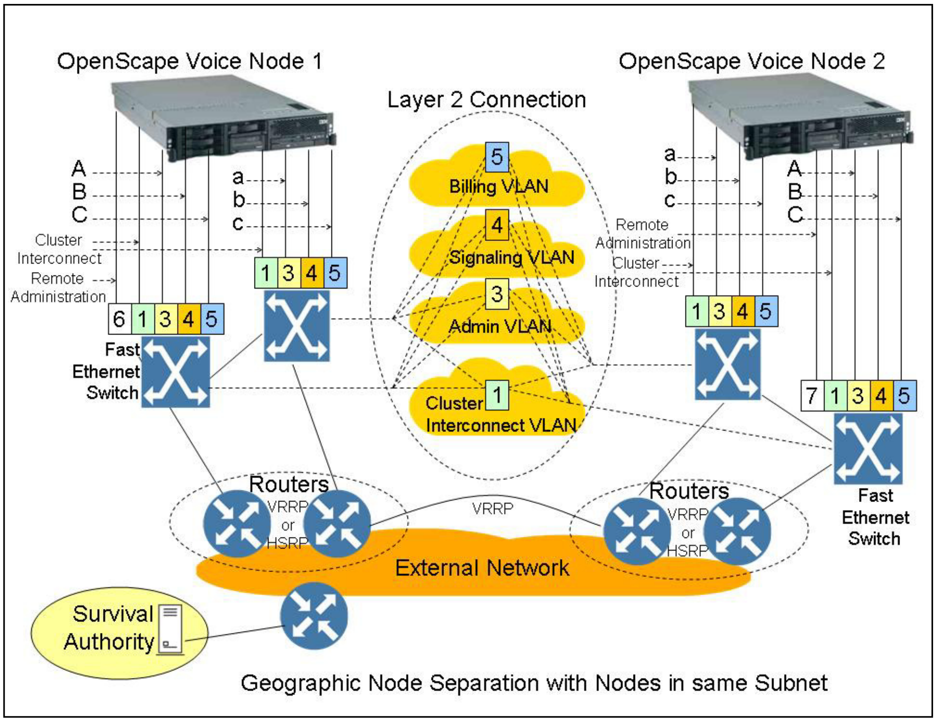


Figure 51 Geographic Separation—Nodes in Same Subnet

In this configuration, there is no impact for the integrated Unify OpenScape Voice server because everything works as in the co-located case.

When using the same logical subnets at both nodes, the virtual IP addresses that are normally activated on each node may failover to the partner node’s subnet.

The following is required to support this solution for node separation:

- Two redundant layer-2 connections between the two locations where the nodes are located.

  The figures illustrate this as a layer-2 bridge, but modern L2/L3 Ethernet switches and routers can provide this functionality through VLAN tagging and/or L2TP (layer-2 tunneling protocol). Separate VLAN IDs can be assigned for billing, administration, signaling, and the cluster interconnect, when node separation is required. However, it is possible to combine the Unify OpenScape Voice IP subnets:

  – The x-channel can be merged into the admin subnet.

  – Billing and Admin can be combined.

  - Billing, Admin and Signaling can be combined.

Note: It is recommended to separate Signaling from the other OAM&P subnets.

- Two layer-2 LAN switches at each location with connection to the routers of the WAN. The second LAN switch is recommended at each site to prevent a single LAN switch outage from triggering a node failover.

- Layer-3 router connections to each site with capability of rerouting the same IP destination address to the partner site.

- Each Unify OpenScape Voice node is connected to the WAN for OAM&P, signaling, and billing/CDR. For redundancy reasons, the connection to the routers is run through two LAN switches. Switchover for a failed Ethernet interface is performed by the Linux bonding driver as in the co-located case.

- The two nodes of the Unify OpenScape Voice cluster are connected with a redundant x-channel. The two x-channels are not directly cabled, but extended with the help of network equipment. Switchover for a failed Ethernet interface is performed by the Linux bonding driver.

- The Unify OpenScape Voice maintenance controller is connected with the partner Unify OpenScape Voice node through an IPMI connection. This allows the Unify OpenScape Voice node to power down its partner in case both links of the redundant cluster interconnect go down (“split brain avoidance”).

- An external server running the Survival Authority is required. It should be in a location separate from the two Unify OpenScape Voice nodes, and is typically co-located with the Unify OpenScape Voice Assistant server, on the administration VLAN, reachable through router by both Unify OpenScape Voice nodes. If there is complete failure of the cluster interconnect links, and node shutdown through the maintenance controller link is unsuccessful or cannot be confirmed, the running Unify OpenScape Voice nodes will send a request to the survival authority. The survival authority will—if asked—only grant survival to one of the nodes of a cluster. This eliminates the possibility of split-brain occurring—where both nodes of a cluster would be active at the same time. The occurrence of the “Survival” request by a node of the cluster triggers the setting of a switch in the survival authority (Unify OpenScape Voice Assistant) that can only be reset manually by a crafts person.

- Installation of two media servers (one at each node site) is recommended to prevent loss of media functions (that is, tones and announcements) in the event of a location failure.

All redundant links must use separate physical paths for maximum reliability.

Linux’ IP address/routing tables need to be configured to deal with asymmetric traffic that may result from certain failure conditions, for example, node failure.

The Unify OpenScape Voice server includes the standard set of Linux IP analysis commands, including **ifconfig**, **route**, **arp**, and **ip**, however, no manual configuration at the console level is required. Setup is automatic.

13.3.2 L3 Geographic Separation - Different Subnets

This section describes the interconnections for Unify OpenScape Voice when the nodes are geographically separated with different subnets. This configuration is also known as the *separated-networks configuration*.

For L3 geo separation, Unify OpenScape Voice is installed in a geographically separated configuration where the two nodes are usually on separate IP subnets (see Figure 52, "Geographic Separation with Nodes in Different Subnets").

In L3 geo separation, all network elements that communicate with the Unify OpenScape Voice cluster need to support two IP addresses to continue communication in case of a node failure or, a network failure disabling the node communication. It is recommended that these network elements use DNS-SRV.

If a device is set up to use a particular Unify OpenScape Voice node by default—perhaps because this node is closer to the device—the device needs to implement a way to revert back to the default Unify OpenScape Voice IP address after having switched to the partner IP address for any reason.

The following are other characteristics of this configuration:

- The two nodes are usually connected to different IP networks and all communication between the nodes is routed over the network. The cross-channel is just another subnet with local redundancy via the Linux bonding driver, as are the other three subnets.

- The maintenance controller is only connected to one LAN switch, as in all the other configurations. One difference between this and the configuration described in Section 13.3.1, “L2 Geographic Separation - Same Subnets”, is that the network does not need to be set up to reroute traffic to the other data center if the routers of a particular data center are unavailable.
- In order to protect against a network failure that disables node-to-node communication, the Survival Authority is mandatory for this scenario and all geographically separated installations.
- If a device is connected to the node via TLS and the node or network connectivity fails, the TLS connection needs to be re-established with the IP address of the partner node. This can be done by:
  - The device itself. For SIP phones, this is the only option.
  - The Unify OpenScape Voice node that takes over, as long as TLS with mutual authentication is provisioned for the node.

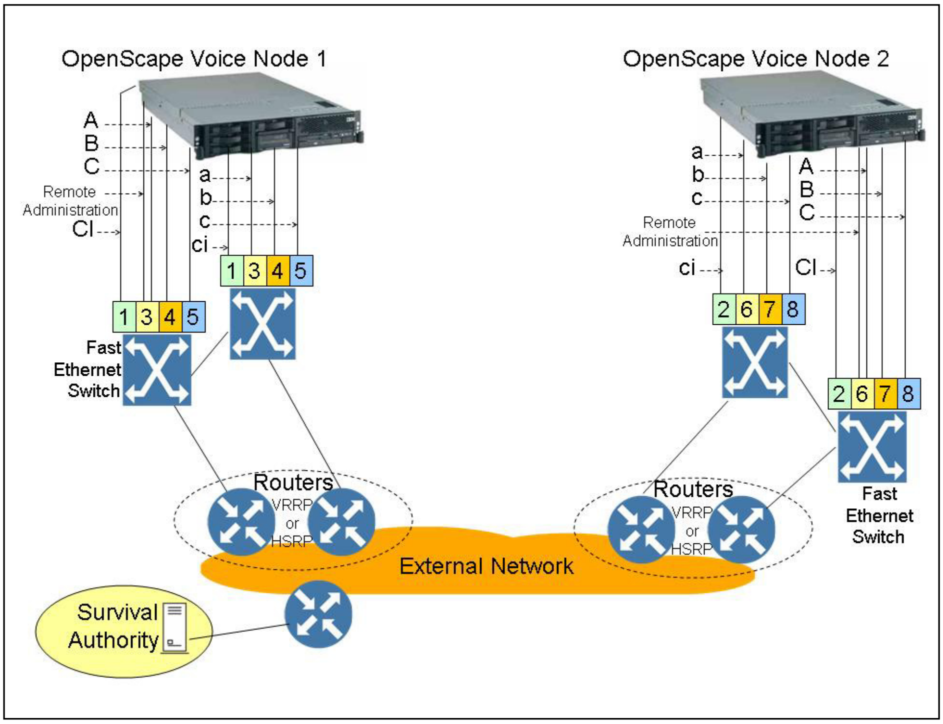


Figure 52 Geographic Separation with Nodes in Different Subnets

It is possible, but not recommended, to connected the cross-channel directly via LAN bridges. This option is not further discussed in this chapter, but is shown in Figure 53.

Note: Figure 52 and Figure 53 show four separate subnets. The Admin, Billing and Signalling subnets can be combined. However, it is recommended to separate Signaling from the other OAM&P subnets.

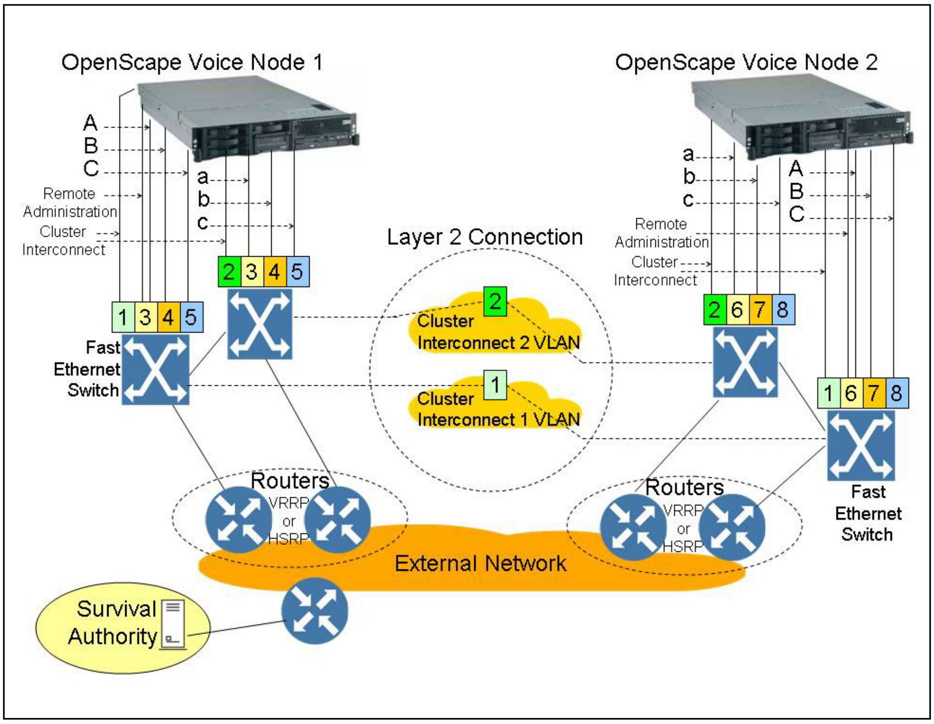


Figure 53 *Geographic Separation—Nodes in Different Subnets with Cross-Channel Connected Via LAN Bridges*

13.3.2.1 Cluster Interconnect Requirements

Bandwidth

The required cluster interconnect bandwidth depends on the size and call load of the Unify OpenScape Voice. It ranges from 1.5 Mbit/sec for an installation with less than 1,000 lines to 100 Mbit/sec for 100,000 lines. It is recommended that an initial installation has at least 30 percent available bandwidth capacity because the latency of the interconnect is adversely affected when total use nears 100 percent.

Refer to Section 13.1.3.1, “Cluster Interconnect Requirements” for a discussion of bandwidth.

Latency

Tests indicate roundtrip latency should be less than 100 msec. Longer delays may impede SIP signaling, resulting in feature malfunctions, or result in unwanted alarms and recovery actions.

This interval is long enough so that a small message and response can span transcontinental distances. This interval also allows for recovery from lost packets or other errors that can cause a few requests or responses to be lost in the interconnect.

The IP addresses of the network interfaces used for the cluster interconnect need to be configured on both nodes, so the two nodes can communicate with each other over the cluster interconnect.

In order to satisfy the latency requirement, the following should be applied:

- Layer-2 priority routing through VLAN tagging and QoS setting on the Ethernet port of the LAN switch
- Layer-3 priority routing through differentiated services code point (DSCP) setting.

  The cluster interconnect packets are to be routed with priority over the customer’s IP network.

The customer’s network must configured in a way that satisfies these performance requirements

Note: A cluster interconnect that runs over a public network (Internet) is not supported.

Reliability

The reliability requirements for the cluster interconnect involve several factors. Unify OpenScape Voice Cluster used for internode communication, guarantees that messages are delivered correctly and in order to its clients. It was designed with fairly reliable communications in mind. When the cluster interconnect is reliable, there is very low overhead, but when it is unreliable, the overhead increases. This is similar to other protocols like TCP/IP; errors in the interconnect will result in messages being resent. Resending messages consumes bandwidth and increases latency and should be avoided at all times.

Since this feature will use an IP connection for the cluster interconnect and the error rate and packet loss of an IP connection cannot be easily controlled, the only way to satisfy this requirement is to allow some excess bandwidth for the cluster interconnect. This is the rationale for the note:

Note: However, during maximum load, the bandwidth utilization should not exceed 70%.

13.4 Unify OpenScape Voice Node Failover

13.4.1 Overview

The Unify OpenScape Voice two-node cluster normally runs in active-active redundancy mode with node 1 being the backup of node 2, and vice versa. For that reason, if node 1 fails, node 2 provides all functions of node 1 in addition to its own functions. For example:

- If the master database is on node 1, the previously standby database on node 2 becomes master.
- All call processing handled by the SIP signaling manager process of node 1 is taken over by its associated standby process running on node 2.
- If Unify OpenScape Voice is installed with virtual IP addresses, the IP addresses of node 1 are activated on node 2 (in addition to the IP addresses of node 2).
- If Unify OpenScape Voice is not installed with virtual IP addresses, Unify OpenScape Voice communication partners need to continue existing or start new communication with the IP address of the partner node..

13.4.2 Node Failure Detection

A total node failure is detected by Unify OpenScape Voice Cluster running on the partner node. Unify OpenScape Voice Cluster exchanges keep-alive messages between the two nodes over the duplicated cross-channel. If the heartbeat fails for 15 sec (default, can be configured), first Unify OpenScape Voice Cluster verifies that the partner is actually out of service.

Before Unify OpenScape Voice Cluster informs RTP that the partner node is down (which triggers RTP to start the software switchover), it verifies that the other node is out of service with the help of one of the following shutdown agents:

- SA_IPMI
- SA_DOWN, which interfaces with the Survival Authority

This operation is necessary to avoid a split-brain situation where two nodes of a cluster think that they are controlling the same resources, which in case of Unify OpenScape Voice are database and IP addresses.

As described below, the manner in which split-brain avoidance is accomplished depends in large part on whether a Survival Authority is present.

13.4.2.1 Operation with Survival Authority

If a Survival Authority is present, the STONITH operation described above initially takes place (with minor variations in the wait time before certain actions occur).

If STONITH is not successful, Unify OpenScape Voice requests permission from it to switch over. If a node does not get permission or receives no response, it reboots itself.

Depending on whether the standalone service option described in Section 13.1.7, “Standalone Service” is enabled, the node that does not get the permission to take over from the Survival Authority may stay active.

13.5 Other Failure Scenarios

13.5.1 Co-Located Nodes

In this configuration, the cluster is guarded against the following failures without loss of service:

- Node failure
- LAN switch failure
- Ethernet cable failure
- Router failure
- Survival Authority failure

Failures of the following units are alarmed:

- Node
- Ethernet port
- Port pair (bonding driver)
- Communication between node and Survival Authority
- Communication between node and own or partner maintenance controller
- Communication with other network elements

13.5.1.1 Single Failures

Table 100 lists single failures and their impacts to the co-located configuration.

Failure Type	Impact
Node	Refer to Section 13.4.2, “Node Failure Detection”.

Table 100 Single Failure Scenarios—Redundancy with Co-Located Nodes (Seite 1 von 2)

Failure Type	**Impact**
LAN switch	Each bonding driver on each node detects the failure of the LAN switch and fails over the IP address if it was active. The routers reroute the traffic to the surviving LAN switch. Because the cluster interconnect is not connected to the LAN switches, it is not affected by the LAN switch failure. The failed LAN switch causes unavailability of the following: • Survival Authority for both nodes • The maintenance controller of the connected node, which means no remote reset, power-cycle, or status query capability
Cable or Ethernet card	The bonding driver in control of this Ethernet interface fails over to the backup Ethernet interface on the same node.
Router	The standby router takes over for the failing router. Redundant routers are using the VRRP or HSRP protocol to fail over.
Survival Authority	No impacts. The Survival Authority is only needed after a double cross-channel failure combined with broken connections between the Unify OpenScape Voice admin port and the partner maintenance controller.

Table 100 Single Failure Scenarios—Redundancy with Co-Located Nodes (Seite 2 von 2)

13.5.1.2 Double Failures

Table 101 lists double failures and their impacts to the co-located configuration.

	Second Cross-Channel	Partner Node	Second Router	Cable or Ethernet Card on Partner	Own Cable or Ethernet Card	Partner LAN Switch
Own LAN Switch	🟩	Unify OpenScape Voice node and Ethernet failover	LAN failover	LAN failover	One node loses (partial) network connectivity	**Total outage**
Own Cable or Ethernet Card	🟩	Unify OpenScape Voice node and Ethernet failover	🟩	🟩	One node may lose some network connectivity (see note)	
Cable or Ethernet Card on Partner Node	🟩	Unify OpenScape Voice node failover	🟩	One node may lose some network connectivity (see note)		

Table 101 Double Failure Scenarios—Redundancy with Co-Located Nodes (Seite 1 von 2)

Router		Unify OpenScape Voice node failover	**Total outage**			
Own Node	Unify OpenScape Voice node failover	**Total outage**				
Cross-Channel	Deactivation of one node					
Note: Loss of network connectivity of one node is described in Section 13.5.1.3, “Network Connectivity Failure of One Node”.						

Table 101 Double Failure Scenarios—Redundancy with Co-Located Nodes (Seite 2 von 2)

13.5.1.3 Network Connectivity Failure of One Node

A double Ethernet failure or a combination of partial network failures may disable one or more network communication links of a node. Table 102 lists these failures and their impacts to the co-located configuration.

Failure Type	Impact
Admin network	If one node cannot be reached for administration and maintenance—that is, if both admin Ethernet ports of the Linux bonding driver are unavailable—Unify OpenScape Voiceprovisioning and maintenance is still possible via the partner node. Only direct hardware maintenance is not possible. Unify OpenScape Voice Assistant signals that it lost communication with the node. It may still receive alarms from the other node if the active alarming process happens to run on the other node. **Note**: The remote admin interface (provided by the maintenance controller) is nonredundant. For that reason, a failure of the maintenance controller or the Ethernet cable that connects it with the LAN switch results in an outage of the remote admin capabilities of that node.
Signaling network	If one node cannot exchange signaling messages—that is, if both signaling Ethernet ports of the Linux bonding driver are unavailable—it tries to send messages via the partner node as long as the cross-channel is available. Connected devices can switch their signaling to the IP address of the partner node. But in a shared network configuration, connected devices are usually configured with only one HiPath IP address relying on this virtual IP address to move to the partner node. This however, is only done after a node failure.
Billing network	If the communication between a node and its connected billing servers is not possible—that is, if both billing Ethernet ports of the Linux bonding driver are unavailable—the consequences depend on whether billing files reported via push or poll mode: • **If in Push mode:** If Unify OpenScape Voice pushes the billing file and does not get a response, the CDR Handler software node tries another billing server IP address and, if unsuccessful, switches over to the other node and tries to send the billing files from there. • **If in Poll mode:** If the active CDR handler runs on the node with the lost communication, the external billing server cannot read the CDR files. Unify OpenScape Voice is dimensioned to store billing files for five days. If communication cannot be re-established within this time, the craft needs to manually switch over the CDR handler software process.

Table 102 Network Connectivity Failure Scenarios—Redundancy with Co-Located Nodes (Seite 1 von 2)

Failure Type	Impact
Cluster interconnect	This is discussed in detail in Section 13.4.2, “Node Failure Detection”. To avoid a split-brain situation, a complete cluster interconnect failure leads to the deactivation of one of the two nodes unless the standalone service feature is enabled.

Table 102 Network Connectivity Failure Scenarios—Redundancy with Co-Located Nodes (Seite 2 von 2)

13.5.2 L2 Geographic Separation - Same Subnet

In this configuration, the cluster is guarded against single and most double failures in the same manner as in the co-located deployment. In addition, geographic separation protects against catastrophic sites failures such as fire, flooding, earthquake, hurricanes, and so forth.

13.5.2.1 Single Failures

Table 103 lists single failures and their impacts for geographic separation with nodes in the same subnet.

Failure Type	Impact
Node	Refer to Section 13.4.2, “Node Failure Detection”.
LAN switch	Refer to Table 100. Note that one cross-channel is impacted.
Cable or Ethernet card	Refer to Table 100.
Router	Refer to Table 100.
Survival Authority	Refer to Table 100.
Bridge	An outage of the L2 bridge or one of the redundant network connections between two L2 bridges between the two data centers results in the loss of one of the cluster interconnect connections. All site-to-site LAN traffic uses the remaining LAN bridge.

Table 103 Single Failure Scenarios—Geographic Separation with Nodes in Same Subnet(Seite 1 von 2)

Failure Type	Impact
Site	A site failure results in a failure of the redundant cross-channel and is handled by the surviving node like a node failure. Because communication with the partner maintenance controller is not possible in this case, the Survival Authority is required to give permission to the surviving node to switch over, especially to take over the virtual IP addresses (refer to Section 13.4.2, “Node Failure Detection”.)
Network	A network failure that disables the cross-channel looks to the Unify OpenScape Voice node like a node or site failure, and is therefore treated the same way. The difference that both nodes are active after the failure and may cause a split-brain scenario in which IP addresses are active at both locations. Depending on the network failure, the maintenance controller of one node may still be accessible to the partner. In this case this node is power-cycled and stopped at the command prompt until the cross-channel is back. If power-cycling of the partner node is not possible the Survival Authority decides which node stays up and which needs to go down. It is also possible that a node cannot communicate with the Survival Authority, in which case it will deactivate itself. Unless the StandAlone Feature is enabled, see also Node Failover. **Issue**: When the surviving node takes over the virtual IP addresses the router of the data center with the deactivated node may not realize that he IP addresses are now active at a different location and thus continue to send IP packets to the LAN with the deactivated node. **Attention**: Manual intervention may be needed to reconfigure the routing network. However, some LAN switches can be configured to deactivate the LAN cable towards the router when a failure of the link to the HiPath node is detected. With this modification, the router can detect a HiPath node failure by the failure of the connected Ethernet link and craft initiated rerouting would not be needed.

Table 103 Single Failure Scenarios—Geographic Separation with Nodes in Same Subnet(Seite 2 von 2)

13.5.2.2 Additional Double Failures

Refer to Table 101, "Double Failure Scenarios—Redundancy with Co-Located Nodes". Due to the additional routers, LAN switches, and bridges, the following double failure scenarios are also applicable:

- **Double router failure at one data center**: The node loses connection, but is still connected to the partner node. The impacts are described in Section 13.5.1.3, “Network Connectivity Failure of One Node”.
- **Double LAN failure at one data center:** The node is completely isolated from the network and the partner takes over with the help of the Survival Authority; the maintenance controller of the isolated node is not available.
- **Double bridge failure:** Refer to the description of network failure in Table 103, "Single Failure Scenarios—Geographic Separation with Nodes in Same Subnet".

13.5.3 L3 Geographic Separation - Different Subnets

In this configuration, the cluster is guarded against single and most double failures in the same manner as in the co-located deployment. In addition geo-separation protects against catastrophic sites failures such as fire, flooding, earthquake, hurricanes.

Table 104 lists potential failures and their impacts for geographic separation with nodes in different subnets.

Failure Type	Impact
Node	The Unify OpenScape Voice node detects a partner node failure by failed cross-channel communication. In order to make sure that the failed node is out of service, the node power-cycles its partner by exchanging messages with the maintenance controller of the failed node. At that point, the Unify OpenScape Voice software takes over and all communication has to use a different IP address.
LAN switch	Refer to Table 100. Note that one cross-channel is impacted.
Cable or Ethernet card	Refer to Table 100.
Router	Refer to Table 100.
Survival Authority	Refer to Table 100.

Table 104 Failure Scenarios—Geographic Separation with Nodes in Different Subnets (Seite 1 von 2)

Failure Type	Impact
Site	A site failure results in a failure of the redundant cross-channel and is handled by the surviving node like a node failure. Since communication with the partner maintenance controller is not possible in this case the Survival Authority is required to give permission to the surviving node to switch-over. Refer to Section 13.4, “Unify OpenScape Voice Node Failover”.
Network and double failures	The potential impacts of double failures (LAN, cable, router, Ethernet card) are failures of node-to-network connectivity. Refer to Section 13.5.1.3, “Network Connectivity Failure of One Node”.
Network failure with TLS usage	Before Unify OpenScape Voice starts a new SIP call, it reads information about the existing TLS connection between Unify OpenScape Voice and applicable SIP phones from the database; it then uses this information for the duration of the call. If this connection information changes during the call such that the phone creates a new TLS connection on the other node after a communication failure, mid-call events as well as the final BYE messages will fail. This shortcoming will be addressed in a future release. The following are examples of mid-call events: • Unify OpenScape Voice-initiated session timing (which can cause a stable call to fail) • Putting a call on hold • Starting a three-way conference • Consultation • Call transfer • BYE message (which ensures an accurate CDR record)

Table 104 Failure Scenarios—Geographic Separation with Nodes in Different Subnets (Seite 2 von 2)

14 Call Admission Control

Call admission control (CAC), also known as *resource management* (RM), is the mechanism by which new calls may be refused by Unify OpenScape Voice if the IP network does not have the capacity (bandwidth) to handle the call with a acceptable quality of service.

14.1 Overview

CAC provides an additional tool to ensure adequate voice quality for IP telephone calls. It ensures that real-time media calls are only established when the necessary bandwidth resources are available on all access links that exist between the following:

- The enterprise core network and the subnets serving its branch offices
- Branch offices that have dedicated access links to each other, in addition to other links present in the enterprise network

Real-time media calls should not be routed over networks that cannot guarantee an acceptable quality of service (QoS). An enterprise core network and the subnets serving its branch offices must provide sufficient bandwidth to support the real-time media traffic they are required to handle. It is also necessary for the real-time media packets to be correctly classified so that the network routers can provide the appropriate priority processing through their queues.

Loss of media packets can still occur at the aggregation layer that exists on the bandwidth-limited access link that exists between a branch office LAN and the backbone WAN. This can happen when the total bandwidth capacity of the access link is overbooked to an extent that forces the access routers to drop even high-priority real-time media packets. The result is a poor quality connection for all multimedia calls that are routed over the overbooked access link. CAC provides the bandwidth management that prevents these poor-quality connections from being established.

In the traditional telephony world, a circuit (line or trunk) is either busy or idle. When busy, the circuit is dedicated to a single call and so voice quality is predictable and assured. In contrast, LAN and WAN links are shared resources. When too many calls are routed over a LAN or WAN link, the result is not a call blockage, as in the telephony world, but reduced voice quality due to delayed or lost voice packets.

The feature allows the administrator to limit the number of calls and/or the amount of bandwidth used for phone calls on any LAN or WAN link. When used in coordination with effective VLAN and packet prioritization schemes to segregate voice and data traffic, CAC provides an effective means to assure good voice quality. This segregation and prioritization of voice and data traffic is important because CAC only manages telephone calls, and does not see or control the amount of data traffic on the network.

The network planner must determine how much bandwidth is required between the sites, and how much of that bandwidth can be used for voice, video, and fax traffic. Once established, CAC permits the rules to be enforced.

Consider the following simple scenario, illustrated in Figure 54, where a branch office is connected to the core network (WAN) via an access router. The LAN within the branch office is over-provisioned and has the capacity to guarantee good quality of service for real-time media. However, the bandwidth for access to the core network is limited, and the access router may start dropping voice packets if the capacity is exceeded.

In this scenario, the support for CAC/bandwidth management is required to assure that voice calls over the bandwidth-limited link are only allowed if there is enough bandwidth to guarantee an acceptable quality of service.

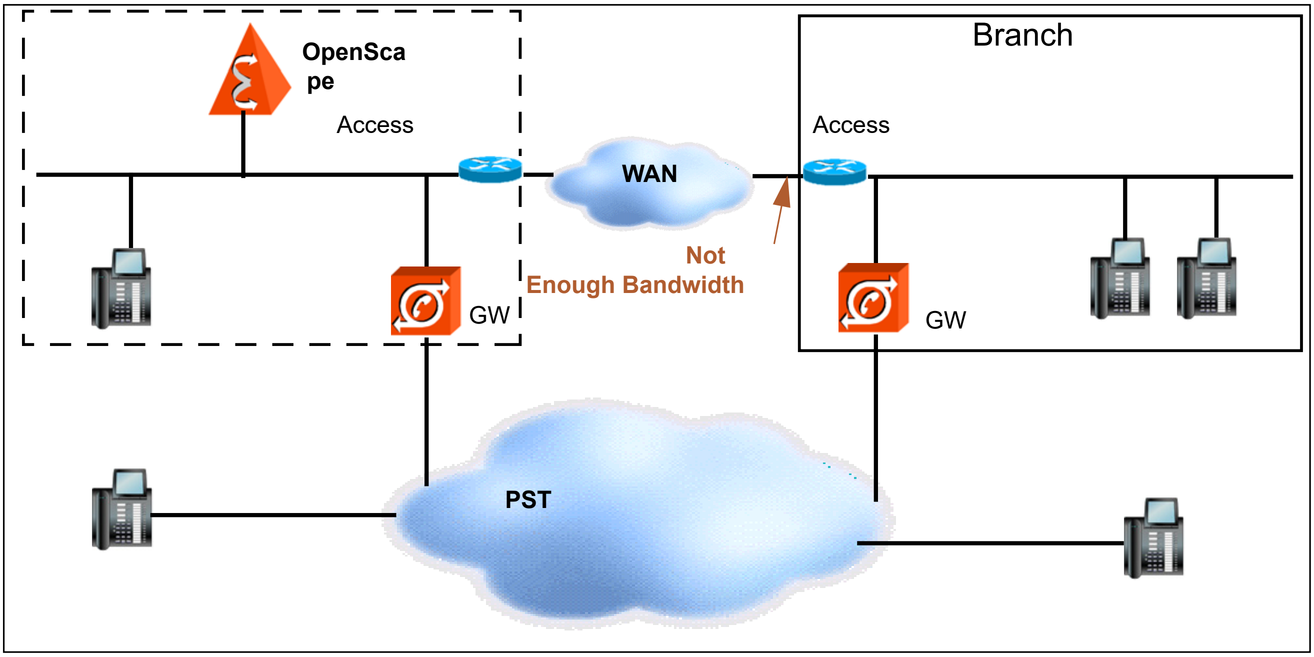


Figure 54 Call Admission Control—Branch Office with Bandwidth-Limited link

14.2 Supported Network Topologies

CAC supports the following network topologies:

- Star network
- Tree network
- Mesh network

Unify OpenScape Voice supports CAC for networks that use any combination of star, tree, and mesh network topologies.

14.2.1 Star Network

As shown in Figure 55, the star topology assumes that RTP traffic from and to each branch location is routed through a single bandwidth-limited access link to and from the backbone WAN.

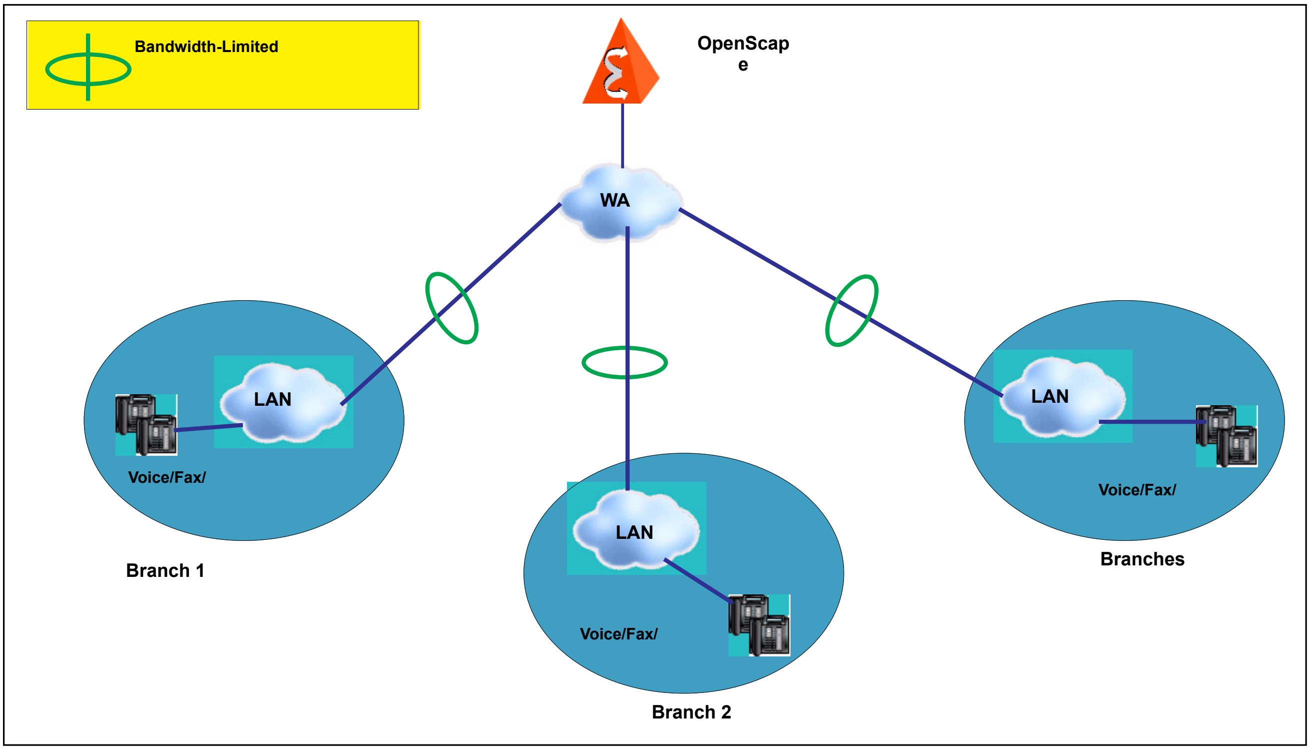


Figure 55 Call Admission Control—Star Network Topology

14.2.2 Tree Network

Some Unify OpenScape Voice customers use tree topologies, for which multiple levels of bandwidth-limited links need to be considered (Figure 56). In this topology, multiple levels of bandwidth-limited links are present. For example, a main branch office (Branch 1 in the figure) might have a 1-Mbps access link to the backbone WAN with ten sub-branches connected to the main branch via 200 Kbps links. In this scenario, two levels of bandwidth-limited links must be considered: from the sub-branches to the main branch, and from the main branch to the WAN.

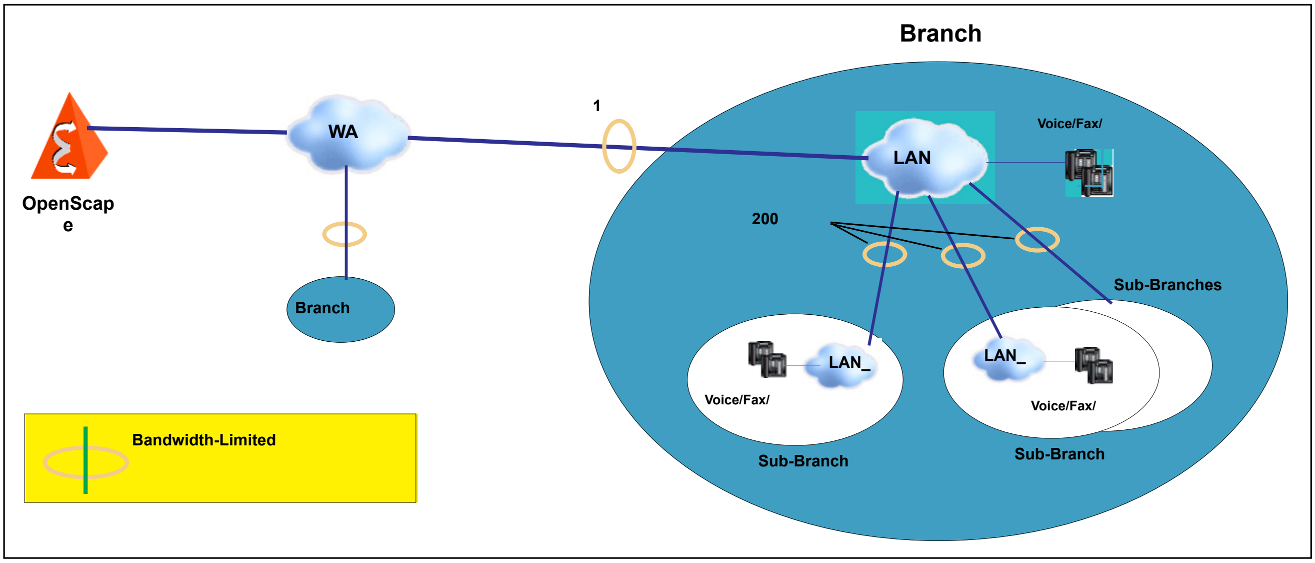


Figure 56 Call Admission Control—Tree Network Topology

14.2.3 Mesh Network

A mesh network topology (Figure 57) is used when some branch locations have dedicated links to other branches. For these branches, the RTP traffic is routed via a direct link between the two branch locations instead of routing through a backbone WAN.

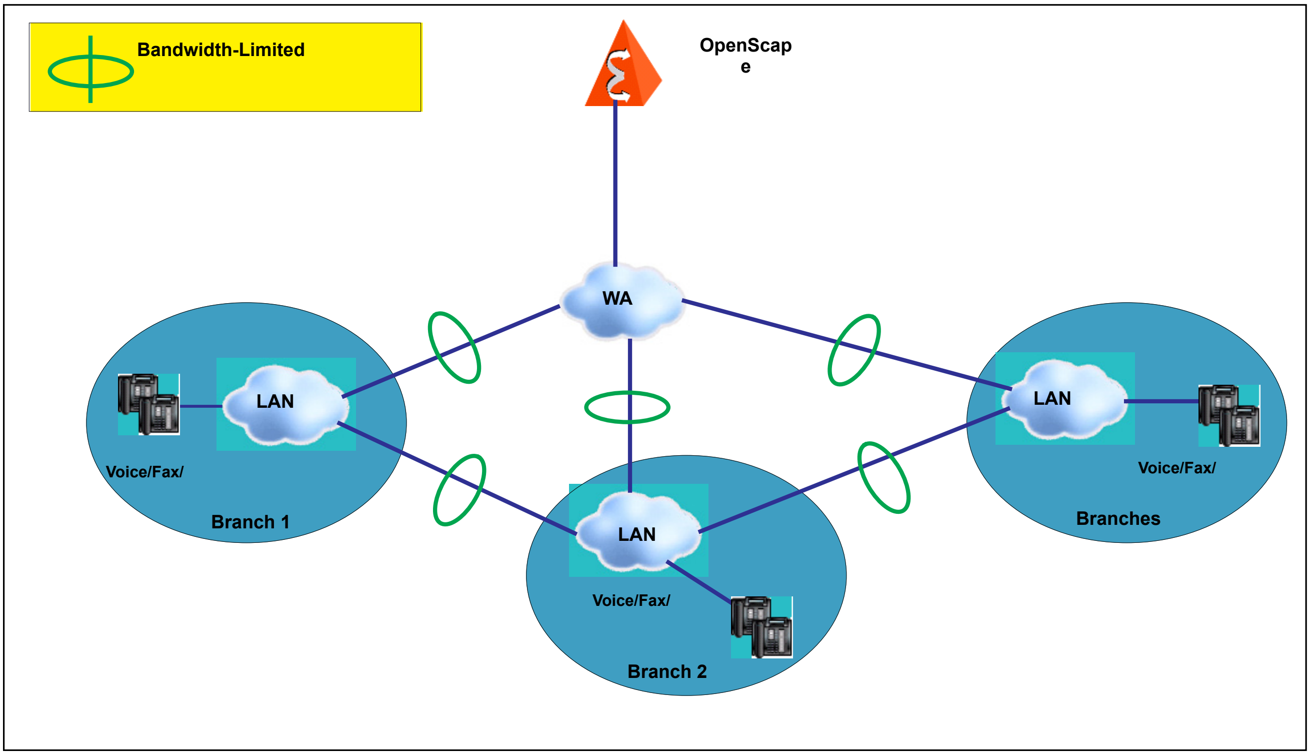


Figure 57 Call Admission Control—Mesh Network Topology

14.3 Concepts

In simplest terms, CAC permits the administrator to group subscribers and gateways into logical groups known as *CAC groups*, then defines or limits the amount of bandwidth which is available for calls between the groups.

Groups may be defined by or based on, subscriber number ranges (DNs), IP addresses, or subnets. A rule that sets the limit between groups is known as a *CAC policy*. If a new call exceeds that limit, it may be blocked or rerouted.

14.3.1 CAC Groups

A CAC group is required regardless of the type of network topology present. It represents the group of endpoints being served by the bandwidth-limited link which needs to be monitored. A group is the entity to which the CAC policies (see Section 14.3.3, “CAC Policies”) are applied. Unify OpenScape Voice supports the provisioning of up to 3000 CAC groups.

Groups are defined based on one of the following parameters:

- IP address
- Subnet
- Directory number: this can be a DN prefix (such as 1561555*) or the DN of a single user (for example,15615550110)

The definition for a group *cannot* be based on a combination of these parameters. However, a CAC group can be defined by multiple subnets, DNs, or IP addresses with the following limitations:

- Up to 128 IP addresses
- Up to 128 subnets
- Up to 64 DNs (with wildcard support)

Attention: If IPv4 and IPv6 addresses are present, each CAC group member might need to be provisioned twice—once for each IP address type.

Figure 58 shows some valid CAC group definitions.

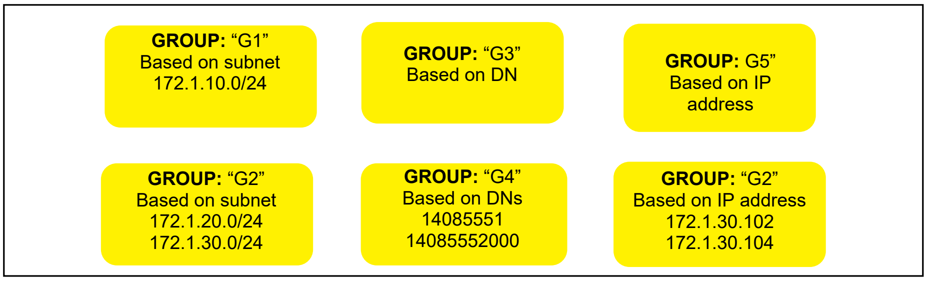


Figure 58 Valid CAC Group Definitions

In addition, CAC groups can be provisioned with the following information needed to support a backup access link for subscriber rerouting:

- Access router type
- Access route IP address and interface name

Refer also to Section 10.3, “Subscriber Rerouting”.

If two or more CAC groups have overlapping definitions, the internal CAC solution prioritizes the CAC groups as follows:

- CAC groups based on IP address have the highest priority, followed by CAC groups based on subnet.
- Subnets with a bigger mask have higher priority—for example, 171.1.10.0/24 has a higher priority than 171.1.0.0/16.
- CAC groups based on DN have the lowest priority.

14.3.2 Parent CAC Groups

A *parent CAC group* is required if a tree network topology is present. Its purpose is to establish relationships with higher- and subordinate-level CAC groups. A parent CAC group is just like any other CAC group, except that it is defined based on CAC groups instead of IP addresses, subnets, or DNs.

The administrator can define up to four levels of CAC groups and up to 300 child CAC groups. A CAC group can only be assigned to one parent CAC group.

Figure 59 shows how the child CAC groups and policies are provisioned to monitor the bandwidth at the first level, which is the level between the branches and the LAN that connects them.

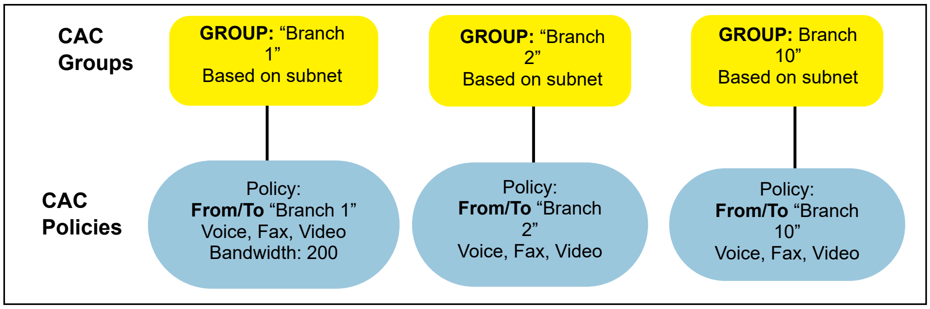

CAC Groups
GROUP: “Branch 1” Based on subnet
GROUP: “Branch 2” Based on subnet
GROUP: Branch 10” Based on subnet
CAC Policies
Policy: From/To “Branch 1” Voice, Fax, Video Bandwidth: 200
Policy: From/To “Branch 2” Voice, Fax, Video
Policy: From/To “Branch 10” Voice, Fax, Video

Figure 59 CAC Groups and Policies for First Level of Tree Network

Figure 60, "CAC Groups and Policies for Second Level of Tree Network Topology" illustrates how the parent CAC group and policy are provisioned to monitor the bandwidth at the second level, which is the level between the LAN and the WAN.

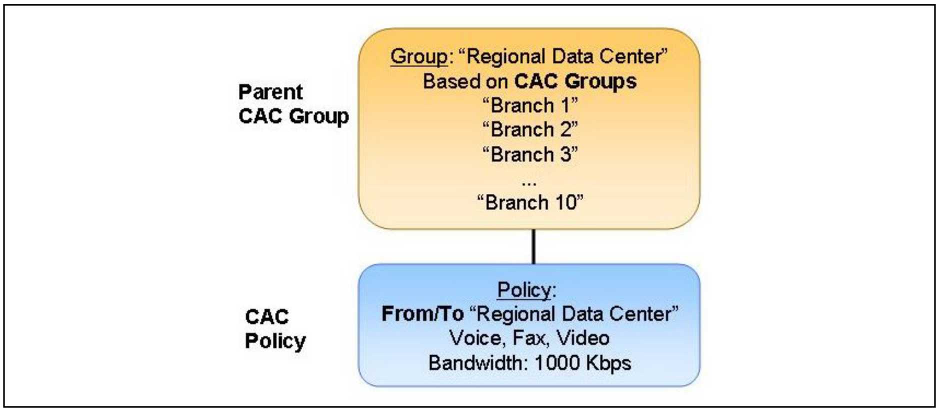


Figure 60 CAC Groups and Policies for Second Level of Tree Network Topology

14.3.3 CAC Policies

A CAC policy is assigned to a CAC group and represents the characteristics for the bandwidth-limited link being monitored.

Unify OpenScape Voice supports CAC policies for voice (RTP), video (RTP) and/or T.38 Fax (UDPTL).

A CAC policy contains the following information:

- The CAC group or parent CAC group to which the policy applies. The policy applies to all calls to and from the group.
- The traffic type controlled by the CAC policy. This can be voice (RTP), video (RTP), fax (T.38 over UDPTL), all three types, or a combination of two types
- The capacity limits the policy enforces for a primary link and optionally for a secondary (backup) link. Unify OpenScape Voice can limit the calls over a bandwidth-limited link based on number of calls, bandwidth limit, or both, as follows:
  - **Number of calls:** The concurrent calls per policy are counted. When the limit is reached, no new calls are admitted.
  - **Bandwidth limit:** Unify OpenScape Voice calculates the used bandwidth based on the negotiated codecs in the SDP. The bandwidth limit is the common limit for the traffic types associated with the CAC policy—for example, if the CAC policy is only applicable for voice, the bandwidth limit is exclusive for voice traffic.

The bandwidth limit must be entered considering the common limit reserved for voice/video/fax for upstream and downstream traffic. For instance, if a value of 1 Mbps is entered, it indicates that the upstream bandwidth is 1 Mbps and the downstream bandwidth is 1 Mbps as well.

– **Both:** If both number of calls and bandwidth limit are defined, the limit is enforced as soon as one is reached.

Note: The primary and the secondary link capacities must use the same criteria. For example, if the primary capacity is based on bandwidth limit, the secondary capacity must also be based on bandwidth limit.

- Whether to generate alarms when usage increases above the applicable threshold value. If alarm generation is enabled, the Internal Resource Manager (IRM):

  – Sends an alarm when the usage gets above the high threshold

  – Clears the alarm when the usage gets below the low threshold

  Default values may be used for both thresholds; the administrator can also specify custom values if desired.

- The permitted voice codecs that may be used for SIP and SIP-Q voice calls routed over the bandwidth-limited link represented by the CAC policy. Limiting permitted voice codecs in this manner optimizes the usage of the bandwidth and allow more simultaneous connections, while still guaranteeing an acceptable quality of service.

  For example, the administrator can limit voice calls placed between branch offices that are routed over the WAN to use codecs that support audio compression, such as G.729, while allowing voice calls within a branch office to use uncompressed G.711 codecs.

- The permitted video codecs that may be used for SIP and SIP-Q voice calls routed over the bandwidth-limited link represented by the CAC policy. Limiting permitted video codecs in this manner provides benefits comparable to the ability to limit voice codecs as described above.

- A flag that indicates whether connections to the media server for announcements/tones are ignored for bandwidth calculations.

Some features require a media server to collect DTMF digits or play a tone/announcement. The connection to the media server may be routed over a bandwidth-limited link when the media server is located elsewhere in the network. Such media server connections can occur even when the feature involves endpoint devices that are located within the same CAC group.

- **When this option is disabled:** Insufficient bandwidth to the media server can result in the feature to either be blocked or to continue without progress tones, depending on the feature scenario.
- **When this option is enabled:** Bandwidth used for media server connections are ignored for the purpose of bandwidth management. This allows the media server always to play tones/announcements and collect DTMF digits, even when bandwidth limitations exist. Occasional degradation in speech quality may occur due to temporary overbooking of a bandwidth-limited link when this option is enabled.

Note: Only connections for tones and announcements are ignored when this option is set. Connections for media server applications, such as conferencing and unified messaging, are always counted in the bandwidth calculations.

- A flag that indicates whether answered calls are allowed even if insufficient bandwidth is present. This can occur in scenarios in which the resource reservation only takes place when the destination answers (when the SDP offer is included in the SIP 200 OK response).

  This option, when set, eliminates the possibility of a situation in which a bandwidth limitation could prevent the media stream from being connected after a subscriber has already answered a call. Occasional degradation in speech quality may occur due to temporary overbooking of a bandwidth-limited link when this option is enabled.

- A flag that indicates whether Unify OpenScape Voice should allow a video call to proceed as an audio-only call in case there is not enough bandwidth for the video stream. This flag is only applicable for CAC policies which include the video traffic type.

One CAC policy can only be related to one CAC group. A CAC group, on the other hand, can be related to multiple CAC policies as long as the same traffic type is not used by more than one policy.

For example:

One policy for audio, another policy for fax (OK)

or

One policy for both audio and fax, another policy for video (OK)

but not

One policy for audio and video, another policy for fax and video (not allowed because video is defined twice)

Therefore, a CAC group can be related to up to three CAC policies—one policy for voice, one for video, and one for fax.

Figure 61, "CAC Policy Relationships to CAC Groups" shows the relationship between the CAC policies and CAC groups.

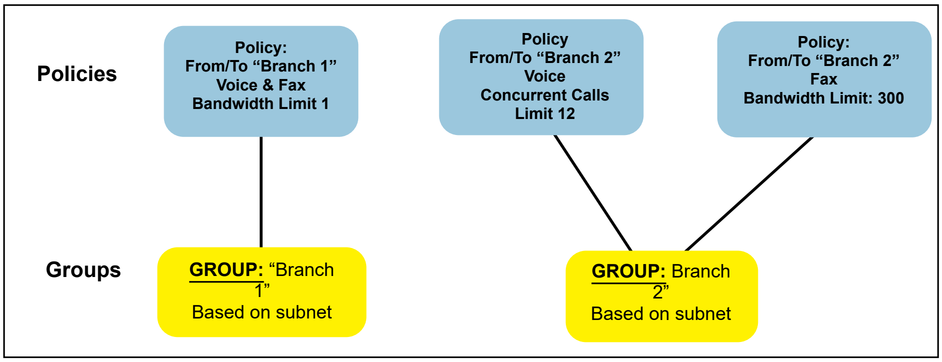

Policies
Policy: From/To "Branch 1" Voice & Fax Bandwidth Limit 1
Policy From/To "Branch 2" Voice Concurrent Calls Limit 12
Policy: From/To "Branch 2" Fax Bandwidth Limit: 300
Groups
GROUP: "Branch 1" Based on subnet
GROUP: Branch 2" Based on subnet

Figure 61 CAC Policy Relationships to CAC Groups

Unify OpenScape Voice supports the provisioning of up to 6000 CAC policies; this limit includes group-to-group CAC policies, which are described in the following section.

Note: When a new CAC policy is provisioned, Unify OpenScape Voice does not apply the policy to any existing calls. Only new calls after the policy has been provisioned are monitored by Unify OpenScape Voice.

14.3.4 Group-to-Group CAC Policies

A *group-to-group CAC policy* is required if a mesh network topology is present. This policy is used to represent the properties of a dedicated bandwidth-limited link between two CAC groups—for example, between two branch offices that have a dedicated link to one another.

A group-to-group CAC policy contains the same information as a CAC policy. However:

- The administrator must specify additional information so that it is assigned to two CAC groups rather than one.

- It does not have secondary link capacities.

Figure 62, "Group-to-Group CAC Policies" provides examples of group-to-group CAC policy usage. In these examples, group-to-group CAC policies are present for:

- The voice traffic between branches 1 and 2. A separate policy is applicable to the fax and video traffic between the branches.
- The voice, fax, and video traffic between branches 2 and 3.

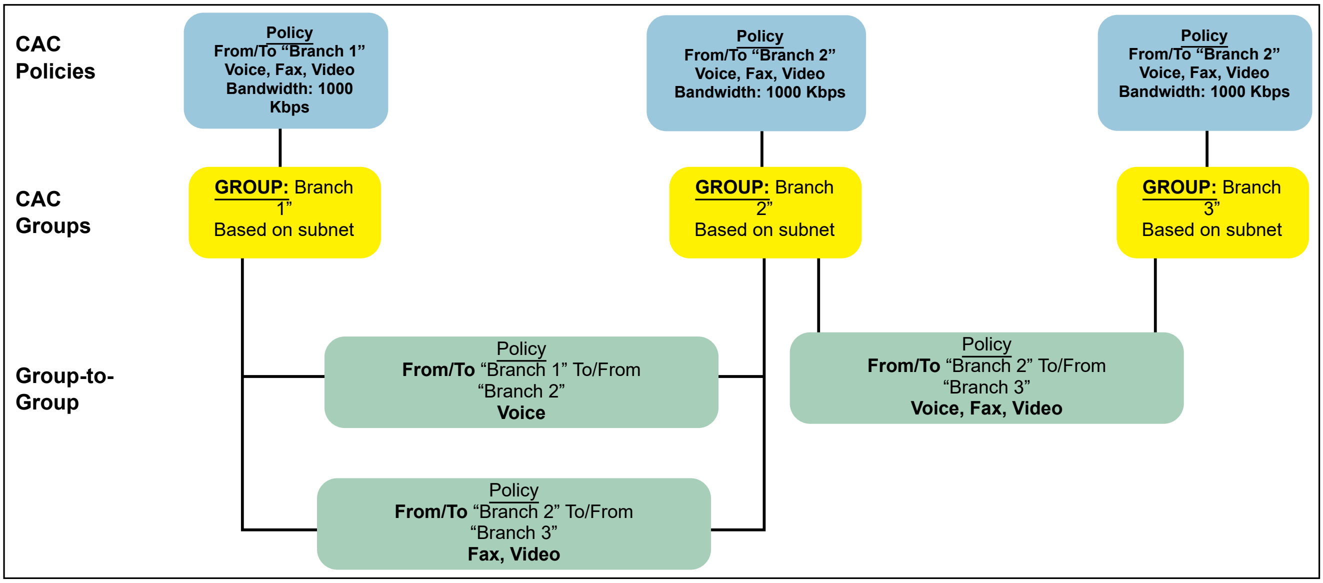

CAC Policies
Policy From/To "Branch 1" Voice, Fax, Video Bandwidth: 1000 Kbps
Policy From/To "Branch 2" Voice, Fax, Video Bandwidth: 1000 Kbps
Policy From/To "Branch 2" Voice, Fax, Video Bandwidth: 1000 Kbps
CAC Groups
GROUP: Branch 1" Based on subnet
GROUP: Branch 2" Based on subnet
GROUP: Branch 3" Based on subnet
Group-to-Group
Policy From/To "Branch 1" To/From "Branch 2" Voice
Policy From/To "Branch 2" To/From "Branch 3" Voice, Fax, Video
Policy From/To "Branch 2" To/From "Branch 3" Fax, Video

Figure 62 Group-to-Group CAC Policies

14.4 Functional Operation

A resource manager (RM) function within Unify OpenScape Voice's universal call engine (UCE) integrates bandwidth management with call processing in order to provide robust call handling, such as the rerouting of a call via the PSTN when there is insufficient bandwidth in the enterprise network to carry the call, based on bandwidth availability.

When a new call is placed, the following takes place:

1. The predicted bandwidth needed for the new call is compared to the remaining available bandwidth for each bottleneck link in the connection based on the CAC group and policies assigned to the originating and destination endpoints.
2. Unify OpenScape Voice reserves the bandwidth and allows the call to proceed if there is sufficient bandwidth on each bottleneck link in the route.

3. After the call is answered and connected, Unify OpenScape Voice adjusts the bandwidth reservation for the call based on the actual negotiated codec that is selected by the source and destination endpoints.

4. After the call is released, the bandwidth resource is also released.

Unify OpenScape Voice reroutes or denies the call if there is insufficient bandwidth on any of the bottleneck links. Refer to Section 14.5, “CAC Rerouting” and Section 14.6, “Call Denial”.

14.5 CAC Rerouting

One of the benefits of the integrated CAC solution is Unify OpenScape Voice's ability to provide rerouting via the PSTN in case there is not enough bandwidth in the applicable bandwidth-limited link, whether this link is between branch offices or from the branch office to the WAN. The rerouting call scenarios are tightly coupled with Unify OpenScape Voice’s ability to reroute calls based on a provisionable set of SIP response codes. Refer also to Chapter 10, “Gateway and Subscriber Rerouting”.

Among other things, this feature provides for the rerouting of calls to SIP gateways, SIP-Q gateways, or SIP subscribers if Unify OpenScape Voice receives a SIP response code indicating a bandwidth restriction (for example, `606 Not Acceptable`).

For the integrated CAC solution, Unify OpenScape Voice does not actually receive a SIP 606 response code from the terminating B-side of the call. However, the RM function in the terminating SIP session manager internally responds with the same error message as if a SIP 606 response code was received in response to an INVITE message sent to the B-side. No INVITE message is actually sent to the B-party in case of bandwidth limitation.

Figure 63 provides an example in which the RM reroutes the call via gateway GwyBoc1 using the rerouting rules discussed in Chapter 10, “Gateway and Subscriber Rerouting”.

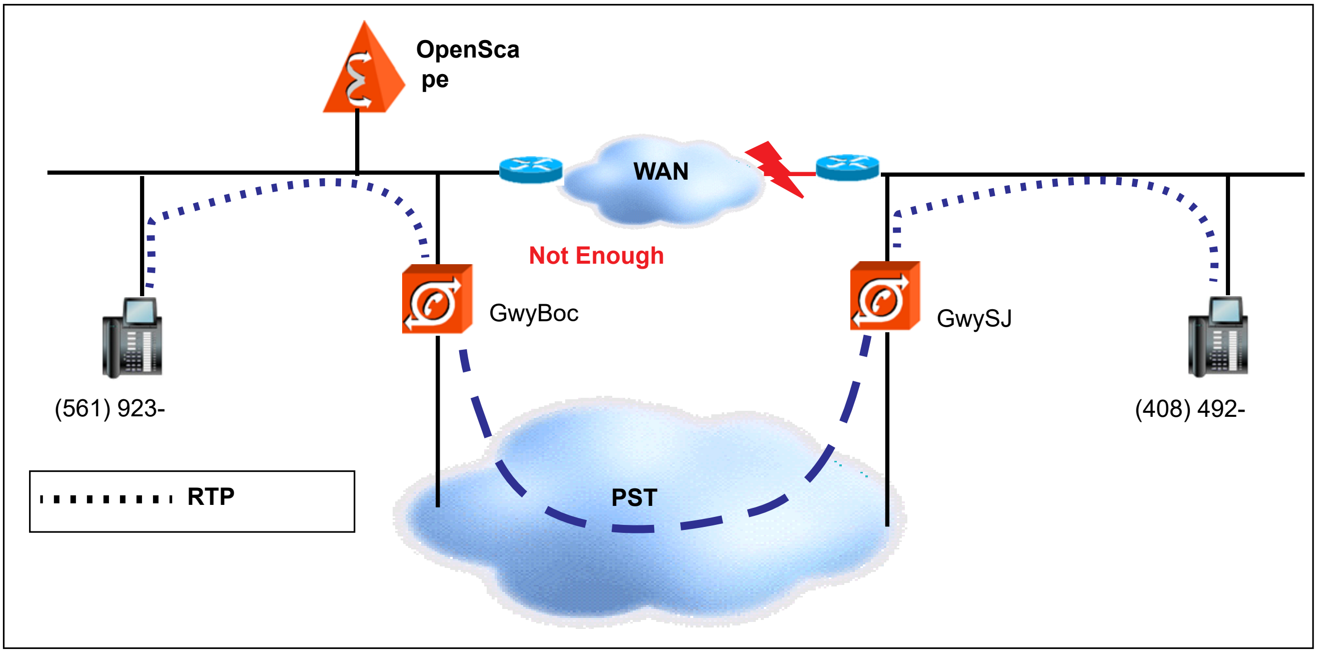


Figure 63 Call Admission Control—Rerouting Based On Insufficient Bandwidth

14.6 Call Denial

Attention: The information in this section is only applicable to non-emergency calls. CAC never denies emergency calls.

When CAC rerouting is not possible or is not configured, Unify OpenScape Voice returns the SIP 606 response code to the calling SIP endpoint. It is a local function of the SIP endpoint as to how the 606 response code is handled—for example, the announcement the calling user hears or the display received.

14.7 Monitoring of Concurrent Calls and Bandwidth Utilization

As described in Section 14.3.3, “CAC Policies”, a CAC policy can limit the calls over a bandwidth-limited link based on number of calls, bandwidth limit, or both.

Unify OpenScape Voice Assistant and the CLI can be used to display the current status for each provisioned CAC policy. This means displaying the number of concurrent calls and the actual bandwidth usage applicable to the CAC policy at any given time.

Both the number of concurrent calls and the actual bandwidth usage are displayed independent of whether the CAC policy is limiting the calls based on number of calls, bandwidth limit, or both.

14.8 Dynamic Handling of Link Failures

Unify OpenScape Voice permits optional provisioning of primary and secondary link capacities for each CAC policy. The ability permits the support of an access router that can switch over to a backup link (with a different bandwidth capacity) than the primary link, if the primary link fails. Figure 64, "Sample Configuration for Dynamic Handling of Link Failures" provides a simple example of this configuration.

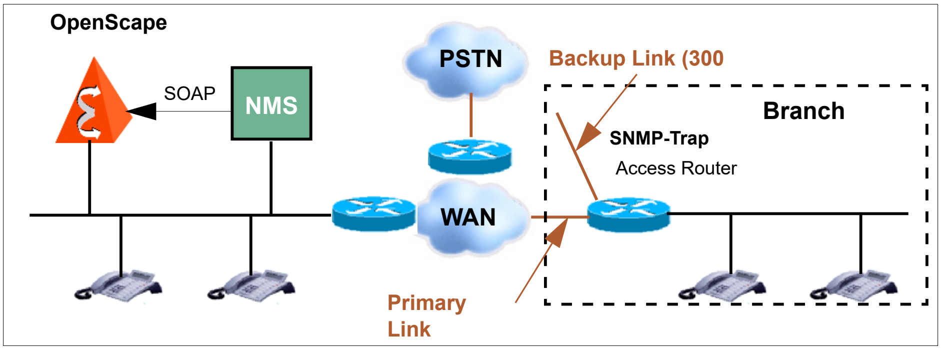


Figure 64 Sample Configuration for Dynamic Handling of Link

The primary or secondary capacity can be dynamically selected by the customer's network management system (NMS) via a SOAP/XML interface. If the NMS becomes aware of an access router's link failure, it uses the Link Failure Web Service to notify Unify OpenScape Voice to use the secondary capacity for the CAC policy of the associated access link. If the primary link access is restored, the Link Failure Web Service also provides a command to Unify OpenScape Voice to switch back to the primary capacity of the CAC policy. Refer to the *Unify OpenScape Voice Application Developer's Manual: Volume 2, Link Failure Management* for more information about this Web service.

When a backup link having a different bandwidth capacity than the primary link exists for a given CAC group, additional parameters need to be defined in the corresponding CAC group and CAC policy configuration. For the example topology shown in Figure 64, the CAC group and CAC policy shown in Figure 65 must be created for the branch office.

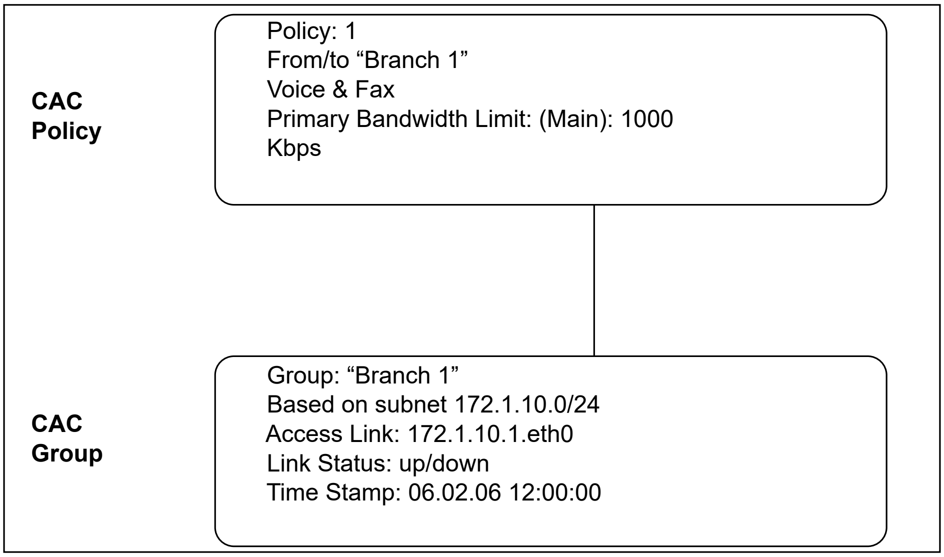

CAC Policy
Policy: 1
From/to “Branch 1”
Voice & Fax
Primary Bandwidth Limit: (Main): 1000 Kbps
CAC Group
Group: “Branch 1”
Based on subnet 172.1.10.0/24
Access Link: 172.1.10.1.eth0
Link Status: up/down
Time Stamp: 06.02.06 12:00:00

Figure 65 Sample CAC Group and CAC Policy for Dynamic Handling of Link Failures

14.9 Bandwidth Calculation

As described in Section 14.3.3, “CAC Policies”, the CAC policies in the Unify OpenScape Voice server will limit the calls over a bandwidth-limited link based on number of calls, bandwidth limit, or both. In case of bandwidth-based policies, the Unify OpenScape Voice server behavior is as follows:

1. For new calls, the Unify OpenScape Voice server calculates the required bandwidth ($BW_{REQUIRED}$) based on the worst-case codec in the call request. The Unify OpenScape Voice server then adds the required bandwidth of the call to the currently used bandwidth (BW_{USED}); and compares it to the limit provisioned for the policy (BW_{LIMIT}). If the limit is not reached ($BW_{USED} + BW_{REQUIRED} =< BW_{LIMIT}$), the call is allowed and the required bandwidth is reserved ($BW_{USED} = BW_{USED} + BW_{REQUIRED}$).
2. After the call is established, the Unify OpenScape Voice server calculates the actual bandwidth (BW_{ACTUAL}) used by the call based on the negotiated codec in the call answer. The Unify OpenScape Voice server then updates the currently used bandwidth with the actual bandwidth used by the call ($BW_{USED} = BW_{USED} + [BW_{ACTUAL} - BW_{REQUIRED}]$).
3. When the call is disconnected, the Unify OpenScape Voice server releases the actual bandwidth (BW_{ACTUAL}) used by the call ($BW_{USED} = BW_{USED} - BW_{ACTUAL}$).

The current CAC/bandwidth management solution performs bandwidth reservations based on the endpoint's signaling address, as opposed to the media address. This is because the resource reservation must be done before the called party starts alerting and because the Unify OpenScape Voice server does not know the media address for the called party until it answers.

The signaling address and the media address usually match. One exception may be in scenarios in which there is a non-transparent proxy—for example, another Unify OpenScape Voice server—in the way. In these scenarios, the endpoints behind the proxy are considered to be in a different domain, and this feature only performs the reservation up to the proxy.

For instance, consider the network topology shown in Figure 66, "Call Admission Control—Endpoints Behind Another Unify OpenScape Voice Server", in which Unify OpenScape Voice server **A** serves Branch Office 1, and Unify OpenScape Voice server **B** serves Branch Office 2. In this case, the bandwidth management for the bottleneck link to Branch Office 1(L1) is performed by Unify OpenScape Voice server **A**. The bandwidth management for the bottleneck link to Branch Office 2 (L2), on the other hand, is performed by Unify OpenScape Voice server **B**.

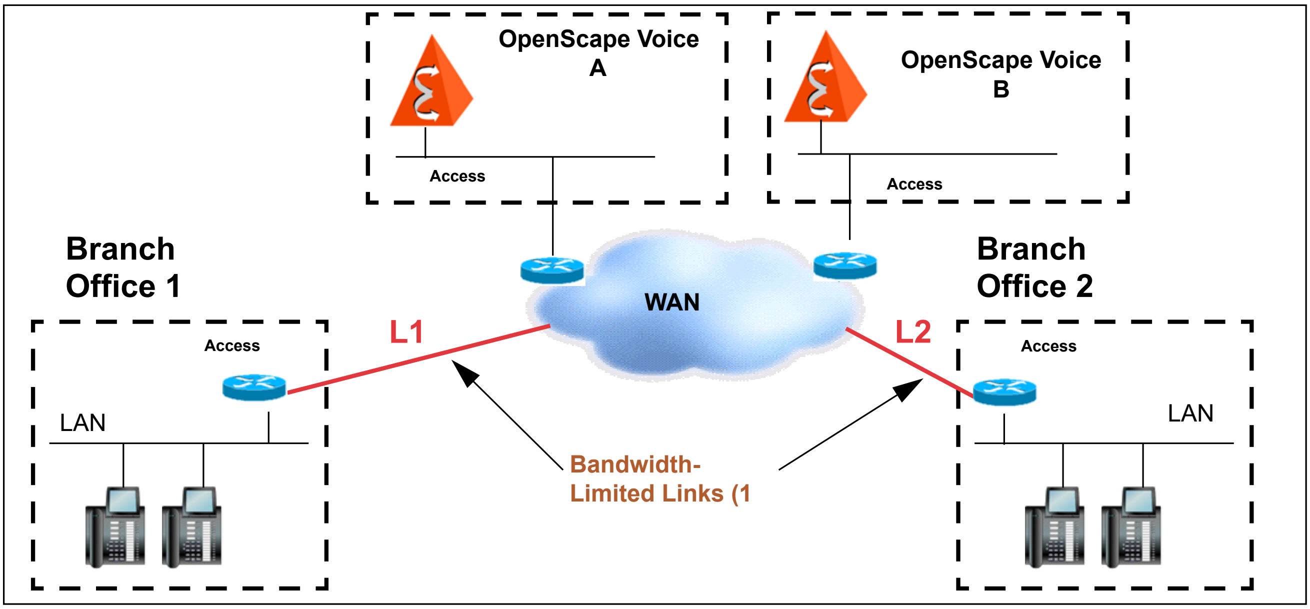


Figure 66 Call Admission Control—Endpoints Behind Another Unify OpenScape Voice Server

14.9.1 Bandwidth Calculation Factors

The IRM calculates only the IP bandwidth required to transport the media payload. It does not take in consideration the overhead added by the Layer 2 (L2) transport protocol, for example, Ethernet, ATM, Frame Relay, and so on. The IRM considers the transport of UDP media packets over Internet Protocol version 4 (IPv4) or IPv6. When IPv6 is present, the IRM is able to consider the additional overhead for the IPv6 header when performing bandwidth calculations. Furthermore, the IRM supports the ICE-Lite semantics, which are used in the Unify OpenScape Voice solution by dual-stack devices that support IPv4 and IPv6. The CAC implementation evaluates the ICE-Lite parameters to verify whether IPv6 is being offered; if it is, CAC considers the extra bandwidth it requires.

The IRM does not consider multicast SDP sessions. Nor does it consider any mechanisms that reduce the overhead of IP, UDP and RTP headers, such as RTP header compression, which may be present in the network.

A voice call requires two unidirectional RTP channels. The IRM assumes that the bandwidth required by both channels is always the same, that is, the audio streams are always symmetric.

The IRM does not take silence suppression into consideration for bandwidth calculation.

Unknown static and dynamic payload types are treated, by default, as a 64 kbps codec with a packetization interval of 20 ms. However, both the bit rate and packetization interval for these “unknown” payload types is configurable.

The IRM provides an overload protection mechanism in case of high-traffic volume.

The IRM switches into overload mode when its internal queue of requests reaches a high-threshold limit. In this mode, new call requests are rejected and an alarm will be generated. The IRM switches back to normal mode when the internal request queue depth reaches a low-threshold.

14.9.2 Bandwidth Calculation Settings

Unify OpenScape Voice uses the bandwidth control parameters specified in Unify OpenScape Voice Assistant to perform bandwidth calculations for CAC.

The default values assigned to these parameters are sufficient for most environments. However, the values of these parameters can be adjusted to tailor CAC to a particular environment. Refer to the *OpenScape Voice, Configuration, Administrator Documentation* for more information.

14.9.3 Bandwidth Requirements for Codecs

Bandwidth requirements for codecs vary depending on the codec type, the link speed, and whether payload encryption is used. Use of codecs that provide compression introduces a trade-off of speech quality against additional capacity.

The IRM computes bandwidth for the following codec types:

- G.711 A-law
- G.711 μ-law
- G.722
- G722.1 (24, 32, and 48 kbps)
- G.723.1
- G.726 (16, 24, 32 and 40 kbps)
- G.728
- G.729 (includes G.729, G.729A, G.729B and G.729A/B)
- iLBC (internet Low Bit Rate Codec) [RFC3952]
- AAC-LC (MP4A-LATM)
- AMR (Adaptive Multi-Rate codec) [RFC3267]
- AMR-WB (Adaptive Multi-Rate Wideband codec) [RFC3267]
- H263 (MPEG-4/ASP) Video
- H264 (MPEG-4/AVC Video

Refer to the *OpenScape Voice, Configuration, Administrator Documentation* for more information.

14.9.4 Audio Codec Considerations

Table 105 lists considerations when using certain audio codecs.

Codec	Applicable Considerations
G723	The G.723 codec has two bit-rates associated with it: 5.3 kbps and 6.4 kbps. Both rates are a mandatory part of the encoder and decoder and it is possible to switch between the rates at any 30 ms frame boundary. For bandwidth calculation purposes, the IRM assumes a bit rate of 6.4kbps, that is, the worst-case scenario.
iLBC	The iLBC codec supports two basic frame lengths: 30 ms at 13.33 kbps and 20 ms at 15.2 kbps. For bandwidth calculation purposes, the IRM assumes a bit rate of 15.2 kbps, that is, the worst-case scenario.
AMR	The AMR codec is a multi-mode codec that supports 8 narrow band speech-encoding modes with bit rates between 4.75 and 12.2 kbps. The sampling frequency used in AMR is 8000 Hz and the speech encoding is performed on 20 ms speech frames. For bandwidth calculation purposes, the IRM assumes a bit rate of 12.2 kbps, that is, the worst-case scenario.
AMR-WB	The AMR-WB codec is also a multi-mode speech codec that supports 9 wide band speech-encoding modes with respective bit rates ranging from 6.6 to 23.85 kbps. The sampling frequency used in AMR-WB is 16000 Hz and the speech processing is performed on 20 ms frames. For bandwidth calculation purposes, the IRM assumes a bit rate of 23.85 kbps, that is, the worst-case scenario.

Table 105 Audio Codec Considerations

14.9.5 Video Considerations

CAC was enhanced to support video. This support includes an internal CAC solution support for the following video codecs:

- H263 [RFC2190]
- H264 [RFC3984]
- MPEG4 – For MPEG-4, only the subtypes ASP (Advanced Simple Profile, Part 2) and AVC (Advanced Video Codec, Part10) are handled, as they are the same as the ITU codecs above. Other subtypes are handled as unknown codecs.

All other video codecs are treated as Unknown.

Other than the video codec, all other characteristics for a video call—for example, picture size, frame rate, and the like—are not negotiated via the SDP offer and answer mechanism. In the SDP offer and answer negotiation, each party only informs the other what they can receive, not what they are going to transmit.

The actual bandwidth being used by the video stream is constantly changing and will usually be a lower (up to 90%) than the maximum figure specified in the SDP offer and answer.

Due to these restrictions, the internal CAC solution uses statically configured values for the bandwidth requirements for the video streams for the different video codecs supported by Unify OpenScape Voice. The internal CAC solution also uses statically configured values for the bandwidth requirements for unknown video codecs.

The following parameters required for video bandwidth calculation can be configured on the Unify OpenScape Voice system:

- **H.263 Bandwidth:** The estimated bandwidth required by the video stream for an H.263 call (Default = 160 kbps)
- **H.264 Bandwidth:** The estimated bandwidth required by the video stream for an H.264 call (Table 106lists H.264 Video Codec Default Bandwidth Values Per Profile Level)
- **Unknown Bandwidth:** The estimated bandwidth required by the video stream for unknown video codecs (Default = 128 kbps)

Note that the internal CAC solution makes the bandwidth calculations, assuming a symmetrical RTP stream. If a CAC policy has a bandwidth limit of 1 Mbps, it means that the link’s upstream capacity is 1 Mbps and the downstream capacity is also 1 Mbps. Therefore, if the H.263 Bandwidth parameter is set to 160 kbps, it indicates that this bandwidth will be reserved for 160 Kbps upstream and 160 Kbps downstream.

The bandwidth calculations for H.264 codecs, which are performed during the SDP negotiation, also take into consideration the video profile level associated with the codec. This calculation also adds a fixed percentage value depending on whether:

- The transport takes place on IPv4 or IPv6 addresses.
- SRTP usage is present.

Profile Level	Default Bandwidth
1	64 kbps
1b	128 kbps
1.1	192 kbps
1.2	384 kbps
1.3	768 kbps
2	2000 kbps
2.1, 2.2	4000 kbps
3	10000 kbps
3.1	14000 kbps
3.2, 4	20000 kbps
4.1, 4.2	50000 kbps
5	135000 kbps
5.1	240000 kbps

Table 106 H.264 Video Codec Default Bandwidth Values Per Profile Level

14.9.6 Fax Considerations

For fax calls, most of the bandwidth is used in one direction. The IRM, however, reserves the same amount of bandwidth in both directions since it cannot determine the direction in which the Fax will be transmitted.

For Fax using T.38, the IRM only considers the transport of T.38 over UDP Transport Layer (UDPTL).

14.10 Establishing and Overriding Codec Restrictions

The internal CAC solution in Unify OpenScape Voice allows the system administrator to limit the voice codecs which can be used over a specific link. If required, the administrator can also assign attributes to endpoints and subscribers that override restrictions that are otherwise in effect.

Note: This is feature is also applicable to video codecs.This feature is *not* applicable to T.38 Fax over UDPTL in either version.

14.10.1 Establishing Restrictions

Limitation of codecs is required for the purpose of limiting the amount of bandwidth that is used for media streams (RTP/voice) traffic over bandwidth-limited (bottleneck) links in the network.

For example, voice codec restriction permits the customer to have excellent voice quality in local connections by setting the preferred codecs for all phones and endpoints to high-quality codecs—for example, G.711 or G.722. For WAN connections, however, the customer may prefer to restrict the allowed codecs to compressed codecs only—for example, G.723 or G.729. In this manner, the customer can optimize the usage of the bandwidth and allow more simultaneous connections while still guaranteeing an acceptable quality of service.

As an example, consider the network topology in Figure 67.

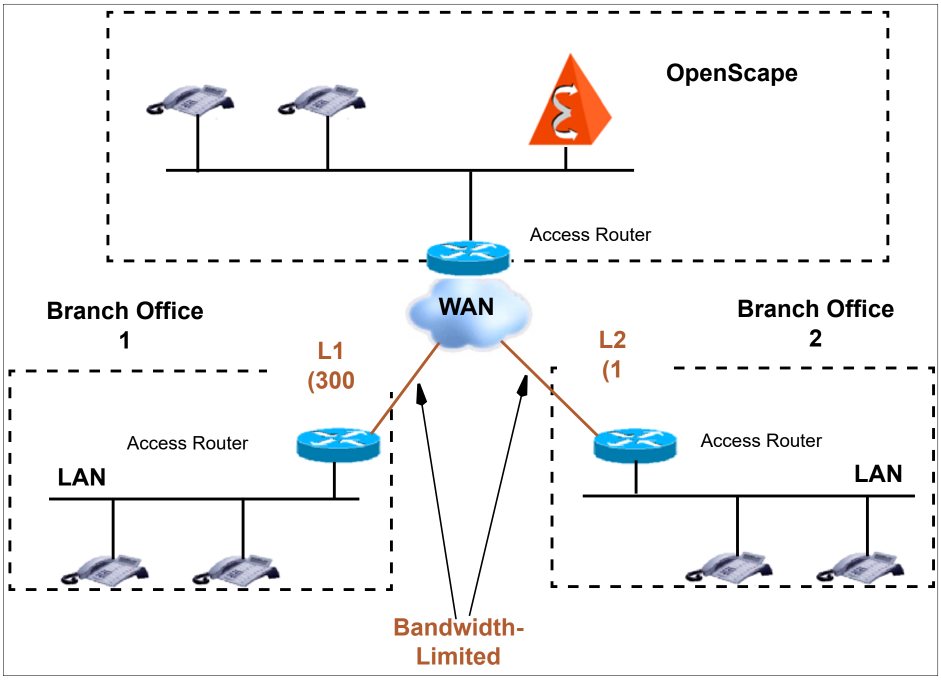


Figure 67 Sample Network Topology Requiring Voice Codec

Now assume that the administrator only wants to allow G.729 for calls over the L1 link because it only supports 300 Kbps. On the other hand, there need be no restrictions for calls over the L2 link that supports 1 Mbps—that is, all codecs are allowed.

In this case, the CAC groups and policies shown in Figure 68, "Sample CAC Policies to Restrict Voice Codecs" should be created to control the traffic over the bandwidth-limited links L1 and L2. The CAC groups and policies can be created in a comparable manner to limit the video codecs.

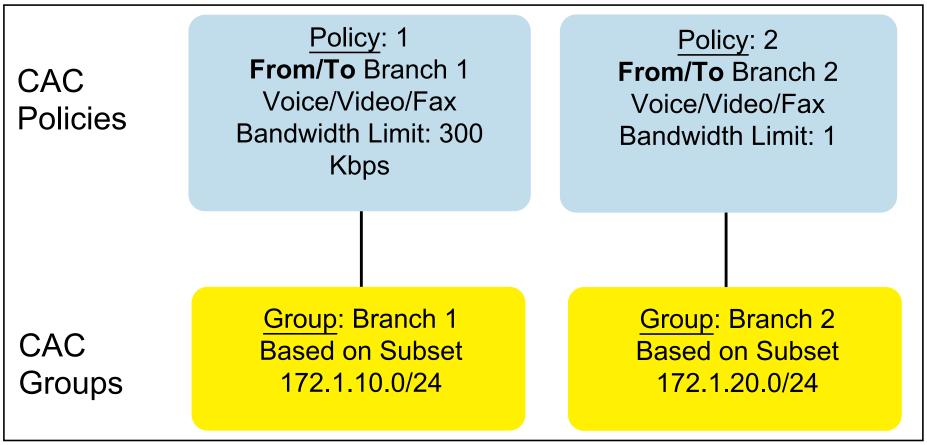


Figure 68 Sample CAC Policies to Restrict Voice Codecs

14.10.2 Overriding Restrictions

When codec restrictions are in place, they are applicable to all calls on the bandwidth-limited link. However, the administrator can override, on a per-endpoint and/or per-subscriber basis, the codec restrictions the CAC policy imposes. After doing so, the entity (endpoint or subscriber) can perform normal codec negotiation, using all codecs offered by the endpoints.

The following are examples of scenarios in which this ability is useful:

- Calls to and from unknown destinations that exit and enter the VoIP network via a particular endpoint (gateway)
- Calls to the media server that provides large conferencing support
- Calls to and from an executive

14.11 Traffic Measurements

The Unify OpenScape Voice server provides traffic measurements for Call Admission Control (CAC). The following measurements shall be collected for each provisioned CAC Group:

- CAC policy ID
- CAC policy name
- CAC Group Name
- Number of Offered Calls
- Number of Blocked Calls

Number of Offered Calls: This counter is incremented each time Unify OpenScape Voice attempts to route a call over the access link associated with a CAC Group. A call that is successfully completed over multiple access links (for example, a call between two branch locations) shall be counted as an offered call in both the originating and terminating CAC groups. However, if the call is blocked due to bandwidth limitations on the originating access link, only the offered calls counter of the originating CAC group shall be incremented; the offered calls counter of the terminating CAC group shall not be incremented. In the same way, if the call is blocked due to bandwidth limitations on the terminating access link, only the offered calls counter of the terminating CAC group shall be incremented; the offered calls counter of the originating CAC group shall not be incremented.

This counter shall only be incremented if the call being established requires the *Concurrent Number Of Calls* counter for the CAC Policy to be incremented as well. This means, for instance, that the Offered Calls counter is only incremented by 1 in scenarios where the call is forked to multiple destinations in the same CAC group (for example, keysets with multiple line appearances, simultaneous ringing, multiple contacts, and the like).

Number of Blocked Calls: This counter is incremented each time Unify OpenScape Voice attempts to route a call over the access link associated with a CAC group but the call is denied or rerouted due to the CAC limitations imposed by the associated CAC policy. Notice that a “blocked call” in this context may have been successfully completed by rerouting via an alternate route, for example, via the local PSTN gateway.

The CAC measurements are stored in a log file for post-processing.

14.12 General Administration Concept

Unify OpenScape Voice Assistant supports the following under Unify OpenScape Voice → Administration → **Call Admission Control Management**:

- **Resource Management menu**:
  - Enabling the internal CAC solution
  - Configuration of parameters used for bandwidth calculation
- **CAC Groups menu**: Provisioning CAC groups
- **CAC Policies menu**: Provisioning CAC policies and group-to-group CAC policies
- **Call Admission menu:** Monitoring current status of all CAC groups, including current calls and bandwidth utilization

Voice codec restrictions are overridden by activating the Override IRM Codec Restriction attribute at either of the following paths:

- Unify OpenScape Voice → Business Group → Members → **Endpoints**
- Unify OpenScape Voice → Business Group → Members → **Subscribers**

Administration of the CAC group’s scheduling is performed in Operational Measurements Management (OMM). This includes setting the Logging Interval and the Retention Period for the measurements. This data can be invaluable to the network planner in evaluating the performance of the network and finding remedies for observed problems.

15 Media

15.1 Media Encryption

For customers who want added network security, the Unify OpenScape Voice server supports the use of secure real-time transport protocol (SRTP) as a means to secure its media traffic.

Refer to the *Unify OpenScape Voice Design and Planning Manual: Volume 3, Security Reference* for more information about media stream security.

15.1.1 SRTP Overview

SRTP in the Unify OpenScape Voice solution involves the coordination of SRTP implementation across multiple products. SRTP provides a framework for encryption and message authentication of Real-Time Transport Protocol (RTP) and Real-Time Transport Control Protocol (RTCP). Media encryption is entirely controlled by the media endpoints; the role of the Unify OpenScape Voice server is only to facilitate the negotiation of encryption parameters between the endpoints.

Encrypted media (SRTP) with the MIKEY Profile 0 key management protocol is supported by the following:

- Unify OpenStage, optiPoint 410 S/420 S phone families, optiClient 130 S, and selected third-party SIP phones
- OpenScape Media Server
- OpenScape Xpressions
- OpenScape Branch
- RG 8700
- Mediatrix gateways
- OpenScape SBC
- Connections between two Unify OpenScape Voice systems signaled over the SIP-Q interface
- Connections between Unify OpenScape Voice and the OpenScape 4000
- Connections between Unify OpenScape Voice and the HiPath 3000

- OpenScape Video endpoints (OpenScape Video VHD100, VHD400, VHD600).

15.1.2 Interworking with Non-SRTP Endpoints

Interworking with non-SRTP endpoints is supported via negotiation to RTP with no encryption.

The MIKEY keys for payload encryption are negotiated during the SDP offer- answer exchange. This procedure is performed in accordance with the Best Effort SRTP mechanism, which follows a standards-based approach and allows for backward compatibility.

However, certain third-party endpoints do not support Best Effort SRTP. To ensure that a call to one of these endpoints completes successfully, Unify OpenScape Voice can remove the SRTP-related attributes from the SDP offer before sending to the terminating node. Doing so ensures that the terminating side need not deal with the SRTP negotiation mechanism, and instead can negotiate the call to an unsecured mode.

Unify OpenScape Voice is preconfigured during installation or upgrade with a list of devices that are known to have problems with the Best Effort SRTP mechanism. The administrator can additionally do the following:

- Enable and disable Unify OpenScape Voice’s ability to determine if B-side is compliant with Best Effort SRTP on a system wide basis.
- If needed, add additional devices to the preconfigured list, which is located on the Best Effort SRTP tab of the SIP Settings screen. This is done by adding parts of the SIP User Agent header of the applicable devices to the list.
- Indicate whether a specific endpoint or subscriber should check for Best Effort SRTP. Depending on the endpoint or subscriber type, the options are as follows:
  - **Dynamic endpoints and subscribers**: The default operation is usually Automatic, which means that the system wide setting determines whether this check takes place. Other options are On and Off.
  - **Static endpoints and subscribers**: The default is On; Off is also an option.
  - **SIP-Q endpoints**: The only valid option is On.

For subscriber endpoints, this configuration is performed by modifying the Attributes tab of the Subscriber screen; for non-subscriber endpoints, by modifying the Attributes tab of the Endpoint screen.

15.1.3 Planning Considerations

- Use of encrypted media requires as a precondition the use of transport layer security (TLS) transport and digest authentication on the SIP signaling connection between the media endpoints and the Unify OpenScape Voice server. Unify OpenScape Voice supports up to 50,000 TLS subscribers, depending on average call rate and feature configuration.

  In addition, negotiation of the encryption parameters increases the number of messages required in many SIP call flows, negatively influencing switch capacity in terms of BHCA (busy hour call attempts) by as much as 20%. For encrypted calls, there is also an estimated 10% increase in network bandwidth requirements.

  Therefore, the planner must balance the need for security against the negative impact on bandwidth requirements and performance. A logical first step may be to configure only selected phones (for example, executive telephones) for TLS and secure media, until the overall impact on the network can be observed. The planner needs to understand, however, that both phones in a connection must be configured for TLS and secure media in order for a call between them to be secure.

- For an SRTP session to be successfully established, the time-of-day clock of the two communicating media endpoints needs to be synchronized within the allowable clock skew range. If the time-of-day clocks of the media endpoints are outside of the allowed range, an attempt to establish an SRTP session will fail and the media connection will fall back to using unsecured RTP. The default maximum time skew window is 180 seconds (3 minutes). Time zone differences between the communicating media endpoints are accounted for by the use of a UTP timestamp. For this reason it is strongly recommended to use Network Time Protocol (NTP) to maintain an accurate time-of-day clock setting in all media endpoint devices that use payload encryption.

- When TLS is used for SIP, all endpoints (gateways, phones, and soft clients) must be configured to register (or in the case of gateways, permanently registered) at node 1 of the cluster. This means that the system is operating in the active-standby mode. In the event that the active node fails, the standby node will become active within 30 seconds, with no loss of existing calls and minimal impact to subscribers. This configuration has the following consequences:

– In case of large systems (more than 15,000 subscribers), Unify OpenScape Voice server call handling capacity (maximum stable calls) may somewhat reduced.

– In case of a geographically separated cluster, this restriction may have a modest impact on the signaling bandwidth required between the sites, but no impact on the audio bandwidth requirements between the sites. Signaling bandwidth is impacted to this extent:

  - Signaling messages that would be carried across the cluster interconnect links in a balanced (active-active) configuration will be carried, instead, over the signaling VLAN and/or common WAN between the sites.

  - Endpoints at the standby (node 2) site will send all call control signaling messages to the active (node 1) remote site. This can amount to as much as 250 bits per second per endpoint. If the remote site has 10,000 phones, this could amount to as much as 2.5 Mbps in additional inter-location signaling, but would typically be less

These configuration restrictions will be removed in V4R1.

15.2 Early Media

For calls encountering early media, Unify OpenScape Voice server may signal SIP messages containing different SDP answers towards the originating SIP interface (SIP UAC) within the same dialog. If the SIP UAC interface is unable to process multiple SDP answers in the same dialog before answer, the following configuration options should be considered:

1. If the external SIP endpoint device, gateway or appliance can be configured to support the OpenScape Voice signaling procedures this configuration should be used.

2. In some networks, the solution proposed in option 1 above may not be viable. Therefore, as an alternative, when the SIP UAC interface is associated with a SIP endpoint such as a SIP Service Provider, configuration of the SIP Endpoint’s or Subscriber’s attribute “Support Media Redirection” should be set to enabled. When enabled, any media change requiring a new SDP answer be sent to

the SIP interface before the call is answered will result in the SIP UAC being redirected requiring the dialog to be reestablished to receive the new SDP answer.

Note: The SIP UAC interface must support SIP redirect server procedures.

3. In some networks neither solution proposed under option 1 or 2 may be viable. Therefore, the Unify OpenScape Voice server answers the call for a Hunt Group (e.g., Overflow, Night Service, CFNR, etc.) when answered by a user.

A Erlang B Carried Traffic Capacity Table

This appendix contains the Erlang B carried traffic capacity table and rules for using it.

A.1 Introduction

The Erlang B table in Section A.3, “Erlang B Table” provides the correlation between traffic levels in Erlangs, blockage levels in percent, and the number of trunks required. For information on Erlangs and blockage levels, refer to Section 4.1.1, “Traffic Measurement Units”.

Note that the **Number of Trunks** column is incremented by one between one and 200 trunks, then incremented by five between 200 and 1000 trunks. Therefore, some rounding up might be required to obtain the number of trunks you need. This is explained in Section A.2, “Using the Table”.

A.2 Using the Table

To find the required number for trunks for a desired Erlang value and a desired blockage level:

1. Find the column with the desired blockage level.
2. In this column, find the row with the desired Erlang value. If the specific Erlang value is not found, find the row with the next Erlang value.
3. In this row, find the required number of trunks in the **Number of Trunks** column.

For example, assume you have a PBX with 2000 lines, 294.4 Erlangs, and a 0.50 percent blockage level, and you need to calculate the required number of trunks. Do the following:

1. Find the column for the 0.50 percent blockage level.
2. Within this column, look for 294.4. This value is not found. Go to the next value, which is 297.85.
3. In the row showing the value 297.85, read the value for the required number of trunks. This value is 330. You need 330 trunks.

A.3 Erlang B Table

Number of Trunks	Blockage Levels in Percent									
	0.01	**0.05**	**0.10**	**0.50**	**1.00**	**2.00**	**5.00**	**10.00**	**15.00**	**20.00**
1	0.00	0.00	0.00	0.01	0.01	0.02	0.05	0.10	0.15	0.20
2	0.01	0.03	0.05	0.10	0.15	0.22	0.36	0.54	0.68	0.80
3	0.09	0.15	0.19	0.35	0.45	0.59	0.85	1.14	1.36	1.54
4	0.23	0.36	0.44	0.70	0.86	1.07	1.45	1.84	2.12	2.36
5	0.45	0.65	0.76	1.13	1.35	1.62	2.11	2.59	2.94	3.21
6	0.73	1.00	1.14	1.61	1.89	2.23	2.81	3.38	3.78	4.09
7	1.05	1.39	1.58	2.15	2.48	2.88	3.55	4.20	4.64	4.98
8	1.42	1.83	2.05	2.72	3.10	3.55	4.32	5.04	5.52	5.90
9	1.83	2.30	2.55	3.32	3.74	4.26	5.10	5.89	6.42	6.82
10	2.26	2.80	3.09	3.94	4.42	4.98	5.91	6.76	7.32	7.75
11	2.72	3.33	3.65	4.59	5.11	5.72	6.72	7.64	8.24	8.69
12	3.21	3.88	4.23	5.25	5.82	6.48	7.55	8.53	9.16	9.63
13	3.71	4.44	4.83	5.93	6.54	7.25	8.39	9.42	10.09	10.58
14	4.24	5.03	5.44	6.63	7.28	8.04	9.24	10.33	11.02	11.53
15	4.78	5.63	6.07	7.34	8.03	8.83	10.10	11.24	11.96	12.49
16	5.34	6.25	6.71	8.06	8.79	9.63	10.97	12.15	12.90	13.44
17	5.91	6.87	7.37	8.79	9.56	10.44	11.84	13.07	13.85	14.41
18	6.49	7.51	8.04	9.53	10.33	11.26	12.72	13.99	14.79	15.37
19	7.09	8.17	8.72	10.28	11.12	12.09	13.60	14.92	15.75	16.34
20	7.70	8.83	9.40	11.04	11.91	12.92	14.49	15.86	16.70	17.30
21	8.32	9.50	10.10	11.80	12.71	13.76	15.38	16.79	17.66	18.28
22	8.95	10.18	10.80	12.57	13.51	14.60	16.28	17.72	18.62	19.25
23	9.58	10.86	11.51	13.35	14.32	15.45	17.18	18.66	19.58	20.22
24	10.23	11.56	12.23	14.13	15.14	16.30	18.08	19.61	20.54	21.20
25	10.88	12.26	12.96	14.92	15.96	17.15	18.99	20.55	21.50	22.17
26	11.54	12.97	13.69	15.72	16.79	18.02	19.90	21.50	22.47	23.15
27	12.21	13.68	14.42	16.52	17.62	18.88	20.81	22.45	23.43	24.13
28	12.88	14.40	15.17	17.32	18.45	19.75	21.72	23.40	24.40	25.11
29	13.56	15.13	15.91	18.13	19.29	20.62	22.64	24.35	25.37	26.09
30	14.24	15.86	16.67	18.94	20.13	21.49	23.56	25.30	26.34	27.07
31	14.94	16.59	17.42	19.75	20.98	22.37	24.48	26.26	27.32	28.05
32	15.63	17.33	18.19	20.57	21.83	23.25	25.41	27.21	28.29	29.03

Table 107 Erlang B Table (Seite 1 von 11)

Number of Trunks	Blockage Levels in Percent									
	0.01	**0.05**	**0.10**	**0.50**	**1.00**	**2.00**	**5.00**	**10.00**	**15.00**	**20.00**
33	16.33	18.08	18.95	21.40	22.68	24.13	26.33	28.17	29.26	30.01
34	17.04	18.83	19.72	22.22	23.54	25.02	27.26	29.13	30.24	31.00
35	17.75	19.58	20.50	23.05	24.39	25.91	28.19	30.09	31.22	31.98
36	18.47	20.34	21.27	23.89	25.25	26.80	29.12	31.05	32.19	32.96
37	19.19	21.10	22.06	24.72	26.12	27.69	30.06	32.02	33.17	33.95
38	19.91	21.86	22.84	25.56	26.98	28.58	30.99	32.98	34.15	34.93
39	20.64	22.63	23.63	26.40	27.85	29.48	31.93	33.94	35.12	35.93
40	21.37	23.40	24.42	27.24	28.72	30.38	32.86	34.91	36.10	36.92
41	22.10	24.18	25.21	28.09	29.59	31.28	33.80	35.88	37.08	37.90
42	22.84	24.95	26.01	28.94	30.46	32.18	34.74	36.84	38.06	38.89
43	23.58	25.74	26.81	29.79	31.34	33.08	35.68	37.81	39.04	39.88
44	24.33	26.52	27.61	30.64	32.22	33.99	36.63	38.78	40.02	40.87
45	25.08	27.30	28.42	31.50	33.10	34.89	37.57	39.75	41.01	41.86
46	25.83	28.09	29.23	32.35	33.98	35.80	38.52	40.72	41.99	42.85
47	26.58	28.89	30.04	33.21	34.86	36.71	39.46	41.69	42.97	43.84
48	27.34	29.68	30.85	34.08	35.75	37.62	40.41	42.66	43.96	44.83
49	28.10	30.48	31.66	34.94	36.63	38.54	41.36	43.63	44.94	45.82
50	28.86	31.28	32.48	35.80	37.52	39.45	42.31	44.61	45.92	46.81
51	29.63	32.08	33.30	36.67	38.41	40.36	43.26	45.58	46.91	47.80
52	30.40	32.88	34.12	37.54	39.30	41.28	44.21	46.55	47.89	48.79
53	31.17	33.69	34.94	38.41	40.20	42.20	45.16	47.53	48.88	49.78
54	31.94	34.50	35.77	39.28	41.09	43.12	46.11	48.50	49.86	50.77
55	32.71	35.31	36.59	40.15	41.99	44.04	47.06	49.48	50.85	51.76
56	33.49	36.12	37.42	41.02	42.88	44.96	48.02	50.45	51.83	52.75
57	34.27	36.93	38.25	41.90	43.78	45.88	48.97	51.43	52.82	53.74
58	35.05	37.75	39.08	42.78	44.68	46.81	49.93	52.41	53.81	54.74
59	35.83	38.56	39.92	43.65	45.58	47.73	50.88	53.38	54.79	55.73
60	36.62	39.38	40.75	44.53	46.48	48.65	51.84	54.36	55.78	56.72
61	37.41	40.20	41.59	45.41	47.38	49.58	52.80	55.34	56.77	57.71
62	38.20	41.02	42.43	46.30	48.29	50.51	53.75	56.32	57.76	58.71
63	38.99	41.85	43.27	47.18	49.19	51.43	54.71	57.30	58.74	59.70
64	39.78	42.67	44.11	48.06	50.09	52.36	55.67	58.28	59.73	60.69
65	40.57	43.50	44.95	48.95	51.00	53.29	56.63	59.26	60.72	61.68
66	41.37	44.33	45.80	49.84	51.91	54.22	57.59	60.24	61.71	62.68
67	42.17	45.16	46.64	50.72	52.82	55.15	58.55	61.22	62.70	63.67

Table 107 Erlang B Table (Seite 2 von 11)

Number of Trunks	Blockage Levels in Percent									
	0.01	**0.05**	**0.10**	**0.50**	**1.00**	**2.00**	**5.00**	**10.00**	**15.00**	**20.00**
68	42.97	45.99	47.49	51.61	53.73	56.08	59.51	62.20	63.69	64.66
69	43.77	46.82	48.34	52.50	54.64	57.01	60.48	63.18	64.67	65.66
70	44.57	47.66	49.19	53.39	55.55	57.95	61.44	64.16	65.66	66.65
71	45.38	48.49	50.04	54.29	56.46	58.88	62.40	65.14	66.65	67.64
72	46.18	49.33	50.89	55.18	57.37	59.82	63.36	66.12	67.64	68.64
73	46.99	50.17	51.75	56.07	58.29	60.75	64.33	67.10	68.63	69.63
74	47.80	51.01	52.60	56.97	59.20	61.69	65.29	68.08	69.62	70.63
75	48.61	51.85	53.46	57.86	60.12	62.62	66.26	69.07	70.61	71.62
76	49.42	52.69	54.31	58.76	61.04	63.56	67.22	70.05	71.60	72.62
77	50.23	53.54	55.17	59.66	61.95	64.50	68.18	71.03	72.59	73.61
78	51.05	54.38	56.03	60.56	62.87	65.44	69.15	72.02	73.58	74.60
79	51.86	55.23	56.89	61.45	63.79	66.38	70.11	73.00	74.57	75.60
80	52.68	56.07	57.75	62.35	64.71	67.31	71.08	73.98	75.56	76.59
81	53.50	56.92	58.61	63.26	65.63	68.25	72.05	74.97	76.55	77.59
82	54.32	57.77	59.48	64.16	66.55	69.20	73.01	75.95	77.54	78.58
83	55.14	58.62	60.34	65.06	67.47	70.14	73.98	76.94	78.53	79.58
84	55.96	59.47	61.21	65.96	68.39	71.08	74.95	77.92	79.52	80.57
85	56.79	60.32	62.07	66.87	69.31	72.02	75.92	78.91	80.51	81.57
86	57.61	61.17	62.94	67.77	70.24	72.96	76.88	79.89	81.51	82.56
87	58.44	62.03	63.81	68.68	71.16	73.91	77.85	80.88	82.52	83.56
88	59.26	62.88	64.68	69.58	72.09	74.85	78.82	81.86	83.51	84.55
89	60.09	63.74	65.55	70.49	73.01	75.80	79.79	82.85	84.50	85.55
90	60.92	64.60	66.42	71.40	73.94	76.74	80.76	83.83	85.49	86.54
91	61.75	65.45	67.29	72.30	74.86	77.69	81.73	84.82	86.49	87.54
92	62.58	66.31	68.16	73.21	75.79	78.63	82.70	85.79	87.48	88.53
93	63.41	67.17	69.03	74.12	76.72	79.58	83.67	86.78	88.47	89.53
94	64.24	68.03	69.91	75.03	77.65	80.52	84.64	87.77	89.46	90.53
95	65.08	68.89	70.78	75.94	78.57	81.47	85.62	88.75	90.46	91.52
96	65.91	69.75	71.66	76.85	79.50	82.42	86.59	89.74	91.45	92.52
97	66.75	70.62	72.53	77.77	80.43	83.37	87.56	90.73	92.44	93.51
98	67.58	71.48	73.41	78.68	81.36	84.31	88.53	91.72	93.44	94.51
99	68.42	72.35	74.29	79.59	82.29	85.26	89.50	92.70	94.43	95.50
100	69.26	73.21	75.17	80.50	83.23	86.21	90.48	93.69	95.42	96.50
101	70.10	74.08	76.05	81.42	84.16	87.16	91.45	94.68	96.42	97.50
102	70.94	74.94	76.93	82.33	85.09	88.11	92.42	95.67	97.41	98.49

Table 107 Erlang B Table (Seite 3 von 11)

Number of Trunks	Blockage Levels in Percent									
	0.01	0.05	0.10	0.50	1.00	2.00	5.00	10.00	15.00	20.00
103	71.78	75.81	77.81	83.25	86.02	89.06	93.40	96.66	98.40	99.49
104	72.62	76.68	78.69	84.16	86.96	90.01	94.37	97.65	99.40	100.48
105	73.46	77.55	79.57	85.08	87.89	90.96	95.34	98.63	100.39	101.48
106	74.31	78.42	80.45	86.00	88.82	91.91	96.32	99.62	101.39	102.47
107	75.15	79.29	81.34	86.91	89.76	92.87	97.29	100.61	102.38	103.47
108	76.00	80.16	82.22	87.83	90.69	93.82	98.27	101.60	103.37	104.47
109	76.84	81.03	83.10	88.75	91.63	94.77	99.24	102.59	104.37	105.46
110	77.69	81.90	83.99	89.67	92.56	95.72	100.22	103.58	105.36	106.46
111	78.54	82.78	84.88	90.59	93.50	96.68	101.19	104.57	106.36	107.46
112	79.38	83.65	85.76	91.51	94.43	97.63	102.17	105.56	107.35	108.45
113	80.23	84.53	86.65	92.43	95.37	98.58	103.14	106.55	108.34	109.45
114	81.08	85.40	87.54	93.35	96.31	99.54	104.12	107.54	109.34	110.44
115	81.93	86.28	88.42	94.27	97.24	100.49	105.10	108.53	110.33	111.44
116	82.78	87.15	89.31	95.19	98.18	101.45	106.07	109.52	111.33	112.44
117	83.64	88.03	90.20	96.11	99.12	102.40	107.05	110.50	112.32	113.43
118	84.49	88.91	91.09	97.04	100.06	103.36	108.03	111.50	113.32	114.43
119	85.34	89.79	91.98	97.96	101.00	104.32	109.00	112.47	114.31	115.43
120	86.19	90.66	92.87	98.88	101.94	105.28	109.98	113.47	115.31	116.42
121	87.05	91.54	93.76	99.81	102.87	106.23	110.96	114.46	116.30	117.42
122	87.90	92.42	94.66	100.73	103.81	107.19	111.93	115.45	117.30	118.41
123	88.76	93.30	95.55	101.66	104.75	108.14	112.91	116.44	118.29	119.41
124	89.62	94.19	96.44	102.58	105.70	109.10	113.89	117.43	119.29	120.44
125	90.47	95.07	97.33	103.51	106.64	110.05	114.87	118.42	120.28	121.44
126	91.33	95.95	98.23	104.43	107.58	111.01	115.85	119.41	121.28	122.44
127	92.19	96.83	99.12	105.36	108.52	111.97	116.82	120.40	122.27	123.43
128	93.05	97.72	100.02	106.29	109.46	112.93	117.80	121.39	123.27	124.43
129	93.91	98.60	100.91	107.21	110.40	113.89	118.78	122.38	124.26	125.43
130	94.77	99.49	101.81	108.14	111.35	114.85	119.76	123.38	125.26	126.43
131	95.63	100.37	102.71	109.07	112.29	115.80	120.74	124.37	126.25	127.42
132	96.49	101.26	103.60	110.00	113.23	116.76	121.72	125.36	127.25	128.42
133	97.35	102.14	104.50	110.92	114.18	117.72	122.70	126.35	128.24	129.42
134	98.21	103.03	105.40	111.85	115.12	118.68	123.68	127.34	129.24	130.42
135	99.08	103.91	106.30	112.78	116.06	119.64	124.66	128.33	130.24	131.41
136	99.94	104.80	107.19	113.71	117.01	120.60	125.64	129.32	131.23	132.41
137	100.81	105.69	108.09	114.64	117.95	121.57	126.62	130.31	132.23	133.41

Table 107 Erlang B Table (Seite 4 von 11)

Number of Trunks	Blockage Levels in Percent									
	0.01	0.05	0.10	0.50	1.00	2.00	5.00	10.00	15.00	20.00
138	101.67	106.58	108.99	115.57	118.90	122.53	127.60	131.30	133.22	134.41
139	102.54	107.47	109.89	116.50	119.84	123.49	128.58	132.29	134.22	135.41
140	103.40	108.35	110.79	117.43	120.79	124.45	129.56	133.28	135.21	136.40
141	104.27	109.24	111.69	118.36	121.74	125.41	130.54	134.27	136.21	137.40
142	105.14	110.13	112.60	119.30	122.68	126.37	131.52	135.26	137.21	138.40
143	106.00	111.02	113.50	120.23	123.63	127.34	132.50	136.25	138.20	139.40
144	106.87	111.91	114.40	121.16	124.57	128.30	133.48	137.24	139.20	140.39
145	107.74	112.81	115.30	122.09	125.52	129.25	134.46	138.24	140.19	141.39
146	108.61	113.70	116.21	123.02	126.47	130.22	135.44	139.23	141.19	142.39
147	109.48	114.59	117.11	123.96	127.42	131.18	136.42	140.22	142.19	143.39
148	110.35	115.48	118.01	124.89	128.36	132.14	137.40	141.21	143.18	144.39
149	111.22	116.38	118.92	125.82	129.31	133.10	138.39	142.20	144.18	145.38
150	112.09	117.27	119.82	126.76	130.26	134.07	139.37	143.19	145.17	146.38
151	112.96	118.16	120.73	127.69	131.21	135.03	140.35	144.20	146.17	147.38
152	113.83	119.06	121.63	128.63	132.16	135.99	141.33	145.19	147.17	148.38
153	114.71	119.95	122.54	129.56	133.11	136.96	142.31	146.19	148.16	149.38
154	115.58	120.85	123.44	130.50	134.06	137.92	143.30	147.18	149.16	150.37
155	116.45	121.74	124.35	131.43	135.00	138.88	144.28	148.17	150.16	151.37
156	117.33	122.64	125.26	132.37	135.95	139.85	145.26	149.16	151.15	152.37
157	118.20	123.53	126.16	133.31	136.90	140.81	146.24	150.16	152.15	153.37
158	119.08	124.43	127.07	134.24	137.85	141.78	147.22	151.15	153.14	154.37
159	119.95	125.33	127.98	135.18	138.80	142.74	148.21	152.14	154.14	155.37
160	120.83	126.23	128.89	136.12	139.76	143.71	149.19	153.14	155.14	156.36
161	121.70	127.12	129.79	137.05	140.71	144.67	150.17	154.13	156.13	157.36
162	122.58	128.02	130.70	137.99	141.66	145.64	151.16	155.12	157.13	158.36
163	123.46	128.92	131.61	138.93	142.61	146.60	152.14	156.11	158.13	159.36
164	124.33	129.82	132.52	139.87	143.55	147.57	153.12	157.11	159.12	160.36
165	125.21	130.72	133.43	140.80	144.51	148.53	154.11	158.10	160.12	161.36
166	126.09	131.62	134.34	141.74	145.46	149.50	155.09	159.09	161.12	162.35
167	126.97	132.52	135.25	142.68	146.41	150.47	156.07	160.09	162.11	163.35
168	127.85	133.42	136.16	143.62	147.36	151.43	157.06	161.08	163.11	164.35
169	128.72	134.32	137.07	144.56	148.32	152.40	158.04	162.07	164.11	165.35
170	129.60	135.22	137.98	145.50	149.27	153.37	159.02	163.07	165.10	166.35
171	130.48	136.12	138.90	146.44	150.22	154.33	160.01	164.06	166.10	167.35
172	131.36	137.02	139.81	147.38	151.18	155.30	160.99	165.05	167.10	168.34

Table 107 Erlang B Table (Seite 5 von 11)

Number of Trunks	Blockage Levels in Percent									
	0.01	**0.05**	**0.10**	**0.50**	**1.00**	**2.00**	**5.00**	**10.00**	**15.00**	**20.00**
173	132.25	137.92	140.72	148.32	152.13	156.27	161.98	166.05	168.09	169.34
174	133.13	138.83	141.63	149.26	153.08	157.23	162.96	167.04	169.09	170.34
175	134.01	139.73	142.55	150.20	154.04	158.20	163.94	168.03	170.09	171.34
176	134.89	140.63	143.46	151.14	154.99	159.17	164.93	169.03	171.08	172.34
177	135.77	141.53	144.37	152.08	155.95	160.14	165.91	170.02	172.08	173.34
178	136.66	142.44	145.29	153.02	156.90	161.10	166.90	171.02	173.08	174.33
179	137.54	143.34	146.20	153.96	157.86	162.07	167.88	172.01	174.08	175.33
180	138.42	144.25	147.11	154.90	158.81	163.04	168.87	173.00	175.07	176.33
181	139.31	145.15	148.03	155.84	159.77	164.01	169.85	174.00	176.07	177.33
182	140.19	146.06	148.94	156.78	160.72	164.98	170.84	174.99	177.07	178.33
183	141.07	146.96	149.86	157.73	161.68	165.94	171.82	175.98	178.06	179.33
184	141.96	147.87	150.78	158.67	162.63	166.91	172.81	176.98	179.06	180.33
185	142.84	148.77	151.69	159.61	163.59	167.88	173.79	177.97	180.06	181.32
186	143.73	149.68	152.61	160.55	164.54	168.85	174.78	178.97	181.05	182.32
187	144.62	150.58	153.52	161.50	165.50	169.82	175.76	179.96	182.05	183.32
188	145.50	151.49	154.44	162.44	166.45	170.79	176.75	180.95	183.05	184.32
189	146.39	152.40	155.36	163.38	167.41	171.76	177.73	181.95	184.05	185.32
190	147.28	153.30	156.27	164.33	168.37	172.73	178.72	182.94	185.04	186.32
191	148.16	154.21	157.19	165.27	169.32	173.70	179.70	183.94	186.04	187.32
192	149.05	155.12	158.11	166.21	170.28	174.67	180.69	184.93	187.04	188.31
193	149.94	156.03	159.03	167.16	171.24	175.64	181.67	185.93	188.03	189.31
194	150.83	156.94	159.94	168.10	172.20	176.61	182.66	186.92	189.03	190.31
195	151.72	157.84	160.86	169.05	173.16	177.58	183.65	187.91	190.03	191.31
196	152.60	158.75	161.78	169.99	174.11	178.55	184.63	188.91	191.03	192.31
197	153.49	159.66	162.70	170.94	175.07	179.52	185.62	189.90	192.02	193.31
198	154.38	160.57	163.62	171.88	176.03	180.49	186.60	190.90	193.02	194.31
199	155.28	161.48	164.54	172.83	176.98	181.46	187.59	191.89	194.02	195.30
200	156.17	162.39	165.46	173.77	177.94	182.43	188.58	192.89	195.02	196.30
205	160.62	166.94	170.06	178.50	182.73	187.28	193.51	197.86	200.00	201.30
210	165.08	171.50	174.67	183.24	187.53	192.15	198.44	202.83	204.99	206.29
215	169.55	176.07	179.28	187.98	192.33	197.01	203.38	207.81	209.98	211.28
220	174.03	180.64	183.89	192.72	197.13	201.88	208.32	212.78	214.96	216.28
225	178.51	185.22	188.52	197.46	201.94	206.74	213.26	217.76	219.95	221.27
230	183.00	189.80	193.15	202.22	206.75	211.61	218.20	222.73	224.94	226.27
235	187.49	194.39	197.78	206.97	211.56	216.48	223.14	227.71	229.93	231.26

Table 107 Erlang B Table (Seite 6 von 11)

Number of Trunks	Blockage Levels in Percent									
	0.01	**0.05**	**0.10**	**0.50**	**1.00**	**2.00**	**5.00**	**10.00**	**15.00**	**20.00**
240	192.00	198.98	202.42	211.73	216.37	221.36	228.08	232.69	234.92	236.26
245	196.50	203.58	207.06	216.48	221.19	226.23	233.02	237.67	239.91	241.25
250	201.01	208.18	211.71	221.25	226.01	231.11	237.97	242.64	244.90	246.25
255	205.53	212.79	216.36	226.02	230.83	235.99	242.92	247.62	249.88	251.24
260	210.06	217.40	221.02	230.79	235.66	240.87	247.86	252.60	254.87	256.24
265	214.58	222.02	225.67	235.56	240.49	245.76	252.81	257.58	259.86	261.23
270	219.12	226.63	230.34	240.34	245.31	250.64	257.76	262.56	264.85	266.23
275	223.66	231.26	235.00	245.12	250.15	255.53	262.71	267.54	269.84	271.22
280	228.20	235.89	239.67	249.90	254.99	260.42	267.66	272.52	274.83	276.22
285	232.75	240.52	244.35	254.69	259.83	265.31	272.62	277.50	279.82	281.22
290	237.30	245.16	249.03	259.47	264.67	270.20	277.57	282.48	284.81	286.21
295	241.85	249.80	253.71	264.26	269.51	275.10	282.52	287.46	289.80	291.21
300	246.41	254.44	258.39	269.06	274.35	279.99	287.48	292.48	294.79	296.20
305	250.98	259.09	263.08	273.86	279.20	284.89	292.44	297.47	299.79	301.20
310	255.55	263.74	267.77	278.65	284.05	289.79	297.39	302.45	304.84	306.20
315	260.12	268.39	272.46	283.45	288.90	294.69	302.35	307.44	309.83	311.19
320	264.69	273.05	277.16	288.25	293.75	299.59	307.31	312.42	314.82	316.19
325	269.27	277.71	281.86	293.05	298.60	304.49	312.27	317.41	319.82	321.18
330	273.86	282.37	286.56	297.85	303.46	309.40	317.23	322.40	324.81	326.18
335	278.44	287.03	291.27	302.66	308.31	314.30	322.19	327.38	329.81	331.18
340	283.03	291.70	295.97	307.47	313.17	319.21	327.15	332.37	334.80	336.17
345	287.63	296.37	300.68	312.28	318.03	324.12	332.11	337.36	339.80	341.17
350	292.22	301.05	305.39	317.09	322.89	329.02	337.07	342.34	344.79	346.17
355	296.82	305.73	310.11	321.91	327.75	333.93	342.03	347.33	349.79	351.16
360	301.43	310.41	314.82	326.72	332.62	338.85	347.00	352.32	354.78	356.16
365	306.03	315.09	319.54	331.55	337.48	343.76	351.96	357.31	359.78	361.15
370	310.64	319.77	324.27	336.37	342.35	348.67	356.93	362.30	364.77	366.15
375	315.25	324.46	328.99	341.19	347.22	353.59	361.89	367.28	369.77	371.15
380	319.87	329.15	333.72	346.01	352.09	358.50	366.86	372.27	374.76	376.14
385	324.49	333.84	338.44	350.84	356.96	363.42	371.82	377.26	379.76	381.14
390	329.11	338.54	343.17	355.67	361.83	368.33	376.79	382.25	384.75	386.14
395	333.73	343.24	347.91	360.49	366.71	373.25	381.76	387.24	389.75	391.13
400	338.36	347.94	352.64	365.32	371.58	378.17	386.72	392.23	394.74	396.13
405	342.99	352.64	357.38	370.16	376.46	383.09	391.69	397.22	399.74	401.13
410	347.61	357.34	362.12	374.99	381.34	388.01	396.66	402.21	404.74	406.12

Table 107 Erlang B Table (Seite 7 von 11)

Number of Trunks	Blockage Levels in Percent									
	0.01	**0.05**	**0.10**	**0.50**	**1.00**	**2.00**	**5.00**	**10.00**	**15.00**	**20.00**
415	352.25	362.05	366.86	379.82	386.21	392.93	401.63	407.20	409.73	411.12
420	356.88	366.75	371.60	384.66	391.09	397.86	406.60	412.19	414.73	416.12
425	361.52	371.46	376.34	389.49	395.97	402.78	411.57	417.18	419.72	421.11
430	366.16	376.17	381.09	394.33	400.86	407.70	416.54	422.17	424.72	426.11
435	370.81	380.89	385.84	399.17	405.74	412.63	421.51	427.16	429.72	431.10
440	375.45	385.60	390.59	404.01	410.62	417.55	426.48	432.15	434.71	436.10
445	380.10	390.32	395.34	408.86	415.51	422.48	431.45	437.14	439.71	441.10
450	384.75	395.04	400.09	413.70	420.39	427.41	436.42	442.13	444.71	446.09
455	389.40	399.76	404.85	418.54	425.28	432.33	441.40	447.13	449.70	451.09
460	394.06	404.48	409.60	423.39	430.17	437.26	446.37	452.12	454.70	456.09
465	398.71	409.21	414.36	428.24	435.06	442.19	451.34	457.11	459.69	461.08
470	403.37	413.93	419.12	433.08	439.95	447.12	456.31	462.10	464.69	466.08
475	408.03	418.66	423.88	437.93	444.84	452.05	461.29	467.09	469.69	471.08
480	412.70	423.39	428.64	442.78	449.73	456.98	466.26	472.08	474.69	476.07
485	417.36	428.12	433.41	447.64	454.62	461.92	471.24	477.08	479.68	481.07
490	422.03	432.85	438.17	452.49	459.52	466.85	476.21	482.07	484.68	486.07
495	426.70	437.59	442.94	457.34	464.41	471.78	481.19	487.06	489.68	491.06
500	431.37	442.32	447.71	462.20	469.31	476.72	486.16	492.05	494.67	496.06
505	436.04	447.06	452.48	467.05	474.20	481.65	491.14	497.04	499.67	501.05
510	440.71	451.80	457.25	471.91	479.10	486.58	496.11	502.04	504.67	506.05
515	445.39	456.54	462.03	476.77	484.00	491.52	501.09	507.03	509.66	511.05
520	450.07	461.28	466.81	481.63	488.90	496.46	506.06	512.02	514.66	516.04
525	454.75	466.03	471.58	486.49	493.80	501.39	511.04	517.02	519.66	521.04
530	459.43	470.77	476.35	491.35	498.70	506.33	516.02	522.01	524.66	526.03
535	464.11	475.52	481.13	496.21	503.60	511.27	520.99	527.00	529.65	531.03
540	468.79	480.27	485.91	501.07	508.48	516.21	525.97	531.99	534.65	536.03
545	473.48	485.02	490.70	505.94	513.38	521.15	530.95	536.99	539.65	541.02
550	478.17	489.77	495.47	510.80	518.29	526.09	535.93	541.98	544.64	546.02
555	482.86	494.52	500.26	515.67	523.19	531.02	540.90	546.97	549.64	551.02
560	487.55	499.27	505.04	520.54	528.09	535.97	545.88	551.97	554.64	556.01
565	492.24	504.02	509.83	525.40	533.00	540.91	550.86	556.96	559.64	561.01
570	496.93	508.78	514.61	530.27	537.90	545.85	555.84	561.95	564.63	566.00
575	501.63	513.54	519.40	535.13	542.81	550.79	560.82	566.95	569.63	571.00
580	506.32	518.30	524.19	540.00	547.71	555.73	565.80	571.94	574.63	576.00
585	511.03	523.06	528.98	544.86	552.62	560.67	570.78	576.94	579.63	580.99

Table 107 Erlang B Table (Seite 8 von 11)

Number of Trunks	Blockage Levels in Percent									
	0.01	**0.05**	**0.10**	**0.50**	**1.00**	**2.00**	**5.00**	**10.00**	**15.00**	**20.00**
590	515.73	527.82	533.77	549.74	557.53	565.62	575.76	581.93	584.62	585.99
595	520.43	532.58	538.56	554.61	562.44	570.56	580.74	586.92	589.62	590.98
600	525.13	537.34	543.35	559.48	567.34	575.51	585.72	591.92	594.62	595.98
605	529.83	542.11	548.15	564.35	572.25	580.45	590.70	596.91	599.62	600.97
610	534.54	546.88	552.95	569.23	577.16	585.40	595.68	601.91	604.61	605.97
615	539.25	551.64	557.74	574.10	582.07	590.34	600.66	606.90	609.61	610.97
620	543.95	556.41	562.54	578.98	586.99	595.29	605.64	611.89	614.61	615.96
625	548.66	561.18	567.34	583.85	591.90	600.23	610.62	616.89	619.61	620.96
630	553.37	565.96	572.14	588.73	596.81	605.18	615.60	621.88	624.61	626.11
635	558.08	570.72	576.94	593.60	601.72	610.13	620.58	626.88	629.60	631.11
640	562.80	575.49	581.74	598.48	606.64	615.07	625.56	631.87	634.60	636.11
645	567.51	580.27	586.54	603.36	611.55	620.02	630.54	636.87	639.60	641.11
650	572.23	585.04	591.34	608.24	616.46	624.97	635.53	641.86	644.60	646.11
655	576.94	589.82	596.15	613.12	621.38	629.92	640.51	646.86	649.59	651.11
660	581.66	594.59	600.95	618.00	626.29	634.87	645.49	651.85	654.59	656.11
665	586.38	599.37	605.76	622.88	631.21	639.82	650.47	656.85	659.59	661.11
670	591.10	604.15	610.57	627.76	636.13	644.77	655.46	661.84	664.59	666.11
675	595.82	608.93	615.37	632.65	641.04	649.72	660.44	666.83	669.59	671.11
680	600.54	613.71	620.18	637.53	645.96	654.67	665.42	671.83	674.58	676.10
685	605.27	618.49	624.99	642.41	650.88	659.62	670.40	676.82	679.58	681.10
690	609.99	623.27	629.80	647.30	655.80	664.57	675.39	681.82	684.58	686.10
695	614.72	628.05	634.61	652.18	660.72	669.52	680.37	686.81	689.58	691.10
700	619.45	632.83	639.43	657.07	665.63	674.47	685.35	691.81	694.58	696.10
705	624.17	637.62	644.24	661.95	670.55	679.42	690.34	696.80	699.57	701.10
710	628.90	642.40	649.05	666.84	675.47	684.38	695.32	701.80	704.57	706.10
715	633.63	647.19	653.87	671.73	680.40	689.33	700.30	706.80	709.57	711.10
720	638.37	651.98	658.68	676.61	685.32	694.28	705.29	711.79	714.57	716.10
725	643.10	656.77	663.50	681.50	690.24	699.24	710.27	716.79	719.57	721.10
730	647.83	661.56	668.32	686.39	695.16	704.19	715.26	721.78	724.56	726.10
735	652.57	666.35	673.14	691.28	700.08	709.14	720.24	726.78	729.56	731.10
740	657.30	671.14	677.95	696.17	705.01	714.10	725.23	731.77	734.56	736.10
745	662.04	675.94	682.77	701.06	709.93	719.05	730.21	736.77	739.56	741.10
750	666.78	680.73	687.59	705.95	714.85	724.01	735.20	741.76	744.56	746.09
755	671.51	685.52	692.42	710.84	719.78	728.96	740.18	746.76	749.55	751.09
760	676.25	690.32	697.24	715.74	724.70	733.92	745.17	751.75	754.55	756.09

Table 107 Erlang B Table (Seite 9 von 11)

Number of Trunks	Blockage Levels in Percent									
	0.01	0.05	0.10	0.50	1.00	2.00	5.00	10.00	15.00	20.00
765	680.99	695.11	702.06	720.63	729.63	738.87	750.15	756.75	759.55	761.09
770	685.74	699.91	706.88	725.52	734.55	743.83	755.14	761.75	764.55	766.09
775	690.48	704.70	711.71	730.41	739.48	748.79	760.12	766.74	769.55	771.09
780	695.22	709.50	716.53	735.31	744.40	753.74	765.11	771.74	774.55	776.09
785	699.97	714.30	721.36	740.20	749.33	758.70	770.09	776.73	779.54	781.09
790	704.71	719.10	726.19	745.10	754.25	763.66	775.08	781.73	784.54	786.09
795	709.46	723.90	731.01	749.99	759.18	768.61	780.06	786.72	789.54	791.09
800	714.21	728.70	735.83	754.89	764.11	773.57	785.05	791.72	794.54	796.09
805	718.95	733.50	740.66	759.78	769.04	778.53	790.04	796.72	799.54	801.09
810	723.70	738.30	745.48	764.68	773.97	783.49	795.02	801.71	804.53	806.09
815	728.44	743.11	750.31	769.58	778.89	788.45	800.01	806.71	809.53	811.09
820	733.20	747.91	755.14	774.47	783.82	793.41	805.00	811.70	814.53	816.09
825	737.95	752.72	759.97	779.37	788.75	798.36	809.98	816.70	819.53	821.08
830	742.70	757.52	764.80	784.27	793.68	803.32	814.97	821.69	824.53	826.08
835	747.46	762.33	769.64	789.17	798.61	808.28	819.96	826.69	829.53	831.08
840	752.21	767.13	774.47	794.07	803.54	813.21	825.00	831.69	834.52	836.08
845	756.97	771.94	779.30	798.97	808.47	818.17	829.99	836.68	839.52	841.08
850	761.72	776.75	784.13	803.87	813.40	823.13	834.97	841.68	844.52	846.08
855	766.48	781.56	788.97	808.79	818.33	828.09	839.96	846.68	849.52	851.08
860	771.24	786.37	793.80	813.69	823.27	833.05	844.95	851.67	854.52	856.08
865	775.99	791.18	798.64	818.59	828.20	838.01	849.94	856.67	859.52	861.08
870	780.75	795.99	803.47	823.49	833.13	842.97	854.92	861.66	864.51	866.08
875	785.51	800.80	808.31	828.39	838.06	847.93	859.91	866.66	869.51	871.08
880	790.27	805.61	813.15	833.30	842.99	852.89	864.90	871.66	874.51	876.08
885	795.04	810.42	817.98	838.20	847.93	857.85	869.88	876.65	879.51	881.08
890	799.80	815.24	822.82	843.10	852.86	862.82	874.87	881.65	884.51	886.08
895	804.57	820.05	827.66	848.01	857.79	867.78	879.86	886.64	889.51	891.08
900	809.33	824.87	832.50	852.91	862.73	872.74	884.85	891.64	894.50	896.08
905	814.09	829.68	837.34	857.82	867.66	877.70	889.84	896.64	899.50	901.08
910	818.85	834.50	842.18	862.72	872.60	882.66	894.82	901.63	904.50	906.08
915	823.62	839.32	847.02	867.63	877.53	887.63	899.81	906.63	909.50	911.07
920	828.39	844.12	851.86	872.54	882.47	892.59	904.80	911.63	914.50	916.07
925	833.16	848.94	856.70	877.44	887.40	897.55	909.79	916.62	919.50	921.07
930	837.92	853.76	861.54	882.35	892.34	902.51	914.78	921.62	924.49	926.07
935	842.69	858.58	866.39	887.26	897.27	907.48	919.76	926.62	929.49	931.07

Table 107 Erlang B Table (Seite 10 von 11)

Number of Trunks	Blockage Levels in Percent									
	0.01	**0.05**	**0.10**	**0.50**	**1.00**	**2.00**	**5.00**	**10.00**	**15.00**	**20.00**
940	847.46	863.39	871.23	892.17	902.21	912.44	924.75	931.61	934.49	936.07
945	852.23	868.21	876.07	897.07	907.15	917.40	929.74	936.61	939.49	941.07
950	857.00	873.03	880.92	901.98	912.08	922.37	934.73	941.60	944.49	946.07
955	861.77	877.85	885.76	906.89	917.02	927.33	939.72	946.60	949.49	951.07
960	866.54	882.68	890.61	911.80	921.96	932.30	944.71	951.60	954.48	956.07
965	871.31	887.50	895.45	916.71	926.89	937.26	949.70	956.59	959.48	961.07
970	876.08	892.32	900.30	921.62	931.83	942.22	954.68	961.59	964.48	966.07
975	880.85	897.14	905.15	926.53	936.80	947.19	959.67	966.59	969.48	971.07
980	885.63	901.97	909.99	931.44	941.73	952.15	964.66	971.58	974.48	976.07
985	890.40	906.79	914.84	936.35	946.67	957.12	969.65	976.58	979.48	981.07
990	895.18	911.61	919.69	941.26	951.61	962.08	974.64	981.58	984.47	986.07
995	899.96	916.44	924.54	946.17	956.55	967.05	979.63	986.57	989.47	991.07
1000	904.74	921.26	929.39	951.09	961.49	972.02	984.62	991.57	994.47	996.07

Table 107 Erlang B Table (Seite 11 von 11)

B Subnetting Scheme

B.1 Network Assignments

Table 108 illustrates one possible subnetting scheme for Unify OpenScape Voice. Appendix C, “Cluster Addressing Scheme” illustrates another valid configuration. A Class C network (a.b.c.0) is subnetted to provide eight subnets, each holding up to 30 host addresses. Selection of the Class C network is customer-specific. There are no restrictions on the value of this Class C network.

It is possible to combine the Unify OpenScape Voice IP subnets:

- The x-channel can be merged into the admin subnet.
- Billing and Admin can be combined.
- Billing, Admin and Signaling can be combined.

Note: It is recommended to separate Signaling from the other OAM&P subnets.

Network	Host Address Range	Broadcast Address	Subnet Mask	Purpose
0	a.b.c.1 to a.b.c.30	a.b.c.31	255.255.255.224	Admin VLAN
1	a.b.c.33 to a.b.c.62	a.b.c.63	255.255.255.224	Signaling VLAN
2	a.b.c.65 to a.b.c.94	a.b.c.95	255.255.255.224	CDR/Billing VLAN
3	a.b.c.97 to a.b.c.126	a.b.c.127	255.255.255.224	(unused)
4	a.b.c.129 to a.b.c.158	a.b.c.159	255.255.255.224	(unused)
5	a.b.c.161 to a.b.c.190	a.b.c.191	255.255.255.224	(unused)
6	a.b.c.193 to a.b.c.222	a.b.c.223	255.255.255.224	Voice VLAN
7	a.b.c.225 to a.b.c.254	a.b.c.255	255.255.255.224	Layer 2 Switch Maintenance
8	10.1.c.d			Cluster Private IP Network

Table 108 Network Assignments (Required)

B.2 Routed Subnets

The networks 0, 1, 2, 6, and 7 given in Table 108 all need to be routed by the IP network. The VLAN setup allows for the desired separation of the Administration, Signaling, CDR/Billing, and voice traffic within the IP network.

B.3 Non-Routed Networks

Networks 3, 4, and 5 are currently unused.

Network 8 is for private cluster communication internally and cannot be routed.

C Cluster Addressing Scheme

The cluster addressing scheme recommended by Unify is given in Table 109.

IP Address Function	Subnet	Remarks	Virtual? (see note)
Node	Admin	The node IP address used for installation and all OAM&P functions.	No
LSM	Admin	On this IP address, Unify OpenScape Voice receives SNMP traps from routers reporting link status changes.	Yes
Billing	Billing	For sending billing (CDR) files.	No
X-Channel	X-Channel	For node-to-node communication.	No
Signaling	Signaling	Static IP address for the signaling network. Not used for traffic.	No
SIP	Signaling	SIP signaling over TCP, UDP, or unilateral TLS.	Yes
SIP mutual TLS	Signaling	SIP signaling over mutual TLS.	Yes
MGCP	Signaling	MGCP signaling for media server.	Yes
CSTA	Signaling	CSTA signaling over TCP.	Yes
SBC LAN	Signaling	Local IP address for the SBC function of the IBM x 3250, used for signaling and media.	No
RSA	Admin	Integrated maintenance controller of node (IMM, iRMC, or VMK).	No
Outside Unify OpenScape Voice			
Gateway for RSA	Admin	Router IP to reach maintenance controller of partner node.	
SuperUser	Admin	IP address of management server with superuser privileges (generally the internal Unify OpenScape Voice Assistant).	
Gateway for X-channel	X-Channel	Router IP, if the x-channel is configured as a layer-3 routable link.	
Default router	Signaling	Default router for all Unify OpenScape Voice traffic not explicitly routed by static routes or source-based routing.	
Survival authority	Admin	Needs to be accessible from both nodes' admin network; has to be installed at a third location.	

Table 109 Cluster Addressing Scheme (Seite 1 von 2)

IP Address Function	Subnet	Remarks	Virtual? (see note)
NTP servers	Admin	Needs to be accessible from both nodes’ admin network.	
Note: May move if nodes share the same network.			

Table 109 Cluster Addressing Scheme (Seite 2 von 2)

D Demonstration Scenarios and Test Results

This chapter contains scripted scenarios and their expected consequences in the Unify OpenScape Voice solution.

D.1 Components Not Tested

Because of the fragility of the following components and the possible negative impact upon the hardware and system, the following components were not tested.

- Hard drives—disk failure tests were not attempted.
- Fans—fan failure tests were not attempted.

D.2 Power Redundancy Tests

Prerequisites for these tests are a collocated Unify OpenScape Voice cluster consisting of two server nodes.

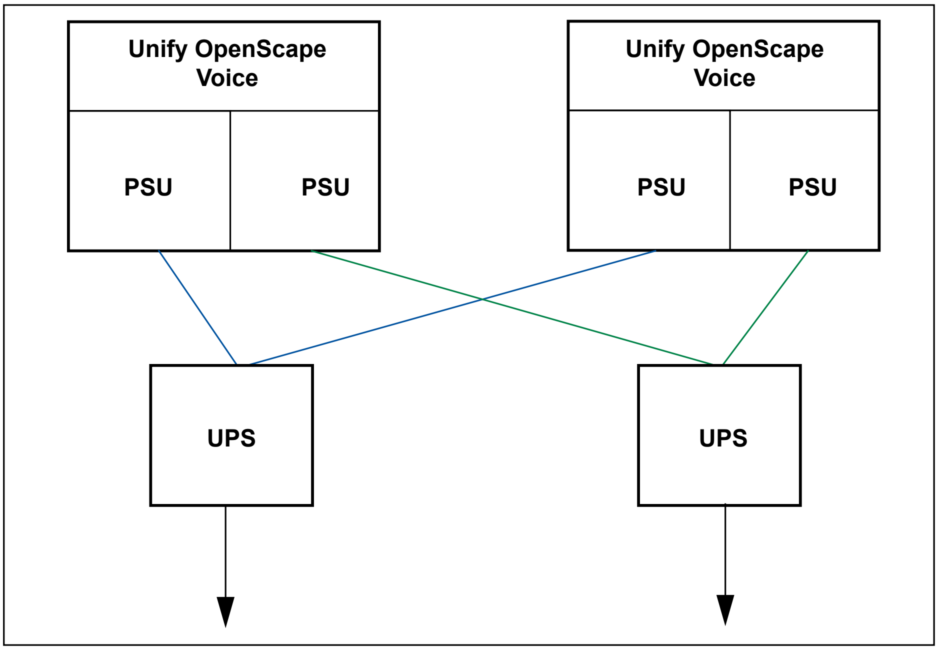


Figure 69 Power Redundancy Test Prerequisites

Table 110, "Power Redundancy Tests" describes the test and provides the results.

#	Test Description	Results
1.	Unplug PSU1 cable from Unify OpenScape Voice node 1	Cluster operates normally.
2.	Unplug PSU2 cable from Unify OpenScape Voice node 1	Cluster operates normally.
3.	Unplug PSU1 cable from Unify OpenScape Voice node 2	Cluster operates normally.
4.	Unplug PSU2 cable from Unify OpenScape Voice node 2	Cluster operates normally.
5.	Simulate power down of UPS1	Cluster operates normally.
6.	Simulate power down of UPS2	Cluster operates normally.

Table 110 Power Redundancy Tests

D.3 Interface Redundancy Tests

Prerequisites for these tests are a collocated Unify OpenScape Voice cluster consisting of two server nodes as shown in Figure 70.

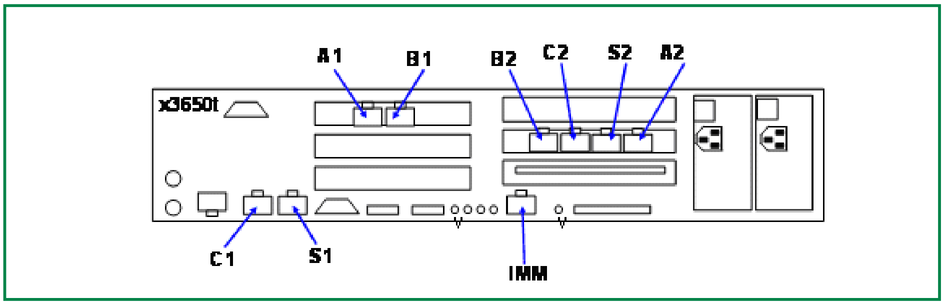


Figure 70 Platform Cable Assignments

With these cable assignments, the assignments shown in Figure 70 are valid for all servers.

Network	Ethernet # Primary Active	Ethernet # Secondary Bonded Inactive
Admin	A1	A2
Billing	B1	B2
Signaling	S1	S2
Cluster-Interconnect #1	C1	
Cluster-Interconnect #2	C2	

Table 111 Platform Cable Assignments

D.3.1 Ethernet Cable Redundancy Tests

Note that Unify OpenScape Voice sends an alarm for each failing Ethernet cable.

#	Test Description	Results
1.	Unplug A1 cable from Unify OpenScape Voice node 1	Linux bond driver activates A2. Admin network operates normal.
2.	Unplug A2 cable from Unify OpenScape Voice node 1	Linux bond driver activates A1. Signaling network operates normal.
3.	Unplug S1 cable from Unify OpenScape Voice node 1	Linux bond driver activates S2. Signaling network operates normal.
4.	Unplug S2 cable from Unify OpenScape Voice node 1	Linux bond driver activates S1. Signaling network operates normal.
5.	Unplug B1 cable from Unify OpenScape Voice node 1	Linux bond driver activates B2. Billing network operates normal.
6.	Unplug B2 cable from Unify OpenScape Voice node 1	Linux bond driver activates B1. Billing network operates normal.
7.	Unplug C1 cable from Unify OpenScape Voice node 1	Cluster operates normal on single interconnect.
8.	Unplug C2 cable from Unify OpenScape Voice node 1	Cluster operates normal on single interconnect.
9.	Unplug A1 cable from Unify OpenScape Voice node 2	Linux bond driver activates A2. Admin network operates normal.
10.	Unplug A2 cable from Unify OpenScape Voice node 2	Linux bond driver activates A1. Admin network operates normal.
11.	Unplug S1 cable from Unify OpenScape Voice node 2	Linux bond driver activates S2. Signaling network operates normal.
12.	Unplug S2 cable from Unify OpenScape Voice node 2	Linux bond driver activates S1. Signaling network operates normal.
13.	Unplug B1 cable from Unify OpenScape Voice node 2	Linux bond driver activates B2. Billing network operates normal.
14.	Unplug B2 cable from Unify OpenScape Voice node 2	Linux bond driver activates B1. Billing network operates normal.
15.	Unplug C1 cable from Unify OpenScape Voice node 2	Cluster operates normal on single interconnect.
16.	Unplug C2 cable from Unify OpenScape Voice node 2	Cluster operates normal on single interconnect.

Table 112 Ethernet Cable Redundancy Tests

D.3.2 Ethernet Card Failure Tests

Ethernet card failures are tested by removing all cables from a single card.

#	Test Description	Results
1.	Unplug A1 and B1 cables from Unify OpenScape Voice node 1.	Linux bond driver activates A2 and B2. Admin and Billing networks operate normally.
2.	Unplug C1 and S1 cables from Unify OpenScape Voice node 1.	Linux bond driver activates S2. Signaling network operates normal. Cluster operates normal on single interconnect
3.	Unplug A1, B2, C2, and S2 cables from Unify OpenScape Voice node 1.	Linux bond driver activates A1, B1, and S1. Admin, Billing, and Signaling networks operate normally. Cluster operates normal on single interconnect
4.	Unplug A1 and B1 cables from Unify OpenScape Voice node 2.	Linux bond driver activates A2 and B2. Admin and Billing networks operate normally.
5.	Unplug C1 and S1 cables from Unify OpenScape Voice node 2.	Linux bond driver activates S2. Signaling network operates normal. Cluster operates normal on single interconnect
6.	Unplug A1, B2, C2, and S2 cables from Unify OpenScape Voice node 2.	Linux bond driver activates A1, B1, and S1. Admin, Billing, and Signaling networks operate normally. Cluster operates normal on single interconnect

Table 113 Ethernet Card Failure Tests

D.4 Double Ethernet Card Failure Tests

Ethernet card failures are tested by removing all cables from a single card.

Lots of tests can be run on Ethernet cable or card failures. The result depends on which cards failed where. Table 114, "Double Ethernet Card Failure Tests Results" shows the results of each failure.

	(A1,B1) Node 1	(S1,C1) Node 1	(A2, B2, C2, S2) Node 1	(A1, B1) Node 2	(S1, C1) Node 2	(A2, B2, C2, S2) Node 2
(A1, B1) Node 1	■	1)	3)	1)	1)	1)
(S1, C1) Node 1	1)	■	2)	1)	1)	2)
(A2, B2, C2, S2) Node 1	3)	2)	■	1)	2)	1)
(A1, B1) Node 2	1)	1)	1)	■	1)	3)
(S1,C1) Node 2	1)	1)	2)	1)	■	2)
(A2, B2, C2, S2) Node 2	1)	2)	1)	3)	2)	■

With:

1) Ethernet failovers. Cluster operates normal. No loss of service.

2) Node 2 powers down, node 1 takes over. No loss of service.

3) Admin and Billing networks lost on this node.

Table 114 Double Ethernet Card Failure Tests Results

D.4.1 Single Router Failure Tests

Each location of the Unify OpenScape Voice cluster were equipped with a redundant router pair.

#	Test Description	Results
1.	Removed power from primary Router A.	Admin, billing and signaling network operate normal. Cluster operates normal.
2.	Removed power from primary Router B.	Admin, billing and signaling network operate normal. Cluster operates normal.

Table 115 Single Router Failure Tests

D.4.2 Node Failovers

For node failovers, the following simulations were done:

- **IMM inaccessible:** Pulled the respective cable. If pulled, an alarm might be generated (system runs check once every 10 minutes)
- **Unify OpenScape Voice Failed:** Unify OpenScape Voice was powered down from the front panel by pushing the reset pin.

- **Cluster-Interconnect down:** pulled both cluster-interconnect cables C1 and C2 on one of the nodes.

D.4.2.1 Without Survival Authority

Note: The survival authority is optional for a two-node cluster connected to the same IP network.

After each test, the clusters were restored, that is, the cables were plugged back in, the nodes were powered up, and so on.

If more than one action was required, the -1 or -2 in Table 116 shows the order in which the action was taken. Table 116 also shows the results of the actions.

#	Node 1		Cluster-Interconnect	Node 2		Result
	IMM	Unify OpenScape Voice		Unify OpenScape Voice	IMM	
1.	–	Powerdown	–		–	Node 2 takes over (30-45 sec)
2.	–	–	–	Powerdown	–	Node 1 takes over (10-25 sec)
3.	Pull-1	–	–		Pull-2	Cluster running normal
4.	Pull-1	–	Pull-2		–	Node 1 takes over (10-25 sec)
5.	–	–	Pull-2		Pull-1	Node 2 takes over (30-45 sec)
6.	Pull-1	–	–	Powerdown -2	–	Node 1 takes over (10-25 sec)
7.	–	Powerdown -2	–		Pull-1	Node 2 takes over (30-45 sec)

Table 116 Node Failovers without Survival Authority

D.4.2.2 With Survival Authority

With a survival authority installed, the following tests were run. Where indicated in Table 117, the survival mode flag was reset:

#	Node 1		Cluster-Interconnect	Node 2		Result
	IMM	Unify OpenScape Voice		Unify OpenScape Voice	IMM	
1.	–	Powerdown	–		–	Node 2 takes over (30-45 sec)
2.	–	–	–	Powerdown	–	Node 1 takes over (10-25 sec)
3.	Pull-1	–	–		Pull-2	Cluster running normal
4.	Pull-1	–	Pull-2		–	Node 1 takes over (10-25 sec)
5.	–	–	Pull-2		Pull-1	Node 2 takes over (60-75 sec)
6.	Pull-1	–	–	Powerdown -2	–	Node 1 takes over (10-25 sec)
7.	–	Powerdown -2	–		Pull-1	Node 2 takes over (60-75 sec)
8.	Pull-1	–	Pull-3	–	Pull-2	Node 1 takes over (25-45 sec); survival mode flag reset
9.	–	–	–	Powerdown -2	Pull-1	Node 1 takes over (25-45 sec). Test was also done by removing both power cables. Survival mode flag was reset
10.	Pull-1	Powerdown -2				Node 2 takes over (75-95 sec). Test was also done by removing both power cables. Survival mode flag was reset

Table 117 Node Failovers with Survival Authority

D.5 Collocated Cluster Deployment Model Tests: Single LAN Switch Failure

A requirement for these tests was that the cluster must be connected to *two* LAN switches. Table 118, "Single LAN Switch Failure Test Results" gives a description of the test along with the results.

#	Test Description	Results
1.	Removed power from primary LAN Switch A	Admin, billing, and signaling networks operate normally.
2.	Removed power from primary LAN Switch B	Admin, billing, and signaling networks operate normally.

Table 118 Single LAN Switch Failure Test Results

D.6 Geographic Node Separation

D.6.1 Single LAN Switch Failure Tests

A requirement for these tests was that the cluster must be connected to *two* LAN switches (total = 4 LAN switches). Table 119 gives a description of the test along with the results.

#	Test Description	Results
1.	Removed power from primary LAN Switch A in Location 1.	Admin, billing, and signaling networks operate normally. Cluster operates normally on a single interconnect.
2.	Removed power from secondary LAN Switch B in Location 1.	Admin, billing, and signaling networks operate normally. Cluster operates normally on a single interconnect.
3.	Removed power from primary LAN Switch A in Location 2.	Admin, billing, and signaling networks operate normally. Cluster operates normally on a single interconnect.
4.	Removed power from secondary LAN Switch B in Location 2.	Admin, billing, and signaling networks operate normally. Cluster operates normally on a single interconnect.

Table 119 Single LAN Switch Failure Test Results

D.6.2 Single Router Failure Tests

Each Unify OpenScape Voice cluster must be equipped with a redundant router pair. Table 120 gives a description of the test along with the results.

#	Test Description	Results
1.	Removed power from primary Router A in Location 1.	Admin, billing, and signaling networks operate normally. Cluster operates normally.
2.	Removed power from secondary Router B in Location 1.	Admin, billing, and signaling networks operate normally. Cluster operates normally.
3.	Removed power from primary Router A in Location 2.	Admin, billing, and signaling networks operate normally. Cluster operates normally.
4.	Removed power from secondary Router B in Location 2.	Admin, billing, and signaling networks operate normally. Cluster operates normally.

Table 120 Single Router Failure Test Results

D.6.3 Single L2 Bridge Failure Tests

A single Layer-2 (L2) bridge failure was tested by unplugging one of the WAN connections of the L2 bridge (see Table 121). When a hardware redundant L2 bridge was used, the layer-2 bridge was powered off instead.

#	Test Description	Results
1.	Unplugged first WAN connection from Layer-2 bridge	Admin, billing, and signaling networks operate normally. Cluster operates normal on single interconnect.
2.	Unplugged second WAN connection from Layer-2 bridge	Admin, billing, and signaling networks operate normally. Cluster operates normal on single interconnect.

Table 121 Single L2 Bridge Failure Tests

D.6.4 Double Failure Tests—Single Failure in Unify OpenScape Voice Cluster Location

Each of the tests assumed that the IMM card was connected to LAN switch A. The legend below the table explain the numbers in each cell.

	LAN A LOCATION 1	LAN B LOCATION 1	L2-Bridge A LOCATION 1	L2-Bridge B LOCATION 1	Router A LOCATION 1	Router B LOCATION 1
LAN A LOCATION 2	1)	4)	1)	4)	2)	2)
LAN B LOCATION 2	3)	1)	3)	1)	2)	2)
L2-Bridge A LOCATION 2	1)	4)	1)	6)	2)	2)
L2-Bridge B LOCATION 2	3)	1)	5)	1)	2)	2)
Router A LOCATION 2	2)	2)	2)	2)	2)	2)
Router B LOCATION 2	2)	2)	2)	2)	2)	2)

With:

1) Admin, billing, and signaling network operate normal. Cluster operates normal on single interconnect.

2) Admin, billing, and signaling network operate normal. Cluster operates normal.

3) Node 2 powers down, node 1 takes over. No loss of service.

4) Node 1 powers down, node 2 takes over. No loss of service.

5) Node 2 powers down, node 1 takes over. Manual rerouting in the network is necessary in case of same VLANs. No loss of service in other cases.

6) Node 1 powers down, node 2 takes over. Manual rerouting in the network is necessary in case of same VLANs. No loss of service in other cases.

Table 122 Double Ethernet Card Failure Tests Results

D.6.5 Double Failure Tests—Within the Same Unify OpenScape Voice Cluster Location

Location 1 results are shown in Table 123.

	LAN A LOCATION 1	LAN B LOCATION 1	L2-Bridge A LOCATION 1
LAN A LOCATION 1	1)	3)	3)
L2-Bridge A LOCATION 1	3)	1)	3)
Router A LOCATION 1	3)	3)	2)

With:

Table 123 Double Failure Tests for Location 1 (Seite 1 von 2)

1)Node 2 powers down, node 1 takes over. Manual rerouting in the network is necessary in case of same VLANs. No loss of service in other cases.

2) Cluster operates normal except in different subnets' case, where all devices must contact the primary service's address on node 2.

3) Admin, billing, and signaling network operate normal. Cluster operates normal.

Table 123 Double Failure Tests for Location 1 (Seite 2 von 2)

Location 2 results are shown in Table 124. The legend below the table explain the numbers in each cell.

	LAN A LOCATION 2	LAN B LOCATION 2	L2-Bridge A LOCATION 2
LAN A LOCATION 2	1)	3)	3)
L2-Bridge A LOCATION 2	3)	1)	3)
Router A LOCATION 2	3)	3)	2)

With:

1)Node 1 powers down, node 2 takes over. Manual rerouting in the network is necessary in case of same VLANs. No loss of service in other cases.

2) Cluster operates normal except in different subnets' case, where all devices must contact the primary service's address on node 1.

3) Admin, billing, and signaling network operate normal. Cluster operates normal.

Table 124 Double Failure Tests for Location 1

E SIP Overview

E.1 Definition and Background

Session Initiation Protocol (SIP) is a signaling protocol used to initiate, manage and terminate sessions in an IP network. A session may be a two-way telephone call or it could be a multimedia conference session.

The Internet Engineering Task Force (IETF) introduced SIP for services related to Voice over IP (VoIP), and its popularity has steadily grown. It can be used with voice, data, or even video sessions. The noteworthy feature of SIP is that it is used to set up and control sessions, and is not involved with the data exchange within a session. The audio or video media is handled by other protocols, for example, Real-Time Transport Protocol (RTP).

Initially, private branch exchange and central office switch-based telephony system were the main instruments for transmitting voice; however, the Internet has changed that. As Internet Protocol (IP) bandwidth increased, methods were sought that would enable customers to use some of the bandwidth for voice as well as data. The ability to combine voice and data over the same physical medium offered the promised to reduced the operating and plant cost. Several solutions for combining voice and data were put forward, but the solution presented by IETF was finally accepted as the standard. The development of SIP evolved over several years.

Initial Internet drafts were presented in 1996 with improvements occurring over several years. In 1999, SIP published Request for Comment (RFC) 2543 as a standard. Later it was modified and a more up-to-date version was published as RFC 3261. That document should be consulted for specific details of the SIP standard, as this appendix is rather introductory and high-level in nature.

E.2 Protocol Terminology

It is helpful to clarify the various terms used when discussing the SIP protocol:

- **Messages** are the individual text exchanges that occur between a server and a client. There can be two basic types of messages: requests and responses.
- A **transaction** occurs between a client and a server and made up of all the messages from the first request sent by the client to the server up to and including the final response sent from the server

to the client. If the request is an INVITE and the final response is a non-2xx, the transaction also includes an ACK to the response. The ACK for a 2xx response to an INVITE request is a separate transaction.

- **Dialog** is a peer-to-peer SIP relationship between two user agents that persists for some time. A dialog is identified by a Call-ID, a local tag, and a remote tag.
- The **call** of a called party comprises of all the dialogs in which it is involved. It may be thought of as a session.

A caller may have connections to a number of called parties at a time forming a number of dialogs. All these dialogs make a single call.

E.3 Functions

The scope of SIP is confined to the setup, modification, and termination of sessions. Its purposes can be summarized as follows:

- It allows for the establishment of a user location.
- It provides a method to allow feature negotiation so that all of the participants in a session can agree on the features to be supported among them.
- It can effectively exercise call management - for example adding, terminating, or transferring participants.
- It allows for changing features of a session while it is in progress.

Other functions are done with other protocols. SIP:

- Does not describe sessions. This is handled by the Session Description Protocol.
- Does not control conferences.
- Does not act as a resource reservation protocol.
- Does not provide Quality of Service (QoS)
- Can work other protocols to ensure these functions are carried out.
- Can and does function with SOAP, HTTP, XML, VXML, WSDL, UDDI, SDP and others.

E.4 Components

In a typical SIP scenario, the devices interacting are called User Agents (UA).

User Agents may operate as a:

- User Agent Client (UAC), which initiates requests and send those to servers.
- User Agent Server (UAS), which receives requests, processes them, and generates responses.

Note: A single User Agent may handle both functions.

Clients: Typically, the idea of clients are associated to the end users which may be applications running on the systems used by people. The applications may be a softclient running on a personal computer (PC). Or it may be a telephone running a SIP application. In any case, this phone or application generates a request when you try to call another person over the network and sends the request to a server—generally a proxy server.

Servers: Servers are part of the network and they are set up to handle the requests sent by clients. These servers may be one of the following types:

- **Proxy server**: These are the most common type of server in a SIP environment. When a request is generated, the exact address of the recipient is not known in advance. So the client sends the request to a proxy server. The server, on behalf of the client, forwards the request to another proxy server or the recipient itself.
- **Redirect server**: A redirect server redirects or sends the request back to the client indicating that the client has to try a different route to get to the recipient. This happens when a recipient has moved from its original position either temporarily or permanently.
- **Registrar**: One of the key jobs of the servers is to determine the location of an user in a network. Users *must* register their locations to a registrar. The users *must* periodically refresh their locations by registering, that is, by sending a special type of message to a registrar server.
- **Location server**: The addresses that users send to a registrar are stored in a location server.

E.5 Request Methods

SIP requests are the codes used by SIP for communication and are complemented by SIP responses, which generally indicate whether the request succeeded or failed; and if it failed, why it failed. The various components in a SIP network *must* send or receive command for the system to operate smoothly. The seven commands are listed in Table 125.

SIP Request Method	Function
INVITE	Indicates a client is being invited to participate in a call session.
ACK	Confirms that the client has received a final response to an INVITE request.
CANCEL	Cancels any pending searches but does not terminate a call that has already been accepted. It is used if a client sends an INVITE and then changes its decision to call the recipient.
BYE	Terminates a call and can be sent by either the caller or the called party.
REGISTER	Registers the address listed in the `To` header field with a SIP server. Basically, it registers a user’s current location.
INFO	Used for mid-session signaling.
OPTIONS	Queries the capabilities of servers.

Table 125 SIP Request Methods and Their Functions

Each of these SIP request methods are described next.

E.6 Session Example

To gain a better understanding of SIP, a typical example is presented in Figure 71, "Typical SIP Call".

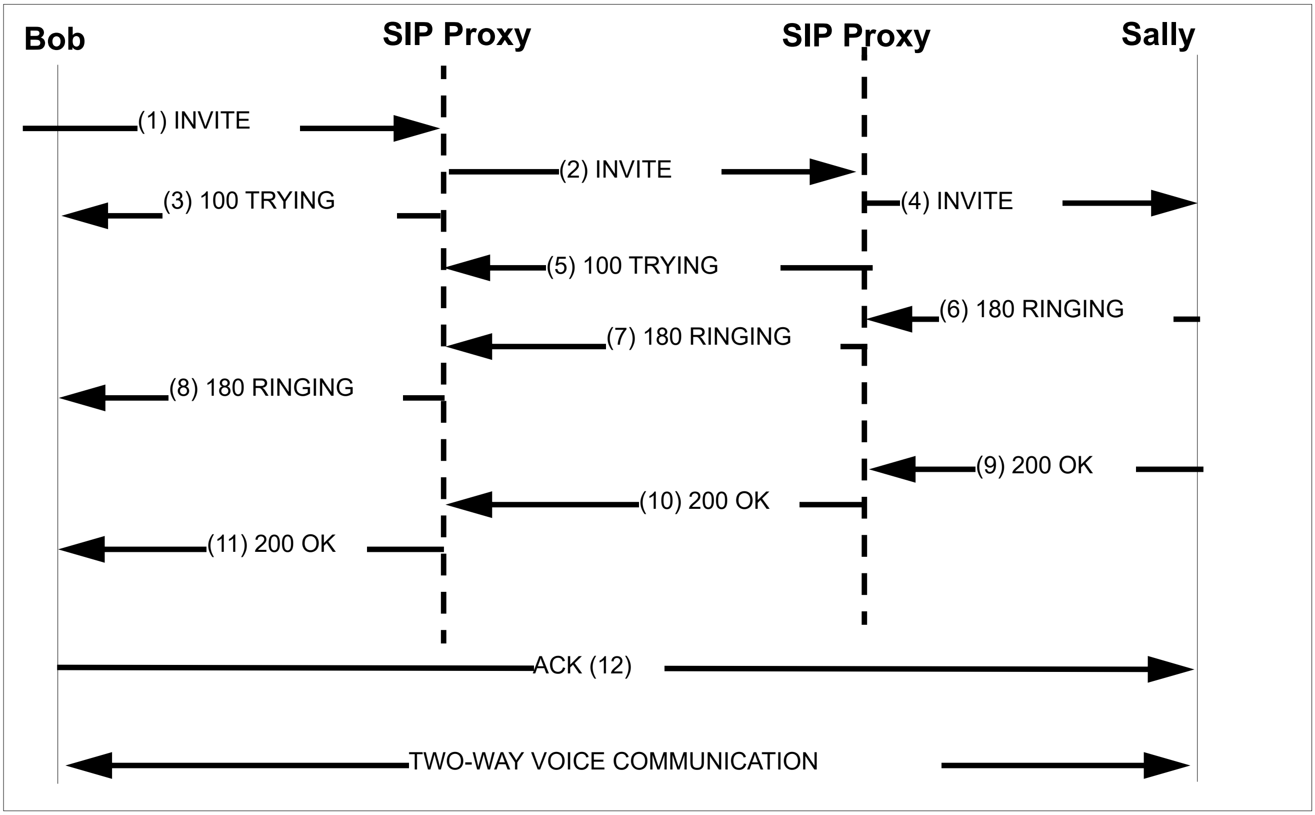


Figure 71 Typical SIP Call

Before understanding the methods, first you should understand the pictorial diagram. Bob uses his SIP phone to reach the SIP phone of Sally. Proxy 1 and Proxy 2 help set up the session on behalf of the users. The messages appear vertically in the sequence they occur—that is, the message on top (INVITE 1) comes first, followed by others. The direction of arrows shows the sender and recipient of each message. Each message contains a 3-digit number followed by a name. The 3-digit number is the numerical code of the associated message that is understood by the machines.

The transaction starts with Bob making an INVITE request for Sally. But Bob doesn't know the exact location of Sally in the IP network. So Bob’s machine passes the request to SIP Proxy 1. On behalf of Bob, SIP Proxy 1 forwards an INVITE request for Sally to SIP Proxy 2. SIP Proxy 1 sends a TRYING response to Bob indicating that it is trying to reach Sally.

Upon receiving INVITE 2 from SIP Proxy 1, SIP Proxy 2 works in a similar fashion as SIP Proxy 1. It forwards an INVITE request to Sally. It should be noted that SIP Proxy 2 knows the location of Sally. If it didn't know the location, it would have forwarded it to another proxy server. So an INVITE request may travel through several proxies before reaching the endpoint or recipient. After forwarding INVITE 3, SIP Proxy 2 issues a TRYING response to SIP Proxy 1.

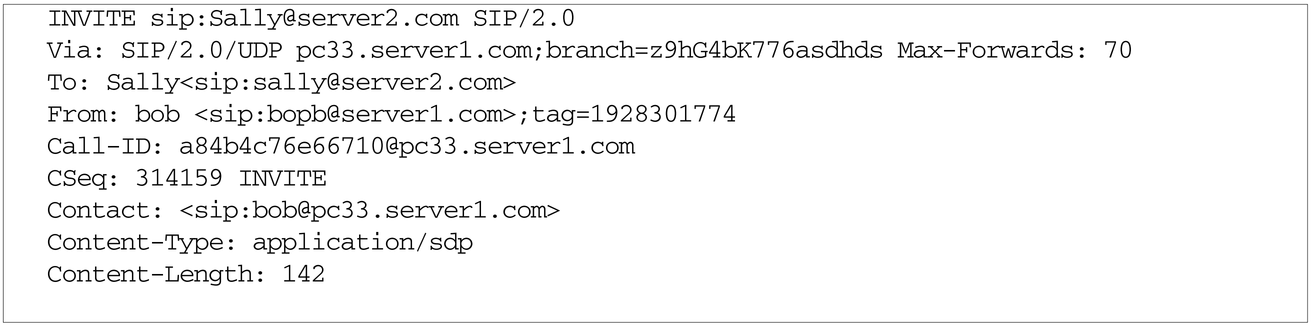
The SIP phone, upon receiving the INVITE request, starts ringing Sally, indicating that a call request has come. Sally's SIP phone sends a RINGING response back to SIP Proxy 2 which reaches Bob through SIP Proxy 1. So Bob gets a feedback that Sally has received the INVITE request.

Sally can accept or decline the call. In this case, Sally decides to accept it. As soon as she accepts the call, a 200 OK response is sent by the Sally's phone to SIP Proxy 2. This response eventually reaches Bob's phone. Bob's phone sends an ACK message to confirm the setup of the call. The media exchange takes place between Bob's phone and Sally's. The proxy servers are not involved in the media exchange. Media flow is controlled using protocols different from SIP, for example, RTP

When one party in the session decides to disconnect, it sends a BYE message to the other party. The other party sends a 200 OK message to confirm the termination of the session. Now that an example has been shown, the request message format will be discussed.

E.7 Request Message Format

Requests are sent by clients to servers. The contents of the request message is discussed below. Figure 72 shows the format of INVITE request as sent by Bob.



```
INVITE sip:Sally@server2.com SIP/2.0
Via: SIP/2.0/UDP pc33.server1.com;branch=z9hG4bK776asdhds Max-Forwards: 70
To: Sally<sip:sally@server2.com>
From: bob <sip:bopb@server1.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.server1.com
CSeq: 314159 INVITE
Contact: <sip:bob@pc33.server1.com>
Content-Type: application/sdp
Content-Length: 142
```

Figure 72 Bob's INVITE Request

The first line of the text-encoded message is called Request-Line. It identifies that the message is a request.

Request-Line

Method SP Request-URI SP SIP-Version CRLF (SP = single-space & CRLF= Carriage Return + Line Feed)

Here the method is INVITE, request-uri is “bob@server2.com” and SIP version is 2.

The following lines are a set of header fields.

Via: It contains the local address of bob, that is, pc33.server1.com where it is expecting the responses to come.

Max-Forward: It is used to limit the number of hops that this request may take before reaching the recipient. It is decreased by one at each hop. It is necessary to prevent the request from traveling forever in a loop.

To: It contains a display name “Sally” and a SIP or SIPS URI <sally@server2.com>

From: It also contains a display name “bob” and a SIP or SIPS URI <bob@server1.com>. It also contains a tag which is a pseudo-random sequence inserted by the SIP application. It works as an identifier of the caller in the dialog.

Call-ID: It is a globally unique identifier of the call generated as the combination of a pseudo-random string and the SIP phone’s IP address.

The Call-ID is unique for a call. A call may contain several dialogs. Each dialog is uniquely identified by a combination of **From**, **To** and **Call-ID**.

CSeq: Contains an integer and a method name. When a transaction starts, the first message is given a random **CSeq**. After that it is incremented by one with each new message. It is used to detect non-delivery of a message or out-of-order delivery of messages.

Contact: It contains a SIP or SIPS URI that is a direct route to Bob. It contains a username and a fully qualified domain name (FQDN). It may also have an IP address.

Via: It is used to send the response to the request. Contact field is used to send future requests. That is why the 200 OK response from Sally goes to Bob through proxies. But when Sally generates a BYE request (a new request and not a response to INVITE), it goes directly to Bob bypassing the proxies.

Content-Type: It contains a description of the message body.

Content-Length: It is an octet (byte) count of the message body.

The header may contain other header fields also. However, those fields are optional. Note that the body of the message is not shown here. The body is used to convey information about the media session written in Session Description Protocol (SDP).

E.7.1 INVITE

A SIP INVITE request indicates that a user or service wishes to participate in a session.

Called UA Begins Alerting & Returns “180 Ringing” Response to Calling UA

Accepts Call with Similar Session Description

E.7.2 ACK

ACK is used to acknowledge the reception of a final response to an INVITE. Client originating INVITE request issues ACK after receiving response. In essence, this is a “three-way handshake”

INVITE from calling UA

Final response from called UA

ACK from calling UA

E.7.3 CANCEL

CANCEL is used to cancel pending transactions:

If the Calling UA hangs up after called UA begins ringing, but does not answer.

The Calling UA Sends CANCEL.

When the Called UA receives CANCEL, it stops ringing and sends a “200 OK” response, and then sends a “487 Transaction Canceled” response

Calling UA finishes “three-way handshake” by sending ACK

E.7.4 BYE

BYE is used to end sessions:

For two-party call, first UA to hang up sends BYE

Second UA sees BYE and sends “200 OK” response

For Multicast

BYE may be optionally sent when one party leaves

Session not affected

For more than eight (8) participants BYE usually not sent to reduce traffic

E.7.5 REGISTER

REGISTER is used to inform a server (the *registrar*) about its current location and also contains times when registration is valid. The Registrar supports user registered even at several locations. Servers then search until user is located.

E.7.6 OPTIONS

OPTIONS is used to query a server about its capabilities. The method to be used, Session Description Protocols (SDP). Replies are with a 200 OK response.

Now that SIP requests have been discussed, a discussion of the SIP response message is in order.

E.8 Response Message Format

Figure 73 shows the SIP response of Sally.

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP site4.server2.com;branch=z9hG4bKnashds8;received=192.0.2.3
Via: SIP/2.0/UDP site3.server1.com;branch=z9hG4bK77ef4c2312983.1;re-
ceived=192.0.2.2
Via: SIP/2.0/UDP pc33.server1.com;branch=z9hG4bK776asdhds;received=192.0.2.1
To: sally <sip:sally@server2.com>;tag=a6c85cf
From: bob <sip:bob@server1.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.server1.com
CSeq: 314159 INVITE
Contact: <sip:sally@192.0.2.4>
Content-Type: application/sdp
Content-Length: 131
```

Figure 73 Sally's Response Message

Status Line

The first line in a response is called Status line.

SIP-Version SP Status-Code SP Reason-Phrase CRLF

[SP = single-space & CRLF = Carriage Return + Line Feed].

Here SIP version is 2, Status-Code is 200 with a reason phrase indicating a status of OK.

The header fields that follow the status line are similar to those in a request. The differences are discussed here.

Via: There is more than one Via field. It is because each element through which the INVITE request has passed has added its identity in the Via field. Three Via fields are added by SIP phone of Bob, Proxy Server 1, the first proxy, and Proxy Server 2, the second proxy. The response retraces the path of INVITE using the Via fields. On its way back, each element removes the corresponding Via field before forwarding it back to the caller.

To: Note that the To field now contains a tag. This tag is used to represent the called party, in this case Sally, in a dialog.

Contact: It contains the exact address of Sally. So Bob doesn't need to use the proxy servers to find Sally in the future.

Note that this is a 2xx response. However, responses can be different depending on particular situations. More about this later.

E.9 Response Types

The first digit of a Status-Code defines the category of response. For example, any response between 100 and 199 is categorized as a 1xx (informational) response. As listed in Table 126, SIP/2.0 allows six types of responses.

General Code	Code Range	Response Class	Comment
1xx	100-199	Informational	Request received, continuing to process the request
2xx	200-299	Success	The action was successfully received, recognized, and accepted
3xx	300-399	Redirection	Further action is required to complete the request
4xx	400-499	Client Error	The request contains syntax or other errors preventing it from being fulfilled at this server
5xx	500-599	Server Error	The server failed to fulfill an apparently valid request
6xx	600-699	Global Failure	This request cannot be fulfilled at any server

Table 126 SIP Response Code Categories

E.9.1 Informational Responses

The 1xx responses (Table 127) provide information concerning the INVITE messages.

Response Code	Response	Comment
100	Trying	The 100 (Trying) response indicates that the INVITE has been received and that the proxy is working on behalf of the user agent to route the INVITE to the destination.
180	Ringing or alerting	The UA receiving the INVITE is trying to alert the user. This response *may* be used to initiate local ringback.
181	Call is being Forwarded	A server *may* use this status code to indicate that the call is being forwarded to a different set of destinations.
182	Queued	The called party is temporarily unavailable, but the server has decided to queue the call rather than reject it. When the called party becomes available, it will return the appropriate final status response. The reason phrase *may* give further details about the status of the call, for example, “3 calls queued; expected waiting time is 12 minutes”. The server *may* also issue several 182 (Queued) responses to update the caller about the status of the queued call.
183	Session Progress	The 183 (Session Progress) response is used to convey information about the progress of the call that is not otherwise classified. The Reason-Phrase, header fields, or message body MAY be used to convey more details about the call progress.

Table 127 SIP Informational (1xx) Responses

E.9.2 Success Responses

The 2xx responses (Table 128) provide information indicating that the request was successful and may give additional information.

Response Code	Response	Comment
200	OK	The request was successful.
202	Accepted	The request has succeeded. The information returned with the response depends on the method used in the request.

Table 128 SIP Success (2xx) Responses

E.9.3 Redirection Responses

The 3xx responses (Table 129) give information about the user's new location, or about alternative services that might be able to satisfy the call.

Respons e Code	Response	Comment
300	Multiple Choices	The address in the request resolved to several choices, each with its own specific location, and the user (or UA) can select a preferred communication end point and redirect its request to that location.
301	Moved Permanentl y	The user can no longer be found at the address in the Request-URI, and the requesting client SHOULD retry at the new address given by the Contact header field (Section 20.10). The requestor SHOULD update any local directories, address books, and user location caches with this new value and redirect future requests to the address(es) listed.
302	Moved Temporarily	The requesting client *should* retry the request at the new address(es) given by the Contact header field (Section 20.10). The Request-URI of the new request uses the value of the Contact header field in the response. The duration of the validity of the Contact URI can be indicated through an Expires (Section 20.19) header field or an expires parameter in the Contact header field. Both proxies and UAs MAY cache this URI for the duration of the expiration time. If there is no explicit expiration time, the address is only valid once for repeating, and *must not* be cached for future transactions. If the URI cached from the Contact header field fails, the Request- URI from the redirected request MAY be tried again a single time. The temporary URI may have become out-of-date sooner than the expiration time, and a new temporary URI may be available.
305	Use Proxy	The requested resource *must* be accessed through the proxy given by the Contact field. The Contact field gives the URI of the proxy. The recipient is expected to repeat this single request via the proxy. **305** (Use Proxy) responses *must* only be generated by User Agent Servers.
380	Alternative Service	The call was not successful, but alternative services are possible. The alternative services are described in the message body of the response. Formats for such bodies are not defined here, and may be the subject of future standardization.

Table 129 SIP Redirection (3xx) Responses

E.9.4 Client Error Responses

The 4xx responses (Table 130, "SIP Client Error (4xx) Responses") are definite failure responses from a particular server. The client *SHOULD not* retry the same request without modification (for example, adding appropriate authorization). However, the same request to a different server might be successful.

Note: Table 130 is *not* a comprehensive list of client error responses.

Response Code	Response	Comment
400	Bad Request	The request could not be understood due to malformed syntax. The Reason-Phrase *should* identify the syntax problem in more detail, for example, “Missing Call-ID header field”.
401	Unauthorized	The request requires user authentication. This response is issued by User Agent Servers and registrars, while 407 (Proxy Authentication Required) is used by proxy servers.
402	Payment Required	Reserved for future use.
403	Forbidden	The server understood the request, but is refusing to fulfill it. Authorization will not help, and the request *should not* be repeated.
404	Not Found	The server has definitive information that the user does not exist at the domain specified in the **Request-URI**. This status is also returned if the domain in the **Request-URI** does not match any of the domains handled by the recipient of the request.
482	Loop Detected	The server has detected a loop
484	Address Incomplete	The server received a request with a Request-URI that was incomplete. Additional information *should* be provided in the reason phrase. This status code allows overlapped dialing. With overlapped dialing, the client does not know the length of the dialing string. It sends strings of increasing lengths, prompting the user for more input, until it no longer receives a 484 (Address Incomplete) status response.

Table 130 SIP Client Error (4xx) Responses(Seite 1 von 2)

Respons e Code	**Response**	**Comment**
486	Busy Here	The called party's end system was contacted successfully, but the called party is currently not willing or able to take additional calls at this end system. The response *may* indicate a better time to call in the **Retry-After** header field. The user could also be available elsewhere, such as through a voice mail service. Status **600** (Busy Everywhere) *should* be used if the client knows that no other end system will be able to accept this call.

Table 130 SIP Client Error (4xx) Responses(Seite 2 von 2)

E.9.5 Server Error Responses

The 5xx responses (Table 131, "SIP Server Error (5xx) Responses") are failure responses given when a server itself has erred.

Respons e Code	**Response**	**Comment**
500	Internal Severe Error	The server encountered an unexpected condition that prevented it from fulfilling the request. The client *may* display the specific error condition and *may* retry the request after several seconds. If the condition is temporary, the server *may* indicate when the client may retry the request using the **Retry-After** header field.
501	Not Implemented	The server does not support the functionality required to fulfill the request. This is the appropriate response when a UAS does not recognize the request method and is not capable of supporting it for any user. (Proxies forward all requests regardless of method.) **Note** that a **405** (Method Not Allowed) is sent when the server recognizes the request method, but that method is not allowed or supported.
502	Bad Gateway	The server, while acting as a gateway or proxy, received an invalid response from the downstream server it accessed in attempting to fulfill the request.

Table 131 SIP Server Error (5xx) Responses

Respons e Code	Response	Comment
503	Service Unavailable	The server is temporarily unable to process the request due to a temporary overloading or maintenance of the server. The server *may* indicate when the client should retry the request in a **Retry-After** header field. If no **Retry-After** is given, the client *must* act as if it had received a **500** (Server Internal Error) response. A client (proxy or UAC) receiving a **503** (Service Unavailable) *should* attempt to forward the request to an alternate server. It *should not* forward any other requests to that server for the duration specified in the **Retry-After** header field, if present. Servers *may* refuse the connection or drop the request instead of responding with **503** (Service Unavailable).
504	Gateway Timeout	The server did not receive a timely response from an external server it accessed in attempting to process the request. The **408** (Request Timeout) should be used instead if there was no response within the period specified in the **Expires** header field from the upstream server.
505	SIP Version Not Supported	The server does not support, or refuses to support, the SIP protocol version that was used in the request. The server is indicating that it is unable or unwilling to complete the request using the same major version as the client, other than with this error message.
513	Message too Large	The server was unable to process the request since the message length exceeded its capabilities.

Table 131 SIP Server Error (5xx) Responses

E.9.6 Global Failure Responses

The 6xx responses (Table 132) indicate that a server has definitive information about a particular user, not just the particular instance indicated in the Request-URI.

Respons e Code	Response	Comment
600	Busy Everywher e	The called party's end system was contacted successfully but the called party is busy and does not wish to take the call at this time. The response *may* indicate a better time to call in the **Retry-After** header field. If the called party does not wish to reveal the reason for declining the call, the called party uses status code **603** (Decline) instead. This status response is returned only if the client knows that no other end point (such as a voice mail system) will answer the request. Otherwise, **486** (Busy Here) should be returned.
603	Decline	The called party's machine was successfully contacted but the user explicitly does not wish to or cannot participate. The response *may* indicate a better time to call in the **Retry-After** header field. This status response is returned only if the client knows that no other end point will answer the request.
604	Does Not Exist Anywhere	The server has authoritative information that the user indicated in the **Request-URI** does not exist anywhere.
606	Not Acceptable	The user's agent was contacted successfully but some aspects of the session description such as the requested media, bandwidth, or addressing style were not acceptable.

Table 132 SIP Global Failure (6xx) Responses

Please note that the difference between a proxy server and a registration or a location server is often only logical. Physically they may be situated on the same machine.

E.10 Registration

Initially in a SIP session, the caller does not know the address of the called party. Obtaining this address is one of the roles of the proxy servers. The proxy server has the task of finding out the exact location of the recipient.

The proxy server is able to determine the location of the recipients because initially each user registers (reports) its current location to a registrar server. The application sends a REGISTER message informing the server of its present location. The registrar stores this information, called a binding (between the user and its present address), in a location server which is used by other proxies to locate the user.

If User A uses the IP 177.33.25.141 as its current location and registers it with the server. For example, if you log on from a different computer using your username, the application registers the username with the IP address of that computer. The Expire field reflects the duration for which this registration will be valid. So User A has to refresh its registration from time to time.

There is a functional difference between a proxy, registration, or a location server but it may only logical. Each of these functions may be on the same machine.

List of Abbreviations

Abbreviation	Definition
ACD	automatic call distribution
ALI	automatic location identification
AoR	Address of Record
AP	access point
API	application programming interface
ATC	attendant console
B-channel	bearer channel
BE	back end
BG	business group
BGL	business group line = subsciber
BHCA	busy hour call attempts
BRI	basic rate interface
CAC	call admission control
CAMA	centralized automatic message accounting
CAP	common application platform
CAS	centralized attendant service
CBN	Call Back Number
CCBS	completion of calls to busy subscriber
CCNR	completion of calls on no reply
CCS	centum call seconds
CDR	call detail recording
CLA	Customer License Agent
CLC	Customer License Client
CLI	command line interface
CLM	Customer License Manager
CLS	Customer Licensing Server
CO	central office
CorNet	Corporate Network
COS	class of service
CPN	calling party number
CS	communication servers

CSTA	computer-supported telecommunications applications
D-channel	data channel
DHCP	dynamic host configuration protocol
DID	direct inward dialing
DLS	deployment service
DN	directory number
DNS	domain name system
DSP	digital signal processor
DTMF	dual-tone multifrequency
DTS	direct trunk select
ELIN	Emergency Location Identifier Number
ERL	echo return loss
FE	front end
FQDN	fully-qualified domain name
FTP	file transfer protocol
GUI	graphical user interface
HLM	HiPath License Management
HSRP	hot standby routing protocol
ICMP	Internet control message protocol
IM	International Market
IP	Internet protocol
IPMI	Intelligent Platform Management Interface
IPsec	Internet protocol security
ISDN	integrated services digital network
IS-IS	Intermediate System - Intermediate System protocol
ISO	International Standards Organization
IVR	interactive voice response
L2	layer-2
L2TP	layer-2 tunneling protocol
LAN	local area network
LD	Location Domain
LDAP	lightweight directory access protocol
LIN	location identification number
MAC	moves, adds, and changes; *also* media access control
MGCP	media gateway control protocol; IETF standard RFC 2705
MHLG	multiline hunt group

MIB	management information block
MOS	mean opinion score
MS	media server
MTBF	mean time between failures
NANP	North American numbering plan
NAPT	network address port translation
NAT	network address translation
NB/BB	narrowband/broadband
NOA	nature of address
NOC	Network Operations Center
NPI	numbering plan identifier
NSC	National Support Center
NSG	Network Systems Group
OAM&P	operation, administration, maintenance, and provisioning
OSPF	Open Shortest Path First
PAT	Port Address Translation
PBX	private branch exchange
PCM	pulse code modulation
PNP	private numbering plan
PRI	primary rate interface
PSAP	public safety answering point
PSTN	public switched telephone network
PT	Port
QoS	quality of service
QSIG	signaling at the Q-reference point
RA	routing area
RTP	real-time transport protocol
SBC	session border controller
SIP	session initiation protocol
SM	signaling manager
SMG	survivable media gateway
SMR	system maintenance release
SOAP	simple object access protocol
SNMP	simple network management protocol
TA	terminal adapter
TCP	transmission control protocol

TDM	time-division multiplexing
TEHO	tail-end hop-off
TON	type of number
TTUD	*an abbreviation for the combination of these protocols in the following order:* TLS, TCP, UDP
UCE	universal call engine
UM	User Management
UMS	unified messaging system
VM	voice mail
VoIP	voice over IP
VRRP	Virtual Router Redundancy Protocol
WAN	wide area network
XML	extended markup language

Index