A MITEL
PRODUCT
GUIDE

Unify OpenScape Voice

OpenScape Voice V10

Feature Description

07/2024

A31003-H80A0-F100-16-7618

Mitel

Notices

Trademarks

Contents

1 OpenScape Voice System Overview

OpenScape Voice is a native SIP real-time IP system designed to provide enterprises with a robust service creation and delivery infrastructure. Scalable to as many as 100,000 users per two active redundant servers, and a virtually unlimited number of users in a large network, OpenScape Voice can be deployed and managed as a world-class, lowest power consuming data center solution. Not only does it provide enterprise class communications functionality; it also reduces the associated CO2 footprint of the enterprise.

OpenScape Voice creates technology choices that allow customers to implement communication strategies at their own pace (e.g. voice and video communications). It is designed to provide architectural strength to such a framework through its scalability, resiliency, adherence to open standards, manageability and its ability to function powerfully as an IT / Data Center based communications solution.

1.1 OpenScape Voice Administration and Configuration – About this Documentation

The documentation at hand describes the administration, configuration, functionality and usage of the OpenScape Voice system. A number of elements in the user interface are user- and application-specific and therefore only visible if the appropriate application is installed.

Prerequisites for the Target User (Administrator)

Adequate administrator access rights are required to perform administrative tasks within the OpenScape Voice system. Please refer to the corresponding sections about user profiles and access rights for more information.

Target Audience for this Documentation

This documentation addresses administrators who configure and manage a communications network with OpenScape products. For making full use of the information provided in this documentation we assume the following knowledge:

- Knowledge of the general working method of communications systems.
- Knowledge of terms used in the environment of communications systems.
- Practical knowledge of how to configure and manage communications systems.

Practical Hints on Working with the User Interface

- **Mandatory fields** are highlighted in **bold** type in the user interface of the OpenScape Voice Assistant.
- Unless explicitly specified otherwise, only valid ASCII characters (a-z, A-Z, 0-9, and underscores) must be used when entering names and other attributes of OpenScape Voice-managed entities. Do **not** use special characters or spaces.
- A powerful, configurable **Search and Filtering** functionality provides for quick, focused search and retrieval of specific information. For details, please refer to the *Search and Filter Functionality* section.

- **Office Codes** can be longer than 9 digits (up to 14 digits).
- The **Destination Code Table** can be provisioned with a range of codes.
- The **Code Restriction Service** accepts the wildcard "*".

Support of IPv6 in OpenScape Voice Environments

OpenScape Voice supports IPv6 on the SIP client interface. IPV6 networks in mixed configurations (IPV4 parts and IPV6 parts) are supported by the OpenScape Voice Assistant. The OpenScape Voice Assistant itself is deploying IPV4 presently. The OpenScape Voice Assistant is able to administer IPV6 addresses (128 bits) in the OpenScape Voice switch and DLS (DlsAPI).

1.2 OpenScape Voice System Components

OpenScape Voice is a carrier-class softswitch that is scalable from 300 to 100,000 users per system. When networked, the number of subscribers is virtually limitless. The system runs on highly reliable, fault-tolerant servers using SuSE Linux Enterprise Server Operating System. The core protocol of OpenScape Voice is IETF Session Initiation Protocol (SIP).

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

Hardware for OpenScape Voice

The following servers can be used as computing nodes for V10 OpenScape Voice:

- Lenovo SR-530 for new deployments
- Lenovo x3550 M5 for existing deployments
- Fujitsu RX200 S7 for existing deployments

Software for OpenScape Voice

Among other functions, this software controls call processing, signaling, and cluster operation in redundant systems.

Tools for System Administration and Provisioning

- **Graphical User Interface** for **Common Management Platform** and integrated applications, including:
  - **OpenScape Voice Assistant**
  - **OpenScape Voice Media Server**
  - **OpenScape UC Application**
  - **OpenScape SBC**
  - **OpenScape Branch**
  - **Deployment and Licensing Service** (DLS) for managing SIP endpoints
- **Command Line Interface (CLI)** for system administration and provisioning

Applications

Unify applications such as OpenScape Xpressions, OpenScape Contact Center, and OpenScape UC Application provide such functionality as unified messaging, computer-telephony integration, and call center support.

Supported Devices

Hard Phones

- OpenScape Desk CP telephones (Models 100, 200, 205, 400, 600, 600E, 700, 700X)
- Limited support for SIP-compliant third-party devices
- Cordless IP handset, base station and server software

Soft Clients

- OpenScape Desktop Client Personal Edition
- OpenScape Web Client
- OpenScape Desktop Web Embedded Edition

Analog Adapters

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

SIP Gateways - for Access to the PSTN and other TDM Networks

Gateways

- OpenScape 4000
- OpenScape Branch appliance OSB 550 / 550 HA

Other Network Devices

- Session Border Controllers

  - OpenScape SBC
  - Acme Packet SBCs

  NOTICE: The OpenScape Branch products include integrated SBCs, so they do not require the use of an external SBC.

- OpenScape Media Server

  NOTICE: Hardware recommendations for the OpenScape Media Server are specified in the section *Media Servers Supported By OpenScape Voice.*

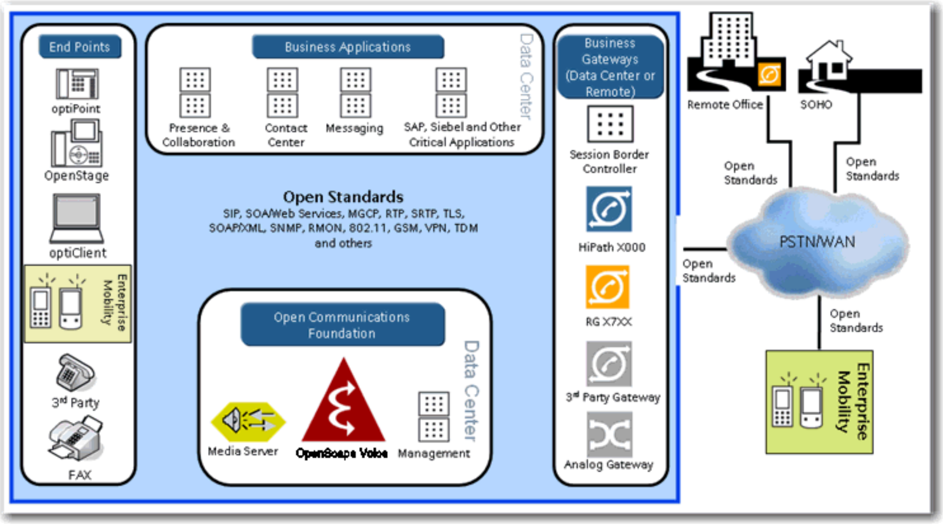


Figure 1: OpenScape Voice Main Components

1.3 OpenScape Voice Deployment Models

OpenScape Voice can be deployed either as a Single Server or as a Dual-Node (Redundant) installation for highest reliability, integrated or functionally distributed architectures, single site, or geographically separated installations. It is scalable from a few hundred to 100,000 users per single system, and a virtually unlimited number of users per network. By ensuring that all functions and applications maintain constant, unrestricted availability, OpenScape Voice provides a new level of quality in IP communications.

OpenScape Voice Configuration Options

Integrated Simplex

In the integrated simplex deployment model, the OpenScape Voice Assistant administration application, OpenScape Media Server, Deployment Licence Service (DLS), Common Management Platform (CMP), and OpenScape UC Application are all installed on a single server.

- This configuration can support up to 5000 OpenScape Voice subscribers if OpenScape UC Application is not activated. The subsequent table shows the measured mix of users for the supported hardware platforms when the OpenScape UC Application is activated. The formula assumptions (footnoted in the subsequent table) are:

  BHCA per user is 5
  CSTA originated calling (ringback tone) is 18 seconds
  Call duration (time the average call is connected) is 180 seconds

- In redundant (offboard) configurations, the customer has the option of installing any of the support applications (Assistant, Media Server, DLS, CMP) on separate servers. OpenScape UC Application is ALWAYS installed on a separate server.
- For customers demanding maximum system availability, configurations based on a Duplex System (two redundant nodes) are recommended. On

a simplex system, service-related actions like upgrades will incur an outage (system downtime).

Standard Duplex

In the Standard Duplex deployment model, the OpenScape Voice system runs on two servers, with all supporting applications (CMP, Assistant, Media Server, and DLS) installed on external servers. The two OpenScape Voice nodes can be co-located or geographically separated. The standard duplex configuration can support up to 100,000 subscribers under certain traffic and feature configurations.

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

Table 1: Application Server Performance Limits

Application	Server Type	Example	Performance Limit
OpenScape UC Application	2 quad-core	FSC RX 300 S3	5000 subscribers
CMP / OpenScape VoiceAssistant	1 dual-core	FSC TX 150 S5	20,000 subscribers
	2 quad-core	FSC RX 300 S3	100,000 subscribers
OpenScape Media Server	1 dual-core	FSC RX 300 S3	150 channels (G.711) or 52 channels (G.729)
Xpressions	1 dual-core	FSC TX 150 S5	4000 subscribers 60 voice mail channels (G.711)

Standard Duplex Large

The Standard Duplex Large extends the capacity of the Standard Duplex deployment with an added capacity of max 200,000 DNs provisioned in the database. However, the limit of maximum 100,000 registered subscribers and therefore the call model remains the same as the Standard Duplex deployment. The additional provisioned DNs are useful in a large DLS mobility setup, where a virtual device along with a real device need to be provisioned per subscriber, but only one at a time can be registered to the OSV.

Redundant (Node-Separated) Configurations

The OpenScape Voice node redundancy can be deployed in the following ways:

- Geographically co-located cluster nodes
- Geographically separated cluster nodes, where the interconnect link is a layer-3 connection (recommended)
- Geographically separated with the cluster nodes in the same VLANs/subnets with the interconnect link served by a layer-2 connection

Other Configuration Options

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 OpenScape Voicesolution. It provides access to the following components:

- OpenScape Voice Assistant: A unified graphical administration tool, OpenScape Voice Assistant runs under (as part of) the CMP and provides for the administration of OpenScape Voiceusing a standard web browser. On Integrated systems the Assistant software is installed and runs on the OpenScape Voice server itself. On Standard (non-Integrated) systems the Assistant software is installed on a separate Linux server.

  In a cluster environment, the Assistant runs active-active, with instances on both nodes of the duplex system. The active instances of OpenScape Voice Assistant maintain database synchronization of administration updates to the master OpenScape Voice database.

- OpenScape Media Server: On Integrated systems (under 5000 lines only) the software is installed and runs on the OpenScape Voice server itself. On Standard (non-Integrated) systems the software is installed on a separate Linux server. 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): DLS is a Java-based application with a browser-based user interface that is used to configure and manage Gateways, Soft clients, and SIP telephones connected to the OpenScape Voicesystem. On Integrated systems the Assistant software is installed and runs on the OpenScape Voice server itself. On Standard (non-Integrated) systems the software is installed on a separate Linux server.

- OpenScape UC Application is an advanced unified communication application which can provide voice mail, conferencing, mobility, and presence service for OpenScape Voice subscribers. On Integrated systems the Assistant software is installed and runs on the OpenScape Voice server itself. On Standard (non-Integrated) systems the Assistant software is installed on a separate Linux server.

1.4 OpenScape Voice Hardware Architecture

The OpenScape Voice Hardware includes the servers that can be used as computing nodes for OpenScape Voice, and the Ethernet switch.

Computing Nodes

The following servers can be used as computing nodes for V10 OpenScape Voice:

- Lenovo SR-530 for new deployments
- Lenovo x3550 M5 for existing deployments

- Fujitsu RX200 S7 for existing deployments

Ethernet Switch

Ethernet Switch Requirements

The Ethernet switch provides RJ-45 copper 10/100 Fast Ethernet paths for system management, control, transfer of call detail record files, and database maintenance and mirroring. Two Gigabit copper ports and two fiber ports deliver two active uplinks for greater throughput and two redundant uplinks.

- Single-node integrated OpenScape Voice system: One VLAN-capable with at least four ports on the OpenScape Voice side and gratuitous ARP support. If the customer premises has a dual subnet LAN configuration, two LAN switches can be used.
- Redundant OpenScape Voice system: Two VLAN-capable with two high-speed links, at least seven ports on the OpenScape Voice side, and gratuitous ARP support.
- Geographically separated node configuration: Two LAN switches for each node.

1.4.1 OpenScape Voice Hardware – IBM x3550 M3 Server

The IBM x3550 M3 can be used as the computing node in both the redundant configurations and the simplex configuration. The X3550 M3 is housed in a rack-mountable enclosure.

IBM x3550 M3 Product Attributes

- Processor: Two 2.66 GHz 6-core Intel Xeon 5650 processors
- Memory: 8 GB of Double Data Rate 3 (DDR3) memory
- Hard Disk Drives: Two 300 GB hot-swappable HDDs in RAID 1
- CD/DVD drive
- Disk controller: Internal on-board RAID controller
- Ethernet interfaces:
  - For a single-node OpenScape Voice server: Four 100/1000BT ports (three are used). One Dual port Gigabit Ethernet daughter card provides two ports in addition to the two system board ports.
  - For a redundant OpenScape Voice server: Eight 100/1000BT ports. One Dual port Gigabit Ethernet daughter card and one Quad port Gigabit Ethernet PCI card provide six ports in addition to the two system board ports.
- Remote Supervision: One Intel Management Module with optional Virtual Media Key (VMK)
- USB 2.0 Ports: 4 (2 front, 2 rear)
- Power supply: Two hot-swappable AC power supplies. DC power is optional.

1.4.2 OpenScape Voice Hardware – IBM x3550 M4 Server

The IBM x3550 M4 can be used as the computing node in both the redundant configurations and the simplex configuration. The X3550 M4 is housed in a rack-mountable enclosure.

IBM x3550 M4 Product Attributes

- Processor: Two 2.00 GHz 6-Core Intel Xeon E5-2620 CPUs
- Memory: 32 GB of Double Data Rate 3 (DDR3) memory
- Hard Disk Drives: Two 300 GB hot-swappable HDDs in RAID 1
- CD/DVD drive
- Disk controller: Internal on-board RAID controller
- Ethernet interfaces:
  - For a single-node OpenScape Voice server: Four 100/1000BT ports (three are used). One Dual port Gigabit Ethernet daughter card provides two ports in addition to the two system board ports.
  - For a redundant OpenScape Voice server: Eight 100/1000BT ports. One Dual port Gigabit Ethernet daughter card and one Quad port Gigabit Ethernet PCI card provide six ports in addition to the two system board ports.
- Remote Supervision: One Intel Management Module with optional Virtual Media Key (VMK)
- Universal Serial Bus (USB) ports: Six (two at the front, four at the back)
- Power supply: Two hot-swappable AC power supplies. DC power is optional.

1.4.3 OpenScape Voice Hardware - FTS Primergy RX200 S6 Server

The OpenScape Voice hardware platform runs on highly reliable, fault-tolerant computing nodes (servers). In addition to the servers themselves, Ethernet switches are required. Redundant configurations can be geographically co-located or geographically separated, depending on the system size and the enterprise’s needs.

The Fujitsu Technology Solutions (FTS) PRIMERGY RX200 S6 server is used as the computing node in both of the redundant configurations and the simplex configuration. The OpenScape Voice redundant system consists of two FTS RX200 S6 servers.

Housed within a rack-mountable enclosure, the FTS RX200 server is equipped for OpenScape Voice as follows:

- Processor: Two 2.66 GHz 6-Core Intel Xeon X5650 processors
- Memory: 12 GB of Double Data Rate 3 (DDR3) memory
- Hard disk drives: Two 300 GB hot-swappable HDDs in RAID1
- CD/DVD drive
- Disk controller: Internal on-board RAID controller

- Ethernet interfaces
  1) For a single-node OpenScape Voice server: Four 1000PT Cu Ip ports (three are used). One Dual port Gigabit Ethernet PCI card provides two ports in addition to the two system board ports
  2) For a redundant OpenScape Voice server: Eight 100/1000BT ports. One Dual Port Gigabit Ethernet PCI card and one Quad ports Gigabit Ethernet PCI card providing six ports in addition to the two system board ports
- Universal Serial Bus (USB) ports: Six (three at the front, three at the back)
- Remote supervision: One Integrated Remote Management Controller (iRMC)
- Power supply: Two hot-swappable 110/220 AC power supplies

1.4.4 OpenScape Voice Hardware - FTS Primergy RX200 S7 Server

The OpenScape Voice hardware platform runs on highly reliable, fault-tolerant computing nodes (servers). In addition to the servers themselves, Ethernet switches are required. Redundant configurations can be geographically co-located or geographically separated, depending on the system size and the enterprise’s needs.

The Fujitsu Technology Solutions (FTS) PRIMERGY RX200 S7 Server is used as the computing node in both of the redundant configurations and the simplex configuration. The OpenScape Voice redundant system consists of two FTS RX200 S7 servers.

Housed within a rack-mountable enclosure, the FTS RX200 S7 server is equipped for OpenScape Voice as follows:

- Processor: Two 2.00 GHz 6-Core Intel Xeon E5-2620 CPUs
- Memory: 32 GB of Double Data Rate 3 (DDR3) memory
- Hard disk drives: Two 300 GB hot-swappable HDDs in RAID1
- CD/DVD drive
- Disk controller: Internal on-board RAID controller
- Ethernet interfaces
  1) For a single-node OpenScape Voice server: Four 1000PT Cu Ip ports (three are used). One Dual port Gigabit Ethernet PCI card provides two ports in addition to the two system board ports
  2) For a redundant OpenScape Voice server: Eight 100/1000BT ports. One Dual Port Gigabit Ethernet PCI card and one Quad ports Gigabit Ethernet PCI card providing six ports in addition to the two system board ports
- Universal Serial Bus (USB) ports: Five (two at the front, three at the back)
- Remote supervision: One Integrated Remote Management Controller (iRMC)
- Power supply: Two hot-swappable 110/220 AC power supplies

1.5 OpenScape Voice Software Architecture

The OpenScape Voice platform uses third-party, open platform software including the operating system, signaling stacks, and database products. The OpenScape Voice software uses modular Linux packaging.

OpenScape Voice Software Components

- Platform elements, which include the operating system, PRIMECLUSTER, RTP middleware, and OpenScape Voice middleware functions
- Call control and processing elements, which include the universal call engine (UCE), signaling managers, and Service Logic Execution Environment (SLEE) services
- Support for SIP, SIP-Q, CSTA, and MGCP (for Media Servers) signaling protocols
- Address translation and routing
- QoS control for IP bearer traffic
- Element and network management interfaces, sometimes known as operation, administration, maintenance, and provisioning (OAM&P)

The figure below shows the OpenScape Voice software components.

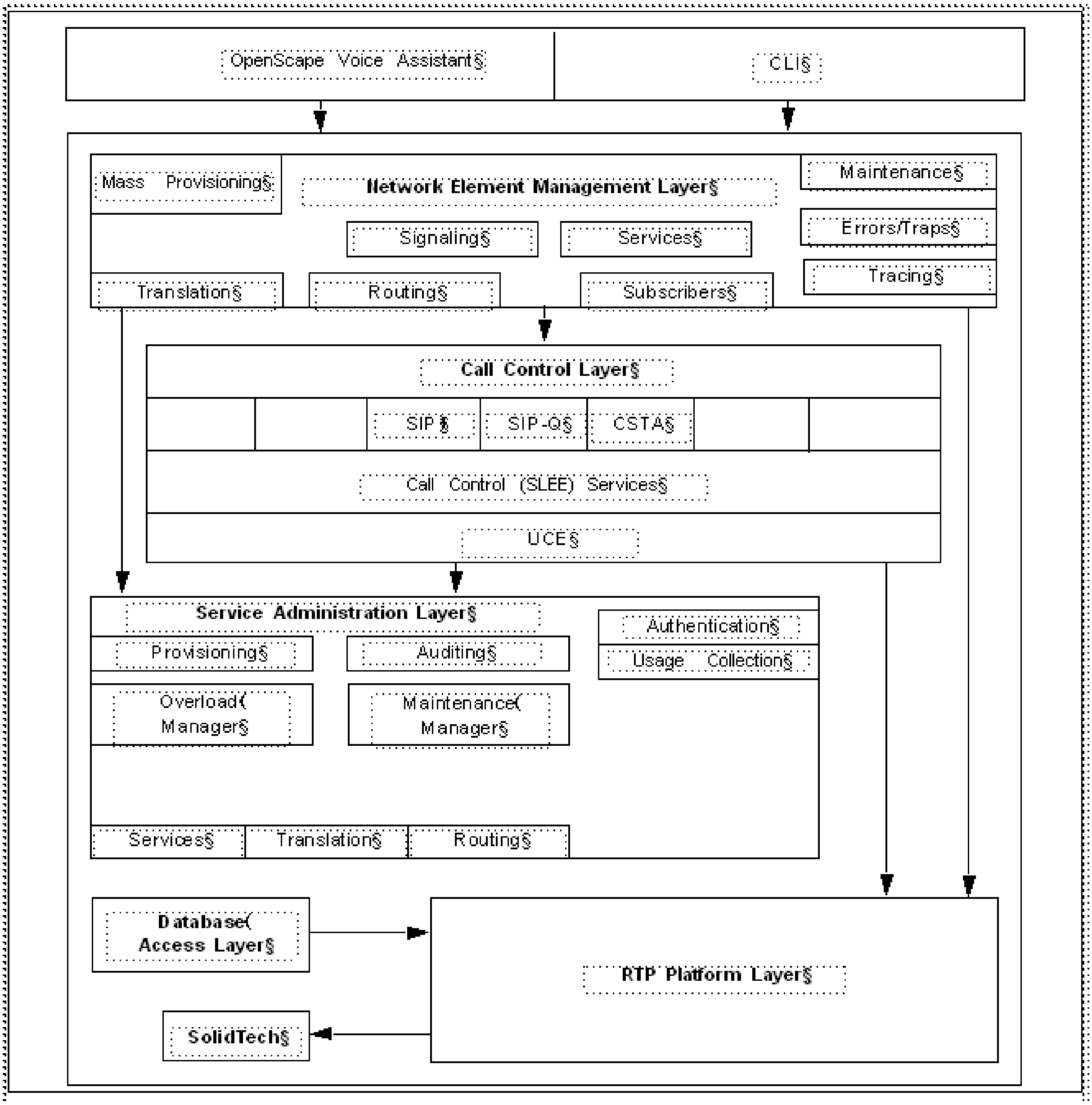


Figure 2: OpenScape Voice Software components

1.5.1 OpenScape Voice Software – Platform Components

The OpenScape Voice software platform combines platform elements, call processing elements, and support for applicable signaling protocols and endpoint types. Of particular importance are the following:

Linux Operating System

PRIMECLUSTER

SolidTech Database

RTP Middleware

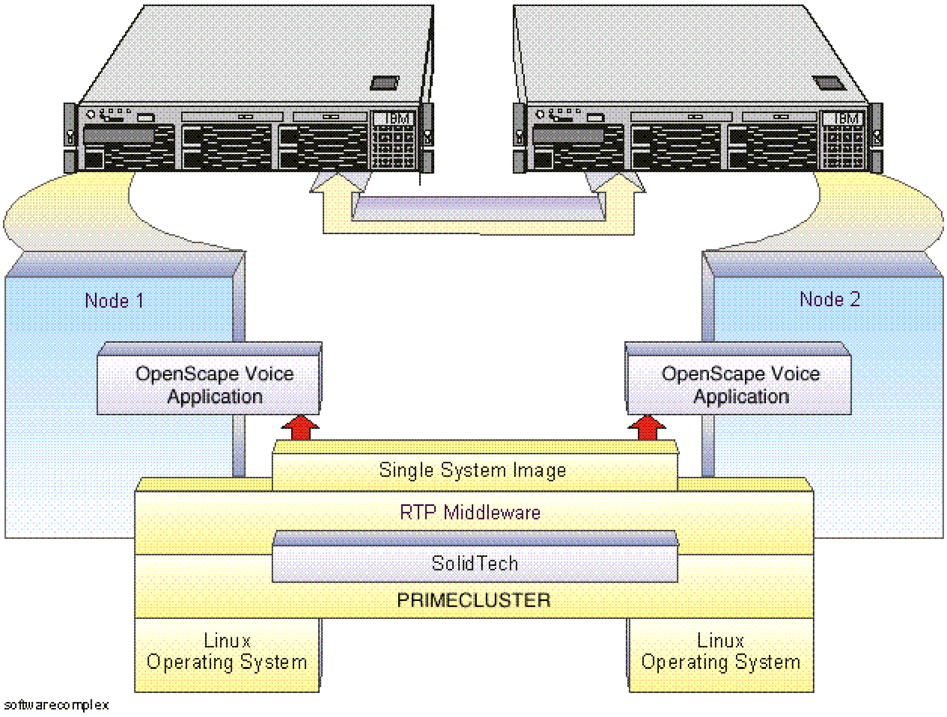
OpenScape Voice Middleware

- Resilient Telco Platform (RTP): This middleware provides message communication between processes and manages message queues to provide location transparency and data resiliency. In redundant systems, the RTP also supports the operation of the two partner nodes.

- Universal Call Engine (UCE): This key call processing component provides a secure, generic interface to set up and release calls through the system. It provides common logic to all signaling managers to route calls through the OpenScape Voice server. Refer to the *OpenScape Voice Software Architecture - Call Control* section of the present documentation for details about UCE.

- Network Element Management: Provides the capability to perform OAM&P tasks by deploying user-oriented application components for provisioning, management, and service. Refer to the corresponding sections of the present documentation for details about Network Element Management and about the UI Management Tools used by OpenScape Voice.

The subsequent figure shows the OpenScape Voice platform components.



OpenScape Voice uses the SuSe LINUX Enterprise Server 12 (SLES-12) operating system.

PRIMECLUSTER does the following:

- Links individual nodes into a cluster
- Provides information about cluster membership and the status of each member node

A single-node system is cluster-ready, which means that the PRIMECLUSTER software is installed, although not used.

OpenScape Voice uses the SolidTech database, which is a shared-nothing database with data replication between the two nodes. The two SolidTech databases run in hot-standby mode, where changes are written to the primary database only, then replicated by the database to other node. Data can be read from both nodes.

For data writes, the OpenScape Voice applications attach to the primary database, which may be located on its own node or (in a redundant configuration) on its partner node. When changes are made to the primary database, they are automatically replicated to the secondary database and only committed when both databases are updated.

In case of a node failure, the application may lose the primary database connection. Controlled by the RTP watchdog, the secondary database becomes the primary, the applications connect to the new primary database, and normal operation resumes.

The RTP (Resilient Telco Platform) is a distributed computing and fault-tolerant platform that is the underlying middleware for OpenScape Voice. The use of a distributed architecture provides redundancy at the computing element level and at the process level.

The RTP is a distributed computing and fault-tolerant platform that is the underlying middleware for OpenScape Voice. The use of a distributed architecture provides redundancy at the computing element level and at the process level.

The RTP provides services that implement applications with location transparency and data resiliency, as follows:

- Location transparency is achieved by using a logical naming mechanism for the redundant process instances, which is referred to as aliasing. Each process instance may have an alias that acts as a redundant instance. The configuration of aliases includes active-standby and active-active. Alias members may be in the same node or in the partner node.
- Data resiliency ensures that data is stored and replicated such that if a process fails, the data is still available. Upon failure of a process, data is stored in such a way that it remains available when the process is restarted. Upon failure of one node, data is available to the processes in the other node.

  Network element management uses these mechanisms to monitor the OpenScape Voice application processes such as the UCE, signaling managers, connection control manager, routing manager, AAA manager, and usage collection. When any process becomes unavailable, network element management is informed, then generates the appropriate critical alarms. It is also informed when a process becomes available, so that the corresponding alarms can be cleared.

In addition to the RTP Middleware components, the OpenScape Voice software provides the following middleware functions:

Component	Description
Real-time trace	The real-time trace is used for debugging purposes. It is used to create event files that track the execution behavior, at different severity levels, of selected RTP and OpenScape Voice processes. Refer also to the OpenScape Voice Service Manual: Volume 5, Diagnostic Tools: Real-Time Trace, RapidStat, Call Trace.
TCP/TLS/ UDP (TTUD) dispatcher	Each node has multiple IP addresses for load distribution and resiliency reasons. The (TTUD) dispatcher provides these multiple communication channels to the external IP network.
OPLOG	OpenScape Voice software uses this component to store non-alarmed events in different log files. Logged events are counted and may generate threshold crossing alarms if too many log events are reported within 5 or 15 minutes.

1.5.2 OpenScape Voice Software Architecture – Call Control

Call control provides the core call processing center. It incorporates call processing components including the UCE, signaling managers, and call control services dynamically loaded into the UCE.

Universal Call Engine

Service Layer

Signaling Managers (SIP, SIP-Q, CSTA, Connection Control Manager)

SIP Signaling Manager

SIP-Q Signaling Manager

CSTA Signaling Manager

Connection Control Manager

SLEE Services

Real-Time Data Management

Call Resource Auditing

The key component of the OpenScape Voice call processing function is the protocol-independent UCE, which contains the generic switching functions of OpenScape Voice. It provides the following:

- A secure, generic interface to set up and release calls through the system
- Common logic to all signaling managers to route calls through the system

A large number of APIs provided to the UCE are crucial to OpenScape Voice programmability and the ability to interoperate with standards-based equipment.

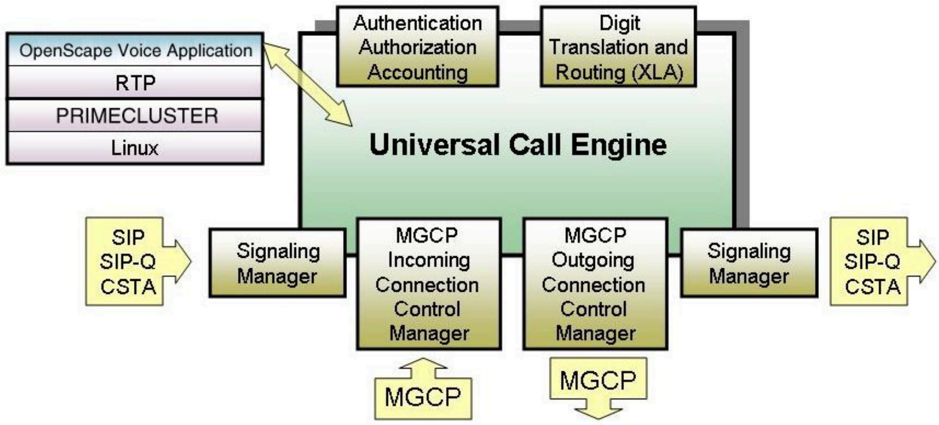
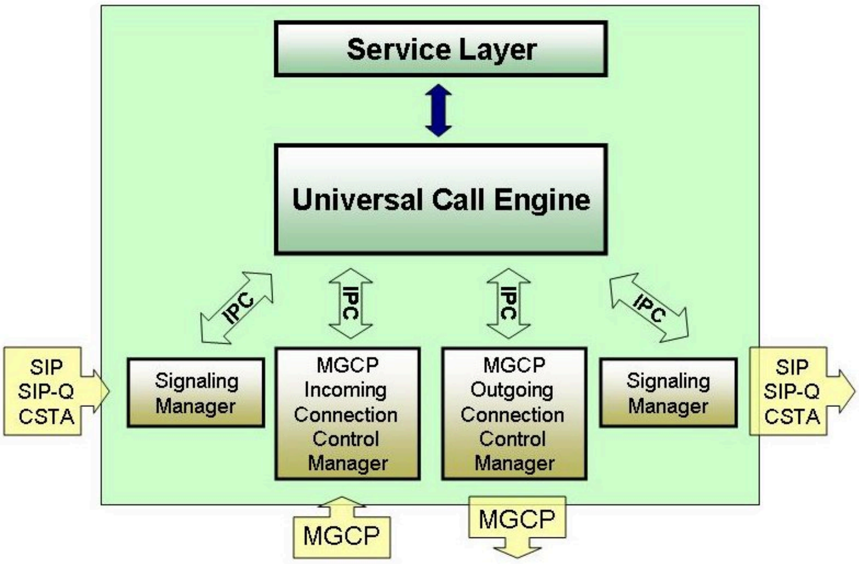

OpenScape Voice Application
RTP
PRIMECLUSTER
Linux
Authentication Authorization Accounting
Digit Translation and Routing (XLA)
Universal Call Engine
SIP SIP-Q CSTA
Signaling Manager
MGCP Incoming Connection Control Manager
MGCP Outgoing Connection Control Manager
Signaling Manager
SIP SIP-Q CSTA
MGCP
MGCP

Figure 3: UCE Interfaces

Component	Description
Incoming transaction segment (ITS)	This component executes the originating (inbound) call logic on the A-side.

Component	Description
Outgoing transaction segment (OTS)	This component executes the terminating (outbound) call logic on the B-side.
Associator segment (AS)	This component preserves the overall call topology and maintains the relationship between each ITS and OTS involved in a single call.
Central distributor module	This component brokers messages among the ITS, OTS, and AS.

The UCE interacts with the service layer, signaling managers, and connection control manager.



The following are the main functions of the service layer:

- Managing access and user/subscriber related resources
- Managing call admission control by ensuring that enough bandwidth is provided
- Authenticating subscribers prior to call setup by means of the authentication, authorization, and accounting (AAA) services
- Matching of the subscribed capabilities of the users involved in each call with the resources allocated to that call
- Enabling mediation between call signaling through communication with various signaling managers
- Providing access to digit translation and routing (XLA)
- Selecting the outgoing signaling manager based on the results from call routing
- Generating CDRs by means of the usage collection function
- Coordinating the connection and release of physical and logical switching resources and the switching of connections by using the connection control manager

- Coordinating features and supplementary services that are dynamically loaded into the UCE

The following are the main functions of the signaling managers:

- Handling all protocol functionality, such as:

  Message encoding and decoding
  Protocol state event processing
  Protocol conformance checks
  Protocol specific timers
- Interfacing with the signaling stacks where appropriate
- Adapting the external protocol messages to the common secure, normalized interface defined by the UCE
- Receiving and sending maintenance- and administration-related protocol messages
- Interacting with the OpenScape Voice maintenance functions

The SIP signaling manager transports message traffic between SIP endpoints and the UCE. It communicates with SIP endpoints through TCP (default), TLS or UDP connections, and does the following:

- Converts call control messages between SIP, SDP, and UCE formats
- Manages SIP sessions

Registration processing is controlled by a separate process, known as the SIP registrar, that handles REGISTER requests and responses.

NOTICE:

SDP transparency enables the SIP signaling manager to forward the received SDP data to the second leg of the call without any modification in the parameters. Refer to the Feature Description section of the present documentation for more information.

The SIP-Q signaling manager is an integral part of the SIP signaling manager, and is considered a trunking interface. It translates QSIG protocol that is tunneled in a QSIG multipurpose Internet mail extensions (MIME) format, then interworks it with SIP endpoints, local voice mail equipment, media servers, and other SIP-Q destinations. It supports a robust QSIG feature set and supplementary services.

The SIP-Q signaling manager can also act as a tandem node in the network. It communicates with other signaling managers via the UCE. Supported transport types include TCP (default) and TLS over TCP.

The CSTA signaling manager transports and handles CSTA message traffic between CTI applications and the UCE. It communicates with the relevant application through TCP (default) or TLS over TCP connections, managing a CSTA session and converting call control messages between CSTA and UCE formats.

The connection control manager oversees creation and deletion of the media connections associated with a call. It supports the media servers associated with the system, and communicates directly with the UCE over UDP connections; a signaling manager is not required.

Because the OpenScape Voice servers and its media servers can be geographically separated, a control protocol is required between them that permits OpenScape Voice to make and break a connection in the media gateways. The connection control manager implements these protocols and shields the UCE from the details.

The Services Logic Execution Environment (SLEE), also known as the OpenScape Voice services framework, is a collection of application programming interfaces (APIs) within the UCE. SLEE services can be categorized as follows:

- Network- vs. Nodal-Based

  A service with execution logic that spans more than one network node is considered a network-based service. CSTA and CCBS/NR are examples of these.

  A service with execution logic that is confined entirely within a single network node is considered a nodal-based service. Call transfer is an example of this.

- Call-Related vs. Non-Call-Related

  A service with execution logic that is a part of a specific call is considered a call related service. OpenScape Voice-based call forwarding is an example of this.

  A service with execution logic that is not confined to any specific call is considered a non-call related service. The latter is less frequent than call-related services. Message waiting indication is an example of this.

The execution of native services is influenced by UCE events passed between the UCE components. These events can be observed, modified, or discarded to provide specific behavior modifications to basic call services. Services beyond basic call run under the control of the UCE’s feature segment (FS) component.

OpenScape Voice supports memory-based data management for real-time data access. It also supports dynamic data synchronization between nodes. This provides swift recovery response times when node failover occurs.

OpenScape Voice audits call resources. Audits are performed on a configurable, regular basis to ensure proper OpenScape Voice operation.

1.5.3 OpenScape Voice Software Architecture – Endpoint Support

OpenScape Voice provides support for SIP, MGCP, and analog endpoints.

SIP Endpoints

MGCP Endpoints

Analog Endpoints

OpenScape Voice supports SIP endpoints, including SIP telephones, the OpenScape UC Application Personal Edition, and third-party SIP endpoints.

OpenScape Voice supports the media server as an MGCP endpoint and it uses the media gateway control protocol (MGCP), which is an IP-based signaling protocol.

An analog endpoint, such as an analog telephone or fax machine, is physically connected to a SIP analog adapter.

OpenScape Voice supports connections to analog endpoints by contacting the SIP analog adapter directly.

1.5.4 OpenScape Voice Software Architecture – Signaling Protocols

OpenScape Voice supports the processing and interactions of the following signaling protocols:

- SIP
- SIP-Q
- CSTA
- MGCP
- QSIG

1.5.5 OpenScape Voice Software Architecture – Address Translation and Routing

Address translation is the process of interpreting incoming digits and determining the appropriate destination or feature.

Internet Protocol Version 6 (IPv6) Support

Other Characteristics

OpenScape Voice is a combined SIP back-to-back user agent and SIP registrar. It provides alias translation; dynamic endpoint registration and unregistration; call routing; and call admission control.

The OpenScape Voice SIP registrar supports dynamic and static (permanent) alias registrations, and performs alias translation to resolve aliases to an IP transport address, when it receives a call request from the endpoint. If another server manages the endpoint, the aliases are translated into the call signaling transport address of the far-end server.

As a back-to-back user agent, OpenScape Voice remains as part of the signaling path for the entire duration of the call, so it can provide features and services for the entire life of the call. However, the actual media streams (voice, data, and video) do not pass through the OpenScape Voice server, but are negotiated and routed directly between the endpoints.

SIP endpoints can be manually programmed with the IP address or FQDN of the OpenScape Voice registrar, or they can automatically obtain the address via a DHCP or DNS server which has been configured with this information.

NOTICE:

Refer to the specific Feature descriptions in the present documentation for more information about address translation and routing features.

Internet Protocol version 6 (IPv6) is a network layer IP standard (RF 2460), which follows IPv4 as the second version of the Internet Protocol.

The main advantage of IPv6 is the increase in the number of addresses available for networked devices

- The IPv4 uses 32-bit addresses, which allows about 2^32 = 4.3 billion IP addresses.
- The IPv6 uses 128-bit addresses, which allows about 2^128 IP addresses.

IPv6 addresses are typically composed of two logical parts: a 64-bit (sub-) network prefix, and a 64-bit host part, which is either automatically generated from the interface's MAC address or assigned sequentially.

IPv6 addresses are represented in the form of eight hexadecimal numbers divided by colons, for example:

```
2001:0db8:0000:0000:0000:0000:1428:57ab
```

To shorten the notation of addresses, leading zeroes in any of the groups can be omitted, for example:

```
2001:0db8:0:0:0:0:1428:57ab
```

Finally, a group of all zeroes, or consecutive groups of all zeroes, can be substituted by a double colon, for example:

```
2001:0db8::1428:57ab
```

NOTICE:

The double colon shortcut can be used only once in the notation of an IPv6 address.

If there are more groups of all zeroes that are not consecutive, only one may be substituted by the double colon; the others would have to be noted as 0.

1.5.6 OpenScape Voice Software Architecture – QoS Control

OpenScape Voice assists the administrator in assuring adequate voice quality of service by providing call admission control (resource reservation) and enforced codec selection on narrow-bandwidth data links:

- Call admission control rejects new call requests when additional calls might exceed the bandwidth of the network, jeopardizing the quality of connections already established.

- Enforced codec selection permits the administrator to identify IP links with restricted bandwidth where a narrow-bandwidth codec is the best choice.

1.5.7 OpenScape Voice Software Architecture – Network Element Management

Network element management provides the capability to operation, administration, maintenance and provisioning (OAM&P) tasks. OAM&P tasks are performed by deploying user-oriented application components that provide the capability to:

Service Management Provisioning

Mass Provisioning

Call Detail Records (CDRs)

Image Installations and Upgrades

Online Patching

Split-Mode Upgrades

Backup and Restore

- Perform service management provisioning through the CLI and OpenScape Voice Assistant
- Perform mass provisioning

> **NOTICE:**
>
> For detailed information about how to perform mass provisioning, refer to the OpenScape Voice V10, Interface Manual: Volume 2, SOAP/XML Subscriber Interface Provisioning, Administrator Documentation, chapter *Import and Export of SOAP Provisioned Data.*

- Generate call detail records (CDRs)
- Perform image installations and upgrades on OpenScape Voice and its applications
- Implement rolling upgrades on OpenScape Voice
- Implement split-mode upgrades on OpenScape Voice and its applications
- Back up and restore the system

The Common Management Platform, the OpenScape Voice Assistantand the CLI provide the element management interfaces. Additionally, external applications can provide the interface to perform network management for OpenScape Voice and all supported features and applications.

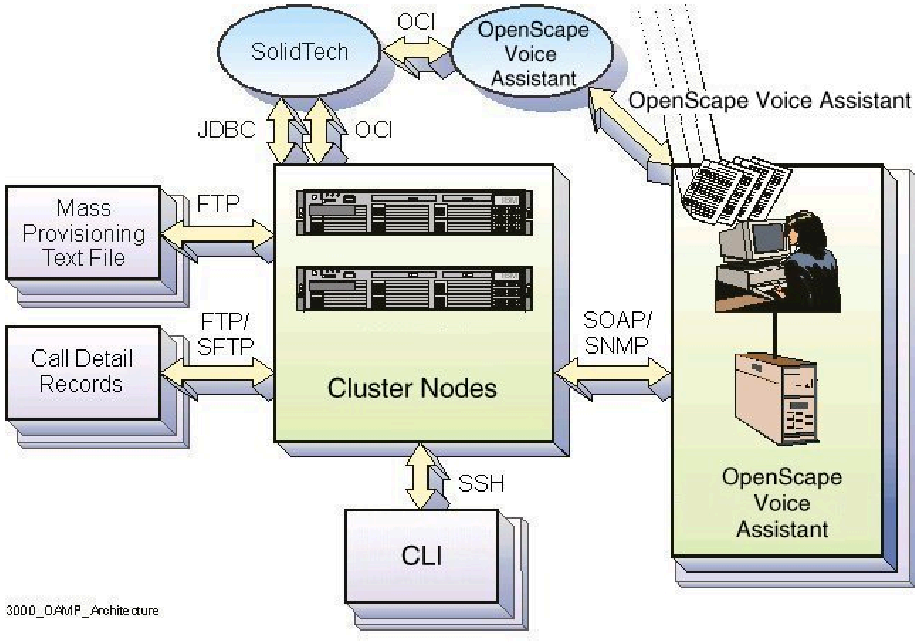

SolidTech
OCI
OpenScape Voice Assistant
JDBC
OCI
OpenScape Voice Assistant
Mass Provisioning Text File
FTP
Call Detail Records
FTP/ SFTP
Cluster Nodes
SOAP/ SNMP
SSH
CLI
OpenScape Voice Assistant
3000_OAMP_Architecture

Figure 4: OpenScape Voice OAM&P Architecture

The CLI and OpenScape Voice Assistantprovide the ability to:

- Provision and view network topology data
- Configure OpenScape Voice for its operational environment
- Analyze measurements and operational statistics
- Monitor alarms, alerts, and traps

These tools also provide the ability to configure other aspects of the system.

Mass Provisioning provides the following:

- Expert-mode CLI commands to populate and configure the OpenScape Voice databases
- SOAP mass provisioning commands to simplify the creation of large numbers of subscribers

OpenScape Voice generates and maintains CDRs for usage collection and billing purposes. The UCE maintains CDR information in the active call context, which can follow the call from process to process and, in a redundant system, from node to node.

At the end of every call, a CDR is generated. However, intermediate CDRs are also generated once every 30 minutes; CDRs also are generated intermittently for long-duration calls, such as those that pass over midnight more than once.The RTP ticket manager handles the individual CDRs.

The CDR handler manages the internal binary billing files through the RTP API, then makes them available to a billing server. The CDR handler also converts and formats these internal binary billing files. The completed and formatted billing files can be transferred from the OpenScape Voice server through FTP or SFTP, depending on the file transfer method and the capabilities of the billing server.

Imaging is an efficient and automated process for installing and upgrading the OpenScape Voice software and its applications. An image does the following:

- Reduces time required for initial installations and version upgrades
- Reduces manual steps by eliminating individual steps to install each software component, eliminating the need to raise the installation to the latest patch level, and eliminating MOPs during installation
- Increases reliability in the installation and upgrade process by automating the installation
- Provides a common method for installs and upgrades, reducing the number of procedures that need to be supported
- Provides a common installation method for both supported hardware platforms

Imaging is supported on each of the OpenScape Voice deployment models, as described in the *Deployment Models* section.

Software installation for new OpenScape Voice systems consists of booting/ loading from a DVD and populating site-specific configurations parameters such as IP addresses.

The DVD contains a complete reference image that facilitates a fast install. An off-line Install Wizard is provided to create site-specific configuration parameters beforehand, which are automatically installed during the boot from DVD. The system can then be configured with subscriber, routing, and translation data to become ready for service.

During the installation, upgrade, or migration to V10, the hard drive for each node is divided into two partitions of equal size. These partitions are referred to as the primary partition and the secondary partition. The partition on which the running software resides is known as the active partition (which could be either the primary or secondary partition); the other is known as the fallback partition. Should the active partition become unstable, one option is to recover by booting off the fallback partition that contains the backup. Contact your next level of support for assistance.

Online patching, sometimes known as a rolling upgrade, is used to implement patches and software maintenance releases (SMRs) on the OpenScape Voice software. It performs a software update without affecting service.

In a cluster, online patching of the OpenScape Voice software can be performed as long as the new software is compatible with the old software. In this case, one node is stopped and updated with new software. After this process is complete, the same process takes place on the partner node.

A split-mode upgrade is used to implement major and minor version upgrades and migrations on redundant systems. This method upgrades both the OpenScape Voice software and that of its applications.

A split-mode upgrade is essentially a fresh install of the new version of base software onto one node while the other node remains in service at the old version level and continues to process traffic. Many of the split mode upgrade scripts and some of the same tasks are used to upgrade or migrate a single-node system, but a single-node system is out of service until the upgrade or migration is completed.

Upgrades and migrations performed on V10 and later redundant systems use an improved upgrade process that greatly increases the automation of the process, which minimizes both the upgrade execution time and the possibility of technician errors.

OpenScape Voice enables backup and restore of the file system and database. The administration tool used to perform these tasks varies as follows:

- File system backup, database backup, and database restore: Either the CLI or OpenScape Voice Assistant can be used.
- File system restore: The CLI must be used.

The maintenance manager server runs OpenScape Voice maintenance tasks (known as jobs); it supports the starting, stopping, and querying of jobs through a client/server API.

NOTICE:

New license files will need to be reinstalled after performing a restore. For that reason, it is strongly recommended that backup license files be readily available.

1.6 Private Communications Networks

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

CorNet and SIP

CorNet-NQ and SIP-Q

- 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 private networks 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

CorNet is a family of protocols used for private networks made up of ISDN compatible TDM trunk facilities (T1-spans and E1-spans). These protocols provide sophisticated feature operation and are still valuable where legacy PBXs and trunking facilities are available. CorNet is supported by older PBXs such as the Hicom 300 and Rolm 9006 family.

VoIP private networks controlled by OpenScape Voice use the SIP protocol, which is standardized by the Internet Engineering Task Force (IETF) and provides similar functionality to CorNet. SIP is an evolving open standard. When used for interswitch communication, in some ways it is more capable than CorNet and in some ways it is less capable.

Table 2: Feature Availability in CorNet and SIP Environments

Feature	CorNet	SIP
Call transfer with path optimization	x	x media path only
Call forwarding with path optimization	x	x media path only
Caller name display	x	x
Called party name	x	x
Call hold	x	x
CCBS/CCNR (callback with supervision)	x	x

CorNet-NQ is the latest member of the CorNet protocol family, supported by the OpenScape 4000 PBX and HiPath 3000 PBX. CorNet-NQ is a variation of industry standard ETSI/ISO QSIG (an ISDN standard for private networks) with proprietary CorNet extensions for additional feature transparency.

OpenScape Voice, OpenScape 4000, and HiPath 3000 support a subset of CorNet-NQ transported over SIP, a protocol referred to in this document as SIP-Q. The subsequent table lists the feature availability over SIP-Q.

Table 3: CorNet-NQ Feature Support via SIP-Q

SIP-Q Feature Support	OSV to 4K	OSV to OSV	OSV to 3K
Basic Call	Yes	Yes	Yes
E 911 LOC ID 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

SIP-Q Feature Support	OSV to 4K	OSV to OSV	OSV to 3K
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)	Yes	Yes	Yes
Do Not Disturb Override (DNDO)	No	No	No
Call Deflection (CD) (per call/user invoked)	Yes	Yes	Yes
Call Offer (CO)	No	No	No
Call Intrusion (CI) (override) *	Yes*	Yes*	Yes*
Recall (RE) (transfer security) *	Yes*	Yes*	Yes*
Malicious Call Identification*	Yes*	Yes*	Yes*
Call Hold/Retrieve (CH)	Yes	Yes	Yes
Advice of Charge (AOC)	No	No	No
Three Way Conference	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

SIP-Q Feature Support	OSV to 4K	OSV to OSV	OSV to 3K
Call Pickup (PICKUP)	Yes	Yes	Yes

* Local function only.

** Immediate - based on called party authorization. No originating party control is provided.

*** Local pickup of arriving SIP-Q calls is supported.

**** E911 is applicable to OSV - OSV when the 2nd OSV is a tandem before reaching the GW.

***** Applicable for OSV-OSV in order to optimize the signaling path.

1.6.1 Network Interfaces – Gateways

OpenScape Voice supports the use of Gateways for:

Survivability

Branch Office Accessibility

Gateways Supported by OpenScape Voice

- Survivability purposes, providing access to the PSTN when necessary
- Branch Office accessibility purposes, which supports the communications environment across the enterprise, office, home office, and mobile locations

Survivability is the capability of a network to maintain service continuity in the presence of faults within the network. In the OpenScape Voice environment, survivability mechanisms such as protection and restoration have been implemented either on a per-link basis, on a per-path basis, or throughout an entire network to alleviate service disruption. This environment also provides managed redundant IP voice systems that take advantage of IP’s inherent survivability and rerouting capabilities. Additionally, the VoIP network’s ability to make call routing decisions based on the IP network’s status results in a robust and survivable voice communications system.

The OpenScape Voice landscape network can terminate calls in one of two places:

- To another IP telephony device/endpoint
- To a VoIP gateway that interfaces to the local PSTN

Call routing redundancy schemes provide that outbound calls reach the PSTN even if the preferred local gateway or PSTN service is not operating.

OpenScape Voice supports a variety of branch office solutions—from small to very large locations—by using direct workpoint client connections through a media gateway. These options support the communications environment across the enterprise, office, home office, and mobile locations.

To protect the business processes per site, a survivability solution can be added to each remote side, which maintains existing calls and ensures that small branch offices can continue to access the following basic operations during WAN failures or if OpenScape Voice is unavailable for another reason:

- Internal SIP-to-SIP calls can be made
- Calls to the PSTN can be made
- Incoming calls can be received from an alternate CO trunk

OpenScape Voice supports the following Gateways. Gateway support varies by country.

- OpenScape SBC series Gateways

  This media gateway ensures that station-to-station calls, PSTN access, and United States emergency services access (E9-1-1) are available at all times in remote branches. It supports the ANSI and ETSI PRI protocols, QSIG tunneling to the OpenScape 4000 interface, and E9-1-1 LIN server provisioning.
- HG 3450 or HG 3500 Gateway, used in the OpenScape 4000

  These media gateways support the networking of one or more OpenScape 4000s with the OpenScape Voice IP network infrastructure. Voice data is transferred in packets through LAN/WAN networks. It processes calls between circuit-switched networks and LANs; performs protocol translation, and support SIP trunking through IP networks.
- HG 1500 Gateway, used in the HiPath 3000

  This media gateway supports the networking of one or more HiPath 3000s with the OpenScape Voice network infrastructure.
- Mediatrix Gateways

  These media and signaling gateways are small branch office gateways that connect endpoints in an office serving 200 or fewer subscribers. Because they are ISDN gateways, they support ISDN switching, router function, and a gateway which converts ISDN voice data into Internet Protocol IP data streams or voice over IP, and vice versa.

Table 4: Comparison of Supported Gateways

Gateway	Number of Interfaces	Survivability	Management	OSV Interface
HG3540 or HG3500	HG3540 (without QoS data collection [QDC]): 45 or 90 channels HG3540 (with QDC): 42 or 84 channels HG3500: 60 or 120 channels	Optional OpenScape Branch SIP proxy	OpenScape 4000 Assistant or Hicom Domain Management Service (HDMS)	SIP-Q
HG 1500	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	Optional OpenScape Branch SIP proxy	HiPath 5000	SIP-Q

Gateway	Number of Interfaces	Survivability	Management	OSV Interface
Mediatrix series	Up to two T1/E1 spans Up to four S0 BRIsUp to four analog interfaces	Optional OpenScape Branch SIP proxy SIP proxy	Telnet command line or WBM	SIP

Enterprises can also continue to use their previously installed third-party SIP gateways—for example, the Cisco 3700—with OpenScape Voice. The supported functionality depends on how these gateways adhere to the relevant SIP standards.

Interoperability testing may be required to confirm feature behavior. The HiPath Ready Lab is available to vendors seeking to certify their products for use with OpenScape Voice.

1.6.2 Network Interfaces – SIP-Q Private Networking

SIP Private Networking replaces the SIP-Q protocol currently used for OpenScape Voice-to-OpenScape Voice connections. This eliminates the need to convert between SIP and SIP-Q protocol for a station-to-station call between two OpenScape Voice systems. SIP Private Networking is sometimes also referred to as Enterprise SIP Trunking or Enterprise SIP Peering.

SIP-Q Private Networking Interface -- Physical Connectivity

SIP-Q Private Networking Interface -- Logical Connectivity

The deployment strategy for multiple 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 OpenScape SBC using SIP-Q protocol—the networking between the 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 OpenScape Voice systems must be via the SIP private networking interface.

The figure below shows the physical connectivity for a simple network of two OpenScape Voice systems in a network; each duplex system consists of two processing nodes.

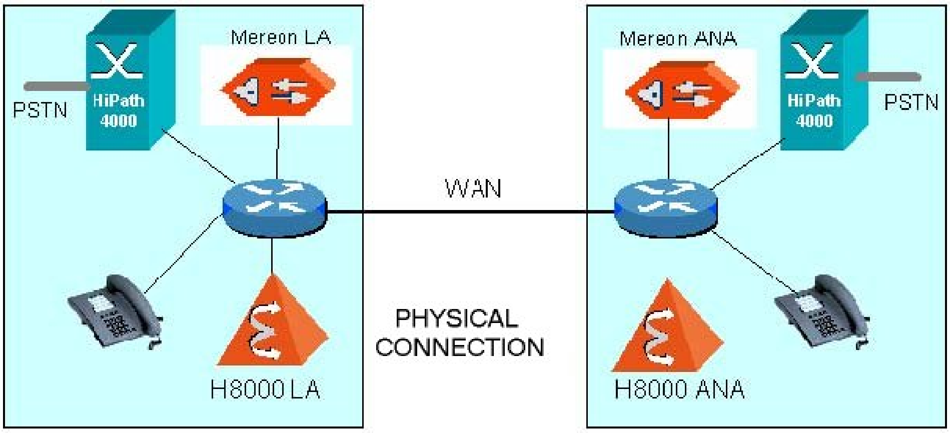


Figure 5: Two OpenScape Voice Systems in Simple SIP-Q Network -- Physical Connectivity

The figure below shows the logical connectivity for a simple network of two OpenScape Voice systems in a network; it may look quite different from the physical connectivity.

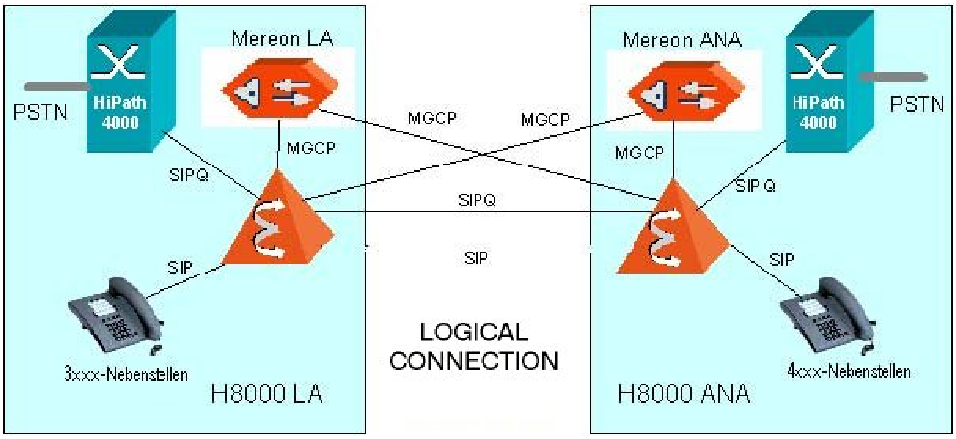


Figure 6: Two OpenScape Voice Systems in Simple SIP-Q Network -- Logical Connectivity

- The OpenScape 4000 switches, each equipped with one or more HG 3540 orHG 3500 gateways, provide the PSTN interface. Because of the larger message sizes resulting from the QSIG additions to SIP, the signaling link between OpenScape Voice and HG 3540 or HG 3500 must be TCP or TLS (UDP is not an option).

  The gateways are defined in the OpenScape Voice database as SIP endpoints. 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 OpenScape Voice system. This means that it accepts SIP-Q signaling from only one OpenScape Voice, and routes all inbound PSTN calls to that OpenScape Voice system. Therefore, if traffic from the LA gateway is destined for a subscriber in ANA, the signaling will “tandem” through the LA OpenScape Voice (and the ANA

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 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 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 OpenScape Voice, the partner 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 OpenScape Voice to permit the tandem calls.
- The endpoints (gateways and peer OpenScape Voice systems) must be marked as trusted endpoints, to prevent unwanted SIP digest authentication challenges on these links.

NOTICE:

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 theOpenScape Voice subscriber who is the originator or target of the call.

Extension dialing between the OpenScape Voice systems and between the OpenScape Voice systems and the OpenScape 4000 subscribers can be configured. However, there are numerous feature restrictions when calls go between OpenScape Voice switches or between a OpenScape Voice and OpenScape 4000 subscriber. Refer to *Private Communications Networks* for details.

1.6.3 Network Interfaces – SIP Trunking to Service Providers

While numerous enterprises have previously adopted VoIP, it was primarily utilized for internal communication within the enterprise LAN. In this context, VoIP served as a direct substitute for conventional wireline telephony. External calls necessitated a PSTN gateway at the enterprise's edge. These practices led to reduced administrative expenses and lowered internal call costs, ultimately yielding a commendable return on investment (ROI).

SIP Trunking

Traditional Trunking vs. IP Networks

With SIP trunking, however, the potential for ROI is far greater because SIP trunking takes the VoIP concept 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 OpenScape Voice SIP trunking interface to SIP service providers is described in the OpenScape Voice Interface Manual: Volume 6, SIP Service Providers Interface. OpenScape Voice has successfully interoperated with SIP service providers including Verizon Business (United States and Europe), Level3, Cbeyond, Italtel, Arcor, T-Systems, BT, and Entel.

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.

1.6.4 Session Border Control

The Session Border Control solution is deployed when VoIP networks need to extend SIP-based applications beyond the enterprise network boundaries—for example, when SIP clients of the OpenScape Voice system are not all within the same IP network.

An SBC (Session Border Controller) is basically a SIP-aware firewall that also serves as a SIP proxy or back-to-back SIP User Agent (B2BUA). A centrally located Acme Packet SBC behaves as a B2BUA whereas the OpenScape Branch SBC behaves as a proxy. The SBC is given a publicly accessible URL and IP address, and SIP phones on the Internet use this as the address of their SIP registrar and proxy. The SBC also has a second IP address, and a separate

LAN connection, in the corporate LAN. Its function is to analyze, modify, and relay messaging between the phone and the OpenScape Voice system. Only proper SIP and media (RTP) packets are permitted through the firewall function.

Most enterprises switching to a VoIP solution will want to support mobile workers, home workers, and teleworkers, and provide VoIP services for these workers. Because of the well-known security problems within the public Internet, connectivity between the customer's private IP LAN and WAN network and the public network must be restricted by the use of firewalls and other mechanisms. The SIP signaling required to operate remote endpoints will not pass successfully through standard security firewalls. Therefore, if the customer wants to have remote users that are connected to OpenScape Voice via the Internet, access through an SBC is generally preferable.

When a remote phone registers with the SBC on the public IP address, the SBC performs a deep packet inspection, fulfilling its firewall role, then relays this registration request (appropriately modified) to the OpenScape Voice system. When OpenScape Voice registers the new phone, it sees the phone IP address as one assigned to the SBC. Likewise, audio packets will be directed to and through the SBC after appropriate modification.

An SBC also provides enhanced customer-network security by providing SIP-aware security functionality including dynamic RTP/SRTP pinholing, stateful SIP protocol validation, DoS mitigation, and network topology hiding.

If the number of phones utilizing the SBC is significant, the High Availability option should be considered. Although the SBC has firewall-type functionality, for additional security it is customary to isolate the SBC from the Internet behind a standard Internet firewall, to provide additional security.

NOTICE:

If OpenScape Voice and the SBC are utilized to connect two parties who are both in the Internet, the voice channel between the endpoints need not go through the SBC, but can be a direct endpoint-to-endpoint connection within the Internet. Some SBC models provide a configuration option flag to control whether the audio streams in this case will pass through the SBC (where they might, for example, be recorded), or will be allowed to flow directly between the two Internet endpoints.

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

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

Refer to the OpenScape Voice Solutions Reference Manual: Session Border Control, for detailed information.

1.7 OpenScape Voice Cluster Redundancy

Overview

Configuration Options

Hardware Redundancy

Computing Node

Ethernet Switch

Remote Access Card

Software Components Contributing to Redundancy

PRIMECLUSTER

Resilient Telco Platform (RTP)

Reliability is the primary goal of OpenScape Voice, and clustering is necessary to provide this reliability. A reliable component structure provides an effective base for cluster administration.The OpenScape Voice hardware and software components work together to attain the following reliability goals:

- To provide faster data replication and better performance for peak traffic in normal operation by using a two-node active-active configuration, with each node acting as hot/standby for its partner. This configuration also protects against silent faults through continuous hardware/software monitoring and testing.
- To minimize node switchover, which reduces transient call loss and network connectivity outages. This is accomplished with redundant local disks, network connections for each node, and power supplies. Each node also contains duplicated Ethernet cards which ensure that the physical path for the external communication with one node is backed up by a second path —a second Ethernet port on a different Ethernet card, and a second LAN switch.
- To provide static load sharing for fast and reliable busy/idle handling, because only one node writes the busy/idle and call status for the subscriber or feature server.
- To provide effective component management through process configuration control using process and alias groups.

The OpenScape Voice redundant configuration can be deployed as follows:

- Geographically co-located cluster nodes
- Geographically separated with the cluster nodes in the same VLANs/subnets with the interconnect link served by a layer-2 connection
- Geographically separated with the cluster nodes in different VLANs/subnets with the interconnect link served by a layer-2 connection
- Geographically separated with the cluster nodes where the interconnect link is a layer-3 connection

Refer to the corresponding sections in the present documentation for details about hardware and software redundancy, redundant configurations and survivability.

To ensure quality of hardware, the OpenScape Voice software is only run on certified platforms that are selected for their reliability and are tested rigorously. The subsequent table shows the hardware platforms that are certified to run the OpenScape Voice software in a redundant configuration.

Each computing node has eight 1 Gbit/s Ethernet links set up as four pairs. A redundant pair of crossover cables, controlled by PRIMECLUSTER, interconnects the nodes.

The two Ethernet switches are layer-2 LAN switches that allow several devices to interconnect. The computing nodes connect to the external network via both Ethernet switches. This process gives the system a measure of redundancy, and protects it in the event that one of the Ethernet switches fails.

With clusters, there is always the necessity to resolve the situation where two nodes of a cluster think that they are in charge of the same resources and functions—for example, when the two nodes cannot communicate. In this situation, it must be ensured that a node can only become active when the other node has been stopped unconditionally. This capability is sometimes referred to as split-brain avoidance.

The split-brain avoidance mechanism of PRIMECLUSTER requires a safe hardware interface to eliminate a node by powering it down or rebooting it. Depending on the server, the connection is provided by:

- x3650T: Intel management module (IMM)

PRIMECLUSTER supports the cluster interconnect and offer applications well-defined interfaces which are required for cluster operation. These interfaces include internode communication which is used by processes on different nodes to communicate with each other.

Unlike other external communication interfaces that are available in every operating system, the internode communication supports redundant connections for availability reasons and a low latency protocol. A short latency period (the time required to send a message to another system and receive an acknowledgment) is just as important to the scalability of a cluster as the line throughput rate, though both are closely linked.

OpenScape Voice uses the RTP to run and manage the processes necessary for configuration, call processing, performance monitoring, and system maintenance. RTP provides redundancy and load sharing capabilities by enabling multiple computing elements, or logical nodes, within the system. While one process may be running on one CE, another process may be running on another CE within the system. Because the RTP can initiate multiple instances of the same process, different instances of the same process may run on different CEs within the system.

Functional Description

Failover Strategy

OpenScape Voice supports redundant active/active applications for cluster softswitches. During normal operation, the cluster operates in an active/active mode. When a hardware or software failure occurs, a backup node takes over the traffic of the failed node, preserving stable calls by accessing the partner context pool. In this mode:

- Traffic is distributed evenly across the available nodes and across the available call processing instances within each node.
- Each node serves as a backup to the other node.
- During call processing, each process saves its contexts to the backup node at various points in the call

The primary focus of the OpenScape Voice failover strategy is to preserve stable calls and billing data, and to ensure that resources are not left in an unresponsive state—such that a given resource cannot be accessed without restarting a device, gateway, or the system itself.

Refer to the corresponding sections in the present documentation and to the *OpenScape Voice V10 Design and Planning Manual, Volume 2, SIP Network Planning*, for details about possible failures and failover strategies.

1.8 Administration Tools for OpenScape Voice

This chapter describes the network administration tools used to provision and maintain the OpenScape Voice system.

OpenScape Voice Assistant

OpenScape Branch Management Portal

Command Line Tools for OpenScape Voice

Command Line Interface (CLI)

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 OpenScape Voice are:

- OpenScape Voice Assistant, which provides a web browser-based GUI for administration and management of the system
- The command line interface (CLI), whose basis is provided by RTP (Fujitsu Siemens Real-time Telecommunications Platform software) and is extended by Unify with softswitch-specific commands and command line tools for OpenScape Voice

The OpenScape Voice Assistant brings the administration of OpenScape Voice together into one web-based tool, replacing the NMC and SMC products.
The Assistant is accessible from any PC with a suitable web browser and connectivity to OpenScape Voice. The Assistant can reside on OpenScape Voice itself (for installations with fewer than 5000 subscribers), or on a separate server for larger installations.

The 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.

OpenScape Voice Assistant (so named to match the system release it supports) provides the following:

- Single web-based tool for administration and maintenance
- Dashboard for status visibility and access to all system components (OpenScape Voice, OpenScape Media Server, phones, and gateways)

  Web-based GUI for subscriber, dial plan and integrated OpenScape Media Server Configuration
- Role-based access to specific administration functions
- Support of SIP phones via integration with DLS phone deployment server

  Software download
  General configuration
- Integration into HiPath Management Landscape

  HiPath Accounting Management
  HiPath Fault Management
  HiPath User Management (V2.2 and later)

Refer to the *OpenScape Voice Assistant Feature Configuration* section of the present documentation for additional information.

The following GUI-based tools can be used to manage the functions specific to the OpenScape Branch platform and to administer the OpenScape Branch appliance:

- The **OpenScape Common Management Portal**, accessible directly via a Web browser after entering the IP address and the login credentials required.

In addition to providing a dashboard view of all branches, these tools provide access to the following:

- Alarms
- Media server
- Security
- Survivability features
- Utilities, such as Import and Export

The alarms generated by the OpenScape Branch platform are integrated into the CMP, so that a consolidated view of the alarms can be provided.

The following Command Line Tools can be used to administer the OpenScape Voice system:

- /unisphere/srx3000/srx/startup/srxqry: Querying the current status of the OpenScape Voice system

  For details regarding the srxqry command functionality and command options, enter `srxqry -h` at the command line.

- /root/bin/pkgversion: Querying the installed OpenScape Voice software package version and patch level (srx login credentials are required to run this command)

  Command line parameters:

  pkgversion -p returns the list of patches installed on the system
  pkgversion -ps returns the list of patch sets installed on the system
  pkgversion -m returns the list of all MOPs installed on the system

The CLI is a traditional command line application that interfaces with and manages OpenScape Voice. 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). OpenScape Voice does not let users do a simple Telnet or FTP session due to the security implemented during installation.

1.9 Media Servers Supported by OpenScape Voice

OpenScape Voice supports the media servers listed below. As appropriate, redundant media servers can be deployed in the OpenScape Voice network.

Supported Media Servers

Hardware Recommendations for OpenScape Media Server

One or more media servers is necessary to do the following:

- Provide tones and announcements to support the functionality of many OpenScape Voice features
- Provide music on hold
- Support the station-controlled conference feature by performing media mixing and transcoding where necessary

- OpenScape Media Server

This media server is the company´s software-only media server offering. In addition to the basic media server functions described above, the OpenScape Media Servercan be implemented as an internal media server on the integrated OpenScape Voice server, or as an external media server. It is configured using OpenScape Voice Assistant.

HW Profiles / Load Values	HW Specifications
Low-End Server Up to 350 concurrent G711 channels* Up to 15,000 BHCA	**1 x CPU Intel W3520 or E5620 or better**4 or 8 GB RAM (depending on usage) 2 * 73 GB SAS hard disks (RAID 1 configuration) GigaBit Ethernet
Mid-Range Server Up to 700 concurrent G711 channels* Up to 30,000 BHCA	**2 CPUs Intel E5620 or better**4 or 8 GB RAM (depending on usage) 2 x 73 GB SAS hard disks (RAID 1 configuration) GigaBit Ethernet
High-End Server Up to 1,000 concurrent G711 channels* Up to 45,000 BHCA	**2 CPUs Intel E5650 or better**8 GB RAM 2 x 73 GB SAS hard disks (RAID 1 configuration) GigaBit Ethernet
- The figures above are for a single-node Media Server. - All servers must be certified for SUSE SLES 12. - Recommendation: Use Intel CPUs based on "Nehalem" architecture for higher performance. * Note G.729 impact: A single G729 channel consumes as much as three G711 channels.	

- RadiSys Convedia CMS-1000

This media server is the cost-effective, entry-level member of the family of RadiSys media servers. Although it is no longer orderable for new installations, the CMS-1000 is supported on OpenScape Voice. It is configured via its own administration system, which is accessed separately from the OpenScape Voice administration tools.

- RadiSys Convedia CMS-3000

This media server uses the same software as the CMS-1000, but it runs on an improved hardware platform. It offers the same interfaces and functionality as the CMS-1000, but offers significant advantages, such as increased port capacity and processing speed.

- RadiSys Convedia CMS-3000 SEC

This media server uses the same software as the CMS-1000 and CMS-3000, and runs on the same hardware platform as the CMS-3000. It offers the same interfaces and functionality as the CMS-3000; however, it facilitates a more secure infrastructure and better traffic control.

1.10 OpenScape Voice Applications

OpenScape Voice supports the following applications:

- OpenScape Xpressions: This application combines voice, fax, e-mail, and short message service (SMS) services on a Windows 2003 platform to provide a unified messaging system. Built using modular, scalable client/server architecture, OpenScape Xpressions can be configured to meet users’ individual communication needs.

- OpenScape Voice Assistant: This application is a Web-based call control and communication filtering application that enables users to manage incoming voice and e-mail communications from their desktop. It offers computer telephony integration (CTI) features such as click-to-dial, call logging, LDAP address book search, rules-based communication filters, and routing capabilities.
- OpenScape Contact Center: This contact center application provides an intuitive agent interface with powerful visual management tools. It also offers an attendant console desktop that includes the productivity features of the agent desktop and several attendant-specific features. Attendants can be located anywhere the IP network extends because the desktop integrates on top of the attendant’s SIP endpoint.

- CallTicket: This component of the Open Communications Solution for CRM solution suite is an enhanced attendant console offering when compared to OpenScape Contact Center Attendant. In addition to the standard call handling capabilities of an OpenScape Contact Center agent, Call Ticket attendants can park calls and camp on (also known as append) calls to a busy destination. CallTicket attendants can also:

- Monitor subscribers to determine idle or busy conditions and current forwarding status

  Set or clear call forward unconditional destinations for any subscriber
- HiPath Meta Management: This comprehensive management solution permits for unified administration of networks made up of HiPath real-time IP systems, applications, and industry-standard third-party products. It consists of Fault Management, User Management, Accounting Management, and QOS Management.

- HiPath Serviceability Platform for Applications (HiSPA): OpenScape Voice provides an interface to HiSPA, which is a network that allows Enterprise Services to install patches on the HiPath family of products in accordance with service contract agreements.

NOTICE:

HiSPA will be available in a future product release.

- OpenScape UC Application: This application is a high-functionality collaboration application that fits into an enterprise’s existing voice and data infrastructure, linking together telephones, voice mail, e-mail, text messaging, directories, calendaring, instant messaging and conferencing services.

- HiPath DAKS: With its superior flexibility and versatile possibilities to transmit and receive information, the Digital Alarm and Communication Server HiPath DAKS is a powerful solution for the automation and optimization of critical communication in emergency and crisis situations.

- DAKS offers connectivity to traditional PBX systems (via S0/S2M) as well as to VoIP/SIP systems (e.g. via Gbit Ethernet)

DAKS communicates with telephones (stationary, cell phones, DECT, WiFi), but also with pagers and PCs or PDAs via special WEB clients

DAKS takes calls and calls users direct, through-connects audio sources, and switches subscribers to bilateral calls or conferences

DAKS informs with voice announcements or display texts or SMS messages and delivers multimedia information (e.g. videos)

DAKS offers special emergency call functions in HiPath networks

DAKS communicates with host systems and external sensors or actuators

DAKS locates handsets as well as tags or medallions, both in DECT and in WiFi infrastructures

DAKS can control public address (PA) systems and many more

These capabilities enable HiPath DAKS to implement the following vast range of alarm, communications and security services:

Broadcasts and Alarms

Protective Staff Monitoring

Telephone Conferences

Announcement Services

One-Number Service

E-Mail Service (Mail2Phone)

For details, please refer to the HiPath DAKS documentation.

- Call Ticket (Concierge): Integration of the Call Ticket application with OpenScape Voice and OpenScape Contact Center creates a comprehensive Attendant solution with powerful call queueing, call transfer, monitoring and reporting capabilities. For details, please refer to the Call Ticket documentation.

1.11 OpenScape Voice Subscriber Endpoint Support

OpenScape Voice supports the following SIP subscriber endpoints. Contact your company representative about the third-party SIP endpoints available for use with OpenScape Voice.

- OpenScape Desk Phone CP100/200/205/400/600/: This family is part of a new generation of universal input-output devices for efficient business communications. The OpenScape Desk Phone CP is a universal solution for efficient and professional telephony. .

- OpenScape UC Application Personal Edition: This endpoint is an IP softphone for installation on notebook and desktop PCs. It has been released for operation under: Windows 7 (32 bits) only Professional, Ultimate and Enterprise Editions, Windows 8 (32bits) only Pro and Enterprise Editions ("N" editions are not supported), Windows 7 (64 bits) - only Professional, Ultimate and Enterprise Editions, Windows 8 (64 bits) - only Pro and Enterprise Editions ("N" Editions are not supported), Windows 10 (32 bits) - only Pro and Enterprise Editions ("N" Editions are not supported), Windows 10 (64 bits) - only Pro and Enterprise Editions ("N"Editions are not supported)

DLS enables software distribution and configuration of endpoints. DLS also supports plug-and-play operation.

Connection of analog endpoints—for example, analog telephones, modems, and fax machines—is performed using the Mediatrix 4102 or HiPath AP 1120 analog adapter.

1.12 OpenScape Voice Features Summary

This section provides a high-level overview of the features provided by OpenScape Voice. The individual features are described in detail in the corresponding functional areas of the present documentation, .e. g. *OpenScape Voice-based Call Forwarding Features*.

NOTICE:

Some features have dependencies to and interactions with other features. The Feature Interaction Tool available on the Unify Intranet under http://wiki.dev.global-intra.net/publishwiki/index.php/Feature_Interactions_Matrix_(FIM) allows registered Unify users to search for and display the descriptions of dependencies and interactions of all OpenScape Voice features, and to create a matrix covering all dependencies and interactions of these features.

SIP Subscriber Endpoint User Features

Keyset Telephony User Features

OpenScape Voice-based Call Forwarding User Features

Other User Features

Business Group Features

Other Group Features

Routing and Translation Features

Call Admission Control Features

QSIG Tunneling Features

CDR Features

Security Features

Serviceability Features

SIP Signaling Features

CSTA Support Features

System Functions and Features

In addition to the features provided by OpenScape Voice, local user features reside in SIP subscriber endpoints. Refer to the applicable user manual for information about those features.

Keyset telephone user features provide multiple line capability, and other associated functions, for a SIP endpoint configured as a keyset. Keysets are sometimes known as multiline telephones.

Any of the following SIP endpoints can be configured as keysets:

- OpenScape Desk Phone CP 100/200/205/400/600/600E/700/700X

A keyset telephone is configured with a primary line (also known as a prime line), which is the main DN of a keyset telephone associated with the device. A keyset telephone can also have additional secondary and phantom line appearances.

The following are the keyset telephone user features:

Audible ringing on rollover lines	Multiline appearance
Delayed ringing	Multiline origination and transfer
Direct station select	Multiline preference
Keyset operation modes	Phantom lines
Line focus	Preview
Line key operation modes	Visual indicators for line and feature key status
Line reservation	
Manual hold	

OpenScape Voice-based call forwarding user features provide a means to customize the handling of calls when a subscriber is unavailable to answer them. SIP endpoints also have local call forwarding features. Refer to the applicable user manual for information about those features.The following are the OpenScape Voice-based call forwarding user features:

Call forwarding—return	System call forwarding, internal/ external—all calls (CFSIE-all)
Call forwarding -- unreachable	System call forwarding, internal/ external—busy (CFSIE-busy)
Station call forwarding -- all calls	System call forwarding, internal/ external—do not disturb (CFSIE-DND)
Station call forwarding—busy line (CFBL)	System call forwarding, internal/ external—don’t answer (CFSIE-DA)
Station call forwarding—don’t answer (CFDA)	
Station call forwarding—fixed	
Station call forwarding—remote activation	
Station call forwarding—remote call forwarding	
Station call forwarding—time-of-day	

Station call forwarding—voice mail	

Other OpenScape Voice user features provide such capabilities as calling identity delivery and suppression, abbreviated dialing, redial, and call return features.

The following are the other user features provided by OpenScape Voice:

Anonymous call rejection	Last incoming number redial (LINR)
Call completion on busy subscriber/no reply (CCBS/NR)	Last outgoing number redial (LONR)
Call pickup—directed	Multiple contacts
Caller identity service	Music on hold
Calling identity delivery and suppression (CIDS)	Screening list editing
Click to answer	Simultaneous ringing
Conference, station-controlled	Station dialing
Customer-originated trace	Station speed calling
Directory number announcement	System speed calling
Directory number announcement	Teleworking
DLS mobility	Toll and call restrictions
Do not disturb (DND)	Transfer
Executive override	Transfer security
Feature status notification	Virtual DN
Hot desking	

The business group concept provides the basic capabilities for handling a group of subscribers associated with a single enterprise. It also permits OpenScape Voice to recognize the associations of the subscribers the group contains.

Business group features simplify such tasks as dialing plan administration, intragroup communication, and traffic measurements. The following are the business group features:

Attendant answering position (AAP)	Business group web portal
Business group access codes	Direct inward dialing (DID)
Business group account codes	Direct outward dialing (DOD)
Business group authorization codes	Distinctive ringing
Business group billing	Extension dialing
Business group department names	Group-level feature administration
Business group main number	Message detail recording
Business group numbering plan	Night bell call pickup
Business group traffic measurements	Station restrictions

Other group features pertain to pickup groups, which allows users to answer calls on behalf of one another; hunt groups, which permit calls to be routed to an idle line within a group of specified lines. The following are the other group features:

Call pickup—group	Hunt group—no answer advance
Feature profiles	Hunt group—overflow
Hunt group	Hunt group—queuing
Hunt group—make busy	Hunt group—stop hunt
Hunt group—music on hold	Hunt group—traffic measurements
Hunt group—night service	Uniform call distribution (UCD)

Routing and translation features provide such capabilities as public numbering plan compliance and routing that varies depending upon such factors as origin, traffic, and time of day. The following are the routing and translation features:

A-side signaling-based routing	Media server digit map management
Alternate routing	North American Numbering Plan compliance
Alternate routing with overflow among route types	Numbering plans, business group
Call diversion for invalid destinations	Origin-dependent routing
Cost-effective routing	Rerouting based on SIP response codes and WAN outages
Digit modification for digit outpulsing	Source-based IP routing
E.164 compliance	Subscriber routing options
ENUM (electronic number mapping)	Time-of-day routing
Intercept treatment	Vertical service codes
International translation support	Voice VPN
Leading digit and most-matched digit translation	

The integrated call admission control (CAC) features provide for management of the bandwidth used for the transport of media traffic (such as RTP audio, T.38 fax, and video) through the bottleneck links that may exist in an enterprise network. This feature ensures that real-time media calls are only established when the necessary bandwidth resources are available on all access links that exist between the two communicating endpoints.

The following are examples of the functionality the call admission control feature provides:

CAC rerouting to SIP subscribers or alternate SIP gatewaysCall denialDynamic handling of link failures

QSIG tunneling features support SIP-Q, which permits OpenScape Voice to interwork with another OpenScape Voice system, the OpenScape 4000, the HiPath 3000, or a QSIG PBX.

CDR features simplify call tracking and billing for OpenScape Voice. The following are the CDR features:

Call detail record generation	
Intermediate long duration records	
Message detail recording	
Usage reporting	

Security features provide security for various aspects of the system, such as billing records, data files, and administration interfaces. The following are the security features:

Account and password management security	OpenScape Voice Assistant security
Billing records security	Provisioning and security logging
Data file security	Secure CLI
Defending denial of service attacks	Secure Shell on the OpenScape Voice Assistantinterface
Event logging	Secure storage of CDR password
File transfer security	SIP privacy mechanism
Hypertext transfer protocol over SSL	TLS support—network connections
IPsec baseline	TLS support—subscriber access
Login categories	Virus protection
Media stream security	VLAN provisioning

These features provide mechanisms to improve serviceability, such as diagnostics and debug tools, code controls, and administrator controls. The following are the serviceability features:

Administrator identification and authentication	Process debug tool
Backup and restore	Query of subscriber transient operational status
Basic traffic tool	RapidStat
Call trace	Real-time trace
Continuous trace	Remote patching
Database versioning	Remote restart
Maintenance manager	System software and patch level status
Mass provisioning	System upgrade
On-demand audits	

These features support SIP signaling and the interworking with other elements such as application servers, voice conferencing applications, and voice mail systems. The following are the SIP signaling features:

Application-provided billing party	Interworking with Microsoft OCS Mediation Server

Application-provided call correlation	Interworking with OpenScape SBC
HTTP digest authentication	Interworking with SIP service providers
Integration with CallTicket	Interworking with unified messaging systems
Integration with Microsoft Exchange 12 unified messaging server	Interworking with voice mail systems
Integration with OpenScape Contact Center	SIP privacy mechanism
Integration with OpenScape Xpressions	SIP REFER method support
Integration with OpenScape V2.3	SIP session timing
Integration with OpenScape UC ApplicationV3	SIP UA registration renewal during WAN outage
Integration with OpenScape VoiceLink	
Interworking with application servers	

OpenScape Voice provides a standard European Computer Manufacturers' Association (ECMA) Computer Supported Telecommunications Applications (CSTA) protocol interface to external CTI applications, which permits applications such as the OpenScape UC Application, and OpenScape Contact Center to control the OpenScape VoiceSIP endpoints.

The following are examples of the functionality the CSTA support features provide:

CSTA services support	Message waiting indicator
Application-provided caller identification	One number service
Flexible digit processing	OpenScape Voice-provided calling name
Integration with Fault Management	Private network number support

These features that support such tasks as alarm reporting, message waiting indicator control, and recovery handling. The following are the system functions and features:

Agent for OAM&P	Media server support
Alarm reporting	Message waiting indicator
Announcements	Multiple language announcements
Data synchronization	Multiple time zone support
Display number modification	Overload handling
Emergency calling	Recovery handling
Feature execution for unreachable subscribers	SDP transparency
Internal audits	Silence suppression disabling

Interworking with automated attendant systems	SOAP interface
Local management	System history log
	T.38 fax support

1.13 OpenScape Voice System Performance and Capacities

Assumptions

The performance criteria were measured under controlled lab conditions to ensure consistency across platforms. Where accurate measurements are not yet available, an indication is given which explains whether the figure being quoted is an estimate, an expectation, or derived in some other way.

Call Modeling Criteria

A call model is characterized as a selection of signaling protocols (for example, SIP and MGCP) and traffic patterns. The subsequent table lists the protocols used by OpenScape Voice and where they are used.

Table 5: OpenScape Voice Protocols

Protocol	Used for Subscriber Lines	Used for Trunks (Gateways)	Used Inter-Switch	Comments
SIP	X	X	X	
SIP-Q		X	X	OpenScape 4000, HiPath 3000, OpenScape SBC, interswitch
CSTA	X			Interface to OpenScape UC Application, and OpenScape Contact Center
MGCP				Media server only

Performance as a Function of Number of Messages

The assumption of the call performance model is that the usage of OpenScape Voice processing power of each call and each feature is related to the number of external messages (in and out). Therefore, the only inputs for the performance prediction are: The number of additional messages for each feature usage per half-call

- The number of messages per protocol type for each line and trunk half-call
- The number of additional messages for each feature usage per half-call

Overall Performance

Depending on the hardware platform, the OpenScape Voice server is capable of the following busy hour call rates in a SIP tandem switching configuration:

- IBM x3650 T: More than 150 calls per second
- IBM x3250

These rates are applicable in an environment that consists only of SIP endpoint-to-endpoint calls, with no features configured.

However, the actual call rate depends on feature configuration and usage. When subscriber features such as keyset operation, CSTA, SIP-Q, TLS, CAC, and pickup groups are heavily used, the supported call rate can be as low as 30 calls per second for the x3650 T.

If an enterprise requires a busy hour call rate higher than these stated rates, Unify Engineering or Technical Sales should be consulted for a detailed analysis.

System Capacities

Table 6: System Capacities

Parameter	OpenScape Voice Standard Duplex	OpenScape Voice Integrated Simplex/Duplex	OpenScape Voice Entry
TCP Connections	327681[1]	5000	800
TLS sockets	50000	5000	800
Unique keyset DNs	100000	5000	800
Average Keyset line appearances	2	2	2
Maximum simultaneous line appearances on a keyset phone[2]	10	10	10
Business Groups	6000	600	100
Numbering Plans	5999	600	100
Total trunks (SIP and SIPQ) Standard PBX*	60000	5000	2500
Total trunks (SIP and SIPQ) Tandem*	60000	5000	400
Total SIPQ-Q trunks*	20000	5000	800
Prefix Access Codes	35000	18000	9000
Destination Code table entries	200000	10000	5000

Parameter	OpenScape Voice Standard Duplex	OpenScape Voice Integrated Simplex/Duplex	OpenScape Voice Entry
Destinations (two routes per destination average)	54000	27000	14000
Route Lists	54000	27000	14000
Routing Areas	30000	15000	7500
Classes of Service	30000	15000	7500
Number of Hunt Groups	25000	1250	200
Hunt Group size	2048	200	100
Hunt Group memberships per subscriber	32	32	32
Number of Pickup Groups	10000	1000	100
Pickup Group size	64	64	64
Pickup Group memberships per subscriber	1	1	1
Maximum Station Controlled Conference participants	16	16	16
Feature Profile per subscriber	1	1	1
Simultaneous SIPQ calls half calls (max.)	20000	5000	800
Simultaneous SIPQ calls tandem (max.)	10000	5000	400
Simultaneous SIPQ calls (SIP + SIPQ)	60000	5000	2500
OS Voice Users/ UC Users		700/300 for IBM3650T	600/200
Note: Some of the numbers are extrapolated from Standard installation.			
* Recommended limits, not enforced			

<table>
<tr><th>Parameter</th><th>OpenScape Voice Standard Duplex</th><th>OpenScape Voice Integrated Simplex/Duplex</th><th>OpenScape Voice Entry</th></tr>
<tr><td colspan="4">[1] - The number of TCP connections per OpenScape Voice node is 16348
- During normal operation within an OpenScape Voice Standard Duplex system all users within a branch may be supported by a TCP connection established per branch proxy or proxy (SBC). - If a survivable branch proxy is used, a TCP connection may be required for each user or gateway to continue operation when the proxy is bypassed by OpenScape Voice.- Branch gateways may be supported using the same branch TCP connection unless the gateway requires dynamic registration. - Each local TCP user within the OpenScape Voice datacenter requires a TCP connection.- When a central SBC is deployed, a TCP connection may be required for each branch, branch gateway, gateway or remote user.</td></tr>
<tr><td colspan="4">[2] Each keyset is assigned a primary line, also known as the prime line, and can be assigned up to 10 lines or more, depending on the endpoint type. The primary line is the DN for that keyset. The primary line and each secondary or phantom line are assigned to separate line keys. A keyset cannot have a line appearance of a DFT.</td></tr>
</table>

MTBF of Hardware

Including installed PCI cards and the shared disk arrays, the calculated hardware availability for two nodes is 99.9997%.

Number of Ethernet Interfaces

For the OpenScape Voice non redundant system, the IBM x3650 Tare equipped with five 100/1000BaseT Ethernet ports; for a redundant system, each node has nine ports.

Refer to the corresponding sections in the present documentation for more information.

1.14 OpenScape Voice Statistics, Accounting and Diagnosis

Statistics and Accounting Measurements

Operational Measurements

Diagnostics

OpenScape Voice allows access via CLI to data from various performance counters and statistics. This data can be displayed in its native form. It can also be extracted by external applications to generate reports useful for the enterprise customer's ongoing management and monitoring of OpenScape Voice.

Performance counters and statistics are provided for the following entities

- Operational measurements (OM)
- CDR system

- UCE performance data—completed call, terminated call, and interworking call statistics
- SIP performance data—messages sent and received by client and by server
- Message counters
- Errors in transaction portion—message type, general problem, invoke problem, return result problem
- Audits and recovery performance data
- Overload handling performance data for SIP and MGCP
- Services performance data

  Anonymous call rejection
  Call forwarding (OpenScape Voice-based)
  Calling identity delivery
  Extension dialing (sometimes known as intercom call)
  Screening list editing
  Speed calling
  Toll-free
  Voice mail

The operational measurements (OM) features enable administrators to monitor the performance and usage of OpenScape Voice resources, including network traffic management (NTM) code controls and business groups. In addition to viewing usage data through OpenScape Voice Assistant, this data is stored in OM files on the OpenScape Voice server.

OpenScape Voice provides traffic measurements that are collected and recorded as CSV files by the operational measurements manager (OMM). The files may then be downloaded through secure FTP to any platform associated with the collection of performance data. The files may be transferred in either binary or ASCII format.

The following types of traffic measurement data are collected:

- Event-based traffic measurements: These measurements are cumulative, and are driven by specific event occurrences such as successful calls, call failures, and any kind of state transition. This type of traffic data is measured for each business group by using the following peg usage counters:

  Originating calls
  Terminating calls
  Intragroup calls
  Feature usage
  Feature activation
  Feature deactivation
  Dial 8, Dial 9 Calls
  Direct Inward Dialing (DID)
  Attendant attempts
  Attendant overflows
- Usage-based traffic measurements: These measurements are based on the cumulative duration of a specified event or condition. This type of traffic data is measured for each business group by using the following usage register counters:

  Intragroup usage
  Originating usage

Terminating usage

The CLI and OpenScape Voice Assistantsupport test line origination (TLO) to run diagnostic tests on network connections.

The TLO tool allows service personnel to run test calls. These test calls utilize individual circuit paths and use signaling to test connections between OpenScape Voice and adjoining Class 4/5 switches. After the addressed switch performs the appropriate loopback or tone generation, the switch determines and reports the quality of the voice paths.

1.15 The OpenScape Voice Solution

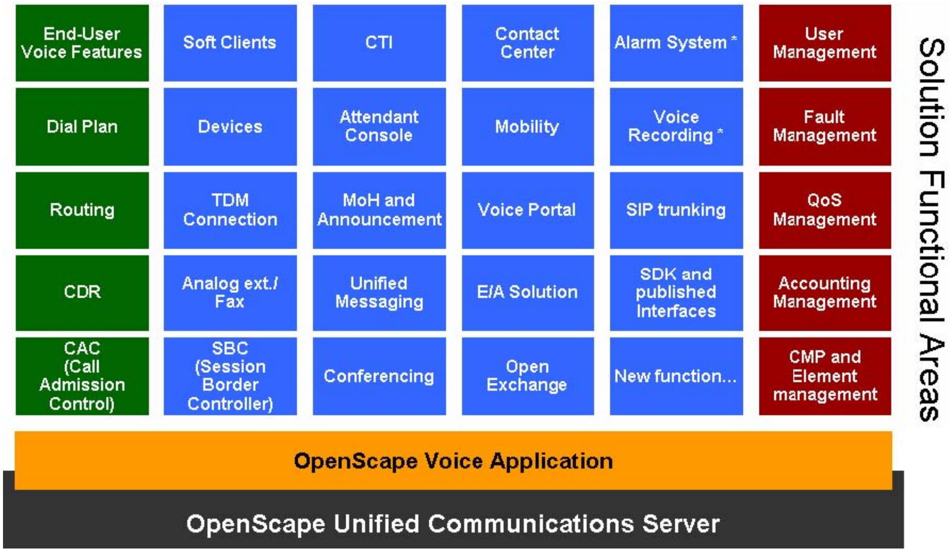
The OpenScape Voice Solution is a set of products, functionalities and capabilities that are put together to form a large ecosystem from which customer specific solutions can be derived. It delivers powerful communications functionality provided through a choice of components / products included in a rich solution set that builds the basis of the enterprise communications infrastructure. It is built around the OpenScape Voice Application and operates within the framework of the OpenScape UC Server.

OpenScape Voice Solution V10

OpenScape Voice Application

OpenScape Voice Solution V10 Functional Sets

The OpenScape Voice Solution strengthens customer choices in solutions for messaging, trunking/gateways, survivable branch solutions, applications, endpoints, interoperability through open standards and management.



End-User Voice Features	Soft Clients	CTI	Contact Center	Alarm System *	User Management
Dial Plan	Devices	Attendant Console	Mobility	Voice Recording *	Fault Management
Routing	TDM Connection	MoH and Announcement	Voice Portal	SIP trunking	QoS Management
CDR	Analog ext./ Fax	Unified Messaging	E/A Solution	SDK and published Interfaces	Accounting Management
CAC (Call Admission Control)	SBC (Session Border Controller)	Conferencing	Open Exchange	New function...	CMP and Element management

Solution Functional Areas

OpenScape Voice Application

OpenScape Unified Communications Server

Figure 7: OpenScape Voice Application and Functional Areas making up the OpenScape Voice Solution V7

The OpenScape Voice Solution V7 comprises the following:

- OpenScape Unified Communications Server

- OpenScape Voice Application
- OpenScape Voice Solution V10 Functional Sets

OpenScape Voice Application is a core component in the OpenScape Voice Solution V10. OpenScape Voice Solution is an ecosystem built around the OpenScape Voice Application.

OpenScape Voice is a native SIP real-time IP system designed to provide enterprises with a robust service creation and delivery infrastructure. Scalable to as many as 100,000 users per two active redundant servers, and a virtually unlimited number of users in a large network, OpenScape Voice can be deployed and managed as a world-class, lowest power consuming data center solution. Not only does it provide enterprise class communications functionality, but also reduces the associated CO2 footprint of the enterprise.

OpenScape Voice creates technology choices that allow customers to implement communication strategies at their own pace (e.g. voice and video communications). It is designed to provide architectural strength to such a framework through its scalability, resiliency, adherence to open standards, manageability and its ability to function powerfully as an IT / Data Center based communications solution.

- End-User Voice Features
- Dial Plan
- Call Detail Recording (CDR)
- Routing
- Call Admission Control (CAC)
- Soft Clients
- Devices
- TDM Connection
- Analog Extension/Fax
- Session Border Controller (SBC)
- Computer-Telephony Integration (CTI)
- Attendant Console
- Music on Hold and Announcements
- Unified Messaging
- Conferencing
- Contact Center
- Mobility
- Voice Portal
- Executive/Assistant Solution
- OpenExchange
- Alarm System
- Voice Recording
- SIP Trunking
- SDK and Published Interfaces
- User Management
- Fault Management
- Quality of Service (QoS) Management
- Accounting Management
- Configuration Management Portal and Element Management

2 Administration Concept

You administer the OpenScape communications solution preferably with your browser-based configuration interface – the Common Management Platform (CMP).

The available features of the Common Management Platform are divided into the following areas:

- General management features that you use to administer node-spanning system features of the OpenScape communications solution.
- Special management features that you use to administer system functions of selected system nodes.

General Management Features

- System Management

  Using the system management you can quickly gain an overview of the available system nodes and their logical grouping (clustering). Furthermore, it provides auxiliary means to configure these system nodes and to log this configuration.
- Domain Management

  With the domain management you can divide the OpenScape system into different domains. The system can be split into domains, where each domain corresponds to a separate administration area with independent administration rights. All users, resources and profiles in the system are assigned to precisely one domain and are not visible in another domain.

  NOTICE:

  OpenScape Voice can currently only be operated with one domain– the predefined system domain **system**.
- Profile Management

  The profile management enables you to administer the access privileges for the OpenScape system in a standardized way.
- User Management

  With the user management you administer the user accounts for administrators and system users.

  NOTICE:

  System users are only deployed when you also use OpenScape UC Application with your communications solution.
- Resource Management

  With the resource management you administer selected system resources that provide the different components of the OpenScape system.

- Contact List Management

  With the contact list management you administer contact lists that the users of the OpenScape system can deploy.

  > **NOTICE:**
  >
  > The contact list management is only required when you use OpenScape UC Application with your communications solution.

- License Management

  The legal use of the OpenScape system features requires licenses. You can use the license management to activate these licenses and to view activated license information.
- Alarms and Fault Messages

  The various OpenScape system components create alarms and error messages when detecting irregularities in the system. The associated alarm and error information is merged in the alarm and error messages.
- Logging

  Important OpenScape system data is recorded in the background and stored in log files.
- Audit Log

  The audit log logs all important activities performed by the users in the scope of the administration.
- Backup and Restore

  You can back up the system configuration and the system data of the OpenScape system in regular intervals or when required. You can use the information backed up in this way for restoring the OpenScape system.
- Import and Export

  You can import and export data of the system and domain administration.
- Software Repository

  In the Software Repository you can store and manage upgrade files for the different applications on an OpenScape system.
- Download Center

  In the download center you can centrally provide documents, general software and tools for users to download.

The general management features are always component of the Common Management Platform. Which of the features available therein are offered to you for administration depends on the access privileges assigned to your user account.

Special Management Features

You are provided with special management features via individual administration interfaces that integrate in the Common Management Platform interface. For example, by the OpenScape Voice Assistant with which you administer and configure the communications systemOpenScape Voice.

Special management features are only available in the Common Management Platform when the associated system component is used in your OpenScape communications solution. Which of the features available therein are then offered to you for administration depends on the access privileges assigned to your user account.

Further Management Aid

For administering a OpenScape communications solution the following further aid exist independently from the Common Management Platform.

- Local Management

  The local management provides a command line via which OpenScape Voice can be administered on site. The local management comprises configuration, monitoring and administration of the internal OpenScape Voice system software processes.
- Deployment Service (DLS)

  You can use the Deployment Service to manage the OpenScape Voice work points. The Deployment Service has a Java-supported, web-based user interface and is executed in a web browser.

  The Deployment Service can be executed on the OpenScape Voice system or externally on a separate Windows server. It is integrated in the OpenScape Voice Assistant to combine the tasks of creating a subscriber in the OpenScape Voice system and to add the endpoint information of the subscriber to the Deployment Service, performed as single task.

  The Deployment Service is required for supporting the mobility feature on Unify SIP endpoints. In particular, it provides options used for migrating existing workpoints and implementing standards for mobile users.
- Maintenance Manager (MMGR)

  The Maintenance Manager serves for activating and controlling OpenScape Voice maintenance jobs – for example, to back up and restore files.
- Agent for operation, administration, maintenance and provisioning

  The agent for operation, administration, maintenance and provisioning (OAM&P) realizes the OAM&P interface to the OpenScape Voice Assistant. Via this interface you handle all management jobs that concern the OpenScape Voice system.
- Generic Export Mechanism

  The Generic Export Mechanism (GEM) is used to synchronize data between OpenScape Voice and the CAP / CSTA interface.
- Various component individual command line tools

  You find lists and descriptions for these tools in the chapters of the related system components.

2.1 Operating the Common Management Portal (CMP)

The Common Management Portal is the browser-based configuration interface for the OpenScape communications solution. It provides general management features that you use to administer node-spanning system functions of the OpenScape communications solution, and also special management features that you use to administer system functions of selected system nodes.

The Common Management Portal user interface consists of HTML pages that can be displayed with a web browser. Thus the Common Management Portal works platform-independent under all prevalent operating systems.

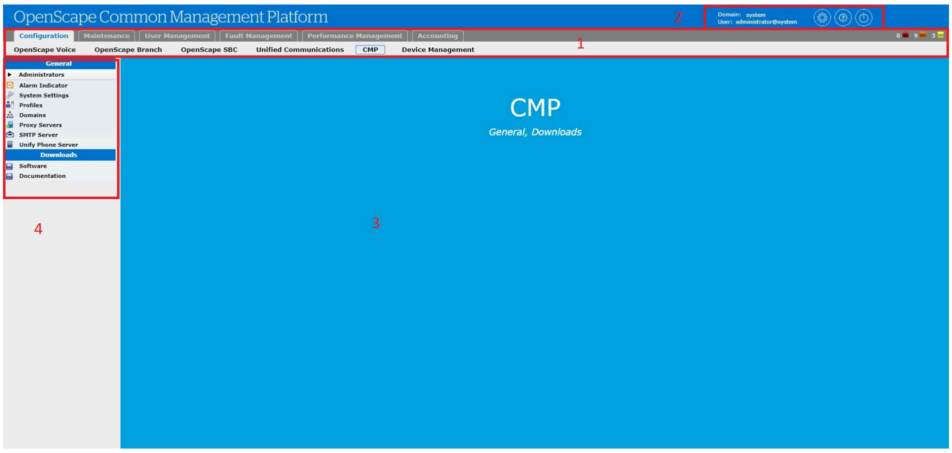
The Common Management Portal user interface is divided into the following areas:

1) Navigation bar

2) System bar

3) Work area

4) Navigation tree



You can adjust selected Common Management Portal elements to individual requirements.

The CMP is optimized for:

- Internet Explorer 7.0
- Internet Explorer 8.0 (compatibility mode)
- Internet Explorer 9.0 (compatibility mode)
- Internet Explorer 10.0 (compatibility mode)
- Internet Explorer 11.0 (compatibility mode)
- Firefox ESR45 (Extended Support Release)

NOTICE:

Using different versions of the browsers above may lead to rendering errors and/or limited functionality.

When using the Common Management Portal please note that you should set the web browser used in a way that it allows pop-ups in general or at least for the internet address under which the Common Management Portal is accessible.

2.1.1 CMP Work Area

The Common Management Platform work area lists comprehensive information and displays different activity options. The number and selection of information and activity items depends on the entry you have chosen in the navigation tree. The information area above each list displays a description of the information and actions.

The name of mandatory system settings are marked in bold text.

The work area contains the following general elements:

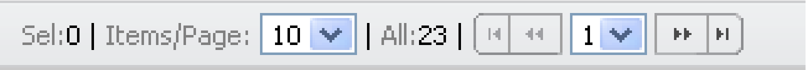
- Lists

  The work area displays the actual information about the entry selected in the navigation tree in the form of lists.

  You can sort the list elements in ascending or descending order.

  If a list cannot be completely displayed in the work area due to its length, it will extend over several pages.

  On pages that display a numerus amount of items you can customize the list according to your preference with the following options:



1) "Sel" :the amount of items ticked in the checkbox. This option appears only if a checkbox is available in the list
2) Items/Page: you can choose from the pull down menu the amount of (10,20,50,100,200) items displayed per page

   At the beginning of you Administrator user session all lists are initialized with the default value.

   Whenever you change the default items(rows)/page value (you have "customize" it) of a list in CMP this value is saved per Administrator User id, which means whenever you logoff and login CMP applies the value you have set for this list.

   You can preset the number of rows (items) /page for all the non "customized" lists and you can also force it to all lists, including "customized" lists as it is described in Section 3.2.2.1, "Settings"
3) All: total amount of items in the list
4) If the total amount of items exeeds the items/page slection then you can use the page navigator. Use << and >> to page forward and back in the list. Use |< and >| to jump to the beginning or end of the list. You can use the Page drop-down list to select a specific page

  You have the option to sort the list entries by clicking the title in the column headings. For this to be done the column headings must be highlighted in blue.

  If you click the column heading a second time, the sort sequence changes from ascending to descending or from descending to ascending.

  If you wish to mark all list elements, click in the gray list header row on the checkbox at the start of the row.

NOTICE:

The sorting is for the entire list not just the page you are currently on

- General Icons / Buttons

  The general icons and buttons shown in the work area are dependent on the selection of the entry in the navigation tree. The icons/buttons shown below are possible and have the following meanings:

Elemen	Function
ⓘ	**Information** icon Displays information about the topic represented in the work area in the information bar. A note also appears here when you enter the wrong value.
?	**Help** icon Invokes the help for the topic concerned.
↻	**Refresh** icon Updates the page shown (forexample, when displaying list entries).

- Information bar

  The information bar describes which information is currently displayed in the work area. If you enter an invalid value in an entry field, the information bar will also indicate the type of input error. The relevant entry field appears in a red frame.

- Action Menu

  You can use the action menu to initiate specific functions for a list entry in a list (e. g. edit a user). The action menu appears always on the right-hand margin of a list entry. Whether an action menu is provided in a list or not depends on the list selected. Most of the functions in the action menu can also be reached with the buttons displayed in the work area. In instances where there are two ways of initiating a function, this manual describes the button procedure.

Elemen	Function
▸	**Action Menu** icon Opens the action menu for the associated list entry

- Filter

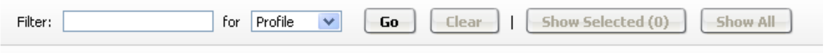
  You can use the filter function in the work area to filter displayed lists according to a specific search item. Setting a filter reduces the total number of items displayed and makes it easier to identify those desired.

  Within the search text only the wildcard * is allowed. It can be used instead of several arbitrary charcters. Logical operators are not supported.

  Besides filtering by a specific search term, it is also possible to select certain items with a check mark. These marked items can then be displayed with

Show Selected (). If this selective display is no longer desired, all items can be displayed again with **Show All**.

The filter function also supports the * wildcard search.



An advanced filter in which additional criteria can be selected for filtering the lists is available for alarms, error messages and audit logs. The criteria for the advanced filter are described in the associated sections.

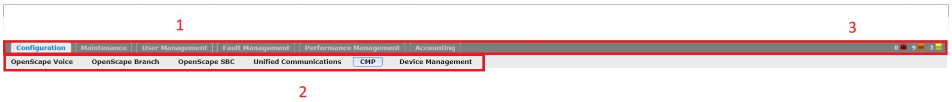
- Dialogs

  There are many work area elements that open additional dialogs in which you can set component-depending values. In these dialogs the names of the fields where entries are mandatory are bolded.

2.1.2 CMP Navigation Bar

In the Common Management Platform navigation bar you can see the different navigation tabs. Each navigation tab contains a navigation menu with different navigation menu options.

The OpenScape applications installed on your OpenScape system and the access privileges of your user account determine which navigation tabs and navigation menu options you see.



The navigation bar contains the following elements

1) Navigation tab

When you click a navigation tab, the menu items assigned to the tab appear in the navigation menu. The default navigation menu item assigned to the tab is highlighted. The navigation tree belonging to the menu item appears on the left in the browser window, while the work area displays the associated home page.

2) Navigation menu

When you click a navigation menu item, the navigation tree opens and the default entry assigned to the menu item is highlighted. The home page is displayed in the work area.

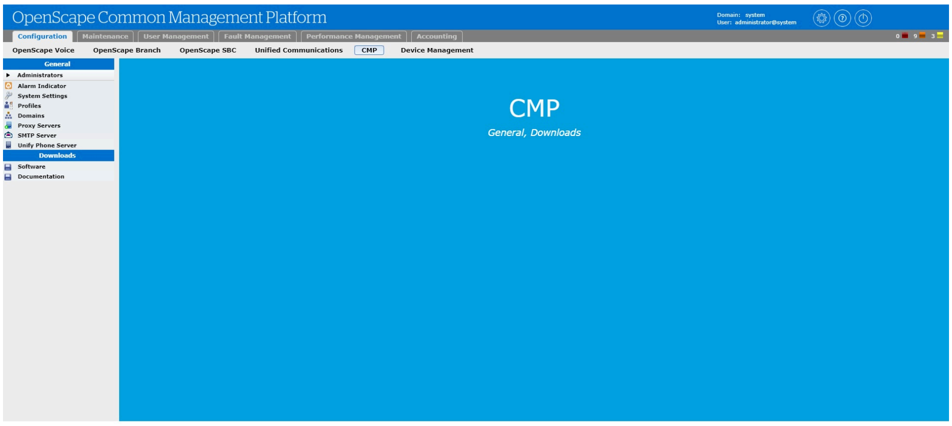
3) Alarm Preferences

The three most crucial alarms types are depicted. Critical, Major and Minor alarm appear in their respective colour.

2.1.3 CMP Navigation Tree

For each navigation menu option the associated navigation tree opens next to the work area in the Common Management Platform. The tree contains all topics that belong to the selected navigation menu option.

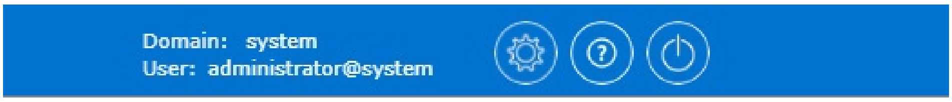
If you click a navigation menu item, a navigation tree unfolds in the navigation area to the left; in the workspace, the home page for the selected navigation menu item is displayed. The navigation tree contains all entries associated with the current navigation menu item. Some individual entries are grouped and you can display or hide these groupings. The name of the navigation menu item is repeated once more at the top of the navigation tree. To hide the entries, click the "down arrow" icon in the group name. The entries disappear and a "right arrow" icon is displayed. Click the right arrow icon to display the entries again. When you click one of the displayed subitems, the associated page is displayed in the workspace. .



Domain: system
User: administrator@system

2.1.4 CMP System Bar

On the Common Management Platform system bar you can see the domain you are looged in and the user ID with which you are logged in at the Common Management Platform.



Domain: system
User: administrator@system

The system bar contains the following elements.

1) Name of the current user

Displays the user ID with which you are logged in at the Common Management Platform.

2) Menu bar

When you click an option in the menu bar, a list of further menu options appears. The menu options comprise functions which are common to all applications, as well as further entries which depend on the installed applications and your administrator rights.

For the Common Management Platform the following menu entries can be available:

- **Settings** > **General**

  Defines basic CMP settings for the logged in administrator.
- **Settings** > **Change Password**

  On this tab you can change your user password for the CMP. This is only possible if your user profile is set up accordingly (Symphonia Administrator).
- **Help**

  Opens the online help.
- **Logout**

  Log-out the logged on administrator from the Common Management Platform.

2.1.5 Adjusting the CMP User Interface

You can adjust selected Common Management Portal elements to individual requirements.

Within this scope, you can customize the following Common Management Portal interface elements:

- The Unify logo in the Common Management Portal login dialog
- The Unify logo on the Common Management Portal user interface
- Interface texts based on OpenScape product names
- Various general interface texts

For changing such interface elements there is the `rebrand.sh` script. The configuration settings for this script are stored in the associated configuration file `input`.

During the Common Management Portal installation, the `rebrand.sh` script and its configuration file `input` is stored in the following directory:

<Osc#Install [1]>`/share/tomcat/webapps/management/`

If you operate the OpenScape system as integrated cluster system, you need to adjust the CMP user interface on both nodes.

After a Common Management Portal upgrade or after installing a software patch of the same main version, modifications once performed are maintained. A new installation via setup DVD, however, recreates the original logos, product and interface texts. In this case you need to execute the `rebrand.sh` script once again.

NOTICE:

A new configurator file is created on the folder `rebranding` when the `rebrand.sh` script has completed successfully.

[1] <Osc-Install > is the setup directory of the OpenScape system: /opt/siemens/ or /enterprise/

This configurator file contains the flag **bluewash** which is marked as **on** when the `rebrand.sh` script is finished. During an upgrade or during installing a software patch of the same main version the system checks the flag **bluewash**. If it is set to **on** the `rebrand.sh` script is automatically executed after the update process in order to maintain the modifications. If the flag **bluewash** is set to **off** the software update reset all modifications to their default.

The `input` configuration file

The `input` configuration file contains the settings for all changeable interface texts. The following tables give an overview of these settings.

NOTICE:

If you change texts in the configuration file `input`, please do not remove blanks from the settings identifiers.

Table 7: Rebrand script parameters for brand and product names

Settings identifier	Assigned interface text
__BRAND_NAME__	Brand name in different pop-up messages
__OS_VOICE__	Product name for the OpenScape Voice component
__OS_BRANCH__	Product name for the component OpenScape Voice Branch

The following restrictions apply for brand and product names:

- The value of each setting must be one to 20 characters long.
- The value of each setting may contain the following characters of an English or German keyboard:
  - a – z and A – Z
  - 0 – 9
  - Special characters can be provided on the input file, some of them must be protected with single quotes, others with double quotes and other with nothing according to the first two columns of the following table, last column displays characters that are not supported by the input file:

Supported Special Characters:	Used as:	Special Characters NOT supported
!	‘!’	/
@	“@”	\
#	“#”	=
%	“%”	^
&	“&”	$
(	“(“	.
)	“)”	*

Supported Special Characters:	Used as:	Special Characters NOT supported
_	_	[
-	“-“	]
+	“+”	“
{	“{“	,
}	“}”	`
|	“|”	<
:	“:”	>
;	“;”	
~	“~”	
?	“?”	
‘	“ ‘ ”	

- The value of each setting may contain the following additional characters of a German keyboard:
  – ä, ö, ü, ß, μ, €

NOTICE:

If you wish to use special characters in the `input` configuration file, you need to back up the file in the UTF-8 format. You can use e.g. the Microsoft Editor (Notepad) for this purpose.

The following areas exist for these brand and product names in the configuration file.

- The definition area, in which the settings to be newly used are defined under the above identifiers.
- The area for the settings of the last modification. The identifiers of the associated settings begin with `OLD`. After you have executed the `rebrand.sh` script, the settings of the definition area are automatically copied into this area.
- The area for default settings. The identifiers of the associated settings begin with `DEFAULT`. Here the settings are defined with which the Common Management Portal was shipped. Never change the settings in this area as they may be needed for restoring the default values for the Common Management Portal.

Table 8: Other rebrand script parameters

Settings identifier	Assigned interface text
FOOTER	Text of the trademark note in the Common Management Portal footer

Settings identifier	Assigned interface text
Framework.alarmDisplayString	Original identifier for the OpenSOA framework in the alarm protocol and for active alarms
Framework.alarmFilterDisplayString	Original identifier for the OpenSOA framework in the alarm protocol filter
INFORMATION_LINK	Is not yet used on the Common Management Portal user interface.
PRIVACY_LINK	Is not yet used on the Common Management Portal user interface.
dc_bcpath	Is not yet used on the Common Management Portal user interface.
alarms.sourceFramework	Original alarm identifier for the OpenSOA framework in the alarm protocol filter
COPYRIGHT	Is not yet used on the Common Management Portal user interface.
editProfile.H8kAst	Application identifier for the associated user profiles
editProfile.OpenBranchAssistant	Application identifier for the associated user profiles
ApplicationOverview.OSVOICE	Identifier for the OpenScape Voice connection on the application side
importExportCentralized.ExportOscVoice	Internal identifier for the import / export functionality

The value for the following miscellaneous settings must not exceed 20 characters:

- editProfile.H8kAst
- editProfile.OpenBranchAssistant

2.2 User Accounts for Administrators

You need to log on to the CMP with an administrator account for administering the OpenScape communications solution therein. The administrator accounts are managed in the Common Management Platform with the help of the domain management, user management, user profile management and access control lists.

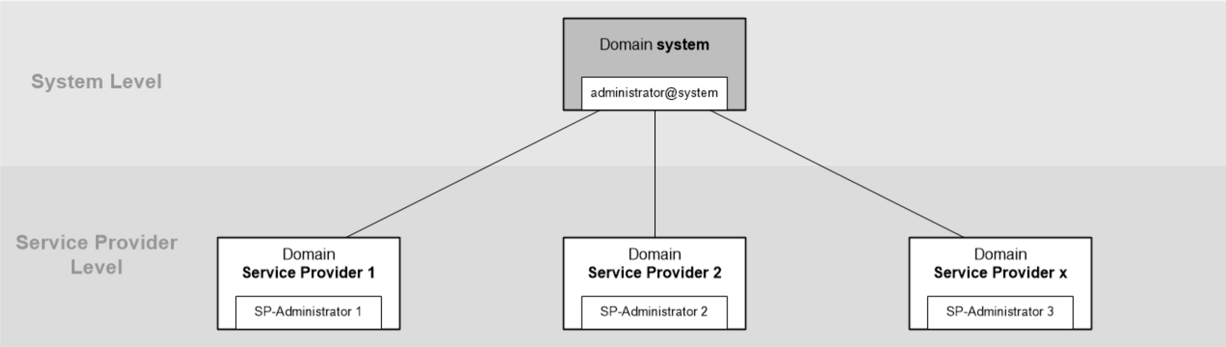
2.2.1 Domain Management

With the domain management you can divide the OpenScape system into different domains. The system can be split into domains, where each domain corresponds to a separate administration area with independent administration rights.

NOTICE:

OpenScape Voice can currently only be operated with one domain– the predefined system domain **system**. To organize the access rights of OpenScape Voice subscribers you can use access control lists.

The following figure describes the domain concept.



The domain concept divides into the following levels.

- System level

  On the system level exists the defaulted domain **system** with the default administrator **administrator@system**. This defaulted administrator can configure service provider domains and define further administrators and service provider administrators. You cannot delete the **system** domain.

- Service Provider Level

  On the service provider level exist service provider domains that can be created by the administrators of the system level. When an administrator creates a new service provider domain, he/she also becomes service provider administrator of the new service provider domain by default and is thus a foreign user for this domain. If an individual administrator is configured for the new service provider domain, he/she can withdraw the administrator privileges for the relevant service provider domain from the foreign user.

  A service provider administrator can define further administrators on the service provider level.

Domains can only be added, edited and deleted by administrators who have the **Domain Management** privilege.

2.2.2 Profile Management

The profile management enables you to administer the access privileges for the -OpenScape system in a standardized way.

A profile consists of a collection of access privileges. By assigning such a profile to an administrator, you grant this person all access privileges of the relevant profile.

Each user-profile is assigned to exactly one domain.

Furthermore, each profile is assigned to a specific application. This application determines which type of access privileges the profile contains. If a profile is e.g. assigned to the Symphonia application, it controls the access privileges for the features of the CMP – for example for the domain administration. For which applications user-profiles are available depends on the OpenScape components installed with the system.

To use the user-profile management for limiting the configuration scope of the Common Management Platform, the access privileges control the display of the menu options an administrator can see on the navigation bar or in the navigation tree. If, for example, an administrator has not been assigned the **Domain** privilege, he/she cannot see the **Domains** navigation menu on the **CMP** navigation tab.

We can generally distinguish three types of profiles.

- Default profiles
- System profiles
- Customer profiles

2.2.2.1 Default Profiles

Default user-profiles are automatically created upon the system setup. Default profiles are indicated with the icon in the Common Management Platform profile list and can neither be deleted nor modified. Which default profiles are altogether available in the Common Management Platform depends on the OpenScape components installed with the system.

Each default profile is assigned to a specific application. This application determines which type of access privileges the default profile contains. If a default profile is e.g. assigned to the Symphonia application, it controls the access privileges for the features of the Common Management Platform – for example for the profile or domain administration. For which applications default profiles are available depends on the OpenScape components installed with the system.

In the Common Management Platform, default profiles may be available for the following applications.

- CMP

  Provides the default user profiles for CMP.
- E / A Cockpit

  Provides the default user profiles for E / A Cockpit.

- OpenScape UC App

  Provides the default user-profiles for the access privileges of the OpenScape UC Application.

  NOTICE:

  TheOpenScape UC App is only available when you also use OpenScape UC Application with your communications solution.

- OpenScapeVoice

  Provides the default user-profiles for the access privileges of the OpenScape Voice Assistant.
- Symphonia

  Provides the default user-profiles for the access privileges of the Common Management Platform.

2.2.2.2 Default Profiles of the CMP

Common Management Platform application contains all the necessary permission to control the access to the various CMP features.The default profiles for the CMP are automatically created during the CMP setup and can neither be deleted nor modified.

Following profiles are installed automatically with CMP:

- A profile named **Super Administrator** is created by default and contains all the CMP permissions except the ones that are linked with licenses
- A profile named **Service Technician** is created by default and contains all the CMP permissions except the ones that are linked with licenses
- A profile named **Customer Administrator** is created by default and contains all the CMP permissions except the ones that are linked with licenses, Profile and Domain Management, SSDP, Software and Documentation Downloads, Importing and Exporting files.
- A profile named **OS User Management Feature Package LDAP** is created by default and contains all the CMP permissions that are linked to the OS_UM_FP1 Licence
- A profile named **OS User Management Feature Package OS ILA** is created by default and contains all the CMP permissions that are linked to the OS_UM_FP2 Licence

NOTICE:

No other profiles will be automatically installed with CMP.

NOTICE:

The default CMP profiles can’t be edited.

Following profile handling is performed:

- For fresh/new installations the administrator account that is created automatically is assigned with the Super Administrator profile.

- For upgrades, the assigned profiles of the default administrator account are not modified.
- For upgrades, the assigned profiles of the default administrator account are not modified.
  1) The administrator that created the subdomain automatically becomes a foreign user in that subdomain
  2) This foreign user is automatically assigned the Symphonia/Administrator profile in the subdomain
  3) CMP assigns to this foreign user the profile CMP/Super Administrator in the subdomain

2.2.2.3 Default Profiles of the OpenScape Voice Assistant

The default user-profiles for the OpenScape Voice Assistant are automatically created during the OpenScape Voice Assistant setup. In the Common Management Platform profile list they are indicated with the OpenScape Voice application and the icon and can neither be deleted nor modified.

With the OpenScape Voice Assistant the following default user-profiles are installed. These profiles are administrator profiles that control access to the OpenScape Voice Assistant features.

- Customer Administrator
- Basic Administrator
- Security Administrator
- Super Administrator

An OpenScape Voice administrator must be able to access the Common Management Platform features also. This requires the assignment of a Common Management Platform user-profile that has sufficient access privileges to the administrator's user account.

The following table describes which Common Management Platform default user-profile must be assigned to the respective administrators for OpenScape Voice.

Default user-profile for OpenScape Voice Assistant	Minimum required default user-profile for Symphonia Application
Customer Administrator	CMP login
Basic Administrator	CMP login
Security Administrator	CMP login
Super Administrator	CMP login

User Management Levels

It is possible to create administrators with access restriction in the level of tabs within the Subscriber Management and Signaling Management menu. Each administrator will have either read access only or full access (Read/Write) or no access at all to a specific tab in these management screen, based on permissions per subscriber/signaling functional area.

Each tab in the Subscriber (Main Office or Branch Office)/Signaling main screen has an 1-to-1 association with the permissions provided. If the "Read" access is assigned to a profile, the tab associated with this permission is visible to the profile. If the "Write" access is granted for a tab then the "Read" access is automatically assigned and the user is allowed to view and modify the contents of this tab. If the "Read" access is not granted then the tab is hidden.

Buttons are also associated with the subscriber management permissions:

- The **Add**, **Clone**, **Delete**, **Change DN** and **Device Management** buttons require full access (all the permissions granted) in order to be visible to a profile.
- The **Registration Status** button requires **Connection (Read)** permissions in order to be visible to a profile.
- The **Transient Status** button requires **Main Office Subscribers (General-Read)** or **Branch Office Subscribers (General-Read)** permissions in order to be visible to a profile.
- The **Quick Add Subscriber** menu requires full access (all the permissions granted) in order to be visible to a profile.
- Based on the assigned subscriber permissions the administrator is able to view the corresponding tabs in the **Edit**, **Quick Edit**, **Bulk Edit** subscriber management screens.

> **NOTICE:**
>
> If a profile has Read only permissions the **Bulk Edit** button shall be deactivated.

Overview of the Access Privilege Assignment

The OpenScape Voice Assistant access privileges are available in the Common Management Platform profile management under the OpenScape Voice application.

The below table shows in detail how these access privileges are assigned to the OpenScape Voice Assistant default user-profiles by default.

Name and short description of the Common Management Platform privilege	Basic Administ	Custome Administ	Securtiy Administ	Super Administrator
Basic Management Allows access to the **OpenScape Voice** tab in the Common Management Platform.	✓	✓	✓	✓
Communication System Access List Allows viewing all systems in the communication system list and administering the list entries. The administrator need not be a member of the access lists for communication systems.			✓	✓

Name and short description of the Common Management Platform privilege	Basic Administ	Custome Administ	Securtiy Administ	Super Administrator
Communication System Management Adds the administrator to the communication systems access list.	✓	✓	✓	✓
Communication System Settings Allows editing the settings of the displayed communication systems.		✓		✓
Call Admission Control Allows administering the call admission control of the communications systems.				✓
Number Display Allows administering the display number modification.				✓
Global Numbering Plan Allows administering the following settings: • Translation • Destinations and routes • Endpoint management				✓
Business Group Access List Allows viewing all business groups and creating or deleting new business groups for all displayed communication systems. The administrator need not be a member of the business group access lists.				✓
Business Group Management Adds the administrator to the business group access list for all displayed communication systems.		✓		✓
Business Group Settings Allows administering all displayed business groups. Within this scope you can also edit special business group settings – e. g. feature profiles, endpoint profiles, hunt and pickup groups.		✓		✓
Directory Numbers Allows administering office codes and home directory numbers.		✓		✓

Name and short description of the Common Management Platform privilege	Basic Administ	Custome Administ	Securtiy Administ	Super Administrator
Number Display		✓		✓
Main Office Subscribers (General-Read) Allows view access of the content of tab **General** in the subscribers management menu.		✓		✓
General (Write) Allows view and modifications of the content of tab **General** in the subscribers management menu.		✓		✓
Display (Read) Allows view access of the content of tab **Display** in the subscribers management menu.		✓		✓
Display (Write) Allows view and modifications of the content of tab **Display** in the subscribers management menu.		✓		✓
Connection (Read) Allows view access of the content of tab **Connection** in the subscribers management menu.		✓		✓
Connection (Write) Allows view and modifications of the content of tab **Connection** in the subscribers management menu.		✓		✓
Routing (Read) Allows view access of the content of tab **Routing** in the subscribers management menu.		✓		✓
Routing (Write) Allows view and modifications of the content of tab **Routing** in the subscribers management menu.		✓		✓
Security (Read) Allows view access of the content of tab **Security** in the subscribers management menu.		✓		✓

Name and short description of the Common Management Platform privilege	Basic Administ	Custome Administ	Securtiy Administ	Super Administrator
Security (Write) Allows view and modifications of the content of tab **Security** in the subscribers management menu.		✓		✓
Keyset (Read) Allows view access of the content of tab **Keyset** in the subscribers management menu.		✓		✓
Keyset (Write) Allows view and modifications of the content of tab **Keyset** in the subscribers management menu.		✓		✓
Groups (Read) Allows view access of the content of tab **Groups** in the subscribers management menu.		✓		✓
Groups (Write) Allows view and modifications of the content of tab **Groups** in the subscribers management menu.		✓		✓
Features (Read) Allows view access of the content of tab **Features** in the subscribers management menu.		✓		✓
Features (Write) Allows view and modifications of the content of tab **Features** in the subscribers management menu.		✓		✓
Applications (Read) Allows view access of the content of tab **Applications** in the subscribers management menu.		✓		✓
Applications (Write) Allows view and modifications of the content of tab **Applications** in the subscribers management menu.		✓		✓
Main Office Endpoints Allows administering main office endpoints.		✓		✓

Name and short description of the Common Management Platform privilege	Basic Administ	Custome Administ	Securtiy Administ	Super Administrator
Branch Offices Access List Allows viewing all Branch Offices and creating or deleting new ones. The administrator need not be a member of the Branch Office access list.		✓		✓
Branch Office Management Allows administering OpenScape Branch		✓		✓
Branch Office Settings Allows administering the general settings of OpenScape Branch		✓		✓
Branch Office Subscribers (General-Read) Allows view access of the content of tab **General** in the branch office subscribers management.		✓		✓
General (Write) Allows view and modifications of the content of tab **General** in the subscribers management menu.		✓		✓
Connection (Read) Allows view access of the content of tab **Connection** in the subscribers management menu.		✓		✓
Connection (Write) Allows view and modifications of the content of tab **Connection** in the subscribers management menu.		✓		✓
Routing (Read) Allows view access of the content of tab **Routing** in the subscribers management menu.		✓		✓
Routing (Write) Allows view and modifications of the content of tab **Routing** in the subscribers management menu.		✓		✓
Security (Read) Allows view access of the content of tab **Security** in the subscribers management menu.		✓		✓

Name and short description of the Common Management Platform privilege	Basic Administ	Custome Administ	Securtiy Administ	Super Administrator
Security (Write) Allows view and modifications of the content of tab **Security** in the subscribers management menu.		✓		✓
Keyset (Read) Allows view access of the content of tab **Keyset** in the subscribers management menu.		✓		✓
Keyset (Write) Allows view and modifications of the content of tab **Keyset** in the subscribers management menu.		✓		✓
Groups (Read) Allows view access of the content of tab **Groups** in the subscribers management menu.		✓		✓
Groups (Write) Allows view and modifications of the content of tab **Groups** in the subscribers management menu.		✓		✓
Features (Read) Allows view access of the content of tab **Features** in the subscribers management menu.		✓		✓
Features (Write) Allows view and modifications of the content of tab **Features** in the subscribers management menu.		✓		✓
Applications (Read) Allows view access of the content of tab **Applications** in the subscribers management menu.		✓		✓
Applications (Write) Allows view and modifications of the content of tab **Applications** in the subscribers management menu.		✓		✓
Branch Office Endpoints Allows administering the endpoint settings of OpenScape Branch		✓		✓

Name and short description of the Common Management Platform privilege	Basic Administ	Custome Administ	Securtiy Administ	Super Administrator
OpenBranch Allows access to the **OpenScape Branch** tab in the Common Management Platform		✓		✓
Private Numbering Plan Access List Allows viewing all numbering plans and creating or deleting new ones. The administrator need not be a member of the access list for the numbering plan.		✓		✓
Private Numbering Plan Management Adds the administrator of all displayed communication systems or business groups to the numbering plan access list.		✓		✓
Private Numbering Plan Settings Allows administering numbering plans. This comprises the administration of the following elements of private numbering plans: • Translation • Destinations and routes		✓		✓
Business Group Reports Allows using statistics for business groups and MLHGs.		✓		✓
Directory Numbers Allows administering office codes and home directory numbers.				✓
ENUM Allows administering ENUM settings.				✓
Feature Management Allows administering the OpenScape Voice Feature Settings.				✓
Global Settings Allows administering the general OpenScape Voice settings and the signaling management.			✓	✓
Database Password			✓	✓

Name and short description of the Common Management Platform privilege	Basic Administ	Custome Administ	Securtiy Administ	Super Administrator
Node.cfg Parameters Allows administering EZIP setting screen (node.cfg parameters)			✓	✓
Other Global Settings				✓
Licensing Allows administering statistics intervals for dynamic, trunking and OpenScape mobile licenses. Furthermore, the created statistics can be displayed.				✓
MediaServer Allows administering the OpenScape Voice settings for Media Server.				✓
Signaling Management Allows administering the OpenScape Voice settings for Signaling Management.				✓
CSTA (Read) Provides read-only access to the pop-up CSTA Settings window.				✓
CSTA (Write) Provides full access (read/write) to the pop-up CSTA Settings window.				✓
Digest Authentication Provides full access (read/write) to the pop-up Digest Authentication window.				✓
SIP Provides full access (read/write) to the pop-up SIP Settings				✓
SIP-Q Provides full access (read/write) to the pop-up SIP-Q Settings window.				✓
TLS Provides full access (read/write) to the pop-up TLS Settings window.				✓

Name and short description of the Common Management Platform privilege	Basic Administ	Custome Administ	Securtiy Administ	Super Administrator
Basic Configuration Allows administering settings in the OpenScape Voice Assistant.	✓			✓

2.2.2.4 Customer Profiles

In addition to the default and system profiles, you can also create individual profiles– so-called customer profiles.

Customer profiles are indicated in the Common Management Platform profile list with the icon. You can use them to provide user groups with standardized privilege levels, which are adjusted to the requirements and the level of knowledge of the relevant users.

We recommend to exclusively use customer profiles as far as possible.

Every feature of CMP has a corresponding permission defined in order to allow/ restrict the access to this feature

Profiles containing sets of these permissions can be created in order to model the different Roles that the CMP Admin Users may have.The assignment of these profiles to CMP Admin Users is essentially equivalent with granting the permissions described by the Role to the CMP Admin User. In order for a feature to work properly, additional non-CMP permission may be required to be granted to a User (e.g. Symphonia permissions) reference.

- The CMP permissions are used primarily to restrict access to various CMP screens in the User Interface level
- CMP permission do not restrict the access to Assistant screens
- CMP permission do not restrict access to Symphonia services Export of configuration data

2.2.3 Special Handling of CMP Administrator Permission

Special handling of CMP Administrator Permissions is required in order to prevent the Admin Users from locking themselves out of the system and allowing them to regain access in case they are locked out of the system.

Following restrictions are applied to the CMP Admin User Permission:

- It is not allowed to remove this permission from the last, unlocked CMP admin User.

  This special handling is required in order to prevent the Users from locking themselves out of the system.
- **NOTICE:** An unlocked CMP Admin User account is neither explicitly locked nor locked due to too many unsuccessful logins

- It is not allowed to remove this permission from a CMP application Profile ONLY IF there is at least one other CMP application profile that contains this feature AND there is at least one, unlocked CMP Admin User that has this profile assigned.

  This special handling is required in order to prevent the Users from locking themselves out of the system when modifying Profiles.
- It is possible for an administrator to login to the CMP server using ssh and as root user execute the following script :

  ```
  #./opt/siemens/servicetools/security/resetUserAccount.sh

  resetUserAccount.sh <userURI> <new passphrase> [<path to
  installation directory>]
  ```

  This script will create the Super Administrator Profile with the default configuration and assign it to a specific symphonia user.

  This special handling is required in order to allow the administrator to regain access to CMP Admin Users Management in case s/he is locked out of the system by an operation that is not covered by the above two rules.
- It is possible for an administrator to explicitly lock an administrator. In this case, the system does not make any effort to protect the User from locking themselves out of the system. The administrator has to login to the CMP server using ssh and as root user execute a script that will unlock the locked user in order to regain access to CMP.

  The same applies when the administrator is locked out of the system due to too many unsuccessful login.

2.2.4 UC User Administration

With the UC user management you administer the UC user accounts for the OpenScape system. This comprises in particular the user-individual contact information and access privileges.

Each UC user account specifies information about the following areas:

- General information
- Password/PIN
- Contact information
- Profiles
- Resources

These areas contain the following information:

General information

Information	Meaning
Login name	Specifies the user ID of the user account. The user deploys the user ID when logging on to the system. The following special characters must not be used for the user ID: • @-character • Semicolon • Blank at the beginning or end of a login name
Domain	Default value is system
Display Name	Specifies the name displayed for the user account in the program's interface.
Home time zone	Specifies for the user account the date and time default format in the program interface of OpenScape UC Application.
Default language	Specifies the following for the user account: • The language in which the web client program interface appears after the user has logged in. • The language in which the voice portal plays greetings after the user identification.
Address Translation Context	You can choose from the available Address Translation Contexts or configure another Address Translation Contexts in the Configuration section of UC.
User locked	Locks the user account out of the OpenScape UC Application.

Password/PIN

Information	Meaning
Login password locked:	Shows whether the password-based access via the UC user account has automatically been locked. If the access is locked, the relevant user has entered an incorrect password too often while trying to log in.
Telephony PIN locked:	Shows whether the telephone-based access via the user account has automatically been locked. If the access is locked, the relevant user has entered an incorrect PIN too often while trying to log in.
Login Password	Specifies a new password for the user account. Passwords are assigned according to different policies that apply to the entire system.

Information	Meaning
Login Password never expires	Specifies that the password is infinitely valid. If the **Password never expires** and **User has to change password at next login** options are active at the same time, the relevant user needs to change his/her password at the next password-based login. The changed password is then infinitely valid.
User has to change login password at next login	Specifies that the relevant user needs to change the password at the next password-based login. This option is only valid until the next password-based login. After the login this option is disabled for the user account again. If the **Password never expires** and **User has to change password at next login** options are active at the same time, the relevant user needs to change his/her password at the next password-based login. The changed password is then infinitely valid.
New Telephony PIN	Specifies a new PIN for the user account.
Telephony PIN never expires	Specifies that the PIN is infinitely valid. If the **PIN never expires** and **User has to change PIN at next login** options are active at the same time, the relevant user needs to change his/her PIN at the next PIN-based login. The changed PIN is then infinitely valid.
User has to change telephony PIN at next login	Specifies that the relevant user needs to change the PIN at the next PIN-based login. This option is only valid until the next PIN-based login. After the login this option is disabled for the user account again. If the **PIN never expires** and **User has to change PIN at next login** options are active at the same time, the relevant user needs to change his/her PIN at the next PIN-based login. The changed PIN is then infinitely valid.

Contact information

Contains comprehensive contact information about the user of the user account.

Profiles

Lists all user profiles that are assigned to the user account.

Resources

Lists all resources that are assigned to the user account. These can be:

- Voicemail number

  OpenScape UC Application uses a workflow for incoming calls. This workflow always ends in the voicemail box of the called user. In this way no call is lost even if the called user cannot answer the phone. The voicemail number specifies the number of the called user´s voicemail box.
- Queue number

  Specifies the number of a multi-line hunt group used for the Ask-Me feature.
- User devices

  Specifies the subscribers associated to the user. If you use OpenScape UC Application one of these subscribers can be set as ONS number.

2.2.5 Policy for User Passwords

You can define system-spanning requirements, CMP administrator and/or UC user passwords have to satisfy.

IMPORTANT:

The password policy is applied per Server, so if the UC application and CMP are located on the same server they will have the same password policy

To comply with the default requirements a CMP administrator and/or UC user password must:

- comprise at least eight characters
- contain at least one capital letter
- contain at least one digit
- contain at least one special character
- contain each character not more than three times in succession

Furthermore, the following applies by default:

- Each user must change his/her password after 90 days at the next password-based login.

  NOTICE: This system-spanning setting can be disabled for the respective UC user. If this is desired, activate the **Telephony PIN never expires** option on the **Password / PIN** tab of the relevant UC user settings.
- A CMP administrator and/or UC user must not enter an incorrect password more than five times. If this number is exceeded, his/her user account is automatically locked for password-based access.

  Locking the password-based access does not influence the PIN-based access of the relevant UC user via telephone.
- The last five passwords of a CMP administrator and/or UC user are stored in a password history. An CMP administrator and/or UC user cannot configure a password that is contained in the password history.

You can adjust these policies, valid for the entire system, in the following XML file:

`PassphrasePolicyConfig.xml`

You find this file in the following folder of the computer system set up on CMP server:

`/opt/siemens/respectively/enterprise/common/conf/`

Extract from the file `PassphrasePolicyConfig.xml`

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<PassphrasePolicyConfig version="2.0">
   <PassphrasePolicy>
      <Type>pwd</Type>
      <MinimumAge>86400000</MinimumAge>
      <MaximumAge>7776000000</MaximumAge>
      <MinimumLength>8</MinimumLength>
      <MaximumLength>0</MaximumLength>
      <MinimumDigits>1</MinimumDigits>
      <MinimumSpecialCharacters>1</
      MinimumSpecialCharacters>
      <MinimumUpperCaseCharacters>1</
      MinimumUpperCaseCharacters>
      <MaximumRepeatedCharacters>3</
      MaximumRepeatedCharacters>
      <MaximumFailedAttempts>5</MaximumFailedAttempts>
      <PasswordHistoryDepth>5</PasswordHistoryDepth>
      <LockoutTime>1800000</LockoutTime>
   </PassphrasePolicy>
   ...
```

The following parameters of this XML file control the user password policies valid for the entire system.

- **MinimumAge**

  Specifies the period after a password alteration in which a user must not change his/her password again. This period is only effective between two password modifications performed by a user himself/herself. If the administrator resets the user password, the relevant user can immediately change his/her password.

  The set value is evaluated in milliseconds.
- **MaximumAge**

  Specifies the period after which a user must change his/her password the next time he/she logs in. This period is only effective between two password modifications performed by a user himself/herself. If the administrator resets the user password, the relevant user must only change his/her password if the **User has to change login password at next login** option of the user settings is also active.

If you set value `0`, you disable the automatic password alteration prompt.

The set value is evaluated in milliseconds.

> **NOTICE:**
>
> This system-spanning setting can be disabled for the respective user. If this is desired, activate the **Telephony PIN never expires** option on the **Password / PIN** tab of the relevant user settings

- **MinimumLength**

  Specifies the number of characters a user password must at least consist of.
- **MaximumLength**

  Specifies the number of characters a user password must not exceed. If you set value `0` this policy is not used.
- **MinimumDigits**

  Specifies the number of digits a user password must at least contain. This number is included in the number of **MinimumLength** and **MaximumLength**.
- **MinimumSpecialCharacters**

  Specifies the number of special characters a user password must at least contain. This number is included in the number of **MinimumLength** and **MaximumLength**.
- **MinimumUpperCaseCharacters**

  Specifies the number of capital letters a user password must at least contain. This number is included in the number of **MinimumLength** and **MaximumLength**.
- **MaximumRepeatedCharacters**

  Specifies how often a letter, special character or digit may successively occur in the user password.

  Example: The password *Schifffahrer* (German for skipper or boat passenger) is only valid if this parameter has at least been set to `3`. For, letter *f* appears in the password three times in a row.

  If you set value `0` this policy is not used.
- **MaximumFailedAttempts**

  Specifies how often a user may enter an incorrect password during the password-based login. If a user exceeds this number, his/her user account will automatically be locked for password-based access.

  Locking the password-based access does not influence the PIN-based access of the relevant user via telephone.

- **PasswordHistoryDepth**

  Specifies how many of the last passwords are stored in the password history of each user. A user cannot configure a password that is contained in the password history.
- **LockoutTime**

  Specifies how long the password-based access is locked for a user if he/ she has entered an incorrect password more often than is defined under **MaximumFailedAttempts**.

  When the specified period has elapsed, the password-based access is automatically released again for the relevant user. A locked access can also be released again before the set time has elapsed. The administrator must in this case assign a new password in the user settings.

  If you set value `0` for **LockoutTime**, the password-based access for users is not automatically unlocked again. The administrator must in this case assign a new password in the user settings.

  The set value is evaluated in milliseconds.

2.2.6 Policy for UC User PINs

You can define system-spanning requirements, UC user PINs have to satisfy.

A UC user PIN must comprise 8 to 16 digits by default.

Furthermore, the following applies by default:

- Each UC user must change his/her PIN after 90 days at the next PIN-based login

  NOTICE: This system-spanning setting can be disabled for the respective user. If this is desired, activate the **Telephony PIN never expires** option on the **Password / PIN** tab of the relevant user settings.
- A user must not enter an incorrect PIN more than five times. If this number is exceeded, his/her user account is automatically locked for PIN-based access.

  Locking the PIN-based access does not influence the password-based access of the relevant user.
- The last five PINs of a user are stored in a PIN history. A UC user cannot configure a PIN that is contained in his/her PIN history.

You can adjust these policies, valid for the entire system, in the following XML file:

`PassphrasePolicyConfig.xml`

You find this file in the following folder of the computer system set up on OpenScape UC Application:

<Osc#Install [2]>`/common/conf/`

Extract from the file `PassphrasePolicyConfig.xml`

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<PassphrasePolicyConfig version="2.0">
   <...>
   <PassphrasePolicy>
      <Type>pin</Type>
      <MinimumAge>86400000</MinimumAge>
      <MaximumAge>7776000000</MaximumAge>
      <MinimumLength>8</MinimumLength>
      <MaximumLength>16</MaximumLength>
      <MinimumDigits>8</MinimumDigits>
      <MinimumUpperCaseCharacters>0</
      MinimumUpperCaseCharacters>
      <MaximumRepeatedCharacters>0</
      MaximumRepeatedCharacters>
      <MaximumFailedAttempts>5</MaximumFailedAttempts>
      <PasswordHistoryDepth>5</PasswordHistoryDepth>
      <LockoutTime>1800000</LockoutTime>
   </PassphrasePolicy>
```

The following parameters of this XML file control the user PIN policies valid for the entire system.

- **MinimumAge**

  Specifies the period after a PIN alteration in which a user must not change his/her PIN again. This period is only effective between two PIN modifications performed by a user himself/herself. If the administrator resets the user PIN, the relevant user can immediately change his/her PIN.

  The set value is evaluated in milliseconds.

[2] <Osc-Install > is the setup directory of the OpenScape system: /opt/siemens/ respectively /enterprise/

- **MaximumAge**

  Specifies the period after which a user must change his/her PIN the next time he/she logs in. If you set value `0`, you disable the automatic PIN alteration prompt.

  The set value is evaluated in milliseconds.

  NOTICE:

  This system-spanning setting can be disabled for the respective user. If this is desired, activate the **Telephony PIN never expires** option on the **Password / PIN** tab of the relevant user settings.

- **MinimumLength**

  Specifies the number of characters a user PIN must at least consist of.

- **MaximumLength**

  Specifies the number of characters a user PIN must not exceed. If you set value `0` this policy is not used.

- **MinimumDigits**

  Specifies the number of digits a user password must at least contain.

  NOTICE:

  On a telephone, users can only enter digits but no letters. Therefore, this parameter must correspond to the setting under **MinimumLength**.

- **MinimumSpecialCharacters**

  Since users can only enter digits but no letters on a telephone, this setting does not apply for PINs.

  It must have value `0`.

- **MinimumUpperCaseCharacters**

  Since users can only enter digits but no letters on a telephone, this setting does not apply for PINs.

  It must have value `0`.

- **MaximumRepeatedCharacters**

  Specifies how often a digit may successively occur in the PIN.

  Example: The PIN *`455587`* is only valid if this parameter has at least been set to `3`. For, digit *5* appears in the PIN three times in a row.

  If you set value `0` this policy is not used.

- **MaximumFailedAttempts**

  Specifies how often a user may enter an incorrect PIN during the PIN-based login. If a user exceeds this number, his/her user account will automatically be locked for PIN-based access.

  Locking the PIN-based access does not influence the password-based access of the relevant user.
- **PasswordHistoryDepth**

  Specifies how many of the last PINs are stored in the PIN history of each user. A user cannot configure a PIN that is contained in his/her PIN history.
- **LockoutTime**

  Specifies how long the telephone-based access is locked for a user if he/she has entered an incorrect PIN more often than is defined under **MaximumFailedAttempts**.When the specified period has elapsed, the telephone-based access is automatically released again for the relevant user.

  A locked access can also be released again before the set time has elapsed. The administrator must in this case assign a new PIN in the user settings.

  If you set value `0` for **LockoutTime**, the telephone-based access for users is not automatically unlocked again. The administrator must in this case assign a new PIN in the user settings.

  The set value is evaluated in milliseconds.

2.2.7 Foreign-User Management

CMP can currently only be operated with one domain– the predefined system domain **system**. Therefore, no foreign users are currently supported.

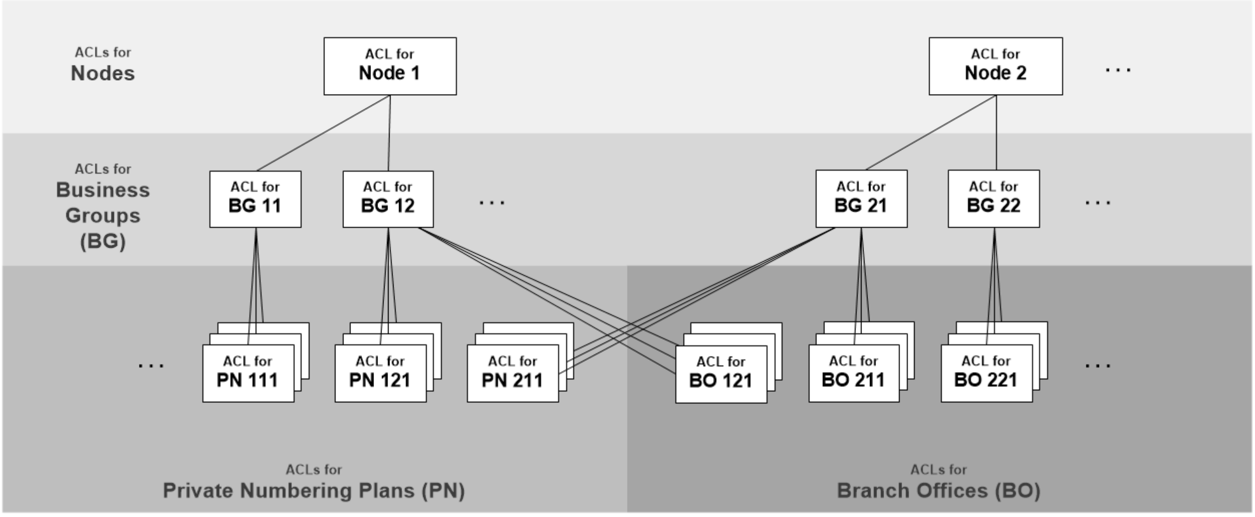
2.2.8 Access Control Lists

You can use access control lists to control which administrators may see selected configuration units in the OpenScape Voice Assistant as available. Even if a configuration unit is displayed to an administrator as available, he/she cannot access its settings.

OpenScape Voice uses an individual access control list for each of the following configuration units:

- OpenScape Voice system
- Business group
- Private numbering plan
- Branch office

The following figure is an example of how these access control lists (ACL) depend on each other hierarchically.



If an administrator account has been entered in an access control list, the configuration unit is displayed to the account's user in OpenScape Voice Assistant as available that controls the respective access control list. This requires the administrator account having CMP access and being entered in the access control lists that are possibly superior to the relevant access control list.

If, for example, the branch office *BO211* is to be displayed to an administrator as available, the following must be ensured:

- The **Basic Management** privilege must have been assigned to the administrator account for the **Symphonia** application.
- The administrator account must have been added to the access control list of the *BO211* branch office.
- The administrator account must have been added to the superordinate access control list of the business group *BG21*, in which the relevant branch office has been configured.
- The administrator account must have been added to the superordinate access control list of the OpenScape Voice system *System2*, in which the relevant business group has been configured.

The administrator account must be added to the access control list in the following sequence:

1) To the access control list of the OpenScape Voice system
2) To the access control list of the business group
3) To the access control list of the branch office

Before an administrator can be added to an access control list, his/her administrator account must be assigned the management privilege that associates the relevant configuration unit.

This means in detail:

If an administrator is to be added to this access control list, …	… he/she must have been assigned in particular the privilege for the application OpenScape Voice:
Access control list of an OpenScape Voice system	**Communication System Management**
Access control list of a business group	**Business Group Management**

If an administrator is to be added to this access control list, …	… he/she must have been assigned in particular the privilege for the application OpenScape Voice:
Access control list of a private numbering plan	**Private Numbering Plan Management**
Access control list of a branch office	**Branch Office Management**

To enable an administrator viewing and editing the settings of a configuration unit displayed as available, his/her administrator account must be assigned the configuration privilege that associates the relevant configuration unit.

If, for example, an administrator is to see the *BO211* office branch and edit its settings, the following must be ensured:

- The **Basic Management** privilege must have been assigned to the administrator account for the **Symphonia** application.
- The following privileges must have been assigned to the administrator account for the application **OpenScape Voice**:
  - **Communication System Management**
  - **Business Group Management**
  - **Branch Office Management**
  - **Communication System Settings**
  - **Business Group Settings**
  - **Branch Office Settings**
- The administrator account must at least be itemized in the above access control lists.

Editing access control lists

The following must be ensured for an administrator to edit an access control list:

- The **Basic Management** privilege must have been assigned to the administrator account for the **Symphonia** application.
- The administrator account must have been assigned the privilege for configuring an access control list of the relevant configuration unit. This means in detail:

If an administrator is to edit these access control lists, …	**… he/she must have been assigned this privilege for the application OpenScape Voice:**
All access control lists for OpenScape Voice systems	**Communication System Access List**
All access control lists for business groups	**Business Group Access List**
All access control lists for private numbering plans	**Private Numbering Plan Access List**

If an administrator is to edit these access control lists, …	… he/she must have been assigned this privilege for the application OpenScape Voice:
All access control lists for branch offices	**Branch Offices Access List**

NOTICE:

Each of these privileges makes sure that the relevant administrator account is automatically added to all access control lists of the relevant configuration units.

- The administrator account must be assigned the privilege that associates the relevant configuration unit:

If an administrator is to edit these access control lists, …	… he/she must have been assigned this privilege for the application OpenScape Voice:
All access control lists for OpenScape Voice systems	**Communication System Settings**
All access control lists for business groups	**Business Group Settings**
All access control lists for private numbering plans	**Private Numbering Plan Settings**
All access control lists for branch offices	**Branch Office Settings**

If, for example, an administrator is to configure the access control list of the *BO211* office branch, the following must be ensured:

- The **Basic Management** privilege must have been assigned to the administrator account for the **Symphonia** application.
- The following privileges must have been assigned to the administrator account for the application **OpenScape Voice**:
  - **Communication System Management**
  - **Business Group Management**
  - **Branch Office Management**
  - **Communication System Settings**
  - **Business Group Settings**
  - **Branch Office Settings**
- The **Branch Offices Access List** privilege must have been assigned to the administrator account for the **OpenScape Voice** application.

You cannot allow an administrator to only edit the access control list of single selected OpenScape Voice systems, business groups, branch offices or private numbering plans.

Related concepts

Default User-Profiles of the OpenScape Voice Assistant

2.3 Account Role Management

The frequent maintenance of operating system user accounts has increasingly become an important aspect of system security assurance. Current industry best practices, for example, require a change of account passwords ranging from a maximum of 90 days to as little as 60 days. The ability to modify system global account and password related security parameters is also required.

The following functional administration requirements for automating account management in the OpenScape Voice server (OSV) and OSV Assistant are introduced:

- User account functions (create, delete, password change, lock, unlock)
- User security levels (roles)
- Temporary accounts that expire automatically
- Cluster and/or site wide synchronization of user account states
- Password parameter profiles (minimum length, complexity)
- Account restriction profiles (max/min/warn days)

The OSV Assistant provides the customer interfacing for automated administration of OSV user accounts. It also provides an interface to update important system-wide account and password security parameters on a set of one or more simplex hosts or clusters. The most relevant security parameters include:

- Password minimum length (8, 14 characters)
- Password complexity (at least 2 profiles)
- Account expiration and warning periods (in days)

2.4 Account Profiles

The Account Profiles allows you to view the available profiles. It is not possible to edit them, In case the system is cluster and the nodes are out of sync the selected active profile will be applied on both nodes.

Navigate to **Configuration** > **OpenScape Voice** > **Administration** > **General Settings** > **Account Profiles**

In the pop up window appears with four tabs:

- **Password**
- **User**
- **SSH**
- **Security**

Password

You can select an active password profile from the dropdown menu. For each profile its parameters are depicted in the parameters’ list. These parameters are:

- Minimum length
- Minimum upper case letters
- Minimum lower case letters
- Minimum digits
- Minimum special characters
- Minimum difference

- Maximum repeats

User

You can select an active user profile from the dropdown menu. For each profile its parameters are depicted in the parameters’ list. These parameters are:

- Minimum length
- Maximum length
- Minimum days
- Maximum days
- Warning days
- Expiration days

SSH

You can select an active Ssh profile from the dropdown menu. For each profile its parameters are depicted in the parameters’ list. These parameters are:

- Method
- Key protocol
- Cipher

Security

You can select an active security profile from the dropdown menu. For each profile its parameters are depicted in the parameters’ list. These parameters are:

- FIPS mode
- CAC
- Network tools
- FTP
- Login failure

2.5 System Management

Using the system management you can quickly gain an overview of the available system nodes and their logical grouping (clustering). Furthermore, it provides auxiliary means to configure these system nodes and to log this configuration.

The system management is divided into the following areas:

- System Status
  - Nodes
  - Applications
- Node Groups
- 3rd Party Nodes
- Xpression Node
- OpenScape 4000 Node
- SNMP Node

The system management is domain-spanning. It cannot be used by service provider administrators, since these administrators should not be in a position to display the installed components.

2.5.1 System Overview

The system overview provides information about the structure of the OpenScape system and the status of the associated system nodes. Furthermore, you can arrange the various system nodes in a logic order and configure associated applications.

The System overview is divided into the following areas:

- Nodes
- Applications

The system overview is domain-spanning. It cannot be used by service provider administrators, since these administrators should not be in a position to display the installed components.

Nodes

Under Nodes you are provided with an overview of the available system nodes, the connections to 3rd party systems and their groups (nodes cluster).

For each node you can display a so-called dashboard. Depending on the system node type this dashboard can comprise detailed information about the following topics:

- Individually configurable note for the system node
- Alarms for the system node
- System information about the hardware of the system node
- Applications installed on the system node and their software versions
- Actions executable for the system node. E. g:
  - Show status information about the nodes system health by means of Rapidstat.
  - Show related log files.
  - Show information of related services and components.
  - Configure settings of related services and components.
  - Show the version of installed software packages.
- Operational status information

You find details about the displayed node type dependent information in the chapters about the corresponding node type.

Applications

Under Applications you are provided with an overview of all applications that are installed on the system nodes. In particular, you learn in which software version the application is installed and on which system node.

The action menu (▸) of an application entry lets you configure application individual settings. You find details about the application individual settings in the chapters about the corresponding application.

2.5.2 System Dashboard overview

The dashboard contains detailed information on a selected system node. This detailed information includes for example hardware information, alarm information, installed applications and their software level.

The Dashboards for the OpenScape Voice system is of the type **Communication System**.

2.5.2.1 The Communication System Dashboard

The **Dashboard** type **Communication System** (OpenScape Voice), provides a variety of performance and system information.

This dashboard consists of the following areas:

Dashboard <name>

Contains the **Note** for the specific Node.

Alarm summary:

The following information is provided:

- Number of **Critical** alarms (red).
- Number of **Major** alarms (orange).
- Number of **Minor** alarms (yellow).
- Number of **Warning** alarms (cyan).

System Info

The system info presents the following information:

- **CPU** (Central Processing Unit):

  This is the percentage of CPU usage. This is snapshot information for a small period. Depending on the system load it will indicate from 0% to 100% of usage.
- **Memory**:

  This is the percentage of RAM memory use - a snapshot information for a small period. Depending on the system load it will indicate from 0% to 100% of usage.
- **Date/Time**

  Shows the time at the system.
- **Last Reboot**

  It shows date and time of latest system reboot.

Applications

The application **Name** and the **Software Version** are displayed with the following naming convention:

Vx Ry.p.e

Where :

x=Major Release

y=Minor Release

p=Patchset

e=Emergency Patch

For example V7 R1.5.2 means Version 7, minor release 1, patchset 5, emergency patch 2

Actions

The **Actions** section provides various buttons to display advanced information. The options (buttons) that are shown on the dashboard depend on the deployment and include:

- OSV Rapidstat.
- Core Network Interfaces
- Show/Change Node status
- Show services status
- Show software package
- UC Rapidstat
- Backup version
- Synchronize versions
- Configure hardware.

2.5.3 Software Package Overview

The software packet overview displays which software packages are installed on a selected system node of the OpenScape system.

The software packet overview is domain-spanning. It cannot be used by service provider administrators, since these administrators should not be in a position to display the installed components.

What software packets are displayed in the overview depends on the node you open the software packet overview for.

For each software packet the following information is displayed:

- **Software**

  Displays the name of the corresponding software packet.
- **Version / Build**

  Displays the version and build number of the corresponding software packet.
- **Installation Media**

  Displays from what medium the corresponding software packet was installed. If the corresponding RPM packet was installed manually the value **unknown** is shown.
- **Date** (Installation Media)

  Displays when the corresponding software packet was installed.
- **Update Media**

  Displays from what medium the corresponding software packet was updated. If the corresponding RPM packet was updated manually the value **unknown** is shown.

- **Date** (Update Media)

  Displays when the corresponding software packet was updated. If no date is displayed, the software packet has never been updated so far.

If a text is not fully displayed, you can display the full text as tool tip. To open the tool tip move the mouse pointer over the truncated text.

2.5.4 Node Groups

The system nodes of an OpenScape system can be combined in node groups. This lets you manage the different system nodes in logic groups.

If a system node is not assigned to an individual node group, it belongs to the node group Root. The node group Root is automatically configured after the installation of the OpenScape system and cannot be deleted.

2.5.5 3rd Party Nodes

An OpenScape system can be connected to 3rd party nodes to provide OpenScape users with additional web applications. 3rd party nodes can be connected via Telnet, HTTP, HTTPS, or SSH to the OpenScape system.

2.5.6 Node List of the OpenScape Media Server

Via the OpenScape Media Server node list you can display which OpenScape Media Servers are available in the OpenScape system. Furthermore, you can configure the available OpenScape Media Servers there.

The OpenScape Media Server node list is domain-spanning. It cannot be used by service provider administrators, since these administrators should not be in a position to display the installed components.

2.6 Software Repository

You can store and manage upgrade file packages in the Common Management Platform Software Repository. These packages belong to the various applications of an OpenScape system.

An upgrade file package comprises at least one upgrade file and one reference file. The reference file has the file extension `*.spa` and references all upgrade files contained in the upgrade file package.

How to upgrade an OpenScape application via the Software Repository of the Common Management Platform is described in the relevant manuals of the respective application.

2.7 Concept of the Consistency Check

The consistency check checks important configuration parameters of OpenScape UC Application and the functionality of its components resulting from this. For example, you can determine whether the configuration of OpenScape UC Application is consistent or faulty configurations hamper the system performance.

The consistency check is based on individual check scripts that determine which components and configurations are checked.

In the Common Management Platform, you can choose from the following default check scripts to perform a consistency check:

- Check script OpenScape UC
- Check script User Configuration

Each of these check scripts controls the performance of individual checks.

Check script OpenScape UC

Checks the following for OpenScape UC Application:

- Related to OpenScape Voice
  - Whether all office codes are fully configured.
  - Whether the CSTA connection is configured.
  - Whether the CSTA interface of OpenScape Voice can be reached.
- Related to the OpenScape Media Server
  - Whether OpenScape Voice is configured as SIP server and can be reached.
  - Whether a TTS system is configured and can be reached.
- Related to the voice portal
  - If OpenScape Xpressions is configured for OpenScape users: Whether the settings for Trusted Transfer Mode (TTM) are configured.
- Related to licenses
  - Whether a valid license is installed for OpenScape UC Application.
  - Whether a valid license is installed for the TTS system.
- Related to the groupware connection
  - Whether the connected groupware system can be reached.
  - Whether the configured account data allows access to the groupware system.
  - Whether e-mails can be sent via the configured SMTP system.

Check script User Configuration

Checks the following for each configured OpenScape user:

- Whether the user account of the user is locked.
- Whether a subscriber has been selected as one-number device for the user.
- Whether the selected one-number device is available as subscriber in the OpenScape Voice System.
- Whether the **ONS in / out** option is activated in the OpenScape Voice system for the selected one-number device.
- Whether CSTA is activated in the OpenScape Voice system for the selected one-number device.

- Whether the OpenScape database contains a contact entry associated to the user.
- Whether the user's contact data contain a phone number.
- Whether a user profile has been assigned to the user.
- Whether a voicemail number has been configured for the user.
- Whether an external ID for the groupware connection has been assigned to the user.
- Whether the groupware system of the configured external ID is configured.

2.8 Download Center

You can use the download center to download different resources from a central place.

Among these resources are:

- Software
- Documentation

Software and Documentation

Software and documentation to be provided in the download center for downloading must be stored in the following folders on the OpenScape computer system.

- Software:

  <Osc#Install [3]>`/share/tomcat/webapps/management/downloads/software`
- Documentation:

  <Osc#Install >`/share/tomcat/webapps/management/downloads/documentation`

> **IMPORTANT:**
>
> If the download center is not pre-configured (which is usually the case for a fresh installation) you will have to create the folders for the paths above: `downloads/software` and `downloads/documentation`.

To improve the file management, create in each of these folders a new subfolder – e. g. `CMP_Software`.

Besides the actual download files both folders must contain a contents file that summarizes all available files with their document information. This contents file must be called `filelist.xml` and have the following general XML structure depending on the resource type:

Table 9: Structure of the contents file for software

```
<filelist>
    <file>
```

[3] <Osc-Install> is the setup directory of the OpenScape system:`/opt/siemens/` or `/enterprise/`

```
        <filename>pdf-reader.exe</filename>
        <title>PDF Reader 9.2</title>
        <description>PDF Reader for Windows XP</description>
        <version>9.2.1245</version>
    </file>
    …
</filelist>
```

Table 10: Structure of the contents file for documentation

```
<filelist>
    <file>
        <filename>OpenScape_GER.doc</filename>
        <title>OpenScape-Dokumentation</title>
        <language>Deutsch</language>
        <orderNo>10-200-4587-100</orderNo>
    </file>
    <file>
        <filename>OpenScape_ENG.doc</filename>
        <title>OpenScape Documentation</title>
        <language>English</language>
        <orderNo>10-200-4587-200</orderNo>
    </file>
    …
</filelist>
```

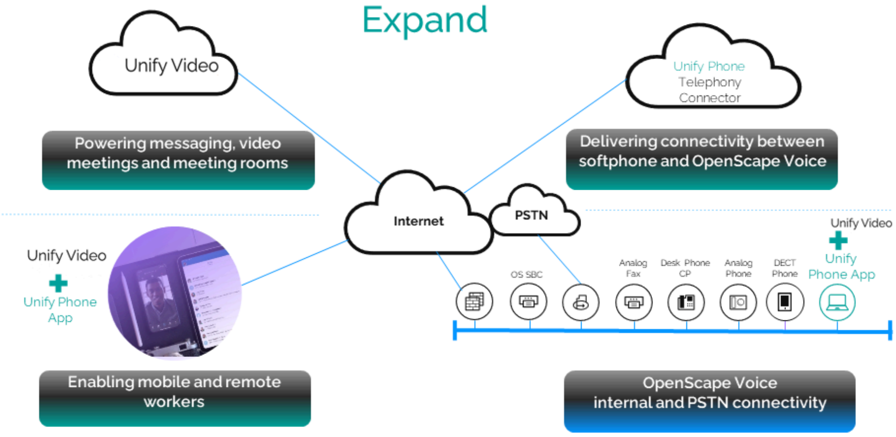
2.9 OpenScape UC Application

OpenScape UC Application is a unified, real-time UC application suite optimized for business process integration. It fits into an enterprise’s existing voice and data infrastructure and ties together phones, voicemail, e-mail, text-messaging, calendaring, instant messaging, and conferencing 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.

You find detailed information about OpenScape UC Application in the associated product manuals.

2.10 Unify Phone

Unify Phone is a telephony connector for Unify Video. It acts as a bridge between OpenScape Voice and Unify Video, enabling users to make and receive phone calls on their business phone number using the Unify Phone app.


Expand
Unify Video
Powering messaging, video meetings and meeting rooms
Unify Phone Telephony Connector
Delivering connectivity between softphone and OpenScape Voice
Internet
PSTN
Unify Video
Unify Phone App
Enabling mobile and remote workers
OS SBC
Analog Fax
Desk Phone CP
Analog Phone
DECT Phone
Unify Video
Unify Phone App
OpenScape Voice internal and PSTN connectivity

Features

Unify Phone supports the following features:

- Make call
- Answer, decline or drop a call
- Send DTMF commands in a call
- Hold and retrieve
- Mute/ Unmute
- Transfer call
- Pull call from other Unify Phone clients or desk phone
- Push call to desk phone
- Make or answer a second call
- Swap calls (alternate)
- Merge two calls into a conference
- Call forwarding
- Alternative number (One Number Service)
- Call routing
- Voicemail
- Cross-launch from Unify Video

You can find detailed information about Unify Phone in the associated product manuals.

To configure Unify Phone with OpenScape Voice, see also *OpenScape Voice V10 Service Manual: Service Documentation*.

2.11 Contact List Management

Using the contact list management you administer the different contact lists of the OpenScape system.

NOTICE:

The contact list management is only required if you use OpenScape UC Application.

The OpenScape system provides different contact lists. We can generally distinguish two types.

- Global contact lists
- Private contact lists

Global Contact List

Global contact lists contain the global contact data of users. For example, the contact data of a company's employees. OpenScape UC Application currently supports as global contact lists:

- The integrated global contact list of OpenScape UC Application.

  NOTICE:

  As soon as contact information is defined for a user account in Common Management Platform , a new contact is created in the integrated global contact list of OpenScape UC Application with this contact information.

- An external LDAPdirectory that is connected to OpenScape UC Application via the LDAP connector.

You can use the contact list management to do the following:

- Define, which of these global contact lists should be used. In these active contact lists the OpenScape applications can then look for contact information.
- Manage contacts in the global contact list that is integrated in OpenScape UC Application.

NOTICE:

OpenScape UC Application has only read-access to the contacts of a connected LDAP directory.

Private Contact List

Private contact lists contain contact data that single users maintain for their own use. Such data can only be created and edited by the respective user and via the OpenScape applications.

You can use the contact list management to define where the private contact list of the various OpenScape users shall be managed. For the time being, this can be one of the following places:

- The integrated OpenScape contact database.
- A groupware system connected to OpenScape UC Application via the groupware connector.

The OpenScape applications use certain services to access the contact lists. To this, the services need to register with the OpenScape system beforehand. In certain circumstances, a service may be configured, but not registered, in which case it cannot be accessed.

2.12 HiPath OpenScape Configuration

If you use OpenScape UC Application, CSTA connections must be configured and administered between OpenScape UC Application and the communications systems used.

NOTICE:

The HiPath OpenScape configuration is only used when you deploy OpenScape UC Application.

Via these connections the following features are enabled.

- Monitoring the status of terminal devices
- Monitoring and controlling connections in the relevant communications system

Configuring a CSTA connection also activates a function that copies the subscriber information of the communications system as resources to OpenScape UC Application

As soon as such a resource is assigned to a UC Application user, OpenScape UC Application sets a CTI monitor point in the relevant communications system for the relevant subscriber and starts CTI monitoring for him/her.

2.13 Resource Management

The resource management is used to administer information of various OpenScape resources. These resource information is used by OpenScape UC Application to monitor the related resources of the corresponding systems and to control them if needed.

NOTICE:

The resource management is only required if you use OpenScape UC Application.

Resources are combined into resource groups.

Possible resource groups are:

- OpenScape Voice resources
- OpenScape 4000 resources
- Media server resources

Via the Common Management Platform user management you can assign these resources to users.

2.13.1 OpenScape Voice Resources

The OpenScape Voice resources group contains resources available for the OpenScape Voice communications system in the Common Management Platform. The resources of this group are configured with OpenScape Voice Assistant on OpenScape Voice. They can therefore only restrictedly be edited via the resource management of the Common Management Platform. OpenScape Voice resources can only be deleted and added in the OpenScape Voice Assistant.

For the OpenScape resources group the Common Management Platform administers the following resources with the described settings.

- **Office Codes**

  Each office code is identified by its individual **Office Code ID**.

  An office code represents the general portions of a phone number that precedes the extension number. These are:

  Country code – **Area code** – **PBX number**

  Example: `0049 - 89 - 722`

  NOTICE:

  The PBX number is also called the site number or system number.

  In case of an OpenScape Voice system the office codes are configured with the OpenScape Voice Assistant.

  An office code may contain a so-called **overlap**. This overlap specifies if and to what extent the office code and the associated extensions overlap.

  Example: A fully qualified phone number be `492404902100`. The office code is `492404902` and the extension `2100`. In this example, one digit of the extension and office code overlap – namely digit `2`. The **overlap** in this example is thus `1`.

  If an office code is to use an **overlap**, it must be configured via the resource management of the Common Management Platform.

  Furthermore, the office code contains the codes **international** and **national**. These codes are the digits that you must dial for making an international call or for a call outside your own area network.

  So that an office code is fully configured from the OpenScape UC Application view, values must have been specified for the following fields:

  – **Overlap**
  – **International**
  – **National**

  Whether or not an office code is fully configured in this sense displays the list of available resources in the **Complete** column.

- **Private Number Codes**

  Each private number code is uniquely identified by their individual **PN-Code-ID**.

  With private number codes you can define customer-individual numbering plans of up to three levels in order to map internal corporate structures, forexample. The private number code is structured analogously to the central office code and also represents the portions of the phone number that precede the extension number:

  Barrier code– **Level 2 code**– **Level 1 code**– **Level 0 code**

  Example: `8 – 11 – 22 – 33`

  > **NOTICE:**
  >
  > No value must be specified in the **Barrier Code** field.

  The **barrier code** indicates that a private number code is involved. The level codes map a customer-individual phone number structure and need not correspond to the “country code - area code - office code” scheme.

  A private number code may contain a so-called **overlap**. This **overlap** specifies if and to what extent the private number code and the associated extensions overlap.

  Example: A fully qualified phone number be `492404902100`. The office code is `492404902` and the extension `2100`. In this example, one digit of the extension and office code overlap – namely digit `2`. The **overlap** in this example is thus 1.

  If a private number code is to use an overlap for, it must be configured via the resource management of the Common Management Platform.

  Furthermore, a private number code contains the **Level 2** and **Level 1** prefix. These prefixes are the digits you need to dial for a call outside the relevant level.

  > **NOTICE:**
  >
  > No values must be specified in the **Level 1 Prefix** and **Level 2 Prefix** fields.

  > **NOTICE:**
  >
  > All OpenScape Voice subscribers who have been configured for private numbering plans must be of the same level type – of type L0, of type L1 or of type L2. If different level types are

to be used, an individual OpenScape Voice system must be configured for each level type.

NOTICE:

Every private number code must be unique for the associated OpenScape Voice system.

NOTICE:

Every private number code must comprise at least three digits. Synchronization with OpenScape UC Application will otherwise fail.

NOTICE:

Every private number code must be able to be translated in the associated private numbering plan by OpenScape Voice without using a barrier code, a level 1 or level 2 prefix.

- **Phone Numbers** (Extension)

  The phone number defines the extension of OpenScape Voice. It is assigned to an **office code** or a **private number code**.

2.13.2 OpenScape 4000 Resources

The group of OpenScape 4000 resources contains resources that are available to the OpenScape 4000 communications system in the Common Management Platform.

The Common Management Platform administer the following resources for the group of OpenScape 4000 resources:

- **Office Codes**
- **Prefixes**
- **Voice Subscribers**

NOTICE:

Please obtain detailed information about these resources and their settings from the OpenScape 4000 product documentation.

The resources of this group are configured with the OpenScape 4000 administration interface on the OpenScape 4000 system. Therefore, they can be only edited via the resource management of the Common Management Platform.

The settings of these resources must be transferred from OpenScape UC Application to the OpenScape database by provisioning tools. After the relevant resources have been transmitted, they are available in the Common Management Platform.

2.13.3 Media Server Resources

The Media Server Resources group contains the resources available for the OpenScape in the Common Management Platform. You can configure the resources of this group with the Common Management Platform.

For the Media Server Resources group the Common Management Platform administers the following resources with the described settings.

- **Office Codes**

  Each office code is identified by its individual **Office Code ID**.

  An office code represents the general portions of a phone number that precedes the extension number. These are:

  Country code – **Area code** – **PBX number**

  Example: `49 - 89 - 722`

  > **NOTICE:**
  >
  > The PBX number is also called the site number or system number.

  > **NOTICE:**
  >
  > An office code should not contain any phone number prefixes.

  An office code may contain a so-called **overlap**. This overlap specifies if and to what extent the office code and the associated extensions overlap.

  Example: A fully qualified phone number be `492404902100`. The office code is `492404902` and the extension `2100`. In this example, one digit of the extension and office code overlap – namely digit `2`. The **overlap** for this example is thus `1`.

  If an OSV office code is to use an **overlap**, it must be configured via the resource management of the Common Management Platform.

  Furthermore, an office code contains the office codes **International** and **National**. These codes determine the digits that you must dial for making an international call or for a call outside your own area network.
- **Private Number Codes**

  Each private number code is uniquely identified by its individual **PN-Code-ID** .

  With private number codes you can define customer-individual numbering plans of up to three levels in order to map internal corporate structures, forexample. The private number code is structured analogously to the central office code and also represents the portions of the phone number that precede the extension number:

Barrier code– **Level 2 code**– **Level 1 code**– **Level 0 code**

Example: 8 – 11 – 22 – 33

NOTICE:

A private number code should not contain any phone number prefixes.

The **barrier code** indicates that a private number code is involved. The level codes map a customer-individual phone number structure and need not correspond to the “country code - area code - office code” scheme.

A private number code may contain a so-called **overlap**. This **overlap** specifies if and to what extent the private number code and the associated extensions overlap.

Example: A fully qualified phone number be 492404902100. The office code is 492404902 and the extension 2100. In this example, one digit of the extension and office code overlap – namely digit 2. The **overlap** for this example is thus 1.

If a private number code is to use an overlap for OpenScape Voice, it must be configured via the resource management of the Common Management Platform.

Furthermore, a private number code contains the **Level 2 prefix** and **Level 1 prefix**. These prefixes are the digits you need to dial for a call outside the relevant level.

- **Conference Devices**

  A conference device of the OpenScape Media Server corresponds to the phone number for an OpenScape Voice or OpenScape 4000 system.

  It defines an extension that is assigned to an SIP domain (SIP domain ID) and to an office code or a private number code.

  The conference type specifies whether the device is associated to the conference portal or the voice portal of the OpenScape Media Server.

3 User Telephony

This package of features is a collection of functions usable for subscribers.

3.1 Business Group Features

The BG (Business Group) concept provides the basic capabilities for handling a group of subscribers associated with a single enterprise simplify such tasks. Subscriber and EP (Endpoint) features allow further different usage and configuration. It also permits OpenScape Voice to recognize the associations of the subscribers.

3.1.1 BG (Business Group) Feature

The BG (Business Group) concept provides the basic capabilities for handling a group of subscribers associated with a single enterprise. It also permits OpenScape Voice to recognize the associations of the subscribers the BG contains.

This is the summary of BG features:

- Virtual DN (Directory Number)
- DID (Direct Inward Dialing)
- Group-Level Feature Administration
- Multiple Time Zone Support
- Silence Suppression Disabling
- T.38 Fax Support

Related concepts

BG (Business Group) on page 433

3.1.2 Direct Inward Dialing

The DID (Direct Inward Dialing) feature allows an external caller to dial a national or international number and connect directly to an OpenScape Voice subscriber.

The Contact information for the set of DID numbers, that is assigned to the OpenScape Voice Enterprise server should be provisioned (static registration) at the Service Provider. The Service Provider sends all incoming call requests that are directed to any of the DID numbers to the Contact address that has been statically registered for the OpenScape Voice server. The Service Provider is not aware of actually existing or currently registered clients within the OpenScape Voice server.

3.1.3 Multiple Time Zone Support

OpenScape Voice supports subscribers in multiple time zones. The OpenScape Voice server itself has a default time zone. The default is for subscribers to be assigned to that time zone; alternately, they can be assigned to another if warranted.

OpenScape Voice supports subscribers in at least 12 time zones. For all time related items that are not specific to an individual subscriber, OpenScape Voice and its associated servers use the system time.

All of these elements are synchronized to a common time source through the use of NTP (Network Time Protocol).

Functional Sequence

Each time zone has the following data associated with it:

- A delta value that specifies how it differs from GMT (Greenwich Mean Time). This delta can indicate -12 to +14 hours, with resolution at intervals as short as 15 minutes depending on the country in which the time zone is located.
- When or if Daylight Savings Time starts and stops. Associated changes occur automatically on the appropriate dates.

Offset Representation

The RTP `Srx/DB/IsTimeZoneGMTLinuxDefault` determines how the time zones are represented as offsets:

- if set to `RTPTrue` (default), the GMT offsets are set according to the OS defaults e.g. `GMT0 = 0, GMT+1= -60, GMT-1 = 60, GMT+2 = -120, GMT-2=120,...`
- if set to `RTPFalse` , the GMT offsets are set as the inverse of the OS defaults e.g. `GMT0 = 0, GMT+1= 60, GMT-1 = -60, GMT+2 = 120, GMT-2=-120,...`

System Specific Information

Each OpenScape Voice subscriber has a home time zone. If one is not specified, it defaults to the main OpenScape Voice local time. The time zone defines the way in which the subscriber's time-dependent services work.

These capabilities ensure that the following features and applications report, as applicable, the date and time information that is relevant for correct feature/ application operation and utilization:

- Enhanced Call Forwarding
- Malicious call trace
- Hot desking
- Return call
- Time-of-day routing

Other Characteristics

CDR (Call Detail Record) times are recorded using GMT. The offset to local time (using the subscriber's time zone) is also recorded.

If Daylight Savings Time changes occur while a call is in process, necessary adjustments are made to ensure the CDR record reports the correct start time and call duration.

Switchwide CDR-type reports that occur once every 24 hours (for example, for long duration calls) are generated once a day based on the default switch time. They are not generated multiple times for various subscriber time zone groupings.

Related concepts

RTP Management via OpenScape Voice Assistant on page 961

3.1.4 Silence Suppression Disabling

The Silence Suppression Disabling feature enables proper fax transmission through the applicable gateways when the start of the fax is detected. This feature is needed when G.711 is used for fax/modem transmission.

3.1.5 T.38 Fax Support

The T.38 Fax Support feature provides support for T.38 facsimile UDPTL (User Datagram Protocol Transport Layer) according to RFC 2833. The capability to send, receive, and process the signals to and from the gateway for tone detection and T.38 fax relay events is provided.

Support of the loose call agent controlled mechanism is provided, since it is not required to identify the support for T.38 at the start of the call.

An administration parameter is provided for trunk gateways and SIP endpoints to select the T.38 fax relay support capability.

3.1.6 Virtual DN (Directory Number)

The Virtual DN (Directory Number) feature permits the administrator to create a DN that does not have a connection. The DN can be used for station RCF (Remote Call Forwarding) or it can be a means of reserving a number for future use.

If the DN is being used for station RCF, it cannot be subscribed to any other services.

3.2 Subscriber Features

Subscriber Features (a.k.a. services) in OpenScape Voice represent end user telephony functionality - most of them related with call processing. Features can be implicitly (via an associated Feature Profile) or/and explicitly assigned to subscribers.

An example of an OpenScape Voice Feature is Call Forwarding on No Reply.

Feature Data

Feature Data exist at Switch level, FP level and Subscriber Level.

- Switch Wide feature data are stored in RTP parameters and affect all subscribers the same way. They are primarily used in order to meet needs of various customers as it regards to the detailed behaviour of a feature. They rarely change after initial set-up and only few of them are managed via Assistant. Example of Switch Wide service Data is `Srx/Service/CFLoopMaxCount`

- Feature data stored at feature profile level follow the same structure as feature data that are stored at subscriber level. They are meant to control service behaviour of services at subscriber level. Example of a Service Data stored at profile/subscriber level is the Call Forward Destination Number.

When a feature is explicitely assigned to a profile or subscriber, the feature data are initialized to their (built-in) defaults.

When a feature is inherited by a subscriber, the feature data that are stored at the profile level are also inherited.

If a subscriber inherits a feature from its associated profile and either the feature data are changed at the associated profile or another profile is associated to the subscriber, the administrator decides, whether the subscriber’s current feature data shall be preserved or replaced.

If the feature is explicitely Assigned to the subscriber, feature data are not passed from profile to subscriber.

System Specific Information

Only subscribers with the compatible attributes can subscribe to features.
For example, Call Waiting is not applicable to SIP subscribers and Busy Line Verification is not applicable for Enterprise customers.Features that have attributes will also have a "Local" parameter. The Local parameters apply when a feature is inherited from a feature profile. They are used when displaying data to indicate the attributes that are overwritten locally (at the subscriber/BG level), and are used when updating data to reset the locally overwritten feature data to the values at the feature profile level. To avoid redundancy, this Local parameter is not listed for every feature.

Features are organized to the following categories:

- Display Features
- Call Forwarding Features
- Station Restriction Features
- CSTA Features
- Tones, Ringing, Announcements
- Intercom Call Features
- Abbreviated Dialing Features
- General Features
- Call Screening Features
- Silent Monitoring Features

Other Characteristics

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.

Access codes are required to activate/deactivate operation of many OpenScape Voice features. The required access codes are usually added during the initial installation of the system; however, any additional codes can be added at the **Prefix Access Codes**.

Related concepts

RTP Management via OpenScape Voice Assistant on page 961

3.2.1 Single Load Line (SLL) Feature

Starting from V10, OpenScape Voice does support the Single Load Line feature (SLL). The SLL feature allows to deliver corrections and provide customers with new features available in the latest product software without requiring any changes in licenses and cost.

SLL lifts the previous restriction of disallowing an earlier version license file to exist after the OSV version is upgraded, e.g. allowing OSV to operate a V10 software with a V10 license.

New features are either marked as **Free** or **Buy**:

- **Free**- features that can be used without restrictions.
- **Buy**- features that are time limited in case the license is not updated to the corresponding version.

NOTICE:

SLL is applicable as long as the licensed version is still supported. If a licensed version has reached end of support (M44 milestone), a (final) update to a higher, supported version can be performed. However, subsequent product updates will require a license for a supported version to be installed (except for customers which have EMSS contract in place).

3.2.2 Subscriber-level Feature Provisioning

Features may be applied directly to individual subscribers and those direct subscriptions override feature settings from the associated Feature Profile (if any). Overrides may be performed for an entire feature or for just a specific attribute of a feature.

Assignment State

In subscriber feature settings, the **Assignment** state of a feature can be one of the following:

- **Assigned**

  This setting indicates that the feature is directly assigned to the subscriber. That is, feature status and feature attributes do not depend on the relationship of the subscriber with a Feature Profile and are not affected by changes at Feature Profiles.

- **Denied**

  This setting indicates that the subscriber is not allowed to inherit the feature from any feature profile.

  > **NOTICE:**
  >
  > Note that in OpenScape Voice Assistant currently both the **Denied** and **Not Assigned** states are represented as the absence of the feature in the subscriber’s list of assigned features.

- **Inherited**

  The feature is not explicitly assigned to the subscriber but is inherited from the associated feature profile. If it is removed from the profile, it will automatically be removed from all "Members" (i.e. associated subscribers).

  The inherited feature configuration data can be modified at the subscriber level (for some features even by the subscriber) without changing the assignment state.

  For example, when the end user from the WebClient activates the Busy or Unconditional forwarding the Subscriber assignment from “inherited” changes to “inherited with local data” automatically, and remains to that assignment state “inherited with local data” even if the forwarding is disabled from the WebClient.

- **Inherited with Local Data**

  This value indicates that the subscriber feature is inherited from the associated Feature Profile. In case the data change in the subscriber feature menu, then the local data will be "activated".

- **SwitchWide**

  This value indicates that the feature is set switch wide and thus all subscribers have access to it.

  Switch Wide assignment is controlled via RTP parameter, and affects all subscribers.

  Currently, only the feature MCT (Malicious Call Trace) is by default assigned to all users at switch level.

- **Not Assigned**

  This value indicates that the feature is not assigned to this subscriber and is not visible in the Subscriber feature list.

Feature Management

The following actions are possible for a feature during subscriber management:

- **Add Feature**

  Add this feature at the subscriber level and/or replace any existing definition of the feature that the subscriber might have at the feature profile level or directly at the subscriber level.

  As a result, the feature is in **Assigned** state on subscriber level.

- **Edit Feature**

  The feature must already exist from either being previously provisioned at the Feature Profile Level (i.e. **Assignment** state **Inherited**) or provisioned directly at the subscriber level (i.e. **Assignment** state **Assigned**).

  The administrator can "locally" overwrite the feature data using this operation.

  NOTICE:

  "Local" feature data modifications do not change the **Assignment** state of the feature.

- **Delete Feature**

  The result of this action depends on the feature's **Assignment** state at the time it is executed:

  – **Assignment** state = **Assigned**

    In this case the subscriber-level settings are deleted and reset to the settings from the associated feature profile (if any).

    If there is no associated feature profile or if the feature is **Not Assigned** to the associated feature profile, it will be **Not Assigned** to the subscriber as well. Otherwise it will be **Inherited** from the associated Feature Profile.

  – **Assignment** State = **Inherited**

    In this case the feature is put to the **Denied** state.

- **Set Feature Profile**

  The result of this action depends on the individual features' **Assignment** states at the time it is executed:

  – **Assignment** state = **Assigned** or **Denied**

    In this case all subscriber-level feature settings - including **Assignment** state - are preserved.

  – **Assignment** State = **Inherited**

    If the feature is **Assigned** to the newly selected profile, it will remain **Inherited** at the subscriber-level. Subscriber-level feature data are reset to the profile-level feature data unless the **Preserve Subscriber Settings** option is passed to the action.

    If the feature is **Not Assigned** to the newly selected profile, it will be removed from the subscriber, i.e. the subscriber-level **Assignment** state will become **Not Assigned**. Subscriber-level feature data are dropped.

  – **Assignment** State = **Not Assigned**

    If the feature is **Assigned** to the newly selected profile, it will be cascaded to the subscriber, i.e. its subscriber-level **Assignment** state will become **Inherited**.

    If the feature is **Not Assigned** to the newly selected profile, it will remain **Not Assigned** at the subscriber-level.

Change Assignment Status

The Subscriber Feature status can be one of the **Assigned**, **Denied**, **Inherited**, **Inherited with Local Data** and **Not Assigned**. The administrator has the ability to change the feature assignment on any of the Features in the Subscriber

Features list, but not all transitions are offered. The table below describes all the possible transitions of Feature assignment status.

Table 11: Feature Assignment Status transitions

New value / Old value	New value: Assigned	New value: Inherited	New value: Inherited with Local Data	New value: Denied	New value: Switch Wide
Old value: Assigned	Remains Assigned	The transition is permitted only if the feature is included in the already selected feature profile. The feature profile data of the feature will be activated in this case	The transition is permitted only if the feature is included in the already selected feature profile. In case the data have been changed in feature then the local data will be "activated".	Denied	The transition is permitted only if the feature is not included in the already selected feature profile and the RTP parameter of the feature is set to True.
Old value: Inherited	Change to Assigned	Remains Inherited	change the values of feature profile to the values from feature (if they differ)	Denied	The transition is not possible
Old value: Inherited with Local Data	Change to Assigned	Change the values of feature (if they differ) to the values from feature profile	Remains Inherited with Local Data	Denied	The transition is not possible

New value / Old value	New value: Assigned	New value: Inherited	New value: Inherited with Local Data	New value: Denied	New value: Switch Wide
Old value: Denied	Change to Assigned	The transition is permitted only if the feature is included in the already selected feature profile. The feature profile data of the feature will be activated in this case	The transition is permitted only if the feature is included in the already selected feature profile. In case the data have been changed in feature then the local data will be “activated”.	Remains Denied	The transition is not possible in case the feature belongs to feature profile selected for the subsciriber.
Old value: Switch Wide	Change to Assigned	The auto transition is possible only if the feature is included in the already selected feature profile. The feature profile data of the feature will be activated in this case	The transition is not possible	Denied	Remains Switch Wide

- In case a Feature Profile is selected for a Subscriber which contains a Feature that is already selected for a subscriber status **Assigned**, the same Feature status will be remained
- In case an **Inherited with Local Data** feature will be set to **Assigned**, the data values of the feature will remain the ones that have been set last in the feature.
- In case an **Inherited** feature will be set to **Assigned**, the data values of the feature will remain the ones that have been set last in the feature (by the Feature profile).
- If no **Inherited with Local Data** status is set in the feature then the data that are stored in the pop up window of feature configuration are lost.
- In case the feature is not configurable the **Inherited with Local Data** assignment status will not be available for the feature status.

The possible transitions from one status to another with Switch Wide features that either belong or not to a Feature Profile are depicted in the table below.

Assignment Status	Feature does not belong to Feature Profile and is not Switch Wide	Feature belongs to Feature Profile and is not Switch Wide	Feature does not belong to Feature Profile and is Switch Wide	Feature belongs to Feature Profile and is Switch Wide
Assigned	Assigned / Denied	Assigned / Inherited / Inherited with Local Data / Denied	Assigned / Denied / Switch Wide	Assigned / Inherited / Inherited with Local Data / Denied
Inherited	-	Assigned / Inherited / Inherited with Local Data / Denied	-	Assigned / Inherited / Inherited with Local Data / Denied
Inherited with Local Data	-	Assigned / Inherited / Inherited with Local Data / Denied	-	Assigned / Inherited / Inherited with Local Data / Denied
Denied	Assigned / Denied	Assigned / Inherited / Inherited with Local Data / Denied	Assigned / Denied / Switch Wide	Assigned / Inherited / Inherited with Local Data / Denied
Switch Wide	-	-	Assigned / Denied / Switch Wide	- (no transition possible with combo box)

3.2.3 Feature Profiles

A Feature Profile (FP) is an administrator-defined set of subscriber features with associated feature data that can be assigned to multiple subscribers. By creating and configuring FPs, the basic feature environment for certain user groups can be maintained at a central place, which dramatically simplifies subscriber feature administration.

FPs can be created at two different levels:

- **Switch level**

  FPs created at the switch level can be assigned to all subscribers on the related switch.
- **Business Group level**

  FPs created within a specific BG (Business Group) can only be assigned to the subscribers of this BG.

Multiple Feature Profiles for every Switch and its BGs can be created.

Feature Profile Management

During FP management features can be added/deleted to/from the FP, or feature attributes can be modified. The following actions are possible for a feature within a feature profile:

- **Add**

  Add this feature to the feature profile or replace any existing definition of the feature data that the feature profile might have.
- **Edit**

  Modify the feature data that the feature profile has. The feature must already exist at the Feature Profile Level.

  If the **Reset Subscriber Lines** is used, the modifications are applied to all subscribers that inherit the related feature from this feature profile.
- **Delete**

  Remove the feature from the Feature Profile

Assignment Status

The status of a feature in a Feature Profile can be one of the following:

- **Not Assigned**

  The feature is not assigned to the profile.

  NOTICE:

  Note that in OpenScape Voice Assistant the **Not Assigned** state is represented as the absence of the feature in the list of assigned features.
- **Assigned**

  The feature is assigned to the profile.

Modifying a feature’s data at the Feature Profile doesn’t change the feature’s assignment state at the Feature Profile.

Default Feature Profile

In every BG a single BG-level FP can be marked as **Default Feature Profile**, i.e. the FP that shall will be automatically assigned to newly created subscribers unless the administrator explicitely deselects it or selects a different one.

When a new BG is created via the **Quick Add Business Group** task, a basic BG-level FP named `FP_<BG name>` is automatically created and marked as Default FP.

System Specific Information

Theoretically, OpenScape Voice supports up to 100,000 Feature Profiles. In practice, however, the actual number of Feature Profiles in use is generally much lower.

Related concepts

Hot Desking on page 273

Night Bell Call Pickup on page 313

OpenScape Voice-based Call Forwarding Features on page 286

Call Pickup Groups on page 309
Directed Call Pickup
Bridged Calls and Privacy
One Number Service on page 280
Serial Ringing on page 277
Simultaneous Ringing on page 278
Simultaneous Ringing Remote Activation on page 279

3.2.4 LoST Servers

OSV has been enhanced to validate the location information received from the phone or provisioned locally on the emergency subnet. This is done via the Location to Service Translation (LoST) interface with the LoST server provisioned on the BG that the location is associated with.OSV caches the location information and routing data mapping. This data is used during emergency calls, in case the LoST server is unreachable or fails to respond.

OSV performs LoST query during new registrations or refresh registrations (when the location of the device changes) in order to validate the location and caches the ESRP SIP URI responses. OSV performs periodic LoST queries whenever the location information to ESRP SIP URI mapping expires.

3.2.5 Mobile Client Profiles

The OpenScape Mobile RTP parameters are moved into a Mobile Client Profile configurable via the OpenScape Voice Assistant and CLI. These profiles can be created System-wide or Business Group-wide. Each user is assigned exactly one Mobile Client Profile. Mobile Client Profiles can be System-wide or Business Group specific. They can be assigned to and used by a subscriber

A Mobile Client Profile defined on a BG-level that is marked as default profile replaces the default profile defined on a system-wide level. When creating a new OSMO subscriber the default BG-level profile is pre-populated as default, and if there is none then the default global mobile client profile is suggested.

3.2.6 LIN Pools

The OpenScape Mobile RTP parameters are moved into a Mobile Client Profile configurable via the OpenScape Voice Assistant and CLI. These profiles can be created System-wide or Business Group-wide. Each user is assigned exactly one Mobile Client Profile. Mobile Client Profiles can be System-wide or Business Group specific. They can be assigned to and used by a subscriber

Using the same ELIN with the same CBN for multiple subnets is needed in order to configure multiple subnets on the same location. Whereas using the same CBN with different ELINs allows the administrator to use one CBN for multiple locations so that the costs can be reduced.

Because of the complexity and the inconsistencies that arise when using the same ELIN and CBN in different LIN pools it will not be possible to use the same ELIN and CBN in different LIN pools. A LIN pool corresponds to a location and gives the ability to have multiple emergency callbacks active for the same location. It does not make sense that some of the ELIN/CBN pairs that are used in a LIN pool are also present in a different LIN pool that is used in another location. If this would be allowed then the LIN pools would have to coordinate because they allocate ELIN/CBN is a round-robin fashion and if an ELIN/CBN pair was allocated from one LIN pool it would have to be somehow indicated in the other LIN pool as well as allocated so that the next available pair is chosen on a subsequent emergency call.

For that reason all locations will be associated with one LIN pool. The LIN pool will be able to contain 1 or more ELIN/CBN pairs. So even 1 ELIN/CBN will create a LIN pool. It will not be possible to create the same ELIN/CBN pair in the same or different LIN pools. The sharing of CBNs will be done by sharing of LIN pools. So each subnet will be able to be associated with none or with one LIN pool but no more than one. The LIN pool could be shared among many subnets. This way there cannot exist subnets that share only some of the same ELIN/CBN pairs but also use distinct ELIN/CBN pairs.

LIN Administration

The LIN (Location Identification Identifier) conveyed with an emergency call is used by the PSAP (Public Safety Answering Point) to query the ALI (Automatic Location Identification) database for important related data, such as location and callback number.

The ALI database must be *pre-populated* with the LINs and their associated data by the responsible operator in advance of any emergency call being dialled.

In case of change in the corporate domain (new/modified/deleted LINs and/or data), ALI data have to be updated manually. There is no *automated* capability to populate the E911 ALI database with LIN records.

Provisioning Aspects

In OpenScape Voice, LIN pools are assigned to IP subnets, representing E911 Emergency Resource Locations.

For each LIN the following parameters are to be specified:

- **Location Identification Number**:

  This is a string of digits with maximum length 20. A leading "+" sign is allowed.
- **Callback Number**:

  The Callback Number is used by the PSAP station to call back to the ERL in case the emergency call was interrupted. If the **Use Default Callback Destination** flag is not set, the callback is propagated to the original caller.

  The Callback number must be a vacant DN and unique throughout the switch.
- **Default Callback Destination**:

  If the **Use Default Callback Destination** flag is not set, the **Default Callback Destination** is only used as a fallback in case the original caller doesn't answer the PSAP callback. The same **Default Callback Destination** (e.g. an attendant position) can be used for different LINs and in different subnets.

  The **Default Callback Destination** must be subscriber.

- **Use Default Callback Destination**

  If this flag is set, a PSAP callback to the LIN’s **Callback Number** is immediately forwarded to the **Default Callback Destination**.

The **Location Information** and **Callback Number**s are mandatory and have to be made available to the PSAP’s ALI DB before an emergency call can be successfully established.

OpenScape Voice supports 100000 LINs per BG.

Signaling Aspects

Delivery of the LIN (and other E911 parameters) to the appropriate PSAP is by way of the PSTN (Public Switched Telephone Network) gateway, using SIP or SIP-Q. The elements used for LIN transport in the private network are:

- Clear text in the SIP body in case if SIP interface
- GNF format in the `From` and `AI` headers when the interface used is SIP

  This allows the OpenScape Voice server to identify that the LIN is a public number with a nature of address (NOA) of International.
- CornetNQ element in case if SIPQ interface

The PSTN interface utilized by the PSAP is traditionally an analog CAMA trunk, although some PSAPs now use an ISDN PRI interface. As CAMA and ISDN/ PRI curcuits do not have the ability to transmit location information the LIN is sent to the PSTN in the Calling Party Number.

An administrable flag in the **Emergency Calling** setup controls **LIN substitution**, i.e. whether OpenScape Voice sends LIN information as a separate information element *in addition* to the calling party number, or 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, if PRI (Primary Rate Interface) is used instead of CAMA (Centralized Automatic Message Accounting).

3.2.7 Policy Stores

ESRP, OSV and the CMP have been enhanced to provide the new functionality that is needed to support policy sets that are stored in a external Policy Store. The web service interface for the ESRP and the Policy Store is using the SOAP protocol.

A Policy Store is using a Web Service for storing and retrieving policies by other functional elements (for example, PSAPs) that define a policy, that is the DownstreamRoutingPolicy for an ESRP. A specific policy set is known by that name and the agency whose policy is being stored or retrieved.

3.3 Station Restriction Features

Station Restriction Features provide *static* limitations on calls originated or terminated at a Business Group’s subscribers and endpoints based on a generic or administrator-defined traffic classification.

Authorization Code

Line Restrictions

Toll and Call Restrictions

With the Authorization Code feature a subscriber can be forced to provide (dial) an authorization code if he or she attempts to set up certain off-net calls.

With the Line Restrictions feature a subscriber can be limited to intra-BG traffic (including or excluding call forwarding and call transfer by an attendant)

With the Toll and Call Restrictions feature a subscriber or endpoint can be temporarily or permanently precluded from making calls of certain traffic types. In addition certain destinations can be explicitely prohibited.

3.3.1 Toll and Call Restrictions

The TRS (Toll and Call Restrictions) feature provides the capability to block an endpoint’s or a subscriber’s access to certain traffic types and/or to a configurable list of destinations. The corresponding entity can be provisioned with a *Standard* and an *Alternate* Class of Restriction, with the possibility of scheduled switchovers and manual switchovers via feature access codes and PIN (the latter for subscribers only).

Traffic Types and Classes of Restriction

The restricted traffic types are declared in so-called *Classes of Restriction* that are used in the Toll and Call Restrictions feature, the Call Forwarding Restrictions feature, the Account Code feature and the BG Authorization Code feature.

The procedure to set up a Class of Restriction can be roughly described in the following way:

1) Define custom Traffic Types, if necessary
2) Assign Traffic Types to new and existing Destination Codes and Code Indexes
3) Create the required Classes of Restriction, comprising those traffic types that shall be restricted in any of the related features

Feature Provisioning

The administrator configures the feature at the endpoint profile, the feature profile or the subscriber level by specifying the following parameters:

- In the **Standard** tab:

  A **Class of Restriction**, that is the set of traffic types that is blocked "by default" for the related endpoints or subscribers. The Standard Class of Restriction may be "null", which means "no restriction".

  Enable Logical Partitioning: Check this flag (`rtp parameter Srx/Main/LogicalPartitioning`) to enable the logical partitioning feature for call and conference scenarios.

  By default this flag is unchecked (`RtpFalse`).

  Logical partitioning allows a PBX (OSV) to be configured in a way that calls that pass through a PSTN gateway cannot connect directly to a subscriber or a PSTN endpoint/gateway in another geographic location even when a feature (such as basic call, call transfer, call forward, call pickup, broadcast call, serial or simultaneous ringing, ONS subscriber using an OND device, EXO, multi-line hunt group (MLHG) and conference) is invoked. This applies both for incoming and outgoing calls when subscribers are involved. Each endpoint and subscriber identify a traffic type that is served through that endpoint (for example PSTN). The intention is to be considered as location, so that a user from a specific location will not be able to reach an endpoint to a restricted location.

  NOTICE: If the logical partitioning feature is enabled:

  – By invoking silent monitoring feature, the supervisor will be able to monitor a (conference) call even if he is not allowed to connect directly with one of the conference participants. However the supervisor will not be able to barge-in/whisper the (conference) call and become an active member of the conference.
  – Emergency calls are allowed even if the subscriber/endpoint is not allowed to connect to the subscriber/endpoint that is used as an emergency destination.
  – In order for a subscriber to initiate a 1-way or 2-way speaker call with a member of a community group, that particular member must be provisioned as DN (Directory Number) in another community group and also be allowed to connect directly to the subscriber, in accordance with logical partitioning restrictions. There should be 1:1 mapping between community group DNs (Directory Numbers) and members.
  – A subscriber that is behind an associated endpoint complies with the specific logical partitioning restrictions of that endpoint.

  Traffic Location: When the logical partitioning is enabled, you can configure for each subscriber as well as for each endpoint profile the new Traffic Location entry. Choose the **Traffic Location** entry from the traffic types. Click the "**...**" and select the Traffic Type from the list, to be used as Traffic Location.
- A **Blocked Call List**, which may comprise DNs (Directory Numbers) or partial DNs such as area codes. Those codes may also comprise wild cards representing "any digit".

- In the **Alternate** tab:

  An **Alternate Class of Restriction** for both scheduled switchover and manual CoSS (Class of Service Switchover) with access code and PIN. Typically, the **Alternate Class of Restriction** will be a superset of the **Standard Class of Restriction**.

  The **Allow COSS Feature Access Codes** parameter determines the activation/deactivation of Class Of Service Switchover.

  The **Enable Duration Timer** parameter determines the duration timer for the manual COSS activation.

  The **Switchover Duration** parameter determines the duration of a manual switchover. This applies to subscribers only.

  The **Schedule Overrides Duration** which allows you to enable or disable the switchover duration to override the day schedule
- **Day Schedule** items, specifying the planned intraweek switchovers between **Standard** and **Alternate Class of Restriction** for regular calendar weeks. This schedule comes in handy for daily closings and weekends.
- **Date Schedule** items, specifying the planned switchovers for particular date ranges such as bank holidays or annual closings.

  If specified, this will override the Day Schedule for those dates.

> **NOTICE:**
>
> A maximum of 168 Date Schedule items per service assignment is allowed, with a maximum of 14 items per month.

Functional Sequence

When OpenScape Voice detects that a restricted subscriber or endpoint is attempting to originate a call, it determines if the dialed digits represent a permitted destination:

- if the dialed digits are permitted, the call proceeds normally.
- if the dialed digits are prohibited, the system routes the call to an announcement or to reorder tone. The treatment can be assigned on a per-subscriber or per-group basis.

Subscriber Rerouting and Toll and Call Restrictions

A system-wide option `Srx/Main/InvokeTRSOnRerouting` determines, whether toll restrictions shall be bypassed (`RtpFalse`) or not (`RtpTrue`) on the subscriber rerouting call leg. Its default value is `RtpFalse`, i.e. Toll and Call restrictions won’t be applied.

Related Features

The Authorization Code feature allows the subscriber to dial authorization code in order to unblock certain restricted traffic types.

If both TRS and Authorization Code feature are active, the TRS takes precedence.

Related concepts

Traffic Types

Classes of Restriction on page 555

3.3.1.1 Manual Class of Service Switchover

A subscriber or CSTA application can dial a feature access code together with a personal PIN to perform a manual CoSS (Class of Service Switchover) between **Standard** and **Alternate Class of Restriction**.

Manual CoSS takes precedence over **Day/Date Schedule**s. That is, if a subscriber initiates a switchover, then it is valid for a configurable **Switchover Duration**, irrespective of the configured **Day/Date Schedule**. After the **Switchover Duration** has expired, the **Day/Date Schedule** (if any) takes effect.

Functional Sequence

If provisioned by the administrator, a subscriber or CSTA application can dial the feature access code

- **CoSS Activate** to switch to his/her **Alternate Class of Restriction**
- **CoSS Deactivate** to switch to his/her **Standard Class of Restriction**

NOTICE:

Dialing a CoSS feature access code if no **Alternate Class of Restriction** is defined is rejected with an announcement.

The required **PIN** can be dialed en-block or can be entered after receiving the announcement from the media server.

Multiple PIN support

In order to support multiple users sharing the same line (subscriber), the number of PINs per line was increased to 5.

If CoSS is successful, then the index (between 1and 5) of the user- dialed PIN is stored in service activation/deactivation CDRs (Call Detail Records) to distinguish which user activated/deactivated the CoSS feature.

If a user (or a different user by using its own PIN) performs CoSS activation twice on the same phone, then the activation is successful with duration value updated and a new activation CDR is generated. Similarly, if the CoSS service is activated by one user but deactivated by another user (using a different PIN), then the deactivation is successful.

3.3.2 Business Group Authorization Codes

The BG (Business Group) Authorization Code feature provides the capability to control a subscriber’s access to certain (off-net) traffic types. When attempting to set up a call of a restricted traffic type, the subscriber has to enter (dial) a valid authorization code.

Traffic Types and Classes of Restriction

The restricted traffic types are declared in so-called *Classes of Restriction* that are used in the Toll and Call Restrictions feature, the Call Forwarding Restrictions feature, the Account Code feature and the BG Authorization Code feature.

The procedure to set up a Class of Restriction can be roughly described in the following way:

1) Define custom Traffic Types, if necessary
2) Assign Traffic Types to new and existing Destination Codes and Code Indexes
3) Create the required Classes of Restriction, comprising those traffic types that shall be restricted in any of the related features

Functional Sequence

The administrator defines the valid Authorization Codes, assigns the Feature to certain subscribers and (optionally) creates a Prefix Access Code for the **Authorization Code** vertical service in the appropriate numbering plans, to allow the subscribers to pre-dial the authorization code.

The subscriber can pre-dial the authorization code, or can post-dial it when prompted to do so.

To set up a call of a traffic type that is not toll-restricted but requires an authorization code, the subscriber proceeds as follows: dials the Public Network Access Code. If an Account Code is also required, the subscriber enters the Account Code first, then presses the # key. At that point, the subscriber does one of the following:

- **Pre-dialing**:

  After entering the Associated Authorization Access Code, the system prompts the subscriber to enter the authorization code. After the Authorization Code is accepted, the system provides another prompt to enter the called number.
- **Post-dialing**:

  The subscriber dials the called number; the system then prompts the subscriber to enter the Authorization Code.

Regardless of the sequence in which the digits are entered, the following takes place after the system attempts to validate the Authorization Code:

- If it is valid, the call completes normally.
- If it is invalid, the system prompts the subscriber to re-enter the Authorization Code. If the second entry is also invalid, the call is given intercept treatment; the caller may instead hear reorder tone.

System Specific Information

An Authorization Code can be from 2 to 14 digits long.

Up to 100,000 Authorization Codes are supported, with a maximum of 50,000 per BG.

Accounting

If **Message Detail Recording** is active for the related BG, information about Authorization Code utilization is included in the Billing Files. The activation can be performed from the Assistant.

Support of Private / Business Call

OpenScape Voice support of Private / Business call is achieved by using the BG authorization code feature. When configuring an authorization code it is possible to optionally assign a subscriber number and set the type to 'Private' or 'Business'. That user is then able to lift all restrictions and make a 'private' or 'business' call from any device that has the 'BG authorization code' feature assigned by using their 'private' or 'business' authorization code.A 'private' call is a 'personal' call in contrast to a 'business' call. In both cases the subscriber number to whom the authorization code belongs is written in the 'paying party' field of the CDR and a flag 'private call' or 'business call' respectively is set in the 'Per call feature extension' field in the CDR. The customer -if desired- may assign the costs of a 'private' call personally to the user making the call.It is also possible to set the type for an authorization code but not assign it to any specific subscriber. In this case only the 'private'/'business' call flag is set in the CDR but not the paying party. This configuration can serve as a general PIN for making e.g. private calls. In this case the call shall be charged to the device where the call was made and not to the user who made the call.

Related concepts

Traffic Types

Classes of Restriction on page 555

3.3.3 Line Restrictions

The Line Restrictions feature lets the administrator restrict the calls permitted to and from a given station. Originating line restrictions refers to restrictions on calls placed from a station; terminating line restrictions refers to restrictions on calls being terminated at a station.

The administrator can assign this feature to the entire BG (Business Group) or to individual subscribers.

Because line restriction is not a visible subscriber service, it does not increment a visible usage counter.

Functional Sequence

OpenScape Voice checks line restrictions before completing calls and performing call transfers. If a call is found to be in violation of configured restriction levels, the system routes the call to error treatment and subsequently releases it.

Other Characteristics

The line restrictions feature is known as station restriction, too.

3.3.3.1 Semi-Restricted Lines

Calls originated at a semi-restricted line and directed to a line outside of its business group and/or calls directed to a semi-restricted line from a line outside of its business group are routed to error treatment (usually reorder tone or special intercept announcement).

Semi-restricted lines have indirect access to and from lines outside the business group for the following types of calls (provided that the appropriate features are available):

- Calls from outside the business group and forwarded to the semi-restricted line by a non-restricted DN.
- Calls from outside the business group and transferred to the semi-restricted line by a non-restricted DN.
- Calls from outside the business group and picked up at the semi-restricted line.
- Calls from a semi-restricted line to an non-restricted business group and forwarded to an outside line.
- Calls from a semi-restricted line to a non-restricted DN and transferred at the DN outside the business group.

The administrator can assign a semi-restricted line to a DN on an originating basis, on a terminating basis, or both.

3.3.3.2 Fully-Restricted Lines

A fully-restricted line has all of the attributes of an semi-restricted line. In addition calls directed to a fully-restricted line from the business group attendant, as well as calls originated at a fully-restricted line and directed to the business group attendant, are routed to error treatment (reorder tone or special intercept announcement).

A fully-restricted line does not have indirect access of any sort to or from lines outside the business group; this should include multiply-forwarded calls.

The administrator can assign a fully-restricted line to a DN on an originating basis on a terminating basis, or both.

3.3.3.3 Fully-Restricted Lines with Attendant Access

A fully-restricted line with attendant access can access the attendant for information and to requests transfers to another DN within the business group. OpenScape Voice does not permit the attendant to transfer a DN with this restriction to points outside of the business group, as well as attempts by the attendant to transfer calls from outside the business group to a DN with this restriction.

All other characteristics of fully-restricted lines are also present.

The administrator can assign a fully-restricted line with attendant access to a DN on an originating basis, on a terminating basis, or both.

3.4 Calling Services

Calling Services features are available for the OpenScape Voice supported SIP endpoints, including Unify SIP telephones, the softclient, the OpenScape UC Application Personal Edition, and third-party SIP endpoints. For the applicable services detailed information is given about local and OpenScape Voice-based features available to the end user.

3.4.1 Account Codes

The Account Code feature allows subscribers to insert a number into the CDR (Call Detail Record) for later allocation of charges. It is typically used for off-line billing and account reconciliation. For example, a lawyer can use this feature to charge a client (identified by an Account Code) for long-distance calls in addition to the usual consultation fee.

NOTICE:

Account Codes are optional and can be entered freely by the subscriber. OpenScape Voice does not maintain any lists of valid Account Codes. Only their "well-formedness" (digits only, length) will be checked.

NOTICE:

The Message Details Records feature for BG must be active in order to include the Account Code in the CDR file.

Pre-dialing vs. Post-dialing

For every switch, the administrator decides, whether Account Code pre-dialing or post-dialing shall be used.

No matter if pre- or post-dialing is used, if an Account Code shall be entered for a call that also requires an Authorization Code, the Account Code must be entered first.

Account Code Pre-dialing

When contained in a Speed Calling list, CSTA MakeCall, SIP phone using a Repertory Dial key, or other en-bloc digit entry method, the dialing sequence is: <Account Code Activation Code><Account Code>#<target DN>

In order to provison Account Code pre-dialing, the *administrator* ...

1) Sets the **Account Code Use** to Pre Dial
2) specifies the minimum and maximum allowed length of an Account Code. Both minimum and maximum length can be between 1 and 14; defaults are 2 and 14, respectively
3) creates a Prefix Access Code for the **Account Code** (activation) vertical service in the appropriate numbering plan(s).
4) assigns the Account Code feature to selected subscribers

Account Code Post-dialing

To use the Account Code feature in a post-dialing switch, the subscriber typically

1) dials the target DN
2) receives a prompt tone or announcement
3) enters the Account Code or - if no Account Code is desired - enters # or *

When contained in a Speed Calling list, CSTA MakeCall, SIP phone using a Repertory Dial key, or other en-bloc digit entry method, the dialing sequence is: <target DN>#<Account Code>

In order to provison Account Code Post-dialing, the *administrator* ...

1) Sets the **Account Code Use** to Post Dial
2) creates and assigns a Class of Restriction that comprises those traffic types for which an Account Code shall be requested; note that for call destinations with **Emergency** traffic type, an Account Code is **never** requested
3) defines the acknowledge type to **Tone** or **Announcement**
4) Enter the **Delay Timer** value (in seconds) to set the Time Delay before playing the Prompt Tone to collect Account Code digits
5) defines the maximum length of a valid account code (positive integer; default: 16)

   Note that the subscriber is free to enter a shorter code by terminating it with the # key
6) optionally creates a system-wide set of DN prefix patterns to be excluded from requiring account codes.

   Such a pattern may consist of digits and the wild card character "%", representing "any digit". For example "1%%%555" means "exclude every DN starting with 1+<NPA>+555".

   Default is an empty string.
7) assigns the Account Code feature to selected subscribers

NOTICE:

In the current implementation, if the subscriber is provisioned for Account Code Service and the call destination has unspecified traffic type, an Account Code is always requested.

Related concepts

Traffic Types

Classes of Restriction on page 555

3.4.2 Call Completion to Busy Subscriber / on No Reply

The CCBS/NR (Call Completion to Busy Subscriber / on No Reply) feature provides subscribers the capability to activate an automatic callback if the called station is busy or is not answering an alerting call.

Functional Sequence

The calling to another subscriber wasn’t successfully finished. The activated CCBS/NR feature works as follows:

- If the called party was busy

  Monitoring begins and the calling party hears a confirmation announcement that the request is received. The called party has no notification of the callback request.

  As soon as the called party goes onhook, the calling party is notified of the called party’s availability and is recalled. When the calling party answers, a new call to the original destination is automatically dialed.
- If the called party did not answer the alerting call

  Monitoring begins and the calling party hears a confirmation announcement that the request is received. The called party becomes available for callback after initiating some activity on the device, then transitioning to idle state.

  As soon as the transition to the idle state occurs, for example, when the called party goes onhook, the calling party is notified of the called party’s availability and is recalled. When the calling party answers, a new call to the original destination is automatically dialed.

  When the called party becomes available to handle the call, the calling party receives a recall that provides the name and number of the called party. The information displayed is consistent with the settings for other features used to control delivery or suppression of calling and called party numbers. However, the callback must be invoked by a SIP subscriber in order for the displays to be provided.
- During these requests, OpenScape Voice supports service retention, which ensures that the CCBS/NR request continues to be active until the target of the request is alerted. However, for interswitch calls, the originating switch must support this functionality in order for it to operate.
- The system administrator can assign one or both of the following to a subscriber:
  - The ability to activate a CCBS/NR request.
  - The ability to deny callbacks placed against the subscriber via the Deny Terminating Features attribute.
- When a CallBack is initiated by an OpenScape Mobile-enabled subscriber, the CallBack recall is routed to A-side using the OpenScape Mobile auto-pilot routing. The routing is the following for OpenScape Mobile auto-pilot routing:
  - The callback request arrives first at the OpenScape Mobile client and then, if the OpenScape Mobile client does not answer or if the client is not registered, the call is routed to DeskPhone (ONS).

NOTICE:

OpenScape Mobile auto-pilot routing is used regardless of the preferred device

Interworking

CCBS/NR is not only supported intraswitch between OpenScape Voice subscribers, but also for the following interswitch scenarios:

- Between subscribers on different OpenScape Voice systems
- Between an OpenScape Voice subscriber and a SIP-Q gateway with a QSIG-compliant PBX subscriber.

- In transit scenarios comprising OpenScape Voice systems and SIP-Q. gateways.

Other Characteristics

The OpenScape Desk Phone CP 100/200/205/400/600/600E/700/700X support this feature.

Computer Supported Telecommunications Applications (CSTA) also supports activation of CCBS/NR requests.

The SIP-Q interface has been enhanced to support incoming CC requests with path reservation signalling.

This feature is formerly known as automatic callback or auto callback.

3.4.2.1 RTP System Parameters

Certain aspects of CCBS (Call Completion on Busy Subscriber) and CCNR (Call Completion on No Reply) are controlled on a systemwide basis by RTP (Resilient Telco Platform) system parameters. Any changes made to these parameters affect all business groups and their members. Typically, these parameters are set during initial system configuration, to enforce global system policies and ensure proper feature interworking.

The following tables present the Call Completion related RTP system parameters. Default values are shown in bold type.

While some of these parameters either affect either CCBS or CCNR, others affect both Call Completion services.

Table 12: RTP System Parameters related to CCBS only

Parameter	Values	Description
Srx/Service/CCS/CCBSFeatureAssignedPerOffice	RTPTrue (True) **RTPFalse** (False)	This parameter enables and disables CCBS.
Srx/Service/CCS/CcbsRequestOperationT2	1 to 5 sec. default: **3** sec.	This parameter defines the T2 call completion request supervision timer, which runs on both sides. It determines how long the monitoring process waits for a response after requesting subscriber status (busy or idle) from the signaling manager.
Srx/Service/CCS/CcbsServiceDurationT3	15-2880 min. default: **30** min.	This parameter defines the service duration timer, which runs on the originating side. It specifies the maximum time a CCBS request remains active.

Parameter	Values	Description
Srx/Service/CCS/CcbsServiceSupervisionT7	15 to 2800 min. default: **30** min.	This parameter defines the T7 call completion supervision timer, which runs on the terminating side. It specifies the maximum time a call completion request is maintained before getting deleted.
Srx/Service/CCS/ MaxNumInCCBSActivationsAllowedPerCustomer	1 to 5 default: **3**	This parameter defines the maximum number of CCBS requests per destination.
Srx/Service/CCS/ MaxNumOutCCBSActivationsAllowedPerCustomer	1 to 5 default: **3**	This parameter defines the maximum number of CCBS requests per originator..
Srx/Service/CCS/CCBSActivationCCS	**True**, False	This parameter allows the activation of CCBS via access code. If set to False, no CCBS will be allowed

Table 13: RTP System Parameters related to CCNR only

Parameter	Values	Description
Srx/Service/CCS/CCNRFeatureAssignedPerOffice	RTPTrue (True) **RTPFalse** (False)	This parameter enables and disables CCNR.
Srx/Service/CCS/CcnrRequestOperationT2	1 to 5 sec. default: **3** sec.	This parameter defines the T2 call completion request supervision timer, which runs on both sides. It determines how long the monitoring process waits for a response after requesting subscriber status (busy or idle) from the signaling manager.
Srx/Service/CCS/CcnrServiceDurationT3	15-2880 min. default: **30** min.	This parameter defines the service duration timer, which runs on the originating side. It specifies the maximum time a CCNR request remains active.
Srx/Service/CCS/CcnrServiceSupervisionT7	15 to 2800 min. default: **30** min.	This parameter defines the T7 call completion supervision timer, which runs on the terminating side. It specifies the maximum time a call completion request is maintained before getting deleted.

Parameter	Values	Description
Srx/Service/CCS/ MaxNumInCCNRActivationsAllowedPerCustomer	1 to 5 default: **3**	This parameter defines the maximum number of CCNR requests per destination.
Srx/Service/CCS/ MaxNumOutCCNRActivationsAllowedPerCustomer	1 to 5 default: **3**	This parameter defines the maximum number of CCNR requests per originator.
Srx/Service/CCS/CcnrOnAnswer	True, **False**	This parameters indicates if CCNR activation is allowed after an answered call.

Table 14: RTP System Parameters related to CCBS and CCNR

Parameter	Values	Description
Srx/Service/CCS/CcsRecallTimerT4	15 to 60 sec. default: **30** sec.	This parameter defines the T4 recall supervision timer, which runs on the originating side. It is started upon sending a recall indication to the calling user and is stopped on receipt of an answer to this indication.
Srx/Service/CCS/CcsIdleGuardT8	1 to 15 sec. default: **5** sec.	This parameter defines the destination B idle guard timer, which runs on the terminating side. It specifies the amount of time the system waits after destination B has become available before recalling user A.
Srx/Service/CCS/CcsRecallT9	15 to 60 sec. default: **35** sec.	This parameter defines the T9 recall supervision timer, which runs on the terminating side. It is started upon sending a recall indication to the calling user and is stopped on receipt of an answer to this indication.
Srx/Service/CCS/CcsRecallT9_EXT	5 to 1800 sec. default: **35** sec.	Similar to CcsRecallT9, but for external (SIPQ) callers. For networks supporting suspend/resume the recommended setting is CcsRecallT9_EXT = CcsRecallT4 + 5 Otherwise CcsRecall T9_EXT should be adjusted to a value equal or slightly less than CcnrServiceSupervisionT7 or CcbsServiceSupervisionT7 (whose default value is 1800 sec).

Parameter	Values	Description
Srx/Service/CCS/CCSSCallIndSupport	**RTPTrue** (True) RTPFalse (False)	This parameter indicates if the CCS call indication is supported.
Srx/Service/CCS/CCSHandleAsEmergencyCall	**0** (no) 1 (yes)	This parameter indicates if a callback needs to be handled as an emergency call if the entire bandwidth is reserved.
Srx/Service/CCS/CCSCacTimerForReleaseB	3 to 999 min. default: **14** min.	This parameters defines the execution retry timer that runs on the terminating side. It defines the time between an unsuccessful execution attempt and the next one.
Srx/Service/CCS/CCSCacTimerForReleaseA	3 to 999 min. default: **14** min.	This parameters defines the recall retry timer that runs on the originating side. It defines the time between an unsuccessful recall attempt and the next one.

Related concepts

RTP Management via OpenScape Voice Assistant on page 961

3.4.3 Deny Terminating Features

The administrator can assign the ability to deny callbacks placed against the subscriber via the Deny Terminating Features attribute.

Related concepts

Call Completion to Busy Subscriber / on No Reply

3.4.4 Click to Answer

The Click-to-Answer feature provides the capability for a SIP endpoint to use a command of certain third-party applications, for example, the Genesys Agent Console application, to answer a SIP call when it is presented. As a result of the command, an answer event is generated and is passed via OpenScape Voice.

This feature is applicable to a subscriber who is also a call center agent on the applicable third-party call center application and can control calls presented through the console application.

Functional Sequence

The application lets the subscriber:

- answer calls
- make calls
- transfer calls

- perform other useful functions.

Other Characteristics

The associated SIP endpoint must be an OpenScape Desk Phone CP.

This functionality is not applicable to keyset telephones.

3.4.5 OpenScape Voice-based Do Not Disturb

The Do Not Disturb (DND) feature provides a subscriber the capability to block incoming calls during periods of time that the subscriber does not wish to be disturbed. Features such as CFSIE-DND and endpoint-based call forwarding on busy can be used to redirect the calling party to another destination while DND is active.

The subscriber can continue to originate calls while DND is active.

Functional Sequence

If DND is active, incoming calls are handled in one of the following ways:

- If an applicable call forwarding is active, the call is diverted to the configured forwarding target
- Otherwise the call is either rejected with SIP message "480 Temporarily Unavailable" (default for external calls) or the call is diverted to an intercept announcement that indicates the reason the call cannot be completed to the expected destination (standard for internal calls).

The administrator defines the behaviour *for external calls* by setting the RTP parameter `Srx/Main/DNDAnnAlways` either to RtpFalse (reject with 480) or RtpTrue (announcement).

Subscribers have to be provisioned for the DND feature in order to be able to use server-based DND.

OpenScape Desk CP telephones should be configured for uaCSTA and Server Based Features. To allow the server-based feature to be de-/activated from generic SIP phones, Prefix Access Codes for the **DND De-/Activate** vertical services have to be created in adequate numbering plans.

Other Characteristics

Unify SIP endpoints also provide an endpoint-based DND feature. However, if configured and active, the OpenScape Voice-based feature takes precedence over the local feature. Server- and endpoint-based DND shouldn’t be active at the same time.

Related concepts

CFSIE - Do Not Disturb on page 299

RTP Management via OpenScape Voice Assistant on page 961

3.4.6 Last Incoming Number Redial

The LINR (Last Incoming Number Redial) feature provides subscribers the capability to perform an activation procedure that automatically sets up a call to the last incoming number.

The incoming number stored can be any of the following:

- The last incoming call that alerted at the subscriber endpoint
- A call retrieved via directed call pickup or group call pickup
- A call retrieved from manual hold.

The subscriber need not know the telephone number of the last incoming call.

The administrator can allow the subscriber to activate LINR for callers who have their calling identity suppressed.

Functional Sequence

OpenScape Voice places a call to the last incoming number stored and the following takes place:

- If the called party is idle: The call begins alerting normally.
- If the called party is busy: The calling subscriber hears busy tone. To camp on to the called party’s station, the subscriber must enter the CCBS access code.

Other Characteristics

This feature is formerly known as automatic recall, auto call, and return call.

3.4.7 Last Outgoing Number Redial

The last outgoing number redial (LONR) feature provides subscribers the capability to perform an activation procedure that automatically sets up a call to the last outgoing number. The subscriber need not know the telephone number of the last outgoing call.

Functional Sequence

The subscriber must activate the LONR feature at the station.

OpenScape Voice places a call to the last outgoing number dialed and the following takes place:

- If the called party is idle:

  The call begins alerting normally.
- If the called party is busy:

  The calling party hears busy tone and can manually activate a callback request if desired.

System Specific Information

LONR attempts can be also limited to intraswitch calls only (calls between business group members) by administrator.

LONR cannot be successfully performed if the called party has station call forwarding: all calls or CFSIE-all active.

Other Characteristics

OpenScape Voice's multiple time zone support capabilities ensure that the correct date and time information is used.

The CCBS/NR feature can be used to camp on to the called party's station if the called party is busy at the time of LONR activation.

Unify SIP endpoints also have local features that simplify redialing of calls.

3.4.8 Multiple Address Appearances

The MAA (Multiple Address Appearances) feature permits the availability of one or more non-shared lines on a single device. A device contains at least one main DN, and can be configured with other DNs in addition to the main DN.

Each MAA line operates local to the device, including line status and call processing. An MAA line can appear on another device by using the multiple contacts feature.

Because MAA lines operate locally, when multiple contacts are in use, each device has simultaneous access to the associated MAA on their device. No status information is shared between the MAA multiple contacts.

Other Characteristics

The MAA non-shared line is configured for the SIP subscriber endpoint with a line type of private. OpenScape Voice views these lines as a basic registration.

3.4.9 Multiple Contacts

The Multiple Contacts feature permits multiple SIP devices to register with the same DN. This ability is especially useful for mobility subscribers because it eliminates the need for separate DNs to be established for office and offsite devices.

Functional Sequence

A subscriber may originate a call from a device (using the DN) independent of the use of the other devices registered as multiple contacts for the same DN.

When a subscriber receives an incoming call, the following instances take place depending on whether the multiple contact devices are idle and whether the subscriber has the attribute **Simultaneous calls not allowed from multiple contacts** enabled:

- When all multiple contact devices are idle:

  Each device is alerted. When one of these devices answers the call, the alerting to the other devices stops.

- When one or more devices are in use:

  OpenScape Voice presents the second call to the device in use as a call waiting (camp-on) call.

  The other idle devices are simultaneously alerted.
- When the subscribers' attribute **Simultaneous calls not allowed from multiple contacts** is enabled and one or more devices are in use:

  OpenScape Voice presents the second call to the device in use as a call waiting (camp-on) call. The other idle devices are not alerted.

  When the device in use returns a Busy notification, then the second call is declined with Busy indication.

Other Characteristics

It is highly recommended that all multiple contact devices be under the control of one subscriber, rather than being shared by multiple subscribers. If multiple subscribers are involved, incoming calls may not be answered by the correct subscriber because incoming calls are distributed to all multiple contact devices.

This feature also ensures that notifications, like message waiting notifications, are transmitted to all registered contacts for the subscriber.

Multiple Contacts vs. Multiline Appearance (Keyset)

The Multiple Contacts feature applies to non-keyset lines only. Keyset enforces line usage, therefore a keyset line can only be used for making or receiving calls, if all its appearances are idle.

On the terminating side, if a second call arrives while there's an ongoing call on a keyset line, only the active phone is alerted.

Multiple Contacts vs Circuit and OpenScape Mobile clients

Circuit and OpenScape Mobile clients are not considered multiple contacts of the subscriber who is using the clients. They register on special subscribers with the indication of OpenScape Mobile Device and act as OND devices for the ONS subscribers.

Related concepts

Multiline Appearance on page 258

3.4.10 Executive Busy Override

The Executive Busy Override feature (also known as Executive Override) provides the capability for an authorized subscriber to bridge into a busy line.

The Executive Busy Override feature gives three capabilities to a subscriber:

- Override

  The subscriber can perform busy overrides.
- Block Override

  The subscriber is protected from overrides by other subscribers.

- Override and Block

  The subscriber can perform busy overrides, but is protected from overrides by other subscribers.

Functional Sequence

The administrator assigns the override and block overide capabilities to certain subscribers and creates Prefix Access Codes for the **ExecutiveOvrRide** service in the appropriate numbering plans.

The subscriber typically uses the feature after first encountering a busy line. The subscriber goes offhook and enters the Executive Busy Override access code, followed by the DN of the subscriber who is the target of the override. After doing so, one of the following takes place:

- If the called party is idle, a normal connection is made.
- If the called party is busy, the two original parties hear an intrusion tone and the overriding party is connected into the existing call with the other two parties, creating a three-way conference.

System Specific Information

Executive Busy Override cannot be initiated:

- If the called party’s DN blocks override attempts
- If the called party is not in a stable call state (for example, if the DN is on hold dialing, or ringing)
- At a DN which already has two calls (for example, an active call and a held call)
- At a DN engaged in a conference.

Depending on the reason it cannot be initiated, the following takes place:

- If the called party's DN is in state that temporarily does not allow Executive Busy Override, the initiator hears a busy tone and sees a corresponding display on the SIP endpoint.
- If the called party cannot implement Executive Busy Override because of an incompatible device or if override attempts are blocked, The initiator hears error tone and sees Connection Refused on the SIP endpoint display.

Related concepts

Intrusion on page 158

Forced Release Intrusion on page 160

3.4.11 Intrusion

Intrusion permits a calling party in the SIP-Q private network with appropriate permissions to intrude upon a busy destination and form a 3-party conference.

Currently only OpenScape 4000 and OScAR-Pro (OpenScape Alarm and Response server - Professional, formerly known as DAKS) support originating a call and invoking intrusion against a busy OSV subscriber. OpenScape Voice does not support originating an Intrusion when the destination is located in the SIP-Q network.

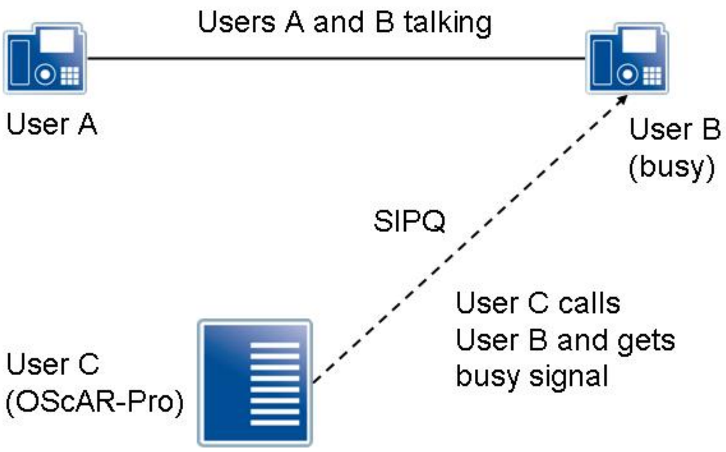


Figure 8: Before

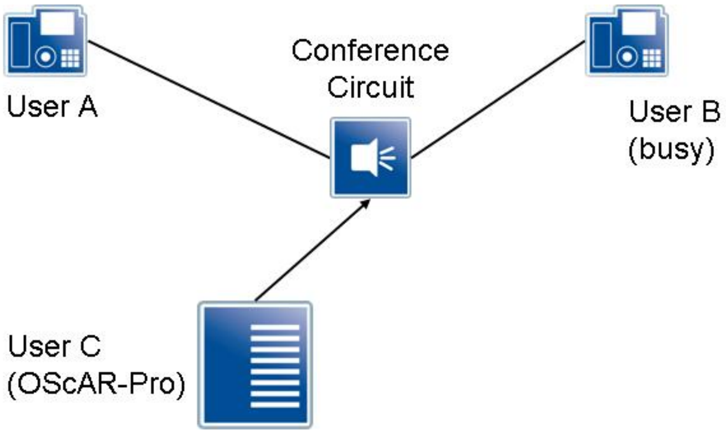


Figure 9: After

Executive Intrusion (Terminating Only)

A voice service that permits a subscriber (or OScAR-Pro), with appropriate permissions, to intrude upon a busy destination as long as the destination allows intrusion.

Currently, the subscriber protection parameter for Executive Busy Override is reused by the Executive Intrusion service to allow/block intrusion. So in order to protect a subscriber from Executive Intrusion, he or she has to be provisioned for **Executive Busy Override** with either the **Block Override** or **Override and Block** option selected.

IMPORTANT:

The parameter **Block Override** applies both to Executive Intrusion and Forced Release Intrusion.

Emergency Intrusion (Terminating Only)

A variant of Intrusion where an emergency operator or OScAR-Pro with appropriate permissions can intrude upon a busy destination.

OScAR-Pro may provide a high priority audio message to the destination.

OpenScape Voice flaggs Emergency Intrusion calls as "Emergency Calls" i.e. they are not subject to Call Admission Control.

Intrusion Conference

Depending on which user leaves the conference first, when Users A and B are connected and User C overrides B:

- if A disconnects, C and B remain connected
- if B disconnects, A and B call is cleared, C recalls B
- if C disconnects, A and B remain connected

When 2 users remain, the conference shall be dropped and the call transitions to 2-party talk state and release the conference circuit.

Facility Rejection

There are several reasons for not accepting an intrusion request, e.g.

- no conference circuit available
- target user is protected against intrusion
- target user is not in a stable 2-party call

In any case, the calling party may still attempt to invoke another service (e.g., CCBS).

Related concepts

Executive Busy Override on page 157

Direct Return Call from Emergency Center on page 251

Forced Release Intrusion on page 160

3.4.12 Forced Release Intrusion

Forced Release Intrusion allows a caller, when reaching a busy destination, to forcefully clear the callee’s current connection. OpenScape Voice supports Forced Release Intrusion requests originating in the SIP-Q private network and terminating at a local subscriber. Subscriber invocation of Forced Release is not supported.

OSV (OpenScape Voice) will only execute the request, if the target subscriber is in a stable voice call (that hasn’t been established via Forced Release Intrusion) or large conference and is not administratively protected against Forced Release Intrusion.

> **IMPORTANT:**
>
> The parameter **Block Override** shall be used from the subscriber in order to prevent a forced release when he/she is busy. This parameter applies both to Executive Intrusion and Forced Release Intrusion.

If this is the case, OSV will either

- clear the subscriber’s stable 2-party call, or
- remove the subscriber from his/her current conference

in order for the intruder and the now-idle subscriber to connect into a new call.

NOTICE: There is no warning tone or announcement provided to the called party and call partner(s) prior to releasing the call.

Because the SIP phone/client does not support facility invocation when busy, the feature requires that the called user goes on-hook after the forced release. Then, the called user is immediately called and, upon answer, is joined into a connection with the caller that invoked the forced release.

NOTICE:

The caller may require Terminating Feature Override capabilities in order to successfully establish the call to the intended subscriber.

If Forced Release Intrusion can't be performed and if the caller may not invoke additional services against the busy subscriber such as CCBS (Call Completion to Busy Subscriber) or Executive Intrusion, OSV terminates the "intrusion call".

A call with forced release permission is subject to CAC (Call Admission Control) unless it includes a classmark for "Emergency Call".

Provisioning

Currently, the subscriber protection parameter for Executive Busy Override is reused by the Intrusion service to allow/block forced release. So in order to protect a subscriber from Executive Intrusion, he or she has to be provisioned for **Executive Busy Override** with either the **Block Override** or **Override and Block** option selected.

Limitations

Forced Release Intrusion

- is not supported for subscribers behind a branch that is in survivability mode
- is currently not indicated in the CDRs

Related concepts

Intrusion on page 158

Executive Busy Override on page 157

Terminating Feature Override (SIP-Q) on page 161

3.4.13 Terminating Feature Override (SIP-Q)

An incoming SIP-Q call may request one or more terminating features to be overridden at the called party, i.e. not to be invoked for that call. For example, an attendant making an urgent call for a particular user wants to terminate to the called party number and not be call forwarded to anyone else.

Any incoming SIP-Q call terminating to an OSV subscriber is checked for CF, DND and Call Pickup Override classmarks. When Override is indicated, the overridden feature(s) shall not be executed if active at the destination.

NOTICE:

Older SIP phones/clients may not support the new feature overrides.

Currently, OSV subscribers can’t be protected against Override requests.

Override Call Pickup

When an incoming call indicates Override Call Pickup and the destination belongs to a pickup group, the group members will *not* be notified of this call. If a directed pickup is attempted, it will be rejected with appropriate response/ cause value.

Override Call Forwarding

When an incoming call indicates override of CF (Call Forwarding), both phone-based and switch-based CF features (if any) shall be disabled for this call. The call will be delivered to the original destination, if possible.

Override Do Not Disturb

When an incoming call indicates override of a DND (Do Not Disturb) both phone-based and switch-based DND features (if any) shall be disabled for this call. The call will be delivered to the original destination rather than cleared or forwarded.

Related concepts

Forced Release Intrusion on page 160

3.4.14 Extension Dialing

The Extension Dialing is a feature applicable inside a business group. The feature allows a subscriber in a business group to dial other subscribers in the same business group by dialing an abbreviated number that is synonymous with the extension number.

Extension dialing permits the dialing of intragroup calls on a 1- to 7-digit basis. An extension-dialed call is an intragroup call dialed using a digit sequence assigned to extension dialing.

Functional Sequence

When a digit sequence assigned to extension dialing is entered at a station, OpenScape Voice can convert extension to the directory number of the called station. After OpenScape Voice determines the DN of the called station, it completes the call in the normal manner.

The extension dialing feature is assigned to the business group as a whole; after it is assigned, all stations within the business group have the feature.

System Specific Information

Any of the fully or semi-restricted limitations and restrictions of the group or station also apply to calls dialed by extension.

Other Characteristics

Per-group traffic measurements of all extension-call attempts and durations are available.

Extension dialing is also known as station-to-station dialing.

3.4.15 Selective Call Acceptance

The Selective Call Acceptance feature provides the capability to build a list of numbers (known as a screening list) from which the subscriber wants to accept incoming calls. This feature can be provisioned at the feature profile level with a denied option at the subscriber level.

Either the subscriber or the administrator creates a selective call acceptance list (screening list), that contains up to 32 entries. These entries represent the calling numbers for which calls should be connected to the subscriber. Each entry can contain up to 15 digits.

NOTICE: The screening list entries are numbers that can be extensions if the subscriber is within a BG.. The entries can be partial numbers, where the beginning part of the number is compared. Associated with each DN is a presentation status for it, specifying public or private.

If the subscriber's selective call acceptance list is empty, OpenScape Voice prompts the subscriber to add entries to the list. As soon as a valid entry is provided, the feature is activated.

The subscriber can specify from time to time, if needed one of the following actions to perform:

- Activate or deactivate the feature
- Hear the entries that are currently on the list
- Add or delete entries to and from the list.

Requirements

The administrator specifies via GUI:

- Whether the feature is currently active. The subscriber is permitted to activate and deactivate it with the respective Feature Code Access.
- A 1- 7 digit PIN that a caller who is not on the screening list of the called party can use to contact the subscriber. This functionality is optional and activated when a valid PIN is entered in the field.
- Whether to forward rejected calls to another destination, or to play a denial announcement to the caller.

NOTICE:

If selective call acceptance is active, but the screening list is empty, all calls are rejected.

Functional Sequence

When a caller's number matches a number on the acceptance list, the call is completed.

When the caller's number is not on the acceptance list, one of the following occurs:

- The caller hears an announcement that indicates the subscriber does not accept calls from this number.
- The caller hears an announcement prompting him to enter the correct PIN to enable the call to be completed. If the PIN is not correct the caller is rejected.
- The call is routed to the configured forwarding destination.

Other Characteristics

The selective call acceptance feature is sometimes known as selective caller accept.

3.4.16 Selective Call Rejection

The SCR (Selective Call Rejection) feature provides the capability to build a list of numbers (known as a screening list) from which the subscriber does not want to accept incoming calls.

A screening list, created by the subscriber or the administrator contains up to 32 entries. These entries represent the calling numbers for which calls should be rejected. Each entry can contain up to 15 digits.

Functional Sequence

The subscriber has to specify one of the following actions to perform:

- Activate or deactivate the feature
- Hear the entries that are currently on the list
- Add or delete entries to and from the list

The subscriber selects the option to activate the feature and gets a confirmation tone or announcement to acknowledge. If the subscriber’s selective call rejection list is empty, OpenScape Voice prompts the subscriber to add entries to the list. As soon as a valid entry is provided, the feature is activated. If selective call rejection is active, but the screening list is empty, all calls are accepted.

When a caller's number does not match a number on the rejection list, the call is completed. When the caller's number matches a number on the rejection list, the caller hears an announcement that indicates the subscriber does not accept calls from the number.As long as the calling DN is on the station’s screening list, routing to a rejection announcement takes place regardless of whether the station is busy or idle. The subscriber does not receive any announcement when a call has been rejected.

System Specific Information

This feature can be provisioned at the feature profile level with a denied option at the subscriber level.

CDRs are provided on a usage-sensitive basis. The following are the CDRs maintained for this feature:

- SCR activation
- SCR deactivation
- SCR screening list editing
- SCR screening list created
- SCR screening list deleted

Other Characteristics

The selective call rejection feature is sometimes known as selective caller reject.

3.4.17 Park to Server

The **Park to Server** feature allows a subscriber to transfer calls to server-side destinations (**Parking Spaces**), from where they can be retreived by authorized subscribers. Once a call has been parked, the user’s line is free to originate or receive other calls. If a parked call is not retrieved before a configurable **Recall Timer** expires, the parking subscriber will be recalled.

Parking is not possible if:

- all **Parking Spaces** are occupied
- a manually requested **Parking Space** is occupied or invalid
- the call is a conference or emergency call
- the party to be parked is an Attendant
- the party to be parked has already been parked

On the user agent side, the Park to Server feature does not require any protocol extensions other than those for consultation and transfer.

Parking Lots and Parking Spaces

During provisioning for the **Park to Server** feature, a subscriber is associated with a **Parking Lot**, i.e. a named pool of server-side destinations that can be used for parking.

Each of these destinations (**Parking Spaces**) is capable of holding a single call and is addressed by a number.

A **Parking Lot** is a BG (Business Group) object and can be shared among subscribers within the same BG. Some subscribers may only be allowed to park calls, while others may only be allowed to retrieve calls from their associated **Parking Lot**.

When a subscriber (with **Parking allowed** permission) parks a call to his/her **Parking Lot**, the parked call is associated with a **Parking Space** number. Any subscriber who has been provisioned to use the same **Parking Lot** with **Retrieval allowed** permission and who knows the **Parking Space** number, is able to retrieve the call.

Provisioning

The administrator has to perform the following tasks:

1) Create **Parking Lots** for personal or shared use

   This includes defining the **Parking Space** number range (implicitely: the **Parking Lot** size) and the **Recall Timer** for unretrieved calls.

2) Provision subscribers for the **Park to Server** feature

   This includes assigning a (previously created) **Parking Lot** and granting the **Parking allowed** and/or **Retrieval allowed** permissions.

   As a prerequisiter, the subscribers must also be provisioned for **Call Transfer**.

3) Create **Access Codes** for parking and retrieval.

Related concepts

Call Transfer on page 171

3.4.17.1 Park to Server - Feature Usage

If an attendant or subscriber (provisioned for the **Partk to Server** feature) is on an active call, he/she can park the call at a server-side **Parking Space** by invoking consultation transfer, dialing the **Partk to Server** access code and completing the call transfer. The **Parking Space** selection can be performed either automatically (by the server) or manually (by subscriber input). A retrieving subscriber dials the **Park Retrieve** access code and has to specify the correct **Parking Space** number.

Automatic Parking

In the automatic mode the **Parking Space** number is selected by the system and provided to the subscriber by a voice response:

1) User *A* talks to user *B*.
2) *A* puts *B* on hold at the client
3) *A* dials the **Park to Server** access code (e.g. `*26`):
   - An announcement is played indicating the system-selected **Parking Space** number
   - A second announcement prompts the user to complete the **Call Transfer**: after this announcement the user has 10 secs to complete the transfer and hence complete the **Park to Server** procedure.

   NOTICE:

   The user can also complete the transfer right after the first announcement without waiting for the second one.

4) *A* completes the transfer (within 10 secs) and the call is parked.

Manual Parking

Experienced subscribers may speed up these procedures by dialing the required Parking Space number:

1) User *A* talks to user *B*.
2) *A* puts *B* on hold at the client.

3) *A* dials the **Park to Server** access code (e.g. `*26`) immediately followed by a specific **Parking Space** number (e.g. `8`)

   - An announcement is played repeating the user-selected Parking Space number
   - A second announcement prompts the user to complete the **Call Transfer**: after this announcement the user has 10 secs to complete the transfer and hence complete the **Park to Server** procedure.

> **NOTICE:**
>
> The user can also complete the transfer right after the first announcement without waiting for the second one.

4) *A* completes the transfer (within 10 secs): the call is parked to the server.

Retrieve a Parked Call

Suppose User *B* has been parked in **Parking Lot** *L* at **Parking Space** number *s*. Then User *C* (provisioned to retrieve calls from **Parking Lot** *L*) has two options:

- Either

  1) dial the **Park Retrieve** access code (e.g: `*27`)

     An announcement is played to the user to enter the number of the **Parking Space** that he/she wants to retrieve the call from, followed by a `#`.

  2) Dial `s#`

- or dial the **Park Retrieve** access code (e.g: `*27`) immediately followed by the **Parking Space** number *s*.

In both cases a call is established between users B and C.

3.4.17.2 Park to Server Recall

A **Park to Server Recall** occurs when a call has been parked using the **Park to Server** feature, and the **Recall Timer** of the associated **Parking Lot** expires without the call being retrieved.

The subscriber that originally parked the call is recalled using the same procedures as Call Transfer Security and therefore the feature interactions are derived from the Call Transfer Security feature interactions.

Functional Sequence

The recall is attempted up to a maximum of 3 times with the recall timer being restarted after each attempt. If the recall is not successful (i.e. does not reach an alerting state) after reaching the maximum number of recall attempts, the call remains parked until retrieved or released.

> **NOTICE:**
>
> When phone based features are used (rather than OpenScape Voice Centralized features) the recall can not bypass preAlert

checks (e.g. Do Not Disturb, Call Forwarding, etc.) at the recalled device.

3.4.17.3 Feature Access Codes for Park to Server

Feature access codes enable subscribers to Park and/or Retrieve calls to/from the server. A feature access code can either be dialed or it can be assigned to a function key on the subscribers’ phones, providing seamless access to server-side features.

The required access codes are usually created during the initial installation of the OpenScape Voice system; however, additional codes can be added at any time.

Technically, a Feature Access Code is a special instance of a PAC (Prefix Access Code), defining a sequence of keys (0-9, #, *) that enable callers to invoke a specific server-side feature. It can be created either globally (i.e. in the Global Numbering Plan) or locally (i.e. in a Private Numbering Plan). In OpenScape Voice Assistant such a "Feature PAC" has to be created with

- Prefix Type: Vertical Service
- Nature of Address: Unknown
- Destination Type: Service

and one of the available Service destinations.

Table 15: Park to Server related Service destinations

Service Name	**Service Descrition**	Example PAC
Park to Server	Call Park to Server	*26
Park Retrieve	Call Park Retrieve from Server	*27

3.4.18 Station Dialing

The Station Dialing features permit a subscriber to invoke dialing to access another station or public network destination or enter control digits to control a voice mail system or IVR device and operate many OpenScape Voice subscriber features.

The subscriber is permitted to invoke offhook, onhook, or hot keypad dialing to:

- Access another station or public network (external) destination
- Enter control digits to control a voice mail system or IVR device
- Activate, deactivate, and configure many OpenScape Voice subscriber features for example, station call forwarding.

Functional Sequence

The different types of dialing work as follows:

- Offhook dialing

  After lifting the handset, the subscriber obtains dial tone, and enters keypad digits. The subscriber can select OK to complete dialing or wait for the interdigit timeout. Offhook dialing makes use of context dialing functionality, which lets the subscriber enter and modify the digits before selecting OK as long as the interdigit timeout has not expired. This method is sometimes known as enbloc dialing.
- On-hook dialing

  After entering keypad digits without lifting the handset the subscriber may select OK to complete dialing or wait for timeout. Onhook dialing also uses context dialing functionality, as described above.
- Hot keypad dialing

  This dialing allows immediate processing of digit input by the subscriber when the digits input match a digit pattern in the local device’s dial plan. If this match is recognized, the interdigit timeout does need not to elapse.

3.4.19 Direct Outward Dialing

The DOD (Direct Outward Dialing) feature allows subscribers to have direct outward dialing access to the PSTN (Public Switched Telephone Network). This access is usually signaled using a 1- to 5-digit PSTN access code that is defined in the BG (Business Group) dialing plan.

The use of the PSTN access code ensures no conflicts with the extension-dialing pattern.

Functional Sequence

When the subscriber enters the PSTN access code, OpenScape Voice recognizes the digit sequence and permits the subscriber to dial the external number. After the subscriber finishes dialing, OpenScape Voice completes the call in the usual manner.

System Specific Information

An OpenScape Voice subscriber can also dial the access code and outside number in one sequence. In this case, OpenScape Voice strips the access code from the dialed number and replaces the called party number with the remaining digits.

3.4.20 Station Speed Calling

The Station Speed Calling feature provides subscribers the capability to place frequently dialed numbers in a speed calling list for personal use only, or to share with others. This feature can be provisioned at the business group level with a denied option at the subscriber level. The types of station speed calling are: One-digit and Two-digit station speed calling. The types differ in the calls to be placed in a repertory of frequently called numbers.

This feature can be provisioned at the business group level with a denied option at the subscriber level.

The feature supports two types of station speed calling:

- One-digit station speed calling:

  This feature allows a subscriber to place calls to a repertory of frequently called numbers by dialing a 1-digit speed calling code. Eight numbers can be placed in the list.
- Two-digit station speed calling:

  This feature allows a subscriber to place calls to a repertory of 30 frequently called numbers by dialing a 2-digit speed calling code.

The administrator provides the speed calling lists to a subscriber:

- A private list is used by one subscriber, who can modify any entry.
- A shared list is owned by one subscriber, but can be used by many subscribers. Only the owner can modify the list entries.

A subscriber can have both a one-digit and a two-digit list. They can both be private, or one can be private with the other one shared.

Functional Sequence

After activation of station speed calling the subscriber enters the number associated with the entry. Now the subscriber can select **Dial** or the number is automatically dialed after a 4-second timeout expires.

Other Characteristics

Stations with speed calling should be given standard originating treatment up to the point where the first digit is collected.

Speed calling can be used any time dialing is appropriate. The speed calling entry must supply all dialing information, including applicable access codes.

The feature is sometimes known as speed dial.

Unify SIP endpoints also have local features that simplify the dialing of frequently-used numbers.

3.4.21 System Speed Dialing

The System Speed Dialing feature provides administrators the capability to create centralized speed dialing lists that are available to an entire business group.

OpenScape Voice supports up to 10,000 system speed dialing lists with a combined (lists/BG and entries/lists) total of one million (1,000,000) entries. For each business group two (2) lists can be assigned at the same time (out of the 10,000 available lists) to a subscriber, with up to 100,000 entries per list. Each one of the two lists is accessed through an access code (e.g. Speed Dial System 1 and Speed Dial System 2).

> **NOTICE:**
>
> The speed dial entry limitations are valid for the system and the BG. So you may assign all 10,000 available speed dial lists of the system to one BG or distribute them over several BGs.

A system speed dialing list entry can contain up to 30 characters, which can be a combination of digits, the number sign (#), and the asterisk (*). Because of this, a list entry can contain access codes and account codes, in addition to the dialed party number itself.

Functional Sequence

To dial a system speed dialing list entry, the subscriber can use two ways:

- Direct access by the access code associated with Speed Dial System1 or Speed Dial System 2, followed by the speed dial list entry number.

  The entry number can range from 0 to 99999; it can consist of one, two, three, four or five digits.
- Suffix dialing is also allowed after the “#” character, in the case that a List Entry Data includes only part of the DN. For example, if a List Entry Data includes an Office Code, a subscriber can dial System Speed 1 (or 2) access code, followed by the List Entry ID, followed by “#”, followed by the remaining digits (eg. DN’s extension).
- By entering redial or selected dialing key set up for Speed Dial System 1 or Speed Dial System 2 (if present), followed by the speed list entry number.

After selecting list entry the subscriber can select **Dial** or wait until the number is automatically dialed after a 4-second timeout expires.

Speed dialing entries also support suffix dialing. In this case the subscriber may be prompted to enter a PIN after OpenScape Voice executes the speed calling entry.

Other Characteristics

The feature system speed calling is sometimes known as BG speed dial.

Unify SIP endpoints have local features that simplify the dialing of frequently-used numbers.

3.4.22 Call Transfer

The Call Transfer feature permits a subscriber to manually redirect an established call to another party as and when required. The transfer may be performed with or without consulting the transfer-to party.

Call Transfer is implemented as an interaction between the SIP endpoint and OpenScape Voice: the different types of transfer requests are generated by the telephone (on behalf of the user) and the processing and checking (e.g. for transfer restrictions) is performed by OpenScape Voice.

The Call Transfer Security feature ensures that unsuccessfully transferred calls are recalled to the transferring party.

Transfer Types

The following transfer types are supported:

- Transfer with third-party consultation:

  This type permits a screened transfer. After speaking with the transfer-to party, the subscriber can transfer the first party to the transfer destination.

- Unscreened transfer

  This type permits the subscriber to perform a call transfer prior to the transferred-to destination answering the call. The transfer request is completed during ringing or call waiting (camp-on).

  The subscriber has some control over the attempted transfer:

  – Upon the subscriber hearing ringback tone and seeing a display, the subscriber can complete the transfer before the destination answers.

  – The subscriber can also wait until the destination answers before completing the transfer.
- Blind transfer

  This type permits a transfer without consultation to another party. With blind transfer the subscriber does not control the call during the transfer.

NOTICE:

A blind transfer where the transferred and transferred-to parties are the same is blocked.

Transfer Restrictions

The subscriber is allowed to perform the transfer provided that he or she is allowed to call the transfer-to party and that no additional transfer restrictions apply. The following restrictions can be provisioned per subscriber:

- No restrictions, i.e. all calls (internal/external) can be transferred to all destinations.
- The subscriber is not allowed to transfer the call if both the transferred and transferred-to parties are external. All other calls can be transferred.
- Transfer is allowed for internal calls only, and to internal destinations only.

Restricted Trunk Transfer

Starting with OpenScape Voice Version 5, there is a new option to disallow call transfers that would result in bypassing existing Toll and Call Restrictions: if an OSV subscriber has Toll and Call Restrictions that would prevent him from calling a certain PSTN Number, then another OSV subscriber can be disallowed to use call transfer to establish a connection between the two.

There is a complementary configuration option to force the release of large conferences when, in case of two parties remaining in conference, one party is restricted to call the second party.

"Restricted Trunk Transfer" can be activated and deactivated through subscriber provisioning.

Call Detail Records

For complex call scenarios, for example, when a call is transferred with consultation, a thread identifier correlates the CDRs associated with each leg of the call.

Related concepts

Toll and Call Restrictions

Park to Server on page 165

3.4.22.1 Call Transfer Security (with Intercept)

The Call Transfer Security feature provides the capability to ensure that a subscriber performs an unscreened/blind transfer to an invalid destination and that the transferred party is not left ringing for too long at another internal subscriber's endpoint. The transferring party is recalled and/or the call is redirected to its transfer intercept destination.

The administrator can enable a subscriber's Transfer Security feature for internal calls only, external calls only, or both.

> **NOTICE:** Transfer security is not provided for calls transferred to external destinations.

Immediate vs. Delayed Recall

For transferred calls, the transferring party receives *immediate recall*, and the transferred-to party is released, in the following instances:

- Incomplete or invalid dialing
- Attempt to transfer to a party that goes on hook prior to transfer
- Provisioned restrictions on the subscriber attempting the transfer, the party being transferred, or the transferred-to party.

The transferring party receives *delayed recall*, and the transferred-to party is released, if the transferred-to party doesn't answer within the configured time-out.

When endpoint-based CFNA is invoked and the forward-to destination is unable to accept the call, OpenScape Voice immediately redirects the call to the transfer security intercept destination associated with the forwarding station's DN.

Call Transfer Security with Intercept

Call Transfer Security with Intercept redirects the transferred party to the transferring subscriber's Call Transfer Intercept Destination, in the following instances:

- A call transfer recall occurs and the transferring subscriber is busy and cannot be camped onto or doesn't answer within the configured time-out.
- An *endpoint-based* CFNA (Call Forwarding on No Answer) is invoked at the transferred-to party and the forward-to destination is unable to accept the call. In this case OpenScape Voice immediately redirects the call to the transfer security intercept destination associated with the forwarding subscriber.

  This functionality is also known as **CFNA Intercept**.

> **NOTICE:** CFNA Intercept is for transferred calls only and not for CFNA-forwarded calls in general. Furthermore it is not implemented for calls redirected outside the BG or to the public network.

3.4.22.2 Phone Displays

During Call Transfer, if all parties are located in the same OpenScape Voice system, extended information about the involved parties is presented on the related phones' displays. This information depends on the type of transfer being performed.

Table 16: Blind Transfer

Transfer Status	Transferring Party (Party A) Display	Transferred Party (Party B) Display	Transferred-To Party (Party C) Display
Party A calls party B, party B answers-or-Party B calls party A, party A answers	Party B's name and number	Party A's name and number	-
Party A puts party B on consultation hold by selecting: **Blind Transfer**	-	Party A's name and number; see note 1	-
Party A performs a blind transfer to party C, party C is ringing	-	Party C's name and number	Party B's name and number
Party C answers	-	Party C's name and number	Party B's name and number

1 Party B may or may not receive Held display, but does hear music.

Table 17: Unscreened Transfer

Transfer Status	Transferring Party (Party A) Display	Transferred Party (Party B) Display	Transferred-To Party (Party C) Display
Party A calls party B, party B answers-or-Party B calls party A, party A answers	Party B's name and number	Party A's name and number	-
Party A puts party B on consultation hold by selecting: **Consult/Transfer**	-	Party A's name and number; see note 1	-
Party A performs a blind transfer to party C, party C is ringing	Party C's name and number	Party A's name and number	Party A's name and number
Party A transfers party B to party C	-	Party C's name and number	Party B's name and number

Transfer Status	Transferring Party (Party A) Display	Transferred Party (Party B) Display	Transferred-To Party (Party C) Display
Party C answers	-	Party C’s name and number	Party B’s name and number

1 Party B may or may not receive Held display, but does hear music.

Table 18: Transfer with Third-party Consultation

Transfer Status	Transferring Party (Party A) Display	Transferred Party (Party B)Display	Transferred-To Party (Party C) Display
Party A calls party B, party B answers-or-Party B calls party A, party A answers	Party B’s name and number	Party A’s name and number	-
Party A puts party B on consultation hold by selecting: **Consult/Transfer**	-	Party A’s name and number; see note 1	-
Party A calls party C, party C is ringing	Party C’s name and number	Party A’s name and number, see note 2	Party A’s name and number
Party C answers	Party C’s name and number	Party A’s name and number, see note 2	Party A’s name and number
A alternates between party B and party C (optional)	Party B’s name and number	Party A’s name and number	Party A’s name and number, see note 2
Party A transfers party B to party C	-	Party C’s name and number	Party B’s name and number

1 Party B may or may not receive the Held display, but does hear music.2 Depending on the endpoint and software release, party B or C might also receive Held display.

3.4.23 Automatic Collect Call Blocking

This feature provides the subscriber to be protected from collect calls automatically by OpenScape Voice. The ACCB service may be assigned to subscribers (BGLs) and to feature profiles. The ACCB feature is only applicable to the original called OSCV subscriber. If the call is forwarded or redirected (transferred) any ACCB service assigned to the new target subscriber is not applied i.e. if the original called OSCV subscriber does not have ACCB but the new target (due to forwarding/transfer) does have ACCB then ACCB will not be applied.

The ACCB service is assigned to any OpenScape Voice subscriber and does not interact with any existing features.

The ACCB service will immediately terminate if the A-side (calling side) of the call is not a NNI (Network-to-Network Interface) interface with the 'Automatic Collect Call Blocking supported' endpoint attribute enabled.

Functional Sequence

When an incoming call to an OpenScape Voice subscriber arrives via an ACCB capable Gateway OpenScape Voice will check to see if the called subscriber has the ACCB service enabled. If the service is enabled OpenScape Voice will use SIP or SIPQ signaling to notify the Gateway that the called subscriber does not wish to receive collect calls.When the Gateway receives this ACCB indication from OpenScape Voice the Gateway will signal to the PSTN that the call should be rejected if it is a collect call. The PSTN will release the call if it is indeed a collect call, or will allow the call to proceed if it is not a collect call.When the PSTN releases a call due to ACCB, OpenScape Voice has no indication that this is anything other than a normal release by the calling party, therefore the release cause will be "normal clearing".

UCE checks for ACCB service assigned to the called subscriber number. So in the case of Keyset lines, the Keyset device that answers the call is not relevant as far as the ACCB service is concerned. ACCB is always Line Based not Device Based.

System Specific Information

The ACCB service is currently only available with SIP signaling to AudioCodes Gateways and with SIPQ signaling to OpenScape 4000.

This feature is only available when the called subscriber and the PSTN gateway are served by the same OpenScape Voice system. The feature is not available over Private Networking i.e. when the called subscriber and the PSTN gateway are not served by the same OpenScape Voice system.

The PSTN Gateway endpoints where both the Gateway, and the PSTN office that the Gateway connects to, must support the signaling procedures required for Automatic Collect Call Blocking.

3.4.24 CSTA Support

CSTA (Computer-Supported Telecommunications Applications) is an abstraction layer for telecommunications applications. It implements a telephone device model that enables CTI (Computer Telephony Integration) applications to work with a wide range of telephone devices. OpenScape Voice has native CSTA support.

The CSTA Standard

Originally developed in 1992, CSTA has continued to be developed and refined over the years. It is often the model that most CTI applications are built on and claim compliance with. It became an OSI (Open Systems Interconnection) standard in July 2000. It is currently being maintained by ECMA (European Computer Manufacturers Association) International.

OpenScape applications Assistant, Contact Center, and UC Application support the standard and connect to OpenScape Voice via its CSTA interface.

CSTA applies with the Unify Common Application Platform (CAP) to control and monitor telecommunication activities on SIP endpoints.

The OpenScape Voice CSTA Implementation

OpenScape Voice's CSTA Service is a call processing component that subscribes for call processing events in the UCE (Universal Call Engine) and sends CSTA information messages to the CSTASM (CSTA Signaling Manager). The latter receives CSTA information messages from the CSTA Service and handles conversions to GNF (Global Number Format) as needed.

Related concepts

Signaling Management on page 667

3.4.24.1 CSTA (Computer Supported Telecommunications Applications) Support Features

OpenScape Voice provides a standard European Computer Manufacturers' Association (ECMA) Computer Supported Telecommunications Applications (CSTA) protocol interface to external CTI applications, which permits applications such as the OpenScape UC Application, and OpenScape Contact Center to control the OpenScape Voice SIP endpoints. It also describes other OpenScape Voice capabilities relevant to applications that utilize the CSTA interface.

The support comprises the following features:

- CSTA Protocol Interface

  This feature provides a CSTA protocol interface to applications, that support the ECMA standard.

  CSTA Protocol Interface provides the ability to control and monitor telecommunication activities on SIP endpoints.
- CSTA Services Support

  OpenScape Voice supports a list of standard CSTA services. These services are also applicable to ONS call control support, with the exception of the following categories:

  – Capability exchange services
  – System registration services
  – System status services
- Application Populated Caller ID

  CSTA-enabled ACD (Automatic Call Distribution) applications (for example, OpenScape Contact Center) can supply the information necessary to change the callback number provided to the called party on a dynamic basis. This ability complies with United States Federal Communications Commission (FCC) regulations that require telemarketing agents to provide a name and dialable callback number when they make outbound calls.
- Data Synchronization

  CSTA-enabled applications use the data synchronization feature.

  When subscribers are created, modified, or deleted, OpenScape Voice Assistant generates a log file with the XML stream for subscribers registered for the relevant external application. This file is transferred on a daily basis to the CAP server. At a predetermined time during the night, CAP runs a script to import the file and update its database.

- Flexible Digit Processing

  The flexible digit processing capability can be used on all calls originated from CSTA-enabled applications, including the Make Call, Consultation Call, and Deflect Call messages.

- Integration with Fault Management

  An internal mechanism is available to send SNMP traps and notifications and to integrate this information seamlessly into HiPath Fault Management.

- Message Waiting Indicator

  OpenScape Voice allows for a CSTA-monitored device to report MWI changes to the monitoring application.

- Multiple Time Zone Support

  The CAP supports time zone information as delivered by the system database regardless of zone or location.

  OpenScape Voice's multiple time zone support capabilities ensure that the correct date and time information is used.

- One Number Service

  is a licensed subscriber mobility service that is based on CSTA services. It is possible to provision CSTA Access and ONS Inbound/Outbound for a subscriber that does not have a registering device. Refer to the table below for supported CSTA services and events for ONS – IO subscribers.

- OpenScape Voice-Provided Calling Name

  OpenScape Voice provides the calling name via the call monitoring events to the CSTA-enabled application. This calling name is only presented to the application user if the external directory does not match an entry for the subscriber's DN.

- Private Network Number Support

  The CSTA interface has the capability to recognize and send private network numbers and other non-DID numbers in device IDs. This includes supporting private network numbers used in the OND (one number service device) tag portion of the device ID. Because of this, a subscriber home DN can be provisioned as DID (with national and international numbers) or non-DID.

- Call Routing Service

  A Call Routing Service (CRS) enables B-side routing of calls by a CSTA-enabled application. The CRS service is similar to OpenScape Voice's ONS (One Number Service) and runs at the same priority.

- Bridged Call

  The bridged call feature permits Business Group Keyset users with a shared Multi-line Appearance to establish a conference by pressing the line key of the line they wish to bridge onto. It is possible to bridge onto a line involved in a stable two-party call or a Station Controlled Conference (SCC). The Bridging capability is available to Business Group Keyset users who have a shared line appearance they wish to bridge onto and the line/BGL to be bridged onto is subscribed to the Station Controlled Conference feature.

NOTICE:

A subscriber may have only one routing service assigned. Therefore ONS and CRS are mutually exclusive features and may not be assigned in parallel.

3.4.24.2 CSTA Services Support

OpenScape Voice supports a wide range of standard CSTA services.

Table 19: OpenScape Voice-Supported CSTA Services

Category	Services Supported
Capability exchange services	Get CSTA features Get logical device information Get switching function capabilities Get switching function devices Switching function devices
System registration services	System register
System status services	Request system statusSystem status
Monitoring services	Change monitor filter Monitor start (device monitor only) Monitor stop (device monitor only)
Snapshot services	Snapshot call Snapshot device Snapshot device data
Application session services	Start application session Stop application session Reset application session timer Application session terminated

Category	Services Supported
Call control services	Accept call Alternate call Answer call Callback call-related Clear connection Conference call (see note 1) Consultation call Deflect call (target is the alerting party) Directed pickup call Group pickup call Hold call Make call Reconnect call Retrieve call (from hold) Single-step transfer Transfer call
Call control events	Conferenced (see note 1) Connection cleared Delivered Diverted Established Failed Held Network reached Offered Originated Queued Retrieved Service initiated Transferred
Call associated features	Change connection information Generate digits Call information

Category	Services Supported
Physical device feature services (OpenScape Desk Phone CP only)	Get message waiting indicator Get microphone mute Get speaker volume Set microphone mute Set speaker volume
Physical device feature events (OpenScape Desk Phone CP only)	Message waiting status
Logical device feature services	Call back non-call-related Get agent state Get do not disturb Get forwarding Set agent state Set forwarding
Logical device feature events	Agent busy Agent not ready Agent ready Agent working after call Callback event Do not disturb Forwarding
Device maintenance events	Back in service Out of service Device capability changed
Route Registration Services	Route Register Route Register Cancel Route Register Abort
Call Routing Services	Route Request Route Select Route End Re-Route Route Reject
Message Waiting Indication	Set MWI (on/off)
1. For ONS call control support, this service is applicable to the registering device only.	

NOTICE:

When callback is activated via the CSTA application, there is an indication, instead of an announcement, on the CSTA application when the callback has been rejected.

3.4.24.3 Application Populated Caller ID

APCID (Application Populated Caller ID) provides SIP or CSTA enabled outbound call center applications with the capability to present to the called party a valid callback number for the specific marketing customer’s outbound campaign.

APCID addresses a regulatory requirement. The FCC posted a ruling stating that telemarketing companies need to send caller ID with a real callback number for each separate marketing entity. In other words, outbound calls from a single company would need to have unique caller ID that is populated by product type or individual customer in a multi-tenant environment.

System Specific Information

There are no provisioned parameters on the OpenScape Voice. APCID is provided via SIP and CSTA application interfaces. The external SIP or CSTA application activates this feature by providing additional information in their respective protocols.

3.4.24.4 CSTA Call Routing

The CSTA (Computer-Supported Telecommunications Applications) Call Routing feature enables an external CSTA "routing device" to influence the routing of a call. CSTA Routing registration and Call Control services are exposed to meet the basic functional requirements defined in the ECMA 269 CSTA standard.

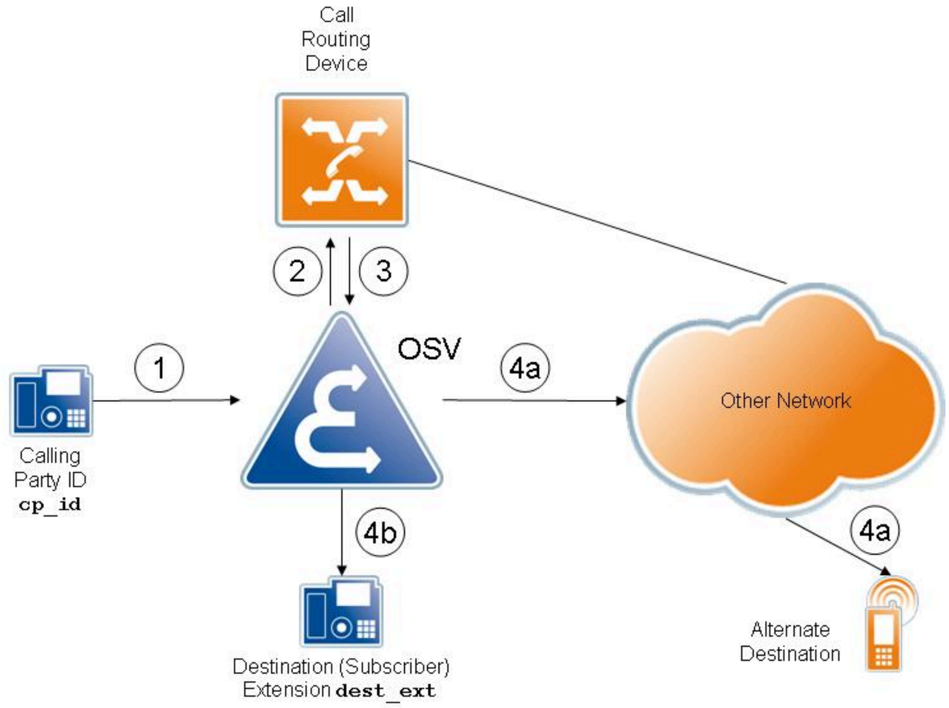


Figure 10: CSTA Call Routing - High Level Diagram

1) `cp_id` calls extension `dest_ext`
2) OSV sends Route Request for "`cp_id` calls `dest_ext`".
3) "Routing Device" resolves the real destination, based on the callee's routing preferences (managed OSV-external) and returns a Route Selection command to OSV, pointing to a new "Destination Code".
4) Depending on the returned "Destination Code", OSV either

   a) delivers the call to the local extension
   b) routes the call to an alternate destination

A routing device is provisioned via Assistant. Similar to ONS (One Number Service) the routing device is created by assigning the CSTA Call Routing feature to a subscriber.

NOTICE:

Since a subscriber may have only one routing service assigned, ONS and CSTA Call Routing are mutually exclusive features and may not be assigned to the same subscriber.

Limitations

If the CSTA Call Routing feature is provisioned on a subscriber then this subscriber may not be assigned as a Hunt Group pilot and vice versa.

The CSTA Call Routing feature is also mutually exclusive with Simultaneous Ringing and Hot Desking

3.5 Calling Identity Services

The CIS (Calling Identity Services) are a collection of features related to call related Identity Management. The delivered Number and Name form a user's identity and can be presented to the called or calling party. The information may be updated as the call progresses.

The format of the number identity of a user (Subscriber or Endpoint) to be presented to another user (Subscriber or Endpoint) can be controlled via the Display Number Modification tables of OpenScape Voice.

Supported SIP Headers

For internal and external calls to an OpenScape Voice Subscriber, OpenScape Voice uses the `P-Asserted-Identity` header field in SIP provisional and final responses to convey the identity of the called/connected party.

> **NOTICE:**
>
> Not all SIP phones and endpoints may support this header field and may end up keeping the dialed number on the display.

For internal and external calls from and to SIP Trunking endpoints (gateways, applications, …), those SIP Trunking endpoints that support the `P-Preferred-Identity` header field rather than the `P-Asserted-Identity` header field, will receive the internal or external identity in this header field by provisioning the **Send P-Preferred-Identity rather than P-Asserted-Identity** attribute on the SIP Trunking endpoint. However, OpenScape Voice will always ignore received identities in the `P-Preferred-Identity` header field.

3.5.1 Number and Name Delivery

Number and Name Delivery is an automatic feature of OpenScape Voice. Together Number and Name form a user's identity. The identity of the calling party is delivered to the called party and vice versa, the identity of the called/ connected party is delivered to the calling party.

The display number modification feature ensures that the digits appearing in the display of the endpoint or application represent a dialable number, in the format required to dial back the calling, called, or connected party.

The identity of a user that is provisioned as an OpenScape Voice subscriber contains

- Internal Name and Internal Number (aka Subscriber DN) for internal calls.

  The Subscriber DN is delivered as Internal Number unless the subscriber is provisioned to use a different **Displayed Extension Number** (max. 10 digits) for internal calls.

- External Number (aka **External Caller ID**) for external calls. If no **External Caller ID** is available then for external calls:
  - If the subscriber is a MLHG member and it is provisioned to use the **Main Pilot DN** for external calls, then the **Main Pilot DN** is used, provided it is an E.164 number.
  - If the Subscriber’s **Directory Number** is a **Public** DN (flag configured on the Subscriber), then this DN is used.
  - If the called party is in the public network accessed via a SIP Trunking endpoint with **Default Home DN** configured, then that SIP Trunking endpoint's **Default Home DN** is used.
  - If none of the above return a useful E.164 number, then the **BG Display number** is used.

Related Features

Delivery of an OpenScape subscriber's identity depends furthermore on the configuration of the features **Number Permanent Presentation Status** and **Name Permanent Presentation Status** for that subscriber. These features may restrict the presentation of a user's internal or external identity towards other users.

The identity of users that are not provisioned as Subscribers in OpenScape Voice may also be delivered by the endpoints that deliver the incoming call or terminate the outgoing call. OpenScape Voice's ability to look for these identities can be provisioned via the **Privacy** feature that is provisionable on endpoint profiles for SIP Trunking endpoints. Possible values for Privacy are:

- Basic: do not look for or send identities in the SIP `P-Asserted-Identity` header field. The only identity being transferred is the calling party's identity in the SIP `From` header field.
- Full: look for and send identities in the SIP `P-Asserted-Identity` header field. Calling, Alerting, Busy and Connected party's identities will be delivered and received.
- Full-Send: do not look for, but send identities in the SIP `P-Asserted-Identity` header field.
- Full-Receive: look for, but don't send identities in the SIP `P-Asserted-Identity` header field.

In case no Name identity was transmitted by the remote party, OpenScape Voice will not assign any name to the party.

Unique Extension Numbers

Certain interoparability scenarios require unique **Displayed Extension Number**s per BG. This uniqueness can be enforced by setting the RTP parameter `to_be_defined` to "active" (default is "inactive").

NOTICE:

Setting `to_be_defined` to "active" will clear duplicate **Displayed Extension Number**s. This might invalidate an incompatible configuration!

Note that modifying `to_be_defined` will only take effect after the system has been rebooted from runlevel 3.

Related concepts

Number Permanent Presentation Status on page 187

Name Permanent Presentation Status on page 187

3.5.1.1 Number Identities

OpenScape Voice uses one of the following numbers as Number Identity.

Subscriber's Directory Number (Home DN)

This is the main number associated with the subscriber. The subscriber's Directory Number can be either a Public (E.164) or a Private (L2, L1, or L0) number.

The definition on whether the Home DN is a Public or Private number is part of the subscriber profile data:

- If the subscriber's **Type of Number** field is set to **Public**, it means that the Home DN assigned to the subscriber is a public (E.164) number.
- Otherwise, it means that the Home DN is a private (L2, L1 or L0) number.

External Caller ID

The **External Caller ID** feature provides the subscriber with a second number which must be used for all external calls, incoming and outgoing.

This feature is useful, for instance, when the subscriber's **Directory Number** (Home DN) is **Private** (i.e. L2, L1 or L0 number). In this case, the subscriber's **Directory Number** cannot be used for external calls.

This feature can also be used if the subscriber wants to hide his **Directory Number** for calls to (or from) the public network.

Main Pilot DN

The administrator has the option to configure a subscriber that is an MLHG member to use the Name and Number of the **Main Pilot DN** as the subscriber's identity for Internal and/or External calls.

Note that the **External Caller ID** has higher priority than the option to use the Main Pilot DN for external calls. If the administrator wants the subscriber to use the **Main Pilot DN** as identity for external calls, he/she needs to remove any **External Caller ID** configured for the subscriber.

Default Home DN

OpenScape Voice introduces a new **Default Home DN** which can be assigned to an endpoint.

For *external* calls to a SIP endpoint (SIP Trunking, SIP Private Networking or SIP-Q Private Networking), if the calling party does not have a **Public** number, OpenScape Voice will use the **Default Home DN** (if configured on the SIP endpoint) as the calling party number.

BG Display Number

The BG’s **Display Number** is the default number that will be used to send to the public network in case OpenScape Voice has no other public number available for a subscriber.

3.5.2 Number Permanent Presentation Status

Number Permanent Presentation Status indicates the default presentation setting (“Allowed” or “Restricted”) of an OpenScape Voice subscriber's number identity, which is used for the Number and Name Delivery. When the subscriber originates a call, it is used to determine whether or not presentation of the number of their identity to the called party is restricted. When they are called, it is used to determine whether or not presentation of the number of their identity to the calling party is restricted.

The following can be provisioned for Number Permanent Presentation Status:

- **Calling Party Number** for internal calls (Allowed or Restricted)
- **Connected Party Number** for internal calls (Allowed or Restricted)
- **Calling Party Number** for external calls (Allowed or Restricted)
- **Connected Party Number** for external calls (Allowed or Restricted)

Related concepts

Number and Name Delivery on page 184

3.5.3 Name Permanent Presentation Status

The Name Permanent Presentation Status feature describes a subscriber’s default Name Delivery behaviour in the Number and Name Delivery context. When the subscriber originates a call, it is used to determine whether or not presentation of the name of their identity to the called party is restricted. When the subscriber is called, it is used to determine whether or not presentation of the name of their identity to the calling party is restricted.

This service also allows the administrator to prioritize which Name should be used (i.e. Subscriber Name, BG Name or Department Name) for different types of call.

The following can be provisioned for Name Permanent Presentation Status:

- The Name Permanent Presentation Status for internal and external calls
  - **Calling Party Name** for internal calls (Allowed or Restricted)
  - **Connected Party Name** for internal calls (Allowed or Restricted)
  - **Calling Party Name** for external calls (Allowed or Restricted)
  - **Connected Party Name** for external calls (Allowed or Restricted)
- For each of the four call types (internal/external, calling/connected) the order in which the names
  - **Business Group Name**, **Department Name**, **Subscriber Name** or **None** for internal calls
  - **Business Group Name**, **Subscriber Name** or **None** for external calls

  shall be presented, if available.

Related concepts

Number and Name Delivery on page 184

3.5.4 Enhanced Forwarded-Call Info

Enhanced Forwarded-Call Info feature is shown on all OpenScape Desk CP phones and IP deskphones with its CSTA and Server Features set. It shows Forwarded Target on Forwarded Phone statically for CFV (always)/ CFSIE-All/ CFSIE-All (Internal and External, but not both at the same time. If this is the case, only Internal/ External is shown) and Phone CFAll. Also it shows calling number and display info on forwarded phone briefly during an incoming call for all Forwarding flavors.

3.5.5 Outgoing CID Suppression and Delivery Per Call

The forced Outgoing CID (Caller ID) Suppression and Delivery Per Call feature allows subscribers forcing either delivery or suppression of their calling identity (name and number) parameters for a particular call.

The feature can be provisioned at the feature profile or at the subscriber level.

In addition the administrator has to create

- a Prefix Access Code for the Force Calling Identity Delivery vertical service to allow the user to force the presentation status for both name and number to "Allowed" for a single call. The suggested access code is *64.

  If CID delivery is "Allowed" for a call, the connected party's line receives

  – the calling party's Number
  – the calling party's Name if the call is internal
- a Prefix Access Code for the Force Calling Identity Suppression vertical service to allow the user to force the presentation status for both name and number to "Restricted" for a single call. The suggested access code is *66.

  If CID delivery is "Restricted" for a call, the connected party's line receives a "Private/Anonymous" indication for the calling party's Number and Name (name only if the call is internal).

The subscriber is allowed to dial these access codes at the beginning of a call or while a call is active.

The feature can be activated in one of the following ways:

- The user dials the access code only.

  In this case the user receives a Recall Dial Tone, and then dials the intended called party's number (in-band) to complete the call.
- The user can enter the access code and the called party's number at once. The user will not receive Recall Dial Tone. Instead the call is setup with the desired presentation status to the called party.

Counters are provided for feature activation attempts.

3.5.6 Outgoing CID Suppression

The Outgoing CID (Caller ID) Suppression feature suppresses the presentation of the calling identity (name and number) parameters for any subsequent call made by the subscriber.

The feature can be provisioned at the feature profile or at the subscriber level:

- Assigned in a feature profile. The settings of the feature can then be inherited by subscribers that have this feature profile assigned.
- Inherited at subscriber level. (Inheritance can be Denied at subscriber level)
- Assigned at subscriber level

In addition the administrator has to create

- a Prefix Access Code for activating the Calling Identity Suppression vertical service that forces the presentation status for both name and number to “Restricted” for all subsequent calls. The default number for this PAC is *52. The called party’s line receives a Private/Anonymous indication for the calling party’s Number and Name.

  NOTICE:

  While **Outgoing CID Suppression** is activated, presentation of the calling identity shall be restricted unless overridden by the existing **Outgoing CID Delivery Per Call feature** (with default prefix access code #51).

- a Prefix Access Code for deactivating the Calling Identity Suppression vertical service that forces the presentation status for both name and number to “Allowed” for all subsequent calls. The default number for this PAC is #52. The called party’s line receives the calling party’s Number and Name.

  NOTICE:

  While CID Suppression is not activated, presentation of the calling identity shall be allowed unless overridden by the following features – in this order:

  -**Outgoing CID Suppression Per Call** feature (with default prefix access code *51).

  -**Number Permanent Presentation Status** set to Restricted.

  -**Name Permanent Presentation Status** set to Restricted.

- a Prefix Access Code for toggling the Calling Identity Suppression vertical service so the presentation status for both name and number for all subsequent calls toggle from currently “Allowed” to “Restricted” or vice versa from “Restricted” to “Allowed”. The default number for this PAC is **52.

  This access code may also be entered on a Feature Toggle Key on an OpenScape Desk Phone CP endpoint.

The **Outgoing CID Suppression** service access codes can be found in the following table:

Service Name	Service Description	Default Access Code
CIDS Activate	Activate Calling Identity Suppression	*52
CIDS Deactivate	Deactivate Calling Identity Suppression	#52
CIDS Toggle	Toggle Calling Identity Suppression	**52

Counters are provided for feature activation attempts.

3.5.7 Alternative CID

The Alternative CID (Caller ID) per call feature allows an administrator to provision a list of up to 10 alternative calling identities for an individual subscriber. The subscriber can dial a service access code and the 1 digit index of this list to select the calling party identity to be used prior to making an off-net call.

Feature Provisioning

The feature can be provisioned at the feature profile or at the subscriber level:

- Assigned in a feature profile. The settings of the feature can then be inherited by subscribers that have this feature profile assigned.
- Inherited at subscriber level. (Inheritance can be Denied at subscriber level)
- Assigned at subscriber level

In addition the administrator has to create:

- a Prefix Access Code for activating the Alternative CID vertical service that allows the subscriber to select the index of an administrator-defined alternative calling party identity list. The default number for this PAC is *53.

Feature Activation

The feature is activated on a per call base and in one of the following ways:

- The user dials the service access code for alternative calling identity (default: *53) followed by the index (single digit between 0 and 9) followed by the called party number. When this combination is dialed and assuming that an administrator provisioned a number and a name for the selected index, then the provisioned number and name shall be used for the outbound call to the called party.
- When no called party is provided following the alternative calling identity selection and the index the user receives a Recall Dial Tone, and then dials the intended called party's number (in-band) to complete the call.

A service counter counts the number of alternative calling identity executions.

The subscriber’s name shall not be overridden if the name is not part of the alternative calling identity

IMPORTANT:

For security reasons, only administrators can populate the alternative calling identity list in order to prevent users from performing masquerade attacks (impersonation of another user).

The call made to the called party shall be signaled as an external call even if a call to the called party without alternative calling party would be signaled as an internal call.

Alternative Calling Identity Interrogation

A subscriber can always find out which alternative calling identities are available by activating the feature and calling the DN announcement feature. If the feature is active and the selected index has an alternative calling party configured, then the alternative calling party number is played back to the calling party.

The name is not played back.

3.5.8 Anonymous Call Rejection

The ACR (Anonymous Call Rejection) feature provides subscribers the capability to reject calls from parties who have a privacy feature active (such as caller ID blocking) that prevents the delivery of the calling number to the called party.

The administrator specifies whether the feature is always active, or if the subscriber is permitted to activate and deactivate it.

Functional Sequence

When anonymous call rejection is activated, OpenScape Voice checks incoming calls to determine if the presentation of the calling party’s DN is allowed. This check is performed regardless of whether the subscriber’s extension is offhook or idle.

- If presentation is allowed or if the presentation status is unavailable:

  OpenScape Voice completes the call. Screening of calls, however, may depend on the precedence of other features that a called party has active on the line.
- If presentation is restricted:

  OpenScape Voice does not complete the call and the subscriber does not receive alerting for the call. Instead, the caller hears a denial announcement that informs the calling party that the system cannot accept the call unless the calling party information is made public. If the calling party does not hang up within 10 to 12 seconds of completion of the announcement, the system automatically disconnects the call.

Other characteristics

Different anonymous call rejection traffic measurements are maintained on a per-SPCS basis.

Maintenance measurements can be available on demand for number of incoming calls, number of activations and number of deactivations.

Call detail recording (CDR) is provided.

The Anonymous Call Rejection feature is known as anonymous caller rejection.

3.5.9 Distinctive Ringing

The Distinctive Ringing feature provides the ability for subscribers of a BG to hear different ringing indications for internal (within the same Business Group) and external calls (different Business Groups).

This feature permits the subscriber to distinguish internal and external calls based on the melody defined in the endpoint.

The administrator controls internal ringing for the entire business group.

Requirements

The distinctive ringing feature is available for subscribers of the following SIP endpoint:

- OpenScape Desk Phone CP
- OpenScape DeskPhone IP

The actual alert indication strings (known as Bellcore-dr1 and Bellcore-dr2) must be defined in the telephone's alert indication section. If the strings are not defined in the telephone, the telephone rings with a default cadence for all calls, regardless of whether they are internal or external.

Functional Sequence

When the distinctive ringing feature is active for a business group, a different internal ringing pattern (Bellcore-dr1) is sent to the telephone for calls received from subscribers within the business group.

If this capability is not provisioned, the internal ringing pattern sent to the telephone is the same as the pattern defined for external calls (Bellcore-dr2).

3.5.10 Directory Number Announcement

The DN (Directory Number) Announcement feature permits callers to determine the DN of the line from which they are calling.

This feature is also useful for service personnel, because it enables them to verify that the correct line pair is assigned to the DN that is expected.

For example, a caller can use this to determine the DN of a telephone in a conference room or reception area.

Functional Sequence

The subscriber enters an specific access code, a connection is made to an announcement that states the DN of the line from which the call is being made.

3.5.11 Business Group Department Names

The Business Group Department Names feature permits a business group subscriber to be associated with a specific department. A Department can be used for billing purposes or from OSV V8 onwards it can also be used for emergency calling purposes.

Up to 200 department names are supported for each business group.

Billing Department

The department is used for billing purposes and the Department name can be delivered as an alternative to the calling or connected party name.

Emergency Department

The Department is used for emergency calling purposes.

The Emergency Department supports the OSV emergency calling feature to use the subscriber DN in order to discover the location of the calling user.

In order to use the subscriber DN the subscriber must be assigned to an Emergency Department and this Emergency Department must be assigned to an emergency subnet.

Upgrade

During upgrades to OSV V8 all existing Departments are migrated as Billing Departments, since in previous versions they were used for this purpose.

3.5.12 Malicious Call Trace

The Malicious Call Trace feature provides subscribers the capability to generate an automatic trace of the last call received. Subscribers typically use this feature in response to malicious, harassing, or nuisance calls, in order to provide a trace over time of such activity.

A class mark at the subscriber level is required for access to this feature.

The subscriber activates this feature via a one- or a two-step procedure. An RTP parameter determines whether a trace is activated via a one- or two-step procedure.

The RTP parameter `Srx/Main/MCTActivationLevel` defines two activation levels. Activation level 1 produces the trace without any additional user activity (other than the SAC dialing). Activation level 2 requires the user to press 1 digit while hearing an announcement with the directions.

Functional Sequence

The subscriber activates this feature in one of the following ways:

- One-step procedure in which `MCTActivationLevel=1`:

  After finishing a call, the subscriber enters an access code (usually *57) and the trace is immediately initiated.
- Two-step procedure in which `MCTActivationLevel=2`:

  After entering the access code, OpenScape Voice prompts the subscriber to dial a number to initiate the trace.

Before doing so, the subscriber can cancel the trace by going on hook.

After the trace is complete, the collected information is written to a file accessible to the administrator.

Enhanced Malicious Call Trace

Malicious Call Trace Services

Navigate to **CMP** > **OpenScape Voice** > **Business Group** > **Members** > **Subscribers** > **Add** > **Features**

The **Malicious Call Trace** feature is by default in the **Subscriber Features** list. Change the **Assignment** from **Switch-wide** to **Assigned** and put the parameter `MCTActivationLevel=1` to activate the enhanced MCT.

- Call Tracing of Terminating Calls

  To invoke the MCT feature after the nuisance call, the user may:

  – Invoke the MCT feature to collect call trace data for the previous call and an SNMP trap/alarm is generated against CMP. The user must dial `*571` or `*57`.
  – Enable MCT data collection for future calls. The user must dial `*572`
  – Disable MCT data collection for future calls. The user must dial `*573`
- Outgoing Call Tracing

  You must configure a specific list of DN as a Destination Code Point for Outgoing Call Tracing. The Destination Code point is configured to insert a new MCT Traffic Type whenever the destination DN is dialed. Whenever the MCT service detects that the new MCT Traffic Type is being used for a call, an MCT data collection is performed in addition to routing the call to the destination. The outgoing call trace remains active until the administrator removes the Destination Code point for the specific list DN.
- Tracing of In-Progress Calls

  Configure the subscriber DN MCT feature data enabling the user invocation of MCT data collection for an in-progress call. Since OSV deploys MCT switch-wide, the user may invoke Tracing of In-Progress Calls at any time. You must

  – Ensure Call Hold is subscribed
  – Disable Music On-Hold for the subscriber.
  – Inform the MCT feature user how to use the feature. The user can either dial the MCT DAC and select the appropriate option to invoke the Tracing of In-Progress Call or dial `*57`, `*571` or `*572` during the call.

Other Characteristics

The Malicious Call Trace feature is known as Customer Originated Trace.

Related concepts

RTP Management via OpenScape Voice Assistant on page 961

3.5.13 Caller ID for phone-based Recording Parties

Recording caller ID in phone-based recording parties is an enhacement feature to the OpenScape phone recording feature. It allows OpenScape Voice to send the connected party’s identity information in the call towards a recording application. No other information except the call partner identity is sent to the recording application.

Phone Recording Feature

In the recording solutions which use phone recording feature, the Session Recording Client (SRC) -the phone with Call Recording feature enabled- upon receiving or making a call, initiates a second call towards the recording application and creates a conference bridge. The recording application is a SIP user agent that stores the information for future retrieval and playback (SRS - Session Recording Server). The data stream is diffused both at the called party and the recording application.

The recording session between the subscriber’s phone and the recording application provides only the identity of the subscriber’s phone and not of the call partner, although the information for the last one is critical for recording solutions.

OpenScape Voice Recording Feature

In order to provide to the recording application the identity of the call partner, the OpenScape Voice system finds the Communication Session (CS), containing the subject of recording between two or more SIP phones and retrieves the call partner identity. Meanwhile the call is treated as a normal call and the call partner identity is sent to the recording application.

Limitations

Along with this feature there are some limitations regarding the delivery of the call partner identity in certain feature interactions.

- The SRC (Session Recording Client - the phone with Call Recording feature enabled) makes or receive a second call (CS) while involved in a CS. If the Recording Session (RS) is already established, the identity of the call partner in the second CS will not be delivered to the SRS.
- If the SRC is tranferred to a new party and the RS is already established, the identity of the tranferred-to (new) party will not be delivered to the SRS.
- The SRC is added to a large conference in which the RS is already established. The conference participant data will not be delivered to the SRS.
- The SRC creates an OSV large conference and the RS is already established. The participant data will not be delivered to the SRS.
- The SRC is added or creates a large conference and the RS is initiated afterwards. No identity information will be delivered to the SRS.
- The SRC uses a line appearance to bridge-in in a call. No identity information will be delivered to the SRS in the RS that can be established afterwards.
- The SRC uses executive override to barge-in a call. No identity information will be delivered to the SRS in the RS that can be established afterwards.
- The SRC uses SILM to silent monitor or barge-in in a call. No identity information will be delivered to the SRS in the RS that can be established afterwards.
- The SRC has multiple contacts and more than one of the contacts has an active session. In this case when the RS is initiated, the identity information of the call partner from the oldest active session will be sent to the SRS.
- The SRC has two held sessions when the RS is initiated. In this case the identity information of the call partner of the oldest session will be sent to the RS.
- The SRC is alternating from an inactive to an active session (media update transient state) when the RS is initiated. In this case the identity informations of the call partner of the oldest session might be delivered to the SRS.
- If the RS is initiated while the SRC is not yet connected to the B-party then the identity of the connected party will not be delivered to the SRS.
- If CSTA makeCall is received and uaCSTA is not allowed for the caller (for example, in case makeCall with private data or uaCSTA are not configured on the phone), the identity of the call partner can not be delivered to the SRS.

Activation/Deactivation

The feature can be activated/deactivated through the RTP parameter `Srx/Service/Rec/EnablePhoneRecordingCallerId`. In order to activate the feature the value of the RTP parameter must be set to true. The default value is false, in order to prevent Phone Recording failures to those who are not interested in using this feature.

3.5.14 OpenScape Voice Call Recording Solution Based on SIPREC

SIPREC defines a SIP client (UAC) and a SIP server (UAS) interface, used to establish a Recording Session (RS) to record a SIP multimedia Communication Session (CS) between two SIP peers.

The SIPREC architecture identifies key roles for the SIPREC UAC as a SIPREC client (SRC) and SIPREC UAS as a SIPREC server (SRS). The SRC establishes an RS with the SRS whenever a multimedia CS is to be recorded. The RS is established as a typical multimedia session.

The SIPREC based OpenScape Voice Call Recording solution offers an OpenScape Voice over IP (VoIP) recording solution for calls passing through a remote OpenScape Branch. This solution is a hybrid one, as each solution component provides a contribution in the overall call recording solution.

The OpenScape Voice Call Recording solution based on SIPREC is introduced in order to overcome the loss of recorded speech with CSTA based recording solution, that exists in case of network delays.

OpenScape Voice is responsible for determining when a subscriber or SIP interface is involved in a call to be recorded. It also provides proprietary SIP signaling indications to a SIPREC client, capable OpenScape Branch involved in the communication session that the call is to be recorded.

Inter/Intra-branch Call Recording

The SIPREC implementation is supported for:

- Unify Devices
- UC web client (non-WebRTC)
- OSMO

For devices the following features are supported:

- Call recording for both calling and called participant
- Hold / Retrieve
- Call Consult / Transfer
- Call Pickup Call Recording - Group Call Pickup (CPU)
- Call Forwarding
- Large Conferencing

For UC clients (web and OSMO) with ONS/OND the following features are supported:

- Call recording for both calling and called participant
- Hold/Retrieve
- Call Pickup
- Call Consult / Transfer
- UC Conference

For use cases outside the scope of SIPREC call recording architecture, call recording relies on the existing SILM Service.

NOTICE: SIPREC based OpenScape Voice Call Recording solution does not use the OpenScape Media Server as a conference bridge, to support the media stream breakout to the recorder.

NOTICE: Contact Center solution does not support SIPREC.

3.6 Attendants

Attendants features are supported by OpenScape Voice. It uses an attendant console desktop that includes the productivity features of the agent desktop and several attendant-specific features. Attendants can be located anywhere the IP network extends because the desktop integrates on top of the attendant’s SIP EP (Endpoint).

3.6.1 AAP (Attendant Answering Position)

The APP (Attendant Answering Position) feature provides support for a SIP-based AAP using a DFT (Digital Feature Telephone), keyset telephone, or a soft client. The AAP functionality includes night service (automatic and manual control) to route calls to predefined night stations or other answering devices, that can be voice messaging, an automated attendant application, or a night bell device.

AAPs have the capability to:

- Act as a night service destination and to manually activate night service for the business
- Extend calls to other destination within the private network or external destinations
- Camp on to busy stations
- Be recalled
- Access external trunk resources
- Prevent calls made or extended within the private network from being transferred, held, or overridden with the exception of inter-AAP calls
- Simultaneously handle multiple call presentation (for example, to the business and operator lines)
- Trace malicious calls
- Provide through-connect and trunk-to-trunk connections
- Perform inter-AAP call transfers
- Display the name and number related to incoming business calls

Functional Sequence

The system administrator identifies a hunt group as an attendant answering group. The administrator also specifies values for the following capabilities available to all hunt groups:

- Time-in-queue threshold value
- Night service DN (Directory Number)
- An automatic make busy on no answer advance

System Specific Information

One or more AAPs may be provisioned per business group.

Attendant Answering Groups

The Attendant Answering Groups (AAG) are multiline hunt groups (MLHG) that support distribution and queuing of calls to Attendant Answering Positions (AAPs) and Night Answering Positions (NAP).

When a call (external or internal) is offered to an AAG, the hunt group logic distributes the call to an available Attendant Answering Positions DN. An available AAP DN is an AAP DN that is available for hunting (not Make Busy) and the AAP DN is not active on a call.For more information regarding the configuration of MLHG, see chapters *Hunt Groups* and *Make Busy*

When the night service is enabled manually via the OSV Assistant or when all Attendant Answering Positions (AAP) DNs in the group are unavailable for hunting (Make Busy), the distribution of calls to Night Answering Positions (NAP) DN occurs. For information regarding the Night Service, see chapter *Night Service*.

3.6.2 Interworking with an Automated Attendant System

An Automated Attendant System can be used with OpenScape Voice. A system of this type accepts all incoming calls and leads the caller through a menu offering different options, such as Company Operator Assistance, Direct Extension Dialing, voice-controlled services, and voice mail connection.

3.6.3 Main Number

The BG (Business Group) Main Number feature provides for a published directory number for each BG. The attendant can answer this number or it can be assigned as the first number in a BG range (extension range). The Main Number can be also be a pseudo number, and not assigned to a dedicated line. It can be mapped to any extension in the BG, such as the attendant’s assigned line.

This feature enables you to add or update both Main Numbers (subscribers) and attendant numbers of a BG. You can add as many new numbers as necessary. The Main Number resource includes both the main number (subscriber) and the attendant or auto-attendant, which is usually a recorded message that asks you to enter the extension of the person to whom you want to speak.

In the BG Main Number dialog the list of Main Numbers are displayed:

Column	Description
Main Number	Displays the list of Main Numbers defined for the selected BG.

Column	Description
Attendant Number	Displays the list of Attendant Numbers defined for the selected Main Number.
Auto Attendant Number	Displays the list of Auto Attendant Numbers defined for the selected Main Number.
Enabled	Displays the Auto Attendant Status. Possible values: Yes / No

3.7 Subscriber Location Identification

A characteristic of IP communication environments is the ability to move phones and other clients within the corporate network. For certain call processing features such as E911 (Enhanced 911) or CAC (Call Admission Control), subscriber mobility is a challenge, because the adequate call handling depends on the current geographical location of the calling and/or called party. OpenScape Voice supports several location identification concepts.

Note that OpenScape Voice does *not* implement any location functionality itself, but it is able to collect location related data during registration and call setup and to provide this information to interested services for location-based feature execution.

Stationary Subscribers

For stationary (groups of) subscribers the location of the calling/called subscriber can be determined from the respective DN (Directory Number) or other statically provisioned data such as the subscriber’s Calling Location or Route Area.

CAC supports location identification based on DNs.

Mobile Subscribers Directly Connected to OpenScape Voice

If a subscriber is mobile but directly attached to OpenScape Voice, its IP address can be used for location purposes. For this to work, the network planner has to

- divide the enterprise work area (campus, building, floor, work room) into areas of appropriate size,
- assign a suitable IP address range to the area; and
- configure the DHCP server(s) to assign IP addresses in accordance with this network plan.

An Auto Discovery Mechanism via DHCP Relay with DHCP Option 82 (Relay Agent Information Option) is the recommended solution.

NOTICE:

As a prerequisite, **mobile user agents have to be provisioned for DHCP!** Statically assigned IP addresses can **not** convey dynamic location information.

Both E911 and CAC support location identification based on IP subnets.

Mobile Subscribers Behind an SBC - Location Domains

With OpenScape Voice Version 5 an additional location logic based on *Location Domains* (i.e. unique fully qualified domain names that identify geographical locations) was introduced. These *Location Domains* are either

- signalled from the subscriber devices towards OpenScape Voice
  - in the `To` header field URI of a SIP `REGISTER`
  - in the `From` header field host part of the URI of a SIP `INVITE`
- assigned via endpoint provisioning for NNI (Network-to-Network Interface) endpoints and via Media Server provisioning for Media Servers.

The proposed way to deploy *Location Domains* to subscriber devices is to use DHCP Option 120 (SIP Server Discovery) along with Option 82.

NOTICE:

As a prerequisite, **mobile user agents have to be provisioned for DHCP!** Otherwise they cannot discover their current Location Domain.

Currently, *Location Domains* are used

- for processing Emergency Calls
- to control CAC (Call Admission Control) restrictions
- to track the geographical location of calling and called party in CDRs

OpenScape Voice Assistant can handle FQDNs with up to 64 characters length.

NOTICE:

This feature is only applicable to users behind an SBC or Proxy. SIP users connecting directly to OpenScape Voice should **not** provide Location Domains in their SIP signaling in order to avoid interfering with the FQDN feature.

These users may utilize domain names within their SIP identities however only a single DNS SRV or FQDN node identity may be used, limiting support to a single Location Domain.

OSV Location Database

Some features require location information for the called subscriber to be available during call setup: e.g. CAC uses the called subscriber’s location to determine its CAC group.

Because this location information can not be obtained "just in time" from the corresponding initial `INVITE`, it has to be extracted from the callee’s previous `REGISTER` request and saved to a Location Database (similar to handling of `Contact` addresses in SIP `REGISTER` requests).

Related concepts

Emergency Calling
Emergency Calling Table
CAC (Call Admission Control) Group
CAC (Call Admission Control) on page 203
CAC Group Measurements

3.7.1 DHCP Relay Agents and Option 82

Using DHCP (Dynamic Host Configuration Protocol) Relay Agents with DHCP Option 82 (*DHCP Relay Agent Information* option; RFC 3046) a DHCP server receives information about the layer 2 port the host is connected to. This enables centralized, location-dependent host configuration - even when hosts are mobile.

Functional Sequence

1) The client broadcasts a DHCPDISCOVER

2) The *Relay Agent* adds the *Relay Agent Information* consisting of

- the *Circuit ID* of the port from which the agent received the packet
- the *Remote ID* of the agent (typically the *Relay Agent*’s MAC address)
- the *GiAddr*, i.e. the Gateway IP Address of the *Relay Agent* (as part of the normal *DHCP Relay* message)

and unicasts it to its configured DHCP server

3) The DHCP server uses the *Relay Agent Information* to determine the adequate host configuration and sends it back to the *Relay Agent* in a DHCPOFFER

4) The Relay Agent forwards the DHCPOFFER to the client

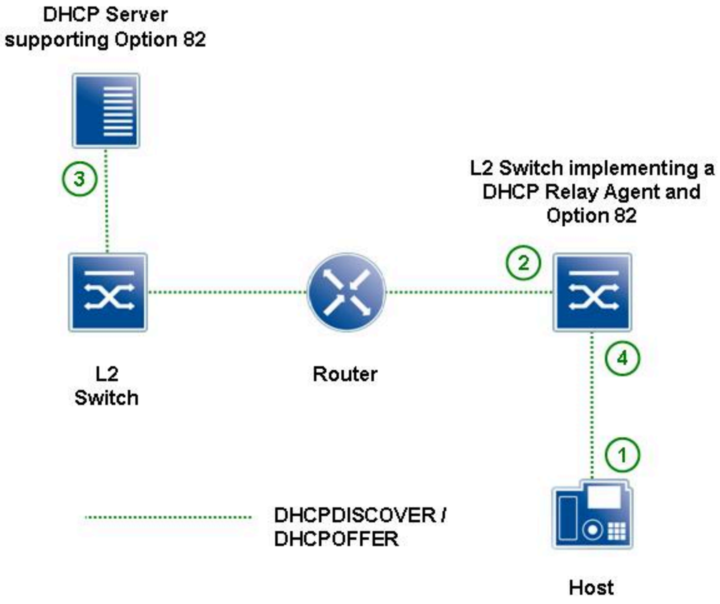


Figure 11: DHCP Address Assignment and SIP Registration (Example)

NOTICE:

It is the network administrator’s task to understand the wire-map of the layer 2 network and to configure the DHCP server so that it delivers the desired host configuration (IP addresses etc.)

3.7.2 Location Domain Discovery via DHCP Option 120

DHCP option 120 (SIP Server Discovery; RFC 3361) allows SIP clients to discover a DNS (Domain Name System; RFC 103) fully-qualified domain name of a SIP server. If consistently assigned, this Location Domain can identify the client’s geographical location.

The proposed way to deploy the Location Domains to the clients is to use DHCP Relay Agents with Option 82 to convey the geographical location of the clients to the DHCP server and then use Option 120 to assign the appropriate *Location Domain* to the clients.

The DNS servers must also be configured so that all Location Domains resolve to the address of the SIP Registration/Location Server (i.e. OSV or central SBC). In other words, all the FQDNs are aliases for the "real" SIP Registration/ Location Server domain.

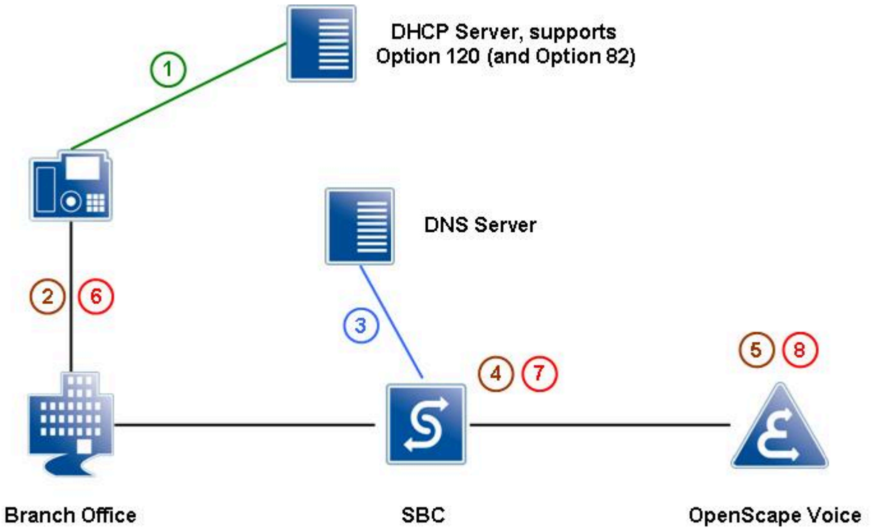


Figure 12: Location Domain Discovery and Propagation (Example)

1) Phone receives site specific domain name via DHCP Option 120
2) Phone sends domain name as host part of `To` header field in SIP `Register` request
3) DNS server resolves Location Domain to the address of OpenScape Voice
4) SBC does not change the domain name in the `To` header field
5) OpenScape Voice saves the domain name for each Contact in its Location Database
6) Phone sends domain name as host part of `From` header field in SIP `INVITE` request
7) SBC does not change the domain name in the `From` header field
8) OpenScape Voice provides the conveyed domain name to interested services

Static Location Domain Provisioning at OSV

NNI (Network-to-Network Interface) endpoints that are configured in for static registration, or NNI endpoints that do send `REGISTER` requests to OSCV but are unable to provide Location Domain information in SIP requests, may require an alternative means to configure a Location Domain for the endpoint. A new NNI endpoint configuration parameter allows the administrator to configure a location domain name to be used for calls via the endpoint. If this parameter is configured then it will used as the location domain and information from the SIP signalling shall not be used to determine the location domain.

A Location Domain can also be provisioned for each Media Server.

NOTICE:

Currently those statically provisioned Location Domains are only used for CAC.

3.8 CAC (Call Admission Control)

OpenScape Voices's CAC (Call Admission Control), also known as IRM (Internal Resource Management) is the mechanism by which new calls may be refused by OpenScape Voice, if the IP network does not have the capacity (bandwidth) to handle the call with a acceptable quality of service.

Introduction

In the traditional telephony world, a circuit (line or trunk) is either busy or idle. A circuit is dedicated to a single call and so voice quality is predictable and assured. If all available circuits are busy, new call attempts are rejected.

In contrast, IP links are shared resources and hence can be "overbooked". If too many calls are routed over a bandwidth-limited LAN or WAN link, this doesn't result in call blockage, as in the circuit-switched world, but in reduced quality due to delayed or lost media packets.

In an enterprise network congestion may occur

- on access links between the enterprise core network and the subnets serving its branch offices
- on dedicated access links between branch offices (that may exist in addition to other links present in the enterprise network)
- at the aggregation layer between branch office LANs and the backbone WAN.

  This can happen when the total bandwidth capacity of the related access links 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 these access links.

Consider the following simple scenario:

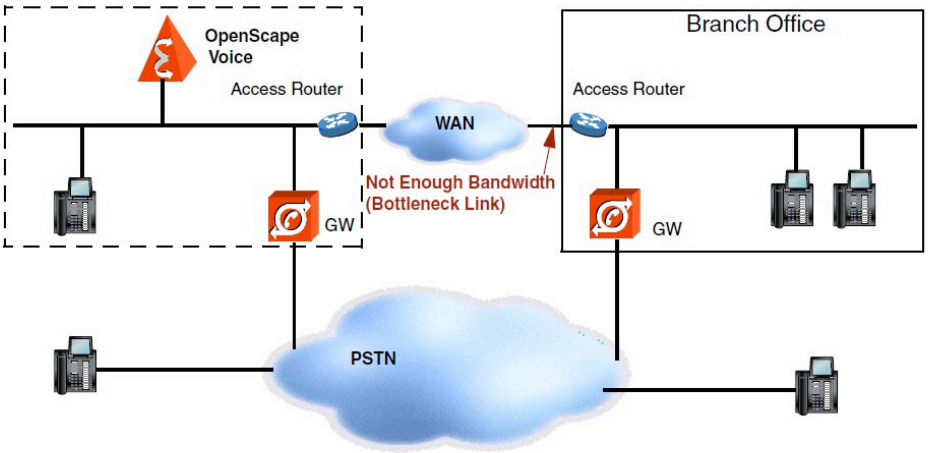


Figure 13: Branch Office with Bandwidth-Limited link

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 QoS for real time media. However, the bandwidth for access to the core network is limited, and the access router may start dropping media packets if the capacity is exceeded.

Resource Management

Real-time media calls should not be routed over networks that cannot guarantee an acceptable QoS (Quality of Service). CAC provides the means to prevent these poor-quality connections from being established. A new call (of type *T* = voice, video or fax) can only be established, if the maximum allowed number of calls and/or the bandwidth limit (for type *T*) hasn’t been reached on all involved access links.

When used in conjunction with effective VLAN and packet prioritization schemes to segregate call media and and data traffic, CAC provides an effective means to assure good quality.

NOTICE:

Proper segregation and prioritization of voice and data traffic is important because CAC only manages calls, and does not see or control the amount of other 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.

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.

If a call cannot be established due to missing resources, it may be either blocked or rerouted.

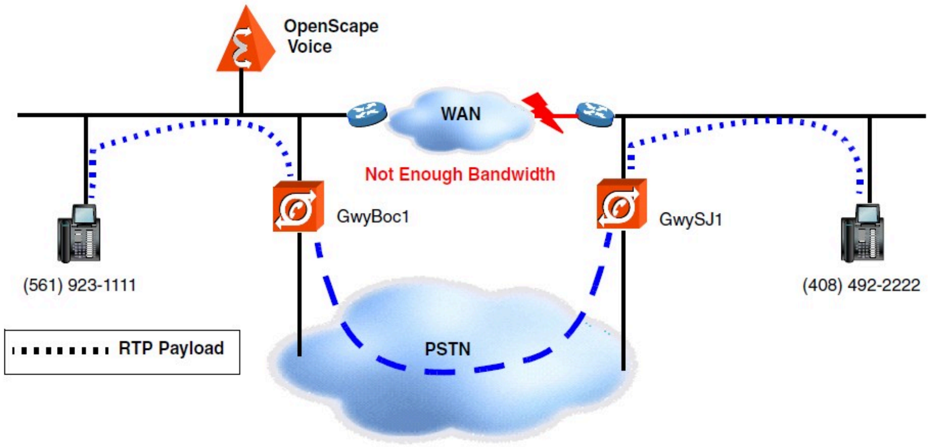


Figure 14: Rerouting Based On Insufficient Bandwidth

CAC Administration in OpenScape Voice

CAC can be administrated via OpenScape Voice Assistant. In simplest terms, the administrator can

1) enable resource management, set the parameters used for bandwidth calculation and enable "high bandwidth usage" alarms
2) create groups of subscribers and gateways sharing the same bottleneck links

   These *CAC Groups* may be defined based on DNs (Directory Numbers), IP addresses or Location Domains.
3) define media-stream related policies to be applied to

   - calls traversing the bottleneck link between a CAC Group and the core network (Regular CAC Policies)
   - calls traversing a dedicated bottleneck link between two CAC Groups (Group-to-Group CAC policies)

   These *CAC Policies* may also restrict the allowed codecs.

Requirements

For scenarios involving two or more OpenScape Voice systems, each system is responsible for the bandwidth management of its own endpoints. The only requirement is that there cannot be endpoints that belong to two (or more) OpenScape Voice systems served by the same bandwidth-limited link-for example, in the same branch location. All endpoints served by a particular bandwidth-limited link must be configured in the same OpenScape Voice system.

Related concepts

Subscriber Location Identification on page 199

3.8.1 Supported Network Topologies - Star Network

A star network is a LAN in which all nodes are directly connected to one central node (hub or a switch).

The star topology assumes that RTP (Real-Time Transport Protocol) traffic from and to each branch location is routed through a single bandwidth-limited access link to and from the backbone WAN.

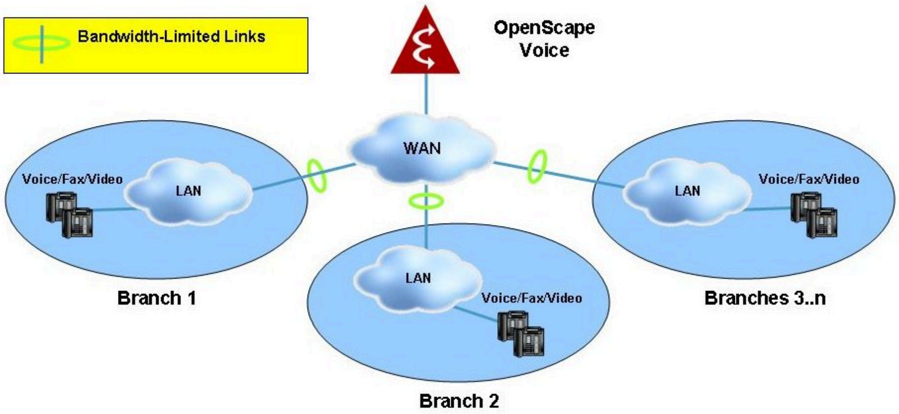


Figure 15: CAC (Call Admission Control) — star network topology

3.8.2 Supported Network Topologies - Tree network

The tree network topology integrates multiple star topologies together onto a bus.

Some OpenScape Voice customers use tree topologies, for which multiple levels of bandwidth-limited links need to be considered. In this topology, multiple levels of bandwidth-limited links are present.

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.

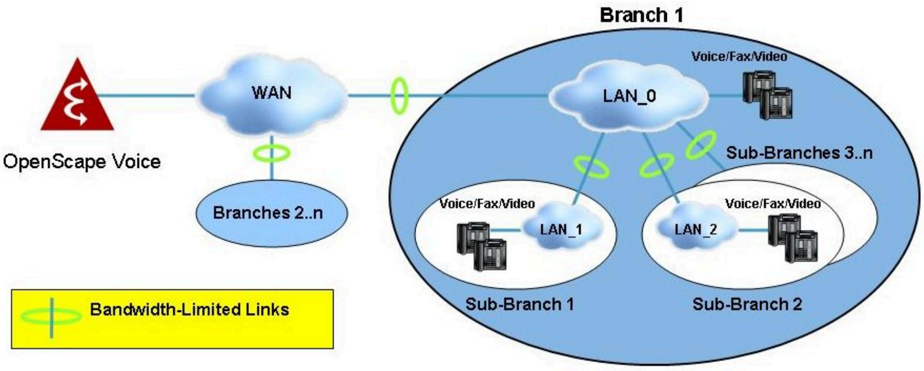


Figure 16: CAC (Call Admission Control) — tree network topology

3.8.3 Parent CAC (Call Admission Control) Group

A parent CAC (Call Admission Control) 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 (Directory Numbers).

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.

The figure below shows how the child CAC Groups and CAC Policies are provisioned to monitor the bandwidth at the first level, which is the level between the branches and the LAN that connects them.

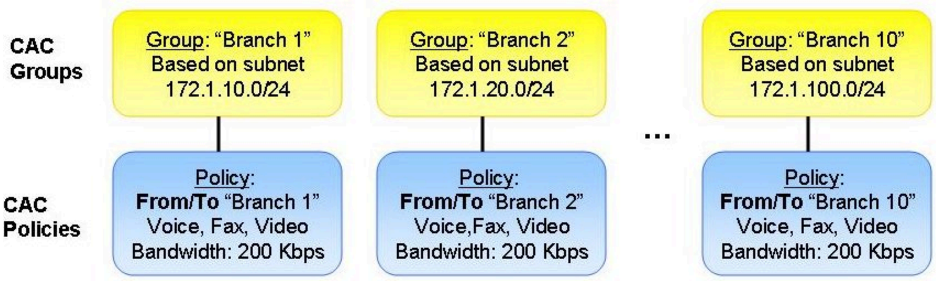

CAC Groups
Group: "Branch 1" Based on subnet 172.1.10.0/24
Group: "Branch 2" Based on subnet 172.1.20.0/24
...
Group: "Branch 10" Based on subnet 172.1.100.0/24
CAC Policies
Policy: From/To "Branch 1" Voice, Fax, Video Bandwidth: 200 Kbps
Policy: From/To "Branch 2" Voice,Fax, Video Bandwidth: 200 Kbps
Policy: From/To "Branch 10" Voice, Fax, Video Bandwidth: 200 Kbps

Figure 17: CAC Groups and Policies for first level of tree network topology

The next figure illustrates how the parent CAC Group and CAC Policy are provisioned to monitor the bandwidth at the second level, which is the level between the LAN and the WAN.

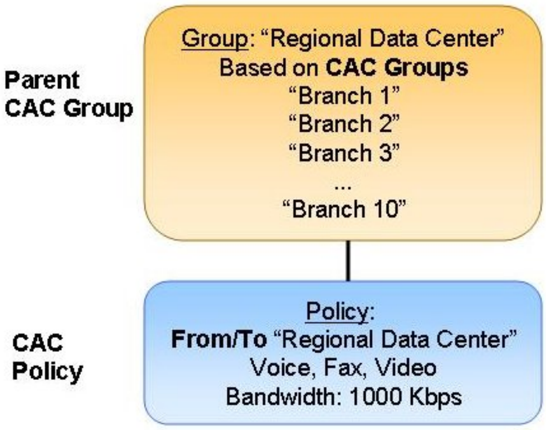

Parent CAC Group
Group: "Regional Data Center" Based on CAC Groups "Branch 1" "Branch 2" "Branch 3" ... "Branch 10"
CAC Policy
Policy: From/To "Regional Data Center" Voice, Fax, Video Bandwidth: 1000 Kbps

Figure 18: CAC Groups and CAC Policies for second level of tree network topology

3.8.4 Supported Network Topologies - Mesh Network

A mesh network consists of several nodes that are all connected to each other.

When the mesh network topology is used, some branch locations have dedicated links to other branch locations. For these branches, the RTP (Real-Time Transport Protocol) traffic is routed via a direct link between the two branch locations instead of routing through a backbone WAN.

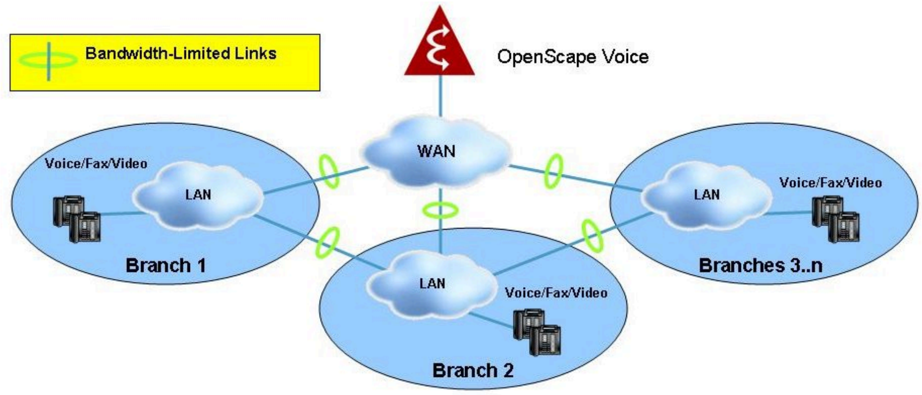


Figure 19: CAC (Call Admission Control) — mesh network topology

OpenScape Voice supports CAC for networks that use any combination of star, tree, and mesh network topologies.

3.8.5 Resource Management

An IRM (Internal Resource Manager) function within OpenScape Voice's UCE (Universal Call Engine) integrates bandwidth management with call processing in order to provide robust call handling, such as the rerouting of a call via the PSTN (Public Switched Telephone Network) when there is insufficient bandwidth in the enterprise network to carry the call, based on bandwidth availability.

The IRM can limit the calls over a bandwidth-limited link based on

- Number of Calls:

  the concurrent calls per link are simply counted, and when the limit is reached, no new calls are admitted.
- Bandwidth Limit:

  the OpenScape Voice calculates the used bandwidth based on the negotiated codecs in the SDP.
- Both:

  If both are defined then the limit will be enforced as soon as one is crossed.

Functional Sequence

In case of bandwidth-based policies, Open Scape Voice’s behavior for new calls will be as follows:

1) The IRM calculates the required bandwidth based on the most bandwidth-consuming codec(s) in the SDP offer. It then adds the required bandwidth

to the currently used bandwidth and compares it to the limit provisioned for the applicable policy. If the limit is not reached, the required bandwidth is reserved and the call is allowed to proceed. Otherwise the call is terminated.

2) Once the offered SDP is answered, the IRM calculates the actual bandwidth used by the call based on the negotiated codec in the SDP answer. The OpenScape Voice then updates the resource reservation with the actual bandwidth used by the call.

3) When the call is disconnected, the IRM releases reserved resources used by the call.

Offerless INVITE

When an initial offer *without session description* (SDP) is received, a "dummy reservation" for the most bandwidth-consuming *voice* codec allowed for that link is attempted. If this fails, the call is dropped immediately.

Otherwise the call proceeds and when the first 200 OK with SDP offer arrives from the callee, IRM releases the "dummy reservation" and tries to reserve the actually required media resources. This may fail if the SDP tries to include a media type *other than voice* (e.g. video) and the required resources are not available. In this case a 606 Not Acceptable is sent to the caller and the call is dropped. Otherwise the 200 OK is forwarded to the caller.

Dropping answered calls can be prevented by setting the **Allow Answered Calls** flag in the related CAC policy, but this may result in overbooking the CAC policies’ resources.

3.8.6 CAC Traffic Data in Switch

The measurements are written into files. One file is created for every collection interval that contains all the CAC data for that interval. The file names indicate that the data is for CACs and have a timestamp indicating the time and interval length for the collected data.The file naming is consistent with the existing OMM file naming for other measurement groups, such as Trunk Group and PRI data. Logging for CAC is done using Time Base Logging.

3.8.7 CAC Group Measurements

The CAC measurements are stored in a log file for post-processing. Although OpenScape Voice does not offer a mechanism to read these measurements in real time, OpenScape Voice Assistant allows the administrator to view the information in the stored log files in a table format.

Measurement	Description
CAC Policy ID	The CAC policy ID is used as the unique identifier for the counters. If there are two policy IDs associated with the sane CAC Group, two counters are used, one for each policy ID. For Group-to-Group CAC Policies, the group name in the reports must have the following format: `*Group 1, -> Group 2*`,where `*Group 1`,and `*Group 2` ,are the names of the two CAC Groups.
CA C Policy Name	The CAC policy Name is used to provide a user friendly identifier of each CAC POLICY. For Group-To-Group CAC Policies, the group name included in the reports must have the following format: "Group1 <-> Group2", where Group1 and Group2 are the names of the two CAC Groups.
CAC Group Name	This 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 are applied. Groups are defined based on one of the following parameters: • Subnet (up to 64 subnets may be used) • IP Address (up to 64 IP addresses may be used) • Location Domains • Directory Number: this can be a DN prefix (for example, 1561555*) or the DN of a single user (for example, 15615550110). Up to 64 DNs (with wildcards support) may be used
Number of Offered Calls	This counter is incremented each time the 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) is 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 is incremented; the offered calls counter of the terminating CAC group is not 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 is incremented; the offered calls counter of the originating CAC group is not incremented.

Measurement	Description
Number of Blocked Calls	This counter is incremented each time the 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 through an alternate route, for example, through the local PSTN gateway.
Max number of concurrent calls	This counter reports the maximum number of concurrent calls within the monitor interval per CAC policy.
Max used bandwidth	This counter reports the maximum used bandwidth in bits per second within the monitor interval per CAC policy.
Voice offered	This counter reports the number of allowed Voice calls. Offered counters are always increasing. ASAC must be enabled for the counter to work.
Voice blocked	This counter reports the number of blocked Voice calls. Blocked counters are allowed only when a call is blocked by impacted policy. ASAC must be enabled for the counter to work.
Video offered	This counter reports the number of allowed Video calls. Offered counters are always increasing. ASAC must be enabled for the counter to work.
Video blocked	This counter reports the number of blocked Video calls. Blocked counters are allowed only when a call is blocked by impacted policy. ASAC must be enabled for the counter to work.

The following measurements are collected for each provisioned CAC Group:

3.8.8 CAC Record Format

Traffic measurements are collected and recorded by the Operational Measurements Manager (OMM) in the form of CSV files. Using FTP (actually Secure FTP) these files may be downloaded to any Telco platform concerned with the collection of performance data. The files may be transferred in either binary or ASCII format.

Each record is in CSV format and contains the following information:

```
2022-15-06T15:30:00.0

1,CAC_POLICY_NAME_1,CAC_NAME_1,50,32,3,40000,1,2,3,4

2,CAC_POLICY_NAME_2,CAC_NAME_2,32,10,2,30000,2,1,4,3

3,CAC_POLICY_NAME_3,CAC_NAME_3,1,4,5,32000,2,0,3,1

;;;END OF FILE
```

Table 20: Analysis of Log File Information

CAC Log Line(s)	Description	Example
First	Time of Logging	2003-02-20T20:30:00.0
Middle	OM Data of all the CAC Groups. One CAC in each Line (in the example, we have 3)	1,CAC_POLICY_NAME_1,CAC_NAME_1,50,32,3,40000,1,2,3,4 2,CAC_POLICY_NAME_2,CAC_NAME_2,32,10,2,30000,2,1,4,3 3,CAC_POLICY_NAME_3,CAC_NAME_3,1,4,5,32000,2,0,3,1
Last	End of File Mark	;;;END OF FILE

The following measurements are included in the OM Data of each CAC group:

- CAC Policy ID
- CAC Policy name
- CAC Group name
- Number of offered calls
- Number of blocked calls
- Maximum number of calls
- Maximum bandwidth
- Number of offered voice calls
- Number of blocked voice calls
- Number of offered video calls
- Number of blocked video calls
- Maximum value for the counter

3.8.9 Bandwidth Calculation Settings

OpenScape Voice uses the bandwidth control parameters specified in 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.

Related concepts

Bandwidth Requirements for Audio Codecs on page 213

3.8.10 Bandwidth Calculation Factors

The IRM (internal resource manager) 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.

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.

3.8.11 Bandwidth Requirements for Audio Codecs

Bandwidth requirements for audio 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 two tables below show 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.

Functional Sequence

When the calling party rings, the system reserves bandwidth for the worst-case scenario. When the called party answers, the system reserves the actual bandwidth used, based on the codecs used by the subscribers.

Table 21: Bandwidth Requirements - No Calls Using Payload Encryption

Codec	Codec Bit Rate (kbps)	Packetization Interval (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
		40	74.88	4	13	26
		50	73.216	4	13	27
		60	72.107	4	13	27
G.722.1 @ 24 Kbps	24	20	41.6	7	24	48
		40	33.28	9	30	60
		60	30.507	9	32	65
G.722.1 @ 32 Kbps	32	20	49.92	6	20	40
		40	41.6	7	24	48
		60	38.827	7	25	51
G.722.1 @ 48 Kbps	48	20	66.56	4	15	30
		40	58.24	5	17	34
		60	55.467	5	18	36
G.723.1	6.4	30	17.75	16	56	112
		60	12.203	24	81	163
G.729	8	10	41.60	7	24	48
		20	24.96	12	40	80
		30	19.41	15	51	103
		40	16.640	18	60	120
		50	14.976	20	66	133
		60	13.867	21	72	144
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

Codec	Codec Bit Rate (kbps)	Packetization Interval (ms)	Required Bandwidth (kbps)	Number of Calls Possible at a Given Link Speed		
				300 kbps	1 Mbps	2 Mbps
G.726-40	40	10	74.88	4	13	26
		20	58.24	5	17	34
		30	52.69	5	18	37
AAC - LC	96	32	110.240	2	9	18
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 22: Bandwidth Requirements - All Calls Using Payload Encryption(Worst Case)

Codec	Codec Bit Rate (kbps)	Packetization Interval (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
		40	76.96	3	12	25
		50	74.88	4	13	26
		60	73.493	4	13	27
G.722.1 @ 24 Kbps	24	20	45.76	6	21	43
		40	35.36	8	28	56
		60	31.893	9	31	62
G.722.1 @ 32 Kbps	32	20	54.08	5	18	36
		40	43.68	6	22	45
		60	40.213	7	24	49
G.722.1 @ 48 Kbps	48	20	70.72	4	14	28
		40	60.32	4	16	33
		60	56.853	5	17	35
G.723.1	6.4	30	20.52	14	48	97
		60	13.589	22	73	147
G.729	8	10	49.92	6	20	40

Codec	Codec Bit Rate (kbps)	Packetization Interval (ms)	Required Bandwidth (kbps)	Number of Calls Possible at a Given Link Speed		
				300 kbps	1 Mbps	2 Mbps
		20	29.12	10	34	68
		30	22.187	13	45	90
		40	18.72	16	53	106
		50	16.64	18	60	120
		60	15.253	19	65	131
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
AAC - LC	96	32	112.84	2	8	17
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

Related concepts

Bandwidth Calculation Settings on page 212

3.8.12 Bandwidth Fax Considerations

The internal CAC solution in 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.

3.8.13 Video Considerations

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 internal CAC solution continues to use statically configured values for the bandwidth requirements for the video streams provided via H.323 and unknown video codecs as described.

However, 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.

The actual bandwidth being used by the video stream is constantly changing and will usually be a lot 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 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 OpenScape Voice system:

- **H.263 Bandwidth:** The estimated bandwidth required by the video stream for an H.263 call
  - Possible values=32-960000 kbps
  - Default = 160 kbps
- **H.264 Bandwidth:** The estimated bandwidth required by the video stream for an H.264 call
  - Possible values=32-960000 kbps
  - Default = 64 kbps
- **Unknown Bandwidth:** The estimated bandwidth required by the video stream for unknown video codecs
  - Possible values=32-960000 kbps
  - Default = 128 kbps

These values are stored in the same parm file as the other bandwidth calculation parameters. In addition, these values are configurable via the OpenScape Voice Assistant.

NOTICE:

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.

Video CAC enhancements

Call Admission Control in the OpenScape Voice has been enhanced to ensure correct bandwidth calculation for video. With HD endpoints the bandwidth used by the endpoints can be as high as 1.2 Mbit/s, providing the bandwidth is available.

OpenScape Voice Video Service

To integrate Video service in OpenScape Voice and to make the video service aware, the following subfeatures have been added:

- CDR enhancements (Call type,Bit rate etc.).
- Business Group Line (control which BGL can make Video calls - this will ensure that HD conference capable lines has enough bandwidth).
- Routing based on Service required. (E.g. based on Video service request (in SDP), route to Video GW.)

Functional Sequence

The IRM shall process requests for Video calls according to the following rules:

1) Enough Bandwidth for Both the Audio and Video Streams: The Video call is allowed (i.e. IRM sends a positive response).
2) Not Enough Bandwidth for the Audio Stream: The Video call is not allowed (i.e. IRM sends a negative response with Error Code = "Insufficient Resources").
3) Enough Bandwidth for the Audio Stream, Not Enough Bandwidth for the Video Stream:

   a) Video Tone or Announcement (i.e. MEDIA_SERVER_ANNOUNCEMENT flag is set): The Video call is not allowed (i.e. IRM sends a negative response with Error Code = "Insufficient Resources").
   b) New flag ("Audio only allowed when Video requested") is NOT set for the CAC Policy: The Video call is not allowed (i.e. IRM sends a negative response with Error Code = "Insufficient Resources").
   c) New flag ("Audio only allowed when Video requested") is set for the CAC Policy: Audio only call is allowed. In this case, the IRM modifies the SDP offer to cancel the video portion and sends back a positive response.

3.8.14 Enhanced Video Call Support

The OpenScape Voice server provides specific video service support allowing video calls to be identified and handled separately if required in the server. With this feature the OpenScape Voice will be able to enable users for Video support and allow routing of calls based on the video media type.

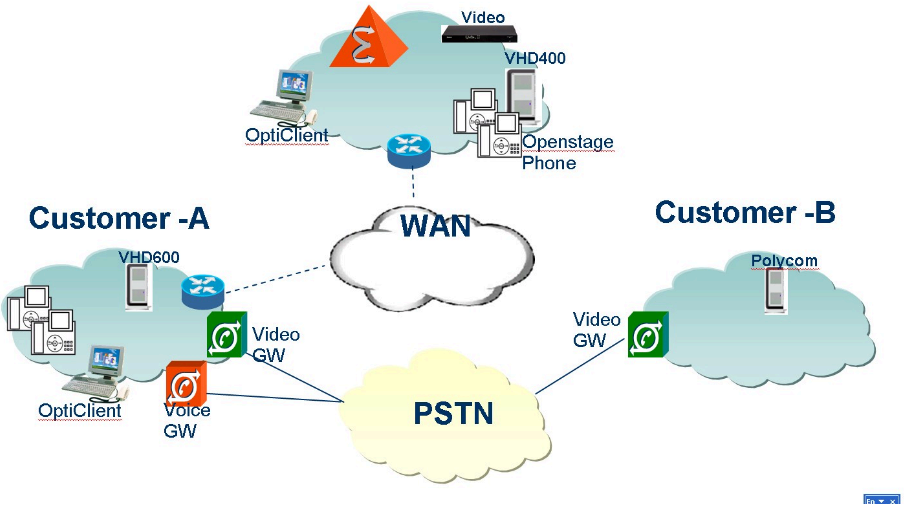


Figure 20: Video Service Landscape for the OpenScape Voice solution

Video Characteristics in CDR's

Once a video call had been negotiated end to end, the OpenScape Voice server will record as part of the internal CDR records, information regarding the Media Type and the bit-rate used for the call.

For this purpose the following existing fields in the CDR will be used:

- Field # 20 "Bearer Capability Request" - to save the bit- rate for the call.
  - If video call is made field 20 will show "3 (Circuit mode 64 Kbps)".
- Field # 104 "Media Type" that is a bitwise data and reflects audio, audio/video or video depending how it is set by the component using its method in the CDR
  - If video call is made field 104 will show "3 (Audio, Video)".

Routing Calls Based on Video Capabilities

Gateway Routes for destinations on the OpenScape Voice server will be provisioned such that they are identified as preferred gateways supporting video calls. Based on the SDP offer indicating as video call, the OpenScape Voice will be able to route the call over a preferred gateway for video if the route is configured as such.

Such a provisioning will allow OpenScape Voice to prioritize and dynamically route calls for video over preferred gateways connected to the server.

In order to achieve preferred gateway routes for video calls, firstly gateways that will handle video calls will be identified. Next routes will be configured with destinations pointing to such gateways with their bearer capabilities set to "Unrestricted" (Data64KB).

When a video call is made, OpenScape Voice will identify the call to be a video call and set the call to the same bearer capabilities value such that the preferred gateway routes for the call can be identified by selecting a preferred gateway for the matched route.

This will ultimately ensure that the call is routed over the preferred gateway.

Enable Video Service for Subscribers

The **Video Call Allowed** feature allows or dis-allows an subscriber to make or receive video calls.

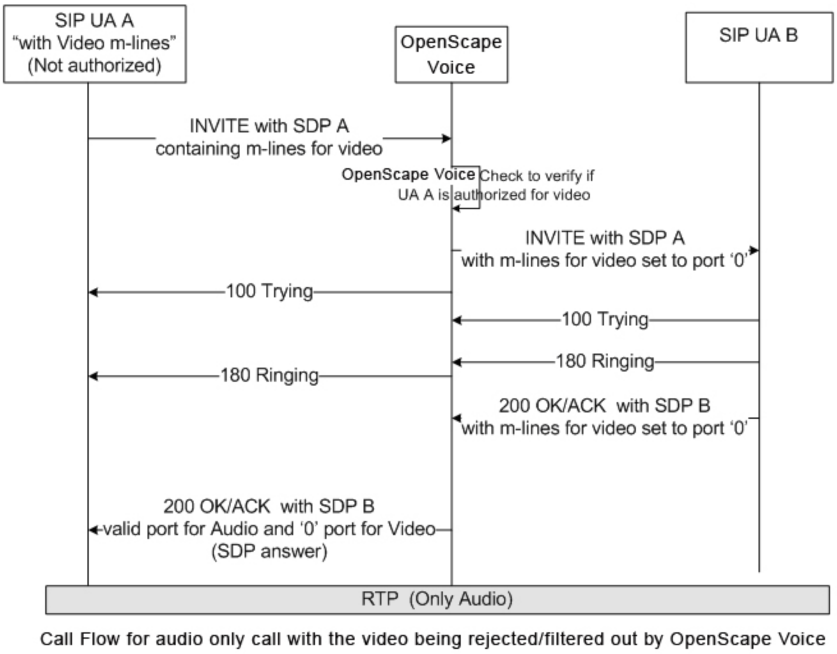

SIP UA A
"with Video m-lines"
(Not authorized)
OpenScape Voice
SIP UA B
INVITE with SDP A
containing m-lines for video
OpenScape Voice Check to verify if
UA A is authorized for video
INVITE with SDP A
with m-lines for video set to port '0'
100 Trying
100 Trying
180 Ringing
180 Ringing
200 OK/ACK with SDP B
with m-lines for video set to port '0'
200 OK/ACK with SDP B
valid port for Audio and '0' port for Video
(SDP answer)
RTP (Only Audio)
Call Flow for audio only call with the video being rejected/filtered out by OpenScape Voice

Figure 21: Overview of OpenScape Voice Filtering out Video from the Call

The **Video Call Allowed** attribute is available on a per subscriber endpoint basis and available to all contacts of that subscriber. The default is "allow video calls for all subscribers", but the administrator can block video calls from/to a particular subscriber:

- If the **Video Call Allowed** check mark is turned **ON**, then the OpenScape Voice will allow video calls across the server.
- If the **Video Call Allowed** check mark is turned **OFF**, then even if subscriber makes video calls, the port of all video m-lines will be set to zero by the OpenScape Voice server before routing the call to intended receiver.

3.8.15 Establishing Codec Restrictions

The internal CAC solution in OpenScape Voice restricts the voice codecs for calls between SIP/SIP-Q endpoints. This feature is also applicable for MGCP connections to the Media Server for announcements, tones or conference.

NOTICE:

This feature is not applicable to T.38 Fax over UDPTL in either version.

The internal CAC solution in 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.

Enhanced CAC codec restrictions also include calls to the Media Server via MGCP. The subscriber has the (switch-wide) capability to either restrict or not the MGCP sessions, when the flag **Ignore MS Calls** is applied to a CAC policy.

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 e.g. 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.

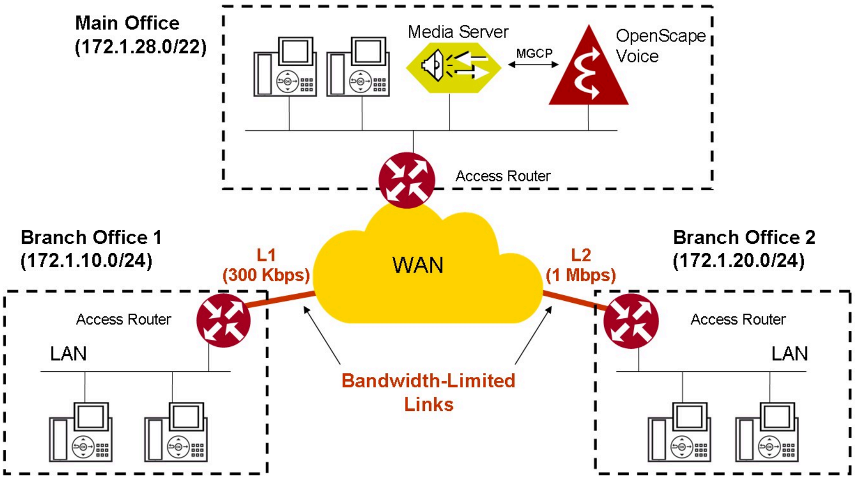


Figure 22: Sample Network Topology Requiring Voice Codec Restriction

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 below 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.

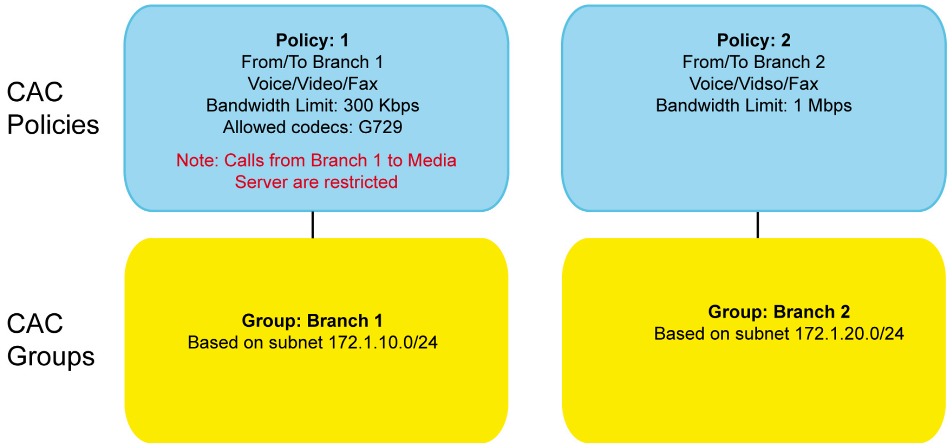


Figure 23: Sample CAC Policies to Restrict Voice Codecs

3.8.16 Overriding Codec 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

3.8.17 Dynamic Handling of Link Failures

OpenScape Voice permits optional provisioning of primary and secondary link capacities for each CAC (Call Admission Control) 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.

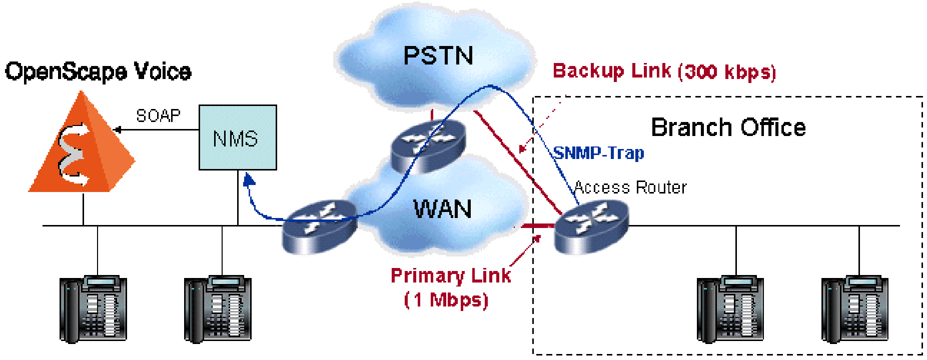


Figure 24: Sample Configuration for Dynamic Handling of Link Failures

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 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 OpenScape Voice to switch back to the primary capacity of the CAC policy.

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.

The Figure below provides a simple example of this configuration:

For this example, the CAC Group and CAC Policy shown in the figure below must be created for the branch office:

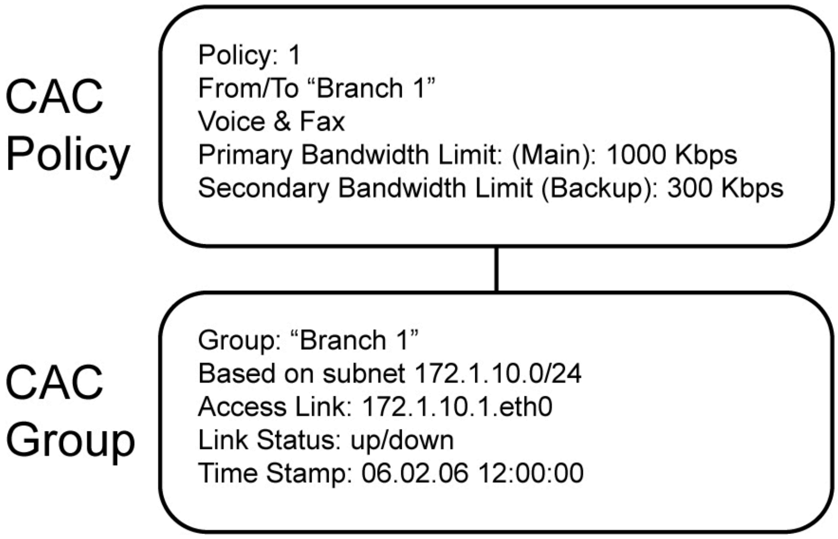

CAC
Policy
Policy: 1
From/To “Branch 1”
Voice & Fax
Primary Bandwidth Limit: (Main): 1000 Kbps
Secondary Bandwidth Limit (Backup): 300 Kbps
CAC
Group
Group: “Branch 1”
Based on subnet 172.1.10.0/24
Access Link: 172.1.10.1.eth0
Link Status: up/down
Time Stamp: 06.02.06 12:00:00

Figure 25: Sample CAC Group and CAC Policy for Dynamic Handling of Link Failures

3.8.18 CAC Administration from OpenScape Voice Assistant

The CAC/Resource Management feature can be administrated from the OpenScape Voice Assistant. It is enabled and configured at the switch level. Codec restrictions defined in CAC Policies can be overridden at the endpoint or subscriber level.

For scenarios involving two or more OpenScape Voices, each OpenScape Voice is responsible for the bandwidth management of its own endpoints. The only requirement is that there cannot be endpoints that belong to two (or more) OpenScape Voices served by the same bandwidth-limited link, for example, in the same branch location. All endpoints served by a particular bandwidth-limited link must be configured in the same OpenScape Voice

Functional Sequence

OpenScape Voice Assistant supports the following topics under the menu

OpenScape Voice > **Administration** > **Call Admission Control Management**

- **Resource Management** menu:
  - Enabling the internal CAC solution
  - Configuration of parameters used for bandwidth calculation
- **Groups** menu:
  - Provisioning CAC groups
- **Policies** menu:
  - Provisioning CAC policies and group-to-group CAC policies
- **Monitoring** 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:

OpenScape Voice > **Business Group** > **Members** > **Endpoints**

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 measurements. This data can be invaluable to the network planner in evaluating the performance of the network and finding remedies for observed problems.

3.8.19 CAC (Call Admission Control) Group

A CAC (Call Admission Control) Group represents the group of endpoints being served by each bandwidth-limited link which needs to be monitored. 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 are applied.

CAC Group Definition

When a call is set up, the CAC service enforces the restrictions imposed on the calling and called party, according to their CAC Group.

A CAC Group, in turn, is intended to represent a particular segment of the corporate network. It should be provisioned to contain all subscribers, that are **currently** located at this segment. A CAC Group can be defined based on the following attributes:

- IP addresses

  Can for example be used for endpoints representing a network segment behind an SBC (from OSV’s perspective)

  Up to 128 constituent IP adresses can be provisioned per group.
- IP subnets

  Typically used for corporate network segments that are not hidden by an intermediate SBC

  Up to 128 constituent IP subnets can be provisioned per group.
- DNs or DN prefixes (such as 1561555*)

  From the resource perspective this only makes sense if the subscribers are immobile and the DN assignment "mirrors" the network segmentation.

  Up to 64 constituent DNs or DN prefixes can be provisioned per group.
- CAC Groups

  This is used to impose common restrictions on a group of "child" CAC groups.

- Location Domains

  The preferred solution for network segments behind SBCs (from OSV’s perspective).

  Location Domains created via endpoint provisioning shall take precedence over any *Location Domain* information received via SIP signalling

  Up to 64 constituent Location Domains can be provisioned per group.

Defining a CAC Group based on different attribute types is not possible.

If there are mobile users that are allowed to connect via different network segments, the DN-based definition doesn’t serve well. See the topics on Location Identification for the proposed solution.

> **NOTICE:**
>
> As a prerequisite, **mobile user agents have to be provisioned for DHCP!**

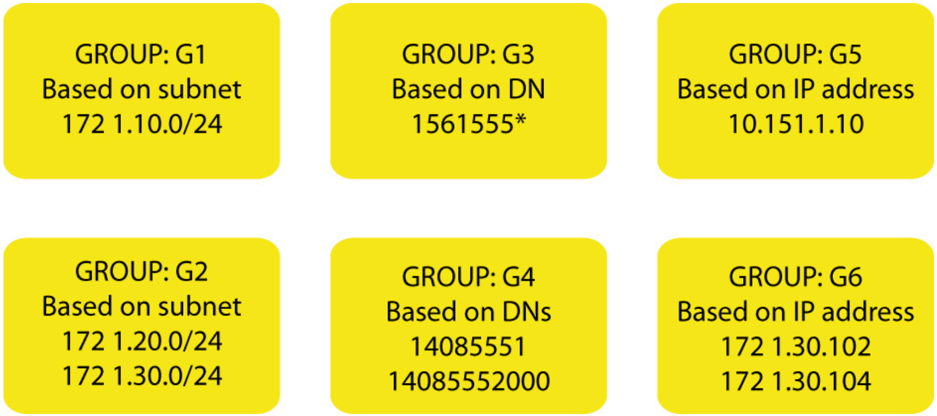


Figure 26: Valid CAC group definitions.

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

Overlapping Group Definitions

If two or more CAC groups have overlapping definitions, the CAC service prioritizes the CAC groups.

- If the **Prioritize Location Domains** flag is set then the following priority is applied:

  CAC groups based on Location Domains

  CAC groups based on IP address

  CAC groups based on Subnets - 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 DNs

- If the **Prioritize Location Domains** flag is not set (default) then the following priority is applied:

  CAC groups based on IP address

  CAC groups based on Subnets - 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 Location Domains

  CAC groups based on DNs

RTP Parameters

To support up to 6000 CAC groups in OpenScape Voice ;at, the default values of the following RTP parameters have been modified:

- Srx/Rdal/RdalGroupPolicyTblSize from 1000000 to 12000000 bytes
- Srx/Rdal/RdalPolicyBWTblSize from 5000000 to 12000000 bytes
- Srx/Rdal/RdalIpMapDataTblSize from 1400000 to 12000000 bytes
- Srx/Rdal/RdalDnMapDataTblSize from 1000000 to 12000000 bytes
- Srx/Rdal/RdalGrpToGrpTblSize from 1000000 to 12000000 bytes
- Srx/Rdal/RdalParentGrpTblSize from 100000 to 12000000 bytes
- Srx/Rdal/RdalResvDataTblSize from 15000000 to 12000000 bytes
- Srx/Rdal/RdalSdpOlineTblSize from 2000000 to 12000000 bytes

and the following new RTP parameters were introduced:

- Srx/Rdal/RdalGroupDefTblSize (default value 12000000 bytes)
- Srx/Rdal/RdalSSDnMapDataTblSize (default value 12000000 bytes)

3.8.20 CAC (Call Admission Control) Policies

A CAC (Call Admission Control) Policy is assigned to a CAC Group and represents the characteristics for the bandwidth-limited link being monitored. OpenScape Voice supports CAC Policies for voice-RTP (Real-time Transport Protocol), SRTP (Secure Real-time Transport Protocol),video-RTP and/or T.38 Fax-UDPTL (User Datagram Protocol Transport Layer).

CAC Monitoring

A CAC policy can limit the calls over a bandwidth-limited link based on number of calls, bandwidth limit, or both.

OpenScape Voice Assistant 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 DND displayed independent of whether the CAC policy is limiting the calls based on number of calls, bandwidth limit, or both.

General information

Each CAC Policy contains the following information:

- The CAC Group or parent CAC Group to which the policy applies. The CAC Policy applies to all calls to and from the CAC Group.

- The traffic type controlled by the CAC Policy. This can be:
  - Only Voice (RTP)
  - Only Fax (T.38 over UDPTL)
  - Only Video (RTP)
  - Combined Voice/Fax
  - Combined Voice/Video
  - Combined Fax/Video
  - Combined Voice/Fax/Video
- The capacity limits the CAC Policy enforces for a primary link and optionally for a secondary (backup) link. The primary and secondary capacities can be defined based on the number of calls, bandwidth limit, or both, as follows
  - **Number of calls:**

    The concurrent calls per CAC Policy are counted. When the limit is reached, no new calls are admitted.
  - **Bandwidth limit:**

    OpenScape Voice calculates the used bandwidth based on the negotiated codecs in the SDP (Session Description Protocol). 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.

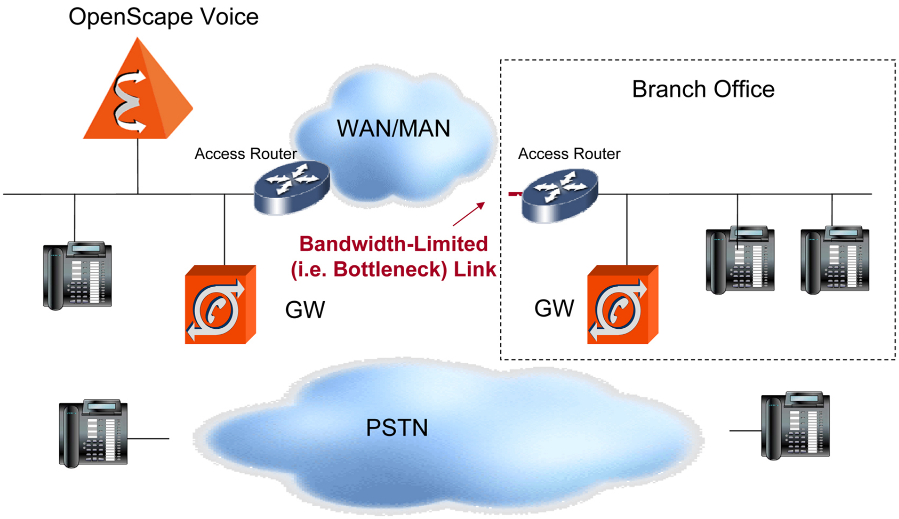


Figure 27: Branch office with bandwidth-limited link

– **Both:**

  If both number of calls and bandwidth limit are defined, the limit is enforced as soon as one is reached.

NOTICE:

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 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.
- 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 (Dual Tone Multifrequency) 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.

NOTICE:

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 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 Policies as long as the **same traffic type is not used** by more than one policy.

- One CAC Policy for audio, another CAC Policy for fax (OK)
- **or** one CAC Policy for both audio and fax, another CAC Policy for video (OK).
- **But not** one CAC Policy for audio and video, another CAC Policy for fax and video (not allowed because video is defined twice).

With the introduction of the Video traffic type, there can be up to 3 CAC Policies assigned to the same CAC Group (one policy for Voice, one for FAx and one for Video).

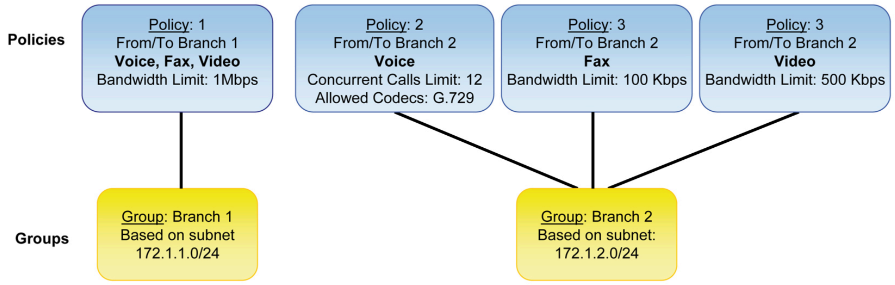


Figure 28: CAC Policy Relationships to CAC Groups

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.

NOTICE:

When a new CAC policy is provisioned, OpenScape Voice does not apply the policy to any existing calls. Only new calls after the policy has been provisioned are monitored by OpenScape Voice.

Functional Sequence

In case of bandwidth-based CAC Policies, the OpenScape Voice server behavior is as follows:

1) For new calls, the OpenScape Voice server calculates the required bandwidth (BWREQUIRED) based on the worst-case codec in the call request. The OpenScape Voice server then adds the required bandwidth of the call to the currently used bandwidth (BWUSED) and compares it to the limit provisioned for the CAC Policy (BWLIMIT). If the limit is not reached (BWUSED + BWREQUIRED =< BWLIMIT), the call is allowed and the required bandwidth is reserved (BWUSED = BWUSED + BWREQUIRED).
2) After the call is established, the OpenScape Voice server calculates the actual bandwidth (BWACTUAL) used by the call based on the negotiated codec in the call answer. The OpenScape Voice server then updates the currently used bandwidth with the actual bandwidth used by the call (BWUSED = BWUSED + [BWACTUAL - BWREQUIRED]).
3) When the call is disconnected, the OpenScape Voice server releases the actual bandwidth (BWACTUAL) used by the call (BWUSED = BWUSED - BWACTUAL).

System Specific Information

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 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 OpenScape Voice server — in the way. In these scenarios, the EPs (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 below, in which OpenScape Voice server A serves Branch Office 1, and 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 OpenScape Voice server A. The bandwidth management for the bottleneck link to Branch Office 2 (L2), on the other hand, is performed by OpenScape Voice server B.

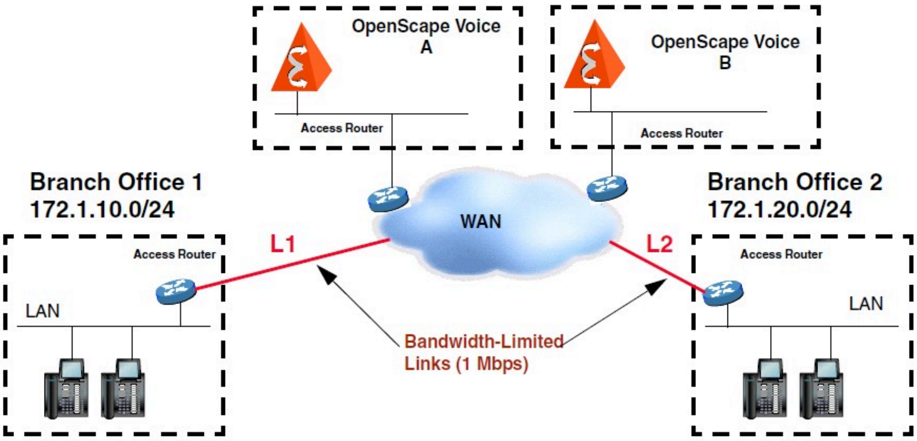


Figure 29: Endpoints Behind Another OpenScape Voice Server

3.8.21 Group-To-Group CAC (Call Admission Control) 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.

The figure below 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

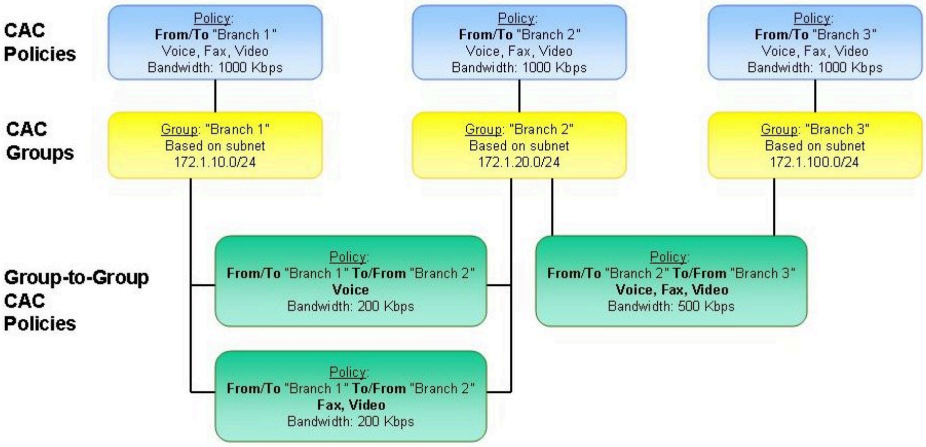

CAC Policies
CAC Groups
Group-to-Group CAC Policies
Policy: From/To "Branch 1" Voice, Fax, Video Bandwidth: 1000 Kbps
Policy: From/To "Branch 2" Voice, Fax, Video Bandwidth: 1000 Kbps
Policy: From/To "Branch 3" Voice, Fax, Video Bandwidth: 1000 Kbps
Group: "Branch 1" Based on subnet 172.1.10.0/24
Group: "Branch 2" Based on subnet 172.1.20.0/24
Group: "Branch 3" Based on subnet 172.1.100.0/24
Policy: From/To "Branch 1" To/From "Branch 2" Voice Bandwidth: 200 Kbps
Policy: From/To "Branch 2" To/From "Branch 3" Voice, Fax, Video Bandwidth: 500 Kbps
Policy: From/To "Branch 1" To/From "Branch 2" Fax, Video Bandwidth: 200 Kbps

Figure 30: Call Admission Control — Group-To-Group CAC Policies

3.8.22 CAC (Call Admission Control) Rerouting

This feature provides the rerouting of calls to SIP gateways, SIP-Q gateways or SIP subscribers if OpenScape Voice receives a SIP response code indicating a bandwidth restriction.

Due to the integrated CAC (Call Admission Control) solution OpenScape Voice provides rerouting via the PSTN (Public Switched Telephone Network) 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 OpenScape Voice’s ability to reroute calls based on a provisionable set of SIP response codes.

Among other things, this feature provides for the rerouting of calls to SIP gateways, SIP-Q gateways, or SIP subscribers if OpenScape Voice receives a SIP response code indicating a bandwidth restriction (for example, `606 Not Acceptable`).

Functional Sequence

1) For the integrated CAC solution, OpenScape Voice does not actually receive a SIP 606 response code from the terminating B-side of the call.
2) However, the RM (Resource Management) 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.
3) No INVITE message is sent to the B-party in case of bandwidth limitation

Other characteristics

- A correlated CAC restricted subscriber rerouted call ends up to need another subscriber rerouting due to CAC restrictions between the called party and the party that the called party forwarded to, the forwarding should be thrown back to the original outgoing call and applied from there. This will allow saving PSTN resources (calling and forwarded-to party may have no CAC restrictions) and also the complexity of the resulting call is greatly reduced. Calls are tied in the OpenScape Voice.

- Incoming gateway calls in a CAC restricted branch to a local branch office subscriber (no CAC restriction on this call as both gateway and subscriber are in the same CAC Group) is forwarded to a central VMS (Voice Mail Server) located in the data center. As the Voice Mail Server is administered as a trunk, endpoint rerouting would be activated for the call to VM (Voice Mail). If all routes for endpoint rerouting are exhausted, enhanced CAC restricted subscriber rerouting will be tried. Calls are tied in the OpenScape Voice.

3.8.22.1 Gateway and Subscriber Rerouting

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.

- **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 OpenScape Voice features - for example, group features that are needed by subscribers in a branch.

3.8.22.2 Gateway Rerouting

When a call is being directed by 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).

Calls may also be rejected due to the following:

- Processor overload conditions in the gateway
- Partial gateway system failures
- WAN congestion

- Other maintenance problems

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 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 the table below will, by default cause a gateway to attempt rerouting.

Table 23: SIP Response Codes That Cause Rerouting

Number	Name	Number	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
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		

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 craftsperson must enable the following SIP systemwide features:

- Rerouting for SIP endpoints
- Registration renewal

A provisionable audit interval time can be set by the craftsperson. 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.

3.8.22.3 Basic CAC-Restricted Subscriber Rerouting

Subscriber rerouting is a feature that can provide additional reliability for remote subscribers connected to OpenScape Voice by a WAN link which has restricted bandwidth or less-than-desired reliability.

When a single OpenScape Voice system supports subscribers that are geographically distributed, most subscribers are typically co-located with OpenScape Voice. However, many subscribers 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.

If the WAN link between the sites 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 below, subscriber 31002 (in Florida) dials subscriber 21001 (in San Jose). Because the WAN link is congested, 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 OpenScape Voice via the PSTN.
- In backup mode, the survivable branch office proxy or gateway can continue to communicate with OpenScape Voice via a backup link through the PSTN. This option requires appropriate provisioning of the applicable CAC groups.

This feature is extended to permit its use:

- If the calling party is not a subscriber registered on 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, OpenScape Branch.
- built into the remote PSTN gateway, as in the case of the OSB gateway.

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.

Requirements

To enable the subscriber rerouting feature, the following hardware configuration and database parameters need to be configured:

- The SIP phones in the branch must have a valid public E.164 number, be configured with the IP address of the proxy, and the proxy must be configured with the IP address of OpenScape Voice. The phones then register with the proxy, which relays the registration message to OpenScape Voice after adding a second VIA-header.

- In OpenScape Voice Assistant:
  - Each branch subscriber that is served by the proxy must be identified, by filling in the Associated Endpoint field with the Endpoint name of the serving proxy. This field must match the endpoint name of the OSB survivable proxy in order for the feature to be activated.
  - The SIP proxy endpoint can be configured with the “Survivable Endpoint” attribute.
  - The SIP proxy endpoint can have the following additional attributes selected:

Table 24: Selectable attributes (none of them applicable to subscriber endpoints)

Attribute	Description
Enhanced Subscriber Rerouting	Select this attribute to enable enhanced subscriber routing, which pertains to the ability to reroute forwarded calls and hunt group calls.
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 ist not commonly used, and should not be selected for gateway endpoints.
SIP Proxy	If selected (enabled), the endpoint is a SIP proxy applicable only to SIP endpoint.This attribute is not applicable for SIP Private Networking.
Route Via Proxy	When selected (enabled) together with the SIP Proxy attribute, this endpoint is on the route when the OpenScape Voice is making an outbound call to a subscriber that has this endpoint as its Associated Endpoint.

Attribute	Description
Allow Proxy Bypass	Proxy Bypass is a system-wide OpenScape Voice feature that is turned on per default. It is only used when deploying Type 2 or 5 branch offices. If selected (enabled), Proxy Bypass allows OpenScape Voice to bypass the recorded proxy in a contact if an INVITE request to the contact's recorded proxy does not receive a response within a specified time.This attribute is not applicable for SIP Private Networking.

- Enable subscriber rerouting by setting “Enable Rerouting to SIP Subscribers” and defining a “Subscriber Rerouting Prefix Access Code”. The suggested Rerouting PAC is “*001”.
- Define CAC Groups so that subscribers and endpoints in each branch office are logically grouped. Be sure to include any proxy endpoint and media gateways in the CAC Group for the branch they belong to or represent. The policies for the CAC Groups can vary, but the simplest is to restrict the number of inter-CAC group calls to 0.

Functional Sequence

As in the case of **Gateway rerouting**, when the feature is enabled, alternate routing is triggered when the remote location is blocked due to bandwidth restrictions.

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 administrator must provision a subscriber rerouting prefix access code. 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.

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.

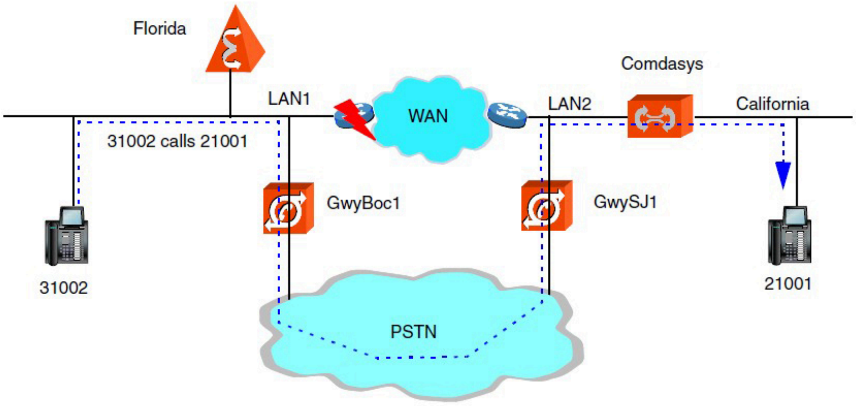


Figure 31: Subscriber Rerouting Example

Subscriber Rerouting and Toll and Call Restrictions

A system-wide option `Srx/Main/InvokeRestrictionsOnRerouting` determines, whether toll restrictions shall be bypassed (`RtpFalse`) or not (`RtpTrue`) on the subscriber rerouting call leg. Its default value is `RtpFalse`, i.e. Toll and Call restrictions won’t be applied.

3.8.22.4 Rerouting PSTN (Public Switched Telephone Network) Calls to Alternate Gateways

PSTN (Public Switched Telephone Network) calls can also be rerouted to alternate SIP or SIP-Q gateways.

Assume that OpenScape Voice is provisioned for tail-end hop-off. Whenever a Boca Raton subscriber dials a local number in San Jose, the PSTN gateway in San Jose is chosen as the first route out of the network, making this otherwise long-distance call a local call in San Jose and therefore less expensive.

This scenario, however, requires the RTP (Real-time Transport Protocol) media stream to go through the bandwidth-limited links that connect the Boca and the San Jose branch offices to the WAN.

If there is not enough bandwidth available in either link, the resource reservation is not successful and the RM (Resource Manager) function generates a negative response equivalent to a SIP 606 response code.

OpenScape Voice then reroutes the call via the local gateway to reach the right number via the PSTN or SIP-Q gateway.

Related concepts

Rerouting a Call to a SIP Subscriber on page 244

3.8.22.5 Enhanced CAC-Restricted Subscriber Rerouting

Correlation Framework Service

As the CAC-Rerouted call passes through the PSTN, the only possible correlating factor can be the called party number. Calling party numbers are not necessarily transparently transported by the central office and user-to-user ISDN services come at a higher cost. E.g. in ISDN, transporting the CLIP/CLIR is a subscribed service. If not subscribed, the CO routinely replaces any delivered CLIP/CLIR with a standard CLIP/CLIR for the whole trunk. Analog Central Offices may or may not transport Caller ID.

Using the Called Party Number requires the subscription to the Direct Inward Dialing (DID) service on the connection with the central office. This means that the numbers that will be used to correlate the CAC-Rerouted call legs must be directly addressable from the public network without passing through an attendant.

As it cannot be guaranteed that the number of the called party is actually a DID number (the called party may only have a private number, indicated in the OpenScape Voice by not setting the External Directory Number flag), a special pool of DID numbers must be reserved in each survivable branch office to support this feature. Even in case the called party does have a valid DID number, a number from the DID pool should be used. The reason for this is that the correlation service uses only the DID number to correlate the call legs. So, on the terminating CAC-rerouted call leg, the correlation service blindly goes and looks for the originating CAC-Rerouted call leg. On a glare situation, where the OpenScape Voice reroutes a call and at the same time a 'real' PSTN subscriber calls the called party, then the correlation service might correlate the wrong calls together and present the 'real' PSTN subscriber as the calling OpenScape Voice subscriber to the B-party. The OpenScape Voice's only choice in a glare situation would be to clear both calls. By using a number from the DID pool, the CAC-rerouted call can be thrown back to the originating CAC-rerouted call leg which can reestablish the call and the call from the PSTN can be safely cleared as the called number does not belong to any subscriber.

Survivability

CAC-Restricted Subscriber Rerouting has a limitation that it is only allowed for called subscribers that have a valid E.164 number in the public network. With the use of the DID-pool (which of course are guaranteed to be valid E.164 numbers in the public network), Enhanced CAC-Restricted Subscriber Rerouting lifts this restriction because it is not the called subscribers number anymore that is rerouted, but the DID number from the DID pool. This means that Subscriber Rerouting will also be activated for:

- Calls to subscribers that only have a private number. Due to the correlation service the private number is linked to a public DID number from the DID pool.
- Calls to DLS mobility subscribers. The OpenScape Voice must allow calls to DLS mobility subscribers in the branch office to succeed. This means that the restriction that for rerouting to take place, the subscriber has to be registered from his/her home branch is lifted. Due to the correlation service, the call to the DLS Mobility subscriber is replaced with a call to a DID number from the DID pool of the branch office where the subscriber is registered.
- Calls diverted to a Voice Mail Server. The OpenScape Voice must allow calls to be forwarded to a Voice Mail System even in situations where the Voice Mail System is not accessible due to a CAC restriction. After all routes to the Voice Mail Server are exhausted, the CAC restricted Voice Mail Server can be contacted via the PSTN using a DID number from the DID pool of the office where the Voice Mail Server is located.
- Hunt groups must have the Enable Rerouting advanced attribute selected.

Requirements

To enable Enhanced Subscriber Rerouting, the following configuration steps are necessary.

1) Configure a representative endpoints for each branch office. In most cases, a branch proxy will be the representative endpoint of the branch office. In these cases, the proxy endpoint should be configured with the “Survivable Endpoint” attribute. The proxy endpoint may also have attributes “SIP Proxy”, “Route Via Proxy”, and “Allow Proxy Bypass” set.

  - A pseudo-branch office without a proxy may also be necessary to provide this feature for main office subscribers. This requires configuration of a dummy representative endpoint. This dummy endpoint should also be configured with the “Survivable Endpoint” and “Do Not Audit” attributes. The “SIP Proxy” attribute must not be set.

2) Configure Branch Offices. Each branch office must have a representative endpoint. This will either be a proxy endpoint for the branch or a dummy endpoint for a pseudo-branch office. Each branch office must also have a DID Pool configured with DNs that are delivered through the PSTN for Enhanced Subscriber Rerouted calls
3) Create DNs for DID Pool Usage. Each branch office needs a small pool of local DID numbers for rerouting calls through the PSTN. At least two such DID numbers should be configured per branch taking as a general rule one DID number for each 180 branch users. These must be free Home DNs. These numbers are local to the branch such that calls made to the PSTN using these numbers are delivered to a gateway present in the CAC restricted branch.
4) Define CAC Groups. Define CAC Groups so that subscribers and endpoints in each branch office are logically grouped. Many options exist, but the simplest arrangement is to define one CAC Group per branch office and include all branch office members in the CAC Group by their IP address. Be sure to include any proxy endpoint and media gateways in the CAC Group for the branch they belong to or represent. The policies for the CAC Groups can vary, but the simplest is to restrict the number of inter-CAC group calls to 0.Specify the branch office associated with each CAC Group when defining the CAC groups.
5) Enable Resource Management and Configure a Subscriber Rerouting PAC at the System Level. Turn on resource management system wide by selecting “Enable Resource Management”. Enable subscriber rerouting by setting “Enable Rerouting to SIP Subscribers” and defining a “Subscriber Rerouting Prefix Access Code”. The suggested Rerouting PAC is “*001”.
6) Configure Rerouting to PSTN in each branch office. This step is simplified if each branch office uses a unique numbering plan. The system-wide Rerouting PAC is prefixed to a DID Pool number for the destination branch office. So each branch office's numbering plan must route calls of format ReroutingPAC+DIDNumber out a local gateway to the PSTN. For more information, see chapter **How to Create/Edit a Hunt Group**, step 32

Functional Sequence

The actual enhanced subscriber rerouting is activated when a CAC restriction is detected when OSV intends to send a call to the CAC restricted branch. When the reroute request is because of a CAC-Restriction, then AS shall first checks whether the destination of the call (B) belongs to a branch office with a DID pool and if so retrieve a DID number from that branch office's DID pool. The correct DID pool for the called party is found in two possibilities - in order of preference

- If the called party belongs to a CAC Group which has an Associated Branch Office, use the DID pool of the Associated Branch Office.
- If the called party registered via a branch office's proxy, use the DID pool of the branch office of the associated endpoint of the called party's contact.

OSV prefixes the DID number with the Subscriber Rerouting PAC and offers the resulting dial string to translation using the numbering plan of one of the following 3 possibilities in order of preference:

- If the calling party belongs to a CAC Group which has an Associated Branch Office, use the numbering plan of the Branch Office's Representative Endpoint.
- If the calling party registered via a branch office's proxy, use the associated endpoint of the calling party's contact
- In all other cases, the numbering plan of the calling party is used.

The call is made to the PSTN and if the right DID numbers were configured on the target branch office, the call should enter via the gateway of the target branch office and be reoffered to OSV. At this point OSV correlates the outgoing call vs the incoming call based on the called party number of the incoming call (translation is set up to point to the enhanced subscriber rerouting (TIE) service). Once correlated, the called party is called (this time there shouldn't be any CAC restriction because the incoming call came from the branch office where the called party is located) and the DID number used to tie outgoing call with incoming call is released and can be reused for other calls.

Other characteristics

The Enhanced CAC-Restricted Subscriber Rerouting feature allows calls originated in the PSTN to be rerouted as well.

If no DID number can be seized from the DID pool, the solution automatically falls back to basic CAC-Restricted Subscriber Rerouting solution which uses the called party's number for setting up the rerouting through the PSTN. This will only work if the called party has a public number and the subscriber did not use DLS mobility from another branch office than his own.

If the Originating CAC-Rerouted call leg receives a release and the DID is still reserved, this would indicate a problem with shared memory between the cluster nodes and a fallback to basic CAC-Restricted Subscriber Rerouting is attempted.

Related concepts

Rerouting a Call to a SIP Subscriber on page 244

3.8.22.6 Enhanced CAC Restricted Subscriber Rerouting for Endpoints

Incoming gateway calls in a CAC restricted branch to a local branch office subscriber (no CAC restriction on this call as both gateway and subscriber are in the same CAC group) are forwarded to a central Voice Mail Server located in the data center.

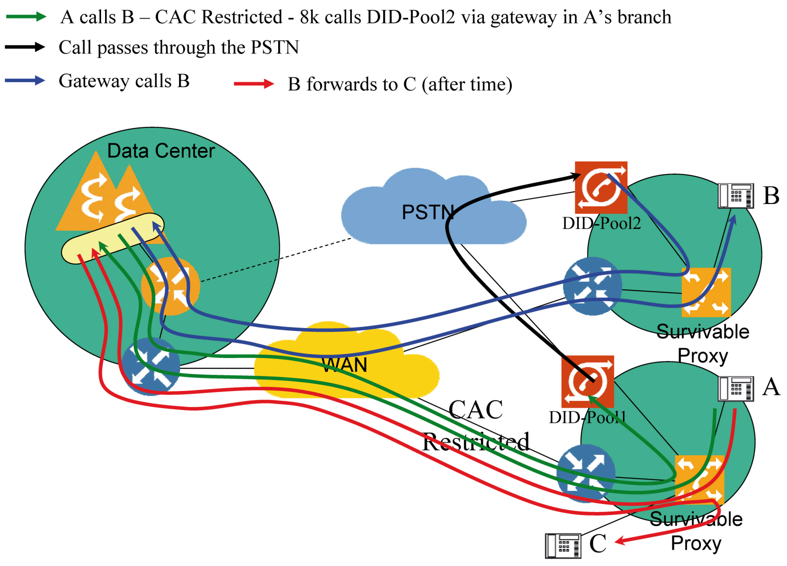

A calls B – CAC Restricted - 8k calls DID-Pool2 via gateway in A's branch
Call passes through the PSTN
Gateway calls B
B forwards to C (after time)
Data Center
PSTN
DID-Pool2
B
Survivable Proxy
WAN
A
DID-Pool1
CAC Restricted
Survivable Proxy
C

Figure 32: Enhanced CAC Restricted Subscriber Rerouting for Endpoints

As the Voice Mail Server is administered as a trunk, endpoint rerouting would be activated for the call to Voice Mail. If all routes for endpoint rerouting are exhausted, enhanced CAC restricted subscriber rerouting will be tried. Calls are tied in the OpenScape Voice.

Related concepts

Rerouting a Call to a SIP Subscriber on page 244

3.8.22.7 Double CAC Restrictions in case of Call Forwarding

In scenarios where a correlated CAC restricted subscriber rerouted call ends up to need another subscriber rerouting due to CAC restrictions between the called party and the party that the called party forwarded to.

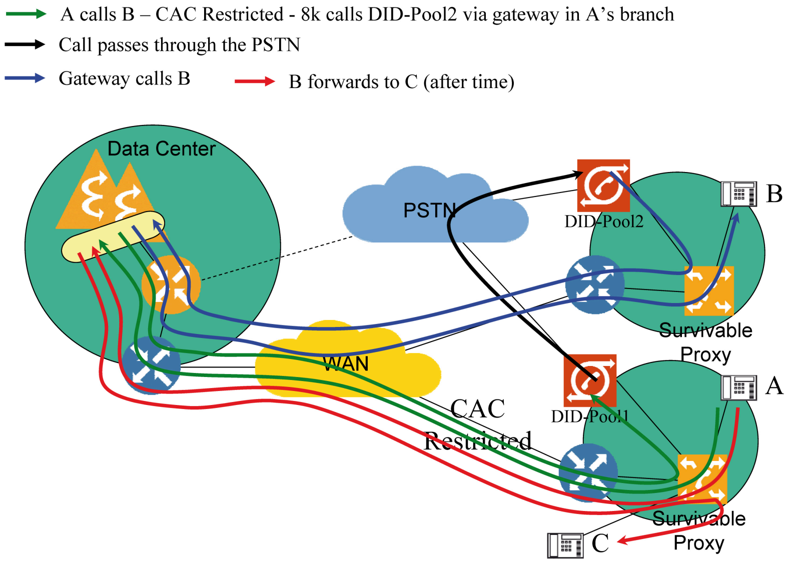

A calls B – CAC Restricted - 8k calls DID-Pool2 via gateway in A’s branch
Call passes through the PSTN
Gateway calls B
B forwards to C (after time)
Data Center
PSTN
DID-Pool2
B
Survivable
Proxy
WAN
CAC
Restricted
DID-Pool1
A
Survivable
Proxy
C

Figure 33: Double CAC Restrictions in case of Call Forwarding

The forwarding should be thrown back to the original outgoing call and applied from there. This will allow saving PSTN resources (calling and forwarded-to party may have no CAC restrictions) and also the complexity of the resulting call is greatly reduced. Calls are tied in the OpenScape Voice.

3.8.22.8 Enable Endpoint Rerouting (Automatic Proxy Registration and Enabling Proxy Bypass)

OpenScape Voice always operates under the assumption that Endpoint Rerouting is requested in case a route in the route set returned by translation does not result in a successful call establishment.

OpenScape Voice also operates under the assumption that Proxy Registration is requested.

Proxy Bypass is not a system wide feature. It is now necessary to turn on bypassing a configured proxy by setting the new attribute "Allow Proxy Bypass" on the SIP Proxy endpoint.

A new fallback concept, Fallback to Local Numbering Plan with Modified Number, has been introduced in V10R1, where the transformed number after passing through the common or global numbering plan (modifications done up to the destination table) will be kept for fallback to the private numbering plan.

3.8.23 Rerouting a Call to a SIP Subscriber

One of the benefits of the integrated CAC (Call Admission Control) solution is OpenScape Voice's ability to provide rerouting via the PSTN (Public Switched Telephone Network) 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.

Prerequisites

Rerouting of calls to SIP subscribers via the PSTN can be performed if the following conditions are met:

- The called SIP subscriber is registered from a survivable branch.
- The called SIP subscriber resides in that survivable branch. This means that the called SIP subscriber is registered with its provisioned survivable SIP EP (Endpoint) (its SIP proxy). The administration of the called SIP subscriber to become survivable is enabled by assigning the survivable SIP proxy as the associated SIP endpoint to the SIP subscriber.
- The called subscriber has a valid public E.164 number.
- Furthermore one of the following conditions have to be met:
- – The calling SIP subscriber is calling from a different survivable branch.
  – The calling SIP subscriber is directly registered with OpenScape Voice.
  – The calling device is a SIP EP (SIP gateway) that has the rerouting option set, and there is a last diverting user for the call which is a provisioned OpenScape Voice SIP subscriber.

Assume that a SIP subscriber in the Boca Raton, Florida, branch calls a SIP subscriber in the San Jose, California, branch. This scenario requires the RTP (Real-time Transport Protocol) payload to route through the bandwidth-limited links that connect the Boca and the San Jose branch offices to the WAN.

If there is not enough bandwidth available in either link, the resource reservation is not successful and the RM (Resource Manager) function sends a negative response equivalent to a SIP 606 response code. OpenScape Voice then reroutes the call between these two subscribers through their local SIP gateways and the PSTN.

Related concepts

Rerouting Based on SIP Response Codes and WAN Outages

Rerouting PSTN (Public Switched Telephone Network) Calls to Alternate Gateways on page 238

Enhanced CAC-Restricted Subscriber Rerouting on page 238

Enhanced CAC Restricted Subscriber Rerouting for Endpoints on page 241

Signaling Management on page 667

3.9 Emergency Calling

When an emergency call is made either from within the internal corporate network or (from V8 onwards) made within OSCS Cloud or any Hosted Edition deployment, Open Scape Voice’s built-in E911 (Enhanced 911) support provides the capability to forward the call to the gateway served by the appropriate PSAP (Public Safety Answering Point) jurisdiction. By conveying location identifiers registered in the PSAP's ALI (Automatic Location Identification) database, it enables the PSAP operator to retrieve information about the caller's geographical location and place a response call to either the originator of the emergency call or a designated on-site destination.

OSV's Emergency Calling service is applicable to most Emergency regulatory requirements for enterprise systems. For example, the location identification number and callback numbers are up to 25 digits in length.

The E911 application is embedded in OpenScape Voice's generic software and is referred to as **Emergency Calling** table. Since this application is embedded, there is no separate server and there is no additional cost for implementing the E911 functionality. Performance is directly tied to the resiliency of the system and the remote gateways in the enterprise network.

OpenScape Voice can support the routing and correct user location reporting for E911 calls made by its users when located on the corporate network.

NOTICE:

OSV Emergency Calling service can determine the correct location for subscribers registered in OSCS Cloud or any Hosted Edition deployment using the subscriber DN (this can be accomplished as long as the subscribers are assigned to an emergency department and this emergency department is assigned to an emergency calling entry).

RedSky E911 integration

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

OSV integration with RedSky solution provides location information to Public Safety Access Points (PSAPs) that has much finer granularity than the alternative subnet-based solution can offer.

OSV interworks with the following RedSky services:

RedSky E911 Manager

This is can be a simplex or redundant (i.e. active/standby mode) deployment. OSV supports both options. Signaling will be sent to the active node. When the active node is not responding switching to the redundant node is transparent. RedSky Mgr is not connected or integrated in anyway with OSBs. OSBs continues to use their Emergency Calling service when in survivability mode.

RedSky E911 Anywhere

This 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 the E911 call to the Local PSAP.

SIP connectivity through an SBC to RedSky E911 Anywhere Network Services is supported.

IMPORTANT:

Remote users registered behind an SBC are not supported. If any of such users originates an E911 call, the IP of the SBC is sent to the RedSky E911 Manager for the ELIN discovery.

Location Identification

When an emergency number is dialled by a device/client, the E911 service looks up an ELIN (Enhanced Location Identification Number) associated with the subscriber's location and the correct route to the PSAP. The ELIN has previously been registered with the PSAP with additional information.

The location can be derived from

- the subscriber's DN
- the subscriber's IP subnet or IP address

  typically used for mobile subscribers attached to OSV without intermediate SBC
- the subscriber's *Location Domain*

  The preferred solution for subscribers behind SBCs

NOTICE:

As a prerequisite, **mobile user agents have to be provisioned for DHCP!**

RedSky Location Identification

OSV is enhanced to retrieve during registration of the subscriber endpoints the ELIN (emergency Location Identification Number). OSV stores the ELIN and when an E911 call is made it retrieves the ELIN from the DB in-memory and includes it in the outgoing call routed to the RedSky E911 Anywhere Service GW.

IMPORTANT: In case OSV can not find an ELIN from RedSky E911 Manager, it fallbacks to the current E911 BG Subnet tables in order to find the provisioned LIN and route to the emergency destination.

Source Location-based Translation and Routing

The routing of calls in OpenScape Voice is generally fixed by the subscriber's assigned PNP (Private Numbering Plan). Regardless of the subscriber's physical location - within an office/branch, from a hotel connection or even from home - whenever there is IP connectivity to OpenScape Voice, the subscriber can authenticate against the system and is bound to the same PNP. Unless exceptions are enforced by other processes or external applications, dialled numbers are always translated in the same way and the resulting calls are routed to the same destinations.

An Emergency Calling implementation obviously requires such an exception: otherwise, emergency dialling could easily result in accessing emergency services that are far from the subscriber's current geographical location.

The emergency call routing is implemented as an extension of the standard PNP number translation:

1) depending on the caller’s geographical location, a different "route" suffix is appended to the Emergency code (Destination Type: Service; Service: Emergency) configured in the PNP or GNP
2) the suffixed Emergency code is retranslated.

   The resulting number must route to the appropriate gateway to reach the PSAP.

As mentioned above, the corporate network has to be structured in a way that allows to derive a subscriber’s location from its current IP address or location domain.

This permits the traditional PNP-based routing strategies to be used for standard calls, while invoking a more robust, location-based routing strategy when emergency services are required.

PIDF-LO

Whenever a call to an Emergency destination is made, OSV performs a number of actions in order to retrieve caller location information, route to send the call and callback number and provide them to the destination of the emergency call.

OSV now works as follows:

- If the phone sends PIDF-LO in its INVITE message, OSV adds it in the outgoing INVITE even if NG911 is not enabled/provisioned.
- If the phone does not send PIDF-LO, but PIDF-LO data exists on OSV because of provisioning, OSV adds it in the outgoing INVITE even if NG911 is not enabled/provisioned.
- If no data is available at all, either from phone or OSV, OSV will construct PIDF-LO with the NAM tag only for the outgoing INVITE only when the parameter **Overwrite NAM with LIN** has a value other than *Passthrough*.

The PIDF-LO data is available to OSV by either the calling device itself (location aware devices) or by provisioned emergency subnets' data if the former aren't available.

3.9.1 Emergency Call Processing

When a subscriber dials an emergency number (typically 911 or 112) from within the corporate network or from within OSCS Cloud or any Hosted Edition deployment, OpenScape Voice uses the subscriber’s DN or the current IP address to lookup the associated Emergency Calling data for this subscriber. It retrieves an ELIN (Location Information Number) and the Route number for egress to the gateway of the calling user's PSAP (Public Safety Answering Point) jurisdiction.

Supported Gateways

In order to provide the Emergency Calling feature, OpenScape Voice requires a Unify or Cisco PSTN gateway to provide the break-out to the adequate local central office (ultimately a PSAP jurisdiction) corresponding to a subscriber’s current location within the corporate network.

Other adjunct equipment like the *Telident S.T.S.* (Station Translation System) or the *Tone Commander Call Locator* can provide additional gateway functionality and emergency call management/auditing.

Functional Sequence when RedSky is NOT enabled on the switch

When an emergency call is processed, OSV shall first try to find the emergency calling entry, that the user belongs to, using the subscriber DN (for this to happen the subscriber must be assigned to an emergency department and this emergency department must be assigned to an emergency calling entry). If no entry is found then the existing look-up logic shall be followed:

1) A caller places an emergency call by sending an INVITE to OpenScape Voice

2) OSV first tries to look up and retrieve an appropriate LIN (the LIN is inserted in the INVITE) and **Route** number from the **Emergency Calling** (E911) table with the following logic:

- Initially try to find the emergency calling entry, that the user belongs to, using the subscriber DN (for this to happen the subscriber must be assigned to an emergency department and this emergency department must be assigned to an emergency calling entry).
- If X-Siemens-Location header field is present in the incoming INVITE request then:
  - If an IP address is explicitly indicated (in the format X-Siemens-Location:IP=123.123.123.123), supported only by OSXpert, then try to find the BG emergency subnet using as key the IP address.
  - If a location domain is indicated, then try to find the BG emergency subnet using as key the location domain
- Try to find the BG emergency subnet using as key the contact’s IPv4.
- Try to find the BG emergency Subnet using as key the contact’s IPv6

NOTICE:

If no subnet is found, the call cannot be routed correctly and it is either routed to an on-site answering position or an announcement is played.

3) The Route parameter (via translation) leads the call to a particular gateway that is served by the public network’s E911 tandem office. It can then route the call to the proper PSAP jurisdiction serving the caller.

NOTICE:

If an emergency call cannot be routed to a PSAP operator, the call can be optionally routed to an E911 Default Emergency Number (Directory Number format) as an added precaution.

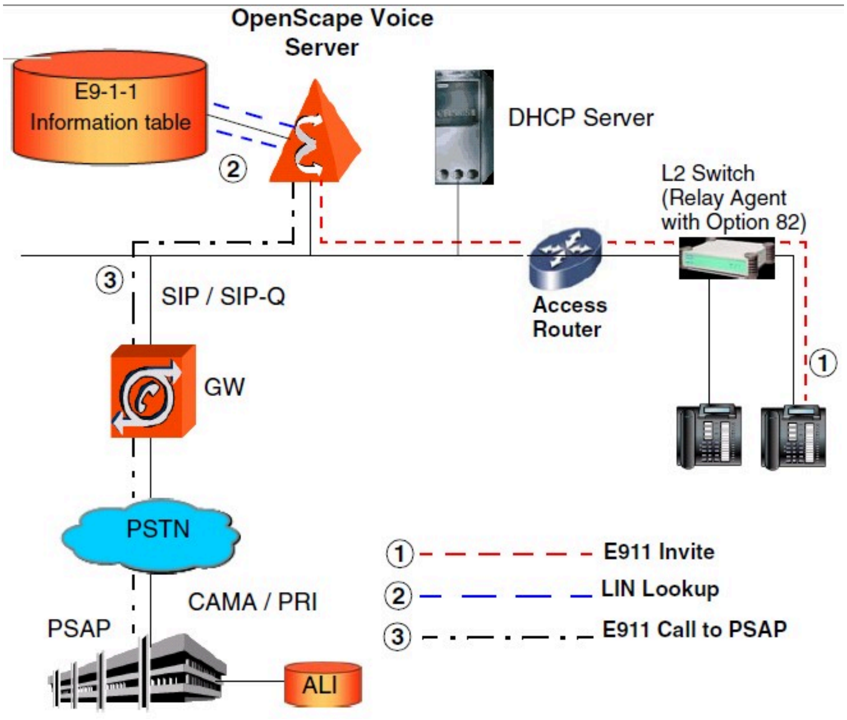


Figure 34: Emergency Call Flow

If an OpenScape Voice system is serving multiple geographic locations, and E911 service is a requirement, links (and routes) to each responsible PSAP will be required.

3.9.2 Emergency Call Processing with RedSky Application

When a subscriber dials an emergency number (typically 911) from within the corporate network, OpenScape Voice retrieves the ELIN (Emergency Location Information Number) from the DB in-memory and includes it in the outgoing call routed to the RedSky E911 Anywhere Service GW that relays the call to the corresponding PSAP.

Endpoint Registration and Publishing to RedSky Manager

RedSky E911 Manager must always be notified of the registrations of SIP subscribers and an ELIN is assigned to each subscriber. This is accomplished with the following actions:

- When a SIP subscriber registers successfully, or is unregistered, the OSV will send periodically a PUBLISH message to the active RedSky E911 Manager. The PUBLISH will contain registrations that have been identified as “new” registrations or un-registrations by OSV. 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.
- The RedSky E911 Manager will use the Contact-URI to discover the exact location of the registering device. After the exact location is determined an ELIN is assigned to it. The RedSky E911 Manager stores the registration

records published by OSV and needs to be made aware of any unregistered events.

- When the RedSky E911 Manager server starts up, it will start listening for PUBLISH messages. Upon receipt of a PUBLISH message, RedSky E911 Manager will execute its normal Network Discovery operations (using either IP Ranges or port-level discovery), and send the resulting ELIN back to OSV using a PUBLISH message. As the PUBLISH message will not contain a MAC address, if port-level discovery is required, it will be the responsibility of the RedSky E911 Manager server to dynamically determine the MAC address based on the IP Address using the ARP tables on the appropriate network switch(es).
- OSV shall send a batch of registered and unregistered contacts in a single PUBLISH message on administered intervals or when the number of the contacts reaches a predefined maximum number.

IMPORTANT:

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

IMPORTANT:

If a contact is registered using an FQDN, then RedSky E911 Manager must be able to resolve the FQDN. If RedSky E911 Manager can not resolve the FQDN, then it will not send an ELIN for this contact and OSV shall fallback to the E911 Subnet Tables in order to retrieve a provisioned LIN.

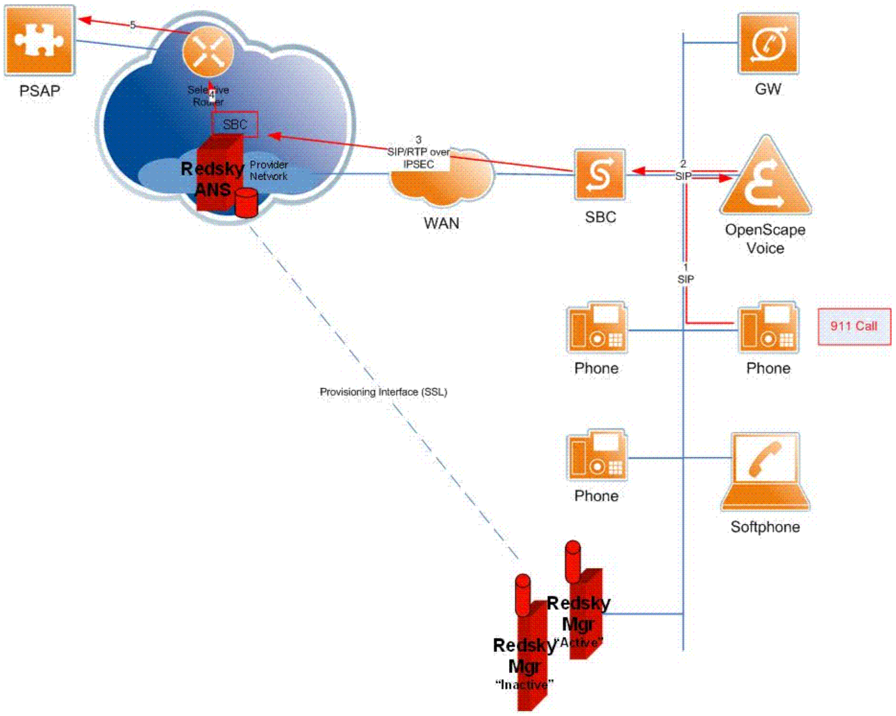


Figure 35: RedSky Emergency node configuration

Publishing from RedSky E911 Manager

RedSky E911 Manager asynchronously sends a PUBLISH message back to OSV for every new association of a registered device with the following:

- Received contact information
- The unique identifier of the contact
- The ELIN assigned to the contact.

NOTICE: The PUBLISH message from RedSky E911 Manager may contain multiple registration records. RedSky E911 Manager supports multiple contacts and will assign an ELIN for each registered contact.

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

If a change has been made directly in the RedSky E911 Manager database and OSV is not yet aware of it (e.g., communication with the RedSky server is not available), when an emergency call is made, OSV shall use the ELIN previously associated with the contact when it registered. Users can make changes directly in the RedSky E911 Manager database and RedSky will notify the PSAP of these changes (e.g., making an ELIN change after a phone has been moved and re-registered).

NOTICE:

When there is no messaging traffic between OSV and active RedSky E911 Manager node, OSV uses a keep-alive mechanism to check this connection. If there is no response from active RedSky E911 Manager, OSV establishes the connection with standby RedSky E911 Manager server.

Outgoing Emergency call

When an emergency call is originated by an OSV subscriber, the emergency call service is directed to the RedSky Anywhere service only if there is an ELIN found in OSV DB.

If no ELIN is available OSV searches for a subnet in the E911 BG Subnet entries and routes the call to the provisioned destination.

If there is no subnet found the call is routed to the default emergency destination.

Related concepts

Direct Return Call from Emergency Center on page 251

3.9.3 Direct Return Call from Emergency Center

OpenScape Voice supports a callback mechanism that allows return calls to be placed from a PSAP (Public Safety Answering Point) directly to the device which placed the emergency call in case the call was interrupted. This works no matter to which callback number the delivered LIN (Location Identification

Number) is mapped in the ALI (Automatic Location Identification) database and even with lines that are not provisioned for DID (Direct Inward Dialling). For Return Call from PSAP a special ring tone and display is generated.

Functional Sequence

This direct callback is achieved in the following way: During emergency call processing OpenScape Voice

1) determines the appropriate entry in the Emergency Calling table and - therein - the first unused LIN from the assigned LIN-pool.
2) saves the callers DN, IP address and port number and associates it with the LIN's configured Callback Number

> **NOTICE:**
>
> A Callback Number has to be configured for every LIN in OpenScape Voice. It must be a registered DID number and it *must* be identical to the Callback Number mapped to the LIN in the ALI database of the responsible PSAP.

The PSAP operator will not know the name of the emergency caller (except during conversation), only the location and Callback Number stored for the received LIN is displayed on the PSAP monitor.

When a call to this **Callback Number** arrives via a gateway, OpenScape Voice

1) identifies this as an emergency callback
2) retrieves the DN, IP address and port number of the original Emergency Call and forwards the callback accordingly

LIN Pooling

Although LINs will be marked as unused after a certain time, the assignment logic might break if the number of emergency callers exceeds the number of LINs in the corresponding pool, so from a subscriber's point of view it is desireable to have an individual LIN and Callback Number. The downside of this is:

1) A Callback Number has to be a registered DID number. In some countries (e.g. USA) each DID number has an associated carrier fee/charge associated with it.
2) The amount of provisioning that has to be done
3) A Business Group's Emergency Calling table is limited to 6000 entries.

If many users reside at the same location (from a PSAP's perspective) and this location can be identified by an IP address mask *M* (or location domain *D*), then associating *M* (or *D*) with a LIN pool in an Emergency Calling table entry, will greatly simplify provisioning, reduce the size of the Emergency Calling table and, ultimately, reduce costs.

Default Callback Numbers

For every LIN the administrator should configure a **Default Callback Destination** to which the callback should be forwarded in case the original emergency caller cannot be reached.

By selecting the **Use Default Callback Destination** option during LIN configuration, the callback to the original subscriber is disabled for this LIN and the return call is immediately routed to the **Default Callback Destination**. E.g. small businesses located in one building, one floor, may prefer to have one LIN to represent all possible callers and emergency callbacks to be directed to the front security desk.

Emergency Calling

Before Version 5 of OpenScape Voice, an Emergency Return Call was signalled as normal external call towards its recipient. Since Version 5, OpenScape Voice signals Emergency Return calls and DAKS calls with a specific “Alert (Alarm ringing)” setting distinctively, which results in an emergency alerting tone at the phone (if supported and provisioned). The Emergency Ringing feature can be specified as a system-wide setting

Feature Interaction

OpenScape Voice features preventing the return call to terminate on the subscriber (e.g. OSV-based Call Forwarding or Do not Disturb) are bypassed.

Features, which are not activated on the system but on the device (e.g. device-based Call Forwarding or Do Not Disturb) will **NOT** be overridden by an emergency callback!

Related concepts

Intrusion on page 158

Emergency Call Processing with RedSky Application on page 249

3.9.4 Emergency Calling Table

To enable the built-in Emergency Call capability, each BG (Business Group) is provisioned with an **Emergency Calling** table that is provisioned using OpenScape Voice Assistant.

The maximum number of entries in the Emergency Calling table is 6000 per BG.

Emergency Calling Subnet Identification

Every **Emergency Calling** table entry can be defined by:

- **Department** or
- **IPV4 Address/Subnet** and/or
- **IPV6 Address/Subnet** and/or
- a valid **Location Domain** or
- a combination of all of the above

NOTICE: The **IPV4 Address/Subnet** and **IPV6 Address/ Subnet** must be entered in CIDR format.

You also have the option to enter a:

- **Description**
- **Branch Office** by clicking on the **...** button and choosing from the given list.

> **NOTICE:** This field updates the selected OSB's emergency data with the specific OSV's subnet entry data.

Different **Emergency Calling** table entries may overlap. OpenScape Voice selects the smallest possible subnet containing the emergency caller's IP address.

IPV6 networks in mixed configurations (IPV4 parts and IPV6 parts) are supported by the OpenScape Voice Assistant. Although the OpenScape Voice Assistant itself is currently deployed on IPV4, it is able to administer IPV6 addresses (128 bits) in the OpenScape Voice switch and DLS (DlsAPI).

An example of a typical IPV6 address is `2001:db8:0:0:0:3:4:AA55`. A sequence of zeros can be abbreviated to a pair of colons, "::", but only once in each address string. So the address above can be equivalently written as `2001:db8::3:4:AA55`. If the address is part of a longer string that allows colons to be used for other purposes, the IPv6 address should be enclosed in square brackets to eliminate ambiguity: `[2001:db8::3:4:AA55]`.

Subnet Configuration

Several additional parameters are provisioned with the subnet, determining the behavior for outgoing emergency calls.

- **Send LIN instead of CPN**:

  With this flag OpenScape Voice can be forced to send the LIN (Location Identification Number) instead of the CPN (Calling Party Number) in emergency INVITEs. Default is false, i.e. the CPN is sent.
- **Digits to append**:

  This number can be up to 4 digits long. By suffixing the dialed emergency number and subsequent retranslation it determines the gateway to which the emergency call shall be routed in order to reach the PSAP (Public Safety Answering Point)
- **Overwrite NAM with LIN**

  Indicates how OSV will handle the NAM field into the PIDF-LO of outgoing Emergency Calls. Possible values are:

  – **Passthrough**: This is the default value. Select this value if you don't want to overwrite NAM with LIN
  – **Write if empty**: Select this value to overwrite NAM with LIN only when the NAM value received from the device is empty.
  – **Overwrite**: Select this value to overwrite NAM with LIN.

LIN Administration

Each **Emergency Calling** table entry can be provisioned with a pool of LINs (Location Identification Numbers). The maximum number of LINs per BG is 100,000.

3.9.5 LIN Administration

The LIN (Location Identification Identifier) conveyed with an emergency call is used by the PSAP (Public Safety Answering Point) to query the ALI (Automatic

Location Identification) database for important related data, such as location and callback number.

The ALI database must be *pre-populated* with the LINs and their associated data by the responsible operator in advance of any emergency call being dialled.

In case of change in the corporate domain (new/modified/deleted LINs and/or data), ALI data have to be updated manually. There is no *automated* capability to populate the E911 ALI database with LIN records.

Provisioning Aspects

In OpenScape Voice, LIN pools are assigned to IP subnets, representing E911 Emergency Resource Locations.

For each LIN the following parameters are to be specified:

- **Location Identification Number**:

  This is a string of digits with maximum length 20. A leading "+" sign is allowed.
- **Callback Number**:

  The Callback Number is used by the PSAP station to call back to the ERL in case the emergency call was interrupted. If the **Use Default Callback Destination** flag is not set, the callback is propagated to the original caller.

  The Callback number must be a vacant DN and unique throughout the switch.
- **Default Callback Destination**:

  If the **Use Default Callback Destination** flag is not set, the **Default Callback Destination** is only used as a fallback in case the original caller doesn't answer the PSAP callback. The same **Default Callback Destination** (e.g. an attendant position) can be used for different LINs and in different subnets.

  The **Default Callback Destination** must be subscriber.
- **Use Default Callback Destination**

  If this flag is set, a PSAP callback to the LIN’s **Callback Number** is immediately forwarded to the **Default Callback Destination**.

The **Location Information** and **Callback Number**s are mandatory and have to be made available to the PSAP’s ALI DB before an emergency call can be successfully established.

OpenScape Voice supports 100000 LINs per BG.

Signaling Aspects

Delivery of the LIN (and other E911 parameters) to the appropriate PSAP is by way of the PSTN (Public Switched Telephone Network) gateway, using SIP or SIP-Q. The elements used for LIN transport in the private network are:

- Clear text in the SIP body in case if SIP interface
- GNF format in the `From` and `AI` headers when the interface used is SIP

  This allows the OpenScape Voice server to identify that the LIN is a public number with a nature of address (NOA) of International.
- CornetNQ element in case if SIPQ interface

The PSTN interface utilized by the PSAP is traditionally an analog CAMA trunk, although some PSAPs now use an ISDN PRI interface. As CAMA and ISDN/PRI curcuits do not have the ability to transmit location information the LIN is sent to the PSTN in the Calling Party Number.

An administrable flag in the **Emergency Calling** setup controls **LIN substitution**, i.e. whether OpenScape Voice sends LIN information as a separate information element *in addition* to the calling party number, or 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, if PRI (Primary Rate Interface) is used instead of CAMA (Centralized Automatic Message Accounting).

3.10 Precedence And Preemption (MLPP)

The Precedence and Preemption Service (P&P SVC) is used to handle precedence calling, including authorizing users to make preemption calls as well as IP EI endpoint call preemption. OSV provides a new Precedence and Preemption service which can be assigned to subscribers. The service is configured per-subscriber, identifying service related data for authorizing P&P calling.

The Emergency Call with Precedence feature utilizes the MLPP preemption capability to "preempt" normal calls when routing emergency calls through a gateway operating at full call capacity or bandwidth constrained link. When such limits are exceeded, the existing network preemption algorithm is utilized, treating normal calls as equivalent to "Precedence Level = ROUTINE". When preemption occurs, the call is released with both SIP interfaces receiving indications informing them that the call has been released due to lack of resources to allow an emergency call proceed.

3.11 Precedence Call Diversion

The Precedence Call Diversion feature is a new service that can be set on a Subscriber as well as on a Feature Profile level. The goal is to have the Precedence Call Diversion feature assigned to the Feature Profile and each Subscriber using a specific Feature Profile will get the same treatment. If a subscriber wants a different treatment, then a new Feature Profile can be created and the subscriber can be under that Feature Profile. The Precedence Call Diversion service has a lower priority than the Precedence And Preemption service

4 Mobility and Collaboration

Mobility is the idea that business users can access their communications from anywhere at any time. Because users don't have to be sitting at a specific desk in a specific office, they can stay in touch wherever their work takes them.

Collaboration is the ability of two or more coworkers to complete their tasks collaboratively, even if it's as simple as answering a call for a colleague who's away from her desk. The idea of providing mobility and collaboration to business users is not new; after all, road warriors have been working from cell phones and email for quite some time now, and administrative assistants have been answering the telephone for their bosses for decades.

What makes OpenScape Voice different is its foundation in the concept of Open Communications.

"Open Communications is Unify' human-centric and business-oriented approach of unifying communications based on open standards. It binds the IT, voice and mobile domains together to speed up decisions by making global collaboration easy. Open Communications provides intuitive, mobile and synchronized communications - overcoming the fragmentation of today's communications landscape."

4.1 Keyset Telephone

This chapter describes features specific to keyset operations. These features provide support for rich collaboration solutions, helping subscribers to better streamline their calling processes

Any of the following SIP endpoints can be configured as keysets:

- OpenScape Desk Phone CP 100/200/205/400/600/600E/700/700X

For Clients, ODC-PE can be configured as keyset

The keyset operations features provide multiple line capability, and other associated functions, for a SIP telephone configured as a keyset. Keysets are sometimes known as multiline telephones.

Important Terms and Definitions

Primary Line (or Prime Line)	The keyset line that identifies a keyset telephone. Every keyset phone has a single primary line.
Phantom Line	A line that is not assigned as a primary line on any keyset
Private Line	A line (primary or phantom) that appears on only one keyset
Shared Line	A line (primary or phantom) that may appear on multiple keysets

Secondary Line	A line on a keyset that is a shared appearance of a primary line of another keyset, but not of this keyset

Restrictions

The restrictions of using a phone that doesn't support the keyset subscription package as a keyset line appearance are listed below:

- Line state is not shown
- Cannot retrieve manual held call - hold call in another phone, retrieve on this phone
- Cannot put a call in manual hold - hold on this phone, retrieve in another phone
- No call forwarding notification – if the system call forwarding is activated for that line on another phone, this phone won’t be notified about it and therefore the user won’t know call forwarding is active.
- Line reservation doesn’t work – the user will be allowed to dial when the line is already in use, then will get a 503 back from OSV
- Longer time to recover stuck lines – the typical scenario is that of phones behind a proxy: when proxies go into survivable mode and back into normal mode, OSV gets a NOTIFY/no-dialog message from the keyset phones. This is used to immediately free up lines that were in use before the proxy went into survivable mode. Without that mechanism we need to rely on session timers, which may take up to 15 minutest to free up a call.
- OSV will log a “keyset line subscription mismatch” when the line is used

4.1.1 Multiline Appearance

The Multiline Appearance (MLA) feature allows for multiple lines (i.e. subscribers) to be assigned to a keyset and for a line to be assigned to multiple keysets. This is particularly useful for executive-assistant arrangements.

Each keyset is assigned a primary line, and can be assigned up to 10 lines, depending on the endpoint type. The primary line is the DN for that keyset.

NOTICE:

A keyset cannot have a line appearance of a DFT (Digital Feature Telephone)

Call Handling

Calls are directed as follows:

- Calls to the primary line of a keyset are simultaneously directed to all other keysets that have that line configured as a primary or secondary line.

NOTICE:

A keyset line can be registered as the primary line from more than one keyset device at the same time.

- Calls to a phantom line are simultaneously directed to all keysets that have that line configured as a shared phantom line.

On the keysets, the primary line and each secondary or phantom lines are assigned to separate line keys. A user can press the line key associated with a line at any keyset to originate, answer, hold, retrieve or reject calls. The LED for each line key indicates the status of the associated DN and the action of the telephone when a line key is pressed.

What actually happens when a call is rejected on a shared line depends on the RTP (Resilient Telco Platform) Parameter Srx/Sip/KeysetCallRejectionMode.

- If set to 0 (default), the device stops alerting, but the call is not released and hence can be retrieved at other appearances of the line.

  Note that the line remains busy until the caller goes onhook. It can not be freed from the rejecting phone.
- If set to 1, the result depends on the line type:
  - rejecting a call on the keyset’s primary line will release the call
  - rejecting a call on the keyset’s secondary line will stop the alert but NOT release the call (with the consequences stated above)

Ring Preferences

For OpenScape Desk CP keyset telephones, the administrator can assign one of the following ring preferences to each line appearance:

- Ring: The line always audibly alerts when an incoming call is presented and calling party information appears on the display.
- No ring: The associated line key LED indicates an incoming call, but no audible alerting occurs and no calling party information appears on the display.
- Delay ring: The line audibly alerts after a configured delay and calling party information appears on the display

For OpenScape Desk CP keyset telephones, this feature requires configuration in OpenScape Voice and in the endpoint.

Networking

All line appearances must reside on the same switch and within the same IP addressing domain.

Related concepts

Multiple Contacts on page 156

Executive/Assistant Groups

RTP Management via OpenScape Voice Assistant on page 961

Multiple Prime Line Registrations on page 259

4.1.1.1 Multiple Prime Line Registrations

Since Version 5R1 of OpenScape Voice a subscriber can register as the primary line from more than one keyset device at the same time - without requiring additional dynamic licenses.

Before Version 5R1, when a primary keyset line *L* was already registered from a device D_1, the attempt to register from another device D_2 resulted in *L* being unregistered from D_1. Additionally, all secondary lines registered for D_1 were also automatically unregistered. Starting with Version 5, *L* can now register from both D_1 and D_2 (similar to a multiple contact scenario).

The phones using the same primary line are not required to have the same secondary line configurations. For example, a phone may have three secondary line appearances, while another phone may have only one of them.

The number of bindings (registrations) for a primary line is subject to the same pre-set limits as for regular keyset lines. The maximum number of bindings for a keyset line is configured to a default of 40, i.e. by default the number of prime lines plus secondary lines can't exceed 40. Once that many bindings are in the system for that particular line, attempts to register another contact address will be rejected. Please do not change the default configuration without consulting your service partner.

Usage Scenario

An executive can now

1) answer a call using her desk phone
2) put the call on hold on the desk phone
3) walk to the conference room, where another phone with the same primary line is configured
4) retrieve the call on the conference room phone and continue talking

Before Version 5R1 this could have only been solved by configuring the executive's phone number as a secondary line appearance of the conference room phone. However, this requires a different primary line for the conference room phone and hence an additional dynamic license.

Related concepts

Multiline Appearance on page 258

4.1.2 Multiline Preferences

The multiline preference feature allows a keyset to automatically select which line it uses when the user originates or answers a call. In addition, it lets a user override the automatic selection of a line and manually select the line to use.

This feature is controlled via the endpoint.

The multiline preferences for terminating calls are as follows:

- Ringing line preference: The line in the alerting or audible ringing state is automatically selected when the user goes offhook. In the case of multiple lines alerting or ringing the lines are selected on the one that has been alerting the longest. When a terminating call exists, the terminating line preference takes priority over originating line preference.
- Ringing line preference with preference for prime line: The line in the alerting or audible ringing state is automatically selected when the user goes offhook. However, if the prime line is alerting, it is given priority.
- Incoming line preference: The earliest line to start audible ringing is selected, or else the earliest alerting (ringing suppression ignored) line is selected.

- Incoming line preference with preference for prime line: The earliest line to start audible ringing is selected, or else the earliest alerting (ringing suppression ignored) line is selected. However, if the prime line is alerting, it is given priority.
- No preference: The user manually selects a line by pressing its line key before going offhook, or by pressing the speaker key, to answer a call. Manual line selection overrides automatic line preferences.

The multiline preferences for originating calls are as follows:

- Idle line preference: This is the default. The line preference order, or rank, is used to select the line. The highest ranked idle line is selected.
- Prime line preference: The prime line is selected.
- Last line preference: The last line used (originating or terminating) is selected.
- No preference: The user manually selects a line by pressing its line key before going offhook, or by pressing the speaker key, to originate a call. Manual line selection overrides automatic line preferences.

Automatic line selection occurs whenever an outgoing call commences and a line has not been pre-selected. Automatic line selection also occurs when a line needs to be reserved for dialling and a line has not been pre-selected - for example, when entering a digit via the keypad while on-hook and idle. Ringing line preference is the default.

4.1.3 Multiline Origination and Transfer

The multiline origination and transfer feature provides the capability to originate or answer calls at any line appearance at any keyset and to transfer calls via consultation transfer or manual hold.

This feature is controlled via the endpoint.

A keyset user can originate and answer calls manually and automatically. To originate calls:

- A user can manually select a line by pressing a line key before going off-hook, pressing the speaker key, or using onhook dialing to originate a call.
- A line may be automatically selected if the idle line preference is active at the time the user goes off-hook, presses the speaker key, or uses onhook dialing to originate a call.

To answer calls:

- A user can manually select a line by pressing a line key before going off-hook, or by pressing the speaker key, to answer a call.
- A line may be automatically selected if the ringing line preference is active at the time the user goes off-hook, or presses the speaker key, to answer a call.

A keyset user can use the transfer capabilities associated with this feature as follows:

- Call transfer via consultation transfer: Transfer can be accomplished by placing the call on consultation hold and consulting with a second party using the display. The user can then transfer the held party by going onhook after he consulted party answers.
- Call transfer via manual hold: Transfer can be accomplished by placing the call on manual hold and selecting a different line and consulting with

a second keyset (having the same line appearance of the held line). The second party can then retrieve the call from manual hold if no restrictions exist.

4.1.4 Delayed Ringing

The delayed ringing feature provides the capability to provision each keyset line key with an option to delay audible ringing when a call is presented to the line. The associated incoming call is not affected.

This feature is particularly useful for executive-assistant arrangements because it allows the assistant to answer calls for the executive’s secondary line appearance before the executive hears the line ringing.

An immediate ring key provides the capability to temporarily override delayed ringing for all lines on the endpoint configured for ringing.

The administrator assigns delayed ringing to a line appearance and defines the duration of the delay before audible alerting. Furthermore, he assigns the Immediate Ring feature key to the device.

Functional Operation

When a call is presented to a line provisioned for delayed ringing, the associated line key LED flashes to indicate that the call is present. Upon timeout of the delay ring timer, the device begins to audibly alert (ring), and the associated incoming call display is presented.

To override delayed ringing, the user can also activate and deactivate immediate ringing by pressing the Immediate Ring key. The key’s associated LED lights to indicate when it is active, and Immediate Ring Activated or Immediate Ring Deactivated appears in the display as applicable

Related concepts

Executive/Assistant Groups

4.1.5 Audible Ringing on Rollover Lines

The Audible Ringing on Rollover Lines feature permits lines to audibly signal new incoming calls while the subscriber is active on the keyset. This feature is also known as rollover ringing.

For OpenScape Desk CP keyset telephones, the system administrator specifies the following:

- Whether the ringer option is enabled. Rollover ringing only applies to lines that have this option enabled - that is, rollover ringing only takes place if the applicable line otherwise rings when it is idle.
- One of the following rollover ring options for each keyset:
  - No ring when active on the telephone
  - Alert ring when active on the telephone
  - Alert beep when active on the telephone
  - Standard ring when active on the telephone

The selected option applies to all line appearances on the keyset. The user controls the volume of the rollover ring. The rollover ring option is used by the telephone when any line appearance other than the one in use is in the ringing state. When the telephone is idle, normal ringing is applied.

If the user at an idle telephone answers one incoming call on a line appearance while other lines are still ringing, the ringing changes from normal ringing to rollover ringing. Likewise, if the user releases a call and returns the phone to idle while rollover ringing is active, it changes to normal ringing.

Rollover ring is not applied for lines that are set for alerting only. These lines do not ring even if the phone is idle.

4.1.6 Direct Station Selection

The Direct Station Selection (DSS) feature provides a user access to multiple functions for a given internal DN by using a single key (DSS key) with associated status indication. On OpenScape Desk Phone CP endpoints, DSS keys that can initiate direct calls and have feature override capabilities are known as DSS-direct (DSS-D) keys.

Both types of DSS keys function within the user's business group, and not between business groups.

For OpenScape Desk CP keyset telephones, the administrator programs DSS/ DSS-D destinations. Users cannot program them locally at their telephones because the administrator must create a line key to allow this type of operation.

Depending on the endpoint type and its configuration per line key:

- A DSS key initiates a basic call, which is treated as a normal A-B call.
- A DSS-D key initiates a direct call, which overrides redirection at the call destination.

Both types of keys can be used to:

- Show status of the destination associated with the key (idle, busy, or ringing)
- Pick up a ringing call
- Initiate a call by pressing the applicable key
- Initiate a consultation call
- Transfer calls

The telephone does not audibly alert; instead, the DSS LED provides the following displays:

- Off: The associated line is idle.
- On: The associated line has a call in progress or on hold.
- Flashing: The associated line is ringing.

NOTICE:

The DSS LED reflects the status of the line (DN) programmed for the DSS/ DSS-D key, not the status of the user associated with the prime DN device.

A blinking DSS/DSS-D key at subscriber A’s phone indicates an incoming call for another subscriber (subscriber B) with the same key appearance.

When subscriber A presses the key, the call is forwarded to the prime line of subscriber B, and subscriber B is connected to the call. The keyset rejects the forwarding attempt if subscriber B's prime line is busy.

NOTICE:

When picking up a call through DSS, it is possible to indicate to the initially calling party that the call was answered elsewhere. This is enabled/disabled through the RTP parameter `Srx/SIP/DSSPickupIndication`.

Number of DSS keys supported

The number of DSS keys on OpenScape Desk Phone CP depends on the number of programmable keys.

NOTICE:

Please see the OpenScape Desk Phone CP manual of all the models for extra details.

- For normal DSS operation, the number of DSS keys matches up to the number of programmable keys, including also the key modules (where are applicable).
- For DSS operation which is combined with other features (e.g. MLHG), the maximum number of DSS keys that is supported, is 29.

4.1.7 Keyset Operation Modes

The keyset operation modes feature permits an administrator to specify whether a keyset telephone uses the data of the primary line or the data of the line in use for call origination and features.

This option is particularly useful for executive and assistant arrangements. For example, if an assistant places calls on behalf of an executive, the assistant's telephone can have a line appearance of the executive. If marked for line-based operation, the assistant can easily place calls on behalf of an executive, and the executive can subsequently retrieve them when the assistant successfully reaches the person the executive seeks.

For OpenScape Desk CP keyset telephones, keyset operation modes are usually evaluated during the provisioning of the OpenScape Voice environment and are applicable to all line types, including phantom lines.

NOTICE:

For OpenScape Desk CP keyset telephones, this feature is controlled via OpenScape Voice.

For each line of each keyset, the administrator configures the keyset operation mode as follows:

- Device-based operation: This mode is the default. It uses the data of the primary line for call origination and features.

- Line-based operation: This mode uses the data of the line currently in use for call origination and features.

For call termination, the calling party is sent displayable identification information based on the line or device involved in terminating the call. When a specific device answers the call, the identification might differ from the identification provided when the call was alerting all the devices sharing the applicable line.

Device-based Operation

When the keyset user originates a call, the configured data of the primary line (its configured name and DN) is referenced in caller and called ID services. When the user originates a call, the following takes place:

- If the call is originated on the primary line, services provisioned on the primary DN are initiated if they do not require a feature access code to operate. Some examples are transfer, CSTA (Computer Supported Telecommunications Application) support, and calling name.
- If the call is originated on a secondary line, services provisioned on the primary DN are initiated if they do not require a feature access code to operate. Additionally, a subset of services provisioned on the secondary DN are initiated. These services are line-based and do require a feature access code to operate - for example, CSTA support.

The following OpenScape Voice features always use the primary line's configured data regardless of the keyset operation mode:

- Called party name and number upon alerting
- OpenScape Voice-based station speed calling

The following OpenScape Voice features use the primary line's configured data if the telephone is configured for device-based operation:

- Calling party name and number upon alerting or answer
- Called/connected party name and number upon answer
- Call transfer if provisioned on the primary line that originates the operation

Line-based Operation

When the keyset user originates a call, the configured data of the selected line (the primary or secondary DN’s name and number) is referenced in caller and called ID services. When the user originates a call with a secondary line, all services configured to be provisioned on the DN of the secondary line are initiated if they do not require a feature access code to operate.

In addition to ringing and incoming call termination, the following OpenScape Voice features always operate with the selected line regardless of the keyset operation mode:

- Immediate recall from consultation hold
- Manual hold, including recall
- Unconditional call forwarding
- Malicious call trace
- Toll and call restrictions
- Hunt group
- CSTA

The following OpenScape Voice features operate with the selected line only if the telephone is configured for line-based operation:

- Calling party name and number upon alerting or answer
- Called/connected party name and number upon answer
- Call transfer, if provisioned on the line that originates the operation

Call Data Records

When a keyset user initiates a call from a line configured for line-based operation, OpenScape Voice records the line used and the device from where the call was initiated.

Related concepts

Executive/Assistant Groups

Call Forwarding - Unconditional (Station-controllable) on page 287

Hunt Groups

4.1.8 Line Focus

The line focus feature ensures that the OpenScape Desk Phone CP display contains the appropriate information, depending on the keyset line currently in use.

This feature is controlled via the endpoint.

A keyset line has the focus when the display contains information pertaining to it. When a call is connected, that line has the focus. When the call clears, focus is applied to the next suitable line. When a line is alerting, focus is determined by terminating line preferences.

Call handling actions (such as placing calls on manual hold) also impact focus. If there is no suitable line, no line has the focus, and the display returns to idle mode.

The menu and function key actions apply to the line with the focus. However, in the case of a pop-up display, any functions that impact the audio path (such as hookswitch or loudspeaker actions) still apply to the currently active line. When a line key has the focus, its associated LED flutters.

4.1.9 Line Key Operation Modes

The Line Key Operation Modes feature provides the capability to automatically place an active line on manual hold.

The OpenScape Desk CP keyset telephones also support a configurable option to either place the call on manual hold or to release it when the user is active on one line and selects the same line or a different line.

This feature is controlled via the endpoint.

A keyset user can automatically hold the call of the active line as follows:

- Active line key: When the user presses the line key for the active line, the call is automatically placed on manual hold. The telephone can become idle or can start ringing if another line was alerting at the time the line was placed on hold.

Similarly, if the user selects an alerting line while active on another line, the active line’s call is placed on manual hold.

- Inactive line key: When the user presses the line key of an inactive line, the active line call is automatically placed on manual hold and the user is connected to the previously inactive line.

For an OpenScape Desk CP keyset telephone, the telephone can instead be configured to release the call when another line is selected. The default setting is to place the call on manual hold.

Call Data Records

Based on system configuration upon retrieval of a call, the billing for the remainder of the call is assigned to the primary line of the station answering the recall.

Related concepts

Manual Hold on page 267

4.1.10 Line Reservation

The Line Reservation feature is available for OpenScape Desk CP keyset telephones. It permits a keyset user to reserve a line when dialing a destination or selecting a line.

With Line Reservation

- incoming calls cannot interfere with outgoing call initiation
- two keysets with the same line appearance cannot use the same line and attempt to dial simultaneously.

The keyset telephone automatically reserves a line whenever the user is being prompted for a destination address and hears dial tone. The line key LED indicates this reserved state.

One line can be reserved at a time on a given keyset.The keyset cancels the reservation after a preconfigured period determined by the reservation timer. The server also runs a timer so it can force the line to be released if reserved for an excessively long period.

4.1.11 Manual Hold

The Manual Hold Feature allows a keyset user to place the call on the active line in a waiting position. The keyset user can then go onhook without losing the call and can place or answer another call on a different line key.

The held call can be retrieved by other keysets sharing the line appearance, assuming they support the required Manual Hold signaling. A hold ringback timer ensures that the caller is not left on hold indefinitely.

Unify SIP endpoints support the SIP signaling event package that supports this feature. Other SIP telephones that do not support this package cannot signal a call on Manual Hold. As a result, the call is treated as a consultation hold, which requires that the same station user retrieves the call from consultation hold.

A DFT (Digital Feature Telephone), which is a telephone with no line keys, does not have access to the Manual Hold feature. Holding of a connection is via the call hold feature. Refer to the applicable user manual.

IMPORTANT:

Depending on the configuration of the device, pressing the line key can release a call instead of placing it on Manual Hold. See Line Key Operation Modes.

A keyset user can press the line key, press the Hold key, or use the display of the active line to place that call on Manual Hold. After doing so:

- The line key LED shows the hold status on all keysets with that line appearance.
- The user can hang up and originate or answer a call on another line on that keyset.
- Any user with that line appearance can press the line key and retrieve the held call.
- A hold ringback timer is started. If the timer expires, the held call is presented as an alerting call to all keysets sharing that line. Each line has its own configurable timer.

Manual Hold is available for simple two-party calls, but not for consultations or three-way calls.

When a call is retrieved from hold, the parties receive the following displays:

- The retrieving party’s display contains the name and number of the retrieved party if it is available for presentation.
- The retrieved party’s display contains the name and number of the retrieving party if it is available for presentation.

These displays are present if the two parties are on different OpenScape Voice systems, or if one is on OpenScape Voice and one is on the OpenScape 4000. The connection must be SIP-Q, and the two parties must be members of the same business group.

Related concepts

Line Key Operation Modes on page 266

Bridged Calls and Privacy

4.1.12 Phantom Lines

A Phantom Line is identical to a normal line in all respects, except that a Phantom Line is not assigned to any device as a primary line. This line type can appear as a private line on one keyset or as a shared secondary line on two or more keysets.

Phantom Lines are particularly useful as rollover lines. For example, sales representatives can have the administrator configure the primary line to roll over to a Phantom Line. This configuration is beneficial because when the representative speaks to the second party, there is great flexibility in holding, transferring, or redirecting the call.

In addition, Phantom Lines are also useful for query/intercom lines, which automatically set up a call between two users - for example, an executive and an assistant - when either user presses the Query (Intercom) key. This configuration is beneficial because both users' primary lines remain free while they are speaking to one another.This feature requires configuration in OpenScape Voice and in the endpoint.

The function of a Phantom Line is identical to a normal line in all respects. Its DN can be called, and the line can be answered, held, used to originate calls, and in all other operations used in the same manner as other line types.

4.1.13 Visual Indicators for Line and Feature Key Status

The Visual Indicator features allow the keyset user to view the various states (for example, ringing, hold, consult) of a line via its associated LED and to view the various states of a feature key (for example, call pickup group) via its associated LED.

This feature is controlled via the CoS endpoint.

Each line key (primary, secondary, phantom) on a keyset has a corresponding Visual Indicator (LED) to indicate the status of that line.

Table 25: Line Status LED Indicators for OpenScape Desk Phone CP phones

Line Status	Line Type	LED State	Flash Rate	Comments
idle	primary or secondary	off	n/a	-
offhook / dial / busy	primary	flutter - or - on	50ms on 50ms off	This LED state is applicable to the line with the focus.
	secondary	on	n/a	This indication is given on other appearances of the active line.
ringing / alerting	primary or secondary	flash	500ms on 500ms off	
manual hold	primary or secondary	wink	450ms on 50ms off	

Line Status	Line Type	LED State	Flash Rate	Comments
consultation hold	primary	flutter - or - on	50ms on 50ms off	• This LED state is applicable to the line with the focus. • The LED changes only at the holding telephone; there is no change for shared views of the same line.
unconditional call forwarding	secondary	on	n/a	This indication is given on other appearances of the active line.
	primary or secondary	blink	50ms on 450ms off	If this feature is active, this indication is given as long as feature status notification is also active.

If the telephone is not an OpenScape Desk CP, the user cannot see the status of shared lines other than new alerting calls.

4.1.14 Bridged Calls and Privacy

The Bridged Call feature permits keyset users with a shared multi-line appearance to establish or join a station-controlled large conference by pressing the line key of the line they wish to bridge onto. Lines can be protected against bridging by setting the privacy flag (default).

It is possible to bridge onto a line involved in a 2-party call or station controlled conference, provided that the existing call or conference is stable connected and the maximum size of a station controlled conference hasn’t been reached. A user attempting to bridge onto a line that is not in a suitable state for bridging will receive a rejection indication.

Usage Scenarios

This feature is particularly interesting for executive/assistant arrangements based on multi-line appearance, where assistants answer and originate calls on behalf of their executives, using the executives’ secondary line appearances. In this scenario, the Bridged Call feature permits the following workflows:

- An executive bridges onto a call on their line while the secretary is still on the line after answering or making a call
- An executive is on a line with another party and wants to get one or more people on the call. The assistant can then
  1) bridge onto the executive’s call by pressing the executive's line appearance key on their phone
  2) use the normal Station Controlled Conference features to add the required parties to the conference.
  3) leave the conference
- An executive is on a call and wants other people to join the call by pressing a line button on another phone in his office.

Another usage scenario is an emergency number in the enterprise. When someone calls this number it might be necessary that several people in the

Security and Medical Departments should be involved. The first person that answer the call stops the alerting at the other keysets. The other parties at their desks know that the line has rung and may subsequently enter the call by hitting the active line key. With call bridging a conference is formed all required parties are part of this conference.

Finally, in Newspaper, Radio and TV newsrooms there is typically a hotline for the public to call to report newsworthy events. When a call comes in to this hotline, multiple people may want to bridge onto that call to participate in the conversation.

Feature Interaction

All participants of the resulting conference retain all normal features such as Pickup, Consultation and Add To Conference (if subscribed), with the exception of Manual Hold: if a participant in the bridged call places the conference on hold then this is treated as Consultation Hold, i.e. other keysets with a shared appearance of the line on hold will not be able to retrieve the call from hold and only the user placing the call on hold can retrieve the call from hold.

CSTA (Computer Supported Telecommunications Applications) Service is notified if a line joins or creates a Large Conference as a result of Bridging.

A Large Conference provisioning option is provided at the Business Group Services level to inhibit playing of the conference entry tone when new parties bridge onto an existing call/conference.

Privacy

A keyset line attribute **Privacy** is available in the BG (Business Group) keyset line provisioning options. It is not possible to bridge onto a line whose Privacy option is enabled. This is the default.

Administrator can set the “Keyset Privacy” attribute; it can also be changed by the users from their own phones. A feature key and a status lamp can be programmed in an OpenScape Desk CP keyset phone. The feature key is used to toggle the call privacy status for the prime line on that phone. The lamp indicates current status of call privacy. Keyset toggle event is used to signal the toggle event and status update between OSV and the OpenScape Desk CP phone.

The user is allowed to toggle the call privacy status when prime line is idle, or in an active call. If the user toggles call privacy from “off” to “on” while there is an ongoing call on the prime line, it sets the line to be private immediately. Meanwhile all other Keysets with a shared appearance of the same line which have bridged into the call are disconnected.

The **Privacy** option doesn’t affect the operation of Manual Hold i.e. a keyset line with Privacy enabled that has been placed on Manual Hold may still be retrieved from hold by another keyset.

Accounting

A per call feature extension value is provided in the CDR to indicate a bridged call.

Requirements

The Bridged Call feature

- is supported on OpenScape Desk Phone CP family of SIP endpoints.

- is available (only) to BG keyset users who are also subscribed to the Station Controlled Conference feature
- is available with any approved Media Server that supports the Station Controlled Large Conference feature.

4.1.15 3rd Call Leg

The 3rd Call Leg Feature allows to handle three simultaneous calls at a keyset telephone.

For instance, it is possible for a subscriber to

1) have a primary call
2) pick up a secondary call and
3) perform a consultation call

in parallel.

4.2 User Mobility

Mobility is the idea that business users can access their communications from anywhere at any time. Because users don’t have to be sitting at a specific desk in a specific office, they can stay in touch wherever their work takes them.

Hot Desking and DLS Mobility

Hot Desking and DLS Mobility are two of the OpenScape Voice features that provide support for mobility solutions. They allow enterprises with mobile workers to reduce overall office space, while still providing employees with comfortable workspaces when they are in the office. With either feature, incoming calls are automatically routed to the remote telephone, and outgoing calls placed from the remote telephone show the user’s normal calling party information, not the information for the remote telephone.

Multiple Ringing

The Serial Ringing and Simultaneous Ringing features provide subscribers the capability to be rung at several locations, either sequentially or simultaneously. This is especially useful for those whose job duties require them to be in or around many different work areas throughout the day.

Remote Feature Activation Capabilities

The Remote Activation of Unconditional Call Forwarding (RACF) and Simultaneous Ringing are optional capabilities of the Unconditional Call Forwarding and Simultaneous Ringing core features, respectively. They provide the subscriber the capability to activate, deactivate, and change the properties of the respective core feature from locations other than the subscriber’s station, using a previously assigned PIN.

Related concepts

Call Forwarding - Remote Activation on page 288

4.2.1 Hot Desking

The Hot Desking feature, sometimes also known as Hoteling, provides subscribers with the capability to log on to and use a telephone in another office, or at another position in the same office. With certain limitations, the telephone in the other office or position has the same OpenScape Voice-provided features and capabilities as the telephone in the subscriber's usual office or position.

NOTICE:

It is highly recommended that the user’s physical “home” phone, if one is used, and the “remote” phone be the same type and configuration for a better user experience.

Hot desking should not be used in parallel with One Number Service!

Hot Desking is part of the OpenScape Voice base license, so no additional licenses are required for its use.

The administrator

- enables this feature at the business group level
- enables this feature at the feature profile or subscriber level, specifying the role of the related line either as Home Base or Remote
- configures the feature access codes for activation and deactivation
- can assign a function key to the hot desking feature, known as the State key. If a State key is present and the user presses it, the display prompts the user to enter the DN of the home office telephone and her subscriber PIN.

To activate the hot desking feature at the remote office telephone, the subscriber goes offhook, enters the activation feature access code, the DN of the home office telephone and her subscriber PIN.

To deactivate the hot desking feature:

- at the remote office telephone where the subscriber is currently logged on, she goes offhook and enters the deactivation access code.
- from any other remote office telephone, the subscriber goes offhook, enters the deactivation access code, the DN of the home office telephone, and her subscriber PIN.

Limitations of Hot Desking

The following are the limitations of hot desking:

- Telephone-based features are not transferred from the home office telephone to the remote office telephone.
- The remote office telephone does not provide status information for OpenScape Voice-based call forwarding or OpenScape Voice-based DND.
- The user cannot control OpenScape Voice-based call forwarding features at the remote office telephone.
- Although the home office telephone can be a keyset, the remote office telephone cannot.
- The user does not have access to hunt group functionality.

Hot Desking with Message Waiting Indication (MWI)

For Hot Desking functionality to work properly with MWI it is necessary to consider the following:

- In order to receive an MWI for a Hot Desking Remote DN, the OSV should be configured to route the MWI to the RemoteDN (in addition to the HomeDn).
- The Message Waiting Indication feature requires that a corresponding Destination Code with same NOA, as defined by the Srx/Main/MwiNatureOfAddress parameter, be provisioned to allow the MWI request to be routed successfully to the subcriber.
- In addition to the MWI feature requirement to provision a DN code for the MWI DN using the same Nature of Address value as RTP parm: Srx/Main/MwiNatureOfAddress, it is also required to use Class of Service = -1 (default) and ratearea = -1 (default).

Related concepts

Feature Profiles on page 135

OpenScape Voice-based Call Forwarding Features on page 286

Hunt Groups

Solution Comparison: Hot Desking versus DLS Mobility on page 275

One Number Service on page 280

4.2.2 DLS Mobility

The DLS (Deployment Service) mobility feature is an advanced feature that is controlled and configured via a separate DLS server. Using the DLS server permits the creation of mobility-enabled devices, which are able to provide the user interface configured for the mobile user when the subscriber logs on to it.

For example, the mobility-enabled device provides:

- All personal data, such as call numbers, passwords, and privileges
- The subscriber’s customized key configuration and layout
- Advanced user data such as caller lists and display module data
- Accurate status indications for all OpenScape Voice-based features, including call forwarding and DND (Do Not Disturb)
- Access to hunt group functionality

DLS mobility is one of the OpenScape Voice features that provides support for mobility solutions. It allows enterprises with many mobile workers to reduce overall office space, while still providing employees with comfortable workspaces when they are in the office.This feature is applicable to OpenScape Desk CP phones.

Guidelines for Implementation and Use

- A dedicated Mobile User DN is required for any mobility-enabled user. This DN is registered at OpenScape Voice as long as the mobile user is logged on at any mobility-enabled device.
- A mobile user can optionally be assigned a non-mobile telephone (home device). If a home device is assigned, the mobility-enabled device takes on its characteristics when the subscriber registers to it.

- If a home device is present, it must be located on the same DLS server as the mobility-enabled device.
- DLS mobility supports interworking between OpenScape Desk CP phones. This permits a user with an OpenScape Desk Phone CP home device to use an OpenScape Desk CP telephone as the mobility-enabled device, and vice versa.
- It is recommended that non-managed user data - for example, screen savers, logos, ring tones - be minimized for mobile users. The size of the non-managed user data has significant effects on DLS performance and the number of supported mobile users.

Licensing

DLS Mobile User licenses must be ordered for all mobile user DNs before they can be configured in the DLS server. According to the OpenScape Voice dynamic licensing model, which builds on concurrently registered DNs, the mobile user DNs do not require additional OpenScape Voice dynamic user licenses.

System Specific Information

Depending on the type of DLS server present, up to 100,000 mobile users and 100,000 mobility-enabled devices are supported.

Related concepts

OpenScape Voice-based Call Forwarding Features on page 286

Hunt Groups

Solution Comparison: Hot Desking versus DLS Mobility on page 275

4.2.3 Solution Comparison: Hot Desking versus DLS Mobility

Hot Desking and DLS (Deployment Service) Mobility are two of the OpenScape Voice features that provide support for mobility solutions.However, Hot Desking and DLS Mobility differ both in how they are implemented as well as in the scope of functions they provide to end users.

It is important to note that hot desking and DLS mobility are not mutually exclusive features. In many enterprises, only a portion of the workforce needs the added enhancements provided by DLS mobility. In this case, any number of the enterprise’s phones could be enabled for DLS mobility, with user licenses then being purchased for only those employees who need DLS mobility.

Table 26: Solution Comparison: Hot Desking versus DLS Mobility

Hot Desking	DLS Mobility
Controlled and configured by OpenScape Voice	Controlled and configured by a separate deployment (DLS) server. Additionally provides the DlsAPI web service interface that allows third-party applications to connect to the DLS and to drive all mobility actions (logons, logoffs, create mobile users, etc.).

Hot Desking	DLS Mobility
The number of hot desking users is limited by the number of dynamic OpenScape Voice user licenses.	Supports up to 100,000 devices. These can be HFA, SIP, or mobility-enabled SIP devices, or mobile users. Refer to DLS documentation for details
Requires one OpenScape Voice dynamic license per user.	Requires one OpenScape Voice dynamic user license and one DLS Mobility license per mobility-enabled user.
The remote office telephone and the home office telephone must be hosted by the same OpenScape Voice, and both must be in the same business group.	All devices used by a subscriber must be located on the same DLS server.
Transfers only OpenScape Voice-based features to the remote office telephone.	Transfers the following to the remote device: • OpenScape Voice-based features. • Telephone-based features. • All personal data, such as call numbers, passwords, and privileges. • Customized key configuration and layout, including screen savers. • Advanced user data such as caller lists and display module data. Note that the size of the non-managed user data should not exceed 200 Kbytes. Therefore, it is recommended that screen savers, logos, ringtones, and the like NOT be saved as non-managed user data. The size of this data will have a significant impact on the DLS performance as well as on the number of mobile users that are supported. Refer to the DLS documentation for details.
Does not support the following OpenScape Voice-features on the remote office telephone: • Call forwarding • Hunt groups	Supports all OpenScape Voice-based and all telephone-based features assigned to the user.
Does not provide status information for the following OpenScape Voice-based features on the remote office telephone: • Call forwarding • DND	Provides accurate status indications for all OpenScape Voice-features, including call forwarding and DND.

Related concepts

Hot Desking on page 273
DLS Mobility on page 274
OpenScape Voice-based Call Forwarding Features on page 286
Hunt Groups

4.2.4 Serial Ringing

The Serial Ringing feature provides subscribers the capability to be sequentially rung at a series of locations. This is especially useful for those whose job duties require them to be in or around many different work areas throughout the day.

This feature optionally includes the ability for the caller to instantly transfer to the callee’s voice mailbox, rather than waiting for the call to progress through all locations to do so.

The administrator assigns the Serial Ringing feature to a subscriber, then associates it with one of the user’s DNs, referred to as the main DN. After this step, either the subscriber or the administrator creates a screening list, known as a Serial Ringing List, that contains up to six DNs. These DNs represent the additional locations that ring when an incoming call arrives at the main DN, and the sequence in which they are rung. To allow control from the endpoint, the administrator has to create the corresponding Feature Access Code.

After entering this Feature Access Code, the subscriber hears an announcement that provides the feature name, its current status (active or inactive), and the number of DNs currently on the list. OpenScape Voice then prompts the user to specify one of the following actions to perform:

- Activate or deactivate the feature
- Hear the DNs that are currently on the list
- Add or delete DNs to and from the list

A confirmation tone or announcement is provided to acknowledge the activation. If the subscriber’s serial ringing list is empty, OpenScape Voice prompts the subscriber to enter DNs into the list. As soon as a valid DN is entered, the feature is activated.

After the feature is activated, incoming calls cause the main DN to ring. If it is not answered in the configured ring duration interval, the next destination DN is rung for its configured ring duration interval. The first DN to answer is connected.

NOTICE:

OpenScape Voice uses the subscriber’s dialing characteristics, rather than the caller's, when it sets up calls to the numbers in the Serial Ringing List.

If there is no answer after all destination DNs are rung, the call is then routed to one of the following:

- The user's station Call Forwarding - Don’t Answer destination (if defined)
- An intercept announcement

If there is no answer at a given destination DN, OpenScape Voice provides an intercept announcement before attempting the next number in the list. The options are the following:

- An announcement that keeps the caller apprised of the call's progress - for example, "Trying to reach the user at a different number."
- An announcement that provides the above information, and also gives the option for the caller to press a digit to be instantly routed to the called party's voice mailbox.

Related Features

The Simultaneous Ringing feature is similar to this feature, but it rings several locations at the same time.

Related concepts

Feature Profiles on page 135
Feature Access Codes for User Mobility on page 284
Call Forwarding on No Reply (Station-controllable) on page 289
Simultaneous Ringing on page 278

4.2.5 Simultaneous Ringing

The Simultaneous Ringing feature provides subscribers the capability to be simultaneously rung at multiple locations. This is especially useful for subscribers, whose job duties require them to be in or around many different work areas throughout the day.

The administrator configures the associated access codes and assigns the Simultaneous Ringing feature to a subscriber's DN (Directory Number), which is referred to as the main DN in the following description. This main DN must be registered with OpenScape Voice for the feature to operate.

After this step, either the subscriber or the system administrator creates a screening list, known as a Simultaneous Ringing List, that contains up to six DNs. These DNs represent the additional locations that ring when an incoming call arrives at the main DN. To allow control from the endpoint, the administrator has to create Feature Access Code for activation, deactivation and list editing.

After entering the Feature Access Code for list editing, the subscriber hears an announcement that provides the feature name, its current status (active or inactive), and the number of DNs currently on the list. OpenScape Voice then prompts the user to specify one of the following actions to perform:

- Activate or deactivate the feature
- Hear the DNs that are currently on the list
- Add or delete DNs to and from the list

A confirmation tone or announcement is provided to acknowledge the activation. If the subscriber's serial ringing list is empty, OpenScape Voice prompts the subscriber to enter DNs into the list. As soon as a valid DN is entered, the feature is activated.

After the feature is activated, incoming calls cause the main DN and each destination DN to ring. The first DN to answer is connected. If the call is forwarded to another DN, such as voice mail, it rings until answered.

NOTICE:

OpenScape Voice uses the subscriber’s dialing characteristics, rather than the caller's, when it sets up calls to the numbers in the Simultaneous Ringing List.

Related Features

- The Serial Ringing feature is similar to this feature, but it rings one location at a time.
- The Simultaneous Ringing - Remote Activation feature provides the subscriber the capability to manage Simultaneous Ringing from locations other than the subscriber’s station.

Related concepts

Feature Profiles on page 135
Serial Ringing on page 277
Feature Access Codes for User Mobility on page 284
Simultaneous Ringing Remote Activation on page 279
Night Bell Call Pickup on page 313

4.2.6 Simultaneous Ringing Remote Activation

The Simultaneous Ringing Remote Activation feature is an optional capability of the Simultaneous Ringing feature. It provides the subscriber the capability to manage the feature from locations other than the subscriber’s station - for example, from home or from another work station.

The system administrator does the following:

- Creates a DN to use as the RFA (Remote Feature Access) number.
- Defines the remote activation PIN. This PIN can be unique to each subscriber, or it can be shared by all subscribers using a given feature profile.

The user accesses the simultaneous ringing feature remotely as follows:

1) The user dials the remote activation DN associated with the feature.
2) When OpenScape Voice detects a call to the remote activation DN, it connects the caller to the media server. The media server prompts the caller to enter the correct home DN and PIN.
3) The user dials the correct home DN (main number) followed by the correct PIN. The media server collects these digits and passes them to OpenScape Voice.
4) OpenScape Voice confirms the PIN and provides a confirmation tone or announcement to the user.

After performing these steps, the user has the same access to the simultaneous ringing feature as if it were accessed from the home DN. However, local (non-PSTN extensions) must be prefixed with the digits 02. For example, if the local extension is 1020, the user must enter 021020 for the change to take effect.

Requirements

To subscribe to this feature, the subscriber must also have the Simultaneous Ringing feature.

NOTICE:

In a multiple branch environment it is strongly recommended that the PACs (Prefix Access Codes) for remotely accessible services such as Simultaneous Ringing are the same for all NPs (Numbering Plans). Otherwise the remote access DNs for each NP must be provisioned to ensure that the call arrives from the PSTN via a gateway in the same NP.

Related concepts

Feature Profiles on page 135

Simultaneous Ringing on page 278

4.2.7 Teleworking

The teleworking feature provides a solution that permits OpenScape Voice users who work remotely to have access to the telephone features they can access while at their primary office locations.

Contact your Unify representative about the availability of teleworking solutions applicable to other SIP endpoints.

4.2.8 One Number Service

The One Number Service (ONS) features are a group of CSTA (Computer Supported Telecommunications Applications) capabilities that permit CSTA- and ONS-enabled applications to take on the responsibility of routing users' calls. This advanced CSTA service permits ONS-enabled applications to create, route, track, and provide call control for multiple inbound and outbound calls using CSTA OpenScape Voice call control services for any device, located anywhere, for the entire duration of the call.

ONS functionality is especially suitable for mobile users with multiple associated devices, including external devices such as mobile telephones. It permits the application to hold, consult, transfer during consultation, single-step transfer, alternate, and conference the ONS call, even if one or both of the connected parties are located in the public network. In addition, it enables features such as:

- Personalized workflow using rules-based call routing
- Single point of contact on inbound and outbound calls
- Setting preferred devices on inbound and outbound calls

Examples for CSTA and ONS-enabled applications are HiPath ComAssistant and OpenScape UC (Unified Communications) Application.

NOTICE:

ONS should not be used in parallel with Hot Desking

IMPORTANT:

If a subscriber number is assigned as ONS you should not delete the subscriber from OSV because it will create an inconsistent state in UC database. The subscriber with assigned ONS can be unassigned from the user and removed from UC database by using CMP-UM or HPUM.

Supported CSTA Call Control Services

ONS supports the following standard CSTA call control services:

- Make Call
- Clear Connection
- Accept Call
- Deflect Call
- Answer Call
- Hold Call
- Retrieve Call
- Transfer Call
- Single Step Transfer Call
- Consultation Call
- Alternate Call
- Reconnect Call
- Conference Call
- Generate Digits from any associated device

Standard CSTA call control events are sent for ONS calls, including the Offered event on inbound calls. An offered call suspends call processing for two seconds, which gives the CSTA-enabled application time to move the call to a specific associated device.

Requirements

Each ONS subscriber should be provisioned for the following:

- CSTA service
- Call Forwarding - Unreachable (in case the link to the ONS-enabled application is not functioning)
- Call Transfer (so transfers can be performed)

In addition, all caller ID services should be set properly.

Functional Sequence

For outbound calls, the subscriber uses the CSTA application interface to originate a call through any associated device, anywhere - for example, a PBX telephone, a mobile telephone, a hotel telephone, or a home telephone. For the called party, the call appears as if it were placed from the subscriber's business phone number.

For inbound calls, the CSTA application provides the functionality to correctly route these calls to any of the subscriber’s preferred associated devices, including voice mail. For the calling party, the call appears as if it were answered from the subscriber's business phone number.

When an external associated device is involved in either type of call, OpenScape Voice processes consultation calls initiated by the CSTA and ONS-enabled application such that a second call leg is not created to the gateway. An external device is any device connected through a SIP- or SIP-Q gateway - for example, a PSTN, another OpenScape Voice system, OpenScape 4000, or HiPath 3000 or a third-party PBX.

Related concepts

Feature Profiles on page 135

Hot Desking on page 273

4.2.8.1 Manually Triggered Consultation Calls for Internal ONDs

Several features that can be manually invoked at an OND (One Number Service Device) during an active ONS (One Number Service) call, result in establishing an additional call leg to the OND. For some of them - and if the involved OND is *internal* (i.e. a registered subscriber device in the OpenScape Voice) - the second call leg will be identified as a consultation call associated with the active ONS call. This enables subsequent manual feature activations for consultation calls.

For an *internal* OND involved in an ONS call, the following manually invoked features will result in a consultation call associated with the existing ONS call (ONS consultation call, for short):

- Direct consultation call via keypad dialing or rep-dial key
- Directed Call Pickup
- Call Pickup Group

> **NOTICE:**
>
> A direct call from a secondary line or another contact of the OND is *not* associated with an existing ONS call.

Once an ONS consultation call is stable, the call service normally available on each call leg will be available via CSTA. and the following subsequent manual feature activations become possible:

- Alternate (Toggle)
- Reconnect held call (clear and return)
- Hold / Retrieve
- Clear Connection
- Complete Transfer (screened)
- Blind Transfer
- Conference

4.2.8.2 OND Consultation

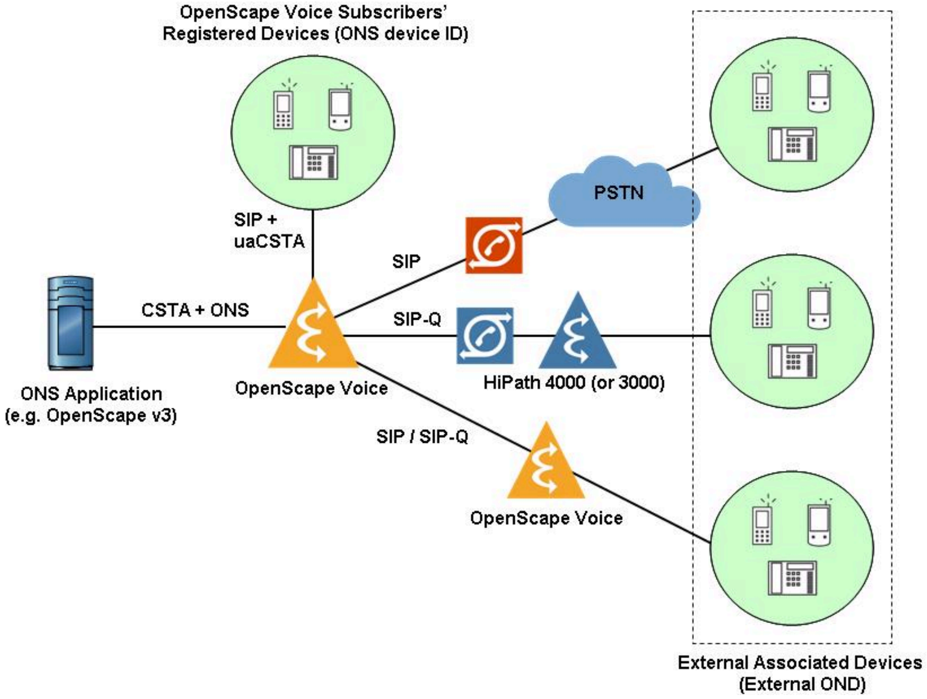
The OND (One Number Service Device) Consultation feature allow a CSTA/ ONS application to initiate a consultation call from an external OND (e.g. cell phone, home phone ...) without creating a second call leg to the OND device.

> **NOTICE:**
>
> *External* means that the OND device is not a registered subscriber device in the OpenScape Voice.
>
> In normal 3PCC (3rd party call control) consultation initiated via CSTA a new call leg to the consulting device is created.

OND Consultation is controlled entirely by the OpenScape Voice, including alternating between the parties, reconnecting to the held party, music on hold.

Application Scenario

ONS applications such as OpenScape enable users to choose a preferred voice device to use in inbound or outbound calls depending on user-specified rules. In some cases, the preferred device is outside the OSV switching domain, for example a device in the PSTN such as a cell phone or home phone.


OpenScape Voice Subscribers' Registered Devices (ONS device ID)
SIP + uaCSTA
CSTA + ONS
ONS Application (e.g. OpenScape v3)
OpenScape Voice
SIP
PSTN
SIP-Q
HiPath 4000 (or 3000)
SIP / SIP-Q
OpenScape Voice
External Associated Devices (External OND)

Consider the following setup:

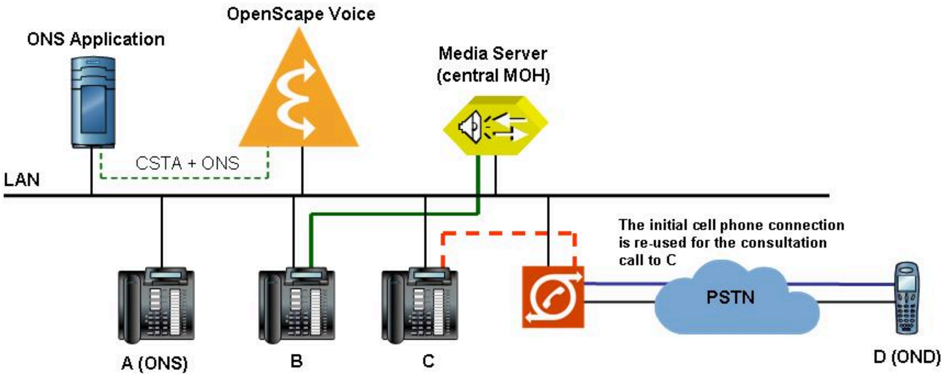
- Subscriber A is provisioned on the OpenScape Voice with CSTA and ONS
- Device D is a cell phone owned by subscriber A
- Devices B and C are the registered devices for subscribers B and C respectively.

Now assume that user A (ONS) uses a click-to-dial CSTA application to call user B using device-D (OND). This is a standard ONS-IO Outbound call which uses 3PCC to set up the prompting call leg to device D on behalf of subscriber A. When device-D answers the prompting-call, the OSV extends the call to device B. User B sees the incoming call with user A's identity and answers the call.

The voice media for the call is now established between devices D and B (represented by the solid blue line in the figure below). Note that this call uses the services of subscriber A, even though the registered device for subscriber A (i.e. device A) is not involved in this call.

The resulting call is reflected as A|D <--> B.

With OND Consulting, when the CSTA ONS application initiates a consultation call, the OpenScape Voice will not create a second call leg to the gateway. Instead, the OSV will put the existing ONS call (A|D<-->B) on hold and it will use the existing call leg to the OND device for the new consultation call. If subscriber A is provisioned for central Music on Hold (MOH), device B will be connected to the Media Server. Otherwise, device B is put in local hold.The figure below illustrates this behavior. Note that the consultation call A|D<-->C reuses the original call from the External OND device (represented by the solid blue line).



NOTICE: It is not supported to Alternate/Reconnect between incoming calls established on a preferred device being an External OND e.g. a mobile phone. Alternating between these calls can only be administered via the external OND.

4.2.9 Feature Access Codes for User Mobility

Feature Access Codes enable subscribers to control Mobility Features from their endpoints. A Feature Access Code can either be dialed or it can be assigned to a function key on the subscribers' phones, providing seamless access to server-side features.

The required access codes are usually created during the initial installation of the OpenScape Voice system; however, additional codes can be added at any time.

Technically, a Feature Access Code is a special instance of a PAC (Prefix Access Code), defining a sequence of keys (0-9, #, *) that enable callers to invoke a specific server-side feature. It can be created either globally (i.e. in the Global Numbering Plan) or locally (i.e. in a Private Numbering Plan). In OpenScape Voice Assistant such a "Feature PAC" has to be created with

- Prefix Type: Vertical Service

- Nature of Address: Unknown
- Destination Type: Service

and one of the available Service destinations.

NOTICE:

In a multiple branch environment it is strongly recommended that the PACs (Prefix Access Codes) for remotely accessible services such as Simultaneous Ringing are the same for all NPs (Numbering Plans). Otherwise the remote access DNs for each NP must be provisioned to ensure that the call arrives from the PSTN via a gateway in the same NP.

Table 27: User Mobility related Service destinations

Feature	**Action**	Service	Example PAC
Hot Desking	activate	HD Activate	*35
	deactivate	HD Deactivate	*36
Serial Ringing	Screening List Editing (via TUI)	Serial Ringing SLE	*40
Simultaneous Ringing	activate	SRS Activate	*41
	deactivate	SRS Deactivate	*42
	control via TUI	SRS Edit	*43

TUI = Telephone User Interface

Related concepts

Serial Ringing on page 277

Simultaneous Ringing on page 278

4.2.10 RTP System Parameters

Certain aspects of Mobility services are controlled on a systemwide basis by RTP (Resilient Telco Platform) system parameters. Any changes made to these parameters affect all business groups and their members. Typically, these parameters are set during initial system configuration, to enforce global system policies and ensure proper feature interworking.

For example, the following properties can be modified by setting RTP system parameters:

- The maximum times a call can be forwarded
- Whether a subscriber hears a tone or announcement to confirm that a particular service is activated or deactivated

While some of these parameters affect all types of CF services, others control only certain types.

The following table presents the Mobility related RTP system parameters. Default values are shown in bold type.

Table 28: RTP System Parameters related to Mobility services

Parameter	Values	Description	Relevance
Srx/Main/ SRCFDATimeout	**0** - 30 seconds	When Enhanced CF (Call Forwarding), CF - No Reply or CF - Voice Mail is active, this parameter is used to extend the value of the Ring Duration field for the related CF service(s). This additional time interval provides the time necessary for calls to progress - for example, the next destination to be rung on a serial ringing list - so the call is not forwarded too soon. For example, assume the following: • The Ring Duration is defined as 20 seconds. • This RTP parameter is defined as 10 seconds. The two time intervals are added together, resulting in a total time interval of 30 seconds before a call is forwarded to the destination this service specifies.	Simultaneous Ringing

Furthermore, the CSTA related RTP parameters have to be set appropriately in order to operate the One Number Service.

Related concepts

RTP Management via OpenScape Voice Assistant on page 961

4.3 OpenScape Voice-based Call Forwarding Features

OpenScape Voice-based call forwarding features provide a means to customize the handling of calls when a subscriber is unavailable to answer them.

All OpenScape Voice-based call forwarding features can be provisioned at the feature profile level with possible modifications at the subscriber level.

OpenScape Voice vs. Endpoint-Based Call Forwarding

Unify SIP endpoints also provide the capability to configure and control local call forwarding. However, it is strongly recommended that the endpoint-based call forwarding features are not used simultaneously with call forwarding features that reside in OpenScape Voice.

The following are the recommendations for usage of this feature:

- OpenScape Desk Phone CP endpoints should use OpenScape Voice-based station call forwarding because it provides a more consistent call flow with better feature interaction checks.
- All other endpoints should use endpoint-based call forwarding.

Station-Controllable Call Forwarding

For some call forwarding features, the subscriber may be allowed to control the call forwarding behavior to a certain extent. For instance, he may be allowed to

- activate and deactivate the feature
- specify the forwarding destination

Station control is possible via feature access codes or OpenScape Desk Phone CP CSTA (Computer Supported Telecommunications Applications) over SIP.

Requirements

The following are the forwarding target requirements:

- The number must be a routable destination in the private network or in the PSTN - for example, it cannot be a feature access code.
- The number must be compatible with any toll and call restrictions in effect for the called subscriber.

Note that the called DN’s dialing characteristics, rather than the caller's, are used when forwarding the call.

Accounting

When a call is forwarded, CDRs (Call Detail Records) are generated as follows:

- One standard CDR for the call leg that takes place between the original calling party and the final forwarded-to (connected) party. This CDR type is generated for all calls.
- One call forwarding CDR for each call leg created when the original call is forwarded.

Because OpenScape Voice permits up to five forwards per call, up to five of these CDRs can be generated. For example, assume that party A calls party B. Party B forwards to party C; party C then forwards to party D. In this scenario:

- A standard CDR is generated for the A-to-D call.
- Individual call forwarding CDRs are generated for the B-to-C and C-to-D call legs.

Intermediate CDRs provide backup information to allow partial charging for long duration calls (calls lasting longer than 30 minutes) if a standard CDR is not generated due to some type of failure. As soon as a standard CDR is available for a call, any intermediate CDRs are no longer needed, so they are automatically discarded.

Related concepts

Feature Profiles on page 135

Hot Desking on page 273

DLS Mobility on page 274

Solution Comparison: Hot Desking versus DLS Mobility on page 275

4.3.1 Call Forwarding - Unconditional (Station-controllable)

The station-controllable Call Forwarding - Unconditional (CFU) feature, sometimes known as Call Forwarding - All Calls, provides the capability to redirect all calls intended for the subscriber to another destination. This feature can be controlled from the station.

If the subscriber is not permitted to modify the forwarding destination, the resulting forwarding logic is also known as Fixed Call Forwarding.

The administrator specifies:

- Whether the feature is always active, or if the subscriber is permitted to activate and deactivate it
- The forwarding destination. The administrator can also configure the feature such that the subscriber can supply or modify the forwarding destination

Related concepts

Call Forwarding - Remote Activation on page 288

Call Forwarding - Return on page 299

Selective Call Forwarding (Station-controllable) on page 290

Enhanced Call Forwarding on page 292

Call Forwarding - Voice Mail

CFSIE - All Calls on page 297

Call Forwarding Restrictions on page 301

OpenScape Desk Phone CP Feature Access on page 303

Feature Access Codes for Call Forwarding on page 304

RTP System Parameters on page 305

Keyset Operation Modes on page 264

4.3.2 Call Forwarding - Remote Activation

The Call Forwarding - Remote Activation feature, sometimes known as RACF (Remote Activation Call Forwarding), is an optional capability of the Call Forwarding - Unconditional feature. It allows subscribers to control Call Forwarding - Unconditional from any location.

This capability permits the subscriber to manage station call forwarding options and change forwarding destinations from home or from another work location.

Remote Activation is one of the OpenScape Voice features that provides support for mobility solutions. It ensures that employees have full control over their telephone calls even when they are offsite.

The administrator sets the RTP (Resilient Telco Platform) parameter Srx/Main/RACFCfmTreat to specify if tones or announcements should be used on a systemwide basis to confirm that the feature has been successfully activated. After doing so, the administrator:

- Creates a DN to use as the RACF access number.
- Defines the RACF PIN. This PIN can be unique to each subscriber, or it can be shared by all subscribers using a given feature profile.

Requirements

- A DN has to be defined as the RACF access number.

- The subscriber must also have the Unconditional Call Forwarding feature.

NOTICE:

In a multiple branch environment it is strongly recommended that the PACs (Prefix Access Codes) for remotely accessible services such as Unconditional Call Forwarding are the same for all NPs (Numbering Plans). Otherwise the remote access DNs for each NP must be provisioned to ensure that the call arrives from the PSTN via a gateway in the same NP.

Related concepts

Call Forwarding - Unconditional (Station-controllable) on page 287
RTP System Parameters on page 305
User Mobility on page 272
RTP Management via OpenScape Voice Assistant on page 961

4.3.3 Call Forwarding on Busy (Station-controllable)

The station-controllable Call Forwarding on Busy (CFB) feature, sometimes known as Call Forwarding - Busy Line (CFBL), provides the capability to redirect calls intended for the subscriber to another destination when the subscriber's station is in use.

If the subscriber is not permitted to modify the forwarding destination, the resulting forwarding logic is also known as Fixed Call Forwarding.

The administrator specifies:

- Whether the feature is always active, or if the subscriber is permitted to activate and deactivate it
- The forwarding destination. The administrator can also configure the feature such that the subscriber can supply or modify the forwarding destination

Related concepts

Call Forwarding - Return on page 299
Enhanced Call Forwarding on page 292
CFSIE - Busy on page 298
Call Forwarding - Voice Mail
Call Forwarding Restrictions on page 301
OpenScape Desk Phone CP Feature Access on page 303
Feature Access Codes for Call Forwarding on page 304
RTP System Parameters on page 305
Hunt Groups

4.3.4 Call Forwarding on No Reply (Station-controllable)

The station-controllable Call Forwarding on No Reply feature, sometimes known as Call Forwarding - Don't Answer (CFDA), provides the capability to redirect calls intended for the subscriber to another destination if the call is not answered after a preset number of rings.

If the subscriber is not permitted to modify the forwarding destination, the resulting forwarding logic is also known as Fixed Call Forwarding.

The administrator specifies:

- Whether the feature is always active, or if the subscriber is permitted to activate and deactivate it
- The ring duration
- The forwarding destination. The administrator can also configure the feature such that the subscriber can supply or modify the forwarding destination

Related concepts

Call Forwarding - Return on page 299
Enhanced Call Forwarding on page 292
Call Forwarding - Voice Mail
CFSIE - Don’t Answer
Call Forwarding Restrictions on page 301
OpenScape Desk Phone CP Feature Access on page 303
Feature Access Codes for Call Forwarding on page 304
RTP System Parameters on page 305
Serial Ringing on page 277

4.3.5 Selective Call Forwarding (Station-controllable)

The station-controllable Selective Call Forwarding (SCF) feature allows to selectively forward calls based on the caller’s identity. This is achieved by preparing a list of numbers (screening list) that may either serve as *White List* or *Black List*.

Selective Call Forwarding is independent of other call forwarding features. Calls from DNs that cannot be determined, or that are not on the list, can be forwarded to a destination defined in another call forwarding service.

The administrator

- may activate/deactivate the feature on behalf of the subscriber
- defines the forwarding destination
- defines the role of the associated screening list:
  - White list: Calls from the numbers appearing on the list are forwarded
  - Black list: Calls from numbers not appearing on the list are forwarded
- may add calling numbers to the screening list.

The subscriber uses the corresponding feature access code to

- activate or deactivate the feature
- add or remove numbers from the screening list

Note that the subscriber can neither change the forwarding destination nor the screening list role.

Requirements

In order to enable station control, the corresponding feature access code (SLE Select CFwd) has to be created at the business group level.

Functional Sequence

When a caller's number matches a number on the screening list, call handling depends on the defined usage of the screening list.

If it is a white list, the call is forwarded to the redirect number. This can be another telephone, another subscriber, voice mail, or an announcement. When the caller's number is not on the forwarding list, the call is completed as usual.

If it is a black list, the call is completed to the subscriber.

System Specific Information

The screening list may contain up to 32 entries.

Related concepts

Call Forwarding - Unconditional (Station-controllable) on page 287
Call Forwarding - Return on page 299
Enhanced Call Forwarding on page 292
Call Forwarding - Voice Mail
CFSIE - All Calls on page 297
Call Forwarding Restrictions on page 301
Feature Access Codes for Call Forwarding on page 304
RTP System Parameters on page 305

4.3.6 Call Forwarding - Dependable / Unreachable

The Call Forwarding - Dependable feature, also known as Call Forwarding - Unreachable , provides the capability to forward calls for the subscriber's line to another line when the destination is unreachable due to being either unregistered, not responding (unplugged) or audit blocked. Different forwarding targets can be specified for internal calls (from within the business group) and external calls (from outside the business group).

NOTICE:

Because an increasing number of enterprise users are mobile users, which may result in their home DNs being unregistered for substantial periods of time, it is imperative that a Call Forwarding -Dependable / Unreachable destination be provisioned for all subscribers.

The administrator activates and deactivates the feature and provides the redirect numbers for internal and external calls.

If Call Forwarding - Dependable / Unreachable is activated and the subscriber receives a call while he or she is unreachable, then:

- If the call is *internal* and a routable redirect number is configured, the call is forwarded to this internal redirect number.

- If the call is *external* and a routable redirect number is configured, the call is forwarded to this *external* redirect number.
- In any other case, the feature is not invoked.

Feature Interaction

The Call Forwarding -Dependable / Unreachable feature overrides several of the station or system forwarding events that would otherwise take place while the subscriber is in the unreachable state.

If a subscriber is unreachable, the OpenScape Voice-based call forwarding types have the following precedence, if activated:

1) Call Forwarding - Unconditional
2) Call Forwarding - Dependable / Unreachable
3) Call Forwarding - No Reply
4) Call Forwarding - Busy

Related concepts

Call Forwarding - Return on page 299
Call Forwarding Restrictions on page 301
RTP System Parameters on page 305

4.3.7 Enhanced Call Forwarding

The Enhanced Call Forwarding (ECF) feature, sometimes known as Call Forwarding - Time-of-Day (CF-ToD), provides sophisticated call forwarding based on a configurable schedule, on the forwarding condition (unconditional, busy, no answer) and on the caller identity.

This feature is useful if an enterprise wants to set up a fixed schedule for handling incoming calls - for example, calls to the customer service department. By specifying a schedule, calls can be routed differently based on the time of day or day of the week. Calls received after normal business hours might route to a voice mailbox or to another location that is currently open.

OpenScape Voice’s multiple time zone support capabilities ensure that the correct date and time information is used.

NOTICE:

It is not necessary for the related DN to subscribe to CF - Unconditional, CFBL (Call Forwarding - Busy Line), or CFDA (Call Forwarding - Don’t Answer) in order to use Enhanced Call Forwarding.

The administrator defines:

- Whether the feature is active
- The ring duration (for no answer condition)

- A time-of-day schedule that provides the following information:
  - The day of the week and the start and end times that the forwarding will be done. The schedule entries cannot overlap.

    IMPORTANT:

    For the OSV Assistant starting from UC V7 R3.0.8 the end time 12:00 am is allowed even if the start time is not the same (12:00 am). For the OSV starting from V7R1.48.1, the end time as 12:00 am is allowed and OSV calculates that as 24h (00:00:00-23:59:59). This means that the following two cases are now available:

    12:00am - 12:00am = all day (00:00:00 - 23:59:59) and

    xx:xx - 12:00am = From xx:xx until end of day (23:59:59).

    For example, adding the following ECF: DAY Monday, Start time 12:00am - End time 12:am, OSV will handle it as a call forward for Monday 00:00:00-23:59:59

  - The forwarding condition, which can be one of "Always", "Line is Busy", "No Answer" or "Busy no answer" (i.e. busy or no answer)
  - The Forward-to DN to be routed to when forwarding.
  - The affected caller group, i.e. whether to forward all calls, or only those contained in the Caller List, or only those not contained in the Caller List
- A configurable Caller List that can be used for selective forwarding.

There is an RTP-parameter, `Srx/DB/IsTimeZoneGMTLinuxDefault`, which can revert the + to - and the - to + for GMT-timezones. This parameter indicates whether to use the default POSIX-style signs in the Zone names and the output abbreviations. POSIX has positive signs west of Greenwich, but many people expect positive signs east of Greenwich. For example, TZ=Etc/GMT+4 uses the abbreviation GMT+4 and corresponds to 4 hours behind UTC even though many people would expect it to mean 4 hours ahead of UTC.

Related concepts

Call Forwarding - Unconditional (Station-controllable) on page 287
Call Forwarding on Busy (Station-controllable) on page 289
Call Forwarding on No Reply (Station-controllable) on page 289
Selective Call Forwarding (Station-controllable) on page 290
Call Forwarding - Return on page 299
Call Forwarding - Voice Mail
Call Forwarding Restrictions on page 301
RTP System Parameters on page 305

4.3.8 Call Forwarding - Voice Mail

The Call Forwarding - Voice Mail (CFVM) feature provides the capability to redirect calls intended for the subscriber to the voice mail system and -more important - it ensures that MWI (Message Waiting Indication) is delivered to the SIP endpoint when a new voice mail message is present.

CFVM Redirecting conditions

A call is redirected to the voice mail when one of the following occurs:

- the called station is in use
- the call remains unanswered for a preset number of rings
- the call is rejected by the user. (Optional condition defined by the Administrator)
- the call is rejected by the Do Not Disturb status. (Optional condition defined by the Administrator)

CFVM can be used independently, or it can be used in conjunction with other call forwarding features:

- If it is used independently, all unanswered, busy calls, calls rejected by the User or by DND are forwarded to voice mail, and the user receives MWI.
- If it is used in conjunction with other call forwarding features, different targets can be assigned to different scenarios, and the user receives MWI for the calls that were routed to voice mail. This capability is useful, for example, if a user wants unanswered calls to route to an assistant, and busy-forwarded calls to route to voice mail.

The administrator can also specify the conditions under which a MWI indication from the voice-mail system is considered valid. Based on the subscription state and status of the subscriber’s CFVM feature:

- If CFVM is not subscribed, the user does not receive MWI
- If CFVM is subscribed but inactive, the acceptance of an MWI indication for a voice mail subscriber is based on the setting of the RTP (Resilient Telco Platform) parameter Srx/Main/MwiOnVMInactive:
  - When set to True, an MWI indication is accepted and processed.
  - When set to False, an MWI indication is ignored.
- If CFVM is subscribed and active, a MWI is accepted and processed.

CFVM in Combination with CFB and/or CFDA

The administrator sets the RTP parameter Srx/Main/CFVMCompatibility to specify if it is allowed to combine CFVM with any of the station-controlled call forwarding features CFB (Call Forwarding - Busy) or CFDA (Call Forwarding - Don’t Answer).

If set to False, CFVM can not be combined with CFB or CFDA. This is the default.

If set to True, these combinations are allowed, i.e. CFVM and CFB and/or CFDA can be assigned to the same subscriber. Note that if CFVM and CFB/ CFDA are active, the latter take precedence in a busy line/no answer situation.

4.3.8.1 Message Waiting Indication

The MWI (Message Waiting Indication) feature permits the reception of a subscriber’s MWI status from a voice mail system via SIP. In a multiple-platform environment (for example, when a OpenScape 4000 is present), OpenScape Voice sends and receives MWI over SIP-Q.

Depending on the type of SIP endpoint the subscriber uses, the following indications are possible:

- Audible message waiting indication, which provides a special dial tone (sometimes called message-waiting dial tone)
- VMWI (Visual MWI), which illuminates a light (indicator) on the telephone
- Both

Functional Sequence

When a call cannot be answered by a subscriber of a voice mail system (sometimes known as a message storage and retrieval [MSR] system), the following takes place:

- If the voice mail system is connected to OpenScape Voice via SIP: Whenever a call is automatically redirected by a station call forwarding feature from the subscriber's DN to the voice mail system, the caller is automatically redirected to the called party’s voice mailbox.
- If the voice mail system is connected to OpenScape Voice via SIP-Q (the voice mail system is located in the OpenScape 4000 SIP-Q network): The caller is automatically redirected to the called party’s voice mailbox. After the call is redirected, the calling party can then leave a message for the voice mail system subscriber. After the voice mail system sends a request, OpenScape Voice updates the status of the MWI in order to provide the subscriber notification of the waiting message.

OpenScape Voice supports the message waiting indicator notification function according to the mandatory requirements of GR-866-CORE. VMWI is supported according to GR-1401-CORE.

The indications are provided through signaling and interworking with Unify or third-party voice mail systems.

Other Characteristics

OpenScape Voice ensures that subscribers continue to receive accurate MWI in any of the following circumstances:

- The SIP endpoint loses power temporarily.
- A restart of the SIP endpoint becomes necessary.
- A temporary WAN outage prevents an update of the MWI when a message was left for the subscriber.
- A hot desking subscriber logs in at a remote office telephone.
- The SIP endpoint is not registered at the time the SIP message would otherwise be sent.

4.3.9 Call Forwarding System-Internal/External (CFSIE)

The Call Forwarding System-Internal/External (CFSIE) features provide administrators the capability to redirect calls intended for the subscriber's line to another line. Different forwarding targets can be specified for internal calls (from within the business group) and external calls (from outside the business group).

The administrator specifies whether any of the four CFSIE features (CFSIE - All, CFSIE - Busy, CFSIE - No Answer, and CFSIE - Do Not Disturb) are enabled for a given subscriber.

At the forwarded-to subscriber (Subscriber C), the Calling Number is updated with the DN of the originator (Subscriber A, when A calls B and B is forwarded to C).

When an incoming call is forwarded due to one of the CFSIE features, additional information on the forwarding is sent to each subscriber involved in the forwarding. Depending on the endpoint configuration, the following displays and tones are possible:

- Calling party name and number display
- Forwarded-to party name and number display

Both visible and audible indications can be separately activated and deactivated.

CFSIE and Station-controllable Call Forwarding

The administrator allows the end user to configure different call forwarding destinations for internal calls and external calls on his phone or from a CSTA application. The CSFIE feature is exposed via the CSTA/uaCSTA interface, so uaCSTA-enabled phones and CSTA applications “endpoints” can access it.

The privilege to configure CFSIE from endpoints is controlled by the administrator at the subscriber level. According to the CSTA standard each of the internal or external variations of a CFSIE type can be turned on/off separately. As a consequence the privilege to configure the internal or external variation of a CFSIE type is also granted separately by the administrator.

The privilege to configure the CFSIE feature is sent to the endpoint so it can adjust the UI dynamically to indicate to the user which features are configurable.

The end user can access the Call Forwarding features assigned to the endpoint with the following privileges:

- For the configurable CF features the user can enable/disable them, change their destinations.
- For the un-configurable features the user can view their current status and their forwarding destinations.

IMPORTANT:

If the configuration of a CFSIE feature is changed from the administrator side (i.e. via Assistant), the endpoint is informed so it can update the display with latest information.

The Cal forwarding types that can be configured by the end-user (if permitted by the Administrator) are the following:

- Call Forwarding Unconditional (also referred to as call forwarding-immediate, call forwarding-all or CFU)
- Call Forwarding Busy (also referred to as CFB)
- Call Forwarding No Answer (also referred to as call forwarding-no reply, CFNR, or CFNA).

IMPORTANT:

When active, station-controllable call forwarding supersedes system-level call forwarding.

Internal Call vs. External Call

The following indicates how all CFSIE features classify a call:

- Internal call (within the same business group):
  - Subscribers with a configured DN
  - Subscribers in a gateway (such as theOpenScape 4000), where the SIP/SIP-Q protocol indicates that the calling party is private
- External call:
  - Subscribers in another business group
  - Subscribers in a gateway (such as the OpenScape 4000), where the SIP/SIP-Q protocol does not indicate that the calling party is private or that it is marked as public only
  - Subscribers in a gateway (such as the OpenScape 4000), where the SIP/SIP-Q protocols indicates that the calling party is public

From V7 onwards in case of a Blind Transfer (the call is transferred without notifying the recipient or checking if he is busy) the administrator can choose if the CFSIE classifies the call as Internal or External is according to the transferring or transferred party.

E.g. A calls B, B is blind transferred to C, C has CFSIE activated

A is the Transferred party

B is the Transferring party

C is the Transferred-to party

IMPORTANT:

This feature only works if the transferring party and transferred-to party are in the same OSV. If the call is transferred to the OSV by another OSV or 4K, the first OSV is not aware that the transfer happened on the remote side thus the calling party (transferring party) will always be used by CFSIE to determine an internal/external call.

NOTICE:

In previous to V7 versions and for attendant and semi-attendant call transfers the call is classified by CFSIE as internal or external only according to the Transferred party.

4.3.9.1 CFSIE - All Calls

The CFSIE-All (Call Forwarding System-Internal/External - All Calls) feature provides administrators the capability to redirect all calls intended for the subscriber's line to another line. Different forwarding targets can be specified for internal calls and external calls.

When a caller dials the DN of a station that has CFSIE-All active, OpenScape Voice forwards the caller to the predetermined forwarding target. The subscriber can continue to originate calls.

Related concepts

Call Forwarding - Unconditional (Station-controllable) on page 287
Selective Call Forwarding (Station-controllable) on page 290
Call Forwarding System-Internal/External (CFSIE)
Call Forwarding - Return on page 299
CFSIE - Busy on page 298
CFSIE - Don’t Answer
CFSIE - Do Not Disturb on page 299
Call Forwarding Restrictions on page 301
RTP System Parameters on page 305

4.3.9.2 CFSIE - Busy

The OpenScape Voice-based CFSIE-Busy (Call Forwarding System-Internal/External - Busy) feature provides administrators the capability to redirect calls received when the subscriber’s station is in use. Different forwarding targets can be specified for internal calls and external calls.

When a caller dials the DN of a station that has CFSIE-Busy active, one of the following occurs:

- If the destination is idle, the subscriber is alerted normally.
- If the destination is busy, OpenScape Voice forwards the caller to the predetermined forwarding target.

Related concepts

Call Forwarding on Busy (Station-controllable) on page 289
Call Forwarding System-Internal/External (CFSIE)
CFSIE - All Calls on page 297
Call Forwarding - Return on page 299
CFSIE - Don’t Answer
CFSIE - Do Not Disturb on page 299
Call Forwarding Restrictions on page 301
RTP System Parameters on page 305

4.3.9.3 CFSIE - Don’t Answer

The CFSIE-DA (Call Forwarding System-Internal/External - Don’t Answer) feature provides administrators the capability to redirect calls that remain unanswered for a certain time. Different forwarding targets can be specified for internal calls and external calls.

CFSIE-DA also requires the administrator to specify the Maximum Time to Ring before forwarding the call.

From version V7 onwards timers for CFSIE-DA are configurable separately for external and internal calls.

Functional Operation

When a caller dials the DN of a station that has CFSIE-DA active, the subscriber is alerted normally the call is classified as Internal or External and the Maximum Time to Ring timer for the Internal or External call starts. Depending on the progress of the call, one of the following occurs:

- If the subscriber answers the call before the timer expires, the caller is connected to the subscriber and the call progresses normally.
- If the subscriber does not answer the call before the relevant timer expires, OpenScape Voice forwards the caller to the predetermined forwarding target, depending on the call classification (i.e Internal or External).

4.3.9.4 CFSIE - Do Not Disturb

The OpenScape Voice-based CFSIE-DND (Call Forwarding System-Internal/ External - Do Not Disturb) feature provides administrators the capability to redirect calls received while the caller has OpenScape Voice-based DND active. Different forwarding targets can be specified for internal calls and external calls.

When a caller dials the DN of a station that has DND and CFSIE-DND active, OpenScape Voice forwards the caller to the predetermined forwarding target.

Requirements

In order to get CFSIE-DND to work, the system administrator has to set the RTP (Resilient Telco Platform) system parameter Srx/Main/CFSIECompatibility to True. This is the default value.

If this parameter is set to False, calls received are directed to intercept treatment, rather than forwarded.

Related concepts

OpenScape Voice-based Do Not Disturb on page 154
Call Forwarding System-Internal/External (CFSIE)
CFSIE - All Calls on page 297
CFSIE - Busy on page 298
CFSIE - Don’t Answer
Call Forwarding - Return on page 299
RTP Management via OpenScape Voice Assistant on page 961

4.3.10 Call Forwarding - Return

Call Forwarding - Return allows the forwarded-to station to call the forwarding station and override (ignore) the forwarding.

This occurs even when calling party information is not delivered to the subscriber.

Related Features

Call Forwarding - Return is an inherent capability of the following OpenScape Voice-based call forwarding features:

- Call Forwarding - Unconditional
- Call Forwarding - Busy
- Call Forwarding - No Answer
- Call Forwarding - Voice Mail
- CFSIE (Call Forwarding System Internal/External) - All
- CFSIE - Busy
- CFSIE - DND (Do Not Disturb)
- CFSIE - DA (Don’t Answer)
- Selective Call Forwarding
- Enhanced Call Forwarding

Call Forwarding - Return is also an inherent capability of Call Forwarding - Unreachable; however, it operates in a different manner than it does for other call forwarding features. For example, assume that station A has Call Forwarding - unreachable to station B. If station B calls station A while the station is unregistered, station B hears an announcement that the subscriber is not available.

This feature is particularly useful in executive-assistant groups for the following reasons:

- It allows the assistant to call the executive even when the executive’s telephone is forwarded to the assistant.
- In the case of Call Forwarding - Unreachable, it notifies the assistant that the executive is unavailable rather than providing a busy tone.

Related concepts

Call Forwarding - Unconditional (Station-controllable) on page 287
Call Forwarding on Busy (Station-controllable) on page 289
Call Forwarding on No Reply (Station-controllable) on page 289
Selective Call Forwarding (Station-controllable) on page 290
Call Forwarding - Dependable / Unreachable on page 291
Enhanced Call Forwarding on page 292
Call Forwarding System-Internal/External (CFSIE)
CFSIE - All Calls on page 297
CFSIE - Busy on page 298
CFSIE - Don’t Answer
CFSIE - Do Not Disturb on page 299

4.3.11 Remote Call Forwarding

The Remote Call Forwarding (RCF) feature provides the capability to redirect calls placed to a particular access number (the RCF DN) to a fixed destination.

This feature is similar to OpenScape Voice-based Unconditional Call Forwarding with the following exception:

- No physical telephone is associated with the base DN ("Virtual DN").

Call Forwarding Displays are provided for the calling and forwarded-to parties in case of RCF. OSV always sends 181 Call Is Being Forwarded to the calling party whenever there is a diversion (for example, Call Forwarding - All Types).

The SIP 181 response contains a "P-Asserted-Identity" (PAI) header-field with the display information of the diverting/forwarding party (B).

When reception of more than one simultaneous call is desired, the forwarded-to DN associated with the RCF DN can be the pilot number of a hunt group. Although OpenScape Voice does not require that this be the case, doing so permits the forwarded-to party to receive and process simultaneous calls. Call forwarding takes place regardless of the status of the forwarded-to party. If all lines are busy, the calling party might hear busy tone or can alternately be routed to the voice mailbox associated with the DN.

When the DN is being used for station RCF, it cannot be subscribed to any other services.

The system administrator configures the station RCF feature by specifying the following:

- The RCF DN that serves as the access number dialed by outside callers. The RCF DN does not originate.
- The forwarding destination for all calls to the RCF DN.

NOTICE:

RCF to MLHG pilot number is not recommended when the Hunt Group is controlled by OpenScape Contact Center (OSCC). When a Hunt Group is controlled by the OpenScape Contact Center (OSCC), you must configure the SIP subscriber number with Call forwarding unconditional, instead of RCF, for each pilot number.

4.3.12 Call Forwarding Override

Call Forwarding Override (CFO) feature allows an OSV subscriber to dial a Prefix Access Code + DN in order to reach a called party, and meanwhile bypass all call forwarding features configured for that called party.

The usage of CFO is limited to users that belong to the same Business Group. The user that has been assigned the CFO feature doesn’t have the capability to override a feature of another user that belongs to a different organization (BG). The percentage of users in a BG which can be assigned with the CFO feature is not limited.

End users are not allowed to assign the Call Forwarding Override feature to themselves, it can only be done by the administrator.

Once the feature is assigned to a subscriber it is automatically activated.

4.3.13 Call Forwarding Restrictions

With the Call Forwarding Restrictions feature, certain traffic types can be excluded from being used during Call Forwarding execution. System-wide and subscriber specific restrictions can be enforced and apply to both OpenScape Voice-based and endpoint-based call forwardings.

Traffic Types and Classes of Restriction

Traffic type restrictions are declared in so-called *Classes of Restriction* that are used in the Toll and Call Restrictions feature, the Call Forwarding Restrictions feature, the Account Code feature and the BG Authorization Code feature.

The procedure to set up a Class of Restriction can be roughly described in the following way:

1) Define custom Traffic Types, if necessary
2) Assign Traffic Types to new and existing Destination Codes and Code Indexes
3) Create the required Classes of Restriction, comprising those traffic types that shall be restricted in any of the related features

Feature Provisioning

Classes of Restriction for Call Forwarding can be configured globally (system-wide) and for individual subscribers.

Functional Sequence

Upon execution of Call Forwarding, the destination number is validated and the call may not be forwarded due to existing Call Forwarding Restrictions.

Only the Administrator is able to control Call Forwarding Restriction provisioning and not the station user.

When a subscriber attempts to set a call forwarding destination in the OpenScape Voice, the system validates the destination number to see if the subscriber is allowed to forward calls to this destination. If no call forwarding restrictions are specifically assigned to the subscriber, OpenScape Voice checks for a system-wide default Class of Restriction and a default restriction for call forwarding to emergency traffic types.

Activation of call forward local in the SIP endpoint or in the OpenScape Voice via non-validating mechanisms (e.g. the Media Server) can occur. It is suggested the user should initiate a test call after forwarding is active to validate that call forwarding is working.

IMPORTANT:

The Call Forwarding Restrictions feature for Subscribers and System-wide restricts more than just Call Forwarding. It also restricts:

- Hunt Group Overflow DN
- Hunt Group Night Service DN
- Hunt Group Rerouting DN
- SCA Redirect
- CT Security target
- Static OND
- SRS
- SERRNG

Related concepts

Call Forwarding - Unconditional (Station-controllable) on page 287
Call Forwarding on Busy (Station-controllable) on page 289
Call Forwarding on No Reply (Station-controllable) on page 289
Selective Call Forwarding (Station-controllable) on page 290
Call Forwarding - Dependable / Unreachable on page 291
Enhanced Call Forwarding on page 292
Call Forwarding - Voice Mail
Call Forwarding System-Internal/External (CFSIE)
CFSIE - All Calls on page 297
CFSIE - Busy on page 298
CFSIE - Don't Answer
Classes of Restriction on page 555
Traffic Types

4.3.14 OpenScape Desk Phone CP Feature Access

OpenScape Desk Phone CP endpoints can be configured such that their call forwarding and DND (Do Not Disturb) keys control the OpenScape Voice-based Call Forwarding - Unconditional, Call Forwarding - Busy, Call Forwarding - Don't Answer and DND state rather than their endpoint-based counterparts.

Using **Server Based Features** instead of endpoint-based features is recommended for all OpenScape Desk CP phones because it provides a more consistent call flow with better feature interaction checks.

Note however that the **Server Based Features** option applies to all four of the features listed above. For example, it is not possible for the endpoint to control OpenScapeVoice-based call forwarding, but use endpoint-based DND.

Requirements

In addition to the required CF and DND features, the subscriber has to be provisioned for CSTA Access, with a CSTA type of **CSTA over SIP**.

Configuration is also required at the OpenScape Desk Phone CP endpoint to allow **uaCSTA** (User Agent CSTA) and **Server Based Features**.

NOTICE:

Since OpenScape Voice Version 4.0R1 the recommended way to manage essential phone settings is via the Integrated DLS Device Management. From there you can easily activate **uaCSTA** and **Server Based Features** by selecting the corresponding options. This will automatically enable the required services for the related subscriber (CSTA, CF, DND).

If no DLS is available (for the related BG), the required configurations have to be performed manually at the Assistant and the phone.

To enable **uaCSTA** at the switch, the RTP (Resilient Telco Platform) parameter Srx/Sip/UaCstaEnable has to be set to True, which is its default value.

Supported CSTA Call Control Services

The implementation makes use of the following standard CSTA (Computer Supported Telecommunications Applications) call control services:

- Get Forwarding
- Set Forwarding
- Get Do Not Disturb
- Set Do Not Disturb

Related concepts

Call Forwarding - Unconditional (Station-controllable) on page 287

Call Forwarding on Busy (Station-controllable) on page 289

Call Forwarding on No Reply (Station-controllable) on page 289

RTP Management via OpenScape Voice Assistant on page 961

4.3.15 Feature Access Codes for Call Forwarding

Feature access codes enable subscribers to activate or deactivate station-controllable CF (Call Forwarding) services and set CF-related properties from their endpoints. A feature access code can either be dialed or it can be assigned to a function key on the subscribers' phones, providing seamless access to server-side features.

Feature Access Codes are required for OpenScape Desk CP phones to invoke call forwarding features inaccessible by CSTA.

The required access codes are usually created during the initial installation of the OpenScape Voice system; however, additional codes can be added at any time.

Technically, a Feature Access Code is a special instance of a PAC (Prefix Access Code), defining a sequence of keys (0-9, #, *) that enable callers to invoke a specific server-side feature. It can be created either globally (i.e. in the Global Numbering Plan) or locally (i.e. in a Private Numbering Plan). In OpenScape Voice Assistant such a “Feature PAC” has to be created with

- Prefix Type: Vertical Service
- Nature of Address: Unknown
- Destination Type: Service

and one of the available Service destinations.

NOTICE:

In a multiple branch environment it is strongly recommended that the PACs (Prefix Access Codes) for remotely accessible services such as CF - Unconditional are the same for all NPs (Numbering Plans). Otherwise the remote access DNs for each NP must be provisioned to ensure that the call arrives from the PSTN via a gateway in the same NP.

Table 29: CF (Call Forwarding) related Service destinations

Feature	**Action**	Service	Example PAC
CF - Unconditional	activate	CFU Activate	*72
	deactivate	CFU Deactivate	*73
CF - Busy	activate	CFB Activate	*90
	deactivate	CFB Deactivate	*91
CF - No Reply	activate	CFNR Activate	*92
	deactivate	CFNR Deactivate	*93
CF - Selective	edit screening list	SCF SLE	*63
CF - Voice Mail	activate	CFVM Activate	*78
	deactivate	CFVM Deactivate	*79
DND (related to CFSIE-DND)	activate	DND Activate	
	deactivate	DND Deactivate	

Related concepts

Call Forwarding - Unconditional (Station-controllable) on page 287
Call Forwarding on Busy (Station-controllable) on page 289
Call Forwarding on No Reply (Station-controllable) on page 289
Selective Call Forwarding (Station-controllable) on page 290

4.3.16 RTP System Parameters

Certain aspects of CF (Call Forwarding) services are controlled on a systemwide basis by RTP (Resilient Telco Platform) system parameters. Any changes made to these parameters affect all business groups and their members. Typically, these parameters are set during initial system configuration, to enforce global system policies and ensure proper feature interworking.

For example, the following properties can be modified by setting RTP system parameters:

- The maximum times a call can be forwarded
- Whether a subscriber hears a tone or announcement to confirm that a particular service is activated or deactivated

While some of these parameters affect all types of CF services, others control only certain types.

The following table presents the CF related RTP system parameters. Default values are shown in bold type.

Table 30: RTP System Parameters related to Call Forwarding

Parameter	Values	Description	Relevance
Srx/Main/ CFAckTypeActiv	**1** (Tone), 2 (Announcement)	This parameter defines the confirmation type (tone or announcement) the subscriber hears after activating any call forwarding service.	all station-controllableCF services
Srx/Main/ CFAckTypeDeact	**1** (Tone), 2 (Announcement)	This parameter defines the confirmation type (tone or announcement) the subscriber hears after deactivating any call forwarding service.	all station-controllableCF services
Srx/Main/ CFMaxDiversions (CF Max Diversions)	1,2,3,4,**5**	This parameter limits the number of times a call can be forwarded.	all CF services
Srx/Main/ CFSIECompatibility	**RTPTrue** (True) RTPFalse (False)	This parameter defines whether calls received are forwarded or directed to intercept treatment. • When set to True, calls are forwarded to the configured destinations. • When set to False, calls are directed to intercept treatment.	CFSIE - DND
Srx/Main/ CFVMCompatibility	**RTPTrue** (True) RTPFalse (False)	This parameter indicates whether CF - Busy, CF - No Reply, or both can be assigned to a subscriber at the same time CF - Voice Mail is subscribed (for compatibility with older versions). When set to True: • CF - Busy and CF - Voice Mail can be assigned to a subscriber. When both are assigned and active, CF-Busy takes precedence in a busy-line situation. • CF - No Reply and CF - Voice Mail can be assigned to a subscriber. When both are assigned and active, CF - No Reply takes precedence in a no-answer situation because the no-answer timer for CF - Voice Mail does not start. When set to False, only CF - Voice Mail can be assigned to a subscriber.	CF - Busy, No Reply, Voice Mail

Parameter	Values	Description	Relevance
Srx/Main/ MwiOnVMInactive	**RTPTrue** (True) RTPFalse (False)	This parameter defines whether an MWI (Message Waiting Indication) is accepted for a voice mail subscriber when call forwarding to voice mail is not active. • When set to True, an MWI indication is accepted and processed. • When set to False, an MWI indication is ignored.	CF - Voice Mail in combination with CFSIE
Srx/Main/RACFCfmTreat	**1** (Tone), 2 (Announcement)	This parameter defines the confirmation type (tone or announcement) the subscriber hears after remotely activating Unconditional CF	CF - Remote Activation
Srx/Main/ SRCFDATimeout	**0** - 30 seconds	When Simultaneous Ringing is active, this parameter is used to extend the value you specify in the Ring Duration field for the related CF services. This additional time interval provides the time necessary for calls to progress - for example, the next destination to be rung on a serial ringing list - so the call is not forwarded too soon. For example, assume the following: • The Ring Duration is defined as 20 seconds. • This RTP parameter is defined as 10 seconds. The two time intervals are added together, resulting in a total time interval of 30 seconds before a call is forwarded to the destination this service specifies.	CF - Enhanced, No Reply, Voice Mail
Srx/Main/ UseBglExtension OnCFToVoiceMail	**RTPTrue** (True) RTPFalse (False)	This parameter indicates whether extensions should be used in redirecting numbers sent to the voice mail DN. • When set to True, the BGL extension is used for the Original Called Party Number or Redirecting Number field in the Setup message. • When set to False, the E.164 DN is used instead.	CF - Voice Mail

Parameter	Values	Description	Relevance
Srx/Main/ VoiceMailDnList ForBglExtensions	string **(blank)**	This parameter is relevant only if the previous parameter is set to True. It contains the Voice Mail DN(s) that require the use of BGL extensions when redirecting numbers sent to the voice mail DN. The string must be in the form `DN1::DN2::...::DNlast`. If the BGL extension associated with the called party DN appears in this string, that extension is sent in the Diversion Header rather than the E.164 DN.	CF - Voice Mail

Related concepts

Call Forwarding - Unconditional (Station-controllable) on page 287
Call Forwarding - Remote Activation on page 288
Call Forwarding on Busy (Station-controllable) on page 289
Call Forwarding on No Reply (Station-controllable) on page 289
Selective Call Forwarding (Station-controllable) on page 290
Call Forwarding - Dependable / Unreachable on page 291
Enhanced Call Forwarding on page 292
Call Forwarding - Voice Mail
Call Forwarding System-Internal/External (CFSIE)
CFSIE - All Calls on page 297
CFSIE - Busy on page 298
CFSIE - Don’t Answer
RTP Management via OpenScape Voice Assistant on page 961

4.4 Call Pickup

The Call Pickup features of OpenScape Voice allow subscribers to answer calls on behalf of other subscribers.

The Call Pickup Group (CPG) feature permits stations to be combined into pickup groups, which allow one group member to answer a call on behalf of another member.

The Directed Call Pickup feature provides subscribers the capability to answer any ringing, manually held or camped-on station within the business group.

The Night Bell Call Pickup feature permits alternate routing of inbound calls to a night bell such that everyone in the building can hear the alerting call, and can answer the incoming call from any SIP endpoint.

NOTICE:

Call Pickup is limited to lines within the same Business Group.

Networking

Since release 4.0R1 of OpenScape Voice, it is possible to configure CPGs whose members are located at different OpenScape Voice and OpenScape 4000 nodes, i.e. call pickup groups may span the SIP-Q network.

Related concepts

Bridged Calls and Privacy

4.4.1 Call Pickup Groups

The Call Pickup Group (CPG) feature permits to combine several subscribers of the same BG (Business Group) into a pickup group, which allows one group member to answer a call on behalf of another member.

A pickup group can consist of a combination of different user endpoint types, such as DFTs (Digital Feature Telephones) or keyset telephones. A call to any member in the group can be picked up at any other station in the group. When two or more members in the group are ringing at the same time, calls are answered in order of arrival; therefore, the call ringing the longest is automatically picked up first.

For each group, up to eight ringing lines are queued for pickup. If a ninth call rings, it cannot be picked up even if other calls leave the queue or it later becomes the only ringing line in the pickup group.

If there are no alerting calls for the group, and a pickup is attempted, the member who attempts the pickup receives an error indication. This indication might be an interrupted dial tone, a message on the display, or an error tone.

Network-wide Call Pickup Groups

With OpenScape Voice it is possible to configure CPGs whose members are located at different OpenScape Voice and OpenScape 4000 nodes, i.e. a CPG may span across the SIP-Q network.

Administrative Tasks

The administrator configures the pickup groups and creates feature access codes for call pickup initiation from the endpoints. Furthermore, these feature access codes can be assigned to function keys on the group members’ phones.

NOTICE:

Call Pickup Groups can also be administered via the **CMP** under **User Management** > **Administration** > **User & Resources**

CPG network access and routing must be administered and managed across the network (i.e., source-BG access code, destination access codes and destination group numbers).

'Waiting Queue Directory Number' setting for Call Pickup Group

- The selection button for the waiting queue will open a list with all the available Manual-Application Controlled Hunt Groups within the same Business Group

- The user shall be able to select any HG from the list and assign it to the waiting queue for the CPUG.
- Setting a Pilot DN will enable the waiting queue functionality to the unregistered CPUG members
  - The HG must be empty without any agents added
  - Otherwise the request shall be rejected.
- The user shall be able to disable the waiting queue functionality by clearing/ removing the Waiting Queue Directory Number field

Related concepts

Feature Profiles on page 135

Feature Access Codes for Call Pickup

4.4.1.1 Network-wide Call Pickup Groups

Since release 4.0R1 of OpenScape Voice it is possible to configure Call Pickup Groups whose members are located at different OpenScape Voice and OpenScape 4000 nodes, i.e. a CPG (Call Pickup Group) may span across the SIP-Q network.

Each local call pickup group is capable of adding a list of associated remote CPGs located elsewhere in the private SIP-Q network, but within the same BG (Business Group) in the logic of private SIP-Q networking.

Provisioning

The network-wide CPG feature relies on a feature activation and routing mechanism that is based on network-wide unique Access Codes being assigned to the involved OpenScape Voice Business Groups and OpenScape 4000 nodes. For a OpenScape 4000 this Access Code corresponds to its Node ID.

> **NOTICE:**
>
> The provisioning of network-wide unique Access Codes and network-wide CPGs must be carefully planned and administered as a network-wide service at each participating network entity.

On the OpenScape Voice side, the following actions have to be performed:

1) For every local BG (Business Group) that shall be provisioned with a network-wide CPG, the unique Access Code has to be configured as a PAC (Prefix Access Code), pointing to the *Network-wide Feature Activation Service* (**Network Feature**). Furthermore, the Access Code has to be assigned to this BG as its **BG Access Code**.
2) The Destination Access Codes (i.e. Access Codes of remote OpenScape Voice BGs or OpenScape 4000 nodes) have to be made routable across the network. PACs with appropriate destinations have to be created in the appropriate numbering plans.
3) When configuring a network-wide CPG, the associated remote CPGs have to be specified by the Access Code of their enclosing administrative entity (BG or Node) and their identifying number within this entity. Because Access Codes are unique across the network and the identifying numbers are

unique within the enclosing entity, all CPGs can be properly addressed in this way.

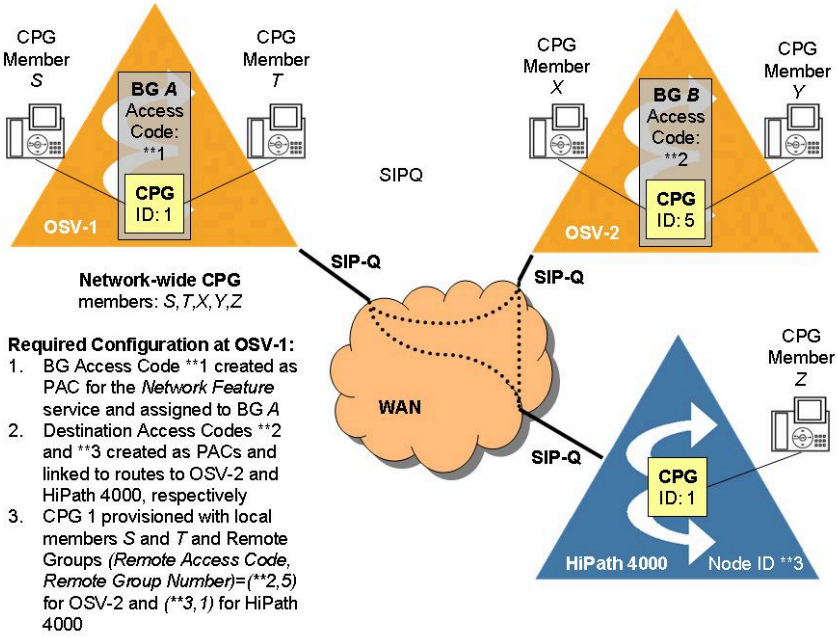
Remote groups may be assigned to only one local group.

Point-to-Point Scenario (Example)

The following figure displays an example for a network-wide CPG, spanning across two OpenScape Voice switches (OSV-1 and OSV-2) and a OpenScape 4000:

- Subscribers S and T are located at CPG 1 in BG A of OSV-1
- Subscribers X and Y are located at CPG 5 in BG B of OSV-2
- Subscriber Z is located at CPG 1 of OpenScape 4000

In order to provison the network-wide CPG, the BG Access Codes and Destination Access Codes have to be configured at both OSVs.



Required Configuration at OSV-1:

1. BG Access Code **1 created as PAC for the *Network Feature* service and assigned to BG *A*
2. Destination Access Codes **2 and **3 created as PACs and linked to routes to OSV-2 and HiPath 4000, respectively
3. CPG 1 provisioned with local members *S* and *T* and Remote Groups *(Remote Access Code, Remote Group Number)=(**2,5)* for OSV-2 and *(**3,1)* for HiPath 4000

Figure 36: Network-wide CPG (Example)

Tandem Scenario (Example)

The following figure displays an example for an OpenScape Voice acting as a (true) tandem node for calls related to a network-wide CPG. Even though the tandem node is not part of the CPG, the access code routing has to be enabled.

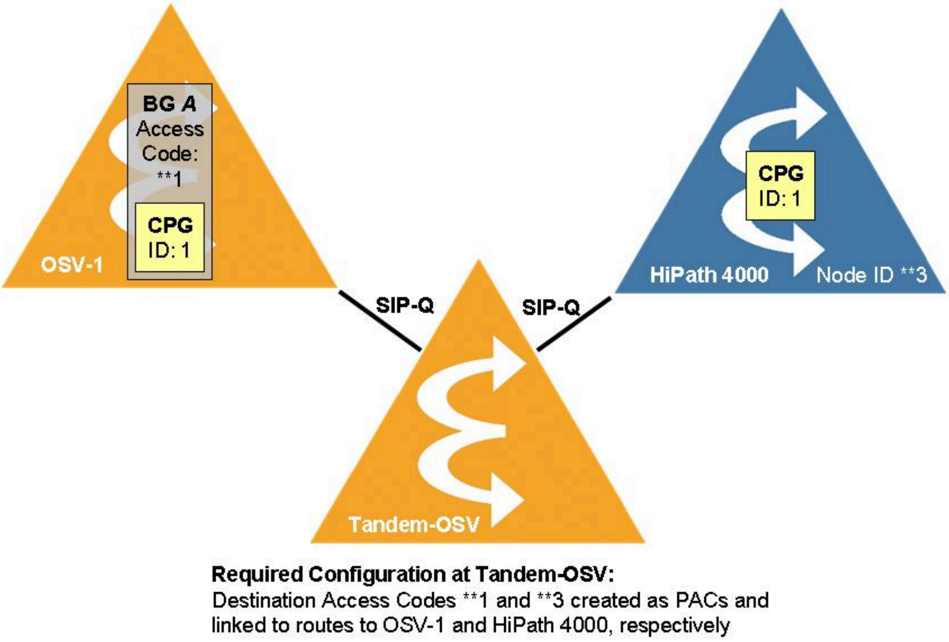

BG A
Access
Code:
**1
CPG
ID: 1
OSV-1
CPG
ID: 1
HiPath 4000
Node ID **3
SIP-Q
SIP-Q
Tandem-OSV
Required Configuration at Tandem-OSV:
Destination Access Codes **1 and **3 created as PACs and
linked to routes to OSV-1 and HiPath 4000, respectively

Figure 37: Network-wide CPG - Tandem Scenario (Example)(

HiPath DX Remote Groups

A network-wide pickup group owned by OpenScape Voice works in dual mode:

- For local subscribers and any remote group which are not located in HiPath DX.
- For HiPath DX remote groups.

The main difference between HiPath DX and HiPath 4K regarding the group pickup feature is HiPath DX does not support Group Indication On/Off feature. OSV does not send Group Indication On/Off to HiPath DX remote groups and does not receive such notifcation from these remote groups. Instead, members of this group must depend on being within hearing distance of a group pickup member that is ringing to indicate that a group pickup is possible.

Moreover when an OSV group member is ringing and a remote DX group member attempts to pick up the call, OSV assigns this caller the group pickup of a ringing user. On the other hand, when a remote group member is ringing and an OSV group member attempts pickup, OSV searches for a local ringing group member. If it finds none, each HiPath DX remote group is serially receiving the pickup request until it is accepted or the last remote group member node rejects the request.

4.4.2 Directed Call Pickup

The Directed Call Pickup feature, sometimes known as Call Pickup - Directed, provides subscribers the capability to answer any ringing, manually held or camped-on station within the business group.

For example, this feature is useful if a subscriber is expecting a call, but will be out of the office for a few minutes. During that time, another subscriber can answer the unavailable subscriber’s calls from his or her own station.

If the picking subscriber is in a call, he can add the picked-up line to the call, creating a 3-way conference. Adding the picked-up line to an existing conference is also possible.

Functional Operation

The administrator provisions the subscriber for Directed Call Pickup and creates a DIR-PICKUP key on the user's OpenScape Desk CP phone or defines a Prefix Access Code (PAC) for this service.

To perform a Directed Call Pickup, the picking subscriber can do one of the following:

- Press the DIR-PICKUP key and enter the internal number of the target station
- Press the right arrow key to access the context menu, then follow the prompts
- Dials the "Call Pickup Directed" PAC and enter the internal number of the target station

If a call was put on **manual hold on a shared line**, then on every keyset that has an appearance of this line, Directed Call Pickup can also be accomplished by pressing the DIR-PICKUP key followed by the target line key (provided that the primary line was provisioned for Directed Call Pickup) or by dialing the "Call Pickup Directed" PAC followed by the internal number of the target station.

Keyset-specific Use

Keyset users can employ the Directed Call Pickup feature to move a call from one line to another, which is a typical requirement in Executive/Assistant arrangements. Consider, for instance, the following scenario:

- A secretary has a keyset with a primary line and a secondary line for her executive
- A PSTN user makes a call to the executive's DN; the secretary answers the call using the executive's line appearance
- The secretary then decides to move the call from the executive's line to her primary line. In order to achieve this, she proceeds as follows:
  - Puts the call on the executive's line on manual hold
  - Presses the line key for her primary line, followed by the DIR-PICKUP key, followed by the line key for the executive's line or Dials the "Call Pickup Directed" PAC and enters the internal number of the executives's line.

4.4.3 Night Bell Call Pickup

The Night Bell Call Pickup feature permits alternate routing of inbound calls to a predefined CPG (Call Pickup Group) such that everyone in the building can hear the alerting call, and can answer the incoming call from any SIP endpoint. Each BG (Business Group) can have a single Night Bell CPG.

Because this feature is assigned to the BG as a whole, it can be used by all business group members and does not require pickup group membership.

The Night Bell Call Pickup feature doesn't interfere with the ability to assign Call Pickup to lines in the BG. There are different access codes defined and used.

In order to provide the Night Bell Call Pickup feature, the administrator has to perform the following tasks:

1) Create a Call Pickup Group that comprises all night bell lines.
2) If multiple bells are to ring simultaneously, assign the Simultaneous Ringing feature to one of them ("Line A"), with the other lines placed into its Simultaneous Ringing list.

> **NOTICE:**
>
> Note that this limits the size of a Night Bell Call Pickup group to the maximum size of a Simultaneous Ringing list.

3) Assign the Night Bell Call Pickup service to the BG, pointing to the previously created Call Pickup Group.
4) Assign a Night Bell Call Pickup access code: this is a PAC (Prefix Access Code) for the vertical service **Night Bell CPU**
5) Optionally, assign a function key on the users' phones

Typically, "Line A" of the Night Bell Call Pickup group will be assigned as the Night Service DN for a MLHG (Multiline Hunt Group), e.g. the MLHG for the attendants in a BG. However, other subscribers could also individually forward calls to "Line A" of the Night Bell Call Pickup group.

Related concepts

Feature Profiles on page 135
Simultaneous Ringing on page 278
Feature Access Codes for Call Pickup
Hunt Groups
Night Service on page 324

4.4.4 Feature Access Codes for Call Pickup

Feature Access Codes enable subscribers to initiate Call Pickup from their endpoints. A Feature Access Code can either be dialed or it can be assigned to a function key on the subscribers' phones, providing seamless access to server-side features.

The required access codes are usually created during the initial installation of the OpenScape Voice system; however, additional codes can be added at any time.

Technically, a Feature Access Code is a special instance of a PAC (Prefix Access Code), defining a sequence of keys (0-9, #, *) that enable callers to invoke a specific server-side feature. It can be created either globally (i.e. in the Global Numbering Plan) or locally (i.e. in a Private Numbering Plan). In OpenScape Voice Assistant such a "Feature PAC" has to be created with

- Prefix Type: Vertical Service
- Nature of Address: Unknown
- Destination Type: Service

and one of the available Service destinations.

Table 31: Call Pickup related Service destinations

Feature	Action	Service	Example PAC
Call Pickup Group	initiate call pickup	Call Pickup Orig	*22
Night Bell Call Pickup	initiate call pickup	Night Bell CPU	*38
Directed Call Pickup	initiate call pickup	Directed Call Pickup	*74

4.5 Hunt Groups

A Hunt Group (HG), sometimes also referred to as Multiline Hunt Group (MLHG), permits the distribution of incoming calls to associated subscribers (members). If a member is busy or does not accept an incoming call, the call is automatically routed to another member of the hunt group.

The HG can be reached at a single DN, the so-called Pilot Number of the HG. A Hunt Group is uniquely identified by its Pilot Number, which cannot be changed after the Hunt Group has been created.

NOTICE:

It is also possible to assign a modifiable, descriptive name to each hunt group, which facilitates its identification in filters, lists, etc.

Pilot DN types

Possible Pilot DN Types:

- Master Hunt Group

  If the Pilot Number is related to a station (i.e. it is assigned to a SIP phone subscriber), the HG is also referred to as Master Hunt Group. The respective station is called Master Station and provides access to certain features that control the hunt group.
- Pilot DN

  If the Pilot Number is not related to a station (i.e. it is assigned to a profile-only subscriber) and is used only as an access number, the HG is also referred to as Pilot DN.

NOTICE:

If the Pilot DN is assigned to a Branch Office the Branch Office Name is populated in the respective MLHG field.

Hunting Types

The hunting types below have the relative hunting sequence:

- Circular Hunting

  An incoming call causes OpenScape Voice to progressively search for an idle station within the hunt group, starting with station position stored when the previous call to the hunt group was made. When a line is selected to complete a call to the group, the line that is one past it in the group is marked to become the starting point for the hunt on the next call to the hunt group. For example, if the last line in the group was chosen for the previous call, this is the first line in the group for the next call.
- Linear Hunting

  An incoming call causes OpenScape Voice to progressively search for an idle station within that hunt group. The hunting sequence starts with the first member and ends with the last member in the group. The first available member is chosen to present the call to.

  The calls are routed to the overflow destination only if the hunting passes the last group member and there either is no queue, the queue is full or the call has been queued for too long.
- UCD - Uniform Call Distribution

  OpenScape Voice routes an incoming call to the station within the hunt group that has been idle the longest.
- Parallel - Call Pickup Model

  All available members of the Hunt Group are alerted simultaneously (similar to a Call Pickup Group) whenever a new call arrives at the Hunt Group.

  NOTICE:

  When a subscriber is already a Member in a Hunt Group that has Type = "Parallel - Call Pickup Group Model", the subscriber cannot be also added as a Member in a Call Pickup Group (an error comes from soapServer preventing this action). Therefore, since the subscriber is not added as a Member in the Call Pickup Group, the action of sending the Group Pickup URI in dls is also prevented.

  NOTICE:

  The Parallel - Call Pickup Model type is currently not applicable for groups with their members being circuit users.
- Parallel – Simultaneous Alerting Model

  All available members of the Hunt Group are alerted simultaneously (similar to the Simultaneous Ringing feature) whenever a new call arrives at the Hunt Group.
- Manual – Application Controlled hunting

  OpenScape Voice does not perform the distribution of calls to agents, and all incoming calls are queued. For the distribution to work:

  – The hunt group must be provisioned as a pilot hunt group.

  – The Pilot Number must be marked for CSTA and must be monitored by a CSTA application, which allows an external application to be notified of calls going into the queue, and to subsequently retrieve (reroute) those calls.

For example, the Concierge application, which is now part of the OpenScape Voice solution, uses Hunt Groups provisioned for Manual Hunting to allow attendants to pick up waiting, unanswered or parked calls.

Conditional / Unconditional

The following two overflow handling "modes" are supported by OSV from V7 onwards for all hunting types except for the Manual – Application Controlled hunting:

- **Conditional**, where calls are routed to the overflow destination only if the hunting passes the last group member and there either is no queue, the queue is full or the call has been queued for too long.

  This is the traditional Linear Hunting mode.
- **Unconditional**, where calls are immediately routed to the overflow destination, if the hunting passes the last group member.

  This behavior is preferable if the overflow destination is again a Hunt Group, e.g. on another switch (network-wide Hunt Group).

  If no overflow destination has been provisioned, then the **Conditional** mode will be used.

Parallel - Call Pickup Model Hunt Groups distribution flow

Parallel - Call Pickup Model hunt group has the following restrictions:

1) A subscriber cannot be a member of a regular Call Pickup Group and a member of a parallel Hunt Group at the same time.
2) A subscriber cannot be a member of more than one Parallel - Call Pickup Model Hunt Groups.

Call distribution is performed as follows:

1) If there are members available and there is no other call being distributed, the procedure is:

   - Search for the next available HG member using the Circular algorithm.
   - Send the call to the selected member. If the call is not successful, find the next member using the Circular algorithm once again.
   - When the selected member receives the call, a Call Pick Up (CPU) notification is sent only to all other available members. The CPU notification indicates that this is a call to the MLHG Pilot DN.
   - Once the call is answered or picked-up and if there is a queue and at least one available agent, the next call in the list is being distributed.
2) If no HG members available, the processing of calls to the Parallel HG is the same as the existing Hunting Types. This means that the call may be queued, deflected to Overflow Destination, Deflected to Night Service DN or Rejected, all according to the HG configuration.
3) A parallel Hunt Group can only distribute one call at a time. Therefore, if a call arrives to the Hunt Group and there is already a call being distributed, the new call is handled as if there are no members available.
4) If a HG member becomes available while there is a distributed call alerting other members, a CPU notification is sent to the member that just became available.

INFO:

Direct calls to a HG member does not trigger any CPU notifications (i.e they are not presented to the other members). The CPU notifications are only sent for calls to the HG Pilot.

NOTICE:

All members must be subscribed to the Call Pickup Group feature.

Parallel - Simultaneous Alerting Model Hunt Group’s distribution flow

Parallel - Simultaneous Alerting Model (Parallel - SA) hunt group doesn’t have the restrictions of the Parallel - Call Pickup Model Hunt Group.

NOTICE:

Successful agent hunting for "Parallel – Simultaneous Alerting Model" MLHGs requires a successful call routing translation of the Pilot DN in the Pilot DN’s numbering plan. The translation starts in the Pilot's numbering plan using the full Pilot DN number (with type of number "Unknown") and is supposed to lead to the actual HomeDN of the Pilot number.

Call distribution is performed as follows:

1) Create a Parallel Alerting List (PAL) containing all available members of the group.
2) MLHG service invokes call setup to all PAL members, in a similar fashion to the Simultaneous Ringing Service. Parallel – SA does the following:
   - If the call setup to one or more PAL members fails then the member is released and alerting continues with the remaining PAL members
   - If the call setup fails on all members then all members are cleared and the call shall follow the overflow provisioned attributes provisioned for the group.
   - During Parallel - SA Hunt Group distribution if a PAL member’s phone invokes redirection (SIP 3xx) then MLHG shall release that member from the PAL.
   - Once the call is answered or picked-up and if there is a queue and at least one available agent, the next call in the list is being distributed.
3) If no HG members are available, the processing of calls to the Parallel - SA HG is the same as for the existing Hunting Types. This means that the call may be queued, deflected to Overflow Destination, Deflected to Night Service DN or Rejected, all according to the HG configuration.
4) A Parallel - SA Hunt Group can only distribute one call at a time. Therefore, if a call arrives to the Hunt Group and there is already a call being distributed, the new call is handled as if there are no members available.

NOTICE:

When the Pilot DN type is “Master Hunt Group” and the Type is “Parallel-Simultaneous Alerting Model” the connection type of Pilot DN should not be SIP but Profile-only

Busy Status

A hunt group is busy when one of the following conditions are present:

- There are no idle members in the group to present the call to, and there are no idle positions in the queue.
- It is in night service.

Upon determining busy, the sequence of treatment is as follows:

1) If the group is in night service, the call is routed to the night service DN.
2) Otherwise, if there is an associated queue with idle positions in the queue, queuing will be performed.
3) Otherwise, if Call Forwarding - Busy Line is active on the group via the pilot DN, the call is forwarded.
4) Otherwise, if an Overflow DN is present, the call is routed to it.,if an Overflow DN is not present then check if a Night Answer DN is provisioned and use that for overflow.
5) Otherwise, busy tone is given. This is the default.

Blocking Status

The blocking status of the hunt group and its members is determined as follows:

- If the pilot DN of the hunt group is dialed, only the blocking state of the pilot DN is checked. If the pilot DN is blocked, hunting does not occur - no matter what the blocking state of the group members is. If it is not blocked, normal hunting occurs.
- If a member's DN is dialed directly, the blocking state of the member’s DN is checked.

Networking

- All members of a hunt group must reside in the same Business Group.
- Calls delivered to members of pilot hunt groups cannot overflow or forward to a remotely located voice mail system.
- Calls originated by a hunt group member can route over a network interface.
- Calls arriving over a network interface can route to a hunt group interface.
- If the pilot line is associated to a PBX, all hunt group members must reside in this very PBX.

System-Specific Information

OpenScape Voice supports up to 25,000 hunt groups. Each hunt group can contain up to 2,048 stations. A station (DN) can be a member of up to 32 hunt groups. Although each station has its own DN, the system administrator can designate it as non-external.

4.5.1 Queuing

Each Hunt Group can optionally have an associated overflow queue to which calls are routed if there are no idle members in the group to present the call to. Queued calls are distributed to the next available line in the Hunt Group as it becomes available (on a first-in, first-out basis).

Queuing provides an enhancement to the basic Hunt Group overflow on busy treatment, modifying both the determination and handling of busy conditions for the group. See the Hunt Group feature description for details about how busy conditions are determined, along with the sequence of treatment upon determining busy.

When a Hunt Group line becomes idle, each group it belongs to must be searched to determine if there are any calls queued that can be processed by that line. The sequence to search the queues is based on the priority of the queues for that member, with the lower-numbered priorities checked before a higher-numbered priority queue. Queues with the same priority can be checked in any sequence.

If the optional Maximum Time in Queue is not specified, a call remains in queue until either the caller abandons or a Hunt Group member becomes idle and the call is distributed. If it is specified, a call remains in the queue only for that maximum duration.

The sequence of treatment upon exceeding that duration in queue is as follows:

1) If there is an overflow DN, the call is routed to it.

2) Otherwise, if there is a night service DN, the call is routed to it.

3) Otherwise, busy tone is given.

The administrator can specify the following for each Hunt Group queue:

- Maximum number of callers that can be simultaneously queued (up to 511)
- Audible treatment heard by a caller while in queue (for example, customizable sequences of ringing, music, announcements, or combinations of these items). A media server is required to provide the audible treatment.
- Maximum time in queue threshold (0 [unlimited time] up to 43,200 seconds [12 hours]). This value is optional.

NOTICE:

It is possible to obtain the calling party information of a queued call via CSTA (Computer Supported Telecommunications Applications).

Related concepts

Overflow on page 320

Night Service on page 324

4.5.2 Overflow

The Overflow feature permits an overflow DN to be assigned to a Hunt Group. This DN is used as destination DN to which unanswered incoming calls are sent when the queue is full.

By assigning an Overflow DN, the administrator modifies the treatment of busy handling within the group, providing a fixed destination for routing the call.

Since OpenScape Voice Version 5 the overflow destination of a *linear* hunt group can not only be a local number (required in earlier releases and still required for other routing algorithms), but can be located in the SIPQ network. Any network routable number (with or without prefix digits depending on number modification rules) is accepted. For other destinations, OpenScape Voice returns an error for an invalid number.

Related concepts

Queuing on page 320

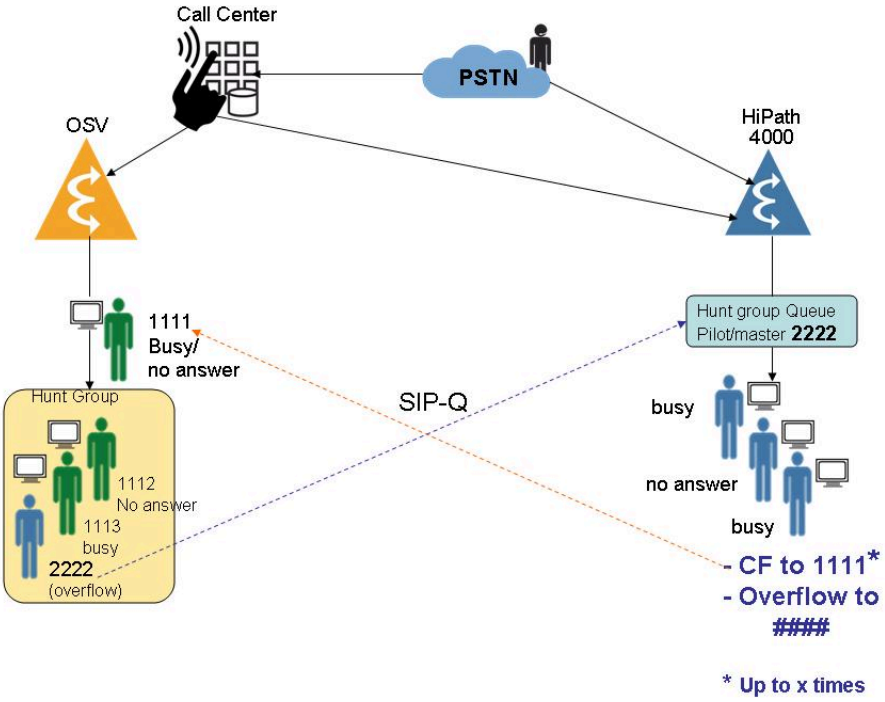
Accounting on page 324

RTP System Parameters on page 327

4.5.3 Network-wide Hunt Groups

Since Version 5 the overflow number in an OpenScape Voice Hunt Group can be a destination in the private SIP-Q network, e.g. a master or pilot hunt group in a OpenScape 4000.

An option for the linear hunting type to be subject to conditional (i.e. legacy) or unconditional (i.e., no conditions placed on advancement) operation is provisionable. This type of call distribution is used widely by call centers.



4.5.4 Make Busy

The Make Busy feature permits a station to appear busy to incoming calls that hunt to the line. Calls to a line's non-hunt DN are still permitted, as are call originations.

To activate the make busy feature, the subscriber goes off-hook, receives a dial tone, and either enters the correct activation access code or presses the Hunt Make Busy key. When the subscriber goes on hook, the call is released. If the subscriber used an access code for the activation, OpenScape Voice also provides an announcement to confirm the activation.

To deactivate the make busy feature, the subscriber goes off-hook, receives a dial tone, and either enters the correct deactivation access code or presses the Hunt Make Busy key again. When the subscriber goes on hook, the call is released. If the subscriber used an access code for the deactivation, OpenScape Voice also provides an announcement to confirm the deactivation.

The subscriber can also enter the make busy toggle access code to switch back and forth between activated and deactivated status.

Auto Make Busy

Make Busy feature is also activated when the Auto Make Busy option is chosen and the **No Answer Advance Timer** expires.

If the hunting type is **Parallel - Call Pickup Model** or **Parallel – Simultaneous Alerting Model**, only the member that received the actual call is made busy. All other members that receive Call Pick Up notifications are available.

The feature only works for Hunt Group Members that have the **Can make the hunt group bus** option set.

4.5.5 Post Call Timer

The **Post Call Timer** option allows the administrator to define the period of time (max 43200sec) before a hunt group member can receive a new call after releasing the previous call.

NOTICE:

If the hunting type is **Parallel - Call Pickup Model** or **Parallel – Simultaneous Alerting Model** the **Post Call Timer** is also applicable for scenarios where the member “answers” the call via Call Pickup.

4.5.6 Send Pilot’s Display Information to Hunt Group Members

This feature allows you to send the Pilot’s display information to the Hunt Group members when a call is hunted.

NOTICE:

If the hunting type is **Parallel - Call Pickup Model** or **Parallel – Simultaneous Alerting Model** the **Post Call Timer** is also applicable for scenarios where the member “answers” the call via Call Pickup.

If this feature is activated, the SIP INVITE message towards the Hunt Group members shall contain a Diversion header-field with the Pilot’s Name and

Number. This will affect the display on the member’s phone in case it supports the Diversion header field, like the OpenScape Desk CP phones.

Example

For instance, consider a call from 815615551234 to a Hunt Group Pilot with Name=“Sales” and Number = 51000. In this case, the display on the Hunt Group member’s OpenScape Desk CP phone would be as follows:

- If the feature is inactive:

  815615551234
- If the feature is active:

  815615551234 -->51000 Sales

4.5.7 Stop Hunt

The stop hunt feature provides the ability to terminate all hunting within the group when encountered on an authorized member of the hunt group. It is checked during the hunt before moving to the next line in the hunt sequence. Calls to a line’s private DN are still permitted, as are call originations.

To activate the stop hunt feature, the subscriber goes off-hook, receives a dial tone, and enters the correct access code or presses the Stop Hunt key.

To deactivate the stop hunt feature, the subscriber goes off-hook, receives a dial tone, and enters the correct access code or presses the Stop Hunt key again.

The subscriber can also enter the stop hunt toggle access code to switch back and forth between activated and deactivated status.

NOTICE:

If the hunting type is **Parallel - Call Pickup Model** or **Parallel – Simultaneous Alerting Model** the Stop Hunt feature is ignored.

4.5.8 No Answer Advance

The No Answer Advance feature is assigned to each Hunt Group’s pilot DN. When a hunted-to station does not answer, this feature causes a resumption of the hunt from the non-answering station’s position following the defined hunt sequence for the group.

This treatment can occur multiple times during the same termination attempt. Each time a call hunts to an idle line, the No Answer Advance timer is set, which permits the feature operation to occur upon a subsequent no-answer. When the No Answer Advance feature is assigned, Auto Make Busy is allowed as an option. When it is assigned, a non-answering line subscribed to the hunt make busy feature is automatically marked Hunt Make Busy.

NOTICE:

If a hunt group is configured for manual hunting and the pilot DN is monitored by a CSTA application, No Answer Advance does not occur when a queued call is deflected to a hunt group member.

Parallel - Call Pickup Model Hunt Group / Parallel – Simultaneous Alerting Model Hunt Group

If the hunting type of the Hunt Group (HG) is set to **Parallel - Call Pickup Model** or **Parallel – Simultaneous Alerting Model**, the No Answer Advance timer defines the duration for which a distributed call alerts the HG members. If this timer expires, the call is immediately moved to the Overflow Destination. If there is no Overflow Destination configured the call is dropped.

4.5.9 Accounting

The CDRs (Call Detail Records) generated by OpenScape Voice provide rich information about calls to a MLHG (Multiline Hunt Group). They allow to reconstruct the related calls, i.e. to have complete knowledge of each call from the time it enters the hunt group until it is successfully handled or missed.

The following details are available:

- MLHG calls are marked with an MLHG flag in the "per call feature extension"
- The "destination party" field contains the number of the hunt group member that answered the call or the party that picked up the call via Call Pickup.
- If the alerted member does not answer, an additional CDR is created before the call advances to the next available member. This additional CDR shall be marked with a new "MLHG advance no answer" flag in the "Call Event Indicator" field. The "destination party" field contains the currently alerted member, i.e. the member who missed the call.
- If a call to a MLHG overflows, an additional CDR is generated. This additional CDR is marked with a new "MLHG overflow" flag in the "Call Event Indicator" field, contains the overflow DN in the "destination party" field and the MLHG pilot DN in the "called party" field.
- If a MLHG call is forwarded to Night Service, the CDR for the forwarded call contains a "MLHG Night Service" flag indicating that this was originally an MLHG call.
- The field "Total Hold Time" in the CDR which contains the total time the call was on hold in tenths of a second. If the held party hangs up while on hold, a "held party hung up" flag shall be set in the "Call Event Indicator" field in the CDR. If the holding party hangs up while the other party is on hold, a new "holding party hung up" flag shall be set in the "Call Event Indicator" field in the CDR.

Related concepts

Overflow on page 320

Night Service on page 324

4.5.10 Night Service

The night service feature permits to route calls to predefined night stations or other answering devices - for example, to voice messaging, to an automated attendant application, or to a night bell device.

The administrator specifies the night service DN.

The feature can be activated by either or both of the following methods:

- *Automatic activation*:

  This takes place when all members of the hunt group are in "make busy" state.
- *Manual activation*:

  This takes place when the administrator activates the feature.

Night answering positions have the capability to:

- Extend calls to other destinations within the private network or to external destinations
- Camp on to busy stations
- Be recalled
- Access external trunk resources

The following are other characteristics associated with this feature:

- Authorized users can pick up calls alerting at night service destinations.
- Although calls alerting at night answer destinations are not prioritized by OpenScape Voice, prioritization may occur within applications monitoring night calls queued at hunt groups.

Related concepts

Night Bell Call Pickup on page 313

Queuing on page 320

Accounting on page 324

4.5.11 Subscriber Rerouting Interaction

A HG (Hunt Group) can be configured to allow three Subscriber Rerouting options to take place for its members. If any of the Subscriber Rerouting options is allowed it will take precedence over the HG distribution logic, otherwise only the HG distribution logic is applied.

The following Rerouting options are available for HG:

- **Enhanced Subscriber Rerouting**

  Enhanced Subscriber Rerouting will be attempted in case a distributed call to a Hunt Group member is rejected due to Call Admission Control before advancing to the next member.

  NOTICE:

  It SHALL NOT be possible to enable the **Enhanced Subscriber Rerouting** for Hunt Groups with Hunting Type set to **Parallel - Call Pickup Model** or **Parallel – Simultaneous Alerting Model**

  NOTICE:

  A Hunt Group is NOT allowed to have the Enhanced Subscriber Rerouting activated if the call to the agent is deflected to an OND which is a registered phone and ONS is not equal to OND. This rule is independent on how RTP parameter *Srx/Main/AllowSubsReroutingForOND* is set.

- **Basic Subscriber Rerouting**

  Basic Subscriber Rerouting will be attempted in case a distributed call to a Hunt Group member is rejected due to Call Admission Control or WAN Failure. The default value for this parameter shall be disabled before advancing to the next member.

  NOTICE:

  It SHALL NOT be possible to enable the **Basic Subscriber Rerouting** option for Hunt Groups with Hunting Type set to Hunting Type set to either **Manual**, **Parallel - Call Pickup Model** or **Parallel – Simultaneous Alerting Model**.

- **Overflow Destination if No Rerouting**

  An Overflow destination is defined in case a distributed call to the Hunt Group member is rejected due to Call Admission Control or WAN Failure AND Subscriber Rerouting (Enhanced or Basic) either fails or is not allowed before advancing to the next member.

  NOTICE:

  The **Overflow Destination if No Rerouting** option is applicable for distributed calls to all Hunt Group members. It is not exclusive for calls distributed to the last Hunt Group member.

NOTICE:

If the HG is provisioned to allow any of the above Subscriber Rerouting options, the Subscriber Rerouting will only take place for members that are provisioned for Subscriber Rerouting.

If none of the three available rerouting options are not provisioned to the HG, Subscriber Rerouting will not be attempted - even for HG members that are provisioned for Subscriber rerouting.

4.5.12 No Intercept Announcement (Local Ring Back)

The No Intercept Announcement feature allows calls queued in an MLHG to receive a local ring back response from the MLHG service. On direct calls to the hunt group, when this option is active, no announcement is provided from the OSV platform media server toward the queued party. Instead the queued party will hear local ring back provided by the network or subscriber device.

When configured for local ring back, the MLHG does not seize any media server circuits for the purpose of providing ring back or any other announces. Instead the MLHG service provides the local ring back to the queued party, if only the No Intercept Announcement feature is enabled.

When activated the following features are disabled for this MLHG:

- Intercept Announcement
- Queue Position Announcement Interval
- Queue Position Announcement

4.5.13 RTP System Parameters

Certain aspects of the Hunt Group service are controlled on a systemwide basis by RTP (Resilient Telco Platform) system parameters. Any changes made to these parameters affect all business groups and their members. Typically, these parameters are set during initial system configuration, to enforce global system policies and ensure proper feature interworking.

For example, the following properties can be modified by setting RTP system parameters:

- The maximum number of Hunt Groups
- The maximum total number of Hunt Group members

The following table presents the Hunt Group related RTP system parameters. Default values are shown in bold type.

Table 32: RTP System Parameters related to Hunt Groups

Parameter	Values	Description
Srx/Mlhg/ maxMlhgTblSize	0-15,000,000 (15,000,000)	This parameter defines the hunt group table size in the hunt group shared memory. In order to support the maximum number of hunt groups in a system (25,000), this parameter must be set at 15,000,000. Note: The UCE processes must be restarted in order for the MLHG service to implement the new values.
Srx/Mlhg/ maxMlhgTermTblSize	0-70,000,000 (**70,000,000**)	This parameter defines the hunt group terminal table size in the hunt group shared memory. In order to support the maximum number of hunt group members in a system (150,000), this parameter must be set at 70,000,000. Note: The UCE processes must be restarted in order for the MLHG service to implement the new values.
Srx/Mlhg /mlhgCACRetryTimer	30-unlimited (**60**)	This parameter defines the time in seconds when call admission control (CAC) restriction without rerouting occurs on a selected hunt group member.
Srx/Mlhg/ MLHGOverflowMaxDiversions	1-**720**	This parameter defines the maximum number of redirections to MLHG overflow DN that are allowed for a call. The MLHG service will disallow a redirection to the configured overflow DN when the maximum value has been reached.

Related concepts

RTP Management via OpenScape Voice Assistant on page 961

Overflow on page 320

4.5.14 Feature Access Codes for Hunt Groups

Feature Access Codes enable Hunt Group members to influence the hunting logic from their endpoints. A Feature Access Code can either be dialed or it can be assigned to a function key on the members’ phones.

The required access codes are usually created during the initial installation of the OpenScape Voice system; however, additional codes can be added at any time.

Technically, a Feature Access Code is a special instance of a PAC (Prefix Access Code), defining a sequence of keys (0-9, #, *) that enable callers to invoke a specific server-side feature. It can be created either globally (i.e. in the Global Numbering Plan) or locally (i.e. in a Private Numbering Plan). In OpenScape Voice Assistant such a "Feature PAC" has to be created with

- Prefix Type: Vertical Service
- Nature of Address: Unknown
- Destination Type: Service

and one of the available Service destinations.

Table 33: Hunt Group related Service destinations

Feature	**Action**	Service	Example PAC
Make Busy	activate	Make Busy Activate	*26
	deactivate	Make Busy Deactivate	*27
	toggle	Make Busy Toggle	*28
Stop Hunt	activate	Stop Hunt Activate	*24
	deactivate	Stop Hunt Deactivate	*25
	toggle	Stop Hunt Toggle	*29

Related concepts

Make Busy

4.6 SILM (Silent Monitoring)

The SILM feature allows executives or supervisors with sufficient privileges to silently listen to an audio call or conference that a subscriber to be monitored participates in. Once in a silent monitoring session, the executive or supervisor can either barge into the conversation (via CSTA or feature key) or terminate the monitoring without affecting the ongoing conversation. It is also possible to barge in without prior "passive" monitoring.

The displays of the monitoring party (supervisor(s)) shall show the monitored party’s name and number even if the monitored party has name and/or number presentation restricted (either permanent restriction or per-call restriction) during the entire duration of the monitoring session.

NOTICE:

The target subscriber is not informed about being silently monitored during the lifetime of the call. This might be prohibited by applicable law.

NOTICE:

When **Silent Monitoring** is invoked, no features assigned to the monitored party (e.g. DND, CFW, SR, SRS, CPU, CW) are invoked.

SILM restrictions

Note that Silent Monitoring of an ONS subscriber requires the CSTA variant.

The SILM features make use of the following information to allow device monitoring:

1) both monitoring subscriber and monitored subscriber reside on the same OpenScape Voice switch and within the same BG
2) SILM is enabled at the BG level
3) the monitoring subscriber is provisioned with the SILM service
4) the subscriber to be monitored is not protected from monitoring

IMPORTANT: SILM may fail for a number of reasons, including bandwidth limitation, media server resources, execution of call control services that do not interact with Silent Monitoring. In any case, the original call is not affected and the monitoring device is played a prompt or an error tone and is dropped gracefully.

The Role of the Media Server

The monitored call will be mediated through the media server:

- monitoring a basic call (one monitored party) requires five (5) conference connections.
- monitoring a conference calls requires one additional connection for each monitoring entity (supervisor, recording device) added to an existing monitoring session.

Following Silent Monitoring solutions/options are supported in OSV Version 7 onwards:

Passive Silent Monitoring

This mode of silent monitoring uses the **Silent Monitoring Tagging** option when configuring the **Silent Monitoring Agent** feature and it forces the payload go through the Media Server. This mode is used by passive recording solutions like HiCorder.

Continuous Silent Monitoring

This solution may be used by supervisor(s) and recording applications. The supervisor (or recording device) follows the active call of the agent – e.g. consultation, alternate, conference. **Continuous Silent Monitoring** session shall remain active until it is terminated by the supervisor (or the recording device).

The Continuous Silent Monitoring can be invoked by :

- using the Silent Monitoring Prefix Access Code (PAC) from a the supervisor's phone or from a SIP recording device .
- a CSTA application using the *JoinCall Service*

Per Call Silent Monitoring

This way of monitoring can ONLY be invoked via CSTA . When the Per Call Silent Monitoring is used, the agent will be monitored ONLY while he is in a stable call. This way of monitoring is used by ASC solutions.

Multiple Monitoring Parties Per Agent

An agent can simultaneously be monitored by one or more Supervisors and one or more Active Recording devices.

Multiple Monitoring Parties Per Call

Two monitored agents are being simultaneously silently monitored by their supervisors and/or their recording devices.

Barge-In

Supervisor has the ability to barge-in (either transitioning from silent monitoring mode or via a new call) on the monitored agent's call. The result shall be a Large conference with the agent the supervisor and other party where each one is allowed to bring new parties in the conference.

Barge-in solution is activated with one of the following ways:

- The supervisor can barge-in in the agent's call by initiating a call towards the SILM Barge-In Prefix Access Code (PAC)
- Activation via CSTA in which the the supervisor can barge-in in the agent's call in two ways:

  - *JoinCall* service request with participation type active

  or

  - *ChangeConnectionInformation* from an existing Silent Monitoring session

  > **NOTICE:**
  >
  > Transition form Barge-In to Silent is not allowed.

- Activation via Toggle Key in which the supervisor that is silently monitoring an agent, he/she can press a predefined Toggle Key to barge-in in the call.

Tone Monitoring

This solution allows you to configure initial and periodic tones that are applied to all parties (monitored party and partner) in the call during a silent monitoring session.

This is configured in the Silent Monitoring Agent feature and on a subscriber basis.

4.6.1 On-demand and Continuous Recording

SILM can also be used for on-demand and continuous recording of conversations and (encrypted) conferences.

On-demand recording can be activated from the recording device by dialing a silent monitoring feature access code and the directory number of the line to be monitored.

In order to support on-demand and continuous recording *via a third party application*, the recording device as well as the monitored device have to be provisioned as CSTA-enabled subscribers. A third party application may invoke recording from the recording device whenever the CSTA events indicate that the line intended to be monitored is active in a call. Note that the recording device will be activated on a per call basis and continuous monitoring is possible only from a third party application.

4.6.2 SILM Service Provisioning

The SILM service has to be provisioned both at the BG (Business Group) and at the subscriber level. Furthermore, the Feature Access Codes for monitor/barge-in have to be created in the affected numbering plans and/or CSTA has to be activated for the monitoring subscribers.

BG Level Provisioning

At the BG level, SILM can be globally activated or deactivated.

- If deactivated, SILM will not be available for this BG.
- If activated, it is possible to define the maximum number of subscribers that may be provisioned with the *Tagged for Monitoring* flag; see below for details. When an administrator attempts to tag a subscriber, the system will check if the current number of monitored tagged subscribers within the BG exceeds the limit, in which case the attempt will fail.

For untagged subscribers, a basic call is not established via the media server. The call will be mediated through the media server as soon as silent monitoring is requested.

For tagged subscribers, even basic calls are established via media server mediation, which will make a subsequent silent monitoring activation more reliable: the monitoring party is simply added to the media server conference bridge as a listen only partner.

NOTICE:

In order to ensure optimal operation, it is recommended that the **Maximum Number of Subscribers Tagged for monitor** shall be set to a value of no more than 20% of the total media server conference channels available to the BG.

Filter for Silent Monitoring Subscribed Features

Subscribers search for Subscribed Feature drop down list includes the following Silent Monitoring features

- *Silent Monitoring Supervisor*
- *Silent Monitoring Agent*

Silent Monitoring Whisper

The Silent Monitoring Whisper feature is a similar mode to the Continuous Silent Monitoring feature, which enables the supervisor (the monitoring party) to "whisper" to the agent (the monitored party) while being already in a silent monitoring condition. In order for the Whisper to be successful the following preconditions must be met:

- Supervisor is authorized with Whisper attribute of Silent Monitoring Supervisor feature.
- Agent is provisioned with Whisper-To attribute of Silent Monitoring Agent feature.
- Supervisor has established a Continuous Silent Monitoring Session against the Agent.
- Agent is in a stable active two party call or is actively participating in a large conference call.

A privileged OSV subscriber is silently monitoring another OSV subscriber who is involved in an active call with a third party. At the same time, the privileged OSV subscriber can escalate to Whisper feature and "whisper" in the monitored OSV subscriber’s earpiece without the third party being able to detect it. The whispering party is able de-escalate the Whisper feature and automatically return to the silent monitoring state or terminate the silent monitoring session by disconnecting.

The Whisper feature is required in call centers where the Supervisor may wish to "whisper" to the monitored Agent for coaching purposes. This feature is also required in Executive/Assistant scenarios where the executive can "whisper" in the assistant’s earpiece without the other party being able to detect it.

The Whisper feature can be invoked from the phone via a feature key while in continuous silent monitoring session. By pressing the same key, the user is able to return to the continuous silent monitoring. It will also be possible to alternate several times from silent to whisper mode and vice versa. The feature can also be invoked from CTI application (via CSTA) while in a silent monitoring session and toggle (using a whisper feature access code) between whisper and silent mode.

NOTICE:

The Whisper feature access code can be only used by pressing the feature toggle key. An attempt to dial the whisper feature access code will be rejected.

Additionally, several advisors can invoke whisper concurrently while silent monitoring the same monitored party. The "whispering" can be heard by all silent monitoring and whispering parties as well as the monitored party but it will not be heard by the other party. Supervisors that monitor one party of the call and supervisors that monitor the other party of the call can also simultaneously whisper to both monitoring parties.

Similarly to the silent monitoring session, the displays of the agent will not be affected when whisper is invoked against him/her. In addition, the displays of the supervisor will continue showing the agent’s name and number even if the agent has name and/or number presentation restricted.

When the monitored party’s call is released or becomes inactive (agent places the call on hold or is placed on hold by the other party) the supervisor will be returned automatically from whisper to silent mode.

IMPORTANT:

For information regarding enabling the Whisper Mode, please refer to chapter “How to Enable the Whisper Mode for all cnf-Circuits” of the document *OpenScape Media Server, Administrator Documentation*

4.6.3 Feature Access Codes for SILM

Feature access codes enable subscribers to start SILM (Silent Monitoring) or barge in to an existing call or conference from their endpoints. A feature access code can either be dialed or it can be assigned to a function key on the subscribers’ phones, providing seamless access to server-side features.

The required access codes are usually created during the initial installation of the OpenScape Voice system; however, additional codes can be added at any time.

Technically, a Feature Access Code is a special instance of a PAC (Prefix Access Code), defining a sequence of keys (0-9, #, *) that enable callers to invoke a specific server-side feature. It can be created either globally (i.e. in the Global Numbering Plan) or locally (i.e. in a Private Numbering Plan). In OpenScape Voice Assistant such a "Feature PAC" has to be created with

- Prefix Type: Vertical Service
- Nature of Address: Unknown
- Destination Type: Service

and one of the available Service destinations.

Table 34: SILM (Silent Monitoring) related Service destinations

Action	Service	Example PAC
start "passive" silent monitoring	SILM Monitor	*72
start "active" silent monitoring	SILM Barge-in	*73

Related concepts
SILM Service Provisioning

4.7 Executive/Assistant Groups

The Executive/Assistant (E/A) Group feature allows executives to streamline their calling processes with the support of one or more assistants. Assistants control and manage calls for executives, providing support with a great degree of flexibility, but without compromising privacy.

One or more assistants can answer all incoming calls, handling them exactly as the executive wants.

In some E/A configurations, incoming calls for the executive are directly forwarded to the assistant, where they are answered, put on hold, or transferred to the executive's line.

In other E/A configurations, both the executive and assistant are signaled simultaneously. The assistant handles calls for the executive using shared line appearances of the executive.

In all E/A configurations, the assistant can monitor all incoming calls on the telephone with an acoustic or visual signal and react accordingly. Executive and assistant may sit at different locations, far away from each other, and still communicate without any restriction or loss of functionality.

NOTICE:

The standard E/A configurations require the use of OpenScape Desk Phone CP 400, CP 600, CP 600E, CP 700 or CP 700X endpoints.

Basic Features

All E/A Group configurations offer the following features:

- The assistant can activate or deactivate the OpenScape Voice-based Unconditional Call Forwarding for the executive's primary line (Call Forwarding - Remote Activation feature).

  If Unconditional Call Forwarding is activated in an E/A arrangement, all incoming calls for an executive are forwarded to an assistant's primary line.
- Incoming calls for the executive are signaled (acoustically and visually) at the assistant's telephone.
- An incoming call for the executive is usually answered by the assistant and then transferred to the executive's primary line.
- Signaling of a camped-on call on the executive's telephone is via the assistant's telephone only.
- Activation of the Call Completion on Busy Subscriber/No Reply (callback) function when the executive's telephone is free.
- If the executive is busy, the assistant can put a call on manual hold until the executive is ready to take it.
- If the executive's primary line is represented as a secondary line appearance on the assistant's telephone, the assistant sees the status (idle, busy, ringing, or hold) of the executive's telephone at all times. This makes

it possible for the assistant to react in different ways depending on the executive's preferences.

4.7.1 E/A Arrangements

E/A (Executive/Assistant) Groups can be deployed in various arrangements, limited to a maximum of four executives and two assistants.

The following figure introduces the standard E/A arrangements supported by OpenScape Voice. These configurations can be set up easily using the OpenScape Voice Assistant's E/A Wizard.

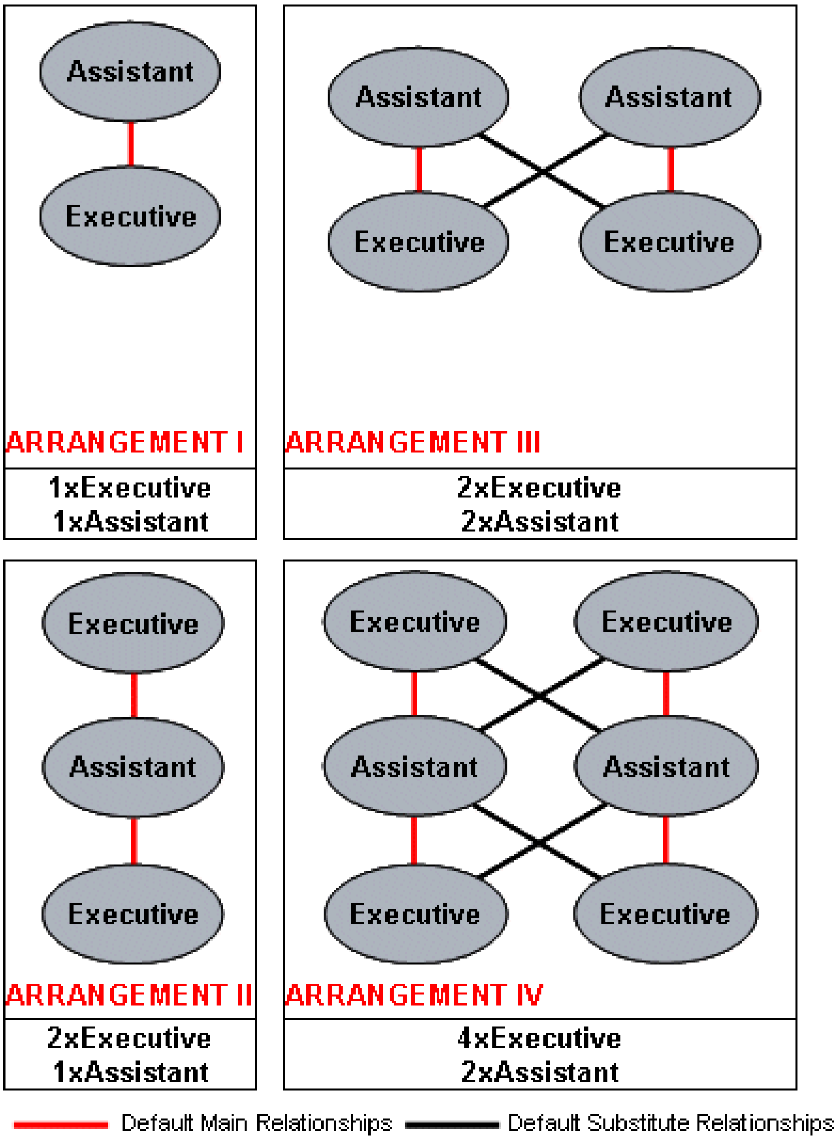


Figure 38: Typical Executive/Assistant Arrangements

Larger E/A Groups are technically feasible but unsupported by the E/A Wizard. They require extensive manual configuration at OpenScape Voice, the DLS (Deployment Service) and the related OpenScape Desk CP phones. They can be provided on a project-specific basis.

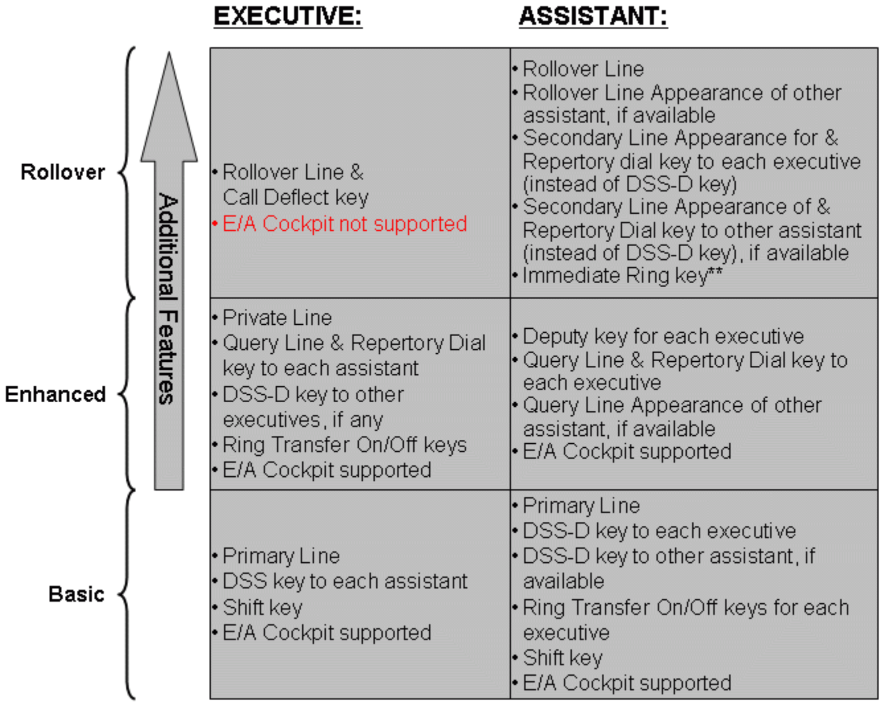
Related concepts

E/A Wizard on page 340

4.7.2 Standard E/A Configurations

The E/A (Executive/Assistant) arrangements can be implemented in several ways that differ in their functionality and flexibility, allowing enterprises to choose the configuration for each executive that best meets that executive's needs.

The following figure introduces the standard E/A configurations supported by OpenScape Voice. These configurations can be set up easily using the OpenScape Voice Assistant's E/A wizard.



Additional Features

	EXECUTIVE:	ASSISTANT:
Rollover	• Rollover Line & Call Deflect key • E/A Cockpit not supported	• Rollover Line • Rollover Line Appearance of other assistant, if available • Secondary Line Appearance for & Repertory dial key to each executive (instead of DSS-D key) • Secondary Line Appearance of & Repertory Dial key to other assistant (instead of DSS-D key), if available • Immediate Ring key**
Enhanced	• Private Line • Query Line & Repertory Dial key to each assistant • DSS-D key to other executives, if any • Ring Transfer On/Off keys • E/A Cockpit supported	• Deputy key for each executive • Query Line & Repertory Dial key to each executive • Query Line Appearance of other assistant, if available • E/A Cockpit supported
Basic	• Primary Line • DSS key to each assistant • Shift key • E/A Cockpit supported	• Primary Line • DSS-D key to each executive • DSS-D key to other assistant, if available • Ring Transfer On/Off keys for each executive • Shift key • E/A Cockpit supported

Figure 39: Standard Executive/Assistant Configurations on OpenScape Voice

NOTICE:

The Rollover configuration is not supported by OpenScape UC Application and hence cannot be used with E/A cockpit.

Related concepts

E/A Wizard on page 340

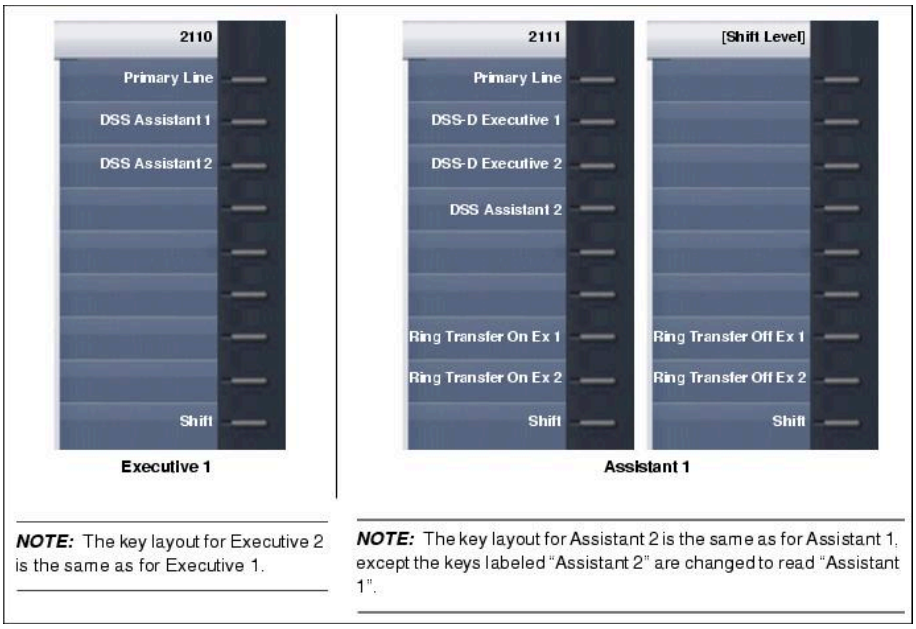
4.7.2.1 Basic E/A Configuration with Call Waiting

In the Basic E/A (Executive/Assistant) configuration a maximum of one additional caller can be handled at the same time. An easy-to-use key layout with a minimum number of keys guarantees an efficient handling of calls.

This solution is recommended for executives who prefer to give their attention to mainly one calling party at a time. It offers the following default features:

- Primary line for each the executive and the assistant.
- DSS (Direct Station Selection) from executive to assistant.
- DSS-D (DSS-Direct) from assistant to executive.
- Remote activation/deactivation of call forwarding from the executive's telephone to the assistant's telephone via the Ring Transfer On/Off keys at the assistants' phones.

The following figure displays the key layout for an arrangement with two Executives and two Assistants.



NOTE: The key layout for Executive 2 is the same as for Executive 1.

NOTE: The key layout for Assistant 2 is the same as for Assistant 1, except the keys labeled "Assistant 2" are changed to read "Assistant 1".

Figure 40: Key layout for Basic E/A Groups with 2 Executives and 2 Assistants

If the E/A Cockpit Application is used, some functionalities are moved from the function keys to the E/A Cockpit graphical user interface.

4.7.2.2 Enhanced E/A Configuration with Call Waiting

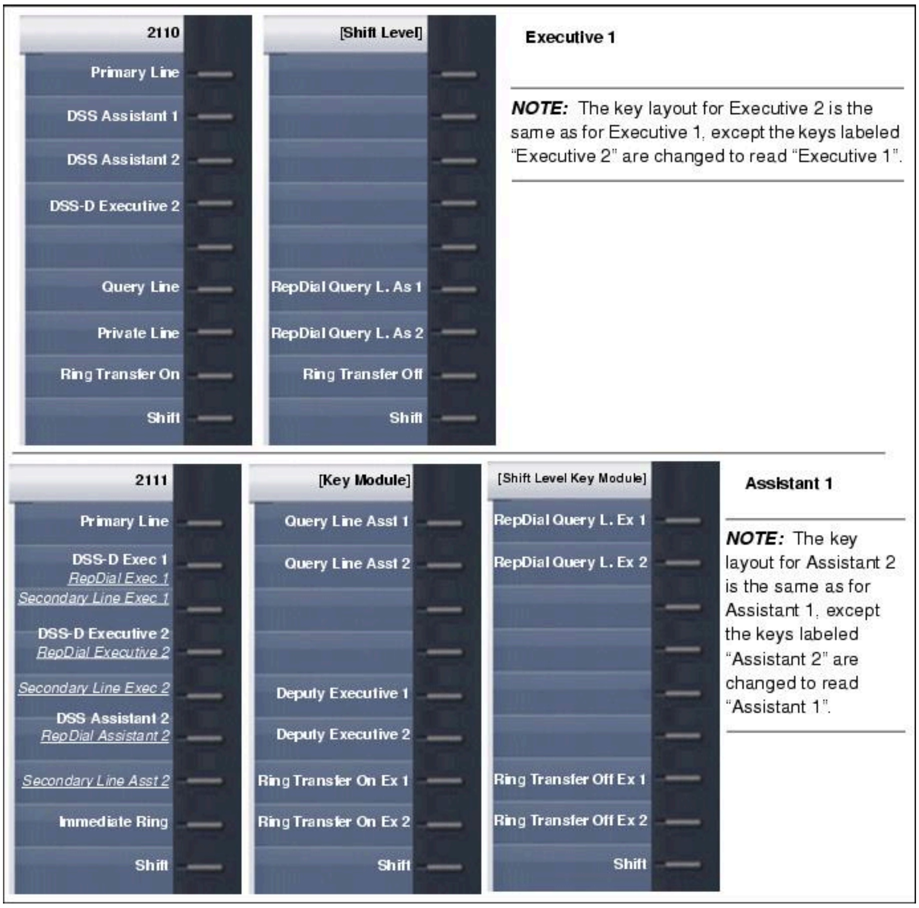
In the enhanced E/A (Executive/Assistant) configuration, query lines for the executives and the DSS-D (Direct Station Selection - Direct) keys from one executive to another executive improve the handling of calls significantly. In addition, executives are provisioned with a private line.

However, these conveniences do not detract from the focus of the executive's primary line, where dedication to the calling party is key and only one additional caller can be handled simultaneously.

This configuration is recommended for executives who require a great deal of flexibility due to frequently changing deputy assistants, but without compromising privacy. It offers the following features:

- Communication between executives and assistants via query lines instead of primary lines.
- DSS-D from one executive to another executive.
- Deputy key for assistants. This permits any other internal user to take over an assistant’s functions.
- Secondary line appearance of the executive’s primary line at the assistant’s telephone to indicate the call forwarding status of the executive at all times.
- Secondary line appearance of one assistant’s primary line at the other assistant’s telephone in combination with an Immediate Ring key to handle incoming calls when the first assistant is away from the desk (the default DSS-D key for calls to the first assistant is replaced by a Repertory Dial key).
- Each executive has a private line with its own unique number for making and receiving calls. This line is not shared with the assistants.

The following figure displays the key layout for an arrangement with two Executives and two Assistants.



NOTE: The key layout for Executive 2 is the same as for Executive 1, except the keys labeled “Executive 2” are changed to read “Executive 1”.

NOTE: The key layout for Assistant 2 is the same as for Assistant 1, except the keys labeled “Assistant 2” are changed to read “Assistant 1”.

Figure 41: Key layout for Enhanced E/A Groups with 2 Executives and 2 Assistants

If the E/A Cockpit Application is used, some functionalities are moved from the function keys to the E/A Cockpit graphical user interface.

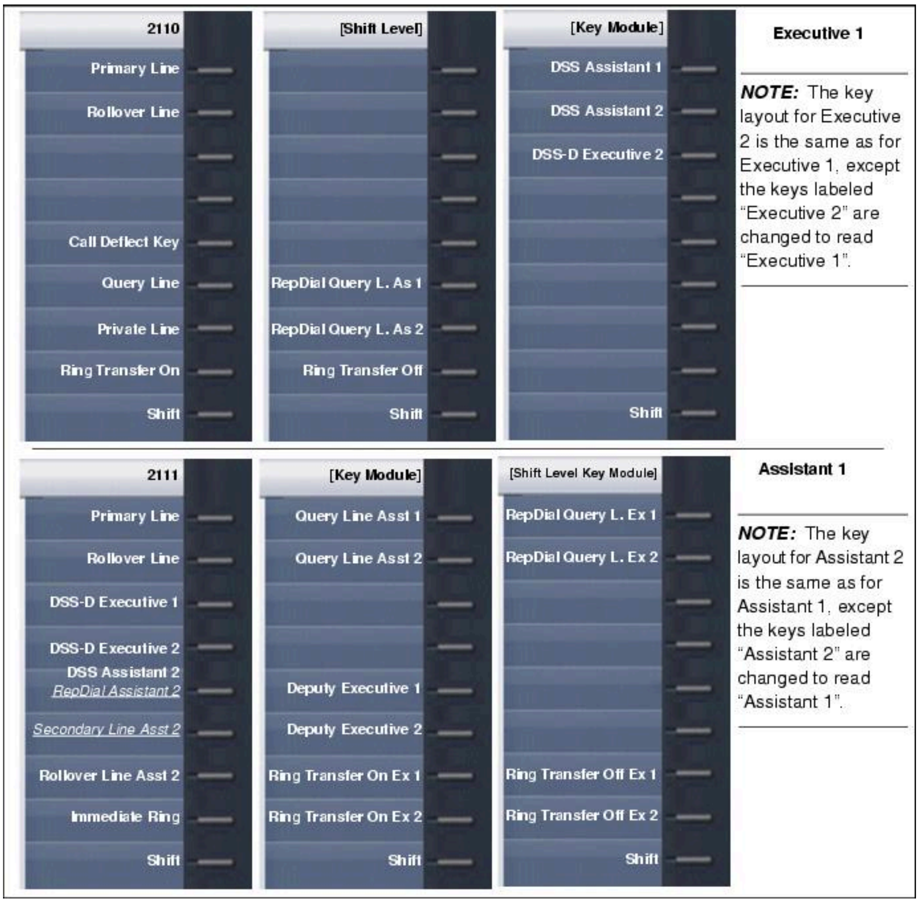
4.7.2.3 Rollover E/A Configuration

The E/A (Executive/Assistant) Solution with Rollover is recommended for executives who are focused on a high degree of availability and fast call handling.

It offers the following additional features:

- Rollover line and Call Deflect key for the executive.
- Rollover line for the assistant.
- Rollover line appearance of the assistant’s rollover line at the other assistant’s telephone to handle additional incoming calls when the first assistant is busy or away from the desk.

The following figure displays the key layout for an arrangement with two Executives and two Assistants:



NOTE: The key layout for Executive 2 is the same as for Executive 1, except the keys labeled “Executive 2” are changed to read “Executive 1”.

NOTE: The key layout for Assistant 2 is the same as for Assistant 1, except the keys labeled “Assistant 2” are changed to read “Assistant 1”.

Figure 42: Key layout for Rollover E/A Groups with 2 Executives and 2 Assistants

IMPORTANT:

The E/A Cockpit Application does not support this configuration!

4.7.3 E/A Wizard

Since Release 4 of OpenScape Voice the creation and maintenance of E/A groups is significantly simplified by an enhanced E/A wizard, available at the OpenScape Voice Assistant. The E/A wizard automatically (re-)configures the involved subscribers and OpenScape Desk CP phones according to the selected configuration type and hence disburdens the administrator from extensive and error-prone manual configuration.

NOTICE:

In order to get the highest benefit from the E/A wizard, a DLS server has to be available. Otherwise, the key setup at the involved phones has to be done manually.

If a DLS is present and E/A Cockpit shall not be used then all the phone configurations are done by the E/A Wizard. If the E/A Cockpit shall be used, then E/A Cockpit must first be configured on the phone before the rest of the configuration is done by E/A Wizard.

Apart from phone configurations the E/A Wizard also performs Subscriber and BG (Business Group) configurations:

- With respect to subscribers this includes adding line appearances for the lines the subscriber will have access to and also enabling and configuring the required services. The call forwarding settings will be modified to suit the E/A group and calls from executives will be forwarded to assistants after the creation of the group.

  The only prerequisite is that the related subscriber lines were created and correctly declared as Primary Keyset or Phantom Lines
- Similarly, services are enabled for the BG.

  A prerequisite for the BG configuration is creating PACs (Prefix Access Codes) for Unconditional Call Forwarding and an Access Number for the RACF (Remote Activation of Call Forwarding) service.

If “with E/A Cockpit” is checked in the wizard, the phone configuration is altered in that some keys are not created on the phones, since the corresponding functionality will be provided by the E/A Cockpit application. Also, the call forwarding service will be enabled but calls will not be forwarded automatically from executives to assistants, because this will also be handled by the E/A Cockpit application.

If no DLS is available, the group can still be created and stored, the line appearances will be set and the services will be configured. But the phone configuration has to be performed manually: either locally or via OpenScape Desk CP’s web interface.

Related concepts

E/A Arrangements on page 335

Standard E/A Configurations on page 336

4.7.4 E/A Cockpit

The E/A (Executive/Assistant) Cockpit feature significantly simplifies the control of an existing E/A (executive/assistant) group from any of its member phones. It is implemented as an OpenScape Desk Phone CP XML application hosted at OpenScape server, creating a rich user interface at the OpenScape Desk CP phone.

Status Management and Dynamic Call Forwarding

The E/A Cockpit introduces an advanced dynamic call forwarding logic that is based on the statuses of the E/A group's members.

From the E/A Cockpit UI (User Interface), an executive can easily

- deactivate call forwarding
- activate static (unconditional) forwarding to her mobile phone, to her voice mail, or to a variable destination that can be set from the UI
- activate dynamic call-forwarding "to assistant", that chooses the forwarding target according to the statuses of her assistants

An assistant can signal

- being "at desk" (available to the E/A group, unconditional call forwarding deactivated) or
- being "off desk" with call-forwarding either deactivated, to his mobile phone, to his voice mail, or to a variable destination that can be set from the UI.

  In addition he can configure and activate a deputy that shall serve the executive in case he and no other assistant is "at desk".

Both executives and assistants can modify their own status as well as the statuses of their related assistants and/or executives from the client UI or, consistently, by using traditional means (feature codes or function keys).

The E/A Cockpit server synchronizes the members' statuses with the OpenScape Voice and propagates status changes and call events to the client UIs.

NOTICE:

For UC Application users, the E/A Cockpit status is synchronized with the UC Application Presence and Preferred Device status.

Remote Activate To Mobile

The "Remote Activate To Mobile" feature allows an executive to remotely activate and deactivate call forwarding "To mobile" by calling her E/A Cockpit phone from a preconfigured mobile number.

Audible Notification

In case an incoming call for an executive is forwarded to the assistant, it is possible to create a notification popup at the executive's phone, to give the executive a chance to pick up the call although it has been forwarded.

In case an incoming call for an executive is not forwarded to the assistant, it is possible to create a notification popup at the assistant's phone, to give the assistant a chance to pick up the call although it has not been forwarded.

With the visible popup an audible alert tone is also generated on the affected phone. Definition of the exact tone as well as tone volume is configured only with the phone.

Further information

Further information can be obtained from the appropriate parts of the UC Application documentation set, e.g. the Executive/Assistant Cockpit, Installation Guide.

4.8 Intercom / Speaker Control

InterCom Calls, also known as Speaker Control Calls (1-way and 2-way), are used for many applications such as Medical Centers, Executive/Assistant arrangements, automotive industry, chemical and energy sector, emergency response centers, and by OScAR-Pro (OpenScape Alarm Response - Professional, formerly known as DAKS). For Intercom calls, the speaker (and microphone) on the destination device is automatically turned on when the call is connected.

Since Version 5, OpenScape Voice supports Intercom functionality over SIP-Q and locally. This includes:

- One-way Intercom, variable and fixed (i.e. invoked via repertory dialing)
- Two-way Intercom, variable and fixed (i.e. invoked via repertory dialing)
- Community Groups

NOTICE:

This feature is non-standard, i.e., based on proprietary CorNet-N and NQ, and will not interwork with ISO/IEC or ECMA standard implementations.

Intercom Features are accessible from idle, dial, talk, and consultation dial states. OSV delivers an Intercom Call to an idle destination.

When the intercom caller or called party is not provisioned for Intercom correctly or the called party disallows an Intercom call from the calling party, the Intercom call will fail. The caller may re-dial the called party normally to speak with that user. If the called partie’s device is not equipped with automatic intercom facilities, the call reverts to a 2-party normal call.

Limitations

- SIP devices supporting Intercom are restricted to OpenScape Desk CP models and OpenScape PE (Personal Edition) clients (when equipped with an intercom speaker and microphone).

  Devices that do not support intercom calling deliver a normal basic call when terminating a speaker call.
- Shared keyset lines cannot be used for Intercom
- A 'rejection' key used to close a speaker call is not supported
- Network-wide members in survivability mode can not access this feature

Use Cases

The primary scenarios where Intercom is required:

- Executive/Assistant environment:

  Executive is able to push a phone key and give a message to the Assistant
- Alarming Application Environment

  The Intercom Feature can be used to make alarm announcements (e.g. via DAKS).

Interworking

Several feature interactions are blocked at both the originating and terminating user. Interworking includes the capability for an incoming call to indicate override (e.g., CF, DND). Intercom depends on that capability, for example, when the destination has activated Call Forwarding or Do Not Disturb.

4.8.1 One-way Intercom

The One-way Intercom feature provides an authorized originating party the capability to initiate an Intercom Call automatically with a 1-way connection (send path only from the originator) to a local destination, another OpenScape Voice or a destination located over SIP-Q.

An OpenScape Voice subcriber can originate a 1-way call to another member of his/her **Community Group** by dialing

1) an access code and
2) the destination’s 1- or 2-digit index number within his/her Community Group

or via a programmed repertory dial key (**Fixed 1-way Intercom**).

NOTICE:

OScAR-Pro (OpenScape Alarm and Response - Professional) Intercom calls are not applicable to Intercom Community Groups. OScAR-Pro can make an intercom call to any OSV subscriber (device-speaker/mic eqipped or reverts to normal call).

Once the Intercom Call is established, the caller's voice or announcement is broadcast through the speaker for all in hearing distance to hear. The caller goes on-hook and the call clears without the destination communicating back to the caller.

Tones and Audio Path Safeguarding

For One-way Intercom calls originated by an OSV subscriber, an initial tone is provided as illustrated in the example figure below.

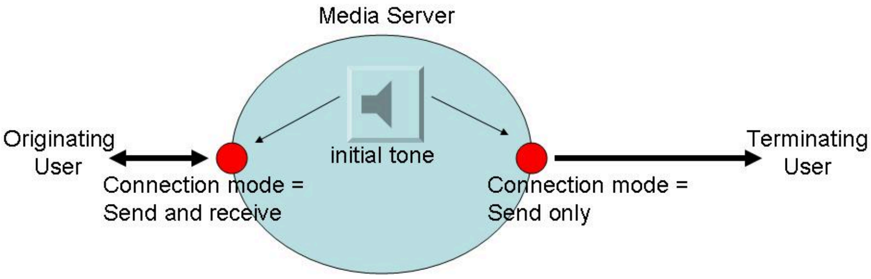

Media Server
Originating User
Connection mode = Send and receive
initial tone
Connection mode = Send only
Terminating User

Figure 43: One-way Intercom zip tone

The conference circuit at the originating side is retained during the call in order to prevent the calling party from receiving audio from the called party.

The system-wide **Terminating Intercom Control** parameter specifies whether OpenScape Vocie shall safeguard *terminating* One-way Intercom Calls in a similar fashion. It is implemented as follows:

- On (default setting)

  The OSV creates a(nother) conference circuit at the terminating side to prevent the called party from sending audio to the calling party.
- Off

  The switch of the terminating subscriber shall not create a MS conference circuit to control the speech path for 1-way intercom calls.

  This may be used to conserve limited Media Server resources, e.g. when OScAR-Pro sends broadcast messages via 1-way intercom calls to multiple subscribers.

NOTICE:

Currently OScAR-Pro only supports Two-way Intercom, so One-way Intercom calls are either OSV-local and inter-OSV.

Feature Access Code

In order to invoke 1-way Intercom, a Prefix Access Code for the Vertical Service **One-Way Intercom** has to be created in the appropriate numbering plan(s).

4.8.2 Two-way Intercom

The Two-way Intercom feature has similar functionality and activation logic as the One-way Intercom, with the added capability of bidirectional communication (with both send and receive paths) automatically using the speaker and microphone facilities at the destination.

As for One-way Intercom, an OpenScape Voice subcriber can originate a 2-way Intercom Call to another member of his/her **Community Group** by dialing an access code and the destination's Community Group member number or via a programmed repertory dial key (**Fixed 2-way Intercom**)..

NOTICE:

OScAR-Pro (OpenScape Alarm and Response - Professional) Intercom calls are not applicable to Intercom Community

Groups. OScAR-Pro can make an intercom call to any OSV subscriber (device-speaker/mic eqipped or reverts to normal call).

Tones

For a Two-way Intercom call, if provisioned, the terminating OSV lets the Media Server provide a periodic tone as shown in the example figure below. When the intercom call is disconnected, OSV clears the Media Server connection.

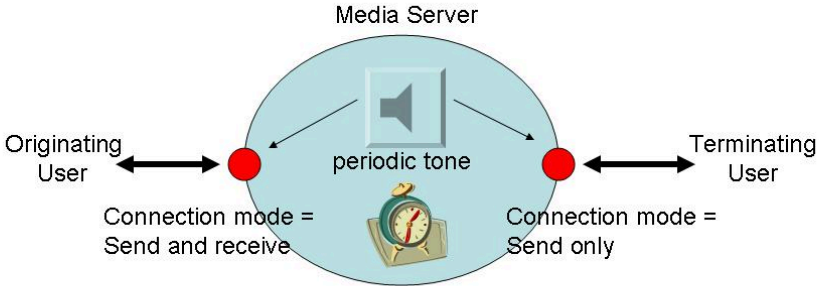

Media Server
Originating User
periodic tone
Terminating User
Connection mode = Send and receive
Connection mode = Send only

Figure 44: Two-way Intercom periodic tone

Feature Access Code

In order to invoke 2-way Intercom, a Prefix Access Code for the Vertical Service **Two-Way Intercom** has to be created in the appropriate numbering plan(s).

4.8.3 Community Groups

Community Groups are used to configure bilateral Intercom Calling capabilities and to provide fast dialing for Intercom Calls.

Any OSV subscriber that shall originate or terminate Intercom calls, has to be provisioned with a personal Community Group, defining the allowed Intercom targets/origins.

NOTICE:

OScAR-Pro (OpenScape Alarm and Response - Professional) Intercom calls are not applicable to Intercom Community Groups. OScAR-Pro can make an intercom call to any OSV subscriber (device-speaker/mic eqipped or reverts to normal call).

An OSV Subscriber *S* is able to initiate a 1-way or 2-way speaker call to a destination *T* locally or over the SIP-Q network

- *T* is a member of *S*'s Community Group
- *S* is an unblocked member of *T*'s Community Group (if *T* is an OSV subscriber)
- *T* is in the same BG (Business Group) as *S* (either locally or during call setup *T*'s gateway is in the same BG as *S*)
- *T*'s device/client is equipped with a loudspeaker (1-way) or loudspeaker and hands-free microphone (2-way) with Auto-answer enabled
- *T* is idle

Otherwise, the call may fail or revert to a normal basic call.

Provisioning

Apart from the group members, the group is provisioned with a **Timer for Periodic Tone** that applies to all terminating two-way Intercom Calls. Possible values are:

- 0, i.e. no tone or
- a value between 5 and 180 seconds

The default is 120 seconds.

The table below is a stylized members table:

Table 35: Community Group members table (example)

COM#	Destination Number	Destination Name	Incoming Block
0	4931700	Dennis	no
1	54321	Mickey	no
etc.			
98	23456	Peter	yes
99	67890	Jeff	no

The COM# (**Community Group Member Number** or COM Number for short) is the (index) number to be dialed after the one-way or two-way intercom access code. This column is searched to identify the destination (member).

For local members, the **Destination Number** should be the member’s fully qualified directory number. For remote members, the member’s calling party number (fully qualified directory number or display number, if configured) must be used instead.

NOTICE:

For incoming intercom calls from remote members, the members table is searched for the calling party number to verify that the calling party is an unblocked member.

In any case this number must be routable according to the subscriber’s numbering plan.

The **Destination Name** field is for descriptive purposes only and is not used for call processing.

The **Incoming Block** flag is set on a Community Group member if intercom requests from this person shall be blocked. When blocking is assigned the intercom fails, but doesn't give the caller an indication, instead just rings the target. The call has reverted to a regular call.

Related concepts

Please select the appropriate help topic on page 656

4.8.4 Intercom: OScAR-Pro Support

OpenScape Voice can distinguish between OScAR-Pro (OpenScape Alarm and Response - Professional, formerly known as DAKS) and subscriber Intercom Calls. If an Intercom Call originates at OScAR-Pro, it shall be delivered to the idle called subscriber without restrictions. In particular, the called party's Community Group is ignored.

OScAR-Pro has a broadcast intercom feature, for example, to make an emergency announcement by invoking Two-way Intercom calls.

NOTICE:

Future releases of OScAR-Pro will support One-way Intercom as well.

OScAR-Pro makes outgoing calls over SIP-Q to a pre-defined list of users. It is possible for OScAR-Pro to make a conference call, i.e., where two people are involved in the intercom call with OScAR-Pro.

OScAR-Pro plays an initial tone in-band to the called party equipment. A periodic tone can be provided by the terminating system. At the OpenScape Voice Assistant, the insertion interval can be set with the **DAKS Periodic Tones** system-wide property.

For details, please refer to the OScAR-Pro Documentation.

4.9 DLS Device Management Integration

With the DLS (Deployment Service) Device Management Integration feature, OpenScape Voice Assistant was enhanced to coordinate OpenScape Voice subscriber management and DLS-based device management. With this feature DLS plug&play is now fully supported by the Assistant.

For configuration changes that are performed *from the Assistant*, settings are consistently applied in either direction:

- when a subscriber is created, a virtual device is seamlessly created in DLS
- when a subscriber is updated, the corresponding DLS devices (virtual and registered) are updated accordingly
- when a subscriber’s device configuration is updated, the subscriber’s configuration is updated accordingly
- when a subscriber is deleted, the administrator decides whether deletion of related devices and line keys in DLS shall take place

NOTICE:

In order to use DLS Device Management Integration it is necessary to assign a DLS to the related Business Groups.

DLS Plug&Play

The goal of DLS Plug&Play is to automatically provide the supported workpoints with the parameters required for registering at a gatekeeper or SIP server.
It is implemented using virtual devices, i.e. a set of device attributes that are

inherited by a real device upon registration to DLS. In particular, when a device registers to DLS, a lookup is made in the DLS DB for a virtual device matching the Terminal Number (E.164) or the Device ID (MAC address) of the registering device. If a match is found, the real device downloads the configuration of the virtual device.

OpenScape Voice Assistant is able to create virtual devices in two ways:

- At the time a subscriber is created
- By explicit creation at the integrated Device Management GUI

Simplified DLS Server Assignment

The association between subscribers and DLS is carried out at the BG (Business Group) instead of the subscriber level. The BG’s configured (default) DLS server is used for *all* the subscribers that belong to this BG. It is also possible to provision a BG without an associated DLS server, but of course this will disable Integrated Device Management.

At the system level, it is possible to define a *Default DLS Server*, which

- will be proposed (preselected in the GUI) as the associated DLS server for Business Groups created via Assistant and
- will be used as the associated DLS server when a new Business Group is retrieved by Assistant during Synchronization.

4.9.1 Data Consistency: OpenScape Voice --> DLS Devices

During subscriber/device management at the OpenScape Voice Assistant, *system-wide* as well as *subscriber specific* OpenScape Voice data are passed to the DLS in order to create/update the related devices. To minimize the load on the DLS, the Assistant monitors whether changes on the relevant attributes were made and updates devices only when needed.

At the time a virtual device is created, both *system-wide* and *user-specific* parameters are passed to the DLS.

When a subscriber is deleted via OpenScape Voice Assistant GUI the administrator can select whether deletion of devices in DLS shall also take place. This includes all devices using the Directory Number of the deleted subscriber as the Terminal Number or the AoR of a Line/DSS key.

Device configuration is updated seamlessly following subscriber configuration updates. This includes the update of virtual devices as well as the installed devices that are already registered to DLS and use the subscriber number as the terminal number or the AoR (Address of Record) of a line/DSS key. During updates only the user specific parameters are set.

In particular, for devices using the DN of the updated subscriber as the Terminal Number, all user specific parameters must be updated. For devices using the DN of the updated subscriber as the AoR in a Line/DSS key, only parameters 7, 8 and 9 of the table below are updated.

The table below presents the OpenScape Voice parameters that are passed to the DLS during subscriber/device management at the Assistant.

Table 36: Data Consistency: OpenScape Voice Data --> Device Datal

	Device Attribute(s)	OSV Data	Source	Type
1	Reg-address	SIP-SM 1 IP address	Assistant DB	System Wide
2	SIP registrar server	SIP-SM 1 IP address	Assistant DB	System Wide
3	SIP server type	-	'OpenScape Voice'	System Wide
4	Reg-port	-	UCD/TCP: 5060 TLS: 5061	User Specific (Depends on Transport Protocol)
5	SIP registrar port	Srx/Sip/IpPort or Srx/Sip/ TLSPort	Assistant DB	User Specific (Depends on Transport Protocol)
6	Time Zone	Time Zone	OSV Subscriber Data	User Specific
7	SIP Realm	SIP Realm	OSV Subscriber Data	User Specific
8	Password	Password	OSV Subscriber Data	User Specific
9	Local Country Code	Country Code	OSV Subscriber Data	User Specific
10	Local Area Code	Area Code	OSV Subscriber Data	User Specific
11	Local District Code	Local Office Code	OSV Subscriber Data	User Specific
12	Terminal Name	Internal Name	OSV Subscriber Data	User Specific
13	Register by Terminal Name	-	FALSE	User Specific
14	Language	Language	OSV Subscriber Data	User Specific
15	Call Pick up URI	PAC with destination = Call Pick Up A	OSV Numbering Plans	System Wide
16	Callback on Busy URI	PAC with destination = CCS	OSV Numbering Plans	System Wide

	Device Attribute(s)	OSV Data	Source	**Type**
17	Callback on No Reply URI	PAC with destination = CCS	OSV Numbering Plans	System Wide
18	Cancel Callback URI	PAC with destination = DCCS	OSV Numbering Plans	System Wide
19	Conference URI	PAC with destination = Large conf	OSV Numbering Plans	System Wide

NOTICE:

When you want to add /edit a Business Group List, all User Name values, Display Name, Unicode Display Name, External Display Name and Unicode External Display Name, will not be transmitted through API to DLS

When determining the PACs (Prefix Access Codes) that are available to the subscriber, private, common and global numbering plans are examined one after the other until a match is found.

PACs are not really system-wide parameters, but for device update purposes they must be treated as such. That is, update of these parameters must not take place every time a subscriber is modified

4.9.2 Data Consistency: DLS Devices --> OpenScape Voice

Provisioning of certain device attributes also requires modifying the related subscriber. If performed from the integrated device management, the subscriber configuration is updated at the time the features are activated on the device.

CSTA Related Settings

The table below presents the CSTA-related device attributes that can be managed from the integrated device management. The required subscriber settings are automatically performed by the Assistant.

Table 37: Data Consistency: Device Data --> OpenScape Voice Data

	Device Attributes	Required Subscriber Features
1	Allow Auto Answer = TRUE	CSTA with appropriate type assigned
2	Allow Beep on Auto Answer = TRUE	CSTA with appropriate type assigned
3	Allow Auto-Reconnect = TRUE	CSTA with appropriate type assigned

	Device Attributes	Required Subscriber Features
4	Allow beep on Auto-Reconnect = TRUE	CSTA with appropriate type assigned
5	Allow uaCSTA = TRUE	CSTA with appropriate type assigned
6	Server-based features (OpenScape Desk CP phones only)	CSTA with type = CSTA over SIP assigned AND CFB (Call Forwarding Busy) assigned with 'activate via = all' AND CFNR (Call Forwarding No Reply) assigned with 'activate via = all' AND CFU (Call Forwarding Unconditional) assigned with 'activate via = all' AND DND (Do Not Disturb) assigned

The appropriate CSTA type depends on the involved device:

- If the device is an OpenScape Desktop Client, the CSTA type is set to **Type 1**
- If the device is an OpenScape Desk CP phone, the CSTA type is set to **CSTA over SIP**
- In all other cases, CSTA is set to **Normal**

Line Key Related Settings

Furthermore, when line keys are added to a device via Assistant, subscriber configuration is seamlessly updated with the corresponding line appearances. For instance, when adding a primary line to a device via the device management GUI, the Assistant sets the subscriber’s **Keyset Use** parameter to **Primary Line**. When adding a secondary line to a device, Assistant must add it a line appearance to the respective subscriber.

4.9.3 DLS Device Management Integration: GUI

The DLS Device Management is integrated in OpenScape Voice Assistant’s subscriber management. On its graphical user interface it permits the display, creation and essential configuration of multiple virtual devices per subscriber.

Default DLS Server

A new attribute is introduced to the DLS list maintained in the OpenScape Voice Assistant to indicate which DLS server shall be used as the "system default".

DLS-BG association

At the time a Business Group is created from Assistant via **Add** or **Quick Add BG**, the BG attribute 's **Default DLS Server** is initially set to the system-wide Default DLS server, or null, if the latter doesn't exist. The administrator may select another (or no) DLS server at any time.

Device Plug&Play Settings in Subscriber Creation Dialogs

When creating a new subscriber in either the **Add Subscriber** or **Quick Add Subscriber** dialog, the administrator decides whether or not a **Phone** or **Client** shall be created. If so, he may further specify the device's ID (=MAC address for phones). In the **Add Subscriber** dialog it is also possible to assign an existing DLS device profile to the device.

Device List

DLS Device Management comprises a list view, which displays all DLS devices using the directory number of a preselected subscriber as the Terminal Number or line/DSS (Direct Station Selection) key as well as the devices that are registered in OpenScape Voice and missing from DLS. Information about registration to the OpenScape Voice is also incorporated, to facilitate quick diagnosis of device/subscriber configuration inconsistencies that may result in registration problems.

Device Management

The Device Management user interface allows an administrator to add, display, edit and delete devices for an existing subscriber. In addition to basic device settings, it is also possible to view and edit the device's key layout. On the edit side, only a limited set of features and Line/DSS (Direct Station Selection) keys are supported.

For subscribers who belong to the main office, the administrator is able through the Device Management menu to create device in deployment server, after having selected a default deployment server at business group level.

For subscribers who belong to a branch office, the administrator is able to use the Device Management functionality to create device in deployment server in the following cases:

- If the branch office inherits the default deployment server from the business group (see Override the default deployment server of business group) and there is a default deployment server configured at business group level.
- If the branch office overrides the configured deployment server at business group level and there is a non empty default deployment server configured at branch office level.

> **NOTICE:**
>
> Whenever th administrator moves subscribers from a branch office to another or changes the assigned default deployment server at branch office or business group level, the deployment servers are not automatically updated according to these changes. Manual intervention of the administrator is needed to update the device management functionality.

4.10 Synchronization of OpenScape Voice - OpenScape Branch

Some feature data that is common on both OSB and OSV can be provisioned on OSV via OSV Assistant and synchronized with OSB, thereby eliminating the provisioning separately on OSV and OSB and enhancing the validity of the data.

The OSV feature data that can be synchronized with OSB is the following:

- Hunt Group Pilot DN
- Hunt Group Pilot DN type
- Hunt Type
- Hunt Group Member Data
- Emergency Calling Subnet Specific Configuration Data

A new data table is created in the OSB database to maintain the data that is being deleted in the OSV via Mass Provisioning, so that the corresponding data from the OSB can be deleted via synchronization process. The retention period of the table is one month. After that period all the table entries are being deleted.

4.11 Authorization Codes Group

The Authorization Codes Group is a feature that allows the administrator to create groups of authorization codes. It is configurable through the OpenScape Voice Assistant.

INFO:

Authorization codes are assigned to subscribers to allow them set up certain off-net calls. When attempting to set up a call of a restricted traffic type, the subscriber has to enter (dial) a valid authorization code.

For each Authorization Codes Group the administrator can assign a class of restriction that contains the traffic types for which the authorization codes of the group can be used to make outbound calls. The administrator will configure all the affected subscribers with the Authorization Code service such that an authorization code is requires to be dialed for all traffic types that are not allowed to be used by default (probably all traffic types).

Authorization Codes Toll Restriction Override service

The Authorization Codes Toll Restriction Override service allows the subscriber to use his/her authorization code to override the toll restrictions applicable to the call in progress. It can be activated for the entire system through the System-wide settings.

Description

When activated, all off-net destinations marked with a generic traffic type (i.e. non-emergency traffic type) will be restricted unless the traffic type is listed in a class of restriction assigned to the authorization group to which the authorization code entered on the call belongs.

After the validation of an entered authorization code, the Authorization Code Toll Restriction Override service when activated, matches the entered authorization code against the Authorization Code Group keys. A key matches an authorization code if its digits are leading digits of the authorization code given.

- If no key matches, then no toll restrictions will be overridden, i.e. the currently traffic types will remain in effect and the call will be released as if it was restricted by the toll restriction service.
- If one key matches, then the traffic type of the call will be looked up in the class of restriction that is associated to the key. If it is listed, then the call may proceed. If it is not listed, the call will be released as if the call was restricted by the toll restriction service.
- If more than one keys matches, the best matching key (based on key length) is used. The traffic type of the call will be looked up in the class of restriction that is associated to the matching key. If it is listed, then the call may proceed. If it is not listed, the call will be released as if the call was restricted by the toll restriction service.

Limitations

Only a single class of restriction can be associated to an authorization code group key. An alternate class of service is not necessary, because a valid authorization code needs to be dialed already to make a call.

Related concepts

Business Group Authorization Codes

Classes of Restriction on page 555

4.12 Broadcast Groups / 1-way Speaker Broadcast

A new feature is available from V8 onwards called “"1-way Speaker Broadcast"”. This feature introduces a new group entity called Broadcast Groups. The members of these groups are OpenScape Voice subscribers belonging to the same business group.

This feature is activated by lifting the handset and pressing a pre-programmed feature key followed by the group number.

The system administrator has the option to restrict which subscribers will have permission to initiate broadcast calls.

Each member of the group shall be provisioned with a role that shall indicate if this member:

- Can initiate a 1-way speaker broadcast call against the other members of this group
- Can receive a 1-way speaker broadcast call from other members in this group
- Can initiate and receive a 1-way speaker broadcast call to/from the other members of this group

An OSV subscriber can be a member of many broadcast groups concurrently and its role may vary in the different groups.

Limitations

- The maximum number of members per broadcast group is 50. A broadcast group must have at least two (2) members.
- The maximum number of broadcast groups per system is 500.
- OpenScape Mobile and Profile Only subscribers cannot be members of a Broadcast Group.

IMPORTANT: If a 1-way speaker broadcast call is invoked against a broadcast group which has already an active 1-way speaker broadcast call, then the invocation shall fail and the initiator shall get a busy tone.

Group members excluded from a 1-way speaker broadcast call

Under certain conditions some member’s phones shall not receive the 1-way speaker broadcast call. Such conditions are the following:

- The member’s phone is busy during the 1-way speaker broadcast call.
- If the member has multiline appearances ONLY the device of the primary line shall receive the 1-way speaker broadcast call.
- If the member has multiple registered contacts or has a primary line registered on multiple devices then the 1-way speaker broadcast call shall not be presented to this member.

Group members against which a 1-way speaker broadcast call will fail

Under the following conditions a 1-way speaker broadcast call against a member will fail and the call leg towards this member shall be released:

- The member’s phone does not support the auto-answer feature or has been configured to ignore it.
- The member has activated DND (Do Not Disturb) service.
- When a member’s phone answers and OSV attempts to create a connection on the conference bridge allocated for this 1-way speaker broadcast call, if there are no Media Server or CAC resources then the call leg towards this member’s phone shall be released.

NOTICE:

In all the above cases, since OSV cannot know before forking the call to these members that it will fail, the call leg shall be released immediately as soon as OSV detects the error condition.

1-way speaker broadcast calls and Security

Each party of a 1-way speaker broadcast call shall affect the global security status of the call.

If all parties have secure connections (end-to-end) with the Media Server then the broadcast will be considered as secure and it will be presented as secure to all the participants.

If one (or more) party(s) doesn’t have secure connection (end-to-end) with the Media Server then the broadcast will be considered as non-secure and it will be presented as non-secure to all the participants.

If a broadcast receiver drops out from the 1-way speaker broadcast call and this affects the global security status of the call, then all the remaining parties' security indication will be updated.

NOTICE:

The receivers shall display the security zone of the initiator. The initiator shall display the lower security zone from the security zones of the receivers that answered the broadcast.

5 Media Services

The OpenScape Voice media services are provided by at least one independent Media server. The functions of this Media Server are controlled by OpenScape Voice via the Media Gateway Control Protocol (MGCP).

The Media Server respectively used provides OpenScape Voice with the following general media services:

- Playback of tones and system announcements
- Playback of music-on-hold
- Managing device-controlled audio conferences of OpenScape Voice (large conferencing)
- Monitoring the telecommunication according to Communications Assistance for Law Enforcement Act (CALEA)

In this media service context the following general features or technologies are also supported:

- Mixing of media streams for conference applications
- Transcoding
- Creation of DTMF tones to support CSTA-compatible applications of OpenScape Voice.
- Inband recognition of DTMF tones
- Support of the following audio codecs:
  - G.711 A-Law
  - G.711 µ-law
  - G.729
- QoS-Features
- Universal allocation of protocol ports for playing tones / system announcements / greetings and for conferences.

5.1 Supported Media Servers

OpenScape Voice can be operated with different selected Media server products.

For the time being it is:

- OpenScape Media Server

5.1.1 OpenScape Media Server

The OpenScape Media Server can be shortly described as Apache Tomcat web server for voice and video applications. It does not use special hardware and is based exclusively on software, of which the main interfaces use Java technology. As integrated Media server of OpenScape Voice it is administered via the Common Management Platform.

In addition to the described general Media server functions the OpenScape Media Server at OpenScape Voice supports the following features:

- Secured payload transmission by Session Description Protocol Security (SDES), Multimedia Internet Keying (MIKEY) and the Secure Real Time Transport Protocol (SRTP)
- Internal Support of Language Varieties

You can use the OpenScape Media Server also as Media server under OpenScape UC Application. In this case the OpenScape Media Server supports the following features in addition:

- Conference portal
- Voice portal
- Secured signaling transmission by the protocol Transport Layer Security (TLS)

NOTICE:

You can also operate the OpenScape Media Server in parallel at OpenScape Voice and OpenScape UC Application.

OpenScape Media Server at OpenScape Voice

The OpenScape Media Server can be used at OpenScape Voice in all operating modes that have been released for OpenScape Voice.

If the performance data of a single OpenScape Media Server do not comply with the desired performance or redundancy requirements, you can also connect a Media server farm with several parallel OpenScape Media Servers to an OpenScape Voice system. In doing so you need to install the same Media server components on all computer systems of the OpenScape Media Server.

The OpenScape Voice system distributes in this case the load among the various OpenScape Media Server.

The OpenScape Media Server supports at OpenScape Voice the following interface protocols:

- Media Gateway Control Protocol (MGCP)
- Real Time Transport Protocol (RTP) / Secure Real Time Transport Protocol (SRTP)
- Simple Network Management Protocol (SNMP) v2c

OpenScape Media Server at OpenScape UC Application

The OpenScape Media Server can be used under OpenScape UC Application in all operating scenarios that have been released for OpenScape UC Application.

If the performance data of a single OpenScape Media Server do not comply with the desired performance or redundancy requirements, you can also connect a Media server farm with several parallel OpenScape Media Servers under OpenScape UC Application. In doing so you need to install the same Media server components on all computer systems of the OpenScape Media Server.

The OpenScape Voice system distributes in this case the load among the various OpenScape Media Server.

The OpenScape Media Server supports under OpenScape UC Application the following interface protocols.

- Media Resource Control Protocol (MRCP)

- Real Time Transport Protocol (RTP) / Secure Real Time Transport Protocol (SRTP)
- Session Initiation Protocol (SIP)
- Simple Network Management Protocol (SNMP) v2c
- Voice Extensible Markup Language (VoiceXML)

5.2 Media Server Farm

If the performance data of a single Media server do not comply with the desired performance or redundancy requirements, you can also connect a Media server farm with several parallel Media servers to an OpenScape Voice system. In this case, the OpenScape Voice system distributes the load among the various Media servers.

NOTICE:

If you use the OpenScape Media Server under OpenScape UC Application, a Media server farm cannot comprise more than a maximum of four OpenScape Media Server.

5.3 Media Server Redundancy on OpenScape Voice

OpenScape Voice supports various redundancy options for connecting Media servers. In this support, any combination of RadiSys and OpenScape Media Server can be used.

Owing to this combinability, the Media server that complies with the respective performance requirements can be used anywhere in the OpenScape system.

OpenScape Voice supports the following redundancy options for connecting Media servers:

- 1+1 redundancy
- N+1 redundancy
- N+K redundancy

Local Media servers can be configured in branches for the redundancy options N+1 and N+K. In this configuration, tones and system announcements need not be transmitted via the WAN, but are available locally. This optimizes the bandwidth use for the WAN.

Redundancy Software Support

Software support of the redundancy mechanism refers to the following main functions:

- Administration of the Media servers, so that they can provide security for each other. Depending on the type of redundancy used, the requirements differ slightly.
- A heartbeat mechanism that interconnects OpenScape Voice and the Media servers via keep-alive messages. This mechanism detects failed connections between systems or their recovery. It also ensures that OpenScape Voice automatically switches over to the connection to another Media server if the connection to the preferred Media server fails.

The following is required for providing this feature:

- The OpenScape Voice feature **automatic Media server audit** must be active. This enables the automatic audit between OpenScape Voice and all Media servers. Furthermore, the following features must have been defined:
  - The number of failed audits before the Media server is locked
  - The number of successful audits before the Media server is put into operation again
  - The control signal interval, which indicates the interval for sending the audits
- An audit circuit must be provided for each Media server. This circuit provides OpenScape Voice with a path for checking the statuses between the single Media servers. This audit circuit enables the control signal for the respective Media server.
- The **Multi Homing** flag must have been disabled for the single Media servers. This flag indicates that the Media server does not have an internal redundancy, and that an IP address is assigned to each fully qualified domain name.

The redundant Media servers must be administered in the same way. Example:

- The announcements IDs of all provided Media servers should match, so that the user does not notice any functional difference when a Media server is taken out of operation.
- The number of ports of the local backup Media server of a branch must correspond to the number of ports of the primary Media server.
- The central backup Media server should contain all languages used by the Media servers it supports.

Bandwidth Administration

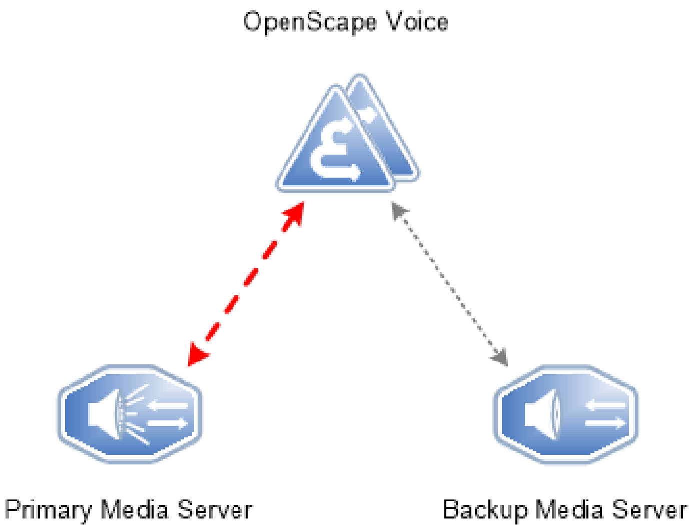
The use of redundant Media servers enables in the following way the administration of the bandwidth between the two OpenScape Voice nodes and between branches:

- Within OpenScape Voice, load balancing occurs between the MGCP signaling managers by even distribution of the subscribers among the two nodes. The MGCP signaling manager of the caller's node is selected.
- For branches, bandwidth administration is achieved in the following way:
  - Installation of a local Media server in each branch
  - Assignment of a tariff zone to each branch
  - Creation of an origin destination for the tariff zone. This destination indicates that the local Media server of the branch is to be used
- In case of geographically separated OpenScape Voice nodes, a Media server that is located at the same branch as the node or is integrated in this node can be configured as primary Media server for local subscribers through use of tariff zones. In this case, the Media server on the other node acts as backup Media server for local subscribers.

5.3.1 1 + 1 Redundancy for Media Servers

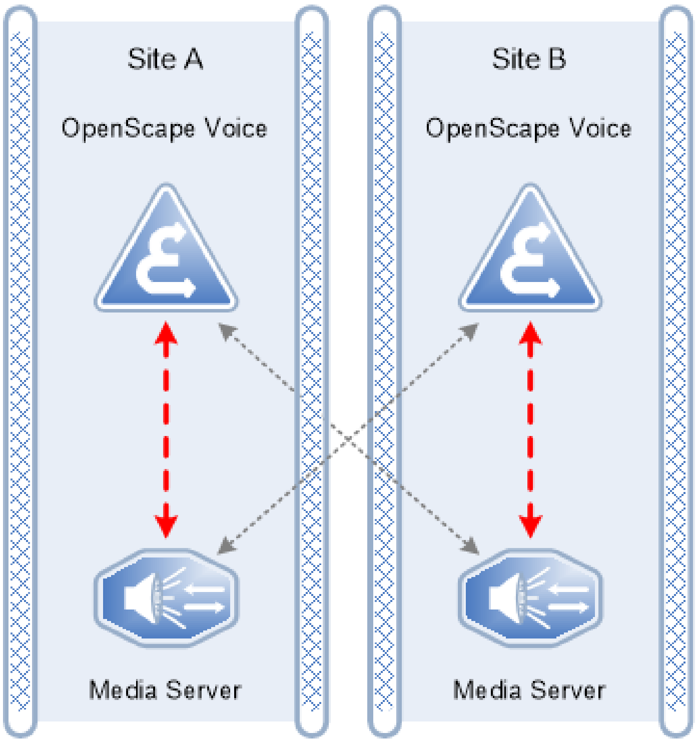
In this redundancy option, one Media server is assigned to each OpenScape Voice cluster node. Each of the two Media servers acts as backup for the other one.

The following figure shows the Media server redundancy in the 1+1 configuration with OpenScape Voice cluster nodes at the same branch.



The Media servers are found at the same branch as the OpenScape Voice cluster nodes. The primary Media server is operable and handles the entire Media server traffic of OpenScape Voice.

The following figure shows a comparable redundancy with geographically separated OpenScape Voice cluster nodes.



The Media servers are usually found at the same branch as the OpenScape Voice cluster nodes. In normal operation one of the following configurations is possible:

- The Media server of branch A is operable and handles the entire Media server traffic of OpenScape Voice. The Media server of branch B serves as backup.
- At both branches the Media servers are primary ones, serving as backup for each other. This option enables the load balancing, since the subscriber load can be distributed among the two Media servers.

In case of a failure and depending on the failure type, the following happens:

- Node failure

  If an OpenScape Voice node fails, the other one takes over. The MGCP signaling manager of the partner node still uses the same Media server as before the node failure.
- Media Server Failure

  If the primary Media server fails, OpenScape Voice switches new Media server traffic to the backup Media server automatically. Existing connections to the failed Media server are not switched over and drop away.
- Failure of a Branch or Building

  If branch A fails completely, the OpenScape Voice partner node registers this event and uses the Media server of branch B from then on.

Support of Several Languages

Both Media servers must be configured for all required languages.

5.3.2 N + 1 Redundancy for Media Servers

In this redundancy option, several (N) Media servers provide local support for branches, and a central Media server serves as backup for all other servers.

In case of the N+1 redundancy, N represents the number of primary Media servers. These are the Media servers that are in top position in the list of Media servers at a destination with Media servers. If N is greater than 1, an origin destination must be created for setting up a specific Media server for a specific branch. This number corresponds to the number of branches and headquarters that have a local Media server.

The following two figures show the N+1 redundancy for Media servers:

- If the OpenScape Voice cluster nodes share the same branch
- If the OpenScape Voice cluster nodes are geographically separated

In both figures, three active and one backup Media server are available for a 3+1 redundancy.

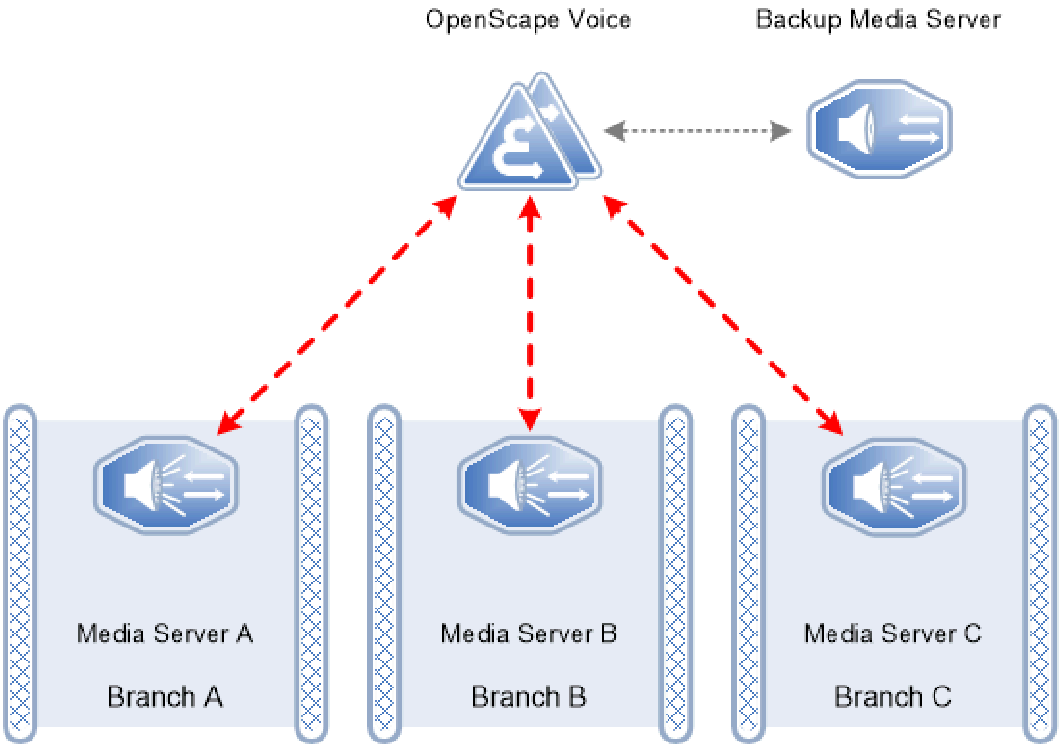


Figure 45: N+1 redundancy – OpenScape Voice cluster nodes at the same branch

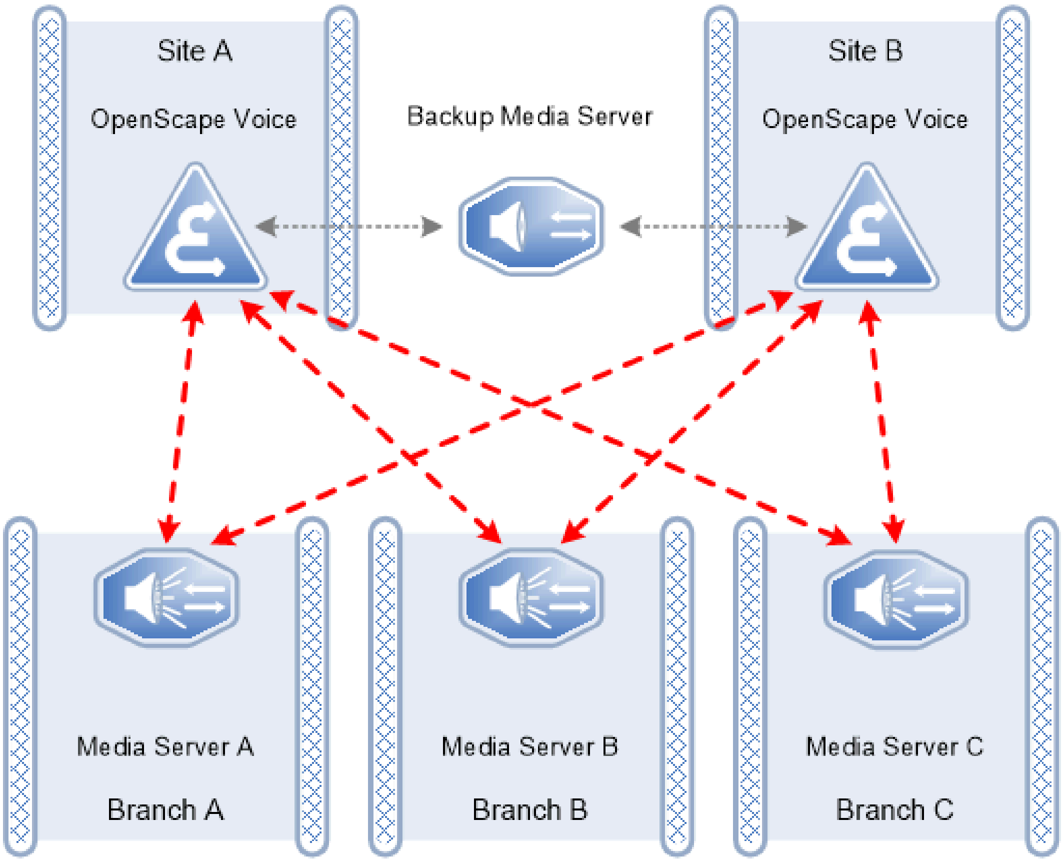


Figure 46: N+1 redundancy – OpenScape Voice cluster nodes geographically separated

In case of a failure and depending on the failure type, the following happens:

- Node failure

  If an OpenScape Voice node fails, the partner node adopts its function. The MGCP signaling manager on the partner node still uses the Media servers like it did before the failure.
- Media Server Failure

  If the Media server in a branch fails, OpenScape Voice registers this event and the branch uses the central backup Media server from then on. Existing connections to the failed Media server are not switched over and drop away. The other branches carry on using their own Media servers.
- Failure of a Branch

  If a branch fails completely, the other branches carry on using their own Media servers and are not affected by the failure.
- WAN Failure

  If the WAN connection to a specific branch collapses, the branch concerned cannot receive tones and system announcements. The subscribers isolated in the branch can still use the Media server inasmuch as they are registered with an OpenScape Voice edge system anew.

  The other branches are not affected by the failure.

Support of Several Languages

The backup Media server must be configured for all languages required by the different Media servers of the branches.

5.3.3 N + K Redundancy for Media Servers

In this redundancy option, several (N) Media servers provide local support for branches. In addition to a central backup Media server, some branches have dedicated backup Media servers. The number of backup Media servers assigned to a primary Media server is represented by K.

In case of an N+K redundancy, N and K represent the following:

- N – Number of primary Media servers
- K – Number of backup Media servers for a specific primary Media server. This number may differ for various primary Media server.

The following two figures show the N + K redundancy for Media servers:

- If the OpenScape Voice cluster nodes share the same branch
- If the OpenScape Voice cluster nodes are geographically separated

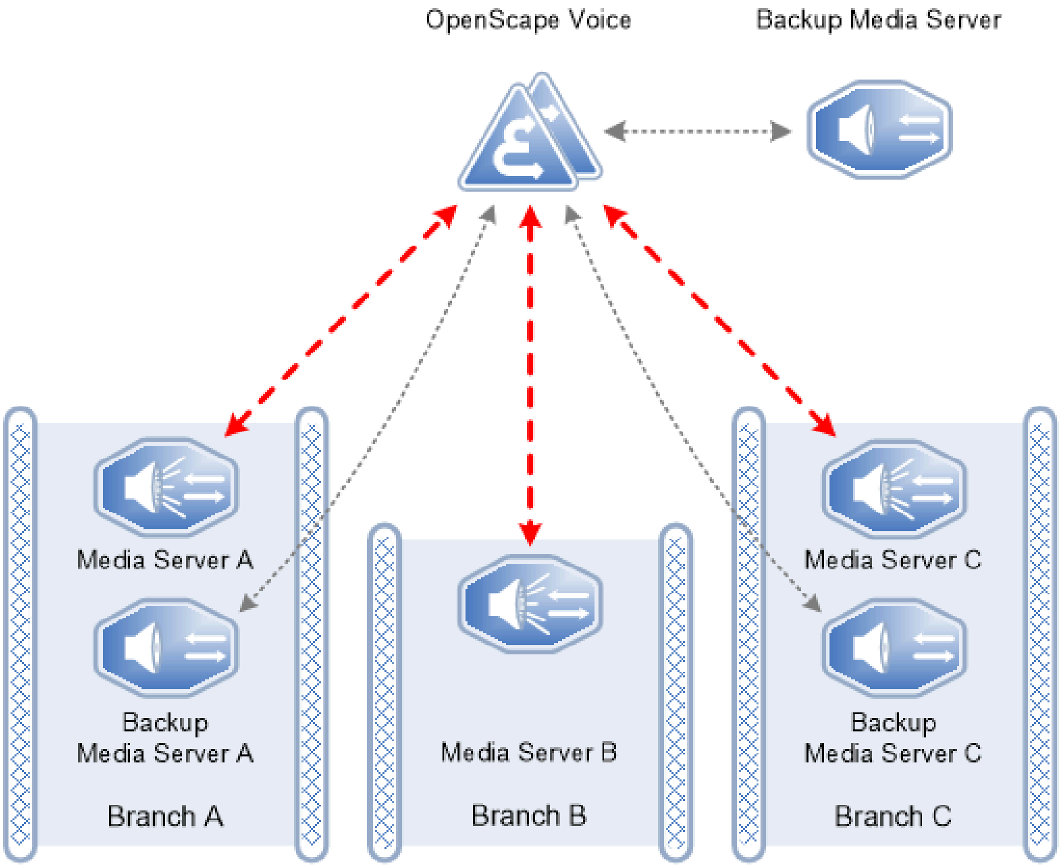


Figure 47: N+K redundancy – OpenScape Voice cluster nodes at the same branch

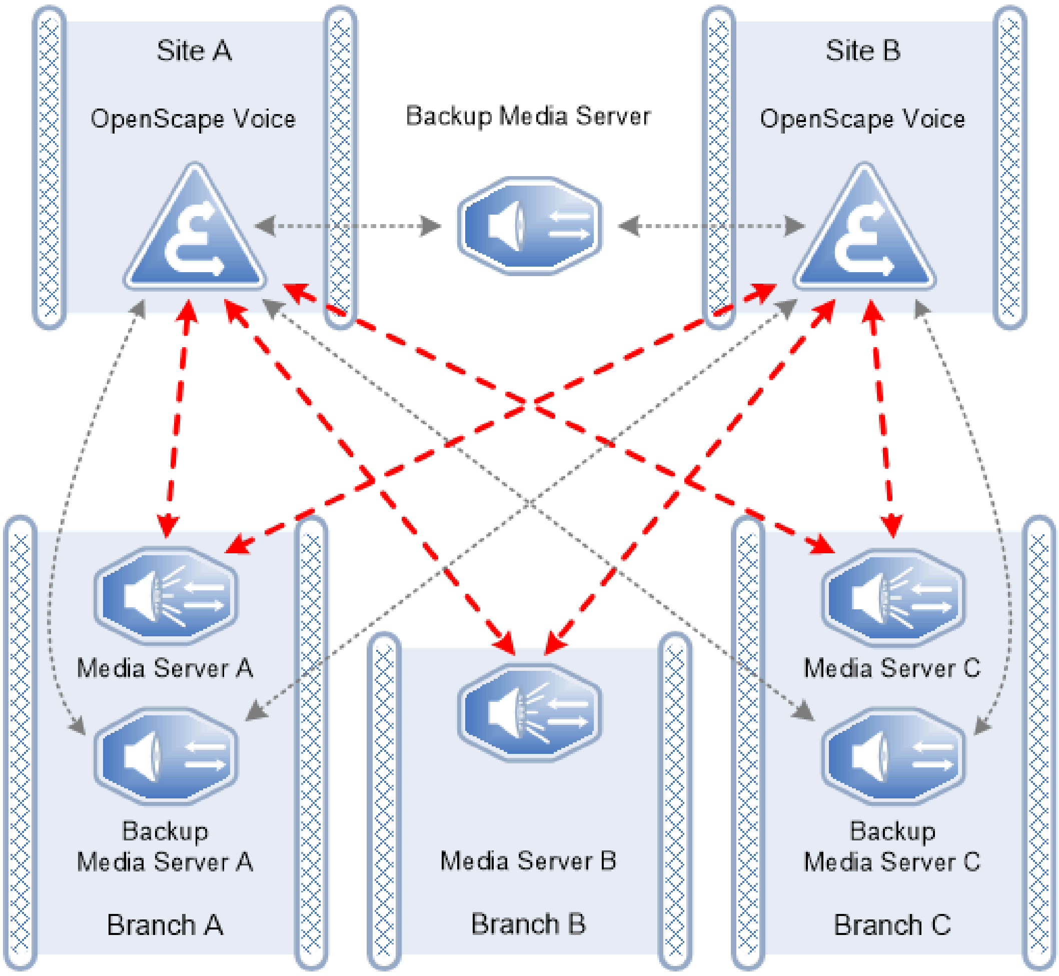


Figure 48: N+K redundancy – OpenScape Voice cluster nodes geographically separated

Both figures contain the following elements:

- Each branch has its own Media server for altogether three primary Media servers.
- On each of the OpenScape Voice cluster nodes you find a central backup Media server.
- Branches A and C have their own backup Media servers, too. These two branches may represent bigger field offices, while branch B may be a smaller field office that does not require a local redundancy.

  As a result, branches A and C have two backup Media servers; branch B has one.

In this scenario the Media servers in the large branches are locally redundant, and the smaller branches use a backup Media server located on one of the OpenScape Voice cluster nodes. In normal operation, the Media servers are operable in all branches and process the entire Media server data traffic of OpenScape Voice. Load balancing is achieved for a branch by assigning it an additional Media server and configuring all Media servers of the branch for load balancing.

In case of a failure and depending on the failure type, the following happens:

- Node Failure

  If an OpenScape Voice node fails, the partner node adopts its function. The MGCP signaling manager on the partner node still uses the Media servers like it did before the failure.
- Media Server Failure

  If one of the three active Media servers fails, OpenScape Voice registers this event. If the branch has its own backup, OpenScape Voice uses this Media server from then on. If the branch does not have its own backup or the backup server fails as well, OpenScape Voice uses the central backup Media server. Existing connections to the failed Media server are not switched over and drop away.
- Failure of a Branch

  If a branch fails completely, the other branches carry on using their own Media servers and are not affected by the failure.
- WAN Failure

  If the WAN connection to a specific branch collapses, the branch concerned cannot receive tones and system announcements. The subscribers isolated in the branch can still use the Media server inasmuch as they are registered with an OpenScape Voice edge system anew.

  The other branches are not affected by the failure.

Support of Several Languages

Each local backup Media server must be configured for all languages required by the different associated Media servers of the branches. The central backup Media server must be configured for all languages required by the different Media servers of the branches.

5.4 Media Server Deployment Scenarios at OpenScape Voice

OpenScape Voice supports different alternatives for connecting Media servers. The defined, general routing mechanisms of the OpenScape Voice system determine the Media server that OpenScape Voice supports in the respective situation.

Depending on the general arrangement of the OpenScape Voice system and its load behavior, various realization alternatives exist for the following areas of the Media server planning:

- Assignment of a Media server to a specific area
- Assignment of a Media server to a specific branch
- System redundancy
- Load distribution
- Backup in case of an error

Though this freedom in planning offers a large number of realization alternatives for Media servers, each selected alternative can be assigned to one of the following basic Media server deployment scenarios:

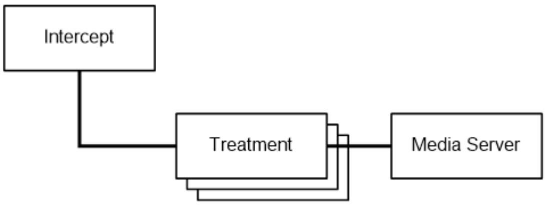
- Central Media server deployment scenarios
- Distributed Media server deployment scenarios

The respective Media server deployment scenario determines in which way OpenScape Voice must be configured for the selected realization alternative.

Central Media server deployment scenarios

A central Media server deployment scenario is based on one of the following routing mechanisms:

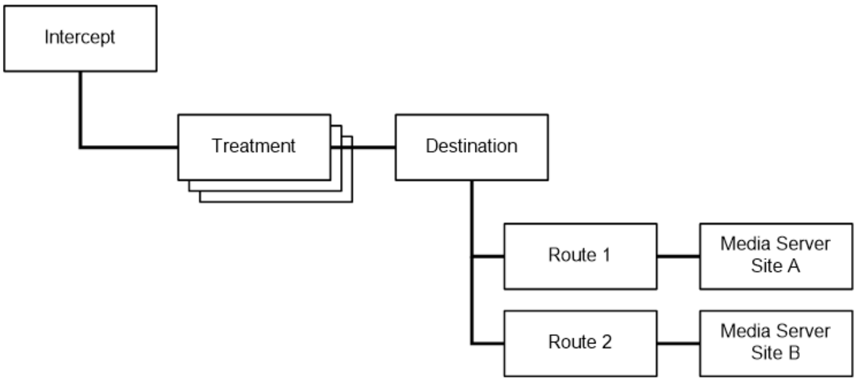
- In case of deployment scenarios with a single Media server, calls are directly routed to the configured Media server gateway.



The following OpenScape Voice deployment scenarios are based on a central Media server deployment scenario with a single Media server gateway:

  - Integrated Simplex and Standard Simplex deployment scenarios
  - Standard Duplex deployment scenarios without geographic separation with a single external OpenScape Media Server
  - Any other individual OpenScape Voice deployment scenario that uses a single Media server gateway

- In case of deployment scenarios with several Media servers, call routing is based on destinations. The Media servers work as redundancy or for load distribution in all routing areas.



The following OpenScape Voice deployment scenarios are based on a central Media server deployment scenario with destinations:

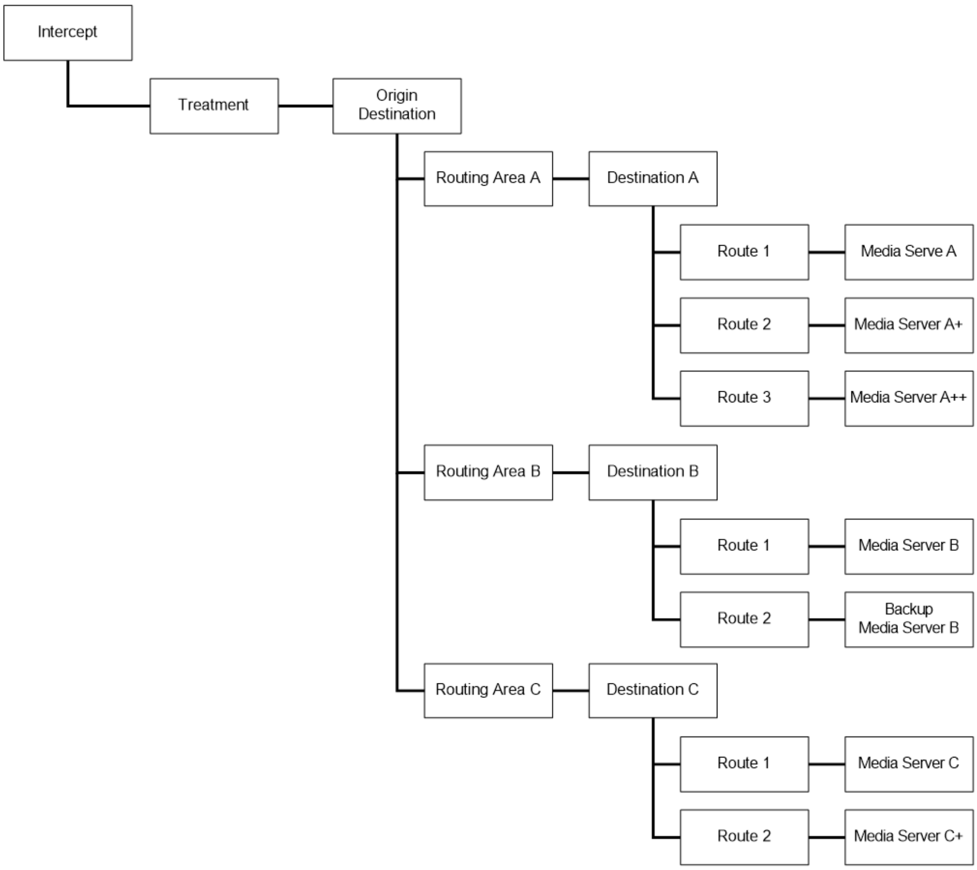
  - Integrated Duplex deployment scenarios without geographic separation with two integrated OpenScape Media Servers
  - Any other individual OpenScape Voice deployment scenario that uses two or more Media servers for redundancy or for load balancing, and that does not require routing.

Distributed Media server deployment scenarios

Distributed Media server deployment scenarios route calls on the basis of an origin destination. Routing occurs according to the routing areas of the following units that are involved in a call, and according to the assigned Media server destination:

- Subscriber
- Location

- Branch



The following OpenScape Voice deployment scenarios are based on a distributed Media server deployment scenario:

- All geographically separated systems with routing based on routing areas of subscribers or locations
- All systems that use the branch concept
- Any other individual OpenScape Voice deployment scenario with more than one Media server gateway and routing based on routing areas

Related concepts

Conferences on page 405

5.4.1 Configuration of a Central Deployment Scenario with One Media Server

In case of a central Media server deployment scenario with a single Media server, calls are directly routed to the configured Media server gateway.

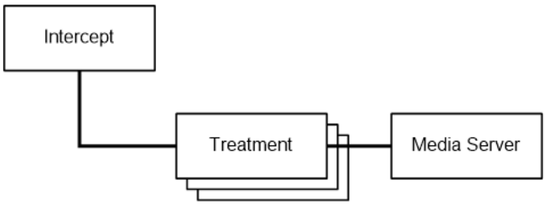


Figure 49: Configuration Representation of a Central Deployment Scenario with One Media Server

The depicted example shows the following structure:

- One Media server has been configured.
- One dropping consists of up to three consecutive treatments.
- Each treatment is assigned to the Media server.

The configuration of a central Media server deployment scenario with a single Media server is divided into the following steps:

- Step 1: How to add a Media server
- Step 2: How to edit Extended options
- Step 3: How to configure circuits
- Step 4: How to assign treatments to the Media server
- Step 5: How to activate the Audit

5.4.2 Configuration of a Central Deployment Scenario with Several Media Servers

In a central Media server deployment scenario with several Media servers, calls are routed based on destinations. The Media servers work as redundancy or for load distribution in all routing areas.

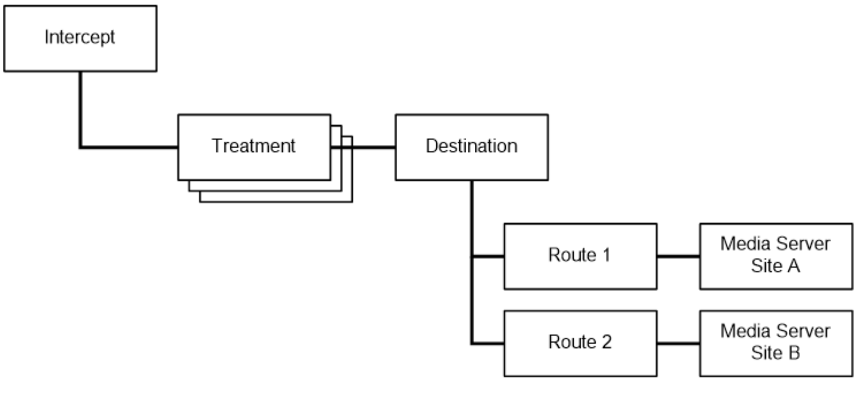


Figure 50: Configuration Representation of a Central Deployment Scenario with Two Media Servers

The depicted example shows the following structure:

- Two Media servers are configured as redundancy to each other or working in the load balancing.
- One dropping consists of up to three consecutive treatments.
- Each treatment is assigned to a target.
- Two routes are connected to the destination – one per Media server.

The configuration of a central Media server deployment scenario with several Media servers is divided into the following steps:

- Step 1: How to add Media servers
- Step 2: How to edit Extended options
- Step 3: How to configure circuits
- Step 4: How to add a destination
- Step 5: How to configure the redundancy / load balancing
- Step 6: How to assign treatments to the destination
- Step 7: How to activate the audit

From V7 onwards if the first connection to an Media Server (MGCP MS) fails OSV attempts to connect to a different Media Server.

5.4.3 Configuration of a Distributed Deployment Scenario without Branches

In a distributed Media server deployment scenario without branches, calls are routed to the desired Media servers on the basis of subscriber-related routing areas.

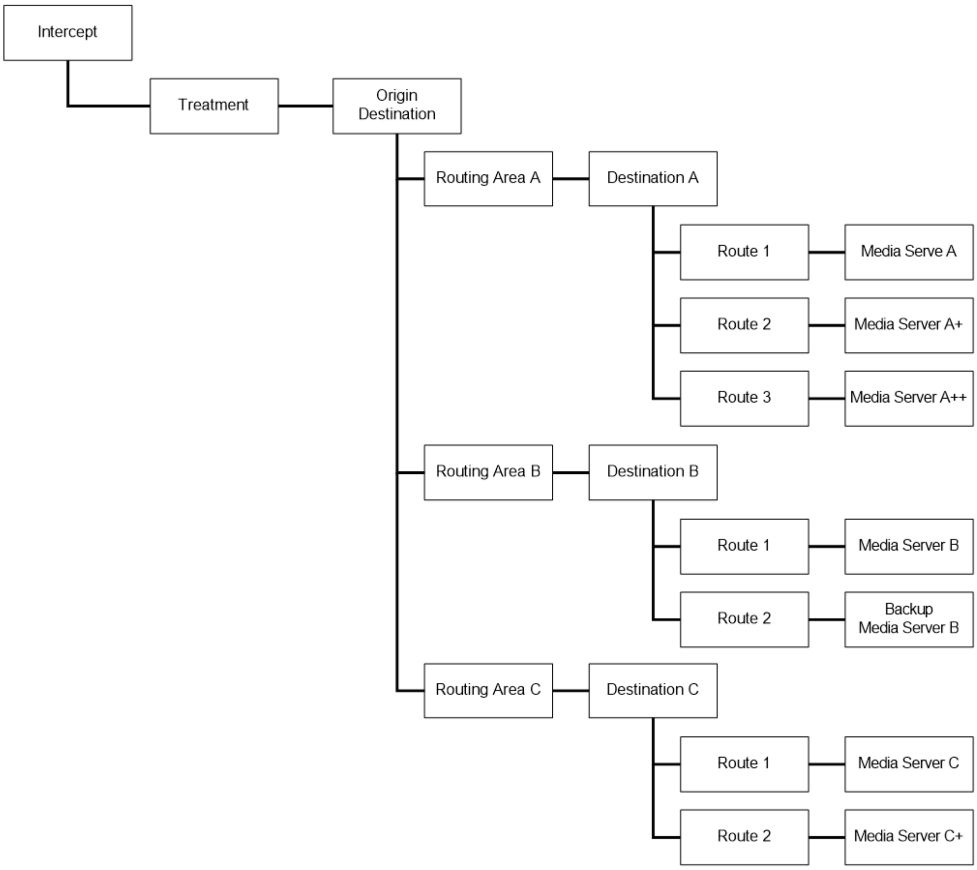


Figure 51: Configuration representation of a distributed deployment scenario without branches

The depicted example shows the following structure:

- Two Media servers are configured as redundancy to each other or working in the load balancing.
- One dropping consists of up to three consecutive treatments.
- Each treatment is assigned to an origin destination according to the routing area of the caller.
- Several routing areas are assigned to the origin destination.
- One destination is assigned to each routing area.
- Several routes are connected to the destination – one per Media server.

The configuration of a distributed Media server deployment scenario without branches is divided into the following steps:

- Step 1: How to add Media servers
- Step 2: How to edit Extended options
- Step 3: How to configure circuits
- Step 4: How to add destinations
- Step 5: How to add an origin destination
- Step 6: How to configure the redundancy / load balancing
- Step 7: How to assign treatments to the origin destination
- Step 8: How to activate the audit

5.4.4 Initial Configuration of a Distributed Deployment Scenario with Branches

The branch concept enables the configuration of several Media servers for each branch. But this concept also always requires the configuration of at least one central Media server that is independent from branches. This server is used for subscribers not configured in branches. This Media server also serves as redundancy for the Media servers at branches.

NOTICE:

You can migrate an existing Media server deployment scenario to a distributed Media server deployment scenario with branches. The decisive advantage of such a migration against a complete reconfiguration is: You transfer existing announcement adjustments for default and individual treatments to the new deployment scenario.

In a distributed Media server deployment scenario with branches, not every Media server needs to provide all available lines. Instead, announcements can e. g. be provided by the respective Media servers of the branches, while the central Media server enables the conference feature. Since the central Media server operates as redundancy for the Media servers of the branches, you need to configure all circuits for this server that are configured for the single Media servers of the branches.

The configuration of a distributed Media server deployment scenario with branches is divided into the following steps:

- Step 1: How to Add Media Servers
- Step 2: How to Edit Extended Options
- Step 3: How to Configure Circuits

- Step 4: How to Modify / Add Routes to the Central Media Server
- Step 5: How to Assign Media Servers to a Branch
- Step 6: How to Configure Redundancy / Load Balancing
- Step 7: How to Assign Announcement Treatments to their Origin Destination
- Step 8: How to Activate the Audit

You can configure the appropriate treatments for this Media Server deployment scenario automatically via the `msconf.sh` script.

NOTICE:

For more information about the automated configuration, refer to *OpenScape Media Server V7, Administrator Documentation*

5.4.5 Migration of an existing Deployment Scenario to a Scenario with Branches

You can migrate an existing Media Server deployment scenario to a distributed Media Server deployment scenario with branches. The decisive advantage of such a migration against a complete reconfiguration is: You transfer existing announcement adjustments for default and individual treatments to the new deployment scenario.

We divide the migration of an existing deployment scenario to a distributed deployment scenario with branches into the following steps:

- Step 1: How to Modify / add Media Servers
- Step 2: How to Modify / Configure Lines
- Step 3: How to Modify / add Routes to the Central Media Server
- Step 4: How to Assign Media Servers to a Branch
- Step 5: How to Configure Redundancy / Load Balancing
- Step 6: How to Activate the Audit
- Step 7: How to Change the Destination for Announcement Treatments

Related concepts

Initial Configuration of a Distributed Deployment Scenario with Branches

5.5 Configuration Concept of the OpenScape Media Server

The configuration concept of the OpenScape Media Server is based on the configuration of the following areas: configuration of the provider modules, configuration of the address bindings, system resource management.

- Configuration of the provider modules

  Defines the behavior of different provider modules of the OpenScape Media Server. The following providers of the OpenScape Media Server have settings that you can configure:

  – MGCP provider

    The MGCP provider makes available an interface of the Media Gateway Control Protocol (MGCP), that corresponds to standard RFC

2705. It interprets the commands sent via the MGCP interface to the OpenScape Media Server for controlling. Playback requests or standard announcement creation is thereby transferred to the relevant services of the OpenScape Media Server. These services then take over the further processing.

– Streaming provider

  The Streaming provider manages and processes the payload of existing real-time connections edited by the OpenScape Media Server. For the Real Time Transport Protocol (RTP) streaming it uses the native auxiliary process Native RTP Unit. This maximizes the number and quality of media streams that are processed by the OpenScape Media Server in real time.

– SIP provider

  The OpenScape Media Server uses the SIP provider to control connections that are based on the Session Initiation Protocol (SIP). The SIP provider also contains all features for registering SIP devices.

  NOTICE:

  Configuring the SIP provider in the OpenScape Media Server is only possible if the OpenScape Media Server is used under OpenScape UC Application.

– MRCP provider

  Via the MRCP provider the OpenScape Media Server can control external TTS software. The MRCP provider uses the Media Resource Control Protocol (MRCP) for this purpose.

  NOTICE:

  Configuring the MRCP provider in the OpenScape Media Server is only possible if the OpenScape Media Server is used under OpenScape UC Application.

– Prompt-Database provider

  The Prompt-Database provider replicates customized welcome and name announcements of the voice portal automatically to all other OpenScape Media Server of a Media server farm.

  NOTICE:

  Replicating voice portal announcements by the Prompt-Database provider can only be configured in the OpenScape Media Server if the OpenScape Media Server is used under OpenScape UC Application.

– Resource Management provider

  You can use the system resource management of the Resource Management provider to proportionately assign operation-critical system resources to individual media applications of the OpenScape Media Server.

- Configuration of the terminals

  A terminal is merely a logical configuration unit within the OpenScape Media Server. It can be best compared with the logical configuration of a terminal device in a PBX.

  NOTICE:

  Configuring terminals in the OpenScape Media Server is only possible if the OpenScape Media Server is used under OpenScape UC Application.

- Configuration of the address bindings

  Specifies which media applications of the OpenScape Media Server can be reached under which phone number.

  NOTICE:

  Configuring address bindings in the OpenScape Media Server is only possible if the OpenScape Media Server is used under OpenScape UC Application.

Configuration of the provider modules

You configure the provider modules of the OpenScape Media Server in the Common Management Platform of OpenScape by default. The settings performed in this way are not stored in the Common Management Platform itself, though, but in the different configuration files of the provider modules.

The following table provides an overview of the configuration files available in the OpenScape Media Server for provider modules.

Providers	Configuration file	Storage location [4]
MGCP provider	mgcp.xml	`/application_host/providers/mgcp`
Streaming provider	streaming-mps.xml	`/application_host/providers/streaming-mps`
SIP provider [5]	sip-connectivity.xml	`/application_host/providers/sip-connectivity`

Besides the settings that you can make in the Common Management Platform, further expert settings exist for the OpenScape Media Server, which are also managed in the described configuration files. These expert settings are

[4] Is based on the directory in which you install the OpenScape Media Server.

[5] Only available in combination with OpenScape UC Application.

already preconfigured in a way that they need not be modified during the usual OpenScape Media Server operation.

Configuration of the address bindings

NOTICE:

Configuring address bindings in the OpenScape Media Server is only possible if the OpenScape Media Server is used under OpenScape UC Application.

Which OpenScape Media Server media application can be reached under which phone number is specified in the so-called address bindings. You configure address bindings in the Common Management Platform of OpenScape UC Application.

Each address binding contains the following information:

- A terminal

  A so-called terminal is assigned the Uniform Resource Identifier (URI) of a media application and at least one phone number expression. This results in an individual assignment of URI and phone number expressions. The terminal is solely a logical configuration unit within the OpenScape Media Server. It can be best compared with the logical configuration of a terminal device in a PBX, which is also assigned specific attributes – e. g. phone numbers.
- Binding attributes

  Specify different properties that determine the communication behavior of the relevant address binding. The binding attributes include, for example, security and codec settings.
- General properties

  Specify media-application-individual settings transferred to the relevant media application when being invoked. Via these settings you can e. g. control the default language of the voice portal.

  General properties influence only the behavior of the media application and do not serve any other purpose in the OpenScape Media Server.
- At least one phone number expression

  Each phone number expression specifies at least one phone number under which the relevant media application is to be reached in the OpenScape Media Server.

  Example: `regexp:sip:+492404901100@.*`

  NOTICE:

  Specify phone numbers always fully qualified in the Global Number Format (GNF) when you use the OpenScape Media Server at OpenScape Voice – example: +492404901100.

Related concepts

System Resources Management on page 409

5.6 Expert Settings of the OpenScape Media Server

Besides the OpenScape Media Server settings, which you can configure in the Common Management Platform, there are more expert settings for various OpenScape Media Server providers. These expert settings are administered in the configuration file of the relevant provider.

The following sections show all expert settings that influence the behavior of the different OpenScape Media Server provider.

For the time being, this concerns the following providers:

- SIP provider

  NOTICE:

  Configuring the SIP provider in the OpenScape Media Server is only possible if the OpenScape Media Server is used under OpenScape UC Application.

- Streaming provider

5.6.1 Expert Settings of the SIP Provider

The following list shows all expert settings that influence the SIP provider behavior.

The expert settings are administered in the following configuration file:

<MS-install [6]>`/application_host/providers/sip-connectivity/sip-connectivity.xml`

NOTICE:

Configuring the SIP provider in the OpenScape Media Server is only possible if the OpenScape Media Server is used under OpenScape UC Application.

- **fallbackToMasterSipServerTime**
  - Default setting: `0 [seconds]`
  - Possible values:

    <1 … 604800> [seconds]

    `0` – deactivates the fallback mechanism

  If the Master SIP server is not operable any more, the SIP provider uses an alternative SIP server (if configured).

  fallbackToMasterSipServerTime specifies the period after which the SIP provider falls back to the Master SIP server, provided, this server is operable again. Start time for the timer is the switch-back to the alternative SIP server.

[6] setup directory of the OpenScape Media Server: `/enterprise/mediaserver/` or `/opt/siemens/mediaserver/`.

- **InboundConnectionAcceptanceTimeout**
  - Default setting: `4000 [ms]`
  - Possible values:

    <Time> [ms]

    `0` – deactivates the time-out mechanism

    NOTICE:

    This setting must not be modified!

  Specifies the period within which the SIP provider expects a reply to inbound calls from internal applications. If an internal application does not answer within this period, the SIP provider transfers the incoming call to other internal, available processes or rejects it as impossible to rout (SIP response “Not found”).
- **InboundConnectionOfferTimeout**
  - Default setting: `600 [ms]`
  - Possible values:

    <Time> [ms]

    `0` – deactivates the time-out mechanism

    NOTICE:

    This setting must not be modified!

  Defines the period within which a correct address binding must be determined for incoming calls. If no correct address binding can be determined within this period, the SIP provider transfers the incoming call to other internal, available processes or rejects it as impossible to rout (SIP response “Not found”).
- **keepAliveRequestInterval**
  - Default setting: `180 [ms]`
  - Possible values:

    <Time> [ms]

    `0` – deactivates the Keep-Alive mechanism

  The SIP provider uses a keep-alive mechanism to check whether the Master SIP server is still operable.

  keepAliveRequestInterval defines in which intervals the SIP provider sends keep-alive-requests to the Master SIP server.

- **keyStore**
  - Default setting: `tls-keystore.jks`
  - Possible values: <path and file name of the keystore>

  Defines the name of the keystore the certificate of which is used by the OpenScape Media Server for the TLS communication.

  The specified keystore must contain a valid certificate for the OpenScape Media Server, which is signed by the root CA and a root certificate of OpenScape Voice.

  The keystore used must be contained in the following directory:

  ```
  osgi\config-beans\host\providers\sip-connectivity
  ```
- **keyStore**Password
  - Default setting: –
  - Possible values: <password>

  To access the keystore configured under **keyStore**, the OpenScape Media Server uses the “password” password by default.

  If the configured keystore uses another password, you need to add the setting **keyStorePassword** to the configuration file and configure in it the password of the keystore used.
- **keyStoreType**
  - Default setting: –
  - Possible values: <file suffix>

  To access the keystore specified under **keyStore**, the OpenScape Media Server uses the database type jks by default.

  If the configured keystore uses another keystore type, you need to add the setting **keyStoreType** to the configuration file and configure in it the database type of the keystore used.

- **listeningPoint**
  - Default setting:

    `<listeningPoint>*:5060/UDP</listeningPoint>`

    `<listeningPoint>*:5060/TCP</listeningPoint>`

    `<listeningPoint>*:5061/TLS</listeningPoint>`
  - Possible values: <list of single listening points>

    NOTICE:

    For each available transport protocol you can configure one listening point at the most.

  Defines the communication settings for the inbound OpenScape Media Server SIP communication in the form of so-called listening points.

  Each listening point consists of the following settings:

  - IP address via which the OpenScape Media Server communicates for the listening point.

    If the host name of the associated computer system can be resolved into an IP address in the network, you can also enter the associated fully qualified host name instead of the IP address.
  - Port on which the OpenScape Media Server receives the data for the relevant listening point.
  - Transport protocol the OpenScape Media Server uses for the listening point.

  These single settings are combined in the form of a listening point, with the OpenScape Media Server using the following format:

  <IP address / host name> : <port number> / <transport protocol>

  If you configure the * character as IP address/host name of a listening point, the OpenScape Media Server uses for the relevant listening point the IP address of the first network board in the computer system.
- **outboundProxy**
  - Default setting: –
  - Possible values:

    <IP Address>

    <fully qualified host name>

  The SIP server may only be accessible via an outbound proxy server. In such a case you can add the **outboundProxy** setting in the configuration file to configure the address of the outbound proxy server.

- **sipServer**

  NOTICE:

  Is configured via the Common Management Platform.

  Defines the data of the SIP servers that the OpenScape Media Server uses for outgoing SIP communication. The following information is specified for each SIP server used:

  – IP address of the SIP server

    If the host name of the associated computer system can be resolved into an IP address in the network, you can also enter the associated fully qualified host name instead of the IP address.

  – Port to which the OpenScape Media Server sends the data for the relevant SIP server.

  – Transport protocol that the OpenScape Media Server uses for the relevant SIP server.

  These single settings are compiled for each SIP server in the following format and specified in one line:

  <IP address / host name> : <port number> / <transport protocol>

  The preferred SIP server appears in the first line.

- **sipSessionTimerExpiration**

  – Default setting: `0` [seconds]

  – Possible values:

    <time> [seconds]

    `0` – deactivates the Keep-Alive mechanism

  The SIP provider can send refresh requests for SIP connections.**sipSessionTimerExpiration** defines, in which intervals the SIP provider sends these refresh requests.

5.6.2 Expert Settings of the Streaming Provider

The following list shows all expert settings that influence the Streaming provider behavior.

The expert settings are administered in the following configuration file:

<MS-install [7]>`/application_host/providers/streaming-mps/streaming-mps.xml`

[7] setup directory of the OpenScape Media Server: `/enterprise/mediaserver/` or `/opt/siemens/mediaserver/`.

- **aliveTimeout**
  - Default setting: `60`
  - Possible values: <time> [seconds]

  Controls the watchdog process, with which the Java Media Framework monitors the process of the native RTP unit.

  aliveTimeout defines a period in which the native RTP unit process must answer. If it fails to do so, it is automatically restarted.
- **defaultLocale**
  - Default setting: `en`
  - Possible values: <language code>

  Defines the language the greetings and tones of which the Streaming provider uses if no language has been specified when OpenScape Voice requests a playback.
- **defaultOptions**
  - Default setting: `-a 0x000700040 -k`
  - Possible values: <command>

  Specifies a text string that is transferred to the native RTP unit as command line command.

  The command interface of the native RTP unit determines the commands that can be transferred here.
- **eventThreadpoolSize**
  - Default setting: `5`
  - Possible values: <number>

  Specifies the size of the event thread pool for the Java Media Framework. This pool processes all events sent to the Java Media Framework by the native RTP unit.
- **fallbackLanguage**
  - Default setting: `5`
  - Possible values: Comma-separated list of the format:

    <four-digit language code > = <language code >

  NOTICE: This can only be used for languages for which a language version has been prioritized with **preferredLanguage**.

  The OpenScape Media Server can play tones and announcements of the respective country from a language packet that contains individual tones as well as individual announcements of this country.

  If a language packet contains only the individual tones of the respective country, the OpenScape Media Server can access only the associated tones. So that also announcements can be played in the relevant language, you need to configure from which alternative language package it shall take them. The announcement language of this alternative language packet is also called fallback language.

Example of Hongkong:

`<preferred-language>zh_hk </preferred-language>`

Defines that the OpenScape Media Server uses the language variety Hongkong for Chinese.

`<fallbackLanguage>zh_hk=en_us</fallbackLanguage>`

Defines that the OpenScape Media Server uses (US) English greetings for the language variety Hongkong.

- **icmpMonitoringEnabled**
  - Default setting: `false`
  - Possible values:

    `true` – activates the ICMP monitoring

    `false` – deactivates the ICMP monitoring

  Network components use the Internet Control Message Protocol (ICMP) for exchanging diagnostics data via the internet protocol. A router may return e.g. ICMP messages to a data source if it needs to dismiss packets of this data source.

  icmpMonitoringEnabled defines whether or not the OpenScape Media Server ICMP monitoring is active.

  When the ICMP monitoring of the OpenScape Media Server is active, the OpenScape Media Server reacts to ICMP messages it receives from the network. If the number of received ICMP messages exceeds a threshold, the Media Server sends appropriate messages to its applications. The applications can to react to this by temporarily stopping or reducing the send activities.

  The described threshold is determined by **icmpMonitoringEnabled**.
- **icmpUnreachableCount**
  - Default setting: `200`
  - Possible values: <time> [seconds]

  If the OpenScape Media Server ICMP monitoring is active (`icmpMonitoringEnabled = true`), the OpenScape Media Server reacts to ICMP messages it receives from the network. If the number of received ICMP messages exceeds a threshold, the Media Server sends appropriate messages to its applications. The applications can to react to this by temporarily stopping or reducing the send activities.

  icmpUnreachableCount defines the amount of the described threshold. The counter for this threshold is reset after a period defined by **icmpRecoveryTime**.
- **icmpRecoveryTime**
  - Default setting: `10`
  - Possible values: <time> [seconds]

  If the OpenScape Media Server ICMP monitoring is active (`icmpMonitoringEnabled = true`), the OpenScape Media Server reacts to ICMP messages it receives from the network. If the number of received ICMP messages exceeds a threshold, the Media Server sends appropriate messages to its applications. The applications can to react to this by temporarily stopping or reducing the send activities.

icmpRecoveryTime defines the time after which the counter for the described threshold is reset.

- **internalFormatList**
  - Default setting: `audio/L16 audio/PCMU audio/PCMA audio/G729`
  - Possible values: Blank-separated list of settings of the following list in the form audio/<format setting>:

    `L16` – Linear16 Bit

    `PCMU` – µ-Law G.711

    `PCMA` – A-Law G.711

    `G729` – G.729

  Defines the audio formats to be used by the OpenScape Media Server.
- **ipAddrMediaServer**

  NOTICE:

  Is configured via the Common Management Platform.

  Defines the IP address that the OpenScape Media Server uses on the computer system for the RTP communication.

  If the host name of the associated computer system can be resolved into an IP address in the network, you can also enter the associated fully qualified host name instead of the IP address.
- **keep-session-open**
  - Default setting: `false`
  - Possible values:

    `true` – TTS session stays open during the connection.

    `false` – TTS session will be closed after the TTS playback.

  NOTICE:

  Set the **false** option here. This reduces the number of TTS licenses the system requires for operation.

  Defines how the OpenScape Media Server handles a connection to the TTS system:
  - Whether it closes the connection after the requested greeting was played via the TTS system.
  - Whether it keeps the connection open until the phone connection that the OpenScape Media Server has opened for the relevant TTS connection is closed.
- **maxG729Proportion**
  - Default setting: `100`
  - Possible values: <0 ... 100> [%]

  Defines which proportion of **numRtpPorts** the OpenScape Media Server may use for G.729 channels at the most. When calculating the increased computing power for a G.729 channel against a G.711 channel please note: A G.729 channel requires the computing power of three G.711 channels.

Example: **numRtpPorts** = 500 [channels], **maxG729Proportion** = 35 [%]

This results in a proportion of 500 ×0,35 = 175 G.711 channels for G.729 channels.

Since each G.729 channel requires the computing power of three G.711 channels, up to 175 / 3 = 58 G.729 channels can be used in this example.

- **multipart-support**
  - Default setting: `-`
  - Possible values:

    `true` – Send Multipart MIME messages

    `false` – do not send any Multipart MIME messages

  Defines whether the OpenScape Media Server can send multipart MIME messages to the ASR or TTS system used.

- **nativeRtpUnitUse10msSched**
  - Default setting: `false`
  - Possible values:

    `true` – 10 ms

    `false` – 20 ms

  Defines the package size used by the OpenScape Media Server.

- **nativeRtpUnitUseLowPrioScheduling**
  - Default setting: `0`
  - Possible values:

    `0` – REALTIME_PRIORITY_CLASS

    `1` – HIGH_PRIORITY_CLASS

  Specifies the process/thread priority used by the native RTP unit.

- **nativeRtpUnitUseRtcClock**
  - Default setting: `true`
  - Possible values:

    `true` – Linux RealTimeClock

    `false` – SystemClock

    IMPORTANT:

    This setting must not be modified in productive systems!

  Defines how the OpenScape Media Server synchronizes the RTP communication.

- **noRtpStreamTimeout**
  - Default setting: `15`
  - Possible values: <time> [seconds]

  Defines a period in which the Streaming provider expects an RTP packet for and RTP connection. If the Streaming provider does not register an RTP package in this period, it may send RTP-Stream-Absent messages to the application layer.

Sending the above RTP-Stream-Absent messages is activated by the **rtpStreamMonitoringEnabled** setting.

- **numberOfProxyObjects**
  - Default setting: `5000`

  Specifies the maximum size of the MFW-Object-Request-Brocker.
- **numMaxRtpPorts**
  - Default setting: `500`
  - Possible values: <= **numRtpPorts**

  IMPORTANT:

  Depends on the hardware you use for the OpenScape Media Server.

  Defines the maximum permissible number of RTP channels that may be configured for the OpenScape Media Server RTP communication.

  The value set here thus represents the top limit of the setting under **numRtpPorts**.
- **numRtpPorts**

  NOTICE:

  Is configured via the Common Management Platform.

  Defines the maximum number of UDP ports that the OpenScape Media Server uses for the RTP transmission of media streams.
- **preferred-format**
  - Default setting: `-`
  - Possible values:

    `G711u`

    `G711a`

    `G729`

  Defines the RTP streaming format that the OpenScape Media Server announces to the MRCP server as preferred format.
- **preferred-language**
  - Default setting: `-`
  - Possible values: Comma-separated list <four-digit language codes >

  Several language varieties can be installed on the OpenScape Media Server for one OpenScape Voice language ID. For example, the language varieties India (en_in) and USA (en_us) for the OpenScape Voice language ID en. In this case the **preferred-language** setting lets you define the language varieties to be used for the associated OpenScape Voice language ID. This is reasonable when you want to use a language variety the code of which consists of four letters for a basic language.

- **recordingSensitivity**
  - Default setting: `50`
  - Possible values: <0 ... 100> [%]

  The OpenScape Media Server uses a voice recorder for voice recordings.

  If this voice recorder operates in the automatic recording mode, **recordingSensitivity** defines the sensitivity for detecting the end of the recording.
- **rfc2833-payload-type**
  - Default setting: `-`
  - Possible values: <encoding according to RFC 2833>

  Defines the payload type used by the Streaming provider for sending RFC 2833 events to the ASR engine.
- **rootFolder**
  - Default setting: `root:///resources/waveRoot`
  - Possible values: <directory path>

  Defines the directory on the OpenScape Media Server computer system in which the greetings and tones for OpenScape Voice are stored. The Streaming provider uses this specification to form absolute path specifications from relative ones.

  The root schema defines that the specified path refers to the root directory of the Application Host. As alternative to the **rootFolder** setting you can also use the file schema.
- **rtpPortRangeStart**

  NOTICE:

  Is configured via the Common Management Platform.

  Defines the first UDP port of the port range used by the OpenScape Media Server for the RTP-based transmission of the media streams.
- **rtpBlacklistedTime**
  - Default setting: `500`
  - Possible values: <0 ... 100>

  The OpenScape Media Server uses an RTP port scanner to detect and fend off Denial-of-Service attacks. Using this scanner the OpenScape Media Server searches all officially free RTP ports for suspicious communication in a round-robin process. The suspicious communication may be caused by a client with wrong communication behavior or a Denial-of-Service attacker.

  If the RTP port scanner could not detect any suspicious communication on a checked RTP channel, it marks this port as safe and the OpenScape Media Server can use it for its communication. If the RTP port scanner detects suspicious communication on a checked RTP channel, this port is integrated in a black list and not be used by the OpenScape Media Server for a specific period.

  rtpBlacklistedTime specifies how long an individual RTP port is not used by the OpenScape Media Server when the RTP port scanner has detected suspicious communication on this port. After expiration of this period, the port can be used by the OpenScape again.

- **rtpScanDuration**
  - Default setting: `500`
  - Possible values: <0 ... 100>

  The OpenScape Media Server uses an RTP port scanner to detect and fend off Denial-of-Service attacks. Using this scanner the OpenScape Media Server searches all officially free RTP ports for suspicious communication in a round-robin process. This involves groups of RTP ports.

  If the RTP port scanner could not detect any suspicious communication on a checked RTP channel, it marks this port as safe and the OpenScape Media Server can use it for its communication.**rtpScanDuration** defines, how long the RTP port scanner searches a group of RTP channels for suspicious communication per round-robin cycle.
- **rtpScanWindowSize**
  - Default setting: `500`
  - Possible values:

    0 – deactivates the RTP port scanner

    <1 ... 100>

  The OpenScape Media Server uses an RTP port scanner to detect and fend off Denial-of-Service attacks. Using this scanner the OpenScape Media Server searches all officially free RTP ports for suspicious communication in a round-robin process. This involves groups of RTP ports.

  If the RTP port scanner could not detect any suspicious communication on a checked RTP channel, it marks this port as safe and the OpenScape Media Server can use it for its communication.**rtpScanDuration** defines, how long the RTP port scanner searches a group of RTP channels for suspicious communication per round-robin cycle.
- **rtpStreamMonitoringEnabled**
  - Default setting: `false`
  - Possible values:

    `true` – Activates the RTP package monitoring

    `false` – Deactivates RTP package monitoring.

  Defines whether the Streaming provider sends RTP-Stream-Absent messages to the application layer if no RTP packages have been registered for an RTP connection with in a specific period.
- **rtpTypeOfService**

  NOTICE:

  Is configured via the Common Management Platform.

  Defines the quality of service (QoS) used for the RTP communication between OpenScape Media Server and telephones. You can choose from the standardized service qualities.

- **socketManagerRxPort**
  - Default setting: `7000`
  - Possible values: <port number>

  Specifies the receiving port via which the Java portion of the Media Framework receives information from the native portion.
- **socketManagerTxPort**
  - Default setting: `7001`
  - Possible values: <port number>

  Specifies the send port via which the Java portion of the Media Framework sends information to the native portion.
- **zombiObjectTimeout**
  - Default setting: `86400`
  - Possible values: <1 … 604800> [seconds]

  The Media Framework uses a so-called “zombie” scanner that checks in 60-second intervals all assigned / active MFW objects for their topicality. If the scanner finds an object in this search the age of which exceeds a specified period, it is removed from the internal assignment table as so-called “zombie”.

  zombiObjectTimeout defines the length of the described period.

  You can see whether the “Zombie” scanner finds outdated MFW objects when you configure the log level **FINEST** for the following log category:

  com.siemens.media.mfw.native.MfwNativeObjectManager

  Search the log for a line of the following format:

  ```
  start scanning for possible outdated MFW zombi-objects
  (zombis detected till now: '<xxx>' - items in alloc-list
  '<zzz>'
  ```

  In smooth operation, value `0` should always be displayed for `<xxx>`.

  If the “Zombie” scanner finds outdated MFW objects, an error message of the following format is issued:

  ```
  15:02:43,365 ERROR native.MfwNativeObjectManager[]!
  ```

  ```
  MFW object zombi detected .. will be freed!
  ```

5.7 Tones for OpenScape Voice

One of the most prominent Media server features is to provide tones for OpenScape Voice when required. Tones are country-specific; in each country individual requirements on tone frequency, tone duration and pause intervals between the single tone sections apply for tones.

Each tone is realized by a sound file. In such a file, several tone frequencies of different playback length can be combined with specific pause intervals.

Depending on the signaling exchanged between the Media Server and the following instances, a large number of tones can be played:

- Subscriber endpoints

  The Media server plays simple telephone tones when the signaling indicates that this is not possible at the endpoint. Examples of such tones are ringback tone, dial tone, busy tone and call-waiting tone.
- Remote gateways

  The Media Server plays network tones when the signaling indicates that this is not possible at the remote gateway. An example is here the network busy tone, which indicates that calls can currently not be made via the network.

Furthermore, the Media Server is always in charge of playing specific tones – for example:

- An EG-internal busy tone is played under specific error conditions – for example, when the subscriber dials an invalid destination.
- When a person joins or leaves a conference, a zip tone is played.

5.7.1 Supported Countries

The OpenScape Voice system is released for various countries. Consequently, it supports the country-specific tones for each released country.

The country the tones of which OpenScape Voice plays can be specified system-wide for all subscribers or individually for the single subscriber. This specification is valid for tones and system announcements.

The following table shows for which countries OpenScape Voice provides country-specific tones and which Media Server needs to be respectively used.

NOTICE:

The languages listed here do not describe the language support of the media applications provided by the OpenScape Media Server under OpenScape UC Application.

Country	OpenScape Media Server
Argentina	✓
Australia	✓
Belgium	✓
Bosnia and Herzegovina	✓
Brazil	✓
Bulgaria	✓
Chile	✓
China	✓
Colombia	✓

Country	OpenScape Media Server
Denmark	✓
Germany	✓
Ecuador	✓
Estonia	✓
Finland	✓
France	✓
Greece	✓
Great Britain	✓
Hong Kong	✓
India	✓
Indonesia	✓
Ireland	✓
Italy	✓
Japan	✓
Canada	✓
Korea	✓
Croatia	✓
Latvia	✓
Lithuania	✓
Luxembourg	
Malaysia	✓
Morocco	✓
Mexico	✓
New Zealand	
Netherlands	✓
Norway	✓
Austria	✓
Peru	✓

Country	OpenScape Media Server
Philippines	✓
Poland	✓
Portugal	✓
Romania	✓
Russia	✓
Sweden	✓
Switzerland	
Serbia	✓
Singapore	✓
Slovakia	✓
Slovenia	✓
Spain	✓
South Africa	✓
Taiwan	✓
Thailand	✓
Czech Republic	✓
Turkey	✓
Hungary	✓
USA	✓
Venezuela	✓
United Arab Emirates	✓
Vietnam	✓

5.8 System Announcements for OpenScape Voice

One of the most prominent Media server features is to provide system announcements for OpenScape Voice when required. Every system announcement exists for all languages that OpenScape Voice supports. The system announcements can thus be used for each country in which one of the supported language is spoken.

NOTICE:

The system announcements described here are independent from those that the OpenScape Media Server manages for the voice and conference portal of OpenScape UC Application.

A system announcement of OpenScape Voice consists of at least one sound segment played to a subscriber. Besides the sound segments, additional settings can be defined in OpenScape Voice for a system announcement – e. g. how often a sound segment is played to a subscriber or the playback pause between the single sound segments.

OpenScape Voice requests the Media server to play system announcements appropriate for selected events or states. These requests comprise information about the sound files and the relevant target subscriber.

OpenScape Voice is shipped with many default system announcements that can be administered via CLI or OpenScape Voice Assistant. Furthermore, customer-individual system announcements can be created and managed by the system administrator.

Each Media server provides for each supported language a so-called Basic-Announcement-Unit-Set (BAU-Set). These BAU-sets are used for system announcements playback and contain in most cases the following:

- Cardinal numbers
- Ordinal number
- Date and time specifications
- Names for weekdays and months
- Currency names
- Commonly used words – e. g. and, the, etc

The Media server system announcements can be divided in the following main categories:

- Intercept announcements
- Interactive announcements

5.8.1 System Announcement Categories

Media server system announcements can be divided into two categories: intercept announcements and interactive announcements. During the system announcement handling the Media server is controlled by OpenScape Voice for both system announcement types.

Intercept Announcements

OpenScape Voice uses intercept announcements in particular to react to dropped calls. In this way OpenScape Voice can create error announcements or other notes that are played to a subscriber when he/she sets up a connection.

Intercept announcements can be grouped as follows:

- System Announcements with a permanent content – e. g. *The called subscriber is currently not available. Please hang up and try again later.*
- System Announcements with variable contents include at least one individual parameter – e. g. *The phone number 321-9876 you have dialed has changed. The new phone number is 321-6789.*

A OpenScape Voice intercept announcement can consist of up to three tones, system announcements or a combination of these that are all controlled by OpenScape Voice. After OpenScape Voice has requested the Media server to play the system announcement, the Media server performs all required activities independently.

Interactive announcements

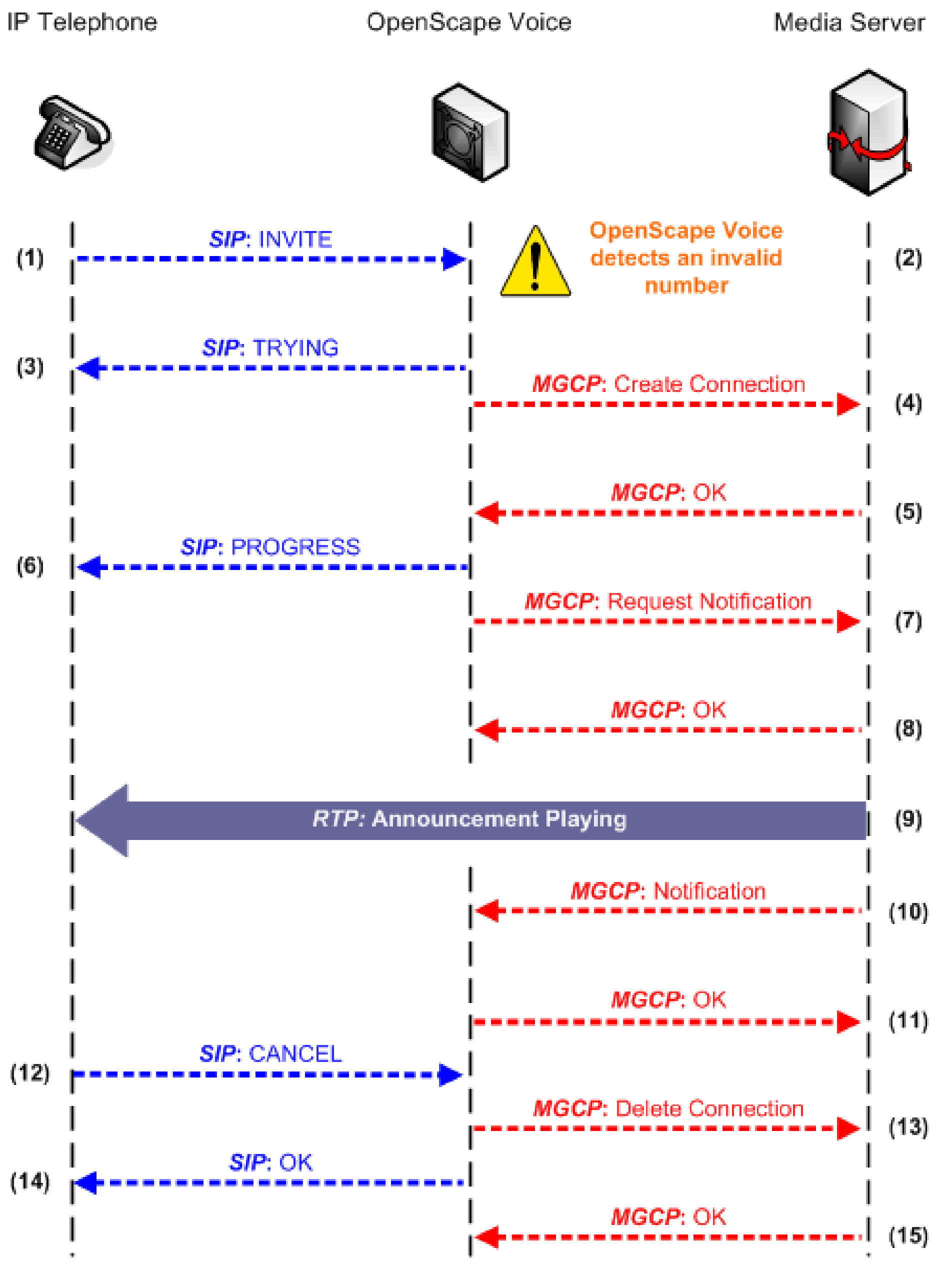
Interactive announcements assume caller actions – e. g. pushing telephone keys to generate DTMF tones or entering voice commands (IVR). Example: *The phone number 321-9876 you have dialed has changed. The new phone number is 321-6789. If you want to be connected to the new phone number, push 1.*

The caller's reaction to the system announcement determines how OpenScape Voice subsequently handles the connection.

5.8.2 System Announcement Playback

OpenScape Voice controls the Media server in a way that it plays system announcements as they are appropriate for individual events or circumstances. In the scope of this control, information is transferred that defines the respective system announcements and the relevant target device.

The following figure illustrates how this controlled announcement playback works by the example of a subscriber who has entered wrong phone numbers.



1) The terminal device establishes a new communication connection via the SIP protocol. In doing so it uses the INVITE command to transfer the desired target phone number to OpenScape Voice.

2) OpenScape Voice identifies the transferred phone number as an invalid information.

3) With a TRYING message, OpenScape Voice signals the terminal device that the desired connection setup is being processed.

4) The system announcement for an incorrect phone number entry must be transferred by OpenScape Voice to the terminal device. To this, OpenScape Voice establishes an individual MGCP connection to control the OpenScape Media Server.

5) The accepts this connection request.

6) With a PROGRESS message, OpenScape Voice signals the terminal device that the requested connection setup is still being processed.

7) OpenScape Voice sends the command REQUESTNOTIFICATION to the OpenScape Media Server and induces it in this way to send the desired system announcement to the relevant terminal device. In this process the following information is transferred:

- the ID of the system announcement the OpenScape Media Server is to transmit to the terminal device.
- the ID of the language in which the system announcement is to be played.
- the IP address of the terminal device to which the specified greeting is to be sent.

8) The OpenScape Media Server confirms receipt of the sent information.

9) Subsequently, the OpenScape Media Server transmits the specified system announcement to the terminal device through an independent RTP connection.

10) After the greeting has been transmitted, the OpenScape Media Server informs the OpenScape Voice in a NOTIFICATION message accordingly.

11) OpenScape Voice confirms receipt of the sent message.

12) The terminal device closes the connection to OpenScape Voice.

13) OpenScape Voice closes the connection to the OpenScape Media Server.

14) OpenScape Voice confirms that the connection to the terminal device is closed.

15) OpenScape Media Server confirms that the connection to OpenScape Voice is closed.

5.8.3 Supported Languages for System Announcements

The OpenScape Voice system is released for various countries. Consequently, it supports the country-specific tones for each released country. In contrast, country-specific system announcements are not provided for each released country. If no system announcements are available in a country-specific language, an alternative announcement language can be configured for this country. This can be a language also commonly used in the relevant country.

The language in which OpenScape Voice plays system announcements can be specified system-wide for all subscribers or individually for the single subscriber. This specification is valid for tones and system announcements.

The following table shows:

- For which countries OpenScape Voice is released
- Which announcement language / alternative announcement language is recommended for the respective country
- Which Media server supports the respective announcement language / alternative announcement language

NOTICE:

The languages listed here do not describe the language support of the media applications provided by the OpenScape Media Server under OpenScape UC Application.

Country	Language / alternative language	OpenScape Media Server
Argentina	Spanish (Argentina)	✓
Australia	English (UK)	✓
Austria	German	✓
Belgium	French, German, Dutch	✓ / ✓ / ✓
Bosnia and Herzegovina	Serbian	✓
Brazil	Portuguese (Brazil)	✓
Bulgaria	Bulgarian	✓
Canada	French (Canada)	✓
Chile	Spanish (Argentina)	✓
China	Chinese	✓
Colombia	Spanish (Mexico)	✓
Croatia	Croatian	✓
Czech Republic	Czech	✓
Denmark	Danish	✓
Ecuador	Spanish (Mexico)	✓
Estonia	Estonian	✓
Finland	Finnish	✓
France	French	✓
Germany	German	✓
Great Britain	English (UK)	✓
Greece	Greek	✓
Hong Kong	English (U. S.)	✓
Hungary	Hungarian	✓
India	English (UK)	✓
Indonesia	English (U. S.)	✓
Ireland	English (UK)	✓
Italy	Italian	✓
Japan	English (U. S.)	✓

Country	Language / alternative language	OpenScape Media Server
Korea	English (U. S.)	✓
Latvia	Latvian	✓
Lithuania	English (UK)	✓
Luxemburg	French	
Malaysia	English (U. S.)	✓
Mexico	Spanish (Mexico)	✓
Morocco	French	✓
Netherlands	Dutch	✓
New Zealand	English (UK)	
Norway	Norwegian	✓
Peru	Spanish (Mexico)	✓
Philippines	English (U. S.)	✓
Poland	Polish	✓
Portugal	Portuguese	✓
Romania	Romanian	✓
Russia	Russian	✓
Serbia	Serbian	✓
Singapore	English (U. S.)	✓
Slovakia	Slovakian	✓
Slovenia	Slovenian	✓
South Africa	English (UK)	✓
Spain	Spanish / Catalan / Basque	✓ / ✓ ✓
Sweden	Swedish	✓
Switzerland	French, German, Italian	
Taiwan	English (U. S.)	✓
Thailand	English (U. S.)	✓
Turkey	Turkish	✓
United Arab Emirates	Arabic	✓

Country	Language / alternative language	OpenScape Media Server
USA	English (U. S.)	✓
Venezuela	Spanish (Mexico)	✓
Vietnam	English (U. S.)	✓

NOTICE:

If OpenScape Voice uses different language versions for one language, you need to use an individual Media server for each language version. If, for example, you want to use the languages English (UK) and English (US) for an OpenScape Voice system, you need to use a Media server for English (UK) and one for English (US).

Handling of missing country-specific system announcements in the OpenScape Media Server

An individual language packet is delivered along with the OpenScape Media Server for each supported country. Such a language packet always contains the country-specific tones. Whether a language packet also contains country-specific system announcements depends on the respective language packet and thus on the respective country.

If a language packet is installed for an OpenScape Voice language ID on the OpenScape Media Server that contains the individual tones as well as system announcements of the relevant country, the OpenScape Media Server can automatically play the tones and system announcements of the respective country. The "tone language" and announcement language correspond in this case to the language ID that OpenScape Voice invokes.

If the language packet contains only the individual tones of the respective country, the OpenScape Media Server can access only the associated tones. So that in this case also system announcements can be played in the relevant language, you need to configure from which alternative language packet the OpenScape Media Server shall take them. The announcement language of this alternative language packet is also called fallback language. The "tone language" corresponds in this case to the language ID that OpenScape Voice invokes; the announcement language corresponds to the fallback language.

The OpenScape Media Server thus always uses the tones of the language packet that is defined by the OpenScape Voice language ID.

As a result, a language packet that corresponds to the required tone scheme must always be installed for a defined OpenScape Voice language ID in the OpenScape Media Server. The OpenScape Media Server would otherwise play the wrong tones. For example, the language packet Spanish (Mexico) might be useful to some American companies; however, it must still not be used outside of Mexico since the OpenScape Media Server would otherwise play the country-specific tones of Mexico. But these are different from those used in the US.

The following table provides information about the country and language support of the OpenScape Media Server at OpenScape Voice.

- The countries for which the OpenScape Media Server provides language packets
- Under which language code the country-specific language packet is administered in the OpenScape Media Server

NOTICE:

For each country, the respective language packet must be installed in the OpenScape Media Server. This is the only way to ensure that the OpenScape Media Server plays the correct, country-specific tones.

- If a language packet contains besides the country specific tones also the country specific system announcements
- The alternative language whose system announcements are recommended for configuration if the language packet itself does not contain system announcements. The listed alternative languages are already preset as fallback languages in the OpenScape Media Server default settings.

Table 38: Language packets in the OpenScape Media Server

Country	Language code	Individual system announcements	Preconfigured fallback language
Argentina	es_ar	✓	
Australia	en_au		en
Belgium	nl_be		nl
Bosnia and Herzegovina	bs		sr
Brazil	pt_br	✓	
Bulgaria	bg	✓	
Chile	es_cl		es_ar
China	zh	✓	
Colombia	es_co		es_mx
Denmark	da	✓	
Germany	de	✓	
Ecuador	es_ec		es_mx
Estonia	et	✓	
Finland	fi	✓	
France	fr	✓	
Greece	el	✓	
Great Britain / Ireland	en	✓	
Hong Kong	zh_hk		en_us

Country	Language code	Individual system announcements	Preconfigured fallback language
India	en_in		en
Indonesia	ind		en_us
Italy	it	✓	
Japan	jpn		en_us
Canada	fr_ca	✓	
Korea	ko		en_us
Croatia	hr	✓	
Latvia	lv	✓	
Lithuania	lt		en
Malaysia	mal		en_us
Morocco	fr_ma		fr
Mexico	es_mx	✓	
Netherlands	nl	✓	
Norway	no	✓	
Austria	de_at		de
Peru	es_pe		en_mx
Philippines	en_ph		en_us
Poland	pl	✓	
Portugal	pt	✓	
Romania	ro	✓	
Russia	ru	✓	
Sweden	sve	✓	
Serbia	sr	✓	
Singapore	zh_sg		en_us
Slovakia	sk	✓	
Slovenia	sl	✓	
Spain	es	✓	
Spain (Catalan)	ca	✓	
Spain (Basque)	eus	✓	
South Africa	en_za		en

Country	Language code	Individual system announcements	Preconfigured fallback language
Taiwan	zh_tw		en_us
Thailand	th		en_us
Czech Republic	cs	✓	
Turkey	tr	✓	
Hungary	hu	✓	
USA	en_us	✓	
Venezuela	es_ve		es_mx
United Arab Emirates	ar	✓	
Vietnam	vi		en_us

The OSV Assistant currently also allows the selection of a non supported language, which means that it is not iso integrated and there is no language pack installed on OMS, either as default, or as a supported language, which can later be assigned to a subscriber.

- When a non supported language is set to default, the system fallbacks to English, as the system default. English is played on the announcements for all the subscribers who have not explicitly been assigned an installed language.
- When a non supported language is selected as supported, and is explicitly assigned to a subscriber, then the system fallbacks to English, for this specific subscriber, no matter which language is set to default, or which other languages might be installed.

Related concepts

Language Varieties of System Announcements on page 402

5.8.4 Language Varieties of System Announcements

So that the Media server can play a system announcement or tone, the OpenScape Voice must transfer the ID of the language for which the greeting or tone is to be played to the server. OpenScape Voice supports currently no locale IDs, but only language IDs. Therefore, OpenScape Voice cannot expressly prompt a Media server to play a system announcement in a language variety– e. g. in Brazilian, which would be a language variety of Portuguese. To support language varieties just the same, the OpenScape Media Server enables the playback of language varieties internally.

NOTICE:

Before you install a language variety with a four-letter language code on the OpenScape Media Server, you need to install the associated language variety with a two-letter code.

Example: Before you can install the language variety with code en_us, the language variety with code en must have been installed.

The reason is: The setup files for language varieties with a four-letter code only contain the greetings that differentiate from the associated language variety with a two-letter code.

If there are several language varieties installed for one OpenScape Voice language ID in the OpenScape Media Server, the OpenScape Media Server determines internally which of these language varieties is used for this language ID.

Depending on the language varieties installed on the OpenScape Media Server for a basic language, this results in the following behavior:

- Only one language variety is installed on the OpenScape Media Server for a language ID:

  The OpenScape Media Server then uses the installed language variety for the language ID.

  Example: Only the language variety for Germany (de) is installed on the OpenScape Media Server for the language ID de. System Announcements and tones for the language ID de are thus played in the language variety for Germany (de).
- Several language varieties are installed on the OpenScape Media Server for one language ID:

  The OpenScape Media Server then uses the language variety with the two-letter language code for this language ID.

  Example: The language varieties for Germany (de) and Austria (de_at) are installed on the OpenScape Media Server for the language ID de. System Announcements and tones for the language ID de are thus played in the language variety for Germany (de).

If required, you can configure a different, individual prioritization.

NOTICE:

If OpenScape Voice uses different language versions for one language, you need to use an individual Media server for each language version. If, for example, you want to use the languages English (UK) and English (US) for an OpenScape Voice system, you need to use a Media server for English (UK) and one for English (US).

Related concepts

Supported Languages for System Announcements on page 396

5.8.5 RTP System Parameters for System Announcements

The behavior of OpenScape Voice system announcements is influenced by a system-wide setting – by a so-called Resilient Telco Platform system parameter (RTP system parameter).

The following table shows the RTP system parameter that influences the behavior of the OpenScape Voice system announcements. The default setting of this RTP system parameter is bolded.

Parameter	Value	Description
`Srx/Main/` `StartAnnDelayTimer`	Whole number (**300**)	Defines the time in milliseconds after whi announcement is played back delayed. T does not increase the time to set up the c connection.

5.9 Music-on-Hold (OpenScape Voice-based)

The OpenScape Voice-based feature music-on-hold enables callers to hear music while their call is being held. The feature can be directly assigned to a subscriber or be integrated in a feature profile that is directly assigned to the subscriber. In case of a collective line the trigger number of the collective line is regarded as subscriber. If the music-on-hold feature has been configured, a subscriber always hears music while being held in waiting state. This applies to: making a consultation call, holding an active call, manually holding an active call and CSTA-initiated hold.

NOTICE:

Unify SIP devices can also locally provide music-on-hold. However, the OpenScape Voice-based feature is then preferred to the local one.

The system administrator determines the music-on-hold used by specifying the drop name that is linked to the music file. This music can be the same each time a subscriber's call is held. The administrator can optionally specify music files for:

- Each feature profile. That means, all users who have been assigned this feature have their callers listening to the same music (if applicable).
- Each trigger number. That means, with calls of the associated collective line the same music is played (if applicable).
- Each single line

The availability of this feature depends on the services assigned to the holding subscriber. When this feature is invoked, the following happens:

1) The unit (endpoint, line, gateway) where the music is to be heard is connected to a Media server that provides the music. This Media server can be a separate one or the same Media server that also provides other system announcements.
2) Since music-on-hold is considered a system announcement, a default announcement connection is set up between the receiving unit and the Media server.
3) The system routes the announcement ID for the music source and the endpoint information to the Media server.
4) The Media server plays the music until the caller is released from the waiting loop.

It is the customer's responsibility to create and provide the Wav files for the music-on-hold.

The Wav files are stored on the Media server.

The music-on-hold can also consist of several linked files and be played in a loop.

Feature Interaction SILM (Silent Monitoring) - MOH (Music on Hold)

The interaction of Silent Monitoring with Music on Hold feature is allowed with the following restrictions:

1) The MOH intercept "MOH_Default_Tr" can be provisioned with only one (1) treatment.
2) This treatment should be configured as a loop announcement (it=-1).

> **NOTICE:**
>
> In case, you want to use two (or even more) different wav files for the MOH intercept, then both (or more) wav files should be included in one treatment that should be provisioned as loop announcement (it=1)

Direct SIP Connectivity to MS Lync 2013

An OSV subscriber activates the feature MOH.When the OSV subscriber is in a call with a Lync subscriber and puts the call on hold, then the Lync client listens to the OSV MOH. However, the Lync client has no indication that the call is on hold.In order for the Lync client to indicate that the call is on hold, the MOH feature should be deactivated by the OSV subscriber.

5.10 Conferences

OpenScape Voice support different types of conferences: Station-controlled conferences (large conference), meet-me conferences and ad hoc conferences.

OpenScape Voice supports a central Media server and branch office Media servers. For reasons of reliability, backup Media servers can also be configured. The following applies:

- The route list defines how the conference request is routed. The central Media server can be configured to be the default destination if all other options to secure the Media server in the branch fail – e. g. due to overload or unavailability.
- Conference lines for a business group must be assigned to the same Media server; distributing the various conferees of a single conference among different Media servers is not supported.

  A conference shall always be created on the Media server which is the primary Media server of the conference creator. If the primary Media server is not available, the backup Media server will be used.
- The backup Media server is only activated when the central Media server has been ascertained as being unavailable.

Related concepts

Media Server Deployment Scenarios at OpenScape Voice on page 367

5.10.1 Meet-Me Conferences

Meet-me conferences are scheduled in advance. They require a separate conference application – e. g. the conference portal of the OpenScape Media Server.

5.10.2 Ad-hoc Conferences

An ad-hoc conference is an unscheduled conference that may be created without pre-planning and it only applies for audio or voice.

The OpenScape user selects either multiple contacts from the contact list or creates manually a list of participants using directory access, creates the conference and starts it immediately. Ad-hoc conferences require a separate conference application – e. g. the conference portal of the OpenScape Media Server.

5.10.3 Station-controlled Conferences (Large Conference)

Via station-controlled conferences, OpenScape Voice users can stage a conference with a total of 48 participants. The maximum number of conference participants can be restricted by the performance of the Media Server used or by creating the Business Group Service. With the OpenScape Media Server you can use the maximum number of conference participants. Station-controlled conferences are set up as required (ad-hoc). The participants of a station-controlled conference can be members of the same or of different business groups or be participants in the public network.

The Media server has the task of mixing the media streams. If required, it also takes on the transcoding job – e. g. from G.729 to G.711. This transcoding ensures that conference participants can hear each other even if the involved devices use different codecs for the media streams.

Station-controlled conferences can be provided on business group level with a prohibition option on participant level.

Please refer to the description of the SIP devices to learn which SIP devices support station controlled conferences.

The device Openstage 15/20/40/60/80 shows a list of all participants during a station-controlled conference. This list is automatically updated as soon as members join or leave the conference and contains the name and phone number of each participant. The phone number is displayed in a dialable format.

When all participants of an OSV Large Conference are secure then the conference is considered secure and all the participants' displays indicate secure call. When the conference is secure the Openstage 40/60/80 devices have a padlock icon displayed.

Each time a new participant is added/removed/modified, and this affects the security status of the Conference, all the participants are informed about the change and their displays regarding the security status are updated.

Categorization of conference participants / participants

Conference participants or participants in station-controlled conferences can be categorized as follows:

- Conscious and unconscious conference participants
  - A conscious conference participant is aware of the current phone call being a conference call. A conscious conference participant can be an active or passive participant (see the following categorization).
  - An unconscious conference participant is unaware of the current phone call being a conference call. To him/her it is a simple point-to-point connection. Unconscious conference participants are always passive participants (see the following categorization).
- Active and passive participants
  - An active participant can invoke extended functions related to the conferencing feature; for example, he/she can initiate a conference and add further participants. Active participants are always conscious conference participants. They must belong to the same business group as the conference initiator and be registered for the conference feature.
  - A passive participant can talk to other conference participants but cannot invoke any advanced functions in the conference feature context. Passive participants can either be conscious or unconscious conference participants. Members of other business groups and participants in the public network are always passive participants.

Use of a station-controlled conference

To set up the conference the user first initiates two calls (a held and a consultation call) and pushes the Conference key. This user is a conscious conference participant and active participant. Depending on the additional features assigned to the other participants, these participants can:

- Hold calls. Conscious conference participants can also stop music from being played during the conference.
- Toggle held and active calls.
- If the conference participant is active and conscious:
  - Add another participant to the conference. You find more information in the corresponding user manual.
  - In case of OpenStage phones: Displaying a conference participants list that can be browsed. The display is automatically updated as soon as participants join or leave the conference.
  - Remove the participant who joined last by dialing the corresponding prefix access code.

    This feature is commonly used when a user has inadvertently added an unwanted or unavailable participant to the conference. To cut and reestablish the connection to all conference participants only for removing an unwanted one is thus not necessary.

NOTICE:

The system administrator defines the access code to be used for removing the participant who joined last.

Restrictions on Subscribers in Station-controlled Conferences

By Toll and Call Restrictions a subscriber may be restricted to call other selected parties.

Station-controlled conferences can be configured to be automatically released, when in the case of two parties remaining in conference, one party is restricted by Toll and Call Restrictions from calling the second party. This setting is business-group-related.

Technical Restrictions on Station-controlled Conferences

A conference participant may only take part in several conferences using the same phone number if he/she does not use an OpenScape Voice participant for this purpose.

Related features

The configuration of an SIP endpoint decides whether station-controlled conferences are available for this endpoint or whether three-way conferences must be used instead. We recommend to configure endpoints for station-controlled conferences. This ensures consistent operation under all users.

Configuration of station-controlled conferences

The configuration of station-controlled conferences is performed in three steps:

- Step 1: How to activate station-controlled conferences
- Step 2: How to configure the access code
- Step 3: How to configure station-controlled conferences for participants via feature profile

The default set RTP parameters of the system environment used may have to be subsequently adjusted.

Related concepts

RTP System Parameters for Station-Controlled Conferences on page 408

5.10.4 RTP System Parameters for Station-Controlled Conferences

The behavior of station-controlled conferences is influenced by different, system-wide settings – by so-called Resilient Telco Platform system parameters (RTP system parameters). Changing one of these settings influences the behavior for all business groups and their members.

The following table shows all RTP system parameters that influence the behavior of station-controlled conferences. The default settings of these RTP system parameters are bolded.

Parameter	Value	Description
`Srx/Main/LCSIPUnity`	Whole number (**3000**)	Defines the maximum number of co per Media server.
`Srx/Main/ LCSMaxNumConfPorts`	Whole number (**16**)	Defines the maximum number of co conference endpoint.

Related concepts

Station-controlled Conferences (Large Conference) on page 406

5.11 System Announcements and User Greetings for OpenScape UC Application

The OpenScape Media Server provides the conference and voice portal of OpenScape UC Application. In this scope the OpenScape Media Server manages the system announcements and user greetings of these portals. The system announcements are the same for all OpenScape users. The user greetings can be customized by each OpenScape user and define welcome greetings and name greetings.

NOTICE:

The system announcements described here are independent from those that the OpenScape Media Server manages for OpenScape Voice.

OpenScape users may configure their individual user greetings for the voice portal. In doing so they customize these user greetings always only on the OpenScape Media Server the voice portal of which they are currently logged in to. If you use OpenScape UC Application with a Media server farm, all other OpenScape Media Servers of the farm use the origin version of the user greetings.

So that modified user greetings are automatically available on each OpenScape Media Server of a Media server farm, the OpenScape Media Server supports a replication mechanism. This mechanism replicates modified voice portal user greetings to all other OpenScape Media Servers of the Media server farm automatically.

NOTICE:

If you use a Media server farm, you should configure each remote OpenScape Media Server for user greeting replication on each OpenScape Media Server of the Media server farm.

5.12 System Resources Management

You can use the system resource management of the OpenScape Media Server to proportionately assign operation-critical system resources to individual media applications of the OpenScape Media Server – e. g. to the conference portal user access. In this way it is possible to split up the operation-critical system resources according to their use and to guarantee each media application a specific number of operation-critical system resources.

The OpenScape Media Server internally manages different operation-critical system resources. Among these you find in particular the following:

- RTPchannels

  The OpenScape Media Server uses RTP channels for in and outbound voice communication Each RTP channel resource specifies a bidirectional transmission channel.
- Conference mixing unit

  The OpenScape Media Server uses a conference mixing unit to interconnect conference participants. For each conference a conference mixing unit is required in the OpenScape Media Server.
- Application instances

  The OpenScape Media Server usually manages for each media application several instances. For the speech respectively conference portal this means:

  – one voice portal instance for each user logged in to the voice portal
  – one conference portal instance for each user just logging on to the conference portal
  – one conference portal instance for each active conference room

To proportionately assign a system resource to an individual media application, you first need to determine how many resources of the relevant type are altogether available. Since the OpenScape Media Server operates software-based, this number of resources is defaulted by the performance of the computer system used.

After the maximum number of a resource type has been determined, the relevant resources can be divided user-individually.

The listed system resources are assigned the following resource type names in the OpenScape Media Server system resource management:

- RTP channel – resource type **RTPChannel**
- Conference mixing unit – resource type **ConfMixingUnit**
- Application instance – resource type **ApplicationInstance**

Related concepts

Configuration Concept of the OpenScape Media Server on page 373

5.13 Connection of the OpenScape Media Server to Several SIP Servers

If you use OpenScape UC Application, the OpenScape Media Server is connected to the OpenScape Voice system via an SIP trunk. In this way it can accept incoming connection requests or set up outgoing ones. So that communication is still possible even if the connected OpenScape Voice system or the connection to the system fail, the OpenScape Media Server can be connected to different OpenScape Voice systems.

NOTICE:

The OpenScape Media Server is only connected to OpenScape Voice via SIP if it is used under OpenScape UC Application.

NOTICE:

If the OpenScape Media Server is used with OpenScape UC Application, it always requires an SIP trunk for communicating with OpenScape Voice. If no SIP trunk is configured in OpenScape Voice for the OpenScape Media Server, the communication between OpenScape Media Server and OpenScape Voice will fail.

If the OpenScape Media Server is connected to several SIP servers, it differentiates the relevant SIP connections as follows.

- Master connection

  Describes the connection to the preferred OpenScape Voice system.
- Alternative connections

  Describes the connections to all further OpenScape Voice systems.

By default, the OpenScape Media Server uses the master connection to communicate. If, however, the preferred OpenScape Voice system or the connection to this system fails, the server communicates via the next configured alternative connection that is operable.

When the preferred OpenScape Voice system and the connection to the system are available again, the OpenScape Media Server may use this system again after a specific period. The OpenScape Media Server does not switch back to the master connection by default.

5.14 Media Applications of the OpenScape Media Server

The OpenScape Media Server can execute different internal media applications to provide the user with extended media services. These media applications are configured via the OpenScape Media Server settings.

NOTICE:

Media applications are available in the OpenScape Media Server only if the OpenScape Media Server is used under OpenScape UC Application.

The OpenScape Media Server currently realizes the following internal media applications:

- Conference Portal

- Voice portal

The so-called address bindings determine under which phone number a media application can be reached.

Each address binding contains the following information:

- A terminal

  A so-called terminal is assigned the URI of a media application and at least one phone number expression. This results in an individual assignment of URI and phone number expressions.

  The terminal is solely a logical configuration unit within the OpenScape Media Server. It can be best compared with the logical configuration of a terminal device in a PBX, which is also assigned specific attributes – e. g. phone numbers.
- Binding Attributes

  Specify different properties that determine the communication behavior of the relevant address binding.

  The binding attributes include, for example, security and codec settings.
- General Properties

  Specify media-application-individual settings transferred to the relevant media application when being invoked.

  Via these settings you can e. g. control the default language of the voice portal. General properties influence only the behavior of the media application and do not serve any other purpose in the OpenScape Media Server.

  Each general property consists of a key and an associated value. The key determines the property that is controlled; the value determines the setting of the relevant property.

  Example: The voice portal is to start with the Chinese TUI under a specific address binding.

  – **Key**: `symLanguage`
  – **Value**: `ZH-CN`
- At least one phone number expression

  Each phone number expression specifies at least one phone number under which the relevant media application is to be reached in the OpenScape Media Server.

  Example: regexp:sip:+492404901100@.*

  NOTICE:

  Specify phone numbers always fully qualified in the GNF format when you use the OpenScape Media Server at OpenScape Voice – example: +492404901100.

5.14.1 Conference Portal of the OpenScape Media Server

The conference portal is automatically installed with the OpenScape Media Server. With the conference portal the OpenScape Media Server provides conference rooms in which users can gather and hold audio conferences. Users may deploy any telephone or softphone as terminal device.

NOTICE:

The system resources management is available in the OpenScape Media Server only if the OpenScape Media Server is used under OpenScape UC Application.

The conferences can be scheduled and controlled via telephone user interface (TUI) of the OpenScape Media Server or via an associated conference client application.

The OpenScape Media Server conference portal supports the following types of conferences:

- Meet-me conferences
- Ad-hoc conferences

Supported Languages

The conference portal supports the following languages:

- Chinese (China)
- German (Germany)
- English (UK)
- English (U.S.)
- French (France)
- Italian (Italy)
- Portuguese (Brazil)
- Portuguese (Portugal)
- Spanish (Spain)

The language version the conference portal deploys for a user depends on the respective user who logs in to the conference portal.

For this purpose, the conference portal searches for the user in the OpenScape UC Application user database and evaluates the user language configured there. If the conference portal supports the language determined in this way, the TUI is switched to the relevant language version. If the determined language is not available to the conference portal or the relevant user is not contained in the user database, the TUI is reproduced in the default language.

If you have not specified an individual default language for the conference portal, the default language is English (U.S.).

General Properties for the conference portal

To start the conference portal with an individual configuration you need to configure the corresponding general properties in the associated address binding. The OpenScape Media Server then transfers these general properties with the configured URI upon the conference portal invocation.

The conference portal supports the following general properties.

- **calloutGracePeriod**
  - Default setting: `30 000` [ms]
  - Possible values: <time> [ms]

  The conference portal can call participants at the start of a conference.

  calloutGracePeriod specifies how long the conference portal waits until such a call is answered.

- **fastTransfer**
  - Default setting: `true`
  - Possible values:

    `true` – Level 2 system announcements are played

    `false` – Level 2 system announcements are not played.

  The system announcements of the conference portal are divided into two levels:

  - Level 1: System announcements for essential information

    e. g. “Enter your PIN”
  - Level 2: System announcements for additional information

    e. g. “Your PIN has been accepted”.

  fastTransfer specifies whether Level 2 system announcements are played to the caller.
- **fastWelcome**
  - Default setting: `true`
  - Possible values:

    `true` – Do not play welcome greetings

    `false` – Play welcome greetings.

  Specifies whether a welcome greeting is played to the conference participant when he/she logs on to the conference.
- **language**
  - Default setting: `en_US`
  - Possible values:

    `de_de` – German (Germany)

    `en_gb` – English (UK)

    `en_us` – English (U.S.)

    `es_es` – Spanish (Spain)

    `fr_fr` – French (France)

    `it_it` – Italian (Italy)

    `pt_br` – Portuguese (Brazil)

    `pt_pt` – Portuguese (Portugal)

    `zh_cn` – Chinese (Mandarin)

  Specifies in which language the conference portal represents the TUI to a caller.
- **rejoinGracePeriode**
  - Default setting: `300 000` [ms]
  - Possible values: <time> [ms]

  For technical reasons that concern a participant's connection to the conference, he/she may have to quit – e. g., when the phone connection is cut. If such a conference participant rejoins the conference within a specific period, he/she is automatically assigned to the previous conference without having to make any further entries.

rejoinGracePeriod specifies within which period an inadvertently disconnected conference participant is automatically reassigned to the previous conference.

- **useNeutralWelcome**
  - Default setting: `true`
  - Possible values:

    `true` – neutral welcome greeting

    `false` – OpenScape-welcome greeting.

  The conference portal may use one of the following welcome greeting:

  - Neutral, product-independent welcome greeting
  - OpenScape-welcome greeting

  useNeutralWelcome specifies which of these welcome greeting the conference portal uses.

5.14.2 Voice Portal of the OpenScape Media Server

The voice portal is automatically installed with the OpenScape Media Server. It provides users with a telephone user interface (TUI), via which the users can access the comprehensive Unified Communications services of OpenScape UC Application. The user operates this telephone user interface via the keypad of his/her telephone.

NOTICE:

The voice portal is available in the OpenScape Media Server only if the OpenScape Media Server is used under OpenScape UC Application.

The voice portal comprises a total of two TUI accesses:

- User access

  This access is deployed by OpenScape users to e.g. configure OpenScape UC Application-individually or to access the Unified Communications services of OpenScape UC Application.
- Guest access

  This access is deployed by callers who are no OpenScape users. Here you can e. g. leave messages for OpenScape users.

The voice portal is realized as web application and uses the internal Tomcat web server of the OpenScape Media Server. It does not create any HTML-based contents, though, but uses VoiceXML for the output. These VoiceXML contents are interpreted by the VoiceXML browser of the OpenScape Media Server and played from there to the user who has logged in to the voice portal with his/her telephone via the OpenScape Media Server.

The web application of the voice portal is stored in the following directory on the OpenScape Media Server computer system:

```
…/mediaserver/application_host/providers/tomcat/tomcat-
home/webapps/
```

Supported Languages

The voice portal supports the following languages:

- Chinese (China)
- German (Germany)
- English (UK)
- English (U.S.)
- French (France)
- Italian (Italy)
- Portuguese (Brazil)
- Portuguese (Portugal)
- Spanish (Spain)

The language version the voice portal deploys for a user depends on the respective user who logs in to the voice portal.

For this purpose, the voice portal searches for the user in the OpenScape UC Application user database and evaluates the user language configured there. If the voice portal supports the language determined in this way, the TUI is switched to the relevant language version. If the determined language is not available to the voice portal or the relevant user is not contained in the user database, the TUI is reproduced in the default language.

If you have not specified an individual default language for the voice portal, the default language is English (USA).

General Properties for the Voice Portal

To start the voice portal with an individual configuration you need to configure the corresponding general properties in the associated address binding. The OpenScape Media Server then transfers these general properties with the configured URI upon the voice portal invocation.

The voice portal supports the following general properties.

- **Expressions**
  - Default setting: –
  - Possible values: <phone number>

  Specifies under which phone number the relevant voice portal access can be reached.

- **guessLanguages**
  - Default setting: `-`
  - Possible values: <comma-separated list of at least one of the settings>

    `de_DE` – German (Germany)

    `en_GB` – English (UK)

    `en_US` – English (U.S.)

    `es_ES` – Spanish (Spain)

    `fr_FR` – French (France)

    `it_IT` – Italian (Italy)

    `pt_BR` – Portuguese (Brazil)

    `pt_PT` – Portuguese (Portugal)

    `zh_CN` – Chinese (Mandarin)

    NOTICE:

    Cannot be configured for the guest portal.

  Using the text-to-speech feature of OpenScape UC Application, users can have texts read out. In this process the system can automatically optimize the voice output by analyzing the message text sentence-wise and using the text-to-speech engine for the recognized language.

  guessLanguages defines as regards which languages the text-to-speech feature analyses message texts.

- **operator**
  - Default setting: `-`
  - Possible values: <phone number>

    NOTICE:

    Cannot be configured for the guest portal.

  Specifies under which phone number a caller can reach the operator.

- **subjectSuffix**
  - Default setting: `-`
  - Possible values: <subject attachment as text>

  When the voice portal creates a voice message, a permanently defined text can be attached to the associated subject information.

  subjectSuffix defines the text that is attached to the subject information.

- **symLanguage**
  - Default setting: `en_us`
  - Possible values:

    `de_DE` – German (Germany)

    `en_GB` – English (UK)

    `en_US` – English (U.S.)

    `es_ES` – Spanish (Spain)

    `fr_FR` – French (France)

    `it_IT` – Italian (Italy)

    `pt_BR` – Portuguese (Brazil)

    `pt_PT` – Portuguese (Portugal)

    `zh_CN` – Chinese (Mandarin)

  Specifies the voice portal access default language.

  The language version the voice portal deploys for a user depends on the respective user who logs in to the voice portal. For this purpose, the voice portal searches for the user in the OpenScape UC Application user database and evaluates the user language configured there. If the voice portal supports the language determined in this way, the TUI is switched to the relevant language version. If the determined language is not available to the voice portal or the relevant user is not contained in the user database, the TUI is reproduced in the default language.
- **symDomain**
  - Default setting: `system`
  - Possible values: <SIP domain ID>

  NOTICE:

  Cannot be configured for the guest portal.

  Specifies the SIP default domain used by the voice portal.
- **thirdPartyVMNumber**
  - Default setting: `–`
  - Possible values: <phone number>

  NOTICE:

  Cannot be configured for the guest portal.

  If you integrate OpenScape UC Application in the voicemail system of a third-party supplier, you need to specify the access number for the relevant voicemail system with **thirdPartyVMNumber**.

- **transferTimeout**
  - Default setting: -
  - Possible values: <time> [seconds]

  NOTICE:

  Cannot be configured for the guest portal.

  Specifies how long the system attempts to reach the dialed phone number in case of a forwarding.
- **ttsLanguage**
  - Default setting: -
  - Possible values: <comma-separated list of at least one of the settings>

    `de_DE` – German (Germany)

    `en_GB` – English (UK)

    `en_US` – English (U.S.)

    `zh_CN` – Chinese (Mandarin)

  NOTICE:

  Cannot be configured for the guest portal.

  Using the text-to-speech feature of OpenScape UC Application, users can have texts read out. In this process the user can optimize the text output quality by selecting the text-to-speech engine in the voice portal TUI that is optimized for the language of the respective text.

  ttsLanguage specifies for which languages text-to-speech engines can be selected in the voice portal TUI.
- **useSubjectSuffix**
  - Default setting: `no`
  - Possible values: <time> [seconds]

    `yes` – Activates attaching text to the subject.

    `no` – Deactivates attaching text to the subject.

  NOTICE:

  Cannot be configured for the guest portal.

  When the voice portal creates a voice message, a permanently defined text can be attached to the associated subject information.

  useSubjectSuffix activates attaching the text defined in **subjectSuffix**.
- **voicePortalNumber**
  - Default setting: -
  - Possible values: <phone number in the GNF format>

  If a user needs to specify a phone number in the voice portal, he/she will do this always with reference to the respective location. For example, as pure extension or as phone number with area code but without international prefix. But this leads to problems if the voice portal e.g. is located in a country different from the caller's.

To evade such phone number problems, the OpenScape system transfers all phone numbers before the actual evaluation into a normalized phone number format. These normalized phone numbers then contain all information that the phone number uniquely localizes.

To normalize a phone number, the OpenScape system requires a so-called phone number context, which needs to be configured in OpenScape Voice in the form of a Multi Line Hunt Group (MLHG).

voicePortalNumber specifies the pilot number of the Multi Line Hunt Group (MLHG) the phone number context of which is to be used for the phone number normalization of the respective voice portal access.

- **xprTrustedTransferDomain**
  - Default setting: `49`
  - Possible values: <number>

  NOTICE:

  Cannot be configured for the guest portal.

  Specifies the ID of the trusted domain that is or will be configured in the XPR system as local trusted domain. If the voice portal receives a forwarded TTM call from the XPR server, it checks the domain ID forwarded with the call. If this forwarded domain ID does not correspond to the one configured here, the call will be rejected as unauthorized.
- **xprTrustedTransfeParam**
  - Default setting: `p0v1p1v2 p2v1 p3v4 p4v4 p5v2 p6v1`
  - Possible values: <phone number schema>

  NOTICE:

  Cannot be configured for the guest portal.

  If a user is forwarded to the XPR server via the Trusted Transfer Mode of OpenScape UC Application or vice versa, different information must be exchanged between OpenScape UC Application and the XPR server with the forwarding. The calling number schema specifies in which format this information is exchanged.
- **xprNumber**
  - Default setting: `-`
  - Possible values: <phone number>

  NOTICE:

  Cannot be configured for the guest portal.

  If you connect OpenScape UC Application with an XPR server via the Trusted Transfer Mode, you need to specify the access number for the XPR PhoneMail script with **xprNumber**.

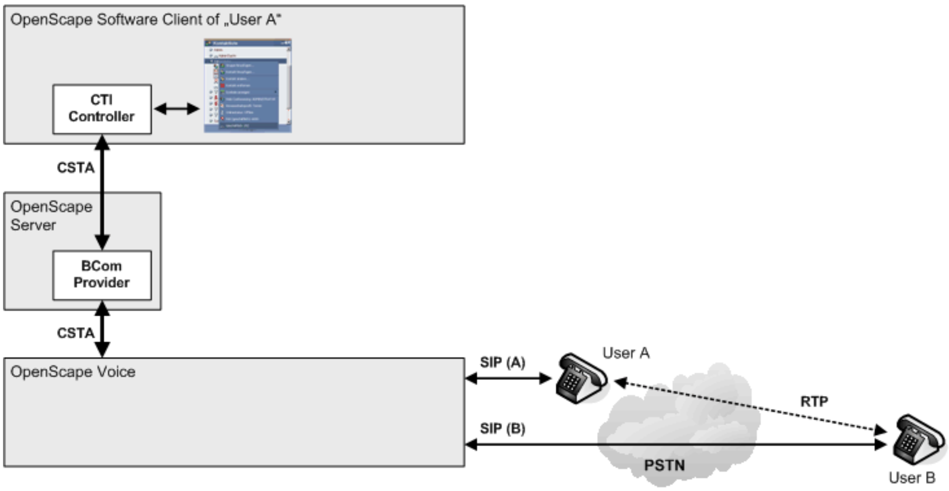
5.15 Transfer Conference of the OpenScape Media Server

From an existing telephone connection with two subscribers a conference is often to be established. The transfer conference does not realize such a conference device-controlled but via the conference portal of OpenScape UC Application.

NOTICE:

The transfer conference is available in the OpenScape Media Server only if the OpenScape Media Server is used under OpenScape UC Application.

The following figures show how the transfer conference works.

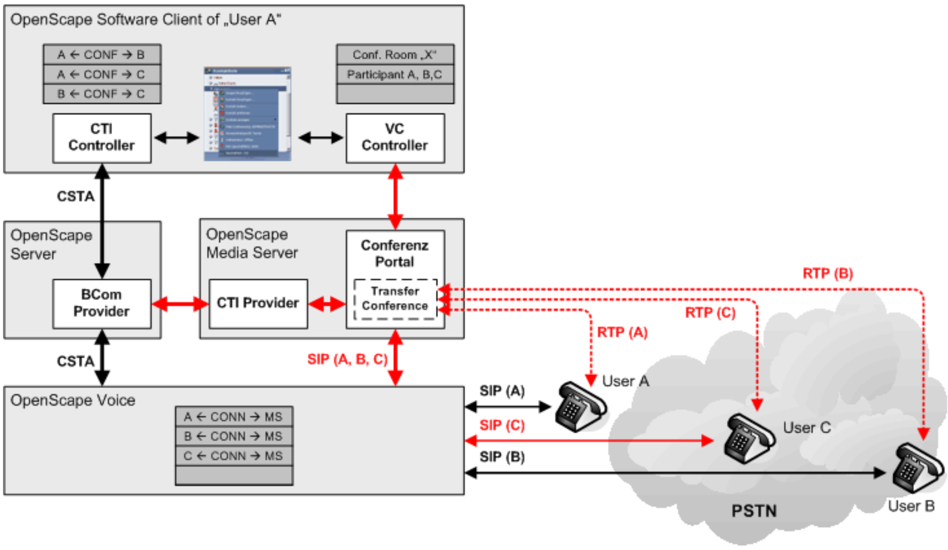


The transfer conference mechanism starts with a simple telephone connection and two subscribers who are connected via OpenScape Voice. The SIP signaling of the phone connection is led via OpenScape Voice. The RTP-based payload is directly exchanged between the telephones.

In the depicted example, one of the two subscribers is an OpenScape user A who can control his/her telephone via a software client. The software client communicates via its CTI controller and the CSTA protocol with the BCom provider of the OpenScape server. The BCom provider also communicates via CSTA with OpenScape Voice and controls in particular the telephone of user A.

The second subscriber to the phone connection is e.g. an external subscriber.

Based on the existing phone connection and via the GUI of his/her software client user A can initiate an ad-hoc conference to integrate a new subscriber in the existing connection. The following happens:



1) The BCom provider of the OpenScape server cuts the connection between the subscribers A and B in OpenScape and connects the two resulting connection fragments to a new transfer conference in the conference portal. To this, the BCom provider controls OpenScape via appropriate CTI commands.
2) At the same time the BCom provider of the OpenScape server transfers all information about the rerouted connections and their subscribers to the CTI provider of the OpenScape Media Server. The CTI provider then forwards the information to the conference portal. In this way the conference portal can determine which of the newly arriving calls are to be routed into a common transfer conference. Furthermore, the conference portal is thus enabled to suppress default greetings of the portal for the relevant users.
3) Besides the subscribers A and B, also the new conference participant is added to the transfer conference.

Eventually, all users are in a common transfer conference of the conference portal. In this scenario the SIP signaling of the phone connection leads via OpenScape to the conference portal. The RTP-based payload is processed by a conference mixing unit of the OpenScape Media Server.

After the users have been connected in the transfer conference of the conference portal, this conference can be controlled as usual via the Virtual Conference Controller (VC-Controller) of the software client.

The available information about the state of the different connections differ in the system components involved.

- In OpenScape Voice the participating connections are registered as CONNECTED. In OpenScape Voice such connections are not known as conference connections.
- In the CTI controller of the software client the connections are registered as CONFERENCED. The CTI controller receives the additional information about the conference state from the BCom provider of the OpenScape server, which has received it from the CTI provider of the OpenScape Media Server.
- In the Virtual Conference Controller of the software client all users are registered as subscribers to a common conference. The Virtual Conference Controller receives this comprehensive information directly from the OpenScape Media Server conference portal.

5.16 Connection of OpenScape UC Application and OpenScape Xpressions

You can connect OpenScape UC Application to OpenScape Xpressions. Such a connection extends the Unified Messaging features of the PhoneMail application of OpenScape Xpressions by the Unified Communications features of OpenScape UC Application.

If OpenScape Xpressions is connected with the OpenScape system, the Unified Communications features of OpenScape UC Application integrate in the PhoneMail user menu of OpenScape Xpressions. The user will not realize whether a selected feature is enabled by OpenScape Xpressions or by OpenScape UC Application. He/she will receive the impression as if working with a Unified Communications system centrally providing all available features.

If an XPRuser logs on to the PhoneMail application and selects a Unified Communications feature enabled by OpenScape UC Application, the XPR server forwards the call to the user access of the voice portal. There, the XPR user is automatically authenticated without any further inputs required. Subsequently, the user menu associated to the selected feature will be directly announced to the XPR user.

To enable the described behavior, the XPR server transfers various information to OpenScape UC Application along with the call. The XPR server encodes this information in the originator number of the forwarded call, using the Trusted Transfer Mode (TTM) phone number format for the encoding.

Restrictions on the Connection of OpenScape UC Application and OpenScape Xpressions

- For the time being, the Trusted Transfer Mode has only been approved for usage at OpenScape Voice.
- The XPRserver and OpenScape UC Application must be connected to the same OpenScape Voice system.
- The connection supports only 1:1 relationships between an XPR server and a voice portal of OpenScape UC Application.
- The start character of the TTM phone number format must not be filtered out by the PBX or a gateway between XPRserver and OpenScape UC Application.

5.16.1 Phone Number Format of the Trusted Transfer Mode (TTM)

You can connect OpenScape UC Application to OpenScape Xpressions. In this case the phone number format of the trusted transfer mode determines the structure in which OpenScape UC Application and OpenScape Xpressions exchange information.

The TTM phone number format has the following general structure:

```
<start character><trusted domain><original system><user informatio
```

The various TTM phone number format elements specify the following:

- Start Character

  The start character is an indicator for the OpenScape components involved to recognize the relevant phone number as a number in TTM phone number format.

  The start character can be, for example, the * character or any other non-numerical character.
- Trusted Domain

  Specifies the ID of the system that has created the relevant phone number. This ID is evaluated by the system that receives the information. Forwarded calls with invalid ID will not be accepted by the receiving system.
- Original System

  The original system defines from which system the trusted transfer is induced.

  – From the XPR server if an XPR user switches under PhoneMail to OpenScape UC Application features.
  – From OpenScape UC Application if the XPR user returns to the PhoneMail features.
- User Information

  The user information specifies:

  – The caller’s number (ANI))
  – The user's voice box number
  – The user language
  – The TUI point of entry

The calling number schema determines the format of the various elements of the TTM phone number format.

5.16.2 Calling Number Schema of the Trusted Transfer Mode (TTM)

You can connect OpenScape UC Application to OpenScape Xpressions. In this case the phone number format of the trusted transfer mode determines the structure in which OpenScape UC Application and OpenScape Xpressions exchange information. The calling number schema defines how the single information of the phone number format is formatted.

The calling number schema consists of several consecutive sections. The notation of these sections depends on whether you contemplate the calling number schema under OpenScape UC Application or on the XPR server.

Notation under OpenScape UC Application

In the -OpenScapesystem the sections of the calling number schema always have the following format:

p<argument index> v<argument length>

- Argument index

  A running number that serially numbers the different consecutive arguments of the user information.
- Argument length

  The permanent number of digits contained in the relevant argument.

Notation on XPR server

On the XPRserver the sections of the calling number schema always have the following format:

%<argument index> $<argument length>

Only the first section of the calling number schema deviates from this format. This first section always describes a single character – the start character. Therefore, only the character used as start character needs to be specified for this first argument. It is prefixed with a p in addition.

- Argument index

  A running number that serially numbers the different consecutive arguments of the user information.
- Argument length

  The permanent number of digits contained in the relevant argument.

Operating mode of the calling number schema

Permanently defaulted phone number format:	<S><TD><ORG><ANI><UID><OTUI><LNG>
Calling number schema (OpenScape UC Application):	p0v1p1v1p2v1p3v4p4v4p5v2p6v1
Calling number schema (XPR Server):	p*%1 $1 %2 $1 %3 $4 %4 $4 %5 $2 %6 $1
Transferred originator number	*9055485548026

Decoded this results in:

• p0 / p*:	Start character (S)	: *
• p1 / %1:	Trusted Domain (TD)	:9
• p2 / %2:	Original system (ORG)	:0
• p3 / %3:	ANI	:5548
• p4 / %4:	User ID (UID)	:5548
• p5 / %5:	Original TUI User Entry Point (OTUI)	:02
• p6 / %6:	Language (LNG)	:6

In the example, four-digit extensions are used. For, argument length 4 has been set for parameter 3 (p3 respectively %3).

If you want to use a different length for the extensions you need to configure a different argument length for the parameters 3 and 4. In doing so please note that the total length of the phone number expression must normally not exceed a maximum length. This length is defaulted by the PBX used.

NOTICE:

OpenScape Voice supports Calling Numbers up to a maximum of 30 digits. Numbers longer than 30 digits will be truncated at the end.

Calling number schemas of different extension lengths

Extension length	OpenScape UC Application	XPRServer
Three-digit	p0v1p1v1 p2v1 p3v**3** p4v**3** p5v2 p6v1	p*%1$1 %2$1 %3$**3** %4$**3** %5$2 %6$1
Four-digit	p0v1p1v1 p2v1 p3v**4** p4v**4** p5v2 p6v1	p*%1$1 %2$1 %3$**4** %4$**4** %5$2 %6$1
Five-digit	p0v1p1v1 p2v1 p3v**5** p4v**5** p5v2 p6v1	p*%1$1 %2$1 %3$**5** %4$**5** %5$2 %6$1

NOTICE:

When you change the calling number schema you need to perform this modification for the OpenScape UC Application as well as for the XPR server.

5.17 RTP System Parameters for Media Services

The general behavior of the OpenScape Voice media services are influenced by system-wide settings – by so-called Resilient Telco Platform system parameters (RTP system parameters).

The following table shows the RTP system parameters that influence the behavior of the OpenScape Voice media services. The default setting of these RTP system parameters is bolded.

Parameter	Value	Description
`Srx/mgcp/RtpMsgQueueUsageHighThreshold`	0 … 100 (**90**)	Defines in percent the upper threshol message queue of the Call Control M OpenScape Voice. When this threshold is exceeded for t message queue the overload state of Manager will be set. As a result all re connections from OpenScape Voice t servers are rejected.
`Srx/mgcp/RtpMsgQueueUsageLowThreshold`	0 … 100 (**80**)	Defines in percent the lower threshol message queue of the Call Control M OpenScape Voice. When this threshold is under-run for t message queue the overload state of Manager will be cleared. As a result r connections from OpenScape Voice t servers are no longer rejected in gen

6 Call Control

Call control provides the core call processing center. It incorporates call processing components including the UCE (Universal Call Engine), signaling managers, and call control services dynamically loaded into the UCE.

The key component of the OpenScape Voice call processing function is the protocol-independent UCE, which contains the generic switching functions of OpenScape Voice. It provides the following:

- A secure, generic interface to set up and release calls through the system
- Common logic to all signaling managers to route calls through the system

A large number of APIs provided to the UCE are crucial to OpenScape Voice programmability and the ability to interoperate with standards-based equipment.

6.1 Numbering Plan

A NP (Numbering Plan). A numbering plan is a type of numbering scheme with a set of routing rules to allocate telephone numbers to subscribers and to route telephone calls in a telephone network.

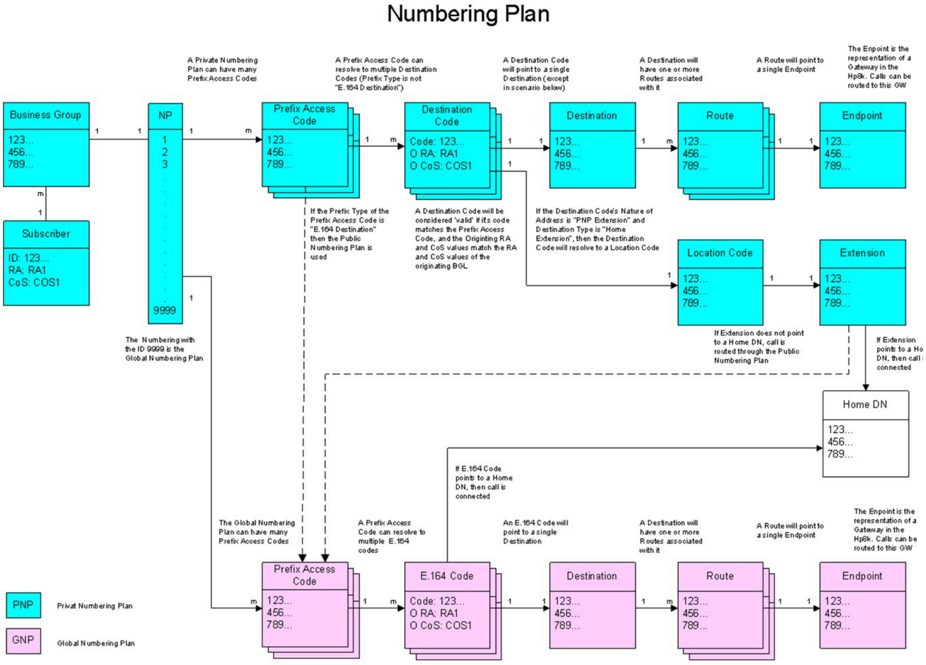

Numbering Plan
A Private Numbering Plan can have many Prefix Access Codes
A Prefix Access Code can resolve to multiple Destination Codes (Prefix Type is not "E.164 Destination")
A Destination Code will point to a single Destination (except in scenario below)
A Destination will have one or more Routes associated with it
A Route will point to a single Endpoint
The Enpoint is the representation of a Gateway in the Hp8k. Calls can be routed to this GW
Business Group
123...
456...
789...
NP
1
2
3
9999
Prefix Access Code
Destination Code
Code: 123...
O RA: RA1
O CoS: COS1
Destination
Route
Endpoint
Subscriber
ID: 123...
RA: RA1
CoS: COS1
1
m
If the Prefix Type of the Prefix Access Code is "E.164 Destination" then the Public Numbering Plan is used
A Destination Code will be considered 'valid' if it's code matches the Prefix Access Code, and the Originting RA and CoS values match the RA and CoS values of the originating BGL
If the Destination Code's Nature of Address is "PNP Extension" and Destination Type is "Home Extension", then the Destination Code will resolve to a Location Code
Location Code
Extension
The Numbering with the ID 9999 is the Global Numbering Plan
If Extension does not point to a Home DN, call is routed through the Public Numbering Plan
If Extension points to a Ho DN, then call i connected
Home DN
If E.164 Code points to a Home DN, then call is connected
The Global Numbering Plan can have many Prefix Access Codes
A Prefix Access Code can resolve to multiple E.164 codes
An E.164 Code will point to a single Destination
A Destination will have one or more Routes associated with it
A Route will point to a single Endpoint
The Enpoint is the representation of a Gateway in the Hp8k. Calls can be routed to this GW
E.164 Code
PNP
Privat Numbering Plan
GNP
Global Numbering Plan

Figure 52: Numbering Plan

A Numbering Plan specifies the format and structure of the numbers used within that plan. It typically consists of decimal digits segmented into groups in order to identify specific elements used for Identification, Routing, and Charging capabilities

Within a business group, there can be multiple numbering plans. At least one Business Group is needed for every dial plan together with one Numbering Plan. In one Business Group, the numbering plan can either be a **CNP (Common Numbering Plan)** or a **PNP (Private Numbering Plan)**.

When the Numbering Plan is created, a feature profile can be created for all users that are added to this Numbering Plan.

The following general rules must be observed when creating dialing plans:

A subscriber's **PNP (Private Numbering Plan)** sets up the routing rules that are **local** to the subscriber

A subscriber's business group **CNP (Common Numbering Plan)** sets up the routing rules that are **common** to a **specific** business group.

The OpenScape Voice **GNP (Global Numbering Plan)** sets up the routing rules that are **common** to all business groups.

Functional Sequence (Dialing Plans)

When a number is being translated, the translation engine (XLA) requires the originating party information in order to:

1) find the numbering plan (PNP, CNP or GNP) to start the translation
2) find the routing area
3) find the calling location
4) find the class of service
5) find the signaling type (SIP, MGCP, …)
6) find the bearer capability (speech, data, video, etc.)

All translation of implicit numbers starts with the PAC table of the subscriber's private numbering plan. Translation of explicit numbers starts in the destination code table of the subscriber's private numbering plan.

The goal of the translation engine is to determine one or multiple destinations. Valid destinations are endpoints, subscribers or a service.

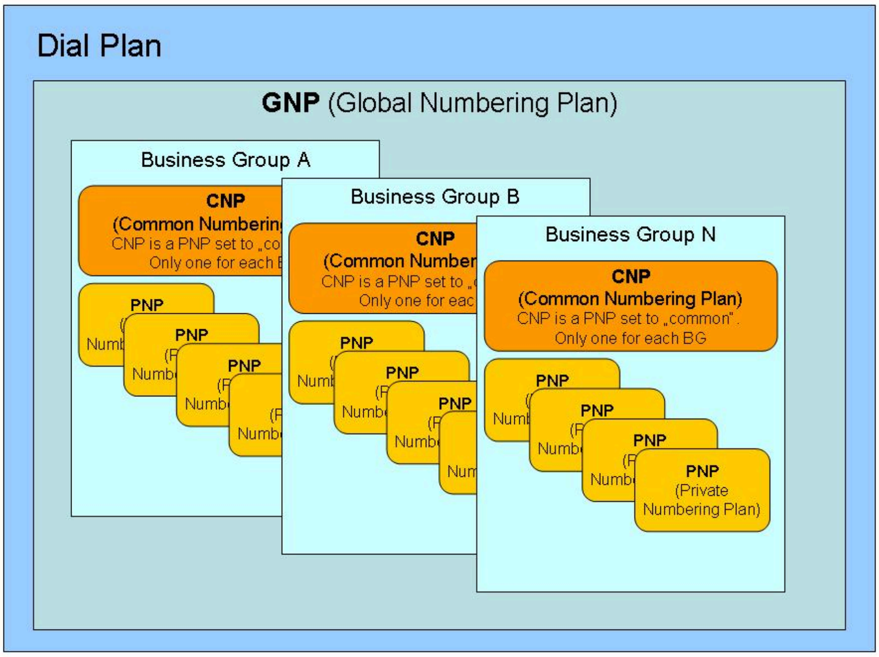


Figure 53: Dial Plan

6.1.1 PNP (Private Numbering Plan)

The private numbering plan is a customized plan for business group customers. A business group could be assigned with many numbering plans and all subscribers belonging to that business group could be covered by different Private numbering plan of that business group. A PNP (Private Numbering Plan) is used in a private network by subscribers belonging to either a Tenant, Business, or VPN group. A single OpenScape Voice system supports up to 999 PNPs.

NOTICE:

The default private numbering plan is used during the subscriber's creation. The common numbering plan is used to contain the common dialing plan for the business group. There can only be one common numbering plan per business group.

PNP Number Types

The PNP defines 3 types of numbers:

- **Local Number:** The local number (or subscriber number) must always be dialed in its entirety. The first few digits in the local number typically indicate smaller geographical areas or individual telephone exchanges. In mobile networks they may indicate a network provider in case the area code does not. Callers from a number with a given area/country code usually do not need to (but optionally may) include the particular area/country code in the number dialed, which enables shorter "dial strings" to be used. Devices that dial phone numbers automatically can include the full number with area and access codes, since there is no additional annoyance related to dialing extra digits..
- **RN (Regional Number):** The regional number is a particular form of a PNP Number which is unambiguous in the region concerned.

  NOTICE:

  A **Region** is the entire domain or a sub-domain of a PNP but does not necessarily correspond to a geographical area of a PISN.
- **Complete Number:** A number which is unambiguous in the entire PNP, i.e. which corresponds to the highest regional level employed in that PISN (Private Integrated Service Network).

Structure of Numbers

Depending upon the customer's wishes, 3 levels of private numbering plans are possible:

- L0 private numbering plan: no L1 or L2 level numbers exist in this type of numbering plan. Normalized numbers are L0 numbers
- L1 private numbering plan: no L2 level numbers exist in this type of numbering plan. Normalized numbers are L1 numbers.
- L2 private numbering plan: Normalized numbers are L2 numbers

A private numbering plan administrator must define an L1 code for each L2 private numbering plan number. This means that for an L2 private numbering plan, all numbers within the private numbering plan must have an L2 code and an L1 code defined. Equally so, for an L1 private numbering plan, all numbers within the private numbering plan must have an L1 code defined.

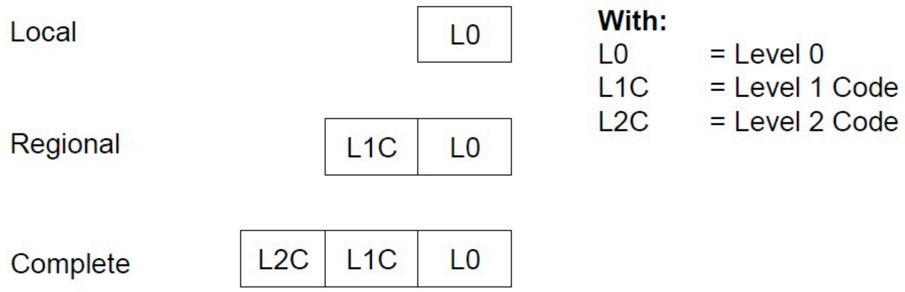


Figure 54: Structure for a Private Number

Further information

A PNP consists of digits that are grouped to identify specific elements used for identification, routing and charging capabilities to identify countries, national destinations, and subscribers. In a PNP, these elements identify the locations and stations. Additional PNPs are useful for different locations within one BG (Business Group).

BGs create their own individual PNPs based on the information provided in global translation and routing.

The PNP is a customized plan for the BG customers. A BG could be assigned with many NPs (Numbering Plans), and all subscribers belonging to that BG could be covered by different PNPs of that BG.

An individual subscriber belongs to a BG and uses the group's NP by default.

NOTICE:

If a group is not assigned to a specific NP, the default NP in the system is used. If the default NP is used, the subscriber must use the default PAC (PAC), destinations and E.164 NP.

PNP Configuration data

The PNP (i.e. the NP for a specific BG) provides the following configuration data categories:

- PAC
- Destination Code
- Location Code
- Extension
- Destination
- Route
- EP (Endpoint)

- EPP (Endpoint Profile)

6.1.2 CNP (Common Numbering Plan)

The BG's **CNP (Common Numbering Plan)** is used to set up routing and translation rules that are common to one business group (typically when multiple business groups exist). Only one numbering plan per business group can be assigned as a Common numbering plan. The CNP is an optional user-defined PNP which is assigned the type “Common".

Its purpose is to reduce data entries and use the data tables in many PNPs efficiently in one BG.

All PNPs of a BG can access the CNP data table of the same BG only. They cannot access the CNP of any other BG. The CNP can access the Global NP the same way any other PNP can.

6.1.3 GNP (Global/Public/E.164 Numbering Plan)

The **GNP (Global Numbering Plan** also known as **Public Numbering Plan** or **E.164 Numbering Plan**) is used to set up routing rules that are common to all business groups and allow them to communicate with each other. The Global Numbering Plan is often used for interbusiness group call routing. It is separate from Business Groups.

The components of the global numbering plan are accessible from all business groups and numbering plans. Any data table that needs to be accessed from all BGs/PNPs must be placed in the GNP.

GNP Number Types

It consists of 3 types of numbers:

- subscriber numbers
- national numbers
- international numbers

Structure of Numbers

Within the Global (public/E.164 numbering plan), the country code is mandatory. For each country a national authority may define whether it supports:

- national numbers and local numbers
- only national numbers
- only subscriber numbers

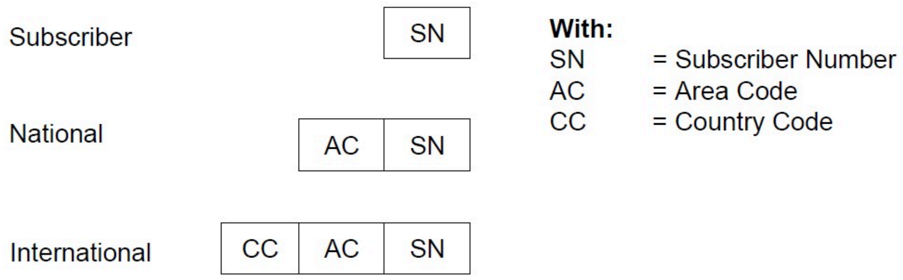


Figure 55: Structure for a public number/Global (E164) Numbering Plan

6.1.4 Open and Closed NP/DP (Numbering Plan/Dialing Plan)

OpenScape Voice supports closed and open numbering plans as well as implicit and explicit numbering. The term open and closed applies to both numbering plans and dialing plans.

I) When used with numbering plans:

An **open numbering plan** is 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 location dialing plans or multi-domain networks. In the enterprise environment, private networks typically use location codes to implement an open numbering plan.

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.

II) When used with dialing plans:

A **closed dialing plan** is a plan where the complete number or international number is used for all calls even if calling in the same area. This may be relaxed to the regional or national level. Many countries define a closed dialing plan, requiring the users to dial national numbers to reach each other even if they are calling from the same region. Otherwise, the dialing plan is called an **open dialing plan**.

The NANP is clearly a closed numbering plan, but the North American Dialing Plan is clearly open. Many countries are closing their dialing plan at the national level. The same rules apply to private dialing plans. Companies may define an open numbering plan, but may decide to operate a closed dialing plan and always dial the complete number.

6.1.5 Implicit and Explicit Numbering Plans

A number accompanied by the numbering plan indicator and the type of number within the indicated numbering plan (if necessary) is called an explicit number. These numbers do not need prefixes for dialing. A number without the numbering plan indicator and optionally the type of number within the indicated numbering plan needs prefixes to distinguish these indicators. Such a number is called an implicit number. Before the nature of the prefix is determined the indicators are defined as Unknown.

An **implicit numbering plan** is one in which the numbers are not accompanied by an indication to which numbering plan they apply.

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 plan** is one in which each number is accompanied by an indication as to which numbering plan it applies.

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 (number 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).

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). For IP connections of OpenScape Voice to the OpenScape 4000 and to other OpenScape Voice systems SIP-Q supports explicit numbering and is the required signaling protocol.

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. 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, OpenScape Voice does not support overlapped sending.

6.1.6 BG (Business Group)

The OpenScape Voice Assistant Business Groups feature enables you to provision large numbers of related subscribers, such as a business or other organization, at one time. Instead of provisioning individual members of the

Business Group (BG), you provision the BG and all members of that BG inherit all of the parameters that you set while provisioning. While you can assign only two services to the BG DN (main number), you can create individual subscribers (BGLs) and provision additional services.

Configuring Business Groups:

During the configuration of a BG an office code, a business group, and a numbering plan must be created as follows:

1) Create **Office Code**
2) Create **Home DN**
3) Create **PNP**

Within the **PNP**, the **PAC (PAC)** table, **Destination Codes/E.164 Codes**, **Destinations**, MLHG (Multiline Hunt Group), the Endpoint Profile, and the Endpoints will be created.

Related concepts

BG (Business Group) Feature on page 126
Business Group Branch Offices on page 438
Subscribers on page 439

6.1.6.1 Calling between Business Groups

Calls between BGs can be enabled by inserting the appropriate entries in the BG PAC 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 dia subscribers in BG1 (with number range 1561923xxxx), this can be accomplished by creating a PAC in BG2 with the values listed in below, 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).

Table 39: Example of BG Dialing: BG2 Dials BG1

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

Prefix Digits	Min length	Max length	Digit Pos	Insert	NOA	Dest. Type
91	12	12	1		Unknown	E.164 Dest

6.1.7 Quick Add BG (Business Group) Feature

The Quick Add Business Group Feature provides a user-friendly and time-saving method of creating a new BG (Business Group) by combining all fields required for creating a BG in one dialog.

The subscriber can configure the basic BG setup including all infrastructure settings such as Office Code and DNs (Directory Numbers), PNP (Private Numbering Plan), BG Feature Profile and intra-BG routing.

Functional Sequence

When creating a BG via the Quick Add Business Group Feature, a Feature Profile with all needed services is created automatically. The default name for the Feature Profile is derived from the BG name. The name pattern is <"FP_" + BG name>.

During the creation of a BG the following entities are also created:

- the Office Code + DNs
- the PNP

  The PNP is named <"NP_" + BG name> and assigned to this BG automatically.

System Specific Information

The default BG status is "active". This information is not displayed on the screen.

NOTICE:

The system may reject the creation of the BG (e.g. in case of insufficient resources, BG name already used, etc.). In such cases a corresponding error message is launched. None of the already created objects (like Office Code, PNP, etc.) are rolled back – they remain existing!

Other Characteristics

The results of the Quick Add BG action are displayed in a dialog which shows a summary of the BG data entered and of all the actions performed by the application while executing the Quick Add BG operation.

The results summary contains the BG name, Office Code, Subscriber number range, Default Feature Profile, Office Code already exists, creation of NP (Numbering Plan), creation of device group.

Results summary with example:

- BG name: Chris01
- Office Code: +49 (89) 722

- subscriber number range: 1000 to 1199
- default Feature Profile: NP_Chris01
- Office Code already exists: +49 (89) 722
- creation of Numbering Plan (NP): NP_Chris01
- creation of device group : Chris01PAC

6.1.7.1 Extension Dialing

Depending on which numbering plan the subscriber belongs to, the extensions from following range can be dialed :

- NP-Boca: 1XXX or 2XXX (depending on which subscriber are created)
- NP-Delray: 1XXXX or 2XXXX (depending on which subscribers are created)
- NP-Berlin: 401 and 402
- NP-Munich: 30001 and 30002

If you want to setup new extensions for some purpose (e.g. 3 digit extension), you need to provision using following steps:

- It is assumed that you already have subscribers created and HomeDNs created. For example, in NP-Boca, instead of using 4 digits extension, you want to use 3 digit extensions (000 to 999).
- In the prefix code table, add new entries, with digits 0 to 9. For each entry, use the following settings:
  - minDigitLenght = 3
  - maxDigitsLenght = 3
  - prefixType = Extension
  - insertDigits = 56152310
  - destType = E164DEST
  - noa = UNKNOWN

NOTICE:

Value of insertDigits field depends on which switch you are using.

6.1.7.2 Configuration of the Extension Dialing

During the Quick Add Business Group Task the administrator has the option to provide the Public Network Access Code and the Extension Length under the Routing Entries section.

- If no input is provided for the Extension Length, no PAC, Destination Code and Extension shall be created.
- If the administrator provides input for the Extension Length, the SOAP command CreateBGSuite shall determine the Extension Code and create the corresponding PAC(s), Destination Code(s) and Extensions based on the method below:

General Requirements

- Maximum PAC Length: 15

- Maximum Extension Length: 12

PAC for the Extension Dialling:

A PAC for the digit is required that is located in the **Extension Length** position within the Home Directory Number start counting from the end. The subscriber must compare the digit located above for the start Home DN and the end Home DN.

- If they are the same, a PAC for this digit must be created.
- If they are different, a PAC for each of them and for each of their intermediate digits must be created.

PAC: (code={ExtensionCode}, dnMinLen=ExtensionLength, dnMaxLen=ExtensionLength, DigitPos=0, PrefixType=ExtensionDialing, NOA=PNPExtension)

Destination for the Extension Dialling:

For each of the created PACs a Destination Code is needed. The Destination Code(s)

DestCode: (code={ExtensionCode}, NOA=PNPExtension, DestType=HomeExtension)

Extension:

For each of the created Destination Codes an Extension is needed. First the Overlap on the Office Code needs to be calculated as:

Overlap = ExtensionLength + OfficeCodeLength - HomeDNLength

- If the Overlap is negative or 0:
  - Extension: (Prefix={ExtensionCode}, length=ExtensionLength,
  - E.164prefix=HomeDN-ExtensionDigits+Prefix,
  - Destination type= HomeDN, Office code=OfficeCode)
- If the Overlap is positive
  - Extension: (Prefix={OverlapDigitsOfOfficeCode}, length=ExtensionLength,
  - E.164prefix=OfficeCode,
  - Destination type= HomeDN, Office code=OfficeCode)

The following example will facilitate the understanding of this method.

The Administrator via the Quick Add Business Group Task creates the BG Nick_res1 by providing the following data:

- Office Code = 30210486
- Home DN Start = 302104862801
- Home DN End = 302104863200
- Extension Length = 5 (i.e. the user will dial 6XXXX

Extension Code

Calculation of the Extension Code: The 5th digit counting from the end is **6** for the HomeDN Start and **6** for the Home DN End. The required PAC for the Extension Code= **{6}**.

PAC:

- PAC: (code=6, dnMinLen=5, dnMaxLen=5, DigitPos=0, PrefixType=ExtensionDialing,
- NOA=PNPExtension)

Destination Code:

- DestCode: (code=6, NOA=PNPExtension, DestType=HomeExtension)

Extension:

- Overlap = 1 (5+8-12)
- E.164prefix=30210486
- Destination type= HomeDN, Office code=30210486)

6.1.8 Business Group Branch Offices

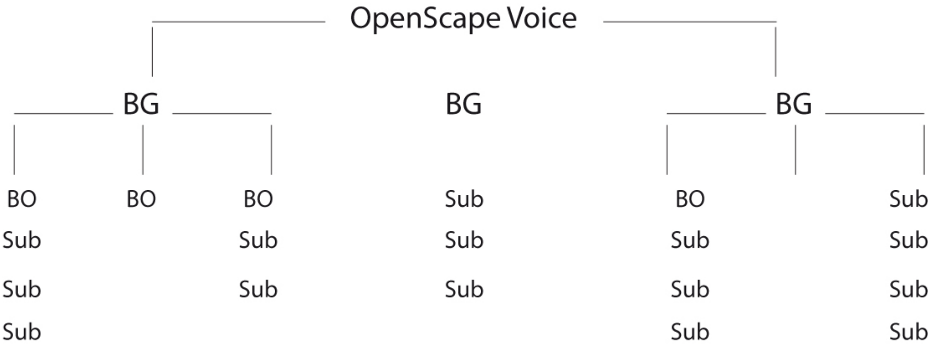
All subscribers that do NOT belong to a specific Branch Office are considered to belong to the "Main Office" which represents the lack (absence) of a Branch Office. So all subscribers in the OpenScape Voice Assistant are displayed under a specific Branch Office or under a “virtual” Branch Office (Main Office).

The relationship between Business Groups (BG) and Branch Offices (BO) within OpenScape Voice is characterized by the following properties:

- One BG can have zero or more BOs.
- One BO always belongs to a BG.
- One BG can have many subscribers (Sub).
- One BO can have many subscribers.

  Subscribers of a BO that belongs to a BG are still considered subscribers of the BG as well as subscribers of the BO.

  For instance, intra-BG feature transparency (such as calling name delivery) applies for subscribers belonging to different BOs of a given BG.
- Subscribers always belong to a BG.
- Subscribers do not always belong to a BO.



Assign and Unassign Media Servers from Branch Office

The buttons **Assign/Unassign** are disabled when you go to MediaServers from BranchOffice= MainOffice.

The buttons **Assign/Unassign** are fully functional ONLY when you go to MediaServers from BranchOffice and you have already applied the needed/ specific provisioning for the Distributed Media Server deployment scenarios with BranchOffices-Automatic Configuration. For further details, please refer to Help paragraph for Media Server Deployment Scenarios at OpenScape Voice

Related concepts

BG (Business Group) on page 433

6.1.9 Subscribers

A subscriber is a SIP user/a SIP telephone equipped with parameters like telephone number or SIP security settings. Any subscriber belongs to a single business group.

The following are important parameters associated with a subscriber:

- Business group, office code, and extension (subscriber number)
- Display name for display on the phone of the call partner
- Routing area to allow site-specific routing
- Keyset operation for multiline appearance
- Class of service to allow authentication-specific routing—for example, allowing international calls for individual subscribers
- Feature profile, which defines a feature template of telephony features and SIP security parameters (Realm = Protection Domain, SIP User Name, SIP Password)

Related concepts

BG (Business Group) on page 433

6.1.10 Basic Subscriber Types

OpenScape Voice subscribers can be categorized into five basic types: Type I, Type II, Type III, Type IV, and Type V.

- **Type I: Subscriber with public network number only.**

  This is the type of subscriber that is most used currently. This subscriber belong to a company that does not provide a private numbering plan.
- **Type II: Subscriber with private network number only.**

  This subscriber belong to a company that does provide a private numbering plan. This company probably does not have very many public network numbers and therefore, must create some users that do not have a public network number. The public network number presented for these users may be the BG Main Number or the number provisioned in the Outgoing Presentation Call Status feature – if assigned to the subscriber.
- **Type III: Subscriber with private network number derived from public network number.**

  This subscriber has a public network number and a private network number linked using the extension part of the public number. For this subscriber, the office code of their Home DN uses the office code of the public network number.
- **Type IV: Subscriber with private network number not derived from public network number.**

  Type IV: Subscriber with private network number not derived from public network number. This subscriber has a public network number and a private network number where the extension part of the public network number and the extension part of the private network number are not the same. For this subscriber, the office code of their Home DN uses the office code of the public network number. The private network number cannot be displayed by the HiPath 8000. Only translation is capable of resolving the private network number to the subscriber who owns the private network number.

- **Type V: Subscriber that only has an extension**

  Type V: Subscriber that only has an extension. These subscribers have neither a private network number nor a public network number. For this subscriber an office code with the leading three digits of the extension must be created. Another approach could be to force the definition of a private location code and force this type of subscriber into the Type II number scheme. The OpenScape Voice currently cannot configure this kind of subscriber.

NOTICE:

There are customers (for example IBM) that actually configure their switch with only Type II numbers and provide a separate public network number for each subscriber via the Outgoing Call Presentation Status feature.

6.1.11 Defining Subscribers within OpenScape Voice

This section describes the creation of a basic numbering plan using the OpenScape Voice Assistant tool.

Functional Sequence

1) The first step in defining the subscribers within a OpenScape Voice is defining a block (or blocks) of E.164 numbers for these 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. These numbers are assigned using OpenScape Voice Assistant. 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 for OpenScape Voice, the definition of subscribers can begin. Before a subscriber line can be defined, the administrator must define at least one BG. Every subscriber line must be assigned to one (and only one) BG.

3) Each BG must be assigned a default (common) numbering plan. The number plan must be given a name before the BG is defined, so that the assignment 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.

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

4) Before the subscriber can be defined, the administrator must define a feature profile, which is the set of default features that each subscriber will be given.

Once the BG and associated feature profile and numbering plan have been defined and selected, subscribers (business group lines [BGLs]) can be created.

6.1.12 Creating Multiple Subscribers

This feature allows the user to create many subscribers (BGLs) comfortably using an existing subscriber (BGL) as a template.

Requirements

There must be at least one existing subscriber (BGL) that is selected as a template.

Functional Sequence

1) Select an existing subscriber (BGL) from a list of subscribers (BGLs). This subscriber (BGL) is called the template subscriber (BGL) or source subscriber (BGL).

2) The user hits an upload button which causes the file to be read into a grid while a first syntactical check is performed.

3) Password can also be used from the source, selected via checkbox.

4) Then the user hits the Submit button. The admin tool will create an error file in the same directory as the original file with an appropriate suffix that contains all original entries that delivered errors with comment lines indicating the error reason. This file may be used for a rerun.

6.1.13 Subscriber ID

A unique ID (identification) is assigned to each subscriber. This 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.

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

NOTICE:

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 OpenScape Voice switches.

OpenScape Voice supports the concept of subscriber groups (within a business group) being physically scattered in locations (sites) that are physically remote from the 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.

6.1.14 Managing BG related Subscribers

Business Groups (BGs) provide a simple method for managing related subscribers. Subscribers (BG members) inherit the features of the Business Group, but the features can be assigned or restricted to individual subscribers.

Editing Subscribers via the Subscriber Dialog

Use the **Business Group** > **Subscribers** dialog of the OpenScape Voice Assistant in order to view, modify or delete the subscriber.

The Subscribers dialog contains the following tabs:

- **General** tab: contains the subscriber configuration data
- **Display** tab: contains all display information of a subscriber
- **Routing** tab: contains all routing information
- **Connection** tab: contains all connection settings for a subscriber
- **Security** tab: contains all possible security settings like SIP Authentication, Secure RTP and PIN Support.
- **Keyset** tab: contains all parameters for provisioning multiple subscribers on a SIP phone.

- **Groups** tab: contains Call Pick Up Group and Hunt Group Membership settings
- **Features** tab: contains all the feature profile settings for a subscriber and all selectable Subscriber Features.
- **Applications** tab: contains all possible application settings (Accounting, DLS)

Editing Subscribers using the Quick Tasks

The fastest and most convenient way to create subscribers is to use the **Quick Add Subscriber** feature.

The advantage of the Quick Add Subscriber feature is that all steps necessary to create a subscriber are grouped into one dialog, thus reducing the time of creating a subscriber to a minimum. The following areas are covered during execution of Quick Add Subscriber:

- Business Group area - covering BG Name, Office Code, Subscriber Number
- Subscriber area - covering Display Name, Routing Area
- Configuration area - covering Keyset Operation, Class of Service, Feature Profile, Add Routing Entry (checkbox)
- SIP Security area - covering Realm, User Name, Password

The feature supports both the creation of individual subscribers and mass provisioning for a given BG. To be able to do a first call, it is supposed that at least two numbers exist with two associated existing SIP phones so that the results can really be verified. After successful creation the plugged in phones are able to register.

The fastest and most convenient way to edit subscribers is to use the **Quick Edit Subscriber** feature.

Quick Edit Subscriber allows the user to directly access the subscriber data, without having to navigate via the BG or PNP of the subscriber. This is especially helpful if the BG or the PNP of the subscriber is not known.

If there are already existing subscribers (BGLs) for the BG, the user may select one as a template. All entries from this subscriber (BGL) will be taken except for the varying entries i.e. number, name, authentication password.

NOTICE:

The Subscriber templates are provided only for OpenScape Voice User Management (no implementation for „Quick Add Subscriber“). The subscriber templates are system wide, i.e. not BG related.

Bulk Editing Subscribers

The **Bulk Edit** feature allows the user to modify more than one data record of the same entity simultaneously via the GUI.

To bulk edit certain subscribers, the checkboxes on the left side must be checked. **Only the activated parameters have an impact on the selected Subscribers**. Parameters without a checkbox are not editable in the **Bulk Edit** mode.

6.1.14.1 Attributes for a SIP Subscriber

This section describes the attributes that can be assigned to subscribers.

Functionality of the attributes

The following bulleted items describe the functionality for each of the attributes available for the selected SIP Subscriber:

- **Transfer HandOff**

  If selected (enabled), during transfer handoff, REFER and NOTIFY transactions will be passed transparently through OSV. Used for TRANSFER_HANDOFF for Genesys.
- **Support Media Redirection**

  If selected (activated), this attribute assigns the Support Media Redirection feature to the selected subscriber.
- **Override Irm Codec Restrictions**

  If selected (enabled), the Override IRM Codec Restrictions attribute will be assigned to the selected subscriber.
- **Allow Sending Insecure Referred by Header.:**

  If selected (activated), this attribute makes sure that calls get charged to the right call account. This is achieved by transporting the user number in the additional SIP CDR header field "X-Siemens-CDR" for the endpoint used.
- **VIP (Very Important Person) Monitoring**

  If selected (activated), this attribute enables the Very Important Person (VIP) status for the subscriber. When the VIP filter is set to "VIP Yes" - all subscribers having the VIP (Very Important Person) monitoring attribute will be displayed.
- **Video Call Allowed**

  If the **Video Call Allowed** check mark is turned **ON** (default), then the OpenScape Voice will allow video calls across the server.

  If the **Video Call Allowed** check mark is turned **OFF**, then even if subscriber makes video calls, the port of all video m-lines will be set to zero by the OpenScape Voice server before routing the call to intended receiver
- **Send Public Identity in From Header**

  This new endpoint attribute is only applicable to the SIP subscribers interface (keysets and non-keysets).

  - If this attribute is not enabled, both the **From** header field and the **apiname** (PAI) header field in the SIP INVITE request to the SIP subscriber contain the calling party’s name and dialable number.
  - If this attribute is enabled, the SIP INVITE request to the SIP subscriber is populated as follows:

    The **From** header field contains the public identity (name and number) of the calling party in Fully Qualified Public Number format.

    The **P-Asserted-Identity (PAI)** header contains the calling party’s name and dialable number.
- **Send International Numbers in Global Number Format (GNF)**

  If selected (enabled), the OpenScape Voice adds a '+' in front of all numbers which have NPI = PUBLIC and NOA = INTERNATIONAL. In order to do this, both Translation and the Display Number Modification tables MUST be provisioned to send numbers with NPI = PUBLIC and NOA = INTERNATIONAL to this endpoint.

NOTICE:

This attribute can be configured both for SIP Trunking and for SIP Private Networking endpoints.

If the endpoint attribute **Send International Numbers in Global Number Format (GNF)** is set to **true** on a **SIP Private Networking** endpoint, then all public numbers are sent to this endpoint in GNF format.

- **Do Not Publish Registration to E911 Data Manager**

  The default value of this attribute is not set (off) and in this case the E911 Data Manager is updated whenever the Subscriber is registered or unregistered.

  If this attribute is set (on) then whenever the Subscriber is registered or unregistered the E911 Data Manager is not informed.

IMPORTANT:

If the attribute is changed from not set (off) to set (on) then the E911 Data Manager is informed and the Subscriber is removed from its Registration Publication table.

- **ACD Call Distribution Device**

  When this attribute is enabled, any call transferred from this subscriber device, is identified to the transferred-to device as an ACD call. The default value is unchecked.

NOTICE:

The transfer service must be enabled in the associated endpoint profile.

- **Reserve** Attributes for Endpoints

  These attributes are reserved to allow for the quick introduction of future functionality. If usage of one of this attributes is required then there will be corresponding release notes issued describing the details. There are three Reserve Attributes available:

- – **Reserve 6**
  – **Reserve 8**
  – **Reserve 9**

NOTICE:

Once a Reserve Attribute has been used then it should be replaced with a proper named attribute as soon as practical

- **Disable Long Call Audit**

  When calling or called party has this attribute set to true, long call audit is disabled for this call. Default value is unchecked.

  If the attribute is checked then it will eliminate the impact of the long call duration timer on Hoot and Ringdown lines used in trading solutions.
- **Send alphanumeric SIP URI when available**

  When this attribute is enabled, it is possible to enable the SIP Endpoint to preferably send alphanumeric SIP URI when one is available.
- **Do not send alphanumeric SIP URI**

  When this attribute is enabled, it is possible to prevent sending an alphanumeric SIP URI to a SIP endpoint
- **Trusted Subscriber**

  If the SIP subscriber has this attribute set then OSV offers the capability to verify whether the IP address used by the SIP subscriber in the bottom Via header is trusted. The attribute is used to support backward compatibility of RTP flag `Srx/Main/AuthTraverseViaHdrs` with the RtpTrue setting.
- **Allow Subscriber Provided Calling Identity**

  If enabled the subscriber is allowed to provide an identity (number and name) to present to the called party. A call with SPCID will always be signaled as an external call. i.e. the presence of the SPCID marks the call as an external call, regardless of the normal internal/external determination.
- **Simultaneous calls not allowed from multiple contacts**

  When this attribute is enabled, OSV will not allow multiple contacts of a subscriber to ring, if one of these contacts is already busy in another call. When a contact initiates a call to the same subscriber DN all other contacts will ring.

  When a call exists between two contacts, an incoming call is sent to the contact that initiated the first call and depending whether call waiting is enabled or not, the call is indicated on the phone or returns busy.

  When a call exists between two contacts, only the initiating contact can initiate an outgoing call but only to other DNs and not to itself.

  This functionality is configured per subscriber, so that certain subscribers can retain the previous logic of allowing multiple calls to multiple contacts at the same time whereas other subscribers can follow the new functionality.This attribute is disabled by default.

  IMPORTANT:

  Circuit clients are not multiple contacts of the subscriber that is using them and as such this functionality is not supported.
- **Disable SRTP**

  When the attribute is checked, then SRTP is not offered to the endpoint and removed when offered by the endpoint. An Encryption license is not checked out with this setting. When the attribute is unchecked SRTP is allowed to and from the endpoint, and If Encryption license checking is enabled in the OSV license file, an Encryption license is checked out when a subscriber registers a contact using TLS. By default the attribute is unchecked.

- **Do Not Allow URNs in R-URI/TO Header for NG911 Calls**

  When the attribute is set, the ESRP replaces the emergency service urn in the R-URI with the URI discovered by the NG911 service. The outgoing message is like a normal call without the NG911 specific R-URI/To headers. The next hop URI is not included in a Route header. When the attribute is not set, then the normal ESRP functionality is applied.The default value of the attribute is FALSE, that means not checked.
- **Do not allow NG911 headers**

  This attribute allows you to control the transport of NG911 headers. When it is set, the NG911 headers are not transported towards the call taker's device. The default value is False, meaning unchecked.
- **Record All Calls**

  Check this attribute to allow an SRC capable OSB to support a RecordingSession (RS). This subject interface is applicable to SIP-NNI and SIPsubscriber endpoints. All calls requiring an RS are managed by the **SRCCapable** OSB.

  NOTICE: This attribute must be checked when the SIPREC based OpenScape Voice Call Recording solution is enabled.
- **Do Not Send Conference Indication (Hide isFocus)**

  When this attribute is checked, it controls the transport of the focus parameter in the contact header, to hide the conference from the originating networks.
- **Do Not Allow Geolocation Info**

  This attribute controls the tranport of (i3) location info over the SIP interface for the particular destination. When checked, the OSV:

  – Strips off the Geolocation header field from the outgoing message
  – Strips off the Geolocation-routing header from the outgoing message
  – Strips off the PIDF-LO document transported in the body of the message for location-by-value use cases

  The default value is False meaning that location info will be transported properly. This attribute does not affect the transport of location info over the CSTA interface.

6.1.15 Quick Add Subscriber

The Quick Add Subscriber Feature provides a user-friendly and time-saving method of creating a new Subscriber by combining all fields required for creating a Subscriber in one dialog.

6.1.16 Bulk Editing Subscribers

The **Bulk Edit** feature allows the user to modify more than one data record of the same entity simultaneously via the GUI.

This modification is possible for the following entities containing no unique fields:

- **Subscribers**

- Endpoints
- Destination Codes

To bulk edit certain parameters, the checkboxes on the left side must be checked. **Only the activated parameters have an impact on the selected Subscribers**. Parameters without a checkbox are not editable in The **Bulk Edit** mode.

6.1.17 Subscriber Templates

The **Subscriber Templates** dialog is used to list, add, edit and delete a Subscriber Template on behalf of OpenScape Voice User Management. The subscriber templates are defined on a per Business Group basis.

Purpose and use of subscriber templates

Typically most subscribers attributes have to be configured in a common way for the various subscribers of the same company.

In order to avoid configuring the same data several times for each individual subscriber, they can be configured in one step (before any subscriber is created) and saved in the form of a template.

When a subscriber is created via OpenScape Voice User Management the template name is used instead of the big number of corresponding attributes hence subscriber creation becomes faster and easier

Data Organization within Subscriber Templates Dialog

The data associated with the Subscriber Templates is organized via tabs. These SUbscriber Template tabs parallel / are the same as those for the Subscriber Dialog.

The Subscribers Templates management contains the following tabs:

- **General** tab: contains the subscriber configuration data
- **Display** tab: contains all display information of a subscriber
- **Routing** tab: contains all routing information
- **Connection** tab: contains all connection settings for a subscriber
- **Security** tab: contains all possible security settings like SIP Authentication, Secure RTP and PIN Support.
- **Keyset** tab: contains all parameters for provisioning multiple subscribers on a SIP phone.
- **Groups** tab: contains Call Pick Up Group and Hunt Group Membership settings
- **Features** tab: contains all the feature profile settings for a subscriber and all selectable Subscriber Features.
- **Applications** tab: contains all possible application settings (Accounting, OpenScape UC, DLS)

6.1.17.1 Attributes for a Subscriber Template

This section describes the attributes that can be assigned to subscribers.

Functionality of the attributes

The following bulleted items describe the functionality for each of the attributes available for the selected SIP Subscriber:

- **Transfer HandOff**

  If selected (enabled), during transfer handoff, REFER and NOTIFY transactions will be passed transparently through OSV. Used for TRANSFER_HANDOFF for Genesys.
- **Support Media Redirection**

  If selected (activated), this attribute assigns the Support Media Redirection feature to the selected subscriber.
- **Override Irm Codec Restrictions**

  If selected (enabled), the Override IRM Codec Restrictions attribute will be assigned to the selected subscriber.
- **Allow Sending Insecure Referred by Header**

  If selected (activated), this attribute makes sure that calls get charged to the right call account. This is achieved by transporting the user number in the additional SIP CDR header field "X-Siemens-CDR" for the endpoint used.
- **VIP (Very Important Person) Monitoring**

  If selected (activated), this attribute enables the Very Important Person (VIP) status for the subscriber. When the VIP filter is set to "VIP Yes" - all subscribers having the VIP (Very Important Person) monitoring attribute will be displayed.
- **Video Call Allowed**

  If the **Video Call Allowed** check mark is turned **ON** (default), then the OpenScape Voice will allow video calls across the server.

  If the **Video Call Allowed** check mark is turned **OFF**, then even if subscriber makes video calls, the port of all video m-lines will be set to zero by the OpenScape Voice server before routing the call to intended receiver
- **Send Public Identity in From Header**

  This attribute is only applicable to the SIP subscribers interface (keysets and non-keysets).

  – If this attribute is not enabled, both the **From** header field and the (PAI) header field in the SIP INVITE request to the SIP subscriber contain the calling party’s name and dialable number.

  – If this attribute is enabled, the SIP INVITE request to the SIP subscriber is populated as follows:

    The **From** header field contains the public identity (name and number) of the calling party in Fully Qualified Public Number format.

    The **P-Asserted-Identity (PAI)** header contains the calling party’s name and dialable number.
- **Send International Numbers in Global Number Format (GNF)**

  If selected (enabled), the OpenScape Voice adds a '+' in front of all numbers which have NPI = PUBLIC and NOA = INTERNATIONAL. In order to do this, both Translation and the Display Number Modification tables MUST be provisioned to send numbers with NPI = PUBLIC and NOA = INTERNATIONAL to this endpoint.

> **NOTICE:**
>
> This attribute can be configured both for SIP Trunking and for SIP Private Networking endpoints.
>
> If the endpoint attribute **Send International Numbers in Global Number Format (GNF)** is set to **true** on a **SIP Private Networking** endpoint, then all public numbers are sent to this endpoint in GNF format.

- **Do Not Publish Registration to E911 Data Manager**

  The default value of this attribute is not set (off) and in this case the E911 Data Manager is updated whenever the Subscriber is registered or unregistered.

  If this attribute is set (on) then whenever the Subscriber is registered or unregistered the E911 Data Manager is not informed.

> **IMPORTANT:**
>
> If the attribute is changed from not set (off) to set (on) then the E911 Data Manager is informed and the Subscriber is removed from its Registration Publication table.

- **Reserve** Attributes for Endpoints

  These attributes are reserved to allow for the quick introduction of future functionality. If usage of one of this attributes is required then there will be corresponding release notes issued describing the details. There are three Reserve Attributes available:

- – **Reserve 1**
  – **Reserve 2**
  – **Reserve 3**

> **NOTICE:**
>
> Once a Reserve Attribute has been used then it should be replaced with a proper named attribute as soon as practical

- **Disable Long Call Audit**

  When calling or called party has this attribute set to true, long call audit is disabled for this call. Default value is unchecked.

  If the attribute is checked then it will eliminate the impact of the long call duration timer on Hoot and Ringdown lines used in trading solutions.

- **Trusted Subscriber**

  If the SIP subscriber has this attribute set then OSV offers the capability to verify whether the IP address used by the SIP subscriber in the bottom Via header is trusted. The attribute is used to support backward compatibility of RTP flag `Srx/Main/AuthTraverseViaHdrs` with the RtpTrue setting.

- **Allow Subscriber Provided Calling Identity**

  If enabled the subscriber is allowed to provide an identity (number and name) to present to the called party. A call with SPCID will always be signaled as an external call. i.e. the presence of the SPCID marks the call as an external call, regardless of the normal internal/external determination.

6.1.18 BG (Business Group) NP (Numbering Plan) - Normalization

The normalization feature normalizes telephone numbers from local to national format and from national to international format.

This normalization can take place at the PAC (Prefix Access Code) table level or at the Destination Code level.

If a normalization is performed at the Destination Code level, it is accomplished by a generic code processing mechanism that provides the capability to modify the called party number and its nature of address after translation.

Requirements

This feature requires that a code processing destination type is defined. The selected entry in the code processing table does the following:

- Defines a rule for modifying the dialed number (delete and add digits) and changing the NOA (Nature of Address) before the next routing step.
- Gives the option to retranslate the number, which causes the system to use the modified number on a new pass through the Global Number Code table or go to a specified destination of a different type.

The following are examples of the normalization:

- A number dialed without a LAC (Local Area Code) can be normalized to a national number. For example, a subscriber number of 72212345 can be normalized to 8972212345, where 89 is the LAC.
- A number dialed without an LAC can be normalized to an international number. For example, a subscriber number of 72212345 can be normalized to 49 8972212345, where 49 is the Country Code (CC) and 89 is the LAC.
- A number dialed with an LAC can be normalized to an international number. For example, a subscriber number of 89 72212345 can be normalized to 49 8972212345, where 49 is the CC and 89 is the LAC.

6.1.19 BG (Business Group) NP (Numbering Plan) - Types and Codes

The BG (Business Group) NP (Numbering Plans) provide the dialing plans specific to a BG. To reach lines outside of the BG, the caller usually dials an access code.

Each BG can support several NP types listed in the table below.

Table 40: Types of Business Group Numbering Plans

Numbering Plan Type	Description
DN-level (formerly known as BGL-level*) primary (* BGL = Business Group Line)	This NP is assigned to the subscriber's endpoint profile. Translation always start at this level. However, if the administrator does not assign this NP, the BG's default NP is automatically assigned to the DN (Directory Number) and is used during processing of a call.
BG common numbering and routing	This NP provides an additional NP at the BG level. It permits all numbering and routing that is shared by a BG to be provisioned in a common NP that can be used by all BG members.
BG default	This NP is an empty initial NP that is automatically created by OpenScape Voice Assistant when a new BG is created. • If the BG will have only one NP, this default NP will be the BG's one and only NP. • If the BG will have multiple NPs to support multiple locations within the BG, this default NP becomes the common numbering and routing plan described above.
System default (E.164- or NANP-compliant)	This NP, also known as the Global Numbering Plan, can be used for common public dial plan access and can be used by any BG.

These multiple NP types are useful for the following reasons:

- Access is retained to features available only to members of the same BG. Regardless of the number of branch offices present in an OpenScape Voice network, all subscribers can be combined into one BG.
- Because a common dialing and routing plan is present, it is unnecessary to separately update each branch office's NP when an additional branch office is added.

Specific access codes

A BG's NP also specifies the access codes listed in the next table:

Table 41: Access Codes Defined in Business Group Numbering Plans

Access Code Type	Number of Digits	Description
Attendant	1 to 5	Connects an OpenScape Voice user to the attendant. Many times, it is defined as the digit 0.
PSTN (Public Switched Telephone Network)	1 to 5	Connects an OpenScape Voice user to the public network. Many times, it is defined as the digit 9. Also known as off-net call prefix and off-net access code.

Access Code Type	Number of Digits	Description
Private Network	1 to 6	Gives access to private networks. For example, dialing the digit 8 could lead to connection to a private network. Also known as on-net call prefix and on-net access code.

- The subscriber can use * and # as the first (and perhaps only) digit of any of the access codes.
- If needed, the customer can specify a code from 1 to 5 digits for use as an equivalent to *.
- * code conflicts are resolved by use of critical inter-digit timing or use of # as an end-of-dialing indicator.

6.1.20 BG (Business Group) NP (Numbering Plan) - Configuration

In order to permit extension number calling between members of a BG, the BG numbering plan must be configured with the appropriate Prefix access code (New destination code table entries and 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.

6.1.21 BG NP Configuration - 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 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 OpenScape Voice Assistant, the administrator can go directly from the Destination Code table to the Extensions table by clicking the table name on the left, or the Extensions tab near the top right of the display.

- **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).
- **Destination Name** – the destination name is a valid entry in the destination table, and is required. In the example below it indicates the home DN table associated with this block of extensions (1561923).

BG NP Configuration

Table 42: Prefix Access Code Table Entries Permitting E.164 Dialing

Field	Input Value	Comment
Digits	1561923	
Minimum length	11	
Maximum length	11	
L2 length	6	Delete 6 digits
Digit Position	6	Leave blank.
Prefix Type	Extension Dialing	
Nature of Address	PNP Extension	Only valid choice
Destination Type	None	Go to BG destination code table

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 the table below:

Table 43: Second Prefix Access Code Table Entries Permitting Extension Dialing

Field	Input Value	Comment
Digits	31	
Minimum length	5	
Maximum length	5	
L2 length	0	Delete 6 digits
Digit Position		No digits deleted.
Prefix Type	Extension Dialing	Leave blank

Field	Input Value	Comment
Nature of Address	PNP Extension	Only valid choice
Destination Type	None	Go to BG destination code table

Continuing the same example, the administrator should add the entry shown in the following code table:

Table 44: Destination Code Table Entries

Field	Input Value	Comment
Destination Code	31	
Nature of Address	PNP Extension	
Class of Service		Leave blank
Traffic Type		Do not assign a traffic type
Routing Area		Leave blank.
DN Office Code	Extension Dialing	Leave blank
Destination Type	PNP Extension	Go to the Extension table for routing
Destination Name	None	

To complete the example started above, a new entry is created with the fields filled in as shown in the following table:

Table 45: BG Extensions Table Entries

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	15619231	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	1561923	Pick from the list of home office codes

Although extension numbers are used for routing, in this example, the endpoints are not identified nor are they 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.

6.1.22 Location Codes and Private Numbering Plans

The Location Code defines the segmentation of the dialed numbers. The Location Code is derived from the Prefix Access Code.

The Location Code is segmented into Country Code (L2), Area Code (L1) and Local Office Code (L0). If the matching Location Code contains also digits which are part of the extension numbers, those need to be skipped.

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 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

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.

- A **PNP 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.
- A **PNP L1** private number is the private network equivalent of a national number in the public network.
- A **PNP L2** private number is the private network equivalent of an international number in the public network.

Using 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 OpenScape Voice switch in the private network.

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, 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.

Functional Sequence

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 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.

Location code definition for a Level 3 PNP network might look like the one shown in the following table:

Table 46: Location Code—Level 3 Example

Parameter	Value	Comment/Note
Location code digit string	1408492	This is a level 3 PNP location code.
L0 length	3	994
L1 length	3	492
L2 length	1	408

Parameter	Value	Comment/Note
Digits to skip	6	The 2 in 492 is part of the extension number.

An example location code definition for a L0 PNP network might look like the one shown in the following table:

Table 47: Location Code—L0 Example

Parameter	Value	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.

Related concepts

Please select the appropriate help topic on page 657

6.1.22.1 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.

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.

6.1.22.2 Using PNP Location Codes

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 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, system wide.

The location code information also can also play a role in determining how the caller ID is displayed on the OpenScape Voice subscriber endpoints and call logsOn calls between subscribers belonging to different numbering plans, the Display Number Modification logic can be configured to display the appropriate PNP number of the other party number, rather than public number.

6.1.23 PAC (Prefix Access Codes)

The PAC (Prefix Access Code) is the code entered in the numbering plan (GNP and PNP). A call can only be routed if the dialed digits are matching a PAC.

Rules for Translation

Each private numbering plan contains rules for translating numbers. The implicit numbers (where numbering plan indicator and type of number are unknown) are matched against the subscriber numbering plan’s prefix access code table (PAC).

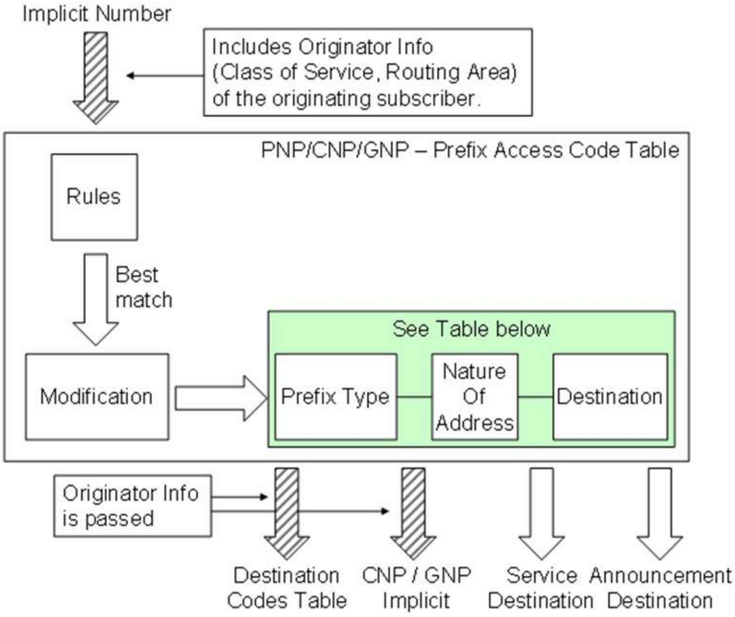


Figure 56: Prefix Access Code Table

Prefix Access Codes for PNP and GNP:

There are two possibilities to edit PAC:

- via the **GNP-Prefix Access Codes dialog** for Private and Global Translation and Routing
- via the **PNP- Prefix Access Codes dialog** for a selected Business Group

It is strongly recommended to have all default service access codes in the GNP and override them in the PNP if they need to be different for the users of that PNP.

NOTICE:

A call can only be routed if the dialed digits are matching a PAC.

A Prefix Access Code defines the dialing sequence of a number plan for E.164 and PNP. This table translates prefix codes, feature access codes, speed codes, and other access codes, and determines the nature of address (NOA).

Prefix Access Codes are created to define single digits or strings of digits that enable callers to select specific networks, number formats, and services. For example, a caller uses an international Prefix Access Code to indicate that the subsequent digits in the dialed number identify an international public telecommunication number.

A simple prefix access code transforms an extension to international format and forward that number to the global numbering plan, where a common routing on the base of international numbers should be performed.

When the subscriber creates a Prefix Access Code, he/she has to specify the following properties:

- **Prefix Type:** The prefix type describes what the prefix is used for.

  Below is the list of prefix types that can be selected when adding a prefix access code to a PNP/CNP/GNP with the OpenScape Voice:

  – **Vertical Service** (PNP/CNP/GNP) — vertical service code or feature access code.

    The VSC (Vertical Service Code) feature provides for user-dialed codes, such as FAC (Feature Access Codes), that allow access to features and services. Services invoked by VSCs include OpenScape Voice-based station call forwarding, customer-originated trace, and many others.

    NOTICE:

    For more information about the available services for **Vertical Service** selected as Prefix Type, see the table below.

  – **Speed Calling** (PNP/CNP/GNP) — The Speed Calling service enables subscribers to dial telephone numbers using fewer digits than is normally required. The subscriber dials a Speed Calling code to reach a frequently dialed number. The Speed Dialing feature allows intercom numbers and access codes + DN (e.g., 9 + DN) in the speed dial list.

  – **Invalid Code** (PNP/CNP/GNP) — a digit prefix that must be blocked.

  – **Extension Dialing** (PNP/CNP) — internal extension number prefix.

    The extension dialing feature allows a subscriber in a business group to dial other subscribers in the same business group by dialing an abbreviated number that is synonymous with the extension number.

  – **Off-net Access** (PNP/CNP) — A prefix access code to permit access to remote destinations using facilities provided by the PSTN or a third-part service provider.

  – **On-net Access** (PNP/CNP) — 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.

  – **Attendant** (PNP/CNP) — The attendant is always a local function, though a centralized attendant can be accessed as well. As it is a local function the prefix access code table usually modifies the digits to a local extension or hunt group and then forwards the result to the destination codes table. When using a centralized attendant, the attendant code is forwarded as an on-net access number to the CNP, where it can be handled. One could also go to the GNP.

  – **Private Facility** (PNP/CNP) — private facility access code.

  – **Service Code** (PNP/CNP) — Short dial sequences used to obtain access to external carrier provided services. Examples are 911, 112 etc.

  – **Satellite Avoidance** (PNP/CNP) — Route codes passed to external carriers to inform them about routing requirements to properly handle the call type. Certain call types are unable to cope with network delays so the carrier must be made aware to route the call to the destination using the appropriate circuits.

  – **Circuit Switched Data** (PNP/CNP) — Route codes passed to external carriers to inform them about routing requirements to properly handle the call type. Certain call types are unable to cope with network delays so the

carrier must be made aware to route the call to the destination using the appropriate circuits.
  - **Hotline Voice Grade** (PNP/CNP) — The carrier is informed of this access to use the proper circuits for the call type (voice).
  - **Hotline Data Grade** (PNP/CNP) — The carrier is informed of this access to use the proper circuits for the call type (data).
  - **No Prefix** (GNP)— The number does not include any prefix digits.
- **NOA (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. Possible values are:
  - **Unknown** — The NOA is Unknown.
  - **Subscriber** — The DN is an E.164 subscriber number that does not include the country code or area code.
  - **National** — The DN is an E.164 national number that includes the area code, but does not include the country code.
  - **International** — The DN is an E.164 international number that includes both the country code and the area code.
  - **PNP Level 0** — The number is PNP Level 0 (subscriber) number. The L0 is mapped by UCE to QSIG TON/NPI of subscriber number, private numbering plan.
  - **PNP Level 1** — PNP L1: The number is PNP Level 1 (national) number. The L1 is mapped by UCE to QSIG TON/NPI of national number, private numbering plan.
  - **PNP Level 2** — The number is PNP Level 2 (international) number. The L2 is mapped by UCE to QSIG TON/NPI of international number, private numbering plan.
  - **PNP Extension** — The number is an extension number in Private Numbering Plan. The Prefix Type E.164 Prefix Extension, along with DN Minimum Length and DN Maximum Length should determine the extension number.

Table 48: Overview Nature Of Address

Nature of Address	Numbering Plan Indicator	Type of Number
Unknown	Unknown	Unknown
Subscriber	E.164	Subscriber
National	E.164	National
International	E.164	International
PNP Level 0	PNP	L0
PNP Level 1	PNP	L1
PNP Level 2	PNP	L2
PNP Extension	PNP	Abbreviated

The purpose of the Prefix Access Code table is to find a matching rule for any dialed implicit number (unknown NOA). The matching rule either delivers a NOA which is not unknown and/or delivers a new destination. The prefix access code table also allows modification of the dialed string. This modification consists of removing leading digits and pretending new digits.

- **Destination Type:** The Destination with which to associate the Prefix Access Code. The Destination Type indicates how to route the call. Supported destination types are:
  - **None** — destination cannot be determined yet. The results from the prefix access code translation are passed to the destination table of this numbering plan. None means the resulting digits will be processed in the user's numbering plan's destination codes table.
  - **Destination** — The 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.
  - **BG Common Destination** — 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.
  - **Service** — The output goes to a "service destination" which is one of the predefined system features (like call forward activation).
  - **E.164 Destination** — The destination is determined by translation in the E164 numbering plan. The NOA must be **Unknown** and the digits to be translated in the E164 numbering plan should comply with the E164 plan. The output of translation is fed to the E.164 translation tables defined via Global Numbering Plan section of OpenScape Voice Assistant
  - **Invalid Code** — Points to an invalid dialed number. Only available for prefixType **Attendant**.
  - **Local Toll** — When an unknown member is converted to a subscriber number by the prefix access codes table, it may be presented to a local toll table that will attempt to normalize the number to a GNF number (including the +) based on the information in the local toll table.

    NOTICE:

    The NOA must be set to **Subscriber**.

- **Destination Name:** The digit position at which to continue further digit translation of the dialed number. A list of Destination Names/Services/ Announcements is shown.
  - If destination type is **Destination**, the destination name must point to a generic destination created in the system. The call is routed using the routes assigned to the destination.
  - If destination type is **Service**, the destination name must point to pre-defined service name. Internally XLA stores the values as Undefined or the service Id. The digits are translated by XLA into service Id and return to calling component which starts the service if the calling party is allowed to invoke the service.
  - If destination type is **Invalid Code**, the destination name can be UNDEFINED or point to a intercept in the intercept table. The call is sent to the intercept treatment

Dependencies between Prefix Type, NOA and Destination Type on PNP/ CNP Level:

Values for **NOA** and **Destination Type** selectable from the drop-down lists depend on the Prefix Type selection as follows:

Table 49: Some prefix types implicitly determine the destination type. Others need an explicit destination. The following table clarifies this (PNP/ CNP):

Prefix Type	Nature of Address	Destination Type / Destination	Next table
Vertical Service	Unknown	Service	Specific Service
Speed Calling	Unknown	Service	Speed Calling Service
Invalid Code	Unknown	Invalid Code	Announcement
Extension Dialing	Unknown	None	Destination Codes (this PNP
		CNP	Prefix Access Code (CNP)
		GNP	Prefix Access Code (GNP)
	PNP Extension	None	Destination Codes (this PNP)
		CNP	Prefix Access Code (CNP)
Attendant	Unknown	None	Destination Codes (this PNP)
		CNP	Prefix Access Code (CNP)
		GNP	Prefix Access Code (GNP)
	Subscriber	None	Destination Codes (this PNP
		CNP	Prefix Access Code (CNP)
	National	None	Destination Codes (this PNP)
		CNP	Prefix Access Code (CNP)
	International	None	Destination Codes (this PNP)
		CNP	Prefix Access Code (CNP)
On-net Accesss	Unknown	None	Destination Codes (this PNP)
		CNP	Prefix Access Code (CNP)
		GNP	Prefix Access Code (GNP)
	Subscriber	None	Destination Codes (this PNP)
		CNP	Prefix Access Code (CNP)
		GNP	Prefix Access Code (GNP)
	National	None	Destination Codes (this PNP
		CNP	Prefix Access Code (CNP)
		GNP	Prefix Access Code (GNP)
	International	None	Destination Codes (this PNP
		CNP	Prefix Access Code (CNP)
		GNP	Prefix Access Code (GNP)
	PNP Level 0	None	Destination Codes (this PNP
		CNP	Prefix Access Code (CNP)

Prefix Type	Nature of Address	Destination Type / Destination	Next table
	PNP Level 1	None	Prefix Access Code (GNP)
		CNP	Destination Codes (this PNP
	PNP Level 2	None	Prefix Access Code (CNP)
		CNP	Prefix Access Code (GNP)
Off-net Access	Unknown	None	Destination Codes (this PNP)
		CNP	Prefix Access Code (CNP)
		GNP	Prefix Access Code (GNP)
	Subscriber	None	Destination Codes (this PNP)
		CNP	Prefix Access Code (CNP)
		GNP	Prefix Access Code (GNP)
	National	None	Destination Codes (this PNP)
		CNP	Prefix Access Code (CNP)
		GNP	Prefix Access Code (GNP)
	International	None	Destination Codes (this PNP)
		CNP	Prefix Access Code (CNP)
		GNP	Prefix Access Code (GNP)

Dependencies between Prefix Type, NOA and Destination Type on GNP Level:

Values for **NOA** and **Destination Type** selectable from the drop-down lists depend on the Prefix Type selection as follows:

Table 50: The following table displays the allowed combinations (GNP):

Prefix Type	Nature of Address	Destination Type / Destination	Next table
Vertical Service	Unknown	Service	Specific Service
Speed Calling	Unknown	Service	Speed Calling Service
Invalid Code	Unknown	Invalid Code	Announcement
No Prefix	Unknown	None	Destination Codes (GNP) a.k.a. E164 Codes
	Subscriber		
	National		
	International		

Available Services for Prefix Type "Vertical Service" (PNP/CNP/GNP):

Table 51: Definition and Description of Services listed in Service List dialog

Displayed Service Name	Full Destination Name	Service Type[8]	Description
Account Code	Account Code Entry	B	The Account Codes for Business Groups feature allows the subscriber to add an account code to the CDR (Call Detail Record) of a call in order to separate telecommunications charges.
ACR Activate	Activate Anonymous Caller Rejection	B	Activate the ACR (Anonymous Call Rejection) which is a CLASS feature that allows subscribers to reject calls from parties who have a privacy feature active (such as Caller ID Blocking) that prevents the delivery of their calling number to the called party.
ACR Deactivate	Deactivate Anonymous Caller Rejection	B	Deactivate the Anonymous Call Rejection (ACR) service.
Alternative Calling Identity	Activate Alternative Calling Identity	B	The Alternative Calling Identity allows a subscriber to select the index of an administrator-defined alternative calling party identity list. The alternative calling party identity contains at least a number in GNF format (public number) and may also contain an alternative name. The alternative calling identity is activated on a per call basis.
Authorization Code	Pre-Dial Authorization Code	B	An authorization code is a sequence of digits dialed by a subscriber when placing a call in order for a call of a certain traffic type(s) not to be blocked. When used, an authorization code does not imply a location; it is simply used to allow a call.
Call Pickup Directed	Directed Call Pickup	B	With the Directed Call Pickup feature, a subscriber can answer (i.e., pickup) any ringing, manually held or camped-on station within their Business Group (BG). This includes calls that originated either internal to the BG or external to the BG.
Call Pickup Orig	Group Call Pickup	B	The Group Call Pickup service allows a subscriber to answer any other ringing line in the same Call Pickup (CPU) group. Call Pickup groups are created by the Business Group (BG) administrator. Every BG can be configured for its own CPU feature access code.
Call Privacy Toggle	Toggle keyset call privacy setting	B	With this feature user can press a feature key on the keyset phone to toggle the call privacy status of its prime line. When call privacy is active, OSV prevents any shared appearances of the user’s prime line from bridging into that line.

[8] Service is available :

A= Only via PNP/CNP Destination Code, GNP E.164 Code, and GNP Home DN

B= Only via PNP/CNP/GNP PAC vertical service and GNP Home DN (not via Destination Code or GNP E.164 Code)

Displayed Service Name	Full Destination Name	Service Type[8]	Description
Callback Activate	Activate Call Completion Service (CCBS or CCNR)	B	CCBS or CCNR allows a subscriber to perform an activation procedure to start the monitoring of a called party that is busy or not answering. The subscriber will be notified by a special alerting pattern when the destination device becomes available.
Callback Deactivate	Deactivate Call Completion Service (CCBS or CCNR)	B	Deactivate Call Completion Service
CFB Activate	Activate Call Forwarding Busy	B	Activate the Call Forwarding Busy Line (CFBL) which allows a station user to forward a call to another station if their phone (the base station) is in use.
CFB Deactivate	Deactivate Call Forwarding Busy	B	Deactivate the Call Forwarding Busy Line (CFBL) service.
CFNR Activate	Activate Call Forwarding No Reply	B	Call Forwarding - Do Not Answer (CFDA) (or Call Forwarding No Reply (CFNR)) allows a subscriber to forward a call to another number if an incoming call is not answered in a certain number of seconds. The forward-to number is selected at the time of activation.
CFNR Deactivate	Deactivate Call Forwarding No Reply	B	Deactivate Call Forwarding No Reply
CFU Activate	Activate Call Forwarding Unconditional	B	Call Forwarding Unconditional (CFU) (or Call Forwarding - All (CF-ALL) or Call Forwarding Variable (CFV)) is a call forwarding variant which provides the capability to forward all calls intended for the subscriber’s DN to another DN. The subscriber cannot receive and answer calls while CFU is active, but can originate calls.
CFU Deactivate	Deactivate Call Forwarding Unconditional	B	Deactivate CFU
CFVM Activate	Activate Call Forwarding Voice Mail	B	Call Forwarding - Voice Mail (CFVM) allows a station user to forward their calls to Voice Mail whenever their phone does not answer (similar to CFDA), when their phone is busy (similar to CFBL), when call is rejected by the User or by Do Not Disturb status.

[8] Service is available :

A= Only via PNP/CNP Destination Code, GNP E.164 Code, and GNP Home DN

B= Only via PNP/CNP/GNP PAC vertical service and GNP Home DN (not via Destination Code or GNP E.164 Code)

Displayed Service Name	Full Destination Name	Service Type[8]	Description
CFVM Deactivate	Deactivate Call Forwarding Voice Mail	B	Deactivate Call Forwarding to Voicemail
CFW Override	Call forwarding override	B	Call Forwarding Override (CFO) feature allows an OSV subscriber to dial a Prefix Access Code + DN in order to reach a called party, and meanwhile bypass all call forwarding features configured for that called party. The usage of CFO is limited to users that belong to the same Business Group
CID Delivery	Caller Identity Delivery Per Call	B	The Calling Identity Delivery (CID) feature allows subscribers to deliver their calling identity parameters (name and number).
CID Suppression	Caller Identity Suppression Per Call	B	The Calling Identity Suppression (CID) feature allows subscribers to suppress their calling identity parameters (name and number).
CMB	Connect to Mailbox	B	The Connect to Mailbox (CMB) service allows the user to dial a prefix access code followed by a mailbox number. It is not assignable to a subscriber or a feature profile, it can be invoked by any subscriber using the PAC.
Conf Delete Last Party	Station Controlled Conference - Delete Last Participant	B	Allows the deletion of the last participant added to the conference. The previous name of this vertical service was "DelLastConferee"
Conference Factory	Station Controlled Conference Factory Number	B	A Large Conference refers to an ad-hoc formed Station Controlled Conference (SCC). SCC allows the user to establish a conference call involving up to 48 conferees (including the user). the "Conference Factory" vertical service must be configured with the Conference Factory URI number. This is the URI that will be sent by the SIP phones for setting up the conference calls. previous name of this vertical service was "ConferenceFctNr"
COSS Activate	Activate Class Of Service Switchover	B	The 'Class of Service Switchover' feature, also known as 'Alternate toll restriction' feature, is used to assign alternative class of restrictions to a designated line
COSS Deactivate	Deactivate Class Of Service Switchover	B	Deactivate Class Of Service Switchove

[8] Service is available :

A= Only via PNP/CNP Destination Code, GNP E.164 Code, and GNP Home DN

B= Only via PNP/CNP/GNP PAC vertical service and GNP Home DN (not via Destination Code or GNP E.164 Code)

Displayed Service Name	Full Destination Name	Service Type[8]	Description
DID Pool Number	DID Pool Number for Enhanced Subscriber Rerouting	B	When Enhanced Subscriber Rerouting is permitted then OpenScape Voice can create the following rerouting number based on the number of the called subscriber: Rerouting Prefix Access Code followed by the free number in the DID pool of the called subscriber’s branch office location (where the called subscriber registered from)
DN Announcement	Directory Number Announcement	B	The DN Announcement (DNA) feature announces the DN of the endpoint from which the caller/subscriber dialed the access code. For example, when using a handset with an unknown DN, this would allow a user to discover the DN for receiving calls while using that handset.
DND Activate	Activate Do Not Disturb	B	Activate the DND (Do Not Disturb) service which allows a subscriber to block all incoming calls. The subscriber can, however, make outgoing calls while the Do Not Disturb service is activated. Also allows the subscriber, who does not want to be disturbed with calls terminating to them, to have the terminating calls immediately diverted to an announcement indicating the reason for not completing the call.
DND Deactivate	Deactivate Do Not Disturb	B	The Deactivate Do Not Disturb (DACTDND) feature allows subscribers to deactivate the Do Not Disturb service, thereby allowing incoming calls to terminate to their telephones.
Executive Override	Executive Busy Override	B	Executive phone can barge-in in assistant's call
HD Activate	Activate Hot Desking Service	B	Activate Hot Desking (HD) which allows a subscriber who is a member of a Business Group with HD service to log onto and use a telephone in a remote office. The telephone in the remote office (called the remote office telephone) will have all of the same OpenScape Voice provided features and capabilities as the telephone in the subscribers office (called the home office telephone). All originating and terminating features of the subscribers home office telephone are made available on the remote office telephone. Features/capabilities that are provided by the home office telephone itself (and not by the OpenScape Voice) may not be available in the remote office telephone. The remote office telephone and the home office telephone must be hosted by the same OpenScape Voice

[8] Service is available :

A= Only via PNP/CNP Destination Code, GNP E.164 Code, and GNP Home DN

B= Only via PNP/CNP/GNP PAC vertical service and GNP Home DN (not via Destination Code or GNP E.164 Code)

Displayed Service Name	Full Destination Name	Service Type[8]	Description
HD Deactivate	Deactivate Hot Desking Service	B	Deactivate the Hot Desking (HD) service.
Intercom 1-Way	1-Way Intercom Call (Speaker Call)	B	One-way Intercom feature provides an authorized originating party the capability to initiate an Intercom Call automatically with a 1-way connection (send path only from the originator) to a local destination, another OpenScape Voice or a destination located over SIP-Q.
Intercom 2-Way	2-Way Intercom Call (Speaker Call)	B	Two-way Intercom feature has similar functionality and activation logic as the One-way Intercom, with the added capability of bidirectional communication (with both send and receive paths) automatically using the speaker and microphone facilities at the destination.
LINR	Last Incoming Call Number Redial	B	The ETSI LINR feature allows a subscriber to place a call to the number that was last stored in the incoming memory slot. If the action is denied, a negative acknowledgment is sent to the subscriber trying to use the service. Otherwise, the call is placed and continues as a normal call.
LONR	Last Outgoing Call Number Redial	B	The ETSI LONR feature allows a subscriber to place a call to the number that was last stored in the outgoing memory slot. If the action is denied, a negative acknowledgment is sent to the subscriber trying to use the service. Otherwise, the call is placed and continues as a normal call.
Make Busy Activate	Activate MLHG Make Busy	B	The Hunt Make Busy feature permits a station to appear busy to incoming calls that hunt to the line. Calls to a line's non-hunt DN are still allowed, as are call originations The activation of this feature is either via an access code or a key assignment on the SIP (Session Initiation Protocol) phone.
Make Busy Deactivate	Deactivate MLHGT Make Busy	B	Deactivate the Make Busy service.
Make Busy Toggle	Toggle MLHG Terminal Make Busy	B	Each MLHG line can optionally have a Hunt Make Busy capability. Hunt Make Busy, as used here, is the Carrier feature which causes a terminal(s) to appear busy to incoming calls that hunt to the line. Calls to their non-hunt DN are still allowed, as are call originations. Hunt Make Busy will be available via a toggle access code. Access codes can be defined for the office as a whole, along with values per Business Group.
MCT	Malicious Call Trace	B	The Customer Malicious Call Trace feature enables a user to generate a record with information of the last call received.

[8] Service is available :

A= Only via PNP/CNP Destination Code, GNP E.164 Code, and GNP Home DN

B= Only via PNP/CNP/GNP PAC vertical service and GNP Home DN (not via Destination Code or GNP E.164 Code)

Displayed Service Name	Full Destination Name	Service Type[8]	Description
Network Feature	Network Feature Activation over SIP-Q	B	Used for Network Call Pickup Groups
Night Bell CPU	Business Group Night Bell Call Pickup	B	Call Pickup (CPU) can be used for any appropriately provided station or AAP within the business group to pick-up an alerting call on a universal (centralized) night answer position.
Outgoing CID Suppression	Activate Outgoing CID Suppression	B	Forces the presentation status for both name and number to “Restricted” for all subsequent calls. The called party’s line receives a Private/Anonymous indication for the calling party’s Number and Name.
Outgoing CID Suppression Deactivate	Deactivate Outgoing CID Suppression	B	Forces the presentation status for both name and number to “Allowed” for all subsequent calls. The called party’s line receives the calling party’s Number and Name.
Outgoing CID Suppression Toggle	Toggle Outgoing CID Suppression	B	Toggles the presentation status for both name and number for all subsequent calls either from currently “Allowed” to “Restricted” or vice versa from “Restricted” to “Allowed”. This access code may also be entered on a Feature Toggle Key on OpenScape Desk Phone CP.
Park Retrieve	Call Park Retrieve from Server	B	The parked call can be retrieved by dialing the "Park Retrieve" PAC from any phone (as long as the subscriber DN associated with the phone has the "Park To Server" feature assigned with that particular Parking Lot)
Park to Server	Call Park to Server	B	Call Park to Server was the PAC assigned for the "Park to Station" feature. ("Park to Station" feature should not be used as a vertical service. "Park to Station" feature is not supported in the current version.)
PIN Edit	Edit Personal Identification Number	B	The PIN (Personal Identification Number) service is used to create, modify or delete the PIN used by various services including HD.
SCA SLE	Screening List Editing Selective Call Acceptance	B	Screening List Editing allows screening list feature customers to be able to maintain their screening list features. The Selective Call Acceptance (SCA) feature allows a subscriber to build a list of numbers (screening list) from which the subscriber wants to accept incoming calls.
SCF SLE	Selective Call Forwarding Screening List Editing	B	The Selective Call Forwarding (SCF) feature allows a subscriber to build a list of numbers (screening list) that they would like to have call forwarded.

[8] Service is available :

A= Only via PNP/CNP Destination Code, GNP E.164 Code, and GNP Home DN

B= Only via PNP/CNP/GNP PAC vertical service and GNP Home DN (not via Destination Code or GNP E.164 Code)

Displayed Service Name	Full Destination Name	Service Type[8]	Description
SCR SLE	Selective Caller Rejection Screening List Editing	B	Edit the Screening List that contains up to 32 numbers (each up to 15 digits in length). These are the numbers which will be rejected. These numbers can be extensions if the subscriber is within a BG . Additionally in the ETSI market, these can be partial numbers, where the beginning part of the number is compared. Associated with each DN is a presentation status for it, specifying public or private.
Serial Ringing SLE	Serial Ringing - Screening List Editing	B	Screening List Editing allows screening list feature customers to be able to maintain their screening list features. The Serial Ringing (SR) feature enables the user (caller), through call redirection, to receive a call at different DNs (Directory Numbers) when the initially dialed DN is busy or does not answer. Serial Ringing provides a list of up to six DNs to be called sequentially when the subscriber is busy or doesn’t answer. A call is set up to each number from the list one at a time for the defined number of rings associated with each list entry. If a number on the list is busy, that number is skipped and the next number on the list is used. The caller has the option of receiving an indication that a serial ringing attempt is taking place. Another option allows the caller to redirect the call to the voice mail of the dialed subscriber.
SILM Barge-in	Silent Monitoring - Barge-in	B	Supervisor can barge-in in monitored subscriber's call
SILM Monitor	Silent Monitoring Monitor	B	Supervisor can silently monitor the subscriber's call
Speed Dial Ind. 1 Edit	Edit One-Digit Individual Speed Dialing List	B	In the One-Digit Speed Dialing List the subscriber can have 8 frequently called numbers, which are referenced by the speed dialing codes 2 through 9
Speed Dial Ind. 2 Edit	Edit Two-Digit Individual Speed Dialing List	B	In the Two-Digit Speed Dialing List the subscriber can have 30 frequently called numbers, which are referenced by the speed dialing codes 21 through 49
Speed Dial Individual	Individual Speed Dialing	B	BG System Speed Dial allows a station user to access 1 or 2 pre-defined BG lists of numbers/destinations and have those numbers/destinations dialed by the system.
Speed Dial System 1	System Speed Dialing First List	B	BG System Speed Dial 1 allows a station user to access a pre-defined BG list of numbers/destinations and have those numbers/destinations dialed by the system

[8] Service is available :

A= Only via PNP/CNP Destination Code, GNP E.164 Code, and GNP Home DN

B= Only via PNP/CNP/GNP PAC vertical service and GNP Home DN (not via Destination Code or GNP E.164 Code)

Displayed Service Name	Full Destination Name	Service Type[8]	Description
Speed Dial System 2	System Speed Dialing Second List	B	BG System Speed Dial 2 allows a station user to access a pre-defined BG list of numbers/destinations and have those numbers/destinations dialed by the system
SRS Activate	Activate Simultaneous Ringing	B	Activate Simultaneous Ringing (SRS) which allows a user to be simultaneously rung at multiple locations. The user is able to establish a Simultaneous Ringing List containing from 1-to-6 Directory Numbers (DNs). On an incoming call to a Simultaneous Ringing user's "Main" DN, the Simultaneous Ringing user's phone plus the DNs in the user's Simultaneous Ringing List are rung simultaneously if the "Main" DN is not busy. The call can be answered at the "Main" DN or any of the other DNs on the list. Upon answer, the calling party is connected to the DN that has answered the call first, and the remaining DNs are disconnected from the call.
SRS Deactivate	Deactivate Simultaneous Ringing	B	Deactivate the Simultaneous Ringing (SRS) service.
SRS Edit	Edit Simultaneous Ringing List	B	The subscriber is able to edit a Simultaneous Ringing List containing from 1-to-6 Directory Numbers (DNs).
Stop Hunt Activate	Activate MLHG Stop Hunt	B	For a given call, the Stop Hunt feature provides the ability to terminate all hunting within the group when encountered on a member of a hunt group. It is checked during the hunt before moving to the next line in the hunt sequence. Calls to a line's non-hunt DN are still allowed, as are call originations. The activation of this feature is either via an access code or a key assignment on the SIP phone.
Stop Hunt Deactivate	Deactivate MLHG Stop Hunt	B	Deactivate the Stop Hunt service.
Stop Hunt Togglet	Toggle MLHG Stop Hunt	B	Each MLHG line can optionally have a Stop Hunt capability. Stop Hunt, as used here, is the Carrier feature which terminates all hunting within the group for that call when encountered on a member of the MLHG (checked before moving to the next line in the hunt sequence). Stop Hunt will be available via a toggle access code. Access codes can be defined for the office as a whole, along with values per Business Group.

[8] Service is available :

A= Only via PNP/CNP Destination Code, GNP E.164 Code, and GNP Home DN

B= Only via PNP/CNP/GNP PAC vertical service and GNP Home DN (not via Destination Code or GNP E.164 Code)

6.1.23.1 Creating the Prefix Access Codes for PSTN Access

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.

6.1.23.2 BG NP Configuration - 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.

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.

BG NP Configuration

Table 52: Prefix Access Code Table Entries Permitting E.164 Dialing

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

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 the table below:

Table 53: Second Prefix Access Code Table Entries Permitting Extension Dialing

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

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.

Numbers with ’+’ sign in the beginning

A number received in the GNF format has '+" sign in the beginning which indicates that the number is a fully qualified E164 public number and has country code, area code as part of the DN.

The PAC table now accepts '+' sign as a valid character. This functionality has removed the need for the signaling component to handle the '+' sign via the hiQ/CSTA/GNFPrefixReplacement RTP parameter.

Below are some sample how the '+' character can be provisioned in the PAC table. Please note that the PAC table provisioning can be done to make the remaining DN as INTERNATIONAL (see first example provisioning) or as NATIONAL number (see second example in the table below).

Below are some sample how the '+' character can be provisioned in the PAC table.

Table 54: Prefix access code table

NPID	Digits	Min Digits	Max Digits to Insert	Digits to Insert	Digits to Delete	Prefix Type	Nature of address	DestType
NP Boca	+15619231	12	12		1		INTL	None
NP Boca	+1	8	12		2		NATL	None
NP Boca	+	8	30		1		INTL	None
NP Delray	+	8	30		1		INTL	BG_COMMON

The above provisioning indicates:

- Within NP_Boca, for any number received with '+15619231' as leading digit and 12 digits in length, delete one digit, set NOA to INTERNATIONAL, and then proceed to the destination_code table of NP_Boca for further translation.
- Within NP_Boca, for any number received with '+1' as leading digit and 12 digits in length, delete two digits, set NOA to NATIONAL, and then proceed to the destination_code table of NP_Boca for further translation.
- Within NP_Boca, for any number received with '+' as leading digit and 8 to 30 digits in length, delete one digits, set NOA to INTERNATIONAL, and then proceed to the destination_code table of NP_Boca for further translation.
- Within NP_Delray, for any number received with '+' as leading digit and 12 digits in length, delete one digit, set NOA to INTERNATIONAL, and then proceed to the PAC table of NP_COMMON_BG for further translation.

6.1.23.3 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 PAC (prefix access code) table controlled via OpenScape Voice Assistant. If 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 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 non

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 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 is not passed through the PAC table, and instead goes directly to the E.164 code table for routing.

By selecting “none” in the destination type field of the PAC access code table entry, 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.

6.1.24 Code Indexes

The concept of a Code Index is to provide a 2-step approach to establishing complex translations when multiple routing areas and classes of service are in use. It creates a template for destination code processing, making it easier to administer complex destination code processing scenarios where routing differs on routing areas and classes of service.

Once the code indices and its patterns are defined, they can be used as destinations for the destination codes tables (PNP/CNP/GNP).

Once created, patterns can be added to the code index. For the patterns the same rules as in Destination Codes Table apply.

Functional Sequence

The code Index is a provisioning optimization technique in which provisioning takes place in two steps:

1) In the first step, all of the routing areas and class of service combinations for a translation results are identified and routing results are assigned to each combination. This set of translation is assigned a code index name.
2) In the second step, all E164 codes that are to be routed identically are assigned to the same code index. The destination for this entry points to a code index name.

Code Index Concept

The concept of a Code Index is to provide a 2-step approach to establishing complex translations when multiple routing areas and classes of service are in use. It creates a template for destination code processing, making it easier to administer complex destination code processing scenarios where routing differs on routing areas and classes of service.

Code Index Pattern (Profile)

For each code index, multiple patterns (profiles) can be created. Each pattern must be a unique combination of routing area and class of service and leads then to a destination.

Not all destination types are supported by the code index table. The following are the supported code index pattern destination types:

- HOMEDN<Office Code>. The office code must exist in advance.
- INV<Invalid Code>
- INTCPT<Announcement>
- SVC<id>: Service / Service Id
- CODE_IDX<code index name>. The code index name must exist in advance. This shows that nesting of code indexes is allowed. Only one layer of nesting is allowed.

NOTICE:

CODE_PROC<code processing table entry name> are not supported by design

NOTICE:

Once the code indices and its patterns are defined, they can be used as destinations for the destination codes tables (PNP/CNP/GNP).

Code Index Routing Area

The Code Index comprises of a grouping of one Routing Area with one Class of Service. Its function is to reduce the number of routing entries. Code Index Destinations are applicable to both Public and Private Numbering Plans.

Up to 20 000 Code Index Destinations may be created. A single Code Index destination can support up to 10 000 Routing Area/COS combinations. Nesting of Code Indexes is possible, i.e. the definition of a Code Index may refer to another Code Index

CodeIndexName = Frank, Routing Area = 5, DestType = Code Index, Destination Name = George, NOA = Code Index

In this example, a Code Index entry is created as Code Index = Frank. The definition of Frank refers to George.

Where George

CodeIndexName = george, Routing Area = 5 , Cos= Sam, TrafficType= IntraLATA, DestType = DEST, Dest = routetochina, NOA = Code Index

Then

Code = 201, Destype=CodeIndex, CodeIndexName= Frank

When code = 201 is translated then XLA will next translate the CodeIndex = Frank and then the Code Index of George.

Only one layer of nesting shall be supported.

6.1.25 Code Processing

The OpenScape Voice Assistant provides a generic code processing functionality. The generic code processing is performed after the original called number has been translated in the E.164 code table.

Code processing involves the capability to modify the digit string and its Nature of Address. With code processing more advanced digit modification is possible than with the modification capabilities of the prefix access codes table or on the routes to SIP endpoints or ENUM operators.

Code Processing Features

The following Code Processing features are provided:

- Modify the called party number and Nature of Address (NOA).
- Retranslate/do not retranslate after code modification.
- If the initial translation provides a traffic type, then this traffic type is overwritten by a new translation.
- If flags are specified for the initial translation (e.g., National Prefix required), then screening is done prior to code processing.
- Nature of Address (NOA) may be modified by code processing.
- Routing Area and COS are applied to initial and retranslation - no changes in these for retranslation
- To prevent a "code processing loop", code processing will be stopped after 2 consecutive retranslations (3 translations in total).

Other characteristics

When the Destination Type **Code Processing** is selected then the following restrictions apply:

- If flags (e.g. National Prefix required) are specified, then the screening as specified by the flags is done prior to Code processing.
- The NOA specified for the code will be overwritten by the NOA returned by the Code Processing entity.
- The Routing Area and COS are applied to both the code and the processed code if retranslation occurs.
- If NPA is specified then it is ignored if code processing is to take place.
- If a traffic type is specified and the Code Processing specifies that a retranslation is required then the traffic type is overridden by the result of the new translation.

Code Processing with Retranslation

When it is **decided to retranslate the modified code**, the Nature of Address can be altered:

- If a Nature of Address is **Unkown**, the modified code will be processed in the prefix access codes table of the PNP (even if the code was modified in the CNP or the GNP).
- If a **kown** Nature of Address is chosen, the modified code will be processed in the destination codes table of the PNP. There is no need to enter a destination as this will be determined by the new translation.

Code Processing without Retranslation (Continuation)

When it is **decided to not re-translate the modified code** a destination type and name must be chosen. The modified code together with the chosen Nature of Address will then be handled by that destination.

Not all destination types are supported by the code processing table. The following are the supported code index pattern destination types:

- DEST<Destination Name and possibly Office Code>. The destination name and the office code must exist in advance.
- HOMEDN<Office Code>. The office code must exist in advance.
- INTCPT<Announcement>
- SVC<id>: Service / Service Id
- TIME_DEST<time destination name>.

NOTICE:

CODE_PROC<code processing table entry name> and CODE_IDX<code index name> are not supported by design

Once the code processing rules are defined, they can be used as destinations for the destination codes tables (PNP/CNP/GNP).

6.1.26 Extensions

OpenScape Voice supports dialing numbers for a subscriber that are shorter than the numbers provided by the public or the private numbering plans. These short numbers are called extensions and they must be the trailing part of either the subscriber number (public numbering plan) or the local number (private numbering plan.

An extension is defined when Nature of Address is set to PNP Extension and Destination Type is set to Home Extension in the Numbering Plan settings

PNP Extension

The number is an extension number in Private Numbering Plan. The Prefix Type E164 Prefix Extension, along with DN Minimum Length and DN Maximum Length should determine the extension number.

Length of Extensions

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.

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 OpenScape Voice switches

The form of number displayed as **caller ID** or **connected party ID** is controlled by a number of configurable options and by the **Display Number Modification** feature

6.1.27 Digit Modification for Digit Outpulsing

The digit modification for digit outpulsing feature provides support for selectively deleting any number of leading digits (up to all digits) from the destination number prefixing new leading digits to the destination number, or both. Digit modification is based on the combination of the Destination Code and the route.

Calls to different destinations that share the same route may require modifying digits differently; and calls to the same destination that are routed over different routes (as with alternate routing) may also require modifying digits differently.

6.1.28 ENUM (Electronic Number Mapping)

ENUM (Electronic Number Mapping) is a DNS-based architecture and protocol for mapping an ITU-T (International Telecommunications Union, Telecommunications Standards Section) recommendation E.164 telephone number into an URI.

A URI is a string of characters that identifies resources such as documents, images, files, databases, e-mail addresses or other resources or services in a common structured format.

The ENUM mechanism converts telephone numbers into service specific URIs.

The operator ENUM feature provides support for the DNS-based architecture and protocol for mapping an E.164-compliant number into a service-specific URI, which is dictated by IETF RFC 3761. This mechanism is only applicable for interswitch connection with SIP gateways.

OpenScape Voice uses this mechanism to route calls to other networks through IP-based means instead of through the PSTN (Public Switched Telephone Network). Up to six ENUM server pairs and at least 100 simultaneous queries are supported. Each server pair can contain a secondary server, which provides a failover mechanism if the primary server cannot process a query.

Requirements

The administrator defines the following:

- The primary ENUM server and an optional secondary server
- The default tier 0 zone, along with information about the primary ENUM server
- Whether ENUM routing is always performed, or if it is performed only to registered endpoints

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 OpenScape Voice must perform ENUM queries on all calls to non-hosted subscribers.

The query resolves the number into a sorted list of URIs.

System specific information

In this scenario, an enterprise might own three OpenScape Voice systems 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 OpenScape Voice system, 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 one of their other OpenScape Voice systems — or if it has to be delivered to the PSTN.

If the primary server does not respond to repeated ENUM queries, all subsequent queries are sent to the secondary server until the primary server becomes available again. Alarming is provided when an ENUM server is not responding to queries, and when a complete ENUM server pair is not responding.

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 100 milliseconds. Longer response times can result in call setup delay and lost calls. The designer should also define the OpenScape Voice routing database in a way that ensures that outbound calls can continue to be routed if an ENUM server fails.

The following is an example of a simple SIP call flow that includes an ENUM query:

1) User A dials user B, who is not located on the same OpenScape Voice system hosting user A.
2) OpenScape Voice launches a query to the ENUM server to determine how to route the call to user B.
3) The ENUM server returns the Naming Authority Pointer (NAPTR) record(s) that contains the routing to user B. If the server cannot return the applicable NAPTR record, it can return an indication that vacant code treatment is to be provided.
4) OpenScape Voice determines that it can route the call on-net (and therefore does not need to go into the PSTN), and sends an INVITE request to the proxy for user B.

5) The far-end switch (most likely another OpenScape Voice system) presents the call to user B.

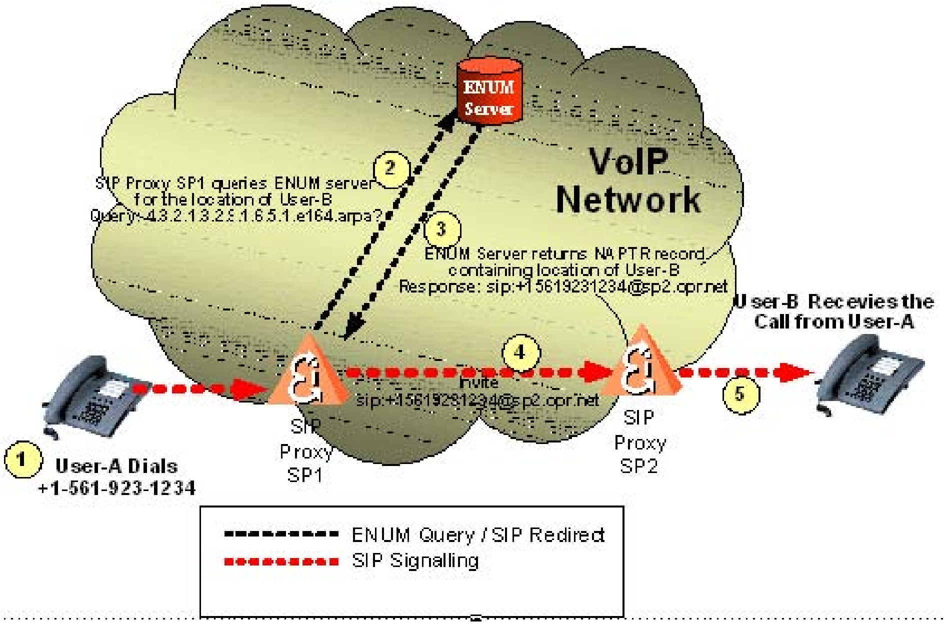

ENUM Server
VoIP Network
2
SIP Proxy SP1 queries ENUM server for the location of User-B
Query: 4.3.2.1.3.2.9.1.6.5.1.e164.arpa?
3
ENUM Server returns NAPTR record containing location of User-B
Response: sip:+15619231234@sp2.cpr.net
User-B Recevies the Call from User-A
4
Invite sip:+15619231234@sp2.cpr.net
5
1
User-A Dials +1-561-923-1234
SIP Proxy SP1
SIP Proxy SP2
ENUM Query / SIP Redirect
SIP Signalling

Figure 57: Simple SIP Call Flow with ENUM Query

6.1.29 Operator ENUM (Electronic Number Mapping) Server

The Operator ENUM Server feature allows up to six ENUM (Electronic Number Mapping) servers to be configured, to list all provisioned ENUM servers, and to create and modify ENUM servers.

6.1.30 ENUM (Electronic Number Mapping) Operator

This feature allows the subscriber to list all provisioned ENUM (Electronic Number Mapping) operators as well as to create and modify ENUM Operators.

6.1.31 Voice VPN

OpenScape Voice, as a VoIP switching system, can be used to create a virtual voice network (a voice VPN) on top of the enterprise’s existing data network topology for connecting subscribers within the enterprise, even if these subscribers are in different locations.

In addition to subscribers directly registered on the OpenScape Voice system, this voice VPN can also include subscribers on traditional PBX (Private Branch eXchange) which are connected to the OpenScape Voice system through a gateway.

OpenScape Voice’s sophisticated dialed number processing permits the administrator to create a PNP (Private Numbering Plan) which can include all subscribers in the VPN. OpenScape Voice can serve as a tandem switch/ routing engine in the VPN, connecting parties on the various PBXs, while at the same time serving directly registered endpoints.

6.1.32 Intercepts

Intercepts are **sequences of up to three treatments** (for example, tones and/ or announcements) OpenScape Voice and its media servers repeat a specified number of times.

The subscriber defines the properties of each treatment, such as a tone's duration or whether an announcement is "barge-in" or "non-barge-in." Once OpenScape Voice and its media servers have finished playing an intercept's treatments as configured in the intercept, OpenScape Voice returns the calling party line to idle, except in the case of calls from analog lines. An Intercept can contain up to three Treatments.

OpenScape Voice provides a series of system pre-defined intercepts. You cannot delete these intercepts, but you can modify the cycle and interval for a system pre-defined Intercept if the subscriber has assigned treatments.

In addition, you can create, edit, and delete user-defined intercepts.

The subscriber can assign treatments to and unassign treatments from intercepts, as well as editing the properties of these treatments and changing the order in which OpenScape Voice requests the treatments within the intercept.

Names that appear in the intercept name list are color coded to indicate their default status and whether they have treatments assigned.

Table 55: Color Coding for Intercepts, Intercepts list view

Color	Description
Red	This intercept: • is a default intercept • does not have a treatment assigned to it You should assign at least one treatment to the intercept.
Green	This intercept: • is a default intercept • has at least one treatment assigned to it Green intercepts can be used by other objects, such as Call Gapping Controls and Trunk Group Controls..
Blue	This intercept: • is using a default intercept or • has at least one treatment assigned to i Blue intercepts can be used by other objects, such as Call Gapping Controls and Trunk Group Controls.

Color	Description
Black	This intercept: • is not using a default intercept • does not have a treatment assigned to it

6.1.32.1 Treatments

OpenScape Voice uses media servers to generate tones and announcements indicating various failure or other conditions the calling party may encounter on a dialed call. These tones and announcements, collectively named treatments, provide explanatory information when a call fails to complete as dialed.

6.1.33 Determine if a call is Internal or External

The internal/external determination logic for a call between 2 parties is determined from analyzing the several factors about the incoming and outgoing side of a call and then aggregating the result for each side.

Factors that determine if a Call is Internal or External

- BG Membership of calling and called side. (If they are members of the same BG)
- RTP parameter `Srx/Main/HandleInterBGCallsAsInternal` [9](Default value is RtpFalse).
- **Public/OffNet Traffic** endpoint attribute enabled on the endpoint of either calling or called side. (Default value is disabled).
- Class-marks received from an originating Private Networking (SIP or SIP-Q) endpoint
- Class-marks received from a terminating Private Networking (SIP or SIP-Q) endpoint
- The BG of the calling or called endpoint is marked as **Trusted**

Call Determination of Outgoing side (Originating)

- If the call originates from a SIP endpoint that has the **Public/OffNet Traffic** attribute set, the originating side's call state shall be: **External**.
- Else, if the call originates from a SIP Private Networking endpoint and the INVITE request contains the X-Siemens-Call-Type with value Org-NWid-external-public, the originating side's call state shall be: **External**.
- Else, if the call originates from a SIP-Q Private Networking endpoint and the SETUP message contains the Classmarks Originating/Terminating Network Identification (octet 6) with value 1 (Public Telephone Network), the originating side's call state shall be: **External**.
- Else, if the RTP parameter `Srx/Main/HandleInterBGCallsAsInternal` is set to RtpTrue, the originating side's call state shall be: **Internal**.

[9] Navigate to **Configuration** > **OpenScape Voice** > **Administration** > **General Settings** > **RTP**

- Otherwise, the originating side’s call state is set to: **Based_on_BG**.

NOTICE:

Based_on_BG indicates that the BG membership will determine if it is an Internal or External call.

Call Determination of Incoming side (Terminating)

- If the call terminates on a SIP endpoint that has the **Public/OffNet Traffic** attribute set, the terminating side’s call state shall be: **External**.
- Else, if the RTP parameter `Srx/Main/HandleInterBGCallsAsInternal` is set to RtpTrue, the originating side’s call state shall be: **Internal**.
- Otherwise, the originating side’s call state is set to: **Based_on_BG**.

NOTICE:

Based_on_BG indicates that the BG membership will determine if it is an Internal or External call.

Aggregation of Incoming and Outgoing side’s call state

The following table contains the aggregation of the originating and terminating side’s call states:

		Outgoing External	**Outgoing Internal**	**Outgoing Based on BG**	
				BGX	**BGY**
Incoming External		External	External	External	External
Incoming Internal		External	Internal	Internal	Internal
Incoming Based on BG	BGX	External	Internal	Internal[10]	(*)
	BGY	External	Internal	(*)[11]	Internal[12]

On a private network call, the originating switch can only make an assumption on the nature of the outgoing call in case it is determined Internal based on above criteria.

The terminating switch may correct the originating switch’s determination of the call type by returning the following Classmarks (SIP-Q) or X-Siemens-Call-Type in the backward direction:

- A Classmarks Originating/Terminating Network Identification (octet 6) with value 1 (Public Telephone Network) received in a SIP-Q message from the terminating switch, shall modify an outgoing side’s call state from **Internal** to **External**.

[10] If both parties are in the same BG (BGX or BGY) the call is determined as internal

[11] (*) If either BGX or BGY are marked as **Trusted** , the aggregated call state is Internal, otherwise the state is External

[12] If both parties are in the same BG (BGX or BGY) the call is determined as internal

- An *X-Siemens-Call-Type* header with value *Org-NWid-external-public* received in a SIP message from the terminating switch shall modify an outgoing side’s call state from **Internal** to **External**.

6.2 Routing and Translation

Routing and translation features provide such capabilities as Public Numbering Plan compliance and routing that varies depending upon such factors as origin, traffic, and time of day.

OpenScape Voice Subscriber Management Configuration

Most of the configuration tasks for subscriber management are accomplished using the Assistant (e.g., configuring BGs (Business Groups), user information and status, connection types, SIP phones, etc.) However, a few tasks in this group can be done using the CLI (Command Line Interface). Mainly, though, the CLI can be used to display these settings once they have been configured.

6.2.1 Common Routing Concept - Mandatory Call Routing Rules

Routing decisions always start on the PNP level and may pass further decisions to the GNP which is common to all BGs. The GNP has a predefined name: E164 NANP (which means E.164 North American Numbering Plan, but is not restricted to US numbering schemes).

Using Business Groups

Use one business group per customer, because of feature restrictions (group features, name displays, callback...) between business groups. Multiple BGs should only be used in case of a hosted scenario, where independent customers are hosted at the same OSV system.

A second BG has to be used for native SIP gateways (does not apply to SIPQ gateways) in case a distinction between internal and external calls (calls from the PSTN) has to be realized. A new endpoint attribute has been introduced (Public/Off-net Traffic) that provides the same effect like the "external BG" in previous versions for incoming and outgoing PSTN calls from this endpoint. This attribute obsoletes the need for an "external" BG.

In case a native SIP gateway is connected to a PBX, where internal and external calls are received, a decision has to be made depending on the requirements from the customer, if the gateway has to be treated as internal or external gateway.

Independent of which number format is used between OSV and gateways, only normalized numbers have to configured within the destination code table, so that the OSV knows what it is dealing with.

The official way to implement call restrictions is via the Toll and Call Restriction Service (based on traffic types).

Independent of which number format is used between OSV and gateways, only normalized numbers have to configured within the destination code table, so that the OSV knows what it is dealing with. Current "best practice", in case the display number modification feature from the OSV is used, is to send calling and called party in international for-mat from the OSV to gateways and vice versa. If the called party can not be send as international, it can be customized at the route of the destination object. The calling party can be adjusted with the display number modification feature for native SIP if needed. However, for incoming calls it is recommended to adjust the calling party information in the native SIP gateway so it is also in effect for survivability mode.

Provisioning of the ’+’ sign

- When a native SIP gateway sends a "+" sign (NOA = International) in front of the called party in the SIP request line of an incoming invite, the OSV checks first the PAC table for call routing translations.
- When a SIPQ gateway sends the called party within a incoming setup message in a explicit format (Nature Of Address defined) the OSV will skip the PAC table for call routing translations.

  In this case, translation of the called party will start directly within the destination code table of the numbering plan assigned to the gateway.

Using Numbering Plans

The Private Numbering plan (aka PNP) is used to set up routing rules that are local to the subscriber.

The Global Numbering Plan (aka GNP) is used to set up routing rules that are common to all business groups.

6.2.2 Common Routing Concept - Open Numbering

In an Open Numbering scenario the subscribers are configured with full E.164 numbers. These E.164 numbers are unique for the complete switch, but the **extensions are not unique!**

A site individual Crosssite prefix is dialed to reach subscribers at other locations. Within the same branch/location subscribers can reach each other by dialing the extension or site prefix + extension

Each location has a local GW for the breakout to the PSTN. Gateway from location 1 is also used for calls to the existing PBX network of the customer

3 different call permission classes, for local, national and international calls. Subscribers are provisioned with corresponding Rate/Routing Area and Toll and Call Restrictions Service (or Class of Service).

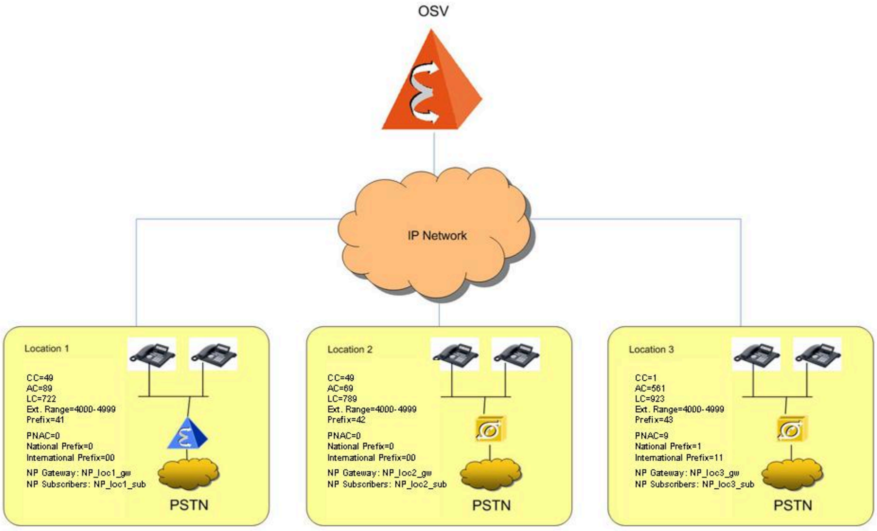


Figure 58: Open Numbering

Subscriber Calls

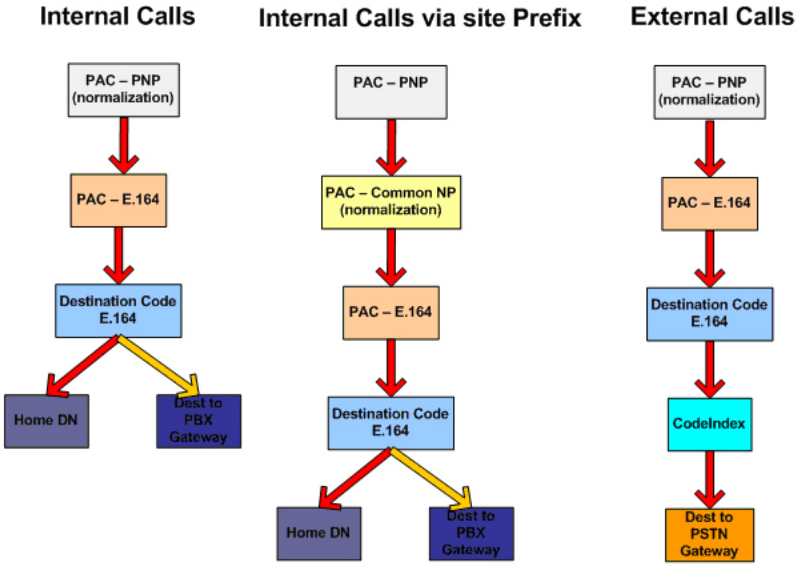


Figure 59: Open Numbering - Subscriber Calls

Configuration and Provisioning of PNP PAC table

The PAC table of the PNP is used to match the dialed number, normalize it and send it up to the GNP.

For hosted scenarios the CNP can be used instead of GNP, depending on the customer requirements.

The crosssite prefixes (41,42,43 - all with min length 6 and max length 6) for dialing between sites can be summarized for the given example with one PAC entry pointing to the common numbering plan, where the BG common normalization is done (to reduce configuration effort).

Table 56: PAC table for location1 (location2 is configured similar (US)

PAC for Calls within same locations (NP_loc1_sub)							
Digits	min Length	max Length	Digit Position	Digits to insert	Prefix Type	NOA	Dest. Type
4	4	4	0	4989722	Extension Dialing	International	E164 Destination
PACs for Calls between locations (NP_loc1_sub)							
Digits	min Length	max Length	Digit Position	Digits to insert	Prefix Type	NOA	Dest. Type
4	6	6	0		Extension Dialing	Unknown	BG Common Destination
PACs for calls to the PSTN (NP_loc1_sub)							
Digits	min Length	max Length	Digit Position	Digits to insert	Prefix Type	NOA	Dest. Type

Table 57: PAC table for location3 (US)

PAC for Calls within same locations (NP_loc3_sub)							
Digits	min Length	max Length	Digit Position	Digits to insert	Prefix Type	NOA	Dest. Type
4	4	4	0	1561923	Extension Dialing	International	E164 Destination
PACs for Calls between locations:							
Digits	min Length	max Length	Digit Position	Digits to insert	Prefix Type	NOA	Dest. Type
4	6	6	0		Extension Dialing	Unknown	BG Common Destination
PACs for calls to the PSTN:							
Digits	min Length	max Length	Digit Position	Digits to insert	Prefix Type	NOA	Dest. Type
9	8	8	1	1561	Off-net Access	International	E164 Destination
9	11	11	1	1	Off-net Access	International	E164 Destination
91	12	12	1		Off-net Access	International	E164 Destination
9011	5	21	4				

Configuration and Provisioning of CNP PAC table

PAC table of the CNP (Common Numbering Plan) is used for the common normalization of the cross site prefixes. After the number has been normalized it is sent up to the Global Numbering Plan.

Table 58: PACs for calls between locations (location dialing)

Digits	min Length	max Length	Digit Positic	Digits to insert	Prefix Type	NOA	Dest. Type
41	6	6	2	4989722	Extension Dialing	International	E164 Destination
42	6	6	2	4969789	Extension Dialing	International	E164 Destination
43	6	6	2	1561923	Extension Dialing	International	E164 Destination

Configuration and Provisioning of GNP PAC table

The GNP PAC table includes PACs from 1 to 9 with min length 1 digit and max length 21 digits. This configuration will match all numbers for the complete world, because the called party is sent normalized from the Private Numbering Plan to the Global Numbering Plan.

Table 59: GNP PAC table

Digits	min Length	max Length	Digit Position	Digits to insert	Prefix Type	NOA	Dest. Type
1	1	21	0		No Prefix	International	None
2	1	21	0		No Prefix	International	None
3	1	21	0		No Prefix	International	None
4	1	21	0		No Prefix	International	None
5	1	21	0		No Prefix	International	None
6	1	21	0		No Prefix	International	None
7	1	21	0		No Prefix	International	None
8	1	21	0		No Prefix	International	None
9	1	21	0		No Prefix	International	None

Configuration and Provisioning of GNP DC table:

> Internal Calls

- For the office codes of location 2 and 3 are 2 destination codes configured with the office code + the 1 digit of the extension range to match only the assigned extension range. Both Destination Codes are pointing to the corresponding HomeDN.
- One and the same destination code can be used to point to the HomeDN and optional to a destination. This configuration is very helpful in case of a migration scenario. The OSV checks first if a HomeDN is available for the called party, if not, the call will be routed following the configuration of the destination. In our example this kind of configuration is used for internal calls to OSV and PBX subscribers located at location1.

Table 60: Destination Codes for internal calls (Global Numbering Plan)

Digits	NOA	Traffic Type	Class of Service	Routing Area	Dest. Type	Dest. Name/ Office Code	DN Office Code
1	International	None			Destination	Dest_gwloc1	4989722
2	International	None			Home DN	4969789	
3	International	None			Home DN	1561923	

> External Calls

In the U.S. typically the destination for international calls will need to have routes that insert the 011 back into the prefix before sending to the PSTN. However, some US carriers do not want this prefix, but want the TON set to International.

In either case different destinations should be designated for each US location for each of international, toll, or local calls so proper digit manipulation can be sent towards the PSTN for US locations (may also be needed in Europe depending on the gateway configuration or SIP carrier requirements)

Dest_gwloc3_int will be used in our example for international calls, while Dest_gwloc3_nat will be used for national calls and Dest_gwloc3_loc for local calls.

For U.S. locations it might be necessary to create many Destination codes/ Code Indexes for external local calls. This is because locations can have multiple area codes plus multiple office codes that split between requiring the formats1NPA-NXX-XXXX and NPA-Nxx-XXXX.

> External Calls: Call routing based on traffic types and code indexes

Traffic types identify the type of call, e.g. national or international. While a COS is an originator attribute, traffic types are a destination attribute. The traffic type check is performed after the destination code has been matched, therefore no multiple destination code entries are needed, as they are if COS is used.

In this scenario, the traffic type is used to mark destination codes with the minimal permission a subscriber needs to use those routes. The needed permission is controlled via the "Toll and Call Restriction" feature configured under subscriber services. Routing areas can be assigned to a subscriber or endpoint to indicate the geographic location of that subscriber.

The Routing Area is an originator attribute. Multiple destination code entries with the same digit sequence will be needed for different locations. Code Indexes provide the capability of provisioning multiple destination codes with the same core parameters. They can be considered as a kind of destination code template, which reduces administrative effort since the template can be used for several destination codes. The usage of Code Indexes is optional.

- **Provisioning for International calls**:

  Destination codes for international calls point to a code index called CI_World. (There is no CI_World destination code listed here for 1, because this is the country code for the U.S. location)

Table 61: Destination codes for international calls point to a code index called CI_World.

Digits	NOA	Traffic Type	Class of Service	Routing Area	Dest. Type	Code Index Name
1	International	None			Code Index Destination	CI_World
2	International	None			Code Index Destination	CI_World
3	International	None			Code Index Destination	CI_World
1	International	None			Code Index Destination	CI_World
2	International	None			Code Index Destination	CI_World
3	International	None			Code Index Destination	CI_World
1	International	None			Code Index Destination	CI_World
2	International	None			Code Index Destination	CI_World
3	International	None			Code Index Destination	CI_World

The Code Index CI_World has for each location a pattern configured. The RA identifies the location of the calling party, while the traffic type marks the traffic from all 3 locations as international traffic.

Table 62: Code Index Patterns for CI_World (Global Numbering Plan)

Class of Service	Traffic Type	Routing Area	Dest. Type	Destination Name
	International	RAloc1	Destination	Dest_gwloc1
	International	RAloc2	Destination	Dest_gwloc2
	International	RAloc3	Destination	Dest_gwloc3_int

- **Provisioning for National calls:**

  A Destination code for the German Country Code points to a code index called CI_GER, while another destination code for the American Country Code points to a code index called CI_US. Those destination codes are needed to filter German and U.S. national traffic

Table 63: Destination Codes for national calls (Global Numbering Plan)

Digits	NOA	Traffic Type	Class of Ser-vice	Routing Area	Dest. Type	Code Index Name
49	International	None			Code Index Destination	CI_GER

Code Index CI_GER has for each location a pattern configured. The RA identifies the location of the calling party, while the traffic type marks traffic from the German locations 1 and 2 as national, and as international for traffic from the American location3.

Table 64: Code Index Patterns for CI_GER (Global Numbering Plan)

Class of Service	Traffic Type	Routing Area	Dest. Type	Destination Name
	National	RAloc1	Destination	Dest_gwloc1
	National	RAloc2	Destination	Dest_gwloc2
	International	RAloc3	Destination	Dest_gwloc3_int

Code Index CI_US is configured similar to CI_GER. The difference is that the traffic type marks traffic from the German locations 1 and 2 as international, and as national for traffic from the American location3. The pattern for US RAloc3 uses Dest_gwloc3_nat as destination, so that we can leave the 1NPA-NXX-XXX pattern towards the PSTN. (Or change it depending on what the Long Distance Carrier may require.)

Table 65: Code Index Patterns for CI_US (Global Numbering Plan)

Class of Service	Traffic Type	Routing Area	Dest. Type	Destination Name
	International	RAloc1	Destination	Dest_gwloc1
	International	RAloc2	Destination	Dest_gwloc2
	National	RAloc3	Destination	Dest_gwloc3_nat

- **Provisioning for Local calls:**

  3 Destination codes for the 3 locations are configured to filter local traffic. For Munich (CC49 + AC89) the destination code points to a code index called CI_Mch, for Frankfurt (CC49 + AC69) it points to a destination code called CI_Fra and for Boca to CI_Boc (CC1 + AC561).

Table 66: Destination Codes for local calls (Global Numbering Plan)

Digits	NOA	Traffic Type	Class of Service	Routing Area	Dest. Type	Code Index Name
4989	International	None			Code Index Destination	CI_Mch
4969	International	None			Code Index Destination	CI_Fra
1561	International	None				CI_Boc

Code Index CI_Mch has for each location a pattern configured. The RA identifies the location of the calling party, while the traffic type marks traffic from location1 (Munich/Germany) as local, traffic from location2 (Frankfurt/Germany) as national, and traffic from location3 (Boca/U.S.) as international.

Table 67: Code Index Patterns for CI_Mch (Global Numbering Plan)

Class of Service	Traffic Type	Routing Area	Dest. Type	Destination Name
	Local	RAloc1	Destination	Dest_gwloc1
	National	RAloc2	Destination	Dest_gwloc2
	International	RAloc3	Destination	Dest_gwloc3_int

Code Index CI_Fra is configured similar to CI_Mch. The difference is that the traffic type marks traffic from location2 (Frankfurt/Germany) as local, traffic from location1 (Munich/Germany) as national, and traffic from location3 (Boca/U.S.) as international.

Table 68: Code Index Patterns for CI_Fra (Global Numbering Plan)

Class of Service	Traffic Type	Routing Area	Dest. Type	Destination Name
	National	RAloc1	Destination	Dest_gwloc1
	Local	RAloc2	Destination	Dest_gwloc2
	International	RAloc3	Destination	Dest_gwloc3_int

Code Index CI_Boc is configured similar to CI_Mch and CI_Fra. The difference is that the traffic type marks traffic from location3 (Boca/U.S.) as local, and traffic from location1 (Munich/Germany) and 2 (Frankfurt/Germany) as international. The pattern for US RAloc3 uses Dest_gwloc3_loc as destination, so that the first 4 digits can be stripped if needed.

Table 69: Code Index Patterns for CI_Boc (Global Numbering Plan))

Class of Service	Traffic Type	Routing Area	Dest. Type	Destination Name
	International	RAloc1	Destination	Dest_gwloc1
	International	RAloc2	Destination	Dest_gwloc2
	Local	RAloc3	Destination	Dest_gwloc3_loc

> External Calls: Call routing based on class of service and code indexes

Class of Service should only be used when Traffic Types are not adequate

RA and COS are both originator attributes. Multiple Destination Codes with the same digit sequence are needed to create a call toll restriction matrix within a shared destination code table.

To reduce the configuration effort, a 2 Level Code Index concept can be used. (usage of Code Indexes is optional)

The first code index determines the calling location via the Rate/Routing Area, and points to a second Code Index. The second Code Index checks the COS

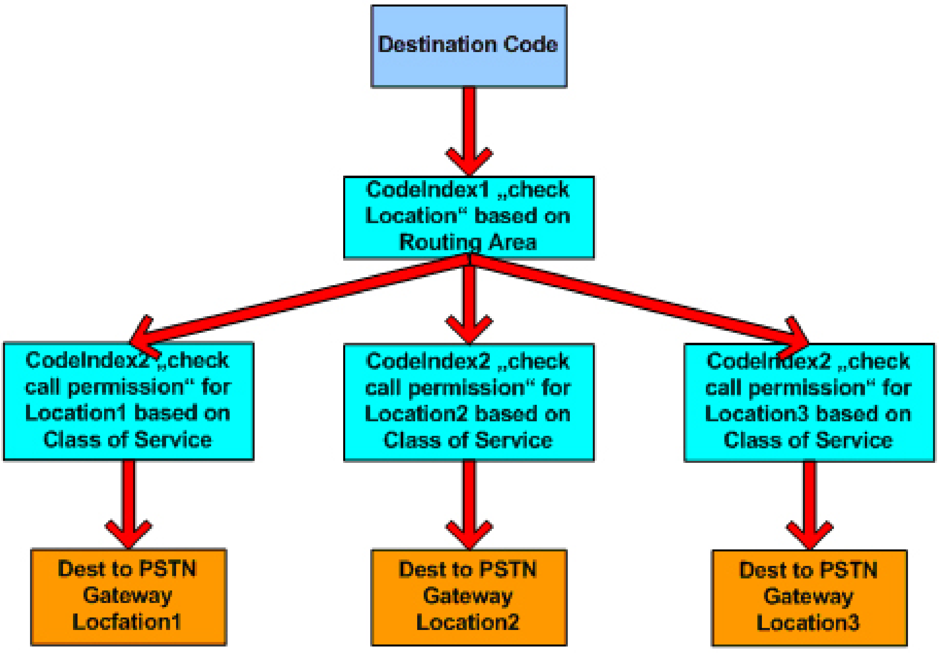

Destination Code
CodeIndex1 „check Location“ based on Routing Area
CodeIndex2 „check call permission“ for Location1 based on Class of Service
CodeIndex2 „check call permission“ for Location2 based on Class of Service
CodeIndex2 „check call permission“ for Location3 based on Class of Service
Dest to PSTN Gateway Locfation1
Dest to PSTN Gateway Location2
Dest to PSTN Gateway Location3

Figure 60: Call routing based on Class of Service and Code Indexes

For each location a code index per "toll restriction class" is configured. In this example those will be 3 code indexes for international, national and local traffic per location. The code indexes include only patterns for COS classes which are required to go forward to a valid destination. If a subscriber doesn't have a corresponding COS assigned, a default pattern is configured, which is pointing to a intercept (TRS_ON

- **Provisioning for International calls**:

  Destination codes for international calls point to a code index called CI_World. (There is no CI_World destination code for 1, because this is the country code for the U.S. location)

Table 70: Destination codes for international calls point to a code index called CI_World.

Digits	NOA	Traffic Type	Class of Service	Routing Area	Dest. Type	Code Index Name
1	International	None			Code Index Destination	CI_World
2	International	None			Code Index Destination	CI_World
3	International	None			Code Index Destination	CI_World
4	International	None			Code Index Destination	CI_World
5	International	None			Code Index Destination	CI_World
6	International	None			Code Index Destination	CI_World

Digits	NOA	Traffic Type	Class of Service	Routing Area	Dest. Type	Code Index Name
7	International	None			Code Index Destination	CI_World
8	International	None			Code Index Destination	CI_World
9	International	None			Code Index Destination	CI_World

The Code Index CI_World has for each location a pattern configured. The RA identifies the location of the calling party. The patterns point depending on the calling location information to a second code index to check the needed call restriction class.

Table 71: Code Index Patterns for CI_World (Global Numbering Plan)

Class of Service	Traffic Type	Routing Area	Dest. Type	Destination Name
CosInternat		RAloc1	Code Index	CI_Interna_loc1
CosInternat		RAloc2	Code Index	CI_Interna_loc2
CosInternat		RAloc3	Code Index	CI_Interna_loc3

CI_Interna_loc1 has a pattern configured for COSInternat pointing to the destination of the gateway from location1. Subscriber with COS COSInternat assigned will be able to use this route. Subscribers that do not have a corresponding COS class assigned will be routed via the default pattern to a intercept (TRS_ON).

Table 72: Code Index Patterns for CI_World (Global Numbering Plan)

Class of Service	Traffic Type	Routing Area	Dest. Type	Destination Name
CosInternat		RAloc1	Destination	Dest_gwloc1
		RAloc2	Intercept	TRS_ON

- **Provisioning for National calls:**

  A Destination code for the German Country Code points to a code index called CI_GER, while another destination code for the U.S. Country Code points to a code index called CI_US. Those destination codes are needed to filter German and U.S. national traffic.

Table 73: Destination Codes for national calls (Global Numbering Plan)

Digits	NOA	Traffic Type	Class of Service	Routing Area	Dest. Type	Code Index Name
49	International	None			Code Index Destination	CI_GER
1	International	None			Code Index Destination	CI_US

The Code Index CI_GER has for each location a pattern configured. The RA identifies the location of the calling party. The patterns point depending on the calling location information to a second code index to check the needed call restriction class.

Table 74: Code Index Patterns for CI_GER (Global Numbering Plan)

Class of Service	Traffic Type	Routing Area	Dest. Type	Destination Name
		RAloc1	Code Index	CI_Nat_loc1
		RAloc2	Code Index	CI_Nat_loc2
		RAloc3	Code Index	CI_Interna_loc3

CI_Nat_loc1 has patterns configured for COSInternat and COSNat pointing to the destination of the gateway from location1. Subscriber from location1 with COS COSInternat or COSNat assigned will be able to use this route. Subscribers that do not have a corresponding COS class assigned will be routed via the default pattern to a intercept (TRS_ON).

Table 75: Code Index Patterns for CI_World (Global Numbering Plan)

Class of Service	Traffic Type	Routing Area	Dest. Type	Destination Name
CosInternat		RAloc1	Destination	Dest_gwloc1
CosNat		RAloc2	Destination	Dest_gwloc1
			Intercept	TRS_ON

The Code Index CI_US has for each location a pattern configured. The RA identifies the location of the calling party. The patterns point depending on the calling location information to a second code index to check the needed call restriction class.

Table 76: Code Index Patterns for CI_GER (Global Numbering Plan)

Class of Service	Traffic Type	Routing Area	Dest. Type	Destination Name
		RAloc1	Code Index	CI_Interna_loc2
		RAloc2	Code Index	CI_Interna_loc2
		RAloc3	Code Index	CI_Nat_loc3

CI_Interna_loc1 has a pattern configured for COSInternat pointing to the destination of the gateway from location1. Subscriber with COS COSInternat assigned will be able to use this route. Subscribers that do not have a corresponding COS class assigned will be routed via the default pattern to a intercept (TRS_ON).

Table 77: Code Index Patterns for CI_World (Global Numbering Plan)

Class of Service	Traffic Type	Routing Area	Dest. Type	Destination Name
CosInternat			Destination	Dest_gwloc1
			Intercept	TRS_ON

- **Provisioning for Local calls:**

  3 Destination codes for the 3 locations are configured to filter local traffic. For Munich (CC49 + AC89) the destination code points to a code index called CI_Mch, for Frankfurt it points to a destination code called CI_Fra (CC49 + AC69) and for Boca to CI_Boc (CC1 + AC561).

Table 78: Destination Codes for local calls (Global Numbering Plan)

Digits	NOA	Traffic Type	Class of Service	Routing Area	Dest. Type	Code Index Name
4989	International	None			Code Index Destination	CI_Mch
4969	International	None			Code Index Destination	CI_Fra
1561	International	None				CI_Boc

The Code Index CI_Mch has for each location a pattern configured. The RA identifies the location of the calling party. The patterns point depending on the calling location information to a second code index to check the needed call restriction class.

Table 79: Code Index Patterns for CI_World (Global Numbering Plan)

Class of Service	Traffic Type	Routing Area	Dest. Type	Destination Name
		RAloc1	Code Index	CI_Interna_loc1
		RAloc2	Code Index	CI_Interna_loc2
		RAloc3	Code Index	CI_Interna_loc3

CI_Local_loc1 has patterns configured COSInternat, COSNat and COSLocal pointing to the destination of the gateway from location1. Subscriber from location1 with COS COSInternat or COSNat or COSLocal assigned will be able to use this route. Subscribers that do not have a corresponding COS class assigned will be routed via the default pattern to a intercept (TRS_ON).

Table 80: Code Index Patterns for CI_World (Global Numbering Plan)

Class of Service	Traffic Type	Routing Area	Dest. Type	Destination Name
CosInternat			Destination	Dest_gwloc1
CosNat			Destination	Dest_gwloc1
CosLocal			Destination	Dest_gwloc1

The Code Index CI_Fra has for each location a pattern configured. The RA identifies the location of the calling party. The patterns point depending on the calling location information to a second code index to check the needed call restriction class.

Table 81: Code Index Patterns for CI_World (Global Numbering Plan)

Class of Service	Traffic Type	Routing Area	Dest. Type	Destination Name
		RAloc1	Code Index	CI_Nat_loc1
		RAloc2	Code Index	CI_Local_loc2
		RAloc3	Code Index	CI_Interna_loc3

CI_National_loc1 has patterns configured COSInternat and COSNat and pointing to the destination of the gateway from location1. Subscriber from location1 with COS COSInternat or COSNat assigned will be able to use this route. Subscribers that do not have a corresponding COS class assigned will be routed via the default pattern to a intercept (TRS_ON).

Table 82: Code Index Patterns for CI_Nat_loc1 (Global Numbering Plan)

Class of Service	Traffic Type	Routing Area	Dest. Type	Destination Name
CosInternat			Destination	Dest_gwloc1
CosNat			Destination	Dest_gwloc1
			Intercept	TRS_ON

The Code Index CI_Boc has for each location a pattern configured. The RA identifies the location of the calling party. The patterns point depending on the calling location information to a second code index to check the needed call restriction class.

Table 83: Code Index Patterns for CI_World (Global Numbering Plan)

Class of Service	Traffic Type	Routing Area	Dest. Type	Destination Name
		RAloc1	Code Index	CI_Interna_loc1
		RAloc2	Code Index	CI_Interna_loc2
		RAloc3	Code Index	CI_Local_loc3

The Code Index CI_Boc has for each location a pattern configured. The RA identifies the location of the calling party. The patterns point depending on the calling location information to a second code index to check the needed call restriction class.

Table 84: Code Index Patterns for CI_Interna_loc1 (Global Numbering Plan)

Class of Service	Traffic Type	Routing Area	Dest. Type	Destination Name
CosInternat			Destination	Dest_gwloc1

Class of Service	Traffic Type	Routing Area	Dest. Type	Destination Name
			Intercept	TRS_ON

Gateway Calls

- Incoming calls from a SIPQ Gateway
  - The OSV will skip the PAC table for incoming calls of a SIPQ gateway, if the SIPQ gateway is configured to send the called party as ISDN/ international. For this case, the translation will start directly in the destination code table of the assigned numbering plan from the gateway. The following is a provisioning example of the destination code entry for location1.

Table 85: Destination Code for incoming SIPQ Gateway Call ISDN/International (NP_loc1_gw))

Digits	NOA	Traffic Type	Class of Service	Routing Area	Dest. Type	Office Code
49897224	International	None			Home DN	4989722

  - If the SIPQ gateway is configured to send just the extension as called party in unknown/unknown, the translation will start in the PAC table of the assigned numbering plan from the gateway. The call will be routed with a normalized number from the PAC table of the gateway's PNP to the Global numbering plan. (The same handling as for subscriber calls) The following is a provisioning example of the destination code entry for location1.

Table 86: Destination Codes for internal calls (Global Numbering Plan)

Digits	min. Length	max Length	Digit Position	Digits to insert	Prefix Type	NOA	Dest. Type
4	4	4	0	4989722	Extension Dialing	International	E164 Destination

- Incoming calls from a Native SIP Gateway
  - SIP generally does not provide the capability to send a Nature of Address or Type of number within Invite messages. Therefore the called party of an incoming SIP Invite message is handled as a number with a unknown format, and the translation will start in the PAC table of the

assigned numbering plan from the gateway endpoint. The following is a provisioning example of the destination code entry for location2.

Table 87: PAC for incoming SIP Gateway Call with normalized number, but without leading "+" (NP_loc2_gw)

Digits	min. Length	max Length	Digit Position	Digits to insert	Prefix Type	NOA	Dest. Type
4969789	7	21	0		Extension Dialing	International	E164 Destination

OR

Table 88: PAC for incoming SIP Gateway Call extension only (NP_loc2_gw)

Digits	min. Length	max Length	Digit Position	Digits to insert	Prefix Type	NOA	Dest. Type
4	4	4	0	4969789	Extension Dialing	International	E164 Destination

- For the calls where the called party is received with "+" sign, the translation is done as follows:

Provisioning of '+' in the prefix table

The OpenScape Voice supports provisioning of '+' in the prefix table which is used for translation purposes. To maintain the backward compatibility, the OpenScape Voice algorithm for translating a DN with leading '+' digit tries to find a match for '+' character in the PAC table:

- If a **match in PAC table is found**, then the OpenScape Voice continues with the rest of the translation and returns translation result.
- If a **the match is not found**, then it will be checked if the hiQ/CSTA/GNFPrefixReplacement RTP parameter empty or not:
  - If RTP parameter is **not empty**, then OpenScape Voice replaces the '+' character with the RTP parameter value, sets the NOA to UNKNOWN and proceeds with the translation in PAC table. If the translation in PAC table is successful, then OpenScape Voice continues with rest of the translation and returns translation result.
  - If the RTP parameter is **empty** or if the translation failed in PAC table, then OpenScape Voice will remove '+' character, set the NOA to INTERNATIONAL. After that OpenScape Voice proceeds with translation in the destination_code table of the same numbering plan.

6.2.3 Common Routing Concept - Closed Numbering

In an Closed Numbering scenario subscribers are configured with full E.164 numbers, The E.164 numbers as well as the **extensions are unique! Within the same branch/location subscribers reach each other by dialing the extension** for the complete switch!

Each location has a local GW for the breakout to the PSTN. Gateway from location 1 is also used for calls to the existing PBX network of the customer.

There are 3 different call permission classes, a separate class for local, national and international calls. OSV subscribers are provisioned with corresponding Rate/Routing Area and Toll and Call Restrictions Service (or Class of Service).

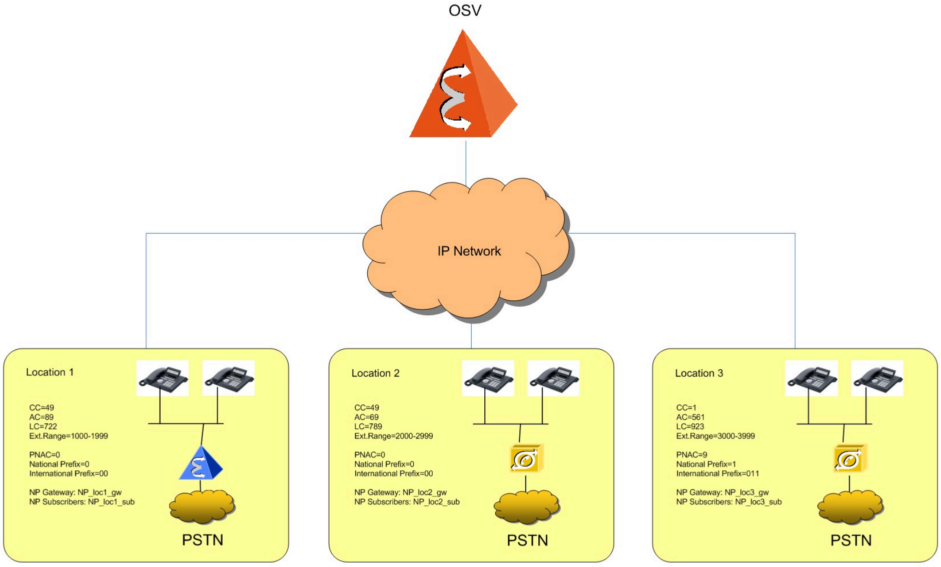


Figure 61: Closed Numbering

Subscriber Calls

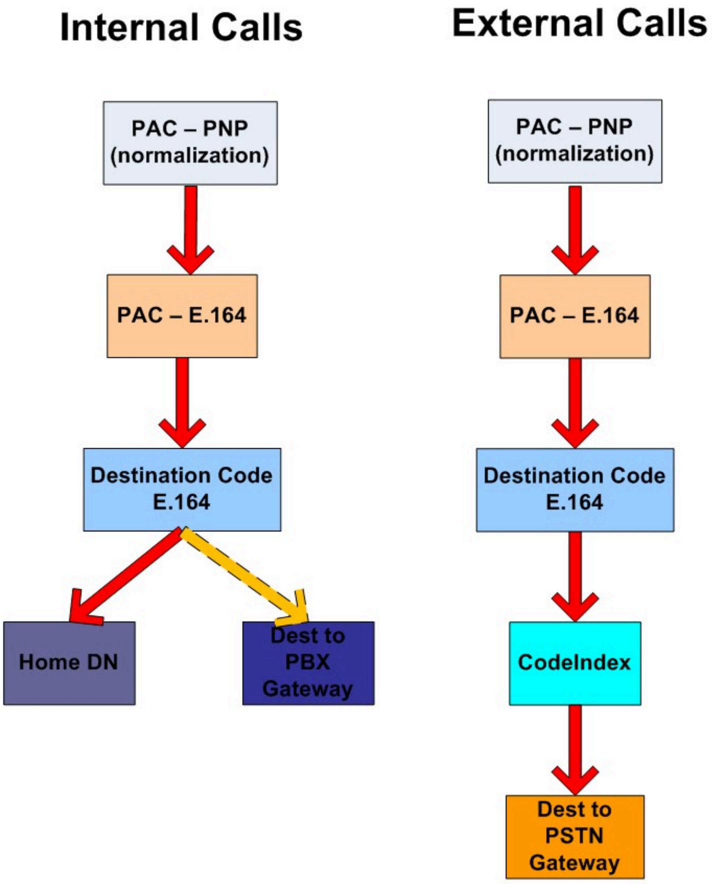


Figure 62: Closed Numbering - Subscriber Calls

Configuration and Provisioning of PNP PAC table

The PAC table of the PNP is used to match the dialed number, normalize it and send it up to the GNP. (note that also the CNP can be used instead of GNP, this depends on the customer requirements).

Although not shown in the picture above, the CNP could be used inbetween the PNP and GNP in case PAC entries can be summarized and therefore the configuration effort can be reduced with common normalizations in the CNP (depending on customer requirements).

Table 89: PAC table for location1 (location2 is configured similar (US)

PAC for Calls within same locations (NP_loc1_sub)							
Digits	min Length	max Length	Digit Position	Digits to insert	Prefix Type	NOA	Dest. Type
1	4	4	0	4989722	Extension Dialing	International	E164 Destination
2	4	4	0	4969789	Extension Dialing	International	E164 Destination

3	4	4	0	1561923	Extension Dialing	International	E164 Destination
PACs for calls to the PSTN (NP_loc1_sub)							
Digits	min Length	max Length	Digit Position	Digits to insert	Prefix Type	NOA	Dest. Type
0	1	21	1	4989	Off-net Access	International	E164 Destination
00	2	21	2	49	Off-net Access	International	E164 Destination
000	3	21	3		Off-net Access	International	E164 Destination

Table 90: PAC table for location3 (US)

PAC for Calls within same locations (NP_loc1_sub)							
Digits	min Length	max Length	Digit Position	Digits to insert	Prefix Type	NOA	Dest. Type
1	4	4	0	1972756	Extension Dialing	International	E164 Destination
2	4	4	0	4969789	Extension Dialing	International	E164 Destination
3	4	4	0	1561923	Extension Dialing	International	E164 Destination
PACs for calls to the PSTN (NP_loc1_sub)							
Digits	min Length	max Length	Digit Position	Digits to insert	Prefix Type	NOA	Dest. Type
9	2	8	1	1561	Off-net Access	International	E164 Destination
9	11	11	1	1	Off-net Access	International	E164 Destination
91	12	12	1		Off-net Access	International	E164 Destination
9011	5	21	4		Off-net Access	International	E164 Destination

Configuration and Provisioning of GNP PAC table

Configuration is the same as for the open numbering plan.

Configuration and Provisioning of GNP DC table:

Configuration is the same as for the open numbering plan.

Gateway Calls

Configuration is the same as for the open numbering plan.

6.2.4 Common Routing Concept - Tail End Hop Off

In an Tail End Hop Off scenario subscribers are configured with full E.164 numbers, **extensions are unique**. Within the same branch/location subscribers reach each other by dialing the extension

Destination gateway for the breakout to the PSTN is chosen depending on the called number. (least cost route)

3 different call permission classes, a separate class for local, national and international calls. OSV subscribers are provisioned with corresponding Rate/ Routing Area and Toll and Call Restrictions Service (or Class of Service).

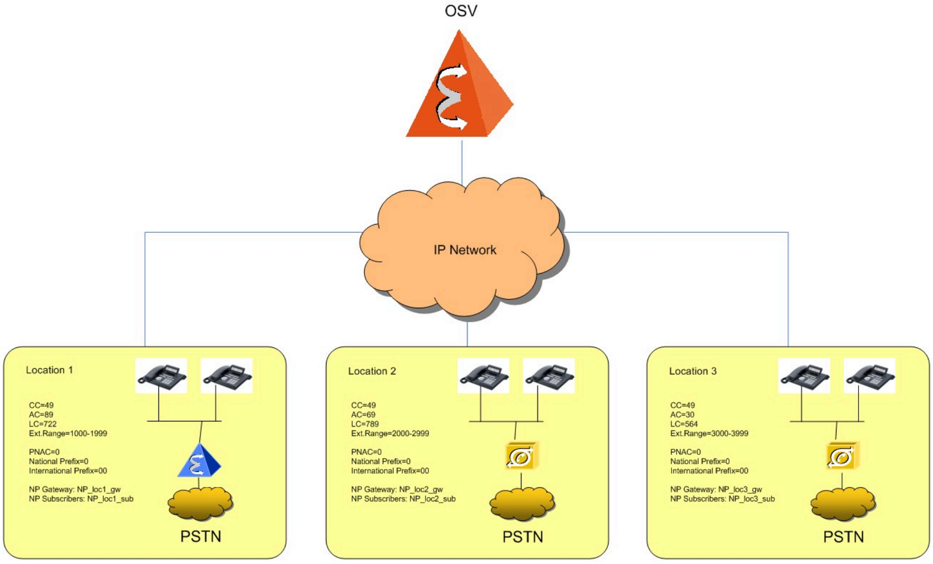


Figure 63: Tail End Hop Off

Subscriber Calls

It is possible to use a fallback mechanism to the private numbering plan of the originating party if the destination gateway becomes unavailable. This mechanism can be used optional and depends on the customer requirements, normally redundancy is provided by a second route at the destination.

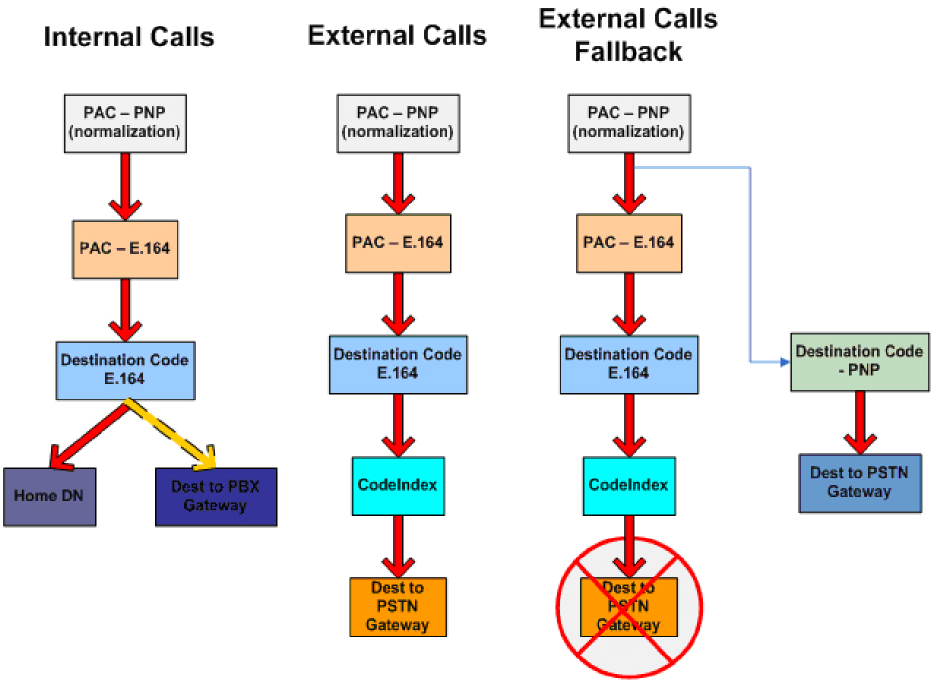


Figure 64: Tail End Hop Off - Subscriber Calls

Configuration and Provisioning of PNP PAC table

The PAC table of the PNP is used to match the dialed number, normalize it and send it up to the GNP.

Depending on the customer requirements, the CNP can also be used instead of GNP.

Allthough not shown in the picture above, the CNP could be used inbetween the PNP and GNP in case PAC entries can be summarized and therefore the configuration effort can be reduced with common normalizations in the CNP (depending on customer requirements).

NOTICE:

It is important to choose a corresponding nature of address (International for this example) in the PAC table, in case the Fallback from CNP/GNP to PNP has to be implemented. Nature of address is an destination attribute, and will be used in case of Fallback to match a destination code in the PNP destination code table.

Table 91: PAC table for location1 (location2 is configured similar)

PAC for Calls within same locations (NP_loc1_sub)							
Digits	min Length	max Length	Digit Position	Digits to insert	Prefix Type	NOA	Dest. Type
4	4	4	0	4989722	Extension Dialing	International	E164 Destination
PACs for calls to the PSTN (NP_loc1_sub)							

Digits	min Length	max Length	Digit Position	Digits to insert	Prefix Type	NOA	Dest. Type
0	1	21	1	4989	Off-net Access	International	E164 Destination
00	2	21	2	49	Off-net Access	International	E164 Destination
000	3	21	3		Off-net Access	International	E164 Destination

Configuration and Provisioning of GNP PAC table

Configuration is the same as for the open and closed numbering plan examples.

Configuration and Provisioning of GNP DC table:

> Internal Calls

- For the office codes of location2 and 3 are 2 destination codes configured with the office code + the first digit of the extension range to match only the assigned extension range. Both Destination Codes are pointing to the corresponding HomeDN.
- One and the same destination code can be used to point to the HomeDN and optional to a destination. This configuration is very helpful in case of a migration scenarios. The OSV checks first if a HomeDN is available for the called party, if not, the call will be routed following the configuration of the destination. In our example this kind of configuration is used for internal calls to OSV and PBX subscribers located at location1.

Table 92: Destination Codes for internal calls (Global Numbering Plan)

Digits	NOA	Traffic Type	Class of Service	Routing Area	Dest. Type	Dest. Name/ Office Code	DN Office Code
4989722	International	None			Destination	Dest_gwloc1	4989722
49697892	International	None			Home DN	4969789	
49305643	International	None			Home DN	4930564	

> External Calls: Call routing based on traffic types and code indexes

Traffic types identify the type of call, e.g. national or international. While a COS is a originator attribute, the traffic type is a destination attribute. The traffic type check is performed after the destination code has been matched, therefore no multiple destination code entries are needed, as they are if COS is used.

In this scenario, the traffic type is used to mark destination codes with the minimal permission a subscriber needs to use those routes. The needed permission is controlled via the "Toll and Call Restriction" feature configured under subscriber services.

Routing areas can be assigned to a subscriber or endpoint to indicate the geographic location of that subscriber. The Routing Area is an originator attribute. Multiple destination code entries with the same digit sequence will be needed for different locations. Code Indexes provide the capability of provisioning multiple destination codes with the same core parameters. They can be considered a kind of destination code template, which reduces administrative effort if template is used for several destination codes.

NOTICE:

The usage of Code Indexes is optional.

- **Provisioning for International calls**:

  Destination codes for international calls point to a code index called CI_World.

Table 93: Destination codes for international calls point to a code index called CI_World.

Digit	NOA	Traffic Type	Class of Service	Routing Area	Dest. Type	Code Index Name
1	International	None			Code Index Destination	CI_World
2	International	None			Code Index Destination	CI_World
3	International	None			Code Index Destination	CI_World
4	International	None			Code Index Destination	CI_World
5	International	None			Code Index Destination	CI_World
6	International	None			Code Index Destination	CI_World
7	International	None			Code Index Destination	CI_World
8	International	None			Code Index Destination	CI_World
9	International	None			Code Index Destination	CI_World

The Code Index CI_World has for each location a pattern configured. The RA identifies the location of the calling party, while the traffic type marks the traffic from all 3 locations as international traffic. For international traffic the destination for the local gateway is chosen

Table 94: Code Index Patterns for CI_World (Global Numbering Plan)

Class of Service	Traffic Type	Routing Area	Dest. Type	Destination Name
	International	RAloc1	Destination	Dest_gwloc1
	International	RAloc2	Destination	Dest_gwloc2

Class of Service	Traffic Type	Routin Area	Dest. Type	Destination Name
	International	RAloc3	Destination	Dest_gwloc3

- **Provisioning for National calls:**

  A Destination code for the German Country Code points to a code index called CI_GER. This destination code is needed to filter German national traffic.

Table 95: Destination Codes for national calls (Global Numbering Plan)

Digit	NOA	Traffic Type	Class of Servic	Routin Area	Dest. Type	Code Index Name
49	International	None			Code Index Destination	CI_GER

Code Index CI_GER has for each location a pattern configured. The RA identifies the location of the calling party, while the traffic type marks traffic from all 3 locations as national. For national traffic the destination for the local gateway is chosen.

Table 96: Code Index Patterns for CI_GER (Global Numbering Plan)

Class of Service	Traffic Type	Routing Area	Dest. Type	Destination Name
	National	RAloc1	Destination	Dest_gwloc1
	National	RAloc2	Destination	Dest_gwloc2
	National	RAloc3	Destination	Dest_gwloc3

- **Provisioning for Local calls:**

  3 Destination codes for the 3 locations are configured to filter local traffic. For Munich (CC49 + AC89) the destination code points to a code index called CI_Mch, for Frankfurt (CC49 + AC69) it points to a destination code called CI_Fra and for Berlin (CC49 + AC30) to CI_Ber.

Table 97: Destination Codes for local calls (Global Numbering Plan)

Digit	NOA	Traffic Type	Class of Servic	Routin Area	Dest. Type	Code Index Name
4989	International	None			Code Index Destination	CI_Mch
4969	International	None			Code Index Destination	CI_Fra
4930	International	None				CI_Ber

Code Index CI_Mch has for each location a pattern configured. The RA identifies the location of the calling party, while the traffic type marks traffic from location1 (Munich/Germany) as local, and traffic from location2 (Frankfurt/

Germany) and 3 (Berlin/Germany) as national. The destination for all 3 patterns is the destination of the gateway for location1 Dest_gwloc1. (least cost)

Table 98: Code Index Patterns for CI_Mch (Global Numbering Plan)

Class of Ser-vice	Traffic Type	Routin Area	Dest. Type	Destination Name
	Local	RAloc1	Destination	Dest_gwloc1
	National	RAloc2	Destination	Dest_gwloc1
	National	RAloc3	Destination	Dest_gwloc1

Code Index CI_Fra is configured similar to CI_Mch. The difference is that the traffic type marks traffic from location2 (Frankfurt/Germany) as local, and traffic from location1 (Munich/Germany) and 3 (Berlin/Germany) as national. The destination for all 3 patterns is the destination of the gateway for location2 Dest_gwloc2. (least cost)

Table 99: Code Index Patterns for CI_Fra (Global Numbering Plan)

Class of Service	Traffic Type	Routin Area	Dest. Type	Destination Name
	National	RAloc1	Destination	Dest_gwloc2
	Local	RAloc2	Destination	Dest_gwloc2
	National	RAloc3	Destination	Dest_gwloc2

Code Index CI_Ber is configured similar to CI_Mch and CI_Fra. The difference is that the traffic type marks traffic from location3 (Berlin/Germany) as local, and traffic from location1 (Munich/Germany) and 2 (Frankfurt/Germany) as national. The destination for all 3 patterns is the destination of the gateway for location3 Dest_gwloc3. (least cost)

Table 100: Code Index Patterns for CI_Boc (Global Numbering Plan)

Class of Service	Traffic Type	Routin Area	Dest. Type	Destination Name
	National	RAloc1	Destination	Dest_gwloc3
	National	RAloc2	Destination	Dest_gwloc3
	Local	RAloc3	Destination	Dest_gwloc3

> External Calls: Call routing based on class of service and code indexes

Class of Service should only be used when Traffic Types are not adequate

RA and COS classes are both originator attributes. Multiple Destination Codes with the same digit sequence are needed to create a call toll restriction matrix within a shared destination code table

For the "tail end hop off" scenario only one code index is used (for open and closed numbering scenarios a 2 Level concept was used). The destination gateway is chosen for local (and national) calls depending on the called number (least cost route), and will therefore always be different. ' In this case, templates to check local and national traffic do not make sense.

The code indexes include only patterns for the COS which are required to go forward to a valid destination. If a subscriber doesn't have a corresponding COS assigned, a default pattern is configured, which is pointing to a intercept (noPermission).

NOTICE:

The usage of Code Indexes is optional.

- **Provisioning for International calls**:

  Destination codes for international calls point to a code index called CI_World.

Table 101: Destination codes for international calls point to a code index called CI_World.

Digit	NOA	Traffic Type	Class of Service	Routing Area	Dest. Type	Code Index Name
1	International	None			Code Index Destination	CI_World
2	International	None			Code Index Destination	CI_World
3	International	None			Code Index Destination	CI_World
4	International	None			Code Index Destination	CI_World
5	International	None			Code Index Destination	CI_World
6	International	None			Code Index Destination	CI_World
7	International	None			Code Index Destination	CI_World
8	International	None			Code Index Destination	CI_World
9	International	None			Code Index Destination	CI_World

The Code Index CI_World has for each location a pattern configured. The RA identifies the location of the calling party. The 3 patterns are configured with COSInternat pointing to the destination of the local gateways. Subscribers with COS COSInternat assigned will be able to use this route. Subscribers that do not have a corresponding COS assigned will be routed via the default pattern to a intercept (noPermission

Table 102: Code Index Patterns for CI_World (Global Numbering Plan)

Class of Ser-vice	Traffic Type	Routing Area	Dest. Type	Destination Name
CosInternat		RAloc1	Destination	Dest_gwloc1

Class of Ser-vice	Traffic Type	Routin Area	Dest. Type	Destination Name
CosInternat		RAloc2	Destination	Dest_gwloc2
CosInternat		RAloc3	Destination	Dest_gwloc3

- **Provisioning for National calls:**

  A Destination code for the German Country Code points to a code index called CI_GER. Those destination codes are needed to filter national traffic for Germany.

Table 103: Destination Codes for national calls (Global Numbering Plan)

Digit	NOA	Traffic Type	Class of Service	Routin Area	Dest. Type	Code Index Name
49	International	None			Code Index Destination	CI_GER

The Code Index CI_GER has for each location 2 patterns configured. The RA identifies the location of the calling party. For each RA, 2 patterns are configured for COSInternat and COSNat which point to the destination of the local gateways. Subscribers from all 3 locations with COSInternat or COSNat assigned will be able to use these routes. Subscribers that do not have a corresponding COS assigned will be routed via the default pattern to a intercept (noPermission).

Table 104: Code Index Patterns for CI_GER (Global Numbering Plan)

Class of Service	Traffic Type	Routing Area	Dest. Type	Destination Name
CosNat	None	RAloc1	Destination	Dest_gwloc1
CosInternat	None	RAloc1	Destination	Dest_gwloc1
CosNat	None	RAloc2	Destination	Dest_gwloc2
CosInternat	None	RAloc2		Dest_gwloc2
CosNat	None	RAloc3		Dest_gwloc3
CosInternat	None	RAloc3		Dest_gwloc3
	None		Intercept	noPermission

- **Provisioning for Local calls:**

  3 Destination codes for the 3 locations are configured to filter local traffic. For Munich (CC49 + AC89) the destination code points to a code index called CI_Mch, for Frankfurt it points to CI_Fra and for Berlin to CI_Ber.

Table 105: Destination Codes for local calls (Global Numbering Plan)

Digit	NOA	Traffic Type	Class of Ser-vice	Routing Area	Dest. Type	Code Index Name
4989	International	None			Code Index Destination	CI_Mch
4969	International	None			Code Index Destination	CI_Fra
4930	International	None			Code Index Destination	CI_Ber

Code Index CI_Mch has for location1 patterns configured for COSInternat, COSNat and COSLocal. For locations 2 and 3 the patterns are COSInternat and COSNat. All patterns point to the destination of the gateway from location1 Dest_gwloc1. (least cost) The RA identifies the location of the calling party. Subscribers from all 3 locations with a corresponding COS assigned are able to use this route. Subscribers that do not have a corresponding COS assigned will be routed via the default pattern to a intercept (noPermission).

Table 106: Code Index Patterns for CI_Mch (Global Numbering Plan)

Class of Service	Traffic Type	Routing Area	Dest. Type	Destination Name
CosNat	None	RAloc1	Destination	Dest_gwloc1
CosInternat	None	RAloc1	Destination	Dest_gwloc1
CosNat	None	RAloc2	Destination	Dest_gwloc2
CosInternat	None	RAloc2		Dest_gwloc2
CosNat	None	RAloc3		Dest_gwloc3
CosInternat	None	RAloc3		Dest_gwloc3
	None		Intercept	noPermission

Code Index CI_Fra is configured similar to CI_Mch. The difference is that for location2 patterns are configured for COSInternat, COSNat and COSLocal. For locations 1 and 3 the patterns are COSInternat and COSNat. All patterns point to the destination of the gateway from location2 Dest_gwloc1. (least cost)

Code Index CI_Ber is configured similar to CI_Mch and CI_Fra. The difference is that for location2 patterns are configured for COSInternat, COSNat and COSLocal For location 1 and 3 the patterns are COSInternat and COSNat. All patterns point to the destination of the gateway from location2 Dest_gwloc1. (least cost)

Optional Fallback Configuration

The destination code table of the subscribers PNP is configured to match all calls that could fallback in case one of the foreign gateways becomes unavailable. The destination chosen for such a call is the destination for the local gateway.

For this national example it is enough to provide the destination code table only with the country code, which will match all possible fall back numbers.

To enable fallback to the local numbering plan the rerouting flag at the route from the destination (CNP or GNP) has to be checked.

Table 107: DC table PNP subscriber location1 with TT (Fallback configuration):

Digits	NOA	Traffic Type	Class of Service	Routing Area	Dest. Type	Dest. Name
49	International	National			Destination	Dest_gwloc1_pnp

Table 108: DC table PNP subscriber location1 with COS (Fallback configuration):

Digits	NOA	Traffic Type	Class of Service	Routing Area	Dest. Type	Dest. Name
49	International	COSNat			Code Index Destination	Dest_gwloc1_pnp
49	International	COSInternat			Code Index Destination	Dest_gwloc1_pnp

Gateway Calls

Configuration is the same as for the open and closed numbering plan examples.

Fallback Routing with Modified Number

When fallback is initiated, the original dialed number is re-translated in the Private Numbering Plan. This new enhancement provides the modification in order for the number as it has been transformed after it has passed through the common or global numbering plan (modifications done up to the destination table), to be kept for fallback to the private numbering plan. A new Destination flag is provided to indicate that fallback will happen with the modified digits. When this flag is set, then during fallback, a new translation will be done on the private numbering plan using the modified digits instead of the original. Translation in the local numbering plan will start from the local and pass through another route.

The new fallback with modified numbers is helpful when modifications are done on the CNP (or GNP) instead of the PNP.

For example if we had the same provisioning as before but all dialed numbers with prefix 0, 00 and 000 are modified in the common numbering plan the provisioning would be:

Table 109: PNP PAC does not modify the number but sends all numbers to the CNP.

Digits	min Length	Max Length	Digit position	Digits to insert	Prefix type	NOA	Dest. Type
0	1	21			Off-net Access	International	BG Common Destination

Table 110: CNP PAC modifies the number and sends all numbers to the GNP.

Digits	min Length	Max Length	Digit position	Digits to insert	Prefix type	NOA	Dest. Type
0	1	21	1	4989	Off-net Access	International	E164 Destination
00	2	21	2	49	Off-net Access	International	E164 Destination
000	3	21	3		Off-net Access	International	E164 Destination

GNP is the same as before

So when the fallback is executed the DC PNP table can be used (with the new fallback not the old).

Table 111: New fallback DC PNP

Digits	NOA	Traffic Type	Dest. Type	Dest. Type
49	International	National	Destination	Dest_gwloc1_pnp
49	International	COSNat	Code Index Destination	Dest_gwloc1_pnp
49	International	CosInternat	Code Index Destination	Dest_gwloc1_pnp

6.2.5 A-Side Signaling-Based Routing

The A-side signaling-based routing feature provides for the selection of a route to a destination based on the signaling protocol of the originating party.

6.2.6 Alternate Routing

The alternate routing feature provides flexibility to support different routes. It provides for the delivery of traffic from a specific subscriber to the network specified by the OpenScape Voice administrator. It also provides the capability to specify a prioritized list of possible routes to reach the destination.

OpenScape Voice evenly distributes the load across routes with the same priority but may use a lower-priority route if the first choice is overloaded or congested, or if the physical equipment is temporarily unavailable.

6.2.7 Alternate Routing with Overflow Among Route Types

The alternate routing and overflow among route types feature provides for calls to be routed to the same destination via alternate routes where a route can be a SIP-Q gateway or SIP server. The routes leading to a destination can be prioritized for routing purposes. Moreover, if one route (such as a SIP-Q gateway) is unavailable, the call can overflow to a different route even if it is of a different type (such as a SIP server).

6.2.8 Call Diversion for Invalid Destinations

After OpenScape Voice processes incoming external calls arriving over a SIP or SIP-Q trunk interface, the call can be diverted to a valid preconfigured alternate destination if translation of the called party results in an invalid destination.

Only calls that fail translation receive this treatment. If calls are translated correctly, but the route assigned is unavailable or unreachable, the existing capabilities are used to handle the call.

The OpenScape Voice administrator provisions this call diversion by assigning a new service to each endpoint profile. This service is activated when the called party fails translation for any reason, and the call is then routed to a destination the administrator also specifies — for example, an attendant or hunt group pilot number.

The following are examples of failure conditions that can cause this to occur:

- Incomplete digits received in the signaling for the called party.
- Dialed number that is not assigned to a subscriber.

6.2.9 Cost-Effective Routing

OpenScape Voice provides the capability to configure call routing to gateway destinations in a manner such that calls use the least expensive path available to the enterprise network, while also ensuring acceptable voice quality. This capability was formerly known as LCR (Least Cost Routing) in legacy systems.

Although cost-effective routing functionality is an inherent part of OpenScape Voice, its use is optional. Depending on an enterprise’ needs:

- Multiple destinations and routes may be configured as described elsewhere in this section.
- A set of static routes may be configured if the enterprise does not require this functionality.

Cost-effective routing is among the OpenScape Voice features that provide support for HiPath OpenExchange, which is useful for enterprises that have multiple sites and PBX (Private Branch eXchange) equipment from multiple vendors.

Comparison of price and quality

Before implementing cost-effective routing, the enterprise chooses preferred routes based on the price schedules it negotiates with its suppliers, balanced with the call quality of the various routes. These comparisons of price and quality are typically determined using off-board software the enterprise uses.

Excel spreadsheets or commercial applications which may integrate directly to the OpenScape Voice billing and QoS (Quality of Service) records.

Choosing preferred routes

On the basis of these comparisons, preferred routes are chosen. These routes are then implemented on OpenScape Voice, and the traffic volumes and costs monitored through reports generated from billing records.

Functional sequence

1) Gateways are defined within OpenScape Voice as SIP endpoints. These endpoints are given endpoint profiles that allow them to be associated with a business group, numbering plan, and routing area.
2) When a call is dialed that requires off-net routing, dialed digits are analyzed by the PAC (Prefix Access Code) table in OpenScape Voice to determine the call’s NoA (Nature of Address) — for example, NATIONAL or INTERNATIONAL.
3) After the NOA is determined, the call is routed to the Destination Code table.
4) The Destination Code table passes the call to one of the following:

   - If a route is not operating, a timeout may occur before OpenScape Voice attempts to use the next route in the destination list. If all routes are not operating, an intercept message is played via the media server.
   - If a trunk is full, the call instantly uses the next route in the list.

Destinations can be prioritized and limited in access by a CoS (Class of Service) or routing area assigned to the calling party. In this way, senior executives can be permitted to overflow to more expensive routes if the low cost carrier's trunk is full, while other callers might hear an intercept announcement — for example, "All circuits are busy; please try again later."

Guidelines for Implementation and Use

Although destinations can be limited in access by a user’s COS or routing area, users cannot use a COS or PIN (Personal Identification Number) to override routing configured in OpenScape Voice.

If all routes are restricted to permit only emergency calling after hours, a user cannot override this in any manner.

6.2.10 International Translation Support

The international translation support feature provides E.164 capabilities needed to address international requirements, such as the handling of hexadecimal digits in the prefix table and the E.164 routing tables.

6.2.11 Business Group Access Codes

The business group access codes feature allows the assignment of feature access codes, network access codes, and attendant access codes to be separately administrable for each business group.

6.2.12 Access Code Routing Concept

OSV uses source-BG access codes (one per BG only) and destination access codes for terminating incoming calls and routing outgoing calls via XLA. The OSV mechanism for this is called Access Code Routing.

The basic access code routing concept is used for Call Pickup network routing and operations. The `cPickInfo` operation received at the calling party switch triggers PR in order to optimize signalling and/or media paths through the network.

The former concept of "Node ID" routing in OSV has been referred to as "access code routing" using source-BG access code

Routing outgoing calls

For outgoing calls, Destination Access codes (unique network-wide) are used for routing a CPU call (call-related call pickup or non-call-related CISCs) to the appropriate network entity/node.

This type of access code routing via Translation (i.e., local digit analysis) facilitates an optimal routing mechanism for the network-wide CPU group service (and optionally PR). Access codes are transmitted in the CorNet-NQ Group CPU operations and must be provisioned by the craft in the appropriate XLA table(s) in the BG.

Routing an outgoing call via this mechanism requires the called number to be a Destination Access codes (unique network-wide).

Routing incoming calls

Tandeming or terminating an incoming call via this mechanism requires treating the called number as a Source-BG ("own") access code (unique network-wide).

NOTICE:

This routing is called "Node ID routing" in OpenScape 4000 terms. Each source-BG access code appears in remote switch’s translation table(s) as Destination Access codes for routing purposes.

For incoming calls, a (one) Source-BG ("own") access code (unique network-wide) value is assignable to each BG.

The above routing mechanism is facilitated by sending/receiving a CPU-related message/method with a:

NOTICE:

The above applies to CPU CISCs (Call Independent Signalling Connection) and the CPU picking up call to a remote called member. It does not apply to the calling party to the called group member call.

The only two services to employ this routing mechanism are:

- SIPQ Network-wide call pickup
- Path Replacement

SIPQ Network-wide call pickup

Since release 4.0R1 of OpenScape Voice it is possible to configure Call Pickup Groups whose members are located at different OpenScape Voice and OpenScape 4000 nodes, i.e. a CPG (Call Pickup Group) may span across the SIP-Q network.

Each local call pickup group is capable of adding a list of associated remote CPGs located elsewhere in OpenScape 4000 and/or OpenScape Voice private SIP-Q network.

The network-wide CPG feature relies on a feature activation and routing mechanism that is based on network-wide unique Access Codes being assigned to the involved OpenScape Voice Business Groups and OpenScape 4000 nodes. For a OpenScape 4000 this Access Code corresponds to its Node ID.

Path Replacement access code routing

PR supports the access code routing mechanism after a transfer when the system parameter "PR-node-ID-routing" is set "on".

The PRpropose rerouting field is be the source-BG access code assigned to this BG. An incoming called party number is matched to the source-BG access code in order to identify whether the call setup for PR treatment should terminate here or be tandemed. LM2853-2 PR shall default to access code routing mechanism after a CPU PR trigger is received.

Since 4k is the only PINX known to use node ID routing, an EP attribute indicates whether PR access code routing is applicable to this end point.

When the attribute is set on, PR employs the following source-BG access code mechanism:

The PR service supports the capability to perform PR based on access code routing (following transfer or pickup) based on the PR-access-code -routing parameter value for on:

- When PR service is started to propose PR for a call, it shall send this BG's assigned source-BG access code as the reroutingNumber (in QSIG prPropose) instead of sending the private network number. This results in the Called Party Number of the new replacement path SETUP message to be an access code for routing to this switch. The Call Identity shall be the only way to identify the proper old path with the new replacement path.
- When the PR service is started on receipt of an incoming Uce_Setup message for the replacement call, when the called party number was a match with this BG's source-BG access code in XLA. Then retrieve the associated data for this PR (based on the CallIdentity match) and process as usual. If the called party number (i.e., access code) does not match the source-BG access code, then this switch is a tandem switch, so UCE shall route this call according to the assigned route.

6.2.12.1 XLA (digit translation and routing) tables

One and multiple XLA table(s)

- If there is **only one XLA table** in the BG, only the private XLA table needs the Access codes to be created by the craft (i.e., call pickup access code, source-BG access code, and destination access codes).

- If there are **multiple private XLA tables** in a BG where an XLA table serves a CPU group member subscriber, each XLA table will need at least the call pickup access code to be created. The SIPQ EP(s) used for NW-wide group CPU could be assigned to the Common XLA table. In this case, the source and destination access codes do not need to be created in each private XLA table. But if EPs need to be assigned to private XLA table(s), then the private XLA table(s) need to include the source and destination access codes and their result (or point to the Common XLA table).

As an option, when the craft has provisioned a Common XLA table, the access codes may be created in the Common XLA table, but, the private XLA tables still need to point/access the Common table, either via a rule or with the actual access code value.

The **source-BG access** is not needed, even if assigned, if both of the following are true:

- no network-wide group CPUs exist in the BG
- Path Replacement -Access -Code -Routing is set to 'off'

6.2.12.2 Source-BG Access Code

The "own" access code for a particular BG. Used for routing and interworks with 4k "node Ids". Unique network-wide.

CPG network access and routing must be administered and managed across the network (i.e., source-BG access code, destination access codes and destination group numbers).

For every local BG (Business Group) that shall be provisioned with a network-wide CPG, the unique Access Code has to be configured as a PAC (Prefix Access Code), pointing to the *Network Feature Activation over SIP-QService* (**Network Feature**). Furthermore, the Access Code has to be assigned to this BG as its **BG Access Code**.

The settings for the **Source-BG Access Code** have to be done in the PNP (Private Numbering Plan)

6.2.13 ONS Subscriber Identity

ONS subscriber identity is the provisioned business group line identity where CSTA + ONS call services are provided.

Subscriber identity is where all ONS routing device monitoring and call control is preformed. Depending on the application requirements ONS Identities are provisioned in one of the two following ways:

- **Registering Device** – physical SIP device that registers using the subscribers ONS identify. Applications typically uses the ONS identity as the subscriber's identity. It is possible that no registering device is currently registered or reachable for the ONS subscriber DN. In this case an alternate destination is provisioned, for example using the Call Forwarding - Dependable Subscriber feature.
- **Non-Registering Device** – ONS subscriber identity provisioned when no SIP device ever registers for the ONS subscriber identity. This ONS subscriber identity is provisioned with SIP subscriber data to permit the customer to purchase a dynamic device license and work as a register

device. Applications typically use the ONS identity as a workgroup identity. In this case an alternate destination should be provisioned using the Call Forwarding - Dependable subscriber feature.

6.2.14 Office Codes

Every Business Group needs to have a Default Office Code assigned to it. When creating a new Business Group or when changing the default office code of a BG, you need to specify or define a Default Office Code to be assigned to the BG, in addition to giving it a BG name and a Display number.

Private Office Code and Private Extensions

The subscriber can do this in the following two ways:

- Selecting an Existing Office Code as Default for a BG
- Creating a New Office Code and Adding Directory Numbers

The **private office code** is the combination of the L2 code, L1 code and the L0 Code.

The **private extension number** is defined as the remainder of the private number after deleting the private office code and then preceded by 0 or more least significant digits of the L0 code. The latter digits are also called the ‘overlapping digits’.

NOTICE:

The term **extension** is also used for the public numbering plan with the same meaning, hence the need to differentiate them by using the term **private extension.** The previous rule shows that a private extension can be converted in a complete private number by combining it with the private office code using some well-defined rule.

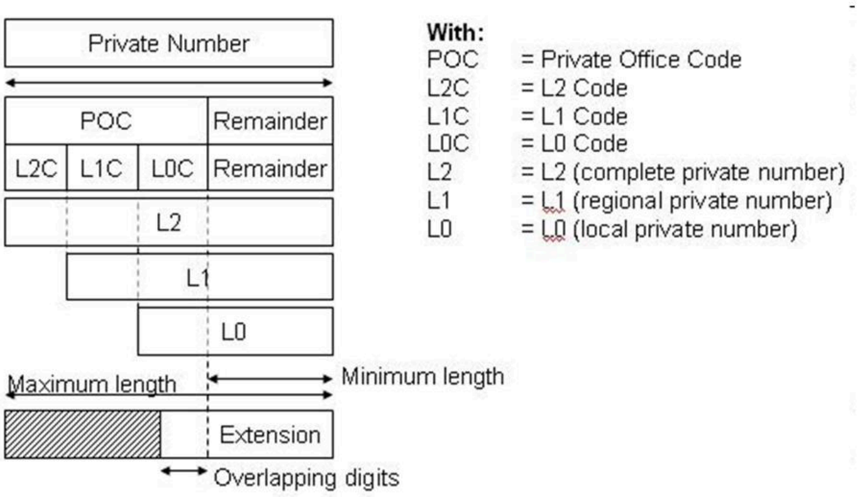


Figure 65: Private Office Code and Extensions

Use of Office Codes within the OpenScape Voice

the office code is used in 2 places:

- In some cases it is used to be able to create a **public number from an extension number**.
- It is used to create a **block of Home Directory Numbers** (public E.164 numbers that are to be registered on the OpenScape Voice).

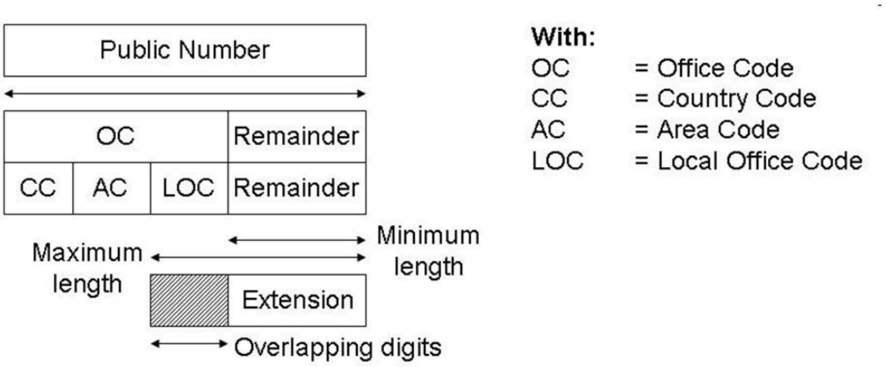


Figure 66: E.164 Office Code, Abbreviated Number and Public Extensions

Flexible Office Codes

The office code consists of CC, AC and possibly the leading digits of the public extension that will be created. Country Code (CC) and Area Code (AC) are optional fields, although the use of an area code is strongly recommended as some features require it to function well. The Local Office Code needs to be carefully chosen as its length may surpass the ‘real’ Local Office Code length depending on how many digits the public extension number consists of.

The office code is composed of CC + AC + LOC where

- CC = Country Code
- AC = Area Code, and
- LOC = Local Office Code

Maximum Length of Office Codes

Office codes can be up to 14 digits.

Relationship between Office Code and Business Group

There is no one-to-one relationship between Office Code and BG. It is possible to use one Office Code in multiple BGs and also to use multiple Office Codes in one BG. However, it is recommended to use one Office Code for one BG..

The newly created or selected office code will be displayed in all other dialogs that require the selection of an office code

By default, with the office code automatically a Prefix Access Code (PAC) in E.164 will be inserted into the global routing table. Thus the office code is recognized as an international number.

However, the admin may uncheck the PAC creation check box (checked by default) to disable the automatic creation.

After selecting or newly creating the default office code for the BG it is easily be possible to create Directory Numbers (DNs) for this office code.

If the admin wants to use an existing Office Code, she/he may also select an existing one. The newly created or selected Office Code will be known in all other pages that require the selection of an Office Code. By default, with the Office Code automatically a PAC (Prefix Access Code) in E.164 will be inserted into the Global Routing Table. Thus the Office Code is recognized as an international number. However, the admin may uncheck the PAC creation check box (checked by default) to disable the automatic creation. After selecting or newly creating the default Office Code for the BG it should easily be possible to create DNs for this Office Code. Please refer to the corresponding section for more information on how to enter the starting and ending DNs.

It is possible to create a new Office Code by entering digits into the following three fields, e.g. for Germany:

Table 112: Sample Office Code

For Germany		For U.S.	
Country Code	49	Country Code	
Area Code	89	Area Code	991
Local Office Code	722	Local Office Code	882

6.2.15 Directory Numbers

Directory Numbers are system resources that can be assigned to Subscribers, Endpoints, Services or Intercept Destinations across the Switch or be reserved for exclusive use within a specific Business Group.

6.2.16 Home Directory Numbers (Home DN)

This is the main number associated with the subscriber. The subscriber's Directory Number can be either a Public (E.164) or a Private (L2, L1, or L0) number.

Home Directory numbers are related to an office code and can be assigned as extension numbers to subscribers, phantom lines, endpoints, services or intercept destinations.

- If the subscriber's "External Directory Number" field is checked, it means that the Home DN assigned to the subscriber is a Public (E.164) number.
- Otherwise, it means that the Home DN is a Private (L2, L1 or L0) number.

NOTICE:

The definition on whether the Home DN is a Public or Private number is not stored as part of the Office Code or even as part of the Home DN itself. This information is part of the subscriber profile data.

Default Home Directory Number

- Home DN assigned to an Endpoint Profile

The "Default Home DN" number can be assigned to an endpoint profile.

For 'External' calls to a SIP endpoint (SIP Trunking, SIP Private Networking or SIP-Q Private Networking), if the calling party does not have a Public number, OpenScape Voice SHALL use the "Default Home DN" (if configured on the SIP endpoint) as the calling party number.

- Home DN used by the Number Modification Library

The "Default Home DN" is also used by the Number Modification Library to optimize all numbers sent to the endpoint (if optimization is required by the Number Modification rule as it is possible to create Number Modification rules where the "Default Home DN" of an endpoint is chosen over the input number to be presented to the endpoint).

Functional Sequence

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 the OpenScape Voice need to be defined. For example, an 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 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 OpenScape Voice subscribers. These number blocks are traditionally called DID number blocks.
3) Some endpoints on 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 OpenScape Voice Assistant), or by using the Office Codes screen (under Global Translation and Routing).

Global Home Directory Number List

In the Global **Home Directory Numbers** List the **Business Group Name** column indicates for each HomeDN if it's reserved for a Business Group or not

If nothing is displayed then the HomeDN is not reserved for a Business Group.

There is the option to filter for HomeDNs that are reserved for a specific Business Group or for not reserved HomeDNs.

- The administrator can see all the HomeDNs of the system via this list, but he can only edit the HomeDNs that are not reserved for a BG.
- The administrator that is BG administrator for a BG can edit non reserved HomeDNs as well as HomeDNs that are reserved for the BG that the user can administer, without having to go the BG specific HomeDN list.
- The administrator can reserve new HomeDNs for a BG. He can also unreserve HomeDNs from a BG (need to provide BG name so to avoid mistakes).
- The reservation cannot be updated for single HomeDNs.
- For the BG administrator that is not System administrator, access to Global HomeDNs list is not allowed. Instead a BG specific HomeDN list is introduced, where edit of single HomeDNs is made possible. (see section 3.1.1.3.2)

BG Specific Home Directory Number List

A Business Group specific Home Directory Number List within the BG menu facilitates the management of the Reserved Directory Numbers.

- The BG administrator can see all the Reserved DNs of the BG via this list but he can't add or delete Reserved DNs..
- The administrator can only edit/modify the Reserved DNs of the BG.
- For the System administrator that is not BG administrator, access to BG specific HomeDNs list is not allowed. .

6.2.17 Main Pilot DN

The administrator has the option to configure a subscriber that is an MLHG member to use the Name and Number of the Main Pilot DN as the subscriber's identity for Internal and/or External calls.

The External Caller ID has higher priority than the option to use the Main Pilot DN for external calls.

If the administrator wants the subscriber to use the Main Pilot DN as identity for external calls, he/she needs to remove any External Caller ID configured for the subscriber.

6.2.18 External Caller ID

The External Caller ID feature provides the subscriber with a second number which must be used for all external calls, incoming and outgoing.

The external caller ID customization feature provides the ability to provision a secondary calling party number, rather than the actual calling party number, to be used for presentation to called parties located outside the BG (Business Group).

This ability is useful if the subscriber:

- when the subscriber's Directory Number (Home DN) is a Private number (i.e. L2, L1 or L0 number). In this case, the subscriber's Directory Number cannot be used for external calls.
- if the subscriber wants to hide his Directory Number for calls to (or from) the public network.
- has a softphone that is used as preferred device for ONS subscriber, this softphone’s External Caller ID field has to be provisioned with ONS's number (CMP, OSV subscriber for OND/softphone number). Then, during UC outage, if the called party wants to call back ONS user, ONS number will be alerted (not softphone).

Requirements

The administrator uses OpenScape Voice Assistant to create a BG for the gateway to be used by the NP (Numbering Plan) of the subscribers that require the distinctive external caller ID handling. When creating this BG, the administrator performs the usual tasks associated with doing so.

The administrator then uses the Calling Number Permanent Presentation Status service to specify the secondary calling party number in the External Caller ID field.

Other Characteristics

The external caller ID is subject to display number modification.

6.2.19 BG Display Number

The BG Display Number is the default number that will be used to send to the public network in case OpenScape Voice has no other public number available for a subscriber.

The display number of the BG is shown when a subscriber makes an external call. The display number is defined during creation of a BG.

6.2.20 Destinations

Destinations are logical targets for off-net or on-net routing.

When a destination is created, the name of the destination is bound to the numbering plan where the destination is created. Destinations are used to route a call to an endpoint representing a gateway. The subscriber creates Destinations to define sets of Routes to E.164 Codes. Destinations can also be Media Servers. While creating a Destination the subscriber has to specify whether this Destination is a Media Server or not.

Non-Media Server Destinations and Routes tables (PNP/CNP/GNP)

For **Non-Media Server Destinations** (destinations not marked as a media server), all endpoints that are found via this destination will be either SIP endpoints or ENUM server routes.

Once a destination is created, routes can be added to the destination.

Media Server Destinations and Routes tables (PNP/CNP/GNP)

When creating a destination it is possible to mark it as pertaining to media servers only, meaning that all endpoints that are found via this destination will be media servers (MGCP endpoints). These **Media Server Destinations** can then be entered for the treatments of specific announcements. They can also be used when creating origin destinations.

Media Server Destinations can be created in the PNP/CNP or GNP. They will be presented when associating them to a treatment or a rate area of an origin destination.

NOTICE:

The media servers must be created before they can be added to a media server destination.

6.2.20.1 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, or 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 however, 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.

6.2.21 Destination Codes

The Destination Codes feature provides destination codes for basic telephone service. The destination code will be used for a call if the dialed or modified (in PAC) digits and the Nature of Address are matching. This field specifies the number configured for this Destination Code. A Destination Code Number is the leftmost digit string pattern identifying a group of Directory Numbers. Destination Codes can be of length 1-15.

Selectable Destination Types for Destination Codes

The destination fields determine where the resulting digit string will be analyzed next if necessary. This determination is done via destination type and destination name. The possible destination types are:

- **Destination**

  By entering a destination type of Destination, the digit string will be directly presented to the destinations table which will eventually lead to a route list of SIP endpoints that will receive the current digit string or a modified digit string, derived from the current digit string. The destination must have been created beforehand and it must be part of the PNP where it is used. This means that a destination cannot be shared by 2 PNPs of the same company even if the routes in the destination are exactly alike. This would actually be an indication that the destination in question actually belongs in the CNP. The OpenScape Voice allows specifying both a destination name and an office code when entering a destination type of “Destination”. If a digit string matches such a destination code, the digit string is first presented to the Home DN table (see below). If no match can be found there, the digits are further presented to the selected destination. This creates a very powerful way of handling number-by-number migrations from existing PBXs to the OpenScape Voice.
- **Service**

  The destination is a feature (also known as service destination). Some services are identified here. These services include:

  – BG Hot Desking
  – BG Main Number
  – Emergency
  – Emergency Callback
  – Precedence Call Div
  – Precedence Preemption
  – RACF (Remote Activation Call Forwarding)
  – RFA (Remote Feature Access)

- **Home DN**

  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. The destination type home DN is used to indicate that the digit string is a Home DN. It also takes the appropriate office code which must of course already exist beforehand. The dialed number is presented directly to the Home DN table. No other entries in translation tables are required.

  NOTICE:

  Remark, that the rule here needs to be specific enough to only push those numbers in the Home DN table that are actually subscribed on the OpenScape Voice. All other numbers if allowed to be dialed, need to point to a destination with routes so outbound calls to these numbers are not blocked. This can be accomplished by not removing the prefix access code used to dial the off-net number. However, CSTA applications like OpenScape, ProCenter allow dialing explicit numbers. In this case the number does enter the destination code table directly and cannot be distinguished from the Home DNs and the destination code should be configured as a destination that can lead to both an off-net route and a Home DN.

- **Intercept**

  If the administrator wants to block access to specific number ranges (e.g. 1-900 calls), intercepts can be defined and announcements can be played to the user dialing the invalid digits. Intercepts are used when calls are made by unauthorized users.

- **Invalid Code**

  It is used when a specific announcement other than the default announcement (“The number you dialed is not in service. Please check the number and dial again”) should be played when dialing a specific destination code.

- **Home Location** (available only at BG-leve)

  The translation of explicit L0, L1 or L2 numbers must go over the Home Location tables. It is recommended to handle all company-wide private dialing within the home location table of the common numbering plan of the company. The local PNP only needs to provide the capability to construct the L0, L1 or L2 number from a private extension used within the PNP. By entering a destination type of Home Location, the digit string will be directly presented to the Locations table of the PNP or CNP. The location code within the Location Codes table must be created already in advance.

- **Home Extension** (available only at BG-level)

  The extension tables only makes sense in the local PNP. It is possible to define the same extension tables in multiple PNPs as long as all PNPs belong to the same business group. Extensions tables (and Location Codes tables) are used for translating an explicit private number. With implicit private numbers one has the chance to use digit manipulation in the prefix access codes tables. With explicit private numbers the digit manipulation must be done in the extensions table. By entering a destination type of

Home Extension, the digit string will be directly presented to the extensions table of the PNP.

- **New Code**

  The **New Code** translation and routing capability allows a Directory Number to be replaced by another DN, and the translation result of the initial DN to be retranslated to the New Code.

  The Destination Code/E.164 Code which allows the association with a specified destination has been enhanced to support the **New Code** functionality. A new Destination Type, New Code and a new field for the New Code string are added. The new Destination Type is implemented for all Numbering Plans.

  With a new code specified, translation will replace the entire digit string with the new specified code and retranslate with NOA = unknown. This means effectively that the number will be presented to the Prefix Access Code table next. There is no modification of the new code number – it is presented to the prefix access code table as it is written in the new code field.

  NOTICE:

  The following restrictions apply for the **New Code** Destination Type: If Destination Type is New Code, Nature of Address cannot be Code Index; If Destination Type is New Code, then the Traffic Type, Destination Name, and DN Office Code parameters are not applicable.

  NOTICE:

  When selecting a new code from **PAC list for destination codes** by clicking the corresponding button on **Add destination code** window, the leading digits of the value that populates the **Destination Code** box are cropped depending on the value of digit position the PAC in question has. For example if the PAC 1234 has digit position 2, the cropped number 34 will appear in the **Destination Code** box. The user has the capability to manually enter the value 1234 in the **Destination Code** box and save the action when the whole digit string is required for the new destination code.

  Example for the use of the New Code Destination Type: The subscriber dials "611" to reach the company´s service bureau. However, the company has several service bureaus in different geographical areas and these are reached via long distance carriers via 800 numbers. Therefore, the 611 must be changed to the appropriate 800 number and then the call needs to be routed to the carrier that "owns" the 800 number.

  Valid characters: 0-9, A-E, *, #. Length: 1 - 30.

- **Code Processing**

  Code processing involves the capability to modify the digit string and its nature of address. Together with this capability a retranslation of the resulting digit string after code processing may be requested. If no retranslation is requested, the code processing rule indicates where the digit string will be processed further. The code processing rule must have been created previously. Code processing rules are created in the translation section of the Global Numbering Plan.

- **Code Index Destination**

  It is possible to create profiles of destination code entries. This is especially useful when there are multiple destination code entries that are always handled the same. The code index name must have been created previously. Code indices are created in the translation section of the Global Numbering Plan.
- **Time Destination** (available only at system-wide level)

  By creating a time destination, it is possible to select different destinations for a dialed string based on the time of the day that the digit string was dialed. This is a crude attempt at creating least cost routing (LCR) rules within the OpenScape Voice and is usually sufficient.
- **Calling Location**

  Calling locations allow you to route emergency calls to the appropriate answering point.

Originator Attributes: Creating Matching Rules

In the originator attributes, the routing area and the class of service can be singled out, which allows creating different rules for specific routing areas and classes of service. If nothing is entered here, any routing area and class of service of the originator are matching. Multiple rules with the same leading digits may be created that only differ on the originator info.

If nothing is entered here, any routing area and class of service of the originator are matching. Multiple rules with the same leading digits may be created that only differ on the originator info. In this case the ‘best match’ rule is as follows:

1) The Nature of Address must always match
2) Based on the leading digits all rules that could match are identified. The rules that could match are rules where:
   - The leading digits allow selection. The more digits the better the match.
   - The routing area and class of service match.
   - he routing area matches with no class of service defined.
   - The class of service matches with no routing area defined.
   - No routing area or class of service are defined
3) The best possible matching rule is then determined. This is the rule with the most amount of leading digits with the most of routing area and/or class of service matching.[#_ftn4 [4]]

Assignable Traffic Types

After a matching destination code has been found, the traffic type of the destination code is matched against the traffic type assigned to the calling subscriber in the Toll Restriction Service feature.

The following traffic types are defined and can be assigned to the destination code:

- **None:** this destination code is available for all traffic types. There is no toll restriction check.
- **International:** subscriber must be allowed to dial internationally.
- **International Worldzone 1:** subscriber must be allowed to dial within worldzone 1 (USA/Canada).

- **Inter LATA:** subscriber must be allowed to dial nationally. InterLATA calls are calls that incur long distance charges.
- **Intra LATA:** subscriber must be allowed to dial within his rate area. IntraLATA calls are calls that incur local charges.
- **TollFree Service:** subscriber must be allowed to dial toll-free services. Toll free calls are calls that are free of charge.
- **Directory Assistance 411:** subscriber must be allowed to dial the public operator for assistance. These calls typically incur a flat fee charge.

Dependencies of Destination Names from selected Destination Types

Depending on the Destination Type selected, the Destination Name field label will change to a label matching the selected Destination Type as follows:

Table 113: Destination Names depending on the Destination Type selection for Destination Codes

Destination Type	Destination Name	Comment
Destination	Destination Name	
Service	Service	
Home DN	Office Code	
Intercept	Intercept Announcement	
Invalid Code	Invalid Code Name	
Home Location	Location Code	only applicable at BG level
Home Extension	Home Extension Name	only applicable at BG level
New Code	New Code	(Valid characters: 0-9, A-E, *, #. Length: 1 - 30)
Code Processing	Code Index Name	
Time Destination	Time Destination	only applicable at system wide level
Calling Location	Calling Location	

Available Services for Destination Codes (selected Destination Type: Service)

Table 114: Definition and Description of Services listed in Service List dialog for Destination Codes:

Abbreviated (Displayed) Destination Name	Full Destination Name	Service Type [13]	Destination Definition
BG Hot Desking	BG Hot Desking Service	A	The BG Hot Desking (HD) service specifies either the Home DN or Remote DN of a Business Group Line (BGL) whose members/subscribers will be able to activate HD through an access code.
BG MainNumber	Business Group Main Number	A	The Business Group Main Number is the published number for a Business Group (BG).
Emergency	Emergency Call	A	Emergency Response Locations (ERL) can be configured in OpenScape Voice per IP subnet or IP address. Each ERL is assigned a Location Identification Number (LIN) and a route suffix. When an emergency call is placed by a subscriber, OpenScape Voise uses the subscriber's contact IP address to look up the ERL and then routes the call to the appropriate Public Safety Answering Point (PSAP) for the user's jurisdiction using the route fix.
Emergency Callback	Callback Number for Emergency Calling	A	The Destination Code Service value EnhEmncyCBSvc is used to define a Callback Number for Emergency Calling. The Service can only be assigned to a Vacant DN or en-bloc to leading digits of Vacant DNs. In case an Emergency Caller has to be called back from the E911 station, such a DN then can be used for the callback, if so entered into the caller's Emergency Calling entity "

[13] Service is available :

A= Only via PNP/CNP Destination Code, GNP E.164 Code, and GNP Home DN

B= Only via PNP/CNP/GNP PAC vertical service and GNP Home DN (not via Destination Code or GNP E.164 Code)

Abbreviated (Displayed) Destination Name	Full Destination Name	Service Type [13]	Destination Definition
MLHG	Multiline Hunt Group	A	"Multiline Hunt Group (MLHG) features permit calls to be routed to an idle line within a group of specified lines (i.e., a multiline hunt group). Each individual line must have its own private Directory Number (DN). A call is placed to a MLHG by dialing the Pilot DN. When a call is placed to a MLHG, the attempt to terminate the call begins with the line (member) designated by the Pilot DN, based on the hunt groups hunt method (sequential or circular). When all lines are busy, overflow treatment is provided to an intercept treatment of Busy Tone. A media server is required for audible treatment. The lines in a single MLHG cannot be a mixture of different business groups nor can they be a mixture of business groups and non-business groups.The OpenScape Voice supports groups of stations that can be accessed through a pilot station number (pilot hunt group) or through a call number of a controlling station (master hunt group). With a pilot hunt group, dialing the pilot number (station) for a group provides access to the pilot group. Calls are not distributed to the pilot station; this number is used only as an access number to the hunt group. With a master hunt group, dialing the master number (station) for a group provides access to the maste hunt group. Calls are distributed to the master station; the master station also has access to certain features that control the hunt group, such as call forwarding.
RACF	Remote Activation of Call Forwarding	A	The Remote Activation Call Forwarding (RACF) feature allows a subscriber who has any of the call forwarding feature variants to activate/deactivate and change the redirect number (for CFV) from another line. The RACF subscribers access their call forwarding feature by dialing the RACF DN, as provided by the operating company. The subscriber receives an announcement requesting them to enter their home DN, followed by an announcement requesting their Personal Identification Number (PIN). Upon verification of the home DN and PIN, an announcement is played requesting the Service Access Code for the type of call forwarding procedure to be attempted.
Remote CF	Remote Call Forwarding	A	The Remote Call Forwarding (RCF) feature allows calls incoming to Remote Call Forwarding subscriber DNs to be forwarded to the remote forwarding address, unless the maximum simultaneous calls allowed for forwarding is reached.

[13] Service is available :

A= Only via PNP/CNP Destination Code, GNP E.164 Code, and GNP Home DN

B= Only via PNP/CNP/GNP PAC vertical service and GNP Home DN (not via Destination Code or GNP E.164 Code)

Abbreviated (Displayed) Destination Name	Full Destination Name	Service Type [13]	Destination Definition
RFA	Remote Feature Access	A	Remote Access is a common function that is used by any feature/service that wants to allow it. The PIN and RFA need only be assigned once and then can be shared by all services allowing Remote Access.

Range of Destination Codes

Destination codes can be provisioned with a range of codes when creating destination codes via the **Add Range** button.

If this option is chosen, the user is promoted to specify the 'begin code' and 'end code' (the 'end code' can have same value as the 'begin code').

This operation results in creating a number of destination codes starting from 'begin code' to 'end code'.

For Example: If the values of 'begin code' is 1 and the value of 'end code' is 9, then 9 destination codes will be provisioned in the system.

6.2.21.1 E.164 Codes

The E.164 Code defines the call routing and treatment with the NOA (Nature of Address), routing area and COS (Class of Service).

E.164 Codes enable the subscriber to associate a code with a destination. E.164 Codes are combinations of digits that provide a complete address to reach a destination in a network. E.164 Codes cannot contain the characters # or *.

The E.164 Code has to be consistent with the PAC (Prefix Access Code) for extensions.

The E.164 function defines sets of E.164 Codes as well as associated destinations, NOAs, and/or traffic types. The E.164 Destination Code includes the routing instructions for all interconnected systems.

Range of E.164 Codes

A range of E.164 Codes can be provisioned with a range of codes when creating E.164 codes via the **Add Range** button. If this option is chosen, the user is promoted to specify the **begin code** and **end code** (the 'end code' can have same value as the 'begin code'). This operation results in creating a number of E.164 codes starting from 'begin code' to 'end code'

[13] Service is available :

A= Only via PNP/CNP Destination Code, GNP E.164 Code, and GNP Home DN

B= Only via PNP/CNP/GNP PAC vertical service and GNP Home DN (not via Destination Code or GNP E.164 Code)

6.2.21.2 Business Group Destination Code Table

After the Business Group Prefix Access Code table analyzes and translates the digits, the Destination Code Table actually routes the call.

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 Extension Number Table**
- 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.

BG NP Configuration

Table 115: Prefix Access Code Table Entries Permitting E.164 Dialing

Field	Input Value	Comment
Digits	1561923	
Minimum length	11	
Maximum length	11	
L2 length	6	Delete 6 digits
Digit Position	6	Leave blank.
Prefix Type	Extension Dialing	
Nature of Address	PNP Extension	Only valid choice
Destination Type	None	Go to BG destination code table

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 the table below:

Table 116: Second Prefix Access Code Table Entries Permitting Extension Dialing

Field	Input Value	Comment
Digits	31	
Minimum length	5	
Maximum length	5	
L2 length	0	Delete 6 digits

Field	Input Value	Comment
Digit Position		No digits deleted.
Prefix Type	Extension Dialing	Leave blank
Nature of Address	PNP Extension	Only valid choice
Destination Type	None	Go to BG destination code table

Continuing the same example, the administrator should add the entry shown in the following code table:

Table 117: Destination Code Table Entries

Field	Input Value	Comment
Destination Code	31	
Nature of Address	PNP Extension	
Class of Service		Leave blank
Traffic Type		Do not assign a traffic type
Routing Area		Leave blank.
DN Office Code	Extension Dialing	Leave blank
Destination Type	PNP Extension	Go to the Extension table for routing
Destination Name	None	

NOTICE:

The destination code table can be provisioned with a range of codes.

This functionality is available for destination codes provisioning in all the private numbering plans as well as Global numbering plan done through Assistant. So, destination code on BG and E.164 will be affected.

6.2.21.3 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:

- The prefix digits which define the block of numbers. These are selected from the list of prefix access codes defined in the previous section.
- The remark field can be left empty (a field for future use).

- The NOA (for example, unknown, international, and so on).

> **NOTICE:**
>
> 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

- 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.
- Traffic type – normally set to none (meaning no specific traffic type).
- 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.

6.2.21.4 E.164 Compliance

The E.164 compliance feature provides the ability to dial or receive any E.164-compliant number.

6.2.21.5 E.164 Code Table Entries

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.

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

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

- **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.
- **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.
- **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.
- **Destination Type:** For an entry related to inbound calls, this will usually be “Home DN”, meaning this number terminates on an 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. If the destination type is set to “Home DN” the destination name must match one of the home DN office codes previously defined..

6.2.21.6 How to Export Destination Code lists

This procedure describes how to export Destination Code lists.

Prerequisites

Adequate administrative permissions

Step by Step

1) Log on to the CMP and navigate to activate the **Configuration** > **OpenScape Voice** tab.
2) Click the **Business Group** icon.
3) Select the switch from the **Switches** dropdown list
4) Select the BG from the **Business Group List** dropdown list.
5) Navigate to **Translation** > **Destination Codes**

6) Click on the **export data to CSV file** button.

IMPORTANT:

If a filter is applied then the extracted data that is displayed is filtered as well.

7) You are prompt to open / save the . csv file with the following information :

- Code
- Class of Service
- Routing Area
- Nature of Address
- Destination Type
- Destination Name

IMPORTANT:

If a check box is ticked in the list or if the list is empty the **export data to CSV file** button is disabled.

NOTICE:

NOTICE: If the Destination Code list exceeds the number of 65536 rows which is the limit of an MS Excel file format then you must be advised to use a text editor in order to view the contents or you can split the data (copy rows from 65536 onwards to a new CSV file) and view the chunks in Excel.

6.2.22 Bulk Editing Destination / E.164 Codes

The **Bulk Edit** feature allows the user to modify more than one data record of the same entity simultaneously via the GUI.

This modification is possible for the following entities:

- Subscribers
- Endpoints
- **Destination Codes / E. 164 Codes**

To bulk edit certain parameters, the checkboxes on the left side must be checked. **Only the activated parameters have an impact on the selected Subscribers**. Parameters without a checkbox are not editable in The **Bulk Edit** mode.

6.2.23 Domain Codes

The Domain Based Routing feature allows the administrator to provision routing based on the hostname received in a SIP Uniform Resource Identifier (URI) rather than based on digits contained in the username of the SIP URI.

Domain Code Characters

A domain code in the Domain Code Table can be one of the following types:

-**Domain name**	e.g. *unify.com*
-**Wildcarded Domain Name**	e.g. **.com*. This indicates all domain codes that end on *.com*
- Alphanumeric SIP URI	: e.g. *Joe.Smith@unify.com*
- **Numeric SIP URI**	: e.g. *+15619231658@unify.com*
- All Numeric SIP URIs	: e.g. *#@unify.com*. This indicates all numeric SIP URIs within the unify.com domain
- Anything	: *

The Domain Code Translation table links a code, that can be:

- an alphanumeric SIP URI domain
- a domain name
- a partial domain name

Assignable Traffic Types

The Domain Code table supports the assigning of a traffic type to an entry. Allowed traffic types are any of the defined traffic types in Global Translation and Routing.

- International
- National
- Local
- Toll Free
- Emergency
- Public Operator
- Directory Assistance

Traffic Type = None is also allowed indicating that this domain code is available for all traffic types. There is no toll restriction check.

The administrator can activate the Toll Restriction Service to restrict access to certain domains for the domain-dialed calls.

Authorization Codes, account codes and call forwarding restrictions are supported as well.

Selectable Destination Types for Domain Codes

The destination fields determine where the resulting digit string will be analyzed next if necessary. This determination is done via destination type and destination name. The possible destination types of the domain code tables are the following:

- **Destination**

  By entering a destination type of Destination, the digit string will be directly presented to the destinations table which will eventually lead to a route list of SIP endpoints that will receive the current digit string or a modified digit string, derived from the current digit string. The destination must have been created beforehand and it must be part of the PNP where it is used. This means that a destination cannot be shared by 2 PNPs of the same company even if the routes in the destination are exactly alike. This would actually be an indication that the destination in question actually belongs in the CNP. The OpenScape Voice allows specifying both a destination name and an office code when entering a destination type of “Destination”. If a digit string matches such a destination code, the digit string is first presented to the Home DN table (see below). If no match can be found there, the digits are further presented to the selected destination. This creates a very powerful way of handling number-by-number migrations from existing PBXs to the OpenScape Voice.
- **Intercept**

  If the administrator wants to block access to specific number ranges (e.g. 1-900 calls), intercepts can be defined and announcements can be played to the user dialing the invalid digits. Intercepts are used when calls are made by unauthorized users.
- **Restricted Code**

  It is used when a specific announcement other than the default announcement (“The number you dialed is not in service. Please check the number and dial again”) should be played when dialing a specific destination code.
- **Fallback to Local Numbering Plan**

  Configuring Fallback to Local Numbering Plan allows you to purposely fail translation in the common or global numbering plan in order to invoke the fallback destination of a private numbering plan domain code.

SIP URI Translation

In versions before V8 SIP URI translation is supported but is limited to a lookup in the alias table to see whether the presented SIP URI matches a configured alias. For backward compatibility reasons, from V8 onwards any URI translation always starts with a lookup in the alias table in order to find out whether the called SIP URI belongs to a subscriber on the OSV before it resolves the SIP URI via the Domain Code table.

The logic for resolving non-local URIs has the following steps:

1) Translation is started within the calling party’s numbering plan’s domain code table.
2) From there translation may be set up to go to the common or to the global numbering plan.It may also, in any of the domain code tables, replace a complete matching URI with a number (GNF number is allowed) which can then be translated using the logic for translating numbers. A complete matching number means that the domain code and the presented SIP URI match exactly (of course after normalization (case-insensitive)).

Fallback to the Local Numbering Plan

Feature ‘Fallback to the Local Numbering Plan’ is supported from V* onwards. The logic for this feature is the same as when used for number translation:

If no available routes were returned via normal translation or if the Destination Type is set to Fallback to Local Numbering Plan then the fallback is automatically executed internally within translation. If routes were returned then a flag is returned to the caller of translation. If translation is then called again with this flag set, then the redirect from the private numbering plan to the common or global numbering plan or from the common numbering plan to the global numbering plan is ignored and translation remains within the private numbering plan – i.e. executes the destination part of the Domain Code.

Destinations used for number translation may be reused for URI translation. Number modification logic at the route level shall not apply to alphanumeric SIP URIs

6.2.24 Time Destinations/Time-of-Day Routing

The Time-of-Day routing allows the routing of calls to the same E.164 Destination Code via different routes depending on the time of day and the day of the week.

The OpenScape Voice administrator can create Time-of-Day destinations and use them in the E.164 code table as destinations. A Time- of-day destination can have one or more day schedules (for example, a weekday schedule, a weekend schedule, and a holiday schedule) with each day of the week being associated with its own schedule.

Time-of-Day based routing allows routing calls to E.164 Destination Codes via different routes depending on the time of day and the day of the week. the subscriber can create Time Destinations and use them in E.164 Codes as destinations. A Time Destination can have one or more day schedules (for example, weekday schedule, weekend schedule and holiday schedule), with each day of the week associated with a day schedule.

Functional Sequence

Once the subscriber has created Time Destinations, the subscriber can assign these Time Destinations to OpenScape Voice Assistant E.164 Codes, in order to specify the E.164 DN (Directory Number) Code with which to associate each Time Destination.

After creating a Time Destination, the subscriber must create at least one day schedule. Then, the subscriber adds at least one period schedule to each existing Day Schedule. Finally, the Day Schedule(s) the subscriber has created are assigned to each day of the week in the subscriber Weekly Schedule for the Time Destination.

NOTICE:

If the subscriber saves the Time Destination record without assigning a valid day schedule to each day of the week, the system displays an error message indicating that the Time Destination record is incomplete and cannot yet be used in an E.164 Code record.

When creating a new Time Destination, the subscriber needs to assign at least one day schedule in its weekly schedule. A day schedule may comprise of one or more Time Periods. The day schedule is considered to be complete if every minute of the day belongs to exactly one Time Period. Time Periods of a day schedule must not overlap.

6.2.25 Origin-Dependent Translation and Routing

The OpenScape Voice system provides origin dependent translation and routing for calls handled by multiple feature servers in a VoIP (Voice over IP) network.

To provide origin dependent routing a parameter known as the OTG (Originating Tenant Group) is passed between system's in a network.

The origin-dependent routing feature allows assigning rate area and class of service to SIP subscribers, SIP servers, and SIP-Q gateways. During routing, originating rate area and class of service are obtained from the incoming SIP subscriber, SIP server or SIP-Q gateway; this information is used to select routes or media servers.

6.2.26 Routes

A route connects the destination with an endpoint representing a gateway. For each Destination the administrator creates and configures one or more Routes with bearer capabilities, types, and leading digit information

Requirements

Each Operator Route has to be configured with a dialing pattern, Class of Service, and Destination

Each route must have a unique combination of routing areas and destinations. It is not possible to assign the same combination of routing areas and destinations to multiple routes.

Types of Routes

The subscriber can create the following **Types of Routes** to a Destination:

- **SIP Endpoint** - if the Destination is NOT a Media Server,
- **ENUM** - if the Destination is NOT a Media Server,
- **MGCP Media Service** (Media Server name and circuit ID) - if the Destination is a Media Server.

Originator Attributes used for routes

Multiple routes can be added to a Destination in order to prioritize the routing to the gateways. Routes can only be added to existing Destinations (Gateways).

The following **Originator Attributes** are used for routes:

- The Originating **Signaling Type**: this is an indication of the type of endpoint that wants to use a route of the destination. The OpenScape Voice currently supports SIP endpoints and subscribers that use translation. If the route is for general use regardless of the originator's signaling type, Undefined can be selected as well.
- The **Bearer Capability**: this is an indication of the type of bearer traffic that the originating party will generate. By creating routes for selective bearer

types, one can have a single logical destination and still route originating fax, video calls differently from speech calls.

Route Lists

For each originator attributes pair, translation will create a **Route List**. For each possible route list, the administrator can select whether the route list must be searched linearly or randomly:

- If a specific route list (e.g. the SIP/Speech route list) is marked prioritized, a **linear search** from lowest route index to highest route index is performed .
- If the route list determined by the originator attributes is not marked as prioritized, the route list is searched a **in random order**.

Route Restrictions

There are the following limitations regarding routes for destinations:

- Translation will allow up to 64 routes (that have the same Originating Signaling Type and Originating Bearer Capability) per destination.
- Translation will only return the first 3 routes of a matching route list even if there are more routes in the route list, for non-prioritized route lists. In order for the OpenScape Voice to effectively use these 3 routes, the feature Endpoint Rerouting must be enabled.
- Translation will return a number of routes set by the RTP parameter

  `Srx/Main/MaximumSelectableRoutes`

  The value of the parameter is an integer with a value range between 3 - 64 and default value 3. It controls the maximum number of routes selected from the route list of a destination during Endpoint Rerouting This parameter is only applicable for prioritized route lists.

  In order for the OpenScape Voice to effectively use these routes, the feature **Endpoint Rerouting** must be enabled.

  NOTICE:

  Prioritized rerouting occurs only when all three routes, with the lower index, return sip server failure responses. In that case the next, based on priority index, three or less routes will be used.

- For each route in the route list, the digit string presented to the destinations table can be modified to suit the needs of the SIP endpoint or the ENUM operator that is the target of the route. The nature of address of the resulting digits can be set as well. This allows the administrator to control very late in the translation how digits will be presented.
- The general rule here is to keep the numbers normalized until the route is determined and modify the digits there.
- The route Type ENUM is used to indicate that the current digit string must be presented to an ENUM operator. The ENUM operator operates on an ENUM server which is a DNS-like server that accepts queries for ENUM entries. The OpenScape Voice may modify the digits in the route table and will then format the digits to the appropriate ENUM format and wait for a response from the ENUM server where to go to. The response will be an IP address or an FQDN for the destination.

Routes Table of XLA Library

The local toll table may be used on an outbound route in order to convert a normalized called party number to the by the carrier expected format (local, national or international).

Two additional NOAs are allowed on the Route table's NOA:

- **LOCAL TOLL:** uses the in the Local Toll field specified local toll table to strip down the called party number to the shortest form required by the carrier. The type of number of the input called party number must be International or National.
- **LOCAL TOLL-PRE:** uses the in the Local Toll field specified local toll table to strip down the called party number to the shortest form required by the carrier and then prefixes the number with the prefixes defined in the DNM Prefixes table. The type of number of the input called party number must be International or National.

There are 2 major advantages when using a defined local toll table:

Two additional NOAs are allowed on the Route table's NOA:

- - In some areas, the local calling area offered by the carriers does not match with the area code of the subscribers; in this case area codes may overlap and even be split. Up to now, in order to deliver the correct called party number to the carrier, each local exchange code of the local calling area needed to be handled separately in the destination codes table and lead to a destination with a route to the local gateway that makes the called party number a local number as specified by the carrier. All these destination codes entries (there can be hundreds) can now be combined to a single destination codes entry that leads to a single destination that points to a route that uses a LOCAL TOLL or LOCAL TOLL-PRE rule to modify the called party number at the outbound route.
- - Even if the local calling area matches with the area code (this is the most common rule), a local toll table entry can simplify the destination codes and destinations tables, because the destinations created for local, national and international traffic can be combined in a single destination leading to a route with a LOCAL TOLL or LOCAL TOLL-PRE rule

This also fits very well into the strategy to only work with normalized numbers in OpenScape Voice translation. When working with normalized numbers in translation, the correlation between translation and number modification mostly disappears. Currently, DNM tables need to be entered to account for normalizing translation results. These translation results are used as presentation numbers in case the carrier does not deliver presentation numbers for alerting or connected parties (which it normally doesn't). Obviously if the PAC table translation already normalizes a number to an international number before entering the destination codes table, the translation result will already show a normalized number and the DNM Normalizations table does not need any additional entries to handle dialing out to the gateway.

6.2.26.1 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 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 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 / insert** can be specified. This permits limited manipulation of the destination digits prior sending the outgoing setup/invite.
- **NOA (Nature of Address)** 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.

6.2.27 Generic Destinations

A generic destination is a physical location in the telephone or IP network that contains a prioritized collection of routes that can be used to arrive at that destination. This is the starting point for finding a free trunk when allocating trunks for an outgoing call.

The generic destination table supports reaching the same E.164 destination code through different types of routes. This allows routing of calls to overflow among gateways and gatekeepers. This table is used for create, delete, and display operations on generic destinations.

Each destination points to the route list that contains the highest priority routes to that destination.

Once the subscriber has created and defined destinations in the OpenScape Voice system, he/she can assign these destinations to E.164 DN (Directory Number) Codes. In addition, the subscriber can assign destinations to Carrier Routes, to associate the destinations with specific carriers.

6.2.28 Bearer Capability-Based Routing

Bearer capability-based routing allows routing of calls to different TKGs (Trunk Groups) based on the originator's bearer capability.

Routes are ordered by their priorities and arranged in a linked list. A single route can belong to many destinations and priority is unique.

Routing is also based on incoming signaling type. A-side signaling-based routing allows the use of different protocols for outgoing calls to the same destination code based on the signaling protocol used by the originating side. The SIP signaling protocol is associated with this route.

If bearer capability and signaling type are entered, the route list is mandatory. Up to 8 routes can be assigned in a route list and at least one route must exist. More than one route list can be assigned to a destination with each list associated with a different bearer capability an signaling type.

Each route is a collection of groups or addresses that provide a path to a destination. There are several types of routes, as follows:

- Gateway — The route points to the gateway EP (Endpoint) which defines the IP address and call signaling type information. The OpenScape Voice system supports up to eight gateway routes per EP.

6.2.29 Leading Digit and Most-Matched Digit Translation

The Leading Digit and Most-matched Digit Translation feature provides mechanisms to quickly and accurately route calls.

- Leading digit translation can be completed at different points (n leading digits in the Destination Codes provisioning, where n is 1 through 15) in a Destination Code. This ability permits translation and routing decisions to be made based on Country Codes, Area Codes, or Office Codes.
- Most-matched digit translation always searches for the longest matching digits to determine the destination. It is used to resolve ambiguity in the codes.

6.2.30 Source-Based IP Routing

For redundant configurations, enterprises have the possibility to define more than one default gateway for OpenScape Voice to use when sending packets to the network from VLAN/subnet-separated networks—specifically, the management, signaling, and billing/CDR (Call Detail Recording) redundant connections from each node.

To implement this capability, routing entries are added at the OS command-line level to specify a default gateway for each interface/subnet.

NOTICE:

This capability should only be deployed if an enterprise does not permit routing between subnets on its network. Always contact your next level of support for assistance in configuring this feature.

6.2.31 Subscriber Routing Options

Several logical database objects provide the capability to route calls in various manners. Common examples of these objects include the PAC (Prefix Access Code), DC (Destination Code), LC (Location Code), and extension tables.

Requirements

When designing the routing for an enterprise, the designer must balance best practices and supported configurations against the need to successfully complete all customer-required routing needs, optimize the OpenScape Voice database and searching functions, and retain the robust routing necessary to complete calls to any required destinations.

The following are the primary options for routing calls between subscribers:

- Extension dialing via PNP (Private Numbering Plan)
- Extension dialing via PNP and GNP (Global Numbering Plan)
- Home DN (Directory Number) dialing via PNP
- Home DN dialing via PNP and GNP

6.2.32 Subscriber Routing Options - Extension Dialing via PNP (Private Numbering Plan)

Extension dialing via the PNP (Private Numbering Plan) allows extension-based dialing to be kept and controlled within the logical confines of the PNP in which the calling subscriber is defined.

It uses the PAC (Prefix Access Code) prefix type of Extension Dialing to mark this call type as extension-to-extension calling within the home extension tables defined in the PNP.

There may be applications and configurations that prefer this type of digit routing and information to allow feature access and processing. This type of strategy retains the legacy extension format that traditional PABX systems do-that is, the maximum length of the extension field entering the home extension table must be between 3 and 8 digits.

Regardless of the digit translation done in the PNP PAC and extended through the PNP destination code and location code translation, the extension table only accepts this range of digit lengths to process and normalize to a fully qualified E.164 number, then sends it to the global home DN (Directory Number) table for analysis and EPP (Endpoint Profile) matching. This method allows the inclusion of an optional component, the location code, if manipulation of digits and locations is necessary when either of the following occurs:

- The subscriber home DN does not match the DID (Direct Inward Dialing) number provided by the PSTN (Public Switched Telephone Network).
- The digits dialed by a subscriber, based on location requirements, do not allow easy translation via the PNP PAC alone.

When this option is implemented, it allows digits received by the PNP PAC to match with a PNP destination code, then proceed to a location code table where the digits can be translated further, as required, before entering the PNP Extension table for normalization and extension to the home DN table containing the EPP for the dialed subscriber. Without this optional component, the routing proceeds from the PNP PAC, to the PNP destination code, then directly to the PNP extension table where it is normalized to the full E.164 address necessary to route the digits to the Home DN for a match and EPP information on the dialed party.

6.2.33 Subscriber Routing Options - Extension Dialing via PNP (Private Numbering Plan) and GNP (Global Numbering Plan)

Extension dialing via the PNP (Private Numbering Plan) and extension to the GNP (Global Numbering Plan) tables allows extension based dialing to be routed to a globally usable set of entries for all BG (Business Groups) and PNPs, to include globally defined gateways/endpoints.

While it uses the PAC (Prefix Access Code) prefix type of Extension Dialing to mark this call type as extension-to-extension calling, it does not leverage the home extension tables or optional location code defined within a PNP. Instead, it sends the digits to the GNP PAC with an NoA (Nature of Access) of Unknown and E.164 destination selected, so that it can be processed and routed via global tables. The selection of the Extension Dialing PAC prefix type, rather than On-Net Access, does the following:

- Permits the potential support of external application and routing scenarios that require this information type
- Future-proofs the calling in the event that on-net access later takes on properties that conflict with the proper operation of extension-based dialing that leverages global tables versus private table entries within a PNP.

This method requires the definition of a PNP PAC that is used to send digits to a GNP PAC that can further provide translations, but most specifically to change the NOA to the required type that allows a match to the home DN (Directory Number) tables. From the GNP PAC, the digits are processed by the Global E.164 Code table, and sent to the proper home DN table required to match to a subscriber's record and access the EP (Endpoint) profile for the dialed SIP device/EP. If properly configured, these entries can potentially be used to process incoming gateway/EP calls that also wish to reach subscribers via global routing tables when the gateway is defined in the GNP or even if they are defined in a BGs PNP.

6.2.34 Subscriber Routing Options- Home DN (Directory Number) Dialing via PNP (Private Numbering Plan)

Home DN (Directory Number) dialing via the PNP (Private Numbering Plan) allows digit-based dialing between subscribers to be kept and controlled within the logical confines of the PNP in which the calling subscriber is defined.

It can be used to process calls both within a PNP, between PNPs in the same BG (Business Group), and even between BG defined in OpenScape Voice.

This type of dialing mirrors the configuration of routing strategies for calls made to external gateways/endpoints, and does not leverage the usage of the PNP location codes and extension tables. Instead, it allows an extremely quick and minimal configuration to simply route the calls to the proper home DN table without any retention of extension-to-extension dialing mechanisms that may be required by external applications and endpoints.

Use of this method require a PNP PAC (Prefix Access Code) to be defined for the digits that a subscriber must dial; then, required translations are performed that are necessary to normalize the digits to access the proper home DN table. This includes setting the NoA (Nature of Access) to the proper setting (International, National, and so on) that carries forward into the destination code table of the PNP. From the PNP PAC, the now normalized digits are sent directly to a PNP destination code that forwards them immediately to the global Home DN table for the subscriber dialed.

6.2.35 Subscriber Routing Options - Home DN (Directory Number) Dialing via PNP (Private Numbering Plan) and GNP (Global Numbering Plan)

Home DN (Directory Number) dialing via the PNP (Private Numbering Plan) and extension to the GNP (Global Numbering Plan) tables allows digit-based dialing to be routed to a globally usable set of entries for all business groups and PNPs, to include globally defined gateways/endpoints.

Like home DN dialing via PNP, it does not leverage any of the extension-based services of the PNP (location code and extension tables), providing a quick and minimal set of entries in the PNP and extending them to be further processed in the GNP tables that mirror the configuration of routing strategies for external gateways/endpoints. It can be used to process calls both within a PNP, between PNPs in the same business group, and even between business groups defined in the OpenScape Voice, as it uses the global tables accessible to all OpenScape Voice business groups and PNPs.

This strategy uses the PAC (Prefix Access Code) prefix type of On-Net Access or Off-Net Access to mark this call type as digit-based calling, and sends the digits to a GNP PAC with an NOA (Nature of Access) of Unknown and E.164 destination selected, so that it can be processed and routed via global tables.

This method requires the definition of a PNP PAC that is used to send digits to a GNP PAC that can further provide translations, but most specifically to change the NOA to the required type that will allow a match to the Home DN tables. From the GNP PAC, the digits are processed by the Global E.164 Code table, then sent to the proper Home DN table required.

6.2.36 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 OpenScape Voice

Assistant navigation bar. Routing areas are sometimes referred to as rate areas, a term commonly used in the public network.

Each subscriber endpoint can be assigned a **Classes of Service** and **Routing Area**.

- The **Routing Area** is normally used to indicate the physical location of the endpoint, especially within installations where OpenScape Voice subscribers are located at multiple geographic sites.
- **Classes 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 **source-based routing** (location-specific routing) configurations, department-specific, and/or prioritized call routing arrangements within a single 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.

6.2.37 Routing Areas

A routing area is created in order to define the Office Codes associated with specific geographical locations within a specific area.

The Routing Area is used to describe the location of subscribers for call routing purposes, e.g. to use the right gateway for routing a call.

A new Routing Area is created in order to define the office codes associated with specific geographical locations within a specific area. Once the subscriber has created a routing area, the subscriber can assign it to TKGs (Trunk Groups) and to E.164 Codes. Then the subscriber can use the routing areas in different translation tables to enable correct routing.

During creation or modification of a Routing Area, it is possible to add one or more Office Codes. Please note that the office codes entered here are only for documentation purposes to indicate that this routing area is related to these office codes.

Routing Area name is a string of characters, which means that the names of Routing Areas can begin with either a letter or a digit.

Related concepts

Please select the appropriate help topic on page 657

6.2.38 Classes of Service

CoS (Classes of Service) are used to control the access rights/permissions of E.164 Destination Codes.

The subscriber creates Classes of Service to identify service properties associated with the line and intersystem facilities. When you create a CoS (Class of Service), you specify the following properties:

- Class of Service name
- Default CPC CoS - the default Class of Service for a subscriber

NOTICE:

The default Class of Service can’t be renamed nor deleted

Once the craft person has created a set of Classes of Services, he/she can assign the Classes of Service to subscribers and E.164 Codes.

There is only one Predefined Class of Service which is **OpenScapeApp** . This service copies the Request-URI in the TO header on an outgoing request.

Subscribers and Endpoints:

The **COS (Class of Service)** is used to classify subscribers or endpoints as belonging to a special type. The OpenScape Voice is preconfigured with the following COS: FGDIN, Hospital, Hotel, OpenScapeApp, OptrScreenReq, Ordinary, Payphone, Prison.

Besides being able to choose any of these predefined COS’s, others can be created. Usually, they are assigned to subscribers to control their calling capabilities based on subscriber characteristics, such as boss, clerk, etc.

The administrator can then create separate rules for the subscribers that have these COS assigned.

NOTICE:

The usage of COS for toll restriction purposes is not recommended as there are no interactions between this configuration and features like speed dial. The COS is assigned statically to the subscriber or endpoint and there is no way of switching the COS based on a PIN or time.

Related concepts

Please select the appropriate help topic on page 657

6.2.39 Calling Locations

Calling Locations can be assigned to a subscriber or an endpoint to indicate the geographic location of that subscriber. Calling Locations are used when specific routing has to be done for these subscribers or endpoints. They can be used to have specific geographic routing of an emergency service or a directory service number. Other solutions are available for the emergency service because of DLS mobility, as it must be a truly local service, regardless of the subscriber’s static home location configuration.

The configuration of the Calling Locations parameters (name and corresponding location code) is completely administered via the OpenScape Voice Assistant on a switch-wide level.

Requirements

Subscribers must ensure that all calling locations are provisioned as E.164 codes: calls from calling locations that are not provisioned as E.164 codes may not be routable.

Emergency calls from another switch cannot be routed based on the calling location because the subscriber's location is not passed to OpenScape Voice.

Related concepts

Please select the appropriate help topic on page 657

6.2.40 Classes of Restriction

The predefined Classes of Restriction are used to make a decision on whether to disallow the call or to request an authorization code before allowing the call to go through, request an Account Code before the call goes through(if system is set to post-dial Account Code) or to restrict Call Forwarding to pertinent targets.

It is possible to create Classes of Restriction where combinations of generic traffic types can be recorded with a mnemonic name. The class of restriction can then be assigned to system-wide Call Forwarding Restrictions, system-wide post-dial Account Codes, to the subscriber's or endpoint's Toll Restriction service, the subscriber's Call Forward Restriction service and the subscriber's Authorization Code service.

NOTICE:

Only generic traffic types can be selected in a class of restriction (i.e. the Emergency traffic type is not offered and therefore cannot be selected)

A class of restriction contains a bitmap of up to 127 generic traffic types. Any renaming or deletion must take into account any potential default class of restriction put in place for Call Forwarding or post-dial Account Code.

System-wide Feature Settings

For Call Forwarding Restrictions and post-dial Account Codes, a system-wide class of restriction can be entered that specifies the traffic types that are restricted per default. When clicking on Feature Settings a pop-up is shown that shows the current system-wide feature settings

The feature Call Forwarding Restrictions shows up as a tab and will allow modification of the default class of restriction for Call Forwarding Restrictions as well as the new default setting for restricting call forwarding to destinations that are marked with the Emergency traffic type. An extension button allows you entering a different class of restriction as the default class of restriction for Call Forwarding Restrictions. A **Clear** button allows you to have no Class of Restriction set.

The feature (post-dial) Account Codes shows up as a tab and will allow modification of the default class of restriction that will prompt for an Account Code, if the subscriber has the Account Code service set. An extension button allows you to enter a different class of restriction as the default class of restriction for Account Codes. A **Clear** button allows you to have no Class of Restriction set.

Functional Sequence

1) To assign restrictions to the subscribers, classes of restrictions are created that can then be assigned to the toll restriction, post-dial account codes, authorization codes and call forwarding restrictions services. When controlling the PSTN access for subscribers, the administrator can restrict any of the generic traffic types that are defined. The emergency traffic type is treated especially because it cannot be assigned in the toll restriction service.
2) After creating a class of restriction it can be assigned to the subscriber for the toll restriction service, the authorization service and the call forwarding restriction service. A class of restriction can also be assigned to an endpoint's toll restriction service. A default class of restriction can be assigned for call forwarding restriction and post-dial account code service.

Related concepts

Business Group Authorization Codes on page 143
Toll and Call Restrictions on page 140
Account Codes on page 147
Call Forwarding Restrictions on page 301
Authorization Codes Group on page 353

6.2.41 Traffic Types

A Traffic Type identifies the type of call, e.g. national, international, etc. Optional (defaults to UNDEFINED or NONE). This is used to set the callType value which is passed to UCE and Services component. Many services, e.g. toll restriction, Auth Code, and Call forwarding restriction make use of the callType returned by XLA. The emergency call type is used by UCE to allow the call even if the user is not authenticated or allowed to make any calls.

Traffic Type ID

“Traffic Type ID” is a standard CDR field of type INT. Its default value is null (0). Possible values for this field are 1 to 128.

The ID of the traffic type is associated with the destination code or code index of the dialed destination.

Traffic Types

Current hard-coded Traffic Types

The OpenScape Voice database initially contains the 8 traffic types. Additional traffic types can be created by an administrator and can then be used on destination codes and code index tables of translation. Traffic types can be administrated on the system level.

The default database contains the following 9 traffic types:

- International
- National
- Local

- Toll Free
- Emergency
- Public Operator
- Directory Assistance
- Destination Code Control (DCC)

  This Traffic Type reduces calls to a specific area or location that has been temporarily designated as "difficult to reach" due to circumstances.
- Malicious Call Trace (MCT)

  This Traffic Type indicates that a destination code collects MCT data, has the name TTMCT and ID 20.

Any of the following old hard-coded traffic types will be visible only if they were previously used.

- **Local**

  Traffic type to indicate a destination code is used for local calls.

  NOTICE:

  Used by TRS & AC services
- **National**

  Traffic type to indicate a destination code is used for national (aka long distance) calls.

  NOTICE:

  Applies only to ETSI markets.
- **International**

  Traffic type to indicate a destination code is used for international calls.

  NOTICE:

  Applies to ANSI, ITU and China markets.
- **InterLATA**

  A call that is placed within one LATA (Local Access Transport Area) and received in a different LATA. These calls are carried by a long distance company and used to specify national long distance calls.
- **IntraLATA**

  These are calls that originate and terminate in the same Local Access Transport Area (LATA), but still require a 1 + in order to complete them. They are used to specify an extended or local toll calls area.

  NOTICE:

  IntraLATA call (IXC/LEC/CONSLD, PSTN) applies to ANSI and ITU market
- **International World Zone 1**

  Traffic type to indicate a destination code is used for international calls to other countries in the North American Numbering Plan. If the OpenScape

Voice is not administered for a country that participates in the North American Numbering Plan, this traffic type can be used as a generic traffic type for e.g. calls to cellular phones.

- **Long Distance Directory Assistance**

  Generic traffic type for e.g. calls to an extended calling area (NANP) or calls to a neighboring country.

- **Directory Assistance 411**

  These calls typically incur a flat fee charge.

  > **NOTICE:**
  >
  > Subscriber must be allowed to dial the public operator for assistance.

- **Directory Assistance Home NPA**

  Dir. Assist. Home NPA — Home Numbering Plan area for example,555-1212 for North American Numbering Plan.

  > **NOTICE:**
  >
  > Applies to ANSI and ITU market. The subscriber must be allowed to dial the public operator within his own zone, determined by the subscribers NPA.

- **Directory Assistance Foreign NPA**

  Dir. Assist. Foreign NPA — foreign numbering plan area (FNPA) for example NPA-555-1212.

  > **NOTICE:**
  >
  > Applies to ANSI and ITU market. The subscriber must be allowed to dial the public operator outside of his own zone

- **Toll Free Service**

  Toll free calls are calls that are free of charge.

  > **NOTICE:**
  >
  > Subscriber must be allowed to dial toll-free services.

- **Emergency**

  Emergency calls.

  > **NOTICE:**
  >
  > Applies to all markets.

Traffic Type Variants

There exist two variants for the traffic types:

- Emergency traffic type
- Generic traffic type

Instead of the current 14 hard-coded traffic types, translation allows selecting any of the configurable traffic types at the destination codes, E164 Codes or Code Index level.

The service data manager offers the capability to create up to 127 generic traffic types

NOTICE:

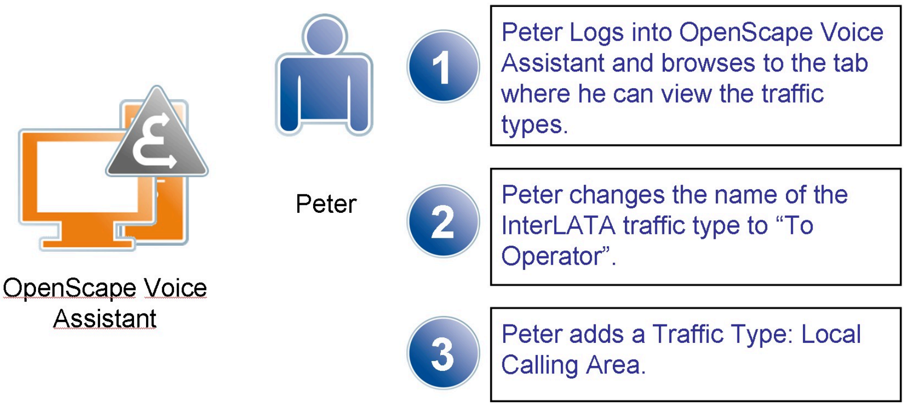
The Emergency Traffic Type is a special non-generic traffic type. It can never be deleted nor it is possible to add or delete additional Emergency variant traffic types. Only renaming is allowed.

Functional Sequence

1) The administrator selects either one of the predefined 14 traffic types or adds a new traffic type. The administrator is allowed to change any of the names, can add more traffic types or can remove unused traffic types (except the Emergency Traffic Type).

NOTICE:

The OpenScape Voice Assistant displays a combination of the current 14 existing traffic types (e.g. Emergency, Local, National and International, International WZ1, IntraLATA and InterLATA) - but only those that are actually used by translation or services.



1 Peter Logs into OpenScape Voice Assistant and browses to the tab where he can view the traffic types.

2 Peter changes the name of the InterLATA traffic type to “To Operator”.

3 Peter adds a Traffic Type: Local Calling Area.

Figure 67: Administrator Creates New Traffic Type

2) After having defined a new traffic type the administrator starts using the traffic type on destination codes or code indexes.

Classes of Restriction

The administrator is able to collect traffic types in Classes of Restriction to be used for:

- Toll Restriction Service
- Call Forwarding Restrictions service,
- Account Code Service and the Authorization Codes service

6.2.42 Routing Calling Locations

Calling Locations can be assigned to a subscriber to indicate the geographic location of that subscriber. They are used when specific routing has to be done for these subscribers. They can be used to have specific geographic routing of an emergency service or a directory service number.

System Specific Information

Calling Locations consist of a set of codes provisioned on a switch-wide level.

Each subscriber can be associated with a calling location. During translation (in the GNP, only), an E.164 code can have the destination type “Calling location”. In this case, the Calling Location code associated with the originating subscriber is translated in the destination code table (the Nature of Address is set to 'CALLING_LOCATION).

Other Characteristics

Emergency calls from another switch cannot be routed based on the calling location because the subscriber's location is not passed to OpenScape Voice.

6.2.43 Display Number Modification

The display number modification feature provides administrators the capability to modify the display format of a number (for example, from international to national format) or to add or remove the PNAC (Public/Private Network Address Code) and prefixes to or from the number before it is presented to a user.

Doing so ensures that the digits that appear in the display of the EP (Endpoint) or application (such as OpenScape Desktop PE) represent a dialable number, in the format required to dial back the c partner. Depending on the call and the wishes of the customer, this can be an extension number, national number, international number, and so forth. As applicable, the dialable number can also have prefixes and PNACs prepended to it.

These capabilities are applicable for display numbers for e.g. calling parties, called parties, and connected parties. redirected parties, transferred parties, alerting parties, busy parties and connected parties.

Requirements

In order for OpenScape Voice to be able to transform numbers to dialable numbers, it needs to be fed with information regarding the numbers that are 'in play' in OpenScape Voice.

- It needs to know about network access codes and prefixes used by specific user groups.
- It needs to know the definition of the public and the private numbering plans.
- It needs to know how to normalize a received number.
- It needs to know how to convert a public number to a private number or vice versa a private number to a public number.
- It needs to know what type of number needs to be shown when presenting a user's number to another user. Users can be external (in the public network) or internal (in the private network)

For this purpose an administrator can populate the following six tables in OpenScape Voice:

- Display Number Prefixes table
- Display Number Definitions table
- Display Number Conversions table
- Display Number Normalizations table
- Display Number Modification table
- Display Number Local Toll table

6.2.43.1 Display Number Modification Concept

OpenScape Voice supports modification of presentation numbers. All numbers which are sent out by the OpenScape Voice are provided either by Translation or by Display Number Modification. Display Number Modification is responsible to provide all numbers which are used for presentation purposes (e.g. calling number, alerting number, connected number, forwarding number).

Presentation Numbers and Dialed Numbers

Presentation Numbers can be calling party numbers, connected party numbers, busy party numbers, alerting party numbers, etc. The only other numbers OpenScape Voice supports next to the presentation numbers are called party numbers. Called party numbers (or also dialed numbers) are the number strings that are dialed by a user in order to reach another user.

Dialed Numbers may be of implicit nature (means that the type of number dialed is conveyed in prefixes pre-pended to the called party's number) or explicit nature (means that the type of number dialed is already known through some other means).

A dialed number string becomes a 'dialable number' string only after OpenScape Voice's translation engine determined that the dialed number string leads to a valid destination be it a Home DN or an external user in a private or public network.

Use of Display Number Modification

The purpose of number modification is to present received presentation numbers in 'dialable' format to the partner of the call. Per definition when a party receives a dialable number, that dialable number can be used as the dialed string when the called party wants to call the calling party.

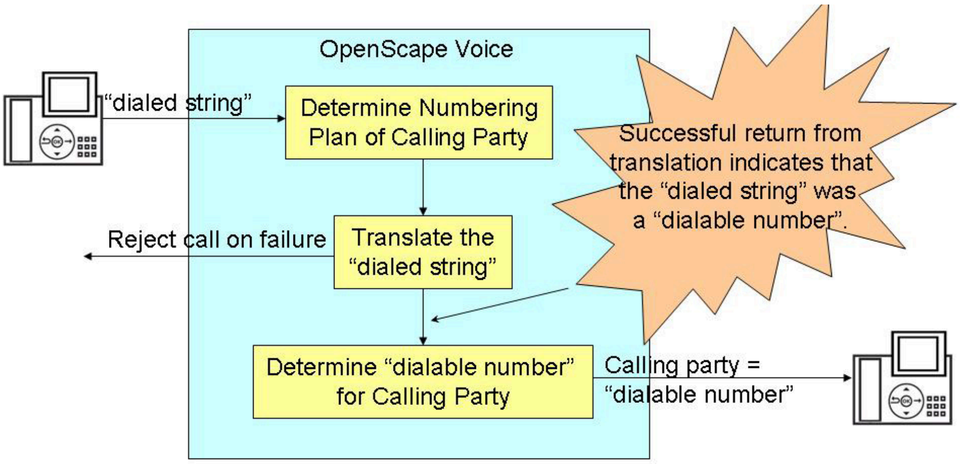

OpenScape Voice
"dialed string"
Determine Numbering Plan of Calling Party
Reject call on failure
Translate the "dialed string"
Successful return from translation indicates that the "dialed string" was a "dialable number".
Determine "dialable number" for Calling Party
Calling party = "dialable number"

Figure 68: Dialable Number

Presenting numbers in dialable format is especially useful for call logs and journals, but it just makes sense to display numbers in a consistent way to users and most users would expect to see a dialable number on their display.

Another use for number modification is for applications and gateways that expect normalized numbers. This normalization can be seen as a special case of creating a dialable number as the application or gateway would expect to receive all dialable numbers in normalized format. Per definition a normalized number of the E164 numbering scheme is an international number. The normalization level of a number of a private numbering scheme depends on what type of private numbering scheme is in effect, but the normalized number is always the highest level number that is applicable in the private numbering scheme (L2, L1 or L0).

The CSTA interface provided by OpenScape Voice uses normalized numbers as device identifiers. Because it only transports implicit numbers, it sends all normalized numbers of the public numbering scheme in Global Number Format (GNF). A GNF number is an international public number preceded by a '+'.

Definitions

Public Numbering Scheme

It defines 3 types of numbers

- subscriber numbers
- national numbers
- international numbers

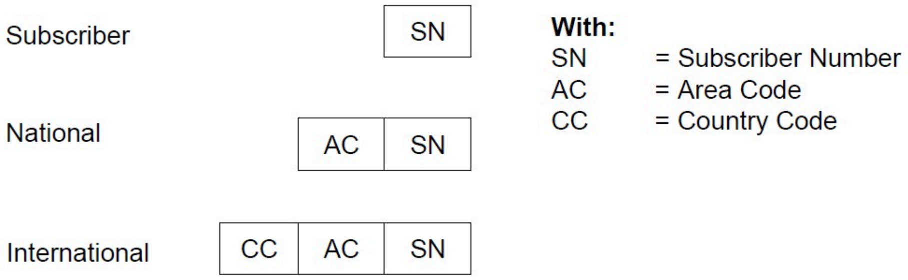


Figure 69: Public (E.164) Numbering scheme

Within the public numbering scheme, the country code is mandatory. For each country a national authority may define whether it supports:

- national numbers and local numbers
- only national numbers
- only subscriber numbers

Private Numbering Scheme

It defines 3 types of numbers

- Local numbers
- Regional numbers
- Complete numbers

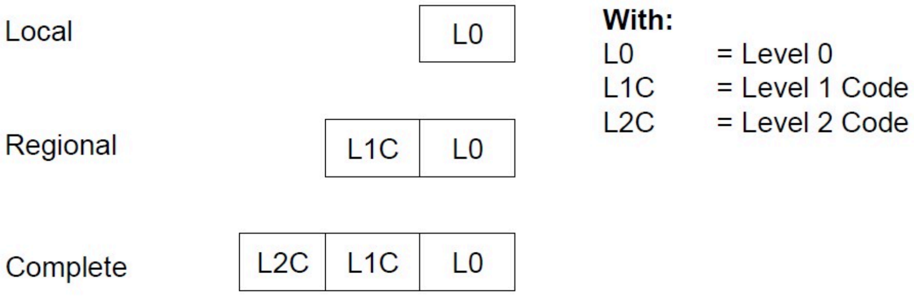


Figure 70: Private Numbering Scheme

Structure of Numbers

Depending upon the customer's wishes, 3 kinds of private numbering schemes can be distinguished:

- L0 private numbering scheme: no L1 or L2 level numbers exist in this type of numbering scheme. Normalized numbers are L0 numbers
- L1 private numbering scheme: no L2 level numbers exist in this type of numbering scheme. Normalized numbers are L1 numbers.
- L2 private numbering scheme: Normalized numbers are L2 numbers

A private numbering scheme administrator should define an L1 code for each L2 private numbering scheme number. This means that for an L2 private numbering scheme, all numbers within the private numbering scheme must have an L2 code and an L1 code defined. Equally so, for an L1 private numbering scheme, all numbers within the private numbering scheme must have an L1 code defined.

Extensions

OpenScape Voice supports dialing numbers for subscribers that are shorter than the numbers defined within the public or the private numbering schemes. These short numbers are called extensions and they must be the trailing part of either the subscriber number (public numbering scheme) or the local number (private numbering scheme).

Prefixes

Because most telephones use implicit dialing, the telephone user must indicate which type of number he/she is dialing by possibly entering a prefix before dialing a number out of a numbering scheme.

The prefixes for the public numbering scheme are defined by the operator providing access to the public network. Typically operators do not require dialing a prefix for subscriber numbers, but do require dialing a national prefix for national numbers and an international prefix for international numbers. E.g. the American public network operators chose '1' as the national prefix and '011' as the international prefix, while the German public network operators chose '0' as the national prefix and '00' as the international prefix.

The prefixes for the private numbering scheme are defined by the private numbering scheme administrator. Because extensions are usually seen as the lowest level in a private numbering scheme (although it is not really defined there), prefixes are possible on L0, L1 and L2 level numbers.

Network Access Codes

Network access codes are used within OpenScape Voice to allow telephone users that dial implicit numbers to differentiate between calls made to the public network and calls made within their own private network.

6.2.43.2 Display Number Modification - Specifics

Creating dialable numbers for SIP-Q endpoints

Number Modification is now called for presentation numbers that need to be sent to a SIP-Q endpoint. Up to now this was governed by a system-wide RTP variable `Srx/Main/OutGoingCallingPartyNumberType`. . This RTP variable was removed in order to allow a more flexible way of creating correct presentation numbers for SIP-Q endpoints.

The administrator must define default settings for Number Modification towards SIP-Q endpoints. Depending on how the private network is generally set up, the default system setting for Number Modification is:

- Originating Context: ANY business group, ANY numbering plan
- Terminating Context: ANY business group, ANY numbering plan, ALL-PN endpoints
- If the private network uses fully qualified public numbers:

Table 118: Modification Rules

Input Type Of Number	Priority	Output Type Of Number	Number Source	Optimize Type Of Number
ANY	1	International	Input Number	NONE
ANY	3	International	BG Display Number	NONE

- If the private network uses fully qualified private numbers:

Table 119: Modification Rules

Input Type Of Number	Priority	Output Type Of Number	Number Source	Optimize Type Of Number
ANY	1	International	Input Number	NONE
ANY	2	Extension	Input Number	NONE
ANY	3	International	BG Display Number	NONE

- If the private network uses fully qualified private numbers but expects NPI/TON set to Unknown this can be controlled at the endpoint level via a new attribute (Set NPI/TON to Unknown)

With these rules in mind, more specific business group, numbering plan or even endpoint specific rules can be created that allow some private networking endpoints to receive their presentation numbers in a different format than other private networking endpoints in OpenScape Voice.

NOTICE:

One of above rules must be created by the administrator in order to provide proper support of private networking endpoints.

Display Extension and Number Modification

Before number modification was introduced, the displayed extension configured on the subscribers was used for presentation numbers inside the BG. This configuration option is kept in place for backward compatibility reasons.

It is used in the following 2 situations:

- When Number Modification fails to deliver an output number.
- When the RTP variable `Srx/NDAL/UseDisplayExtensionForTonOutExt` is set to **RtpTrue**, the configured Display Extension is used in all Number Modification Rules that have the Output Type Of Number set to **Extension**.

Optimization to Extension

Normally an optimization to extension will use the rules defined in the Number Definition table to achieve this optimization. However, if the presenter and receiver both are subscribers of the same numbering plan, then the definition of the presenter's number is used to create the extension number, provided a skip is defined (a skip of 0 means that no extension can be created with this number definition).

6.2.43.3 Creating Dialable Numbers

Dialable numbers are created by analyzing a given number and finding a number modification rule that applies to the presenter of the number (from) and the receiver of the number (to).

NOTICE:

In a basic call scenario, OpenScape Voice creates 3 dialable numbers:

- The Calling Party Number presented by the calling party (from) to the called party (to)

- The Alerting Party Number presented by OpenScape Voice on behalf of the called party (from) to the calling party (to) with presented number the result of translation

- The Connected Party Number presented by the called party (from) to the calling party (to)

Requirements

To be able to create a dialable number, the number modification library needs to know

1) **What is the Number that needs to be made dialable?**

   This number could be the number of an OpenScape Voice subscriber or could be a number received on the network interface.

2) **Who offered the number for presentation?**

   In case the number was obtained from an OpenScape Voice subscriber, it was this subscriber who offered the number. In case the number was received on the network interface, the endpoint (gateway, media server, etc.) that sent the number is the one who offered the number. Instead of the subscriber or endpoint, the number modification library expects the numbering plan used by the subscriber or endpoint.

3) **For whom does a dialable number need to be created?** .

   - In case the dialable number is requested for an OpenScape Voice subscriber, it is this subscriber.
   - In case the dialable number is requested for an endpoint (media server, etc.) or a private or public network (gateway) it is the endpoint.

4) **What is the number of the party that wants to receive a dialable number?**

   This can be an OpenScape Voice subscriber's number or in case the dialable number is created for an endpoint it is the endpoint's configured default Home DN or if that's not configured it is the called party number

In order not to overload the tables that contain the rules on how a number between 2 subscribers or between a subscriber and an endpoint or between 2 endpoints is shown, most table's granularity is constrained to the Private Numbering Plans used by the subscribers or endpoints.

NOTICE:

This means that all OpenScape Voice subscribers that use a particular Private Numbering Plan will receive the same treatment from Display Number Modification. It is however possible to create a number modification rule that applies to a specific endpoint.

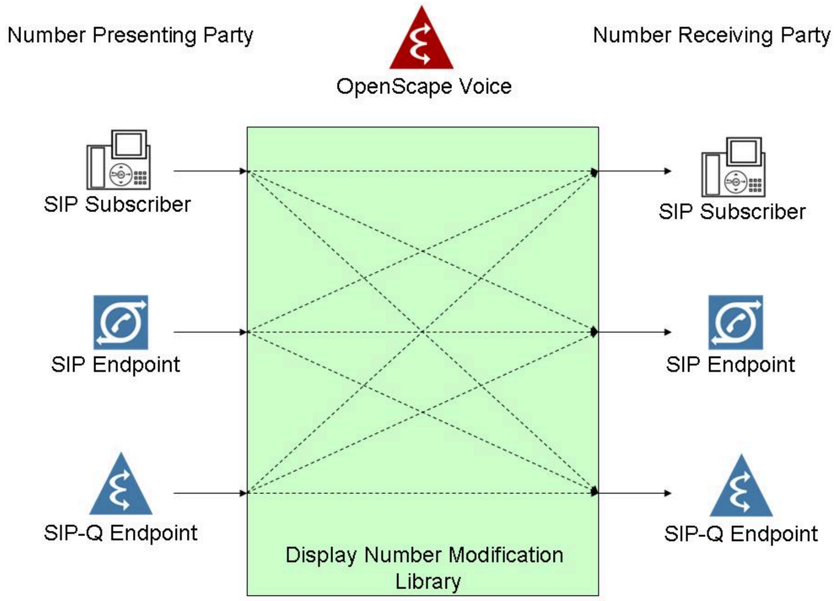


Figure 71: Creating a dialable number using the Number Modification Library

Functional Sequence

There are multiple steps to creating a dialable number and it is very important that a Display Number Modification Library administrator understands the different steps/phases that a presentation number passes through to become a dialable number. Factors taken into consideration by OpenScape Voice are:

- Is the presenter of the number a SIP Subscriber or an endpoint (SIP or SIP-Q)?
- Is the call between the 2 parties an internal or an external call?

This results in 4 basic scenarios:

1) Internal Call where presenter is a SIP subscriber: The number to be presented (input number) is in order of preference:

a) The subscriber's main pilot directory number if configured to use the main pilot directory number as identity for internal calls.

b) The subscriber's directory number.

2) External Call where presenter is a SIP subscriber and receiver is a SIP subscriber: The number to be presented (input number) is in order of preference:

   a) The subscriber's external Caller ID.
   b) The subscriber's main pilot directory number if configured to use the main pilot directory number as identity for external calls.
   c) The subscriber's directory number if it is a public number.
   d) The subscriber's business group's display number.

3) External Call where presenter is a SIP subscriber and receiver is an endpoint (SIP or SIP-Q): The number to be presented (input number) is in order of preference:

   a) The subscriber's external Caller ID.
   b) The subscriber's main pilot directory number if configured to use the main pilot directory number as identity for external calls.
   c) The subscriber's directory number if it is a public number.
   d) The receiver's Default Home Directory Number.
   e) The subscriber's business group's display number.

4) For a call where the presenter is an endpoint (SIP or SIP-Q) The number to be presented (input number) is in order of preference:

   a) The normalized form of the number received from the endpoint (calling party number, connected party number, etc) or the normalized form of the translation result (called party number)
   b) The number received from the endpoint (calling party number, connected party number, etc) or the translation result (called party number)

NOTICE:

OSV will consider the APN (additional party number) information, when included in the ingress SIP-Q Setup Message, to present the actual calling party when the call terminates at an external SIP endpoint/subscriber.

For a call from a SIP-Q endpoint to an internal SIP endpoint/ subscriber the OSV will use the calling party number provided by the ingress SIP-Q Setup Message.

Regarding the definitions of internal and external calls, see chapter Determine if a call is Internal or External

To get the dialable number for any of the above determined numbers, the Number Modification Library does as follows:

- In a first step the presented number is evaluated to determine the type of the number.
- Once the type of number is determined, the best matching Modifications table entry is searched in the Display Number Modification library based on the presenting (from) and the receiving (to) party's context information.
- When found, the modification rule of the entry determines what happens next.
- If the found modification rule fails, OpenScape Voice will keep searching for a match in lower priority Modifications table entries that still match the presenting (from) and receiving (to) party's context information.

Determining the Type Of Number

The general flow for determining the Type of Number for a number for an endpoint is as follows:

- Unless the Type of Number is already determined to be International or L2, the number normalization table is consulted to find out whether normalization entries apply that may upgrade the number to a fully qualified number. If successful, the normalized number and its Type of Number (International, L2 L1 or L0) is determined.
- If the resulting Type of Number remains Unknown (no entry matches in the number normalization table), the number prefix table is used to check if the type of number can be determined from the leading digits of the input number. If successful, the leading digits are stripped from the number and the Type of Number is determined.
- If the resulting Type of Number is still Unknown (no entry matches in the number prefixes table) then a lookup is done - mostly for backward compatibility reasons - in the number definition table to see whether a match there could resolve the Type of Number.

NOTICE:

The result of getting the type of number of a number presented by an endpoint not only determines the Type of the presented Number, it also may change the number to its normalized format.

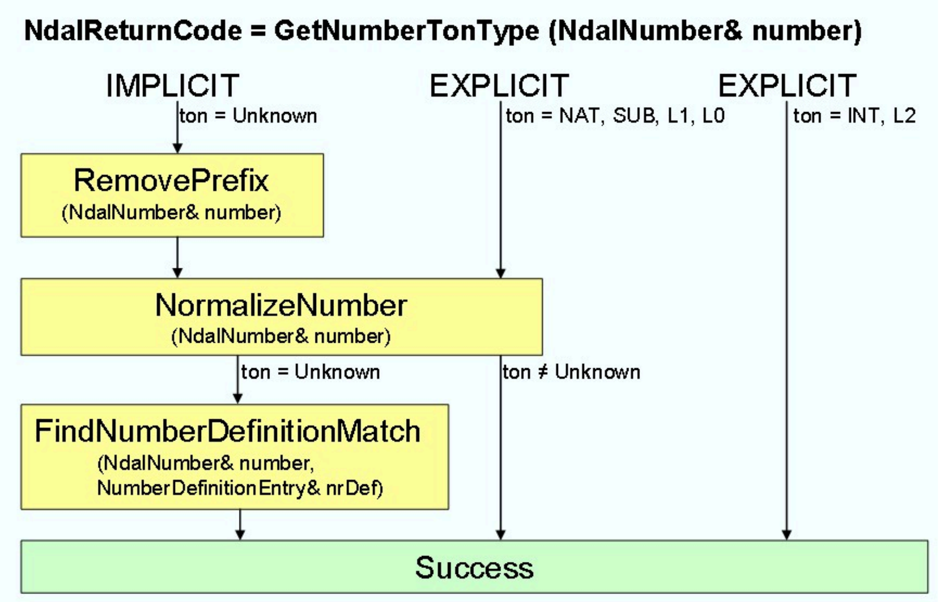


Figure 72: Determining the Type of Number for a Number from an endpoint

The general flow for determining the Type of Number for a number of a subscriber (Home DN) is as follows:

- If the Type of Number is Unknown, a lookup is done in the number definition table to see whether a match there could resolve the Type of Number

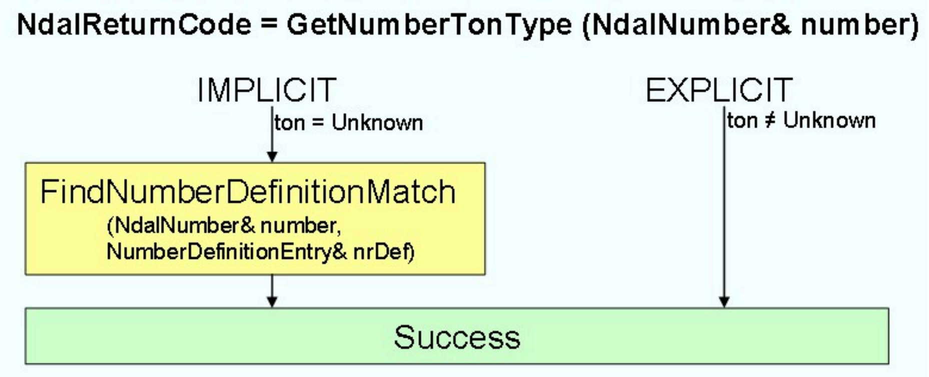

NdalReturnCode = GetNumberTonType (NdalNumber& number)
IMPLICIT
ton = Unknown
EXPLICIT
ton ≠ Unknown
FindNumberDefinitionMatch
(NdalNumber& number,
NumberDefinitionEntry& nrDef)
Success

Figure 73: Determining the Type of Number for a SIP subscriber

Because of the above, it is strongly recommended to enter the number definitions for all office codes used in the OpenScape Voice. Normally, system-wide number definitions can be entered for each public office code and business group specific number definitions can be entered for each private office code. In case of hosted scenarios, public office codes (if shared among multiple business groups) may result in business group specific number definitions as well.

Criteria for Finding a Matching Number Modification Entry

To find a match in the Modifications table of the Display Number Modification library, the context of the number presenter (from) and number receiver (to) and the determined type of number of the presented number are matched against the entries in the Modifications library.

To guarantee a consistent result the entries in the Modifications table are ordered. The following factors determine the priority with which an entry in the number modifications table is looked at (from highest to lowest):

- Rules where the receiver (to) is a specific endpoint.
- Rules where the receiver (to) is a private networking endpoint (SIP or SIP-Q) (ALL-PN).
- Rules where the receiver (to) is an endpoint (ALL).

Within each of these 4 categories, the following priorities are assigned to the receiver's group membership:

- Rules where the receiver (to) uses a specific numbering plan.
- Rules where the receiver (to) belongs to a specific business group (ANY numbering plan).
- Rules where no business group is specified for the receiver (to) (ANY numbering plan of ANY business group).

Within each of these 3 subcategories, the following priorities are assigned to the presenter's group membership:

- Rules where the presenter (from) uses a specific numbering plan.
- Rules where the presenter (from) belongs to a specific business group (ANY numbering plan)
- Rules where no business group is specified for the presenter (from) (ANY numbering plan of ANY business group)

Within each of these 3 subcategories, the following priorities are assigned to the type of number of the presented number (input TON):

- Rules where the input TON is defined (International, National, Subscriber, L2, L1 or L0).
- Rules where the input TON is not defined (ANY)

And finally, within each of these 2 subcategories, the priorities of the Modifications table entry are taken into account (1 - 4).

NOTICE:

The OpenScape Voice Assistant will display the Number Modification rules in the above order when entering the Number Modifications overview screen.

6.2.43.4 Creating Normalized Numbers

Normalized numbers are created for CSTA and also for requests that come in on the SOAP interface. An administrator can force sending normalized numbers on the SIP network interface by setting the **Send Uri in Telephone Subscriber Format** attribute on the SIP endpoint representing the gateway or media server to which normalized numbers need to be sent.

Creating a Normalized Number - General

CSTA always tries to send GNF numbers or fully qualified private numbers to the CSTA applications. A GNF number is a '+' followed by a fully qualified public number.

Functional Sequence

There are multiple steps to creating a normalized number:

1) First the Type of Number of the number to be normalized is determined.

  a) If the Type of Number remains unknown, the normalized form of the number cannot be obtained.

  b) If the Type of Number is International or L2, the number is successfully normalized.

  c) If the Type of Number is National or Subscriber, the Definitions table entry that matches the number is used to normalize the number to an International number. If no Definitions table entry is found or the entry cannot be used to create an International number, the normalized form of the number cannot be obtained.

  d) If the Type of Number is L1 or L0, the Definitions table entry that matches the number is used to normalize the number to an L2, L1 or L0 number. If no Definitions table entry is found, the number is assumed to have the normalized form.

2) The GNF number is then obtained by pre-pending a '+' in front of an international (public) number.

Creating a Normalized Number - for SOAP

SOAP may also be used to request the normalized number of a dialed string. This interface is used by OpenScape UC Application when one creates a preferred device on the OpenScape Desktop Client, but it is also used in some other OpenScape UC related applications such as the voice portal.

In order to do a successful number normalization of a dialed string, the SOAP interface needs to provide all input information. As this interface is mainly used by the OpenScape UC, it was chosen to use the subscriber number (Home Directory Number) of the requesting party to find the private numbering plan in which the dialed string needs to be translated.

In the case of creating a preferred device for the OpenScape Desktop Client, this is the subscriber number of the OpenScape Desktop Client.

Creating the normalized number for SOAP involves 3 basic steps:

1) Obtain the private numbering plan of the requesting party. The requesting party must be a subscriber on OpenScape Voice to which the SOAP request for dialed number normalization is made. The subscriber is looked up and the subscriber's numbering plan is obtained. A normalized number can only be returned if the requestor is a subscriber configured on OpenScape Voice.

2) Ensure that the dialed string is a 'dialable number' by translating the dialed string. A normalized number can only be returned if translation of the dialed string is successful and leads to another subscriber or an endpoint (gateway, media server, etc.). If the translation result leads to a subscriber, the subscriber's number will be used. The type of number will be one of:

- International
- National
- L2
- L1
- L0

If the translation result leads to an endpoint, the number and type of number used for the normalization depend on the provisioned translation tables (Destination Codes and Routes table) as shown in the following table:

Table 120: Obtain Number and Type of Number for endpoints

Translation Result	1) Modified digits and Nature of Address as input to the destination codes table	2) Modified digits and Nature of Address after the Routes table (only provided if there are insertions or deletions)	Use
Subscriber	International / National / L2 / L1 / L0	N/A	1)
ENDPOINT	UNKNOWN	UNKNOWN / Undefined	1)
		International / National / Subscriber / L2 / L1 / L0 / PNP Extension	2)

Translation Result	1) Modified digits and Nature of Address as input to the destination codes table	2) Modified digits and Nature of Address after the Routes table (only provided if there are insertions or deletions)	Use
	International / National / Subscriber / L2 / L1 / L0 / PNP Extension	Don't care	1)

3) Normalize the number using the translation result. For this normalization, the private numbering plan of the translation result is used rather than the private numbering plan of the requesting party.

NOTICE:

If the translation result is PNP Extension, step 3 is skipped and the extension is returned as the normalized number.

6.2.43.5 XLA Endpoints Table - Default Home DN

To support creating Modifications table rules where a default Home DN of an endpoint is chosen over the input number to be presented to an endpoint, the endpoints table needs to allow provisioning a default Home DN.

The Default Home DN is used in 2 ways:

- First to be able to provide a public number to a gateway when either no public number can be created (subscriber only has a private number) or the public number that would be presented is not in the range of DNs that the public operator expects to receive.
- Second to be able to provide a correct definition when creating a calling party number to be sent to a public gateway. By using the Default Home DN's Definitions table entry instead of the translated number's Definitions table entry (which may and should not even exist as it is NOT a number known to OpenScape Voice), the Display Number Modification library can optimize the calling party number correctly based on the Definitions table entry matching the default Home DN.

  Example: if a subscriber makes an international call via a local gateway, then the calling party number to be provided to the gateway should still be in local or national number format.

6.2.43.6 XLA Endpoints Table - Send Unknown Numbers

It is possible to record on the SIP-Q endpoint that numbers need to be sent with Numbering Plan Identifier and Type of Number **Unknown**.

6.2.43.7 Filtered BG-specific View on DNM Tables

The OpenScape Voice Assistant allows the administration of the Display Number Modification tables from the Business Groups tab. This is mainly to support hosted scenarios.

An administrator can make modifications to these Display Number Modification tables with the following restrictions:

DNM Prefixes, Definitions, Normalizations, Conversions and DNM Local Toll Tables:

- In the overview section all rules are shown that are applicable to this BG and all system wide rules. Only the BG specific rules can be modified. The system wide rules are shown for informational purposes only. Only BG specific rules can be created.

DNM Modification Tables:

- In the overview section all rules are shown where this BG is shown in the terminating context setting section and all system wide rules of the terminating context setting (where BG is **ANY**). Only the BG specific rules can be modified. The system wide rules are shown for informational purposes only. Only BG specific rules can be created. The names of business groups and numbering plans, that the administrator is not allowed to see, are anonymized data. It is allowed to delete or modify an anonymized entry as these entries will only affect the displays of endpoints of the own business group..

6.2.44 DNM Prefixes Table

This table specifies the network access codes and prefixes that are defined for a specific numbering plan, a specific business group or system wide. The display number prefixes table allows an administrator to enter the prefixes for the public and the private numbering plan.

The International, National, Subscriber, L2, L1 and L0 columns in the DNM Prefixes overview pane show the combination of Public/Private Network access code (PNAC) and prefix defined for a type of number as follows: <PNAC>-<Prefix>. Depending on the availability of <PNAC> and <Prefix> this is:

Table 121: Showing PNAC and Prefix in the DNM Prefixes Overview

PNAC	Prefix	Show
Yes	Yes	PNAC-Prefix
Yes	No	PNAC-
No	Yes	-Prefix

It is possible to filter on Business Group Name and Numbering Plan Name.

NOTICE:

If the DNM Prefixes overview is shown from within the business group tab of the OpenScape Voice Assistant; then only the system wide entries and the entries specific to the administered business group are shown in the overview.

Requirements

- Table granularity: numbering plan level.
- This table assumes that all subscribers and endpoints using a specific numbering plan use the same prefixes.
- Business group-specific entries can be defined by creating a Prefixes table entry for that specific business group and the 'ANY' numbering plan.
- System-wide entries can be defined by creating a Prefixes table entry for **ANY** business group and **ANY** numbering plan.

NOTICE:

It is highly recommended to provide all prefixes and network access codes for all possible types of numbers.

The DNM Prefixes table is used in 2 situations:

- To find the **type of number** of a number with unknown type of number by finding a matching number prefix rule for it. With the matching rule, the type of number is known and the prefix can be stripped from the unknown number.
- To find the prefix given a specific type of number.

Matching Rules

- **Type of Number is Unknown**

The algorithm used for finding a match for an **unknown type of number** is a best match (i.e. most digits match) algorithm.

DNM Prefixes table entries specified for a specific numbering plan take precedence over business group specific DNM Prefixes table entries which in turn take precedence over system-wide DNM Prefixes table entries

- International
- L2
- National
- L1
- Subscriber
- L0

In case of a tie on the best match the priorization of the Type of Number is as follows:

Table 122: Number Prefix Rules Priorities for best match ties

1	specific	International
2	specific	L2
3	specific	National
4	specific	L1
5	specific	Subscriber

6	specific	L0
7	ANY	International
8	ANY	L2
9	ANY	National
10	ANY	L1
11	ANY	Subscriber
12	ANY	L0

For each Type of Number an entry is searched for the specified numbering plan and if not available an entry for that Type of Number is searched that applies to 'ANY' numbering plan.

- **Type of Number is known**

For a known type of number, the specific prefix for the type of number is looked up in the DNM Prefixes table for the given numbering plan and returned. If no table entry can be found for the given numbering plan the prefix for the type of number is looked up in the business group specific table entries (with numbering plan ANY for the given business group). If still no table entry could be found, the prefix for the type of number is looked up in the system-wide table entries (with numbering plan **ANY** for **ANY** business group).

6.2.45 DNM Definitions Table

The DNM Definitions table specifies the definitions of numbering schemes that exist within a numbering plan, business group or even system wide. It allows OpenScape Voice to decompose a number from the public or private numbering scheme into the code components.

Requirements

- Table granularity: numbering plan level.
- This table assumes that the same definitions apply to all subscribers and endpoints using a specific numbering plan.
- Business group-specific entries can be defined by creating a Definitions table entry for that specific business group and the 'ANY' numbering plan.
- System-wide entries can be defined by creating a Definitions table entry for 'ANY' business group and 'ANY' numbering plan.

NOTICE:

It is highly recommended to provide system-wide Definitions for all public office codes and business group specific Definitions for all private office codes. Other definitions should not be necessary if the normalizations table is correctly filled out.

System-wide definitions can be defined by creating table entries for the **ANY** numbering plan.

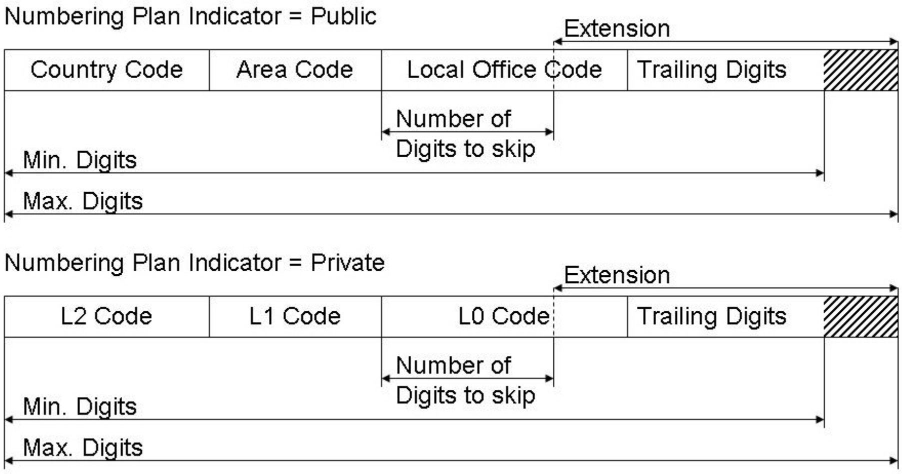


Figure 74: DNM Definitions Number Breakdown

Required content for each component:

The following subsections describe the required content for each component.

Business Group

In the DNM Definitions table, the business group of an entry is entered with one of the following values:

- When business group is **ANY**, the numbering plan must be **ANY** as well.
- When business group is empty, the numbering plan must be **E164NANP**. However, the opposite is not necessarily true: when the numbering plan is E164NANP the business group may or may not be empty.
- When a particular business group is specified, the numbering plan may be **ANY**, **E164NANP** or a numbering plan name belonging to that business group.

Numbering Plan

In the DNM Definitions table, the numbering plan of an entry is entered with one of the following values:

- When numbering plan is **ANY**, the business group may be **ANY** or a specific business group.
- When numbering plan is **E164NANP**, the business group may be empty or a specific business group.
- When a particular Numbering Plan is specified, the business group must be the numbering plan's business group.

NPI (Numbering Plan Indicator)

The **NPI (Numbering Plan Indicator)** column of an entry is used to specify whether the definition is for a private or a public numbering scheme. This is the same identifier that is also supported by ISDN and can have the values Public or Private.

Country/L2 Code

Depending on the value of the Numbering Plan Identifier, this field contains either the Country Code (NPI = Public) or the L2 Code (NPI = Private).

Area/L1 Code

Depending on the value of the Numbering Plan Identifier, this field contains either the Area Code (NPI = Public) or the L1 Code (NPI = Private).

Local/L0 Code

Depending on the value of the Numbering Plan Identifier, this field contains either the Local Office Code (NPI = Public) or the L0 Code (NPI = Private).

Skip (Number of Digits to Skip)

This indicates the numbers of digits to skip in the Local Office Code (NPI = Public) or the L0 Code (NPI = Private) to create an extension.

Min/Max. (Min. Digits/Max. Digits)

This indicates the minimum and maximum number of digits of the Home Directory Numbers of the office codes for which the definition is provided.

Local Toll

The **Local Toll** specifies how public numbers are defined for subscribers with Home Directory Numbers that match this DNM Definitions table entry..

Per default it is assumed that users that have a specific public number actually follow the basic rules that they need to dial local numbers within their own area code, national numbers within their country and international numbers elsewhere. As long as these rules apply, there's no need for a local toll entry on the public number definition. However, if these rules change, as they certainly can in the American market, then the local toll table entry specified on the number definition will be used to find out how a number received from the public network can be optimized to the national or subscriber level for the subscribers of that office code.

There are 2 situations where the local toll table is mandatory:

- When a standalone private office code is created without a number conversion entry that allows the DNM library to find the accompanying public number then the local toll table entry will allow the DNM library to optimize incoming public numbers correctly for these users. E.g. if a branch office has a single access number and all branch office members have private extensions not reachable directly from the public network, then the subscribers of the branch office need to be provisioned with private numbers and the private number definition table entry needs a local toll entry to define the local and national public numbers in the context of the private number subscribers
- When a public office code is created with subscribers that need to dial within split or overlapping area codes. This is the case in e.g. Boca Raton, FL in case the numbers presented to the subscribers need to be in the exact format as specified by the public network.

Matching Rules

The number definition library uses a best match (most digits match) algorithm to find a matching rule.

In case the type of number of the digit string for which a definition is searched is known (one of international, national, subscriber, L2, L1 or L0) each entry in the table is checked for a possible match given that knowledge. The best match (i.e. most digits match) is returned.

In case the type of number of the digit string for which a definition is searched is unknown, the definition table is searched assuming a specific type of number in the following order:

Table 123: Number Definition Rules Priorities for Unknown Numbers

Rule Priority Number	Type of Number assumed	Note
1	International	All entries are searched for a best match on country codes + area codes + local office codes
2	National	All entries are searched for a best match on area codes + local office codes
3	Subscriber	All entries are searched for a best match on local office codes
4	L2	All entries are searched for a best match on L2 codes + L1 codes + L0 codes
5	L1	All entries are searched for a best match on L1 codes + L0 codes
6	L0	All entries are searched for a best match on L0 codes

6.2.46 Display Number Modifications Table

This table defines how an input number is modified from its original form, depending on originating info (BG, NP), terminating info (BG, NP and optionally endpoint). The output type of number may also be specified set for optimization, if desired.

6.2.46.1 Number Modification Rules

Handling of the Output Type Of Number

- The **ANY** Output Type Of Number is only allowed in a number modification rule together with an **ANY** Input Type Of Number. Its meaning is that as a minimum the input Type Of Number needs to be obtained. The following rules apply if optimization is requested in the number modification rule:
- The NORMALIZED Output Type Of Number simply returns the fully qualified form of the Number Source.
- The FQPN Output Type Of Number requires the Number Source to be modified to a fully qualified private number.
- The Extension Output Type Of Number requires the Number Source to be modified to an extension. This is also called a 'forced optimization' and it is subject to the following special rule based on the setting of the RTP variable `Srx/Ndal/DisplayExtensionForTonOutExt:`
  - default value 0 (= don't use the display extension for this forced optimization)
  - value 1 (= use the display extension if available for this forced optimization)

- All other Types of Number force an optimization to the requested Type of Number.

Handling of the Optimize Type Of Number

The following rules apply if optimization is requested in the number modification rule:

- Optimize Type of Number: **None** means that to succeed this modification rule requires the type of number of the input number must be the type of number for the output number. Note that this modification rule may still require the optimization logic to be called because at this point in the logic the input number has been converted to a fully qualified number and the input type of number may not have been a fully qualified number. This is put in place to prevent that with this rule a national number from e.g. Germany would be presented to a subscriber in e.g. the USA.
- Optimize Type of Number: **Extension** means that an optimization to extension is requested. Normal logic of getting dialable numbers applies to continue.
- **For all other optimization requests**: NDAL ensures that the numbering plan identifier of the 'from'-Type Of Number matches the numbering plan identifier of the optimization request. If they match then the normal logic of getting dialable numbers applies to continue. If the numbering plan identifiers differ then the optimization level for this modification rule (as it is a rule that the administrator usually puts in as the ultimate fallback rule) is reset to None before continuing with the logic of getting dialable numbers.

Handling of Inter-BG Numbers

Number Modification will prevent that private numbers are delivered/known outside of the BG. No Inter-BG number modification request (originating and terminating party are in different BGs) will ever generate a private number.

For inter business group rules (where 2 different business group names are specified), the **Output Type Of Number** must be a public Type Of Number: one of **ANY**, International, National, Subscriber or Normalized. Inter business group rules with non-public number outputs will be skipped.

The Number Source field in a number modification rule

The Number Source field has the following possible values:

- **Input Number:** this is the number that was obtained by the OSV using the rules described in the Functional Sequence for Number Modification.
- **Default Home DN:** the Default Home DN number provisioned on the specified endpoint is used instead of the Input Number. This rule can only succeed if the dialable number is created of an endpoint that has a Default Home DN number defined.
- **BG Display Number:** the BG Display Number of the business group of the originating party is used instead of the Input Number. This rule can only succeed if the dialable number is created of a subscriber or endpoint whose business group has a BG Display Number defined.

DNM Modifications Prefix Required Rule/ Prefix Required Flag

The Prefix Required flag can be set to indicate that a prefix should be added by the Number Modification library using the entry in the Number Prefixes table that applies to the terminating party.

Presentation Restricted Flag

The Presentation Restricted flag can be set to indicate that the presentation of the number to the terminating party is not allowed.

6.2.46.2 Creating DNM Modification Rules based on Priority Level

DNM Modification rules are looked at in a very specific order. This order is maintained within the Number Modification library and is roughly as follows:

- The highest priority rules are rules that involve specific endpoints.
- The next highest priority goes to rules that apply to all private networking endpoints (SIP and SIP-Q) (endpoint = ALL-PN)
- Then next highest priority goes to rules that apply to all endpoints (i.e. excluding the subscribers) (endpoint = ALL)
- Lowest priority goes to rules that apply to endpoints and subscribers (endpoint = NONE)

Within each of the above categories, priorities are assigned as follows:

- Specific numbering plan rules have higher priority than business group specific rules
- Business group specific rules have higher priority than system wide rules.
- The terminating context has higher priority than the originating context

Priorities are also assigned to the Input Type Of Number (specific gets higher priority than an ANY rule). Up to 3 ANY Input Type Of Number rules (prioritized 1 to 3) can be specified that take an output type of number that is not ANY. The output type of number ANY automatically receives reserved priority number 4. The priorities 1 to 4 will also apply to the rules with a defined input type of number.

It is not possible to enter 2 modification rules with the same number source field value that only differ on priority.

EXAMPLE

An ANY (input) / INT (output) / 1 (priority) / Input Number (Number Source) rule precludes creating an ANY (input) / INT (output) / 2 (priority) or 3 (priority) / Input Number (Number Source) rule.

NOTICE:

In the OpenScape Voice Assistant, Number Modification rules are shown in order of priority from highest priority to lowest priority. When analyzing a problem in Number Modification, an administrator can then easily find out which rule is not behaving correctly and can then correct the problem.

Fallback Rules

Fallback rules apply when a higher priority rule fails. The number modification library does not necessarily fail anymore when the first or second matching rule does not deliver a result. Instead the next best rule is searched and applied until either no rules are available anymore or a rule ends up into a positive modification.

6.2.46.3 Getting Dialable Numbers

Get Dialable Number is used to provide a dialable display number to a subscriber endpoint or a non-subscriber endpoint. This API returns the 'dialable number' (formatted number) for an input number (i.e. the 'From' number) in the context of the endpoint or subscriber that will receive the dialable number (i.e. the 'To' number).

- from: This is the input number which the caller wants to be formatted by NDAL
- fromExternalCallerId: This field provides a number that can be used by NDAL in lieu of the 'from' number above in case a conversion from private to public must be done and NDAL does not contain the proper number conversion entry to perform this conversion on the 'from' number.
- to: This is the number associated to the endpoint or subscriber that will receive the dialable number. For a subscriber, this is the subscriber's Home DN. For an endpoint, this is either the endpoint's 'Default Home DN' or - if no default Home DN is provisioned - this is the calling/called number provided by the endpoint (or by translation).
- toIsDefaultHomedDn: This flag indicates whether the 'to' number is an endpoint's 'Default Home DN'.

Barring the exceptions described in other section, the general flow for getting a dialable number is then as follows:

- Get Type of Number for the input 'from' number. The result is normally a normalized number (if the normalization tables are populated) or a defined number. The type of number of the 'from' number is now recorded as the TON_IN.
- Find the best matching Number Modification rule, given the input: from, to, and TON_IN. If a rule ends up failing, the next best rule is searched and so forth until there are no more matching rules. If all applicable rules fail, this API returns a failure indication.
- For each found rule
  - The presentation status recorded in the rule is stored in the output number. The number source (Input number, BG Display Number, Default Home DN), TON_OUT (output type of number), the TON_OPT (requested optimization level) and the Prefix required flag are also recorded from the rule for use in this loop.
  - Call Get Fully Qualified Number for the 'from' number. This call will transform the 'from' number to a Fully Qualified Number if it was not done previously by the previous call to Get Type of Number. The resulting type of number of the 'from' number is recorded as the TON_FQN. If this fails, then the rule fails and the next best rule will be searched (see above).
  - Now, the Get Dialable Number API tries to create the requested output type of number. If the numbering plan indicator of the input number ('from') and output type of number are different the following possibilities exist:

    (1) "The number conversion table is searched to convert the input number ('from') to the desired numbering plan (private or public). After the conversion, the TON_FQN is set to the new type of number of

the converted 'from' number. The new TON_FQN is recorded with International (Fully Qualified Public Number must be International).

(2) "If the conversion fails for a conversion from private to public and the Get Dialable Number API was called with an external caller ID number, then the external caller ID number is used as input number ('from') from here on (after running it through the number definition table and the Get Fully Qualified Number API (just like the original 'from').

In all other cases where the conversion fails, the rule fails and the next best rule will be searched

- If the TON_OUT is FQPN, then TON_OUT and TON_OPT are set to TON_FQN.
- If the 'from' and 'to' are in different BGs and the requested TON_OUT is not a public type of number, then the rule fails and the next best rule will be searched
- If the number modification rule requires optimization, the optimization logic is consulted to optimize the 'from' number. If after optimization, the resulting type of number of the 'from' number has a higher level than the requested output type of number (TON_OUT), then the rule fails and the next best rule will be searched
- If a prefix needs to be added to the dialable number then the appropriate number prefix table entry is searched and the network access code and prefix are pre-pended to the dialable number. Regardless whether a prefix is found or not, the Get Dialable Number API returns success with the modified number.

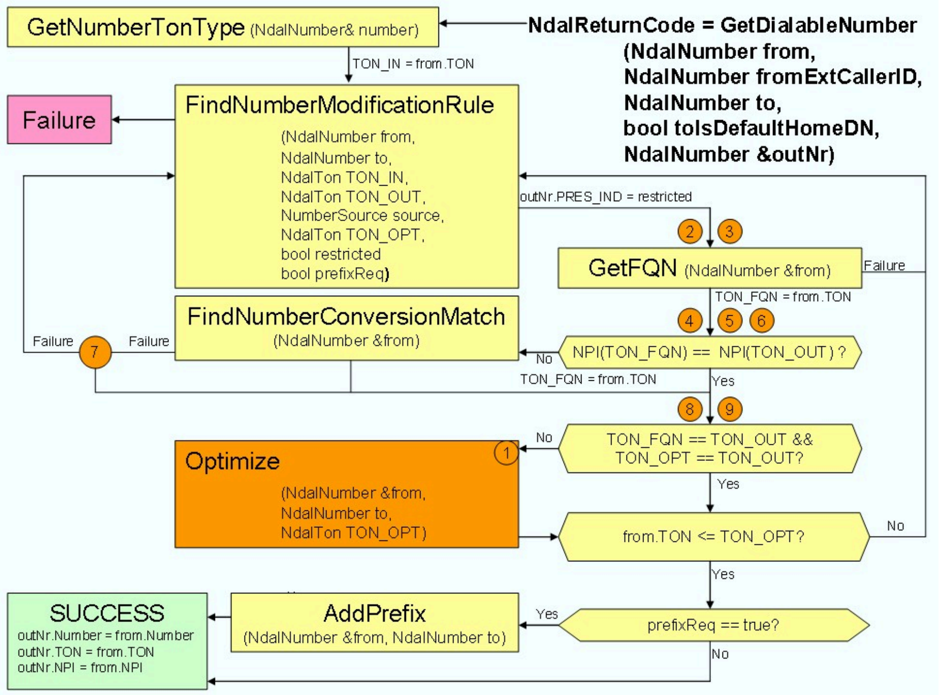

GetNumberTonType (NdalNumber& number)
NdalReturnCode = GetDialableNumber (NdalNumber from, NdalNumber fromExtCallerID, NdalNumber to, bool toIsDefaultHomeDN, NdalNumber &outNr)
TON_IN = from.TON
Failure
FindNumberModificationRule (NdalNumber from, NdalNumber to, NdalTon TON_IN, NdalTon TON_OUT, NumberSource source, NdalTon TON_OPT, bool restricted bool prefixReq)
outNr.PRES_IND = restricted
2
3
GetFQN (NdalNumber &from)
Failure
TON_FQN = from.TON
FindNumberConversionMatch (NdalNumber &from)
Failure
7
Failure
4
5
6
No
NPI(TON_FQN) == NPI(TON_OUT) ?
TON_FQN = from.TON
Yes
8
9
No
TON_FQN == TON_OUT && TON_OPT == TON_OUT?
Optimize (NdalNumber &from, NdalNumber to, NdalTon TON_OPT)
1
Yes
from.TON <= TON_OPT?
No
Yes
SUCCESS
outNr.Number = from.Number
outNr.TON = from.TON
outNr.NPI = from.NPI
AddPrefix (NdalNumber &from, NdalNumber to)
Yes
prefixReq == true?
No

Figure 75: Get Dialable Number API

6.2.46.4 Dialable Number Optimization Logic

The following optimization rules need to be put in place:

- For an optimization to an Extension between 2 subscribers of the same numbering plan, the skip defined on the number definition of the input number is applied to return the extension.
- Any other optimization requires that both the input number and the output party's number are fully qualified numbers. There are 2 methods for optimization from here on:
  - For an optimization to a National or Subscriber number (public numbers), the local toll table of the number definition of the party that will receive the display number (the 'to' number) will be used if available. This will ensure that the public optimized number is presented according to the rules defined for the office code of the receiving subscriber or endpoint.
  - Any other optimization requires a number definition for at least one of the parties - so not only the 'to' party. The components of the number definition can then be used to find out whether country codes, area codes and even local office codes match.

NOTICE:

If a direct optimization of input and output fails because both numbers have different NPIs (e.g. input is public and output is private), the number conversion table will be consulted to try a number optimization with the converted number.

Performing optimization of numbers given a 'from' and a 'to' number.

This is an internal method that performs optimization of numbers given a 'from' and a 'to' number.

If the request is to optimize to an extension between 2 subscribers of the same numbering plan, then the number definition of the 'from' party is sufficient to create the extension provided this number definition does provide a positive skip (a skip of 0 means that no extension can be created with this number definition). This is explained in the Optimize To Extension bullet below.

The remainder of the optimization logic works on fully qualified (private or public) numbers only. For this reason, the 'to' number is given to the GetFQN API. If no fully qualified number can be found for the 'to' number, then no optimization can be done.

In order to compare 'from' and 'to' for optimization, it must be guaranteed that both numbers are at the same type of number when the comparison starts. It may be necessary to find a matching number conversion entry to change the 'to' number from a private number to a public number or vice versa from a public number to a private number. If no number conversion entry could be found, the optimization of the 'from' number based on the 'to' number failed and the optimization logic needs to check whether an optimization using the 'from' number can be done. This is explained in the Optimize With Different NPIs bullet below.

Last but not least a number definition entry is required to be available, either for the 'from' party, the 'to' party or both the 'from' and the 'to' party. Based on which number definition(s) are found, the optimization shall be based on the 'from' and/or the 'to' number definition.

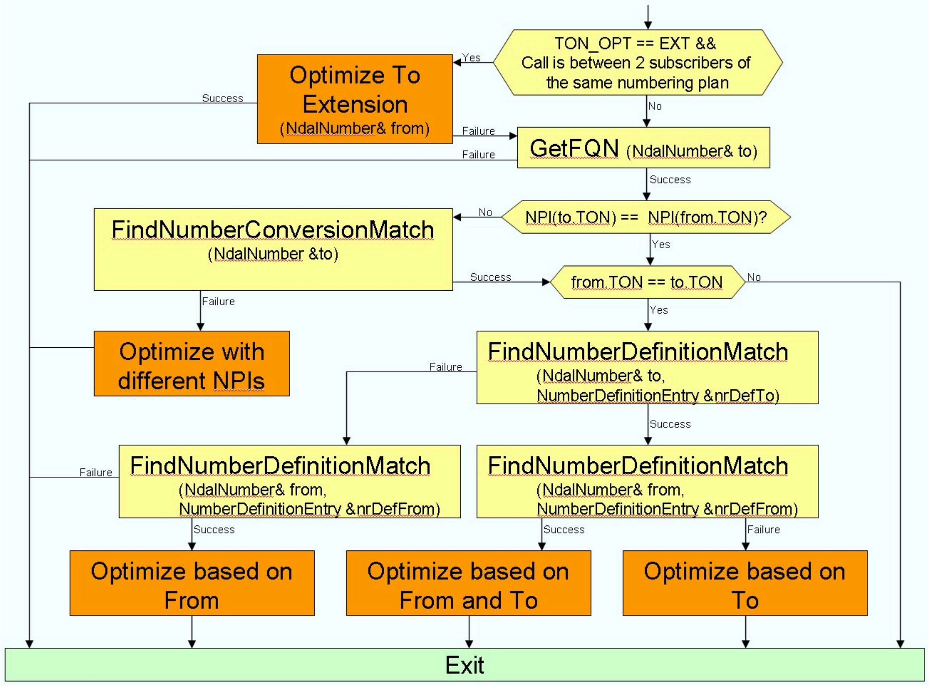


Figure 76: Get Dialable Number API

Optimize to Extension

- Finding the number definition for the 'from' number and if there's a skip defined on this definition, the extension number is calculated with this skip and returned.

Optimize with Different NPIs

- The following is done when converting the NPI of the 'to' number to the NPI of the 'from' number fails:
  - For a request for optimization to extension, the possibility exists that the 'from' number can be converted to get the 'from' and the 'to' on the same NPI. If this succeeds, it is checked whether the 'from' and the 'to' can be optimized all the way to an extension. To do this, the number definitions of both 'from' and 'to' number need to be obtained. If the 'from' number does not have a skip defined, then optimization to extension fails. If a skip is defined and code 2, code 1 and code 0 match exactly for both 'from' and 'to' definition, then the extension number can be calculated with the defined skip on the 'from' and returned.
  - If the 'from' number is public and the 'to' number is private, it is possible that the 'from' number can be optimized using a local toll table defined on the 'to' number's number definition. See also bullet below on Optimize Based on 'from' and Local Toll Table.
  - Else no optimization is possible at this point.

Optimize Based on 'from' Number Definition

- If TON_OPT is Subscriber, L0 or Extension and the 'to' number starts with code2+code1 of the 'from' number, then the 'from' number is modified to the L0 or Subscriber number based on the NPI of the 'from' number.
- If TON_OPT is National, Subscriber, L1 or L0 and the 'to' number starts with code2 of the 'from' number then the 'from' number is the L1 or National number based on the NPI of the 'from' number.

- Else, no optimization is possible.

Optimize Based on 'to' Number Definition

- If a local toll table is attached to the 'to' definition, then the local toll table is used to optimize the 'from' number (see Optimize Based on 'from' and Local Toll Table below). The 'from' number is then the result of this optimization.
- If TON_OPT is Subscriber, L0 or Extension and the 'from' number starts with code2+code1 of the 'to' number, then code2+code1 are stripped from the 'from' number and the TON is set to L0 or Subscriber based on the NPI of the 'from' number.
- If TON_OPT is National, Subscriber, L1, L0 or Extension and the 'from' number starts with code2 of the 'to' number, then code2 is stripped from the 'from' number and the TON is set to L1 or National based on the NPI of the 'from' number.Else, no optimization is possible.

Optimize Based on 'from' and 'to' number definition

- If a local toll table is attached to the 'to' definition, then the local toll table is used to optimize the 'from' number (see Optimize Based on 'from' and Local Toll Table below). The 'from' number is then the result of this optimization.
- If TON_OPT is Subscriber, L0 or Extension and code2 and code1 of the 'from' and the 'to' number match, then code2+code1 are stripped from the 'from' number and the TON is set to L0 or Subscriber based on the NPI of the 'from' number.
- If TON_OPT is National, Subscriber, L1, L0 or Extension and code2 of the 'from' and 'to' number match, then code2 is stripped from the 'from' number and the TON is set to L1 or National based on the NPI of the 'from' number.
- Else, no optimization is possible.

Optimize Based on 'from' and Local Toll Table

- If the 'from' number is not a public number then optimization using the local toll table is not possible.
- If TON_OPT is National and the 'from' number starts with the country code recorded in the local toll table entry then the country code is stripped from the 'from' number and the TON is set to National.
- If TON_OPT is Subscriber and the 'from' number starts with the country code and one of the area codes recorded in the local toll table entry then a lookup is done whether any of the local office codes recorded for the matching are code is matching in the 'from' number.
  - If a match is found then the country code is removed from the 'from' number. The Area code is removed as well if the Include AC flag is not set. The TON of the 'from' number is set to Subscriber.
  - If no match is found then the country code is removed from the 'from' number and the TON is set to National.
- Else, no optimization is possible.

DNM Modifications Optimization Rule/Optimized TON

Table 124: DNM Modifications Optimization Rule

Optimized	OAPN	Input TON	OUTPUT TON	Optimize TON
False	Don't care	False	Don't care	NONE
True	False	ANY	Don't care	EXT

Optimized	OAPN	Input TON	OUTPUT TON	Optimize TON
		ALL/INT	INT	NAT
		ALL/NAT	NAT	SUB
		ALL/SUB	SUB	EXT
		ALL/L2	L2	L1
		ALL/L1	L1	L0
		ALL/L0	L0	EXT
True	True	Don't care	Don't care	EXT

Maximum Optimization

The Maximum optimization level applies to a modification rule. This replaces the previous rules that just allowed optimization one level down or optimization all the way to an extension

6.2.47 Display Number Normalizations Table

This table specifies the entries to normalize any type of input number to a fully qualified public (international) or private (L2, L1 or L0) number. The administrator can specify endpoint specific, numbering plan specific, business group wide and even system wide entries.

Number Normalization

The purpose of this table is to normalize the numbers received from gateways and other trunking endpoints. Therefore, most likely, the administrator will be entering endpoint specific entries in this table.

Requirements

This table and the local toll table are the only tables that require knowledge beyond the boundaries of the OpenScape Voice system being administered. This table contains information about the format of the presentation numbers sent by specific endpoints.

NOTICE:

This table is consulted after the prefixes table has been consulted, so it usually works on defined numbers (not unknown) unless the PNAC and prefixes are not added by the gateway, at which point this table requires normalization entries for Unknown type of numbers.

Matching input numbers

This table allows specifying an **Input Pattern** and **Type of Number** used for matching the number to be normalized and then specifying a modification rule and the resulting type of number of the normalized number. The input pattern allows using wildcards and regular expressions and contains information on how to split the matching digit string in fields that can then be repeated in the modification rule.

This table is also used when a translation results in a call to a specific gateway. If the result of the translation (output of prefix access codes table) is not a fully qualified number then the Normalization table is used to try normalizing the number for presentation purposes in case the gateway does not provide a busy, alerting or connected number.

Input Patterns

In order to limit and even hide the complexity of regular expressions, the input patterns use the following wildcard syntax for pattern elements:

Table 125: Pattern Wildcards

Wildcard	Equivalent element
N	[2-9]
X	[0-9]
Z	0 or more X's
Z{m,n}	Between m and n X's; m must be smaller than n..
Z{n}	Exactly n X's

The only other pattern elements allowed are:

- **[mn]:** m or n with m and n any digit between 0 and 9, *, #.
- **[m-n]:** m through n with m and n and m a digit between 0 and 9. It can be combined with the previous [nm] regular expression. E.g. [04-79] means 0, 4, 5, 6, 7 or 9.
- **n:** a digit between 0 and 9, * or #.

IMPORTANT:

Only one Z can be allowed per input pattern and – when used – it must be the last character in the pattern. The only characters that may follow the Z are the number or numbers between the curly brackets { }.

Pattern elements are joined in pattern fields through the use of the '-' delimiter between 2 pattern elements. Note that the '-' is also allowed inside a pattern element's square brackets and will then not be counted as field numbers.

The maximum length of an input pattern is 64 characters.

EXAMPLE:

Table 126: DNM Normalization Input Pattern Examples

Input Pattern	Description
8011-Z	8011 followed by an open-ended number of digits. Split in 2 fields: • Field1 is 8011. • Field2 contains the remaining digits of the matching input string.

Input Pattern	Description
81-Z{10}	81 followed by a fixed length 10 digit number. Split in 2 fields: • Field1 is 81. • Field2 contains a 10 digit number.
00-Z{10,11}	00 followed by a variable length 10 or 11 digit number. Split in 2 fields: • Field1 is 00. • Field2 contains a 10 or 11 digit number.
XXXX	A 4 digit number in a single field.

If multiple entries could apply to the same input digit string, a weighting factor attributed to the wildcards ensures that specific digits have higher weight then N, followed by X and lastly Z wildcards.

Output Expressions

An output expression is a series of elements and fields where the fields reference the matching digits of the corresponding field in the input pattern. The '-' delimiter is allowed anywhere in the output expression and is ignored in the resulting element string.

The maximum length of an output expression is 64 characters.

EXAMPLE:

Table 127: DNM Normalization Output Expression Examples

Input Pattern	Output Expression	Description
8011-Z	{2}	Return contents of field 2.
81-Z{10}	1{2}	Return '1' followed by the contents of field 2. This would create a US international number from a prefixed national US number.
00-Z{10,11}	32{2}	Return '32' followed by the contents of field 2. This would create a BE international number from a prefixed national BE number.
XXXX	1561555-{1}	Return 1561555 followed by the contents of field 1 (the '-' is ignored). This would create a US international number from a 4 digit extension.

6.2.48 Display Number Conversions Table

This table specifies the number conversion entries that can be created to convert a public normalized number to a private normalized number or a private normalized number to a public normalized number. A special Auto-Reverse parameter allows the administrator to request an automatic creation of the reverse entry; i.e. if a public to private conversion is specified then setting the auto-reverse option will trigger the system to automatically create the private to public number conversion.

The administrator can specify numbering plan specific, business group wide and system wide entries. If the input type of number indicates a public number (International) then the output type of number must indicate a private number (L2, L1 or L0) and vice versa if the input type of number indicates a private number (L2, L1 or L0) then the output type of number must indicate a public number (International).

Input Patterns

This table allows specifying an input pattern used for matching the number to be converted and then specifying an output modification rule and the resulting type of number of the converted output number. Just like the input pattern of the normalizations table, this input pattern allows the same wildcards and regular expressions to be used and contains information on how to split a matching digit string in fields that can be repeated in the output modification rule.

For each entry in the conversions table, the DNM library automatically creates an entry for matching an international public number and converting it to a fully qualified private number (FQPN) and another entry for matching an FQPN and converting it to an international public number if the auto-reverse option is used.

The same weighting as used for the DNM Normalization table ensures that the 498972231212 input pattern entry takes precedence over the less specific 4989722-31XXX entry which also matches for the given input number.

Output Expressions

An output expression is a series of elements and fields where the fields reference the matching digits of the corresponding field in the input pattern. The '-' delimiter is allowed anywhere in the output expression and is ignored in the resulting element string. The maximum length of an output expression is 64 characters.

6.2.49 Display Number Local Toll Table

This table specifies a list of exchange codes that are local given a specified country, area and local exchange code. The area code and exchange code are known as the 'Home Area Code' (aka Home NPA) and 'Home Local Exchange Code' (aka Home LOC). A dial pattern needs to be specified that indicates how numbers are dialed within the Home Area Code if the Local Exchange Code of the number is **NOT** specified in any of the exchange code lists for the specified local toll table.

The Dial Patterns supported are:

- **National**: Area Code + Subscriber Number (if prefixed, national prefix is taken - for NANP this would be 1+10D dialing)
- **Subscriber with Area Code**: Area Code + Subscriber Number (if prefixed, subscriber prefix is taken - for NANP this would be 10D dialing)
- **Subscriber**: Subscriber Number (if prefixed, subscriber prefix is taken - for NANP this would be 7D dialing).

The Exchange code lists specify for each 'local' area code:

- **Area Code**: this can be the Home NPA or a foreign NPA adjacent to the Home NPA.

- **Dial Pattern**: this indicates how numbers are dialed within the given Area Code if the exchange code of the input number is specified in the list of Exchange Codes.
- **Exchange**: a blank or comma separated list of exchange codes, all of equal length that make up the local calling area within the specified area code

DNM Local Toll Table Rules

- The default rule for a local toll table is that all local exchange codes are local within the specified area code and country code and that the area code is not part of the local number. This rule can be specified using the single wildcard '*' for the list of matching local exchange codes.
- No other wildcards or regular expressions are supported on the list of local exchange codes.
- Local Toll tables can be specified system wide or business group specific.
- The exchange codes recorded in a local toll table must all have the same length. It will be allowed to have multiple local toll exchange codes entries with the same area code for the same local toll table. E.g. in the example above it would be allowed to enter another local exchange codes table with the area code 561.

Assigning restrictions

Local Toll table entries can be assigned to entries in the definitions table with the following restrictions:

- A Local Toll table specified for a specific business group cannot be assigned to a system wide definition entry. The reason for this is that system wide definition entries can be seen by every administrator and administrators of other business groups may not have access to other business group resources.
- A Local Toll table specified for a specific business group cannot be assigned to a definition that is specific to another business group for the same reasons as above.

The following table shows some examples of numbers presented to the local toll table for Boca Raton with:

- Country Code: 1
- Home Area Code: 561
- Home Exchange Code: 923
- Dial Pattern: National

And Exchange Code Lists for:

- **Area Code 561**
  - Dial Pattern: Subscriber
  - Exchange Codes: 206 208 210 212 213 218 226 237 239 241 243 245 251 265 266 271 272 274 276 278 279 280 287 288 289 297 300 302 305 306 314 322 330 338 347 350 353 361 362 367 368 372 376 378 381 391 392 393 394 395 400 404 414 416 417 431 435 438 441 442 443 445 447 450 451 454 455 456 457 458 470 477 479 482 483 487 488 495 496 498 499 504 505 520 522 526 542 544 549 558 573 613 620 636 637 638 654 665 666 672 674 699 702 703 705 706 715 716 749 750 756 773 789 807 809 819 824 826 843 852 859 860 862 864 865 866 869 870 883 886 892 893 894 900 901 908 910 912 921 922 923 926 927 929 939 945 948 953 955 961 962 981 982 988 989 991 994 995 997 998 999

- **Area Code 754**
  - Dial Pattern: Subscriber with Area Code
  - Exchange Codes: 227 229 235 242 245 264 366 367 368 484
- **Area Code 954**
  - Dial Pattern: Subscriber with Area Code
  - Exchange Codes: 227 234 242 246 247 254 255 263 281 282 283 301 304 312 317 323 324 333 340 341 344 345 346 354 360 363 366 369 379 415 418 419 420 421 422 425 426 427 428 429 461 464 477 480 481 482 501 509 510 520 531 532 539 543 545 553 569 570 571 573 574 575 580 582 586 590 592 596 597 601 603 621 623 633 642 650 656 657 671 675 688 690 691 692 695 697 698 708 718 719 720 721 722 724 725 726 729 738 743 751 752 753 755 757 773 775 778 780 781 782 783 784 785 786 788 794 796 798 803 818 821 825 827 834 840 856 857 861 867 871 876 899 905 913 917 933 934 935 941 942 943 944 946 947 949 956 957 960 968 969 970 971 972 973 974 975 977 978 979 984

Table 128: Local Toll Table Examples

International Number	Resulting number	Description
International, 498972211111	International, 498972211111	The country codes don't match; therefore the number remains international
International, 15615551212	National, 5615551212	Country code 1 and area code 561 match, but 555 is not found in the exchange codes list. Therefore, the output number is a national number
International, 15615581212	Subscriber, 5581212	Country code 1 and area code 561 match, and 558 is found in the exchange codes list. Therefore, the output number is a subscriber number
International, 19542341111	Subscriber, 9542341111	Country code 1 and area code 954 match, and 234 is found in the exchange codes list. Therefore, the output number is a subscriber number with area code
International, 19542221111	National, 9542221111	Country code 1 and area code 954 match, but 222 is not found in the exchange codes list. Therefore, the output number is a national number

6.2.50 Display Number Modification Use Cases - General Assumptions

This section describes various use cases that will show the provisioning needed to make each use case work.

Assumptions

In all use cases:

- The private network access code is **7.**
- The public network access code is **8** when dialed by a subscriber.
- The public network access code is **9** from or to endpoints.

Private Prefixes:

- For L2 are always **00.**
- For L1 are always **0.**
- For L0 is always **none.**

Public prefixes always match the prefixes defined by the country's public network operators:

- For International: For USA **011**, Europe **00.**
- For National: For USA **1**, Europe **0.**
- For Subscriber **none.**

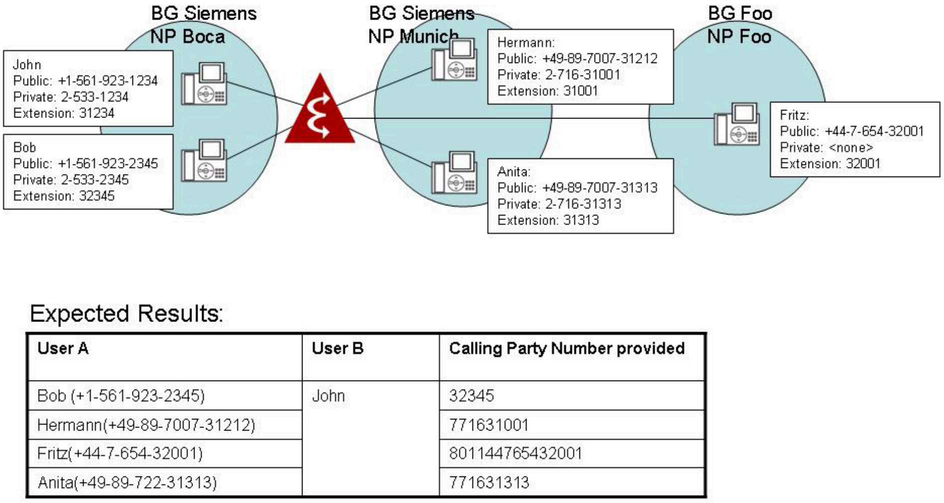
6.2.50.1 Display Number Modification Use Cases - Calls between two SIP Subscribers

SIP Subscribers are configured with E.164 Home DNs

In this use case, the customer prefers to display private numbers within the business group optimized to the extension level. Optimization is also required for calls that go to subscribers of other business groups.

There are 4 use cases handled:

- One where the 2 SIP subscribers both use the same private numbering plan (Bob to John).
- Two where the 2 SIP subscribers use a different private numbering plan but are subscribers of the same business group (Anita to John and Hermann to John: note that Hermann's private number doesn't match his public Home DN solved via a special number conversion rule).
- One where the 2 SIP subscribers belong to different business groups (Fritz to John).



Expected Results:

User A	User B	Calling Party Number provided
Bob (+1-561-923-2345)	John	32345
Hermann(+49-89-7007-31212)		771631001
Fritz(+44-7-654-32001)		801144765432001
Anita(+49-89-722-31313)		771631313

Figure 77: Call between 2 SIP subscribers that are configured with E.164 Home DNs

Table 129: Number prefix table:

Context	International PNAC-Prefix	National PNAC-Prefix	Subscriber PNAC-Prefix	L2 PNAC-Prefix	L1 PNAC-Prefix	L0 PNAC-Prefix
ANY/ANY	0-00	0-0	0-			
Siemens/ANY	8-011	8-1	8		7-0	7-

Table 130: Number definition table requires the office code definitions::

Context	NPI	CC/L2	AC/L1	LOC/L0	Skip	Min	Max	Local Toll
ANY/ANY	Public	1	561	923	2	11	11	
ANY/ANY	Public	49	89	7007	4	9	13	
ANY/ANY	Public	44	7	654	3	11	11	
Siemens/ ANY	Private		2	533	2	8	8	
Siemens/ ANY	Private		2	716	3	9	9	

Table 131: Number conversion table converts public numbers to private numbers and vice versa:

Context	Input Pattern	Input Type of Number	Output Expression	Output Type of Number	Auto-Reverse
Siemens/ANY	1561923-XXXX	International	2533{2}	L1	True
Siemens/ANY	4989700731212	International	271631001	L1	True
Siemens/ANY	49897007-XXXXX	International	2716{2}	L1	True

Table 132: Number modification rule for a single endpoint:

Originating Context	Terminating Context	Input Type of Number	Input Type of Number	Priority	Output Type Of Number	Prefixed	Optimized Type Of Number
ANY/ANY	ANY ANY/NONE	ANY	1	Input Number	L1	No	Extension
ANY/ANY	ANY ANY/NONE	ANY	2	Input Number	International	No	Extension

(1) The first rule covers showing extensions between subscribers within business groups.

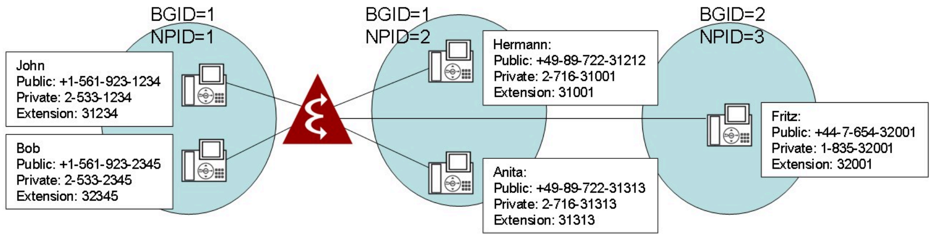
(2) The second rule covers showing public optimized numbers between subscribers of different business groups.

SIP Subscribers are configured with Private Home DNs

In this use case, the customer prefers to display private numbers within the business group optimized to the extension level. Optimization is also required for calls that go to subscribers of other business groups.

The same 4 use cases are described:

- One where the 2 SIP subscribers both use the same private numbering plan (Bob to John).
- Two where the 2 SIP subscribers use a different private numbering plan but are subscribers of the same business group (Anita to John and Hermann to John: note that the special number conversion rule is still required for Hermann in order to provide a public number when making calls outside of the business group. This could also have been solved by assigning an External Caller ID to John).
- One where the 2 SIP subscribers belong to different business groups.



Expected Results:

User A	User B	Calling Party Number provided
Bob (2-533-2345)	John	32345
Hermann(2-716-31001)		771631001
Fritz(1-835-32001)		801144765432001
Anita(2-716-31313)		771631313

Figure 78: Call between 2 SIP subscribers that are configured with Private Home DNs

Table 133: Number prefix table:

Context	International PNAC-Prefix	National PNAC-Prefix	Subscriber PNAC-Prefix	L2 PNAC-Prefix	L1 PNAC-Prefix	L0 PNAC-Prefix
ANY/ANY	0-00	0-0	0-			
Siemens/ANY	8-011	8-1	8		7-0	7-

Table 134: Number definition table requires the office code definitions::

Context	NPI	CC/L2	AC/L1	LOC/L0	Skip	Min	Max	Local Toll
ANY/ANY	Public	1	561	923	2	11	11	
ANY/ANY	Public	49	89	7007	4	9	13	
ANY/ANY	Public	44	7	654	3	11	11	
Siemens/ ANY	Private		2	533	2	8	8	
Siemens/ ANY	Private		2	716	3	9	9	

Table 135: Number conversion table converts public numbers to private numbers and vice versa:

Context	Input Pattern	Input Type of Number	Output Expression	Output Type of Number	Auto-Reverse
Siemens/ANY	1561923-XXXX	International	2533{2}	L1	True
Siemens/ANY	4989700731212	International	271631001	L1	True
Siemens/ANY	49897007-XXXXX	International	2716{2}	L1	True

Table 136: Number modification rule for a single endpoint:

Originating Context	Terminating Context	Input Type of Number	Input Type of Number	Priority	Output Type Of Number	Prefixed	Optimized Type Of Number
ANY/ANY	ANY ANY/NONE	ANY	1	Input Number	L1	No	Extension
ANY/ANY	ANY ANY/NONE	ANY	4	Input Number	ANY	No	Subscriber

(1) The first rule covers showing extensions between subscribers within business groups.

(2) The second rule covers showing public optimized numbers between subscribers of different business groups.

6.2.50.2 Display Number Modification Use Cases - Incoming Calls from a SIP Endpoint (public gateway) to a SIP Subscriber

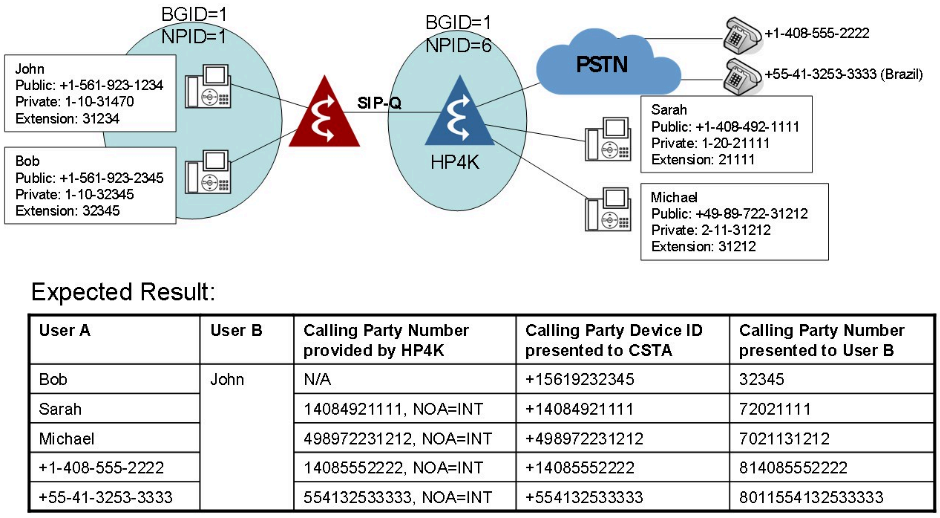
SIP Gateway provides implicit prefixed calling party numbers:

There are 4 use cases described:

- One where the call is from an internal subscriber (Bob to John)
- One where the call is from an international public number (+55-41-3253-3333 to John).
- One where the call is from a national public number (+1-408-555-2222 to John).
- One where the call is from a local public number (+1-561-555-1111 to John).

In this use case, the customer prefers to display optimized public numbers from the gateway. The SIP gateway provides prefixed calling party numbers.

For this use case it does not matter whether the terminating party is configured with an E.164 Home DN or with a Private Home DN. The number conversion rules (not shown) will take care of this.



Expected Result:

User A	User B	Calling Party Number provided by HP4K	Calling Party Device ID presented to CSTA	Calling Party Number presented to User B
Bob	John	N/A	+15619232345	32345
Sarah		14084921111, NOA=INT	+14084921111	72021111
Michael		498972231212, NOA=INT	+498972231212	7021131212
+1-408-555-2222		14085552222, NOA=INT	+14085552222	814085552222
+55-41-3253-3333		554132533333, NOA=INT	+554132533333	8011554132533333

Figure 79: Incoming calls from SIP-Q Endpoint that provides E.164 numbers

Table 137: Number prefix table:

Context	International PNAC-Prefix	National PNAC-Prefix	Subscriber PNAC-Prefix	L2 PNAC-Prefix	L1 PNAC-Prefix	L0 PNAC-Prefix
ANY/ANY	0-00	0-0	0-			
Siemens/ANY	8-011	8-1	8		7-0	7-

Table 138: Number definition table requires the office code definitions::

Context	NPI	CC/L2	AC/L1	LOC/L0	Skip	Min	Max	Local Toll
ANY/ANY	Public	1	561	923	2	11	11	

Table 139: Number normalization rules for the gateway modify the received numbers to International numbers:

Context	Input Type of Number	Input Pattern	Output Type of Number	Output Expression
Siemens/ANY/ALL	Unknown	9011-Z	International	{2}
Siemens/ANY/ALL	Unknown	91-X{10}	International	1{2}
Siemens/ANY/ALL	Unknown	9-X{10}	International	1{2}
Siemens/ANY/ALL	Unknown	9-X{7}	International	1561{2}

Table 140: Number modification rule for a single endpoint:

Originating Context	Terminating Context	Input Type of Number	Input Type of Number	Priority	Output Type Of Number	Prefixed	Optimized Type Of Number
ANY/ANY	ANY/ANY/ NONE	ANY	1	Input Number	L1	No	Extension
ANY/ANY	ANY/ANY/ NONE	ANY	4	Input Number	ANY	No	Subscriber

(1) The first rule covers showing extensions between subscribers within business groups.

(2) The second rule covers showing public optimized numbers towards subscribers of any business group. This rule is no different than the rule created between 2 subscribers of different business groups.

Upon arrival, the presentation numbers of the gateway are first offered to the Number Normalization tables. All numbers will exit the Normalization table as International numbers. OpenScape Voice then uses the number definition of the subscriber to optimize the number towards the subscribers.

SIP Gateway provides implicit non-prefixed calling party numbers

There are 4 use cases described:

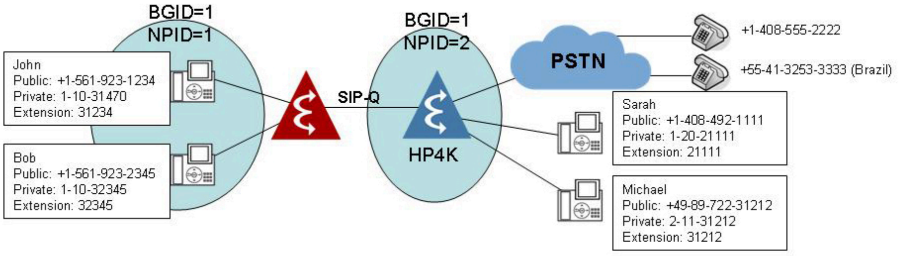
- One where the call is from an internal subscriber (Bob to John)
- One where the call is from an international public number (+55-41-3253-3333 to John).
- One where the call is from a national public number (+1-408-555-2222 to John).
- One where the call is from a local public number (+1-561-555-1111 to John).

In this use case, the customer prefers to display optimized public numbers from the gateway. The SIP gateway provides non-prefixed calling party numbers

For this use case it does not matter whether the terminating party is configured with an E.164 Home DN or with a Private Home DN. The number conversion rules (not shown) will take care of this.

NOTICE:

The gateway is sending numbers without prefixes or any other indication of the sent type of number. This means that the numbers will be ambiguous and a choice will have to be made in some cases as to which type of number is received. E.g. a Belgian international number is 10 digits long - but so is a national American number. Without knowing the type of number a choice must be made whether to interpret the incoming number as a national or an international number.



Expected Results:

User A	User B	Calling Party Number provided by HP4K	Calling Party Device ID presented to CSTA	Calling Party Number presented to User B
Bob	John	N/A	+15619232345	32345
Sarah		12021111, NOA=L1	12021111	72021111
Michael		21131212, NOA=L1	21131212	7021131212
+1-408-555-2222		14085552222, NOA=INT	+14085552222	814085552222
+55-41-3253-3333		554132533333, NOA=INT	+554132533333	8011554132533333

Figure 80: Incoming calls from SIP-Q Endpoint that provides Private/ Public numbers

Table 141: Number prefix table:

Context	International PNAC-Prefix	National PNAC-Prefix	Subscriber PNAC-Prefix	L2 PNAC-Prefix	L1 PNAC-Prefix	L0 PNAC-Prefix
ANY/ANY	0-00	0-0	0-			
Siemens/ANY	8-011	8-1	8		7-0	7-

Table 142: Number definition table requires the office code definitions::

Context	NPI	CC/L2	AC/L1	LOC/L0	Skip	Min	Max	Local Toll
ANY/ANY	Public	1	561	923	2	11	11	

Table 143: Number normalization rule for the gateway:

Context	Input Type of Number	Input Pattern	Output Type of Number	Output Expression
Siemens/ANY/ALL	Unknown	NXX-NXX-XXXX	International	1{1}{2}{3}
Siemens/ANY/ALL	Unknown	NXX-XXXX	International	1{1}{2}
Siemens/ANY/ALL	Unknown	Z	International	{1}

Table 144: Number modification rule for a single endpoint:

Originating Context	Terminating Context	Input Type of Number	Input Type of Number	Priority	Output Type Of Number	Prefixed	Optimized Type Of Number
ANY/ANY	ANY/ANY/ NONE	ANY	1	Input Number	L1	No	Extension
ANY/ANY	ANY/ANY/ NONE	ANY	4	Input Number	ANY	No	Extension

(1) The first rule covers showing extensions between subscribers within business groups.

(2) The second rule covers showing public optimized numbers towards subscribers of any business group. This rule is no different than the rule created between 2 subscribers of different business groups.

Upon arrival, the presentation numbers of the gateway are offered to the Number Normalization tables. All numbers will exit the Normalization table as International numbers. OpenScape Voice then uses the number definition of the subscriber to optimize the number towards the subscribers.

NOTICE:

THE CONFIGURATION OF THIS USE CASE SHOULD BE AVOIDED AS MUCH AS POSSIBLE,

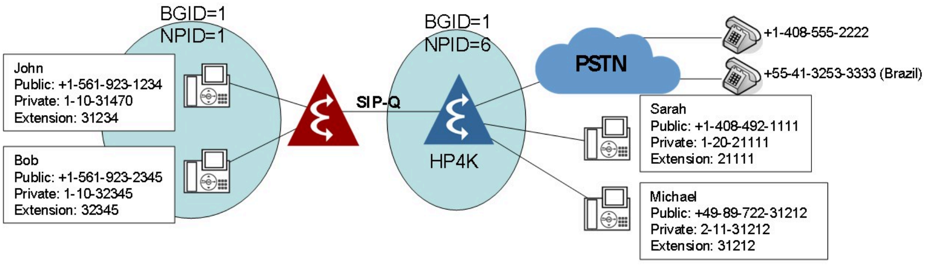
6.2.50.3 Local Toll Table for incoming calls from North American Numbering Plan

Within the North American Numbering Plan (NANP) boundaries between area codes are not as clear-cut as in the rest of the world. To aid in determining whether numbers need to be dialed as local or national numbers, a local toll table needs to be used that will aid number modification in optimizing a normalized International number.

There are 5 use cases described:

- One where the call is from an international public number.
- One where the call is from a national public number.
- One where the call is from a local public number requiring 10 digit dialing (overlapping area code)
- One where the call is from a national public number from an area code for which also local numbers are supported (split area code)
- One where the call is from a local public number (normal 7 digit dialing)

In this use case, the customer prefers to display the numbers as they would have to be dialed in the public network. The network provider always provides national or international calling party numbers.



Expected Result:

User A	User B	Calling Party Number provided by HP4K	Calling Party Device ID presented to CSTA	Calling Party Number presented to User B
Bob	John	N/A	+15619232345	32345
Sarah		14084921111, NOA=INT	+14084921111	72021111
Michael		498972231212, NOA=INT	+498972231212	7021131212
+1-408-555-2222		14085552222, NOA=INT	+14085552222	814085552222
+55-41-3253-3333		554132533333, NOA=INT	+554132533333	8011554132533333

Figure 81: Incoming calls from SIP-Q Endpoint that provides E.164 numbers

Table 145: Number prefix table:

Context	International PNAC-Prefix	National PNAC-Prefix	Subscriber PNAC-Prefix	L2 PNAC-Prefix	L1 PNAC-Prefix	L0 PNAC-Prefix
ANY/ANY	0-00	0-0	0-			
Siemens/ANY	8-011	8-1	8		7-0	7-

Table 146: Number definition table requires the office code definitions::

Context	NPI	CC/L2	AC/L1	LOC/L0	Skip	Min	Max	Local Toll
ANY/ANY	Public	1	561	923	2	11	11	Boca-Toll

Table 147: Local Toll table used for the Boca office code 1-561-923:

Context	Name	Country Code	Home Area Code	Home Exchange Code	Dial Pattern
ANY	Boca-Toll	1	561	923	National

Table 148: Exchange Code Lists belonging to the Boca-Toll table:

Area Code	Dial Pattern	Exchange Codes
561	Subscriber	206 208 210 212 213 218 226 237 239 241 243 245 251 265 266 271 272 274 276 278 279 280 287 288 289 297 300 302 305 306 314 322 330 338 347 350 353 361 362 367 368 372 376 378 381 391 392 393 394 395 400 404 414 416 417 431 435 438 441 442 443 445 447 450 451 454 455 456 457 458 470 477 479 482 483 487 488 495 496 498 499 504 505 520 522 526 542 544 549 558 573 613 620 636 637 638 654 665 666 672 674 699 702 703 705 706 715 716 749 750 756 773 789 807 809 819 824 826 843 852 859 860 862 864 865 866 869 870 883 886 892 893 894 900 901 908 910 912 921 922 923 926 927 929 939 945 948 953 955 961 962 981 982 988 989 991 994 995 997 998 999

Area Code	Dial Pattern	Exchange Codes
754	Subscriber with Area Code	227 229 235 242 245 264 366 367 368 484
954	Subscriber with Area Code	227 234 242 246 247 254 255 263 281 282 283 301 304 312 317 323 324 333 340 341 344 345 346 354 360 363 366 369 379 415 418 419 420 421 422 425 426 427 428 429 461 464 477 480 481 482 501 509 510 520 531 532 539 543 545 553 569 570 571 573 574 575 580 582 586 590 592 596 597 601 603 621 623 633 642 650 656 657 671 675 688 690 691 692 695 697 698 708 718 719 720 721 722 724 725 726 729 738 743 751 752 753 755 757 773 775 778 780 781 782 783 784 785 786 788 794 796 798 803 818 821 825 827 834 840 856 857 861 867 871 876 899 905 913 917 933 934 935 941 942 943 944 946 947 949 956 957 960 968 969 970 971 972 973 974 975 977 978 979 984

Table 149: Number normalization rules for the gateway:

Context	Input Type of Number	Input Pattern	Output Type of Number	Output Expression
Siemens/ANY/ALL	Unknown	9011-Z	International	{2}
Siemens/ANY/ALL	Unknown	91-X{10}	International	1{2}
Siemens/ANY/ALL	Unknown	9-X{10}	International	1{2}
Siemens/ANY/ALL	Unknown	9-X{7}	International	1561{2}

Table 150: Number modification rule for a single endpoint:

Originating Context	Terminating Context	Input Type of Number	Input Type of Number	Priority	Output Type Of Number	Prefixed	Optimized Type Of Number
ANY/ANY	ANY/ANY/	ANY	4	Input Number	ANY	YES	Subscriber

The numbers from the PSTN are normalized to International numbers using the Normalizations table. The modification rule requires any input number to be optimized no further than the Subscriber number format and then prefixed. Because the Boca-Toll toll table is assigned to the Boca Raton, FL office code of the terminating subscriber, this table is used to optimize the International number:

- International/156155581111 matches on country code and on the exchange code 558 in the 561 home area code. The dial pattern of this exchange code list is Subscriber. Therefore the result is the prefixed subscriber number: 85581111.
- International/15616652222 matches on country code but not on the exchange code 665 in the 561 home area code. The dial pattern is therefore the Dial Pattern of the Local toll table: National. Therefore the result is the prefixed national number: 815616651111.
- International/19542273333 matches on country code and on the exchange code 227 in the 954 area code. The dial pattern of this exchange code list is Subscriber with Area Code. Therefore the result is the prefixed subscriber number: 89542273333.

- International/19542104444 matches on country code but not on the exchange code 210 in the 954 area code. The dial pattern is therefore National (note that for non-local numbers of foreign area codes the dial pattern is always National). Therefore the result is the prefixed national number: 819542104444.
- International/554132533333 does not match on country code. For international numbers the dial pattern is always International. Therefore the result is the prefixed international number: 8011554132533333.

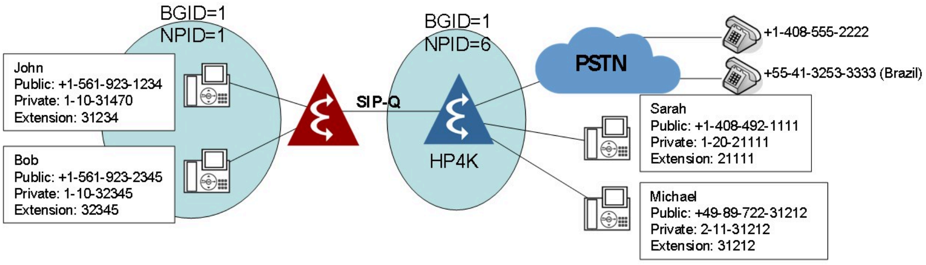
6.2.50.4 Display Number Modification Use Cases - Incoming Calls from a SIPQ Endpoint (public gateway) to a SIP Subscriber

Incoming calls from SIP-Q Endpoint that provides E.164 numbers

In this use case numbers from the customer's network must be displayed as private numbers with prefix. Numbers from the PSTN must be displayed in the shortest dialable format

There are 4 use cases described:

- One where the call is from an internal subscriber (Bob to John)
- Two where the call is from a private network (Sarah to John; Michael to John)
- One where the call is from a national public number (+14085552222 to John)
- One where the call is from an international public number (+554132533333 to John)



Expected Result:

User A	User B	Calling Party Number provided by HP4K	Calling Party Device ID presented to CSTA	Calling Party Number presented to User B
Bob	John	N/A	+15619232345	32345
Sarah		14084921111, NOA=INT	+14084921111	72021111
Michael		498972231212, NOA=INT	+498972231212	7021131212
+1-408-555-2222		14085552222, NOA=INT	+14085552222	814085552222
+55-41-3253-3333		554132533333, NOA=INT	+554132533333	8011554132533333

Figure 82: Incoming calls from SIP-Q Endpoint that provides E.164 numbers

Table 151: Number prefix table:

Context	International PNAC-Prefix	National PNAC-Prefix	Subscriber PNAC-Prefix	L2 PNAC-Prefix	L1 PNAC-Prefix	L0 PNAC-Prefix
ANY/ANY	0-00	0-0	0-			
Siemens/ANY	8-011	8-1	8		7-0	7-

Table 152: Number definition table requires the office code definitions::

Context	NPI	CC/L2	AC/L1	LOC/L0	Skip	Min	Max	Local Toll
ANY/ANY	Public	1	561	923	2	11	11	Boca-Toll
Siemens/ ANY	Private		2	533	2	8	8	Boca-Toll

Table 153: Number conversion table required to offer the private network numbers related to the public numbers received from the SIP-Q endpoint:

Context	Input Pattern	Input Type of Number	Output Expression	Output Type of Number	Auto-Reverse
Siemens/ANY	1561923-XXXX	International	2533{2}	L1	True
Siemens/ANY	1408492-XXXX	International	2876{2}	L1	True
Siemens/ANY	49897007-XXXXX	International	1571{2}	L1	True

Table 154: Number modification rules:

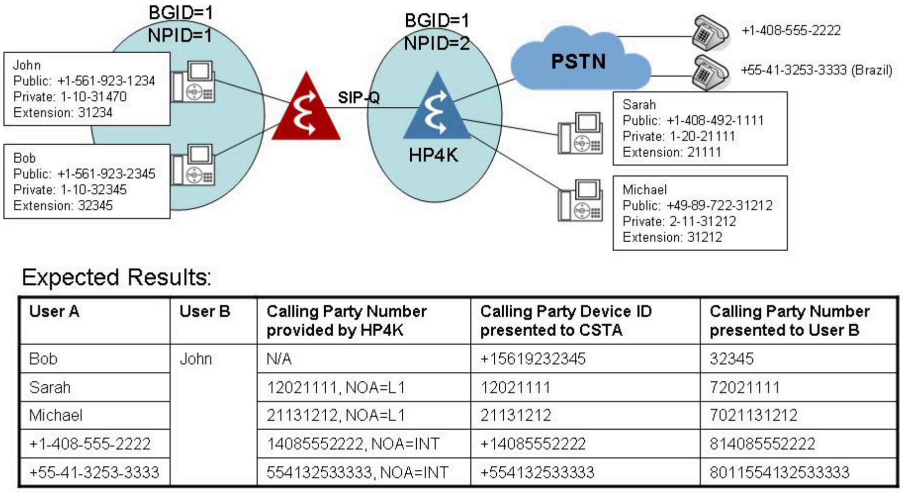
Originating Context	Terminating Context	Input Type of Number	Input Type of Number	Priority	Output Type Of Number	Prefixed	Optimized Type Of Number
ANY/ANY	ANY/ANY/ NONE	ANY	1	Input Number	L1	Yes	Extension
ANY/ANY	ANY/ANY/ NONE	ANY	4	Input Number	ANY	Yes	Subscriber

The numbers from the SIP-Q endpoint are already received normalized. The first modification rule requires any input number to be converted to an L1 number and then may be optimized all the way to extension and possibly be prefixed.

Numbers that cannot be converted to L1 numbers may be optimized to the Subscriber number format. Because the Boca-Toll toll table is assigned to the Boca Raton, FL office code of the terminating subscriber, this table is used to optimize the public number.

Incoming call from SIP-Q Endpoint that provides Private/Public numbers

In this use case, numbers from the customer’s network must also be displayed as private numbers with prefix. Numbers from the PSTN must be displayed in the shortest dialable format.



Expected Results:

User A	User B	Calling Party Number provided by HP4K	Calling Party Device ID presented to CSTA	Calling Party Number presented to User B
Bob	John	N/A	+15619232345	32345
Sarah		12021111, NOA=L1	12021111	72021111
Michael		21131212, NOA=L1	21131212	7021131212
+1-408-555-2222		14085552222, NOA=INT	+14085552222	814085552222
+55-41-3253-3333		554132533333, NOA=INT	+554132533333	8011554132533333

Figure 83: Incoming calls from SIP-Q Endpoint that provides Private/ Public numbers

Table 155: Number prefix table:

Context	International PNAC-Prefix	National PNAC-Prefix	Subscriber PNAC-Prefix	L2 PNAC-Prefix	L1 PNAC-Prefix	L0 PNAC-Prefix
ANY/ANY	0-00	0-0	0-			
Siemens/ANY	8-011	8-1	8		7-0	7-

Table 156: Number definition table requires the office code definitions::

Context	NPI	CC/L2	AC/L1	LOC/L0	Skip	Min	Max	Local Toll
ANY/ANY	Public	1	561	923	2	11	11	Boca-Toll
Siemens/ ANY	Private		2	533	2	8	8	Boca-Toll

Table 157: Number normalization rule for the extensions from Munich:::

Context	Input Type Of Number	Input Pattern	Output Type Of Numer	Output Expression
Siemens/Beeston	Unknown	XXXXX	International	49897007{1}

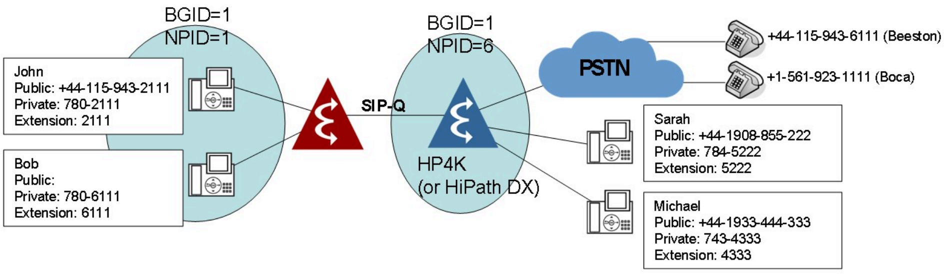
Table 158: Number modification rules:

Originating Context	Terminating Context	Input Type of Number	Input Type of Number	Priority	Output Type Of Number	Prefixed	Optimized Type Of Number
ANY/ANY	ANY/ANY/ NONE	ANY	1	Input Number	L1	Yes	Extension
ANY/ANY	ANY/ANY/ NONE	ANY	4	Input Number	ANY	Yes	Subscriber

The numbers from the SIP-Q endpoint are already received normalized. The first modification rule requires any input number to use the L1 number and then may be optimized all the way to extension and possibly be prefixed. This rule applies to Sarah's and Michael's call to Bob. Numbers that are not L1 numbers or cannot be converted to L1 numbers may be optimized to the Subscriber number format. Because the Boca-Toll toll table is assigned to the Boca Raton, FL office code of the terminating subscriber, this table may be used to optimize the public number.

Incoming call from SIP-Q Endpoint that provides Unknown Private/Public numbers

In this use case, numbers from the customer's network must be displayed as private numbers with prefix. Numbers from the PSTN must be displayed in the shortest dialable format.



Expected Results:

User A	User B	Calling Party Number provided by HP4K	Calling Party Device ID presented to CSTA	Calling Party Number presented to User B
Bob	John	N/A	7806111	6111
Sarah		7845222, NOA=UNK	7845222	7845222
Michael		7434333, NOA=UNK	7434333	7434333
+44-115-943-6111		441159436111, NOA=UNK	+441159436111	99436111
+1-561-923-1111		15619231111, NOA=UNK	+15619231111	90015619231111

Figure 84: Incoming calls from SIP-Q Endpoint that provides Unknown Private/Public numbers

Table 159: Number prefix table:

Context	International PNAC-Prefix	National PNAC-Prefix	Subscriber PNAC-Prefix	L2 PNAC-Prefix	L1 PNAC-Prefix	L0 PNAC-Prefix
ANY/ANY	0-00	0-0	0-			
Siemens/ANY	8-011	8-1	8		7-0	7-

Table 160: Number definition table requires the office code definitions::

Context	NPI	CC/L2	AC/L1	LOC/L0	Skip	Min	Max	Local Toll
ANY/ANY	Public	44	115	943	3	12	12	
Siemens/ ANY	Private		2	780	3	7	7	Beeston- Toll

Table 161: Local Toll table used for the Beeston private office code 780::

Context	Name	Country Code	Home Area Code	Home Exchange Code	Dial Pattern
ANY	Beeston-Toll	44	115	943	National

Table 162: Exchange Code Lists belonging to the Beeston-Toll table::

Area Code	Dial Pattern	Exchange Codes
115	Subscriber	*

Table 163: Number normalization rules to handle the Unknown nature of the presentation numbers::

Context	Input Type Of Number	Input Pattern	Output Type Of Numer	Output Expression
Siemens/Beeston/ALL-PN	Unknown	7XX-XXXX	L0	{1}{2}
Siemens/Beeston/ALL-PN	Unknown	Z	International	{1}

Table 164: Number conversion table required to find the private number associated with Home DNs using the public office code for Beeston

Context	Input Pattern	Input Type Of Number	Output Expression	Output Type Of Number	Auto Reverse
Siemens/ Beeston	44115943-[2-4]XXX	International	780{2}	L0	True

Table 165: Number modification rules:

Originating Context	Terminating Context	Input Type of Number	Input Type of Number	Priority	Output Type Of Number	Prefixed	Optimized Type Of Number
ANY/ANY	ANY/ANY/ NONE	ANY	1	Input Number	L1	Yes	Extension
ANY/ANY	ANY/ANY/ NONE	ANY	4	Input Number	ANY	Yes	Subscriber

The numbers from the SIP-Q endpoint are already normalized however in the Unknown format. The Normalization rules are used to distinguish the L1 numbers from the International numbers. The first modification rule requires any input number to use the L1 number and then may be optimized all the way to extension and possibly be prefixed. This rule applies to Sarah's and Michael's call to Bob. Numbers that are not L1 numbers or cannot be converted to L1 numbers may be optimized to the Subscriber number format. Because the Beeston-Toll toll table is assigned to the Beeston, UK private office code of the terminating subscriber Bob, this table may be used to optimize the public number for Bob.

6.2.50.5 Display Number Modification Use Cases - Outgoing Calls from a SIP Subscriber to a SIP Endpoint (public gateway)

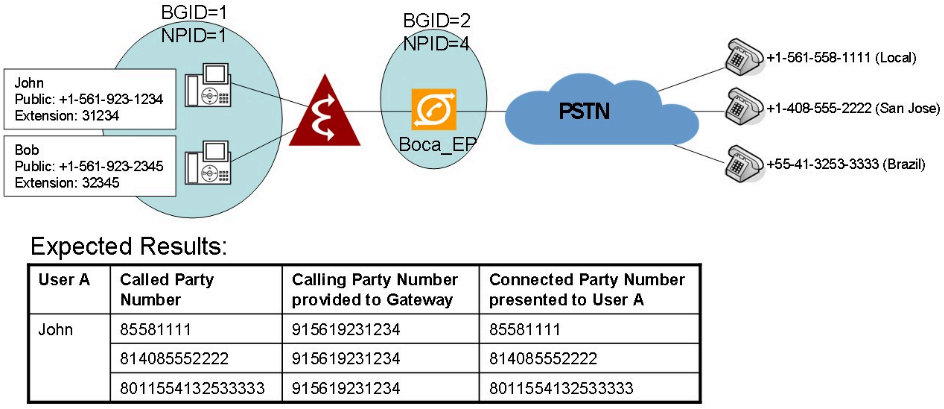
For outgoing calls, the translation tables become important as well. To create the connected party number for a gateway that does not provide a connected party number, the translation result is taken and made dialable.

SIP Gateway expects Prefixed National or International Calling Party Numbers

In this use case the calling party number must be displayed in national/ international prefixed format, while the connected party number should be in shortest dialable format.

There are 3 use cases described:

- One where the call is made to a local public number.
- One where the call is made to a national public number.
- One where the call is made to an international public number.



Expected Results:

User A	Called Party Number	Calling Party Number provided to Gateway	Connected Party Number presented to User A
John	85581111	915619231234	85581111
	814085552222	915619231234	814085552222
	8011554132533333	915619231234	8011554132533333

Figure 85: Outgoing call to SIP Endpoint that expects national or international prefixed numbers

The translation tables - important for creating the connected party number - could be set up as follows (not recommended).

It is recommended that NOA is international when entering the prefix access codes table - but it is shown here to make a point about the number modification when no number is received from the PSTN):

Table 166: Prefix Access Codes Table

Numb. Plan	PAC	Min	Max	Digit Position	Insert Digits	Prefix Type	NOA	Destination
Boca	8011	4	30	4	-	Off-Net	INT	None
Boca	81	12	12	2	-	Off-Net	NAT	None
Boca	8	8	8	1	-	Off-Net	SUB	None

Table 167: Destination Codes Table

Numb. Plan	Digits	NOA	Destination Name
Boca	5	INT	GwyBocaInt
Boca	4	NAT	GwyBocaNat
Boca	5	SUB	GwyBocaSub

Table 168: Destinations Table

Numb. Plan	Destination Name	Route	Endpoint	Delete Digits	Insert Digits	NOA
Boca	GwyBocaInt	1	Boca_EP	0	9011	Unknown
Boca	GwyBocaNat	1	Boca_EP	0	91	Unknown
Boca	GwyBocaSub	1	Boca_EP	0	9	Unknown

For the calling party number, the Display Number Modification tables are consulted for creating the calling party number (originating context) for a call to the called party (terminating context).

Table 169: Number prefix table:

Context	International PNAC-Prefix	National PNAC-Prefix	Subscriber PNAC-Prefix	L2 PNAC-Prefix	L1 PNAC-Prefix	L0 PNAC-Prefix
Siemens/ Siemens	9-011	9-1	9			

Table 170: Number definition table requires the office code definitions:

Context	NPI	CC/L2	AC/L1	LOC/L0	Skip	Min	Max	Local Toll
ANY/ANY	Public	1	561	923	2	11	11	

Table 171: Number modification rule:

Rule Number	Orig.Numb. plan	Term.Numb. plan	Input Type of Number	Ouput Type of Number	Number Transm	Optimized	Optimized as PN
ANY	1	ANY	ANY	ANY-PRE	Transparent	Yes	No

For the connected party number, the Display Number Modification tables are consulted for creating the connected party number from the called party number (originating context) for the calling party (terminating context). For the 3 use cases, the called party number used is the input to the destination codes table, i.e.

- SUB/5551111
- NAT/4085552222
- NT/554132533333

Table 172: Number prefix table:

Context	International PNAC-Prefix	National PNAC-Prefix	Subscriber PNAC-Prefix	L2 PNAC-Prefix	L1 PNAC-Prefix	L0 PNAC-Prefix
Siemens/ Siemens	8-011	8-1	8			

Table 173: Number normalization rules to handle the Subscriber and National Nature of Address from the destination codes table:

Context	Input Type of Number	Input Pattern	Output Type of Number	Output Expression
Siemens/Siemens/Boca_EP	Subscriber	Z	International	1561{1}
Siemens/Siemens/Boca_EP	National	Z	International	1{1}

Table 174: Number modification rules::

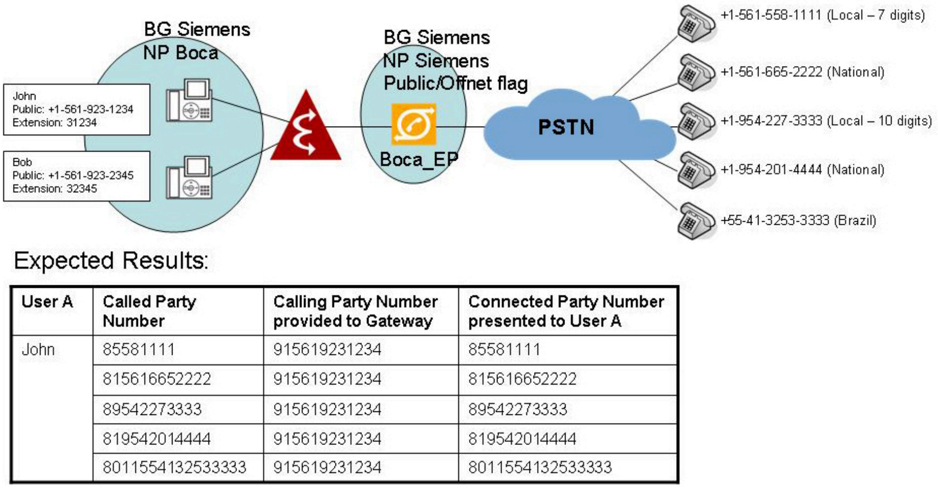
Originating Context	Terminating Context	Input Type of Number	Input Type of Number	Priority	Output Type Of Number	Prefixed	Optimized Type Of Number
ANY/ANY/	ANY/ANY/ NONE	ANY	4	Input Number	ANY	Yes	Subscriber

Local Toll Table for outgoing calls to North American Numbering Plan

In this use case, the customer prefers to dial the public network access code, followed by the digits as they would have to be dialed in the public network. The network provider allows national or international calling party numbers.

There are 5 use cases described:

- One where the call is to an international public number.
- One where the call is to a national public number.
- One where the call is to a local public number requiring 10 digit dialing
- One where the call is to a national public number from an area code for which also local numbers are supported (split area code)
- One where the call is to a local public number (normal 7 digit dialing



Expected Results:

User A	Called Party Number	Calling Party Number provided to Gateway	Connected Party Number presented to User A
John	85581111	915619231234	85581111
	815616652222	915619231234	815616652222
	89542273333	915619231234	89542273333
	819542014444	915619231234	819542014444
	8011554132533333	915619231234	8011554132533333

Figure 86: Local Toll Table for outgoing calls to North American Numbering Plan

This use case will require a lot of entries in the destination codes table because of the way called party numbers are created in the USA. The presentation of the calling party number to the PSTN is just as in the previous use case. However, the presentation of the called number to the calling user requires the use of the local toll table:

Table 175: Number prefix table:

Context	International PNAC-Prefix	National PNAC-Prefix	Subscriber PNAC-Prefix	L2 PNAC-Prefix	L1 PNAC-Prefix	L0 PNAC-Prefix
ANY/ANY	8-011	8-1	8-			

Table 176: Number definition table requires the office code definitions::

Context	NPI	CC/L2	AC/L1	LOC/L0	Skip	Min	Max	Local Toll
ANY/ANY	Public	1	561	923	2	11	11	Boca-Toll

Table 177: Local Toll table used for the Boca office code 1-561-923:

Context	Name	Country Code	Home Area Code	Home Exchange Code	Dial Pattern
ANY	Boca-Toll	1	561	923	National

Table 178: Exchange Code Lists belonging to the Boca-Toll table:

Area Code	Dial Pattern	Exchange Codes
561	Subscriber	206 208 210 212 213 218 226 237 239 241 243 245 251 265 266 271 272 274 276 278 279 280 287 288 289 297 300 302 305 306 314 322 330 338 347 350 353 361 362 367 368 372 376 378 381 391 392 393 394 395 400 404 414 416 417 431 435 438 441 442 443 445 447 450 451 454 455 456 457 458 470 477 479 482 483 487 488 495 496 498 499 504 505 520 522 526 542 544 549 558 573 613 620 636 637 638 654 665 666 672 674 699 702 703 705 706 715 716 749 750 756 773 789 807 809 819 824 826 843 852 859 860 862 864 865 866 869 870 883 886 892 893 894 900 901 908 910 912 921 922 923 926 927 929 939 945 948 953 955 961 962 981 982 988 989 991 994 995 997 998 999
754	Subscriber with Area Code	227 229 235 242 245 264 366 367 368 484
954	Subscriber with Area Code	227 234 242 246 247 254 255 263 281 282 283 301 304 312 317 323 324 333 340 341 344 345 346 354 360 363 366 369 379 415 418 419 420 421 422 425 426 427 428 429 461 464 477 480 481 482 501 509 510 520 531 532 539 543 545 553 569 570 571 573 574 575 580 582 586 590 592 596 597 601 603 621 623 633 642 650 656 657 671 675 688 690 691 692 695 697 698 708 718 719 720 721 722 724 725 726 729 738 743 751 752 753 755 757 773 775 778 780 781 782 783 784 785 786 788 794 796 798 803 818 821 825 827 834 840 856 857 861 867 871 876 899 905 913 917 933 934 935 941 942 943 944 946 947 949 956 957 960 968 969 970 971 972 973 974 975 977 978 979 984

Table 179: Number normalization rules to handle the Subscriber and National Nature of Address from the destination codes table:

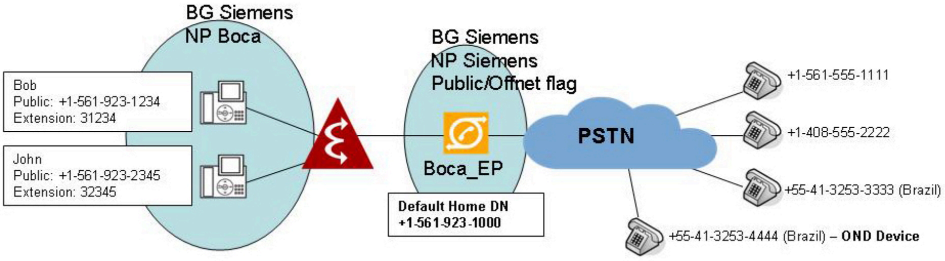
Context	Input Type of Number	Input Pattern	Output Type of Number	Output Expression
Siemens/Siemens/ Boca_EP	Subscriber	Z	International	1561{1}
Siemens/Siemens/ Boca_EP	National	Z	International	1{1}

Table 180: Number modification rules

Originating Context	Terminating Context	Input Type of Number	Input Type of Number	Priority	Output Type Of Number	Prefixed	Optimized Type Of Number
ANY/ANY	ANY/ANY/ NONE	ANY	4	Input Number	ANY	YES	Subscriber

SIP Gateway requires Default Home DN for International Numbers

For incoming calls, the SIP Gateway provides prefixed international or national numbers. For outgoing calls, the PSTN provider accepts only prefixed National numbers as calling party number. In this scenario John is called on his ONS number which deflects the incoming calls to a cell phone number in Brazil.



Expected Results:

User A	User B	Calling Party Number provided by Gateway	Calling Party Device ID presented to CSTA	Calling Party Number sent to GW
Bob	John (ONS) → +55-41-3253-4444 (OND)	N/A	+15619231234	915619231234
+1-561-555-1111		915615551111	+15615551111	915615551111
+1-408-555-2222		914085552222	+14085552222	914085552222
+55-41-3253-3333		9011554132533333	+554132533333	915619231000

Figure 87: Default Home DN used for International Numbers

For the calling party number, the Display Number Modification tables are consulted for creating the calling party number (originating context) for a call to the called party (terminating context).

Table 181: Number prefix table:

Context	International PNAC-Prefix	National PNAC-Prefix	Subscriber PNAC-Prefix	L2 PNAC-Prefix	L1 PNAC-Prefix	L0 PNAC-Prefix
Siemens/ Siemens	9-011	9-1	9			

Table 182: Number definition table requires the office code definitions::

Context	NPI	CC/L2	AC/L1	LOC/L0	Skip	Min	Max	Local Toll
ANY/ANY	Public	1	561	923	2	11	11	Boca-Toll

Table 183: Number definition table requires the office code definitions:

Context	Input Type Of Number	Input Pattern	Output Type Of Number	Output Expression
Siemens/ANY/ALL	Unknown	9011-Z	International	{2}
Siemens/ANY/ALL	Unknown	91-X{10}	International	1{2}

Table 184: Number modification rules

Originating Context	Terminating Context	Input Type of Number	Input Type of Number	Priority	Output Type Of Number	Prefixed	Optimized Type Of Number
ANY/ANY/	Siemens/ Siemens/ Boca_EP	ANY	1	Input Number	National	Yes	None
ANY/ANY/	Siemens/ Siemens/ Boca_EP	ANY	4	Input Number	ANY	Yes	Subscriber

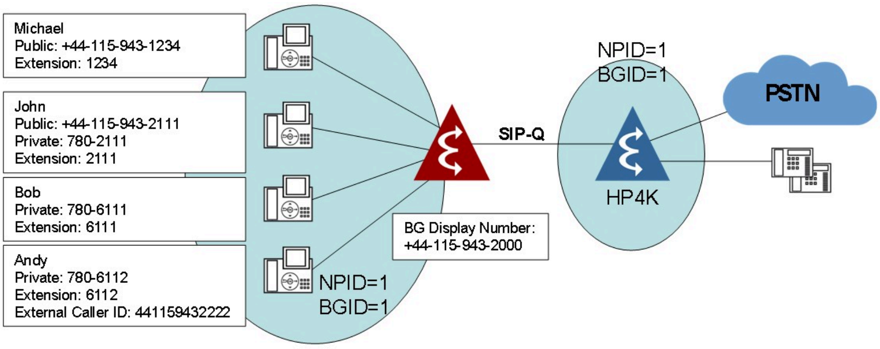
The first rule only succeeds if a national number can be created from the normalized number. An incoming international number from the gateway to John's ONS number cannot be optimized to a national number for the Boca_EP using this rule. The next rule uses the Default Home DN of the gateway which is a US number and can therefore be optimized to a national number for the Boca_EP.

6.2.50.6 Display Number Modification Use Cases - Outgoing Calls from a SIP Subscriber to a SIP-Q Endpoint (Gateway/PBX)

SIP-Q endpoint expects to receive PUBLIC numbers

There are 4 use cases described:

- One where the call is made by Michael to the Beeston PBX.
- One where the call is made by John to the Beeston PBX..
- One where the call is made by Bob to the Beeston PBX. Bob does not have a public number, so the Default Home DN assigned to the Beeston PBX is used for the call.
- One where the call is made by Andy to the Beeston PBX. Andy has an external caller ID configured so this gets used for the call.



Expected Results:

User A	User B	Calling Party Device ID presented to CSTA	Calling Party Number presented sent to HP4K
Michael	HP4K	+441159431234	441159431234, NOA=INT
John		+441159432111	441159432111, NOA=INT
Bob		7806111	441159432000, NOA=INT
Andy		7806112	441159432222, NOA=INT

Figure 88: SIP-Q Endpoint expects to receive public numbers

NOTICE:

Note that for Bob, the Default Home DN assigned to the Beeston SIP-Q endpoint is used, because there's no external caller ID configured.

Table 185: Number definition table requires the office code definitions:

Context	NPI	CC/L2	AC/L1	LOC/L0	Skip	Min	Max	Local Toll
ANY/ANY	Public	4	115	923	3	12	12	Beeston-Tolll

Context	NPI	CC/L2	AC/L1	LOC/L0	Skip	Min	Max	Local Toll
Siemens/ ANY	Private		2	533	3	7	7	Beeston-Toll

Table 186: Number conversion table only for allowed conversions:

Context	Input Pattern	Input Type of Number	Output Expression	Output Type of Number	Auto-Reverse
Siemens/ Beeston	44115943-[1-4]XXX	International	780{2}	L0	True

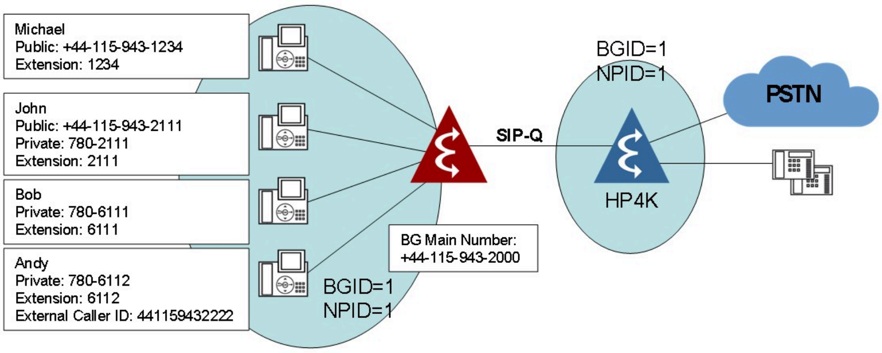
Table 187: Number modification rules:

Originating Context	Terminating Context	Input Type of Number	Input Type of Number	Priority	Output Type Of Number	Prefixed	Optimized Type Of Number
ANY/ANY	Siemens/ Beeston/ Beeston_EP	ANY	1	Input Number	International	No	None
ANY/ANY	Siemens/ Beeston/ Beeston_EP	ANY	2	Default Home DNr	International	No	None

SIP-Q endpoint expects to receive PRIVATE numbers

There are 4 use cases described:

- One where the call is made by Michael to the Beeston PBX. Michael does not have a private number, so his extension (1234) is sent to the Beeston PBX.
- One where the call is made by John to the Beeston PBX. John's private number is sent to the Beeston PBX
- One where the call is made by Bob to the Beeston PBX. Bob's private number is sent to the Beeston PBX
- One where the call is made by Andy to the Beeston PBX. Andy's private number is sent to the Beeston PBX.



Expected Results:

User A	User B	Calling Party Device ID presented to CSTA	Calling Party Number presented sent to HP4K
Michael	HP4K	+441159431234	1234, NOA=Unknown
John		+441159432111	7802111, NOA=L0
Bob		7806111	7806111, NOA=L0
Andy		7806112	7806112, NOA=L0

Figure 89: SIP-Q Endpoint expects to receive private numbers

Table 188: Number definition table requires the office code definitions::

Context	NPI	CC/L2	AC/L1	LOC/L0	Skip	Min	Max	Local Toll
ANY/ANY	Public	44	115	923	3	12	12	Beeston-Tolll
Siemens/ ANY	Private			780	3	7	7	Beeston-Toll

Table 189: Number conversion table only for allowed conversions:

Context	Input Pattern	Input Type of Number	Output Expression	Output Type of Number	Auto-Reverse
Siemens/ Beeston	44115943-[1-4]XXX	International	780{2}	L0	True

Table 190: Number modification rules:

Originating Context	Terminating Context	Input Type of Number	Input Type of Number	Priority	Output Type Of Number	Prefixed	Optimized Type Of Number
ANY/ANY	Siemens/ Beeston/ Beeston_EP	ANY	1	Input Number	International	No	None
ANY/ANY	Siemens/ Beeston/ Beeston_EP	ANY	2	Input Number	International	No	None
ANY/ANY	Siemens/ Beeston/ Beeston_EP	ANY	3	Input Number	International	No	None

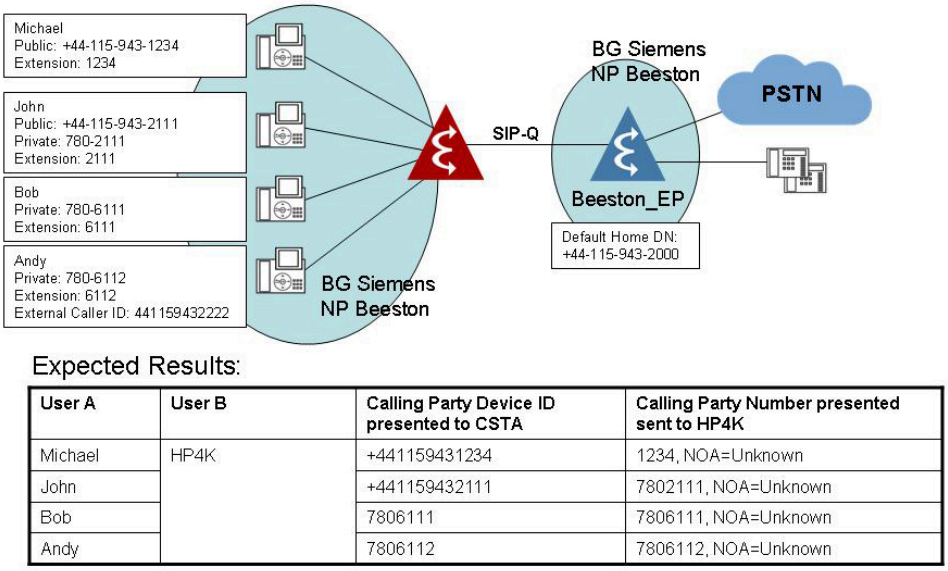
NOTICE:

Note that if no private number can be created, the international (E.164) public number will be presented.

SIP-Q endpoint expects to receive UNKNOWN numbers

This use case behaves pretty much like the use case above SIP-Q endpoint expects to receive PRIVATE numbers except that the numbering plan indicator and the nature of address are set to Unknown.

This is controlled via an attribute on the SIP-Q endpoint (Set NPI/TON to Unknown).



Expected Results:

User A	User B	Calling Party Device ID presented to CSTA	Calling Party Number presented sent to HP4K
Michael	HP4K	+441159431234	1234, NOA=Unknown
John		+441159432111	7802111, NOA=Unknown
Bob		7806111	7806111, NOA=Unknown
Andy		7806112	7806112, NOA=Unknown

Figure 90: SIP-Q Endpoint expects to receive unknown numbers

Table 191: Number definition table requires the office code definitions::

Context	NPI	CC/L2	AC/L1	LOC/L0	Skip	Min	Max	Local Toll
ANY/ANY	Public	44	115	923	3	12	12	Beeston-Tolll
Siemens/ ANY	Private			780	3	7	7	Beeston-Toll

Table 192: Number conversion table only for allowed conversions:

Context	Input Pattern	Input Type of Number	Output Expression	Output Type of Number	Auto-Reverse
Siemens/ Beeston	44115943-[1-4]XXX	International	780{2}	L0	True

Table 193: Number modification rules:

Originating Context	Terminating Context	Input Type of Number	Input Type of Number	Priority	Output Type Of Number	Prefixed	Optimized Type Of Number
ANY/ANY	Siemens/ Beeston/ Beeston_EP	ANY	1	Input Number	FQPN	No	None
ANY/ANY	Siemens/ Beeston/ Beeston_EP	ANY	2	Default Home DN	Extension	No	None
ANY/ANY	Siemens/ Beeston/ Beeston_EP	ANY	3	Input Number	International	No	None

6.2.51 Display Number Modification - Normalization for CSTA

On the CSTA interface device identifiers must be in either GNF (including the '+') or in Fully Qualified Private Number format. This has for consequence that when receiving calls from SIP endpoints or subscribers, normalization of the incoming calling party number may be required. The number normalization tables must be set up to allow this normalization.

Public SIP Subscribers

OpenScape Voice supports 2 types of public SIP subscribers (External DN flag is checked):

- **With country code:** the SIP subscriber is already normalized and the GNF number is presented by inserting a '+' before the Home Directory Number. There are no display number modification rules required in this case.
- **Without country code:** the SIP subscriber is normalized by looking up a match for the subscriber number in the number definition table. When found, a '+' and the country code are added in front of the Home Directory Number.

Private SIP Subscriber

OpenScape Voice supports 3 types of private SIP subscribers:

- With L2 code
- With L1 code (without L2 code)
- With L0 code (without L1 code or L0 code)

The SIP subscriber is normalized by looking up a match for the home directory number in the number definition table. When a match is found, the contents of the definition entry may be used to normalize the number if necessary (this would be very unusal).

SIP Endpoints

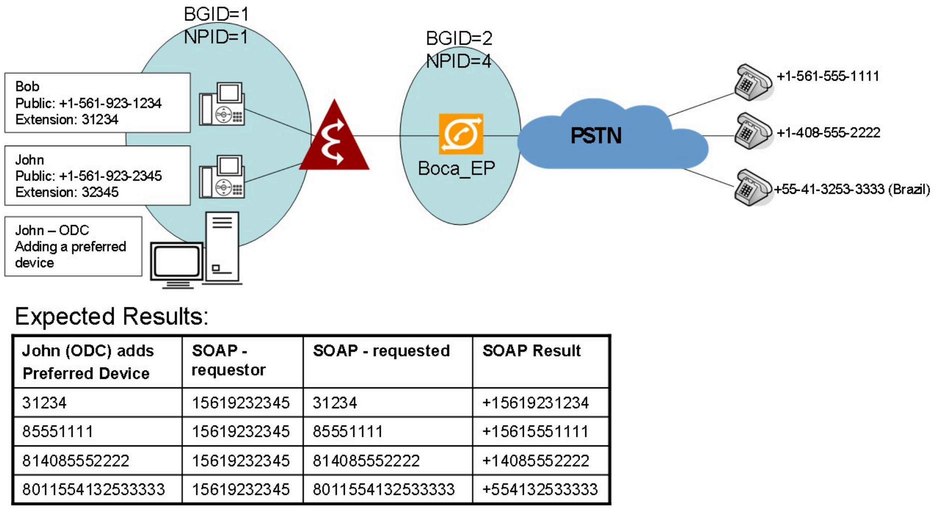
Numbers received from SIP are first subjected to the Number Normalization table. Normally all normalization rules should be found there. However if the normalization rule is not found, normalization can still occur using the number prefixes table (if the received number format is unknown) and/or the number definition table:

SIP-Q Endpoints

Numbers received from SIP-Q endpoints should already be normalized. However, just like with numbers received from SIP endpoints, these numbers are subjected to the Number Normalization table and if necessary the Number Prefixes and/or the Number Definitions table.

6.2.52 Display Number Modification - Normalization for SOAP

Normalization for SOAP is the same as normalization for CSTA, except that instead of the number received from the endpoint or subscriber, the result from translation is used. The SOAP interface allows an application to request the normalized number for a dialed string given the context of the Home Directory Number of a subscriber on OpenScape Voice.



Expected Results:

John (ODC) adds Preferred Device	SOAP - requestor	SOAP - requested	SOAP Result
31234	15619232345	31234	+15619231234
85551111	15619232345	85551111	+15615551111
814085552222	15619232345	814085552222	+14085552222
8011554132533333	15619232345	8011554132533333	+554132533333

Figure 91: Normalization for SOAP

To support the normalization for SOAP (required in case of adding a preferred device to ODC or supporting the OSC Voice Portal), translation tables and number modification tables need to be set up.

Translation tables can be set up as follows:

Table 194: Prefix Access Codes Table

Numb. Plan	PAC	Min	Max	Digit Position	Insert Digits	Prefix Type	NOA	Destination
Boca	8011	4	30	4	-	Off-Net	INT	None
Boca	81	12	12	2	-	Off-Net	NAT	None
Boca	8	8	8	1	-	Off-Net	SUB	None

Table 195: Destination Codes Table

Numb. Plan	Digits	NOA	Destination Name
Boca	5	INT	GwyBocaInt
Boca	4	NAT	GwyBocaNat
Boca	5	SUB	GwyBocaSub

Table 196: Destinations Table

Numb. Plan	Destination Name	Route	Endpoint	Delete Digits	Insert Digits	NOA
Boca	GwyBocaInt	1	Boca_EP	0	9011	Unknown
Boca	GwyBocaNat	1	Boca_EP	0	91	Unknown
Boca	GwyBocaSub	1	Boca_EP	0	9	Unknown

For the calling party number, the NDAL tables are consulted for creating the calling party number (originating context) for a call to the called party (terminating context).

The input to the number modification tables would then be:

- INT/15619231234 (normalized by inserting '+')
- SUB/5551111 (requires number definition)
- NAT/4085552222 (requires number definition)
- INT/554132533333 (normalized by inserting '+')

The number definition rules above will apply as well to normalize national and subscriber numbers to international:

Table 197: Number definition table::

Context	NPI	CC/L2	AC/L1	LOC/L0	Skip	Min	Max	Local Toll
ANY/ANY	Public	1	561	923	2	11	11	Boca-Toll

NOTICE:

The rules for which number to pass to the number modification's normalization function are to use the input from the destination codes table unless the nature of address is unknown at the destination codes table and is not unknown at the route table. In the above example, the nature of address was International, National or Subscriber at the destination codes table and therefore these numbers were used.

SOAP Normalization Exception

As can be seen from the previous, the normalization for SOAP is handled as soon as the number modification rules are entered correctly throughout the system, with the following exception:

Call to a SIP-Q endpoint where translation returned a nature of address EXTENSION. The extension will be sent back as the normalized number.

6.2.53 Accounting Management

This comprehensive OpenScape Voice management solution permits for unified administration of networks made up of OpenScape Voice real-time IP systems, applications, and industry-standard third-party products.

It consists of:

- Fault Management
- User Management
- QOS Management
- **Accounting Management**

6.2.54 SIP UA Forking

OSV supports Microsoft Skype for Business (MS SfB) providing the MS SfB Mediation Server anchors all media streams between the OSV and MS SfB network domain, meaning that there is no ability to bypass the MS SfB Mediation Server in support of a more direct media path. Lack of MS SfB Media Bypass prevents supporting more advanced features in Microsoft's view, leads to possible MS SfB Mediation Server scaling, increased total cost of ownership and potential QoS issues.

With OSV V10.R3.PS30 onwards, OSV supports Microsoft Skype for Business Media Bypass. For calls routed to the MS SfB network, the MS SfB Mediation Server detecting SfB MB is supported exposes the connecting SIP server (OSV) as a SIP UAC to SIP forking responses according to RFC3261/RFC3264.

Two feature functionalities are provided, each addressing various SIP endpoint IETF RFC3261 compliance levels, endpoint early media capabilities and to minimize feature risk:

- OSV Passive Forking (UAC) provides an interworking function which essentially merges multiple MS SfB downstream early dialogs into a single upstream SIP dialog. This functionality shields upstream SIP clients (SIP UAC) establishing sessions with the MS SfB network from being exposed to the full RFC 3261/RFC3264 forking proxy server behavior of the MS SfB Mediation Server.
- OSV Passive Forking (Proxy) reduces the OSV SIP dialog interworking above as OSV behaves more like a SIP proxy.

IMPORTANT:

OSV supports SIP forking only when OSV interworks with Microsoft Skype for Business (MS SfB). Without interworking with Microsoft Skype for Business (MS SfB), OSV doesn’t support SIP UA Forking. This means that OSV establishes only a single early session dialog with UAS, even if UAS (SIP Forking Proxy) sends two provisional responses containing two different tags.

Configuring SIP Passive Forking

In order to configure the MS SfB SIP Forking, you have to follow the steps below

1) Enable the feature. Go to **Configuration** > **OpenScape Voice** > **Administration** > **Signaling Management** > **SIP**

   Click the **SIP UA Forking** tab and select **Enabled** from the drop-down menu of the **OSV Passive Forking** parameter.
2) Add the devices you want to include and assign **SIP UA Forking Capability** to everyone of them. For detailed information, see chapter *How to Configure SIP UA Forking*.
3) If you want to set up Endpoint Templates, go to **Configuration** > **OpenScape Voice** > **Administration** > **General Settings** > **Endpoint Templates**

   Click **Add** and the **Add Endpoint Template** window pops-up. Select the SIP tab and select a value for the SIP UA Forking Support parameter. For detailed information, see chapter *How to Edit SIP Settings for Endpoint Templates*. This step is optional.
4) Set up the Endpoints (Skype for Business side). Go to **Configuration** > **OpenScape Voice** > **Business Group** > **Members** > **Endpoints**

   Click **Add** and the **Add Endpoint Template** window pops-up. Fill in the necessary parameters from the **General** tab. Select the **SIP** tab and select a value for the **SIP UA Forking Support** parameter. Also, enable the **Limited PRACK Support** attribute. For detailed information, see chapters *Endpoints and Endpoint Management* and *How to Configure SIP Settings for the Endpoint*.
5) Set up the Subscribers (OSVA side). Go to **Configuration** > **OpenScape Voice** > **Business Group** > **Members** > **Subscribers**

   Click **Add** and the **Add Subscriber** window pops-up. Fill in the necessary parameters from the **General** tab. Select the **Connection** tab and select a value for the **SIP UA Forking Support** parameter. For detailed information, see chapter *How to Configure Connection Settings for Subscriber*.

Scenarios for setting up OSV Passive Forking

There are four different scenarios for setting up OSV Passive Forking. Of course there are more combinations, but these four scenarios are the proposed ones.

1) **OSV Passive Forking (Proxy) with MS SfB SIP Forking**

   The OSV assumes a SIP proxy server like role in handling early session dialogs. In this configuration, termed **OSV Passive Forking (Proxy)**, the SIP endpoint UA-A as a UAC processes early session media, according to RFC3261.

   For this scenario the configuration must be the following:

   - Endpoint: The parameter **SIP UA Forking Support** must have the value **Full**.
   - Subscriber: If the Subscriber is **Dynamic**, then the **SIP UA Forking Support** parameter must have the value **Automatic** and the Device from the Device Identifier list must have SIP UA Forking Capability "Full". In case of a **Static** subscriber, the **SIP UA Forking Support** parameter must have the value **Full**.
2) **OSV Passive Forking (UAC) with MS SfB SIP Forking**

   In this configuration, the SIP endpoint UA-A supports only a single early session dialog, accepting changes to the early media session as they occur. However this capability deviates from RFC3261 compliance statements requiring that once a UAC receives an SDP answer in a provisional response, establishing an early session dialog, any additional SDP received by that UAC must remain unchanged until the session is answered, meaning, effectively ignored, unless other signaling procedures are supported.

For this scenario the configuration must be the following:

- Endpoint: The parameter **SIP UA Forking Support** must have the value **Full**.
- Subscriber:
  - If the Subscriber is **Dynamic**, then the **SIP UA Forking Support** parameter must have the value **Automatic** and the Device from the **Device Identifier** list must have **SIP UA Forking Capability** "None".
  - If the Subscriber is **Static**, then the **SIP UA Forking Support** parameter must have the value **None**.

3) **OSV Passive Forking - No Support for MS SfB SIP Forking**

If neither *OSV Passive Forking (Proxy)* nor *OSV Passive Forking (UAC)* support is possible for the SIP UAC establishing a SfB session, OSV is able to effectively disable MS SfB early session media changes. In this configuration the SIP UAC user experience should be similar to today's OSV integration where MS SfB Media Bypass (MB) is not possible. In other downstream SIP UAS configurations where downstream the SIP Forking Proxy supports a gateway model to maintain a single session with the SIP UAC.

For this scenario the configuration must be the following:

- Endpoint: The parameter **SIP UA Forking Support** must have the value **None**.
- Subscriber:
  - If the Subscriber is **Dynamic**, then the **SIP UA Forking Support** parameter must have the value **Automatic** and the Device from the **Device Identifier** list must have **SIP UA Forking Capability** "None".
  - If the Subscriber is **Static**, then the **SIP UA Forking Support** parameter must have the value **None**.

4) **Disabling the OSV Passive Forking for specific devices**

For this scenario the configuration must be the following:

- Endpoint: The parameter **SIP UA Forking Support** must have the value **Full**.
- Device: Must have the **SIP UA Forking Capability** "Disabled".
- Subscriber:
  - If the Subscriber is **Dynamic**, then the **SIP UA Forking Support** parameter must have the value **Automatic** and the Device from the Device Identifier list must have SIP UA Forking Capability "Disabled".
  - If the Subscriber is **Static**, then the **SIP UA Forking Support** parameter must have the value **Disabled**.

6.2.55 Endpoints and Endpoint Management

Endpoints are external devices, e.g. Gateways, Proxies or SIP Trunks and also SIP endpoints, like SIP telephones and analog endpoints.

An endpoint is a network component, such as an originating or terminating device. An endpoint can be a DN that does not have a number associated with it yet. A profile enables you to set parameters for that endpoint.

Endpoint State "Registered"

Contacts of SIP Subscribers that are registered via a SIP Proxy can have the special states ‚renewed’ and ‚suspended’.

- **Suspended**

  Whenever a registration binding of a contact that is registered via a SIP Proxy times out, an audit of the registration binding is performed if the Registration Renewal feature is activated.

  The 'Suspended' state is reached by the SIP UA when the audit to the registration binding fails or when a call to the registration binding times out. While in Suspended state, the SIP proxy will continue to be monitored for becoming available again via a scheduled audit and calls will not be attempted directly to the registration binding and features like (Enhanced) Subscriber Rerouting may become active if OpenScape Voice is configured to do so.
- **Renewed**

  Once the SIP proxy of a suspended registration binding becomes accessible again because of a successful scheduled audit, all registration bindings of contacts that previously registered via that proxy enter the 'Renewed' state. During the time that a registration binding is in ‘Renewed’ state, calls can be made again to the registration binding via the SIP proxy.

  The only difference with the ‘Registered’ state is that the registration binding will be removed if the SIP UA contact does not re-register within a single registration cycle.

These states are set by the switch in the case of a WAN outage.

Endpoint Operational States

Endpoints can be in one of the following **Operational States**:

- **Normal State**

  The Normal operational state of a SIP endpoint indicates that communication with the endpoint is possible.
- **Inaccessible state**

  The Inaccessible state of a SIP endpoint indicates that a scheduled audit is running against the SIP endpoint. In this state only OPTIONS requests are sent to the endpoint.
- **Communication Lost state**

  The Communication Lost state indicates that OSV could not communicate with the SIP endpoint. In this state no audit is scheduled or running against the endpoint. In this state, no restrictions are imposed on sending messages to the endpoint, even though they are expected to time out.

IMPORTANT:

When the Periodic Audit is enabled, the operational state of the SIP endpoint changes to **Normal - Auditing** and **Inaccessible - Auditing**. The **Communication Lost** state remains the same.

Endpoint Management Levels

Endpoints and Endpoint Profiles can be managed on the following two levels:

- on the system-wide level
- on the Business Group level.

6.2.55.1 SIPSM (SIP Signaling Manager)

The OSV system communicates to all SIP endpoints (phones, gateways, other SIP servers, etc.) using its SIPSM (SIP Signaling Managers).

1) **SIPSM1** (named sipsm1_vip in `node.cfg`). This SIPSM is used by the 1st node for communicating with:
   - All UDP and TCP endpoints (phones, gateways, servers, etc)
   - TLS phones (not gateways, servers, etc)
2) **SIPSM2** (named sipsm2_vip in `node.cfg`). This SIPSM is used by the 2nd node, and it is used for the same purposes as SIPSM1.
3) **SIPSM3** (named sipsm3_vip in `node.cfg`). This SIPSM is used by 1st node for communicating with:
   - ALL (M)TLS servers and gateways (not phones).
4) **SIPSM4** named sipsm4_vip in `node.cfg`). This SIPSM is used by 2nd node, and it is used for the same purposes as SIPSM3.

When you want to connect your OSV system with another server using (M)TLS, then you must configure in the corresponding endpoint the use of SIPSM3 or SIPSM4.

SIP IP usage in a node failover case depends on the `node.cfg` configuration parameter “Node-Separation”:

- If set to ‘none’, the SIP IPs are moved to the surviving node and an OSV SIP communication partner is not impacted.

  NOTICE: Exception is a node in Stand Alone operation mode, which may happen if X-channel and admin connectivity between the nodes is broken and “Stand Alone Service” is Enabled (another `node.cfg` parameter). In this case the partner IP address is not activated because the OSV node has to assume that its partner node is still active.

- If set to ‘separate’, the SIP IPs never move, which means that a SIP endpoint that is communicating with node 1 needs to be aware of and support the node 2 IP address if node 1 is out of service.

  SIPSM1 -> **SIPSM2** and **SIPSM3** -> **SIPSM4** (and vice versa).

Independent of the node status a SIP endpoint may send its messages to the IP address of the partner node, e.g. after the communication to the currently used node has failed. (Note that in case of TLS the endpoint has to re-register first and create a new TLS connection).Similarly the OSV SW may decide to try to use the partner node for communication to the endpoint, if the communication via the currently used OSV IP is not working.

While support of two OSV SIP IPs is mandatory for the network separated case it is not necessary, therefore optional, for the case with “Node-Separation” = none.

However two OSV SIP IPs are recommended , not necessarily for a co-located OSV cluster, but especially for a so called L2 geo-separated installation, where the two OSV nodes are at different locations.

6.2.55.2 TLS Configuration procedure for connection between Two OpenScape Voice Systems

Three “tools” are needed to configure TLS between two OpenScape Voice systems: NCPE, CLI and the OpenScape Voice Assistant.

The configuration is similar as setting for inter-OSV call via SIPQ (or SIP) over TCP. The difference is **SIMPSM**specially for SIPQ(or SIP) over TLS when configuring endpoints.

1) Before fresh installation for an OSV system, two SIPSM IP addresses (**SIPSM3** and **SIMPSM4**) must be configured into node.cfg via NCPE

2) After installation, check if these two IP address are successfully added into OSV by running command:`netstat –anp |grep ttud`

3) Enter CLI menu and select

- Application-level Management...................6
- Signaling Management.............................2
- SIP Management......................................2
- Set All Parameters....................................1

to enable SIP server version.

4) Open the OpenScape Voice Assistant

5) Create Endpoint Profile

6) Create Endpoint in Global Numbering Plan

7) Create Destination in Global Numbering Plan

8) Create Route for Destination

9) Create PAC in GNP

10) Create e.164 DN and point to the Destination created in step 8

11) Create PAC in PNP and point to E164NANP

6.2.55.3 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).

6.2.55.4 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 endpoint definition must have:

- A name (just an alphanumeric string).
- Type – 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 OpenScape Voice).
- An IP address or FQDN (for example, server31.siemens.com), if the device is to be statically registered.

NOTICE:

If dynamic registration is selected, the user cannot enter an IP addressor 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.
- The name or alias for the gateway. The alias is the name string by which the gateway will register with the OpenScape Voice (if it is dynamically registered) and the name by which the gateway will be known in the SIP registrar database.

NOTICE:

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.

6.2.55.5 Registration Request from SIP Endpoint

The SIP Registrar process receives the registration request and calls XDM to update the shared memory (XLA) and database.

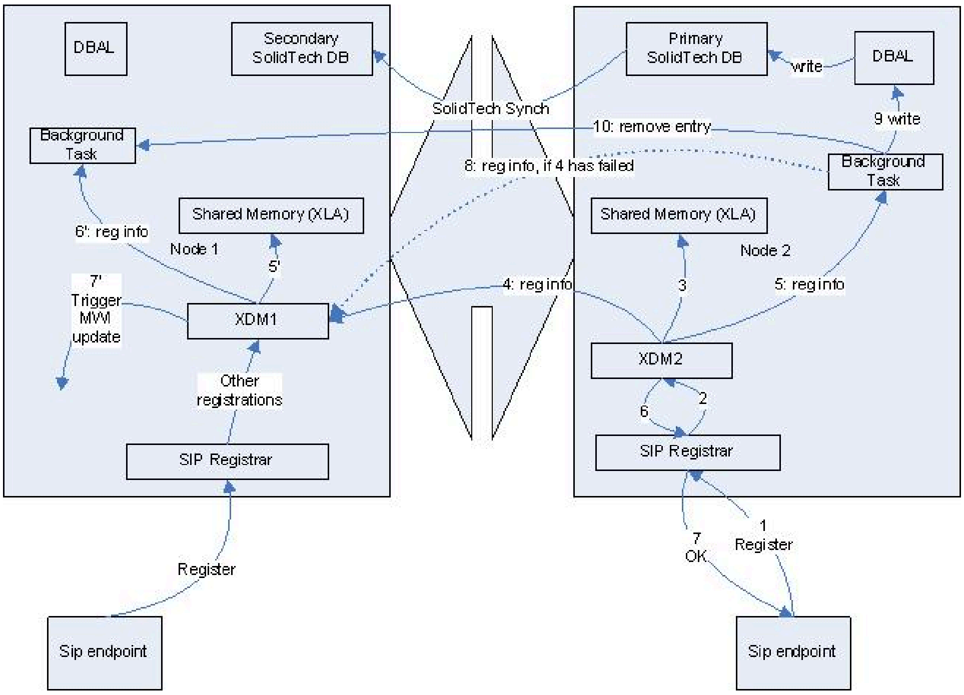


Figure 92: SIP Registrar process

Functional Sequence

XDM updates the memory, sends a best effort synch message to the partner XDM, add an entry to the local background task queue to update the database and acknowledges back to the SIP Registrar.

- If the registration synch message could be sent to the partner the background task entry is marked as 'synchronized".
- If not (most likely because the partner node is out of service, XDM triggers an MWI update by a message to FSN.

The partner XDM reads the registration synch message, updates XLA, stores the message in the background task queue (marked as synchronized) and triggers an MWI update by sending a message to FSN.

The background task on the node with the primary database sequentially stores the registration information in the database. Once stored it informs the background task on the partner node to remove this entry from its queue.

If an entry in the queue is not marked as synchronized the background task tries to send it to the partner XDM. If this is not possible

With this re-design there are no delays in the processing path and it should be possible to handle about 50 registrations per second.

NOTICE:

Today the X3650T IBM server can do 20 new registrations/sec without x-channel delay

The partner node processes registrations in parallel. In order to handle race conditions of registration requests for the same phone received over both nodes, a timestamp is added to the registration synch message and registration updates with an older timestamp are discarded.

Startup of node without connection to partner node

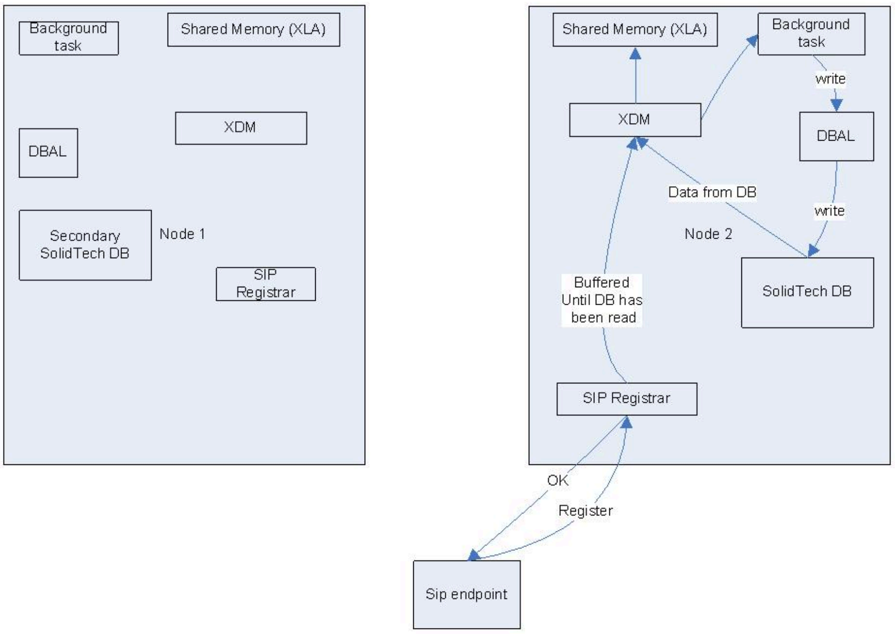
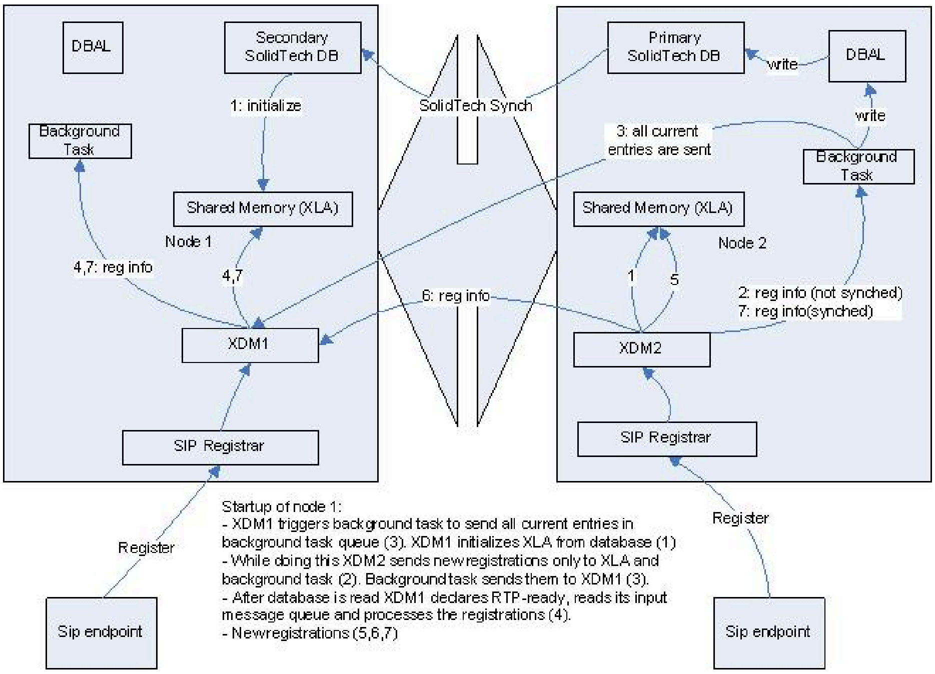


Figure 93: Startup of single node

When a HiPath node starts-up without connection to the partner node XDM initializes XLA with data from the database. New registrations from the SIP registrar are processed after XLA is initialized.

Startup of node with connection to partner node



Startup of node 1:
- XDM1 triggers background task to send all current entries in background task queue (3). XDM1 initializes XLA from database (1)
- While doing this XDM2 sends new registrations only to XLA and background task (2). Background task sends them to XDM1 (3).
- After database is read XDM1 declares RTP-ready, reads its input message queue and processes the registrations (4).
- Newregistrations (5,6,7)

Figure 94: Startup of 2nd node

Before XDM on the starting node reads data from the database it sends a message to the background task on the partner node. The background task marks all current entries in its queue as 'not synchronized', acknowledges back to the starting XDM and starts sending all current entries to the process message queue of the starting XDM.

The starting XDM now updates XLA with registration data from the database while receiving, but not processing, registration synch messages from the partner background task.

Once the database has been read XDM declares RTP-Ready and starts processing messages from its message queue:

- Synch messages from the partner background task
- New registrations from the network
- Synch messages from the partner XDM

Registration synchronization during upgrade and standalone

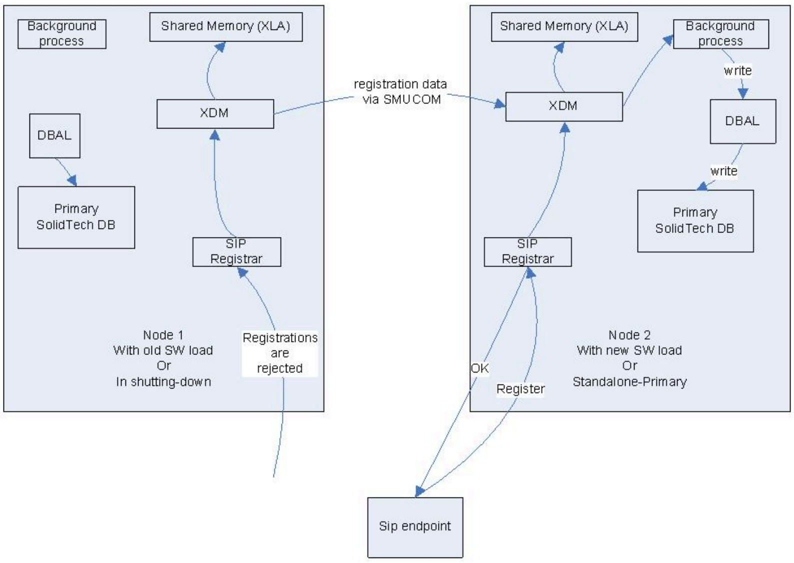


Figure 95: Synchronization during Upgrade and Standalone

When during upgrade call-processing is about to be switched to the node with the new SW load or when a node in standalone-secondary is about to be rebooted to re-join the cluster, registration data need to be synchronized that are not stored in the database of the node that will take over all call processing.

There is no change to current concept. XDM marks all registrations that need to be synchronized and copies them via SMUCOM. There is only one acknowledgement, generated by SMUCOM back to XDM after the last copied registration

There is no 'normal' registration synchronization of XLA and database since RTP and PrimeCluster consider the partner node to be out of service.

Modifications to the current implementation are necessary since not all registrations may be stored in the database, some may still be in the background task queue.

6.2.55.6 Notification of encrypted calls on behalf of Network and 3rd Party Device EPs

OSV inserts the 'secure call' notification header on behalf of 3rd party devices when the call is considered secure and on behalf of network endpoints when these endpoints have been marked as secure via administration.

Up to now in the OSV solution the OSCAR-defined proprietary header '**X-Siemens-Call-Type: ST-secure/ST-insecure**' is being used to notify a device that the call is secure end-to-end. The definition of secure is that both the signaling and the media are encrypted (TLS+SRTP). The indication of the call's security is done via a padlock icon on the device's display. Since the '**X-Siemens-Call-Type**' proprietary header is only supported by Unify devices, such as OpenScape Desk CP phones, a secure call between a Unify device and a 3rd party device does not appear secure on the Unify device. The same problem arises for a call between a Unify device and a device behind a network endpoint such as a gateway or another PBX although the customer may have taken the appropriate measures to consider that endpoint as secure.

Both problems above are solved by having the OSV insert the header '**X-Siemens-Call-Type: ST-secure**' on behalf of 3rd party devices and network endpoints.

To achieve that for network endpoints, the endpoint attribute **Treat endpoint as secure** needs to be enabled.

For 3rd party devices this is enabled globally through **OpenScape Voice** > **Administration** > **Signaling Management** > **SIP**.

6.2.56 Bulk Editing Endpoints

The **Bulk Edit** feature allows the user to modify more than one data record of the same entity simultaneously via the GUI.

This modification is possible for the following entities containing nonunique fields:

- Subscribers
- **Endpoints**
- Destination Codes

To bulk edit certain parameters, the checkboxes on the left side must be checked. **Only the activated parameters have an impact on the selected Subscribers**. Parameters without a checkbox are not editable in The **Bulk Edit** mode.

6.2.57 Aliases

Once you have determined the Endpoints you can create Aliases and, at the same time, associate these Aliases with the Endpoints. For SIP endpoints, up to five aliases are allowed. All Aliases created within OpenScape Voice must be unique. This is because these Aliases are used to determine where a received SIP request originated.

An alias can be an IP address, an FQDN or the combination of IP address/ FQDN and a port separated by a colon:

- IPv4Address (e.g 10.10.10.10 or with port 10.10.10.10:5060)
- IPv6Address or IPv6 Reference (e.g 10::10:10, [10::10:10] or with port [10::10:10]:5060). Entering an IPv6 Address in square brackets is known as IPv6 Reference. Ports can only be added to IPv6 References.
- FQDN

  The RTP parameter `Srx/Sip/CentralSbcSupport` needs to be set to RtpTrue to make OpenScape Voice look for port numbers in addition to the IP Address/FQDN.

Aliases for Endpoints

To know which aliases need to be entered for endpoints, the administrator needs to know the contents of the SIP messages that the endpoints sends to OpenScape Voice. Most requests contain a Contact header and OpenScape Voice will add the host part of the Contact header to the Alias lookup. Some messages do not contain a header. For these messages, OpenScape Voice uses the host or the host:port pof the Bottom Via header for the Alias lookup. For endpoints that register, the user part, user@host or the user@host:port part of the To header of the REGISTER request is used for the Alias lookup.

Aliases for Subscribers

OpenScape Voice automatically creates an alias with the subscriber's Home Directory Number when creating a subscriber.Requests from subscribers are recognized by looking up the user or user@host or user@host:port part of the received From header as Aliases, with the exception of the REGISTER request in which case this informations is obtained from the To header.

Aliases for ENUM

When OpenScape Voice contacts an ENUM server for translation, the resulting FQDN received from the ENUM server is looked up as an Alias in order to ensure that the endpoint or subscriber that will receive the call is either registered or trusted by OpenScape Voice.

Aliases for Hosting

In a hosted environment, multiple Business Groups can be spanned across OpenScape Voice systems by setting up so-called 'virtual endpoints'.

A virtual endpoint is an endpoint that is created with a single Alias that is an FQDN that resolves to the own SIP server as IP address. As long as the endpoint uses that same FQDN to send SIP requests to OpenScape Voice, it will be recognized by this FQDN (which is the host part of the Request URI) rather than by the host part of the Contact header or the bottom Via header.

As the request URI of a SIP request always points to the intended target OpenScape Voice system, this results in the following:

1) The OpenScape Voice that is sending the request must be set up to use FQDNs rather than IP addresses in the Primary Signaling field because this FQDN will be used by the target OpenScape Voice as an alias to find the OpenScape Voice system that sent the request.

2) The OpenScape Voice that is receiving the request must configure the FQDN received in the domain part of the Request URI as an alias for the endpoint that represents the sending OpenScape Voice.

Translation

The OpenScape Voice SIP registrar supports dynamic and static (permanent) alias registrations, and performs alias translation to resolve aliases to an IP transport address, when it receives a call request from the endpoint. If another server manages the endpoint, the aliases are translated into the call signaling transport address of the far-end server. These aliases are case-sensitive.

When to Use Ports in Aliases

The use of ports in aliases is necessary when there are multiple endpoints sharing the same IP address or FQDN. So, the `Srx/Sip/CentralSbcSupport` RTP parameter should always be set to RtpTrue.

An example of proper usage would be obviously when a central SBC replaces the IP addresses, it receives on the access side with its core side IP address and assigns a different core side port number for each access side IP address.

Without looking for ports in the SIP requests, OpenScape Voice would not have a chance to determine from which endpoint the request originated.

Another usage could be to force the endpoint that sends SIP requests to use TLS security. TLS connections are usually opened from a different port (port 5061) than TCP connections or UDP packets (both from port 5060). To guarantee OpenScape Voice only accepts packets sent from the secure port 5061, an alias with the IP address or FQDN and the secure port can be administered on OpenScape Voice. If the endpoint sends packets from its unsecure port, OpenScape Voice will reject the incoming request with a 403 Forbidden response.

6.2.58 Attributes for a SIP Endpoint

The SIP Endpoint Attributes affect how OpenScape Voice handles the SIP header fields.

Functionality of the attributes

The following bulleted items describe the functionality for each of the attributes available for the selected SIP endpoint:

- **Supports SIP UPDATE Method for Display Updates**

  This attribute indicates whether the SIP Trunking endpoint supports receiving a SIP UPDATE method without SDP and with a P-Asserted-Identity (or P-Preferred-Identity) header field for display updates. This attribute is only applicable for SIP Trunking endpoints and it is automatically enabled for SIP Private Networking endpoints. In addition, this attribute only makes a difference if the SIP Trunking Endpoint Profile has Privacy Support set to Full or Full-Send.

  NOTICE: The OSV only supports SIP UPDATE in the special case of Display Updates.

- **UPDATE for Confirmed Dialogs Supported**

  NOTICE: This attribute is no longer in use.

- **Survivable Endpoint**

  If selected (enabled), the endpoint provides survivability in a branch office.

  NOTICE:

  This attribute is required for the "Subscriber Rerouting" feature. Subscriber rerouting is only executed for subscribers whose Associated Endpoint has this attribute set; applicable only to SIP endpoint.

- **SIP Proxy**

  If selected (enabled), the endpoint is a SIP proxy, applicable only to SIP endpoint.

  This attribute is not applicable for SIP Private Networking.

- **Central SBC**

  This attribute is introduced from OSV V8 onwards for proxy/SBC endpoints and can be selected (enabled) only if the **SIP Proxy** attribute is enabled. **Central SBC** attribute and **Allow Proxy Bypass attribute** are mutually exclusive so if one is checked the other automatically is unchecked. If the attribute is selected (enabled) it indicates that the endpoint is a Central SBC and any subscriber associated to this endpoint is considered a remote user from the SIP-Registar and is allowed to register only if the respective check box **Registration via Central SBC Allowed** is ticked.

  NOTICE:

  From V8 onwards, to control whether a subscriber is allowed or not to register via a Central SBC, the endpoint attribute **Central SBC** must be set for all endpoints that are central SBCs. If this precondition is met, whether a subscriber is allowed or not to register via the central SBC can be controlled via the subscriber checkbox **Registration via Central SBC Allowed**.

- **Route via Proxy**

  When selected (enabled), this endpoint can be:

  – a SIP proxy, when selecting the SIP Proxy attribute, requesting to be on the route when the OpenScape Voice is making an outbound call to a subscriber that has this endpoint as its Associated Endpoint.
  – a SIP endpoint with a valid Associated Endpoint, for example an OSB proxy, which is configured to route the calls via proxy. This attribute is required when OSV should also route the SIP singling via proxy.

  IMPORTANT:

  The parameter `Srx/Sip/CentralSbcSupport` related to **Route via Proxy** attribute is by default set to **RtpTrue**. If it is changed to **RtpFalse** the attribute under the endpoint configuration will have no effect and routing problems may also be created.

- **Allow Proxy Bypass**

  Proxy Bypass allows OpenScape Voice to bypass the recorded proxy in a contact if an INVITE request to the contact's recorded proxy does not receive a response within a specified time.

  This attribute is not applicable for SIP Private Networking.

  Use the “Proxy bypass” attribute for the OSB proxy endpoint when it operates in the following modes: Proxy, SBC Proxy and Proxy ACD

  Don’t use the “Proxy bypass” attribute for the OSB proxy endpoint when it operates in the following modes: Proxy ATA and Branch SBC

- **Public/Offnet Traffic**

  When selected (activated), this attribute allows the subscriber marking all calls from/to an endpoint as external regardless whether the called or calling is intra-BG or not. OpenScape Voice doesn’t update the displays for External Calls, when the call is forwarded/diverted or transferred.

IMPORTANT:

When you need to update the displays for External Calls, set the parameter `Srx/Main/UpdateDisplaysForExternalCalls` to RtpTrue. Then OSV updates the display for parties involved in an external call whenever the partner information changes, exactly as for internal Calls.

NOTICE: The `Srx/Main/UpdateDisplaysForExternalCalls` parameter must be set to RTpTrue in case the SIPREC based OpenScape Voice Call Recording solution is enabled.

- **Accept Billing Number**

  When selected (activated), this attribute makes sure that calls get charged to the right call account.

  NOTICE:

  This attribute is achieved by transporting the user number in the additional SIP CDR header field "X-Siemens-CDR" for the endpoint used.

- **Use Billing Number for Display Purposes**

  This attribute can be activated only if the attribute **Accept Billing Number** is activated.

  The combination of both attributes is used on endpoints that send charge numbers for outbound calls or blind transfers and where the Administrator wishes to use this number for display purposes.

  Currently OpenScape Xpressions and OpenScape UC conference bridge send a charge number for outbound calls.

  The possible combination of these two attributes (**Accept Billing Number** and **Use Billing Number for Display Purposes**) have the following result:

  – Not having either attribute set, means that the charge number in a received X-Siemens-CDR header is ignored.
  – Having only **Accept Billing Number** set but not **Use Billing Number for Display Purposes**, means that the charge number is used for authorization and authentication purposes and will show up in CDR records. If however the "charge number" and "From number" of the incoming INVITE request have different formats of the same subscriber number, the charge number is used as display number (e.g. when setting up Xpressions mailbox using extensions of subscribers).
  – Having both **Accept Billing Number** and **Use Billing Number for Display Purposes** set, means that the charge number is used for authorization and authentication purposes and will show up in CDR records and is used for display purposes as well.

- **Allow Sending of Insecure Referred-By Header**

  If selected (activated), this attribute makes sure that calls get charged to the right call account.

  NOTICE:

  This attribute is achieved by transporting the user number in the additional SIP CDR header field "X-Siemens-CDR" for the endpoint used.

- **Override IRM Codec Restriction**

  If selected (enabled), the Override IRM Codec Restrictions attribute will be assigned to the selected subscriber.

- **Transfer HandOff**

  If selected (enabled), during transfer handoff, REFER and NOTIFY transactions will be passed transparently through OSV. Used for TRANSFER_HANDOFF for Genesys.

- **Send P-Preferred-Identity rather than P-Asserted-Identity**

  If selected (enabled), a P-Preferred-Identity (PPI) header field will be sent whenever a P-Asserted-Identity (PAI) header field would normally be sent.

  This attribute is primarily intended for use when connecting to a SIP Service Provider that does not accept a P-Asserted-Identity SIP header field.

  NOTICE:

  This attribute can only be configurable for SIP Trunking endpoints. This attribute is automatically disabled for SIP Private Networking endpoints.

  The **Diversion header** field is used on the SIP Private Networking interface to transport the diverting/re-directing party number and the reason for the diversion.

- **Send domain name in From and P-Preferred-Identity headers**

  If selected (enabled), the host part of the From and P-Preferred-Identity (or P-Asserted-Identity) SIP header fields will contain the domain name of the OpenScape Voice node.

  Note that if calling number presentation restrictions apply the host part of the From header field will contain 'anonymous invalid'.

  NOTICE:

  This attribute is primarily intended for use when connecting to a SIP Service Provider that does not accept dotted IP addresses in calling user identification SIP header fields.

- **Send Redirect Number instead of calling number for redirected calls**

  If selected (enabled), a call that is redirected to the endpoint will have the last redirecting or transferring party's identity in the From and P-Asserted-Identity (or P-Preferred-Identity) SIP header fields. This attribute is primarily intended for use when connecting to a SIP Service Provider that does not understand the Diversion header field.

NOTICE:

This attribute can only be configured for SIP Trunking endpoints. This attribute is automatically disabled for SIP Private Networking endpoints.

- **Do not send Diversion header**

  If selected (enabled), a SIP Diversion header field will not be sent. This attribute is primarily intended for use when connecting to a SIP Service Provider that can not accept a Diversion SIP header field. When this attribute is selected the 'Send forwarding number rather than calling number for forwarded calls' attribute will generally also be required.

  This attribute is normally used in conjunction with one of the following attributes:

  – Send redirecting number rather than calling number for redirected calls
  – Send authentication number in P-Asserted-Identity header
  – Send authentication number in From header

  NOTICE:

  This attribute can only be configured for SIP Trunking endpoints. This attribute is automatically disabled for SIP Private Networking endpoints.

- **Do not Send Invite without SDP**

  If selected (enabled), SIP reINVITE requests that do not include SDP will not be sent during redirection procedures. OpenScape Voice will reuse the SDP previously received from the endpoint to send as an SDP offer to the new partner endpoint. When the SDP answer is received the new SDP will be sent in a reINVITE and the 200 OK answer will be consumed by OpenScape Voice, if there is no change in SDP.*

  *When a codec or a port change occurs in this SDP, media renegotiation will be triggered. This attribute is also used when certain 3PCC (and other) Enterprise services are used. In this case, OSV sends an initial INVITE with a dummy SDP, instead of offer less INVITE. The attribute’s endpoint must meet the one mandatory requirement that the endpoint does not support SRTP.

  NOTICE:

  This attribute is primarily intended for use when connecting to a SIP Service Provider that can not accept a reINVITE request without SDP.

  NOTICE:

  "Do not send invite without SDP" is not used when OSV receives the initial INVITE without SDP offer and the terminating endpoint is configured with "Do not send invite without SDP".

- **Send International Numbers in Global Number Format (GNF)**

  When selected (enabled), the OpenScape Voice adds a '+' in front of all numbers which have NPI = PUBLIC and NOA = INTERNATIONAL. In order to do this, both Translation and the Display Number Modification tables MUST be provisioned to send numbers with NPI = PUBLIC and NOA = INTERNATIONAL to this endpoint. The following header field URI's apply:

  – Request-URI
  – From
  – To
  – P-Asserted-Identity
  – P-Preferred-Identity
  – Diversion
  – Referred-By

  NOTICE:

  This attribute can be configured both for SIP Trunking and for SIP Private Networking endpoints.

  If the endpoint attribute **Send International Numbers in Global Number Format (GNF)** is set to **true** on a **SIP Private Networking** endpoint, then all public numbers are sent to this endpoint in GNF format.

- **Rerouting Direct Incoming Calls**

  Check this checkbox to enable the rerouting of direct incoming calls through the PSTN. Values: Enabled/Disabled.

  NOTICE:

  Although using Subscriber Rerouting through the PSTN is useful during WAN failures and CAC bandwidth restrictions, it can also lead to additional charges for the PSTN calls.

- **Rerouting Forwarded Calls**

  If selected (enabled), this attribute allows subscriber rerouting of incoming calls through the SIP endpoint that are forwarded to a survivable SIP subscriber.

  NOTICE:

  Although using Subscriber Rerouting through the PSTN is useful during WAN failures and CAC bandwidth restrictions, it can also lead to additional charges for the PSTN calls.

- **Enhanced Subscriber Rerouting**

  If selected (enabled), this attribute enables enhanced subscriber routing, which pertains to the ability to reroute forwarded calls and hunt group calls.

- **Automatic Collect Call Blocking supported**

  When this option is enabled, calls from a PSTN Gateway (e.g. AudioCodes) to the subscriber result in additional SIP signaling (SIP INFO request) between OpenScape Voice and the PSTN Gateway.

  NOTICE:

  The PSTN Gateway recognizes this additional SIP signaling as an indication that collect calls are not allowed to this subscriber and initiates special CAS/ISDN signaling procedures ('double answer') towards the PSTN central office. These CAS/ISDN signaling procedures result in the call being cleared by the central office if the incoming call is a collect call. If the incoming call is not a collect call then the call proceeds as normal.

- **Send Authentication Number in P-Asserted-Identity header** (renamed **Send Authentication Number**) for SIP-Q endpoints.

  If this attribute is set then the P-Asserted-Identity (PAI) header contains the calling party's name and the dialable number.

  IMPORTANT:

  When setting the **Send Authentication Number in P-Asserted-Identity header** attribute, the display rules that are usually used for populating the PAI header are overridden, apart from the Number Display Modification rules. However, if the RTP parameter `Srx/Main/setDisplayRulesWhenAuthNumInPAI` is set to **RtpTrue**, then the display rules that are usually used for populating the PAI header will not get overridden.

  The authentication number is the number that the PSTN provider expects in order to allow the call to proceed.

  It depends on the provider which Authentication Header is used to get the authentication information. Three different parameters can be set to give the provider the required diverting or transferring party to appear on this or one of the following headers:

- **Send Authentication Number in Diversion Header**

  If this attribute is enabled, the Do Not Send Diversion Header attribute must be disabled.

  NOTICE:

  This attribute only applies to SIP Trunking endpoints.

- **Send Authentication Number in From Header**

  The authentication number is the number that the PSTN provider expects in order to allow the call to proceed.

  It depends on the provider which Authentication Header is used to get the authentication information. Some providers only use the From header and therefore require the diverting or transferring party to appear in the From header. Others look in the P-Asserted-Identity for this information. Others again look in the Diversion header.

NOTICE:

This attribute can only be configured for SIP Trunking endpoints. This attribute is automatically disabled for SIP Private Networking endpoints.

IMPORTANT:

When this attribute is activated due to the Emergency Calling Subnets functionality (see chapter "Emergency Calling") configuration via a SIP trunking endpoint, a Default HomeDN is needed. The Default HomeDN is used for fallback purposes (for example, when a call from a CPS endpoint is routed to the SIP trunk endpoint, OSV is not aware of any HomeDN number which is to be used) therefore the Default HomeDN has to be configured. For more information, see chapter "Home Directory Numbers".

- **Use SIP Endpoint Default Home DN as Authentication Number**

  If this attribute is set, the Default Home DN provisioned for the SIP endpoint is used to populate the authenticated number.
- **Use Subscriber Home DN as Authentication Number**

  If this attribute is set, the OSV call originator or feature subscriber’s Home DN is used to populate the authenticated number.

NOTICE:

The attributes **Use SIP Endpoint Default Home DN as Authentication Number** and **Use Subscriber Home DN as Authentication Number** are used to control what authentication identity is to be used when sending the INVITE requests towards a SIP endpoint. They are mutually exclusive. The default (unselected or unchecked) identifies that the existing OSV identity field selection logic applies.

- **Set NPI/TON to Unknown**

  This endpoint attribute only applies to SIP-Q Private Networking endpoints. It is unchecked and grayed out for SIP Private Networking and SIP Trunking endpoints. When set, all presentation numbers sent to the SIP-Q PBX or gateway will have their numbering plan identifier and type of number reset to Unknown. This is necessary in case the SIP-Q network was set up using an unknown numbering plan. This attribute will be checked by SIPSM.
- **Include Restricted Numbers in From Header**

  If the SIP Trunking Endpoint Profile's Privacy Support is set to Full (or Full-Send) and the SIP endpoint has the "Include Restricted Numbers in From Header" attribute, the OpenScape Voice SHALL NOT anonymize the Name and User portion of the From header field when the calling party identity is restricted.

NOTICE:

This attribute is only be configurable for SIP Trunking endpoints and it is automatically disabled for SIP Private Networking endpoints. In addition, this attribute makes only a difference if the SIP Trunking Endpoint Profile has Privacy Support set to Full or Full-Send.

- **SIPQ Truncated MIME**

  The private network allows OSV registered user agents/clients to communicate with other users/resources in the private network connected via LAN/WAN using SIP protocol, or, for migrating customers, SIPQ protocol (i.e., SIP signaling with QSIG protocol embedded as a **MIME** for call control and supplementary service interoperability) for interworking with legacy QSIG private networks. SIP Trunking is used to interwork calls over the public network (IP or non-IP based) via "mediating GWs" (e.g., OpenScape SBC, SBC) which provide functions such as Network Address Translation (NAT), proxy services, media conversion.
- **Enable Session Timing**

  SIP SM provides the Session Timing endpoint attribute (Endpoint_Session_Timer) that will identify the Session Timing option per SIP-NNI/SIPQ endpoint.

  When enabled, session timing will be possible on the SIP-NNI/SIPQ interface for all calls that exist on that link.

  Enable/disable session timing on a specific endpoint:

  – When "Enable Session Timer" attribute is **true** session timing is invoked.
  – When "Enable Session Timer" attribute is **false** session timing is not invoked.

  If session timing is **enabled** the SIP INVITE request to NNI and SIP endpoints will include the tags to enable session timer for that call. OpenScape Voice and the endpoint will negotiate who will refresh the session during the call (usually OpenScape Voice ends up being the refresher).

  When the RTP parameter `"Srx/Sip/Session_Timer"` is set to **YES** then session timing feature is enabled only for subscribers. If the RTP parameter value is set to **NO** then the session timing feature is disabled for subscribers. For SIP-NNI/SIPQ endpoints, session timing feature is enabled if only the value of the SIP-NNI/SIPQ endpoint attribute is enabled.

  There will be no linkage between the switch wide session timing attribute (via RTP parameter) and the endpoint attribute to control session timing. The following rules to enable/disable session timing will apply for various endpoints.

Switch-wide optionRTP parameter	SIPNNI/SIPQ Endpoint attribute	Session timing on subscriber devices	Session timing on SIP-NNI/ SIPQ Endpoint
Session Timing Enabled	Session Timing Disabled	Session Timing Enabled	Session Timing Disabled

Switch-wide optionRTP parameter	SIPNNI/SIPQ Endpoint attribute	Session timing on subscriber devices	Session timing on SIP-NNI/ SIPQ Endpoint
	Session Timing Enabled	Session Timing Enabled	Session Timing Enabled
Session Timing Disabled	Session Timing Disabled	Session Timing Disabled	Session Timing Disabled
	Session Timing Enabled	Session Timing Disabled	Session Timing Enabled

NOTICE:

There is no linkage between the RTP parameter to control session timing and the endpoint attribute (applicable per endpoint). RTP parameter applies to subscribers only. Endpoint attribute applies per endpoint (SIP or SIPQ). Default value for the attributes is false which is applied during upgrades.

- **Ignore Answer for Announcement**
- **Enable TLS RFC5626 Ping**

  The attribute enables the RFC5626 connectivity check feature for outgoing TLS connections. The default value for this attribute is disabled/unchecked.
- **Enable TLS Dual Path Method**

  The attribute enables the ’Dual Path’ method, in which a client to server TLS connection is used for all outgoing SIP requests. SIP responses are expected to be received on the same TLS connection as the SIP request that is responded to. The default value for this attribute is disabled/ unchecked.

IMPORTANT:

The attributes **Enable TLS RFC5626 Ping** and **Enable TLS Dual Path Method** can be selected only for MTLS endpoints. To set an Endpoint as MTLS the **Transport protocol** value must be set to **MTLS**.

- **Ignore Receipt of 181 Call is Being Forwarded**

  Enabling this attribute, allows SIPSM to ignore the 181 Response Code for trunk gateways when external OND forward calls to different networks. OSV only supports call forwarding from an internal OND and the attribute is used for cases where the trunk gateways cannot honor the DSS call type (do not forward) indication on their terminating side.
- **Reserve** Attributes for Endpoints

  The intention of the reserved attributes is to use them only in exceptional cases where the regular process of adding endpoint attributes can not be applied due to time constraints. Usage of these reserve attributes must be explicitly approved by development management before proceeding. There are three Reserve Attributes available:
- – **Reserve 6**

- **Reserve 8**

NOTICE:

Once a Reserve Attribute has been used then it should be replaced with a proper named attribute as soon as practical.

- **Use extended max count for loop prevention**

  The attribute is used for Endpoints that common numbers terminate too and you want to allow common numbers to use a higher max CFLoop counter (i.e. RTP parameter `Srx/Service/CFLoopMaxCountExtended`) while maintaining a low max counter for the overall system (i.e. RTP Parameter `Srx/Service/CFLoopMaxCount`).

  When the attribute is set then the extended max counter has the value of RTP parameter `Srx/Service/CFLoopMaxCountExtended.`

- **Do Not Audit Endpoint**

  By setting this attribute, the audit of that specific Endpoint can be turned off. The default value is enabled.

INFO:

The **Do Not Audit Endpoint** attribute should only be used for dummy Endpoints.

- **Use Proxy/SBC ANAT settings for calls to subscribers**

  This attribute can be selected only for proxy endpoints (‘SIP proxy’ attribute set)

- **Support for Callback Path Reservation**
- **Send Progress to Stop Call Processing Supervision Timer**
- **Limited PRACK Support**

  The PRACK-Lite feature provides a limited form of RFC3262 PRACK within OSV, supporting PRACK on a half-call basis and only for SIP network-network interfaces:

  - There is no end-to-end PRACK behavior - OSV as a B2BUA supports all requirements for PRACK as a SIP UAC or SIP UAS, i.e., with PRACK-Lite, PRACK interworking is always performed on each interface independently.
  - OSV does not support PRACK for SIP subscriber interfaces. A SIP Subscriber will not receive any indications that PRACK is used in the network.
  - CSTA, SIP-Q and OSV Services are not aware of any PRACK communication requirements.
  - PRACK interworking is supported only if enabled on a per-SIP network-network interface basis. Only if PRACK support is enabled will a SIP network-network interfaces receive indications from OSV that PRACK is supported or required.
  - PRACK with additional SDP Offer is not supported. In this case, PRACK will be rejected with a "403 Forbidden" response.

- **Support Media Redirection**

  Use this attribute for the SIP endpoint, which is not able to process multiple SDP answers in the same dialog.

  When this endpoint attribute is enabled and there is a need for redirection before the call is answered (for example, Call Forward No Answer), OSV redirects the dialog to be reestablished by sending a "302 Moved Temporarily" response, to receive the new SDP offer. OpenScape Voice sends a "302 Moved Temporarily" response to SIP UAC to perform redirection and an rtag URI parameter is included in the Contact header. This rtag parameter is returned in the request URI of the subsequent new SIP INVITE.

  NOTICE:

  The SIP UAC must support SIP redirect server procedure, in order to use the SIP endpoint attribute “Support Media Redirection”.

- **Voice Mail Server**

  This endpoint attribute must be set for voice mail endpoints (for example XPR) only. It is used as an indication for calls that are forwarded/redirected to the Voice Mail server.

- **Disable Long Call Audit**

  When calling or called party has this attribute set to true, long call audit is disabled for this call. Default value is unchecked.

  If the attribute is checked then it will eliminate the impact of the long call duration timer on Hoot and ARD (Automatic Ring Down) lines used in trading solutions.

  It will also use the RTP `Srx/Sip/Reduced_Session_Timer_Value` to define the minimum session refresh value for calls to/from the SIP endpoint with this attribute checked. The default value for **Srx/Sip/Reduced_Session_Timer_Value** is 90000 (90 seconds). The allowed range for the parameter is 60000-1800000.

- **Send/Receive Impact Level**

  The attribute is used to control the ’Impact Level’ notifications that the endpoint sends/receives to/from other endpoints. ’Impact Level’ notifications inform the user when an incoming call originates from a lower security zone, or when an outgoing call terminates in a lower security zone.

  Possible values: Checked and Unchecked. Default value: unchecked (false).

  NOTICE:

  The attribute is applicable only for SIP-Q endpoints. In addition appropriate SIP settings must be configured in order for the attribute to be enabled.

- **Do not send alphanumeric SIP URI**

  When this attribute is enabled, it is possible to prevent sending an alphanumeric SIP URI to a SIP endpoint. The default value is unchecked (false).

- **Send alphanumeric SIP URI when available**

  When this attribute is enabled, it is possible to enable the SIP Endpoint to preferably send alphanumeric SIP URI when one is available. The default value is unchecked (false).
- **Support Peer Domains**

  When this attribute is enabled, it allows an SBC to send its IP address or FQDN to a Contact URI parameter in case it receives a contact URI from a dynamic peering domain. The default value is unchecked (false).
- **ACD Call Distribution Device**

  When this attribute is enabled, any call transferred from this endpoint device, is identified to the transferred-to device as an ACD call. The default value is unchecked (false).

  NOTICE:

  The transfer service must be enabled in the associated endpoint profile.
- **Apply Default Home DN for Incoming Calls**

  This endpoint attribute is set to support alphanumeric SIP URI calling identity replacement with an TN alias for incoming tenant calls routed to destinations unable to process alphanumeric SIP URI's. OSV utilizes the configured SIP endpoint default home DN for the tenant TN alias as the calling identity which may also be used as tenant specific authenticated number. The default value is unchecked (false).

  NOTICE:

  This attribute is not configurable for "SIP-Q Signaling" Endpoints and Endpoint Templates.
- **Allow endpoint to Unregister Stale Registrations**

  When this endpoint attribute is set, unregistration messages initiated by the endpoint will not be challenged by OSV with digest authentication as long as the endpoint is recorded to have been on the path that was taken on the initial registration of the contact which expired at this endpoint.
- **Enable Media Termination Point (MTP) Flow**

  This EP attribute must be set when interworking with Cisco™ endpoints that have the Media Termination Point (MTP) feature enabled.
- **Video Call Allowed**

  If the **Video Call Allowed** check mark is turned **ON** (default), then the OpenScape Voice will allow video calls across the server.

  If the **Video Call Allowed** check mark is turned **OFF**, then even if endpoint makes video calls, the port of all video m-lines will be set to zero by the OpenScape Voice server before routing the call to intended receiver.
- **Trusted Subscriber**

  When this SIP subscriber endpoint attribute is set then OSV offers the capability to verify whether the IP address used by the SIP subscriber in the bottom Via header is trusted. The attribute is used to support backward compatibility of RTP flag **Srx/Main/AuthTraverseViaHdrs** with the **RtpTrue** setting.

- **Enable Fast Connect**

  This Endpoint attribute is available only for SIP-Q endpoints and when checked it enables a fast connection for SIP-Q connections in direct call scenarios.
- **Circuit Connector Appliance**

  This Endpoint is applicable only to non-subscriber endpoints and when checked OSV supports sending/receiving ansible client API JSON mime objects in the body of SIP messages over the SIP trunking interface.
- **Add Route Header**

  This Endpoint SIP attribute is applicable only for SIP Trunking endpoints and, when checked, enables adding a Route Header to SIP requests other than the initial INVITE.
- **Disable SRTP**

  When the attribute is checked, then SRTP is not offered to the endpoint and removed when offered by the endpoint. An Encryption license is not checked out with this setting. When the attribute is unchecked SRTP is allowed to and from the endpoint, and If Encryption license checking is enabled in the OSV license file, an Encryption license is checked out when a subscriber registers a contact using TLS. By default the attribute is unchecked.
- **Include OSV SIP User-Agent header field**

  This attribute allows the SIP Provider to use this SIP attribute to be able to recognize a SIP soft switch and apply dynamically a profile to this SIP soft switch and monitor it.
- **Do Not Allow URNs in R-URI/TO Header for NG911 Calls**

  When the attribute is set, the ESRP replaces the emergency service urn in the R-URI with the URI discovered by the NG911 service. The outgoing message is like a normal call without the NG911 specific R-URI/To headers. The next hop URI is not included in a Route header. When the attribute is not set, then the normal ESRP functionality is applied. The default value of the attribute is False, that means not checked.
- **Accept x-channel header**

  When this attribute is set, the Endpoint accepts and parses the SIP proprietary X-Channel header
- **Suppress SPE in SIPQ**

  When this attribute is set, the SIP-Q interface does not send a security indication. SPE stands for Signaling and Payload Encryption. This attribute is only valid for the SIP-Q Signaling Endpoint Type.
- **Do not allow NG911 headers**

  This attribute allows you to control the transport of NG911 headers. When it is set, the NG911 headers are not transported towards the call taker's device. The default value is False, meaning unchecked.
- **Retrieve CBN from P-A-I header**

  This attribute allows the extraction of the Callback Number (CBN) from either the From header or the P-A-I header. Enabling this attribute, allows you to provision for each ingress endpoint configured, from which header the callback number can be retrieved from. The default value is False, meaning unchecked.

NOTICE:

This attribute is only applicable in ESRP mode.

- **Record All Calls**

  Check this attribute to allow an SRC capable OSB to support a Recording Session (RS). This subject interface is applicable to SIP-NNI and SIP subscriber endpoints. All calls requiring an RS are managed by the **SRC Capable** OSB.
- **SRC Capable**

  Check this attribute to allow an SRC capable OSB to support a Recording Session (RS). This subject interface is applicable only to SIP-NNI endpoint. Use this attribute to identify that a call is being managed by an OSB which also includes SRC agent capabilities.

  NOTICE:

  All **Record All Calls** subject interfaces must be routed via an **SRC Capable** interface which is also configured with **Route via Proxy**. This means that all calls requiring an RS are managed by the **SRC Capable** OSB.
- **Add Endpoint Name in Sip URI**

  By enabling this attribute, OSV generates a `To` header and `Request-Line` in the OPTIONS message by using SIP-URIs with the following format: `sip:userInfo@Host:port` where **UserInfo = Endpoint Name** and **Host: Endpoint IP Address** as a result. Its default value is **False**, meaning unchecked.

  NOTICE:

  The Attribute value affects only the SIP-NNI/SIP-T endpoints and controls only the requirement that is related to the To header and Request-Line SIP-URIs format.

  NOTICE: This attribute must be checked when the SIPREC based OpenScape Voice Call Recording solution is enabled.
- **Do Not Send Conference Indication (Hide isFocus)**

  When this attribute is checked, it controls the transport of the focus parameter in the contact header, to hide the conference from the originating networks.

- **Do Not Allow Geolocation Info**

  This attribute controls the transport of (i3) location info over the SIP interface for the particular destination. When checked, the OSV:

  – Strips off the Geolocation header field from the outgoing message
  – Strips off the Geolocation-routing header from the outgoing message
  – Strips off the PIDF-LO document transported in the body of the message for location-by-value use cases

  The default value is False meaning that location info will be transported properly. This attribute does not affect the transport of location info over the CSTA interface.
- **Ignore Location by Value on SIP INVITE/REINVITE**

  This attribute enables ESRP to ignore location value on SIP INVITE (reINVITE) and automatically refresh location by calling party before proceeding with setup. The default value is False, meaning unchecked.
- **Support Foreign Peer Domains**

  This attribute enables the usage of URI based routing without having the remote URL configured in Remote Location domain list. For incoming calls from the Access side (WAN), the call will be accepted when the destination in the request URI matches any entry in the white list. When the white list is empty, only outgoing calls coming from the Core side are allowed. This configuration is available only when remote endpoint type is set to `Gateway`.

  IMPORTANT:

  This attribute and the Support Foreign Domains one, are mutually exclusive, meaning you can’t enable them at the same time
- **Support Replaces Header**

  This attribute indicates that a single dialog identified by the header field is to be shut down and logically replaced by the incoming INVITE in which it is contained. This attribute is applicable over SIP trunk.
- **Increment SDP o-line**

  This attribute enables OSV to increment the SDP origin line in some trunk to trunk scenarios and is only applicable over SIP trunk and SIP-Q endpoints. The default value for this attribute is disabled/unchecked.

Applicable Interfaces

The following table summarizes which interfaces are applicable for each SIP Endpoint attributes.

Table 198: Applicability of SIP Endpoint Attributes

SIP Endpoint Attribute	SIP-Q Signaling	SIP Private Networking	SIP Trunking
Supports SIP UPDATE Method for Display Updates	NA	NA	X
UPDATE for Confirmed Dialogs Supported	X	NA	X
Survivable Endpoint	X	NA	X

SIP Endpoint Attribute	SIP-Q Signaling	SIP Private Networking	SIP Trunking
SIP Proxy	X	NA	X
Central SBC	X	NA	X
Route via Proxy	X	NA	X
Allow Proxy Bypass	X	NA	X
Public/Offnet Traffic	X	X	X
Accept Billing Number	X	X	X
Use Billing Number for Display Purposes	X	X	X
Allow Sending of Insecure Referred-By Header	NA	Enabled	X
Override IRM Codec Restriction	X	X	X
Transfer HandOff	X	NA	X
Send P-Preferred-Identity rather than P-Asserted-Identity	NA	Disabled	X
Send domain name in From and P-Preferred-Identity headers	X	NA	X
Send Redirect Number instead of calling number for redirected calls	NA	Disabled	X
Do not send Diversion header	NA	Disabled	X
Do not Send Invite without SDP	Disabled	NA	X
Send International Numbers in Global Number Format (GNF)	X	X	X
Rerouting Direct Incoming Calls	X	X	X
Rerouting Forwarded Calls	X	X	X
Enhanced Subscriber Rerouting	X	X	X
Automatic Collect Call Blocking supported	X	X	X
Send Authentication Number in P-Asserted-Identity header renamed to **Send Authentication Number** for SIP-Q endpoints	X	Disabled	X
Send Authentication Number in Diversion Header	NA	Disabled	X
Send Authentication Number in From Header	NA	Disabled	X
Use SIP Endpoint Default Home DN as Authentication Number	X	X	X

SIP Endpoint Attribute	SIP-Q Signaling	SIP Private Networking	SIP Trunking
Use Subscriber Home DN as Authentication Number	X	X	X
Set NPI/TON to Unknown	X	Disabled	Disabled
Include Restricted Numbers in From Header	NA	Disabled	X
SIPQ Truncated MIME	X	X	X
Enable Session Timer	X	X	X
Ignore Answer for Announcement	X	X	X
Enable TLS RFC5626 Ping	X for MTLS / NA for others	X for MTLS / NA for others	X for MTLS / NA for others
Enable TLS Dual Path Method	X for MTLS / NA for others	X for MTLS / NA for others	X for MTLS / NA for others
Ignore Receipt of 181 Call is Being Forwarded	X	X	X
Reserve 6	X	X	X
Reserve 8	X	X	X
Reserve 10	X	X	X
Use extended max count for loop prevention	X	X	X
Do Not Audit Endpoint	X	X	X
Use Proxy/SBC ANAT settings for calls to subscribers	NA	NA	X
Support for Callback Path Reservation	X	NA	NA
Send Progress to Stop Call Processing Supervision Timer	X	X	X
Limited PRACK Support	NA	NA	X
Support Media Redirection	X	X	X
Voice Mail Server	X	X	X
Disable Long Call Audit	X	X	X
Send/Receive Impact Level	X	NA	NA
Do not send alphanumeric SIP URI	X	X	X
Send alphanumeric SIP URI when available	X	X	X
Support Peer Domains	X	X	X
ACD Call Distribution Device	X	X	X

SIP Endpoint Attribute	SIP-Q Signaling	SIP Private Networking	SIP Trunking
Apply Default Home DN for Incoming Calls	NA	X	X
Allow endpoint to Unregister Stale Registrations	X	X	X
Enable Media Termination Point (MTP) Flow	X	X	X
Video call allowed	X	X	X
Trusted Subscriber	X	X	X
Enable Fast Connect	X	NA	NA
Circuit Connector Appliance	X	X	X
Add Route Header	Disabled	Disabled	X
Disable SRTP	X	X	X
Include OSV SIP User-Agent header field	NA	NA	X
Do Not Allow URNs in R-URI/TO Header for NG911 Calls	X	X	X
Accept x-channel header	X	X	X
Suppress SPE in SIPQ	X	NA	NA
Do not allow NG911 headers	Disabled	X	X
Retrieve CBN from P-A-I header	Disabled	X	X
Record All Calls	Disabled	X	X
SRC Capable	Disabled	X	X
Add Endpoint Name in Sip URI	X	X	X
Do not send Conference Indication (Hide isFocus)	X	X	X
Do Not Allow Geolocation Info	X	X	X
Ignore Location by Value on SIP INVITE/ REINVITE	X	X	X
Support Replaces Header	NA	NA	X
Increment SDP o-line	X	NA	X

- X = Attribute can be enabled or disabled
- Disabled = Attribute is automatically disabled;
- Enabled = Attribute is automatically enabled
- NA = Not Applicable

Send authentication in xxx header attributes

Most SIP Service Providers (SP) authenticate all incoming SIP calls to the SP to assert that the call has been originated by a subscriber (DID Number) that belongs to that SP.

For basic calls from a SIP subscriber to the SIP Service Provider the authentication is done with the calling party number provided in the **From** header or in the **P-Asserted-Identity (PAI)** header field.

The **From** header field contains the public identity (name and number) of the calling party in Fully Qualified Public Number format.

The **P-Asserted-Identity (PAI)** header contains the calling party’s name and dialable number.

However, for calls that are redirected or transferred to the SP, the calling party number may not be a subscriber that belongs in that SP. For these scenarios, the SP needs to authenticate the call based on the number of the redirecting or transferring subscriber. The **Send authentication number in xxx header** attributes are used in these scenarios to indicate in which SIP header-field(s) the OpenScape Voice system needs to include the number of the redirecting or transferring subscriber which will be used for authentication.

It is possible to set all three "Send authentication number in xxx header" attributes at the same time. In this case, the redirecting or transferring subscriber DN used for authentication would be included in the From, P-Asserted-Identity (or P-Preferred-Identity) and Diversion header-fields

6.2.58.1 Number and Name Identification on the SIP Private Networking interface: PAI-, From-, Private- and To- Header

PAI (P-Asserted Identity) Header

A P-Asserted-Identity (PAI) header field is used on the SIP Private Networking interface to carry identity information. The number in the PAI header field shall be a fully qualified number. It shall be a private number if the Srx/Main/OutGoingCallingPartyNumberType RTP variable is set to 1 (private) or 2 (unknown) and shall be a public number if the RTP variable is set to 0 (public). The information within the PAI header field can be used by the receiver for display purposes, feature handling, and billing features. .

In order to provide SIP-Q equivalent operation, the receipt and sending of PAI header field must be supported on the SIP Private Networking interface in the following requests:

- INVITE, re-INVITE, UPDATE w/o SDP
- and responses: 8X, 200 OK, 3XX, 480, 486

FROM Header

A From header field is used on the SIP Private Networking interface to indicate the calling party. The originating OSVC system may remove the original identity information from the received From header field from the client and may insert name and number information from the HiPath database. This header field always contains the public identity of the calling party. If the calling party does not have an external DID number, the BG main directory number is substituted. This information can be used by the receiver for display, billing. The calling party number may be sent to the public network. The From header field shall not be anonymized by the originating OSVC. Instead the terminating OSVC shall anonymize the From header field based on the value of the Privacy header field. This applies to all cases where the calling party activated (either through configuration or via access code) identification restriction.

PRIVATE Header

A Privacy header field is used on the SIP Private Networking interface to indicate whether the number and name in the PAI and the From header fields are restricted.

The number and name information should not be anonymized until sent on the SIP subscriber interface or towards an untrusted SIP endpoint. OSVC uses the Privacy header field value "id" to indicate that the name and number in the PAI and From header fields are restricted.

When only the name is restricted (i.e. the number is not restricted), then the name is anonymized (i.e. set to "anonymous") at local OSVC before sending the header field on the SIP Private Networking interface.

When only the number is restricted (i.e. the name is not restricted), then the Privacy header field must be set with value "id" to indicate restriction of the number. Unfortunately, this means that though the name is not restricted it will be anonymized at the OSVC interworking the SIP Private Networking to an untrusted SIP endpoint or to the SIP-Q Private Networking interface.

PAI and Privacy header fields are used during most feature operations. When an endpoint is configured for SIP Private Networking, configuration of Full Privacy support (i.e. 'trusted') SIP endpoint is implied. This means that even if it is not explicitly configured, this setting is assumed by the OSVC.

TO Header

A To header field is used on the SIP Private Networking interface to indicate the original called party to a called subscriber. No constraints on content (any URI scheme is supported).

6.2.59 EPP (Endpoint Profiles)

The OpenScape Voice Assistant EPP (Endpoint Profile) feature enables the administrator to create and manage an EPP for SIP network servers.

An endpoint is a network component, such as an originating or terminating device. An end point can be a DN (Directory Number) that does not have a number associated with it yet. An EPP enables you to set parameters for that end point..

6.2.59.1 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.

When initially created, the only parameter required for an endpoint profile is the profile name. Everything else can be defaulted, in the normal case.

6.2.60 EP (Endpoint) Template

EP (Endpoint) Templates contain a pre configured set of EP (Endpoint) Attributes and thus allow for easier EP administration.

Listed Endpoint Templates can be applied to an Endpoint. Applying an Endpoint Template to an Endpoint means assigning the Endpoint Attributes configured in the Endpoint Template to the Endpoint. The changes are reflected on the **Endpoint** > **Attributes** tab on the Endpoint dialog

Setting SIP Attributes for SIP trunking endpoints via Endpoint Templates

OpenScape Voice Assistant provides the ability to use endpoint templates that automatically assign SIP attributes to SIP trunking endpoints without having to manually assign each attribute individually.

SIP Trunk Service Providers

The system has predefined Endpoint Templates that can be applied to Endpoints of the SIP Trunk Service Providers.

NOTICE:

The SIP Trunk Service Providers endpoint templates are used only if OSV is connected to the provider via VPN or MLPS. If you are connecting OSV to the SSP via SBC then the templates you should use are SBC Endpoint Templates.

NOTICE:

The SIP Trunk Service Provider Endpoint Templates may have set a few or even none of the available Endpoint Attributes depending on the Provider’s configuration.

The Endpoint Templates defined by the system cannot be edited or deleted.

Dummy Endpoint Template

Dummy Endpoint Template is a system defined template with the following attributes and SIP configurations:

- Attributes:

  -Do Not Audit

  -Survivable

- SIP Configuration

  ANAT Support =Disabled

  SIP Trunking = true

  Registration Type =Dynamic

  ICE Support = Enabled

  SIP UA Forking Support = Automatic

To create a Dummy endpoint with the Dummy Endpoint Template you just have to provide a name (no endpoint should register using the Dummy name) and assign to it the Dummy Endpoint Template according to the instructions of chapter "*How to Assign an Endpoint Template to an Endpoint".*

NOTICE: Dummy endpoints – if used as a representative endpoint – still use a defined endpoint profile because it may be used for translation

6.3 OSV Call Control Dispatcher Pages (NOT FOR PRINT)

6.3.1 Please select the appropriate help topic

The GUI element from which the online help was called is used in different contexts. The adequate help topic depends on the task you are about to perform. Please select the appropriate one from the list of related topics.

6.3.2 Please select the appropriate help topic

The GUI element from which the online help was called is used in different contexts. The adequate help topic depends on the task you are about to perform. Please select the appropriate one from the list of related topics.

Related concepts

Community Groups on page 345

6.3.3 Please select the appropriate help topic

The GUI element from which the online help was called is used in different contexts. The adequate help topic depends on the task you are about to perform. Please select the appropriate one from the list of related topics.

Related concepts

OpenScape UC Application
Call Detail Record (CDR) on page 933

6.3.4 Please select the appropriate help topic

The GUI element from which the online help was called is used in different contexts. The adequate help topic depends on the task you are about to perform. Please select the appropriate one from the list of related topics.

Related concepts

Attributes for a SIP Subscriber

Classes of Service on page 553

Calling Locations on page 554

Location Codes and Private Numbering Plans on page 456

Routing Areas on page 553

6.3.5 Please select the appropriate help topic

The GUI element from which the online help was called is used in different contexts. The adequate help topic depends on the task you are about to perform. Please select the appropriate one from the list of related topics.

6.3.6 Please select the appropriate help topic

The GUI element from which the online help was called is used in different contexts. The adequate help topic depends on the task you are about to perform. Please select the appropriate one from the list of related topics.

6.3.7 Please select the appropriate help topic

The GUI element from which the online help was called is used in different contexts. The adequate help topic depends on the task you are about to perform. Please select the appropriate one from the list of related topics.

Related concepts

Emergency Calling

6.3.8 Please select the appropriate help topic

The GUI element from which the online help was called is used in different contexts. The adequate help topic depends on the task you are about to perform. Please select the appropriate one from the list of related topics.

6.3.9 Please select the appropriate help topic

The GUI element from which the online help was called is used in different contexts. The adequate help topic depends on the task you are about to perform. Please select the appropriate one from the list of related topics.

7 Connectivity

7.1 Networking

OpenScape Voice is a carrier-class SIP 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 IBM eServer xSeries servers using SuSe Linux Enterprise Server Operating System from Novell. The core protocol of OpenScape Voice is SIP. In addition to industry-standard SIP, OpenScape Voice supports SIP-Q (QSIG over SIP) for interfacing to legacy PBX systems.

7.1.1 Media Gateways HG 3540 and HG 3500

The media gateways HG 3540 and HG 3500 support the networking of one or more OpenScape 4000s with the OpenScape Voice IP network infrastructure. Voice data is transferred in packets through LAN/WAN networks. It processes call between circuit-switched networks and LANs; performs protocol translation, and support SIP trunking through IP networks.

The HiPath HG 3540 media gateway, used with the OpenScape 4000 V3.0, is a central component of the OpenScape 4000 IP convergence platform. The HG 3500 V4, used with the OpenScape 4000 V4R1 and later, is a comparable gateway that provides a higher capacity and up to 50% better performance than its predecessor.

Either of these gateways use SIP-Q to interface with the OpenScape Voice system, which permits it to interconnect PBX TDM and IP-based endpoints to endpoints in the public circuit-switched networks. It provides:

- Processing of incoming and outgoing calls between circuit-switched networks and LANs.
- Protocol translation between different transmission formats, communications procedures, and audio codecs.
- Support of SIP-Q trunking through IP networks, with full interworking support for and transparent transmission of all ISDN features of the configured ISDN protocol.

Other Characteristics

Either gateway can be configured in a point-to-multipoint voice and data network to provide companies operating at numerous dispersed locations with a high degree of network function transparency.

Each management station running TCP/IP and a compatible Web browser can access either gateway with password authorization. Either gateway also includes an embedded Web server.

7.1.2 Media Gateway HG 1500

The HiPath HG 1500 media gateway, used with the HiPath 3000 V7.0, is a central component of the HiPath 3000 IP convergence platform. It supports the networking of one or more HiPath 3000s with the OpenScape Voice IP network infrastructure.

Voice data is transferred in packets through LAN/WAN networks.The HG 1500 uses SIP-Q to interface with OpenScape Voice, which permits it to interconnect OpenScape Voice endpoints to endpoints in the public circuitswitched networks. It provides:

- Processing of incoming and outgoing calls between circuit-switched networks and LANs.
- Protocol translation between different transmission formats, communications procedures, and audio codecs.
- Support of SIP-Q trunking through IP networks, with full interworking support for and transparent transmission of all ISDN features of the configured ISDN protocol.

Other Characteristics

The following are the supported scenarios:

NOTICE:

These capabilities are only available on a PSR basis.

- HiPath 3000 as an exchange gateway for 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 OpenScape Voice with TDM (digital, analog, DECT) and IP/HFA subscribers connected to the HiPath 3000 gateway.
- Several HiPath 3000 systems as exchange gateways for digital exchange lines (ISDN, CAS, T1) for OpenScape Voice with TDM (digital, analog, DECT) and IP/HFA subscribers connected to the H3K gateways.

The HG 1500 can be configured in a point-to-multipoint voice and data network to provide companies operating at numerous dispersed locations with a high degree of network function transparency. Each management station running TCP/IP and a compatible Web browser can access the HG 1500 with password authorization. The HG 1500 also includes an embedded Web server.

7.1.3 SIP Private Networking

SIP Private Networking is the network protocol of choice when no QSIG legacy PBXs are in the customer network. This eliminates the need to convert between SIP and SIP-Q protocol for a station-to-station call between two OpenScape Voice systems. SIP Private Networking is sometimes also referred to as Enterprise SIP Trunking or Enterprise SIP Peering.

When the originating interface (i.e. SIP subscriber or SIP trunking endpoint) is SIP, the SIP Private Networking interface shall be used when the call is routed to another OSVC or the SIP Trunking interface when the call is routed to a gateway, configured for interworking SIP to a non-QSIG protocol (e.g. OpenScape SBC).

When the originating interface is a SIP-Q Private Networking endpoint, then SIP-Q Private Networking shall be used when the call is routed to another OSVC or gateway, configured for interworking SIP-Q to QSIG (e.g. OpenScape SBC, HiPath 3000 or HiPath 4000).

The basic rule is to provision trunking routes through the private network with the same protocol as used for the incoming call request at the originating OSVC system. This way, one or no conversion between SIP and SIP-Q occurs on the end-to-end path of any one call.

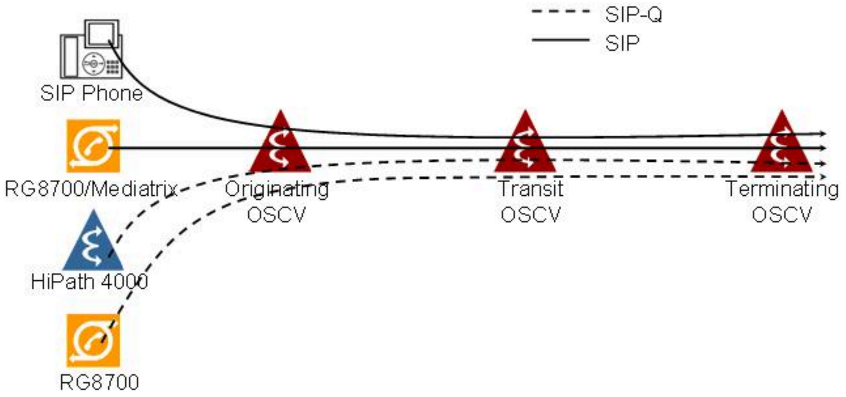


Figure 96: Routing principles for SIP/SIP-Q Routing

In order to achieve SIP-Q equivalency, the following SIP-Q functions/features must be available on the SIP interface to create the SIP Private Networking interface.

- Transport of CDR information (e.g. Global ID, Thread ID)
- Call Transfer Information to support proper CDR records in originating, transit and terminating OSVC systems.
- Call Diversion Information to support privacy in diversion headers in forwarding, transit and forwarded-to OSVC systems.
- Identification Information to support proper CDR records and proper displays.

7.1.4 SIP-Q Private Networking

The SIP-Q protocol refers to SIP signaling with QSIG protocol, using Unify CorNet-NQ extensions and is used for interworking between different systems, which does not support native SIP signaling.

The SIP-Q protocol is used for the following:

- Interworking between OpenScape Voice systems. By using SIP-Q rather than SIP, features can be supported between the systems.
- Interworking between OpenScape Voice and other systems that support the SIP-Q procedures—for example, the OpenScape 4000.

- Interworking between the OpenScape Voice system and other systems that support QSIG procedures—for example, an Avaya PBX. In this configuration:

  SIP-Q is used between OpenScape Voice and a SIP-Q compatible gateway, such as the OpenScape SBC.

  A QSIG TDM trunk is used between the OpenScape SBC and the other system.

7.1.5 Support of Wildcard DNS

An RTP parameter `Srx/Sip/WildcardedResponsibleDomains` has been introduced to bypass the DNS query and the sipsm cached FQDNs, as well as to reduce the heap cache for FQDN entries. The user can use the OpenScape Voice’s FQDN for location information and for the CAC feature. As a result, there can be many FQDNs created to identify subscriber's location for example “010001.022208.osv02.pvg.sipprovider.us”. DNS servers may setup to resolve “osv02.pvg.sipprovider.us” to OSV IP address, but because each FQDN is slightly different from the other, a new query is initiated. Each DNS response is also cached in sipsm. Since DNS queries are network and DNS server dependent, delays may block call processing which in turn may present an overload condition in sipsm.

To ease such a situation, a local/mini FQDN resolver is provided by this RTP-parameter - the IP addresses from this parameter are validated against OSV's IP addresses. The FQDN length shall be greater than 4 characters and shall include at least one dot, for example “x.yy” Example: ”

Syntax

“fqdn1:A<ipv4;ipv4>,fqdn_n:<ipv4_n1;ipv4_n2>” (space or special characters are not allowed)

Example

“.osv01.pvg.sipprovider.us:A<10.10.50.10;10.10.51.10>,.osv01.pvg.sipprovider.com:A<1

7.1.6 Hosting Multiple Private Networks

Multiple Business Groups spanned across OSVC systems in a hosted environment realize the required SIP and/or SIP-Q Private Networking Endpoints for each Business Group via ’virtual endpoints’.

OSVC matches the alias provisioned on a SIP endpoint with the domain part of the URI in the Contact header field of the received SIP/SIP-Q request. A single alias can only lead to a single endpoint; therefore aliases configured on endpoints must be unique. OSVC is only capable of sending its IP address in the domain part of the URI in the Contact header field of an outgoing request to an endpoint. As IP addresses are unique, this can only lead to a single endpoint.

The introduction of the concept of 'virtual endpoints' allows the administrator to create multiple SIP and/or SIP-Q endpoints for the same OSVC system, each with a unique alias, so that the correct endpoint can be found for an incoming request. Before checking for a match on the alias of the domain part of the URI in the Contact header field, OSVC shall check whether there is a matching alias for the domain part of the Request URI of the incoming request.

Functional Sequence

As the request URI of a SIP request always points to the intended target OSVC system, this results in the following:

- The OSVC that is sending the request must be set up to use FQDNs rather than IP addresses in the Primary Signaling field because this FQDN will be used by the target OSVC as an alias to find the OSVC system that sent the request.
- The OSVC that is receiving the request must configure the FQDN received in the domain part of the Request URI as an alias for the endpoint that represents the sending OSVC.

7.1.7 OpenScape Voice Managing SoftSwitches

The OpenScape Voice Assistant supports the Multi-Node Administration and allows the logged-on subscriber to administer several OpenScape Voice switches in parallel, without requiring a second login.

After a subscriber has successfully logged on to the system, a session is created and persists until the subscriber logs out, or is logged out (by e.g. session timeout, application shutdown, or system crash).

NOTICE:

IP packets with the used ports (configured in OSV, SBC, OSB) must be routed transparently in the IP network, meaning that the packets must not be manipulated, for example by a firewall. Functional problems can be the result of non-transparent routing.

Functional Sequence

When the subscriber changes to a different OpenScape Voice switch, the authentication reference/token/ticket is automatically forwarded, so the subscriber does not need to log on a second time.

The windows that belong to the previously selected switch stay operable, and the name of the related OpenScape Voice switch is displayed in the title bar of each.

Unauthenticated subscribers who attempt to access a resource are diverted to an authentication service, and returned only after a successful sign-on.

OpenScape Voice Assistant - OpenScape Voice Switch compatibility

The list of switches display the compatibility status between the OSV assistant and OSV switch for each switch. The comparison is done from the perspective of the OSV versions that are supported by the CMP against the version of the OSV that is administered by the CMP. The version can be both major and minor.

Example: A **CMP (OSV Assistant) version V10** is designed to support 100% of the functionality offered by the following OSV versions:

- OSV V7.0
- OSV V7.1
- OSV V7.2
- OSV V8.0
- OSV V8.1
- OSV V8.2
- OSV V10.0
- OSV V10.1
- OSV V10.2

If CMP administers one of the above OSV versions it will display the message **CMP Fully Compatible with OSV** which means that the complete functionality offered by the OSV is supported by this CMP. If an **OSV V7.3** is added to the CMP, due to the fact that the minor version is higher than the **V7** ones that are supported by the CMP, the message **OSV Fully Compatible with CMP** will be displayed, as the CMP is not aware of the new functionalities that are introduced with **OSV V7.3** and therefore cannot guaranty that it supports 100% the configuration of all **OSV V8.3** features.

So the values for the **CMP - OpenScape Voice Compatibility** field can be:

1) **OSV Fully Compatible with CMP** which means OSV switch version is higher than the CMP version and we have a backwards compatibility (fallback) from OSV so that it matches the Assistant version.
2) **CMP Fully Compatible with OSV** which means Assistant version is higher than the OSV switch version and we have a backwards compatibility (fallback) from Assistant so that it matches the OSV version.

> **NOTICE:**
>
> If Assistant version and OSV switch version are the same then **CMP Fully Compatible with OSV** appears in the “CMP - OpenScape Voice Compatibility” field

3) **Caution: OSV version lower than CMP** which means Assistant version is much higher than OSV version and indicates to the service personnel that they have to be aware of that difference.

Upgrade OpenScape Voice cluster system

The administrator is able to initiate and monitor the upgrade version of an OpenScape Voice cluster system/simplex system using CMP/OpenScape Voice Assistant.

During this upgrade the corresponding switch is not accessible from the Switches list (grayed out) and it is also removed from the dropdown list of the switches in the upper left side of the UI. The switch **Version** obtains the value **Upgrade Version in progress...** and the **Connectivity** column obtains the value "**...**". The administrator cannot provision or edit the settings of the switch until the upgrade is finished.

After the completion of the upgrade the new version of the OpenScape Voice system is displayed in the Switch List, under the **Version** column.

System Specific Information

In case of Onboard Assistant installation scenarios, the Add, Edit and Delete buttons and the checkbox for switch selection are disabled. This prevents altering the switch name and its configuration, and deleting the switch.

The Switch is described by the following data:

- **Name**

  This is the name of the OpenScape Voice switch.

  The OSV switch name must always be identical to the one that is used in `node.cfg`. Otherwise there is danger that the name will change to the valid `node.cfg` node name during synchronization with OSV. This can affect the ALI number used from CMP for distributing licenses to OSB/OSSBC.
- **Switch ID**

  This field displays the ID number under which the switch is registered in the database. The ID is used to facilitate provisioning via import of switch specific data.

  NOTICE:

  This field is not editable and is only displayed for existing switches. It is not displayed when adding a new switch.
- **Use Cluster Name**

  Enable this checkbox in order to use the cluster name instead of the switch name. If you enable the checkbox, the Name field is disabled and the cluster name is used as switch name.
- **IP Address**

  This is the IP address of the switch.
- **srx password**

  This is the password for the system administrator login for node 1. This field is only displayed when you add a new switch.

  The default password is: `2GwN!gb4`
- **NOTICE:**

  When adding a new switch (cluster), the login data for node 2 is not displayed and does not have to be entered by the user. The OpenScape Voice Assistant runs the appropriate scripts to retrieve the information for node 2 automatically.
- **IP address of node 1**

  This is the IP address of node 1 of the selected switch.

  NOTICE:

  This field is not editable and is only displayed for existing switches. It is not displayed when adding a new switch.

- **IP address of node 2**

  For cluster systems, this is the IP address of node 2 of the selected switch.

  NOTICE:

  This field is not editable and is only displayed for existing cluster switches. It is not displayed when adding a new switch.

- **Enable Password(s)**

  Select this checkbox to activate the **New srx password of node1** and/or **New srx password of node2** fields and override the passwords assigned to Node 1 and Node 2.

- **New srx password of node1**

  This is the new srx password of the system administrator login for node 1 which can be edited for an existing switch.

  The default password is: `2GwN!gb4`

  NOTICE:

  This field is only displayed for existing switches. It is not displayed when adding a new switch.

- **New srx password of node2**

  For cluster systems, this is the new srx password of the system administrator login for node 2 which can be edited for an existing switch.

  The default password is: `2GwN!gb4`

  NOTICE:

  This field is only displayed for existing cluster switches. It is not displayed when adding a new switch.

- **Switch Type**

  This value indicates the data transfer mode configured for the switch.

  Possible values:

  Simplex (data can be transferred in both directions, but not simultaneously)

  Duplex (data can be transferred in both directions simultaneously)

  NOTICE:

  This field is not editable and is only displayed for existing switches. It is not displayed when adding a new switch.

- **Test Connection**

  This button checks whether the connection to the switch is working.

  The system attempts to connect to the switch, log in, copy keys as needed, and then disconnect.

  If an error occurs during the connection attempt, or if the operator cancels the connection attempt, all changes made will be rolled back and the configuration settings will remain unchanged. A corresponding error message is displayed mentioning the reason of the failure.

If the connection test completes successfully, a confirmation message is displayed.

- **TLS authentication**

  This checkbox allows you to enable or disable TLS authentication.

  In order to enable TLS authentication, this checkbox must be checked.

  For more details about TLS authentication, refer to the section “TLS (Transport Layer Security) Support”.

  From OpenScape Voice V8 onwards, in order to enable TLS Authentication on all deployments, the needed certificates of OpenScape Voice to OpenScape UC DVD application server, have to be applied manually.For more information, follow the steps described in the guide “OpenScape Solution Set V8, Solution Guide: Certificate Management and TLS, Administrator Documentation”
- **SOAP server port**

  This value specifies the SOAP server port

  Possible values (dropdown list):

  TLS authentication disabled: 8767, 8768, 8769, 8770

  TLS authentication enabled: 8757, 8758, 8759, 8760

7.1.7.1 Manual Grouping of Nodes

Manual Grouping of Nodes is supported. Each node represents a physical entity. Only 1 level of grouping is possible. The group name can be edited by the administration.

The Group is shown in a Tree View (or equivalent). Initially only the group name is shown.

Functional Sequence

When the subscriber changes to a different OpenScape Voice switch, the authentication reference/token/ticket is automatically forwarded, so the subscriber does not need to log on a second time.

The windows that belong to the previously selected switch stay operable, and the name of the related OpenScape Voice switch is displayed in the title bar of each.

Unauthenticated subscribers who attempt to access a resource are diverted to an authentication service, and returned only after a successful sign-on.

System Specific Information

Each node may contain one of the following:

- An OpenScape Voice system.
- An application node containing Symphonia services.
- An OpenScape SBC.

- A 3rd party node.

  Third Party Nodes can be added manually if the node contains a link (HTTP and ssh) to the administration application of the third party software. Supported third party nodes may be e.g.: Convedia Media Server, Mediatrix Gateway, Comdasys SIP Proxy, Video MCUs.

7.1.8 Signaling Management

Signaling Management handles protocol functionality, interfaces and interacts with the OSV maintenance functions.

Signaling Management contains the following items:

- SIP

  The SIP signaling manager supports message traffic on the SIP interface between SIP endpoints and the OSV server.
- SIP-Q

  The SIP-Q signaling manager is an integral part of the SIP signaling manager, and supports message traffic on the SIP-Q interface between SIP-Q endpoints and the OpenScape Voice server.

  The SIP-Q protocol uses SIP messages to tunnel QSIG messages on the SIP interface and is mainly used to support features between PBX'es in a private network environment.

  OSV supports Number Modifications for all numbers in the QSIG MIME body for scenarios where the OpenScape Voice is a SIP-Q Transit switch. This allows displays and supplementary services to work properly in OpenExchange scenarios where the numbering plan is not homogenous between PBXs.

  In order to address this requirement the **Apply Number Modifications for Transit Calls** parameter must be checked and the **Modify Called Party IE for Transit Calls** may have to be checked.

  The **Modify Called Party IE for Transit Calls** attribute can also be used for in OpenExchange scenarios where the numbering plan is homogeneous.

  The **Send CorNet-NQ Additional Party Number in National Format** parameter is used in interworking scenarios (not OpenExchange) with CorNet-NQ switches (e.g. an OpenScape Voice 4000) that require the Additional Party Number operation in ISDN National format as opposed to ISDN International format (default).
- Authentication

  Authentication protects access to the OpenScape Voice server on the SIP interface by requesting authentication (identity verification) of the remote parties (such as other SIP servers and SIP clients).
- TLS Settings

  TLS was chosen as the Information Assurance protocol to secure AS-SP.The use of a certificate from an approved PKI, in combination with TLS, provides a secure process for signaling appliances to authenticate to each other.

- CSTA

  The CSTA signaling manager supports CSTA message traffic on the CSTA interface between CTI applications and the OSV server.

Related concepts

Rerouting a Call to a SIP Subscriber on page 244

CSTA Support on page 176

7.1.9 Operation Mode Management

The Operation Mode feature allows the administrator to view and set the Operation Mode for each node.

In multi-node scenarios, the Operation Mode feature allows the administrator to view and set the Operation Mode for each node of a multi-node switch and thus define the primary and the secondary node.

If two OpenScape Voice nodes can not reach each other due to network problems, all nodes should be able to handle local calls and join together (communicate with each other) after the connection is up again. During this time the Assistant may not be able to administer the OpenScape Voice system at the SAS Secondary node. Only queries are possible.

In multi-node scenarios (e.g. a dual- node OpenScape Voice switch with nodes installed in different subnets), the administrator can use this feature to define which node is the primary and which the secondary node. In case of a network problem between the two nodes, the two nodes will be joined together (communicate with each other again) after the network reestablishment.

NOTICE:

The buttons on Operation Mode menu become active, ONLY when the OpenScape Voice nodes are in one of the following states:

This Node = `STANDALONE PRIMARY`

Partner Node = `UNKNOWN`

or

This Node = `STANDALONE SECONDARY`

Partner Node = `UNKNOWN`

If the OpenScape Voice nodes are on any other state, the buttons are disabled (grey-out).

You may verify also the Operation Mode state from node1 -or/and- node2 with OpenScape Voice `startCli` tool:

```
# su -srx -c startCli
```

Choose 6-1-1-11-1

7.1.10 Remote Access

Remote Access provides secure shell access to Switches and Gateways.

Access to the Switches and Gateways is gained using the Command Line Interface (CLI) over SSH Secure Shell. For this purpose the SSH Secure Shell Client software must be installed on the PC and the PC must have Ethernet or LAN access to the communication system. The PuTTY SSH/Telnet client software can be used for such a purpose.

Functional Sequence

Remote access to the gateways is gained via the SSH (or Telnet) session. How to configure the gateways via the Telnet session is explained in the Telnet documentation.

The SFTP button provides secure FTP connection to switches and gateways. To work properly, the WinSCP setup program must be installed on the client. You must enter the password of user id "sysad" when prompted.

7.1.11 Alarm Email Notification

In OpenScape Voice communication system you have the option to generate an e-mail automaticaly whenever an emergency call is detected.

The Administrator configures a list of recipients that will be automatically notified via e-mail when specific SNMP Trap are detected. The Administrator can also configure the content of the notification e-mail.

7.1.12 SOAP/XML Client Management

The SOAP/XML Client feature allows you to display all Client Profiles available in the system and to add, edit and delete Client Profiles and from OSV V8 onwards it also allows you to configure the Certificate Validation of SOAP clients.

The SOAP (Simple Object Access Protocol) Server is an integrated component of the OpenScape Voice system whose function is to handle provisioning requests for subscriber, endpoint, and business group data, including the creation, deletion, modification, and display of these entities and their associated features, or services.

The SOAP Server expects SOAP/XML requests conforming to the SOAP Server WSDL (Web Services Definition Language) file, which is included as a product deliverable and is made available to external interface partners. In particular, the OpenScape Voice Assistant uses this interface to transmit provisioning requests from the user to the OpenScape Voice system.

Client Profiles are created by defining security and the authorizations that are needed to access SOAP methods. Security is implemented by using TLS on the specific range of ports 8757 through 8766 on the switch. Any input coming on these ports will be secured by TLS. Authorization is achieved by defining the Client Profile for each SOAP Client IP address.

RTP Parameters

Following RTP parameters must be configured for SOAP client management:[14]

- `Srx/Subp/SuperUserIpAddress`:

  Holds the default IP from where ALL SOAP APIs are accessible and therefore this is usually the Element manager's API from where Client profiles can initially be created.

  > **NOTICE:**
  >
  > Once a client profile of Super User role is created for another IP, then Client Profiles can be created from that IP as well.

- `Srx/Subp/Authorization`:

  When set to true enables the SOAP authorization feature.

  From OSV V8 onwards this parameter can be set from the OSV UI with checkbox **Client Roles Enabled** under SOAP/XML Client Settings screen.

  > **IMPORTANT:**
  >
  > If you change the `Srx/Subp/Authorization` parameter to true without setting the `RTP parameter Srx/Subp/SuperUserIpAddress` to the IP address of the current CMP, you will be locked down and must connect manually to the OSV to make the appropriate change via `startCli`

Certificate Verification Levels

Unify Certificate Verification Process requires 3 levels of certificate verification to be supported in all Unify products, including SOAP clients, that perform unattended certificate verification for TLS. From V8 onwards OpenScape Voice supports these three levels as a configuration option and, to ensure uniformity across all Unify products, the three configurable options are named “None”, “Trusted” and “Full” as described below:

- **None**

  No authentication of the remote entity performed.

  The remote entity is not checked at all or any potential errors during the check are ignored. This is the default setting since both **Trusted** and **Full** require administrative steps anyway by configuring the associated (root) CA certificate(s).

  > **IMPORTANT:**
  >
  > It is strongly recommend that the default self-signed TLS server certificate be replaced with a new TLS server certificate and that the certificate verification level be set to either “**Trusted**” or “**Full**”.

[14] RTP Parameters are located in following screen **OpenScape Voice** > **Administration** > **General Settings** > **RTP**

- **Trusted**

  The certificate (including certificate chain) provided by the remote entity is checked :

  that it is trusted. This means the chain of trust for the digital signature provided by the remote entity ends up in one of the (root) CA-certificates, which are pre configured for that interface on the product.

  that all certificates in the chain are not expired (i.e. current date/time is within the certificate's given validity period).

  that none of the certificates in the chain is revoked based on CRL (Certificate Revocation Lists)

- **Full**

  The certificate (including certificate chain) provided by the remote entity is checked against the same criteria as in **Trusted** mode, plus it is checked:

  for correct end entity identity (according to settings in `SubjectAlternativeName` (SAN) and/or the common name (CN) in the Subject). The SAN shall be checked first and only check the CN if the identity was not verified through the SAN. (this is controlled by checkbox **Enable Identity Checking** in TLS Settings)

  for correct use of all critical extensions (e.g. Basic constraints, Key Usage, Extended Key Usage). If an extension is marked critical and is not recognized, the certificate is rejected.

  for correct use of known extensions not marked as critical (e.g. Basic constraints, Key Usage, Extended Key Usage)

  Notes:

  If the received certificate contains the Key Usage extensions, the bits MUST be set to 1 for digitalSignature and keyEncipherment. If one of these bits is not set, the certificate shall be rejected. The bit nonRepudiation (or contentCommitment) is optional.

  If the received certificate contains the Extended Key Usage extension, its content must be verified. If the OSV is the TLS client and receives the certificate from the TLS server, the parameter serverAuth shall be set. On the other way around, if the OSV is the TLS server and receives the certificate from the TLS client, the parameter clientAuth shall be set

Although the Certification Level configuration is a Certificate Management aspect the Administrator may access the relevant screens by navigating to Signalling Management> TLS Settings for the SIP and CSTA application and to General Settings > SOAP/XML Client for the SOAP applications.

7.1.13 HiPath Deployment Service (DLS) Configuration

The DLS server allows you to gain remote access for administrating the connected workpoints.

With this feature it is possible to set up the connection to the DLS Server and to the DLS API or to change the DLS server credentials.

7.1.14 HiPath Deployment Service (DLS) Status

With the DLS Status feature it is possible to get information about the current status of DLS jobs.

This feature can be used by all administrators who have permission to create or modify a subscriber.

Requirements

In order to use this feature, a running OSV Assistant with a connected DLS server is required.

In the DLS the following settings must be configured:

- SIP Registrar and port
- SIP server address and port
- Plug&Play standards

7.1.15 Connection Close by TTUD Time Out Parameter

A number of active but idle connections can lead to resource attacks. The dimension of time to close connection is defined by a TTUD (TCP-TLS-UDP Dispatcher) TimeOut parameter. To avoid the resource leaks this parameter should be a relatively small value.

First Message time out

TTUD can close a connection if no message is received within a certain time. This time is defined by the parameter First Message time out. The value is 90.

Handshake time out

TTUD has a number of active but idle handshakes, TTUD can close a connection if the handshake is not complete within a certain time. This time is defined by this parameter and the value is 30.

7.2 SBC (Session Border Controller)

An SBC (Session Border Controller) can be used in VoIP (Voice over IP) networks to exert control over the signaling and media streams involved in setting up, conducting, and tearing down calls. SBCs are put into the signaling and/or media path between calling and called party.

An SBC provides real-time, interactive communications using SIP (Session Initiation Protocol). It offers the IP-to-IP network boundary for the following.

- Service provider to subscriber
- Service provider to service provider

It also manages the following functions:

- Authentication, authorization, admission, attack and overload protection, lawful intercept, interworking and protocol fixing, and other similar functions.
- Media Stream Transcoding
- Signaling and Media Encryption

Within OpenScape Voice, SBCs are supported with three basic configurations for remote users, branch offices, and SIP service providers.

Several configurations may be supported concurrently by one SBC or separate SBCs may be used for each configuration.

The supported basic configurations can be described as following:

- Remote Users

  The SBC in the main office data center is given a publicly accessible address, and teleworkers use this address for their SIP registrar and proxy for their SIP phones or SIP soft clients. Remote users may not utilize a NAT (considered near-end) or may be reached through a NAT (considered far-end).
- Branch Offices

  The SBC allows the data center to have its own addressing scheme, independent of the addressing schemes of the branch offices.
- SIP Service Providers

  An SBC is used to secure and inter-work the connection between OpenScape Voice and the Provider SIP Server via SIP trunking.

7.2.1 General Description of an SBC (Session Border Controller)

The usage of an SBC (Session Border Controller) enables enterprises to extend SIP-based applications beyond the Enterprise network boundaries, e.g., when users of OpenScape Voice are not all within the same IP network.

Users within each network may not have public IP addresses and/or NAT (Network Address Translation) devices may be deployed within the networks. In these cases, SBCs are used to allow SIP signaling to pass between the user devices and OpenScape Voice. The SBC also provides network topology hiding.

An SBC is basically a SIP-aware firewall that also serves as a SIP proxy or B2BUA (Back-to-Back User Agent). The Acme Packet Net-Net 3800 SBCs behaves as a B2BUA while the OpenScape Branch and Comdasys SBC behaves as a proxy. The SBC is given a publicly accessible URL and IP address, and SIP phones in the internet use this as the address of their SIP registrar and proxy. The SBC also has a second IP address, and a separate LAN connection, in the corporate LAN. Its function is to analyze, modify, and relay messaging between the phone and the OpenScape Voice system. Only proper SIP and media (RTP, Real-Time Transport Protocol) packets are permitted through the firewall function.

7.2.2 Basic Functionality of SBC (Session Border Controller)

An SBC (Session Border Controller), also known as Session Manager or Session Director enables secure reliable voice, video, and multimedia connections across IP networks.

An SBC provides the following functionalities within OpenScape Voice:

- Remote Access

  Subscribers want to use their phones regardless of location. The Acme Packet SBC enables secure access to the OpenScape Voice regardless of public/private network or endpoint type.

- SIP Trunking

  Enterprise network operators realize the significant operational cost savings by transitioning from TDM to IP (SIP) trunking. The Acme Packet SBC enables enterprises to securely connect their IP Telephony solutions to carrier SIP trunking services or between enterprise branch offices.

- Security

  Enterprises want their IP telephony network protected against attacks and compromises. The Acme Packet SBC can be deployed to provide a secure access at all points of interconnect.

- Policy Enforcement

  Allows Enterprises to define, enforce, and audit fine-grained policies on real-time services such as VoIP, video, IM, presence, communications-enable applications and other real-time services.

7.2.3 Additional SBC (Session Border Controller) Capabilities

Apart from the basic NAT (Network Address Translation), ALG (Application Level Gateway and Media Relay functions, SBCs (Session Border Controllers) provide many other features and capabilities that OpenScape Voice customers may wish to use.

In the following overview, the capabilities of the Acme SBC are listed as an example.

- Security
  - Cryptographic authentication
  - Signaling and media encryption
  - Stateful signaling and media validation
  - Denial of service attack mitigation
  - Intrusion prevention
- Routing
  - Least cost routing
  - MoS-based routing
  - CAC (Call Admission Control)
  - Presence-based routing
  - Business rule determination

- Monitoring
  - Session detail recording
  - QoS (Quality of Service) detail recording
  - Instant message recording
  - Voice and video recording
  - File transfer recording
  - System and admin event logging
- Control
  - Signaling and media control
  - QoS control
  - Identity-based access control
  - File transfer control
  - Instant message content control
  - URL access control
- Interoperability
  - Multi-vendor protocol normalization
  - SIP-aware NAT traversal
  - Application-aware session routing
  - H.323 interworking with SIP
  - IPv4 / IPv6 interworking
  - Corporate directory integration

7.2.3.1 SBC (Session Border Controller) Functionality - Dynamic Port Mapping

The Dynamic Port Mapping allows the usage of a single IP address, where the different users are separated via unique ports.

There are different scenarios for Remote Users and Branch Offices.

Remote Users

- UDP connections on the core side between the SBC (Session Border Controller) and OpenScape Voice

  On the core side of the SBC a single IP address is used, but unique ports are assigned for each user.
- TCP/TLS connection on the core side between the SBC and OpenScape Voice

  On the core side of the SBC a single IP address is used but unique ports are assigned for each user. Only a single layer 3 connection is used but unique port numbers are sent in the 2nd Via header field and in the Contact header field to OpenScape Voice.

Branch Office

- UDP/TCP/TLS connections on the core side between the SBC and OpenScape Voice.

  On the core side of the SBC a single IP address is used per Branch, but unique ports are assigned for each user. Only a single layer 3 connection is used but the unique port numbers are sent in the 2nd Via header field and in the Contact header field to OpenScape Voice.

7.2.3.2 SBC (Session Border Controller) Functionality - Support for Branch Survivability

In order to allow fast detection of connectivity loss, particularly in low traffic periods, the SBC (Session Border Controller) must support receiving and sending SIP OPTIONS requests between survivable branch proxies and the OpenScape Voice server. This allows the branch to switch to survivable mode and the OpenScape Voice server to invoke automatic rerouting to the branch via the PSTN (Public Switched Telephone Network).

In order to allow the OpenScape Voice server to differentiate between a branch users UA (User Agent) not responding and a WAN outage the SBC must send a SIP 504 response for SIP request timeouts occurring for requests sent to a branch proxy. At normal traffic levels connectivity failures are likely to be detected by SIP requests timeouts before they are detected by the SIP OPTIONS audit mechanism.

7.2.3.3 SBC (Session Border Controller) Functionality - Registration Caching and Unregistering

Functional Sequence

1) The remote user sends a SIP REGISTER request to the public IP address of the SBC.

2) The SBC assigns a private IP address and port on the core side.

3) The SBC establishes a binding between the remote users IP address and the associated IP address and port on the core side.

4) The SBC replaces the contact address with the private IP address and port that it has assigned for the remote user.

5) The SBC then delegates (i.e. passes on) the SIP REGISTER request to the OpenScape Voice server.

The SBC uses a port mapping technique so that only one contact IP address is used for all the remote users but each user is assigned a unique port number at the single IP address.

When OpenScape Voice wishes to route a call to a remote user, ...

1) it sends a SIP INVITE to the topmost Via header address previously received in the SIP REGISTER request from the SBC, i.e. the SBC core-side interface

2) it associates the Contact address in the SIP INVITE received at an IP address/port on the core-side with a specific remote users public IP address/port. For this step the SBC uses the registration binding information.

3) it forwards the SIP INVITE from the access-side of the SBC to the remote user’s device.

System Specific Information

When a phone is reset, a SIP REGISTER with expiration time = 0 should be sent from the phone to remove the registration contact binding in the SBC and the OpenScape Voice server. If the SBC detects a registration timer expiration for a user it must remove its registration contact binding and send a REGISTER with expiration time = 0 to the OpenScape Voice server.

7.2.3.4 SBC (Session Border Controller) Functionality - Media Stream Handling

The SBC (Session Border Controller) must provide configuration options to allow the system administrator to specify when local media connections are allowed and when the media must be routed via the SBC. The SBC decides which media path is appropriate based on the configured options and the subnets of the calling and called users.

7.2.3.5 SBC (Session Border Controller) Functionality - SBCs and Data Firewalls

SBCs (Session Border Controller) and data firewalls are complementary. The SBC has integrated firewall capabilities on both access and core side and therefore exists in its own DMZ (Demilitarized Zone) for SIP signaling and RTP (Real-time Transport Protocol)/SRTP (Secure Real-time Transport Protocol) media, while the data firewall handles data protocols.

Voice and data traffic should be separated by edge routers into different Virtual LANs (VLANs). The voice VLAN is routed to the SBC and the data VLAN is routed to the data firewall.

If the Enterprise security policies mandate firewalls in front of the SBC then the SBC can use procedures to keep the necessary VoIP ports open through the firewall, e.g., short registration refresh intervals on the access side of the SBC, or TLS (Transport Layer Security)/TCP keep alive procedures. Alternatively the necessary VoIP ports may be opened statically at the firewall.

7.2.3.6 SBC (Session Border Controller) Functionality - Geographic Node Separation

When OpenScape Voice nodes are geographically separated between two data centers for redundancy purposes then an SBC (Session Border Controller) is required at both data centers.

In order for SIP registration data to be synchronized in real-time between the SBC's in the two data centers a layer 2 connection is required between the SBC's.

NOTICE:

The AcmePacket SBC can use a layer 3 IP connection but maximum packet delay that can be tolerated is 50 ms.

If a connection between the SBC's that meets the above requirements is not possible, or if the two data centers are not within the same sub-net, then failover from the primary data center to the secondary data center involves a loss of VoIP connectivity for the users until the users re-register with the secondary data center.

In this scenario the remote user phones must be configured with the IP address of both the primary SBC and the secondary SBC (or use DNS to obtain both IP addresses) and must be able to register with the secondary SBC after detecting failure to communicate with the primary SBC. For this failure scenario remote users will not be able to receive incoming calls until the registration refresh time expires, or until they attempt an outgoing call (which will initiate a re-registration with the other SBC).

The SBC should be configured with a short registration refresh interval on the access side to minimize the outage interval. It is recommended that the short registration interval be 60 seconds, or if in the case of NAT, 30 seconds. Network planning must take account of remote users sending SIP REGISTER requests at such short intervals.

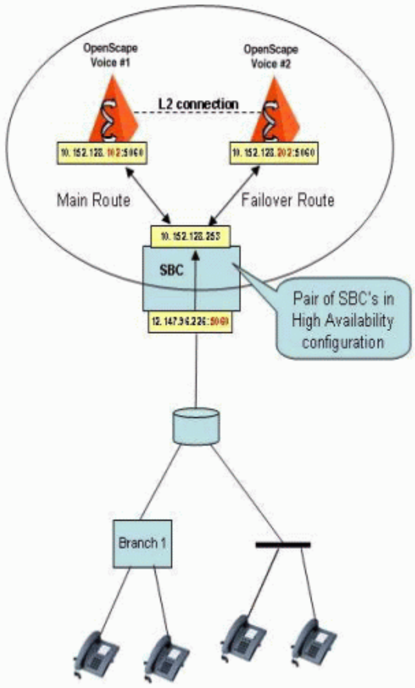
For TLS (Transport Layer Security) transport the OpenScape Voice "connectivity-check" mechanism is not supported. SIP clients may be configured to support the "connectivity-check" but will not receive any support indications for remote users, and are required to provide alternative TLS connectivity checking based on a shortened SIP registration interval controlled by the SBC. The lack of a registration response allows a new TLS connection to the secondary SBC and/or OpenScape Voice server to be quickly established and a new registration request sent to the OpenScape Voice server to minimize the time that a user is unreachable following a failover.

System Specific Information

The following figures show the principles of geographic separation when central SBCs are involved as well as some examples of SBC deployments with Geographically Separated OpenScape Voice nodes:

- The following figure illustrates the redundancy capabilities when both OpenScape Voice nodes and the central SBCs are in the same subnet with full layer 2 connectivity between the network elements:

SIP Signaling:
SBC Solution – Switch Redundancy - same Subnet



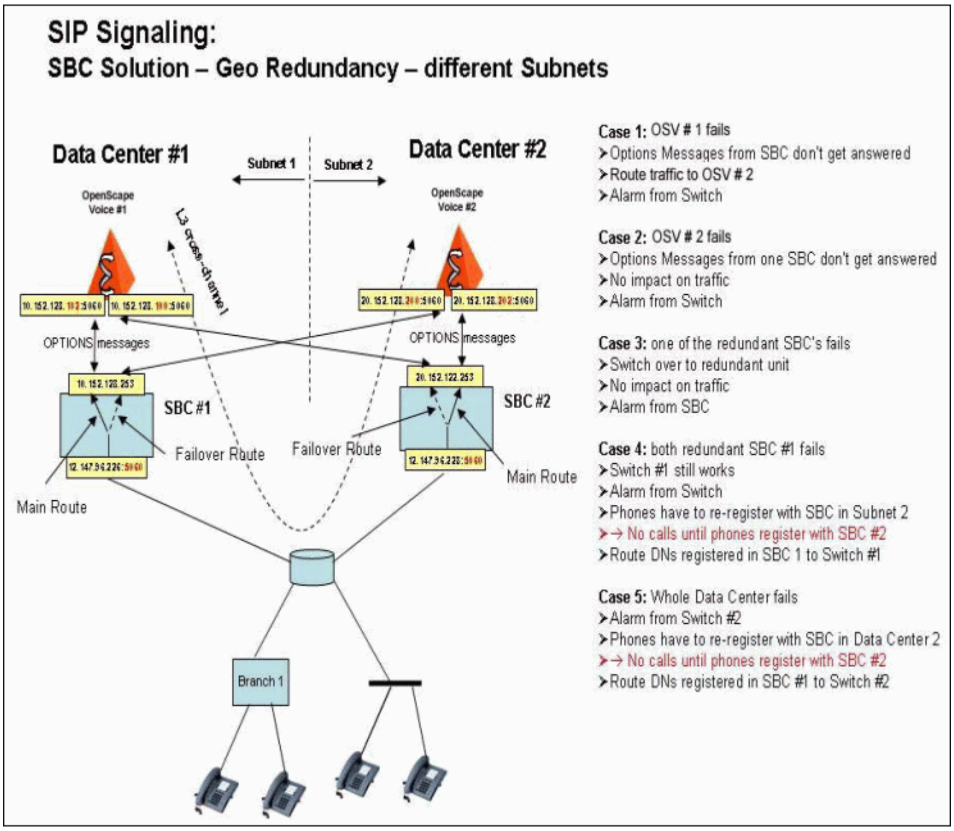
Case 1: OSV # 1 fails
➤OSV # 2 takes over IP address of OSV # 1
➤No impact on Calls
➤Alarm from Switch

Case 2: OSV # 2 fails
➤OSV # 1 takes over IP address of OSV # 2
➤No impact on Calls
➤Alarm from Switch

Case 3: one of the redundant SBC's fails
➤Switch over to redundant unit
➤No impact on Calls
➤Alarm from SBC

Case 4: both redundant SBC's fail
➤Data Center fails
➤Alarm from Switch
➤Phones have to re-register after SBC repaired

- The following figure illustrates the redundancy capabilities when the OpenScape Voice nodes and the central SBCs are in the different data centers with different subnets and only layer 3 connectivity between the data centers:



SIP Signaling:
SBC Solution – Geo Redundancy – different Subnets

Case 1: OSV # 1 fails
- Options Messages from SBC don't get answered
- Route traffic to OSV # 2
- Alarm from Switch

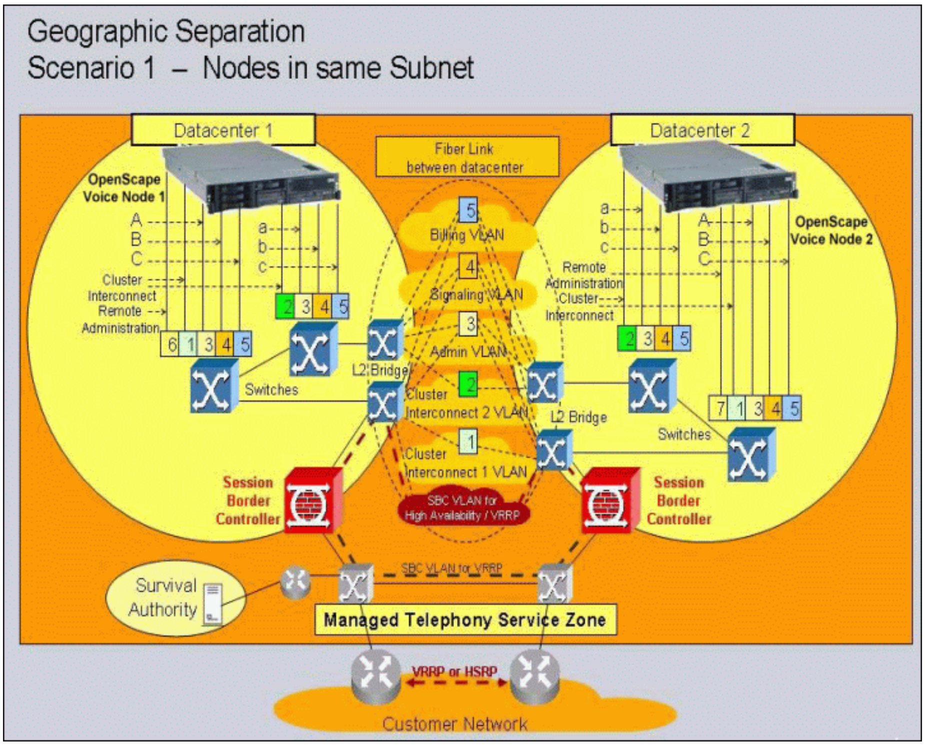
Case 2: OSV # 2 fails
- Options Messages from one SBC don't get answered
- No impact on traffic
- Alarm from Switch

Case 3: one of the redundant SBC's fails
- Switch over to redundant unit
- No impact on traffic
- Alarm from SBC

Case 4: both redundant SBC #1 fails
- Switch #1 still works
- Alarm from Switch
- Phones have to re-register with SBC in Subnet 2
- → No calls until phones register with SBC #2
- Route DNs registered in SBC 1 to Switch #1

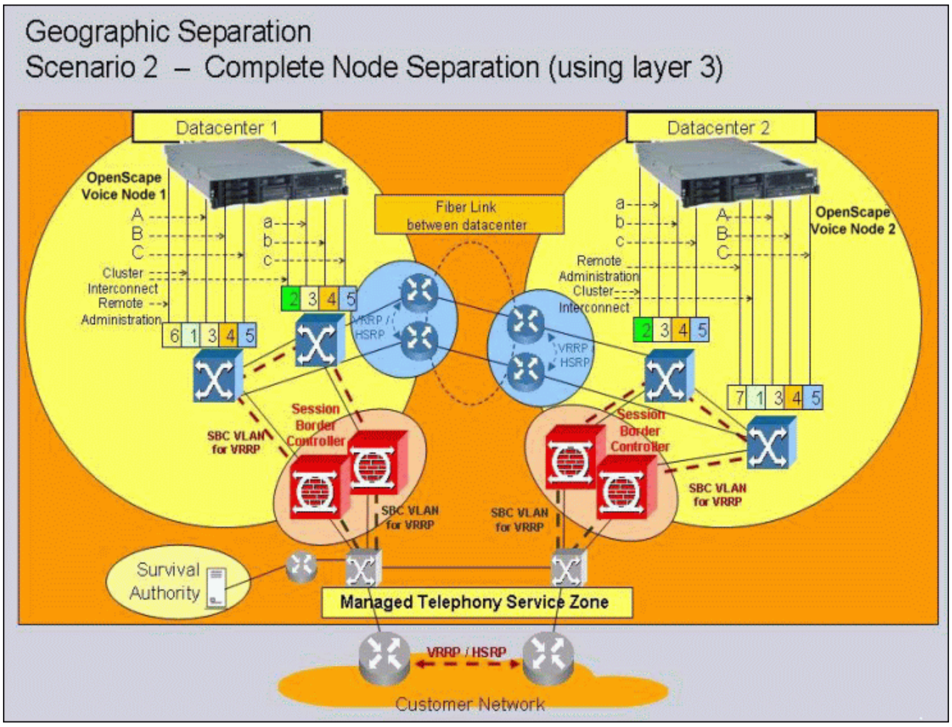
Case 5: Whole Data Center fails
- Alarm from Switch #2
- Phones have to re-register with SBC in Data Center 2
- → No calls until phones register with SBC #2
- Route DNs registered in SBC #1 to Switch #2

- The following figure illustrates the typical physical interconnections in a geographically separated scenario where both data centers are in the same subnet with layer 2 connectivity between the data centers:



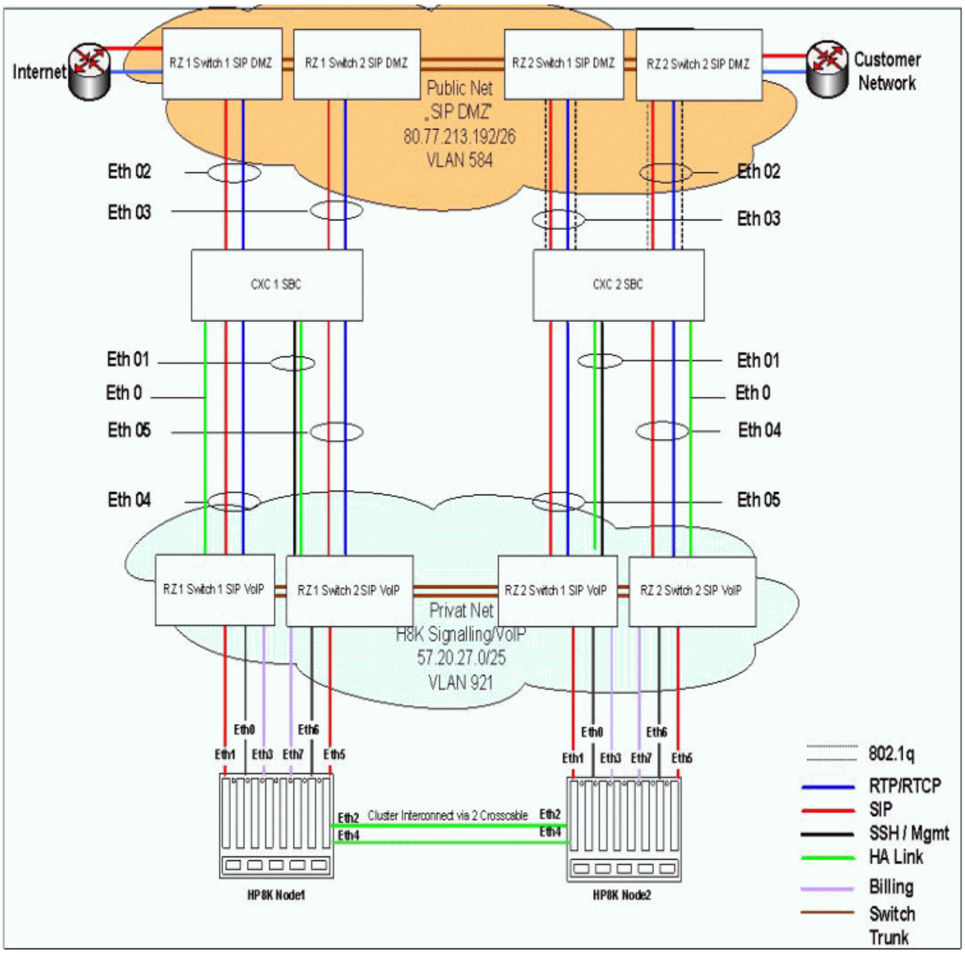
Geographic Separation
Scenario 1 – Nodes in same Subnet

- The following figure illustrates the typical physical interconnections in a geographically separated scenario where the data centers are in different subnets with only layer 3 connectivity between the data centers:



Geographic Separation
Scenario 2 – Complete Node Separation (using layer 3)

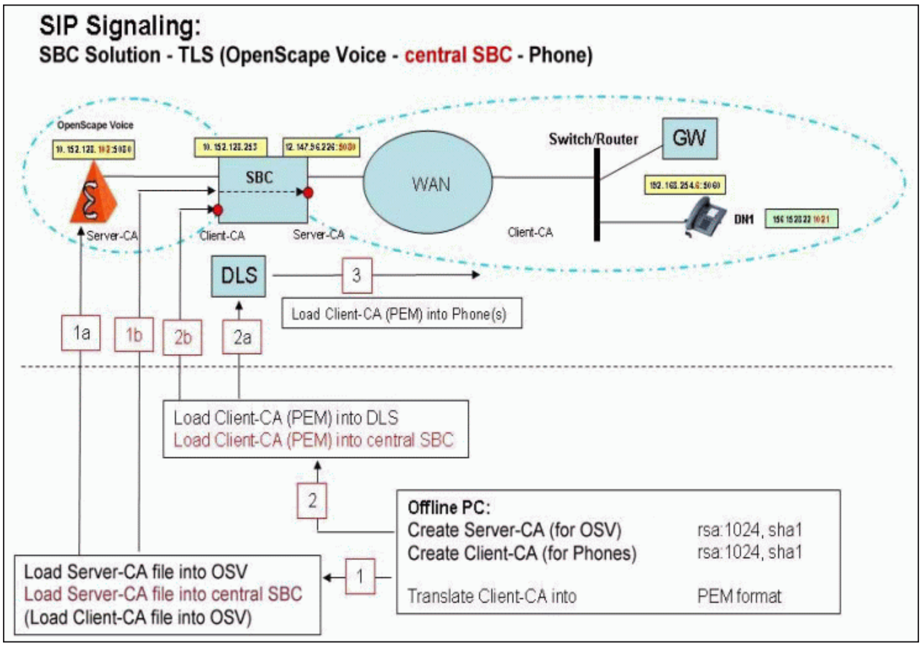
- The following figure illustrates the physical connections at the Acme Packet SBC when two SBCs are used in a high availability configuration with both OpenScape Voice nodes and SBC nodes in the same subnet:



7.2.3.7 Signaling and Media Security

For secure communications, it is recommended that both the signaling connection and media session be secured for end-to-end communications. The Acme Packet, OpenBranch and Comdasys SBCs (Session Border Controllers) support SIP signaling security via TLS (on both the access and core sides of the SBC) and support media security via transparent pass-thru of SRTP (Secure Real-time Transport Protocol) packets as well as mediation with RTP.

The following figure illustrates generation and distribution of CA (Certification Authority) files to network elements including SBC:


SIP Signaling:
SBC Solution - TLS (OpenScape Voice - central SBC - Phone)
OpenScape Voice
10.152.120.102:5060
10.152.120.253
12.147.96.226:5060
SBC
WAN
Switch/Router
GW
192.168.254.6:5060
DN1
156 152022 1021
Server-CA
Client-CA
Server-CA
Client-CA
DLS
3
Load Client-CA (PEM) into Phone(s)
1a
1b
2b
2a
Load Client-CA (PEM) into DLS
Load Client-CA (PEM) into central SBC
2
Offline PC:
Create Server-CA (for OSV) rsa:1024, sha1
Create Client-CA (for Phones) rsa:1024, sha1
Translate Client-CA into PEM format
1
Load Server-CA file into OSV
Load Server-CA file into central SBC
(Load Client-CA file into OSV)

The Acme Packet SBC will also provide full support for the MIKEY (Multimedia Internet Keying) #0 key exchange procedures and will therefore be able to provide mediation between an endpoint device using SRTP on one side of the SBC with an EP (Endpoint) on the other side of the SBC using RTP (Real-time Transport Protocol).

For media sessions the SBC is able to support MIKEY#0 crypto session negotiation in the following combinations with SRTP - RTP session mediation supported as required:

- SRTP - SRTP

  The media stream is secure when the MIKEY#0 crypto session negotiation is successful for the core and access network. For calls established between users on the SBC access, end-to-end secure media is possible only if the session established from the originator and the session established to the destination use SRTP.

- SRTP - RTP

  For SRTP media streams the SBC supports the crypto session negotiation and session mediation when RTP is used on the peer network. Note that the SRTP session may be established from either the access or core network.

NOTICE:

The Acme SBC's are only able to support static media associations, i.e., SRTP-SRTP, or RTP-RTP and is unable to support Unify best effort SRTP negotiation. It is planned to support SRTP-RTP in the future.

For transport signaling, the SBC is able to support several transport signaling combinations for the SBC access and SBC core networks. It is recommended that the transport be secured end-to-end however this is not always possible.

For SIP devices and gateways on the SBC access network, Server Authentication TLS (TLS) is recommended, however TCP and UDP are available.

If SBCs are deployed in a cascaded configuration, for the central SBC access side, Mutual Authentication TLS (mTLS) is recommended. On the SBC core network mTLS is recommended, however TCP and UDP are available.

For an OpenScape Branch (Proxy), mTLS is recommended to be used on the central SBC access, however TCP and UDP are available.

Secure Call User Indications

To ensure end users are provided an accurate indication regarding call security, a proprietary end-to-end call security indication is available. The indication is transported via SIP within the Unify X-Siemens-Call-Type header field. The user will be provided a secure communications indication only if both the calling and called SIP devices support the extension and a secure communications connection is established end-to-end. The call must utilize TLS signaling and SRTP media end-to-end. This can only be achieved where both the SBC access and core are secured using TLS (or mTLS) and SRTP media security is used, i.e., all sessions and signaling traversing the SBC for the call must be secure.

The following call is secure: User A calls User B:

A (TLS+SRTP) -> SBC -> OSV (mTLS+SRTP) -> SBC -> B (TLS+SRTP)

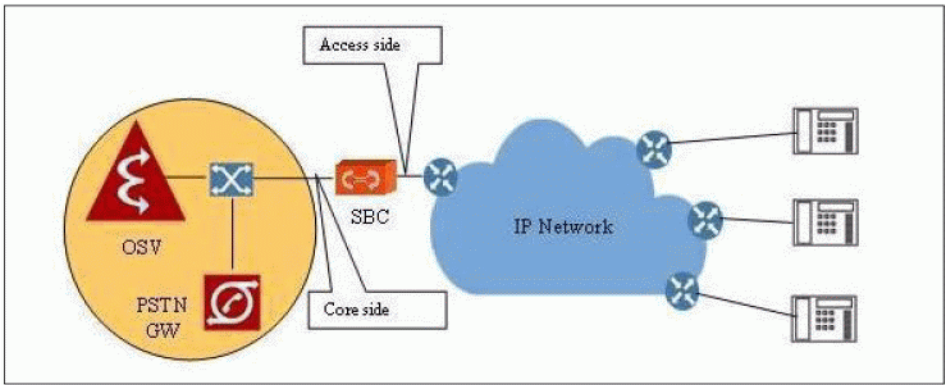
The following call is insecure: User A calls a User in the PSTN accessed via a GW where the GW only supports RTP:

A (TLS+SRTP) -> SBC -> OSV (mTLS+SRTP) -> SBC -> GW (TLS+RTP)

7.2.4 SBC (Session Border Controller) Configuration - Connection of Remote Users

When the remote user is a hard phone there is generally no support for a VPN connection at the phone and use of an SBC (Session Border Controller) to allow connection to the OpenScape Voice server is necessary.

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 OpenScape Voice server.



The following redundancy considerations apply for remote users:

- OpenScape Voice cluster nodes are co-located in one data center (or geo-separated but in the same sub-net).

  If a High Availability SBC cluster is deployed, then failure of one SBC is transparent to the branch users.

  If a non-redundant SBC is used then failure of the SBC results in loss of service until the SBC is repaired.
- OpenScape Voice cluster nodes are geo-separated in different data centers with different sub-nets.

  A data center outage requires the users to register with the SBC in the other data center before they can originate or receive new calls. In this scenario the phones must be configured with the IP addresses of the SBC's in both data centers and must register with the secondary SBC when connectivity to the primary SBC is lost.

7.2.5 SBC (Session Border Controller) Configuration - Connection of Branch Offices

An SBC (Session Border Controller) allows the data center to have its own addressing scheme, independent of the addressing schemes of the branch offices.

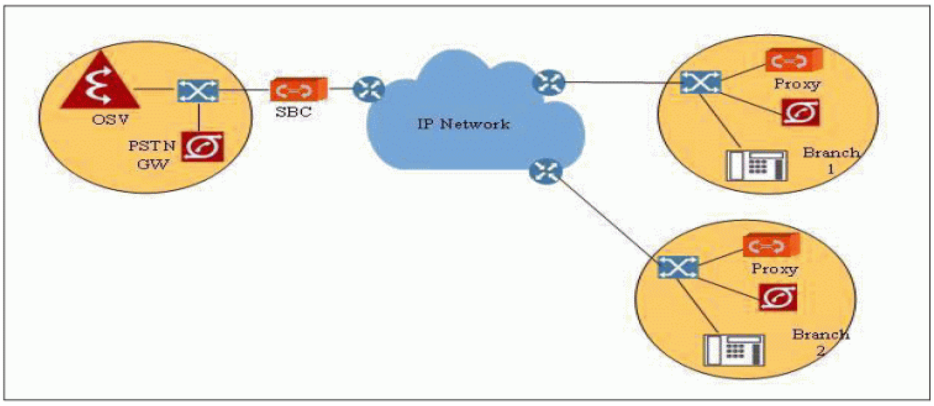
The choice of using a central SBC in the data center or SBCs in each branch office depends on several factors:

- Need for media relay function via an SBC in the data center. The Enterprise policies may require RTP (Real-time Transport Protocol) media to pass through the data center rather than allowing direct media connections between the branches.
- Need for media transcoding at a central media relay SBC, e.g., between SRTP (Secure Real-time Transport Protocol) and RTP or between different payload types (codecs).
- Need for enhanced security/firewall capabilities of a central SBC.
- Need for fast recovery from 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; although if the branches are connected to the data center via the public internet and VPN's are used then the advantage of the branch SBC is lost.

If a branch office includes a PSTN (Public Switched Telephone Network) 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 OpenScape Voice via the SBC.



7.2.6 SBC (Session Border Controller) Configuration - Branch Offices Without Survivability

In a deployment where branch survivability is not required, then users in branch locations may be connected to the OpenScape Voice server via a central SBC (Session Border Controller). This is similar to the remote user scenario, but the branch users are connected via an Enterprise WAN rather than via the public Internet.

If each branch location has its own subnet, then OpenScape Voice based CAC (Call Admission Control) and Emergency Call Location Identification features may be used.

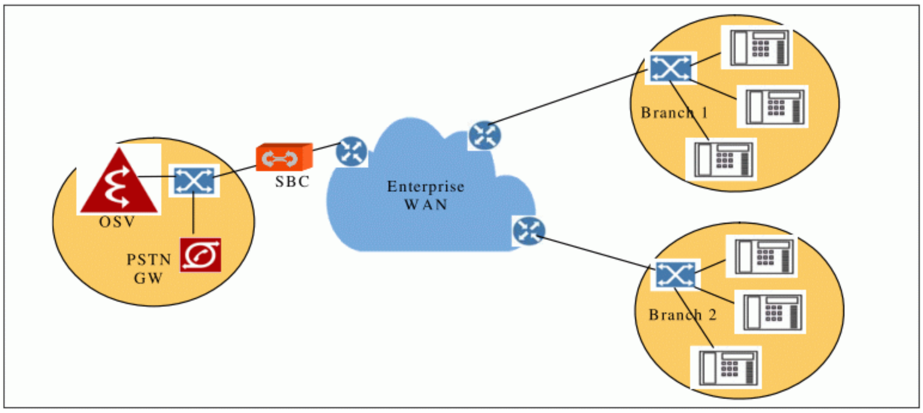
If there is no branch survivability provided, then the following redundancy considerations apply:

- OpenScape Voice cluster nodes are co-located in one data center (or geo-separated but in the same sub-net)

  If a High Availability SBC cluster is deployed, then failure of one SBC is transparent to the branch users.

  If a non-redundant SBC is used, then failure of the SBC results in loss of service until the SBC is repaired.
- OpenScape Voice cluster are geo-separated in different data centers with different sub-nets

  A data center outage requires the branch users register with the SBC in the other data center before they can originate or receive new calls. In this scenario the phones must be configured with DNS SRV or the IP addresses of the SBC's in both data centers and must register with the secondary SBC when connectivity to the primary SBC is lost.

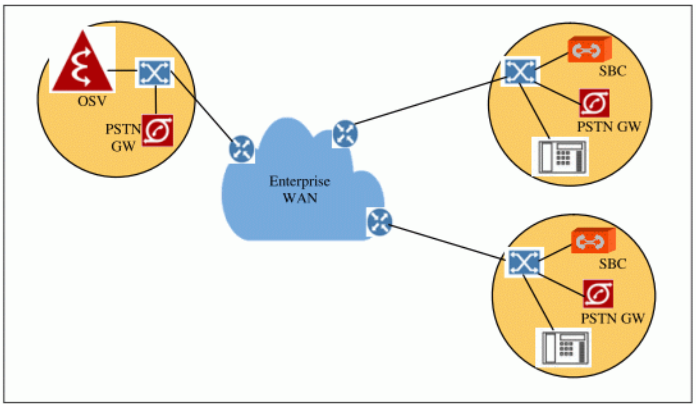


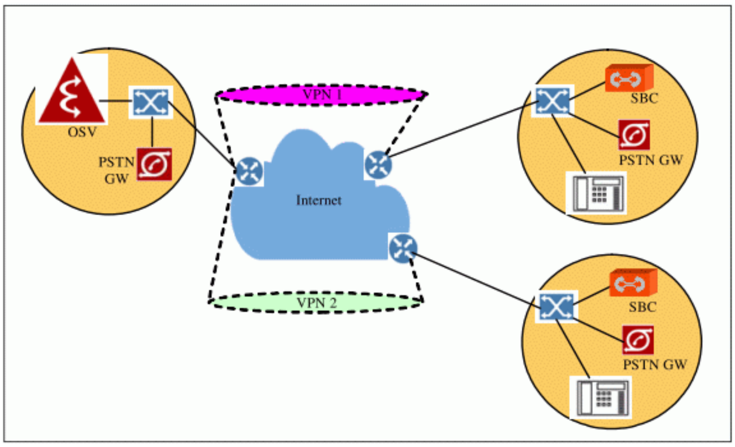
7.2.7 SBC (Session Border Controller) Configuration - SBCs in the Branch Offices (Distributed SBCs)

The SBC (Session Border Controller) allows the branch offices to have their own addressing scheme, independent of the addressing scheme of the data center or other branch offices.

If one must pass through the internet to get from the data center to the branch office, then often the addressing space of the data center is extended to the branch office by creating a VPN tunnel between the data center and the SBC in the branch office. In this scenario there is no central media relay SBC, media connections for inter-branch calls are made directly between branches.

Currently the OpenScape Branch SBC or Comdasys SBC is supported as a branch SBC. These SBCs combine branch survivability and SBC functionality in the same box as well as NAT (Network Address Translation) traversal, firewall pinholing, and (limited) topology hiding for the branch. When VPNs are used between the branch and the data center the Comdasys SBC can be used to terminate the VPNs in the branch and provide dynamic switchover to a secondary VPN if primary VPN fails (in a scenario with geographic separation of OpenScape Voice nodes).

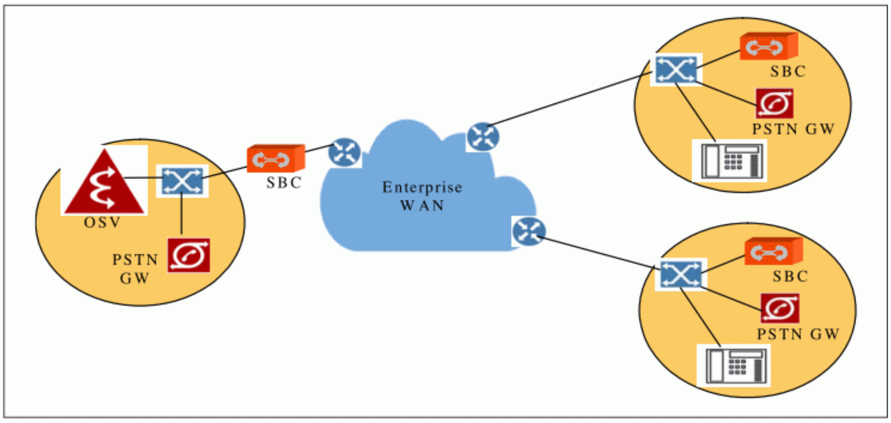




7.2.8 SBC (Session Border Controller) Configuration - SBCs in the Branch Office and in the Data Center (Cascaded SBCs)

In some migration scenarios (where branch SBCs (Session Border Controllers) already exist and a new central SBC is being added) or hosted scenarios (e.g. where direct media connection is allowed only between branches of the same customer), SBCs may be deployed in branch offices and an SBC may also be deployed as a media relay SBC in the data center.

A central SBC may also be necessary to provide firewall pinholing if there are firewalls present between the branch SBC and the data center. In scenarios where a customer requires a SIP-aware Firewall (with port pinholing) in the branch as well as in the data center, then cascaded SBCs may be necessary. The cascaded SBC configuration is not supported as a standard solution, but may be deployed on a project specific basis.



7.2.9 SBC (Session Border Controller) Configuration - Connection to SIP Service Providers

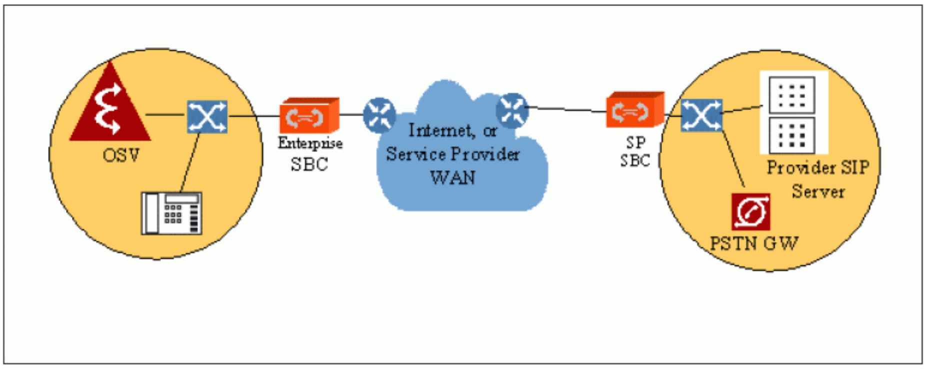
The OpenScape Voice server is located in the main office data center, the connection to the SIP Service Provider is achieved using the internet or the Service Provider WAN/MAN. There is no direct connection between the

OpenScape-Voice and the service provider’s SIP Server. An SBC (Session Border Controller) is used to secure and inter-work 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 (internet/WAN/MAN).

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 (Public Switched Telephone Network) call would always be:

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



7.2.10 OpenScape Voice Configuration - Remote Users (or Users in Branches with no SIP Proxy)

OpenScape Voice allows the usage of connection-less protocols (such as UDP, User Datagram Protocol) as well as connection-oriented protocols (such as TCP).

When UDP transport is used for remote users connecting to the OpenScape Voice via a central SBC (Session Border Controller), there are no provisioning considerations due to the SBC. The remote users are provisioned at OpenScape Voice as if they were local users.

When TCP or TLS (Transport Layer Security) transport is used for remote users connecting to the OpenScape Voice via a central SBC, an EP (Endpoint) should be created. This allows a single TCP/TLS connection to be used between the SBC (Session Border Controller) and OpenScape Voice for all remote user SIP signaling traffic.

Create the EP as a statically registered EP with the IP address/port of the interface created on the core side of the SBC for remote users connecting to the OpenScape Voice. The alias name of the endpoint should also be the IP address of the interface created on the core side of the SBC.

Ensure that Registration Randomization is enabled in OpenScape Voice.

The following EP attributes must also be set:

- SIP Proxy
- Route via Proxy
- Allow Endpoint to Unregister Stale Contact

OpenScape Voice SIP Realm configuration

IMPORTANT:

When Session Border Controllers are used, the OpenScape Voice RTP variable setting `Srx/Sip/AuthTraverseViaHdrs` [15]must be set to `false`. Failure to do so may lead to erroneously accepting and processing of SIP requests from unauthorized SIP interfaces.

The Session Border Controller (SBC) is considered a trusted interface which means all SIP requests originating by the SBC will be accepted as pre-authorized. OpenScape Voice Digest Authentication must be configured to include the network realm consisting of the Session Border Controller inside or core signaling address (IP + port-range). This configuration is common to all OpenScape Voice configurations utilizing Session Border Controllers.

All OpenScape Voice remote users must be excluded from the OpenScape Voice trusted realm to allow proper SIP request authorization. All mapped Session Border Controller addresses (IP + port-range) identifying static or dynamically registering remote user contact addresses must not be included as a trusted realm for OpenScape Voice Digest Authentication.

NOTICE:

Remote SBC End Points having the same SBC core signaling address with different sip port can be included as a trusted realm in the OpenScape Voice server Digest Authentication settings only with the same Digest authentication credentials (Username, password, realm etc). That is why OSV supports a unique Signaling IP entry in the Digest Authentication trusted realm list.

7.2.11 OpenScape Voice Configuration - Branch Users

A single layer 3 connection can be used between the SBC (Session Border Controller) and OpenScape Voice for branch user connecting to the OpenScape Voice via a central SBC.

In order to use this functionality an EP (Endpoint) for each branch must be created. The EP needs to be a statically registered EP with the IP address/port of the interface created on the core side of the SBC for branch users connecting to the OpenScape Voice. The alias name of the EP should also be the IP address of the interface created on the core side of the SBC.

Ensure that Registration Randomization is enabled in OpenScape Voice.

The following endpoint attributes must also be set:

[15] RTP Parameters are located in following screen **OpenScape Voice** > **Administration** > **General Settings** > **RTP**

- SIP Proxy
- Route via Proxy
- RTP (Real-time Transport Protocol) configuration parameter (`Srx/Sip/EnableProxyRegistration` must be set to a value of `true`)
- If a survivable branch proxy is used, the EP shall be marked as survivable.
- The OpenScape Voice registration renewal option should be enabled.
- For OSV V8 onwards configure an endpoint in OSV for the central SBC with protocol TCP/TLS which has the **Central SBC** attribute set.

  If such an endpoint is not configured the SIP registrar may consider a branch user to be a remote user and consequently refuse service to this subscriber depending on the value of the subscriber's **Registration via Central SBC Allowed** flag.

The OpenScape Voice SIP Realm for the Session Border Controller must be configured as defined in chapter OpenScape Voice Configuration - Remote Users (or Users in Branches with no SIP Proxy)

7.2.12 OpenScape Voice Configuration - Comdasys or OpenScape Branch SIP Proxy Configuration

In order to configure the Comdasys Branch or OpenScape Branch as SIP Proxy the PBX (Private Branch eXchange) address, domains and gateways must be specified.

The Comdasys Branch or OpenScape Branch SIP Proxy should configured with:

- PBX Address = IP address of SBC (Session Border Controller) access side
- Domains = IP address of SBC access side
- Gateways = IP address of branch gateway

The OpenScape Voice SIP Realm for the Session Border Controller must be configured as defined in chapter "OpenScape Voice Configuration - Remote Users (or Users in Branches with no SIP Proxy)".

All Comdasys or OpenScape Branch proxy servers are considered trusted network elements, however this trust does not extend to other interfaces behind the proxy server. Within the OpenScape Voice server Digest Authentication settings, the OpenScape Session Border Controller's mapped signaling address (IP+port-range) associated with the Comdasys or OpenScape Branch originating SIP signaling address must be included as a trusted realm in the OpenScape Voice server Digest Authentication settings.

7.2.13 OpenScape Voice Configuration - Branch Gateways

To allow calls to be routed from the OpenScape Voice to the correct gateway additional EPs (Endpoints) need to be created for each SIP Gateway (PSTN (Public Switched Telephone Network) gateway) in a branch.

Gateways may register dynamically or be statically registered.

Support for SIP GW's behind the Branch do not necessary require assignment of an IP address for a SIP EP used as an alias for the GW. It is possible to share the same EP used for routing requests towards branch users. The starting point for such a configuration is the Proxy or Branch configuration.

For the SIP GW's which register dynamically, an EP is used to support the registration but does not necessary require assignment of an IP address provided an alias is identified for the EP and is trusted. not always required. In some cases it is possible to share the same Proxy EP used for routing requests towards branch users.

If the SIP GW requires static registration a unique EP with address associated with SBC core is created. The EP should be configured with an alias name corresponding to the User Name configured in the gateway. The SIP Proxy and Route via Proxy attributes are not required for this EP.

If the SIP GW supports survivability the SIP EP "Survivable Endpoint" should be enabled.

Branch gateway EPs can be associated with an SIP EPP (Endpoint Profile) in order to enable services such as:

- Incoming name delivery
- Voice Mail
- Called name/number delivery
- Call Transfer
- Call Forward Invalid Destination

The OpenScape Voice SIP Realm for the Branch SIP Proxy must be configured as defined in chapter "OpenScape Voice Configuration - Remote Users (or Users in Branches with no SIP Proxy)".

If the OpenScape Branch Gateway is considered a trusted interface, the OpenScape Session Border Controller’s mapped signaling address (IP+port-range) associated with the OpenScape Branch Gateway originating SIP signaling address must be included as a trusted realm in the OpenScape Voice server Digest Authentication settings.

7.2.14 OpenScape Voice Configuration - Mediatrix Branch PSTN (Public Switched Telephone Network) Gateway Configuration

In order to configure the Mediatrix Branch as PSTN Gateway, register host, proxy host and outbound proxy host must be specified.

Server screen

- Register Host = IP address of SBC access side
- Proxy Host = IP address of SBC access side
- Outbound Proxy Host = Comdasys Proxy IP address

Registration screen

- Set Endpoint: register = enable and User Name to name identifying the GW, Mdx-Branch in our example.

7.2.15 OpenScape Voice Configuration - SIP Trunking Gateway Configuration

To allow calls to be routed from the OpenScape Voice to the correct gateway additional Endpoints (EP) need to be created for each SIP Gateway (PSTN (Public Switched Telephone Network) gateway).

Gateways may dynamically register however most are statically registered. Only the static registration scenario is described.

An EP should be created as statically registered with the IP address/port of the interface created on the core side of the SBC for the gateway. The SBC should have its own configuration for associating the SBC core interface to the SBC's peer network interface for the gateway. The EP should be configured with an alias name corresponding to the User Name configured in the gateway. The SIP Proxy and Route via Proxy attributes are not required for this EP.

If the SIP Trunking Gateway is considered a trusted interface, the OpenScape Session Border Controller’s mapped signaling address (IP+port, port range, or FQDN) associated with the SIP Trunking Gateway originating SIP signaling address must be included as a trusted realm in the OpenScape Voice server Digest Authentication settings.

NOTICE:

Remote SBC End Points having the same SBC core signaling address with different sip port can be included as a trusted realm in the OpenScape Voice server Digest Authentication settings only with the same Digest authentication credentials (Username, password, realm etc). That is why OSV supports a unique Signaling IP entry in the Digest Authentication trusted realm list.

For more information see Chapter Proxy Registration Model

7.2.16 Supported SIP Trunk Service Providers

It is the responsibility of the SEC Local Company to arrange any pre-cutover interoperability tests that the SIP Service Provider requires. Most SIP Service Providers require these tests to be performed before allowing live traffic to be routed over the SIP Trunk, even when OpenScape Voice has successfully connected to the same Service Provider at other installations.

OpenScape Voice has successfully connected to the following SIP Service Providers:

- AT&T IP Toll-Free
- AT&T Flex Reach
- BT
- COLT Telecom
- Central SBC
- Comdasys Proxy 1600
- Comdasys Proxy 2600
- Comdasys Proxy 3600

- Comdasys SBC 1600
- Comdasys SBC 2600
- Comdasys SBC 3600
- DTAG/T-Systems
- Global Crossing
- Italtel
- Orange
- Qwest
- Skype
- Telefonica
- Verizon EMEA IP Trunking
- Verizon IPCC Trunking
- Verizon US IP Trunking
- Vodafone / Arcor

7.2.17 Net-Net 3000, Net-Net 4000 Series SBC - Basic Configuration

In the following example the Net-Net 3800 has been used however the configuration is the same for this product series.

This section covers a basic access configuration environment with a single NAT homed in the core side. It also describes how to configure the system in High Availability (HA) mode. All logical IP addresses needed to configure an ACME Net-Net 3800 SBC are listed and described below. They are referenced through out this guide but will need to be replaced by IP addresses specific to the user's network.

Logical IP Address	Description
[accesslip]	IP address of the Acme SD for the access realm.
[accesspri]	For redundancy, Address of primary HA peer (access side).
[accesssec]	For redundancy, Address of secondary HA peer (access side).
[accessmask]	Subnet mask on the access side.
[accessgw]	Default gateway on the access side.
[coreip]	IP address of the Acme SD for the core realm (SIP traffic).
[coreiprtp]	IP address of the Acme SD for the core realm (RTP traffic).
[corepri]	For redundancy, Address of primary HA peer (core side).
[coresec]	For redundancy, Address of secondary HA peer (core side).
[coremask]	Subnet mask on the core side.
[coregw]	Default gateway on the core side.

Logical IP Address	Description
`[internalHomeAdd]`	Internal home address for the SIP-NAT. Must be different from the IP address of the home realm's network interface.
`[sipserver1]`	IP address of SIP server 1 (OSV linked to realm accessRealm).
`[wancom1pri]`	For redundancy, Address of primary HA peer (wancom1).
`[wancom1sec]`	For redundancy,Address of secondary HA peer (wancom1).
`[wancom1mask]`	For redundancy, Subnet mask for wancom1 interface.
`[wancom2pri]`	For redundancy, Address of primary HA peer (wancom2).
`[wancom2sec]`	For redundancy, Address of secondary HA peer (wancom2).
`[wancom2mask]`	For redundancy, Subnet mask for wancom2 interface.

Related concepts

Net-Net 3000, Net-Net 4000 Series SBC - Branch Deployment Scenario using OpenScape Branch (Proxy) on page 800

7.2.17.1 System Configuration

The basic system parameters are configured in the system-config object

```
system-configuration
hostname <your_system_host_name>
description
location
mib-system-contact
mib-system-name
mib-system-location
snmp-enabled enabled
enable-snmp-auth-traps disabled
enable-snmp-syslog-notify disabled
enable-snmp-monitor-traps disabled
snmp-syslog-his-table-length 1
snmp-syslog-level  WARNING
system-log-level WARNING
```

```
syslog-server
address <ip address>
port 514
facility 4
process-log-level NOTICE
process-log-ip-address 0.0.0.0
process-log-port 0
collect
push-interval 15
boot-state disabled
start-time now
sample-interval 5
end-time never
red-collect-state disabled
red-max-trans 1000
red-sync-start-time 5000
red-sync-comp-time 1000
push-success-trap-state disabled
call-trace disabled
internal-trace disabled
log-filter all
default-gateway [gw ip address]
restart enabled
exceptions
telnet-timeout 0
console-timeout 0
remote-control enabled
cli-audit-trail enabled
link-redundancy-state disabled
source-routing enabled
// source-routing - Enable or disable source routing egress
HIP packets //based on source IP addresses.
// source-routing should be enabled
cli-more disabled
terminal-height 24
debug-timeout 0
trap-event-lifetime 0
default-v6-gateway ::
```

```
ipv6-support disabled
clean-up-time-of-day 00:00
```

7.2.17.2 Physical Interfaces

The physical interfaces are configured for the access and core network.

The parameter virtual-mac is covered in the Acme Packet Document 520-0011-03_BCP_High_Availability_Configuration

Configure physical interfaces for the access network

```
phy-interface
name s0p0
operation-type Media
// operating-type should be set to Media for signaling traffic
port 0
slot 0
virtual-mac
admin-state enabled
auto-negotiation enabled
duplex-mode 100
speed 100
overload-protection disabled
```

Configure physical interfaces for the core network

```
phy-interface
name s1p0
operation-type Media
// operating-type should be set to Media for signaling traffic
port 0
slot 1
virtual-mac
admin-state enabled
auto-negotiation enabled
duplex-mode FULL
speed 100
overload-protection disabled
```

Configure physical interface wancom1 & wancom2 for the interconnection of two HA peers (redundancy)

```
phy-interface
name wancom1
operation-type Control
// used for heartbeats & HA
// operating-type should be set to Control for HA traffic
port 1
slot 0
virtual-mac
wancom-health-score 8
overload-protection disabled
```

```
phy-interface
name wancom2
operation-type Control
// used for heartbeats & HA
// operating-type should be set to Control for HA traffic
port 2
slot 0
virtual-mac
wancom-health-score 9
overload-protection disabled
```

7.2.17.3 Network Interfaces

Configure the network interfaces for the access/core sides and wancom ports.

```
network-interface
name s0p0
sub-port-id 0
description Access Network interface
hostname
ip-address [access1ip]
pri-utility-addr  [accesspri]
// for HA only (primary HA peer)
sec-utility-addr [accesssec]
// for HA only (secondary HA peer)
netmask [accessmask]
gateway [accessgw]
```

```
sec-gateway
gw-heartbeat
state enabled
// front interface link detection enabled
heartbeat 10
// time interval in seconds between heartbeats
retry-count  3
// number of retries
retry-timeout 1
// timeout for retries
health-score 30
// amount to subtract from health if heartbeat fails
dns-ip-primary
dns-ip-backup1
dns-ip-backup2
dns-domain
dns-timeout 11
hip-ip-list [access1ip] [access2ip]
ftp-address
icmp-address [access1ip] [access2ip]
// adding a sip-interface to both the hip-ip-list and icmp-address allows this ip address to respond to pings
snmp-address
telnet-address
ssh-address

network-interface
name s1p0
sub-port-id 0
description Core network interface
hostname
ip-address [coreip]
pri-utility-addr [coreippri]
sec-utility-addr [coreipsec]
netmask [coremask]
gateway [coregw]
sec-gateway
gw-heartbeat
```

```
state disabled
heartbeat 0
retry-count  0
retry-timeout 1
health-score 0
dns-ip-primary
dns-ip-backup1
dns-ip-backup2
dns-domain
dns-timeout 11
hip-ip-list [coreip] [coreiprtp]
ftp-address
icmp-address [coreip] [coreiprtp]
// adding a sip-interface to both the hip-ip-list and icmp-address allows this ip address to respond to pings
snmp-address
telnet-address
ssh-address

network-interface
name wancom1
sub-port-id 0
description
hostname
ip-address
pri-utility-addr [wancom1pri]
// address of primary HA peer
sec-utility-addr [wancom1sec]
// address of secondary HA peer
netmask [wancom1mask]
gateway
sec-gateway
gw-heartbeat
state disabled
heartbeat 0
retry-count  0
retry-timeout 1
health-score 0
```

```
dns-ip-primary
dns-ip-backup1
dns-ip-backup2
dns-domain
dns-timeout 11
hip-ip-list
ftp-address
icmp-address
snmp-address
telnet-address
ssh-address

network-interface
name wancom2
sub-port-id 0
description
hostname
ip-address
pri-utility-addr [wancom2pri]
sec-utility-addr [wancom2sec]
netmask [wancom2mask]
gateway
sec-gateway
gw-heartbeat
state disabled
heartbeat 0
retry-count  0
retry-timeout 1
health-score 0
dns-ip-primary
dns-ip-backup1
dns-ip-backup2
dns-domain
dns-timeout 11
hip-ip-list
ftp-address
icmp-address
snmp-address
```

```
telnet-address
ssh-address
```

7.2.17.4 Redundancy Configuration / HA (High Availability)

This element has to be configured for redundancy only. The gateway heartbeat values are configured in the network-interface elements.

configuration path: `redundancy`

(path: `conf t -> system -> redundancy`)

```
redundancy-config
state enabled
log-level  INFO
health-threshold 75
emergency-threshold 50
port 9090
// redundancy protocol uses port 9090
advertisement-time 500
percent-drift 210
initial-time 1250
becoming-standby-time 180000
becoming-active-time 100
cfg-port 1987
cfg-max-trans 10000
cfg-sync-start-time 5000
cfg-sync-comp-time 1000
gateway-heartbeat-interval 0
gateway-heartbeat-retry 0
gateway-heartbeat-timeout 1
gateway-heartbeat-health 0
media-if-peercheck-time 0
peer
name acmenode1
// Target name for node1's name (bootparameters)
state enabled
type Primary
destination
address [wancom1pri]:9090
network-interface wancom1:0
```

```
destination
address [wancom2pri]:9090
network-interface wancom2:0
```

```
peer
name acmenode1
// Target name for node2's name (bootparameters)
state enabled
type Secondary
destination
address [wancom1sec]:9090
network-interface wancom1:0
destination
address [wancom2sec]:9090
network-interface wancom2:0
```

7.2.17.5 Realms

Configure the realms for the access and the core side.

Configuration of realm for the access side

```
realm-config
identifier accessRealm
description
addr-prefix 0.0.0.0
network-interfaces s0p0:0
//network interface : VLAN
mm-in-realm enabled
//media-routing based on realm
mm-in-network enabled
//media-routing based on network
mm-same-ip enabled
//media-routing for clients behind same IP
mm-in-system enabled
//Enable to release media between two SIP peers, between
two //realms on two network interfaces of the same Net-Net
SBC. //Disable to always release the media, regardless of
inter- ///face and realm. The default is enabled
bw-cac-non-mm disabled
msm-release disabled
```

```
qos-enable disabled
generate-UDP-checksum disabled
max-bandwidth 0
fallback-bandwidth 0
max-priority-bandwidth 0
max-latency 0
max-jitter 0
max-packet-loss 0
observ-window-size 0
parent-realm
dns-realm
media-policy
media-sec-policy
in-translationid
out-translationid
in-manipulationid
// Header Manipulation - see sip-manipulation
out-manipulationid
// Header Manipulation - see sip-manipulation
manipulation-string
manipulation-pattern
class-profile
average-rate-limit 0
access-control-trust-level none
invalid-signal-threshold 0
maximum-signal-threshold 0
untrusted-signal-threshold 0
nat-trust-threshold 0
deny-period 30
ext-policy-svr
symmetric-latching enabled
pai-strip disabled
trunk-context
early-media-allow
enforcement-profile
additional-prefixes
restricted-latching none
```

```
restriction-mask 32
accounting-enable enabled
user-cac-mode none
user-cac-bandwidth 0
user-cac-sessions 0
icmp-detect-multiplier 0
icmp-advertisement-interval 0
icmp-target-ip
monthly-minutes 0
net-management-control disabled
delay-media-update disabled
refer-call-transfer disabled
dyn-refer-term disabled
codec-policy
codec-manip-in-realm disabled
constraint-name
call-recording-server-id
xnq-state xnq-unknown
hairpin-id 0
stun-enable disabled
stun-server-ip 0.0.0.0
stun-server-port 3478
stun-changed-ip 0.0.0.0
stun-changed-port 3479
match-media-profiles
qos-constraint
sip-profile
sip-isup-profile
block-rtcp disabled
hide-egress-media-update disabled
```

Configuration of the realm for the core side

```
realm-config
identifier coreRealm
description
addr-prefix [IP address] / [mask]
//should cover OSV addresses
network-interfaces s1p0:0
```

```
//network interface : VLAN
mm-in-realm disabled
mm-in-network enabled
mm-same-ip enabled
mm-in-system enabled
bw-cac-non-mm disabled
msm-release disabled
qos-enable disabled
generate-UDP-checksum disabled
max-bandwidth 0
fallback-bandwidth 0
max-priority-bandwidth 0
max-latency 0
max-jitter 0
max-packet-loss 0
observ-window-size 0
parent-realm
dns-realm
media-policy
media-sec-policy
in-translationid
out-translationid
in-manipulationid
// Header Manipulation - see sip-manipulation
out-manipulationid
// Header Manipulation - see sip-manipulation
manipulation-string
manipulation-pattern
class-profile
average-rate-limit 0
access-control-trust-level none
invalid-signal-threshold 0
maximum-signal-threshold 0
untrusted-signal-threshold 0
nat-trust-threshold 0
deny-period 30
ext-policy-svr
```

```
symmetric-latching disabled
pai-strip disabled
trunk-context
early-media-allow
enforcement-profile
additional-prefixes
restricted-latching none
restriction-mask 32
accounting-enable enabled
user-cac-mode none
user-cac-bandwidth 0
user-cac-sessions 0
icmp-detect-multiplier 0
icmp-advertisement-interval 0
icmp-target-ip
monthly-minutes 0
net-management-control disabled
delay-media-update disabled
refer-call-transfer disabled
dyn-refer-term disabled
codec-policy
codec-manip-in-realm disabled
constraint-name
call-recording-server-id
xnq-state xnq-unknown
hairpin-id 0
stun-enable disabled
stun-server-ip 0.0.0.0
stun-server-port 3478
stun-changed-ip 0.0.0.0
stun-changed-port 3479
match-media-profiles
qos-constraint
sip-profile
sip-isup-profile
block-rtcp disabled
hide-egress-media-update disabled
```

7.2.17.6 Steering Pools (RTP)

Configure the steering pools for the different realms.

Configure the steering pool for the realm "accessRealm"

```
steering-pool
ip-address [access1ip]
start-port 30000
end-port 60000
realm-id accessRealm
// name of the realm
network-interface
```

Configure the steering pool for the realm "coreRealm"

```
steering-pool
ip-address [coreiprtp]
start-port 30000
end-port 60000
realm-id coreRealm
// name of the realm
network-interface
```

7.2.17.7 Global SIP Configuration

Configure the global SIP config element.

```
sip-config
state enabled
operation-mode dialog
dialog-transparency enabled
home-realm-id accessRealm
// home realm
egress-realm-id
nat-mode Public
// mode for sip-nat
registrar-domain *
registrar-host *
registrar-port 5060
register-service-route always
init-timer 500
```

```
max-timer 4000

trans-expire 32

invite-expire 600

inactive-dynamic-conn 32

enforcement-profile

pac-method

pac-interval 10

pac-strategy PropDist

pac-load-weight 1

pac-session-weight 1

pac-route-weight 1

pac-callid-lifetime 600

pac-user-lifetime 3600

red-sip-port 1988

red-max-trans 10000

red-sync-start-time 5000

red-sync-comp-time 1000

add-reason-header disabled

sip-message-len 4096

enum-sag-match disabled

extra-method-stats enabled

// The extra-method-stats option can be used to aid in
debugging and to throttle session traffic at the SIP-method
level. //

// warning: extra-method-stats should not be enabled under
heavy load due to the small performance impact of enabling
extra-method stats. //

registration-cache-limit 0

register-use-to-for-lp enabled

options force-unregistration

// forced unregistration to OSV if remote phones lose
connectivity with sbc. Warning: This option is NOT
supported if digest authentication is enabled in the OSV
server as the SBC has no way of responding to a new on
behalf of an unreachable/disconnected phone //

ignore-other-reg-expires

max-udp-length=0

//no limit for UDP

reg-cache-mode=none

//no cookies for registration cache
```

```
reinvite-trying
//send "100 Trying" for re-INVITEs
set-inv-exp-at-100-resp
//SIP Timer C is set after 100 trying is received
refer-src-routing disabled
add-ucid-header disabled
proxy-sub-events
pass-gruu-contact disabled
sag-lookup-on-redirect disabled
```

NOTICE:

Additional options can be added with +<new_option> e.g. acmeNode1(sip-interface)# options +set-inv-exp-at-100-resp.

IMPORTANT:

If the + is omitted, existing "options" will be overidden.

7.2.17.8 SIP Interfaces

Configure the SIP interface for the different realms.

Configure the SIP interface for the realm "accessRealm"

```
sip-interface
state enabled
realm-id accessRealm
description
sip-port
address [access1ip]
port 5060
transport-protocol [protocol]
// UDP, TCP or TLS
tls-profile
allow-anonymous registered
ims-aka-profile
carriers
trans-expire 0
invite-expire 0
max-redirect-contacts 0
```

```
proxy-mode Proxy

redirect-action Proxy

// forward any 3xx Messages to previous hop

contact-mode loose-route

// set contact-mode to loose-route for TCP, none for UDP

nat-traversal always

nat-interval 30

// Sets the expiration time in seconds for the Net-Net
SBC's cached registration entry for an HNT (Hosted NAT
Traversal) endpoint (ie., an endpoint behind a NAT router).
The default is 30. This timer is used to cause the UA to
send REGISTER messages frequently enough to retain the
port binding in the NAT. Retaining the binding lets inbound
requests to be sent through the NAT. //

tcp-nat-interval 90

// This option is the same as the nat-interval but applies
to TCP subscribers behind a NAT. //

registration-caching enabled

// Enable for use with all UAs, not just those that
are behind NATs. This option should always be enabled
for remote users and endpoints/gateways with dynamic
registration.//

min-reg-expire 300

// This option should not affect traffic on the access sip-
interface.

registration-interval 3600

// Enter the expiration time in seconds that you want the
Net-Net SBC to use in the REGISTER response message sent
back to the UA. The UA then refreshes its registration by
sending another REGISTER message before that time expires.
The default is 3600. A registration interval of zero causes
the Net-Net SBC to pass back the expiration time set by and
returned in the registration response from the registrar.
This setting applies to Non-HNT endpoints //

route-to-registrar enabled

//routing to the registrar to sends all requests that match
a cached registration to the destination defined for the
registrar host. //

secured-network enabled

teluri-scheme disabled

uri-fqdn-domain

options

preserve-user-info

reg-no-port-match
```

```
//dynamic transport protocol change
reg-via-key=all
//enhanced SIP port mapping
reg-via-match
// see note
reg-via-proxy
// see note
reuse-connections
//required for TCP sip-interfaces
strip-route-headers
//strip all route headers
udp-fallback
via-header-transparency
// see note
trust-mode all
max-nat-interval 3600
nat-int-increment 10
nat-test-increment 30
sip-dynamic-hnt enabled
// enable to introduce variations in local phone
registration timer intervals //
stop-recurse 401,407
port-map-start 0
port-map-end 0
in-manipulationid
out-manipulationid
manipulation-string
manipulation-pattern
sip-ims-feature disabled
operator-identifier
anonymous-priority none
max-incoming-conns 0
per-src-ip-max-incoming-conns 0
inactive-conn-timeout 0
untrusted-conn-timeout 0
network-id
ext-policy-server
default-location-string
```

```
charging-vector-mode pass
charging-function-address-mode pass
ccf-address
ecf-address
term-tgrp-mode none
implicit-service-route disabled
rfc2833-payload 101
rfc2833-mode transparent
constraint-name
response-map
local-response-map
ims-aka-feature disabled
enforcement-profile
route-unauthorized-calls
tcp-keepalive none
add-sdp-invite disabled
add-sdp-profiles
sip-profile
sip-isup-profile
```

> **NOTICE:**
>
> options reg-via-proxy, reg-via-match, via-header-transparency and udp-fallback are required when OpenScape Branch is used as Proxy.

Configure the SIP interface for the realm "coreRealm"

```
sip-interface
state enabled
realm-id coreRealm
description
sip-port
address [coreip]
port 5060
transport-protocol [protocol]
// UDP, TCP or TLS
tls-profile
allow-anonymous all
// trusted side
ims-aka-profile
```

```
carriers

trans-expire 0

invite-expire 0

max-redirect-contacts 0

proxy-mode Proxy

redirect-action Proxy

contact-mode loose-route

// set contact-mode to loose-route for TCP, none for UDP

nat-traversal none

// set to none since no phones register from the core side

nat-interval 30

// should not affect traffic on the core sip-interface //

tcp-nat-interval 90

// should not affect traffic on the core sip-interface //

registration-caching disabled

// should always be disabled on the core sip-interface
since subscribers do not register from core side //

min-reg-expire 300

// Defines the minimum expiration value the Net-Net SBC
places in each REGISTER message it sends to the real
registrar. In HNT, the Net-Net SBC chaches the registration
after receiving a response from the real registrar and sets
the expiration time to the NAT interval value. Default
value is 300 seconds.

registration-interval 300

// should not affect traffic on the core sip-interface//

route-to-registrar disabled

//set to disabled on the core sip-interface //

secured-network disabled

teluri-scheme disabled

uri-fqdn-domain

options

reuse connections

//required for TCP sip-interfaces

tcp-port-mapping=nopath

//to support port-mapping on the core side

trust-mode all

max-nat-interval 3600

nat-int-increment 10
```

```
nat-test-increment 30
sip-dynamic-hnt disabled
stop-recurse 401,407
port-map-start 10000
// start of SIP port mapping range
port-map-end 60000
// end of SIP port mapping range
in-manipulationid
out-manipulationid
manipulation-string
manipulation-pattern
sip-ims-feature disabled
operator-identifier
anonymous-priority none
max-incoming-conns 0
per-src-ip-max-incoming-conns 0
inactive-conn-timeout 0
untrusted-conn-timeout 0
network-id
ext-policy-server
default-location-string
charging-vector-mode pass
charging-function-address-mode pass
ccf-address
ecf-address
term-tgrp-mode none
implicit-service-route disabled
rfc2833-payload 101
rfc2833-mode transparent
constraint-name
response-map
local-response-map
ims-aka-feature disabled
enforcement-profile
route-unauthorized-calls
tcp-keepalive none
add-sdp-invite disabled
```

```
add-sdp-profiles
sip-profile
sip-isup-profile
```

7.2.17.9 SIP NAT

Configure the SIP NAT for the access realm (a single sip NAT can also be defined for a core realm).

```
sip-nat
realm-id accessRealm
domain-suffix .access.siemens.net
ext-proxy-address [accessgw]
// Proxy or access GW address
ext-proxy-port 5060
ext-address [access1ip]
home-address [internalHomeAdd]
// ** address in network of realm opposite to realm-id
of sip-nat - cannot match any network interface address.
In this case, it should be an address on the core network
since the realm-id of the current sip-nat is the access
realm. //
home-proxy-address [sipserver]
// OSV
home-proxy-port 5060
route-home-proxy disabled
address-prefix *
tunnel-redirect disabled
use-url-parameter all
parameter-name [parm name]
//should be set to the opposite realm of the current sip-
nat realm-id(i.e., it is access for sip-nat, therefore
parameter-name should be the core-realm's name).
user-nat-tag -acme-
host-nat-tag ACME-
headers
Call-ID Contact f From=ip-ip-tgt i Join
m P-Asserted-Identity r Record-Route Refer-To Referred-by Replaces Reply-To
Route t To=ip-ip-tgt v Via
```

7.2.17.10 SIP Manipulation

Configure the SIP header manipulation rule for the SIP NAT function.

```
sip-manipulation
name NAT_access_out
// name of the ruleset
description sip out manipulations for accessRealm
split-headers
join-headers
header-rule
name manipDiversion
// name of the header rule
header-name Diversion
// name of the header
action manipulate
// header will be manipulated as specified in element rule
comparison-type case-sensitive
msg-type any
//request & response
methods
match-value
new-value
element-rule
name Diversion
parameter-name
type uri-host
action replace
match-val-type ip
comparison-type case-sensitive
match-value
new-value $LOCAL_IP

sip-manipulation
name NAT_core_out
// name of the ruleset
description sip out manipulations for coreRealm
split-headers
join-headers
```

```
header-rule
name addRR
// needed when using TCP and Dynamic Port Mapping
header-name Record Route
// name of the header
action add
// header will added
comparison-type case-sensitive
msg-type any
methods
match-value
new-value <sip:+$LOCAL_IP+:5060;transport=tcp>
header-rule
name manipDiversion
header-name Diversion
action manipulate
comparison-type case-sensitive
msg-type any
methods
match-value
new-value
element-rule
name Diversion
parameter-name
type uri-host
action replace
match-val-type ip
comparison-type case-sensitive
match-value
new-value $LOCAL_IP

sip-manipulation
name NAT_core_int
// needed OpenScape Branch Proxy is used
description in sip manipulations for coreRealm
split-headers
join-headers
header-rule
```

```
name delRR
header-name Record-Route
action delete
comparison-type case-sensitive
msg-type reply
methods invite, subscribe
match-value
new-value
```

7.2.17.11 Session Agents

Configure the session agents for SIP Server (OSV) and access side (OpenScape Branch).

Configure the session agent for SIP Server (OSV)

```
session-agent
hostname [sipserver]
// OSV FQDN
ip-address [sipserver]
// OSV IP
port 5060
state enabled
app-protocol SIP
app-type
transport-method <protocol>
//UDP, UDP+TCP, DynamicTCP, StaticTCP, DynamicTLS or
StaticTLS //
realm-id coreRealm
// core side realm
egress-realm-id
description
carriers
allow-next-hop-lp enabled
constraints disabled
max-sessions 0
max-inbound-sessions 0
max-outbound-sessions 0
max-burst-rate 0
max-inbound-burst-rate 0
```

`max-outbound-burst-rate` *0*

`max-sustain-rate` *0*

`max-inbound-sustain-rate` *0*

`max-outbound-sustain-rate` *0*

`min-seizures` *5*

`min-asr` *0*

time-to-resume *0*

`ttr-no-response` *0*

`in-service-period` *0*

`burst-rate-window` *0*

`sustain-rate-window` *0*

`req-uri-carrier-mode` *None*

`proxy-mode`

`redirect-action`

`loose-routing` *enabled*

`send-media-session` *enabled*

`response-map`

`ping-method*`

`ping-interval` *0*

`ping-send-mode` *keep-alive*

`ping-all-addresses` *disabled*

`ping-in-service-response-codes`

`out-service-response-codes`

`media-profiles`

`in-translationid`

`out-translationid`

`trust-me` *disabled*

`request-uri-headers`

`stop-recurse`

`local-response-map`

`ping-to-user-part`

`ping-from-user-part`

`li-trust-me` *disabled*

`in-manipulationid`

`out-manipulationid`

`manipulation-string`

`manipulation-pattern`

```
p-asserted-id
trunk-group
max-register-sustain-rate 0
early-media-allow
invalidate-registrations disabled
rfc2833-mode none
rfc2833-payload 0
codec-policy
enforcement-profile
refer-call-transfer disabled
reuse-connections NONE
tcp-keepalive none
tcp-reconn-interval 0
max-register-burst-rate 0
register-burst-window 0
sip-profile
sip-isup-profile
```

Configure the session agent for access side (OpenScape Branch)

```
session-agent
hostname [accessgw or Proxy]
// OpenScape Branch IP or FQDN
ip-address [accessgw or Proxy]
// OpenScape Branch IP
port 5060
state enabled
app-protocol SIP
app-type
transport-method <protocol>
//UDP, UDP+TCP, DynamicTCP, StaticTCP, DynamicTLS or
StaticTLS //
realm-id accessRealm
// access side realm
egress-realm-id
description
carriers
allow-next-hop-lp enabled
constraints disabled
```

`max-sessions` *0*

`max-inbound-sessions` *0*

`max-outbound-sessions` *0*

`max-burst-rate` *0*

`max-inbound-burst-rate` *0*

`max-outbound-burst-rate` *0*

`max-sustain-rate` *0*

`max-inbound-sustain-rate` *0*

`max-outbound-sustain-rate` *0*

`min-seizures` *5*

`min-asr` *0*

`time-to-resume` *0*

`ttr-no-response` *0*

`in-service-period` *0*

`burst-rate-window` *0*

`sustain-rate-window` *0*

`req-uri-carrier-mode` *None*

`proxy-mode`

`redirect-action`

`loose-routing` *enabled*

`send-media-session` *enabled*

`response-map`

`ping-method*`

`ping-interval` *0*

`ping-send-mode` *keep-alive*

`ping-all-addresses` *disabled*

`ping-in-service-response-codes`

`out-service-response-codes`

`media-profiles`

`in-translationid`

`out-translationid`

`trust-me` *disabled*

`request-uri-headers`

`stop-recurse`

`local-response-map`

`ping-to-user-part`

`ping-from-user-part`

```
li-trust-me disabled
in-manipulationid
out-manipulationid
manipulation-string
manipulation-pattern
p-asserted-id
trunk-group
max-register-sustain-rate 0
early-media-allow
invalidate-registrations disabled
rfc2833-mode none
rfc2833-payload 0
codec-policy
enforcement-profile
refer-call-transfer disabled
reuse-connections NONE
tcp-keepalive none
tcp-reconn-interval 0
max-register-burst-rate 0
register-burst-window 0
sip-profile
sip-isup-profile
```

7.2.17.12 Local Policies

Configure the local policies for the different realms.

Configure the local policy for the realm "accessRealm"

```
local-policy
from-address *
to-address *
source-realm accessRealm
description
activate-time N/A
deactivate-time N/A
state enabled
policy-priority none
policy-attribute
```

```
next-hop [sipserver]
// OSV FQDN or IP
realm coreRealm
action none
terminate-recursion disabled
carrier
start-time 0000
end-time 2400
days-of-week U-S
cost 0
app-protocol SIP
state enabled
methods
media-profiles
lookup single
next-key
eloc-str-lkup disabled
eloc-str-match
```

Configure the local policy for the realm "coreRealm"

This core side policy is only needed when OpenScape Branch is used or when configuring a "Peering" setup.

```
local-policy
from-address *
to-address *
source-realm coreRealm
description
activate-time N/A
deactivate-time N/A
state enabled
policy-priority none
policy-attribute
next-hop [accessgw or Proxy]
realm accessRealm
action none
terminate-recursion disabled
carrier
start-time 0000
```

```
end-time 2400
days-of-week U-S
cost 0
app-protocol SIP
state enabled
methods
media-profiles
lookup single
next-key
eloc-str-lkup disabled
eloc-str-match
```

7.2.17.13 NTP Configuration

Configure the NTP settings

configuration path: `local-policy` (path: `conf t -> ntp-sync`)

```
ntp-config
server 172.20.33.12
last-modified-by admin@10.232.1.138
last-modified-date 2010-02-17 18:54:36
```

To configure an NTP server, enter the ntp-config text as described above and add the server.

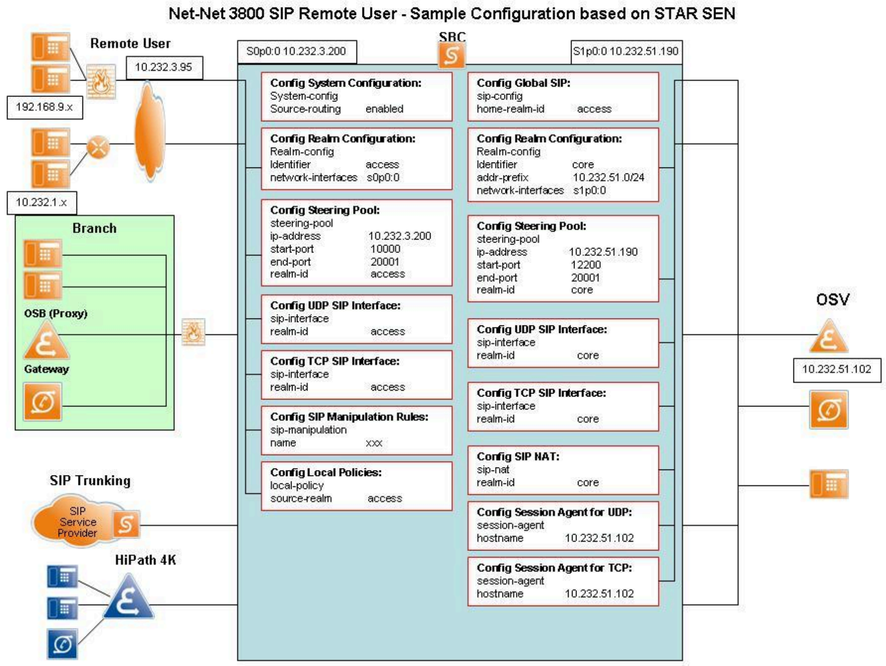
```
SolAcme3800A (ntp-config)
SolAcme3800A (ntp-config) # add-server 172.20.33.12
SolAcme3800A (ntp-config) # done
ntp-config
server 172.20.33.12
last-modified-by admin@10.232.1.138
last-modified-date 2010-02-17 18:27:53
```

NOTICE:

NTP servers should be configured for High Availability Clusters and for TLS

7.2.18 Net-Net 3000, Net-Net 4000 Series SBC - Remote User Deployment Scenario: Nat or No NAT

The following example describes a Remote User Deployment Scenario with and without usage of NAT.



Configuration for NAT or no NAT is nearly identical. Differences will be noted where relevant.

NOTICE:

This section covers both TCP and UDP configuration for phones that are either behind a NAT or NOT behind a NAT. Do not choose both TCP and UDP session-agents and sip-interfaces.

7.2.18.1 Realms - Remote User Deployment Scenario

Create the different realms and associate with the desired network interface.

Create an accessrealm and associate with the desired network interface

Example access realm for remote phones:

```
realm-config
identifier access
description
addr-prefix 0.0.0.0
network-interfaces s0p0:0
mm-in-realm disabled
```

```
mm-in-network disabled
mm-same-ip disabled
mm-in-system enabled
bw-cac-non-mm disabled
msm-release disabled
qos-enable disabled
generate-UDP-checksum disabled
max-bandwidth 0
fallback-bandwidth 0
max-priority-bandwidth 0
max-latency 0
max-jitter 0
max-packet-loss 0
observ-window-size 0
parent-realm
dns-realm
media-policy
media-sec-policy
in-translationid
out-translationid
in-manipulationid
out-manipulationid
manipulation-string
manipulation-pattern
class-profile
average-rate-limit 0
access-control-trust-level none
invalid-signal-threshold 0
maximum-signal-threshold 0
untrusted-signal-threshold 0
nat-trust-threshold 0
deny-period 30
ext-policy-svr
symmetric-latching disabled
pai-strip disabled
trunk-context
early-media-allow
```

```
enforcement-profile
additional-prefixes
restricted-latching none
restriction-mask 32
accounting-enable enabled
user-cac-mode none
user-cac-bandwidth 0
user-cac-sessions 0
icmp-detect-multiplier 0
icmp-advertisement-interval 0
icmp-target-ip
monthly-minutes 0
net-management-control disabled
delay-media-update disabled
refer-call-transfer disabled
dyn-refer-term disabled
codec-policy
codec-manip-in-realm disabled
constraint-name
call-recording-server-id
xnq-state xnq-unknown
hairpin-id 0
stun-enable disabled
stun-server-ip 0.0.0.0
stun-server-port 3478
stun-changed-ip 0.0.0.0
stun-changed-port 3479
match-media-profiles
qos-constraint
sip-profile
sip-isup-profile
block-rtcp disabled
hide-egress-media-update disabled
last-modified-by admin@10.232.1.138
last-modified-date 2010-07-02 19:02:48
```

NOTICE:

In order to disable Media Anchoring for phones behind a NAT router, both mm-in-realm and mm-same-ip must be set to disabled.

Create a core realm and associate it with the network interface for the remote phones

```
realm-config
identifier core
description
addr-prefix 10.232.51.0/24
network-interfaces s1p0:0
mm-in-realm disabled
mm-in-network disabled
mm-same-ip disabled
mm-in-system enabled
bw-cac-non-mm disabled
msm-release disabled
qos-enable disabled
generate-UDP-checksum disabled
max-bandwidth 0
fallback-bandwidth 0
max-priority-bandwidth 0
max-latency 0
max-jitter 0
max-packet-loss 0
observ-window-size 0
parent-realm
dns-realm
media-policy
media-sec-policy
in-translationid
out-translationid
in-manipulationid
out-manipulationid
manipulation-string
manipulation-pattern
class-profile
average-rate-limit 0
access-control-trust-level none
```

```
invalid-signal-threshold 0
maximum-signal-threshold 0
untrusted-signal-threshold 0
nat-trust-threshold 0
deny-period 30
ext-policy-svr
symmetric-latching disabled
pai-strip disabled
trunk-context
early-media-allow
enforcement-profile
additional-prefixes
restricted-latching none
restriction-mask 32
accounting-enable enabled
user-cac-mode none
user-cac-bandwidth 0
user-cac-sessions 0
icmp-detect-multiplier 0
icmp-advertisement-interval 0
icmp-target-ip
monthly-minutes 0
net-management-control disabled
delay-media-update disabled
refer-call-transfer disabled
dyn-refer-term disabled
codec-policy
codec-manip-in-realm disabled
constraint-name
call-recording-server-id
xnq-state xnq-unknown
hairpin-id 0
stun-enable disabled
stun-server-ip 0.0.0.0
stun-server-port 3478
stun-changed-ip 0.0.0.0
stun-changed-port 3479
```

```
match-media-profiles
qos-constraint
sip-profile
sip-isup-profile
block-rtcp disabled
hide-egress-media-update disabled
last-modified-by admin@10.232.1.138
last-modified-date 2010-07-02 19:03:13
```

NOTICE:

10.232.51.0/24 is the signaling network of the OpenScape Voice Server.

In order to disable Media Anchoring for phones behind a NAT router, both mm-in-realm and mm-same-ip must be set to disabled.

7.2.18.2 Steering Pools (RTP Streams) - Remote User Deployment Scenario

Configure the steering pools for the different realms.

Configure the steering pool for the access realm

```
steering-pool
ip-address 10.232.3.200
start-port 10000
end-port 20001
realm-id access
network-interface
last-modified-by admin@10.232.3.122
last-modified-date 2009-11-24 09:11:03
```

Configure the steering pool for the core realm

NOTICE:

When assigning the port range for the steering pool, ensure that it does NOT overlap with the port range of the core sip-interface if the core sip-interface IP address is the same as the steering pool address. In this example, the core sip-interface range is 6000 - 12100 and the steering pool range is 12200 to 20001.

```
steering-pool
ip-address 10.232.51.190
start-port 12200
```

```
end-port 20001
realm-id core
network-interface
last-modified-by admin@10.232.3.138
last-modified-date 2010-01-18 09:11:03
```

7.2.18.3 Global SIP Configuration - Remote User Deployment Scenario

Configure the global SIP configuration parameters.

> **NOTICE:**
>
> Settings in the sip-config context are applied globally to all sip messages in the Acme Packet Net-Net 3800 SBC.

In this example, the sip-config home-realm is the access realm.

```
sip-config
state enabled
operation-mode dialog
dialog-transparency enabled
home-realm-id access
egress-realm-id
nat-mode Public
registrar-domain *
registrar-host *
registrar-port 5060
register-service-route always
init-timer 500
max-timer 4000
trans-expire 32
invite-expire 600
inactive-dynamic-conn 32
enforcement-profile
pac-method
pac-interval  10
pac-strategy PropDist
pac-load-weight 1
pac-session-weight 1
pac-route-weight 1
pac-callid-lifetime 600
```

```
pac-user-lifetime 3600
red-sip-port 1988
red-max-trans 10000
red-sync-start-time 5000
red-sync-comp-time 1000
add-reason-header disabled
sip-message-len 4096
enum-sag-match disabled
extra-method-stats disabled
registration-cache-limit  0
register-use-to-for-lp enabled
options force-unregistration
ignore-other-reg-expires
max-udp-length=0
reg-cache-mode=none
reinvite-trying
set-inv-exp-at-100-resp
refer-src-routing disabled
add-ucid-header disabled
proxy-sub-events
pass-gruu-contact disabled
sag-lookup-on-redirect disabled
last-modified-by admin@10.232.1.138
last-modified-date 2010-02-14 23:18:34
```

Notes

- `force-unregistration` should be enabled in order to unregister subscribers that have lost connectivity to the SBC. The force-unregistration option is NOT supported if digest authentication is enabled in the OSV server as the SBC has no way of responding to a new on behalf of an unreachable/disconnected phone.
- `operation-mode` should be set to dialog.
- `home-realm-id` should be set to the access realm.
- `nat-mode` should be Public.
- The `extra-method-stats` option can be used to aid in debugging and to throttle session traffic at the SIP-method level but should not be enabled under heavy load.

- Ensure the following options are configured:
  - `force-unregistration`
  - `ignore-other-reg-expires`
  - `max-udp-length=0`
  - `reg-cache-mode=none` (reg-cache-mode should be set to none to prevent Acme-cookies from been inserted in messages on the core side)
  - `reinvite-trying` (reinvite-trying should be set in order to send a "100 Trying" for re-INVITEs)
  - `set-inv-exp-at-100-resp`
- Enter the options as follows:

```
SolAcme3820-2A(sip-config)# options +force-unregistration

SolAcme3820-2A(sip-config)# options +ignore-other-reg-expires

SolAcme3820-2A(sip-config)# options +max-udp-length=0

SolAcme3820-2A(sip-config)# options +reg-cache-mode=none

SolAcme3820-2A(sip-config)# options +reinvite-trying

SolAcme3820-2A(sip-config)# options +set-inv-exp-at-100-resp
```

7.2.18.4 SIP Interfaces - Remote User Deployment Scenario

Configure the SIP interfaces for UDP and TCP for the different realms.

Configure the SIP UDP interface for the access realm

```
sip-interface
state enabled
realm-id access
description
sip-port
address 10.232.3.200
port 5060
transport-protocol UDP
tls-profile
allow-anonymous registered
ims-aka-profile
carriers
trans-expire 0
invite-expire 0
max-redirect-contacts 0
proxy-mode Proxy
redirect-action Proxy
```

```
contact-mode none
nat-traversal always
nat-interval 30
tcp-nat-interval 90
registration-caching enabled
min-reg-expire 300
registration-interval 300
route-to-registrar enabled
secured-network enabled
teluri-scheme disabled
uri-fqdn-domain
options
preserve-user-info
reg-no-port-match
reg-via-key=all
reuse-connections
strip-route-headers
trust-mode all
max-nat-interval 3600
nat-int-increment 10
nat-test-increment 30
sip-dynamic-hnt enabled
stop-recurse 401,407
port-map-start  0
port-map-end 0
in-manipulationid
out-manipulationid modmaddr302
manipulation-string
manipulation-pattern
sip-ims-feature disabled
operator-identifier
anonymous-priority none
max-incoming-conns 0
per-src-ip-max-incoming-conns 0
inactive-conn-timeout 0
untrusted-conn-timeout 0
network-id
```

```
ext-policy-server
default-location-string
charging-vector-mode pass
charging-function-address-mode pass
ccf-address
ecf-address
term-tgrp-mode none
implicit-service-route disabled
rfc2833-payload 101
rfc2833-mode transparent
constraint-name
response-map
local-response-map
ims-aka-feature disabled
enforcement-profile
route-unauthorized-calls
tcp-keepalive none
add-sdp-invite disabled
add-sdp-profiles
sip-profile
sip-isup-profile
last-modified-by  admin@10.232.1.138
last-modified-date 2010-05-28 16:46:32
```

Notes:

- 10.232.3.200 is the access sip-interface which phones will register with (SIP Server and SIP registrar).
- `transport-method` - should be UDP.
- `allow-anonymous` should be set to registered.
- `proxy-mode` - should be Proxy in order to forward the messages to the intended party.
- `redirect-action` - should be Proxy in order to forward any 302 Moved Temporarily Messages to the core side.
- `nat-traversal` - should be set to always. Phones not behind a NAT will not use any NAT specific options.
- `nat-interval` - set this to 30 (seconds). Nat-interval defines the local registration refresh interval between the remote phones and the Acme Packet Net-Net 3800 or 4500 SBC. A low value is used to keep the port binding of the NAT.
- `tcp-nat-interval` - This option is the same as the nat-interval but applies to TCP subscribers behind a NAT.
- `registration-caching` - should always be enabled for remote users.

- `min-reg-expire` - This option should not affect traffic on the access sip-interface.
- `registration-interval` - Enter the expiration time in seconds that you want the Net-Net SBC to use in the REGISTER response message sent back to the UA. The UA then refreshes its registration by sending another REGISTER message before that time expires. The default is 3600. A registration interval of zero causes the Net-Net SBC to pass back the expiration time set by and returned in the registration response from the registrar. This setting applies to Non-HNT endpoints.
- `route-to-registrar` - should be enabled. routing to the registrar to sends all requests that match a cached registration to the destination defined for the registrar host.
- `secured-network` - set to enabled for large conference if re-invite for large conference contains a MIKEY and the signaling transport is TCP or UDP, otherwise the large conference will fail.
- `dynamic-sip-hnt` - enable this to introduce variations in local phone registration timer intervals.
- `out-manipulationid` *modmaddr302* - contains the following sip-manipulation rules:
  - correct the contact and maddr IP addresses in INVITE messages generated by 302 Temporarily Moved messages (due to Media Redirection). These INVITE messages contain the home-address as the contact and maddr IP instead of the access sip interface. This sip-manipulation rule is a workaround for Acme Packet ticket 26019.
  - Remove the private sticky port in the From and To headers of SIP messages which occur on the public interface.
- options - The following options are required for remote users:
  - *preserve-user-info*
  - *reg-no-port-match* (SBC will not check Layer 3 port in INVITE & REGISTER messages.
  - *reg-via-key=all* (needed for port-mapping)
  - *reuse-connections* (needed to prevent out-of-order packets for TCP connections)
  - *strip-route-headers*

Configure the SIP UDP interface for the core realm

```
sip-interface
state enabled
realm-id core
description
sip-port
address 10.232.51.190
port 5060
transport-protocol UDP
tls-profile
allow-anonymous all
ims-aka-profile
```

```
carriers
trans-expire 0
invite-expire 0
max-redirect-contacts 0
proxy-mode Proxy
redirect-action Proxy
contact-mode none
nat-traversal none
nat-interval 30
tcp-nat-interval 90
registration-caching disabled
min-reg-expire 300
registration-interval 300
route-to-registrar disabled
secured-network disabled
teluri-scheme disabled
uri-fqdn-domain
trust-mode all
max-nat-interval 3600
nat-int-increment 10
nat-test-increment 30
sip-dynamic-hnt disabled
stop-recurse 401,407
port-map-start  6000
port-map-end 12100
in-manipulationid
out-manipulationid removePort
manipulation-string
manipulation-pattern
sip-ims-feature disabled
operator-identifier
anonymous-priority none
max-incoming-conns 0
per-src-ip-max-incoming-conns 0
inactive-conn-timeout 0
untrusted-conn-timeout 0
network-id
```

```
ext-policy-server
default-location-string
charging-vector-mode pass
charging-function-address-mode pass
ccf-address
ecf-address
term-tgrp-mode none
implicit-service-route disabled
rfc2833-payload 101
rfc2833-mode transparent
constraint-name
response-map
local-response-map
ims-aka-feature disabled
enforcement-profile
route-unauthorized-calls
tcp-keepalive none
add-sdp-invite disabled
add-sdp-profiles
sip-profile
sip-isup-profile
last-modified-by  admin@10.232.1.138
last-modified-date 2010-03-10 14:30:32
```

Notes:

- 10.232.51.190 is the core sip-interface facing the OpenScape Voice Server.
- `transport-method` - should be UDP.
- `allow-anonymous` - should be set to all.
- `proxy-mode` - should be Proxy in order to forward the messages to the intended party.
- `redirect-action` - should be Proxy in order to forward any 302 Moved Temporarily Messages.
- `nat-traversal` - set to none since no phones register from the core side.
- `nat-interval` - should not affect traffic on the core sip-interface.
- `tcp-nat-interval` - should not affect traffic on the core sip-interface.
- `registration-caching` - should always be disabled on the core sip-interface since subscribers do not register from core side.
- `min-reg-expire` - Defines the minimum expiration value the Net-Net SBC places in each REGISTER message it sends to the real registrar. In HNT, the Net-Net SBC caches the registration after receiving a response from the real registrar and sets the expiration time to the NAT interval value. Default value is 300 seconds.

- `registration-interval` - should not affect traffic on the core sip-interface.
- `route-to-registrar` - set to disabled on the core sip-interface.
- `secured-network` - set to disabled unless there are issues with large conference (this was needed only for the access sip-interface).
- port-map-start and port-map-end - together, these define the contact port map range on the core side (sticky ports for contacts in OpenScape Voice Server).
- `out-manipulationid` *removePort* - Remove the private sticky port in the From and To headers of SIP messages which occur on the public interface

Configure the SIP TCP interface for the access realm

```
sip-interface
state enabled
realm-id access
description
sip-port
address 10.232.3.200
port 5060
transport-protocol TCP
tls-profile
allow-anonymous registered
ims-aka-profile
carriers
trans-expire 0
invite-expire 0
max-redirect-contacts 0
proxy-mode Proxy
redirect-action Proxy
contact-mode loose-route
nat-traversal always
nat-interval 30
tcp-nat-interval 90
registration-caching enabled
min-reg-expire 300
registration-interval 300
route-to-registrar enabled
secured-network enabled
teluri-scheme disabled
uri-fqdn-domain
```

`options`

preserve-user-info

reg-no-port-match

reg-via-key=all

reuse-connections

strip-route-headers

via-header-transparency

`trust-mode` *all*

`max-nat-interval` *3600*

`nat-int-increment` *10*

`nat-test-increment` *30*

`sip-dynamic-hnt` *enabled*

`stop-recurse` *401,407*

`port-map-start` *0*

`port-map-end` *0*

`in-manipulationid`

`out-manipulationid` *modmaddr302*

`manipulation-string`

`manipulation-pattern`

`sip-ims-feature` *disabled*

`operator-identifier`

`anonymous-priority` *none*

`max-incoming-conns` *0*

`per-src-ip-max-incoming-conns` *0*

`inactive-conn-timeout` *0*

`untrusted-conn-timeout` *0*

`network-id`

`ext-policy-server`

`default-location-string`

`charging-vector-mode` *pass*

`charging-function-address-mode` *pass*

`ccf-address`

`ecf-address`

`term-tgrp-mode` *none*

`implicit-service-route` *disabled*

`rfc2833-payload` *101*

`rfc2833-mode` *transparent*

```
constraint-name
response-map
local-response-map
ims-aka-feature disabled
enforcement-profile
route-unauthorized-calls
tcp-keepalive none
add-sdp-invite disabled
add-sdp-profiles
sip-profile
sip-isup-profile
last-modified-by  admin@10.232.1.138
last-modified-date 2010-06-04 14:28:32
```

Notes:

- 10.232.3.200 is the access sip-interface which phones will register with (SIP Server and SIP registrar).
- `transport-method` - should be TCP.
- `allow-anonymous` should be set to registered.
- `proxy-mode` - should be Proxy in order to forward the messages to the intended party.
- `redirect-action` - should be Proxy in order to forward any 302 Moved Temporarily Messages to the core side.
- `contact-mode` - should be set to loose-route to include the Record-Route header in a request.

> **NOTICE:**
>
> Note: This may not have an impact when the SBC is operating as a B2BUA.

- `nat-traversal` - should be set to always. Phones not behind a NAT will not use any NAT specific options.
- `nat-interval` - Sets the expiration time in seconds for the Net-Net SBC's cached registration entry for an HNT (Hosted NAT Traversal) endpoint (i.e., an endpoint behind a NAT router). The default is 30. This timer is used to cause the UA to send REGISTER messages frequently enough to retain the port binding in the NAT. Retaining the binding lets inbound requests to be sent through the NAT.
- `tcp-nat-interval` - This option is the same as the nat-interval but applies to TCP subscribers behind a NAT (should apply for THIS sip-interface).
- `registration-caching` - should always be enabled for remote users.
- `min-reg-expire` - This option should not affect traffic on the access sip-interface.
- `registration-interval` - Enter the expiration time in seconds that you want the Net-Net SBC to use in the REGISTER response message sent back to the UA. The UA then refreshes its registration by sending

another REGISTER message before that time expires. The default is 3600. A registration interval of zero causes the Net-Net SBC to pass back the expiration time set by and returned in the registration response from the registrar. This setting applies to Non-HNT endpoints.

- `route-to-registrar` - should be enabled. Routing to the registrar sends all requests that match a cached registration to the destination defined for the registrar host.
- `secured-network` - set to enabled for large conference if re-invite for large conference contains a MIKEY and the signaling transport is TCP or UDP, otherwise the large conference will fail.
- `dynamic-sip-hnt` - enable this to introduce variations in local phone registration timer intervals.
- `out-manipulationid` *modmaddr302* - contains the following sip-manipulation rules:
  - correct the contact and maddr IP addresses in INVITE messages generated by 302 Temporarily Moved messages (due to Media Redirection). These INVITE messages contain the home-address as the contact and maddr IP instead of the access sip interface. This sip-manipulation rule is a workaround for Acme Packet ticket 26019.
  - Remove the private sticky port in the From and To headers of SIP messages which occur on the public interface.
- options - The following options are required for remote users:
  - *preserve-user-info*
  - *reg-no-port-match* (SBC will not check Layer 3 port in INVITE & REGISTER messages.
  - *reg-via-key=all* (needed for port-mapping)
  - *reuse-connections* (needed to prevent out-of-order packets for TCP connections)
  - *strip-route-headers*
  - *via-header-transparency* (Enables the SBC to insert its Via header on top of the top-most Via header received from user equipment (UE).)

Configure the SIP TCP interface for the core realm

```
sip-interface
state enabled
realm-id core
description
sip-port
address 10.232.51.190
port 5060
transport-protocol TCP
tls-profile
allow-anonymous all
ims-aka-profile
carriers
trans-expire 0
```

```
invite-expire 0
max-redirect-contacts 0
proxy-mode Proxy
redirect-action Proxy
contact-mode loose-route
nat-traversal none
nat-interval 30
tcp-nat-interval 90
registration-caching disabled
min-reg-expire 300
registration-interval 300
route-to-registrar disabled
secured-network disabled
teluri-scheme disabled
uri-fqdn-domain
options tcp-port-mapping=nopath
trust-mode all
max-nat-interval 3600
nat-int-increment 10
nat-test-increment 30
sip-dynamic-hnt disabled
stop-recurse 401,407
port-map-start  6000
port-map-end 12100
in-manipulationid
out-manipulationid add_Record_Route
manipulation-string
manipulation-pattern
sip-ims-feature disabled
operator-identifier
anonymous-priority none
max-incoming-conns 0
per-src-ip-max-incoming-conns 0
inactive-conn-timeout 0
untrusted-conn-timeout 0
network-id
ext-policy-server
```

```
default-location-string
charging-vector-mode pass
charging-function-address-mode pass
ccf-address
ecf-address
term-tgrp-mode none
implicit-service-route disabled
rfc2833-payload 101
rfc2833-mode transparent
constraint-name
response-map
local-response-map
ims-aka-feature disabled
enforcement-profile
route-unauthorized-calls
tcp-keepalive none
add-sdp-invite disabled
add-sdp-profiles
sip-profile
sip-isup-profile
last-modified-by  admin@10.232.1.138
last-modified-date 2010-04-27 12:32:45
```

Notes:

- 10.232.51.190 is the core sip-interface facing the OpenScape Voice Server.
- `transport-method` - should be TCP.
- `allow-anonymous` should be set to all.
- `proxy-mode` - should be Proxy in order to forward the messages to the intended party.
- `redirect-action` - should be Proxy in order to forward any 302 Moved Temporarily Messages.
- `contact-mode` - should be set to loose-route to include the Record-Route header in a request.

> **NOTICE:**
>
> This may not have an impact when the SBC is operating as a B2BUA.

- `nat-traversal` - should be set to none since no phones register from the core side.
- `nat-interval` - should not affect traffic on the core sip-interface.
- `tcp-nat-interval` - should not affect traffic on the core sip-interface.
- `registration-caching` - should always be enabled for remote users.

- `min-reg-expire` - This option should not affect traffic on the access sip-interface.
- `registration-chaching` - should always be disabled on the core sip-interface since subscribers do not register from core side.
- `min-reg-expire` - Defines the minimum expiration value the Net-Net SBC places in each REGISTER message it sends to the real registrar. In HNT, the Net-Net SBC caches the registration after receiving a response from the real registrar and sets the expiration time to the NAT interval value. Default value is 300 seconds.
- `registration-interval` - This should not affect traffic on the core sip-interface.
- `route-to-registrar` - set to disabled on the core sip-interface.
- `secured-network` - Enable or disable sending messages on unsecured transport. Set to disabled unless there are issues with large conference (this was needed only for the access sip-interface).
- `port map start and port map end` - together, these define the contact port map range on the core side (sticky ports for subscriber contacts in OpenScape Voice Server).
- `out-manipulationid` *add_Record_Route* - Add the Record-Route header to core the tcp core sip-interface.
- option *tcp-port-mapping=nopath* - should be added. This is a requirement to enable port-mapping (sticky ports) for TCP sip-interfaces in addition to the port-map-start and port-map-end fields.

  Add the option as follows:

  ```
  solAcme3800A(sip-interface)# options +tcp-port-
  mapping=nopath
  ```

7.2.18.5 SIP NAT - Remote User Deployment Scenario

Configure the SIP NAT which is homed in the core (trusted) realm.

`sip-nat`

`realm-id` *core*

`domain-suffix` *.core.siemens.com*

`ext-proxy-address` *10.232.51.102*

`ext-proxy-port` *5060*

`ext-address` *10.232.51.190*

`home-address` *10.232.3.203*

`home-proxy-address`

`home-proxy-port` *5060*

`route-home-proxy` *disabled*

`address-prefix` *

`tunnel-redirect` *disabled*

`use-url-parameter` *all*

`parameter-name` *access*

`user-nat-tag` *-acme-*

```
host-nat-tag ACME-
headers
Call-ID Contact f From=ip-ip-tgt i Join
m P-Asserted-Identity r Record-Route
Refer-To Referred-by Replaces Reply-To
Route t To=ip-ip-tgt v Via
last-modified-by admin@10.232.1.138
last-modified-date 2010-07-16 19:14:41
```

Notes:

- `realm-id` - enter the core realm ID here.
- `domain-suffix` - enter a domain suffix (having core as part of the suffix allows core traffic to be easily identified in traces.
- `ext-proxy-address` - enter the SIP server address, in this case it is the OpenScape Voice sipsm IP address.
- `ext-proxy-port` - sip port of the ext-proxy-address.
- `ext-address` - SBC's core sip-interface IP address (facing OpenScape Voice Server).
- `home-address` - must be set to a unique IP address in the same network as the access sip-interface (i.e., it should not be configured anywhere else within the SBC or outside of the SBC)
- `home-proxy-port` - set to 5060.
- Acme Packet cookies by default are added to the user part of the contact URI which can break features such as large conference. A workaround provided by Acme Packet is to move the cookie from the user part into a parameter. This can be accomplished by setting the use-url-parameter option to "all" and setting the parameter-name field to the name of the access realm.
- The following are the default sip-nat headers that are added:

  Call-ID, Contact, Join, P-Asserted-Identify, Record-Route, Referred-by Refer-To, Replaces, Reply-To, Route, Via. From and To headers need to be replaced as follows in the sip-nat context:

  ```
  SolAcme3800A(sip-nat)# headers From=ip-ip-tgt
  SolAcme3800A(sip-nat)# headers To=ip-ip-tgt
  SolAcme3800A(sip-nat)# headers Referred-by
  SolAcme3800A(sip-nat)# headers P-Asserted-Identity
  SolAcme3800A(sip-nat)# done
  ```

7.2.18.6 SIP Manipulation Rules - Remote User Deployment Scenario

Configure different rules for SIP Manipulation

add_Record_Route

add_Record_Route - used as the out-manipulationid rule for core TCP sip-interface 10.232.51.190.

This rule adds the Record-Route header to INVITE, NOTIFY, REFER and SUBSCRIBE messages passed to the OpenScape Voice server with the SBC's core IP address and port 5060.

```
sip-manipulation
name add_Record_Route
description Add Record_Route header to core interface
split-headers
join-headers
header-rule
name addRR
header-name Record-Route
action add
comparison-type case-sensitive
msg-type any
methods INVITE,NOTIFY,REFER,SUBSCRIBE
match-value
new-value <sip:10.232.51.190:5060;transport=tcp>
last-modified-by admin@10.232.1.138
last-modified-date 2010-06-04 15:08:59
```

modmaddr302

modmaddr302 - used as the out-manipulationid rule for UDP and TCP access sip-interfaces. This rule performs the following manipulations.

- Change the maddr and contact header IP from home-address 10.232.3.203 to sip-interface 10.232.3.200.
- Remove private port from From and To headers

```
sip-manipulation
name modmaddr302
description Change maddr in contact header from home-address 10.232.3.203 to sip-interface 10.232.3.200. Remove private port from the From and To headers
split-headers
join-headers
header-rule
name modmaddr
header-name Contact
action manipulate
comparison-type case-sensitive
msg-type any
methods INVITE
```

```
match-value
new-value
element-rule
name modmaddr
parameter-name maddr
type uri-param
action find-replace-all
match-val-type any
comparison-type case-sensitive
match-value 10.232.3.203
new-value 10.232.3.200
element-rule
name modcontact
parameter-name
type uri-host
action find-replace-all
match-val-type any
comparison-type case-sensitive
match-value 10.232.3.203
new-value 10.232.3.200
header-rule
name removeFromPort
header-name From
action manipulate
comparison-type case-sensitive
msg-type request
methods
match-value
new-value
element-rule
name port
parameter-name
type uri-port
action delete-element
match-val-type any
comparison-type case-sensitive
match-value
```

```
new-value
header-rule
name removeToPort
header-name To
action manipulate
comparison-type case-sensitive
msg-type request
methods
match-value
new-value
element-rule
name port
parameter-name
type uri-port
action delete-element
match-val-type any
comparison-type case-sensitive
match-value
new-value
last-modified-by admin@10.232.1.138
last-modified-date 2010-06-04 14:30:54
```

removePort

removePort - used as the out-manipulationid rule for the core sip-interface. This rule removes private ports from the From and To headers.

```
sip-manipulation
name removePort
description
split-headers
join-headers
header-rule
name removeFromPort
header-name From
action manipulate
comparison-type case-sensitive
msg-type request
methods
match-value
```

```
new-value
element-rule
name port
parameter-name
type uri-port
action delete-element
match-val-type any
comparison-type case-sensitive
match-value
new-value
header-rule
name removeToPort
header-name To
action manipulate
comparison-type case-sensitive
msg-type request
methods
match-value
new-value
element-rule
name port
parameter-name
type uri-port
action delete-element
match-val-type any
comparison-type case-sensitive
match-value
new-value
last-modified-by admin@10.232.3.122
last-modified-date 2009-11-24 19:42:14
```

7.2.18.7 Session Agents - Remote User Deployment Scenario

Session Agents point to the SIP server (OpenScape Voice Server sipsm). Session Agents are the next HOP in routing rules (via a local-policy).

Configure the UDP Session Agent for OpenScape Voice Server

```
session-agent
hostname 10.232.51.102
```

```
ip-address 10.232.51.102
port 5060
state enabled
app-protocol SIP
app-type
transport-method UDP
realm-id core
egress-realm-id
description
carriers
allow-next-hop-lp enabled
constraints disabled
max-sessions 0
max-inbound-sessions 0
max-outbound-sessions 0
max-burst-rate 0
max-inbound-burst-rate 0
max-outbound-burst-rate 0
max-sustain-rate 0
max-inbound-sustain-rate 0
max-outbound-sustain-rate 0
min-seizures 5
min-asr 0
time-to-resume 0
ttr-no-response 0
in-service-period 0
burst-rate-window 0
sustain-rate-window 0
req-uri-carrier-mode None
proxy-mode
redirect-action
loose-routing enabled
send-media-session enabled
response-map
ping-interval 0
ping-interval 0
ping-send-mode keep-alive
```

```
ping-all-addresses disabled
ping-in-service-response-codes
out-service-response-codes
media-profiles
in-translationid
out-translationid
trust-me disabled
request-uri-headers
stop-recurse
local-response-map
ping-to-user-part
ping-from-user-part
li-trust-me disabled
in-manipulationid
out-manipulationid
manipulation-string
manipulation-pattern
p-asserted-id
trunk-group
max-register-sustain-rate 0
early-media-allow
invalidate-registrations disabled
rfc2833-mode none
rfc2833-payload 0
codec-policy
enforcement-profile
refer-call-transfer disabled
reuse-connections NONE
tcp-keepalive enabled
tcp-reconn-interval 10
max-register-burst-rate 0
register-burst-window 0
sip-profile
sip-isup-profile
last-modified-by admin@10.232.1.138
last-modified-date 2010-04-26 18:57:13
```

Notes:

- Openscape Voice Server sipsm = 10.232.51.102.
- `ping-in-service-response-codes` are set to "200,401,403" to keep the OpenScape Voice Server
- `transport-method` should be set to UPD (default) and port should be set to 5060 (default).
- `app-protocol` should be set to SIP (default).
- `realm-id` should be the name of the core realm.
- `ping-method` should not be set (It is NOT set by default). `ping-interval` should be 0 (default)

Configure the TCP Session Agent for OpenScape Voice Server

```
session-agent
hostname 10.232.51.102
ip-address 10.232.51.102
port 5060
state enabled
app-protocol SIP
app-type
transport-method StaticTCP
realm-id core
egress-realm-id
description
carriers
allow-next-hop-lp enabled
constraints disabled
max-sessions 0
max-inbound-sessions 0
max-outbound-sessions 0
max-burst-rate 0
max-inbound-burst-rate 0
max-outbound-burst-rate 0
max-sustain-rate 0
max-inbound-sustain-rate 0
max-outbound-sustain-rate 0
min-seizures 5
min-asr 0
time-to-resume 0
ttr-no-response 0
in-service-period 0
burst-rate-window 0
```

```
sustain-rate-window 0
req-uri-carrier-mode None
proxy-mode
redirect-action
loose-routing enabled
send-media-session enabled
response-map
ping-interval 0
ping-send-mode keep-alive
ping-all-addresses disabled
ping-in-service-response-codes
out-service-response-codes
media-profiles
in-translationid
out-translationid
trust-me disabled
request-uri-headers
stop-recurse
local-response-map
ping-to-user-part
ping-from-user-part
li-trust-me disabled
in-manipulationid
out-manipulationid
manipulation-string
manipulation-pattern
p-asserted-id
trunk-group
max-register-sustain-rate 0
early-media-allow
invalidate-registrations disabled
rfc2833-mode none
rfc2833-payload 0
codec-policy
enforcement-profile
refer-call-transfer disabled
reuse-connections NONE
```

```
tcp-keepalive enabled
tcp-reconn-interval 10
max-register-burst-rate 0
register-burst-window 0
sip-profile
sip-isup-profile
last-modified-by admin@10.232.1.138
last-modified-date 2010-06-26 14:57:23
```

Notes:

- Openscape Voice Server sipsm is 10.232.51.102.
- `transport-method` should be set to StaticTCP and `port` should be set to 5060 (default)..
- `app-protocol` should be set to SIP (default).
- `realm-id` should be the name of the core realm.
- `ping-method` should not be set (It is NOT set by default). `ping-interval` should be 0 (default).

7.2.18.8 Local Policies - Remote User Deployment Scenario

Configure the local policy to route traffic from access realm to OSV

```
local-policy
from-address *
to-address *
source-realm access
description
activate-time N/A
deactivate-time N/A
state enabled
policy-priority none
last-modified-by admin@10.232.3.122
last-modified-date 2009-11-24 18:34:40
policy-attribute
next-hop 10.232.51.102
realm core
action none
terminate-recursion disabled
carrier
start-time 0000
end-time 2400
```

`days-of-week` *U-S*

`cost` *0*

`app-protocol` *SIP*

`state` *enabled*

`methods`

`media-profiles`

`lookup` *single*

`next-key`

`eloc-str-lkup` *disabled*

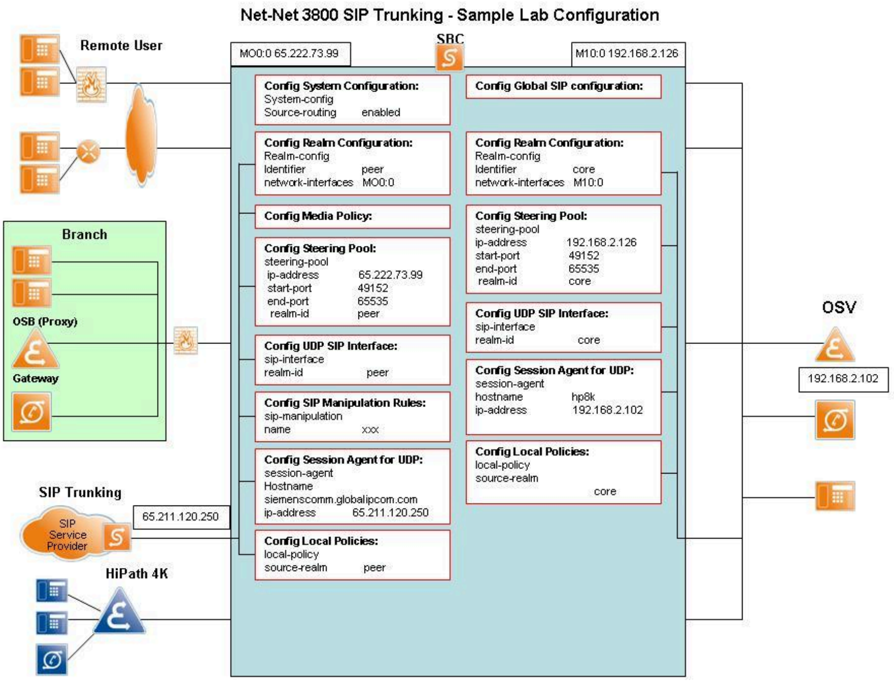
`eloc-str-match`

Notes:

- `source-realm` should be the realm of the remote phones.
- `policy-attribute next-hop` should be the hostname or IP address of OpenScape Voice Server sipsm (as defined in the OSV session agent).
- `policy-attribute realm` should be the core realm assigned to OpenScape Voice Server session agent.
- `app-protocol` should be SIP.

7.2.19 Net-Net 3000, Net-Net 4000 Series SBC - SIP Trunking Deployment Scenario - SIP Service Provider Trunking

This example, based on Verizon illustrates the Acme NN-3800 SBC configuration to support peering between a SIP provider and an OpenScape Voice Server.



```
Config System Configuration:
System-config
Source-routing      enabled

Config Realm Configuration:
Realm-config
Identifier          peer
network-interfaces  MO0:0

Config Media Policy:

Config Steering Pool:
steering-pool
 ip-address         65.222.73.99
 start-port         49152
 end-port           65535
  realm-id          peer

Config UDP SIP Interface:
sip-interface
realm-id              peer

Config SIP Manipulation Rules:
sip-manipulation
name                xxx

Config Session Agent for UDP:
session-agent
Hostname
siemenscomm.globalipcom.com
ip-address         65.211.120.250

Config Local Policies:
local-policy
source-realm        peer
```

```
Config Global SIP configuration:

Config Realm Configuration:
Realm-config
Identifier          core
network-interfaces  M10:0

Config Steering Pool:
steering-pool
ip-address          192.168.2.126
start-port          49152
end-port            65535
 realm-id           core

Config UDP SIP Interface:
sip-interface
realm-id              core

Config Session Agent for UDP:
session-agent
hostname            hp8k
ip-address          192.168.2.102

Config Local Policies:
local-policy
source-realm
                          core
```

7.2.19.1 Realms - SIP Trunking Deployment Scenario

Create the different realms and associate with the desired network interface.

Create a peer realm and associate with the desired network interface

```
realm-config
identifier peer
description
addr-prefix 0.0.0.0
network-interfaces M00:0
mm-in-realm disabled
mm-in-network disabled
mm-same-ip enabled
mm-in-system enabled
bw-cac-non-mm disabled
msm-release disabled
qos-enable disabled
generate-UDP-checksum disabled
max-bandwidth 0
fallback-bandwidth 0
max-priority-bandwidth 0
max-latency 0
max-jitter 0
max-packet-loss 0
observ-window-size 0
parent-realm
dns-realm
media policy add-DSCP
in-translationid
out-translationid
in-manipulationid
out-manipulationid NAT_IP
manipulation-string
manipulation-pattern
class-profile
average-rate-limit 0
access-control-trust-level none
invalid-signal-threshold 0
```

```
maximum-signal-threshold 0
untrusted-signal-threshold 0
nat-trust-threshold 0
deny-period 30
ext-policy-svr
symmetric-latching disabled
pai-strip disabled
trunk-context
early-media-allow
enforcement-profile
additional-prefixes
restricted-latching none
restriction-mask 32
accounting-enable enabled
user-cac-mode none
user-cac-bandwidth 0
user-cac-sessions 0
icmp-detect-multiplier 0
icmp-advertisement-interval 0
icmp-target-ip
monthly-minutes 0
net-management-control disabled
delay-media-update disabled
refer-call-transfer disabled
dyn-refer-term disabled
codec-policy
codec-manip-in-realm disabled
constraint-name
call-recording-server-id
stun-enable disabled
stun-server-ip 0.0.0.0
stun-server-port 3478
stun-changed-ip 0.0.0.0
stun-changed-port 3479
match-media-profiles
qos-constraint
sip-profile
```

```
sip-isup-profile
block-rtcp disabled
hide-egress-media-update disabled
last-modified-by admin@10.232.1.145
last-modified-date 2010-07-02 15:02:48
```

NOTICE:

out-manipulationid is assigned sip-manipulation NAT_IP to NAT the To and From headers (defined in the sip-manipulation section.

Create the Media Policy assigned to the peer realm

```
media-policy
name add-DSCP
tos-settings
media-type message
media-sub-type sip
tos-value 0x1a
media-attributes
tos-settings
media-type rtp
media-sub-type
tos-value 0x2e
media-attributes
last-modified-by admin@10.232.1.134
last-modified-date 2008-07-29 17:28:07
```

Create a core realm and associate it with the desired interface

```
realm-config
identifier core
description
addr-prefix 0.0.0.0
network-interfaces M10:0
mm-in-realm disabled
mm-in-network disabled
mm-same-ip enabled
mm-in-system enabled
bw-cac-non-mm disabled
msm-release disabled
```

```
qos-enable disabled
generate-UDP-checksum disabled
max-bandwidth 0
fallback-bandwidth 0
max-priority-bandwidth 0
max-latency 0
max-jitter 0
max-packet-loss 0
observ-window-size 0
parent-realm
dns-realm
media-policy
in-translationid
out-translationid
in-manipulationid
out-manipulationid NAT_IP
manipulation-string
manipulation-pattern
class-profile
average-rate-limit 0
access-control-trust-level none
invalid-signal-threshold 0
maximum-signal-threshold 0
untrusted-signal-threshold 0
nat-trust-threshold 0
deny-period 30
ext-policy-svr
symmetric-latching disabled
pai-strip disabled
trunk-context
early-media-allow
enforcement-profile
additional-prefixes
restricted-latching none
restriction-mask 32
accounting-enable enabled
user-cac-mode none
```

```
user-cac-bandwidth 0
user-cac-sessions 0
icmp-detect-multiplier 0
icmp-advertisement-interval 0
icmp-target-ip
monthly-minutes 0
net-management-control disabled
delay-media-update disabled
refer-call-transfer disabled
dyn-refer-term disabled
codec-policy
codec-manip-in-realm disabled
constraint-name
call-recording-server-id
stun-enable disabled
stun-server-ip 0.0.0.0
stun-server-port 3478
stun-changed-ip 0.0.0.0
stun-changed-port 3479
match-media-profiles
qos-constraint
sip-profile
sip-isup-profile
block-rtcp disabled
hide-egress-media-update disabled
last-modified-by admin@10.232.1.145
last-modified-date 20109-07-02 19:03:13
```

NOTICE:

out-manipulationid is assigned sip-manipulation NAT_IP to NAT the To and From headers (defined in the sip-manipulation section).

7.2.19.2 Steering Pools (RTP Streams) - SIP Trunking Deployment Scenario

Configure the steering pools for the different realms.

Configure the steering pool for the peer realm

```
steering-pool
```

```
ip-address 65.222.73.99
start-port 49152
end-port 65535
realm-id peer
network-interface
last-modified-by admin@10.232.1.134
last-modified-date 2009-07-29 14:11:03
```

Configure the steering pool for the core realm

```
steering-pool
ip-address 192.168.2.126
start-port 49152
end-port 65535
realm-id core
network-interface
last-modified-by admin@10.232.1.134
last-modified-date 2009-07-29 14:11:03
```

7.2.19.3 Global SIP Configuration - SIP Trunking Deployment Scenario

Configure the global SIP configuration parameters.

```
sip-config
state enabled
operation-mode dialog
dialog-transparency enabled
home-realm-id access
egress-realm-id
nat-mode Public
registrar-domain *
registrar-host *
registrar-port 5060
register-service-route always
init-timer 500
max-timer 4000
trans-expire 32
invite-expire 600
inactive-dynamic-conn 32
enforcement-profile
```

```
pac-method
pac-interval  10
pac-strategy PropDist
pac-load-weight 1
pac-session-weight 1
pac-route-weight 1
pac-callid-lifetime 600
pac-user-lifetime 3600
red-sip-port 1988
red-max-trans 10000
red-sync-start-time 5000
red-sync-comp-time 1000
add-reason-header disabled
sip-message-len 4096
enum-sag-match disabled
extra-method-stats disabled
registration-cache-limit  0
register-use-to-for-lp disabled
options force-unregistration
ignore-other-reg-expires
max-udp-length=0
reg-cache-mode=from
reinvite-trying
set-inv-exp-at-100-resp
refer-src-routing disabled
add-ucid-header disabled
proxy-sub-events
pass-gruu-contact disabled
sag-lookup-on-redirect disabled
last-modified-by admin@10.232.63.222
last-modified-date 2010-03-11 15:18:34
```

Notes

- `force-unregistration` should be enabled in order to unregister subscribers that have lost connectivity to the SBC. The force-unregistration option is NOT supported if digest authentication is enabled in the OSV server as the SBC has no way of responding to a new on behalf of an unreachable/disconnected phone. If registration chaching is NOT used in the sip-interface, this option has no relevance as there will be nothing to unregister.

- `invite-expire` - this timer causes the cancellation of a call if the timer expires prior to the call been answered. The default value is 180 seconds.
- `inactive-dynamic-conn` - this value sets the timer at which TCP or TLS connections with no activity will be torn down.
- The `extra-method-stats` option can be used to aid in debugging and to throttle session traffic at the SIP-method level but should not be enabled under heavy load.
- Ensure the following options are configured:
  - `force-unregistration`
  - `ignore-other-reg-expires`
  - `max-udp-length=0`
  - `reg-cache-mode=from` (Not tested on Acmepacket Net-Net 6.2.0 software. Usually it is set to none to prevent Acme cookies from been inserted in messages on the core side)
  - `reinvite-trying` (reinvite-trying should be set in order to send a "100 Trying" for re-INVITEs)
  - `set-inv-exp-at-100-resp`
- Enter the options as follows:

```
SolAcme3820-2A(sip-config)# options +force-unregistration

SolAcme3820-2A(sip-config)# options +ignore-other-reg-expires

SolAcme3820-2A(sip-config)# options +max-udp-length=0

SolAcme3820-2A(sip-config)# options +reg-cache-mode=from

SolAcme3820-2A(sip-config)# options +reinvite-trying

SolAcme3820-2A(sip-config)# options +set-inv-exp-at-100-resp
```

7.2.19.4 SIP Interfaces - SIP Trunking Deployment Scenario

Configure the SIP interfaces for the different realms.

Configure the SIP interface for the peer realm

`sip-interface`

`state` *enabled*

`realm-id` *peer*

`description`

`sip-port`

`address` *65.222.73.99*

`port` *5060*

`transport-protocol` *UDP*

`tls-profile`

`allow-anonymous` *registered*

`ims-aka-profile`

```
carriers
trans-expire 0
invite-expire 0
max-redirect-contacts 0
proxy-mode
redirect-action
contact-mode none
nat-traversal always
nat-interval 45
tcp-nat-interval 90
registration-caching enabled
min-reg-expire 300
registration-interval 3600
route-to-registrar enabled
secured-network disabled
teluri-scheme disabled
uri-fqdn-domain
trust-mode all
max-nat-interval 3600
nat-int-increment 10
nat-test-increment 30
sip-dynamic-hnt enabled
stop-recurse 401,407
port-map-start  0
port-map-end 0
in-manipulationid
out-manipulationid
manipulation-string
manipulation-pattern
sip-ims-feature disabled
operator-identifier
anonymous-priority none
max-incoming-conns 0
per-src-ip-max-incoming-conns 0
inactive-conn-timeout 0
untrusted-conn-timeout 0
network-id
```

```
ext-policy-server
default-location-string
charging-vector-mode pass
charging-function-address-mode pass
ccf-address
ecf-address
term-tgrp-mode none
implicit-service-route disabled
rfc2833-payload 101
rfc2833-mode transparent
constraint-name
response-map
local-response-map
ims-aka-feature disabled
enforcement-profile
route-unauthorized-calls
tcp-keepalive none
add-sdp-invite disabled
add-sdp-profiles
sip-profile
sip-isup-profile
last-modified-by  admin@10.232.1.111
last-modified-date 2010-07-07 10:46:26
```

Notes:

- `route-to-registrar and registration caching` - although these options are enabled, they should NOT be needed as no registration occurs on the peer interface

Configure the SIP interface for the core realm

```
sip-interface
state enabled
realm-id core
description
sip-port
address 192.168.2.126
port 5060
transport-protocol UDP
tls-profile
```

`allow-anonymous` *all*

`ims-aka-profile`

`carriers`

`trans-expire` *0*

`invite-expire` *0*

`max-redirect-contacts` *0*

`proxy-mode`

`redirect-action`

`contact-mode` *none*

`nat-traversal` *none*

`nat-interval` *30*

`tcp-nat-interval` *90*

`registration-caching` *disabled*

`min-reg-expire` *300*

`registration-interval` *3600*

`route-to-registrar` *disabled*

`secured-network` *disabled*

`teluri-scheme` *disabled*

`uri-fqdn-domain`

`trust-mode` *all*

`max-nat-interval` *3600*

`nat-int-increment` *10*

`nat-test-increment` *30*

`sip-dynamic-hnt` *disabled*

`stop-recurse` *401,407*

`port-map-start` *0*

`port-map-end` *0*

`in-manipulationid`

`out-manipulationid`

`manipulation-string`

`manipulation-pattern`

`sip-ims-feature` *disabled*

`operator-identifier`

`anonymous-priority` *none*

`max-incoming-conns` *0*

`per-src-ip-max-incoming-conns` *0*

`inactive-conn-timeout` *0*

```
untrusted-conn-timeout 0
network-id
ext-policy-server
default-location-string
charging-vector-mode pass
charging-function-address-mode pass
ccf-address
ecf-address
term-tgrp-mode none
implicit-service-route disabled
rfc2833-payload 101
rfc2833-mode transparent
constraint-name
response-map
local-response-map
ims-aka-feature disabled
enforcement-profile
route-unauthorized-calls
tcp-keepalive none
add-sdp-invite disabled
add-sdp-profiles
sip-profile
sip-isup-profile
last-modified-by  admin@10.232.1.134
last-modified-date 2010-07-29 14:15:32
```

7.2.19.5 SIP NAT - SIP Trunking Deployment Scenario

SIP NAT is not used for peer to peer connections

7.2.19.6 SIP Manipulation Rules - SIP Trunking Deployment Scenario

Configure different rules for SIP Manipulation

```
sip-manipulation
name NAT_IP
description
split-headers
```

```
join-headers
header-rule
name manipFrom
header-name From
action manipulate
comparison-type case-sensitive
msg-type request
methods
match-value
new-value
element-rule
name From
parameter-name
type uri-host
action replace
match-val-type ip
comparison-type case-sensitive
match-value
new-value $REMOTE_IP

header-rule
name manipContact
header-name Contact
action manipulate
comparison-type case-sensitive
msg-type request
methods
match-value
new-value
element-rule
name Contact
parameter-name
type uri-host
action replace
match-val-type ip
comparison-type case-sensitive
match-value
new-value $LOCAL_IP
```

```
header-rule
name manipTo
header-name To
action manipulate
comparison-type case-sensitive
msg-type request
methods
match-value
new-value
element-rule
name To
parameter-name
type uri-host
action replace
match-val-type ip
comparison-type case-sensitive
match-value
new-value $REMOTE_IP

header-rule
name manipDiversion
header-name Diversion
action manipulate
comparison-type case-sensitive
msg-type request
methods
match-value
new-value
element-rule
name Diversion
parameter-name
type uri-host
action replace
match-val-type ip
comparison-type case-sensitive
match-value
new-value $LOCAL_IP

header-rule
```

```
name manipPAI
header-name P-Asserted-Identity
action manipulate
comparison-type case-sensitive
msg-type request
methods
match-value
new-value
element-rule
name Pai
parameter-name
type uri-host
action replace
match-val-type ip
comparison-type case-sensitive
match-value
new-value $LOCAL_IP

header-rule
name manipReferredBy
header-name Referred-By
action manipulate
comparison-type case-sensitive
msg-type request
methods
match-value
new-value
element-rule
name ReferredBy
parameter-name
type uri-host
action replace
match-val-type ip
comparison-type case-sensitive
match-value
new-value $LOCAL_IP
last-modified-by admin@10.232.1.138
last-modified-date 2010-02-23 16:19:47
```

7.2.19.7 Session Agents - SIP Trunking Deployment Scenario

Configure the different Session Agents.

Configure the peer Session Agent

```
session-agent
hostname siemenscomm.globalipcom.com
ip-address 65.211.120.250
port 5060
state enabled
app-protocol SIP
app-type
transport-method UDP
realm-id peer
egress-realm-id
description
carriers
allow-next-hop-lp enabled
constraints disabled
max-sessions 0
max-inbound-sessions 0
max-outbound-sessions 0
max-burst-rate 0
max-inbound-burst-rate 0
max-outbound-burst-rate 0
max-sustain-rate 0
max-inbound-sustain-rate 0
max-outbound-sustain-rate 0
min-seizures 5
min-asr 0
time-to-resume 0
ttr-no-response 0
in-service-period 0
burst-rate-window 0
sustain-rate-window 0
req-uri-carrier-mode None
proxy-mode
redirect-action
```

`loose-routing` *enabled*

`send-media-session` *enabled*

`response-map`

`ping method` *`OPTIONS`*

`ping-interval` *16*

`ping-send-mode` *keep-alive*

`ping-all-addresses` *disabled*

`ping-in-service-response-codes`

`out-service-response-codes`

`media-profiles`

`in-translationid`

`out-translationid`

`trust-me` *disabled*

`request-uri-headers`

`stop-recurse`

`local-response-map`

`ping-to-user-part`

`ping-from-user-part`

`li-trust-me` *disabled*

`in-manipulationid`

`out-manipulationid`

`manipulation-string`

`manipulation-pattern`

`p-asserted-id`

`trunk-group`

`max-register-sustain-rate` *0*

`early-media-allow`

`invalidate-registrations` *disabled*

`rfc2833-mode` *none*

`rfc2833-payload` *0*

`codec-policy`

`enforcement-profile`

`refer-call-transfer` *disabled*

`reuse-connections` *NONE*

`tcp-keepalive` *none*

`tcp-reconn-interval` *0*

`max-register-burst-rate` *0*

```
register-burst-window 0
sip-profile
sip-isup-profile
last-modified-by admin@10.232.1.147
last-modified-date 2010-08-25 20:03:13
```

Configure the core Session Agent

```
session-agent
hostname hp8k
ip-address 192.168.2.102
port 5060
state enabled
app-protocol SIP
app-type
transport-method UDP
realm-id core
egress-realm-id
description
carriers
allow-next-hop-lp enabled
constraints disabled
max-sessions 0
max-inbound-sessions 0
max-outbound-sessions 0
max-burst-rate 0
max-inbound-burst-rate 0
max-outbound-burst-rate 0
max-sustain-rate 0
max-inbound-sustain-rate 0
max-outbound-sustain-rate 0
min-seizures 5
min-asr 0
time-to-resume 0
ttr-no-response 0
in-service-period 0
burst-rate-window 0
sustain-rate-window 0
req-uri-carrier-mode None
```

```
proxy-mode
redirect-action
loose-routing enabled
send-media-session enabled
response-map
ping method OPTIONS
ping-interval 16
ping-send-mode keep-alive
ping-all-addresses disabled
ping-in-service-response-codes 200
out-service-response-codes
media-profiles
in-translationid
out-translationid
trust-me disabled
request-uri-headers
stop-recurse
local-response-map
ping-to-user-part
ping-from-user-part
li-trust-me disabled
in-manipulationid
out-manipulationid
manipulation-string
manipulation-pattern
p-asserted-id
trunk-group
max-register-sustain-rate 0
early-media-allow
invalidate-registrations disabled
rfc2833-mode none
rfc2833-payload 0
codec-policy
enforcement-profile
refer-call-transfer disabled
reuse-connections NONE
tcp-keepalive none
```

```
tcp-reconn-interval 0
max-register-burst-rate 0
register-burst-window 0
sip-profile
sip-isup-profile
last-modified-by admin@10.232.1.147
last-modified-date 2010-08-25 20:03:23
```

7.2.19.8 Local Policies - SIP Trunking Deployment Scenario

Configure the local policies for the different routes

Configure local policy to route traffic from core realm (OSV) to peer realm

```
local-policy
from-address *
to-address *
source-realm core
description
activate-time N/A
deactivate-time N/A
state enabled
policy-priority none
last-modified-by admin@10.232.1.134
last-modified-date 2009-07-29 17:34:40
policy-attribute
next-hop siemenscomm.globalipcom.com [63.110.102.247]
realm peer
action none
terminate-recursion disabled
carrier
start-time 0000
end-time 2400
days-of-week U-S
cost 0
app-protocol SIP
state enabled
methods
media-profiles
```

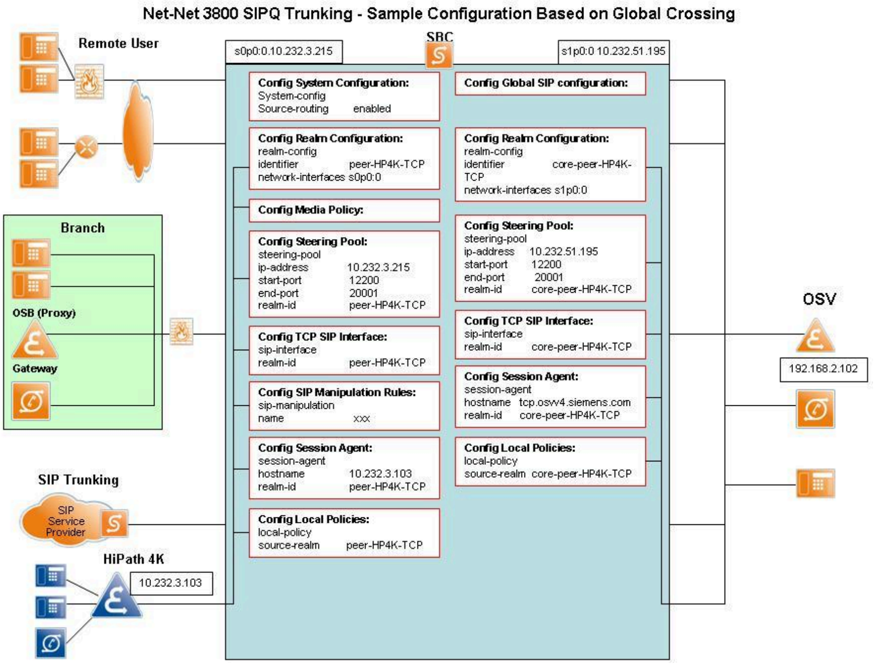
```
lookup single
next-key
eloc-str-lkup disabled
eloc-str-match
```

Configure local policy to route traffic from the peer realm to OSV

```
local-policy
from-address *
to-address *
source-realm peer
description
activate-time N/A
deactivate-time N/A
state enabled
policy-priority none
last-modified-by admin@10.232.1.134
last-modified-date 2009-07-29 14:34:20
policy-attribute
next-hop hp8k
realm core
action none
terminate-recursion disabled
carrier
start-time 0000
end-time 2400
days-of-week U-S
cost 0
app-protocol SIP
state enabled
methods
media-profiles
lookup single
next-key
eloc-str-lkup disabled
eloc-str-match
```

7.2.20 Net-Net 3000, Net-Net 4000 Series SBC - SIPQ Trunking Deployment Scenario

This section provides an example of configuring a HiPath 4000 (dynamic registration) as a peer of an OpenScape Voice Server.



Net-Net 3800 SIPQ Trunking - Sample Configuration Based on Global Crossing

```
Config System Configuration:
System-config
Source-routing       enabled

Config Realm Configuration:
realm-config
identifier             peer-HP4K-TCP
network-interfaces s0p0:0

Config Media Policy:

Config Steering Pool:
steering-pool
ip-address             10.232.3.215
start-port             12200
end-port               20001
realm-id               peer-HP4K-TCP

Config TCP SIP Interface:
sip-interface
realm-id               peer-HP4K-TCP

Config SIP Manipulation Rules:
sip-manipulation
name                   xxx

Config Session Agent:
session-agent
hostname               10.232.3.103
realm-id               peer-HP4K-TCP

Config Local Policies:
local-policy
source-realm       peer-HP4K-TCP

Config Global SIP configuration:

Config Realm Configuration:
realm-config
identifier             core-peer-HP4K-
TCP
network-interfaces s1p0:0

Config Steering Pool:
steering-pool
ip-address    10.232.51.195
start-port     12200
end-port        20001
realm-id       core-peer-HP4K-TCP

Config TCP SIP Interface:
sip-interface
realm-id       core-peer-HP4K-TCP

Config Session Agent:
session-agent
hostname   tcp.osvv4.siemens.com
realm-id     core-peer-HP4K-TCP

Config Local Policies:
local-policy
source-realm  core-peer-HP4K-TCP
```

7.2.20.1 Realms - SIPQ Trunking Deployment Scenario

Create the different realms and associate with the desired network interface.

Create a peer realm and associate with the desired network interface

```
realm-config
identifier peer-HP4K-TCP
description
addr-prefix 0.0.0.0
network-interfaces s0p0:0
mm-in-realm disabled
mm-in-network disabled
mm-same-ip disabled
mm-in-system enabled
bw-cac-non-mm disabled
msm-release disabled
qos-enable disabled
generate-UDP-checksum disabled
```

```
max-bandwidth 0
fallback-bandwidth 0
max-priority-bandwidth 0
max-latency 0
max-jitter 0
max-packet-loss 0
observ-window-size 0
parent-realm
dns-realm
media policy
media sec policy
in-translationid
out-translationid
in-manipulationid
out-manipulationid NAT_IP
manipulation-string
manipulation-pattern
class-profile
average-rate-limit 0
access-control-trust-level none
invalid-signal-threshold 0
maximum-signal-threshold 0
untrusted-signal-threshold 0
nat-trust-threshold 0
deny-period 30
ext-policy-svr
symmetric-latching disabled
pai-strip disabled
trunk-context
early-media-allow
enforcement-profile
additional-prefixes
restricted-latching none
restriction-mask 32
accounting-enable enabled
user-cac-mode none
user-cac-bandwidth 0
```

```
user-cac-sessions 0
icmp-detect-multiplier 0
icmp-advertisement-interval 0
icmp-target-ip
monthly-minutes 0
net-management-control disabled
delay-media-update disabled
refer-call-transfer disabled
dyn-refer-term disabled
codec-policy
codec-manip-in-realm disabled
constraint-name
call-recording-server-id
xnq-state xnq-unknown
hairpin-id 0
stun-enable disabled
stun-server-ip 0.0.0.0
stun-server-port 3478
stun-changed-ip 0.0.0.0
stun-changed-port 3479
match-media-profiles
qos-constraint
sip-profile
sip-isup-profile
block-rtcp disabled
hide-egress-media-update disabled
last-modified-by admin@10.232.1.138
last-modified-date 2010-07-02 18:41:48
```

NOTICE:

out-manipulationid is assigned sip-manipulation NAT_IP to NAT the To and From headers (defined in the sip-manipulation section.

Create the core realm and associate it with the desired interface

```
realm-config
identifier core-peer-HP4K-TCP
description
addr-prefix 0.0.0.0
```

```
network-interfaces s1p0:0
mm-in-realm disabled
mm-in-network disabled
mm-same-ip disabled
mm-in-system enabled
bw-cac-non-mm disabled
msm-release disabled
qos-enable disabled
generate-UDP-checksum disabled
max-bandwidth 0
fallback-bandwidth 0
max-priority-bandwidth 0
max-latency 0
max-jitter 0
max-packet-loss 0
observ-window-size 0
parent-realm
dns-realm
media-policy
media-sec-policy
in-translationid
out-translationid
in-manipulationid
out-manipulationid NAT_IP
manipulation-string
manipulation-pattern
class-profile
average-rate-limit 0
access-control-trust-level none
invalid-signal-threshold 0
maximum-signal-threshold 0
untrusted-signal-threshold 0
nat-trust-threshold 0
deny-period 30
ext-policy-svr
symmetric-latching disabled
pai-strip disabled
```

```
trunk-context
early-media-allow
enforcement-profile
additional-prefixes
restricted-latching none
restriction-mask 32
accounting-enable enabled
user-cac-mode none
user-cac-bandwidth 0
user-cac-sessions 0
icmp-detect-multiplier 0
icmp-advertisement-interval 0
icmp-target-ip
monthly-minutes 0
net-management-control disabled
delay-media-update disabled
refer-call-transfer disabled
dyn-refer-term disabled
codec-policy
codec-manip-in-realm disabled
constraint-name
call-recording-server-id
xnq-state  xnq-unknown
hairpin-id  0
stun-enable disabled
stun-server-ip 0.0.0.0
stun-server-port 3478
stun-changed-ip 0.0.0.0
stun-changed-port 3479
match-media-profiles
qos-constraint
sip-profile
sip-isup-profile
block-rtcp disabled
hide-egress-media-update disabled
last-modified-by admin@10.232.1.138
last-modified-date 20109-07-02 18:41:13
```

NOTICE:

out-manipulationid is assigned sip-manipulation NAT_IP to NAT the To and From headers (defined in the sip-manipulation section).

7.2.20.2 Steering Pools (RTP Streams) - SIPQ Trunking Deployment Scenario

Configure the steering pools for the different realms.

Configure the steering pool for the peer realm

```
steering-pool
ip-address 10.232.3.215
start-port 12200
end-port 20001
realm-id peer-HP4K-TCP
network-interface
last-modified-by admin@10.232.1.138
last-modified-date 2010-02-14 23:22:03
```

Configure the steering pool for the core realm

```
steering-pool
ip-address 10.232.51.195
start-port 12200
end-port 20001
realm-id core-peer-HP4K-TCP
network-interface
last-modified-by admin@10.232.1.138
last-modified-date 2010-02-14 23:11:48
```

7.2.20.3 Global SIP Configuration - SIPQ Trunking Deployment Scenario

Configure the global SIP configuration parameters.

```
sip-config
state enabled
operation-mode dialog
dialog-transparency enabled
home-realm-id access
egress-realm-id
nat-mode Public
```

`registrar-domain` *

`registrar-host` *

`registrar-port` *5060*

`register-service-route` *always*

`init-timer` *500*

`max-timer` *4000*

`trans-expire` *32*

`invite-expire` *600*

`inactive-dynamic-conn` *32*

`enforcement-profile`

`pac-method`

`pac-interval` *10*

`pac-strategy` *PropDist*

`pac-load-weight` *1*

`pac-session-weight` *1*

`pac-route-weight` *1*

`pac-callid-lifetime` *600*

`pac-user-lifetime` *3600*

`red-sip-port` *1988*

`red-max-trans` *10000*

`red-sync-start-time` *5000*

`red-sync-comp-time` *1000*

`add-reason-header` *disabled*

`sip-message-len` *4096*

`enum-sag-match` *disabled*

`extra-method-stats` *enabled*

`registration-cache-limit` *0*

`register-use-to-for-lp` *enabled*

`options` *force-unregistration*

ignore-other-reg-expires

max-udp-length=0

reg-cache-mode=none

reinvite-trying

set-inv-exp-at-100-resp

`refer-src-routing` *disabled*

`add-ucid-header` *disabled*

`proxy-sub-events`

`pass-gruu-contact` *disabled*

`sag-lookup-on-redirect` *disabled*

`last-modified-by` *admin@10.232.1.138*

`last-modified-date` *2010-02-14 23:18:34*

Notes

- `force-unregistration` should be enabled in order to unregister subscribers that have lost connectivity to the SBC. The force-unregistration option is NOT supported if digest authentication is enabled in the OSV server as the SBC has no way of responding to a new on behalf of an unreachable/disconnected phone.
- `invite-expire` - this timer causes the cancellation of a call if the timer expires prior to the call been answered. The default value is 180 seconds.
- `inactive-dynamic-conn` - this value sets the timer at which TCP or TLS connections with no activity will be torn down.
- The `extra-method-stats` option can be used to aid in debugging and to throttle session traffic at the SIP-method level but should not be enabled under heavy load.
- Ensure the following options are configured:
  - `force-unregistration`
  - `ignore-other-reg-expires`
  - `max-udp-length=0`
  - `reg-cache-mode=none` (reg-cache-mode should be set to none to prevent Acme-cookies from been inserted in messages on the core side)
  - `reinvite-trying` (reinvite-trying should be set in order to send a "100 Trying" for re-INVITEs)
  - `set-inv-exp-at-100-resp`
- Enter the options as follows:

```
SolAcme3820-2A(sip-config)# options +force-unregistration

SolAcme3820-2A(sip-config)# options +ignore-other-reg-expires

SolAcme3820-2A(sip-config)# options +max-udp-length=0

SolAcme3820-2A(sip-config)# options +reg-cache-mode=none

SolAcme3820-2A(sip-config)# options +reinvite-trying

SolAcme3820-2A(sip-config)# options +set-inv-exp-at-100-resp
```

7.2.20.4 SIP Interfaces - SIPQ Trunking Deployment Scenario

Configure the SIP interfaces for the different realms.

Configure the SIP interface for the peer realm

`sip-interface`

`state` *enabled*

`realm-id` *peer-HP4K-TCP*

```
description
sip-port
address 10.232.3.215
port 5060
transport-protocol TCP
tls-profile
allow-anonymous all
ims-aka-profile
carriers
trans-expire 0
invite-expire 0
max-redirect-contacts 0
proxy-mode
redirect-action
contact-mode none
nat-traversal none
nat-interval 30
tcp-nat-interval 90
registration-caching enabled
min-reg-expire 300
registration-interval 30
route-to-registrar enabled
secured-network enabled
teluri-scheme disabled
uri-fqdn-domain
options reuse-connections
trust-mode all
max-nat-interval 3600
nat-int-increment 10
nat-test-increment 30
sip-dynamic-hnt disabled
stop-recurse 401,407
port-map-start  0
port-map-end 0
in-manipulationid
out-manipulationid
manipulation-string
```

```
manipulation-pattern
sip-ims-feature disabled
operator-identifier
anonymous-priority none
max-incoming-conns 0
per-src-ip-max-incoming-conns 0
inactive-conn-timeout 0
untrusted-conn-timeout 0
network-id
ext-policy-server
default-location-string
charging-vector-mode pass
charging-function-address-mode pass
ccf-address
ecf-address
term-tgrp-mode none
implicit-service-route disabled
rfc2833-payload 101
rfc2833-mode transparent
constraint-name
response-map
local-response-map
ims-aka-feature disabled
enforcement-profile
route-unauthorized-calls
tcp-keepalive none
add-sdp-invite disabled
add-sdp-profiles
sip-profile
sip-isup-profile
last-modified-by  admin@10.232.1.138
last-modified-date 2010-05-19 14:46:26
```

Notes:

- `registration-interval` - This option was set to 30 seconds in order to detect a registration failure or outage of the HP4K.
- `route-to-registrar` - This option was set to enabled since the HP4K is registering dynamically with the OpenScape Voice Server. The SBC keeps track of the HP4K's registration in the registration cache.

- `secured-network` - set to enabled for large conference if re-invite for large conference contains a MIKEY and the signaling transport is TCP or UDP, otherwise the large conference will fail.
- `options reuse-connections` - this option is required to prevent out of order messages, especially for SIPQ. This is part of the workaround for Acme Packet ticket 19221.

Configure the SIP interface for the core realm

```
sip-interface
state enabled
realm-id core-peer-HP4K-TCP
description
sip-port
address 10.232.51.195
port 5060
transport-protocol TCP
tls-profile
allow-anonymous all
ims-aka-profile
carriers
trans-expire 0
invite-expire 0
max-redirect-contacts 0
proxy-mode
redirect-action
contact-mode none
nat-traversal none
nat-interval 30
tcp-nat-interval 90
registration-caching disabled
min-reg-expire 300
registration-interval 300
route-to-registrar disabled
secured-network disabled
teluri-scheme disabled
uri-fqdn-domain
options reuse-connections
trust-mode all
max-nat-interval 3600
```

`nat-int-increment` *10*

`nat-test-increment` *30*

`sip-dynamic-hnt` *disabled*

`stop-recurse` *401,407*

`port-map-start` *0*

`port-map-end` *0*

`in-manipulationid`

`out-manipulationid`

`manipulation-string`

`manipulation-pattern`

`sip-ims-feature` *disabled*

`operator-identifier`

`anonymous-priority` *none*

`max-incoming-conns` *0*

`per-src-ip-max-incoming-conns` *0*

`inactive-conn-timeout` *0*

`untrusted-conn-timeout` *0*

`network-id`

`ext-policy-server`

`default-location-string`

`charging-vector-mode` *pass*

`charging-function-address-mode` *pass*

`ccf-address`

`ecf-address`

`term-tgrp-mode` *none*

`implicit-service-route` *disabled*

`rfc2833-payload` *101*

`rfc2833-mode` *transparent*

`constraint-name`

`response-map`

`local-response-map`

`ims-aka-feature` *disabled*

`enforcement-profile`

`route-unauthorized-calls`

`tcp-keepalive` *none*

`add-sdp-invite` *disabled*

`add-sdp-profiles`

```
sip-profile
sip-isup-profile
last-modified-by  admin@10.232.1.138
last-modified-date 2010-05-18 17:45:32
```

Notes:

- `registration-caching` - should always be disabled on the core sip-interface since registration does not occur on the core side
- `min-reg-expire` - Defines the minimum expiration value the Net-Net SBC places in each REGISTER message it sends to the real registrar. In HNT, the Net-Net SBC caches the registration after receiving a response from the real registrar and sets the expiration time to the NAT interval value. Default value is 300 seconds.
- `route-to-registrar` - Set this to disabled since registration is occurring on the peer side.
- `options reuse-connections` - this option is required to prevent out of order messages, especially for SIPQ. This is part of the workaround for Acmepacket ticket 19221.

7.2.20.5 SIP NAT - SIPQ Trunking Deployment Scenario

SIP NAT is not used with SIP/SIPQ trunking.

7.2.20.6 SIP Manipulation Rules - SIPQ Trunking Deployment Scenario

Configure different rules for SIP Manipulation for the dynamic registration of HP4K.

```
sip-manipulation
name NAT_IP
description change_IP_to_remote_IP_in_from_and_to_header
split-headers
join-headers

header-rule
name manipFrom
header-name From
action manipulate
comparison-type case-sensitive
msg-type request
methods
match-value
new-value
element-rule
```

```
name From
parameter-name
type uri-host
action replace
match-val-type ip
comparison-type case-sensitive
match-value
new-value $REMOTE_IP

header-rule
name manipTo
header-name To
action manipulate
comparison-type case-sensitive
msg-type request
methods
match-value
new-value
element-rule
name To
parameter-name
type uri-host
action replace
match-val-type ip
comparison-type case-sensitive
match-value
new-value $REMOTE_IP
last-modified-by admin@10.232.1.138
last-modified-date 2010-02-14 23:27:43
```

Additional SIP NAT manipulations that may be needed:

```
sip-manipulation
name NAT_IP
description
split-headers
join-headers
header-rule
name manipDiversion
```

```
header-name Diversion
action manipulate
comparison-type case-sensitive
msg-type request
methods
match-value
new-value
element-rule
name Diversion
parameter-name
type uri-host
action replace
match-val-type ip
comparison-type case-sensitive
match-value
new-value $LOCAL_IP

header-rule
name manipPAI
header-name P-Asserted-Identity
action manipulate
comparison-type case-sensitive
msg-type request
methods
match-value
new-value
element-rule
name Pai
parameter-name
type uri-host
action replace
match-val-type ip
comparison-type case-sensitive
match-value
new-value $LOCAL_IP

header-rule
name manipReferredBy
header-name Referred-By
```

```
action manipulate
comparison-type case-sensitive
msg-type request
methods
match-value
new-value
element-rule
name ReferredBy
parameter-name
type uri-host
action replace
match-val-type ip
comparison-type case-sensitive
match-value
new-value $LOCAL_IP
last-modified-by admin@10.232.1.138
last-modified-date 2010-02-23 16:19:47
```

7.2.20.7 Session Agents - SIPQ Trunking Deployment Scenario

Configure the different Session Agents.

Configure the peer Session Agent

```
session-agent
hostname 10.232.3.103
ip-address
port 5060
state enabled
app-protocol SIP
app-type
transport-method StaticTCP
realm-id peer-HP4K-TCP
egress-realm-id
description
carriers
allow-next-hop-lp enabled
constraints disabled
max-sessions 0
```

```
max-inbound-sessions 0
max-outbound-sessions 0
max-burst-rate 0
max-inbound-burst-rate 0
max-outbound-burst-rate 0
max-sustain-rate 0
max-inbound-sustain-rate 0
max-outbound-sustain-rate 0
min-seizures 5
min-asr 0
time-to-resume 0
ttr-no-response 0
in-service-period 0
burst-rate-window 0
sustain-rate-window 0
req-uri-carrier-mode None
proxy-mode
redirect-action
loose-routing enabled
send-media-session enabled
response-map
ping method
ping-interval 0
ping-send-mode keep-alive
ping-all-addresses disabled
ping-in-service-response-codes
out-service-response-codes
media-profiles
in-translationid
out-translationid
trust-me disabled
request-uri-headers
stop-recurse
local-response-map
ping-to-user-part
ping-from-user-part
li-trust-me disabled
```

```
in-manipulationid
out-manipulationid
manipulation-string
manipulation-pattern
p-asserted-id
trunk-group
max-register-sustain-rate 0
early-media-allow
invalidate-registrations disabled
rfc2833-mode none
rfc2833-payload 0
codec-policy
enforcement-profile
refer-call-transfer disabled
reuse-connections NONE
tcp-keepalive none
tcp-reconn-interval 0
max-register-burst-rate 0
register-burst-window 0
sip-profile
sip-isup-profile
last-modified-by admin@10.232.1.138
last-modified-date 2010-05-28 13:24:13
```

Notes:

- `transport-method` - must be set to StaticTCP for SIPQ connections

Configure the core Session Agent

```
session-agent
hostname tcp.osvV10.unify.com
ip-address 10.232.51.102
port 5060
state enabled
app-protocol SIP
app-type
transport-method StaticTCP
realm-id core-peer-HP4K-TCP
egress-realm-id
```

`description`

`carriers`

`allow-next-hop-lp` *enabled*

`constraints` *disabled*

`max-sessions` *0*

`max-inbound-sessions` *0*

`max-outbound-sessions` *0*

`max-burst-rate` *0*

`max-inbound-burst-rate` *0*

`max-outbound-burst-rate` *0*

`max-sustain-rate` *0*

`max-inbound-sustain-rate` *0*

`max-outbound-sustain-rate` *0*

`min-seizures` *5*

`min-asr` *0*

`time-to-resume` *0*

`ttr-no-response` *0*

`in-service-period` *0*

`burst-rate-window` *0*

`sustain-rate-window` *0*

`req-uri-carrier-mode` *None*

`proxy-mode`

`redirect-action`

`loose-routing` *enabled*

`send-media-session` *enabled*

`response-map`

`ping method`

`ping-interval` *0*

`ping-send-mode` *keep-alive*

`ping-all-addresses` *disabled*

`ping-in-service-response-codes`

`out-service-response-codes`

`media-profiles`

`in-translationid`

`out-translationid`

`trust-me` *disabled*

`request-uri-headers`

```
stop-recurse
local-response-map
ping-to-user-part
ping-from-user-part
li-trust-me disabled
in-manipulationid
out-manipulationid
manipulation-string
manipulation-pattern
p-asserted-id
trunk-group
max-register-sustain-rate 0
early-media-allow
invalidate-registrations disabled
rfc2833-mode none
rfc2833-payload 0
codec-policy
enforcement-profile
refer-call-transfer disabled
reuse-connections NONE
tcp-keepalive none
tcp-reconn-interval 0
max-register-burst-rate 0
register-burst-window 0
sip-profile
sip-isup-profile
last-modified-by admin@10.232.1.138
last-modified-date 2010-08-18 17:44:53
```

Notes:

- `transport-method` - must be set to StaticTCP for SIPQ connections

7.2.20.8 Local Policies - SIPQ Trunking Deployment Scenario

Configure the local policies for the different routes

Configure local policy to route traffic from HP4K to OSV

```
local-policy
from-address *
```

```
to-address *
source-realm peer-HP4K-TCP
description
activate-time N/A
deactivate-time N/A
state enabled
policy-priority none
last-modified-by admin@10.232.1.138
last-modified-date 2009-05-14 15:16:40
policy-attribute
next-hop tcp.osvV10.unify.com
realm core-peer-HP4K-TCP
action none
terminate-recursion disabled
carrier
start-time 0000
end-time 2400
days-of-week U-S
cost 0
app-protocol SIP
state enabled
methods
media-profiles
lookup single
next-key
eloc-str-lkup disabled
eloc-str-match
```

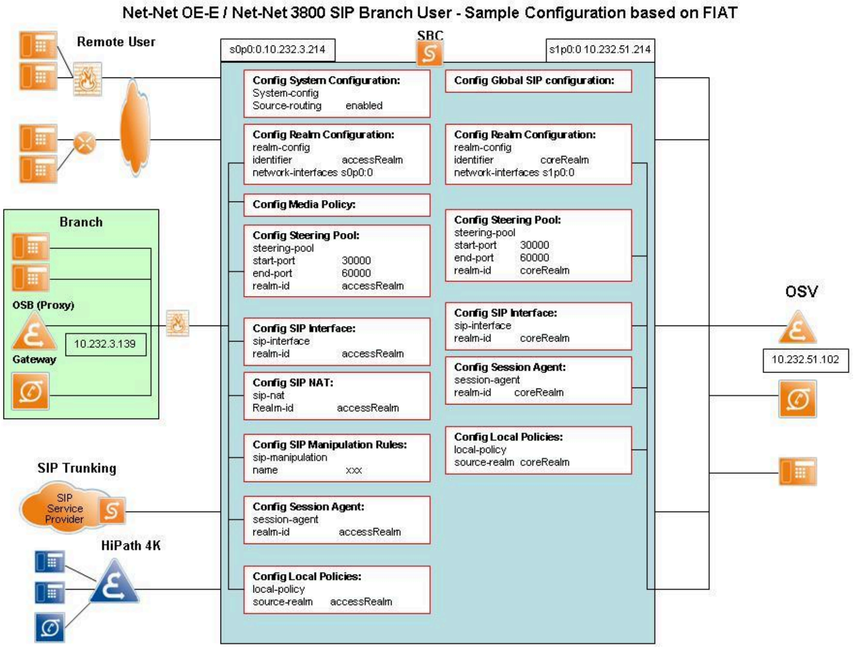
Configure local policy to route traffic from OSV to HP4K realm

```
local-policy
from-address *
to-address *
source-realm core-peer-HP4K-TCP
description
activate-time N/A
deactivate-time N/A
state enabled
policy-priority none
```

```
last-modified-by admin@10.232.1.138
last-modified-date 2010-05-28 13:25:20
policy-attribute
next-hop 10.232.3.103
realm peer-HP4K-TCP
action none
terminate-recursion disabled
carrier
start-time 0000
end-time 2400
days-of-week U-S
cost 0
app-protocol SIP
state enabled
methods
media-profiles
lookup single
next-key
eloc-str-lkup disabled
eloc-str-match
```

7.2.21 Net-Net 3000, Net-Net 4000 Series SBC - Branch Deployment Scenario using OpenScape Branch (Proxy)

The Net-Net 3800 SBC configuration for supporting branch deployments is identical to the one described under "Basic configuration".



Related concepts

Net-Net 3000, Net-Net 4000 Series SBC - Basic Configuration on page 693

7.3 QSIG Tunneling

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.

The SIP-Q signaling method permits public and private network users behind a HiPath 3000, OpenScape 4000, or OpenScape SBC to interoperate with OpenScape Voice. It also supports tunneling of QSIG/CorNet-NQ protocol over SIP protocol as a trunking interface— for example, between two OpenScape Voice systems. Tandem signaling of SIP-Q through multiple OpenScape Voice systems for calls between HiPath 3000 and OpenScape 4000 systems with OpenScape SBC is possible, as well as HiPath 3000 and OpenScape 4000 systems with their integrated gateways.

CorNet-NQ is a Unify proprietary QSIG-based signaling protocol for interconnecting OpenScape Voice systems to one or more QSIG PBX systems. It is a superset of the QSIG-defined Q.931/Q.932 protocol extensions.

A typical corporate network may consist of legacy PBXs employing QSIG networking, interconnected with an IP network employing SIP. A call can originate in either the QSIG or SIP network, and can subsequently be interworked via a gateway that provides translation and mapping between QSIG and SIP.

SIP-Q provides the following features network-wide:

- SIP-Q-to-SIP-Q pass-through

  As example, a legacy user is routed over IP to another legacy user located a distance away. This capability can save TDM costs for an enterprise.
- Failover recovery superior to that of H.323 standard communications.
- Support of media encryption.

Requirements

The following are interworking requirements:

- Interworking between OpenScape Voice and the OpenScape 4000 requires the HiPath gateway 3540 (HG 3540) board for OpenScape 4000 V3 systems, or the HiPath gateway 3500 (HG 3500) board for OpenScape 4000 V4 systems. Each is an integrated gateway used for IP network connectivity that gives the OpenScape 4000 access to IP-based trunking. It serves both line- and trunk-side SIP interfaces.
- Interworking between OpenScape Voice and the HiPath 3000 requires the HG 1500 board.
- The HiPath 3000 or OpenScape 4000 can also use the OpenScape SBC instead of the integrated gateway.

Other Characteristics

Interworking between two or more OpenScape Voice systems is supported. For example, a SIP subscriber in one OpenScape Voice system can call another subscriber/user that is located behind or registered to a second OpenScape Voice system (a SIP subscriber or gateway). CorNet-NQ/QSIG supplementary services are interworked between the subscribers over the SIP-Q trunk.

- From OSV V7.0 and onwards, for OSV - OpenScape 4000 scenarios the chief-secretary operation feature is enhanced to present the OpenScape 4000 Chief’s Name/Number to the OSV calling party (subscriber) when called party is alerted (ringing) or Busy.

-From OSV V8.0 and onwards the enhancement above is applied to scenarios were OSV is acting as a tandem Server.

7.3.1 Path Replacement

Path replacement releases unused links from the network. It is implemented as part of the SIP-Q functionality, and can also be used in a mixed (multi-vendor) environment.

Release links provide a solution that can optimize the media path, or both the media and signaling paths, through the network. This is accomplished by implementing the following:

- Supplementary Service Call Transfer (SS-CT)
- Path Replacement additional network feature (ANF-PR)

NOTICE:

The HiPath 3000 does not support path replacement.

7.3.2 Message Truncation

OpenScape Voice supports truncating a QSIG message tunnelled in a QSIG multipurpose Internet mail extensions (MIME) body, which eliminates the need for the gateway to fragment MIME data. This ability permits OpenScape Voice to interoperate with legacy PBXs that do not support message segmentation.

The administrator uses OpenScape Voice Assistant to configure the `truncate MIME endpoint` attribute. When this attribute is set to `Yes`, it specifies that some elements of the QSIG MIME must be removed. When these elements are removed, the signaling is reduced to only the QSIG protocol, and does not include Unify CorNet-NQ value-added features—for example, CDR, feature permissions, and distinctive ringing for internal and external callers.

OpenScape Voice can be administered to truncate private operations from a QSIG message and not exceed the 260 byte limit for a layer 2 message. This is needed to suppress segmentation at the OpenScape SBC, for example, when the QSIG-compliant PINX does not support message/APDU segmentation.

7.3.3 Call Diversion Over Multiple Platforms

The SIP-Q Interworking for the Call Diversion Service feature is implemented as part of the SIP-Q functionality so it can be used in a mixed (multi-vendor) environment.

This feature provides the following:

- The ability to avoid trombone trunk connections.

When an OpenScape Voice subscriber forwards his telephone call to a user behind a SIP-Q gateway, and another user behind the same SIP-Q gateway calls that OpenScape Voice subscriber, call forwarding rerouting is performed so that link and port resources in the IP network (OpenScape Voice and SIP-Q gateway) are released.

NOTICE:

The HiPath 3000 does not support this call forwarding rerouting.

- The ability to perform forward switching to the forwarded-to user when the calling party switch does not support call forwarding rerouting, which can result in using unnecessary IP link and/or port resources.
- The ability to forward calls to messaging systems across multiple platforms.

7.3.4 Transfer

The call transfer features permit a subscriber to redirect an established call to another party. The subscriber can perform the transfer as long as the subscriber is allowed to call both the caller and the transfer-to party. The interaction between the system and the third party is similar to that during three-way calling, except that when a party with the feature hangs up, the incoming or outgoing call is transferred to the third party.

The QSIG SS-CT and ANF-PR operations are supported for transfer by join (attended, semi-attended, and blind transfer) scenarios in which one or both parties are connected via a SIP-Q gateway. From the QSIG perspective, OpenScape Voice can be a transferring, transferred and transferred-to PBX.

- If the transfer by join fails for any reason, the transferring party is reconnected to the transferred party of the original call. This reconnection occurs as a recall of the transferred party B on behalf of the transferring party A. This applies to semi-attended and blind transfer scenarios.

- After a SIP-Q call transfer, the displays of the connected parties are updated with their partner's name and number.

After the transfer is completed, path replacement is invoked to release unnecessary links.

7.3.5 Interworking with Voice Mail System

The interworking with voice mail systems feature provides signaling and interworking with SIP-based third-party voice mail systems. The capability to support a visual message waiting indicator as well as stutter dial tone is provided by OpenScape Voice as long as the support for this capability is also provided by the voice mail system and the customer premises equipment.

The interworking between OpenScape Voice and a legacy PBX has following properties.

- Voice mail can be located in both or either the OpenScape Voice system or legacy PBX.
- Transfer out of voice mail is possible to anywhere in the network.
- When an new message is received for a user, message waiting indication (MWI) is sent to that OpenScape Voice or legacy user.

7.4 PSTN (Public Switched Telephone Network) Connection

A PSTN (Public Switched Telephone Network) is a domestic telecommunications network usually accessed by telephones, key telephone systems, private branch exchange trunks, and data arrangements. Completing the circuit between the call originator and call receiver in a PSTN requires network signaling in the form of dial pulses or multifrequency tones.

7.4.1 Media Gateways of the Mediatrix Series

Mediatrix media and signaling gateways are small branch office gateways that connect endpoints in an office serving 200 or fewer subscribers. Because they are ISDN gateways, they support ISDN switching, router function, and a gateway which converts ISDN voice data into Internet Protocol IP data streams or voice over IP, and vice versa.

The Mediatrix gateways support the following:

- User-programmable call handling.
- CLI, SNMP, Telnet, and TFTP (Trivial File Transfer Protocol) for configuration and management.
- RS-232 console port for configuration.
- Fax over IP.
- Multiple codecs.

The Mediatrix gateways also support encrypted SRTP (Secure Real-Time Transport Protocol) with the MIKEY (Multimedia Internet Keying) Profile 0 key management protocol.

The following table lists and describes the Mediatrix models. The number of users each supports depends entirely on the following:

- Inbound and outbound traffic load.
- System routing in normal mode and in survivability mode.

Table 199: Mediatrix Gateway User Capacities and Interfaces

Model	Description
1202	Two-port foreign exchange office (FXO) gateway, suitable for access to PSTN analog lines
1204	Four-port FXO gateway, suitable for access to PSTN analog lines
1402	Two ISDN BRI (Basic Rate Interface)
1404	Four ISDN BRI
1531	Single-span T1 PRI (Primary Rate Interface)
1631	Single-span E1 PRI
1632	Dual-span E1 PRI
2404	Four ISDN BRI
3531	Single-span T1 PRI
3532	Dual-span T1 PRI
3631	Single-span E1 PRI
3632	Dual-span E1 PRI
4401	One ISDN BRI
4402	Two ISDN BRI
4404	Four ISDN BRI

7.4.2 Media Gateway OpenScape SBC

The OpenScape SBC is a survivable media gateway designed to facilitate the connection of branch offices to the central corporate network and the use of network-wide resources by the branch offices. It uses SIP to interface to the OpenScape Voice system. At this time, it does not support United States trunk interfaces.

The media gateway OpenScape SBC automatically uses a standby dial-up connection if the IP network fails; it also maintains important station data so that the SIP telephones in the branch offices remain in operation. In a survivability scenario, accounting data is stored locally and made available to OpenScape Voice applications.

This gateway includes a built-in router, and offers a large number of functions for straightforward integration in an existing LAN infrastructure. It is administered via WBM (Web-based Management), which provides integrated management functions for installation and maintenance. Microsoft Internet Explorer is used for system access.

System Specific Information

The OpenScape SBC supports the following:

- Access to ISP using xDSL lines
- IP router
- Firewall
- DynDNS
- DNS server
- DHCP server
- IPsec-based VPN

7.4.3 Media Gateway OpenScape SBC

The OpenScape SBC survivable media gateway provides scalable and standards-based gateway platforms that mediate TDM (Time Division Multiplexing) traffic (in circuit-switched, fixed, or mobile switching networks) to the packet world with carrier-grade reliability.

The media gateway OpenScape SBC ensures that station-to-station calls, PSTN (Public Switched Telephone Network) access, and United States emergency services access (E9-1-1) are available at all times in remote branches. It supports the ANSI and ETSI PRI protocols, QSIG (Q Signaling) tunneling to the OpenScape 4000 interface, and E9-1-1 LIN server provisioning.

It is administered via the OpenScape SBC Assistant, and uses SIP to interface to the OpenScape Voice system. When QSIG tunneling to the HiPath 3000 or OpenScape 4000 is present, SIP-Q is used instead.

System Specific Information

The OpenScape SBC supports the following:

- ANSI and ETSI (European Telecommunications Standards Institute) PRI (Primary Rate Interface) protocols.
- QSIG tunneling to the HiPath 3000 or OpenScape 4000 interface.

- E9-1-1 LIN (Location Identification Number) server provisioning.
- Encrypted SRTP with the MIKEY Profile 0 key management protocol. When the SIP-Q interface is used, the OpenScape SBC is able to build an end-to-end secure call with the OpenScape 4000.
- G.711, G.726, G.729, and G.723.1 codecs.
- Clear mode.
- DTMF (Dual Tone Multifrequency) Events in accordance with RFC 2833.
- T.38 (Fax over IP).
- Geographic node separation by switching between the nodes in case of a node failure.

7.5 SIP Trunking

SIP trunking connects IP telephony with traditional PSTNs (Public Switched Telephone Networks). It enables enterprises to communicate over IP not only within the company, but also to outside PSTNs, thus they can make full use of their installed PBXs (Private Brand eXchanges).

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 theyare 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 serviceproviders, although progress is being made to standardize the enterprise/SIPservice provider interface in standards bodies such as the SIP Forum.

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 OpenScape Voice Assistant or the CLI. 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.

7.5.1 SIP Trunking - CLIP (Calling Line Identification Presentation)

CLIP (Calling Line Identification Presentation) provides the called party with the identity of the calling party. The identity consists of name and telephone number of the calling party. The OpenScape Voice server is able to send identity information for the CLIP feature to a SP (Service Provider).

Identity information to be included in P-Asserted-Identity header fields is inserted by the SSNE (SIP Signaling Network Element) that is responsible for the calling party. Therefore, the SSNE should authenticate the calling party in order make sure that the correct identity information is included.

- The OpenScape Voice server is able to send identity information for the CLIP feature to a Service Provider.
- The OpenScape Voice server is able to process received identity information for the CLIP feature from a Service Provider.

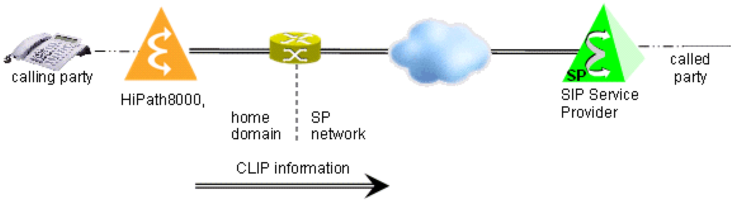
Functional Sequence - Sending requests and responses to SP

1) P-Asserted-Identity header field

If the SP is considered part of the Enterprise “Trust Domain”, OpenScape Voice will include the P-Asserted-Identity header field in SIP INVITE requests. Currently OpenScape Voice does not support sending a private identity in the P-Asserted-Identity header field, this header field will contain the same public identity as the From header field . If the calling party is a member of a user group with a private numbering plan then the callers private numbering identity will not be sent in the P-Asserted-Identity to the SP.

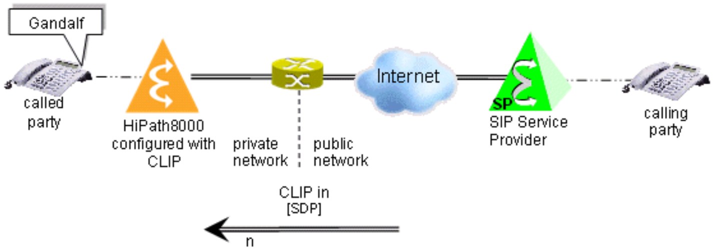
2) From Header field

The OpenScape Voice server that is responsible for the calling party may remove the original identity information from the received From header field from the client and insert appropriate public identity information from the OpenScape Voice database. Usually, this header field contains the desired public PSTN identity of the subscriber.



Functional Sequence - Receiving requests and responses from SP

The Enterprise system SHOULD be able to process a P-Asserted-Identity header field in received INVITE requests from the Service Provider (for example, for display update and call logging purposes). If no P-Asserted-Identity header field is present, identity information from the From header field may be used for these purposes.



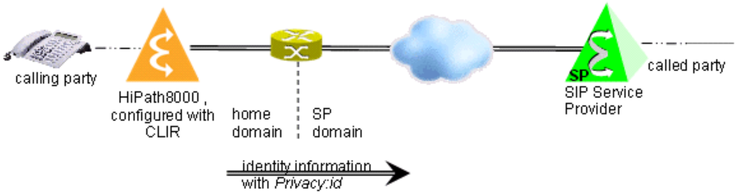
7.5.2 SIP Trunking - CLIR (Calling Line Identification Presentation Restriction)

Calling Line Identification Presentation Restriction (CLIR) prevents the called party from receiving the identity of the calling party.

In order to support CLIR, a SSNE (SIP Signaling Network Element) should be able to send an anonymized From header field, a P-Asserted-Identity header field as well a Privacy header field. A SSNE should also be able to process a received anonymized From header field, a P-Asserted-Identity header field as well as a Privacy header field.

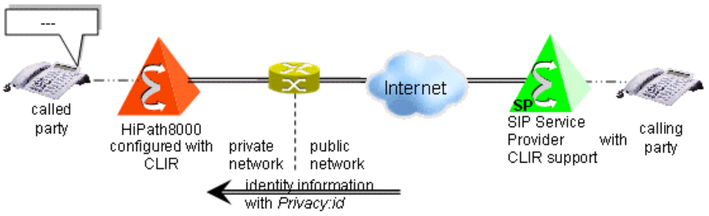
Functional Sequence - Sending requests and responses to SP (Service Provider)

This includes sending a P-Asserted-Identity header field together with a Privacy:id header field. The From header field will be sent with anonymized identity information.


calling party
HiPath8000 , configured with CLIR
home domain
SP domain
SP
SIP Service Provider
called party
identity information with *Privacy:id*

Functional Sequence - Receiving requests and responses from SP

The Enterprise system SHOULD be able to process a received Privacy header field values with id, user, and header as well as support for receiving an anonymous From header field.


---
called party
HiPath8000 configured with CLIR
private network
public network
Internet
SP
SIP Service Provider with CLIR support
calling party
identity information with *Privacy:id*

7.5.3 SIP Trunking - COLP (Connected Line Identification Presentation)

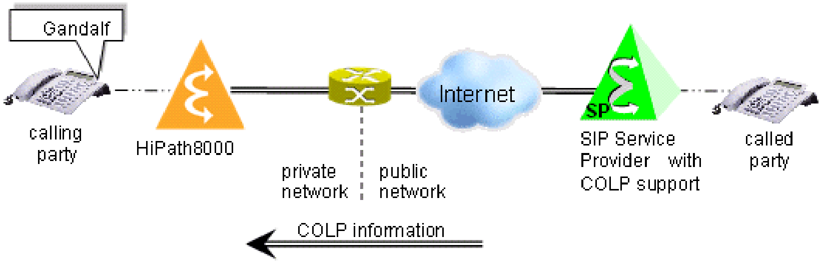
COLP (Connected Line Identification Presentation) provides the calling party with the identity of the connected party. The identity consists of name (optional) and number of the connected party.

Identity information to be included in P-Asserted-Identity header fields in responses is inserted by the SIP server that is responsible for the connected party. The calling party may use this information in order to display the connected party's identity.

- An SSNE (SIP Signaling Network Element) should be able to send identity information for the COLP feature in responses.
- An SSNE should be able to process received identity information for the COLP feature in responses.

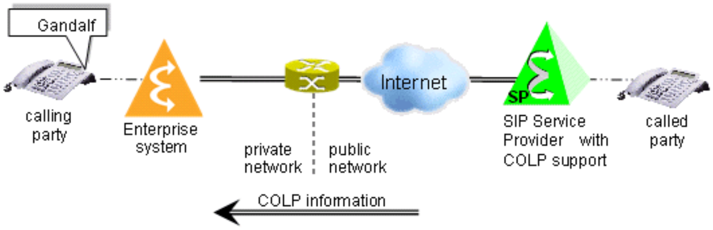
Functional Sequence - Sending requests and responses to SP (Service Provider)

There are no requirements for outgoing calls (client with COLP is at SP). Incoming calls (client with COLP within the OpenScape Voice server) include sending a P-Asserted-Identity header field in 200 responses to dialog creating INVITE requests, if the particular OpenScape Voice client has COLP active. This header field, if present, contains the identity of the called client.



Functional Sequence - Receiving requests and responses from SP

Outgoing calls (client with COLP is at SP) include processing a received P-Asserted-Identity header field in 200 responses to dialog creating INVITE requests. There are no requirements for incoming calls (client with COLP is within the OpenScape Voice server).



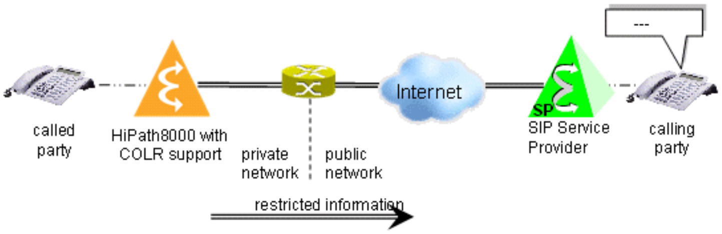
7.5.4 SIP Trunking - COLR (Connected Line Identification Presentation Restriction)

COLR (Connected Line Identification Presentation Restriction) prevents the called party from divulging identity information back to the calling party.

In order to support COLR, a SSNE (SIP Signaling Network Element) should be able to send a P-Asserted-Identity header field as well as a Privacy header field in responses to another SSNE. An SSNE should be able to process a received P-Asserted-Identity header field as well as a Privacy header field in responses from another SSNE.

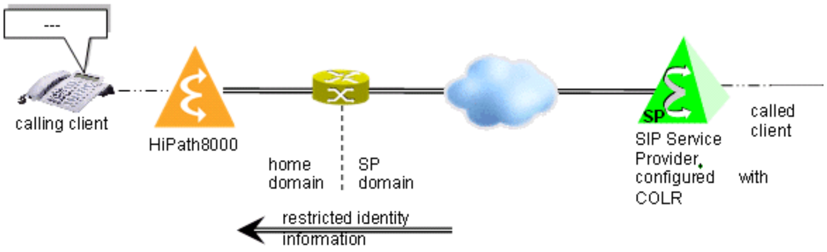
Functional Sequence - Sending requests and responses to SP (Service Provider)

There are no requirements for outgoing calls (clients with COLR is at SP). Incoming calls (client with COLR is within the OpenScape Voice server) require that OpenScape Voice sends a P-Asserted-Identity header field together with a Privacy header field in responses to dialog creating INVITE requests from the Service Provider, if the particular OpenScape Voice client has COLR active.



Functional Sequence - Receiving requests and responses from SP

Outgoing calls (client with COLR is at SP) include processing a received P-Asserted-Identity header field as well as a Privacy header field in 200 responses to dialog creating INVITE requests. There are no requirements for incoming calls.


---
calling client
HiPath8000
home domain
SP domain
restricted identity information
SP
SIP Service Provider, configured with COLR
called client

7.5.5 SIP Trunking - Call Hold, Retrieve and Alternate

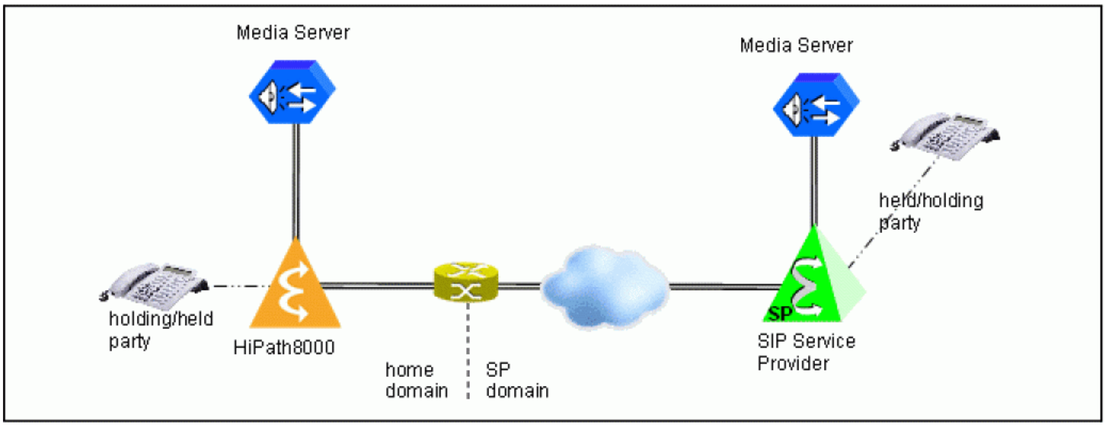
An established call may be put on hold so that the holding party is able to place another call. Meanwhile the held party may receive MOH (Music on Hold). This music on hold may be provided by either the holding party, or by a media server on behalf of the holding party or locally by the held party.

Alternating is a combination of Call Hold and Call Retrieve. Pre-requisite for Alternating is a held call and another (secondary) call that is established after the first call is placed on hold. By executing Alternate the secondary call is placed on hold and the first call is retrieved. This way the user can toggle between two parties by placing the other party on hold each time the Alternate feature is invoked.

An SSNE (SIP Signaling Network Element), acting as a B2BUA (Back-to-Back User Agent) ...

- should be able to place an established call on hold and to retrieve a held call.
- should be able to place an established call on hold and the held party may also place the holding party on hold.
- may be able to alternate between an active call and a held call.

The Media Server shown in the following picture may be included in the OpenScape Voice server. It is not necessarily a separate Media Server host. It is shown as a separate entity only for sake of generality.



There may be either a Media Server within the OpenScape Voice server, or at the Service Provider, or both. It is out of the scope of this specification how the location of the Media Server(s) is made known to the B2BUAs. This may be done for example via configuration.

Typically, the protocol that is used in order to control a Media Server is MGCP (Media Gateway Control Protocol). Some SSNEs hide the MGCP specifics from the participating SIP entities.

- OpenScape Voice sends requests and responses to Service Provider:
  - **Call Hold** includes that on a user request to put an active call on hold, the holding SSNE sends a re-INVITE request to the held client with an SDP offer. This SDP offer contains the attribute line a=inactive or a=sendonly. The OpenScape Voice server also supports the deprecated method of setting the IP address in c= line to 0.0.0.0, (this option can be enabled/disabled via OpenScape Voice configuration).
  - **Call Retrieve** includes that on a user request to retrieve a held call, the holding SSNE sends a re-INVITE request to the held client with an SDP offer. This SDP offer contains the attribute line a=sendrecv.
- OpenScape Voice receives requests and responses from Service Provider:
  - **Call Hold** This includes processing a received re-INVITE request that is sent from a Service Provider to a client. This re-INVITE request contains an SDP offer with the attribute line a=inactive or a=sendonly, which instructs the client to hold the currently active call. An SSNE should pass

any received SDP body unchanged to the destination of the re-INVITE request.

  - **Call Retrieve** includes processing a received re-INVITE request that is sent from a Service Provider to a client. This re-INVITE request contains an SDP offer with the attribute line a=sendrecv, which instructs the client to resume the held call. An SSNE should pass any received SDP body unchanged to the destination of the re-INVITE request.

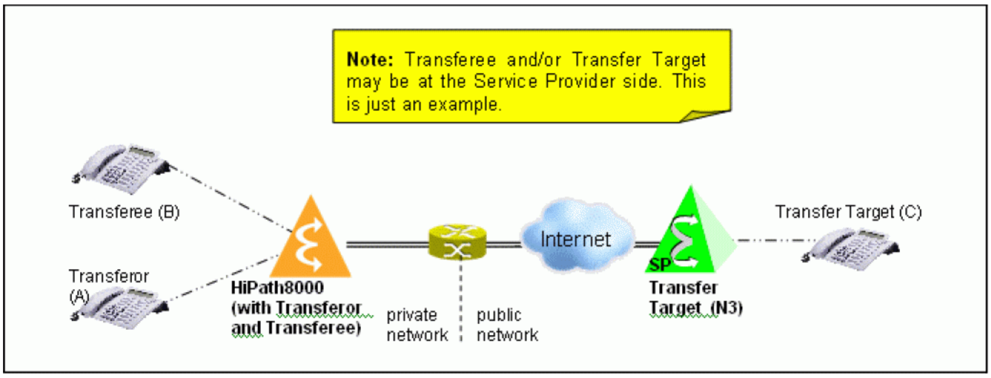
- Service Provider sends requests and responses to OpenScape Voice:
  - **Call Hold** includes that a Service Provider sends a re-INVITE request on an established dialog with an SDP body that contains either the attribute line a=inactive or a=sendonly. The OpenScape Voice server also accepts the deprecated method of setting the IP address in c= line to 0.0.0.0.
  - **Call Retrieve** includes that a Service Provider sends a re-INVITE request on an established dialog with an SDP body that contains the attribute line a=sendrecv.
- Service Provider receives requests and responses from OpenScape Voice:
  - **Call Hold** includes that a client to be held behind a Service Provider is able to process a received re-INVITE request that is sent to a client with an SDP offer that contains either the media attribute a=inactive or a=sendonly. A Service Provider may pass received SDP body transparently to the destination of the re-INVITE request or it may insert its own Media Server address in the SDP body.
  - **Call Retrieve** includes that a held client behind a Service Provider is able to process a received re-INVITE request that is sent to a held client with an SDP offer that contains a media attribute with a=sendrecv. A Service Provider should pass received SDP body transparently to the destination of the re-INVITE request.

7.5.6 SIP Trunking - Call Transfer

Call transfer is a call re-arrangement of an existing call in which one party is replaced with another party. Initially, the transferor is in an active call with the transferee. Then the transferor initiates a call transfer to the transfer target. Finally the transfer target gets connected to the transferee.

Transferor, transferee and transfer target may be within the Enterprise system or behind the Service Provider.

The following graphic depicts an example call transfer scenario with two call transfer participants within the OpenScape Voice server and one party is behind the Service Provider. Any other combination of call transfer participants within the OpenScape Voice server or behind a Service Provider is possible.


Note: Transferee and/or Transfer Target may be at the Service Provider side. This is just an example.
Transferee (B)
Transferor (A)
HiPath8000 (with Transferor and Transferee)
private network
public network
Internet
SP
Transfer Target (N3)
Transfer Target (C)

7.5.7 Attended Call Transfer

Attended Call Transfer allows the user to transfer the call by going on-hook while the destination is ringing; also known as unscreened transfer. The party initiating the transfer receives an audible indication (ringback tone).

Requirements

- **Transferor behavior**

  If Attended Call Transfer is supported, the OpenScape Voice server should be able to perform the role of a transferor by converting a received call transfer indication (for example via SIP REFER request) into a series of re-INVITE requests using third party call control techniques as described as follows:

  – **OpenScape Voice sends requests and responses to Service Provider, transferee is at Service Provider:**

    The OpenScape Voice server should support sending a re-INVITE request on the existing dialog (dialog_1) with no SDP to the transferee. This re-INVITE request SHOULD contain a P-Asserted-Identity header field that indicates the transfer target. This allows the transferee to update its phone display with the identity of the transfer target.

  – **OpenScape Voice sends requests and responses to Service Provider, transfer target is at Service Provider:**

    The OpenScape Voice server should support sending a re-INVITE request on the existing dialog (dialog_2) with the SDP from the transferee (or from the OpenScape Voice B2BUA if it terminates media) to the transfer target. This re-INVITE request SHOULD contain a P-Asserted-Identity header field that indicates the transferee as well as a Referred-By header field that indicates that a call transfer has been performed by the transferor. This allows the transfer target to update its phone display with the identity of the transferee.

  - **OpenScape Voice receives requests and responses from Service Provider:**

    The OpenScape Voice server should support re-INVITE requests with and without SDP in order to support call transfers which are originated outside the OpenScape Voice server.

    > **NOTICE:**
    >
    > The OpenScape Voice server provides a configuration option to accept a SIP REFER request from the Service Provider as a call transfer request (the default operation of the OpenScape Voice server is to not accept SIP REFER requests from a Service Provider). Provisioning at the OpenScape Voice server is necessary to accept a SIP REFER request from a Service Provider.

  - **Service Provider sends requests and responses to OpenScape Voice:**

    A Service Provider may send re-INVITE requests to the OpenScape Voice system with and without SDP. A Service Provider may send a REFER request to the OpenScape Voice server to initiate a call transfer if the OpenScape Voice server has been configured to accept REFER requests from the Service provider.

  - **Service Provider receives requests and responses from OpenScape Voice:**

    No requirements.

- **Transfer Target behavior**

  The OpenScape Voice server should be able to perform the role of a transfer target as described below:

  - **OpenScape Voice sends requests and responses to Service Provider:**

    The OpenScape Voice server should respond to received re-INVITE requests containing SDP according to RFC3264. Furthermore, sending a P-Asserted-Identity header field in responses may be supported in order to allow updating the transferee client display.

  - **OpenScape Voice receives requests and responses from Service Provider:**

    The OpenScape Voice system should support processing of received re-INVITE requests with SDP. Furthermore, it may support a received Referred-By header field as well as a received P-Asserted-Identity header field in received re-INVITE requests.

  - **Service Provider sends requests and responses to OpenScape Voice:**

    A Service Provider should be able to respond to received re-INVITE requests with SDP.

  - **Service Provider receives requests and responses from OpenScape Voice:**

    A Service Provider should support processing of received re-INVITE requests with SDP.

- **Transferee behavior**

  The OpenScape Voice server should be able to perform the role of a transferee as described below:

  - **OpenScape Voice sends requests and responses to Service Provider:**

    The OpenScape Voice server should respond to received re-INVITE requests without SDP according to RFC3264. Furthermore, sending a P-Asserted-Identity header field in responses may be supported in order to allow updating the transferee client display.
  - **OpenScape Voice receives requests and responses from Service Provider:**

    The OpenScape Voice server should support processing of received re-INVITE requests without SDP. Furthermore, it may support a received P-Asserted-Identity header field in received re-INVITE requests.
  - **Service Provider sends requests and responses to OpenScape Voice:**

    A Service Provider should be able to respond to received re-INVITE requests without SDP.
  - **Service Provider receives requests and responses from OpenScape Voice:**

    A Service Provider should support processing of received re-INVITE requests without SDP.

7.5.8 Blind Call Transfer

When a user transfers a call to another user without telling the caller that the call is being transferred. The party initiating the blind transfer does not hear an audible indication (ringback tone).

Requirements

- **Transferor behavior**

  If Blind Call Transfer is supported, the OpenScape Voice server should be able to perform the role of a transferor by converting a received call transfer indication (for example, SIP REFER request) into a series of INVITE/re-INVITE requests using third party call control techniques as described as follows.

  - **OpenScape Voice sends requests and responses to Service Provider, transfer target is at Service Provider:**

    The OpenScape Voice server should support sending a new INVITE request (thereby creating dialog_2) with no SDP to the transfer target. This INVITE request SHOULD contain a P-Asserted-Identity header field that indicates the transferee and may contain a Referred-By header field that indicates that a call transfer has been performed by the transferor. This allows the transfer target to update its phone display with the identity of the transferee.

- **OpenScape Voice sends requests and responses to Service Provider, transferee is at Service Provider:**

  The OpenScape Voice server should support sending a re-INVITE request on the existing dialog (dialog_1) with the received SDP (from the transfer target) to the transferee. This re-INVITE request SHOULD contain a P-Asserted-Identity header field that indicates the transfer target. This allows the transferee to update its phone display with the identity of the transfer target.
- **OpenScape Voice receives requests and responses from Service Provider:**

  The OpenScape Voice server should support re-INVITE requests with and without SDP in order to support call transfers which are originated outside the OpenScape Voice server.

  NOTICE:

  The OpenScape Voice server provides a configuration option to accept a SIP REFER request from the Service Provider as a call transfer request (the default operation of the OpenScape Voice server is to not accept SIP REFER requests from a Service Provider). Provisioning at the OpenScape Voice server is necessary to accept a SIP REFER request from a Service Provider.
- **Service Provider sends requests and responses to OpenScape Voice:**

  A Service Provider may send re-INVITE requests to the OpenScape Voice server with and without SDP. A Service Provider may send a REFER request to the OpenScape Voice server to initiate a call transfer if the OpenScape Voice server has been configured to accept REFER requests from the Service Provider.
- **Service Provider receives requests and responses from OpenScape Voice:**

  No requirements

- **Transfer Target behavior**

  The OpenScape Voice server should be able to perform the role of a transfer target as described as follows:

  - **OpenScape Voice sends requests and responses to Service Provider:**

    The OpenScape Voice server should respond to received INVITE requests containing no SDP according to RFC3264. Furthermore, sending a P-Asserted-Identity header field in responses may be supported in order to allow updating the transferee client display.
  - **OpenScape Voice receives requests and responses from Service Provider:**

    The OpenScape Voice server should support processing of received re-INVITE requests with no SDP. Furthermore, it may support a received Referred-By header field (by copying it to corresponding subsequent requests) as well as a received P-Asserted-Identity header field in received INVITE requests.

  - **Service Provider sends requests and responses to OpenScape Voice:**

    A Service Provider should be able to respond to received INVITE requests with no SDP.

  - **Service Provider receives requests and responses from OpenScape Voice:**

    A Service Provider should support processing of received INVITE requests with no SDP.

- **Transferee behavior**

  The OpenScape Voice server should be able to perform the role of a transferee as described as follows:

  - **OpenScape Voice sends requests and responses to Service Provider:**

    The OpenScape Voice server should respond to received re-INVITE requests with SDP according to RFC3264. Furthermore, sending a P-Asserted-Identity header field in responses may be supported in order to allow updating the transferee client display.

  - **OpenScape Voice receives requests and responses from Service Provider:**

    The OpenScape Voice server should support processing of received re-INVITE requests with SDP. Furthermore, it may support a received P-Asserted-Identity header field in received re-INVITE requests.

  - **Service Provide sends requests and responses to OpenScape Voice:**

    A Service Provider should be able to respond to received re-INVITE requests with SDP.

  - **Service Provider receives requests and responses from OpenScape Voice:**

    A Service Provider should support processing of received re-INVITE requests with SDP.

7.5.9 Semi-Attended Call Transfer

Semi-attended Call Transfer designates the following call transfer scenario: Phone A calls Phone B; Phone B answers, and decides to transfer the call to Phone C; Phone B completes the transfer while phone C is still ringing.

Requirements

- **Transferor behavior**

  If Semi-Attended Call Transfer is supported, the OpenScape Voice server should be able to perform the role of a transferor by converting a received call transfer indication (for example, SIP REFER request) into a series of

INVITE and UPDATE requests using third party call control techniques as described as follows:

- **OpenScape Voice sends requests and responses to Service Provider, transferee is at Service Provider:**

  The OpenScape Voice server should support placing the existing dialog to the transferee on hold.
- **OpenScape Voice sends requests and responses to Service Provider, transfer target is at Service Provider:**

  The OpenScape Voice server should support sending an INVITE request, thereby creating an early dialog (dialog_2). This INVITE request SHOULD contain a P-Asserted-Identity header field that indicates the transferee. This allows the transfer target to update its phone display with the identity of the transferee.

  As soon as the first 180 Ringing or 182 Queued response is received, the transferor user may be disconnected, but the dialog1 SHOULD still be maintained. This is necessary in case the call to the transfer target fails. As the call to the transfer target is still in an early state, it may still undergo forking, be rejected or simply not answered.

  The OpenScape Voice server may send an UPDATE request containing a P-Asserted-Identity header field with the identity of the transferee to the transfer target in order to allow for display updates and call logging.
- **OpenScape Voice receives requests and responses from Service Provider:**

  The OpenScape Voice server should support INVITE and re-INVITE requests with and without SDP in order to support call transfers which are originated outside the OpenScape Voice server.

  > **NOTICE:**
  >
  > The OpenScape Voice server provides a configuration option to accept a SIP REFER request from the Service Provider as a call transfer request (the default operation of the OpenScape Voice server is to not accept SIP REFER requests from a Service Provider). Provisioning at the OpenScape Voice server is necessary to accept a SIP REFER request from a Service Provider.
- **Service Provider sends requests and responses to OpenScape Voice:**

  A Service Provider may send re-INVITE requests to the OpenScape Voice server with and without SDP. A Service Provider may send a REFER request to the OpenScape Voice server to initiate a call transfer if the OpenScape Voice server has been configured to accept REFER requests from the Service Provider.
- **Service Provider receives requests and responses from OpenScape Voice:**

  No requirements.

- **Transfer Target behavior**

  The OpenScape Voice server should be able to perform the role of a transfer target.

- **Transferee behavior**

  The OpenScape Voice server should be able to perform the role of a transferee.

7.5.10 Call Pick-up

Call Pick-up allows subscribers to answer any ringing or camped-on station within the business group.

7.5.11 Call Diversion

Call Diversion is the change of the destination of a call.

There is a wide range of call diversion types available. Examples are Call Diversion Unconditional, Call Diversion on No Reply, Call Diversion on Busy, Call Diversion on Not Logged-In.

Requirements

- **Enterprise diverts call to Service Provider:**

  The Enterprise system MUST be able to divert a call to a Service Provider.

  – Enterprise sends requests and responses to Service Provider:

    The Enterprise system MUST be able to send an INVITE request which contains a Diversion header field with the URI of the diverting party as well as the diversion reason. Furthermore, sending a P-Asserted-Identity header field with the identity of the calling party SHOULD be supported in order to allow updating the client display.

  – Enterprise receives requests and responses from Service Provider:

    No requirements

  – Service Provider sends requests and responses to Enterprise:

    No requirements

  – Service Provider receives requests and responses from Enterprise:

    The Service provider SHOULD be able to process a received INVITE request containing a Diversion header field.

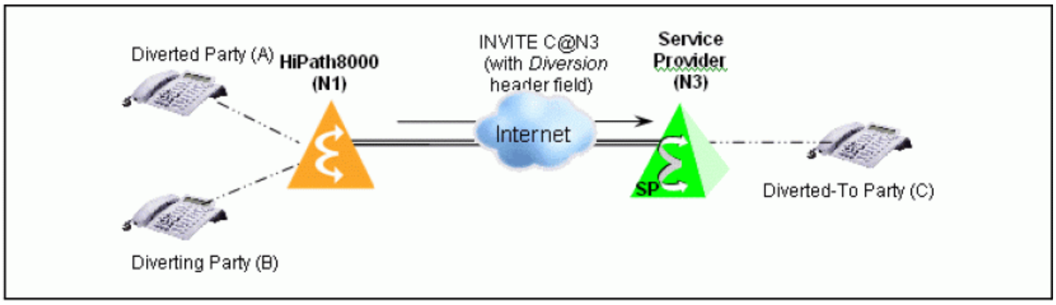
- **Service Provider diverts call to Enterprise:**

  The Service Provider MAY support diverting calls to the Enterprise system or MAY pass diverted calls to the Enterprise system.

  NOTICE:

  Currently no support for actively diverting calls to the Enterprise system using the Diversion header field is available from any Service Provider. Therefore, for the Enterprise system this diverted call is just like a new incoming call.

The following image depicts a call diversion scenario where the Diversion destination is at the Service Provider side:



Description: The calling party A@N1 calls the diverting party B@N2. This call gets diverted to C@N3, for example, due to a received indication from the client or due to a configured call diversion within the Enterprise system, by sending a new INVITE request to the diverted-to destination at the Service Provider side. This new INVITE request may contain a Diversion header field which indicates that this call is a diverted call.

7.5.12 MWI (Message Waiting Indication)

MWI (Message Waiting Indication) is an indication that is rendered on the phone, to inform the user that a message is waiting. This indication involves typically a display indication, an acoustic indication or a lamp on the phone.

Requirements

- **MWI Supplier:**

  Message Waiting Indication (MWI) is an indication that is rendered on the phone, to inform the user that a message is waiting. This indication involves typically a display indication, an acoustic indication or a lamp on the phone.

  An MWI supplier may be within the OpenScape Voice server or at a Service Provider.

  – **OpenScape Voice or Service Provider send requests and responses:**

    If a SSNE is acting as a MWI supplier for subscribers then the SSNE should support the message-summary event package.

    In case the client needs to be notified about a received message (for example when the message count has changed), the SSNE should send a NOTIFY request towards the subscriber including a message-summary event including the following header fields: a Contact header field with the URI of the Media Server, an Event header field with a value of message-summary, a Subscription-State header field with a value of active, and the Content-Type header field with a value of application/simple-message-summary. Details on the event package can be found in RFC3842.

  – **OpenScape Voice or Service Provider receive requests and responses from SSNE:**

    Sending SUBSCRIBE requests for MWI notification is not supported, that is the SSNE will send unsolicited NOTIFY requests as a MWI Supplier.

- **MWI Consumer:**

  An SSNE, acting as a consumer for message waiting notifications, is usually connected to a client that provides a display or a lamp in order to indicate to the user that messages have been stored which can be retrieved by the user.

- **OpenScape Voice or Service Provider send requests and responses to SSNE:**

  The MWI Consumer expects the MWI supplier to support the message-summary event package with implicit subscriptions, that is MWI Consumer does not send SUBSCRIBE requests to the MWI Supplier.

- **OpenScape Voice or Service Provider receive requests and responses from SSNE:**

  An SSNE should support processing a received NOTIFY request containing a message-summary event, if it has an implicit agreement with the MWI supplier that this event is understood.

7.5.13 CCBS (Call Completion to Busy Subscriber) and CCNR (Call Completion to No Replay)

The CCBS (Call Completion to Busy Subscriber) and CCNR (Call Completion on No Reply) features allow a calling subscriber to be automatically connected to a busy or no reply called subscriber when that subscriber becomes available..

The OpenScape Voice implementation is based on the ETSI TISPAN recommendation and uses the “ccbs” and “ccnr” event packages.

7.5.14 3PCC (Third Party Call Control)

3PCC (Third Party Call Control) can be used by OpenScape Voice applications to generate and manipulate calls. These 3PCC generated calls may be calls routed via a SIP Service Provider.

Requirements

In order to support 3PCC the SIP Service Provider must support the procedures described in RFC3725. In particular, the Service Provider must be able to support at least Flow I of RFC 3725 (in fact, accept a SIP INVITE request that does not include an SDP offer and be able to support the SDP offer/answer exchange via the SIP 200 OK and ACK messages).

8 Security

8.1 Event Logging

The security event logging feature permits OpenScape Voice to record security administration actions and OAM&P (Operation, Administration, Maintenance and Provisioning) activity originated over CLI (Command Line Interface), SNMP (Simple Network Management Protocol), SOAP/CLI or SOAP/XML interfaces to OpenScape Voice. It also records OS-level CLI activity.

This feature provides:

- The ability to track down system abusers and hackers that may be involved in system and network intrusions, interruptions, damage and unauthorized configuration changes - for example, to disrupt service or enable toll fraud.
- The ability to investigate recent security-related activity such as the following:
  - Changes to security attributes, services, and access controls such as successful and unsuccessful changes to user IDs and passwords; and successful and unsuccessful login attempts, logouts, or session termination (either local or remote) via the security audit trail
  - Recent non-security related OAM&P activity via the recent change log

This security event log is different from, and is kept completely separate from, the system event log, which logs abnormal runtime activity.

System Specific Information

The security log files are rotated on a daily basis. Archived security log files for the previous 30 days are retained; files older than 30 days are automatically removed.

Although the active security event log files are not encrypted, they are accessible only to CLI users who have the proper authorization. However, these files will be archived to long-term storage as an encrypted file.

SFTP (using IPsec) is used for the secure transfer of the log file data from OpenScape Voice.

8.1.1 Event Log File Data

The general contents of an event log file are described here.

For both the security audit trail and recent change log, each event log entry contains the following information:

- A description of the event or action that is being logged—for example, a password reset, a dialing plan modification, or the creation of a new subscriber.
- The identity and security level of the user or process that initiated the event or action.
- The date and time the event or action occurred. The timestamp is based on the local time zone of the OpenScape Voice server.

- Identity of the system files or resource, system parameter, network element, device or user ID that the event or action impacts. This includes attempts to access files or resources outside of the user's privileges.
- An indication of whether the event or action was successfully implemented.

Although the active security event log files are not encrypted, they are accessible only to OpenScape Voice Assistant users who have the proper authorization. However, after the data is transferred to the OpenScape Voice Assistant, the file will be archived to long-term storage as an encrypted file.

8.1.2 Access to Event Log Data

Event log data are stored in different log files which can be accessed via the OpenScape Voice Assistant.

The following log files provide access to event log data:

- `RtpSecEvtAudit` logs OpenScape Voice application-level security audit events
- `RtpSecEvtChange` logs recent change messages.

These can be displayed using OpenScape Voice Assistant. In addition, these two OpenScape Voice logs, along with the OS-level syslog or LAuS log files, can be displayed and analyzed with commercial syslog tools. Logs associated with the integrated OpenScape Voice must be displayed and analyzed in this manner.

Each file type has a current file and up to 20 days’ worth of archive files associated with it.

FTP (using IPSec) is used for the secure transfer of the log file data from the OpenScape Voice to OpenScape Voice Assistant.

8.1.3 Recent Change Log

The recent change log records all OAM&P (Operation, Administration, Maintenance and Provisioning) activity whether successful or unsuccessful.

It provides the following information:

- Changes to system resources, system parameters, network elements, and end-user devices
- Provisioning commands
- Commands that retrieve customer data
- Data synchronization commands
- Data or network element recovery commands

Also known as Security Event Logging, this functionality allows the recording (in a log file) of all provisioning activities that are performed on the OpenScape Voice system.

8.1.4 Security Audit Trail

The security audit trail supports logging capabilities based on ANSI T1.276-2003 and Telcordia GR-815-CORE.

It provides the following information:

- Any action that changes the security attributes and services, access controls, and other configuration parameters of each network element and management system that is part of the OpenScape Voice infrastructure
- Logins attempts, regardless of their success
- Logouts or session termination, whether local or remote
- Critical security administration actions, both successful and unsuccessful, such as actions affecting user IDs, login passwords, IKE (Internet Key Exchange) pre-shared keys for IPsec, and other security-related system characteristics

  Logging of both OS- and application-level critical security administration activity is performed.

8.1.5 Recent Change Logging in a SOAP Server

Whenever a SOAP (Simple Object Access Protocol) request is received that involves the creation, deletion, modification, or retrieval (e.g., for display/view) of data on the OpenScape Voice system, the Event Logging API function RtpSecEvtSendChangeLogEvent provided by RTP (Real-Time Transport Protocol) is called to log the event.

8.1.6 Recent Change Logging in SOAP Mass Provisioning and SOAP Export

For SOAP (Simple Object Access Protocol) Mass Provisioning, the comma separated string representing the input mass provisioning command from the input file is logged. For SOAP Export, the operation performed is always the retrieving of data and thus the name of the operation is logged with the generic name "soapExport".

The identity of the objects being exported are as specified in the input command. The entire string entered by the operator to execute the command is logged, including all arguments passed to the application, identified explicitly with the name and the value, to describe with detail the operation being performed. defined by the operator (eg: the Start DN; the BG Name, etc.). In the case of exporting a list of DNs (Directory Numbers), the resource logged will be the one given by the -Start DN argument.

NOTICE:

As a result of Event Logging requirements, both SOAP Export and SOAP Mass Provisioning are invoked from within the RTP CLI (Command Line Interface) Expert Mode.

It is still possible to invoke both executables from the command line for testing purposes. This is expected to be used only internally and requires knowledge of a password defined in an RTP parameter that is not customer-accessible.

8.2 Provisioning and Security Logging

The provisioning and security logging feature provides the ability to log all activities and commands in a log file to assist in detecting hacker and access violations.

Alarm reports are generated according to ITU-T (International Telecommunications Union-Telecommunications) Recommendation X.736, *Systems Management: Security Alarm Reporting Function*.

Provisioning and security events can be logged using the log control function of OpenScape Voice Assistant, according to ITU-T Recommendation X.735, *Systems Management: Log Control Function*.

8.2.1 Community Strings

Community strings are like passwords that are used by SNMP. If using the wellknown community string “public” is not desirable, the system administrator can modify the community strings when creating an SNMP configuration. Refer to the OpenScape Voice Installation and Upgrades Guide for instructions to change the SNMP community name string from “public” to meet the site’s security requirements.

8.3 SIP Privacy Mechanism

OpenScape Voice provides SIP privacy capabilities according to IETF RFC 3323, *A Privacy Mechanism for SIP*.

The following features are supported:

- Guidelines for the creation of messages that do not divulge personal identity information
- A privacy service logical role for intermediaries to handle some privacy requirements that user agents cannot satisfy themselves
- Means by which a user can request particular functions from a privacy service

Digest authentication is used to permit a user to hide identity and related personal information when issuing requests. Correspondingly, intermediaries and designated recipients of requests can reject requests whose originator cannot be identified.

In SIP, identity is most commonly carried in the form of a SIP URI and an optional display-name. A SIP AOR (Address of Record) has a form similar to an E-mail address with a SIP URI scheme (for example, sip:alice@atlanta.com). A display-name is a string that contains a name for the identified user (for example, "Alice"). SIP identities of this form commonly appear in the To and From header fields of SIP requests and responses. Users can have many identities that they use in different contexts.

There are numerous other places in SIP messages in which identity-related information can be revealed. For example, the Contact header field contains a SIP URI, one that is commonly as revealing as the address-of-record in the From. In some headers, the originating user agent can conceal identity information as a matter of local policy without affecting the operation of the SIP. However, certain headers are used in the routing of subsequent messages in a dialog, and must therefore be populated with functional data.

The privacy problem is further complicated by proxy servers (also known as intermediaries or, generically, the network) that add headers of their own, such as the Record-Route and Via headers. Information in these headers might inadvertently reveal something about the originator of a message — for example, a Via header might reveal the service provider through whom the user sends requests, which might in turn strongly hint at the user's identity to some recipients. For these reasons, the participation of intermediaries is also crucial to providing privacy in SIP.

8.3.1 SDP (Session Description Protocol) Backward Compatibility for Best Effort SRTP (Secure Real-Time Transport Protocol)

OpenScape Voice supports securing of RTP (Real Time Transport Protocol) calls via SRTP (Secure Real-Time Transport Protocol) using MIKEY (Multimedia Internet Keying) Option 0. The mechanism defined, follows a standards based approach and allows for backward compatibility. There are defined provisions for a SIP end point to reject the SRTP offer if it does not support this mechanism. But certain 3rd party end points fail in the SDP (Session Description Protocol) negotiation and as a result the call setup fails. This feature provides a solution to identify such cases and support a mechanism that will allow for the call setup to succeed between an end point that originates an SRTP offer and an end point that does not comply with the provisions for rejecting such an offer.

The MIKEY keys for payload encryption are negotiated during the SDP offer-answer exchange. The procedure for exchanging the MIKEY keys is followed in accordance with the best effort SRTP mechanism defined in the OSCAR Signaling and Payload Encryption Specification. This mechanism is supported by certain Unify SIP EPs (Endpoints).

Functional Sequence

The administrator controls the determination of the best effort SRTP capabilities of devices via an RTP parameter displayed and modifiable via the OpenScape Voice Assistant.

The administrator is able to switch ON, OFF and AUTO function this feature. If the feature is turned OFF, SIPSM (SIP Signaling Manager) will not check B-side's capabilities to determine to send SRTP. At the same time SIP Registrar functionality will not be changed even if the feature is turned OFF. This allows for fast toggling of the feature in case a administrator needs to quickly turn off the feature because of problems with it.

The administrator is able to add other devices that may not support the mechanism and if they are now part of the solution spectrum of the OpenScape Voice. This allows for fast solutions of problems in the field when a device is discovered to cause problems when it gets offered best effort SRTP.

If the terminating SIP device does not support OSCAR Best Effort SRTP approach, the OpenScape Voice server will remove the SRTP related attributes from the SDP offer before send it to the terminating side. Such a mechanism will ensure that the terminating side need not deal with the SRTP negotiation mechanism and instead can negotiate the call to an unsecured mode.

The secure keys are exchanged within the SDP offer/answer exchange facilitated via the SIP signaling the key exchange to only those devices that do support the mechanism or which behave in a standards conformant manner.

The OpenScape Voice system will be pre-configured during installation with a list of devices that are known to have problems with OSCAR SRTP mechanism. This list is used in case of AUTO feature.

These devices would be displayed on the OpenScape Voice Assistant on the configuration for the SIP Signaling Manager.

System Specific Information

Unify SIP devices, that support establishing secure calls via SRTP, do so by exchanging secure keys between the originating and the terminating side end points.

The mechanism for SDP negotiation provided in this feature allows Unify Endpoints enabled for SRTP to successfully negotiate a call with a 3rd party SIP end point that does not support the Unify best effort SRTP mechanism. Such a call would be setup as an unsecured call.

Other Characteristics

The list of device types can change during run time, it is upgraded automatically. The SIP Registrar has to request update notifications from RTP to be informed about these changes and act upon it.

8.4 Defending DOS (Denial of Service) Attacks

This feature provides the capability to provide protection from SIP-based DOS (Denial of Service) attacks. This protection is in addition to the network-level protection against general DOS attacks.

A SIP-based DOS attack consists of a large volume of SIP messages from a hostile user.

The main defense against DOS attacks is provided by the network design. In addition, border gateway elements, SBCs (Session Border Controllers), and VoIP firewalls can be used to control the volume of VoIP traffic to protect against a SIP-based DOS attack.

Functional Operation

A host-based IDS (Intrusion Detection System) monitors incoming traffic in parallel to the traffic being sent to normal application processing. When incoming traffic from an IP address exceeds the provisioned threshold, all traffic from that IP address is placed on a black list, and is temporarily blocked.

The black list operates as follows:

1) A rule is created in the internal firewall that blocks all traffic from that IP address.

2) After the block period expires, the rule for that IP address is automatically removed from the internal firewall.

The following administrable options permit the system administrator to customize the DoS defense mechanism thresholds and values:

- Rate Threshold: This threshold is used for most traffic. This value is generally a low threshold for end-user traffic.
- Trusted Hosts Exception List: This threshold is used for specific IP addresses that are exempt from rate monitoring. This exception list is generally used for servers that have higher volumes of traffic.
- Block Period: This value specifies the duration the temporary firewall rule is in place to block traffic from a blacklisted IP address.

This feature also provides alarms when the system starts discarding messages due to DOS message filtering.

8.4.1 Spam over Internet Telephony Protection

Due to the general architecture of Internet Telephony a protection concept to avoid spam over Internet Telephony is necessary.

A common misconception is that VoIP systems are more vulnerable to receiving SPIT than non-VoIP systems, but this is not true. SPIT leverages VoIP on the sending side, not the receiving side, because VoIP allows SPIT senders to “power-spam” any telephone number including POTS destinations.

The current best practice for preventing SPIT in a VoIP system is to enforce device authentication and authorization of user endpoint devices, and to provide limiting of excessive call traffic from a single source. OpenScape Voice provides multiple layers of defense against SPIT. Unify SIP phones (OpenScape Desk CP) provides for IEEE 802.1x layer-2 authentication to the customer’s network, which allows an 802.1x-capable LAN switch to enforce an access control policy against the device. The OpenScape Voice system then applies SIP Digest Authentication to prevent against registration hacking, malicious impersonation and unauthorized access to the telephone environment. OpenScape Voice also supports built-in traffic rate monitoring and limiting to protect against a single source from generating excessive call traffic. Furthermore, OpenScape Voice employs network-based calling party identification (P-Asserted ID) to prevent against caller ID spoofing, so that the called user can positively identify the caller.

8.5 Virus Protection

Unify software delivery process protects the integrity of software running on the 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 OpenScape Voice software.

Those protection mechanisms include:

- 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 to the network in general.

8.5.1 File Authentication and Integrity Protection Mechanisms

All files delivered to a service provider or customer, including third-party files, are protected by secure authentication and integrity protection mechanisms, such as digital signatures or symmetric message authentication, that assure that the files received are exactly the files that Unify produced. The installation procedure for all releases, upgrades, patches, etc., includes mechanisms to authenticate the delivered files.

8.5.2 Recommendation on the use of Anti-Virus Scanners

Unify has tested the OpenScape Voice server with various anti-virus scanner products. Unify strongly advises against running an anti-virus scanner of other intrusion detection system on the OpenScape Voice server itself. The following are the reasons for this:

- Although the server is already a low-profile target for viruses, worms and other intruders because it is Linux-based and not Windows-based, its firewall configurations and carefully controlled administrative access minimize its susceptibility.
- Running such scanners can cause a significant increase in server CPU usage, invalidating other capacity calculations. A corporate policy that requires virus scanners on all computers is probably not appropriate to enforce on this type of specialized server; it is recommended that a waiver be sought from such a policy.

Instead, it is more appropriate to scan the software prior to installation and make use of an IDS (such as Tripwire) to monitor the server for changes to the critical files.

8.6 VLAN Provisioning

The VLAN provisioning feature gives administrators the flexibility to provision the IP addresses and interfaces according to enterprise-specific requirements.

This allows, for example, to separate administration-related and billing-related traffic and route them across different ethernet interfaces.

8.7 Data File Security

The security for data files feature protects access to data files by extensive password procedures.

The following password procedures are available:

- During password entry, the password display is suppressed.
- One-way encryption for different file groups.
- Suppression of secret log-in parts within session script (protocol) files.
- Restoration of all file group passwords after recovery or software upgrade.

Each file group can be administered by different attributes and different password groups defining the access modes (e.g. guest, administrator and user).

8.8 File Transfer Security

The File Transfer Security feature provides security mechanisms for the transfer of CDR (Call Detail Record) files or traffic measurement data files.

The initiation of the transfer can be started either by the billing mediation server or the OpenScape Voice server. However, it is preferable for the OpenScape Voice Server to do so.

The OpenScape Voice provides file transfer capability via TCP/IP using FTP, which is based on IETF (Internet Engineering Task Force) RFC 959, FTP.

The following security mechanisms for FTP file transfer are provided.

- FTP authentication

  When a remote user or remote application opens an FTP session, it has to transfer the user ID and password for system access control. The validity of these parameters is checked by the authentication procedure.
- File security

  For each action affecting the file system, the User ID transferred with the authentication procedure is used to check the authority to access each specified file.

NOTICE:

The integrated OpenScape Voice system uses the internal (as opposed to external) Open Scape Voice Assistant. Because of this, it does not use FTP to access data.

8.8.1 FTP Security Options

The file transfer via FTP uses the access control and confidentiality security options of the FTP.

FTP is disabled by default by the OpenScape Voice security policy. However, FTP can be enabled on the billing and management subnets for specific interface partners.

The supported FTP confidentiality options vary by interface and include the following:

- External OpenScape Voice Assistant

  FTP transfers may be protected via IPSec (Internet Protocol Security).

- Basic traffic tool

  SFTP (Secure FTP) is used to securely retrieve data from OpenScape Voice.
- CDR (Call Detail Record) delivery

  If the billing server initiates CDR transfer (als known as file transfer by pull), either FTP or, if the billing server supports it, SFTP (Secure FTP) can be used.
- OS-level FTP for management of the OpenScape Voice Linux servers

  Secure FTP is supported.

8.8.2 Hypertext Transfer Protocol over SSL

Hypertext transfer protocol over SSL (HTTPS) is an extension to HTTP that secures web browser interfaces. There is a server side certificate.

Any authentication with HTTPS is typically done via digest authentication or application-level login.

HTTPS is used to provide security for the following interfaces:

- OpenScape ComAssistant user to CAP/ComAssistant server
- OpenScape UC Application user to OpenScape UC Application server
- OpenScape Voice Assistant web browser client to OpenScape Voice Assistant server (internal or external)

8.8.3 Putty

Remote access to the switches from a client (local machine) is gained using the Command Line Interface (CLI) over SSH Secure Shell. For these purposes the SSH Secure Shell Client software (PuTTY) must be installed on the PC, and the PC must have Ethernet or LAN access to the communication system.

8.8.4 WinSCP

WinSCP allows you to display and query the log files of each individual node (switch) in the system that can be accessed via SFTP.

8.9 Media Encryption

For subscribers who want added network security, the OpenScape Voice server provides SRTP (Secure Real-Time Transport Protocol) as a means to secure its media traffic.

8.9.1 SRTP (Secure Real-Time Transport Protocol) Overview

SRTP (Secure Real-Time Transport Protocol) in the OpenScape Voice solution involves the coordination of SRTP implementation across multiple products.

SRTP provides a framework for encryption and message authentication of RTP (Real-Time Transport Protocol) and RTCP (Real-Time Transport Control Protocol). Media encryption is entirely controlled by the media endpoints; the role of the OpenScape Voice server is only to facilitate the negotiation of encryption parameters between the endpoints.

SRTP sessions are setup through the use of a key management protocol (for example, MIKEY, SDES). For OpenScape Voice solution the preferred key management standard is SDES and certain products such as OpenScape Mobile or various 3rd party products only use SDES for setting up secure communications. However MIKEY#0 is also supported in most of the products and can be used instead.

8.10 Packet Filter Rules Security Management

Packet filtering is used to provide rudimentary firewall protection for OpenScape Voice application software. This mechanism blocks traffic to the OpenScape Voice system, except on those specific IP addresses and ports that are required to be accessible. OpenScape Voice allows for the creating, displaying, and modifying of packet filter rules.

IMPORTANT:

Since Packet Filter Rules are closely related with the security of the OpenScape Voice System the administrator has to be very careful when using the Packet Filter Rules management menu. Only Security Administrator has the permission to access Packet Filter Rules management.

The following table describes the Packet Filter Rules (PFR) Security parameters:

Parameter	Description
Name	Interaction: Read/Create Mandatory field. This parameter indicates the unique Name of each Packet Filtering rule. Maximum length is 63. **NOTICE:** Mandatory field. PFR cannot be created without provision of the Name value. The Packet Filter Rules’ names that start with the "System_" prefix are automatically generated by the system. Security Administrator shall add the prefix "System" in the Name of the autogenerated PFR. **IMPORTANT:** Any change on those Packet Filter Rules should be avoided; otherwise malfunction/damage may be caused to the system.
Description	Interaction: Read/Write This parameter permits a comment describing the rule. Maximum length is 63.
Transport Protocol	This parameter specifies the transport protocol which is used in the transport of packets. Possible values are: • ICMP • UDP • TCP • ALL • ESP • AH • SCTP • ICMPV6 Default value is: ALL .
Direction	This parameter defines the direction of the application of the rule. Possible values are: • Incoming • Outgoing • Both Ways Default value is: Incoming.

Parameter	Description
Action	This parameter specifies whether packets matching the specified rules will be allowed or dropped. Possible values are: • Allow - packets matching the above rules will be allowed. • Drop - packets matching the above rules will be dropped. Default value is: Allow.
Local Alias	Security Manager provides the list of the valid local aliases. For each alias in the list the name, symbolic name and the IP address(es) is(are) provided. In case of a cluster system, a single list with the aliases from both nodes shall be provided. Default value is: ALL.
Local Port Begin	Interaction: Read/Write This parameter specifies the local Port to which the rules are applied. Range of values: 0..65535. The value of 0 indicates all ports. Default value is: 0.
Local Port End	Interaction: Read/Write This parameter specifies the Local port to which the rule is applied. Range of values: 0..65535. If set to 0 then only Local Port Begin is valid. Default value is: 0. **NOTICE:** If the value of this parameter is not greater than Local Port Begin, then the default value should be used.
Remote FQDN (Fully Qualified Domain Name)	Interaction: Read/Write This parameter specifies the Remote FQDN to which the rule applies. Maximum length is 63 characters. **NOTICE:** If the FQDN is specified then the remote IP address and remote subnetmask should not be specified.

Parameter	Description
Remote IP Address	Interaction: Read/Write This parameter specifies the Remote IP to which the rule applies. Valid IP addresses are 1.x.x.x - 223.x.x.x, where each “x” is an integer within the range 0 - 255. Maximum length is 15 (with IPv6 support). **NOTES**: • This parameter is only used if a Fully Qualified Domain Name is not specified. • If the Remote IP Address is set, then Remote Subnet Mask must also be specified.
Remote NetMask	Interaction: Read/Write This parameter specifies the NetMask of the remote host/IP to which this rule applies. 0.0.0.0 and 1.1.1.1 are not valid subnet masks. Default: **255.255.255.255** **NOTICE:** This parameter is only used if a FQDN is not specified.
Remote Port Begin	Interaction: Read/Write This parameter indicates the Remote port to which the rule is applied. Range of values: 0..65535. The value of 0 indicates all ports. Default value is: 0.
Remote Port End	Interaction: Read/Write This parameter indicates the Remote Port to which the rule is applied. Range of values: 0..65535. The value of 0 indicates all ports. Default value is: 0. **NOTICE:** If the value of this parameter is not greater than Remote Port Begin, then the default value should be used.

8.11 IPSec (Internet Protocol Security)

IPSec (Internet Protocol Security) is a security protocol in the network layer that provides cryptographic security services that flexibly support combinations of authentication, integrity, access control, and confidentiality.

OpenScape Voice uses a generic mechanism to provide authentication, integrity, access control, and confidentiality for any server-to-server interface. This implementation makes use of the SLES12 enterprise server.

Usually, IPSec is only configured during installation of the system; a reconfiguration is not required unless the network configuration changes. OpenScape Voice automatically controls the setup of IPSec during system startup.

NOTICE:

Because an incorrect configuration can lead to a total outage of network communication, it is strongly recommended that these tools be used only to monitor the status of the IPSec subsystem.

8.11.1 IPsec Management

The IPSec subsystem is configured during system startup using OpenScape Voice Assistant to configure IPSec rules and profiles.

IPsec-based connections can be created for the following device types:

- OAM&P servers, such as:
  - Common Management Platform
  - External OpenScape Voice Assistant server
- Peer servers, such as:
  - OpenScape UC Application server
  - Billing Server
- External Media Server (MGCP signaling interface)

When provisioning IPsec for a device, the following prerequisites must be created:

- An IPsec profile that describes the IPsec action being performed (Encryption, Authentication or Bypass)
- An IKE profile that describes the parameters used to negotiate between the OpenScape Voice and the remote endpoint

A single IPsec or IKE profile can be shared across multiple devices of different types. It is expected that a few such profiles should be sufficient to describe the required IPsec connectivity for all IPsec-based endpoints.

In addition to the profiles, a pre-shared key is also required and must be specified when assigning an IPsec profile to a device. This key forms the basis for negotiating IPsec connections between the OpenScape Voice and the endpoint.

8.11.2 IPSec (Internet Protocol Security) - Implementation and Usage

Based on the enterprise security policy, IPSec (Internet Protocol Security) can be used between OpenScape Voice and several applications in order to enable secure interfaces.

IPSec can be used between OpenScape Voice and:

- the external OpenScape Voice Assistant or HiPath MetaManagement application to protect the SOAP/SNMP (Simple Network Management Protocol) interface.
- the external media server to protect the MGCP (Media Gateway Control Protocol) interface.
- the OpenScape UC Application server to protect the CSTA III/XML interface.
- the billing server to protect the FTP interface.
- a third-party trusted host or peer server that is not bound to a known OpenScape Voice element type.

The default security policy for the signaling IP addresses is to allow all sources to talk to the OpenScape Voice signaling IP address/port. All ports are blocked for that IP address except the ones required for that signaling protocol.

The default security policy for the management and billing IP addresses is to allow all sources to talk to OpenScape Voice with SSH (Secure Shell). All other ports on the management and billing IP addresses are blocked. As an option, access control can be applied to SSH to restrict which source addresses can log on to the OpenScape Voice secure CLI interface.

Access control is mandatory for FTP, CORBA (Common Object Request Broker Architecture), and SNMP, with or without the use of IPsec.

8.11.3 IPSec (Internet Protocol Security) - Configuration

The OpenSOA-Core framework supports the following deployment scenarios.

- Pure OpenScape Voice

  The entire communication system is operated in a protected subnet and the communication connections need not to be additionally protected.
- Additional autonomous servers

  The additional servers are not necessarily located in a protected subnet and the communication connections between them an the OpenScape Voice system must be protected by a secured tunnel. Such a secured connection can be realized by the IPSec communication protocol.

For more details, please refer to OpenScape Voice Installation and Upgrade Guide Appendix I.

8.11.4 IPSec Profile Management

Once created, the IPSec security profile provides all data required to create an inbound and outbound IPSec policy entry in the Security Policy Database.

NOTICE:

This is an expert level configuration. Default IPSec profiles exist and it is recommended that they are used.

The following table describes the IPSec profile configuration parameters. Default values are in **bold**.

Parameter	Description
Profile Name	Interaction: Read/Create This parameter specifies the unique name of each IPSec entry. The maximum length is 63 characters. This parameter is required for IPSec Profile creation. **NOTE**: Once created, it cannot be modified!
Description	Interaction: Read/Write This parameter specifies a comment (up to 63 characters in length) describing this IPSec Profile.
Protocol	Interaction: Read/Write This parameter specifies the Security protocol to which the IPsec rules apply. Possible values are: • **esp (1)** • `ah (2)` • `espAh (3)` • `None` (this is default if the Packet Control parameter is Bypass) **NOTE**: This parameter cannot be modified after creation. This parameter can only be modified when this IPSec Profile is not attached to any device.
Transport Protocol	Interaction: Read/Write This parameter specifies the transport protocol to which the IPsec rules apply. Possible values are: • `icmp (1)` • `udp (2)` • `tcp (3)` • **all (4)** **NOTE**: This parameter can only be modified when this IPSec Profile is not attached to any device.
Security Mode	Interaction: Read/Write This parameter defines the mode in which IPSec is used. • **transport (1)** **NOTE**: You cannot modify the value of this parameter after creating the IPSec Profile.

Parameter	Description
AH Authentication Algorithm	Interaction: Read/Write This parameter specifies the AH Authentication algorithm used. Possible values are: • `hmacMd5 (1)` • **hmcaShal1 (2)** • `none (3)` (required if you selected ESP (Encapsulating Security Payload) or ESP-AH in the Protocol parameter or if the Packet Control parameter is set to Bypass) **NOTE**: This parameter is only used if you selected AH in the Protocol parameter for this IPSec Profile.
ESP Authentication Algorithm	Interaction: Read/Write This parameter specifies the IPSec ESP Authentication algorithm used by the IKE (Internet Key Exchange) to negotiate a packet authentication algorithm that is used by IPSec. Possible values are: • `hmacMd5 (1)` • **hmcaShal1 (2)** • `None` (required if you selected AH in the Protocol parameter or if the Packet Control parameter is set to Bypass)
Encryption Algorithm	Interaction: Read/Write This parameter specifies which IP ESP Encryption must be used. Possible values are: • `des (1)` • **des3 (2)** • `aes (3)` • `null (4)`
Packet Control	Interaction: Read/Write This parameter confirms the application of the Packet control mechanism. Possible values are: • **apply (1)** • `bypass (2)` **NOTE**: If bypass is selected, then IP security rules are not applied. You cannot modify the value of this parameter after creating the IPSec Profile.

Parameter	Description
Direction	Interaction: Read/Write This parameter defines the direction of the IPSecurity profile. • **bidirectional (1)** **NOTE**: You cannot modify the value of this parameter after creating the IPSec Profile.
Security Association (SA) Life Time	Interaction: Read/Write This parameter specifies the time (in seconds) when the Security expires. Default: **1440** **NOTES**: • This parameter or the SA Life Time in KB parameter is required if Packet control is set to Apply and the key exchange mechanism is either manual or IKE. • In the case of IKE, the value must range from 3 minutes (180 sec) to 24 hours (3640 sec). • For manual keying, the value must range from 180 - 86400, with a default of 3600.
SA Life Time in KB	Interaction: Read/Write This parameter specifies the Kilobytes when the Security expires. Default: **0** **NOTES**: • This parameter or the SA Life Time parameter is required if Packet control is set to Apply and the key exchange mechanism is either manual or IKE. • In the case of IKE, this value cannot be 0 unless the SA Life Time in seconds is greater than 0. • For manual keying, a value of 0 specifies that the Security will not expire.
SubNet Policy Flag	Interaction: Read/Write This flag indicates whether the IPSec Policy is bound to a SubNet. Possible values are: • `on (1)` • `off (2)`

Parameter	Description
SubNet Address	Interaction: Read/Write This parameter indicates to which SubNet address this IPSec policy is bound. Valid IP addresses are 1.x.x.x - 255.x.x.x, where each “x” is an integer within the range 0 - 255. Maximum length is 15. **NOTES**: • You must specify a value for this parameter, if the SubNet Based Policy is enabled (set to ON). • This parameter is valid for MTAs only. • You cannot modify the value of this parameter after creating the IPSec Profile.
SubNet NetMask	Interaction: Read/Write This parameter specifies the subnet mask to which this IPSec Profile is bound. 0.0.0.0 and 1.1.1.1 are not valid subnet masks. Default: **255.255.0.0** **NOTES**: • This parameter is valid for MTAs only. • If Subnet Based Policy is enabled, you must specify a value for this parameter. • You cannot modify the value of this parameter after creating the IPSec Profile.

Parameter	Description
Key Exchange Mechanism	Interaction: Read/Write This parameter specifies the type of key exchange. Possible values are: • Manual — Instead of using IKE for message exchanges to establish the SAs and exchange keys, you provide the keying material and SA information that is necessary for IPSec to communicate. (Anti-replay and on-demand rekeying for phase 2 are not available in manual key management.) **IMPORTANT:** Because a manual key exchange provides less security than an auto key exchange, Key Exchange should be set to manual ONLY FOR THE PURPOSE OF TESTING NETWORK SECURITY. • Auto IKE — IKE is used for message exchanges to establish the SAs and exchange keys. • NOTE: If this parameter is set to Auto IKE, you must assign an IKE Profile when you assign this IPSec Profile. • Auto Kerberos — Kerberos is used for message exchanges to establish the SAs and exchange keys. **NOTE**: If this parameter is set to Auto Kerberos, you must assign a Kerberos Profile when you assign this IPSec Profile. (not used with OpenScape Voice platform) • None — Required if the Packet Control parameter is set to Bypass. If the Packet Control parameter is set to Apply, then this parameter is mandatory. **NOTE**: You cannot modify the value of this parameter after creating the IPSec Profile.

For more details on how to configure IKE profiles please refer to OpenScape Voice Installation and Upgrade Guide, appendix I.

8.11.5 IKE (Internet Key Exchange) Profile Management

In addition to the IPSec security profile providing all data required to create an inbound and outbound IPSec policy entry in the Security Policy Database, it also specifies the underlying key exchange mechanism that will be used for setup of the security associations.

NOTICE:

This is an expert level configuration. Default IKE profiles exist and it is recommended that they are used.

Three types of key exchanges are supported:

- Manual Keys (no key exchange) - keys are specified when associating the profile with a specific device (only applies to Secure End-Points);
- IKE-based Key Exchange - requires an IKE (Internet Key Exchange) profile to be associated with the IPSec profile. Keys are specified when associating the profile with a specific device. The IKE profile specifies IKE-related parameters for use in carrying-out the IKE based key exchange;

The following table describes the IKE Profile Management parameters.

Parameter	Description
Profile Name	Interaction: Read/Create The parameter specifies the unique Name of each IKE entry. Maximum length is 63 characters. This parameter is required for IKE Profile creation. **NOTICE:** Once created, it cannot be modified.
Description	Interaction: Read/Write This parameter allows comments to be input regarding the IKE entry. Maximum length is 63 characters.
Exchange Mode	Interaction: Read/Write This parameter defines the mode in which IKE is used. • `Main (1)` - provides identity protection **NOTICE:** This parameter can only be modified when this IKE Profile is not attached to any device.

Parameter	Description
Authentication Algorithm	Interaction: Read/Write This parameter specifies the IKE Authentication algorithm used. Possible values are: • hmacMd5 (1) • hmacSha1(2) **NOTICE:** This parameter can only be modified when this IKE Profile is not attached to any device.
Encryption Algorithm	Interaction: Read/Write This parameter specifies the IKE Encryption algorithm. Possible values are: • `des (1)` • **des3** (2) **NOTICE:** This parameter can only be modified when this IKE Profile is not attached to any device.
Perfect Forwarding Secrecy	Interaction: Read/Write This parameter specifies whether the perfect forward secret algorithm, which prevents compromising future or past session keys if the current session key has been observed, is enabled or disabled. Possible values are: • Enabled (1) • **Disabled (2)** **NOTICE:** This parameter can only be modified when this IKE Profile is not attached to any device.

Parameter	Description
Authentication Method	Interaction: Read/Write This parameter defines the IKE Authentication algorithm. • preSharedKeys **NOTICE:** This parameter can only be modified when this IKE Profile is not attached to any device.
Oakley Group	Interaction: Read/Write This parameter specifies the Oakley group (Diffie-Hellman group) used for IKE phase 1 negotiation. Possible values are: • group 1 (1) - 768-bit Diffie-Hellman prime modulus group • group 2 (2) - 1,024-bit Diffie-Hellman prime modulus group • group 5 (3) - 1,536-bit Diffie-Hellman prime modulus group **NOTICE:** This parameter can only be modified when this IKE Profile is not attached to any device.
Phase 1 Nonce Length	Interaction: Read/Write An integer which defines the Nonce Length. Possible values are: 8...32. Default: **32** **NOTICE:** If not defined, defaults to a system wide value.
Phase 2 Nonce Length	Interaction: Read/Write An integer which defines the Nonce Length. Possible values are: 8...256. Default: **32** **NOTICE:** If not defined, defaults to a system wide value.

Parameter	Description
ISAKMP Life Time	Interaction: Read/Write This parameter defines the ISAKMP Security Association (SA) Life Time in seconds. A value of 0 signifies that the security will not expire. If not 0, the value must range from 180 sec to 3640 sec. 0..86400 Default: 3600
ISAKMP Life Time KB	Interaction: Read/Write This parameter defines the ISAKMP Security Association (SA) Life Time in kilobytes. A value of 0 signifies that the security will not expire. This value cannot be 0 unless the ISAKMP Life Time Seconds parameter is set greater than 0. Default: **0**
ISAKMP Automatic Reestablish Flag	Interaction: Read/Write This parameter Indicates whether the IKE associations should be re-established after node-failure/reset. Possible values are: • `ON (1)` - connection will be re-established following node status change • `OFF (2)` - first outgoing packet will re-establish IKE connections.
Element Count	Interaction: Read Only This parameter provides the count of elements associated with this IKE profile.

For more details on how to configure IKE profiles please refer to OpenScape Voice Installation and Upgrade Guide, appendix I.

8.11.6 Secure Endpoint Device Security Management

Secure Endpoint Devices are provisioned when a Secure Network Configuration is required. Because all traffic to or from a secure network will only be accepted or transmitted using IPSec, securing the endpoint devices is very important.

NOTICE:

Only IKE (Internet Key Exchange) or manual keying will be allowed for Secure Endpoint objects. If IKE is used then automatic generation of keys or key input will be permitted. If a manual key is to be used then parameters defined in Secure Endpoints will be input.

The following table describes the Secure Endpoint Device Security parameters:

Parameter	Description
Name	Interaction: Read/Create This parameter specifies the unique name of each Secure Endpoint. **NOTICE:** Once you have created a Secure Endpoint, you cannot modify its name.
Description	Interaction: Read/Write This parameter permits the user to write a comment describing the Secure Endpoint.
FQDN (Fully Qualified Domain Name)	Interaction: Read/Write This parameter defines the FQDN of the Secure Endpoint. FQDNs can be of length 1 - 63. **NOTICE:** If the FQDN is specified, then the remote IP address, remote subnet mask, and remote ports should not be specified.
Remote IP Address	Interaction: Read/Write This parameter specifies the IP address of the remote Secure Endpoint. Valid IP addresses are 1.x.x.x - 255.x.x.x, where each “x” is an integer within the range 0 - 255. Do not use leading zeroes in the IP address. **NOTICE:** This parameter is only used if a FQDN is not specified. If the Remote IP Address is set, then Remote Subnet Mask must also be specified.

Parameter	Description
Remote Subnet Mask	Interaction: Read/Write This parameter specifies the Secure Endpoint Remote NetMask for which this security is being applied. 0.0.0.0 and 1.1.1.1 are not valid subnet masks. Default: **255.255.255.255** **NOTICE:** This parameter is only used if a FQDN is not specified.
Remote Port	Interaction: Read/Write This parameter specifies the Secure Endpoint Remote Port for which this security is being applied. 0..65535, default: **0** A value of 0 indicates that the security applies to all ports.
Local Host	Interaction: Read/Write This parameter specifies the Secure Endpoint host to which this security is being applied. Maximum length is 32. **NOTICE:** This string must exist in the /etc/hosts file or this string can be an IP address. Valid Secure Endpoint local IP addresses are 1.x.x.x - 255.x.x.x, where each “x” is an integer within the range 0 - 255. Do not use leading zeroes in the IP address.
Local Port	Interaction: Read/Write This parameter specifies the Secure Endpoint Local Port which the Secure Endpoint attaches to. 0..65535, default: **0** **NOTICE:** A value of 0 indicates that the security applies to all ports.

Parameter	Description
IPSec Profile Name	Interaction: Read/Create This parameter specifies the Secure Endpoint Security Profile Name, which indicates the profile that is attached to the endpoint. **NOTICE:** The IP security profile must have ‘apply’ turned on and the keying mechanism can be either ‘manual’ or ‘IKE’.
IKE Profile Name	Interaction: Read/Write This value is required only if the Key Exchange mechanism is set to IKE and a IPSec Profile is assigned to Secure End Point.
Key General Method	Interaction: Read/Write This parameter indicates whether the IKE key should be generated automatically. • **automatic** • `manual` **NOTICE:** If manual, the key must be entered. Only valid if an IKE profile is associated with this device.
Key Type	Interaction: Read/Write This parameter indicates whether the IKE key type is in HEX or ASCII. • `hex` • **ascii** **NOTICE:** If the Key generation method is manual, then this value must be entered. Only valid if an IKE profile is associated with this device.

Parameter	Description
Preshared Key Length	Interaction: Read/Write (automatic key creation) Read only (manual key creation) This field specifies the length of the key. Possible value in bytes are: 16 - 100 **NOTICE:** You may only specify the length if the pre-shared key is created automatically. If your pre-shared key is created manually, this field is automatically populated in relation to the Context field as follows: • Two characters in HEX = one byte • One character in ASCII = one byte **NOTICE:** This is only applicable if an IKE Profile is associated with this device.
ESP Authentication key Incom	Interaction: Read/Write This parameter specifies the authentication key, which can be 1 - 32 characters long, for inbound ESP encryption. **NOTICE:** This parameter is applicable only if the keying management is manual. If Secure Endpoint ESP Secure Parameter Index Incoming is not set then this parameter is not required. If Secure Endpoint ESP Secure Parameter Index Incoming is set, then either the encryption keys or authentication keys are required.
Incoming ESP Security Parameter Index	Interaction: Read/Write This parameter specifies the security parameter index for inbound ESP encryption. Possible values are: 0 - 4294967295

Parameter	Description
ESP Encryption Key Outgoing	Interaction: Read/Write This parameter specifies the encryption key, which can be 1 - 32 characters long, for outbound ESP encryption. This parameter is applicable only if the keying management is manual. This parameter must be specified if ESP encryption key is defined.
ESP Authentication Key Outgoing	Interaction: Read/Write The parameter specifies the authentication key, which can be 1 - 32 characters long, for outbound ESP encryption. This parameter is applicable only if the keying management is Manual. This parameter must be specified if Secure Endpoint ESP Authentication Key Incoming is specified.
Outgoing ESP Security Parameter Index	Interaction: Read/Write This parameter is applicable only if the keying management is manual. This parameter must be specified if Secure Endpoint ESP Security Parameter Incoming is specified. 0 - 4294967295, default: **4**
Incoming AH Security Parameter Index	Interaction: Read/Write This parameter specifies the security parameter index for inbound AH encryption. Possible values are: 0...4294967295 This parameter is applicable only if the keying management is Manual.
AH Authentication Key Incom	Interaction: Read/Write This parameter specifies the authentication key, which can be 1 - 32 characters long, for inbound AH encryption. This parameter is applicable only if the keying management is Manual. This parameter is required if Secure Endpoint AH 4 Secure Parameter Index Incoming is specified.
AH Authentication Key Outgoing	Interaction: Read/Write This parameter specifies the authentication key, which can be 1 - 32 characters long, for outbound AH encryption. This parameter is applicable only if the keying management is Manual. This parameter is required if Secure Endpoint AH 4 Authentication Key Incoming is specified.
Outgoing AH Security Parameter Index	Interaction: Read/Write This parameter specifies the security parameter index for outbound AH encryption. 0 - 4294967295, default: **4**

8.12 TLS (Transport Layer Security) Support

TLS is an application-independent security protocol defined by the IETF (Internet Engineering Task Force) that provides encryption and data integrity between two communicating applications. TLS (Transport Layer Security) is able to protect SIP signaling messages against loss of integrity, loss of confidentiality, and against replay. It is defined in IETF RFC 2246. The version TLS v1.2 is the default supported one in V10.

8.12.1 TLS (Transport Layer Security) Support - Network Connections

For network connections, the TLS (Transport Layer Security) support feature provides for secure signaling based on TCP and the TLS protocols.

OpenScape Voice optionally supports TLS with mutual authentication to protect the SIP signaling stream between the OpenScape Voice server and other SIP servers. TLS with mutual authentication should be used if the enterprise security policy requires strong authentication and/or encryption of the SIP signaling stream between SIP servers.

TLS with mutual authentication is used to protect a SIP signaling interface between the following:

- Two OpenScape Voice systems to protect the SIP or SIP-Q interface.
- OpenScape Voice and the OpenScape 4000 to protect the SIP-Q interface.
- OpenScape Voice and a third-party trusted host or peer server that is not bound to a known OpenScape Voice element type.
- Optionally instead of IPsec: External OpenScape Voice Assistant and HiPath MetaManagement application to secure OAM&P (Operation, Administration, Maintenance and Provisioning) functions that are performed using SOAP (Simple Object Access Protocol)
- Optionally: Subscriber EP (Endpoint) devices and soft clients (such as OpenScape Desk Phone CP 100/200/205/400/600/600E/700/700X, AP1120 IAD (Integrated Access Device)) to secure the SIP signaling stream
- OpenScape SBC survivable media gateway
- OpenScape SBC survivable media gateway
- OpenScape 4000 gateway
- HiPath 3000 gateway
- Survivable branch offices using OpenScape Branch
- Session border controllers
- Other OpenScape Voice clusters (networked)
- OpenScape Xpressions server for unified messaging

If TLS transport is in use to any SIP phones or endpoints, all endpoints (telephones and softclients) must be configured to register to node 1 of the cluster. This means that the system is operated in an active-standby configuration, with node 1 as the active node and node 2 as the standby node. This operation is distinct from that of an active-active configuration, in which gateways can be configured to register at either node 1 or node 2 during normal operation.

NOTICE: TLS subscribers can register on either node and an endpoints can be connected to the OSV via either node

Server authentication takes place when the TLS connection is established. OpenScape Voice and the interface partner authenticate each other using certificates, which are verified as being valid against a set of pre-stored root certificates.

After authentication is successful, subsequent communication may done over an encrypted connection if confidentiality of the SIP signaling is required. If only strong authentication is required, null encryption is also an alternative.

With mutually authenticated TLS protection of SIP signaling, both interface partners support the role of a TLS client and TLS server. If the TLS connection fails, whichever side detects the failure can re-establish the connection.

8.12.2 TLS (Transport Layer Security) Support - Subscriber Access

For subscriber access, the TLS (Transport Layer Security) support feature provides for secure signaling based on TCP and the TLS protocols.

The IETF’s requirements for SIP signaling, which are defined in IETF RFC 3261, SIP: Session Initiation Protocol, indicate that TLS must be used to provide encryption and data integrity of the SIP signaling stream between proxies, redirect servers, and registrars. OpenScape Voice also optionally supports TLS to protect the SIP signaling stream between OpenScape Voice and SIP endpoints, which is an IETF recommendation but not a requirement. TLS should be used if the enterprise security policy requires encryption of the SIP signaling stream.

If TLS transport is in use to any SIP phones or endpoints, all endpoints (telephones and softclients) must be configured to register to node 1 of the cluster. This means that the system is operated in an active-standby configuration, with node 1 as the active node and node 2 as the standby node. This operation is distinct from that of an active-active configuration, in which approximately half the endpoints register to each of the two nodes during normal operation.

OpenScape Voice supports the following stages of authentication:

- When setting up the TLS connection from the SIP endpoint to OpenScape Voice.
- When responding to a 401 (or 407) challenge from OpenScape Voice in response to any form of a SIP request, such as a SIP REGISTER or SIP INVITE.

Endpoint authentication is performed using HTTP digest authentication over the TLS-secured link. Within a single administrative domain, server authentication takes place when the TLS connection is established. In OpenScape Voice, the SIP server is a proxy with a collocated registrar; because of this, the TLS connection between the SIP endpoint and the server is left open for the duration of the registration.

When TLS is used for SIP endpoint-server communication, a unilateral authentication is performed as part of the TLS handshake. On top of the established TLS connection, the SIP endpoint authenticates towards the server using HTTP digest authentication.

After authentication is successful, subsequent communication is done over an encrypted connection. The SIP endpoint uses this connection to attempt to register with the server (without credentials in the first instance). The user ID and password for HTTP digest authentication are stored in the database of the SIP endpoint device; therefore, the user does not manually supply the ID and password.

With TLS protection of SIP signaling, the SIP telephone takes on the role of a TLS client and OpenScape Voice takes on the role of a TLS server. If the TLS connection fails, the TLS client detects and re-establishes the connection.

8.12.3 TLS (Transport Layer Security) Support - Subscriber Access - Implementation and Usage

The TLS (Transport Layer Security) Support - Subscriber Access Feature can be used in different implementations and scenarios.

The following sections describes different implementation and usage scenarios.

- In addition to TLS, OpenScape Voice also supports TCP and UDP (User Datagram Protocol) as transport layer options for SIP signaling protocols. Therefore, SIP over TCP and SIP over UDP are viable alternatives to SIP over TLS.
- When the SIP URI is used to place a call, it is possible for TLS to be used as the transport protocol by one SIP endpoint and for a different signaling protocol (such as SIP-Q or MGCP (Media Gateway Controller), with or without signaling security) to be used by the other device.
- OpenScape Voice supports TLS on the signaling connection between a SIP endpoint and the SIP signaling manager. Because TLS is applied on a hop-by-hop basis, end-to-end signaling security is achieved only when all hops of the signaling connection use TLS. End-to-end TLS security is not guaranteed if the call leaves the local administrative domain.

> **NOTICE:** An administrative domain is a collection of end systems, intermediate systems, and subnetworks operated by a single organization or administrative authority. In OpenScape Voice, each business group represents a separate administrative domain.

- Nearly all Unify SIP endpoints used with OpenScape Voice support TCP and TLS for SIP signaling transport.

The transport protocol that is used is a configuration option of the SIP endpoint. Other SIP telephones used with OpenScape Voice may only support a subset of this functionality.

8.12.4 CA Certificates and their Usage

CA certificates are used so that their signature can be compared against the CA signature within the certificate being offered by the peer. CA certificates can be stored either all within one file or as separate files.

- If the CA certificates are stored within one file, the file must use the following format:

  ```
  ----BEGIN CERTIFICATE----
  ... (CA certificate in base64 encoding) ...
  ---- END CERTIFICATE ---
  ```
- If certificates are stored in one file TTUD will have to be restarted when a new certificate is added to the file. The default file, `rootcert.pem`, contains the root CA certificate for the OpenScape Voice Server. It can used by peers within the network.
- If CA certificates are stored in separate files they should be stored in the directory using the following RTP parameters:

  ```
  SSL/EndPoint/Server/CertificatesPath
  SSL/MutualAuth/Server/CertificatesPath
  SSL/MutualAuth/Client/CertificatesPath
  ```

  The directory used depends on the type of peer that the certificate is coming from. The RTP parameters above can point to the same directory.

8.12.5 Transparency of Features and Services

Features and services on OpenScape Voice are transparent to the node to which the EP (Endpoint) has a TLS (Transport Layer Security) connection. This allows the EPs to be registered across two nodes in a load sharing arrangement.

8.12.6 PAM Framework

Important topics of PAM framework are described here.

The enforcement of the user account and password settings is done using PAM framework configuration files located in the /etc/pam.d directory which are password-related—login, passwd, sshd, and su. The configuration of these files specifies the default behavior for all applications that manipulate the password.

The table below lists and describes the PAM password default settings.

IMPORTANT:

The arguments that appear in **bold text** must not be changed.

Table 200: PAM Password Default Settings

Module Type	Module Flag	Module Name	Arguments

password	requisite	pam_passwd_mgmt.so	**ask_oldauthtok=update check_oldauthtok**
			pw_iteration_nr=5
			passphrase=0
			enforce=users
			pw_iteration_length=180 min=disable, disable, disabled,8,8
			random=0

password	requisite	pam_pwcheck.so	Configuration parameters are in / etc/ security/ pam_pwcheck.conf.

8.12.6.1 Password Rules and Aging Management

The parameters for password rules and aging management are described here.

Password Rules

Password rules are globally enforced using custom PAM module `pam_passwd_mgmt.so` in /lib/security.

This module checks password strength for PAM-aware password changing programs, such as passwd. In addition to checking regular passwords, it offers support for password history and pass phrases, and can provide randomly generated passwords. All features are optional and can be reconfigured without rebuilding.

There are a number of supported parameters which can be used to modify the behavior of pam_passwd_mgmt. The table below lists and describes each; defaults are in brackets.

Table 201: Parameters to Modify Behavior of pam_passwd_mgmt

Parameter	Description
`min=N0,N1,N2,N3,N4`	This parameter sets the minimum allowed password lengths for different kinds of passwords and pass phrases. The keyword "disabled" can be used to disallow passwords of a given kind regardless of their length. Each subsequent number is required to be no larger than the preceding one. • N0 is used for passwords consisting of characters from one character class only. The character classes are digits, lowercase letters, uppercase letters, and other characters. There is also a special class for non-ASCII characters, which cannot be classified, but are assumed non-digits. • N1 is used for passwords consisting of characters from two character classes, which do not meet the requirements for a pass phrase. • N2 is used for pass phrases. A pass phrase must consist of sufficient words (see the "pass phrase" option below). • N3 is used for passwords consisting of characters from three character classes. • N4 is used for passwords consisting of characters from four character classes. Default: `[min=disabled,24,12,8,7]` When calculating the number of character classes, uppercase letters used as the first character and digits used as the last character of a password are not counted. In addition to being long enough, passwords are required to contain: • Enough different characters for the character classes • The minimum length they have been checked against

Parameter	Description
`max=N`	This parameter sets the maximum allowed password length. This can be used to prevent users from setting passwords which may be too long for some system services. Default: `[max=40]` The value 8 is treated differently. With `max=8`, passwords longer than 8 characters are not rejected, but are truncated to 8 characters for the strength checks; the user will be warned. This is to be used with the traditional DES-based password hashes, which truncate the password at 8 characters. It is important that `max=8` be set if traditional hashes are used; otherwise, some weak passwords pass the checks. Stronger encryption algorithms, such as MD5 or Blowfish, are available by changing the default password encryption algorithm in /etc/security/policy.conf. With the stronger password encryption algorithm, password longer then 8 characters are not truncated. For example, to use Blowfish as the password encryption algorithm set the variable `CRYPT_DEFAULT=2a` in /etc/security/policy.conf.
`passphrase=N`	This parameter sets the number of words required for a pass phrase, or 0 to disable the support for pass phrases. Default: `[passphrase=3]`
`match=N`	This parameter sets the length of common substring required to conclude that a password is at least partially based on information found in a character string, or 0 to disable the substring search. Note that the password is not rejected if a weak substring is found; it is instead subjected to the usual strength requirements with the weak substring removed. The substring search is caseinsensitive, and is able to detect and remove a common substring spelled backwards. Default: `[match=4]`

Parameter	Description
`similar=permit|deny`	This parameter specifies whether a new password can be similar to the old one. The passwords are considered to be similar when there is a sufficiently long common substring and the new password with the substring removed would be weak. Default: `[similar=deny]`
`random=N[,only]`	This parameter sets the size of randomly generated passwords in bits, or 0 to disable this feature. Passwords that contain the offered randomly-generated string are allowed regardless of other possible restrictions. Default: `[random=42]` The `only` modifier can be used to disallow user-chosen passwords.
`enforce=none|users|everyone`	This parameter permits the module to be configured to warn of weak passwords only, but not actually enforce strong passwords. The users setting enforces strong passwords for invocations by non-root users only. Default: `[enforce=everyone]`
`non-unix`	This parameter enables and disables use of getpwnam(3) to obtain the user's personal login information and use that during the password strength checks. Default: `non-unix[]`
`retry=N`	This parameter sets the number of times the module requests a new password if the user fails to provide a sufficiently strong password and enter it twice the first time. Default: `[retry=3]`
`ask_oldauthtok=update|[]`	Ask for the old password as well. Normally, pam_passwd_mgmt leaves this task for subsequent modules. With no argument, the "ask_oldauthtok" option will cause pam_passwd_mgmt to ask for the old password during the preliminary check phase. With "ask_oldauthtok=update", pam_passwd_mgmt will do that during the update phase. Default: `[ask_oldauthtok=update]`

Parameter	Description
`check_oldauthtok []`	This tells pam_passwd_mgmt to validate the old password before giving a new password prompt. Normally, this task is left for subsequent modules. The primary use for this option is when "ask_oldauthtok=update" is also specified, in which case no other module gets a chance to ask for and validate the password. Of course, this will only work with Unix passwords. Default: `check_oldauthtok[]`

`use_first_pass []`
`use_authtok []`
	Use the new password obtained by modules stacked before pam_passwd_mgmt.
	This disables user interaction within pam_passwd_mgmt. With this module, the only difference between "use_first_pass" and "use_authtok" is that the former is incompatible with "ask_oldauthtok".
	Default: `use_first_pass [], use_authtok []`

`pw_iteration_nr=N`	This parameter remembers the last `N` number of passwords and does not allow the user to use it again for the next N password changes. `N` is a number between 1 and 400. Default: `[pw_iteration_nr=5]`
`pw_iteration_length=N`	This parameter is the length in N days during which the password cannot be reused. N is number between 180 and 3650. Default: `[pw_iteration_length=180]`

Password Aging

Password aging rules are globally enforced by one of the following methods:

- By accepting the defaults for accounts creation in /etc/login.defs, which indicate the password aging controls (used by useradd) listed in the table below.

Table 202: Password Aging Control Parameters in /etc/login.defs

Parameter	Description
`PASS_MAX_DAYS=90`	This parameter specifies the maximum number of days a password may be used. Default: `PASS_MAX_DAYS=90`
`PASS_MIN_DAYS=1`	This parameter specifies the minimum number of days allowed between password changes. Default: `PASS_MIN_DAYS=1`

Parameter	Description
`PASS_WARN_AGE=7`	This parameter specifies the number of days' warning given before a password expires. Default: `PASS_WARN_AGE=7`
`PASS_MIN_LEN=8`	This parameter specifies the minimum length of a password. Default: `PASS_MIN_DAYS=8`

Additionally, the following command must be executed to require the user to change the password upon initial logon:

```
change -d 0 <username>
```

- By using the passwd command, as follows:

  ```
  Passwd -x 90 -n 1 -w 14 -i 30 <username>
  ```

  In this command:

  – `-x` sets the maximum number of days before the expiration.
  – `-n` sets the minimum number of days before the next change.
  – `-w` sets the number of days of warning days before the expiration.
  – `-i` sets the login grace period after password expired before the account is locked.

Enforcing root password aging and expiration requires the `AGE_ROOT` parameter in **/etc/security/pam_login_auth.conf** to be enabled. When this parameter is enabled, the root user is prompted to change the password when it expires. However, it is recommended that this parameter be disabled.

IMPORTANT:

Expiration of the root password does not lock the account. However, allowing it to expire breaks the public key-based internode access until a new password is specified.

8.12.6.2 Systemwide Login Configuration Parameters Management

Important topics of systemwide login configuration parameters are described here.

Systemwide login configuration parameters are globally enforced by using the custom PAM module `pam_login_auth.so` in `/lib/security`.

The file `/etc/security/pam_login_auth.conf` contains systemwide login configuration parameters which can be used to modify the behavior of user accounts. This file is write-protected and can only be read or modified by root.

The values configured in this file can be overwritten by inline parameters for `pam_login_auth.so` for specific services.

The table below lists and describes the parameters which can be used to manage global rules that apply to user accounts; defaults are in brackets.

Table 203: Systemwide Login Configuration Parameters

Parameter	Description
`AGE_ROOT`	This parameter enables and disables root password aging. To turn it on, remove the leading #. If the # remains, it is turned off. Default: `[#AGE_ROOT]`
`DEBUG`	This parameter turns on and off debugging statements in syslog. To turn it on, remove the leading #. If the # remains, it is turned off. Default: `[#DEBUG]`
`MAX_SESSIONS=6`	This parameter specifies the maximum number of simultaneous sessions for the same login name, with a valid range of 1 to 99 sessions. Default: `[MAX_SESSIONS=6]`

8.12.6.3 User Login Management

The parameters of the user login management are described here.

The `admin_login_auth` command allows an administrator to examine, set, and clear the count of unsuccessful login attempts. This command is also used to disable or lock out specified users.

```
admin_login_auth: Usage: [-f file] [-s count] [-o
dormant_days]
```

```
[-a alert_days] [-e delete_days] [-c] [-d] [-r] [-v] [-h]
login-name
```

The table below lists and describes the available command options.

NOTICE:

Running the command with no options will print out the contents of the `login_auth_db` file. This allows for an overview of the login attempts for all active users.

One or more users can be specified for options -c, -s, and -d.

Table 204: User Login Management Command Options

Option	Description
`-f file`	This option uses an alternate control file. Without this option the default file `/etc/secure/login_auth_db` is used.
`-s count`	This option sets or resets the count of failed login attempts for the specified accounts. If an attempt is made to set the count greater than the limit, the account is locked on the next login attempt.

Option	Description
-o dormant_days	This optional parameter disables an account after it has been dormant for the specified time. It is generally used with a UNIX cron job.
-e dormant_days (2)	This optional parameter erases an account after it has been dormant for the specified time. It is generally used with a UNIX cron job.
-a alert_days	This optional parameter sends out a system message if an account has been dormant for the specified time. It is generally used with a UNIX cron job.
-e delete_days	This optional parameter erases an account after it has been dormant for the specified time. It is generally used with a UNIX cron job.
-c	This option is used to reset the user accounts. It resets login attempt count, disabled accounts, and locked-out accounts. The login attempt count is normally reset when a successful login occurs.
-d	This option is used to disable the user account. The user account can be enabled with the option -c.
-h	This option is used to display the command line help.
-r	With this option, the program attempts to communicate with “report_account_alarms” to send the event notification to RTP.
-v	This option is used to request verbose mode output. The verbose mode output identifies accounts that have never logged in. Normally these accounts are not included in output of the admin_login_auth command.

The `faillog` command allows an administrator to format the contents of the `/var/ log/faillog` failure log and to maintain failure counts and limits.

```
faillog [-u login-name] [-a] [-t days] [-m max] [-pr]
```

The sequence of the faillog options is significant because each is processed immediately in the specified sequence.

For the system accounts that should not be locked out—for example, srx, cdr, mmgr, and solid—the maximum number of login failures is set to 9999. For example:

```
faillog -u srx -m 9999
```

The table below lists and describes the available command options.

Table 205: Failure Log Management Command Options

Option	Description
-p	This option causes failure entries to be printed in the numeric sequence that corresponds to the login name.

Option	Description
`-u login-name`	This option requests the printing of only the failure record for the specified login name.
`-t days`	This option requests the printing of only the failures that occurred more recently than the specified number of days. This option overrides the user of `-u`.
`-a`	This option causes all users to be selected. When used with the `-p` flag, this option selects all users who have ever had a login failure. It is meaningless with the `-r` flag.
`-r`	This option resets the count of login failures. Write access to `/ var/log/faillog` is required for this option. Entering `-u login-name` causes only the failure count for the specified login name to be reset.
`-m`	This option specifies the maximum number of login failures before the account is disabled. Write access to `/var/log/faillog` is required for this option. • Entering `-m` max causes all accounts to be disabled after the maximum number of failed logins occurs. This may be modified with `-u login-name` to limit this function to login name only. • Selecting a maximum value of 0 has the effect of not placing a limit on the number of failed logins. The maximum failure count should always be 0 for root, in order to prevent a DoS attack against the system.

8.12.7 CLI User Management

The resilient telephony platform (RTP) of the OpenScape Voice server implements its own user management. Creation, modification, and deletion of users, password handling, handling of privileges, and so forth, are completely managed by the management function application programming interface (API). This API also controls the user access to the management functionality (user identification and authorization).

The user management provides the following features:

- Creating, installing, deleting, extending, and modifying of roles.
- Creating, installing, deleting, and modifying of users.
- Getting information on users and roles.
- Getting information about the currently active user sessions.
- Getting information about the currently active management functions for a given user session.
- An option to allow the RTP to use OS authentication of user login. This eliminates the need for a separate RTP user account and login. The RTP still needs to provision users’ RTP permissions for RTP CLI level permissions.
- Linux user account management using pluggable authentication module (PAM) modules for administrable password complexity, aging, reuse, and disable/lockout rules.

The CLI requires a user profile for all users who access the OpenScape Voice. A user with administrator privileges creates the user profiles.

The elements and privileges of a user profile depend on the platform. Table 12 lists the user profile elements.

Table 206: CLI User Profile Elements

Element	Description
User Name	A minimum length of 1 character. Maximum length of 36 characters.
Password	A minimum length of 8 characters. Maximum length of 36 characters.
Privileg	Determines the access a user is granted. The privileges are: • stdop — Read only access. • maxcust — Read/write access. This is the maximum authorization level for clients. • maxint — Read/write access. This is the maximum authorization level for RTP integrators. • super — This is for Unify internal use only.

8.12.7.1 User Privileges and Roles

The user names, roles and privileges described in this section depict those that might by used by a typical customer. Since these attributes are configurable by CLI user management, different user names, roles and privileges may be assigned, as appropriate, for enterprise customers.

The MgmtSession class reads in the list of privileges assigned to the user. By its member function CheckAccess the management classes can verify whether or not the user has access to a particular functionality. Each user is assigned exactly one role containing a list of privileges. Roles can be shared by several users thus making it very efficient to modify the list of privileges for a group of users at once. The RTP has several roles and users pre-installed.

The users, roles and privileges are stored in the following database tables:

- RTP_ADM_USERS
- RTP_ADM_ROLES

Examples for the principle design of these database tables are shown in the tables below.

NOTICE:

At installation time, it is recommended that passwords for predefined user accounts be changed from the default value to a new password that is known only by the appropriate authorized personnel.

Table 207: RTP_ADM_USERS

User	Role	Pass-word	Lock State	Expire Time	Max. Attempts	Max. Inactivity
sysop1	stdop	...	unlocked	Never	3	unlimited
sysop2	stdop	...	unlocked	Never	3	30
sysop3	stdop	...	admlocked	Never	3	30
sysop4	stdop	...	fraudlocked	12/17/1998 10:50:30h	3	30
sysad	maxcust	...	unlocked	11/30/1998 16:17:12h	2	10
intad	maxint	...	unlocked	12/24/1998 18:15:49h	2	unlimited
superad	super	...	unlocked	Never	2	unlimited

Table 208: RTP_ADM_ROLES

Role	Privilege IDs
stdop	UserMgmt_Read, EventMgmt_ReadWrite, AppMgmt_Read, Config_Read
maxcust	UserMgmt_ReadWrite, EventMgmt_ReadWrite, AppMgmt_ReadWrite, Config_ReadWrite
maxint	UserMgmt_ReadWrite, EventMgmt_ReadWrite, AppMgmt_ReadWrite, Config_ReadWrite, IntegratorConfig_ReadWrite
super	UserMgmt_ReadWrite, EventMgmt_ReadWrite, AppMgmt_ReadWrite, Config_ReadWrite, IntegratorConfig_ReadWrite, DeveloperConfig_ReadWrite

Security-related data, such as passwords and the list of privilege IDs is stored in an encrypted way to avoid direct manipulation using low-level database interfaces such as SQL. The RTP_ADM_USERS table not only contains a reference to a role (which is defined in the RTP_ADM_ROLES table) but also the following:

- Information about the LockState (if a user is locked out due to unsuccessful login attempts or explicitly by the system administrator)
- Expiration time of the password (ExpireTime)
- Maximum number of unsuccessful login attempts before the user is locked out implicitly (MaxAttempts)
- Maximum time in minutes without any user activity before the session ends implicitly.

The admin logins and their respective authorization profiles shown in the table below are created in the configuration step of the RTP.

Table 209: Admin Logins and Authorization Profiles

Role	Login	Usage
stdop	sysop1 ... sysop5	Authorization level for a standard administrator of the end customer
maxcust	sysad	Maximum authorization level for end customers
maxint	intad	Maximum authorization level for RTP integrators
super	superad	Unify development use only

The roles and users listed in the table above are defined by default, when the RTP is shipped to the integrator. It is based upon the assumption that the RTP development needs the maximum access to the system (user superad). On the other hand, the system integrator should not be confused by too many details (such configuration parameters that make no sense to be modified by him).

Finally, the end customer (users sysad, sysop1,... sysop5) has even more limited access to configuration parameters. (Although user sysad users sysop1 through sysop5 are not allowed to modify the configuration of the RTP; they have readonly access to most management functions.) It is the responsibility of the person or institution installing an RTP system to assure that only the passwords for the appropriate management logins are given to the system user.

Remote Login Restrictions

Remote root access is disabled except between nodes of a cluster. To perform procedures remotely that require root access, log in as user sysad and then switch to root using the switch user (su-) command.

Root User Restrictions

Some OpenScape Voice scripts requires that root access is enabled. The `PermitRootLogin` parameter in the `/etc/ssh/sshd_config file` is set by default to **Yes**. If access has been denied because the parameter has been changed to **No**, as user root change the parameter to *“PermitRootLogin yes”* in the *sshd_config* file. Restart the sshd daemon with the following command:

```
/etc/init.d/sshd restart.
```

8.12.7.2 Privilege Tree

The privileges as well as the executable functions actually are organized in one common tree structure. Each of the nodes in the tree contains information about a particular privilege, such as `EVENT READ ONLY or CUSTOMER CONFIGURATION PARAMETERS MODIFY`.

Some nodes are also marked as functions; this information is of importance for the user interface components (the local management GUI, or the CLI to the management function API). Those user interface components display to the user the nodes marked as functions (in a menu bar or tool box) as selectable functions. Additional information indicates how to activate the respective function by specifying the name of the Java class. The privilege and function tree structure can be interpreted as structure of categories, functions, subfunctions, subsubfunctions, and so on.

The table below lists the complete function and privilege tree structure (which is assigned to the super role by default). Each element is listed with its textual representation (configuration parameters) and the LocalText object defined in the BasicFunctions class in parentheses (such as CONFIG_PARAM_MGMT). The textual representation is visible in the menu structure of the GUI or CLI menu mode and in the User Management functionality of the GUI and the CLI menu mode.

Table 210: CLI Administrable Permissions

Configuration management	• Customer Configuration Parameters Read Only • Customer Configuration Parameters Modify • Integrator Configuration Parameters Read Only • Integrator Configuration Parameters Modify • Developer Configuration Parameters Read Only • Developer Configuration Parameters Modify • Logging Read Only • Logging Modify • Logging Read Encrypted
Fault management	• Events Read Only • Events Modify • Alarms Read Only • Alarms Modify • Trace Read Only • Trace Modify
Performance management	• Statistics Counters Read Only • Statistics Counters Modify
Security management	• Users Read Only • Users Modify • Users Modify Password
System management	• Process & Node Read Only • Process & Node Modify • Subsystems Read Only • Subsystems Modify • Tickets Read Only • Tickets Modify • SW Installation Read Only • SW Installation Modify

8.12.7.3 Concurrent User Access

The handling of concurrent user access is described here.

Another major feature of the management functions API is the handling of concurrent accesses of multiple users to the same management objects. For this purpose there is another database table as shown in the example in the table below.

Table 211: RTP_ADM_SESSIONS

User	Hostname	Login Time	Server Address	Active Objects
sysop2	Central Mgr1	11/02/1998 07:38:52h	RtpAdmServer01	EventMgmt, Performance-Mgmt, AppMgmt
sysop4	Local Mgr2	11/02/1998 12:57:13h	RtpAdmJserv02	TraceMgmt, PerformanceMgmt
sysad	Local Mgr1	11/02/1998 13:15:07h	RtpAdmJserv01	UserMgmt, EventMgmt

The table above shows an example with a snapshot of all currently existing user sessions. The above-mentioned MgmtSession class controls its contents. The user management function can be used to retrieve the table’s contents for information purposes.

The listed ActiveObjects correspond to instances of the management classes in the management function API. If one user updates data belonging to a particular management object (an EventMgmt object), any other user sessions currently using an object of the same class are informed about the update.

Using the above example: If sysop2 updates event parameters (being handled by his instance of the EventMgmt class), sysad receives a note about this update as he also has an instance of the EventMgmt class. It is up to the respective user interface how this information is handled; it might request the modified data or instead provide a pop-up dialog window informing the user that the data being displayed probably is out of date.

Among others, the update information mechanism is part of the BaseMgmt class in the management function API (InformUpdate member function). Any other management classes inherit their basic functionality from the BaseMgmt class.

8.12.7.4 Remote Access to CLI and FTP

Important topics of remote access to CLI and FTP are described here.

The OpenScape Voice provides secure command-line and file-transfer interfaces using SSH and SFTP. The following describes its functionality:

- The OpenScape Voice blocks unencrypted FTP and RCP and provides SFTP in normal operation, with the exception of IPsec-protected FTP instead of SFTP for machine interfaces to the billing server).

- The OpenScape Voice Admin/Installation server supports SSH for CLI and file transfer.
- The OpenScape Voice terminal server, if installed, disables Telnet and FTP and supports SSH instead.

SSH

OpenSSH, Protocol Version 2 (SSH2), is installed to replace administration- or service-initiated Telnet, FTP, RSH, and RCP CLI and file transfer traffic over an unsecured network. Note that the machine interface to the billing server is protected using IPsec instead of SFTP for uploading of CDR records (transfer by push), the transfer of which is also protected by IPsec.

The OpenScape Voice uses RSH and RCP for installation and upgrade.

Terminal Server

A terminal server may be used to provide remote access to the console port when required by the enterprise’s policies. It is strongly recommended that any terminal server deployed to provide remote access to the console port have secure interfaces for administration or service login. The LX4016S Terminal Server product from MRV Communications is selected, which supports SSHv2.

Administration or Service Access

Since administration or service access must be possible from any machine connected to the customer network with access to the OpenScape Voice, a purely machine-based SSH interface cannot be implemented. Instead, the SSH connection must be based on the administration or service identity.

At installation, a key pair is created for the OpenScape Voice, and the OpenScape Voice is provisioned with the user IDs of all administration or service personnel allowed to access the OpenScape Voice.

During an SSH user login, the OpenScape Voice returns its public key, which is checked by the system administration or service terminal to ensure that communication is correctly occurring with the correct OpenScape Voice. Then the administrator or service technician provides the OpenScape Voice with its user ID and password encrypted with the public key of the OpenScape Voice.

For this to function the administration or service terminal needs to support SSH.

8.12.7.5 Remote Syslog

OSV supports setting up a remote syslog session to a log host server via a Perl based script, `loghost_configuration.pl`. This script is called by OSV CLI administration. By default, the configuration of remote rsyslog forwarding is disabled. The script has to run on both nodes of an OSV cluster following a CLI administration change. The processing of both nodes is handled internal to the loghost script. The remote session configuration uses a UDP connection, by default, which can be changed to TCP or TLS depending on network and audit needs, to communicate with the remote servers. The only prerequisite is that the OSV TLS certificate needs to be installed on the remote rsyslog server.

Running the script

Run the script as root user and use it to:

- Add and remove the OSV remote syslog server connection

- Setup a Linux remote syslog server to test the OSV
- Setup rsyslog statistics files
- Restart or stop syslog
- Display syslog configuration

The script is located at: `/unisphere/srx3000/callp/bin/`

```
#./unisphere/srx3000/callp/bin/loghost_configuration.pl
```

-Help

Name:

`loghost_configuration.pl` - Configure OSV for a remote syslog host

Usage:

- Synopsis 1: OSV only - add/replace/remove rsyslog connection; rsyslog status

```
loghost_configuration.pl -removeloghost_configuration.pl <-
syslog_config|-syslog_status>
```

- Synopsis 2: Remote Server only - set up remote rsyslog system

```
loghost_configuration.pl -rsyslog_setup
```

- Synopsis 3: OSV and Remote Server - restart/stop syslog, collect stats, display configuration, verbose help

```
loghost_configuration.pl -syslog_restart
```

```
loghost_configuration.pl -syslog_stop
```

```
loghost_configuration.pl -syslog_stats_add
```

```
loghost_configuration.pl -syslog_stats_remove
```

```
loghost_configuration.pl [-v 2]
```

```
loghost_configuration.pl -Help
```

Description:

Run the script as root user and use it to:

- Add and remove the OSV remote syslog server connection
- Setup a Linux remote syslog server to test the OSV
- Setup rsyslog statistics files
- Restart or stop syslog
- Display syslog configuration

Add/Replace Syslog Connection to a remote syslog server

```
loghost_configuration.pl -add -remote ipaddr [-port
remote_port] [-udp|-tcp|-tls|-relp] [-verbose N]
loghost_configuration.pl -replace -remote ipaddr [-port
remote_port] [-udp|-tcp|-tls|-relp] [-verbose N]
```

Remove Syslog Connection

```
loghost_configuration.pl -remove
```

Setup Syslog Server

```
loghost_configuration.pl -rsyslog_setup
```

Restart Syslog Service

```
loghost_configuration.pl -syslog_restart
```

Stop Syslog Service

```
loghost_configuration.pl -syslog_stop
```

Setup Syslog Service Stats

```
loghost_configuration.pl -syslog_stats_add
```

Remove Syslog Service Stats

```
loghost_configuration.pl -syslog_stats_remove
```

Display Syslog Configuration and Status

```
loghost_configuration.pl
```

```
loghost_configuration.pl -syslog_config
```

```
loghost_configuration.pl -syslog_status
```

Display Long Help Text

```
loghost_configuration.pl -H
```

Add or Remove OSV rsyslog Connection

OSV only supports a single connection to a syslog server. The connection can be either:

- udp
- tcp
- tls

When adding a remote connection, the only mandatory parameter is the remote syslog server IP/FQDN.

The connection type and port number are optional with default values being udp and 514.

When selecting TCP, the default port value is 514.

When selecting TLS, the default port value is 6514.

NOTICE:

You cannot have TCP and TLS on port 6514

When configuring a cluster, the script must be run on each node. When removing a remote connection no arguments are required and the existing connection is removed. You must first remove the existing connection before adding a new one.

The script's Log file can be found here: `/log/loghost_config.log`

Creating Remote SysLog Server

For the remote rsyslog server after performing the `-rsyslog_setup` no further action is required. Connections can be added/removed from multiple OSV's without the need to change the syslog server configuration.

Options:

```
-h, -help, -Help, -verbose Print help. Verbose level (0=no
output; default=1; verbose=2; full=3) Help displays all
sections of the help text-add, -replace
```

Connect to remote syslog server.

`-remote <ipv4-address>`

Remote syslog server IP address

`-port <port>`

Remote syslog server port to connect to. Default depends on the protocol used.

- UDP 514
- TCP 514
- TLS 6514
- RELP 20514

`-remove`

Remove ipsec configuration associated with remote ip address.

`-rsyslog_setup`

Setup remote syslog server to store log files based on connection type (udp/tcp/tls).

`-syslog_restart`

Restart rsyslog - use to ensure these are up to date with configuration file changes

`-syslog_stop`

Stop rsyslog - stop all syslog logging

`-syslog_config`

Display: `udp|tcp|tls,<ipaddr>,<port>,enabled|disabled`

`-syslog_status`

LOCAL-STATE REMOTE-STATE ACTIVE PARTNER

`[not_]running,[not_]configured,[not_]transferring,[no]match`

Enabled

`not_running, not_configured, not_configured, [no]match`

Disabled

`-udp|-tcp|-tls|-relp`

Defines the type of syslog protocol to use. Default is udp. relp is reliable TCP/TLS

Files:

OSV uses the following files

`/etc/rsyslog.d/0_osv_forward.conf` - syslog forwarder for tcp/udp/tls

`/log/loghost_config.log` - log file from script

`/usr/local/ssl/certs/root.pem` - Root CA TLS certificate (must have same signer as rsyslog server)

`/usr/local/ssl/private/client.pem` - OSV client TLS certificate used for mutual authentication with syslog server

`/var/log/rsyslog` - when remote server is down, directory to store backlog of messages

Remote Syslog Server uses the following files

/etc/rsyslog.d/rsyslog_tls.conf - syslog tls listener

/etc/rsyslog.d/rsyslog_tcp.conf - syslog tcp listener

/etc/rsyslog.d/rsyslog_udp.conf - syslog udp listener

/etc/logrotate.d/rsyslog.lr - rotate the syslog files in /var/log/rsyslog_files

/etc/rsyslog.d/ca.pem - Root CA TLS certificate (must have same signer as OSV client)

/etc/rsyslog.d/server_cert.pem - Server TLS certificate used for validating the syslog server

/etc/rsyslog.d/server_key.pem - Server TLS key used for validating the syslog server

/log/loghost_config.log - log file from script

/var/log/rsyslog_files - remote OSV syslog files one per host

When creating a remote syslog server to test the OSV, the script creates the same certificates that are present on the OSV. These are created in /etc/rsyslog.d files. When setting up a real world environment the test certificates installed by this script should be replaced by customer certificates. This mechanism is outside the scope of this script.

OSV Examples

1) Display configuration data and connection information.

```
loghost_configuration.pl [-v 2]
```

2) Add OSV connection to remote syslog server - default udp port 514, repeat command on both nodes if system is a cluster

```
loghost_configuration.pl -add -remote remote_ip
```

3) Change OSV connection to remote syslog server - use TLS for secure connection, repeat command on both nodes if system is a cluster.

```
loghost_configuration.pl -replace -remote remote_ip -tls
```

4) Remove current OSV connection to remote syslog server, repeat on both nodes if system is a cluster

```
loghost_configuration.pl -remove
```

5) Add OSV TCP connection to remote syslog server using non standard port 10514, repeat on both nodes if system is a cluster. The server must be listening on the none standard port.

```
loghost_configuration.pl -add -remote remote_ip -tcp -
port 10514
```

6) Restart syslog server on this node.

```
loghost_configuration.pl -syslog_restart
```

7) Stop syslog server, only stops the current node

```
loghost_configuration.pl -syslog_stop
```

Remote SysLog Server Examples:

1) Setup Remote Syslog Server

```
loghost_configuration.pl -rsyslog_setup
```

2) Display Configuration Data and Connections

```
loghost_configuration.pl
```

3) Restart Syslog Server.

```
loghost_configuration.pl -syslog_restart
```

Transmitting syslog data to a remote loghost

Configuring the OSV to transmit syslog data to a remote loghost involves 2 steps:

1) Configure the remote loghost using the following command steps:

- Copy

  ```
  /unisphere/srx3000/callp/bin/loghost_configuration.pl
  ```

  from OSV to the remote loghost
- Run

  ```
  /loghost_configuration.pl -rsyslog_setup
  ```

  on the loghost

2) Configure OSV with a remote logging option:

- Run Admin CLI option for "Remote syslog management" (option: 6.1.11)

Remote syslog Management (methods):

Display Remote syslog..........................1

Enable Remote syslog...........................2

Disable Remote syslog..........................3

Return..99

Selection (default: 1): **2**

Provide User Name (root | secad): **secad**

Provide User password: **xxxxxxx**

Select node: <local,remote,both (max length: 32)> (default: local): **both**

Syslog protocol: <0=none,1=udp,**2=tcp**,3=tls (min: 0 max: 3)> (default: 3): **2**

Syslog server IP: <max length: 20 (max length: 32)> (default:):

```
<loghost ipaddr>
```

Syslog server port: < (min: 0 max: 9999)> (default: **514**):

8.13 Certificate Strategy Overview

The OpenScape system uses different security protocols to save the communication between different OpenScape computer systems and the communication via a number of web-based interfaces.

8.13.1 Configuration of Certificate Strategy

In an OpenScape system different security protocols are used. The customer must configure the certificate structure.

The OpenScape system uses the following security protocols.

- TLS / SSL – e. g. for the communication between different OpenScape computer systems
- HTTPS – for the communication via a number of web-based interfaces.

You need to configure a certificate strategy for the smooth, secured communication via these protocols. The OpenScape system then integrates this strategy in the security concept of the customer network.

How to proceed depends on two factors:

- The OpenScape deployment scenario used and its execution
- The available customer environment

The integration of the OpenScape system in the security concept of the customer network depends on the OpenScape deployment scenario.

8.13.2 Deployment Scenario Integrated Simplex

In this deployment scenario, only one OpenScape computer system needs to be integrated in the security concept of the customer network: the application computer.

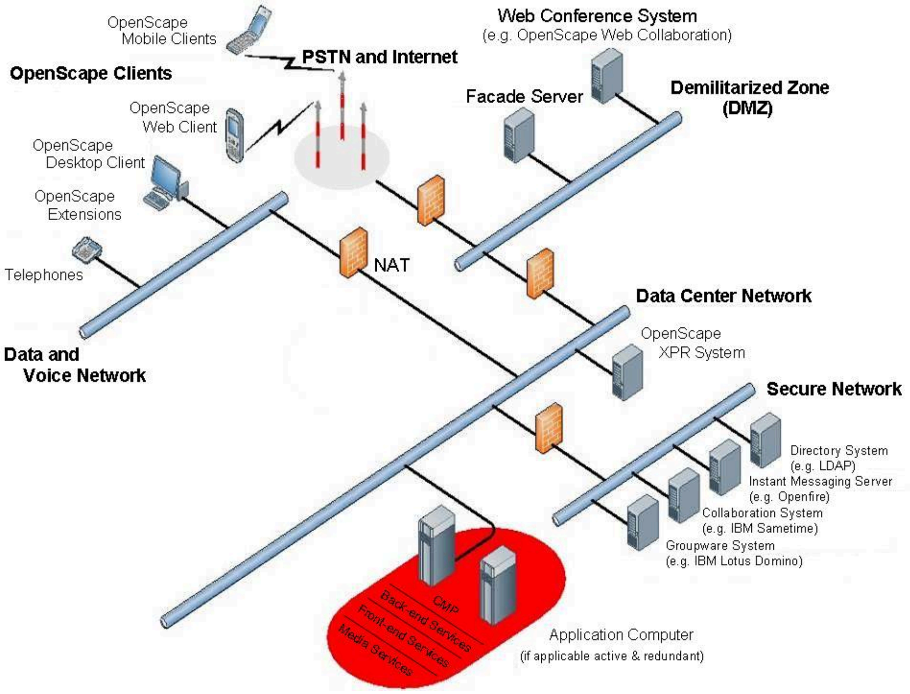
This integration requires a single pair of keys with associated certificate, which needs to be assigned to the application computer. The fully qualified host name (FQHN) of the application computer is specified in the certificate for this assignment.

Key pair and certificate are imported in the keystore of the application computer.

OpenScape computer system to be integrated	Count Key pair/ certificate	Certificate assigned to ...	Keystore storage location
Application computer	1	Application computer	Application computer

Functional Sequence

The following figure shows the deployment scenario Integrated Simplex. All components concerned by the configuration of the certificate strategy in this scenario are red-highlighted.



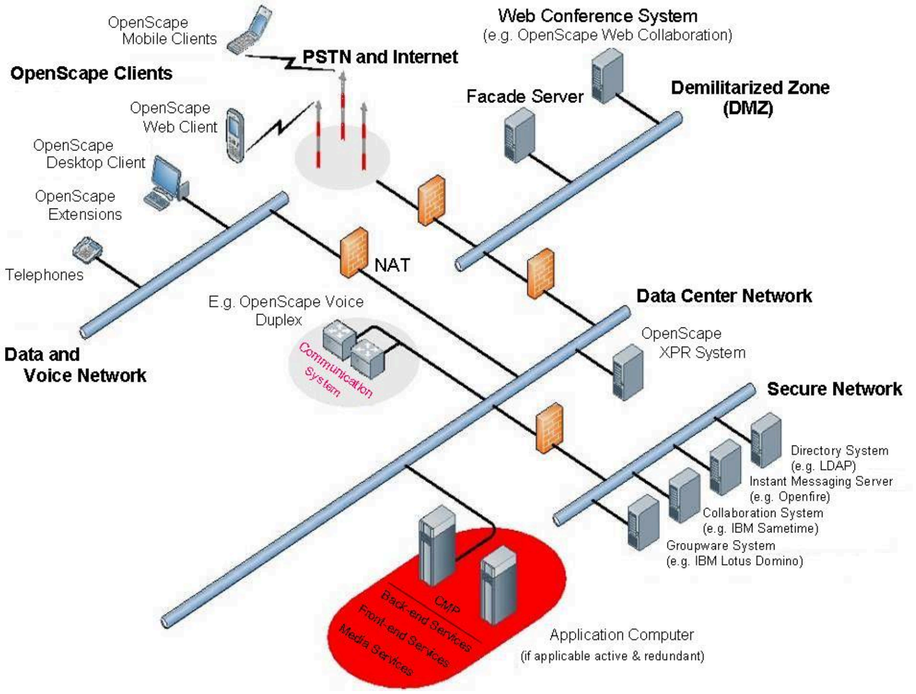
8.13.3 Deployment Scenario Small Duplex

In this deployment scenario the following OpenScape computer systems must be integrated in the security concept of the customer network: The active application computer and the passive application computer (if available).

Only a single pair of keys with associated certificate is required since these computer systems are addressed under the same host name.

The key / certificate pair must be assigned to the application computers. To this, the fully qualified host name (FQHN) of the application computers is specified in the certificate. The key / certificate pair is imported in the keystore of the active and passive application computer.

OpenScape computer system to be integrated	Count Key pair/ certificate	Certificate assigned to ...	Keystore storage location
Application computer (active)	1	Application computer	Application computer
Application computer (passive) (optional)			Passive application computer



8.13.4 Customer Environment 1 (KU1) - PKI with CA

The customer network uses already a Public Key Infrastructure (PKI) with a proprietary Certificate Authority (CA). The customer provides required keys and associated certificates directly as PKCS#12 keystore file.

Functional Sequences

The following requirements apply.

- The password for a PKCS#12 keystore file may contain the following characters only
  - Letters A to Z and a to z
  - Digits 0 to 9
  - The special characters !$%()*+,-./:;=?@[\]^_`{|}~
- The password for a PKCS#12 keystore file and the associated private key must be the same.
- The password for a PKCS#12 keystore file must be known for the configuration.
- The alias name tomcat must have been configured for the certificate in a PKCS#12 keystore file.

Beyond that, the following recommendations apply:

- Private keys should be of type RSA.
- The length of the keys used should be 2048 bit (the key lengths 1024 and 4096 are supported, too).
- The signing algorithm should be MD5 with RSA.

Furthermore, the root certificate of the certificate authority used has already been imported in the client browsers of the OpenScape users.

8.13.5 Customer Environment 2 (KU2) - PKI with CA and CSR

The customer network uses already a Public Key Infrastructure (PKI) with a proprietary Certificate Authority (CA). A Certificate Sign Request (CSR) is required to provide required certificates.

The root certificate of the certificate authority used has already been imported in the client browsers of the OpenScape users.

8.13.6 Customer Environment 3 (KU3) - PKI without CA

The customer already uses a Public Key Infrastructure without proprietary certificate authority.

The root certificate of the certificate authority used has already been imported in the client browsers of the OpenScape users.

8.13.7 Customer Environment 4 (KU4) - PKI Planned

The customer has not used a Public Key Infrastructure so far, but plans to introduce one with the OpenScape system.

8.13.8 Configuration

Configuration steps of the certificate strategy in one of the contemplated customer environments follow the specific of the relevant customer environment.

Configuration step	KU1	KU2	KU3	KU4
Preparing the Configuration of the Certificate Strategy				
• Determining the OpenScape Setup Directory	x	x	x	x
• Determining the Keytool Command	x	x	x	x
• Determining the Keystore Directory	x	x	x	x
• Defining an X.500 Distinguished Name		x	x	x
Configuring a simple Certificate Authority				
• Preparing the Certificate Authority				x
• Creating self-signed Root Certificates				x
Creating a Pair of Keys for the Application Computer		x	x	x
Creating Certificate Sign Requests for the Application Computer		x	x	x
Signing Certificate Sign Requests				x
Importing a Certificate in the Server Keystore		x	x	x

Configuration step	KU1	KU2	KU3	KU4
Storing a provided PKCS#12 File	x			
Activating a Server Keystore for the CMP	x	x	x	x
Configuring a Server Keystore for the OpenScape Application Computer	x	x	x	x
Importing the Root Certificate in the Client Browsers				
• Displaying the Root Certificate				x
• Checking the Root Certificate				x
• Installing the Root Certificate				x

Additionally you may need these instructions to configure the certificate strategy in a customer environment:

- Creating a secure Password
- Combining Certificate Files to a Certificate Chain
- Converting the Format of a Certificate Chain from DER into PEM
- Converting the Format of a Certificate Chain from PKCS#12 into PEM

Related concepts

Creation of Secure Password on page 884

8.13.9 Preparation of Certificate Strategy

Execution of the preparatory steps like determination of OpenScape Setup directory, Keytool command, Keystore directory, directory for the SSL / TLS configuration and definition of an X.500 Distinguished Name is necessary before you can configure the certificate strategy.

8.13.9.1 Definition of an X.500 Distinguished Name

KU2, KU3, KU4: To define the assignment of certificates or keys to computer systems, a unique name, the so-called Distinguished Name (DN), is specified in each certificate or key.

The distinguished name contains the following information that should always be defined:

- **CN** - Common Name

  Define (mandatory) the FQHN (Fully Qualified Host Name) of the computer system to which the certificate and the associated pair of keys are assigned.

  e.g.: filesrv_ac1.domain.com

  In case of a Certificate Authority (CA), CN must define the name of the certificate authority.

  e.g.: HTWK Leipzig CA

- **OU** - Organisation Unit

  Define (mandatory) the name of a smaller organization unit the relevant computer system belongs to, e. g. a department or division:

  e.g.: University Library

Furthermore, the distinguished name contains the following information that can be defined in addition:

- **O** - Organization Name

  May define the name of a larger organization unit the relevant computer system belongs to.

  E.g. HTWK Leipzig
- **L** - Locality

  May define the geographic location for the relevant computer system, e. g. the name of a city.

  E.g. Leipzig
- **C** - Country

  May define the two-digit country code for the location of the relevant computer system.

  E.g. DE
- **ST** - State

  May define the name of a subordinate territory for the location of the relevant computer system.

  NOTICE:

  Instead of the **ST** identifier the Java keytool uses the **S** identifier.

  E.g. SN

Example of a distinguished name as you need to enter it in commands of the Java keytool at a later date: `CN=filesrv_ac1.domain.com, OU=University Library, O=HTWK Leipzig, L=Leipzig, C=DE, S=SN`

8.13.10 Configuration of a Simple Certificate Authority

KU 4: A simple certificate authority configured in this way should only be used for testing purposes on one of the application computer of OpenScape system. The freely available software OpenSSL is used for configuration. This software is usually pre-installed with each Linux operating system.

NOTICE:

The certificate authority configured in this way should only be used for testing purposes.

Use for testing purposes is because the following restrictions:

- A certificate authority should always be configured and operated on a separate computer system.
- Passwords should not be transferred via a command console.
- The random generator used in the following should better be pre-set for a certificate authority.

Functional Sequence

The certificate authority is configured in the following steps:

- Preparing the Certificate Authority
- Creating self-signed Root Certificates.

8.13.11 Creation of a Pair of Keys for the Application Computer

KU2, KU3, KU4: You need to create a pair of keys for the application computer. If you use an active and a passive application computer, both application computers use the same pair of keys, since these computer systems are addressed under the same host name.

The pair of keys of the application computer must be assigned to the application computer. When the pair of keys is created, the distinguished name of the application computer is specified for this assignment.

NOTICE:

If you use an active and a passive application computer, you need to execute the following steps on one of the application computers only.

NOTICE:

Certificates and keys are stored in the so-called keystore of a computer system. Creating such a keystore for accessing it later requires a keystore password. To protect the keystore from unauthorized access, the password should be generated randomly.

Each pair of keys of a keystore can also be protected from unauthorized access by a key password. This key password, however, must usually correspond to the keystore password.

8.13.12 Signing Certificate Sign Requests

KU2, KU3, KU4: The newly created pairs of keys must be signed to confirm the identity of the associated computer systems. To this, the associated certificate sign requests are signed by a certificate authority.

The results in certificates contain the following:

- The public key of the relevant computer system
- Information that identifies the associated computer system
- General information about the certificate itself

You can sign the certificate sign requests in two ways:

- By a certificate authority that you have configured in the scope of these instructions. In this case, proceed as documented for the relevant certificate authority, continue with section "How to Import a Certificate in the Server Keystore".
- By the certificate authority you have configured in “Configuring a simple Certificate Authority”. In this case, proceed as described in section "How to Sign a Certificate Sign Request".

8.13.13 Activation of Server Keystore for the CMP

KU1, KU2, KU3, KU4: When a user invokes the CMP (Common Management Platform) with his/her web browser, the CMP and the web browser exchange their certificates.

This ensures the following:

- CMP and web browser can authenticate themselves as permissible communication partners
- Data can be transmitted encrypted.

So that the CMP uses its new certificate, the new keystore for the CMP must be activated on the application computer.

8.13.14 Import of Root Certificate in the Client Browser

KU4: The OpenScape computer systems authenticate themselves with their configured server certificates against the client browsers of the OpenScape users. So that the client browsers accept these server certificates you need to import the root certificate with which the server certificates of the OpenScape computer systems were signed in the client browsers of the OpenScape users.

> **NOTICE:**
>
> These steps should not be required for customer environments KU1, KU2 and KU3.

The import of the root certificate in the Internet Explorer 8 is done by the following steps required:

- Displaying the Root Certificate
- Checking the Root Certificate
- Installing the Root Certificate.

8.13.15 Supplementing Instructions

Additional instructions to configure the certificate strategy in a customer environment.

The following additional instructions are needed:

- Creating a Secure Password
- Combining Certificate Files to a Certificate Chain
- Converting the Format of a Certificate Chain from DER into PEM

- Converting the Format of a Certificate Chain from PKCS#12 into PEM

8.13.15.1 Creation of Secure Password

Certificates and keys are stored in the so-called keystore of a computer system. Creating such a keystore for accessing it later requires a keystore password. To protect the keystore from unauthorized access, the password should be generated randomly.

Each pair of keys of a keystore can also be protected from unauthorized access by a key password. This key password, however, must usually correspond to the keystore password.

Related concepts

Configuration on page 879

8.13.16 OSV Certificate Management

Certificates are managed via the Certificate Management drop-down menu in OSV Assistant. The drop-down menu consists of the following pop-ups:

- Certificate Key Stores
- Public Certificates
- Trusted CA Certificate Stores
- Certificate Monitoring
- Certificate Revocation List

General Functionality

When a certificate expires an alarm is displayed.

Additionally, the issuer of a specific certificate has the capability to revoke it, e.g. when a certificate has been hacked, or misused or mandatory extensions have been added and thus one or more entries will appear in the Certificate Revocation List (CRL). In this case an alarm is also displayed when the CRL expires (i.e. the **Next Update** field from the CRL is older than the current time. See also How to Configure Certificates in General Settings Menu).

The revoked certificates must be replaced and then the respective CRL entries must be removed by the administrator, in order to avoid displaying alarms when the CRL expires. See also How to Delete a Certificate Revocation List.

NOTICE: If the CRL entry is not removed, alarms can be displayed even if the respective certificate has been replaced.

In case the certificate is revoked again, a new CRL entry will be triggered and the **Next Update** field from the CRL will be updated.

9 Cluster Redundancy and Survivability

9.1 Survivability Overview

Survivability is the capability of a network to maintain service continuity in the presence of faults within the network. In the OpenScape Voice environment, survivability mechanisms such as protection and restoration have been implemented either on a per-link basis, on a per-path basis, or throughout an entire network to alleviate service disruption. This environment also provides managed redundant IP Voice systems that take advantage of IP’s inherent survivability/rerouting capabilities. Plus, the VoIP’s ability to make call routing decisions contingent on the IP network’s status, makes for a robust and survivable voice communications system.

System Specific Information

OpenScape Voice supports a variety of Branch Office Solutions - from small to very large locations – by using direct workpoint client connections through a survivable proxy. This seamlessly supports the communications environment across the enterprise, office, home office and mobile locations. To protect the business processes per site, a survivability solution can be added to each remote side, which maintains existing calls and ensures basic operations even in WAN failures or unreachability of the OpenScape Voice system.

In the OpenScape Voice environment, both redundancy and node separation provide another means to enhance survivability. The OpenScape Voice hardware platform achieves carrier-grade reliability and availability based on the active/active clustered nodes. It supports hot swappable components, active/standby Fast Ethernet links, and crossover network connections through redundant, interconnected Ethernet switches.

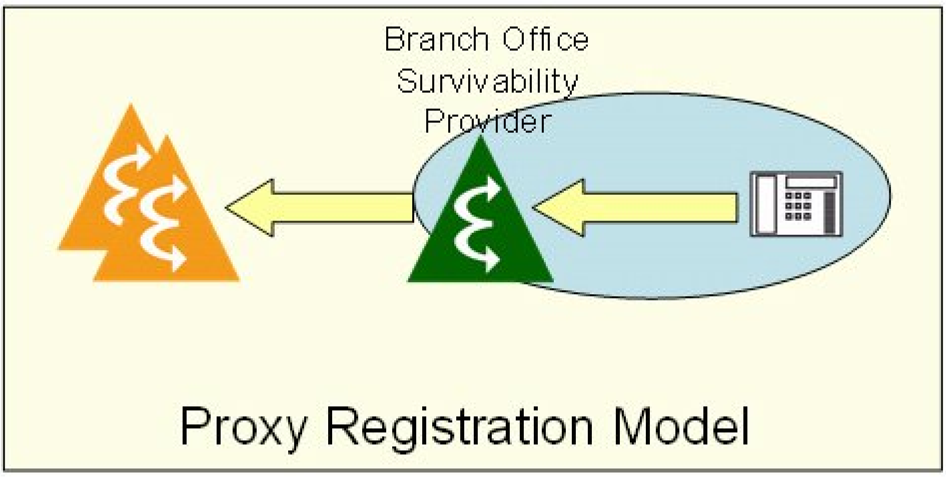
In addition, it is possible to have survivable Media Servers for the OpenScape Voice with 1+1, N+1 and N+k redundancy.

9.1.1 Proxy Registration Model

In the proxy registration model, the phones are configured with the OpenScape Voice as their Primary SIP Server/SIP Registrar. However, the communication layer is set up with DNS SRV records to send all outbound messages to a SIP proxy. With the use of the DNS SRV record, the communication layer would send all outbound messages directly to the OpenScape Voice in case the SIP proxy is not responding. 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 the OpenScape Voice is unreachable.

IMPORTANT:

When the phones are not allowed to bypass the proxy in case of proxy failure, the proxy should be deployed in a high availability configuration.



Other Characteristics

The proxy registration model is a clean survivability solution because all phones in the branch office are 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.

OpenScape Branch can be configured as a survivable SIP proxy

9.1.2 Overload Protection

When branch offices return from survivability mode, the OpenScape Voice is likely to be receiving an extremely high load of registration requests from the phones at the same time or very close together. In case of a proxy registration, these registration requests will all come at about the same time. The OpenScape Voice overload protection is designed to avoid overload in such a case.

Functional Sequence

The OpenScape Voice provides the following defense mechanisms against an abundance of registration requests:

1) The OpenScape Voice as the SIP Registrar controls the time when the phone must refresh its registration or subscription in order to remain registered or subscribed. This time is requested by the phone in the

registration or subscription request and the OpenScape Voice allows to randomize this time via RTP variables:

- `Srx/SipReg/RandomizeRegisterExpiration`. When set to RtpTrue, the registration interval is randomized.
- `Srx/Sip/RandomizeSubscribeExpiration`. When set to RtpTrue, the subscription interval is randomized.
- `Srx/Sip/RandomizeExpirationPercent`. Default value 25; which randomizes the time for the next registration or subscription to somewhere between 75%-100% of the requested registration and subscription interval by the phone.

2) When a proxy in the proxy registration model wants to return from survivability mode, the OpenScape Voice checks the number of requests in the message queue. When the OpenScape Voice is currently experiencing a high load in the queue, it will keep the proxy in survivability mode until the load in the message queue has dropped under a certain value. By keeping the survivable proxies in survivability mode, the OpenScape Voice can organize a controlled return to normal mode, guaranteeing that the OpenScape Voice will be able to handle the load from the branch office.

3) Incoming registration requests during high load conditions of the OpenScape Voice or when the registration queue is full are rejected with a response message that also indicates when the phone may try the registration again. This allows the OpenScape Voice to space out the registrations such that the phone does not needlessly overload the system by trying to register.

9.1.3 General Characteristics of the centralized SBC Branch Office Solution

The Session Border Controller (SBC) in the branch office allows the client to deploy a private LAN and have all communication devices on this private LAN. It translates (NAT) all private IP addresses to IP addresses that are on the same network as the OpenScape Voice (or the media relay SBC). The SBC used is a proxy and not a Back-to-Back User Agent (B2BUA). It hides the topology of the private LAN, but expects at the same time that all communication from the OpenScape Voice happens through a single signaling port.

The SBC uses an audit mechanism that puts subscribers of branches that cannot contact the OpenScape Voice in a suspended mode. In this mode, the OpenScape Voice allows the registration to stay alive although the SIP subscriber cannot refresh it. This is particularly important for survivability. It allows the SIP subscribers to be reached via the PSTN for an extended period of time. During the time that a SIP subscriber is in Suspended mode, the OpenScape Voice audits the SIP subscribers survivability provider (i.c. the SBC). The survivability provider always is the outbound proxy. With the introduction of the Media Relay SBC, the survivability provider is an endpoint behind the outbound proxy. The SIP messaging to detect WAN outages is therefore slightly different.

System Specific Information

There are three major configuration options for the SBC setup:

- Hosted Business Communication Services with small SBC in the Far End
- Hosted Business Communication Services with small SBC in the Far End and Media Relay SBCs in the Data Center

- TLS Subscribers in Branch Office using OSB in proxy mode. For the Branch office proxy solution there is optionally a backup link configuration considered for improved survivability.

Related concepts

Hosted Business Communication Services with small SBC in the Far End on page 888

Hosted Business Communication Services with small SBC in the Far End and Media Relay SBC in Data Center on page 889

TLS Subscribers in Branch Office Using OS Branch in Proxy Mode on page 889

Survivable Branch Office Using Proxies with Backup Link on page 890

Survivable Branch Office Using Proxies with Backup Link Configuration on page 891

Survivable Branch Office Using Proxies with Backup Link and Geographic Node Separation on page 893

Survivable Branch Office Using Proxies with Backup Link and Geographic Node Separation - Failures on page 894

9.1.3.1 Hosted Business Communication Services with small SBC in the Far End

This configuration uses small SBC's in each far-end client-net to communicate with an OpenScape Voice in the data center.

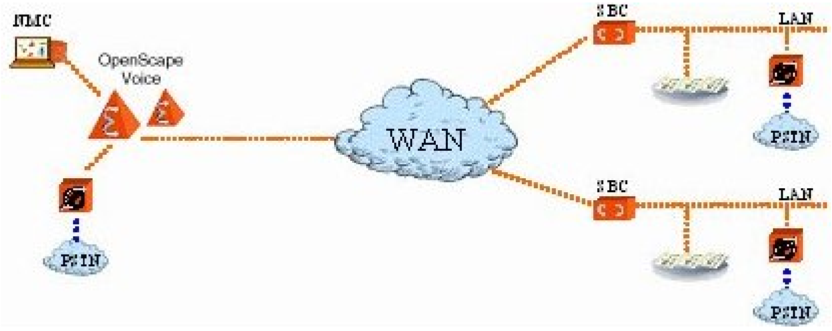
System Specific Information

For this configuration it is mandatory to:

- use the proxy registration model
- configure the SBC as the SIP UA proxy
- Switch off Outbound Proxy Bypass

Furthermore it is recommended to:

- mark the SBC as survivability provider
- use Endpoint Rerouting (specification of up to 3 routes per call)
- use Subscriber Rerouting, which allows the OpenScape Voice to reroute the call (PSTN or other network) for a SIP UA whose primary route is unavailable
- Registration Renewal, that is force the OpenScape Voice to renew the registration if a SIP UAs associated SIP endpoint (survivability provider) is not reachable



Related concepts

General Characteristics of the centralized SBC Branch Office Solution on page 887

9.1.3.2 Hosted Business Communication Services with small SBC in the Far End and Media Relay SBC in Data Center

Each small SBC's in the far-end client-net may be configured to communicate with a Media Relay SBC in the data center. The Media Relay SBC forwards all requests to the OpenScape Voice in the data center, but changes the SDP - if appropriate - to route all media streams between branch offices through the data center.

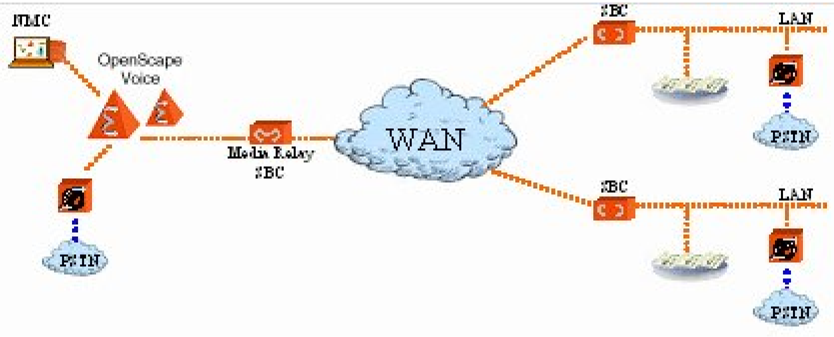
System Specific Information

For this configuration it is mandatory to:

- use the proxy registration model
- mark the Media Relay SBC as a SIP Proxy
- Switch off Outbound Proxy Bypass

Furthermore it is recommended to:

- mark the SBC as survivability provider
- use Endpoint Rerouting (specification of up to 3 routes per call)
- use Subscriber Rerouting, which allows the OpenScape Voice to reroute the call (PSTN or other network) for a SIP UA whose primary route is unavailable
- Registration Renewal, that is force the OpenScape Voice to renew the registration if a SIP UAs associated SIP endpoint (survivability provider) is not reachable



Related concepts

General Characteristics of the centralized SBC Branch Office Solution on page 887

9.1.3.3 TLS Subscribers in Branch Office Using OS Branch in Proxy Mode

In this configuration, there is not actually an SBC configured. Bit still TLS subscribers should never be called directly by the OpenScape Voice. Thus configuration is very similar to the configuration with a small SBC in the far end. The proxy takes the role of the other configuration’s SBC.

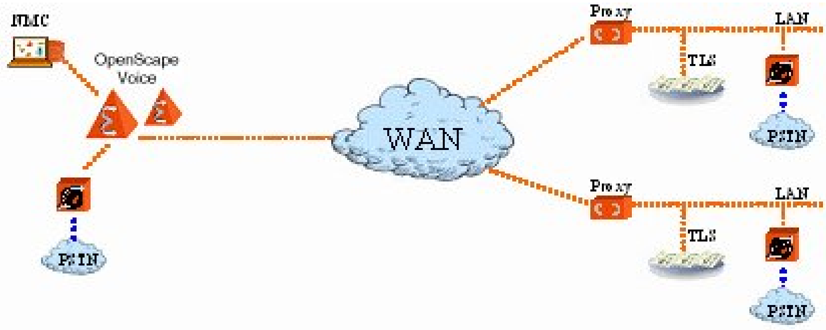
System Specific Information

For this configuration it is mandatory to:

- use the proxy registration model
- mark the used proxy as a SIP Proxy (Outbound Proxy Bypass allowed)

Furthermore it is recommended to:

- mark the proxy as survivability provider
- use Endpoint Rerouting (specification of up to 3 routes per call)
- use Subscriber Rerouting, which allows the OpenScape Voice to reroute the call (PSTN or other network) for a SIP UA whose primary route is unavailable
- Registration Renewal, that is force the OpenScape Voice to renew the registration if a SIP UAs associated SIP endpoint (survivability provider) is not reachable



Related concepts

General Characteristics of the centralized SBC Branch Office Solution on page 887

9.1.4 Survivable Branch Office Using Proxies with Backup Link

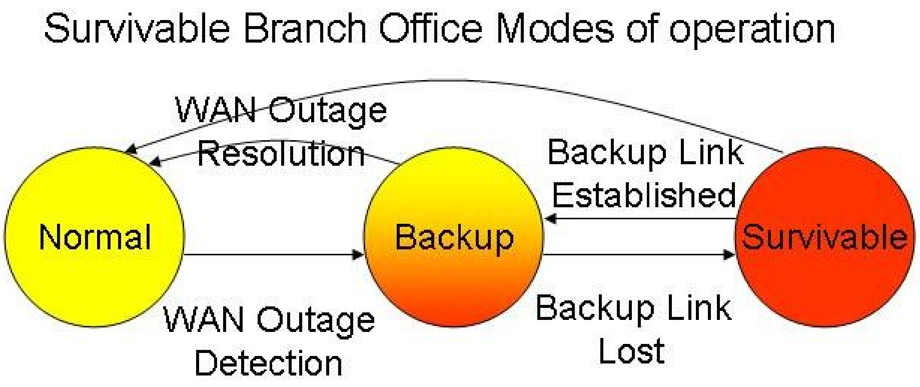
Optionally a backup link via PSTN can be created from branch offices to the main OpenScape Voice. This can mainly be used to protect the branch office from WAN failure, but may also be configured in order to protect against the failure (or admission control rejections due to overload) of the main OpenScape Voice.

System Specific Information

There is a new mode of operation introduced for the feature. In addition to normal and survivable operation there is the backup operation mode.

NOTICE:

The branch office proxy does not recognize any difference between normal and backup mode of operation. It is the routers task to provide the backup link via PSTN.



Other Characteristics

In backup operation as opposed to survivable operation there will be the following:

- No restriction in the feature set or groups configuration in the branch office.

> **NOTICE:**
>
> In backup mode, the OSV enforces a CAC 0 policy on the WAN link to the branch office. This may affect the calls and features between other branches and this branch office. Please see the feature description and interactions for Subscriber Rerouting due to CAC Restriction and Enhanced Subscriber Rerouting.

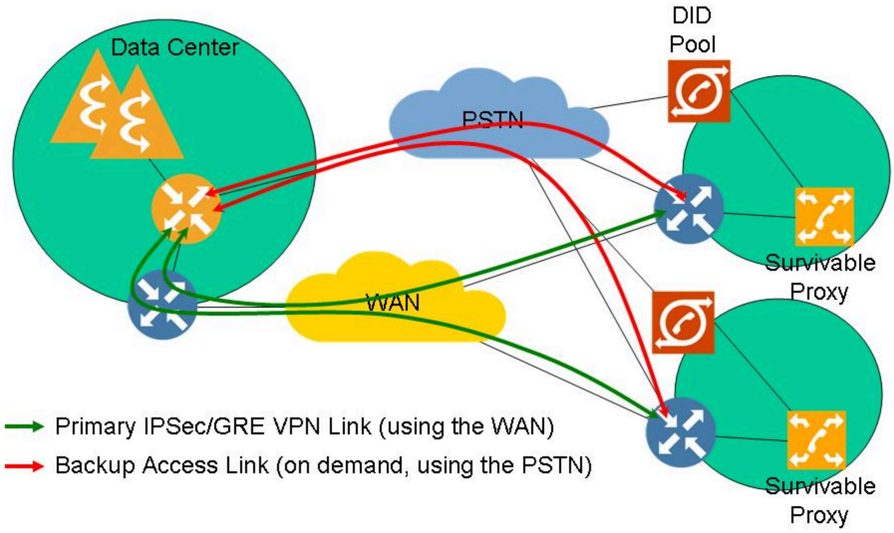
- No loss of CDR records.
- A graceful return to using the main OpenScape Voice must be provided for when it becomes possible for the subscribers to return to using the main OpenScape Voice.

Related concepts

General Characteristics of the centralized SBC Branch Office Solution on page 887

9.1.4.1 Survivable Branch Office Using Proxies with Backup Link Configuration

When a branch office is isolated, the OpenScape Voice cannot provide feature service anymore, because it has no connectivity to the branch. In order to give the OpenScape Voice still access to the branch office, the branch office can set up a backup data connection through the PSTN.


DID
Pool
Data Center
PSTN
WAN
Survivable
Proxy
Survivable
Proxy
Primary IPSec/GRE VPN Link (using the WAN)
Backup Access Link (on demand, using the PSTN)

Requirements

- The data center router is configured to set up the IPSec/GRE VPN tunnels to the branch offices. Each tunnel gets a unique name that is recorded in the CAC group for the branch office that is served with the tunnel.

- The data center router must be configured to be highly available through the Hot Standby Router Protocol (HSRP). This means that each data center must have a redundant pair of Cisco™ 2800 or 3800 series routers.

- The routing tables for a route to the branch office must be set up to try the IPSec/GRE VPN tunnel through the WAN to the branch office with highest priority (lowest metric) and use the dialer watch to check for establishment of the ISDN backup tunnel through the PSTN.

- The link status manager process must listen for messages on virtual IP addresses assigned at configuration time with the NCPE tool. These IP addresses must be addresses from the administration subnet. In case of geographic node separation an IP address in each separated subnet must be assigned.

- The OpenScape Voice must implement a new process (Link Status Manager) that acts as a SNMP (v2c/v3) Manager for the data center router. The purpose of the link status manager will be to receive status-link up/down traps from the data center router delivered via the Inform Request message or as a trap. It must implement a white list of IP addresses that may send these SNMP messages to it.

- The data center router must be set up to send reliable link status notifications for the IPSec/GRE VPN tunnel connections to the Link Status Manager of the OpenScape Voice.
- DID pool for correlation service. This can be created only if the branch office is a survivable branch office (indicated via the 'Survivable' attribute on the branch office's representative endpoint).

Related concepts

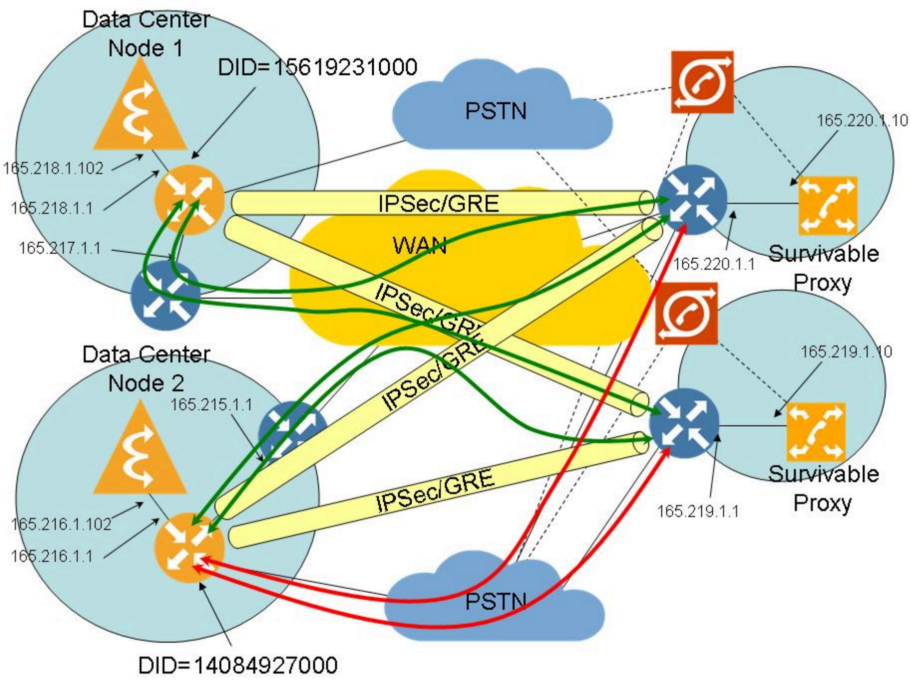
General Characteristics of the centralized SBC Branch Office Solution on page 887

9.1.4.2 Survivable Branch Office Using Proxies with Backup Link and Geographic Node Separation

In case of geographic node separation, each node's data center router must set up IPSec/GRE VPN tunnels to the branch office.

The data center router is set up to route the traffic to the branch offices via the tunnels. The Branch Office's router is set up (using metrics) to:

- primarily send all IP traffic to each of the data centers.
- if this doesn't work, set up a backup access link to the backup data center based on the destination IP address.



Related concepts

General Characteristics of the centralized SBC Branch Office Solution on page 887

9.1.4.3 Survivable Branch Office Using Proxies with Backup Link and Geographic Node Separation - Failures

The backup access link to a data center is only built after the branch office proxy tries to route packets to the faulty IPSec/GRE VPN tunnels that connect the branch office with the desired data center. The data center will activate the backup bandwidth limit only if both tunnels fail, because if one GRE tunnel is OK, this means that the full WAN bandwidth is available to the branch office.

Data Center node 1	Data Center node 2	GRE Tunnel node 1 to Branch Office	GRE Tunnel node 2 to Branch Office	Proxy in Branch Office primarily connected to node 1
Up	Up	Up	Up	Proxy sends all IP traffic to data center node 1.
Up	Up	Up	Down	Proxy sends all IP traffic to data center node 1. Backup ISDN link to node 2 should not be activated because no traffic is going to this data center. Branch office is not CAC restricted.
Up	Up	Down	Up	Proxy sends all traffic to Data Center 2. Branch office is not CAC restricted.
Up	Up	Down	Down	Branch Office Router activates backup ISDN to data center 2. Branch office is CAC restricted.
Up	Down	Up	Up	Proxy sends all IP traffic to data center node 1.
Up	Down	Up	Down	Proxy sends all IP traffic to data center node 1. Backup ISDN link to node 2 should not be activated because no traffic is going to this data center. Branch office is not CAC restricted.
Up	Down	Down	Up	Branch office is in survivable mode.
Up	Down	Down	Down	Branch office is in survivable mode. Backup to node 2 is activated but since node 2 is down, there is no response on this.
Down	Up	Up	Up	Proxy uses node 1 backup IP address on node 2 and sends all IP traffic to data center node 2. Branch office is not CAC restricted.
Down	Up	Up	Down	Branch office router establishes the backup links for the GRE tunnel to node 2. Branch office is CAC restricted.
Down	Up	Down	Up	Node 1 does not respond. Branch office contacts node 2 normally. Branch office is not CAC restricted.

Data Center node 1	Data Center node 2	GRE Tunnel node 1 to Branch Office	GRE Tunnel node 2 to Branch Office	Proxy in Branch Office primarily connected to node 1
Down	Up	Down	Down	Branch office router establishes the backup links for the GRE tunnel to node 2. Branch office is CAC restricted.
Down	Down	-	-	No communication with the OpenScape Voice possible. The branch is in survivable mode. Backup links may have been established based on whether it is just the OpenScape Voice that went down or the entire data center.

Related concepts

General Characteristics of the centralized SBC Branch Office Solution on page 887

9.1.5 Rerouting based on SIP Response Codes, Response Timeout or WAN outage

The OpenScape Voice provides rerouting of SIP calls for unreachable gateways or subscribers in the case of WAN outage or after receipt of a SIP response code indicating an error condition such as a bandwidth restriction (e.g. 606). The SIP calls can be of type off-net (to the PSTN via a SIP gateway), on-net (to another SIP network, such as OpenScape Voice) or to a registered SIP subscriber on a remote branch. A rerouting timer provides rerouting in case no response is received from the SIP gateway, SIP server or SIP subscriber after an INVITE has been sent to them.

Requirements for subscriber rerouting

WAN rerouting for a call to SIP subscribers on a remote branch can rely on particular conditions:

- The called subscriber has to have a valid public E.164 number.
- The called subscriber has to be registered via a survivable proxy, such as OSB. This means that the called subscriber is registered with its provisioned 'Survivable' SIP Proxy endpoint.
- The Associated Endpoint field of the called subscriber must match the endpoint name of the OSB survivable proxy in order for the feature to be activated.
- The SIP proxy endpoint must be configured with the “Survivable Endpoint” attribute.

- The SIP proxy endpoint can have the following additional attributes selected:

Table 212: Selectable attributes (none of them applicable to subscriber endpoints)

Attribute	Description
Enhanced Subscriber Rerouting	Select this attribute to enable enhanced subscriber routing, which pertains to the ability to reroute forwarded calls and hunt group calls. Applicable only for CAC rerouting
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 ist not commonly used, and should not be selected for gateway endpoints.
SIP Proxy	If selected (enabled), the endpoint is a SIP proxy applicable only to SIP endpoint.This attribute is not applicable for SIP Private Networking.
Route Via Proxy	When selected (enabled) together with the SIP Proxy attribute, this endpoint is on the route when the OpenScape Voice is making an outbound call to a subscriber that has this endpoint as its Associated Endpoint.
Allow Proxy Bypass	Proxy Bypass is a system-wide OpenScape Voice feature that is turned on per default. It is only used when deploying Type 2 or 5 branch offices. If selected (enabled), Proxy Bypass allows OpenScape Voice to bypass the recorded proxy in a contact if an INVITE request to the contact's recorded proxy does not receive a response within a specified time.This attribute is not applicable for SIP Private Networking.

- The calling subscriber must be calling from a different survivable branch or must be directly registered with the OpenScape Voice.

- Enable subscriber rerouting by setting “Enable Rerouting to SIP Subscribers” and defining a “Subscriber Rerouting Prefix Access Code”. The suggested Rerouting PAC is “*001”.
- The survivable proxy must be configured to handle the inbound PSTN calls to the isolated subscribers, without the assistance of OpenScape Voice, to handle the case of a total WAN outage (lack of even signaling connectivity).
- OpenScape Voice assigns the **Operational State** to SIP Endpoints. Rerouting will happen to all Endpoint Operational States; for detailed information, see chapter **Endpoints and Endpoint Management**. The Normal State Rerouting depends on the configuration of the OSV SIP Timers. For more information, see chapter **How to Configure Parameters for SIP Timers**.
- For information regarding the Subscriber Registration Status, see chapter **How to Query the Registration Status of a Subscriber**.
- The necessary SRX parameters to be configured can be found in chapter **How to enable Rerouting for SIP Subscribers - System-wide-level**.

Gateway rerouting

For calls to the PSTN via SIP gateways or for calls to another SIP server, rerouting can also be done in case no definitive response code (1xx, 200, 3xx, 4xx, 5xx, 6xx) is received after the OpenScape Voice sends the INVITE message to the SIP gateway or another SIP server. When rerouting becomes necessary, OpenScape Voice does the following:

- Immediately routes all subsequent calls to the next available route.
- Marks the unresponsive first gateway as inaccessible, and stops routing calls to it.
- Performs an audit of the unresponsive gateway for a provisionable time.
- Automatically switches back to the first gateway when the audit mechanism indicates that the gateway has become responsive.

Related concepts

Load Balanced Traffic to Gateways on page 898

Gateway Rerouting on page 898

Other SIP Server

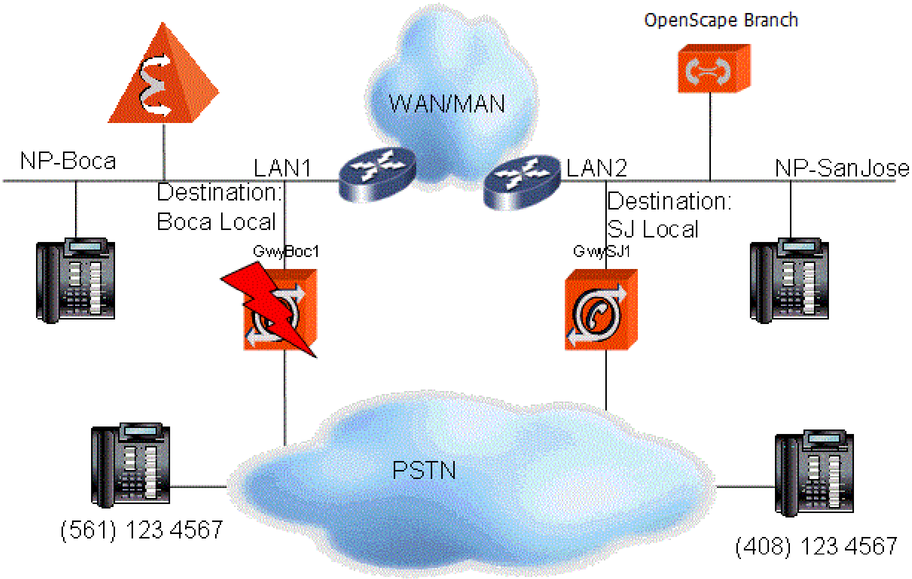
SIP Subscriber

Advanced Gateway SIP Rerouting on page 899

SIP Rerouting Feature Impacts on page 900

9.1.5.1 Gateway Rerouting

When a main office subscriber (Boca) makes a local call to the PSTN, the call is routed to Boca's gateway. If Boca's gateway is out of order, e.g. due to all circuits busy or a hardware failure, the call is rerouted to San Jose's gateway.

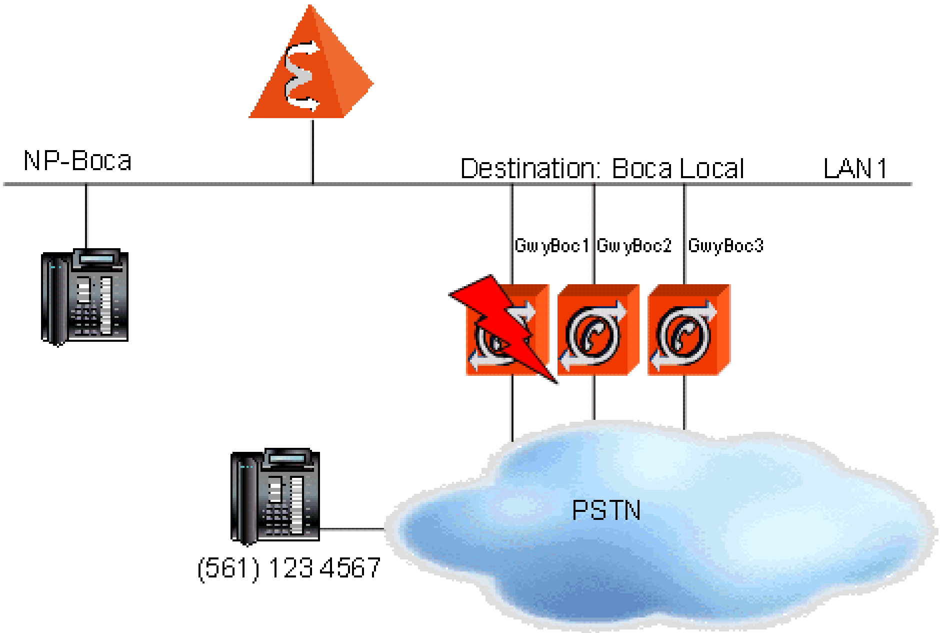


Related concepts

Rerouting based on SIP Response Codes, Response Timeout or WAN outage on page 895

9.1.5.2 Load Balanced Traffic to Gateways

Endpoints of the OpenScape Voice dial a prefix access code to access subscribers in the PSTN. The traffic to the gateways is load balanced by not prioritizing the routes for the “Boca Local” destination. When a gateway returns a rerouting SIP response code, the call is rerouted to another route (that is, gateway) of the “Boca Local” destination.

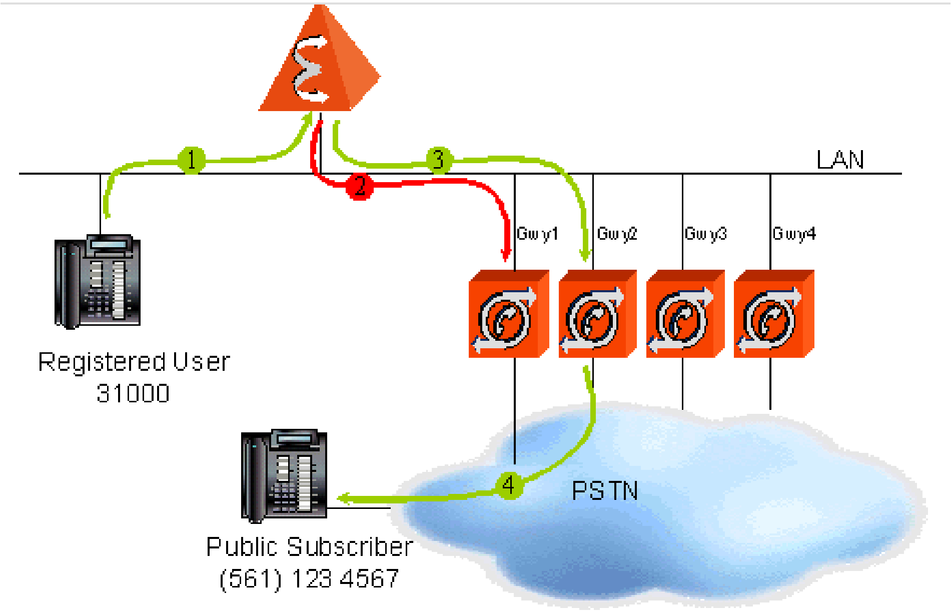


Related concepts

Rerouting based on SIP Response Codes, Response Timeout or WAN outage on page 895

9.1.5.3 Advanced Gateway SIP Rerouting

This scenario shows improvements that minimize the effects of SIP gateways that become "unresponsive". As soon as 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. An audit of the defective gateway is started in order to detect the gateway becoming active again. When the audit is successful, calls can be routed to the gateway again.



1) In a typical scenario, the registered user 31000 makes an outgoing call to the public network subscriber (561) 123 4567. In this example, there are 4 routes administered in the OpenScape Voice for this destination: Gwy1, Gwy2, Gwy3 and Gwy4. The OpenScape Voice will try three of these routes in the provisioned order, when the route list is not prioritized.
2) If Gwy1 is congested or unplugged or faulty, the call to Gwy1 may time out after the provisioned rerouting timeout value. The OpenScape Voice will take the gateway out of service until it is determined to be in service again.
3) The OpenScape Voice will then offer the call to the next provisioned route: Gwy2.
4) Assuming that Gwy2 is operational, the call will reach the requested public network subscriber.

Related concepts

Rerouting based on SIP Response Codes, Response Timeout or WAN outage on page 895

9.1.6 SIP Rerouting Feature Impacts

The rerouting based SIP code has an impact on some features, because some of them will not behave as in the non-failure case.

Functional Description

1) Rerouting for Subscribers:
   - To the OpenScape Voice, rerouting for subscribers looks like a call forwarded by that subscriber. All current feature interactions for a forwarded call by the subscriber apply.

2) Hunt Groups:

- For calls to an MLHG Pilot DN, the Hunt Group settings indicates whether Subscriber Rerouting is allowed for the calls distributed to the MLHG members. Navigate to **OpenScape Voice -> Business Group -> Teams -> Hunt Groups -> Add -> Advanced** and enable the Enable Basic Subscriber Rerouting option by checking the checkbox. This feature controls whether Basic Subscriber Rerouting is allowed in case a distributed call to a HG member is rejected due to Call Admission Control or WAN failure. The default value is unchecked (disabled).

NOTICE:

It is not possible to activate the Enable Basic Subscriber Rerouting parameter for Hunt Groups with Hunting Type set to either Manual, Parallel – Call Pickup Model or Parallel – Simultaneous Alerting Model.

3) Simultaneous Ringing:

- A call to a primary or secondary member of a simultaneous ringing group is rerouted through the PSTN.
- When the primary subscriber of a simultaneous ringing list is experiencing a WAN outage, the call to that primary subscriber is rerouted through the PSTN, but the other members of the simultaneous ringing list are not called.
- When the primary subscriber of a simultaneous ringing list is experiencing a CAC restriction, the call to that primary subscriber is rerouted through the PSTN and then the other members of the simultaneous ringing list are called.

4) Serial Ringing:

- A call to a primary or secondary member of a serial ringing group is rerouted through the PSTN.
- When the primary subscriber of a serial ringing list is experiencing a CAC restriction, the call to that primary subscriber is rerouted through the PSTN and then the serial ringing list is activated on the incoming call from the gateway to the serial ringing list. The serial ringing list will advance from there. If the CAC restriction occurs on another member of the serial ringing list, the call is rerouted. However it will be the last subscriber called in the serial ringing list because the serial ringing list feature is terminated once the call gets rerouted.
- When the primary subscriber of a serial ringing list is experiencing a CAC restriction, the call to that primary subscriber is rerouted through the PSTN and then the serial ringing list is activated on the incoming call from the gateway to the serial ringing list. The serial ringing list will advance from there. If the CAC restriction occurs on another member of the serial ringing list, the call is rerouted. However it will be the last subscriber called in the serial ringing list because the serial ringing list feature is terminated once the call gets rerouted.

5) Do Not Disturb (DND):

- A call to a SIP Proxy Subscriber that has the OpenScape Voice feature Do Not Disturb (DND) activated is not rerouted.

6) Outgoing Call Barring:

- The calling party needs to have the right to make outgoing calls via the PSTN in order for rerouting via the PSTN to take place.

7) Hot Desking:

- This feature allows a branch subscriber to freely move between branches by just registering the SIP subscriber from within another branch. Rerouting will not be activated for these subscribers, because if their external number would be dialed, the destination gateway would not be the Survivable SIP Proxy's gateway, but the gateway in the original branch.

Related concepts

Rerouting based on SIP Response Codes, Response Timeout or WAN outage on page 895

9.1.7 Media Server Survivability with 1+1 Redundancy

The media servers are usually collocated with the OpenScape Voice cluster nodes. Media server survivability can be achieved for both, geographically collocated and separated OpenScape Voice Clusters.

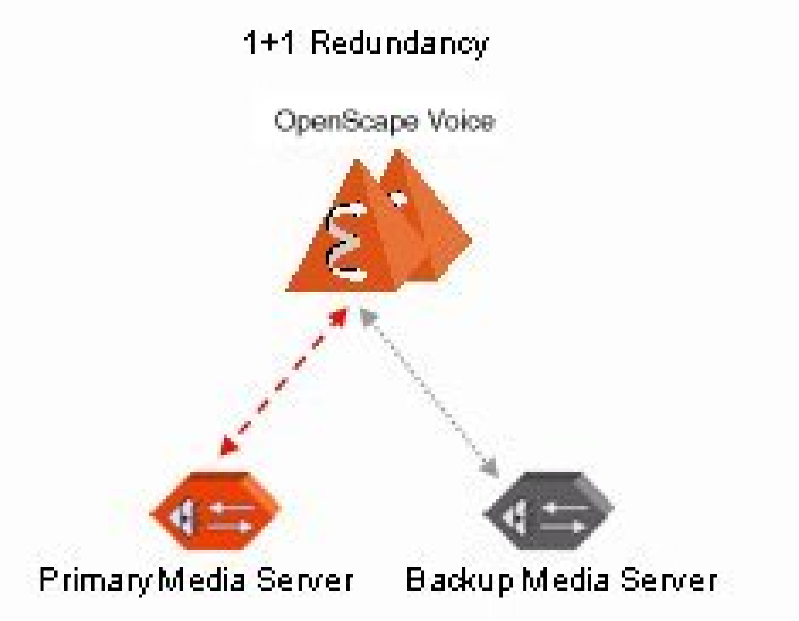
Functional Sequence

In normal operation, the primary media server of site A is operational and handles all the media server traffic from the OpenScape Voice. When the media server of site A becomes inoperative, the OpenScape Voice automatically switches the media server traffic to the backup media server B in site B.

Other Characteristics

Comparable redundancy can be achieved, when the OpenScape Voice cluster nodes and thus usually also the media servers are geographically separated. In normal operation, either of the following configurations are possible:

- The media server of site A is operational and handles all the media server traffic from the OpenScape Voice, and the media server of site B serves as backup.
- For branch offices, load balancing between branch offices is achieved by assigning each branch office its own rate area. The media server resource is assigned to the endpoint based on the endpoint’s rate area.



Related concepts

Failover Scenarios with OpenScape Voice and Media Server on page 903
Media Server Survivability with N+1 Redundancy on page 904
Media Server Survivability with N+k Redundancy on page 905

9.1.8 Failover Scenarios with OpenScape Voice and Media Server

In a cluster system, when a node fails, then established calls will be preserved but any unstable calls may be dropped. When the failing node is the last active node in the system, then all ongoing calls may be dropped.

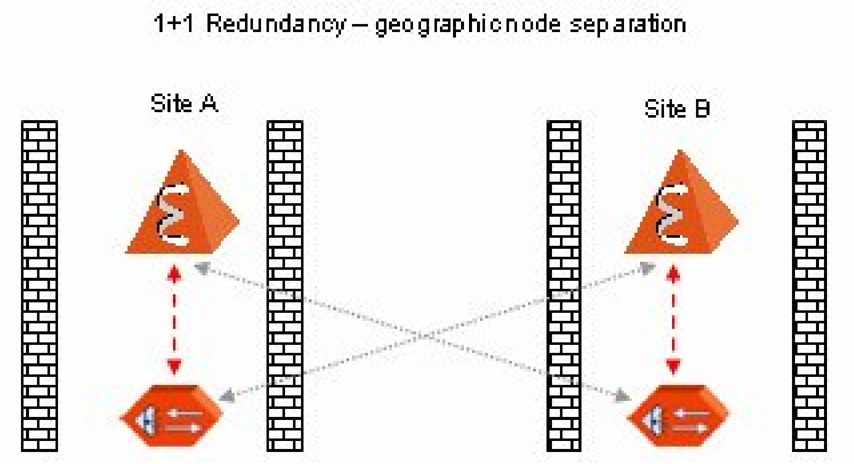
Functional Sequence

There are 3 failover scenarios related to the 1+1 redundancy:

- Node Failure: When an OpenScape Voice node fails, the other node handles all the traffic.

> **NOTICE:**
>
> The MGCP signaling manager on the partner node continues to use the same media server as it did before the node failure took place.

- Media server failure: When the primary media server fails, the OpenScape Voice automatically switches the media server traffic to the backup media server.
- Site or building failure: When there is a total failure of site A, the partner OpenScape Voice node detects this event and starts using the site B media server.



Related concepts

Media Server Survivability with 1+1 Redundancy on page 902

9.1.9 Media Server Survivability with N+1 Redundancy

When the media servers are collocated with the major branch offices, there is a possibility to have only one backup media server located at the OpenScape Voice cluster nodes. This is called N + 1 redundancy, since there is one redundant media server for N branch offices. N + 1 media server survivability can be achieved for both, geographically collocated and separated OpenScape Voice Clusters. In normal operation, the media servers at all branches are operational and handle all the media server traffic from the OpenScape Voice. Load balancing is achieved by assigning each branch office its own rate area.

In N+1 redundancy, N represents the number of primary media servers. These are the media servers that are first in the list of media servers in a destination of media servers. If N is greater than 1, an origin destination must be created to create a specific media server for a specific branch office. This is equal to the number of offices (branch + main) that have a local media server.

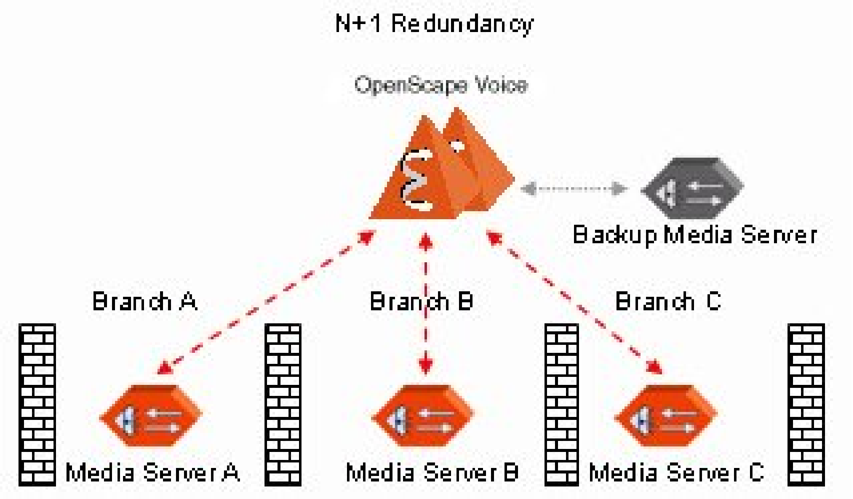
Functional Sequence

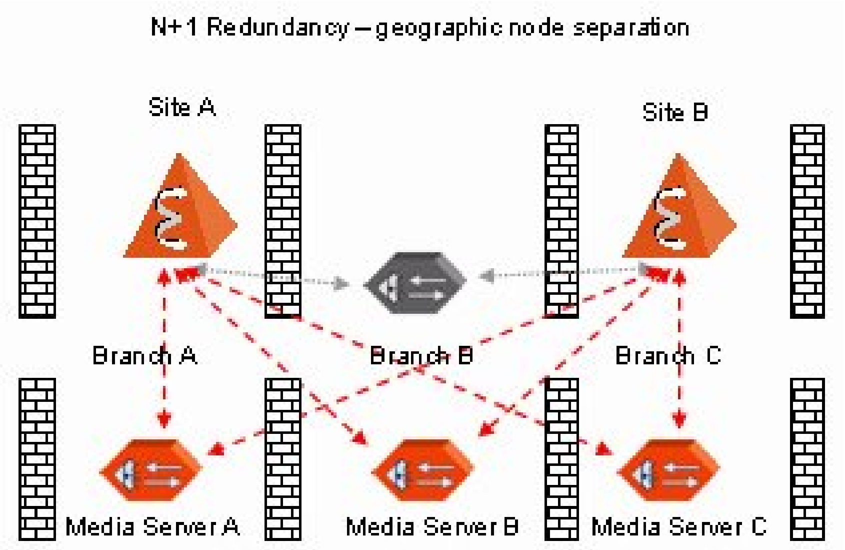
In case of failure, the following takes place depending on the failure type:

- Node failure: When an OpenScape Voice node fails, the other node takes over.

> **NOTICE:**
>
> The MGCP signaling manager on the partner node still uses media servers in the same manner as before the failure.

- Media server failure: When a branch’s media server fails, the OpenScape Voice detects this event and the branch starts using the centralized backup media server. The other branches continue to use their own media servers.
- Branch failure: When an entire branch fails, the other branches continue to use their own media servers and are unaffected by the failure.
- WAN failure: When the WAN connection with a particular branch fails, the other branches are unaffected by the failure.





Related concepts

Media Server Survivability with 1+1 Redundancy on page 902

9.1.10 Media Server Survivability with N+k Redundancy

When the media servers collocated with major branch offices are locally redundant and the smaller branch offices would use a backup media server located at the OpenScape Voice cluster nodes then this is called N + k redundancy. N + k media server survivability can be achieved for both, geographically collocated and separated OpenScape Voice Clusters. In normal operation, the media servers at all branches are operational and handle all the media server traffic from the OpenScape Voice. Load balancing is achieved by assigning each branch office its own rate area.

In N+k redundancy, N represents the number of primary media servers just as it does in N + 1 redundancy. K represents the number of backup media servers for a given primary media server. This number may be different for each primary media server.

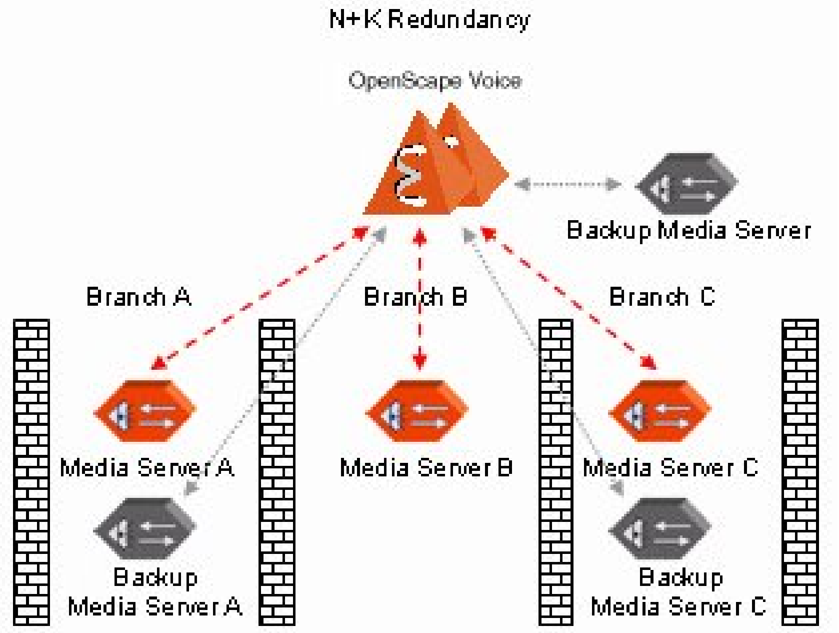
Functional Sequence

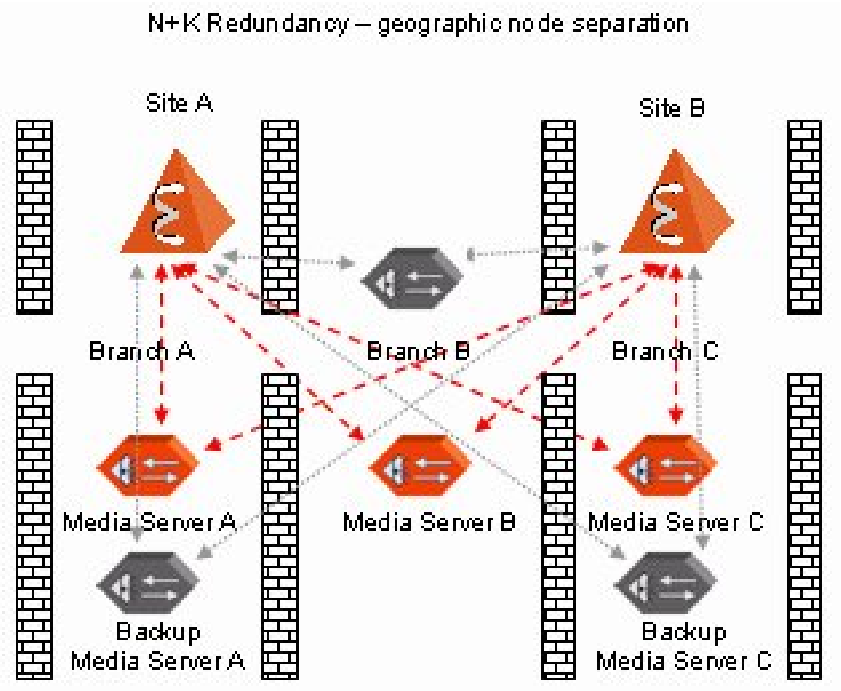
In case of failure, the following takes place depending on the failure type:

- Node failure: When an OpenScape Voice node fails, the other node takes over.

> **NOTICE:**
>
> The MGCP signaling manager on the partner node still uses media servers in the same manner as before the failure.

- Media server failure: When any of the three active media servers fails, the OpenScape Voice detects this event. If the branch has its own backup, the OpenScape Voice starts using that media server. If the branch does not have its own backup, or if the backup server also fails, the OpenScape Voice starts using the centralized backup media server.
- Branch failure: When an entire branch fails, the other branches continue to use their own media servers and are unaffected by the failure.
- WAN failure: When the WAN connection with a particular branch fails, the other branches are unaffected by the failure.





In both figures, the following elements are present:

- Each branch office has its own media server, for a total of three primary media servers.
- One centralized backup media server is located at one of the OpenScape Voice cluster nodes.
- Two branches (A and C) also have their own backup media servers. These two branches might represent larger offices, whereas Branch B might be a smaller branch that does not require local redundancy.

As a result, branches A and C have two backup media servers; branch B has one.

Related concepts

Media Server Survivability with 1+1 Redundancy on page 902

9.2 Cluster Redundancy

Reliability is the primary goal of OpenScape Voice, and clustering is necessary to provide this reliability. A reliable component structure provides an effective base for cluster administration.

The OpenScape Voice hardware and software components work together to attain the following reliability goals:

- To provide faster data replication and better performance for peak traffic in normal operation by using a two-node active-active configuration, with each node acting as hot/standby for its partner. This configuration also protects against silent faults through continuous hardware/software monitoring and testing.
- To minimize node switchover, which reduces transient call loss and network connectivity outages. This is accomplished with redundant local disks,

network connections for each node, and power supplies. Each node also contains duplicated Ethernet cards which ensure that the physical path for the external communication with one node is backed up by a second path —a second Ethernet port on a different Ethernet card, and a second LAN switch.
- To provide static load sharing for fast and reliable busy/idle handling, because only one node writes the busy/idle and call status for the subscriber or feature server.
- To provide effective component management through process configuration control using process and alias groups.

9.2.1 Configuration Options

The OpenScape Voice redundant configuration can be deployed as geographically co-located or separated node configuration. The separated configuration can be distinguished further, into whether nodes are in the same subnet, diffferent subnets or connected only via layer-3 (IP).

> **IMPORTANT:**
>
> Enterprises have the option to define more than one default gateway—specifically, the management, signaling, and billing/CDR redundant connections from each node. However this capability should only be deployed if an enterprise does not permit routing between subnets on its network. Always contact your next level of support for assistance in configuring this feature.

Related concepts

Cluster Redundancy with Geographic Node Separation on page 908
Cluster Redundancy with Co-Located Nodes on page 909

9.2.2 Cluster Redundancy with Geographic Node Separation

Geographic node separation reduces the risk of total loss of voice services when one of the nodes is out of service due to a fire, flood, hurricane, building damage, and so on. OpenScape Voice allows geographic separation of the cluster nodes, either in the same subnet or in different subnets.

System Specific Information

Each node has:

- Six Ethernet links that are paired and bonded to support the management, signaling, and billing/CDR redundant connections from each node.
- A single remote administration link.
- One cluster interconnect link for separation with layer-3 cluster interconnect: Because IP routing is used for the cluster interconnect signaling messages, only a single layer-3 IP connection is required. The company’s WAN can be used for the cluster interconnect instead of a redundant fiber-optic link.

Related concepts

Configuration Options on page 908
Geographic Separation - Nodes in Same Subnet on page 910
Geographic Separation with Layer-3 Cluster Interconnect on page 911

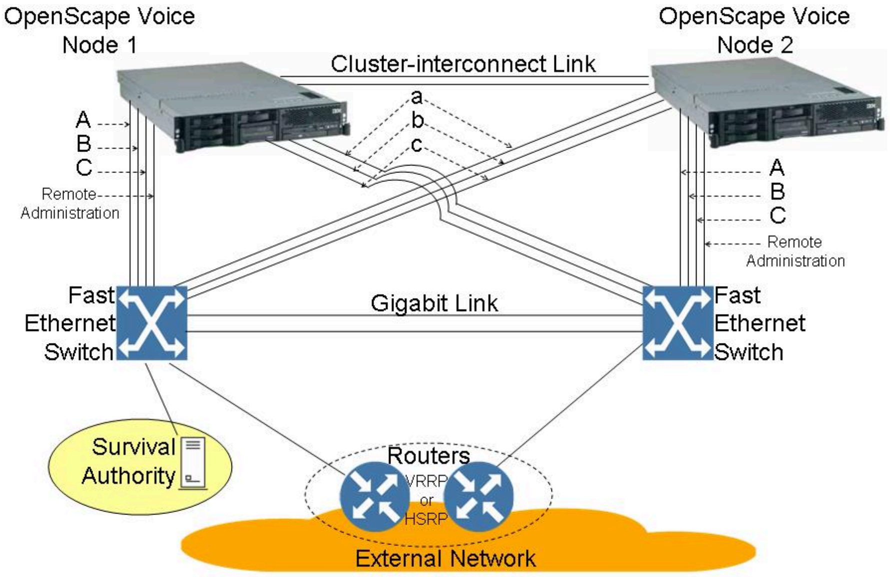
9.2.3 Cluster Redundancy with Co-Located Nodes

One option of an OpenScape Voice redundant system is when two computing nodes are geographically co-located.

Geographically Co-Located Redundant System

Each node has six Ethernet links that are paired and bonded to support three redundant connections from each node. These connections are designated in the figure as follows:

- OAM&P: Path A represents the primary communication path; path a represents its backup path.
- Signaling: Path B represents the primary communication path; path b represents its backup path.
- Billing/CDR: Path C represents the primary communication path; path c represents its backup path.



For example, Port A on node 1 serves as a primary communication path for OAM&P; port a on node 1 acts as a backup when the primary port fails.

Other Characteristics

The following are also present:

- A link, known as the remote access connection, provides the ability to remotely power down and reset a node; it also permits communication with the partner node to verify its status, as described for x3650T and FSCPRIMERGYRX330S1
- Two additional links, which are used for communication between the two nodes (also referred to as cluster interconnect signaling).
- An optional survival authority.

Related concepts

Configuration Options on page 908

9.2.4 Geographic Separation - Nodes in Same Subnet

For cluster redundancy with geographic separation with nodes in the same subnet the nodes may physically reside in the same location or in different locations. The latter case requires a VLAN bridging to logically interconnect them into the same subnet.

NOTICE:

Although other configurations are possible, the configuration shown in the figure is recommended because it helps to avoid routing/packet forwarding loops, therefore minimizing the need for spanning tree protocol (which detects and controls packet forwarding loops). Additional redundant paths can be provided, but doing so results in a more complex LAN switch and router configuration.

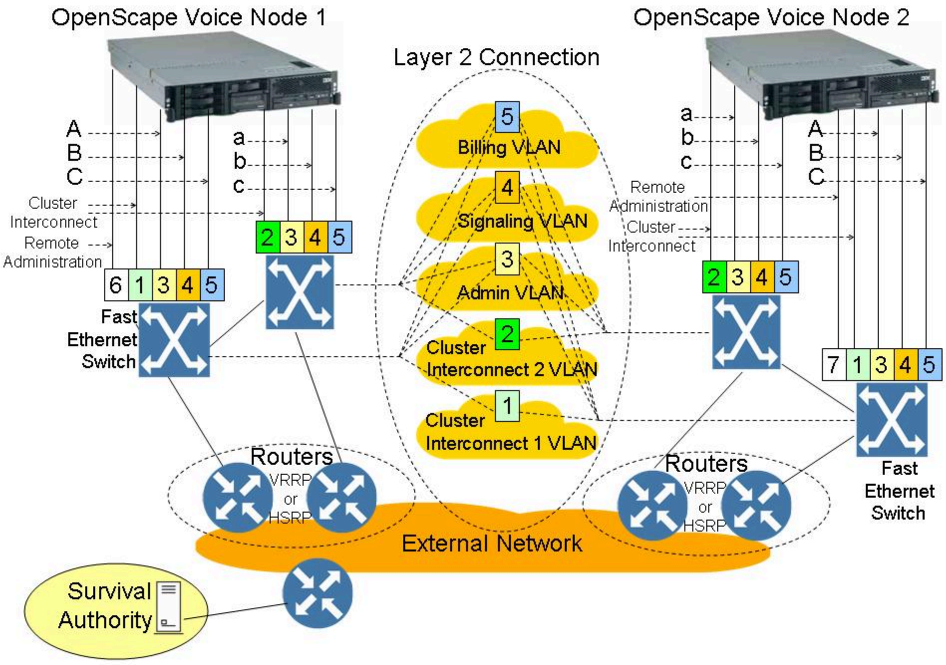
IMPORTANT:

In case of VLAN bridging special care needs to be taken by the network administrator to ensure that the network routers have rerouting capability of these virtual IP addresses to the access routers at either node of the geographically separated cluster.

Requirements

All OpenScape Voice virtual IP addresses have to exist in both locations.

Geographic Separated redundant Systems—Nodes in Same Subnet



Related concepts

Cluster Redundancy with Geographic Node Separation on page 908

9.2.5 Geographic Separation with Layer-3 Cluster Interconnect

For a cluster redundancy with layer-3 cluster interconnect, only a layer-3 IP connection is required between the two nodes.

NOTICE:

This option does not require spanning VLANs between the two nodes.

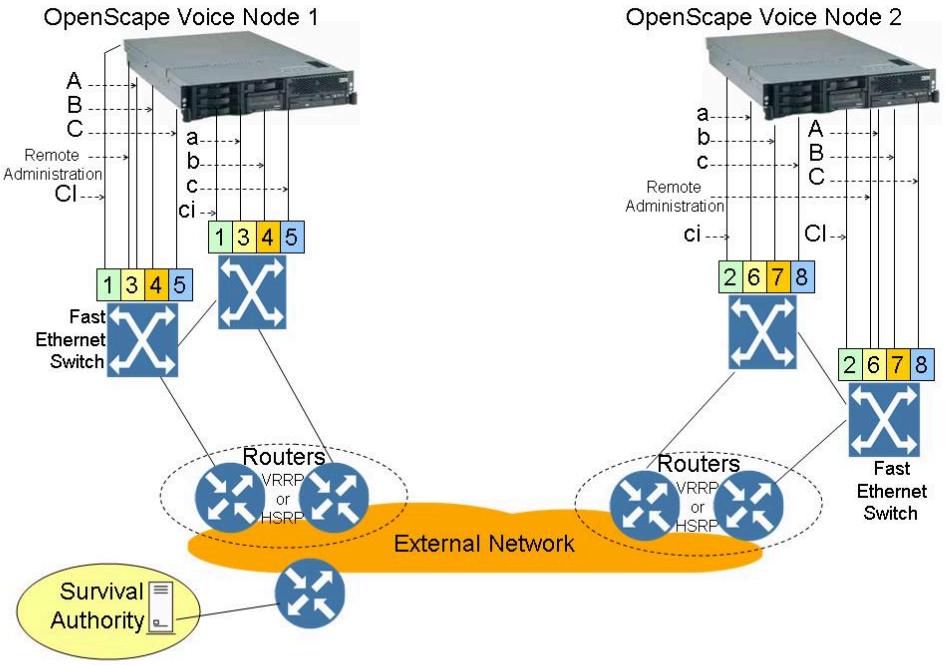
IMPORTANT:

OpenScape Voice also supports the use of low-bandwidth cluster interconnect links, which make geographically separated redundant nodes an economical option for smaller installations. However, degradation in system performance should be expected when these links are used. The performance degradation affects both call processing capabilities as well as mass provisioning times. Packet delays on the interconnect link (any values above 100-ms roundtrip time) can also cause performance degradation in mass provisioning times.

Functional Sequence

If the primary network interface (represented by CI in the figure) fails, the Linux bonding driver uses the backup interface (represented by ci in the figure).

Geographically Separated Redundant System with Layer-3 Cluster Interconnect



Related concepts

Cluster Redundancy with Geographic Node Separation on page 908

9.2.6 Survival Authority

A Survival Authority (SA) decides on the shutdown or continuation of processing for a node in the failover case wherein the two nodes cannot communicate over the cluster cross connects and cannot shutdown the partner node via the maintenance controller. Its main function is to determine which node should continue running, and which node should be shut down during a massive power outage or building failure. In the case of a geographically separated cluster, the Survival Authority is mandatory. For a co-located cluster a SA is optional if the cross connect between both nodes is a physical LAN cable (e.g. both nodes in the same rack) and mandatory if the cross connect link between the nodes is setup over switches. In this case, the SA must be on a separate server (separate subnet).

NOTICE:

A Stand Alone Service (SAS) feature is offered. Instead of shutting down one node, the node that takes over goes into a "Stand Alone Primary" state while the node which is supposed to shutdown and reboot goes into a "Stand Alone Secondary" state. This allows phones local to each node to continue making calls to each other or even calls to the PSTN via the local gateway available on that network.

NOTICE:

Even though there can only be one SA, it is not a single point of failure since it is not needed for OpenScape Voice operation. SA is only needed when the two nodes cannot communicate over the redundant x-channel and the maintenance controller of the partner node.

Functional Sequence

To avoid a split brain situation the SA is the final decision maker when two OpenScape Voice server nodes cannot communicate over the redundant cluster cross connects and the maintenance controller of the partner node.

System Specific Information

In redundant co-located and geo-separated integrated duplex configurations (redundant OpenScape Voice servers with integrated OpenScape Applications software) the survival authority should be installed on a third (off-board) SLES 12 machine. In the case of redundant co-located and geo-separated standard duplex configurations (redundant OpenScape Voice servers without integrated OpenScape Applications software) the Survival Authority is implemented as a software module integrated with the OpenScape Voice Assistant software of the off-board OpenScape Applications server.

More details about installation and configuration of the Survival authority can be found in the following manual:

OpenScape Voice, Service Manual: Installation and Upgrades, Installation Guide

Other Characteristics

The communication between each OpenScape Voice node and the SA is tested every 10 minutes and a failure is alarmed. So in order to have a problem with the Survival Authority, three conditions need to be present:

- Communication failure between OpenScape Voice and SA.
- Survival Authority Alarms are being ignored.
- A node or network failure resulting in failures of both x-channels and communications to the partner maintenance controller.

9.2.7 Standalone Service

When the standalone service is enabled, the node that does not get the permission to take over from the Survival Authority stays active. Standalone service is available to duplex voice server configurations and is intended for geographically separated installations. These geographically separated installations can be layer-3 network separated or geo-separated with layer-2 connectivity (both nodes of the layer-2 configuration are on the the same IP networks but at different locations) . In case of a virtual OSV cluster standalone service is only allowed for a layer-3 network separated installation.

> **NOTICE:**
>
> It is advisable to consider both the benefits and drawbacks of enabling standalone service.

Failure Scenarios

There are 3 failure scenarios with enabled StandAlone service on a layer-2 geographic separated installation:

- Node failure: IMM/iRMC connection is still available. The partner node takes over and activates virtual IPs of failed node.
  - Test case of a node 1 failure: Remove both x-channel cables.
- Network failure: Partner node takes over. It does not activate IPs because they may still be active.
  - Local phones use the IP of their local OSV node.
  - Test case of failure: Removal of cable from both Maintenance Controllers and remove x-channel cables.
- Total Site failure: Same as network failure. There is no virtual IP failover.
  - In total Site failure, phones are probably impacted by the site failure and would not be able to use the fail-over IP on the remote node.

    Test case of the failure: Removal of both power cables of one node.
  - For non-local phones it is recommended to be configured with DNS-SRV, so that they can switch-over to the IP address of the partner node, if needed. Otherwise, connect the phones to an OpenBranch and configure the OpenBranch with the IP addresses of the two OpenScape Voice nodes.

OpenScape Voice distinguishes between node failure and network/site failure by checking the IMM/iRMC connection:

- If there is an X-channel failure plus IMM connectivity failure then there is a Network/Site failure.
- If there is an X-channel failure but IMM connection is still available then there is a node failure.

Other Characteristics

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.

Related concepts

Standalone Service Subscriber Feature Impacts on page 915
Standalone Service Other Network Elements Impacts on page 916
Standalone Service TLS Connection Impacts on page 916

9.2.8 Standalone Service Subscriber Feature Impacts

Feature activation and deactivation, as well as subscriber-controlled input 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.

NOTICE:

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."

System Specific Information

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
- OpenScape Voice-based call forwarding features, including remote activation
- 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)

NOTICE:

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 don't need database writes are still functional—for example:

- Call hold
- Consultation
- Call transfer
- Conference
- Call pickup

Related concepts

Standalone Service on page 913

9.2.9 Standalone Service Other Network Elements Impacts

Because Standalone mode is caused by network connectivity problems, it is very likely that OSV functionality is impacted by communication loss with other VoIP devices.

Especically the OSV node in standalone-secondary is likely to be isolated from other devices (since it lost communication with the partner node and the survival authority).

System Specific Information

Below are examples of reduced or lost functionality caused by communication loss.

- Media servers: No announcements, music on hold, or station-controlled conferences
- PSTN gateways: No calls to and from the PSTN
- OpenScape UC Application, CSTA applications: No presence, one number service (ONS), OpenScape-controlled conferences, or click to dial
- 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

IMPORTANT:

The reduced or lost functionality caused by communication loss is not caused by the standalone operation mode. Both standalone mode and these impacts are results of the network problems.

Related concepts

Standalone Service on page 913

9.2.10 Standalone Service TLS Connection Impacts

Before OpenScape Voice starts a new SIP call, it reads information about the existing TLS connection between OpenScape Voice and applicable SIP phones from the database; it then uses this information for the duration of the call.

NOTICE:

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:

- 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)

Related concepts

Standalone Service on page 913

9.2.11 FSC PrimeCluster Protection Mechanisms

The Fujitsu-Siemens PrimeCluster software allows the OpenScape Voice application software on each node to know the state of the other node. This information is important because in clusters, resources are usually controlled by one of the cluster nodes. All other nodes keep a backup of the resources in case they need to take over control if the controlling node fails. The cluster software has as a task to prevent the so-called “split brain” situation where two nodes of a cluster think that they are controlling the same resource.

NOTICE:

Instead of shutting down one node, the node that takes over goes into a "Stand Alone Primary" state while the node which is supposed to shutdown and reboot goes into a "Stand Alone Secondary" state. This allows phones local to each node to continue making calls to each other or even calls to the PSTN via the local gateway available on that network.

Functional Sequence

To keep track of the state of the other node, the PrimeCluster software maintains a heartbeat between the two nodes through the cluster-interconnect (two interfaces used for redundancy and load balancing of the information that is shared between the two nodes of the cluster). The frequency of the heartbeat is once per 200 milliseconds and once 50 consecutive heartbeats are missed, the PrimeCluster software activates its Split Brain defense mechanism. In this situation, the PrimeCluster software must be ensured that only one of the nodes controls the common resources. This is done by stopping one of the nodes unconditionally. In PrimeCluster terminology, the Split Brain Defense mechanism is called the Shutdown Facility (SF) and it starts any number of Shutdown Agents consecutively until one of the nodes is shutdown. The PrimeCluster provides two shutdown agents in the following order:

- SA_IPMI
- SA_DOWN

After the shutdown agents have run, the OpenScape Voice cluster should have one node shut down and one node active.

In voice server configurations where the nodes share the same subnet (for the Management, Signaling and Billing interfaces) the active node has all virtual IP addresses activated that were running on the shut down node. When a virtual

IP address is activated on the OpenScape Voice node that takes over, it sends out a so-called gratuitous address resolution protocol (ARP) to inform the LAN switches and routers of the network about the new MAC address for the virtual IP address. The routers and the LAN switches then reconfigure to adapt to the new situation. A network scheme in which voice server nodes share the same subnet for the Management, Signaling and Billing interfaces is common for co-located voice server clusters. For voice server configurations with network separation (each node has different subnets for the Management, Signaling and Billing interfaces) endpoints have to switchover to the partner node IP (on the active node). This type of networking scheme is common for geo-separated clusters.

Related concepts

DOWN Shutdown Agent on page 919

Hardware Components on page 920

9.2.12 IPMI Shutdown Agent

The IPMI Shutdown Agent is a mandatory mechanism to avoid split brain situations in case of a loss of communications between nodes in a redundant voice server configuration. It is designed to protect against single point of failure scenarios.

Functional Sequence

IMPORTANT:

There are conceivable situations where no take over occurs, all related to highly unlikely double failures of either the cluster nodes and/or the communication to the survival authority. Some of these can be resolved with the optional DOWN Shutdown Agent.

After PrimeCluster detects that it cannot communicate with its partner node, it checks its node priority. Node 2 has a higher priority than node 1. For node 2, it immediately sends an IPMI set command through the admin network of node 2 to the remote maintenance controller (iRMC/IMM card) of node 1 with the request to power cycle. For the specified IPMI timeout period node 2 will try to read the state of node 1 by querying its remote maintenance controller interface. When node 1 reports that it has power cycled or that it was already power cycled, then in voice server configurations wherein the nodes share the same subnet for the Management, Signaling and Billing interfaces the active node has all the virtual IP addresses activated that were running on the shut down node. When a virtual IP address is activated on the OpenScape Voice node that takes over, it sends out a so-called gratuitous address resolution protocol (ARP) to inform the LAN switches and routers of the network about the new MAC address for the virtual IP address. The routers and the LAN switches then reconfigure to adapt to the new situation. A network scheme in which voice server nodes share the same subnet for the Management, Signaling and Billing interfaces is common for co-located voice server clusters.

For voice server configurations with network separation (each node has different subnets for the Management, Signaling and Billing interfaces) endpoints have to switchover to the partner node IP (of the active node). This type of networking scheme is common for geo-separated clusters. If on the other hand, node 2 fails, then node 1 will detect the cluster-interconnect failure and will start its SA_IPMI. Node 1 will delay its IPMI set command (with the request for node 2 to power cycle) by the total time required for the shutdown agents of node 2 to run (in order not to interfere with any node 2 request). For the specified IPMI timeout period node 1 will try to read the state of node 2 by querying its remote maintenance controller interface. When node 2 reports that it has power cycled or that it was already power cycled node 1 will take over the virtual IP addresses and resources of node 2 (in the same manner as described above for node 2 in the node 1 failure case).

9.2.13 DOWN Shutdown Agent

The DOWN Shutdown Agent is a mechanism to help solve the areas where no take over took place with the standard IPMI Shutdown Agent. The feature is based on the Survival Authority which is mandatory for geographically separated clusters. The Survival Authority is optionally available for co-located clusters, which would allow a node to take over in the case of inter-node communications failure. It is designed to protect against some double failure scenarios (but naturally not a failure of both cluster nodes). A failure of the Survival Authority itself leads to the same scenarios without takeover as the IPMI Shutdown Agent alone.

NOTICE:

A drawback of adding another shutdown agent is that the total waiting time for the secondary node (node 1) to activate the shutdown facility is the sum of all shutdown agents that could be running on the primary node. As a result, the takeover time that involved node 1 taking over from node 2 will increase.

NOTICE:

The Survival Authority functionality is implemented on a third (off-board) SLES 12 machine for redundant co-located and geo-separated integrated duplex configurations (redundant OpenScape Voice servers with integrated OpenScape Applications software). In the case of redundant co-located and geo-separated standard duplex configurations (redundant OpenScape Voice servers without integrated OpenScape Applications software) the Survival Authority is implemented as a software module integrated with the OpenScape Voice Assistant software of the off-board OpenScape Applications server.

Functional Sequence

The DOWN shutdown agent, when activated, will send an SNMP trap through the admin network to a device called the Survival Authority. The SNMP trap contains the information that the partner has left the cluster and that it is awaiting a decision by the Survival Authority on what to do next. The Survival Authority keeps a flag for the "Survival Mode" of each cluster for which it is responsible (more than one cluster is allowed). This flag is initialized to "Off".

On receipt of the SNMP trap, the Survival Authority sends back an SNMP set command with one of two actions: Take Over or Die, hence the name: DOWN Shutdown Agent. The SNMP set command is sent to the IP address of the admin network (same interface the trap was sent from).

- If the flag was set to "Off", the Survival Authority sends Take Over command sets the flag to "On," and records the name of the node that was allowed to survive.
- If the flag was set to "On" and the name of the node requesting advice is not the name that was recorded, then the Survival Authority sends a Die command.
- If the flag was set to “On” and the name of the node requesting advice is the name that was recorded, then the Survival Authority sends the Take Over command again.

The OpenScape Voice (OSC) server is running an SNMP subagent that receives the set request and writes the result (Take Over or Die) in a file that is being read by the DOWN shutdown agent. Upon reading the result, the shutdown agent will cause the node either to take over or to shutdown.

NOTICE:

When inter-node communications are restored, the Survival Mode flag is reset by an SNMP trap sent from the OSC Voice server to the Survival Authority.

NOTICE:

Instead of shutting down one node, the node that takes over goes into a "Stand Alone Primary" state while the node which is supposed to shutdown and reboot goes into a "Stand Alone Secondary" state. This allows phones local to each node to continue making calls to each other or even calls to the PSTN via the local gateway available on that network.

Other Characteristics

When the high priority node (node 2) is powered off, the wait time for node 1 to activate the shutdown agents (after the cluster interconnect failure is detected) is the sum of all shutdown agents that would be run on the high priority node (node 2).

Related concepts

FSC PrimeCluster Protection Mechanisms on page 917

9.2.14 Hardware Components

This section describes the OpenScape Voice; hardware components and how they contribute to cluster redundancy functionality. The three relevant hardware components are the Computing Node, the Ethernet Switch and the Remote Access Card.

System Specific Information

- Computing Node: Each computing node has eight 1 Gbit/s Ethernet links, set up as four pairs. A redundant pair of crossover cables, controlled by PRIMECLUSTER software, interconnects the nodes.
- Ethernet Switch: The two Ethernet switches are layer-2 LAN switches that allow several devices to interconnect. The computing nodes connect to the external network via both Ethernet switches. This process gives the system a measure of redundancy, and protects it in the event that one of the Ethernet switches fails.
- Remote Access Card: With clusters, there is always the necessity to resolve the situation where two nodes of a cluster think that they are in charge of the same resources and functions—for example, when the two nodes cannot communicate. In this situation, it must be ensured that a node can only become active when the other node has been stopped unconditionally. This capability is sometimes referred to as split-brain avoidance. The split-brain avoidance mechanism of PRIMECLUSTER requires a safe hardware interface to eliminate a node by powering it down or rebooting it. Depending on the server, the connection is provided by:

  1) x3650T: IMM

  2) FSCPRIMERGYRX330S1: IRMC

Related concepts

FSC PrimeCluster Protection Mechanisms on page 917

9.2.15 Software Components

This section describes the OpenScape Voice software components and how they contribute to cluster redundancy functionality. Two software components are relevant: the PRIMECLUSTER and the RTP software.

System Specific Information

- PRIMECLUSTER supports the cluster interconnect and offer applications well-defined interfaces which are required for cluster operation. These interfaces include internode communication which is used by processes on different nodes to communicate with each other. Unlike other external communication interfaces that are available in every operating system, the internode communication supports redundant connections for availability reasons and a low latency protocol. A short latency period (the time required to send a message to another system and receive an acknowledgment) is just as important to the scalability of a cluster as the line throughput rate, though both are closely linked.

- OpenScape Voice uses the RTP to run and manage the processes necessary for configuration, call processing, performance monitoring, and system maintenance. RTP provides redundancy and load sharing capabilities by enabling multiple computing elements, or logical nodes, within the system. While one process may be running on one CE, another process may be running on another CE within the system. Because the RTP can initiate multiple instances of the same process, different instances of the same process may run on different CEs within the system.

9.2.16 Functional Description

OpenScape Voice supports redundant active/active applications for cluster softswitches. During normal operation a redundant cluster operates in a loadsharing operation (active/active). Both nodes participate in traffic processing, observe each other and backs up the other nodes configuration data.

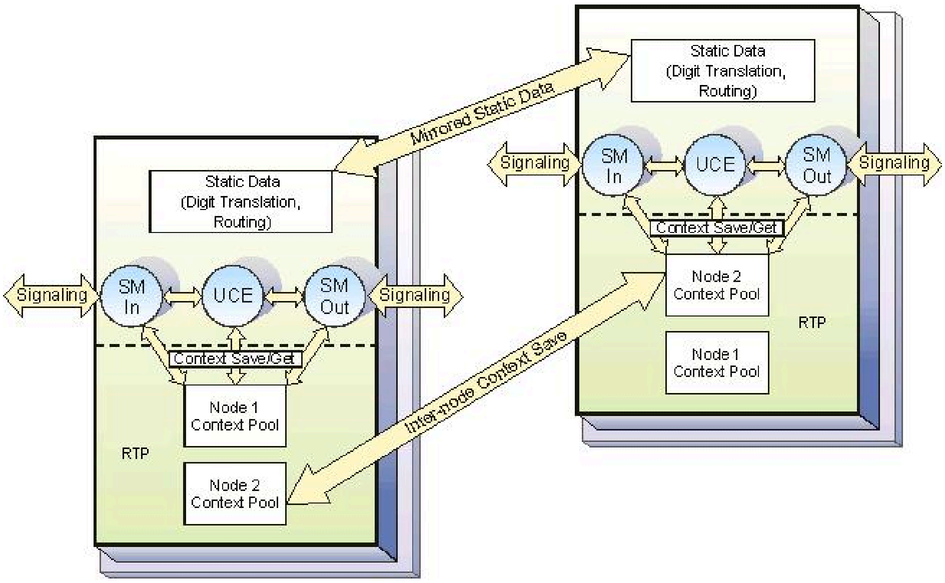
Functional Sequence

During normal operation, the cluster operates in an active/active mode:

- Traffic is distributed evenly across the available nodes and across the available call processing instances within each node.
- Each node serves as a backup to the other node.
- During call processing, each process saves its contexts to the backup node at various points in the call.

The Figure shows a normal active/active mode scenario with the RTP. When a hardware or software failure occurs, a backup node takes over the traffic of the failed node, preserving stable calls by accessing the partner context pool.

Normal Active/Active Mode with RTP Support



RTP

9.2.17 Failover Strategy

The primary focus of the OpenScape Voice failover strategy is to preserve stable calls and billing data, and to ensure that resources are not left in an unresponsive state—such that a given resource cannot be accessed without restarting a device, gateway, or the system itself.

NOTICE:

Beware, that despite cluster redundancy, if a backup hardware or software component fails while it is acting on behalf of a primary, and the primary has not been restored to service, calls may be lost and/or service may be affected. The depth of the service degradation depends on the specific component that failed. Reliability is the primary goal of cluster redundancy.

Related concepts

Process Failure on page 923
Ethernet Failure on page 924
Ethernet Switch Failure on page 925
Router Failure on page 926
Double Ethernet Switch Failure on page 927
Node Failure on page 927
Location Interconnect Failure on page 928
Catastrophic Site Outage on page 929
Double Failures with Collocated Nodes on page 929
Double Failures with Geographical Node Separation on page 930
OpenScape Voice Admin Network Failures on page 930
OpenScape Voice Signaling Network Failures on page 931
OpenScape Voice Billing Network Failures on page 931

9.2.18 Process Failure

Any single process instance failure does not affect service, with the possible exception of the call (context) being processed at the time of the failure. Each call context of a particular type is accessible by all process instances of that same type. If the last accessible process instance of a type fails on a node, the backup instances on the backup node take over. However, if the last accessible process instance of a type fails on the last active node, service is affected.

Last Failing Process	Consequence
Universal Call Engine	All calls dropped with a loss of the last 30 minutes of CDRs.
CSTA Signaling Manager	All CSTA calls dropped and new call attempts denied.
SIP SM Manager	No more call processing.
CDR Handler	CDRs accumulate until process is restarted.
XDM	SIP calls blocked.

For example, all Universal Context Engine (UCE) contexts are accessible by all UCE instances. If the last UCE instance on the last redundant node fails UCE contexts will be lost. But if a UCE fails during initial processing of a call, this call may be affected as well.

Related concepts

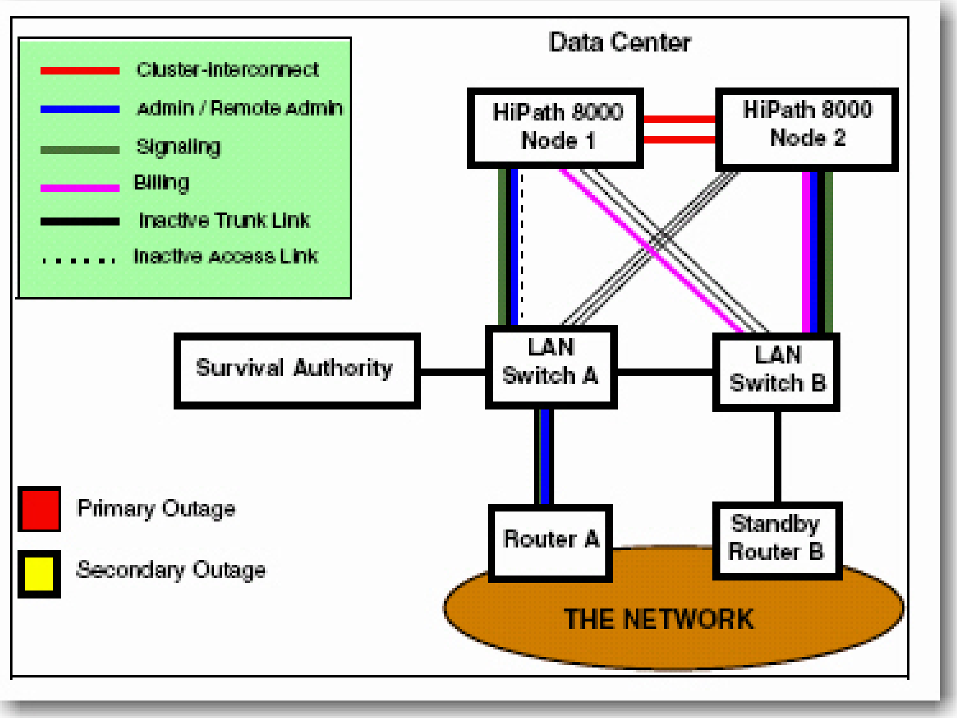
Failover Strategy on page 922

9.2.19 Ethernet Failure

An Ethernet failure can be caused by the failure of an Ethernet card, Ethernet port, or Ethernet cable. If a failure occurs, the OpenScape Voice node's Linux bonding driver switches the IP address to the second Ethernet port on the same OpenScape Voice node, then sends out a gratuitous ARP to update the routing tables in the LAN switch.

Other Characteristics

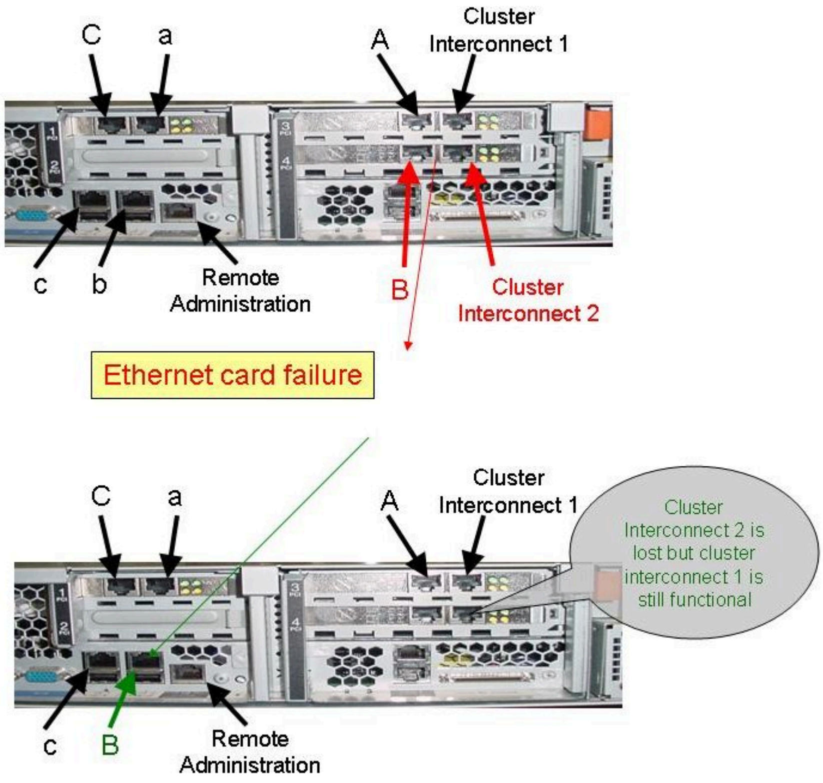
If an Ethernet port fails, that port is switched to its backup port connected to the node's other Ethernet switch. Any traffic on that system component routes to the new Ethernet switch on its path, via the gigabit link to the original Ethernet switch, and continues to its original destination.



For example, if the port to switch A on Node 1 fails, the following takes place:

1) All the data switches to the port to switch B on Node 1.
2) The data passes from the Ethernet switch B, through the Gbit link, to the Ethernet switch A connected to the failed port.
3) The data continues on its intended route.

The Figure below provides an example of this operation. The Ethernet card with the primary port for signaling (eth2) and the second cluster interconnect (eth3) has failed, so the backup port (eth6) has assumed the primary port's (eth2) functionality. Although the second cluster interconnect (eth3) is lost, all interconnect traffic can still flow through the first cluster-interconnect (eth1).



Related concepts

Failover Strategy on page 922

9.2.20 Ethernet Switch Failure

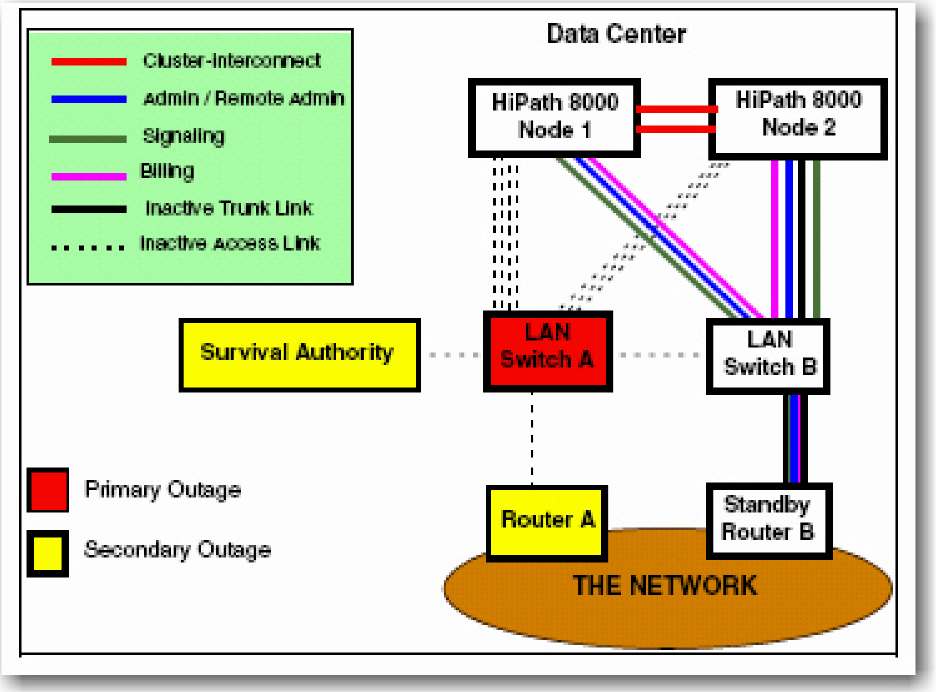
If a failure occurs in the Ethernet switch that is carrying active call data, each system component detects the failure and switches its links to the other Ethernet switch so no data is lost.

Functional Sequence

The Linux bonding driver provides an Ethernet port switchover function. Two Ethernet ports, preferably on different Ethernet cards in the same node, have identical Ethernet address. The bonding driver operates in active/standby mode.

Other Characteristics

For geographically separated configurations, failure of both Ethernet switches at a particular site causes the partner node to take over after consultation with the survival authority.



Related concepts

Failover Strategy on page 922

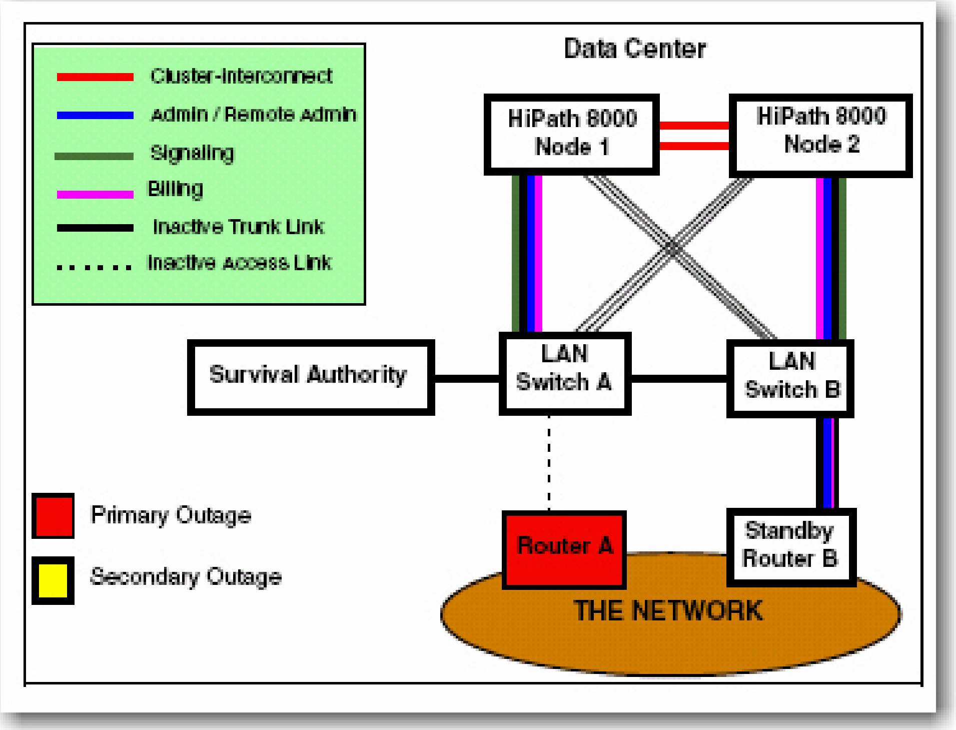
9.2.21 Router Failure

A redundant pair of routers operates in active-standby mode. Each of them being ready to take over the other router’s servicing function in case of a failure.

Functional Sequence

When a failure of the router servicing access to node 1 is detected, the standby router takes over using one of the following protocols:

- Virtual router redundancy protocol (VRRP)
- Hot-standby router protocol (HSRP)



Related concepts

Failover Strategy on page 922

9.2.22 Double Ethernet Switch Failure

A double Ethernet switch failure causes the partner node to take over because of loss of partner cluster interconnect communication after consultation of the Survival Authority. At the same time the router loses connection to the LAN, the WAN reroutes the traffic to the partner location.

Related concepts

Failover Strategy on page 922

9.2.23 Node Failure

If a node fails, stable calls (those in conversation state) are preserved but unstable calls may be dropped.

IMPORTANT:

Two parties shall be able to gracefully release a call established via node 1 after a switchover to node 2. The endpoint will retarget the BYE message to node 2 to ensure safe call clearing.

NOTICE:

If the failing node is the last active node in the system, all ongoing calls and their related billing data are lost.

Functional Sequence

If node 2 cannot reach the remote access connection of node 1, node 2 consults the survival authority and receives the takeover command back to trigger a failover of the IP addresses of node 1 to node 2.

Handling of queued calls in failover scenarios

After a node failover, queued calls are released. This prevents calls to stay in the queue forever, allowing the caller to try again.

To achieve this Survival Authority (SA) is involved. If StandAlone service is active, OpenScape Voice switches to split-brain mode (both nodes can handle calls). After the re-establishment of the x-channel, the failed node restarts.

If StandAlone service is inactive, the failed node restarts immediately.

Related concepts

Failover Strategy on page 922

9.2.24 Location Interconnect Failure

A failure of the interconnection between the two locations is detected by both nodes, and each node takes over the IP addresses of the partner. Signaling traffic is still routed to both nodes as before. Both nodes attempting to take over each other’s function has to be avoided, so one of the nodes will be shut down.

IMPORTANT:

After Shutdown of one of the nodes, the WAN continues to send signaling traffic to the now deactivated node, which cannot be sent to the partner node because the layer-2 bridge is down. Manual intervention is needed to reroute the traffic to location 2.

Functional Sequence

To avoid both nodes attempting to set up and clear calls to the same SIP phone simultaneously, both nodes send an SNMP power-down command to the remote access card of the partner node. This is controlled by different timers, so one node powers down its partner before the partner can send its own power-down command.

Related concepts

Failover Strategy on page 922

9.2.25 Catastrophic Site Outage

If a catastrophic site outage occurs, failover actions vary depending on the type of geographic node separation.

Functional Sequence

- Same subnet: When nodes are in the same subnet, node 2 loses communication with node 1 and takes over the IP addresses of node 1 after consulting the survival authority. The catastrophic failure of node 1’s site is detected by the WAN, and the traffic for node 1 is rerouted to the partner site.

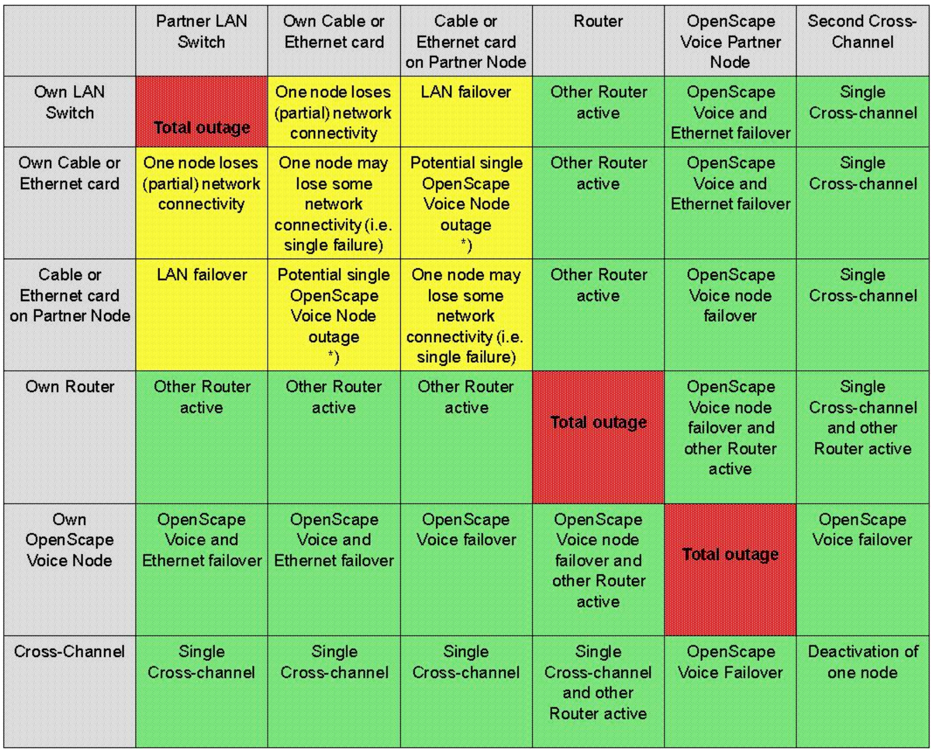
- Different subnets: When nodes are in different subnets or when complete node separation is present, node 2 loses communication with node 1 and activates the backup IP addresses of node 1 on node 2 after consulting the survival authority. The catastrophic failure of node 1’s site is detected by all endpoints, and using DNS SRV, the endpoints reroute the traffic for node 1 to the partner site.

Related concepts

Failover Strategy on page 922

9.2.26 Double Failures with Collocated Nodes

The cluster is also guarded against some double failures of the same kind without loss of service. Depending on which combination of failure occurs there is no outage, some service reduction, or in a few symmetrical double failures a total outage.



	Partner LAN Switch	Own Cable or Ethernet card	Cable or Ethernet card on Partner Node	Router	OpenScape Voice Partner Node	Second Cross-Channel
Own LAN Switch	**Total outage**	One node loses (partial) network connectivity	LAN failover	Other Router active	OpenScape Voice and Ethernet failover	Single Cross-channel
Own Cable or Ethernet card	One node loses (partial) network connectivity	One node may lose some network connectivity (i.e. single failure)	Potential single OpenScape Voice Node outage *)	Other Router active	OpenScape Voice and Ethernet failover	Single Cross-channel
Cable or Ethernet card on Partner Node	LAN failover	Potential single OpenScape Voice Node outage *)	One node may lose some network connectivity (i.e. single failure)	Other Router active	OpenScape Voice node failover	Single Cross-channel
Own Router	Other Router active	Other Router active	Other Router active	**Total outage**	OpenScape Voice node failover and other Router active	Single Cross-channel and other Router active
Own OpenScape Voice Node	OpenScape Voice and Ethernet failover	OpenScape Voice and Ethernet failover	OpenScape Voice failover	OpenScape Voice node failover and other Router active	**Total outage**	OpenScape Voice failover
Cross-Channel	Single Cross-channel	Single Cross-channel	Single Cross-channel	Single Cross-channel and other Router active	OpenScape Voice Failover	Deactivation of one node

*) in these failure cases, one OpenScape Voice may lose one to three of its network connections with potential service impacts, discussed in the related Topics.

Related concepts

Failover Strategy on page 922
OpenScape Voice Admin Network Failures on page 930
OpenScape Voice Signaling Network Failures on page 931
OpenScape Voice Billing Network Failures on page 931

9.2.27 Double Failures with Geographical Node Separation

Geographically separated nodes in the same subnet are protected against the same double failures as collocated ones, but additionally is also guarded against some more double failures of the same kind at one data center without loss of service.

System Specific Information

- Double router failure at one data center: The node loses connection, but is still connected to the partner node. The impact depends on whether the connection to the Admin network or the Signaling network or Billing network is restricted and result in the same as the respective single failure.
- 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: 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.

Related concepts

Failover Strategy on page 922

9.2.28 OpenScape Voice Admin Network Failures

If one node cannot be reached for administration and maintenance—that is, if both admin Ethernet ports of the Linux bonding driver are unavailable—OpenScape Voice provisioning and maintenance is still possible via the partner node. Only direct hardware maintenance is not possible.

NOTICE:

The remote admin interface (provided by the maintenance controller) is non-redundant. For that reason, a failure of the maintenance controller card or the Ethernet cable that connects it with the LAN switch will cause an outage of the remote admin capabilities of that OpenScape Voice node.

Functional Sequence

The administration server will signal that it lost communication with the OpenScape Voice node. It may still receive alarms from the other node if the active alarming process happens to run on the other node. The administration server will not be able to provision OpenScape Voice data if the virtual IP address happens to be on the node with the unavailable admin network.

Related concepts

Failover Strategy on page 922

Double Failures with Collocated Nodes on page 929

9.2.29 OpenScape Voice Signaling Network Failures

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.

NOTICE:

In case of signalling network failure, there will be a call processing outage for the affected node.

Other Characteristics

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.

Related concepts

Failover Strategy on page 922

Double Failures with Collocated Nodes on page 929

9.2.30 OpenScape Voice Billing Network Failures

If the communication of an OpenScape Voice cluster node and its billing network fails - that is, if both billing Ethernet ports of the Linux bonding driver are unavailable - the consequences depend on the file reporting mode.

The consequences of losing the billing network interface on an OpenScape Voice node depend on whether billing files are reported via push or poll mode:

- Push: If the OpenScape Voice pushes the billing file and does not get a response, the CDR Handler node tries another billing server IP address and, if unsuccessful, switches over to the other node.
- Poll: If the active CDR handler runs on the node with the lost communication, the external billing server cannot read the CDR files. The OpenScape Voice is dimensioned to store billing files for 5 days. If communication cannot be re-established within this time, the craftperson should manually switchover the CDR-handler process.

Related concepts

Failover Strategy on page 922

Double Failures with Collocated Nodes on page 929

10 Call Detail Record (CDR)

A Call Detail Record (CDR) is a collection of information for each call that is processed by OpenScape Voice. More complex call scenarios such as transfer, conference, networking, and other OpenScape Voice features may produce multiple CDRs.

OpenScape Voice generates and maintains CDRs for usage collection and billing purposes. The UCE maintains CDR information in the active call context, which can follow the call from process to process and, in a redundant system, from node to node.

Information is collected in order to:

- Track bill-back accounting (for extension, department, division, or company).
- Track and identify special common carrier services (track telephone numbers and call duration to specific locations).
- Track client or user identification (track account numbers, or personal identification numbers (PINs)).
- Track system traffic for analysis (call patterns, trunk usage, and other routing information).
- Track and identify call abuse (Track and identify call abuse (track 900 numbers, unauthorized long distance calls, and personal calls).
- Track calls for different states (e.g., answered, unanswered, rejected) and call scenarios (e.g., Transfer, Call Forward, Callback, etc.

Related concepts

Please select the appropriate help topic on page 656

10.1 Secure Storage of CDR (Call Detail Record) Password

Passwords for the OpenScape Voice CLI (Command Line Interface) login are stored encrypted within the Linux OS. Application-level passwords for transferring CDRs (Call Detail Records) from the OpenScape Voice server to the billing mediation server are stored via two-way encryption within the OpenScape Voice database.

10.2 Create a CDR (Call Detail Record)

At the end of every call, a CDR (Call Detail Record) is generated. However, intermediate CDRs are also generated once every 30 minutes; CDRs also are generated intermittently for long-duration calls, such as those that pass over midnight more than once. The RTP (Real-time Transport Protocol) ticket manager handles the individual CDRs.

10.3 CDR (Call Detail Record) Generation

The CDR (Call Detail Record) generation feature provides comprehensive call accounting data.

CDR generation is a combined effort of Call Control and internal Usage Collection functionality. Internally, CDRs are represented in binary format in Call

Control's context. Usage Collection software converts these records to ASCII CDRs and output them in formatted BFs (Billing Files).

OpenScape Voice generates CDRs that include information such as the following:

- Date and time
- Originating account number
- Destination telephone number
- Carrier identifiers
- Global call identifier, which correlates and combines information from multiple CDRs that pertain to the same call - for example, when a call spans more than one node
- Thread identifier, which correlates separate calls that are part of a complex call scenario - for example, when a call is transferred
- IP address or FQDN (Fully-Qualified Domain Name) / location domain name
- Other related information.

10.4 Store CDR (Call Detail Record)

The CDRs (Call Detail Records) are first stored on the local hard drive and are then pushed to or pulled from a billing server (for example, OpenScape Voice Accounting Management or third party billing application) which post-processes the CDRs.

All CDRs are stored in flat files. You can configure both a primary and secondary node for CDR storage and you can explicitly select one of the CDR delivery methods (Push or Pull).

After they are pushed to the billing server, the files can be:

- Deleted immediately
- Saved, then automatically deleted after a specified retention period
- Saved until the administrator manually deletes them.

NOTICE:

If both. primary and secondary node, fail or in case of an ftp failure, the ticket files will remain in the ticket pool. Ticket pool means the /tpa/CDR loation where the tickets will remain until the link to the primary or the backup billing servers is restored.

If the CDRs are transferred to the backup billing server, they will keep be transferred. Only another ftp failure will cause the OpenScape Voice to try the primary server again.

10.5 Billing Interface

OpenScape Voice uses a FTP interface to the billing system.

OpenScape Voice supports the following modes on the FTP interface to the billing system:

- Pull mode: CDRs (Call Detail Records) are retrieved from the OpenScape Voice by the billing system.

- Push mode: CDRs are delivered to the billing system by the OpenScape Voice.

Functional Operation

CDRs are buffered in the duplicated main memory of OpenScape Voice, and their content transferred to a CDR file on the duplicated persistent storage. Therefore, the maximum amount of data that could be lost in the event of a total system outage is limited to the content of the CDR buffer of the main memory. The CDR data output to a disk file ensures that the probability of CDR data loss is minimized.

The type of file transfer protocol depends on the entity that initiates the CDR transfer:

- If OpenScape Voice initiates CDR transfer (also known as file transfer by push), FTP is used.
- If the billing server initiates the transfer (also known as file transfer by pull), either FTP or, if the billing server supports it, SFTP (Secure FTP) can be used.

FTP connections can be protected with IPsec as long as the billing server supports it.

System Specific Information

The first layer of security for this interface is provided by the network design that separates this traffic from other traffic on the network.

The second layer of protection is provided by the OpenScape Voice itself. The integrated packet filter can be provisioned to limit the IP addresses that can access the OpenScape Voice billing interface.

As a third layer of defense, the OpenScape Voice provides the following additional options for protection:

- SFTP protection of CDR delivery to the billing server by a pull from the billing server
- IPsec protection for FTP pull- or push-mode interface between the OpenScape Voice and the billing server

The ability to provide integrated end-to-end protection of the billing stream via encryption depends on the capabilities of the billing system. The enterprise can also use network-based secure VPNs as an alternative, depending on the enterprise’s security policy.

CDR passwords entered by the customer are stored in encrypted form. These are the passwords used for the FTP or SFTP interface to the billing system and are stored internally to the system.

The system default primary and secondary passwords for initial installations are not encrypted. The encryption takes place when the customer replaces the default passwords with customer-created passwords.

10.6 Billing Server Interface

The interface between the OpenScape Voice and the billing server uses FTP to transfer CDR (Call Detail Record) information. The OpenScape Voice supports SFTP protection for CDR delivery using a pull from the billing server.

IPsec with IKE (Internet Key Exchange) and pre-shared keys is used to secure FTP interfaces between servers.

10.7 CDR (Call Detail Record) Processing

Each CDR (Call Detail Record) is an RTP (Real-time Transport Protocol) ticket. The CDR client uses the RTP ticket writer to write the ticket (CDR) in a ticket file on local disk (/software/twlocal) in binary format. Ticket files are node-specific; their file name includes the node ID, which means they are unique cluster-wide.

Functional Sequence

When certain conditions are met (for example, every 5 minutes, or every 5000 records, or every 5600256 bytes), the ticket manager closes the ticket file and all subsequent ticket data is written to a new ticket file. The ticket manager then copies the ticket file to a ticket pool located on a local node-specific directory (/tpa/CDR). Using the 'remote copy' function of the operating system, an additional copy will be created in the other cluster node ticket pool directory (backup). This procedure guarantees that all ticket data is stored on both cluster nodes at any time. The ticket pools provide storage of “primary” billing data, that is, data not yet sent to an external billing collection system.

The ticket manager then notifies the active CDR handler that a ticket file is available for processing in the ticket pool. The CDR handler also periodically audits the DB to see if any ticket files exist in the ticket pool that it was not notified of for whatever reason.

The CDR handler then converts the binary ticket file to an ASCII CDR BF (Billing File), assigns to it a cluster-wide file sequence number. The BF is now ready to be transferred to/from the billing collection system.

10.8 Monitoring CDR (Call Detail Record) Faults

The CDR (Call Detail Record) Fault Management commands enable the user to obtain lists of events related to CDR faults, based upon differing start times, which are consistent with RTP (Real-time Transport Protocol) “register for events then list callbacks”, but which allow for event filtering within the menu selection itself.

By entering a selection from the CDR Fault Management menu, CDR Fault Management performs an implicit registration for CDR events, and then executes the requisite action selected.

10.9 Monitoring CDR (Call Detail Record) Performance

The OpenScape Voice system displays CDR (Call Detail Record) counters to monitor the performance of the CDR generation and collection engine.

Performance management functions enable the service providers to monitor the network, provide service assurance, and generate reports based on network performance. All call control and signaling components within the OpenScape Voice system contribute to the generation of the performance data in the form of statistics and measurements. One of the devices used to configure, display, and manage these reports is the CLI (Command Line Interface).

10.10 Standard CDR (Call Detail Record)

The standard CDR (Call Detail Record) is produced at the end of each call.

One standard CDR for the call leg that takes place between the original calling party and the final forwarded-to (connected) party. This CDR type is generated for all calls.

Related concepts

Intermediate Long Duration Records on page 939
Queue Record on page 940
Call Forwarding CDR (Call Detail Record) on page 937
Long Call Duration Record on page 938
Change of Software Audit Record on page 941
Feature Activation / Deactivation Record on page 940

10.11 Call Forwarding CDR (Call Detail Record)

When calls are forwarded, either via telephone-based or OpenScape Voice-based forwarding, multiple CDRs (Call Detail Records; standard CDRs and call forwarding CDRs) are generated.

Functional Sequence

For a call that involves Call Forwarding, Call Forwarding CDRs are generated in addition to the Standard CDR; one Call Forwarding CDR is generated for each Call Forwarding leg, up to a maximum of 5.

The Standard CDR field `Additional CDR` is formatted with a value of ‘8’ indicating that the call involved Call Forwarding.

The standard CDR and the associated Call Forwarding CDRs can be correlated together by means of the 32 character numerical sequence part of the `Record ID` and the `Switch ID` fields which always have the same values across these CDRs. An RTP (Real-time Transport Protocol) configuration parameter is available that (if set) causes Call Forwarding CDRs to be generated with Intermediate CDRs, in addition to being generated with Standard CDRs. The default value of this parameter `(Srx/Main/SendCFCDRWithICDR`) is “`RtpFalse`” (not set) and can be configured from the CLI (Command Line Interface) menu by selecting **1 (Configuration Management)**, **2 (Configuration Parameters)**, **3 (modifyParameter)**.

NOTICE:

All BG (Business Group) data apply to the base forwarded from party.

Other Characteristics

If a standard CDR is not generated due to some type of failure an intermediate CDR is generated. Intermediate CDRs provide backup information to allow partial charging for long duration calls (calls lasting longer than 30 minutes). As soon as a standard CDR is available for a call, any intermediate CDRs no longer are needed, so they are automatically discarded.

Assume that party A calls party B. Party B forwards to party C; party C then forwards to party D. In this scenario:

- A standard CDR is generated for the A-to-D call.
- Individual call forwarding CDRs are generated for the B-to-C and C-to-D call legs.

Related concepts

Standard CDR (Call Detail Record) on page 937
Intermediate Long Duration Records on page 939
Queue Record on page 940
Long Call Duration Record on page 938
Change of Software Audit Record on page 941
Feature Activation / Deactivation Record on page 940

10.12 Long Call Duration Record

A Long Call Audit CDR (Call Detail Record) is generated for a call whose duration is longer than two consecutive midnights. The record itself is generated at the 2nd midnight and each midnight thereafter. A Standard CDR is generated when the call is released, with field no. 4 containing the total overall call duration.

The Long Call Audit Records contain essentially the same information as Standard CDR Records, the following fields, including comma delimiters, are not part of the Long Duration Audit Record:

- Attempt Indicator (field #18 in Standard CDR)
- Release Cause / Completion Indicator (field #19 in Standard CDR)
- Call Release Time (field #49 in Standard CDR)
- Incoming Carrier Release Time (field #51 in Standard CDR)
- Outgoing Carrier Release Time (field #53 in Standard CDR)
- IC / INC Call Event Status (field #61 in Standard CDR)

Therefore, the field numbers in the Long Call Audit Record do not match the field numbers in the Standard Call Record (for example, ‘Additional CDRs’ is field no. 94 in the Long Call Audit Record, while it is field no. 100 in the Standard CDR).

NOTICE:

If you have not received statistics for a particular field, or if a field does not apply to your application, it displays a default of either zero (0) or NULL (, ,).

Configuration of RTP parameter Srx/Main/LongCallTimer

The maximum length of a long duration call can be specified via the RTP parameter `Srx/Main/LongCallTimer`.

Valid values ranges from 4 to 240 hours. Default value is 12 hours.

After the expiration of this UCE timer the call will be torn down and a release will besent to both sides of the call to return them to the idle condition.

NOTICE:

A long call timer value of zero (0) will disable this feature and leave a call up indefinitely.

Related concepts

Standard CDR (Call Detail Record) on page 937
Intermediate Long Duration Records on page 939
Queue Record on page 940
Call Forwarding CDR (Call Detail Record) on page 937
Change of Software Audit Record on page 941
Feature Activation / Deactivation Record on page 940

10.13 Intermediate Long Duration Records

The intermediate long duration CDR (Call Detail Record) feature provides the capability to generate intermediate CDRs containing full call information after an administrable time period elapses.

Intermediate CDRs are by default generated every 30 minutes of active and established call time. The Intermediate CDRs is configurable. The intermediate CDRs are additional to the standard CDR.

A record type of Intermediate Call Record indicates intermediate CDR. This information is stored as separate files for backup purposes.

Other Characteristics

The layout is the same as the Standard CDR, with the exception that field no. 2 has a different record type value and field no. 66 has value = 1. For the layout and definitions of all remaining fields, refer to "Standard CDR”.

The standard CDR and any associated intermediate CDRs can be correlated together by means of the 32 character numerical sequence part of the "Record ID" and the "Switch ID" fields which always have the same values across these CDRs.

Related concepts

Standard CDR (Call Detail Record) on page 937
Queue Record on page 940

Call Forwarding CDR (Call Detail Record) on page 937
Long Call Duration Record on page 938
Change of Software Audit Record on page 941
Feature Activation / Deactivation Record on page 940

10.14 Queue Record

When a call is queued, e.g. in hunt group scenarios, a Queue CDR (Call Detail Record) is generated in addition to the Standard CDR, which contains info about the time and duration of queuing.

The Standard CDR field ‘Additional CDRs’ (field no. 100) shows the value ‘2’ indicating that the call involved queuing.

The Standard CDR and the Queue CDRs are correlated to the same call setup by having the fields ‘Switch ID’ and ‘Record ID’ (the 32-character numerical sequence part) with the same field value across these CDRs.

Related concepts

Standard CDR (Call Detail Record) on page 937
Intermediate Long Duration Records on page 939
Call Forwarding CDR (Call Detail Record) on page 937
Long Call Duration Record on page 938
Change of Software Audit Record on page 941
Feature Activation / Deactivation Record on page 940

10.15 Feature Activation / Deactivation Record

Feature Activation / Deactivation Records are produced when a user activates or deactivates certain call features.

Feature Activation / Deactivation Record indicates that a user has activated or deactivated a call feature using access code. Features that generate the feature act/deact records are:

- Anonymous call rejection
- Call completion on No Reply
- Call completion on busy subscriber
- Call forwarding-variable
- Call forwarding-busy line
- Call forwarding-do not answer
- Call forwarding-selective
- Do not disturbed
- Hot line
- Last incoming number redial
- Last outgoing number redial
- Selective call acceptance
- Selective call rejection
- Warm line

NOTICE:

If you have not received statistics for a particular field, or if a field does not apply to your application, it displays a default of either zero (0) or NULL (, ,).

Related concepts

Standard CDR (Call Detail Record) on page 937
Intermediate Long Duration Records on page 939
Queue Record on page 940
Call Forwarding CDR (Call Detail Record) on page 937
Long Call Duration Record on page 938
Change of Software Audit Record on page 941

10.16 Change of Software Audit Record

A Change of Software Audit Record is generated in situations where software modifications have been made on a particular switch (for example, rolling upgrade not new installations).

This CDR (Call Detail Record) is only generated for a rolling upgrade, not for new installations.

Related concepts

Standard CDR (Call Detail Record) on page 937
Intermediate Long Duration Records on page 939
Queue Record on page 940
Call Forwarding CDR (Call Detail Record) on page 937
Long Call Duration Record on page 938
Feature Activation / Deactivation Record on page 940

10.17 Usage Reporting

The usage reporting feature provides for the generation of CDRs (Call Details Records) for all calls, distinguishing between completed and non-completed calls (ring no answer, busy status).

The CDRs include, for example:

- Date and time
- Carrier ID code
- Originating account number
- Destination telephone number
- Duration of call in tenths of seconds
- Calling party number (if available)
- Call status

For the United States, the reference time clock is the United States Department of Commerce's atomic clock timeserver in Boulder, Colorado. Other local, national or international time servers may be used for international markets.

10.18 CDR (Call Detail Record) Handler

The CDR (Call Detail Record) handler manages the internal binary billing files through the RTP (Real-time Transport Protocol) API, then makes them available to a billing server. The CDR handler also converts and formats these internal binary billing files. The completed and formatted billing files can be transferred from the OpenScape Voice server through FTP or SFTP, depending on the file transfer method and the capabilities of the billing server.

10.19 Determining the Call Direction

The call direction (incoming/outgoing/internal) allows a billing application to determine which calls should be charged, for example, outgoing calls to the PSTN (Public Switched Telephone Network). There is no specific field in the CDR (Call Detail Record) for the call direction as this can be determined by the billing application based on other information provided in the CDRs.

The call direction depends on whether the calling and called parties are internal or external.

- If the calling party is external and the called party is internal then the call direction is **incoming**.
- If the calling party is internal and the called party is external then the call direction is **outgoing**.
- If both the calling and the called parties are internal then the call direction is **internal**.
- If both the calling and the called parties are external then the call direction is **transit**.

To determine whether the calling and called parties are internal or external, the billing application, after filtering CDRs with the same GID (Global Call ID), can apply the following basic rules:

1) If the calling party identifier (field 40) is Originating in any of the CDRs then the calling party is internal.
2) If the called party identifier (field 41) is Terminating in any of the CDRs then the called party is internal.
3) If the Ingress SIP EP (Endpoint) address (field 126) belongs to a gateway in any of the CDRs then the calling party is external.
4) If the Egress SIP EP address (field 127) belongs to a gateway in any of the CDRs then the called party is external.

Special Scenario:

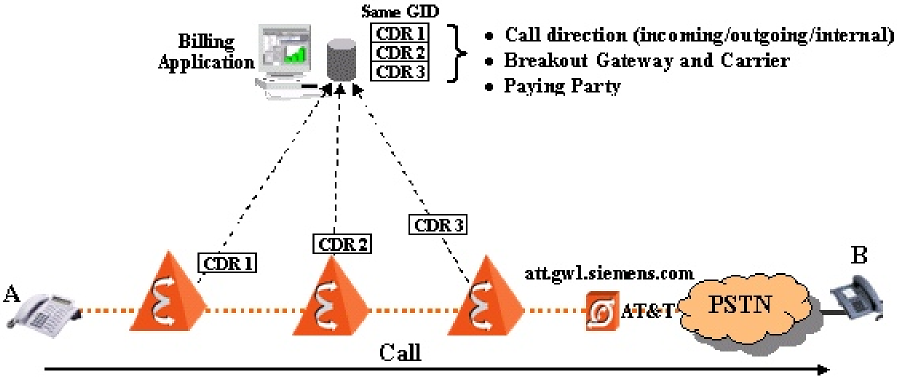
When a call is rerouted through PSTN gateway due to CAC (Call Admission Control) due to bandwidth limits, the resulting connection is seen by the OpenScape Voice as two independent calls with no correlation between them. Call #1 is from the originating SIP phone to the outgoing PSTN gateway

(OpenScape Voice handles the SIP signaling for establishing this connection) and Call #2 is from the incoming PSTN gateway to the terminating SIP phone (OpenScape Voice handles the SIP signaling for this connection, but it is totally independent and without any correlation to Call #1). The only “end-to-end” signaling between the originating SIP phone and the terminating SIP phone is that which is provided by the PSTN connection (that is, the SS7 ISUP (ISDN User Part) connection), which is the reason there may be a reduction of feature transparency.

10.20 Filtering the CDR (Call Detail Records) with the GID (Global Call ID)

OpenScape Voice provides the GID (Global Call ID) in the CDR (Call Detail Record), which the billing application can use to filter CDRs that belong to the same call.

The billing application can then combine and correlate the information contained in the CDRs using straightforward rules to determine which calls to charge, what to charge, and who to charge. This approach is shown in the figure below.



10.21 CDR (Call Detail Record) for BG (Business Group) Features

CDR (Call Detail Record) handling for BG (Business Group) features.

CDR offers special handling for the following features:

- **BG Account Codes**

  The BG Account Codes feature lets the subscriber add a number (the account code) into the CDR record for allocation of charges on billable calls (incoming or outgoing).

  OpenScape Voice includes account codes in CDR reports when configured to do so, the enterprise determines and maintains the correct lists of applicable account codes. You do not explicitly create them on OpenScape Voice.

  The system administrator specifies the number of digits of the account code. It can be from 2 to 14 digits long; its length is the same for all stations in a business group.

- **BG Billing**

  The BG Billing feature supports the MDR-RAO (Message Detail Recording - Regional Accounting Office) per GR-610 MDR (Message Detail Recording) (FSD 02-02-1110).

  This capability can be turned on or off on a per BG basis.

  When BG Billing is enabled, CDR provides the following data for calls from and to the BG as applicable:

  – Customer identification
  – Originating or terminating facility type
  – Originating or terminating facility identification
  – Call completion code
  – Business feature code
  – AAR (Automatic Alternate Routing) pattern group
  – Queue elapsed time
  – Access code
  – Authorization code
  – Account code
  – Dialed digits

- **BG Department Names)**

  The CDR record provides the department name.

- **MDR (Message Detail Recording)**

  The MDR feature provides the capability to include BG Billing information in an OpenScape Voice CDR for a BG call.

  MDR information is provisioned on the BG to provide enough information in the Call Context CDR to support the generation of BAF (Billing AMA Format, AMA = Automatic Message Accounting) MDR modules that are appended to the BAF AMA base structure records, upon mediation of these CDRs for calls originating/terminating from/to BG facilities.

  The **MDR Customer Identification** must be unique for each BG. The MDR information is applicable to the BG only and cannot be provisioned at the BGL (Business Group Line) level.

  When the BG or system administrator enables MDR for a BG, OpenScape Voice populates additional fields, which are specific to the BG, in a standard CDR for any call involving a member of that group.

Related concepts

CDR (Call Detail Record) for Group Features on page 945
CDR (Call Detail Record) for Keyset Telephone User Features on page 946
CDR (Call Detail Record) for QSIG (Q-Signaling) Tunneling Features on page 946
CDR (Call Detail Record) for Routing and Translation Features on page 947
CDR (Call Detail Record) for User Features on page 948

10.22 CDR (Call Detail Record) for Group Features

CDR (Call Detail Record) handling for Group features.

MLHG (Multiline Hunt Group)

- Basic MLHG call

  The member that answers an MLGH call is recorded in the CDR (field "Destination Party"). Therefore statistics per member e.g. number of answered calls, average service time etc. is possible.
- MLHG advance no answer

  A member misses a call and the call advances to the next available member. For this scenario an additional CDR is generated before the call advances to the next available member. The additional CDR is marked with the flag "MLHG advance no answer" in the field 107 " Call Event Indicator". Furthermore the field "Destination Party" contains the current alerting member, i.e. the member who missed the call.
- MLHG CFB (Call Forwarding Busy)

  All members are busy and the queue is full so the call overflows to the overflow DN (Destination Number). For this scenario an additional CDR is generated each time the call overflows to the overflow DN. The additional CDR is marked with the flag "MLHG overflow" in the field 107 " Call Event Indicator". Furthermore the field "Destination Party" contains the overflow DN and the field "Called Party" the flag "MLHG pilot DN".

  Each time a call overflows an additional CDR is generated. Hence all information about all overflows in a multiple overflow scenario are recorded.
- MLHG Night Service

  If the MLHG Night Service feature is activated and the DN is not a Hunt Group member, the information is recorded in the CDR. Therefore in the CDR it is indicated that the call as originally an MLHG call by marking with the flag "MLHG Night Service" in the field 107 " Call Event Indicator".
- MLHG and pickup

  An MLHG call is answered by a member using call pickup. There are two CDRs generated which be linked via CDR field 107 "Call Event Indicator" from the first generated CDR. These two CDRs contains information who answered this call via pickup and who answered it.

Call Pickup

The subscriber's number that picks up the call is recorded in the CDR. Therefore it is possible to link the CDR of activating call pickup and the CDR of the MLHG call being picked up as one call.

Therefore the field "Destination Party" contains information about the party that picked up the call in the original CDR and the CDR of other party of the call pickup activation do has the same information.

Related concepts

CDR (Call Detail Record) for BG (Business Group) Features on page 943
CDR (Call Detail Record) for Keyset Telephone User Features on page 946
CDR (Call Detail Record) for QSIG (Q-Signaling) Tunneling Features on page 946
CDR (Call Detail Record) for Routing and Translation Features on page 947
CDR (Call Detail Record) for User Features on page 948

10.23 CDR (Call Detail Record) for Keyset Telephone User Features

CDR (Call Detail Record) handling for Keyset Telephone User features.

CDR offers special handling for the following features:

- Keyset Operation Modes

  When a keyset user initiates a call from a line configured for line-based operation, OpenScape Voice records the line used and the device from where the call was initiated.
- Line Key Operation

  Based on system configuration upon retrieval of a call, the billing for the remainder of the call is assigned to the primary line of the station answering the recall.
- MLA (Multiline Appearance)

  OpenScape Voice records the line used.
- Phantom Lines

  OpenScape Voice records the line used.

Related concepts

CDR (Call Detail Record) for BG (Business Group) Features on page 943
CDR (Call Detail Record) for Group Features on page 945
CDR (Call Detail Record) for QSIG (Q-Signaling) Tunneling Features on page 946
CDR (Call Detail Record) for Routing and Translation Features on page 947
CDR (Call Detail Record) for User Features on page 948

10.24 CDR (Call Detail Record) for QSIG (Q-Signaling) Tunneling Features

CDR (Call Detail Record) for QSIG tunneling features applies only between OpenScape Voice and the OpenScape 4000. It does not function between

OpenScape Voice and the HiPath 3000, or between OpenScape Voice and and other vendors' QSIG PBX.

Functional Operation

When a call spans more than one node, a global call identifier correlates and combines information from multiple CDRs that pertain to the same call. In addition, a thread identifier (for call segments) is generated/transmitted by OpenScape Voice.

CDR offers special handling for the following features:

- Call Hold

  A party is put on hold and hangs up. Information about this event and how long the party was on hold is recorded.

  The information is available for:

  - Basic Call Hold
  - Multiple Call Hold
  - Held Party Hangs up
  - Consultation Hold-Transfer.

Related concepts

CDR (Call Detail Record) for BG (Business Group) Features on page 943
CDR (Call Detail Record) for Group Features on page 945
CDR (Call Detail Record) for Keyset Telephone User Features on page 946
CDR (Call Detail Record) for Routing and Translation Features on page 947
CDR (Call Detail Record) for User Features on page 948

10.25 CDR (Call Detail Record) for Routing and Translation Features

CDR (Call Detail Record) handling for Routing and Translation features.

CDR offers special handling for the following features:

- ENUM (Electronic Number Mapping)

  Each CDR indicates whether an ENUM query occurred on the call.

- Rerouting Based on SIP Response Codes and WAN Outages

  Separate CDRs are generated for the originating and terminating legs of the rerouted call.

Related concepts

CDR (Call Detail Record) for BG (Business Group) Features on page 943
CDR (Call Detail Record) for Group Features on page 945
CDR (Call Detail Record) for Keyset Telephone User Features on page 946
CDR (Call Detail Record) for QSIG (Q-Signaling) Tunneling Features on page 946
CDR (Call Detail Record) for User Features on page 948

10.26 CDR (Call Detail Record) for User Features

CDR (Call Detail Record) recording offer special handling for user features that reside in OpenScape Voice. Examples of such features are calling identity delivery and suppression features, abbreviated dialing features, redial and call return features, and display features.

CDR offers special handling for the following features:

- Anonymous Call Rejection

  CDR is provided on a usage-sensitive basis.

  CDRs are generated once daily, at the client-scheduled record generation time, for each line with anonymous call rejection. This includes the count of calls and denial treatment since the last record generation.
- Music On Hold — OpenScape Voice-based

  CDR records billing for ONS (One Number Service) inbound/outbound calls, including charges subscribers incur for external associated device usage.
- SCA (Selective Call Acceptance)

  CDRs are provided on a usage-sensitive basis.

  CDRs are generated once daily, at the client-scheduled record generation time, for each line with selective call acceptance. This includes the count of calls and denial treatment since the last record generation. The following are the CDRs associated with this feature:

  – SCA activation
  – SCA deactivation
  – SCA screening list created
  – SCA screening list edited
  – SCA screening list deleted.
- SCR (Selective Call Rejection)

  CDRs are provided on a usage-sensitive basis.

  CDRs are generated once daily, at the client-scheduled record generation time, for each line with ACR. This includes the count of calls and denial treatment since the last record generation. The following are the CDRs maintained for this feature:

  – SCR activation
  – SCR deactivation
  – SCR screening list editing
  – SCR screening list created
  – SCR screening list deleted.
- Serial Ringing

  – A record is created for the original call to the main number. In this CDR, the caller’s number is the “A” number and the main DN (Directory Number) is the “B” number.
  – Up to six CDRs are created, one for each of the other calls that are set up. In these CDRs, the caller’s DN is the calling party number, the DN

being called is the “B” DN, and the main DN is the “charge-to” DN. This is done to assure that the feature owner is made responsible for any charges associated with these six calls.

- Simultaneous Ringing

  – A record is created for the original call to the main number. In this CDR, the caller’s number is the “A” number and the main DN is the “B” number.

  – Up to six CDRs are created, one for each of the other calls that are set up. In these CDRs, the caller’s DN is the calling party number, the DN being called is the “B” DN, and the main DN is the “charge-to” DN. This is done to assure that the feature owner is made responsible for any charges associated with these six calls.

- Transfer Security

  For complex call scenarios — for example, when a call is transfered with consultation — a thread identifier correlates the CDRs associated with each leg of the call.

Related concepts

CDR (Call Detail Record) for BG (Business Group) Features on page 943
CDR (Call Detail Record) for Group Features on page 945
CDR (Call Detail Record) for Keyset Telephone User Features on page 946
CDR (Call Detail Record) for QSIG (Q-Signaling) Tunneling Features on page 946
CDR (Call Detail Record) for Routing and Translation Features on page 947

10.27 BF (Billing Files)

OpenScape Voice outputs ASCII CDRs (Call Data Records) to BFs (Billing Files) that use the formatting and file naming conventions described in the following sections.

BFs are output from the OpenScape Voice in an ASCII comma delimited format. The Record Type (field no. 2) defines the basic structure for CDRs. The layout for each type is presented in this section.

By default, a BF is closed and made available for delivery to an external billing server when one of the following occurs:

- The number of individual CDRs reaches 2,500 or,
- The BF has been open for 5 minutes.

NOTICE:

If you require modification to these defaults, please contact the authorized BLS (Back Level Support) for assistance in changing the RTP (Real-time Transport Protocol) parameter controlling this function.

Filename Format

OpenScape Voice CDRs/BFs use the following filename format:

```
<System Hostname>-<YYYYMMDDTHHMMSS-/+HHMM><File Sequence
Number>.BF
```

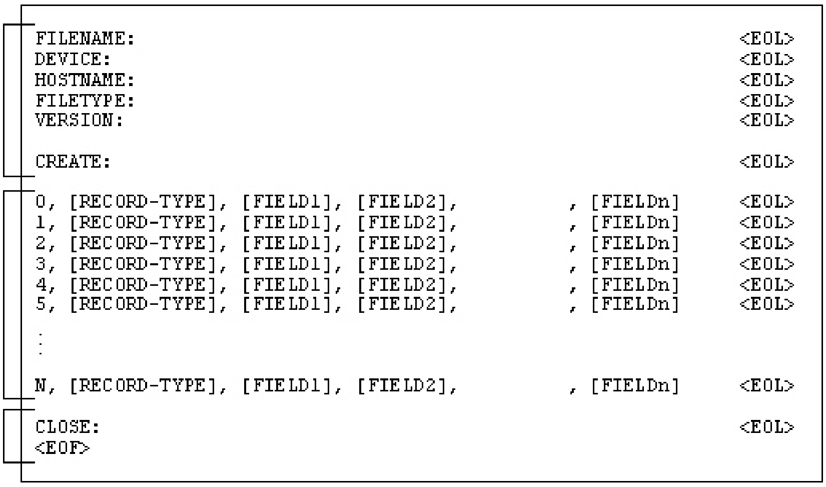
where

- `<System Hostname>` the name configured in the `node.cfg` file. This consists of a customer-assigned hostname of up to 14 characters. This supports the use of Telcordia-assigned CLLI (Common Language Location Identifier) codes as switch hostnames for identifying each OpenScape Voice.
- `<YYYYMMDDTHHMMSS-/+HHMM>` consists of a 20-character date/time stamp, indicating the date and time at which the OpenScape Voice created the billing file. This time format conforms to the UTC (Universal Time Coordinated) standard.
- `<File Sequence Number>` consists of a six-digit integer that increments with each new file the OpenScape Voice generates.

File Format

OpenScape Voice CDRs/BFs are formatted with header and trailer information and can contain Call, Audit, and Feature Activation / Deactivation Records.

Table 1 defines the elements that comprise the header and trailer used in OpenScape Voice BFs. These fields and format must exist inside the ASCII files. All fields must be followed by the “<NL>” character.



```
FILENAME:                                                   <EOL>
DEVICE:                                                     <EOL>
HOSTNAME:                                                   <EOL>
FILETYPE:                                                   <EOL>
VERSION:                                                    <EOL>

CREATE:                                                     <EOL>
0, [RECORD-TYPE], [FIELD1], [FIELD2],         , [FIELDn]    <EOL>
1, [RECORD-TYPE], [FIELD1], [FIELD2],         , [FIELDn]    <EOL>
2, [RECORD-TYPE], [FIELD1], [FIELD2],         , [FIELDn]    <EOL>
3, [RECORD-TYPE], [FIELD1], [FIELD2],         , [FIELDn]    <EOL>
4, [RECORD-TYPE], [FIELD1], [FIELD2],         , [FIELDn]    <EOL>
5, [RECORD-TYPE], [FIELD1], [FIELD2],         , [FIELDn]    <EOL>
:
:
N, [RECORD-TYPE], [FIELD1], [FIELD2],         , [FIELDn]    <EOL>
CLOSE:                                                      <EOL>
<EOF>
```

Figure 97: Billing File Format

The example below shows a billing file (*.BF) consisting of two records (record 0 and record 1).

```
FILENAME: node1vml76-20080201T134705-0500000728.BF

DEVICE: OpenScape Voice

HOSTNAME: node1vml76
```

```
FILETYPE: BILLING

VERSION: 12.00.01


CREATE: 2008-01-02T13:47:05.7-0500


0,00000000,2008-01-02T13:44:11.9-0500,73,node1vml76,2008-01-02T13

0500:FF000100000000002B22A347C0000000,,,73,,15615762009,15615762

010,,,,0,64000,0,16,0,,,0,,,0,,,0,17,17,,,,,,,5,5,900,902,5,5,,,

9,9,2008-01-02T13:44:16.0-0500,2008-01-02T13:44:23.3-0500,2008-01

0500,2008-01-02T13:44:23.5-0500,2008-01-02T13:44:12.1-0500,2008-0


1,00000000,2008-01-02T13:44:37.8-0500,247,node1vml76,2008-01-02T1

0500:FF000100000000004522A347C2000000,,,247,,15615762010,1561576

2008,,,,0,64000,0,16,0,,,0,,,0,,,0,17,17,,,,,,,5,5,900,902,5,5,,,

0500,0,2,1,1,1,1,,10,,0,2448,,,533,0,0,0,0,0,0,0,0,0,533,0,0,0,0,


CLOSE: 2008-01-02T13:47:05.7-0500
```

10.28 CDR (Call Detail Record) Decoder Tool

The CDR (Call Detail Record) decoder tool (cdrdecode) which can be run from the command line interface of OpenScape Voice, takes as input a billing file and outputs the CDRs contained in the file in a readable format, including the field names and their decoded values.

The example below shows a BF (Billing File) when passed through the CDR decoder tool.

```
FILENAME: node1vml76-20080201T134705-0500000728.BF

DEVICE: OpenScape Voice

HOSTNAME: node1vml76

FILETYPE: BILLING

VERSION: 12.00.01
```

```
CREATE: 2008-01-02T13:47:05.7-0500

FILE VERSION OK

---------------

01. Sequential Record Number:0

02. Record Type:00000000 (Standard CDR)

03. Start Time:2008-01-02 T 13:44:11.9-0500

04. Duration of Call (Tenths of seconds):73

05. Switch ID:node1vml76

06. Record ID:2008-01-02T13:44:11.9-
#0500:FF000100000000002B22A347C0000000

09. Call Segment Duration (Tenths of seconds):73

11. Term Number/Called Party:15615762009

12. Orig Number/Calling Party:15615762010

16. Call Type:0(Voice Call)

17. Information Transfer Rate:64000

18. Attempt Indicator:0(Completed)

19. Release Cause/Completion Indicator:16(normal call
 clearing)

20. Bearer Capability Request:0(Circuit mode speech)

23. Operator Indicator:0(Direct Dialed)

26. Originating Nature of Address:0(Voice Call)

29. Route Selection:0(Standard)

30. Ingress Signaling Type:17(SIP)

31. Egress Signaling Type:17(SIP)

38. Incoming Trunk Group Signaling Type:5(Not Provisioned)

39. Outgoing Trunk Group Signaling Type:5(Not Provisioned)

40. Originating Party Identifier:900(Originating Endpoint
 on the OSC Voice)

41. Terminating Party Identifier:902(Terminating Endpoint
 on the# OSC Voice)
```

```
42. JIP Source Indicator:5(Unknown)

43. LRN Source Indicator:5(Unknown)

46. Originating Party Query Status Indicator:9(No query
 done)

47. Terminating Party Query Status Indicator:9(No query
 done)

48. Call Answer Time:2008-01-02 T 13:44:16.0-0500

49. Call Release Time:2008-01-02 T 13:44:23.3-0500

50. Incoming Carrier Connect Time:2008-01-02 T
 13:44:11.9-0500

51. Incoming Carrier Release Time:2008-01-02 T
 13:44:23.5-0500

52. Outgoing Carrier Connect Time:2008-01-02 T
 13:44:12.1-0500

53. Outgoing Carrier Release Time:2008-01-02 T
 13:44:23.4-0500

54. Dialing and Presubscription Indicator:0(No IC/INC
 involved# in call)

55. Calling Party Subaddress Delivery:2(Feature used, but
 not# delivered)

56. Called Party Subaddress Delivery:1(Feature used,
 presumed# delivered)

57. Low-Layer Compatibility Information Delivery:1(Feature
 used,# presumed delivered)

58. High-Layer Compatibility Information
 Delivery:1(Feature# used, presumed delivered)

59. User-to-User Information/Fast Select:1(Feature used,#
 presumed delivered)

61. IC/INC Call Event Status:10(Call abandoned/released
 after# ANM received)

63. Service Feature Codes:0(No Services)

67. Originating Side: Codec Used:533(G.711 64k PCM a-law,
 G.711#64k PCM u-law, G.722 to 64k, G.729)

68. Originating Side: TOS Used:0

69. Originating Side: Reservation Used:0(Default)
```

```
70. Originating: Packets Sent:0

71. Originating: Octets Sent:0

72. Originating: Packets Rcvd:0

73. Originating: Octets Rcvd:0

74. Originating: Packets Lost:0

75. Originating: Inter-arrival Jitter (milliseconds):0

76. Originating: Average Transmission Delay
 (milliseconds):077. Terminating Side: Codec Used:533(G.711
 64k PCM a-law, G.711# 64k PCM u-law, G.722 to 64k, G.729)

78. Terminating Side: TOS Used:0

79. Terminating Side: Reservation Used:0(Default)

80. Terminating: Packets Sent:0

81. Terminating: Octets Sent:0

82. Terminating: Packets Rcvd:0

83. Terminating: Octets Rcvd:0

84. Terminating: Packets Lost:0

85. Terminating: Inter-arrival Jitter (milliseconds):0

86. Terminating: Average Transmission Delay
 (milliseconds):0

87. BG Orig MDR Cust ID:2

88. BG Term MDR Cust ID:2

91. BG Orig Facility Type:1(BG Co-loc Line)

92. BG Term Facility Type:1(BG Co-loc Line)

93. BG Orig Station Facility ID:5762010

94. BG Term Station Facility ID:5762009

95. BG Call Completion Code:0(Completed: no queue)

101.Original Dialed Digits:2009

104.Media Type:1(Audio)

108.Secure RTP Indicator: 1(Normal RTP)
```

```
121.GCID Node: 0-0-0

122.GCID Number: 817

124.GTID Node: 0-0-0

125.GTID Number: 819

126.Ingress SIP Endpoint Address: 10.152.7.175

127.Egress SIP Endpoint Address: 10.152.7.211


01. Sequential Record Number:1

02. Record Type:00000000 (Standard CDR)

03. Start Time:2008-01-02 T 13:44:37.8-0500

04. Duration of Call (Tenths of seconds):247

05. Switch ID:node1vml76

06. Record
 ID:2008-01-02T13:44:37.8-0500:FF00010000000000004522A347C2000000

09. Call Segment Duration (Tenths of seconds):247

11. Term Number/Called Party:15615762010

12. Orig Number/Calling Party:15615762008

16. Call Type:0(Voice Call)

17. Information Transfer Rate:64000

18. Attempt Indicator:0(Completed)

19. Release Cause/Completion Indicator:16(normal call
 clearing)

20. Bearer Capability Request:0(Circuit mode speech)

23. Operator Indicator:0(Direct Dialed)

26. Originating Nature of Address:0(Voice Call)

29. Route Selection:0(Standard)

30. Ingress Signaling Type:17(SIP)

31. Egress Signaling Type:17(SIP)

38. Incoming Trunk Group Signaling Type:5(Not Provisioned)
```

```
39. Outgoing Trunk Group Signaling Type:5(Not Provisioned)

40. Originating Party Identifier:900(Originating Endpoint
 on the OSC Voice)

41. Terminating Party Identifier:902(Terminating Endpoint
 on the#OSC Voice)

42. JIP Source Indicator:5(Unknown)

43. LRN Source Indicator:5(Unknown)

46. Originating Party Query Status Indicator:9(No query
 done)

47. Terminating Party Query Status Indicator:9(No query
 done)

48. Call Answer Time:2008-01-02 T 13:44:40.6-0500

49. Call Release Time:2008-01-02 T 13:45:05.3-0500

50. Incoming Carrier Connect Time:2008-01-02 T
 13:44:37.8-0500

51. Incoming Carrier Release Time:2008-01-02 T
 13:45:05.4-0500

52. Outgoing Carrier Connect Time:2008-01-02 T
 13:44:38.1-0500

53. Outgoing Carrier Release Time:2008-01-02 T
 13:45:05.3-0500

54. Dialing and Presubscription Indicator:0(No IC/INC
 involved in call)

55. Calling Party Subaddress Delivery:2(Feature used, but
 not delivered)

56. Called Party Subaddress Delivery:1(Feature used,
 presumed delivered)

57. Low-Layer Compatibility Information Delivery:1(Feature
 used, presumed delivered)

58. High-Layer Compatibility Information Delivery:1(Feature
 used, presumed delivered)

59. User-to-User Information/Fast Select:1(Feature used,
 presumed delivered)

61. IC/INC Call Event Status:10(Call abandoned/released
 after ANM received)
```

```
63. Service Feature Codes:0(No Services)

67. Originating Side: Codec Used:533(G.711 64k PCM a-law,
 G.71164k PCM u-law, G.722 to 64k, G.729)

68. Originating Side: TOS Used:0

69. Originating Side: Reservation Used:0(Default)

70. Originating: Packets Sent:0

71. Originating: Octets Sent:0

72. Originating: Packets Rcvd:0

73. Originating: Octets Rcvd:0

74. Originating: Packets Lost:0

75. Originating: Inter-arrival Jitter (milliseconds):0

76. Originating: Average Transmission Delay
 (milliseconds):0

77. Terminating Side: Codec Used:533(G.711 64k PCM a-law,
 G.711#64k PCM u-law, G.722 to 64k, G.729)

78. Terminating Side: TOS Used:0

79. Terminating Side: Reservation Used:0(Default)

80. Terminating: Packets Sent:0

81. Terminating: Octets Sent:0

82. Terminating: Packets Rcvd:0

83. Terminating: Octets Rcvd:0

84. Terminating: Packets Lost:0

85. Terminating: Inter-arrival Jitter (milliseconds):0

86. Terminating: Average Transmission Delay
 (milliseconds):0

87. BG Orig MDR Cust ID:2#88. BG Term MDR Cust ID:2

91. BG Orig Facility Type:1(BG Co-loc Line)

92. BG Term Facility Type:1(BG Co-loc Line)

93. BG Orig Station Facility ID:5762008

94. BG Term Station Facility ID:5762010
```

```
95. BG Call Completion Code:0(Completed: no queue)

101.Original Dialed Digits:2010

104.Media Type:1(Audio)

108.Secure RTP Indicator: 1(Normal RTP)

121.GCID Node: 0-0-0

122.GCID Number: 825

124.GTID Node: 0-0-0

125.GTID Number: 827

126.Ingress SIP Endpoint Address: 10.152.7.181

127.Egress SIP Endpoint Address: 10.152.7.175


CLOSE: 2008-01-02T13:47:05.7-0500
```

10.29 Assistant SIP Endpoints Export to OpenScape Voice Accounting Management

For OpenScape Voice AM (Accounting Management) to be able to correctly do call accounting AM needs to have knowledge of all the SIP endpoints (e.g. OpenScape Voice, gateways) that are configured in the network and how they are interconnected. With this feature OpenScape Voice Assistant generates the required information in files that OpenScape Voice AM /COL will import and automatically perform the necessary configuration.

The required information for OpenScape Voice systems is:

- name,
- software version,
- node1 IP,
- node1 name,
- node1 cdr user,
- node1 cdr pass,
- node2 IP,
- node2 name,
- node2 cdr user,
- node2 cdr pass.

Functional Sequence

OpenScape Voice Assistant writes the information for each OpenScape Voice server in a separate XML file. The XML file is generated in the CMP server under `/opt/siemens/assistant/accounting/sipendpoints/` and for simplex version under `/enterprise/assistant/accounting/sipendpoints/`. The file's name for each OpenScape Voice serve shall have the format: `OsvName_SipEndpoints_YYYYMMDDhhmmss.xml`, where OsvName is the OpenScape Voice name as configured in the OpenScape Voice `node.cfg` while YYYYMMDDhhmmss is the year, month, day, hour, minutes and seconds when the file was written.

For each OpenScape Voice subscriber and for each non-subscriber endpoint for this OpenScape Voice, the following information is required by OpenScape Voice AM in order to configure its SIP endpoints table and data sources:

- OSV Name (as configured in the OpenScape Voice Assistant DB)
- OSV node1 name (as configured in the OSV node.cfg)
- OSV node2 name (as configured in the OSV node.cfg)
- OSV PISN ID where this endpoint belongs to-Endpoint name
- Endpoint Type (OpenScape Voice, 4K, PSTN gateway or other)
- Endpoint IP/FQDN
- Endpoint Location: The geographical location of the endpoint.
- PSTN Gateway Service Provider (PSTN gateways only): The telecoms service provider providing access to the PSTN for this gateway

System Specific Information

OpenScape Voice COL is the collection agent that retrieves the CDRs from OpenScape Voice and survivable gateways that produce CDRs such as OpenScape SBC and OpenScape Branch and is bundled with OpenScape Voice AM.

Before OpenScape Voice COL performs a CDR data collection, it must connect via SSH to OpenScape Voice Assistant and retrieve the XML files containing the CDR SFTP info for each OSV server. OpenScape Voice COL subsequently shall perform an automatic configuration of its input lines and shall retrieve the CDRs. Before OpenScape Voice AM performs a data collection, i.e. to read the CDR output from OpenScape Voice COL and process the CDRs, it shall connect via SFTP to OpenScape Voice Assistant and retrieve the XML files containing the non-subscriber SIP endpoints info for each OSV server. OpenScape Voice AM subsequently shall perform an automatic configuration of its data sources (OpenScape Voice systems) and SIP endpoints table and use the new configuration to process the CDRs.

11 Appendix

11.1 Search and Advanced Search Functionality

OpenScape Voice Assistant provides a powerful and flexible configurable Search and Advanced search functionality for quick, focused search and retrieval of specific information.

Search

Search functional helps reducing the search by specifying the search criteria. After applying this functionary, only those elements that match specified search category are displayed as the search result.

Advanced search

The **Advanced...** allows to refine the search even more, by specifying additional criteria in order to retrieve only those elements that match specified search conditions.

Usage of OpenScape Voice Search and Advanced Functionality

The search and advanced functionality offers the following options:

- **Search** (drop-down list)

  The **Search** drop-down list displays search categories matching the area in which you are currently located. Choose the search category to be used as selection criterion in the search process. After applying this search, only those elements that match the specified search category are displayed.
- **Search** (button)

  Click **Search** after selecting a search category from the drop-down list to apply the search.
- **Advanced...** (link)

  Click the **Advanced...** link to define your own advanced search by specifying additional criteria in order to retrieve only those elements that match the specified criteria.

  The **Advanced Search** dialog opens, displaying the search categories that match the area in which you are currently located.

  Configure the criteria for the **Advanced Search**:

  - For fields that accept dates or numbers it is possible to specify a range.
  - For fields that accept specific values, a drop-down list lets you select the available ones.
  - For fields that accept arbitrary text you can use wildcards (e.g. "a*" for listing all the ones that begin with an "a").
- **Advanced Search** / **Add** (button)

  Click **Add** button to store the search criteria in the list.
- **Advanced Search** / **Delete** (button)

  Click **Delete** to discard the search criteria settings.

- **Advanced Search** / **Search** (button)

  Click **Search** button to perform the search and show the result on the main screen.
- **Advanced Search** / **Close** (button)

  Clicking the **Close** button will close the **Advanced Search** dialog without saving the data entered.

11.2 RTP Management via OpenScape Voice Assistant

The RTP (Resilient Telco Platform) Management feature allows the convenient configuration of provisionable OpenScape Voice RTP parameters via a generic interface in the OpenScape Voice Assistant GUI.

Typically, RTP parameters are set during initial switch configuration to enforce global policies and ensure proper feature networking.

The access to the RTP parameter GUI is only possible for administrators with adequate access rights. Since RTP parameters typically affect switch wide configuration in all its range, the administrators must have the access rights to modify switch wide data.

> **NOTICE:**
>
> RTP parameters documented as "For development use only (yes/no): yes" are not visible in the OSV Assistant GUI.

The following parameter data are displayed:

- **Name**

  Name of the RTP parameter as defined in file `RTPparameter.conf`
- **Type**

  Specifies the data type of the RTP parameter

  e.g. Integer, String, Boolean,
- **Unit**

  Specifies the unit of the RTP parameter value

  e.g. days, seconds, binary,
- **Range**

  Specifies the allowed range of RTP parameter value. It depends on type and unit.
- **Process restart is required**

  Determines if a restart is required for any **Value** changes to take effect.
- **Value**

  Specifies the current valid value of the RTP parameter.

> **NOTICE:**
>
> For the configuration of boolean attributes a true/false option is provided via a drop-down menu.

- **Suggested Value**

  Specifies the recommended value for the RTP parameter.
- **Description**

  Displays a detailed description of the impact of the RTP parameter.

> **NOTICE:**
>
> Only the parameter **Value** can be modified, all other parameters are read-only.

Related concepts

Account Codes
Multiple Time Zone Support on page 126
Subscriber Features on page 128
Subscriber-level Feature Provisioning
CAC (Call Admission Control) Group
Malicious Call Trace on page 193
RTP System Parameters on page 150
OpenScape Voice-based Do Not Disturb on page 154
RTP System Parameters on page 305
OpenScape Desk Phone CP Feature Access on page 303
Call Forwarding - Remote Activation on page 288
Call Forwarding System-Internal/External (CFSIE)
CFSIE - Do Not Disturb on page 299
Call Forwarding - Voice Mail
RTP System Parameters on page 327
Multiline Appearance on page 258
SILM Service Provisioning
RTP System Parameters on page 285

11.3 Configuring Advanced Telephony Connector (ATC)

This chapter describes the configuration of Advanced Telephony Connector (ATC). The user must follow the steps in order for ATC to work properly. To register the ATC user at OpenScape Voice (V8R1 or higher), the Dynamic User License is needed.

Procedure

The user has to follow the steps below:

1) Create an Endpoint Profile
2) Create an Endpoint on OSV
3) Create a Subscriber
4) Assign the following features to the Subscriber: **Call Transfer**, **One Number Service** and **CSTA**
5) Enable **Registration via Central SBC allowed**
6) Create a Circuit subscriber

The steps above are explained in detail in the following subchapters.

11.4 Feature Access Codes

OpenScape Voice provides user-dialable codes that allow access to features and services. These Feature Access Codes (sometimes known as VCS (Vertical Service Codes)) can invoke features that reside in OpenScape Voice without special feature keys by entering feature access codes.

NOTICE:

Features that reside in the SIP subscriber endpoint are not invoked with feature access codes.

Access codes are required to ensure the correct operation of many OpenScape Voice features. The required access codes are usually added during the initial installation of the system.

The following table lists the default feature access codes; however, these values listed below may be adapted to the enterprise's custom configuration. Features that do not have specified default access codes are not listed in this table.

Table 213: Default Feature Access Codes

Feature	Access Code
Anonymous call rejection	*77 (activate) *87 (deactivate)
CCBS/NR	*30 (activate) *31 (deactivate)
Call forwarding—all calls	*72 (activate) *73 (deactivate)
Call forwarding—busy line	*90 (activate) *91 (deactivate)
Call forwarding—don't answer	*92 (activate)*93 (deactivate)
Call forwarding, selective—screening list editing	*63
Call pickup—group	*22
Calling ID delivery and suppression	*44 (deliver) *45 (suppress)
Calling name delivery blocking	*68
Calling number delivery blocking	*67
DN announcement	*33
Do not disturb—OpenScape Voice-based	*78 (activate)*79 (deactivate)
Executive override	*35 (activate)*36 (deactivate)*94

Feature	Access Code
Hot desking	*35 (activate) *36 (deactivate)
Hunt group—make busy	*26 (activate) *27 (deactivate) *28 (toggle)
LINR	*32
LONR	*61
Night bell call pickup	*38
Selective call acceptance—screening list editing	*62
Selective call rejection—screening list editing	*60
Serial ringing—screening list editing	*42
Simultaneous ringing	*40 (activate) *41 (deactivate)
Station speed calling, OpenScape Voice-based—one-digit list programming	*74
Station speed calling, OpenScape Voice-based—two-digit list programming	*75
Trace, customer-originated	*57

11.5 SIP Subscriber Endpoint User Features

In addition to the features provided by OpenScape Voice, local user features reside in Unify SIP subscriber endpoints.

The table below lists the local user features; it also indicates the Unify SIP endpoints that support each. Where applicable, the table also includes alternate names for the features.

Refer to OpenScape UC Application documentation for information about the features supported by OpenScape UC Application Personal Edition.

Table 214: Unify SIP Subscriber Endpoint Local Features

Feature	OpenS Desk Phone CP 100 /20 205/ 400/ 600/ 600E/ 700/70(	Open-Scape Desktop Client web embeddec Edition	Open-Scape Desktop Client Persona Edition	oP WL 2 Prof S	Comment
Abbreviated dialing				X	
Access profiles	X	X	X	X	
Address book				X	OpenScape Desk CP SIP telephones permit pictures to be uploaded from a PC and assigned to contacts (Contact directory/contact list) Support of this feature varies by the specific OpenScape Desk Phone CP model.
Advisory tones	X			X	
Alarm clock				X	
Alternate	X	X	X	X	
Anniversary				X	
Audible ringing on rollover lines	X				The audible ringing on rollover lines feature permits lines to audibly signal new incoming calls while the user is active on the keyset. This feature is also known as rollover ringing.
Automatic dialing [16]	X				

[16] The Auto Dial Timer requires the local dial plan option.

Feature	OpenS Desk Phone CP 100 /20 205/ 400/ 600/ 600E/ 700/70	Open-Scape Desktop Client web embedded Edition	Open-Scape Desktop Client Persona Edition	oP WL 2 Prof S	Comment
Automatic recall on held calls	X	X	X		
Bluetooth support	X				Support of this feature varies by the specific OpenScape Desk Phone CP model.
Call deflect	X	X	X		
Call forwarding, unconditional—endpointbased	X		X	X	
Call forwarding on busy—endpoint-based	X		X		
Call forwarding return—endpoint-based	X		X	X	
Call hold	X		X	X	
Call join	X		X	X	Also known as attended transfer.
Call journal/ call list/call log	X		X	X	Support of this feature varies by the specific model.
Call refuse/ call reject	X		X	X	
Call waiting (camp-on)	X		X	X	
Callback request	X		X	X	

Feature	OpenS Desk Phone CP 100 /20 205/ 400/ 600/ 600E/ 700/70	Open-Scape Desktop Client web embedded Edition	Open-Scape Desktop Client Persona Edition	oP WL 2 Prof S	Comment
Codec selection	X		X	X	OpenScape Desk CP telephones support G.722 wideband codec (7 KHz).
Conference[17]	X		X	X	
Configurable DNS name for WBM addressing and phone manager	X	X	X		
Consultation hold	X	X	X	X	
Contact directory/ contact list	X	X	X	X	OpenScape Desk CP SIP telephones permit pictures to be uploaded from a PC and assigned to contacts.
Country settings	X	X	X	X	
DLS user mobility dialing	X				This capability will be available in a future OpenScape Desk Phone CP software version.
Delayed ringing	X				
Deployment service (DLS)	X	X	X		
Direct station select (DSS)	X				Support of this feature varies by the specific OpenScape Desk Phone CP model.

[17] Local 3party conference as well as server based conference is supported.

Feature	OpenS Desk Phone CP 100 /20 205/ 400/ 600/ 600E/ 700/70(	Open-Scape Desktop Client web embeddec Edition	Open-Scape Desktop Client Persona Edition	oP WL 2 Prof S	Comment
Directories	X	X	X	X	
Directory list		X	X	X	
DLS user mobility	X		X		Support of this feature varies by the specific model.
Do not disturb	X		X		
Do-not-interrupt dialing	X				
Drop call key	X	X	X	X	
DTMF tone dialing	X	X	X	X	
Easy answer				X	
easyCom communication circle					
Echo cancellation	X	X	X	X	
Elapsed time display	X			X	
Extended keypad					
Function key programming	X			X	Support of this feature varies by the specific OpenScape Desk Phone CP model.
Handover		X		X	Specific models support handover between different access points.
Handsfree operation	X	X	X	X	Support of this feature varies by the specific model.

Feature	OpenS Desk Phone CP 100 /20 205/ 400/ 600/ 600E/ 700/70(	Open-Scape Desktop Client web embeddec Edition	Open-Scape Desktop Client Persona Edition	oP WL 2 Prof S	Comment
Headset support	X	X	X	X	Support of this feature varies by the specific OpenScape Desk Phone CP model.
Hold, call	X	X	X	X	
Hold, consultation	X	X	X	X	
Hot keypad dialing	X				
Hotline	X		X		Sometimes known as dedicated dialing. This capability will be available in a future OpenScape Desk Phone CP software version.
Hunt group support	X		X		
Instant messaging with OpenScape Voice					
Jitter buffer control	X	X	X	X	The OpenScape Desk Phone CP 100/200/205/400/600/600E/700/700I support adaptive jitter buffer control.
Join	X			X	
Keypad lock	X			X	

Feature	OpenS Desk Phone CP 100 /20 205/ 400/ 600/ 600E/ 700/70	Open-Scape Desktop Client web embedde Edition	Open-Scape Desktop Client Persona Edition	oP WL 2 Prof S	Comment
Keyset operation modes					For OpenScape Desk Phone CP this feature is OpenScape Voice-based. Support of this feature varies by the specific OpenScape Desk Phone CP model.
Language settings	X	X	X	X	
Line focus	X				Support of this feature varies by the specificOpenStage model.
Line key operation modes	X		X		Support of this feature varies by the specificOpenStage model.
Line reservation	X				Support of this feature varies by the specificOpenStage model.
LDAP access	X	X	X	X	Support of this feature varies by the specificOpenStage model.
Local conference	X		X	X	Support of this feature varies by the specificOpenStage model.
Mailbox	X	X	X	X	

Feature	OpenS Desk Phone CP 100 /20 205/ 400/ 600/ 600E/ 700/70(	Open-Scape Desktop Client web embeddec Edition	Open-Scape Desktop Client Persona Edition	oP WL 2 Prof S	Comment
Manual hold	X		X		The multiline appearance (MLA) feature allows for multiple lines to be assigned to a keyset and for a line to be assigned to multiple keysets. This feature is particularly useful for executive-assistant arrangements. For OpenScape Desk CP keyset telephones, this feature is OpenScape Voice-based. Support of this feature varies by the specific OpenScape Desk Phone CP model.
Media encryption	X	X	X		
Media server access	X	X	X	X	
Missed calls list	X	X	X	X	Support of this feature varies by model.
Multiline appearance	X		X		For OpenScape Desk CP keyset telephones, this feature requires configuration in the endpoint and in OpenScape Voice. Support of this feature varies by the specific OpenScape Desk Phone CP model.

Feature	OpenS Desk Phone CP 100 /20 205/ 400/ 600/ 600E/ 700/70(	Open-Scape Desktop Client web embeddec Edition	Open-Scape Desktop Client Persona Edition	oP WL 2 Prof S	Comment
Multiline origination and transfer	X		X		The multiline origination and transfer feature provides the capability to: • Originate or answer calls at any line appearance at any keyset • Transfer calls via consultation transfer • Transfer calls via manual hold This feature is controlled via the endpoint. Support of this feature varies by the specific OpenScape Desk Phone CP model.
Multiline preference	X		X		Support of this feature varies by the specific OpenScape Desk Phone CP model.
Music on hold—endpoint-based	X	X	X	X	
Mute	X	X	X	X	
Night mode				X	

Feature	OpenS Desk Phone CP 100 /20 205/ 400/ 600/ 600E/ 700/70	Open-Scape Desktop Client web embeddec Edition	Open-Scape Desktop Client Persona Edition	oP WL 2 Prof S	Comment
Notebook/ notepad					OpenScape Desk Phone CP models use call logging and redial, which are superior methods to accomplish this functionality.
Onhook dialing	X	X	X	X	
Open listening	X	X	X	X	Support of this feature varies by model.
OpenScape Desk Phone CP Manager	X			X	This freeware tool permits communication with the associated PC and transfer of data. Support of this feature varies by the specific OpenScape Desk Phone CP model.
optiGuide/ TouchGuide	X				OpenScape Desk CP telephones use the TouchGuide.
Outlook integration	X	X	X	X	Synchronization via PC manager is feasible on the OpenScape Desk CP SIP telephones. Support of this feature varies by the specific OpenScape Desk Phone CP model.
Phone Lock	X				
Payload encryption	X	X	X		

Feature	OpenS Desk Phone CP 100 /20 205/ 400/ 600/ 600E/ 700/70(	Open-Scape Desktop Client web embeddec Edition	Open-Scape Desktop Client Persona Edition	oP WL 2 Prof S	Comment
Phantom lines	X		X		A phantom line is identical to a normal line in all respects, except that a phantom line is not assigned to any device as a primary line. This line type can appear as a private line on one keyset or as a shared secondary line on two or more keysets. This feature requires configuration in OpenScape Voice and in the endpoint. Support of this feature varies by the specificOpenStage model.
Phone book	X			X	Support of this feature varies by the specific OpenScape Desk Phone CP model.
Phone lock	X	X	X		
Phone Manager	X				Support of this feature varies by the specific OpenScape Desk Phone CP model.
Pickup group support	X	X	X		
Preview	X				Line preview is available through the OpenScape Desk Phone CP overview screen.

Feature	OpenS Desk Phone CP 100 /20 205/ 400/ 600/ 600E/ 700/70	Open-Scape Desktop Client web embeddec Edition	Open-Scape Desktop Client Persona Edition	oP WL 2 Prof S	Comment
Recall	X				
Redial	X			X	
Registration by number	X	X	X	X	
Repeat dialing	X	X	X	X	OpenScape Desk CP telephones display the called party name as well as the number.
Repertory dialing	X				Support of this feature varies by the specific OpenScape Desk Phone CP model.
Repertory dialing—temporarily shifted keys	X				
Ring tone, variable	X	X	X	X	OpenScape Desk CP SIP telephones permit MP3 ringer tones to be uploaded from a PC and assigned to contacts or groups.
Ringer cutoff	X		X	X	
Room character configuration	X				
ScreenSaver manager	X	X	X		Support of this feature varies by the specific OpenScape Desk Phone CP model.
Second call	X	X	X	X	See also call waiting (camp-on).

Feature	OpenS Desk Phone CP 100 /20 205/ 400/ 600/ 600E/ 700/70(	Open-Scape Desktop Client web embeddec Edition	Open-Scape Desktop Client Persona Edition	oP WL 2 Prof S	Comment
Secure real-time transport protocol (SRTP) support	X	X	X		
Selected dialing	X				Support of this feature varies by the specific OpenScape Desk Phone CP model.
Sensorial navigation	X				Also known as TouchGuide. Support of this feature varies by the specific OpenScape Desk Phone CP model.
Session time support	X	X	X	X	
Silence suppression	X	X	X	X	
SIP Stimulus and SIP Functional modules			X		
Speakerphone	X	X	X	X	The OpenScape Desk Phone CP CP 100/200/205 does not support speakerphone mode.
Stop/ Escape key	X			X	See also drop call key.
Three-way calling	X			X	Also known as local conference.

Feature	OpenS Desk Phone CP 100 /20 205/ 400/ 600/ 600E/ 700/70(	Open-Scape Desktop Client web embeddec Edition	Open-Scape Desktop Client Persona Edition	oP WL 2 Prof S	Comment
Time display	X		X	X	See also elapsed time display. Support of this feature varies by model.
Toggle	X	X	X	X	See also alternate.
Tones and cadences	X	X	X	X	See ring tone, variable.
TouchGuide	X				
Transfer, blind	X	X	X	X	This type permits a transfer without consultation to another party. Blind transfer does not allow the user to control the call during the transfer.

Feature	OpenS Desk Phone CP 100 /20 205/ 400/ 600/ 600E/ 700/70(	Open- Scape Desktop Client web embeddec Edition	Open- Scape Desktop Client Persona Edition	oP WL 2 Prof S	Comment
Transfer, unscreened	X	X	X	X	This type permits the user to perform a call transfer prior to the transferred-to destination answering the call. The transfer request is completed during ringing or call waiting (camp-on). Unlike blind transfer, the user has some control over the attempted transfer. Upon the user hearing ringback tone and seeing a display, the user can complete the transfer before the destination answers. The user can also wait until the destination answers before completing the transfer.
Transfer, with third-party consultation	X	X	X	X	This type permits a screened transfer. After speaking with the transfer-to party, the user can transfer the first party to the transfer destination.
USB support	X	X	X	X	A standard memory stick can be used with the OpenScape Desk CP telephones to back up and restore personal data.

Feature	OpenS Desk Phone CP 100 /20 205/ 400/ 600/ 600E/ 700/70	Open-Scape Desktop Client web embedde Edition	Open-Scape Desktop Client Persona Edition	oP WL 2 Prof S	Comment
Video camera support		X	X		
Video viewer		X	X		
Visual indicators for line and feature key status	X				
VLAN ID via DHCP	X			X	
Volume control	X	X	X	X	
Warmline	X				.
Web-based management tool				X	
Web browser window	X				This capability will be available in a future OpenScape Desk Phone CP endpoint software version.
Xpression access	X	X	X	X	

Abbreviations:

- Prof = Professional

11.6 SIP Overview

This chapter describes the main functions and components as well as response and request methods of the SIP.

11.6.1 SIP Background Information

This chapter describes the motivation that led to the development of SIP.

Initially, Private Branch Exchange and Central Office switch-based telephony system were the main instruments for transmitting voice, however, the Internet has change that. As 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 (Internet Engineering Task Force) 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 RFC 2543 as a standard. Later it was modified and a more up-to-date version was published: RFC 3261.

11.6.2 Functions of SIP

This chapter describes the abilities and disabilities of SIP.

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 QOS (Quality of Service).
- can work other protocols to ensure these functions are carried out.
- can and does function with SOAP (Simple Object Access Protocol), HTTP, XML, VXML, WSDL (Web Services Description Language), UDDI (Universal Description, Discovery and Integration), SDP (Session Description Protocol) and others.

11.6.3 Components of SIP

This chapter describes the terms *Client* and *Server* in context with SIP.

In a typical SIP scenario, the devices interacting are called UA (User Agents). User Agents may operate as:

- a UAC (User Agent Client) which initiates requests and send those to servers.

- a UAS (User Agent Server) which receives requests, processes them, and generate responses.

NOTICE:

You may find that a single User Agent may hand 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 computer. 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 setup to handle the requests sent by clients. These Servers may be:

- *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.

11.6.4 Request Methods of SIP

This chapter describes the purpose of 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 requests and responses for the system to operate smoothly. There are 13 request methods:

- ACK
- BYE
- CANCEL
- INFO
- INVITE
- MESSAGE
- NOTIFY
- OPTIONS
- PRACK
- REFER
- REGISTER
- SUBSCRIBE
- UPDATE

11.6.5 SIP Request Method – ACK

The request method ACK is used to acknowledge the reception of a final response to an INVITE request.

Functional Sequence

Client originating INVITE request issues ACK after receiving response. In essence, this is a three-way handshake:

1) INVITE request from calling UA
2) Final response from called UA
3) ACK request from calling UA

11.6.6 SIP Request Method – BYE

The request method BYE is used to end sessions.

Functional Sequence

On a two-party call:

1) The first UA (User Agent) hangs up and sends a BYE request.
2) The second UA receives the BYE request and sends “200 OK” response.

System Specific Information

On multicast calls BYE requests may be optionally sent when one party leaves. The session is not affected. For more than eight (8) participants a BYE request is usually not sent in order to reduce traffic.

11.6.7 SIP Request Method – CANCEL

The request method CANCEL is used to cancel pending transactions.

System Specific Information

Pending transactions can be:

- The calling UA (User Agent) hangs up after called UA begins ringing, but does not answer.
- The calling UA sends a CANCEL request.
- The called UA receives a CANCEL request, stops ringing and sends a “200 OK” response and a “487 Transaction Canceled” response.
- The calling UA finishes “three-way handshake” by sending an ACK request.

11.6.8 SIP Request Method – INVITE

The request method INVITE is used to indicate that a user or service wishes to participate in a session.

Functional Sequence

The called UA (User Agent) begins alerting and returns “180 Ringing” response to the calling UA. The calling UA accepts the call with similar session description.

11.6.9 SIP Request Method – MESSAGE

This request method may be used to support instant messaging over SIP.

11.6.10 SIP Request Method – NOTIFY

This request method may be used to provide specific event notification. See also SUBSCRIBE method.

11.6.11 SIP Request Method – OPTIONS

The request method OPTIONS is used to query a server about its capabilities.

System Specific Information

The SDP (Session Description Protocol) replies with a "200 OK" response.

11.6.12 SIP Request Method – PRACK

This request method provides a provisional response used to establish a connection before call completion.

11.6.13 SIP Request Method – REFER

This request method provides the signaling for a user to transfer one user to another.

11.6.14 SIP Request Method – REGISTER

The request method REGISTER is used to inform a registrar server about its current location. It also contains information about when the registration is valid.

System Specific Information

The registrar server supports registration of users even at several locations. In this case the registrar server searches until the user is located.

11.6.15 SIP Request Method – SUBSCRIBE

This request method may be used to request notification of specific events. See also NOTIFY method.

11.6.16 SIP Request Method – UPDATE

This request method provides the mechanism for a client to update parameters of a session (such as the set of media streams and their codecs), but has no impact on the state of a dialog.

11.6.17 INVITE Request Message Format of SIP

The INVITE request message format describes which content an INVITE request message must have.

System Specific Information

The header described by the request message format contains the following elements:

- **Request-Line**

  Contains Method SP (Single Space), Request-URI, SP SIP version, CRLF (Carriage Return + Line Feed).
- **Via**

  Contains the local address of the calling user, that is, pc33.server1.com where it is expecting the responses to come.

- **Max-Forward**

  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**

  Contains the display name of the called user and a SIP or SIPS URI.
- **From**

  Contains the display name of the calling user and a SIP or SIPS URI. 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**

  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**

  Contains a SIP or SIPS URI that is a direct route to the calling user. It contains a username and a FQDN (Fully Qualified Domain Name). It may also have an IP address.
- **Via**

  Used to send the response to the request. Contact field is used to send future requests. When a user generates a BYE request (a new request and not a response to INVITE), it goes directly to the other user bypassing the proxies.
- **Content-Type**

  Contains a description of the message body.
- **Content-Length**

  An octet (byte) count of the message body.

11.6.18 Response Message Format of SIP

The INVITE response message format describes which content a response to an INVITE request message must have.

System Specific Information

The header described by the Response Message Format contains the following elements:

- **Status Line**

  Contains SIP version, SP status code, SP reason phrase and CRLF.
- **Via**

  Contains the local address of the calling user, that is, pc33.server1.com where it is expecting the responses to come. There can be more than one

Via fields, because each element through which the INVITE request was being passed has added its identity in the Via field.

- **Max-Forward**

  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 the display name of the called user, a SIP or SIPS (Secure SIP) URI and a tag. The tag is used to represent the called user in a dialog.
- **From**

  Contains the display name of the calling user and a SIP or SIPS URI. 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**

  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**

  Contains the exact address of the called user. So the calling user doesn't need to use the proxy servers to find the called user in the future.
- **Via**

  Used to send the response to the request. Contact field is used to send future requests. When a user generates a BYE request (a new request and not a response to INVITE), it goes directly to the other user bypassing the proxies.
- **Content-Type**

  Contains a description of the message body.
- Content-Length

  An octet (byte) count of the message body.

11.6.19 Response Types of SIP

This chapter describes which status codes exist and which functions they have.

The first digit of a status code defines the category of the response. SIP/2.0 allows the following six response types:

General Code	Code Range	Response Class	Comment
1xx	100-199	Informational	Request received, continuing to process the request

General Code	Code Range	Response Class	Comment
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

11.6.20 SIP Informational Responses

The 1xx responses provide information concerning the INVITE messages.

Table 215: Informational Responses

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 (User Agent) 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.

Response Code	Response	Comment
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.

11.6.21 SIP Success Responses

The 2xx responses provide information indicating that the request was successful and may give additional information.

Table 216: Success Responses

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.

11.6.22 SIP Redirect Responses

The 3xx responses give information about the user's new location, or about alternative services that might be able to satisfy the call.

Table 217: Redirect Responses

Response 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 (User Agent)) can select a preferred communication end point and redirect its request to that location.
301	Moved Permanently	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.

Response Code	Response	Comment
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.

11.6.23 SIP Client Error Responses

The 4xx responses are definite failure responses from a particular server.

Table 218: Client Error Responses (excerpt)

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”.

Response Code	Response	Comment
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.
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.

11.6.24 SIP Server Error Responses

The 5xx responses are failure responses given when a server itself has erred.

Table 219: Server Error Responses

Response 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 (User Agent Server) 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.
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 (User Agent Client)) 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.

Response Code	Response	Comment
505	SIP Version Not Supported	The server does not support, or refuses to support, the SIP 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.

11.6.25 SIP Global Failure Responses

The 6xx responses indicate that a server has definitive information about a particular user, not just the particular instance indicated in the request URI.

Table 220: Global Failure Responses

Response Code	Response	Comment
600	Busy Everywhere	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.

11.6.26 Important Terms

It is helpful to clarify the various terms used when discussing the SIP protocol:

- Messages

  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.

- Transaction

  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

  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.

- Call

  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.

11.6.27 Registration in SIP

This chapter describes the registration process in SIP.

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.

Functional Sequence

1) The user registers (reports) its current location to a registrar server.
2) The user application sends a message called *register* to a registrar server in order to inform it about the present location of the user.
3) The registrar server stores this information on a Location server. This information is called a *binding* (between the user and its present address). It is also used by other proxies to locate the user.

11.6.28 SIP Session Example

This chapter describes an example of a typical SIP session.

The following graphic shows a typical succession of SIP requests and responses:

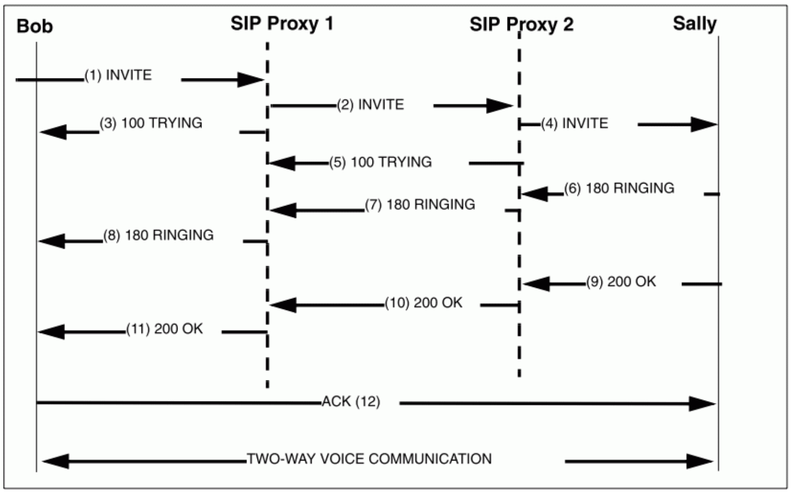


Figure 98: SIP session example

Explanation of the example: User A uses his SIP phone to reach the SIP phone of user B. SIP proxy 1 and SIP proxy 2 help to setup the session on behalf of the users. Each message contains a 3-digit-number followed by a name:

1) The transaction starts with user A making an INVITE request to user B.

2) Since user A doesn't know the exact location of user B in the IP network, user A’s device passes the request through to SIP proxy1. SIP proxy 1 on behalf of user A forwards an INVITE request for user B to SIP proxy 2.

3) SIP proxy 1 sends a TRYING response to user A indicating that it is trying to reach user B.

4) SIP proxy 2, which knows the location of user B, forwards an INVITE request to user B. (If SIP proxy 2 wouldn’t know the location of user B, it would have forwarded it to another SIP proxy server.)

5) After forwarding INVITE 3, SIP proxy 2 issues a TRYING response to SIP proxy 1.

6) The SIP phone, upon receiving the INVITE request, starts ringing user B, indicating that a call request has come. User B’s SIP phone sends a RINGING response back to SIP proxy 2.

7) SIP proxy 2 forwards the RINGING response to SIP proxy 1.

8) SIP proxy 1 forwards the RINGING response to user A.

9) User B accepts the incoming call and a "200 OK" response is sent by user B’s phone to SIP proxy 2.

10) SIP proxy 2 forwards the "200 OK" response to SIP proxy 1.

11) SIP proxy 1 forwards the "200 OK" response to user A.

12) User A’s phone sends an ACK message directly to user B’s phone to confirm the setup of the call.

The media exchange takes place between user A’s and user B’s phones. The proxy servers are not involved in the media exchange. The media flow is controlled using protocols different from SIP, for example, RTP (Real-Time Transport Protocol).

Index