PORTA ONE

PortaSIP

Administrator Guide

55

Maintenance Release

Documentation

©2000-2016 PortaOne, Inc.
All rights reserved

www.portaone.com

Copyright Notice & Disclaimers

Copyright © 2000–2016 PortaOne, Inc. All rights reserved.

PortaSIP® Administrator Guide, May 2016
Maintenance Release 55
V1.55.03

Please address your comments and suggestions to: Sales Department, PortaOne, Inc. Suite #408, 2963 Glen Drive, Coquitlam BC V3B 2P7 Canada.

Changes may be made periodically to the information in this publication. The changes will be incorporated in new editions of the guide. The software described in this document is furnished under a license agreement, and may be used or copied only in accordance with the terms thereof. It is against the law to copy the software on any other medium, except as specifically provided in the license agreement. The licensee may make one copy of the software for backup purposes. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopied, recorded or otherwise, without the prior written permission of PortaOne Inc.

The software license and limited warranty for the accompanying products are set forth in the information packet supplied with the product, and are incorporated herein by this reference. If you cannot locate the software license, contact your PortaOne representative for a copy.

All product names mentioned in this manual are for identification purposes only, and are either trademarks or registered trademarks of their respective owners.

Table of Contents

Preface 5
Hardware and Software Requirements 6
Installation 6

1. System Concepts 7

PortaSIP's Role in Your VoIP Network 8
PortaSIP® Cluster 11
Geographically Dispersed Installation 16
PortaSIP® Performance 18
Call Handling Rules 19
IP Centrex Concepts 23
Call Process / Supported Services 27
Video Calls via SIP 37
Presence 38
Busy Lamp Field (BLF) 41
Call Recording 43
Virtual SIP Servers 44
Call Flow with multiple PortaSIP servers 45
Understanding SIP Call Routing 47
NAT Traversal Guidelines 48
Auto-provisioning IP Phones 56
PortaSIP and Emergency Services (E911) 58

2. Advanced Features 60

User Authentication 61
Special Destinations 64
IP Centrex Call Rating 67
Voice On-net Rating 68
Special Access Codes 68
IP Centrex Feature Management 69
Call Transfer 69
Call Forwarding 75
Call Forking 81
Call Screening 82
Call Parking 84
Call Barring 85
Customer Sites 85
Calls per Second Control 86
Ring-back Tone Generation and Early Media Relying 87
Paging / Intercom Calls 89
SIP Identity 90
Support for Privacy Flags 94
Service Announcements via the Media Server 95
NAT Keep-alive 97
Keep-alive Call Monitoring 97
First Login Greeting 98
Voiceover Announcements 98
SIP TAPI 100

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

Web Call Button 100
Direct Incoming Calls to B2BUA 102
Incoming Call Delivery to an IP PBX with Dynamic IP Address 103
Calls from Vendor via SIP 107
Routing Filters 108
Legal Call Intercept 111
Secure Calling 112
SIP Over TLS 113
Media Encryption in PortaSwitch® 113
Tools for Prevention of VoIP Fraud 118
Protection from DoS Attacks 124
Special Prompt for Calls to Ported Number 125
Caller ID (CNAM) Lookup 126
Comfort Ringtone Generation 127
"Phone Book" for Each Phone Line 127

3. IP Centrex Features 129

4. Messaging Services 143

Instant Messaging 144
SMS Message Processing 145

5. Administration 149

SIP Log Viewer 150
Troubleshooting Common Problems 153
FAQ 154
How to 158

6. Appendices 162

APPENDIX A. Supported SIP RFCs 163
APPENDIX B. Cisco GW Setup for PortaSIP (COMEDIA) 165
APPENDIX C. Client's Sipura Configuration for PortaSIP 165
APPENDIX D. Configuring Windows Messenger for Use as a SIP User Agent 167
APPENDIX E. SJPhone Configuration for PortaSIP 170
APPENDIX F. SIP Devices with Auto-provisioning 172
APPENDIX G. Service Policy Configuration for Ring-back Tone Generation and Early Media Relaying 174

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

Preface

This document provides administrators with information about PortaSIP®'s architecture, functionality and supported features. The last section of the document answers the most frequently asked questions.

Where to get the latest version of this guide

You can access the latest copy of this guide at: **www.portaone.com/support/documentation/**.

Conventions

This publication uses the following conventions:

Commands and keywords are given in **boldface**.

Exclamation mark draws your attention to important actions that must be taken for proper configuration.

NOTE: Notes contain additional information to supplement or accentuate important points in the text.

Timesaver means that you can save time by taking the action described here.

Tips provide information that might help you solve a problem.

Gear points out that this feature must be enabled on the Configuration server.

Trademarks and Copyrights

PortaBilling®, PortaSIP® and PortaSwitch® are registered trademarks of PortaOne, Inc.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

Hardware and Software Requirements

Server System Recommendations

- A minimum of 250 GB of available disk space; this space is required for storing various log files.
- A 64-bit processor (Xeon, Opteron).
- At least 16 GB of RAM, 32 GB recommended.

For additional details and configuration advice, see the *Hardware Recommendations* topic on our website:

http://www.portaone.com/support/hw-requirements/

For information about whether particular hardware is supported by Oracle Enterprise Linux used as the operating system in PortaSwitch®, consult the related document on the Oracle or RedHat website: **https://hardware.redhat.com/**.

Installation

PortaSwitch® installation ISO files contain everything required for installing Oracle Enterprise Linux (64-bit version), PortaSwitch® and the supplementary packages that are necessary for convenient system administration and maintenance.

After the installation is complete you will assign roles (e.g. RADIUS, web interface, PortaSIP, etc.) to individual servers using the configuration server tool – this will automatically enable the required components of PortaSIP® software on each server.

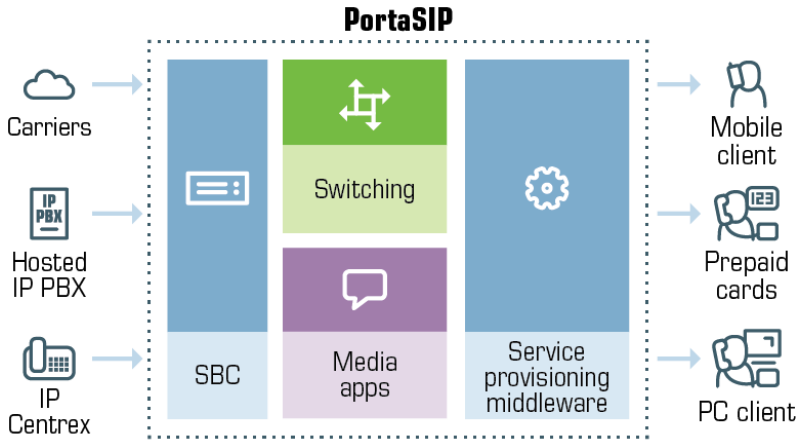
For detailed installation instructions, please refer to the **PortaSwitch® Installation Guide.**

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

1. System Concepts

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

PortaSIP's Role in Your VoIP Network



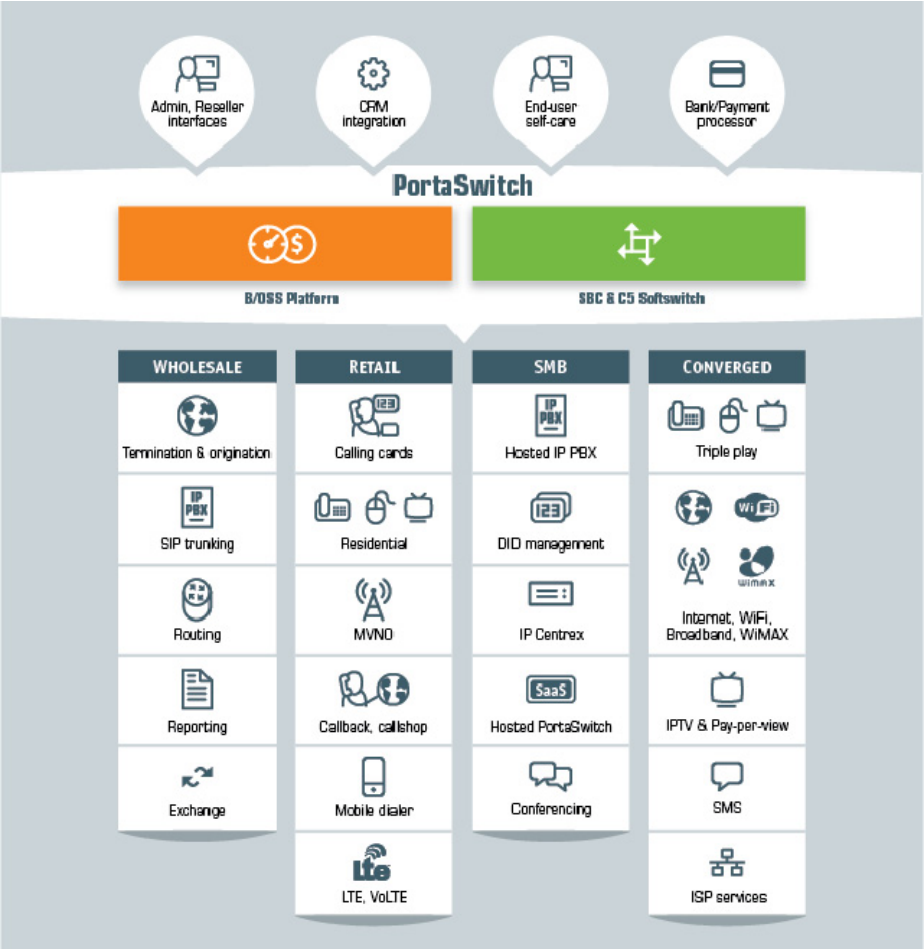
PortaSIP® is a call control software package enabling service providers to build scalable, reliable VoIP networks. Based on the Session Initiation Protocol (SIP), PortaSIP® provides a full array of call routing capabilities to maximize performance for both small and large packet voice networks.

PortaSIP® allows IP Telephony Service Providers to deliver communication services at unusually low initial and operating costs that cannot be matched by yesterday's circuit-switched and narrowband service provider PSTN networks.

In addition to conventional IP telephony services, PortaSIP® provides a solution to the NAT traversal problem and enhances ITSP network management capabilities. It can be used to provide residential, business (IP Centrex) and wholesale traffic exchange services.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

PortaSIP® functions



PortaSIP® provides the following functionalities:

- SIP registration, allowing SIP phones to use the service from any IP address (static or dynamically assigned).
- Multiple hosted IP PBX environments on the same physical server.
- Real-time authorization for all calls, limit on the maximum number of simultaneous calls per customer.
- NAT traversal, media proxying, protection against DoS (Denial of Service) attacks.
- Multi-lingual (voice) error announcements from the media server and customizable greeting upon successful service activation.
- Automatic disconnect of calls when the maximum credit time is reached; ability to dynamically lock the funds required to cover the next interval, thus ensuring overdraft protection even if multiple calls are made concurrently.
- Automatic disconnect of calls when one of the parties goes offline due to a network outage.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

- Various IP Centrex features: call waiting, call transfer, call hold, music on hold, huntgroups, follow-me, etc.
- Fail-over routing – a list of routes arranged according to cost, preference and customer routing plan is supplied by PortaBilling®.
- Forwarding of calls to the voicemail service (Media Server) if a SIP phone is not available.

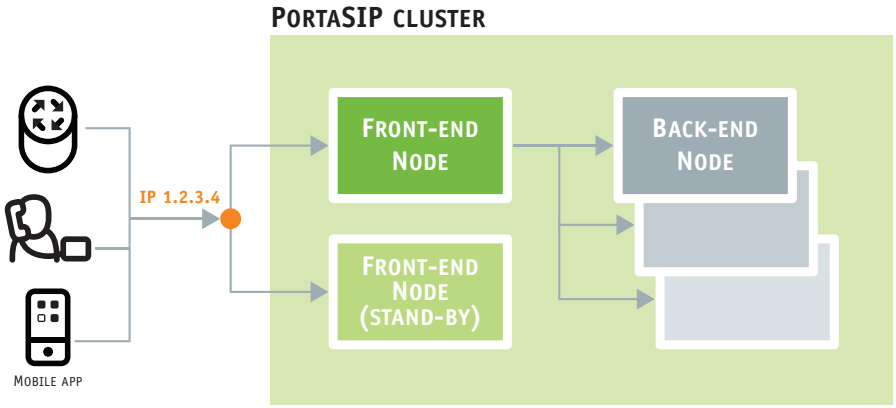
© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

PortaSIP® Cluster

The PortaSIP® cluster combines functions of both SIP switching and media servers and provides a single point of entry (a single visible IP address) to your wholesale partners and SIP trunking, and to your IP Centrex, residential, mobile and other customers. Incoming calls are handled first by a dispatching node and then are evenly distributed to back-end processing nodes. As a result:

- The interconnection process with other carriers and customers becomes really simple.
- Your network topology is not exposed to either your customers or carrier partners.
- In case of a hardware failure at one of the servers, the system automatically reconfigures and keeps processing calls without any changes on the client side.
- Call activity is load-balanced among available processing nodes.
- Your overall traffic processing capability can be easily scaled up by simply adding more back-end PortaSIP® servers.

Architecture



PortaSIP® cluster components

A PortaSIP® cluster consists of the following components:

Dispatching node

- Virtual IP address – The virtual IP address serves as an entry point to the cluster. That is, all SIP traffic sent from / to the cluster is routed via the virtual IP address. This IP address is visible to customers and carrier partners, while your actual network topology is hidden from the outside world.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

The virtual IP address is shared among all dispatching nodes in the cluster, though it is only used by the active dispatching node. The currently active dispatching node, as the center of all communication, is always at the virtual IP address. If this dispatching node becomes unavailable for some reason (e.g. due to a failure), the virtual IP address is switched to another dispatching node that becomes active.

NOTE: The PortaSIP® cluster's virtual IP address must always be public.

- Edge Proxy – The Edge Proxy communicates directly with customers' and vendors' equipment via the SIP protocol, sheltering the core cluster's components from direct access. The Edge Proxy also provides NAT traversal and performs load balancing of incoming traffic among all components in the cluster.
- Processing Node Controller – The Processing Node Controller keeps track of the active components in the cluster. If one or more components become inactive, the Processing Node Controller detects this change and notifies the other cluster's components accordingly.
- Limit Controller – The Limit Controller regulates the number of dialing attempts that can be made by an endpoint (e.g. an IP PBX) each second.
- Cluster Protector – The Cluster Protector is responsible for the cluster's security. It protects the cluster from network threats, such as denial of service attacks.
- Mail Proxy – The Mail Proxy forwards email, voice mail and fax messages to an available processing node for further processing. The Mail Proxy supports IMAP, SMTP and SMTPS protocols.
- SMPP Proxy – The SMPP Proxy performs the following functions:
    - Forwards messages received by the PortaSIP® cluster via the SMPP protocol to the active IMGate for further processing.
    - Transmits messages received from the IMGate to SMSCs (short message service centers) or SMS aggregators for further delivery to mobile networks.

Processing node

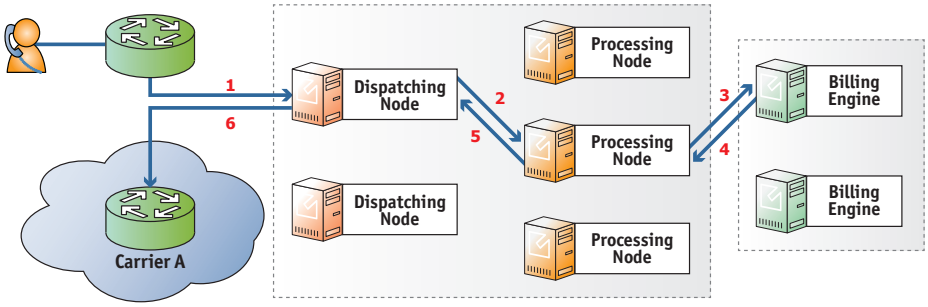
- Call Controller – The Call Controller combines functionalities of the Back-to-Back User Agent, the RTP Proxy and Media Server. Its main tasks include:
    - Processing call initiation requests (INVITE SIP messages) from endpoints and initiating outgoing calls.
    - Transporting the media stream (the actual voice traffic) from one endpoint to another.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

- Playing a number of short voice prompts (such as current balance, maximum allowed call duration, etc.) to end users.

- Registrar – The Registrar processes registration requests from customers' IP phones and stores their location information.
- Subscription Manager – The Subscription Manager communicates both with users' devices and with cluster components handling presence requests and sends notifications about users' availability. This is a key component for providing presence and BLF services where it is important to see whether another party is currently online, off-line, busy, etc.
- IMGate – The IMGate enables online messaging and message storage for offline users (so they can receive messages later).

Usage scenario



- A call originates from your customer's network to the visible IP address of your PortaSIP® cluster.
- The call initiation request is delivered to the currently active dispatching node (1).
- The dispatching node forwards the call to one of the available processing nodes (2).
- The processing node receives the call request and sends an authorization request to PortaBilling® (3).
- PortaBilling® validates the call credentials, balance and other settings (e.g. geo-IP restrictions), and computes a list of outgoing routes. The result is then returned to the processing node (4).
- The processing node attempts to establish an outgoing call leg and sends a call initiation request to the dispatching node (5).
- The dispatching node forwards the call request to the actual gateway of the termination carrier (6).
- All further communication is forwarded via the dispatching node, so the customer (originator) and carrier (terminating party) only see the visible IP address of the PortaSIP® cluster.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

IP Aliasing in PortaSIP® cluster

Beginning with this release, IP aliasing is a simplest way to migrate customers from the classic PortaSIP® installation or even from external providers to the PortaSIP® cluster.

Consider the following example. A service provider has configured a PortaSIP® cluster and uses it. This service provider then acquires some new customers but their IP phones are configured to use another provider's SIP server – and the service provider would like to migrate them to the PortaSIP® cluster.

With IP aliasing functionality, the tedious reconfiguration of each customer's IP phone is not required. Instead, an administrator configures the IP address of the external SIP server as an alias to the PortaSIP® cluster's IP address.

Along with the IP alias, the administrator can also define additional transport ports for the following protocols: UDP, TCP and TLS. This step is optional and only required if standard transport ports for these protocols are blocked for some reason or cannot be used.

The IP aliasing functionality significantly simplifies the migration procedure to the PortaSIP® cluster and makes the entire process of migration fully transparent for end users.

Call delivery to IP phones registered via IP alias

- User A's SIP phone registers with the PortaSIP® cluster via an IP alias and the following record is created in the registration database:

  ```
  sip:User A@IP alias:port
  ```

- User B, whose SIP phone is registered to the PortaSIP® cluster via the main IP address, dials user A's phone number and an INVITE request is sent with the following addresses-of-record (AORs) in the `From:` and `To:` headers:

  ```
  From:User B@IP address
  To:User A@IP address
  ```

  The INVITE request is delivered to the PortaSIP cluster's main IP address (1).
- The dispatching node forwards the call to one of the available processing nodes (2).
- The processing node sends an authorization request to PortaBilling® (3) and receives an authorization response (4).
- Once authorized successfully, the call is further processed. The B2BUA checks the registration database and detects that user A's SIP phone is registered with an IP alias. The B2BUA therefore changes the AORs in the `From:` and `To:` headers as follows (5):

  ```
  From:User B@IP alias
  ```

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

```
To:User A@IP alias
```

- The B2BUA routes the call to the dispatching node (6).
- Finally the dispatching node establishes the call with user A's IP alias (7).

The key point in this scenario is that the same IP address and port for call delivery is used as what was used by the PortaSIP® cluster during the recipient's SIP phone registration.

Handling a failure

While there are multiple *dispatching* nodes (each on its own physical server), only one *dispatching* node is active (receiving and distributing call requests), so all others are on standby. All servers in the cluster exchange heartbeat messages and if the server with the currently active dispatching node becomes unavailable due to hardware failure, the IP address is immediately switched to another server. That dispatching node is then activated to receive and distribute call requests.

The list of available processing nodes is constantly updated – entries are added when a processing node instance is started on a new server and removed when the server where the processing node was running, becomes unavailable due to a hardware failure.

One of the remaining processing nodes immediately disconnects calls handled by a failed node and sends accounting records to the billing engine for these calls. Accordingly, subsequent call attempts are distributed among the remaining processing nodes.

Deployment recommendations

For normal operation, a PortaSIP® cluster requires at least two servers where dispatching nodes are deployed. The number of processing nodes is virtually unlimited and only depends on the required total processing capacity.

The current PortaSIP® cluster architecture allows for the efficient handling of Class 4 services (wholesale traffic exchange, SIP trunking, etc.) and Class 5 services (SIP registration, IP Centrex, presence (UA status publishing), etc.). The BLF service is supported for calls made or received by customer accounts and for calls made to account aliases, too.

Since a PortaSIP® cluster presents a *single* visible IP address to your partners and customers, cluster servers must be located in the same site (geographic area).

Receiving call requests on a single IP address allows you to receive traffic from customers with legacy equipment (which send traffic to a single SIP

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

proxy IP address) and process it in the PortaSIP® cluster, consequently making use of all its benefits. This solution allows you to efficiently scale your system to meet the requirements of growing wholesale call traffic.

FAQ

Can customers connect directly to a processing node?

The PortaSIP® cluster virtual IP address is the only point of entry to your network, therefore only this IP address can be used for registration.

What IP address is provided to my customers and termination partners?

The dispatching node IP address, since it is the center of all communication. The customer (originator) and the carrier (terminating party) see only the visible IP address of the PortaSIP® cluster.

Is there a solution for preventing PortaSIP cluster overload by customers who have a huge CPS rate?

Yes, the PortaSIP® cluster's Limit Controller component allows the enforcement of so many calls per second. With this functionality you can decide upon and restrict the number of dialing attempts that can be made by an endpoint (e.g. a call center PBX) per second.

For more information, please refer to the **Calls per Second Control** section.

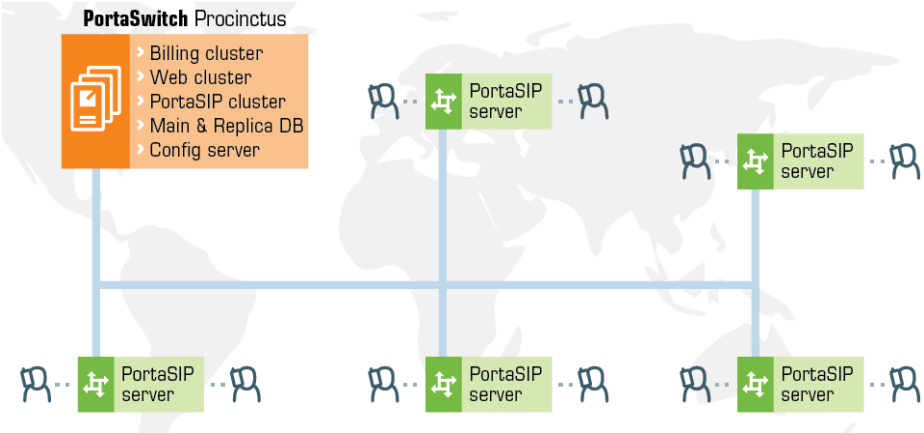
Is there a specific router configuration for the PortaSIP® cluster?

No, there is no additional configuration requirement for routers or other network elements.

Geographically Dispersed Installation

You can install several SIP servers in different geographical locations (as shown below), enabling users within a certain network to use the closest available SIP server. So if user A from Singapore calls user B, also from Singapore, the call will be handled by the PortaSIP server in Singapore, and the voice traffic will travel only via the Singapore backbone.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com



This allows VoIP services to be efficiently provided in a situation which is highly typical for many countries or regions: good, fast Internet connectivity inside the country / region and mediocre connectivity with the rest of the world. For all users inside that region, VoIP traffic (signaling and RTP) will travel on the local backbone, while only small RADIUS packets will travel to the central PortaSwitch® location.

Multi-site PortaSIP® Cluster

Each of your geo-redundant installation sites can have a PortaSIP® cluster with a single point of entry. Though they operate independently, the sites are interconnected, allowing you to provision services without disruption if any of the sites are down or unavailable for any reason.

The deployment of the PortaSIP® cluster on each site simplifies the network and services configuration for administrators. Users are provided with a single visible IP address for each cluster to register with. For example, PortaSwitch® is deployed across two sites: the main site is located in the US and the secondary site is located in Singapore. Each site has the PortaSIP® cluster configured. To start providing services to end users, the administrator provisions only two IP addresses: the US site IP address and the Singapore site IP address. This simplifies service provisioning to users who have previous-generation devices.

Though the PortaSIP® cluster is extensible and can contain virtually an unlimited number of nodes (servers), only one logical node representing the whole cluster, (i.e. the dispatching node) is provisioned in PortaBilling® and defined in the **Usage Charges** section of a product. This significantly simplifies service configuration and product management and serves to reduce the load on administrators.

When using the multi-site PortaSIP® cluster solution, service providers will be able to:

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

- Provide services without disruption, despite whatever disaster may occur to any of the sites within the PortaSwitch® network (fire, flood, power outage, etc.).
- Increase the number of processed call requests and balance loads among nodes within the PortaSIP® cluster on every site.
- Improve the quality of the services provided by defining the IP address of the site that is geographically closest to the user as the primary one to register on (from the example above, users from the US will register with the US site IP address as the primary one while users from Singapore will use the Singapore IP address as their primary one to register).

The ability to perform a software upgrade of a clustered site redundancy solution to newer releases with zero-downtime will be added in future releases.

PortaSIP® Performance

The PortaSIP® cluster is a combination of a dispatching node and a processing node. While the dispatching node is the center of communication in the PortaSIP® cluster (it receives and distributes call requests), the processing node is what handles the call processing. Therefore, when assessing the PortaSIP® cluster performance, the processing node must be considered.

To achieve higher performance, scale up your PortaSIP® cluster with additional processing nodes.

There are three important criteria by which PortaSIP® performance can be assessed:

- How many simultaneously registered SIP phones can it handle?
- How many concurrent calls can it handle?
- What is the maximum number of call attempts per second that it can process?

A single PortaSIP® cluster processing node residing on a separate PortaSIP® server (assuming this server meets the hardware requirements described on **www.portaone.com**) can process about **250 call attempts per second**. This means that every second, 250 users can begin a new phone call on your network (and the same amount of users could end their calls concurrently). In addition, the processing node can process about 500 registration attempts per second (for services such as IP Centrex). Assuming that each phone re-registers every 10 minutes, on average, this translates to more than **150,000 simultaneously registered SIP phones**.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

How many concurrent calls does that translate into?

Assuming the PortaSIP® cluster processing node is working in SIP signaling-only mode, this would primarily depend on the average call duration (ALOC) and call success rate (ASR). Given an aggregated call processing speed of 250 call attempts per second, an average call duration of 5 minutes and a call success rate of 50% (the industry norms), 50% of the 250 attempted calls per second would succeed. This means that 125 calls would be connected while the same amount of previously connected calls would be disconnected. Since the average call duration is 300 seconds (5 minutes), approximately 125 * 300 = **37,500** calls would be in a "connected" state at all times. Obviously if either your ASR or ALOC change, that would have an immediate impact on the number of concurrent calls.

If RTP proxying is done for calls, then another consideration is the amount of voice traffic that has to pass through the server. Voice stream is extremely sensitive to delays in processing, so using a high-end network adapter is highly recommended.

A single PortaSIP® cluster processing node can proxy up to **3,000 concurrent calls**.

How much bandwidth is required for call handling?

For a single call the PortaSIP® cluster normally needs to transfer 10-20 KB of SIP signaling data, and this takes up about 50 bps of the channel.

For the 3,000 calls that the PortaSIP® cluster can proxy, signaling traffic becomes noticeable. If one call takes up 50 bps of the channel, 3,000 calls can take up 150,000 bps which equals 0.15 Mbps.

However, the bandwidth required for SIP signaling is insignificant compared to that used by the RTP stream: 3,000 calls using the g711 codec consume up to 467 Mbps of bandwidth.

Therefore, in order to handle each of the 3,000 concurrent proxied calls you must allocate a sufficient amount of bandwidth for signaling and for RTP proxying – approximately 468 Mbps in total.

Call Handling Rules

When a call comes to PortaSIP®, it has to be authenticated (to verify that it is coming from a legitimate customer or vendor), processed, and then delivered to its destination. Although this sounds simple and straightforward, there are many variations for how exactly it should be

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

done. For example, when handling a call coming from a residential VoIP user, a different approach is used than when processing a call from a wholesale carrier.

In order to allow PortaSIP® to adapt to the requirements of various business models and, at the same time, to process different types of calls, it can follow different scenarios when handling a call. One of the most important things defined by a call handling scenario is the type of authentication to be performed. For example, do we return a challenge to the SIP device and request digest authentication, or do we just take its IP address as the identity for authentication?

Thus PortaSIP's call processing logic consists of call handling rules. Each rule contains:

- conditions to be evaluated against the parameters of incoming calls, to see whether the rule is applicable;
- a selected call handling scenario;
- additional parameters for that scenario.

Call handling rules – conditions

The administrator can define conditions to satisfy each of the following parameters of a call request:

- IP address of the remote party (note that the "signaling" address is used, i.e. the IP address from which PortaSIP receives the INVITE, not the information in the INVITE request itself, e.g. "Contact" or "From").
- The called phone number (CLD).
- The phone number of the calling party (CLI).

Each of these conditions may be empty, in which case no verification is performed. If multiple conditions are listed, they must all satisfy the call request in order to apply this rule. For instance, if the remote IP condition says "1.2.3.4" and the CLD condition says "1234#", the rule will be applied only if the call comes from IP address 1.2.3.4 *and* the destination phone number starts with 1234#.

Call handling rules – multiple rules

When the SIP proxy receives a call initiation (INVITE) request from a SIP device, PortaSIP® determines how to process the call by evaluating the conditions of the first call handling rule against the parameters of the INVITE request. If the conditions do not satisfy the INVITE request, the conditions for the second rule are evaluated, etc. until a rule is found where all the conditions are met to satisfy the INVITE request. PortaSIP® tries to process the call with this rule. PortaSIP® searches an appropriate SIP header (to obtain the identity for authentication) in the INVITE request. If the identity is found, then PortaSIP® sends the

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

authorization request to the billing engine with the obtained identity in the User-Name attribute. If the INVITE request *doesn't* contain an appropriate SIP header or its value (meaning the required identity for authentication can't be obtained), then PortaSIP® proceeds to evaluate the rules until it finds another rule where all the conditions are met to satisfy the INVITE request. PortaSIP® attempts to process the call with this rule. If the appropriate identity is obtained from the INVITE request then PortaSIP® sends the authorization request to the billing engine with this identity in the User-Name attribute.

If no rules satisfy the conditions for a given INVITE request or the appropriate identity can't be obtained from the INVITE request (for those that do satisfy the conditions) then the digest authentication is applied for the call.

Since rules thus work based on the "first match", the order in which they are arranged becomes very important. Normally, you would place more specific rules (e.g. "call comes from IP 5.6.7.8 and CLI starts with 44") at the top of the list, and more generic ones (e.g. "call comes from IP 5.6.7.8") at the bottom.

Note, that prior to Maintenance Release 34 only the top call handling rule that met all of the same conditions (IP address, CLD and CLI satisfied the INVITE request) was used to process the call and the other rules were ignored. With Maintenance Release 34 the other rules *can be used* as well.

Available call handling scenarios

These include:

- Apply **digest** authentication (this is the default call handling scenario).
- Use authentication by **IP**. The identity for authentication is the IP address of the gateway from which PortaSIP® receives the INVITE request.
- Use authentication by **CLI / CLD Tech-Prefix**. The challenge here is to correctly determine the tech-prefix and find out where the actual phone number is, as unfortunately there are no clear rules for this. The default approach is to regard everything to the left of # (including # itself) as the tech-prefix, and all the remaining digits as the phone number. It is also possible to create your own pattern for matching a tech-prefix.
- Use authentication by **CLI / CLD Tech-Prefix and IP**. The default approach here is to use the identity for authentication that consists of everything to the left of the # symbol (including the # symbol) in the CLI / CLD, followed by the remote IP address prefixed with @ (e.g. 977#@122.255.109.2).
- Use authentication by **CLI / CLD**.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

- **CLI (PAI if no CLI)**. The identity for authentication is the phone number of the party calling (CLI). If the CLI is not specified, the identity for authentication contains the value from the PAI header.
- **CLI (RPID if no CLI)**. This method is similar to the previous one, except that the identity for authentication is taken from the RPID header if the CLI is not specified.
- Use authentication by **PAI**.
- Use authentication by **RPID**.
- Use authentication by **CLI (P-Charge-Info)**. When CLI-based authentication is used and the call is forwarded to PortaSIP® for termination, the original caller is charged for the call. In order to charge the forwarder and instead, display an original CLI to the called party, the P-Charge-Info SIP header can be used. This header conveys information about the identity of the party to be charged. If the **P-Charge-Info** SIP header is missing in the authentication request, PortaSIP® will reject the call.
- Use authentication by **Trunk Group ID (tgrp)**. The identity for authentication is the value from the "tgrp" part of the "Contact" header.
- Use authentication by **PCI (P-Charge-Info)**. The identity for authentication is the number from the P-Charge-Info header and the IP address prefixed with @ (e.g. a call from IP address 122.255.109.2 with the P-Charge-Info header <sip:+12349874567@example.com> will be authorized as +12349874567@122.255.109.2).
- **Remote IP**. The identity for authentication is an IP address taken from a custom *Remoteip* SIP header. Note that this IP address is used "as is," without validation.

Call handling rules – auto creation

When you create an account with the ID, which seem to contain an IP address, the system will automatically create a call handling rule to apply IP-based authorization for calls, arriving from this IP address – so you do not have to perform this extra step. Also when you create a VoIP from vendor connection without assigning a vendor account to IP (so authentication by IP address is assumed), a call handling rule will be automatically created for you.

These auto-created rules are displayed on separate tabs in **the Call Handling** screen, so you can easily distinguish them from the rules, created by administrators.

Please consult the *Call Handling* section in the **PortaBilling Web Reference Guide** for more details.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

Precedence of rules displayed on separate tabs

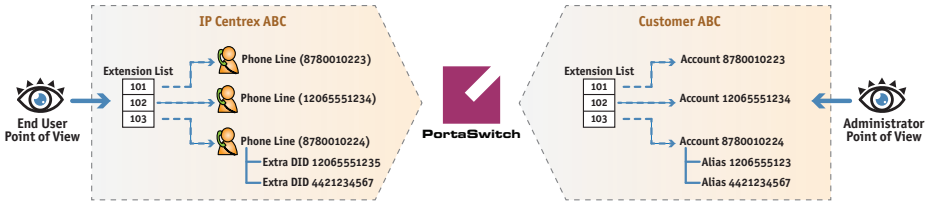
The precedence of rules displayed on separate tabs is the following:

1. First, PortaSIP® searches for a **manually specified** rule that matches the remote IP address.
2. If no matching rule is found, PortaSIP® searches for an **autogenerated rule for accounts** that match the remote IP address.
3. If the previous two searches haven't provided any matching rules, then PortaSIP® searches for an **autogenerated rule for connections** that match the remote IP address.
4. If no matching rule is found up until now, then PortaSIP® searches for an **autogenerated rule for nodes** that match the remote IP address.
5. If PortaSIP® still hasn't found a rule, digest authentication will be applied.

   So when PortaSIP® finds the first matching rule (providing the required identity for authentication has been obtained from the INVITE request), it passes the part used for authentication to PortaBilling® in the User-Name attribute and waits for a response.

IP Centrex Concepts

Users of the hosted PBX or IP Centrex service normally employ a dedicated vocabulary and operate with a very specific set of concepts, such as "extension", "huntgroup" or "phone line". The following table explains the mapping between IP Centrex elements and PortaBilling® entities.



© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

IP PBX Concept or Entity	Entity in PortaBilling	Description
Hosted IP PBX (also hosted IP PBX tenant) or IP Centrex Environment	Customer	A customer object in PortaBilling® represents a company or an individual who uses services on one or more phone lines. The customer pays for all the usage. Each customer has his own individual configuration for the hosted IP PBX service; e.g. a customer can have his own dialing plan, or use any extension number (even if another customer already uses the same extension).
Phone line	Account	A phone line represents the actual IP phone (or an individual line on a multi-line IP phone).
Phone number	Account ID	An account ID is the unique identifier of a phone line across the whole network (not just an individual IP Centrex environment), and so contains the phone number allocated to this phone line.
DID	Alias / Account	DID is a phone number which allows a phone line to be reached directly. Thus you can either add that number as an alias to an existing account, or create a new account and assign this phone number as an account ID.
Extension	Extension	A short dialing code assigned to a particular phone line. An extension only exists in the context of a specific IP Centrex environment; e.g. any user in your organization can use the extension 101 to reach you, but if another customer (even one using the same PortaSwitch system) dials 101 – nothing happens.
Extension list	A table with mapping between extensions and accounts	Defined in the customer information.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

Huntgroup	Huntgroup	A way of distributing an incoming call to multiple extensions according to predefined rules. Each huntgroup has its own dialing code (e.g. 301).
Main line (main phone number)	Account, the main phone number is assigned to this account as an account ID	This account is either provisioned on the secretary's phone (so he/she can answer all incoming calls) or has auto attendant configured, so that incoming calls are automatically forwarded to the Media Server IVR, where the auto attendant is launched.

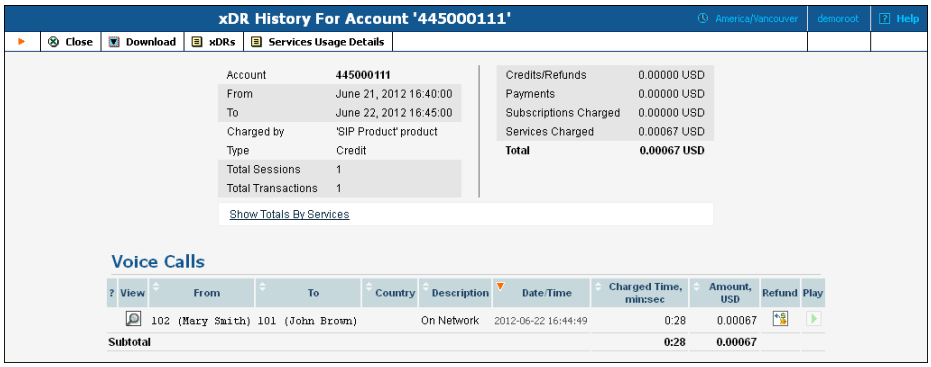
Intra-Centrex Call Presentation

Since people normally use short extension codes to dial their colleagues, these are the numbers that they remember well. So for calls within the same IP Centrex environment, extension numbers should be visible in the call history. On the other hand, if a call is forwarded outside the IP Centrex, the full phone number should be presented. Therefore, call detail presentation is done differently based on context. Let's look at several use cases.

A call between two extensions

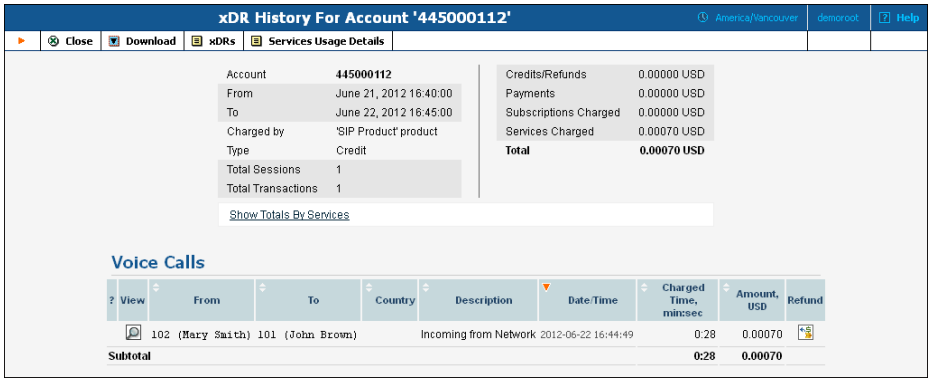
Mary Smith (extension 102) dials 101 to reach her colleague John Brown. When she (or the customer, or the administrator of the IP Centrex environment) sees the CDR, it says:

CLI	CLD
102 (Mary Smith)	101 (John Brown)



The same information is displayed in the incoming CDRs for this call (those viewed by John Brown).

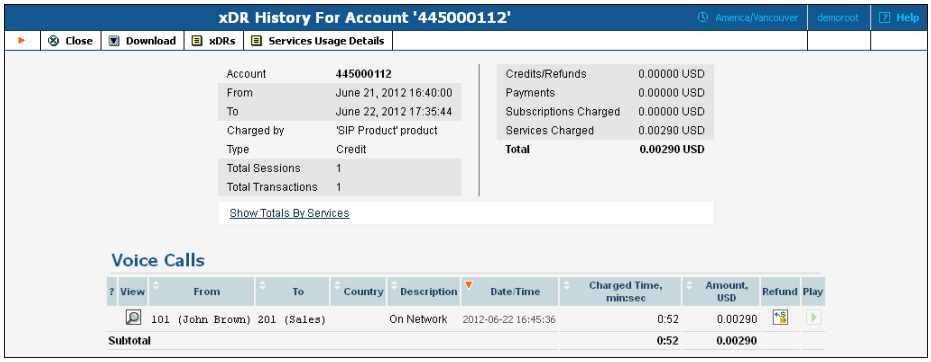
© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com



Calling a huntgroup

John Brown (101) dials 201 (huntgroup) to reach Sales. The CDR then shows the huntgroup number as the CLD:

CLI	CLD
101(John Brown)	201 (Sales)

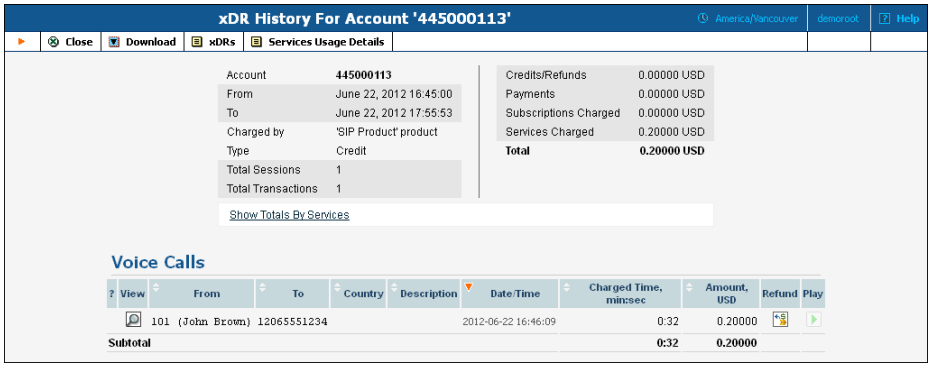


Using abbreviated dialing for an external number

John Brown (101) dials 401 (abbreviated dialing) to reach his partner (12065551234). The displayed CLD contains the latter's full number, as the callee is outside the Centrex environment:

CLI	CLD
101(John Brown)	12065551234

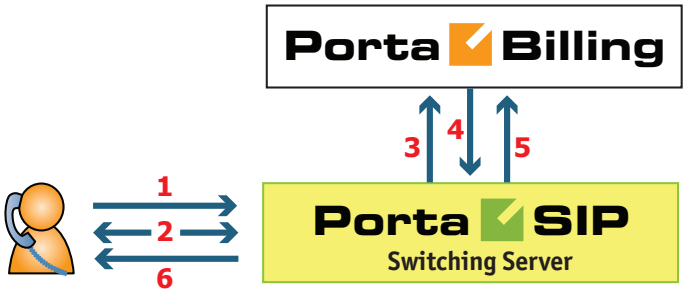
© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com



Call Process / Supported Services

SIP Registration Process

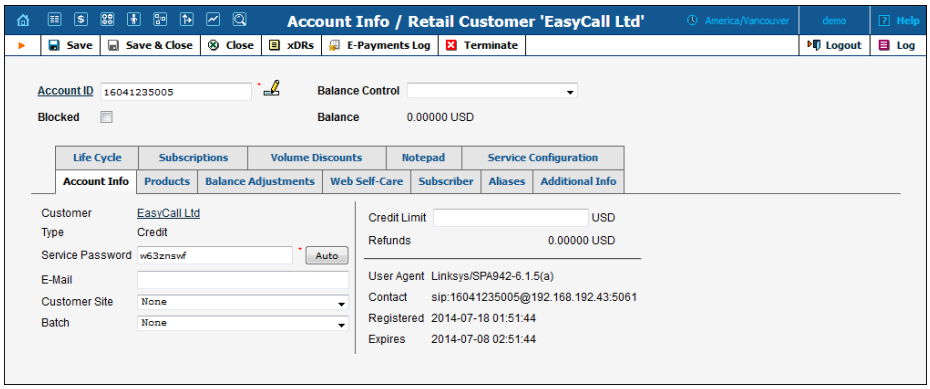
Below is a brief description of the steps followed when an IP phone reaches the Switching Server (hereinafter referred to as SIP server) and attempts to register:



- The SIP server receives a registration request from the IP phone (1).
- The SIP server sends a challenge to the IP phone (this is done instead of having the phone send a password over the Internet) (2).
- The IP phone sends a reply, including a response to the challenge as calculated by the IP phone. The SIP server forwards the received information to PortaBilling® (3).
- PortaBilling® verifies the account information to see whether service is allowed for this account and whether the supplied password is correct, and returns the result to the SIP server (4).
- The SIP server checks if the IP phone is behind a NAT and enters the information in the database of IP phone registrations (5).
- The SIP server sends confirmation to the IP phone that it has been registered (6).

Now you can see the account as registered on the PortaBilling® web interface.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com



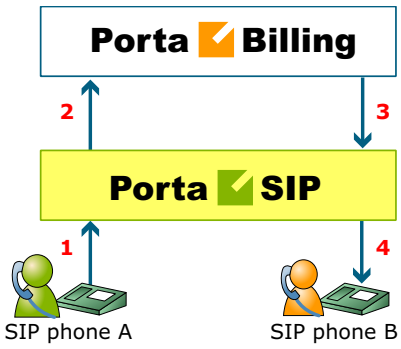
Please note: If PortaBilling® denies account registration (due to wrong account information, a blocked account, etc.), the IP phone will still be informed that it is registered (SIP response code 200) although in reality it is not, and the phone will not be able to use the service. On the first call attempt the user will be informed of the actual state of their account via the Media Server.

SIP UA to SIP UA

An example:

A customer purchases your VoIP services, and two of his employees, A and B, are assigned SIP phone numbers 12027810003 and 12027810009, respectively.
For convenience, the administrator creates two abbreviated dialing rules: 120 for 12027810003 and 121 for 12027810009. Also, he sets up standard US dialing rules, so that users can dial local numbers in the 202 area code by just dialing a 7-digit phone number.

When the called party is online



This is the simplest case:

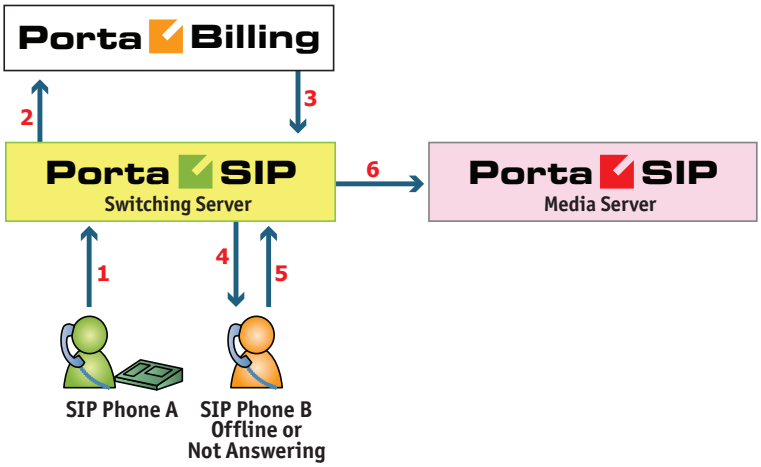
- User A dials user B's number (121). His SIP user agent sends an INVITE request to the Switching Server (hereinafter referred to as SIP server) (1).

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

- The SIP server sends an authorization request to the billing engine (2).
- The billing engine performs several operations:
  - Checks that such an account exists, that it is not blocked / expired, that the supplied password is correct, that the account is allowed to use SIP services, etc.
  - Performs a dialed number translation according to the customer dialing rules or abbreviated dialing table (121 is converted to 12027810009).
  - Checks if A is actually allowed to call that number and what is the maximum allowed call duration.
  - Checks whether the number dialed is one of our SIP accounts, and if it is currently registered.
  - Based on the results of the above operations, the billing engine sends an authorization response to the SIP server (3).

- The SIP server checks its registration database to find the actual contact address of the SIP user agent with that number.
- The SIP server checks the NAT status of both SIP phones.
- The SIP server sends an INVITE to the SIP user agent for user B (4).
- If one of the SIP phones is behind a NAT, the SIP server will be instructed by the billing engine to send a voice stream via the RTP proxy. Otherwise, the SIP server may allow A and B's user agents to talk directly to each other.
- When the call is finished, the SIP server sends accounting information to the billing engine.

The called party is not online



© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

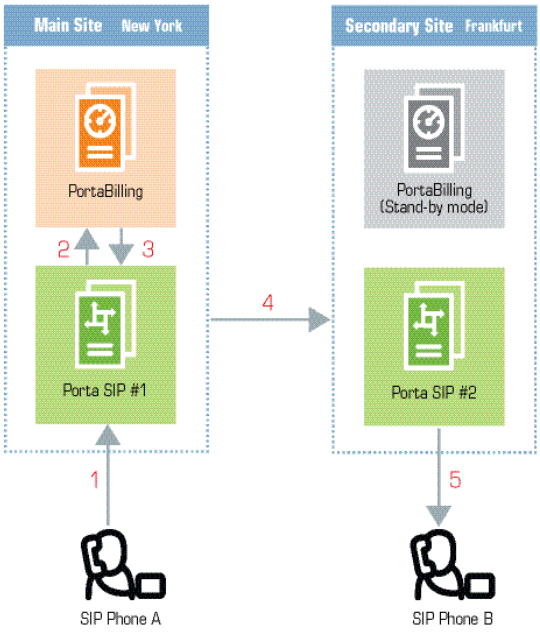
- User A dials 121 in an attempt to reach user B. His SIP user agent sends an INVITE request to the Switching Server (hereinafter referred to as SIP server) (1).
- The SIP server performs authorization in the billing engine (2). The billing engine will perform number translation and determine whether the destination number is actually an account.
- The billing engine checks the registration database, but finds that this account is not online at the moment. If B has unified messaging services enabled, the billing engine will return routing (3) for this call, which will be sent to the Media Server. Thus A will be redirected to a voicemail system, and can leave a message for B (6). The same thing would happen if B were online, but not answering his phone (4), (5).
- In any other case, the call will fail.

Call between multiple PortaSIP® clusters

The multi-site PortaSIP® cluster solution enables you to use PortaSIP® from each site for improved reliability and / or better network utilization.

Let's assume you have two geographically separate sites, each with its own PortaSIP® cluster. The main one is in New York and the secondary one is in Frankfurt. The Frankfurt site serves most of your European customers (i.e. they connect to it via the fast intra-European IP backbone) and acts as a backup for all other users around the world. Thus, the SIP phone seeks to register there if the New York site is down or for some reason, inaccessible.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

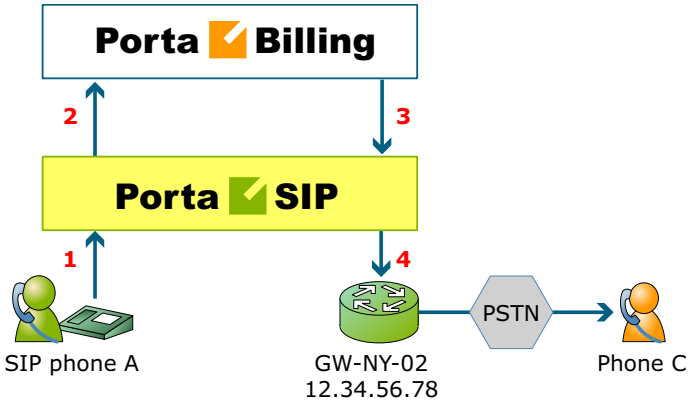


In the example above, user A (assigned SIP phone number 12027810003 and registered to PortaSIP® in New York) calls user B who has phone number 4981234567, currently registered to PortaSIP® in Frankfurt.

- A dials B's number (4981234567). His SIP user agent sends an INVITE request to PortaSIP #1 (**1**).
- PortaSIP #1 sends an authorization request to the billing engine (**2**).
- After all the usual authorization checks, the billing engine determines that the dialed number is one of our SIP accounts and passes this information to PortaSIP #1 (**3**).
- PortaSIP #1 searches for the account having the dialed number as its ID. This account is currently registered to PortaSIP #2, therefore PortaSIP #1 sends an INVITE request to PortaSIP #2 (**4**).
- PortaSIP #2 sends an INVITE request to the SIP phone (**5**).

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

SIP UA to PSTN

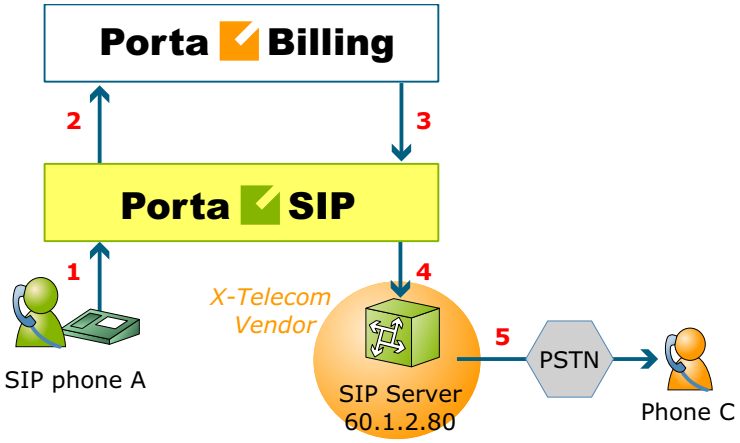


- User A attempts to call his co-worker, user C. C has not been assigned a SIP phone yet, thus he only has a normal PSTN phone number from the 202 area code, and A dials 3001234. A's SIP user agent sends an INVITE request to the Switching Server (hereinafter referred to as SIP server) (1).
- The SIP server sends an authorization request to the billing engine (2).
- Billing performs several operations:
    - Checks that such an account exists, that it is not blocked / expired, that the supplied password is correct, that the account is allowed to use SIP services, etc.
    - Performs a dialed number translation according to the customer dialing rules or abbreviated dialing table (so 3001234 will be converted into 12023001234).
    - Checks if A is actually allowed to call that number, and what is the maximum allowed call duration.
    - Discovers that the destination number is off-net.
    - Computes the routing for this call to the external vendors according to their cost and preferences and the customer's routing plan.

- Based on the results of the above operations, billing sends an authorization response to the SIP server (3).
- The SIP server tries to send a call to all routes returned by the billing engine sequentially, until either a connection is made or the list of routes is exhausted (4).
- When the call is finished, the SIP server sends accounting information to the billing engine.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

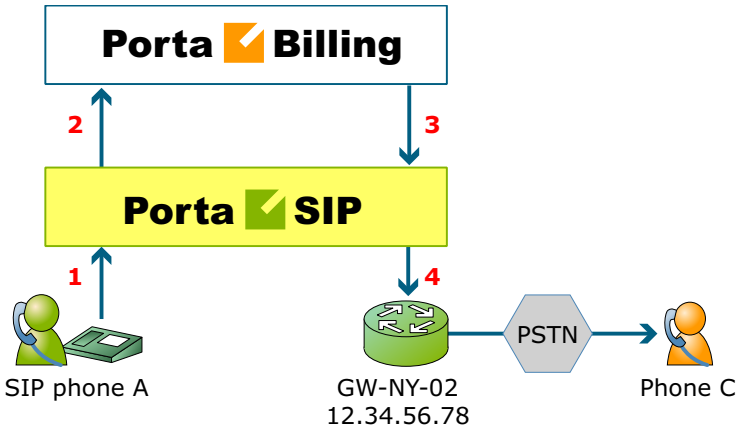
Terminating SIP calls to a vendor using VoIP



- An example: we are able to terminate calls to the US and Canada to a vendor, X-Telecom. This would then be described as a **VoIP to vendor** connection in the billing engine, with the remote address being the address of the vendor's SIP server (or SIP-enabled gateway).
- The billing engine returns the IP address of the vendor's SIP server in the route information, with login / password optional. The PortaSIP server sends an INVITE request to that address (providing the proper credentials), and then proceeds in basically the same way as if it were communicating directly with C's SIP user agent.
- After the call is established, the B2BUA starts the call timer, disconnecting the call once the maximum call duration is exceeded.
- After the call is completed, the B2BUA sends accounting information for the call to the billing engine.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

Terminating SIP calls to a vendor using telephony



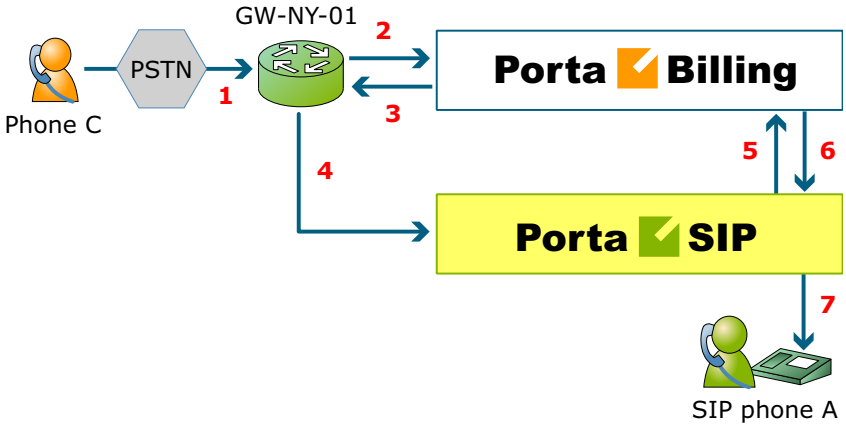
- Let's assume that T1 is connected to Qwest on our gateway **GW-NY-02** in New York, where we are able to terminate calls to the US. This connection would be described as a **PSTN to vendor** connection. The PortaSIP server obtains the address of the GW-NY-02 gateway in the route information.
- The B2BUA sends an INVITE to the remote gateway (GW-NY-02).
- GW-NY-02 performs authentication on the incoming call via the remote IP address. Even if the call was actually originated by A (a dynamic IP address), but the INVITE request to GW-NY-02 arrived from the PortaSIP server, the PortaSIP's IP address will be authenticated. Since PortaSIP is defined as our node, authentication will be successful.

NOTE: Remote IP authentication on the gateway is not required in this case, but is highly recommended. Otherwise, someone else might try to send calls directly to the gateway, bypassing authentication and making such calls for free.

- The call will be routed to the PSTN on the gateway.
- After the call is established, the B2BUA starts the call timer, disconnecting the call once the maximum call duration is exceeded.
- After the call is completed, the B2BUA sends accounting information for the two VoIP call legs to the billing engine. The gateway will also send accounting information about the answer/VoIP and originate/Telephony call legs. The billing engine will combine this information, since accounting from the SIP server allows us to identify who made the call, while accounting from the gateway carries other useful information – for example, through which telephony port the call was terminated.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

PSTN to SIP



This is another important aspect of SIP telephony. Your subscribers not only want to make outgoing calls, they also want other people to be able to call them on their SIP, regardless of where they are at the moment. In order to do so, you will need to obtain a range of phone numbers from your telecom operator, and make sure that calls made to these numbers on the PSTN network are routed to your gateway via the telephony interface.

- C wishes to call A. He thus dials A's phone number (since C is in the US, he dials it using the North American format, 2027810003).
- This call is routed through the telecom network to gateway GW-NY-01. When the incoming call arrives on the gateway (1), it starts a special TCL application PSTN2SIP to handle this call. This application does several things:
    - Converts the phone number to the E.164 format, so that 2027810003 become 12027810003.
    - Performs authorization in the billing engine (2) – whether A is allowed to receive incoming telephony calls from GW-NY-01, and, if you charge for incoming calls, what is the maximum call time allowed, based on A's current balance (3). One important point is that authorization should happen without a password check, since the application does not know the valid password for the SIP account.
    - Starts outgoing call to 12027810003.
    - Starts the timer once the call is established, disconnecting the call when the maximum call duration is exceeded.
    - The gateway is configured such that it knows that calls to 1202781…. numbers should be sent to the PortaSIP server, thus it sends an INVITE to PortaSIP (4).

NOTE: The gateway cannot make this call "on behalf" of A, since even if we know A's account ID, we do not know A's password; therefore, such a call will be rejected. In addition, Cisco gateways currently do not support INVITE with authorization.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

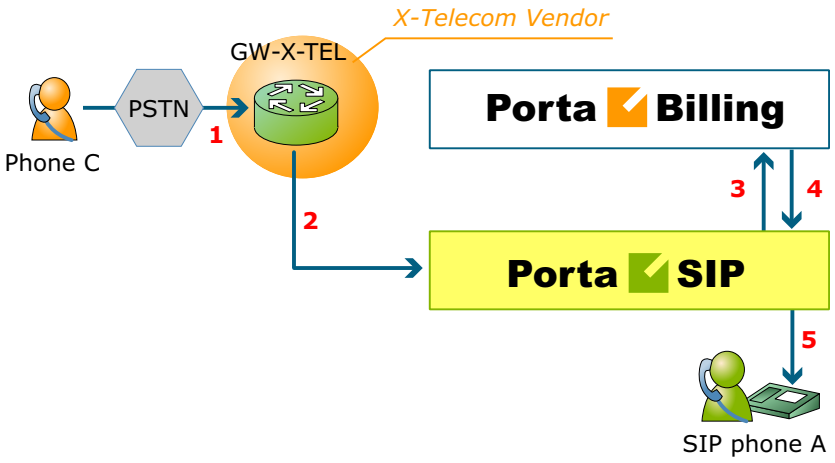
- PortaSIP receives the INVITE, but without authorization information. So the PortaSIP server performs authentication based on the IP address (5), (6). Since this call is made from our trusted node – gateway GW-NY-01 – the call is authorized.
- PortaSIP checks if the SIP user agent of the dialed number (12027810003) is registered at the time. If yes, a call setup request is sent (7).
- If the dialed number belongs to an SIP account with unified messaging services enabled, but this account is not online at the moment or does not answer, the call will be redirected to a voicemail system.
- After the call is completed, the B2BUA sends accounting information for the two VoIP call legs to the billing engine. The gateway will also send accounting information about the answer/Telephony and originate/VoIP call legs. The billing engine will combine this information, since accounting from the SIP server allows us to recognize that the call was terminated directly to the SIP user agent, and not to a vendor, while accounting from the gateway will contain information as to which account should be billed for this call.

PSTN to SIP (via VoIP DID Provider)

In the previous section we discussed traditional PSTN to SIP service, when a call is delivered to your gateway via E1/T1 lines and then forwarded to a SIP phone. This service scheme assumes direct interconnection with the telco that owns DID numbers.

Establishing such direct interconnections with every telco from which you would like to get phone numbers can be problematic (e.g. if you want to give your customers the ability to choose a phone number from any European country, you will need many gateways in different places). Fortunately, however, there are more and more companies which offer incoming DID service, i.e. they already have an interconnection with a specific telecom operator, and so can forward incoming calls on these numbers to you via IP. Thus no extra investment is required to provide phone numbers from a certain country or area, except signing a contract with such a “DID consolidator”.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com



- C wishes to call A on his German phone number. He thus dials A's phone number (since C is in the US, he dials it using the North American format, 0114929876543).
- The call is routed through the telecom network to the gateway of DID consolidator X-Telecom (1).
- X-Telecom in turn forwards this call to your PortaSIP server (2).
- PortaSIP receives an incoming VoIP call and sends an authorization request to the billing engine (3).
- The billing engine detects that this call is coming via a "VoIP from Vendor" connection, so it initiates a special authorization for this call: the call will be billed to the account which receives it. Thus the maximum call time duration is calculated based on A's current balance.
- In the authorization response, PortaSIP is instructed to send the call to A's SIP phone 12027810003 (4).
- PortaSIP sends a call setup request to the SIP phone (5).
- If the dialed number belongs to a SIP account with unified messaging services enabled, and the account is not online at the moment or does not answer, the call will be redirected to a voicemail system.

After the call is completed, A is charged for it; also, costs are calculated for the incoming call according to the tariff associated with X-Telecom's "VoIP from Vendor" connection.

Video Calls via SIP

Video calls, from PortaSIP perspective, are very similar in flow to the conventional (voice only) calls described in the *Call Process / Supported Services* section of this guide). In video calls, however, there are multiple RTP streams: for audio and video.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

SIP signaling flows between end-point and PortaSIP (and PortaSIP performs call validation using PortaBilling® via RADIUS protocol) – in exactly the same manner as it does for voice calls. This allows to control the authorization, authentication, and call flow in accordance with the settings and balance of the account.

Just like a voice call, the RTP streams can go directly from one video end-point to another or be mediated by RTP proxy, if necessary (for instance both end-points are on separate private networks behind NAT).
The main considerations for providing video call service are the following:

- End-points (IP video phones or communication clients) involved need to support video calls (some supported models are Hardware phones: Polycom VVX 1500, Grandstream GXV3140, Grandstream GXV3175; Softphones: eyeBeam, X-Lite, Ekiga).
- In case the call goes to or from PSTN, the gateway should be able to process video calls, too.
- Due to the much higher required bandwidth usually it is advisable to provide video calls only to clients on public IPs, so the RTP streams can be connected directly and no proxying on PortaSIP side is required.

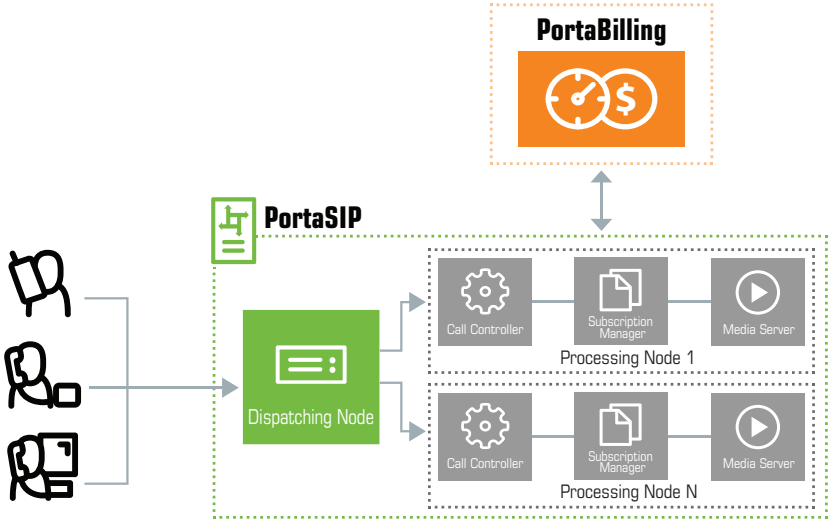
NOTE: The Call Recording functionality is not available for video calls.

Presence

PortaSIP enables IP Telephony Service Providers to deliver a presence service that allows users to monitor each other's availability and make decisions about communicating. Presence information is highly dynamic, and generally indicates whether a user is online or offline, busy or idle, away from or close to a communication device, etc. Having real-time information about presence lets you increase the effectiveness of your communication and enjoy greater flexibility when setting up short-term meetings and conference calls. In other words, it can save you time and money. Today, nearly all VoIP multimedia clients, such as eyeBeam, x-Lite and MS Messenger, support presence services.

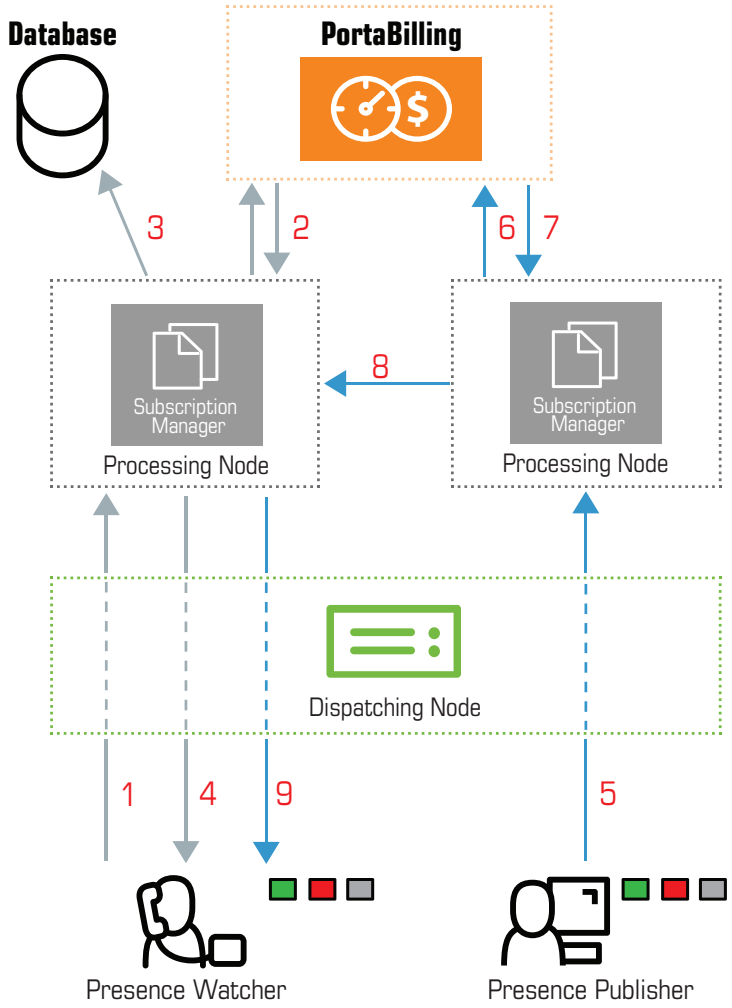
Presence requests are handled using the subscription manager. As it is part of the PortaSIP® cluster processing node, it communicates both with SIP user agents and with the cluster components, and maintains online information for all users registered within your network. It allows SIP user agents to publish subscribe requests and respond to them, and generate notifications of changes in presence status.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com



Typically, the whole process functions in the publish / subscribe manner. Presence information is published from a certain source, e.g. mobile phones, laptop computers, PDAs, desktop PCs, or even other application servers. The subscription manager processes the presence information to form a complete overview of each user's presence. It also resends the user's presence to all other subscription managers within the cluster. The combined presence data is sent to all watchers who have subscribed to the presence service for the given user.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com



- The SIP user agent sends a SUBSCRIBE request to the dispatching node which forwards it to one of the available subscription managers (**1**);
- The subscription manager authorizes the user's account in PortaBilling® (**2**), and records the subscription in the database (**3**).
- Based on the authorization results, the subscription manager sends a response (a 200 OK SIP response) via the dispatching node back to the SIP user agent (**4**).
- The user agent (publisher) sends a PUBLISH request (e.g. when the user is dialing a number) to the dispatching node which forwards it to a currently available subscription manager (**5**).
- The subscription manager sends the authorization request to PortaBilling® (**6**).
- When authorized successfully (**7**), the subscription manager re-sends the PUBLISH request to all the other subscription managers within the PortaSIP® cluster (**8**).

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

- The subscription managers identify the SIP user agents (watchers) who subscribe to the presence for the given user and send NOTIFY requests to the dispatching node, which then forwards the NOTIFY requests to the respective SIP user agents (9).

Busy Lamp Field (BLF)

PortaSwitch® supports the highly popular IP Centrex feature that extends PortaSIP's capability to work with popular models of IP business phones (e.g. Polycom). The BLF service monitors the status (idle, busy, etc.) of individual phone lines in the IP Centrex environment and shows it on the attendant phone console. The status of phone extensions is shown in real time, enabling you to decide whether an incoming call can be forwarded to one of them or not.

As is evident from the name of this feature, phones that can use BLF have a field of lamps. Each lamp reflects the status of a phone line. The behavior and color of the lamps differs from model to model, but the most popular and intuitively perceived ones are the following: 'off' for non-subscribed, 'green' for idle, 'blinking' for ringing and 'red' for busy. In some models, the lamps are combined with buttons that allow you to perform further actions (attended / unattended call forwarding, conferencing, etc.).

Requirements and Configuration

The BLF feature is implemented through the SIP protocol and uses SUBSCRIBE and NOTIFY requests. BLF feature support is embedded in the PortaSIP® cluster, therefore no additional configuration is required.

On the UA side, it is necessary for the phone to be subscribed to notifications regarding particular phone lines (the exact procedures vary from model to model; please refer to the User Guide of the respective phone).

For security purposes, only accounts within the same IP Centrex environment may monitor each other's statuses.

The BLF has been tested and provides full functionality with the following IP phone models:

- Grandstream:
  - Grandstream GXV3275
  - Grandstream GXV3240
  - Grandstream GXP2130
  - Grandstream GXP2140
  - Grandstream GXP2160

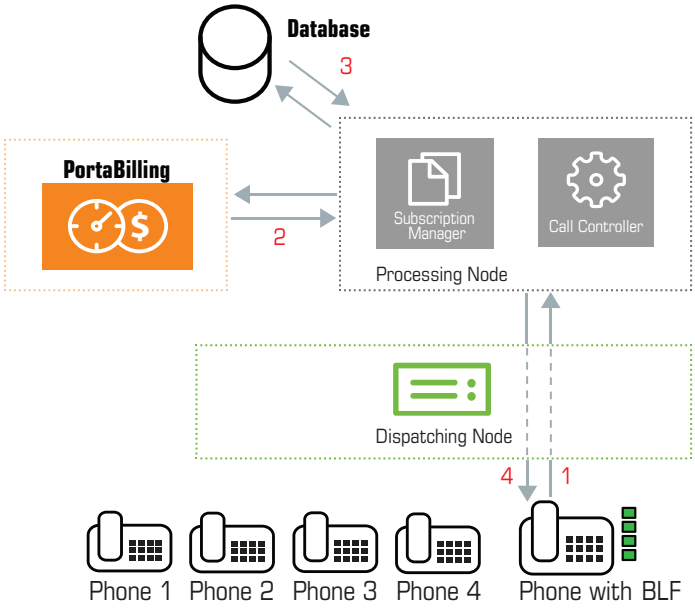
© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

- Polycom:
  - Polycom IP 550
- Yealink:
  - Yealink T21P
  - Yealink T23P
  - Yealink T23G
  - Yealink T27P
  - Yealink T29G
  - Yealink T41P
  - Yealink T48G
  - Yealink SIP-T21P E2 v8x

How It Works

Step 1. Preparation:

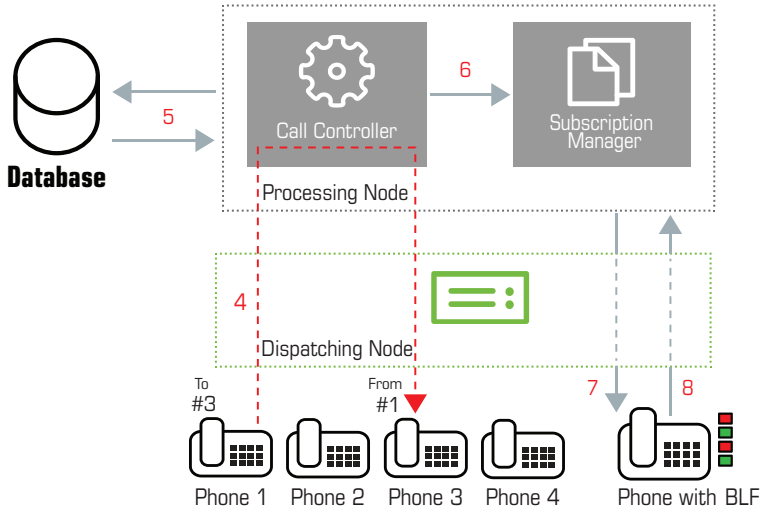
- The SIP user agent sends a SUBSCRIBE request to the dispatching node (1) which forwards it to a currently available subscription manager;
- The subscription manager authorizes it in PortaBilling® (2) and records the subscription in the database (3).
- Based on the results, the subscription manager sends a response (a 200 OK SIP response) via the dispatching node back to the SIP user agent (4).
- The subscription will expire over time and can be periodically renewed by repeating the above procedure.



© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

Step 2. Call Flow:

Any change of status on the extension(s) subscribed to (to idle, ringing, or busy) will be reflected on the Busy Lamp field of the UA. Thus, if Phone 1 calls Phone 3, the call controller establishes the call between the phones (4), checks for the active subscriptions in the database (5), and notifies the subscription manager(s) who handle the presence of these phones (6). The subscription manager updates the statuses of Phones 1 and 3 and sends the NOTIFY request to the UA (7). The NOTIFY request includes XML with dialog-info about the current status of the extension being monitored. The phone acknowledges the NOTIFY request by sending a 200 OK SIP response (8).



Call Recording

Users of IP Centrex services on PortaSwitch can record phone conversations for their extensions, to be played back later.

When the call recording feature is activated for a phone line, PortaSIP will write a copy of the RTP stream for each incoming or outgoing call to a local disk. After that the media stream is passed to a voice conversion server (a dedicated server is required, since voice conversion is a resource-intensive task) where it is transformed into .WAV format, playable on any computer or smart phone. When the conversion is completed (this may take a few minutes), a link for the conversation playback is available on the CDR browser screen.

The process happens as follows:

- Someone dials a phone number, which is assigned to one of your customers. The call is handed over to your network, so it arrives to PortaSIP.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

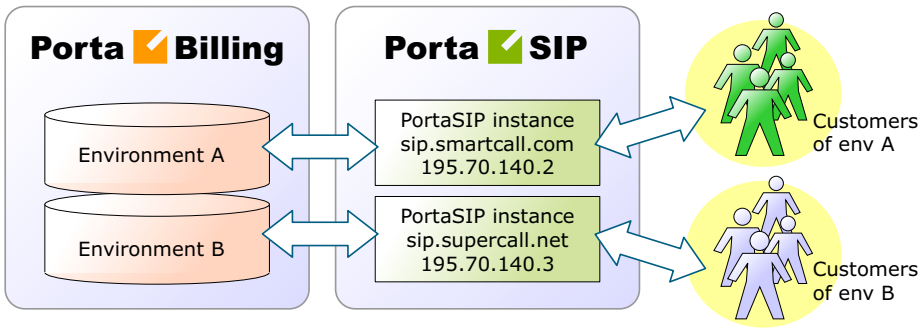
- PortaSIP sends a request to PortaBilling® to obtain call authorization and routing.
- PortaBilling® finds out that the account that is supposed to receive the call has the **Call Recording** feature activated.
- PortaSIP is instructed to proxy the media stream for this call (overriding the **RTP Proxying** policy for the incoming DID vendor) and store a copy of it in a local file.
- After the call is disconnected, the file is transported to the conversion server and the conversion starts.
- When the conversion process is finished, the CDR information about this call is updated in PortaBilling®, and a "Play" link appears in the CDR browser.
- User clicks on the link and his browser is redirected to download the converted .WAV file from the conversion server.

Important notes

- The RTP stream must pass via the PortaSIP® server in order for the PortaSIP® server to record it – so please allocate a sufficient amount of bandwidth for PortaSIP to process these calls without degenerating in sound quality.
- A system can only convert the call if it recognizes the codec used to transport the voice. To ensure that conversations are recorded properly, IP phones must be equipped to use a g729, g723 or g711 codec.
- Call records take up disk space – be prepared for this. In order to store 15 hours of recorded conversations, 1GB of disk space is required.

Virtual SIP Servers

On a single PortaSIP® installation (one physical switching server, one license) you can run multiple virtual PortaSIP® instances, each of them a separate server that can be used in a PortaBilling® virtual environment. The only thing required to create a new SIP instance on the PortaSIP® server side is an extra IP address (IP alias) allocated to that server.



© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

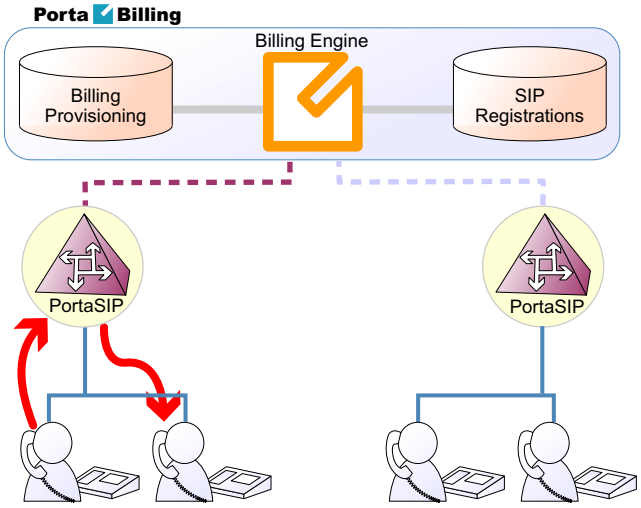
Every virtual SIP server acts as an independent PortaSIP installation.

PortaSIP instances are managed from the web interface of the PortaSwitch configuration server. You can create a new instance, change parameters, move the instance from one physical server to another, and so on.

Call Flow with multiple PortaSIP servers

SIP UA to SIP UA

Case A: Both SIP phones are registered to the same PortaSIP server



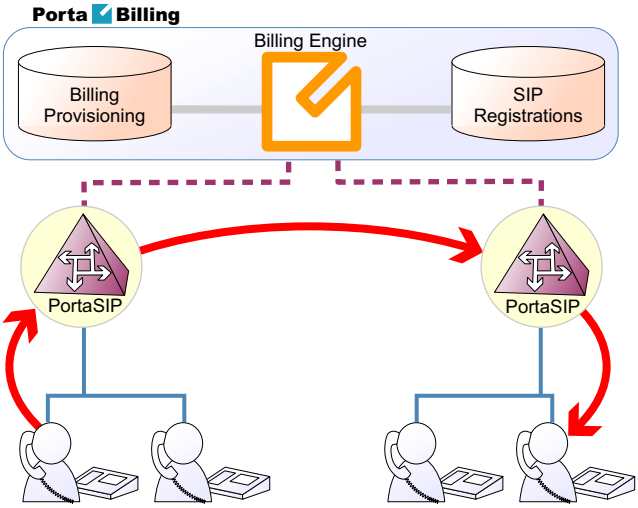
In this case, the call flow is exactly the same as in a situation where only one PortaSIP server is available (discussed earlier in the *SIP UA to SIP UA* section).

- PortaSIP receives an incoming call and requests authorization and routing from PortaBilling®.
- PortaBilling® verifies whether this call should be allowed, and if the destination is one of our SIP accounts.
- PortaBilling® checks the registration database, and returns the address of the PortaSIP server the account is currently registered to in the routing information.
- PortaSIP receives its own address as the route, and sends a call to the SIP phone.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

Case B: SIP phones registered to different PortaSIP servers

In this case, routing information from PortaBilling® will contain the address of the second PortaSIP server (i.e. the one to which the called SIP phone is registered). Thus the first PortaSIP server will send a call there, and then the second PortaSIP server will send the call to the SIP phone.



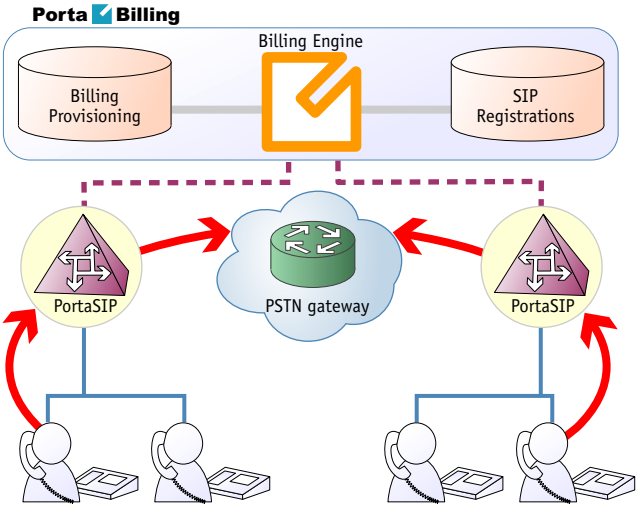
It may be asked why the first (originating) PortaSIP server does not send the call directly to the called SIP phone (since the registration database contains its contact IP:port information)? The answer is that, if the called SIP phone is behind a NAT (and most Internet users are behind a NAT these days), only the server on which the SIP phone has opened a connection can send back a reply – and this is the second PortaSIP server.

Note that, although SIP signaling will travel via both SIP servers, this is not the case with RTP (voice) traffic. Depending on the NAT context of the call and the RTP proxy configuration, PortaSwitch may either connect the RTP stream between the phones directly, or use the RTP proxy on *one* of the SIP servers. So even if two SIP servers are involved in this call, this does not affect call quality, since the RTP stream follows the standard path: SIP phone1 -> SIP server -> SIP phone2.

SIP UA to PSTN

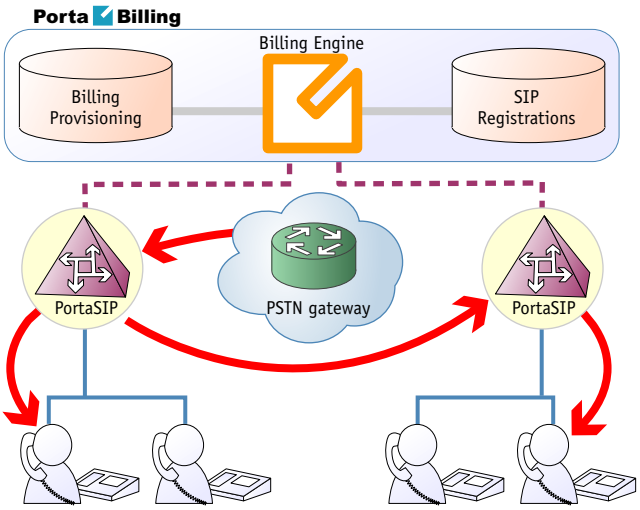
When a SIP phone user makes a call to an off-net destination, only one PortaSIP server and PortaBilling® are involved in the call flow. So this works in exactly the same way as described earlier for SIP to PSTN calls in the case of a single PortaSIP server.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com



PSTN to SIP UA

Again, the call flow is extremely similar to the usual PSTN->SIP call flow. The gateway delivers a call to a PortaSIP server, which then sends the call to the SIP phone.



Understanding SIP Call Routing

When the PortaSIP server has to establish an outgoing call, it must find out where the call is being sent to. To do this, it will ask billing for a list of possible routes. In this case the routing configuration is in one central location, and billing can use information about termination costs, quality or other parameters to choose the best route (least-cost routing, quality-based routing, profit-guarantee, individual routing plans, etc.).

When a call goes through the PortaSIP server, the SIP server may:

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

- Direct the call to one of the registered SIP clients, if the called number belongs to the registered agent.
- Optionally, direct the call to the voicemail box (the Media Server required) if the called number belongs to an account in PortaBilling®, but this account is not currently registered to the SIP server (is offline).
- Route the call to one of the gateways for termination, according to the routing rules specified in PortaBilling®.

Please consult **PortaBilling Administrator Guide** for more information about various routing parameters and methods.

NAT Traversal Guidelines

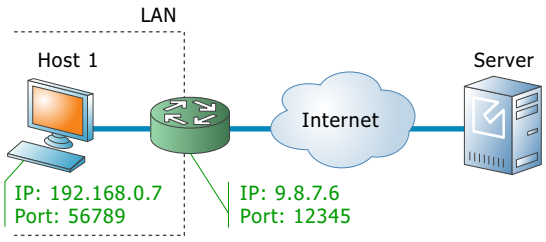
NAT Overview

The purpose of NAT (Network Address Translation) is to allow multiple hosts on a private LAN not directly reachable from a WAN to send information to and receive it from hosts on the WAN. This is done with the help of the NAT server, which is connected to the WAN by one interface with a public IP address, and to the LAN by another interface with a private address. This document describes issues connected with the implementation of NAT and its implications for the operation of PortaSIP, with an overview of some fundamental NAT concepts.

The NAT server acts as a router for hosts on the LAN. When an IP packet addressed to a host on the WAN comes from a host on the LAN, the NAT server replaces the private IP address in the packet with the public IP address of its WAN interface and sends the packet on to its destination. The NAT server also performs in-memory mapping between the public WAN address the packet was sent to and the private LAN address it was received from, so that when the reply comes, it can carry out a reverse translation (i.e. replace the public destination address of the packet with the private one and forward it to the destination on the LAN).

Since the NAT server can potentially map multiple private addresses into a single public one, it is possible that a TCP or UDP packet originally sent from, for example, port A of the host on the private LAN will then, after being processed in the translation, be sent from a completely different port B of the NAT's WAN interface. The following figure illustrates this: here "HOST 1" is a host on a private network with private IP address `192.168.0.7`; "NAT" is the NAT server connected to the WAN via an interface with public IP address `9.8.7.6`; and "Server" is the host on the WAN with which "HOST 1" communicates.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com



A problem relating to the SIP User Agent (UA) arises when the UA is situated behind a NAT server. When establishing a multimedia session, the NAT server sends UDP information indicating which port it should use to send a media stream to the remote UA. Since there is a NAT server between them, the actual UDP port to which the remote UA should send its RTP stream may differ from the port reported by the UA on a private LAN (`12345` vs. `56789` in the figure above) and there is no reliable way for such a UA to discover this mapping.

However, as was noted above, the packets may not have an altered post-translation port in all cases. If the ports are equal, a multimedia session will be established without difficulty. Unfortunately, there are no formal rules that can be applied to ensure correct operation, but there are some factors which influence mapping. The following are the major factors:

- How the NAT server is implemented internally. Most NAT servers try to preserve the original source port when forwarding, if possible. This is not strictly required, however, and therefore some of them will just use a random source port for outgoing connections.
- Whether or not another session has already been established through the NAT from a different host on the LAN with the same source port. In this case, the NAT server is likely to allocate a random port for sending out packets to the WAN. Please note that the term "already established" is somewhat vague in this context. The NAT server has no way to tell when a UDP session is finished, so generally it uses an inactivity timer, removing the mapping when that timer expires. Again, the actual length of the timeout period is implementation-specific and may vary from vendor to vendor, or even from one version by the same vendor to another.

NAT and SIP

There are two parts to a SIP-based phone call. The first is the signaling (that is, the protocol messages that set up the phone call) and the second is the actual media stream (i.e. the RTP packets that travel directly between the end devices, for example, between client and gateway).

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

SIP signaling

SIP signaling can traverse NAT in a fairly straightforward way, since there is usually one proxy. The first hop from NAT receives the SIP messages from the client (via the NAT), and then returns messages to the same location. The proxy needs to return SIP packets to the same port it received them from, i.e. to the `IP:port` that the packets were sent from (not to any standard SIP port, e.g. 5060). SIP has tags which tell the proxy to do this. The "received" tag tells the proxy to return a packet to a specific IP and the "rport" tag contains the port to return it to. Note that SIP signaling should be able to traverse any type of NAT as long as the proxy returns SIP messages to the NAT from the same source port it received the initial message from. The initial SIP message, sent to the proxy `IP:port`, initiates mapping on the NAT, and the proxy returns packets to the NAT from that same `IP:port`. This is enabled in any NAT scenario.

Registering a client which is behind a NAT requires either a registrar that can save the `IP:port` in its registration information, based on the port and IP that it identifies as the source of the SIP message, or a client that is aware of its external mapped address and port and can insert them into the contact information as the `IP:port` for receiving SIP messages. You should be careful to use a registration interval shorter than the keep-alive time for NAT mapping.

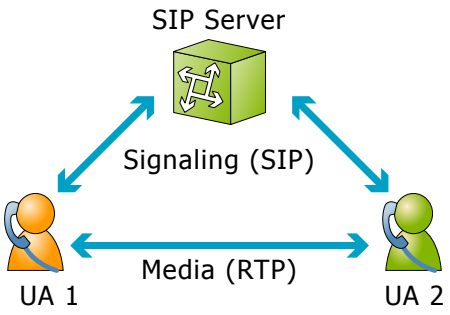
RTP – Media Stream

An RTP that must traverse a NAT cannot be managed as easily as SIP signaling. In the case of RTP, the SIP message body contains the information that the endpoints need in order to communicate directly with each other. This information is contained in the SDP message. The endpoint clients fill in this information according to what they know about themselves. A client sitting behind a NAT knows only its internal `IP:port`, and this is what it enters in the SDP body of the outgoing SIP message. When the destination endpoint wishes to begin sending packets to the originating endpoint, it will use the received SDP information containing the internal `IP:port` of the originating endpoint, and so the packets will never arrive.

Understanding the SIP Server's Role in NAT Traversal

Below is a simplified scheme of a typical SIP call:

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com



It must be understood that SIP signaling messages between two endpoints always pass through a proxy server, while media streams usually flow from one endpoint to another directly. Since the SIP Server is located on a public network, it can identify the real IP addresses of both parties and correct them in the SIP message, if necessary, before sending this message further. Also, the SIP Server can identify the real source ports from which SIP messages arrive, and correct these as well. This allows SIP signaling to flow freely even if one or both UAs participating in a call are on private networks behind NATs.

Unfortunately, due to the fact that an RTP media stream uses a different UDP port, flowing not through the SIP server but directly from one UA to another, there is no such simple and universal NAT traversal solution. There are 3 ways of dealing with this problem:

1. Insert an RTP proxy integrated with the SIP Server into the RTP path. The RTP proxy can then perform the same trick for the media stream as the SIP Server does for signaling: identify the real source IP address / UDP port for each party and use these addresses / ports as targets for RTP, rather than using the private addresses / ports indicated by the UAs. This method helps in all cases where properly configured UAs supporting symmetric media are used. However, it adds another hop in media propagation, thus increasing audio delay and possibly decreasing quality due to greater packet loss.
2. Assume that the NAT will not change the UDP port when resending an RTP stream from its WAN interface, in which case the SIP Server can correct the IP address for the RTP stream in SIP messages. This method is quite unreliable; in some cases it works, while in others it fails.
3. Use “smart” UAs or NAT routers, or a combination of both, which are able to figure out the correct WAN IP address / port for the media by themselves. There are several technologies available for this purpose, such as STUN, UPnP and so on. A detailed description of them lies beyond the scope of this document, but may easily be found on the Internet.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

Which NAT Traversal Method is the Best?

There is no "ideal" solution, since all methods have their own advantages and drawbacks. However, the RTP proxy method is the preferred solution due to the fact that it allows you to provide service **regardless** of the type or configuration of SIP phone and NAT router. Thus you can say to customers: "Take this box, and your IP phone will work anywhere in the world!".

In general, the "smart" method will only work if you are both an ISP and ITSP, and so provide your customers with both DSL / cable routers and SIP phones. In this case, they can only use the service while on your network.

NAT Call Scenarios and Setup Guidelines

With regard to NAT traversal, there are several distinct SIP call scenarios, each of which should be handled differently. These scenarios differ in that, in case 2, the media stream will always pass through one or more NATs, as the endpoints cannot communicate with each other directly, while in cases 1 and 3 it is possible to arrange things so that a media stream flows **directly** from one endpoint to another.

Calls between SIP phones

1. A call is made from one SIP UA (SIP phone) to another SIP UA (SIP phone), with both phones on public IP addresses (outside a NAT). In this case, the phones can communicate directly and no RTP proxying is required.
2. A call is made from one SIP UA (SIP phone) to another SIP UA (SIP phone), and at least one of the phones is on a private network behind a NAT. Here an RTP proxy should be used to prevent "no audio" problems.
3. A call is made from one SIP UA (SIP phone) to another SIP UA (SIP phone), with both phones on the same private network (behind the same NAT). This scenario is likely to be encountered in a corporate environment, where a hosted IP PBX service is provided. In this case, it is beneficial to enable both phones to communicate directly (via their private IP addresses), so that the voice traffic never leaves the LAN.

Calls between SIP phones and remote gateways

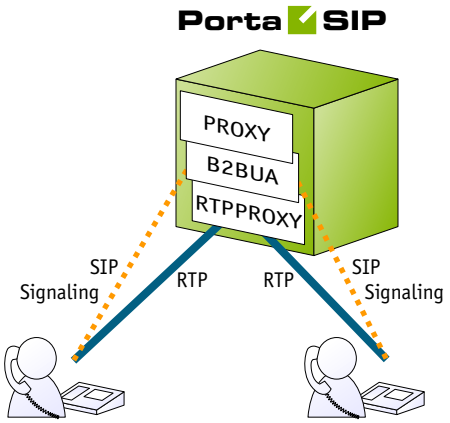
1. A call is made from/to a SIP phone on a public IP address from/to a VoIP GW (a VoIP GW is always assumed to be on a public IP address). In this case, the RTP stream may flow directly between the GW and SIP phone, and no RTP proxying is required.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

2. A call is made from/to a UA under a NAT from/to a VoIP GW, and the remote gateway supports SIP COMEDIA extensions. In this case, the RTP stream may flow directly between the gateway and the SIP phone, and there is no need to use an RTP proxy. However, you need to configure your Cisco GW as per APPENDIX B. Cisco GW Setup for PortaSIP (COMEDIA) in order to ensure proper NAT traversal.
3. A call is made from/to a UA under a NAT from/to a VoIP GW, and the remote gateway does not support SIP COMEDIA extensions. An RTP proxy is required in this case.

RTP Proxy in PortaSIP

This provides an effective NAT traversal solution according to the RTP proxy method described above. The RTP proxy is fully controlled by PortaSIP, and is absolutely transparent to the SIP phone.

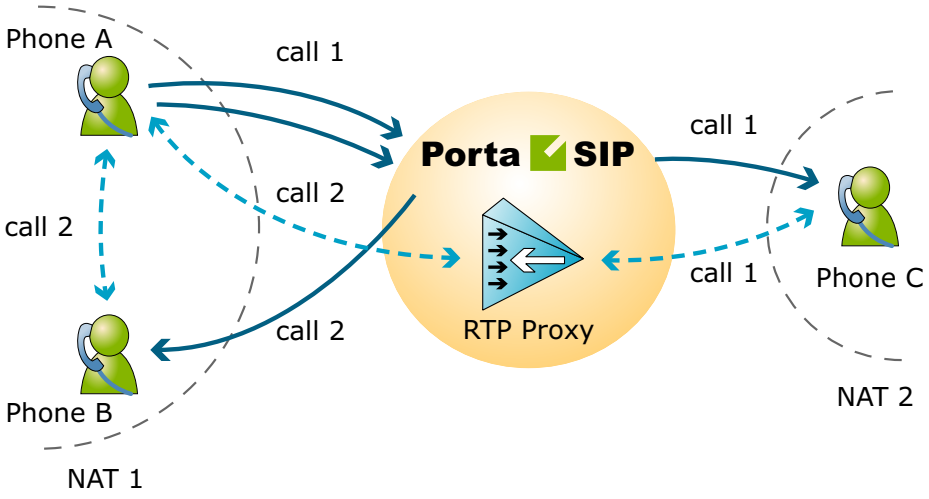


The RTP proxy does not perform any transcoding, and so requires a minimum amount of system resources for call processing. A PortaSIP server doing RTP proxying on an average PC server can support about 750 simultaneous calls.

During the call initiation phase, PortaSwitch® gathers information about the NAT status of both parties (caller and called) participating in the call and decides about RTP proxying.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

Calls between SIP phones



For a SIP phone, the possible conditions are:

- SIP phone on a public IP address.
- SIP phone behind NAT.

Thus, the RTP proxy engagement logic for calls between SIP phones can be summarized as follows:

- If both phones are on public IP addresses, do not use an RTP proxy; rather, allow the media stream to go directly between them.
- If both phones are behind the **same** NAT router, do not use an RTP proxy; rather, allow the media stream to go directly between them.
- Otherwise the RTP proxy is used.

Calls between SIP phones and remote gateways

If the called (or calling) party is a remote gateway or remote SIP proxy, its NAT traversal capabilities are described in the PortaBilling® configuration under connection properties. The possible values are:

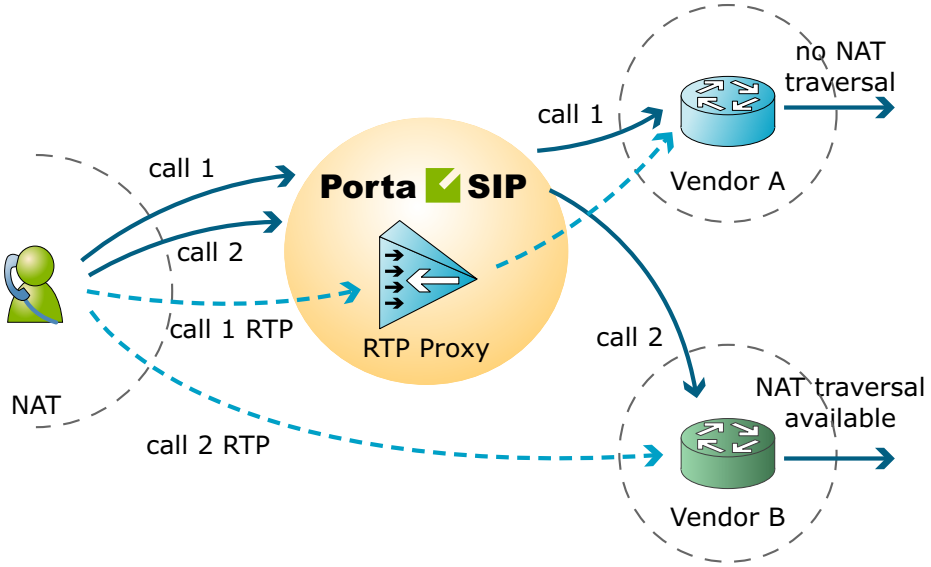
- **Optimal** – This connection supports NAT traversal, so it can communicate with an IP phone behind NAT directly. This is the best possible scenario, since you can entirely avoid using an RTP proxy when exchanging calls with this carrier.
- **OnNat** – This connection does not support NAT traversal. Direct communication with an IP phone is possible only if that phone is on a public IP address.
- **Always** – Regardless of NAT traversal capabilities, you must always use an RTP proxy when communicating with this carrier. This may be necessary if you do not want to allow them to see your customer's real IP address, or perhaps simply because this carrier has a good network connection to your SIP server, but a

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

poor connection to the rest of the world. Thus you will need to proxy his traffic to ensure good call quality.

- **Direct** – Always send a call directly to this gateway, and never engage an RTP proxy.

PortaSIP cannot detect whether a remote gateway supports Comedia extensions (symmetric NAT traversal). If you do not use your own gateway for termination, you should clarify this matter with your vendor and set up the NAT traversal status accordingly.



After the NAT status of the IP phone (behind NAT or on a public IP) and the NAT traversal status of the connection have been identified, a decision is made as follows:

- If the connection has **Always** NAT traversal status, activate the RTP proxy.
- If the connection has **Direct** NAT traversal status, do not activate the RTP proxy.
- If the phone is behind NAT and the connection has **OnNat** status, activate the RTP proxy.
- Otherwise, do not activate the RTP proxy.

In addition to the option of media proxying based on a specific vendor's proxying policy, it is also possible to activate full media proxying for a specific account (phone line) or a specific customer (all accounts under the customer). This can be used to force NAT traversal on the PortaSwitch® side in complex network configurations, or to provide users with an extra level of privacy.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

Auto-provisioning IP Phones

If you provide your VoIP customers with IP phone equipment, you know how laborious and yet important the task of performing initial configuration is. If the equipment is not configured properly, it will not work after being delivered to the customer. Or, even if it works initially, problems will arise if you need to change the IP address of the SIP server. How can you reconfigure thousands of devices that are already on the customer's premises? There are two ways to manage the device configuration.

Manual provisioning

The administrator must login to the device provisioning interface (typically HTTP) and change the required parameters. There are several drawbacks to this method:

- The IP phone must be connected to the Internet when the administrator is performing this operation.
- The administrator must know the device's IP address.
- The IP phone must be on the same LAN as the administrator, or on a public IP address (if the device is behind a NAT / firewall, the administrator will not be able to access it).

Due to these reasons, and since every device must be provisioned individually, this method is acceptable for a testing environment or small-scale service deployment, but totally inappropriate for ITSPs with thousands of IP phones around the world.

Auto-provisioning

This approach is a fundamentally different one. Instead of attempting to contact an IP phone and change its parameters (pop method), the initiative is transferred to the IP phone itself. The device will periodically go to the provisioning server and fetch its configuration file.

IP Phone Provisioning

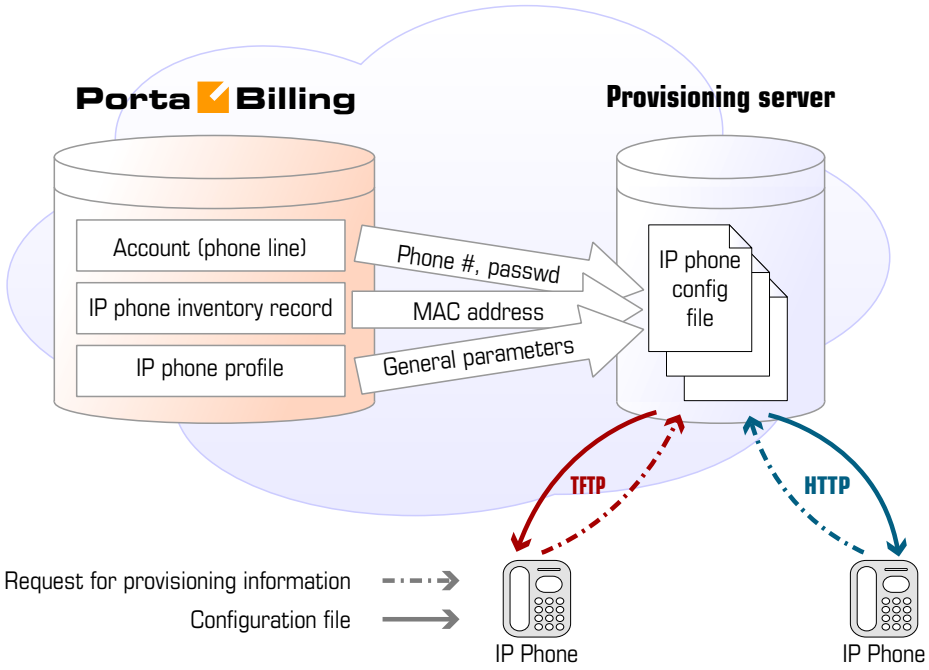
When you use auto-provisioning for an IP phone, instead of entering the same values for codec, server address, and so on into each of a thousand user agents, you can simply create a profile which describes all these parameters. Then PortaBilling® can automatically create a configuration file for the SIP phone and place it on the provisioning server.

The only configuration setting which is required on the IP phone side is the address of the provisioning server, i.e. where it should send a request for its configuration file. When the IP phone connects to the Internet, it

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

will retrieve a specific configuration file for its MAC address from the TFTP or HTTP server and adjust its internal configuration.

If you decide later to change the address of the SIP server, you need only update it once in the profile, and new configuration files will be built for all user agents. Each user agent will then retrieve this file the next time it goes online.



The config file is specific to each user agent, as it contains information such as username and password; thus the user agent must retrieve its own designated config file. The following are defined in the billing configuration:

- The IP phone profile, so that the system knows which generic properties (e.g. preferred codec) to place in the configuration file.
- An entry about the specific IP phone in the CPE inventory (including the device's MAC address), with a specific profile assigned to it.
- The IP phone (or, in the case of a multi-line device, a port on the phone) is assigned to a specific account in the billing.

Auto-provisioning will only work if your IP phone knows the address of your provisioning server. If you buy IP phones retail, you will probably have to change the address of the provisioning server on every phone manually. However, if you place a large enough order with a specific vendor, these settings can be pre-configured by him, so that you may deliver an IP phone directly to the end user without even unwrapping it.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

CPE Inventory

The CPE inventory allows you to keep track of IP devices (SIP phones or adaptors) which are distributed to your customers. The MAC address parameter is essential for every IP phone which is to be automatically provisioned, and so a corresponding entry must be created in the CPE inventory.

PortaSIP and Emergency Services (E911)

One of the most popular types of VoIP services provided by PortaSwitch is the residential telephony service, including a substitute for a traditional PSTN line using a VoIP adaptor. Here the issue of emergency services becomes very important, since customers may not fully switch to a VoIP service provider unless it is resolved. In most countries ITSPs are required to provide emergency services to their customers by the local authorities (e.g. the FCC in the US). Using PortaSwitch, an ITSP can meet all such requirements and start providing residential or business IP telephony services. PortaSwitch offers an FCC-compliant framework for providing E911 services.

There are several components of E911 services:

- Subscriber and subscriber address. The subscriber is the person who is using the telephony service, and his address is his physical location, to which the police / fire department / ambulance should be sent in case of emergency.
- An ITSP is a company providing telephony services to the subscriber.
- PSAP (Public Safety Answering Point) is an agency responsible for answering emergency calls in a specific city or county.
- An E911 provider is the company which delivers emergency calls to the PSAP.

Basically, when a customer dials an emergency number he should be connected to the PSAP which is responsible for his location. The PSAP must immediately obtain the customer's exact address (e.g. including floor number), so that if the customer is incapable of providing his address information an emergency response team may still reach him. How is this done?

E911 service providers

It is virtually impossible for an ITSP to establish a connection with every PSAP in a given country and meet all of their requirements (basically for the same reason why it is impossible for an ITSP to establish a direct interconnection with every telco operator in a country). Fortunately, this is not necessary, as there are companies who provide E911 services in a

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

manner very similar to companies that offer wholesale call termination: you send a call to their network, and they deliver it to the designated destination. Currently there are several companies in the US who provide these sort of services (e.g. Intrado, Dash911), and their number will probably increase. Naturally, local E911 providers will be found in other countries as well.

To accommodate the demand for working with different providers, PortaBilling® uses a plugin model similar to that used for online payments. A corresponding plugin can be developed for each new E911 provider, so that you can effortlessly interconnect with them.

E911 address

Since it is impossible to locate a customer's physical address using the IP address of his phone, and asking the customer to provide his address during emergency calls is simply not acceptable, every IP phone with a 911 service activated must have an address in the PSAP database before an actual emergency is ever made. Therefore, during registration the customer must provide an address where his device will be physically located, and when he changes location (e.g. goes on vacation) he must update this address. When a customer enters an emergency service address, PortaBilling® will validate it with the E911 provider to ensure that the address is valid and contains all the required information. Then a link between phone number and address will be imported to the E911 provider database, so that now if someone calls E911 from this phone, the PSAP will receive complete information about the customer's location.

Special handling of 911 calls

Of course PortaBilling® applies a special policy for processing and routing emergency calls. For instance, even if a customer's account has exceeded its balance, and he cannot make outgoing calls, a 911 call will still go through.

Interconnection with an E911 provider

Two steps are involved here:

- Connecting to the E911 provider's API to validate and populate the customer's address. This API may be different for different providers (for instance, Intrado uses an XML interface). PortaBilling® uses a plugin specific to each E911 vendor.
- Delivering a 911 call to the E911 provider network. The actual method of interconnection depends on the provider, e.g. via SIP, or connection to a provider via PSTN trunks. In PortaSwitch both these interconnection methods are configured using the standard routing tools.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

2. Advanced Features

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

User Authentication

In general, every incoming call to PortaSIP must be authorized, in order to ensure that it comes from a legitimate customer of yours.

Digest authorization

```
PortaSIP  UA                          ser                       b2bua                     AAA
 server   70.68.0.213                 216.231.44.34             216.231.44.34
  time    Sipura/SPA2000-3.1.5        PortaSIP                  PortaSIP                  PortaBilling
 8 Dec    |                           |                         |                         |
10:19:48  @-> (A? 101/I) ♪ INVITE ----->|                         |                         |
10:19:48  |<- (A? 101/I) 100 trying - --@                         |                         |
10:19:48  |                           @-> (A? 101/I) ♪ INVITE ----->|                         |
10:19:48  |                           |<- (A? 101/I) 401 Unauthor --@                         |
10:19:48  |                           @-> (A? 101/A) ACK ---------->|                         |
10:19:48  |<- (A? 101/I) 401 Unauthor --@                         |                         |
10:19:48  @-> (A? 101/A) ACK ---------->|                         |                         |
10:19:48  @-> (A? 102/I) ♪ INVITE ----->|                         |                         |
10:19:48  |<- (A? 102/I) 100 trying - --@                         |                         |
10:19:48  |                           @-> (A? 102/I) ♪ INVITE ----->|                         |
10:19:48  |                           |<- (A? 102/I) 100 Trying ----@                         |
10:19:48  |                           |                         @-> Authorization request --->|
10:19:48  |                           |                         |<- Auth request accepted ----@
```

When the first INVITE request arrives from a SIP phone, the SIP server replies with 401 – Unauthorized and provides the SIP UA with a **challenge** (a long string of randomly generated characters). The SIP UA must compute a response using this challenge, a username, a password, and some other attributes with the MD5 algorithm. This response is then sent back to the SIP server in another INVITE request. The main advantage of this method is that the actual password is never transferred over the Internet (and there is no chance of recovering the password by monitoring challenge / response pairs). Such digest authentication provides a secure and flexible way to identify whether a remote SIP device is indeed a legitimate customer.

Authorization based on IP address

Unfortunately, some SIP UAs (e.g. the Cisco AS5300 / 5350 gateway) do not support digest authentication for outgoing calls. This means that when the SIP UA receives a "401 – Unauthorized" reply from the SIP server, it simply drops the call, as it is unable to proceed with call setup. In this case, PortaSIP can be configured so that it does not challenge the SIP UA upon receiving an INVITE. Rather, it simply sends an authorization request to PortaBilling®, using the SIP UA's remote IP as the identification. The User-Name attribute in the RADIUS authorization request will contain the remote IP address. If an account with such an ID exists in the billing database, and this account is allowed to call the dialed destination, then the call will be allowed to go through. Also, since this scheme leaves no possibility for the remote side to supply a password, PortaSIP will instruct PortaBilling® to skip the password check.

Authorization based on tech-prefix

This method of customer identification is used in circumstances similar to the IP-based authorization described above. It provides extra flexibility,

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

since after the initial configuration is done it is easy to use the same tech-prefix on a different gateway. However, this makes it extremely insecure, since any hacker can do just the same. In this scenario, PortaSIP extracts a certain portion of the destination number from the incoming INVITE request (e.g. if the complete dialed number was 1234#12065551234, the 1234# part will be used for authentication) and then passes it to PortaBilling® in the User-Name attribute.

Multi-DID control

If multiple DIDs (sets of phone numbers) have been allocated to a single user via the Account Alias feature, the PortaSwitch administrator can define whether an alias is allowed independent SIP registration. If the ability for authentication / registration is turned off, the alias cannot be provisioned on the IP phone or used for any other types of service activities. Such an alias is used solely for the purpose of routing incoming calls to that DID to the main account. This extends the available service options to hosted IP PBX and SIP trunking services.

If alias registration is allowed, the alias can basically be used as another account. (Of course, it still shares a balance with the main account.) This is useful for multiline telephones like SPA-941, where each line can have its own DID and be registered to PortaSIP independently.

Caching Authentication during IP Phone Registration

Under normal circumstances, when an IP phone goes online it provides PortaSwitch with information about its current location on the Internet (in SIP terms, this is called registration). It then periodically repeats this so as to keep the contact information updated (this is called re-registration, although technically the information exchanged between the IP phone and PortaSwitch is not any different from that exchanged during initial registration). Subsequent registrations occur at the interval programmed into the IP phone, which is usually somewhere between 10 minutes and one hour. Since the IP phone is the initiator of the registration, there is really nothing PortaSwitch can do to control the process and make re-registrations more or less frequent. (It can, however, advise the IP phone of a time to re-register again, but nothing prevents the IP phone from ignoring this and sending another registration request sooner).

When dealing with a network which contains a large number of IP phones whose re-registration interval is not automatically provisioned from PortaSwitch along with other configuration settings, the average rate of registration is a significant concern. For example, 30,000 properly configured IP phones (which re-register every 30 minutes) would generate about 17 requests per second for processing by both PortaSIP (parsing SIP messages and generating responses) and PortaBilling® (performing

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

account authentication). Yet just 500 IP phones registering too often (e.g. once every 30 seconds) due to a mis-configuration or a firmware bug would result in the same load on the system – and what happens when the number of such "impatient" phones starts growing is easy to imagine.

In order to prevent a situation where a few "rogue" IP phones create a significant load on PortaSwitch, the SIP proxy in PortaSIP performs caching of successful registration information. During the initial registration, the credentials provided by an IP phone are validated in PortaBilling® as usual, and this information is stored in the database following successful registration. Later, when a new registration request arrives from an IP phone, PortaSIP first checks its location database to see whether there is already a registration for that phone number, with the matching contact data (IP address and port on which it is accessible). If a previous registration exists and occurred recently, then PortaSIP simply replies back to the IP phone confirming successful registration. This saves resources on the PortaSIP side (since this process is much shorter than the normal dialog for handling a SIP REGISTER request) and creates zero load on the billing engine (since no authentication request is sent). This process is repeated upon subsequent re-registrations, until eventually the registration information becomes "too old" or the IP address and / or port provided in the request do not match the ones stored in the database (i.e. the IP phone is attempting to register from a new location). At that time the normal registration process will take place: the IP phone receives a challenge request, it sends back a reply calculated using its username and password, and an authentication request is then sent to the billing engine for verification.

In spite of how this may sound, simply confirming registration without verification by billing carries absolutely no security risks in this scenario. If an "evil hacker" sends a REGISTER request spoofing the real customer's IP address and port, he will only accomplish a reconfirmation of the original customer's location. If he uses a different IP address or port in an attempt to intercept the customer's incoming call, the cached information will not be used, and thus he would have to provide valid password information.

The "caching interval" is set to one half of the "recommended registration" interval, so this does not really create more "stale" sessions (where a phone is considered to be online when it has actually already disconnected from the Internet) than the normal scenario. The performance increase is tremendous: on a system with a 5-minute caching time, the amount of registrations per second that a single PortaSIP instance can handle increases 100% (from 400 per second to 800).

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

Special Destinations

Rating based on the actual dialed number may not be applicable in all cases, e.g.

- You give a flat rate for all calls among subscribers, regardless of whether their phone number is from your country or any other country.
- Different rating for incoming and outgoing calls inside your network, inside your reseller network and for calls among the accounts of a single customer.
- Special rating of all calls made to UM or conference access numbers.
- Each customer should be allowed to define several "favorite" numbers and be charged a special rate when calling any of those numbers.

If a billing engine detects one of the special conditions that may require a special rating – it will attempt to authorize and rate the call according to an applicable **special destination**. The rates for special destinations can be added into a "normal" tariff alongside traditional "phone number"-based destinations.

This allows you to easily maintain a flexible configuration for any rating scenario.

Special Destinations for Outgoing and Forwarded Calls

VOICEONNET

A rate for this special destination covers calls made between IP phones connected to PortaSwitch (regardless of the actual phone number). Please refer to the *Voice On-net Rating* section of this guide for more details.

VOICEONNETR

This special destination allows you to create a rate that will be applied to on-net calls among accounts of subcustomers that are managed by the same Reseller – so the Reseller can apply this rate in the tariffs that will be applied to the subscribers.

VOICEONNETRX

Rate for this special destination covers calls made among a single customer's accounts (on-net calls among extensions within the same IP Centrex context).

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

Special Destinations for Incoming Calls

INCOMING

A rate for this destination will be used for an incoming call to an account from any destination – whether it comes from another IP phone or a cell phone / landline outside of the network.

INCOMINGN

A rate for this destination will be used for an incoming call from another IP phone connected to PortaSwitch.

INCOMINGNR

A rate for this special destination is applied to incoming on-net calls among accounts of subcustomers that are managed by the same Reseller.

INCOMINGNRX

A rate for this special destination is applied to incoming calls from other accounts under the same customer (within the same IP Centrex context).

Special Destinations for SMS Messages

MSGN

A rate for this special destination covers messages sent to an IP phone connected to PortaSwitch (regardless of the actual phone number).

MSGNR

This special destination allows you to create a rate to be applied to on-net messages sent among accounts of subcustomers managed by the same reseller – so the reseller can apply this rate in the tariffs to be applied to the subscribers.

MSGNRX

Rate for this special destination covers messages sent among a single customer's accounts (among extensions within the same IP Centrex context).

Other Special Destinations

UM

A rate for this special destination is applied for calls from IP phones to UM access numbers (e.g. to check voice messages).

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

UMRECORD and UMLISTEN

These rates can be used to charge your customer differently for recording (when caller leaves a message for him) and listening to messages. For example, to charge the customer for accessing his own voicemail specify a price for the special destination UMLISTEN, and to provide voice message recording free of charge, specify "0" in the rate for the destination UMRECORD.

UMIVR

A rate for this special destination is used for charging your customers for calls to any IVR application (for example, for conferencing, callback calling, balance information, etc.).

FAV

A rate for this special destination is used when you offer customers a "call friends & family cheaper" type of service. The dialed number is checked against a list of "favorite" numbers defined for each account. If a match is found, the call is rated according to the rate for the `FAV` destination defined in the customer's tariff.

EMERGENCY

A rate for this special destination is applied to calls that are made to emergency numbers.

"|" ("pipe" symbol)

When a rate for this destination is created in a tariff, it would match any dialed number unless there is more specific rate available.

Precedence

To choose a specific rate to be applied to a call, the billing engine first looks up applicable rates for special destinations and if no rate for the special destination is found, it then looks for a rate based on matching a prefix (destination) with an actual phone number. If there is no match using the actual phone prefix, then the billing engine attempts to find a rate with a "|" ("pipe") destination. Thus the special destinations (except the "pipe") have higher priority compared to the "normal" rates. So for instance, if a tariff contains a zero rate for `VOICEONNET`, $0.02/min rate for 1604 (Vancouver, British Columbia) and a zero rate for "|" and the customer dials 16045551234 – the call will be authorized and billed by the zero rate associated with the `VOICEONNET` destination.

There is also a precedence among the special destinations themselves – in general, the longer destination names take priority, so the system chooses

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

the most specific one. For example, when an account receives a phone call from another IP phone – potentially both `INCOMING` and `INCOMINGN` special destinations are applicable, so the billing engine will attempt to look up both of them. If there is a rate for `INCOMINGN` it will be used (since it is more specific), otherwise the rate for the `INCOMING` destination will be applied.

Rate Codes for Measured Resources

Apart from session-based special destinations there are other destinations – rate codes for measured resources.

When charges for consumed resources are calculated and applied to a customer, an xDR is created with a defined service type and rate code and then inserted into the database. These xDRs can be grouped per rate code or service type and used to create statistics reports or be displayed on customer invoices (e.g. an xDR with charges for active calls has the ACTIVECALLS rate code and an xDR with charges for the number of concurrent calls allowed has the ALLOWEDCALLS rate code; both xDRs have the Voice Calls service type).

There is a list of default rate codes that are applicable for available measured parameters:

- **ACTIVECALLS** – This rate code covers charges for the actual number of concurrent calls made by a particular customer's accounts;
- **ALLOWEDCALLS** – This rate code covers charges for the number of concurrent calls allowed for a particular customer.

If necessary, an administrator can specify custom rate codes and use them for invoicing customers or for statistics purposes.

IP Centrex Call Rating

The handling of calls within a specific IP Centrex environment, typically the telephony system for a certain enterprise has been previously discussed, but there is one important issue remaining: how these calls will be charged? We need to have a consistent way of charging all calls between a customer's IP phones, regardless of the actual phone number dialed (for instance, the customer may have phone numbers from different cities or countries).

When a call is made from account A (belonging to this customer) to account B (belonging to this same customer), PortaBilling® will first look up the applicable rate not for the actual phone number, but for the special keyword `VOICEONNETRX`, and (if this rate available) use the price parameters

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

defined by this rate to charge the call. When entering a rate to that destination in the tariff applied to your customers, you can specify how such calls are to be rated – should they be free calls, or charged a nominal amount, and so on. If there is no rate for `VOICEONNETRX` destination in the customer's tariff, then the rate will be retrieved as usual, based on the actual dialed number

Using the `VOICEONNETRX` rate in tariffs allows you to avoid having "SIP-to-SIP" minutes mixed in with "off-net" minutes when products with volume discounts are used.

One associated feature is **Ext-to-ext Distinctive Ring**. When activated, for a call arriving from any IP phone within the same IP Centrex environment PortaSIP will instruct the IP phone to use a ring pattern different from the default one (the phone must support distinctive ringing). This allows the end user to immediately recognize whether the call is coming from one of his co-workers, or from an external number.

Voice On-net Rating

By using VoIP technology and PortaSwitch, Internet telephony service providers can truly make the world "flat" for their customers. It is possible to reach phone numbers in virtually any country in the world, and as easy to make a call to the opposite hemisphere as to your neighbor. ITSPs wishing to offer special pricing for calls made between IP phones connected to PortaSwitch (regardless of the actual phone number) can use the Voice On-Net feature. When enabled, all calls between IP phones will be rated according to the special destination `VOICEONNET`.

So if customer A has a US phone number assigned to him, and calls a phone number in India assigned to another customer in your system, customer A will not be charged the international rate for this call, but rather a special On-Net rate defined by you.

Special Access Codes

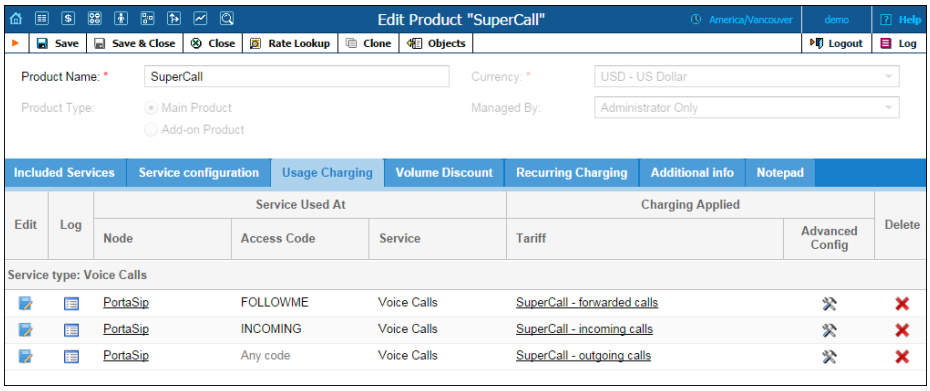
Billing using different rate plans for incoming, outgoing and forwarded calls is done by assigning different access codes to entries in the product's Services and Rating list:

- **INCOMING** – This tariff will apply to calls to the PortaSIP server arriving from outside your network and terminated to one of your SIP phones.
- **FOLLOWME** – This tariff will apply to forwarded calls.
- **OUTGOING** – This tariff will apply to calls originating from IP phones or customer's gateways. Although you may specify

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

OUTGOING as an access code, it is recommended that you keep this entry as a "default", i.e. with an empty access code.

- **TRANSFER** – This charge will apply to transferred calls (attended / unattended transfer).



The information above assumes that PSTN to SIP calls arrive directly to your PortaSIP server. If they arrive via the gateway on your network, replace INCOMING with a row containing your PSTN gateway, as explained in the *How to…* section of this guide.

IP Centrex Feature Management

Convenient and efficient service provisioning is very important when you are managing an IP Centrex / hosted IP PBX environment with tens or even hundreds of IP phones. If you need to change a certain parameter (e.g. CLI number for outgoing calls) for all IP phones, you will naturally want to avoid a situation in which you have to change this parameter manually for every account.

PortaSwitch divides call feature management into two parts:

- Some parameters are defined on the customer level, and so are global for the customer's whole IP Centrex environment.
- Call features can also be managed on the account level. You have the option of either manually overriding a certain parameter's value or specifying that the current value defined at the customer level should be used.

This allows you to define most call feature parameters only once, on the customer level. These will then be automatically propagated to accounts (individual phones).

Call Transfer

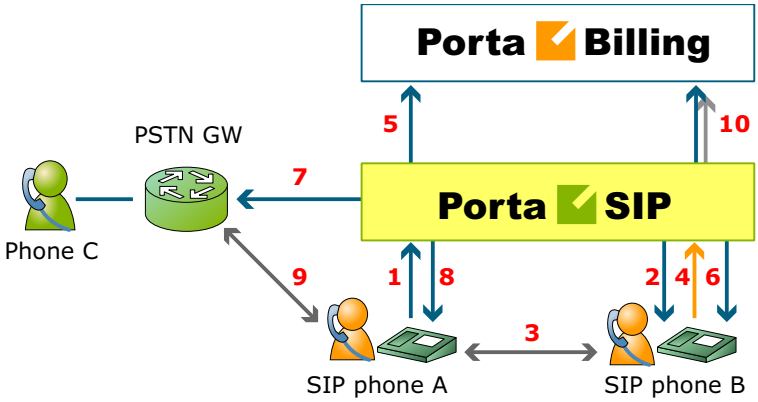
In a typical call transfer, party A sends a SIP REFER message to party B, and this causes party B to initiate a new call according to the parameters

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

specified in the REFER message (destination and the like). While this works just fine with IP phones on your VoIP network, it may not work in the case of SIP to PSTN or PSTN to SIP calls, since you will not always know if your PSTN carrier supports REFER messages (in fact, many do not support it).

To eliminate this problem and allow your users to make call transfers anytime and anywhere, PortaSIP will intercept the REFER message and process it entirely on the PortaSwitch side. Every REFER message is authorized in PortaBilling®. So if A transfers a call to a phone number in India, the billing engine will validate whether A is actually allowed to make this call, and limit the call duration according to A's available funds. After that, PortaSIP will proceed to establish a new outgoing call and connect the transferred party. When the call is finished, A (the party who initiated the transfer) will be charged for the transferred portion of the call; this applies regardless of whether A was the called or calling party in the original call. This allows you to transparently charge call transfers and avoid fraudulent activities (e.g. when an unsuspecting victim is transferred to a very expensive international destination).

Unattended (blind) transfer



- A dials B's phone number (1).
- PortaSIP sends the incoming call to B (2); when B answers, the call is established between A and B (3).
- At a certain moment in the conversation, B performs a call transfer (REFER) to C (4).
- PortaSIP intercepts this message and sends an authorization request to PortaBilling® to check if B is allowed to send a call to this destination and to obtain the routing (5). In the case of a positive reply, PortaSIP starts processing the call transfer.
- The call leg going to B is canceled (6) (since B is no longer a participant in this call); a new outgoing call is sent to C (7), and A (the transferred party) receives a re-INVITE message (8).
- Finally, the call is established between A and C (9).

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

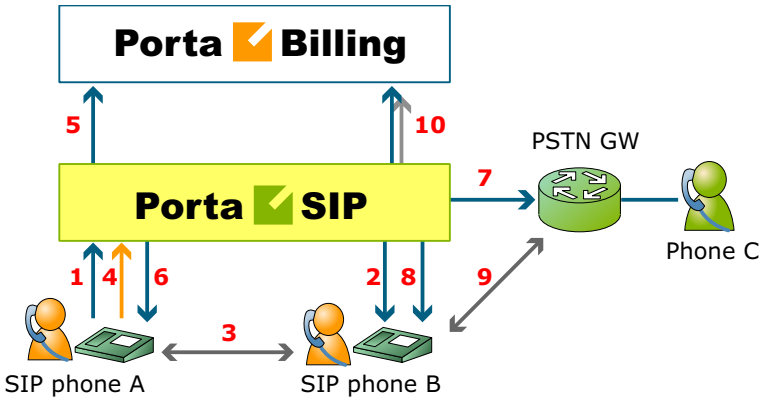
- When either A or C hangs up, the call is terminated and accounting records for two outgoing calls are sent to the billing engine (10): one is the A to B call (charged to its originator, A) and the other is the A to C call (likewise charged to its originator, B).

Assuming that A spoke to B for 5 minutes before B initiated the transfer, then A spoke to C for another 10 minutes, the call charges / CDRs will look like this:

- Under account A: A -> B, 15 minutes.
- Under account B: A -> C, 10 minutes.

As a result, A does not really know that a call transfer took place. A is charged for a normal outgoing call to B, and this is what A will see in the CDR history. B is charged for an outgoing call to C, since B is responsible for the transfer.

A scenario in which it is the calling party who initiates the transfer (shown below) is nearly identical to that described above for a transfer initiated by the called party.



If A called B and, after five minutes of conversation, transferred B to C, and they spoke for ten minutes, there will be two CDRs, both under account A:

- A -> B, 15 minutes.
- B -> C, 10 minutes.

Ring-back Tone Generation and Early Media Relaying during Blind Transfer

PortaSwitch® supports the ring-back tone generation and early media relaying during blind transfer (refer to the **Ring-back Tone Generation and Early Media Relying** section for more details), including scenarios when a call transfer is performed from within an auto-attendant menu.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

The ring back tone generation and early media relaying during blind transfer is controlled via the **transfer_progress** service policy option. Its description is given in the table below.

Option	Description

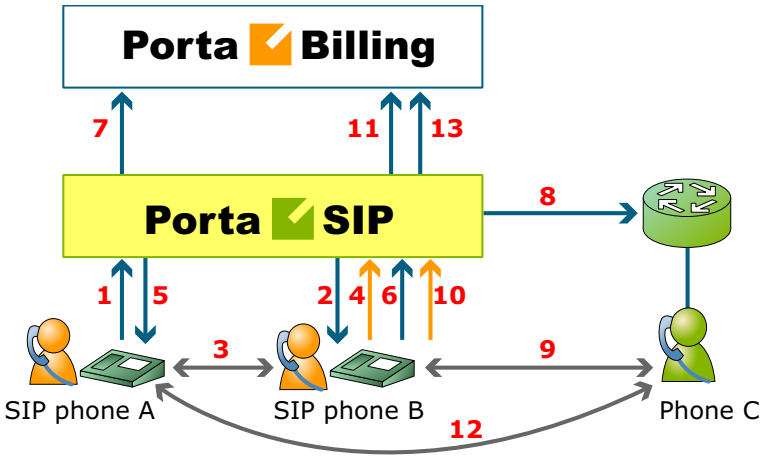
transfer_ progress	• **no_indication** – PortaSwitch® provides no audio indication during a blind transfer.
	• **transferor_moh** – PortaSwitch® plays the Music on Hold prompt when a blind transfer to some destination is initiated. Early media from the transfer target is not relayed.
	• **transferor_moh_or_system** – PortaSwitch® plays the Music on Hold prompt (or the default system prompt if the Music on Hold prompt is not selected) when a blind transfer to some destination is initiated. Early media from the transfer target is not relayed.
	• **ringing_audio** – PortaSwitch® generates a local ring-back tone when:
	  • an 18x Ringing response is received without the SDP.
	  • an 18x Ringing response is received with the SDP, but the RTP media packets are not received within a predefined timeout.
	
	Early media (if sent by the transfer target) is relayed.

An administrator configures a service policy to fine-tune the desired behavior and then assigns this policy to the account that performs the transfer.

This helps to ensure that transferred parties are kept informed about the progress of the call, thus improving the customer's overall experience with PortaSwitch®.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

Attended transfer



- A dials B's phone number (1).
- PortaSIP sends the incoming call to B (2); when B answers, the call is established between A and B (3).
- B places A on hold (4); PortaSIP provides music on hold for A (5).
- B initiates a new outgoing call to C (6). PortaSIP sends an authorization request to PortaBilling® to check if B is allowed to send a call to this destination and to obtain the routing (7). In the case of a positive reply, PortaSIP establishes a call to C (8).
- The call is now established between B and C (9); after a short exchange B decides to bridge A and C together, and a REFER message is sent to PortaSIP (10).
- PortaSIP will now connect A and C together (12) and cancel both of the call legs going to B.
- When either A or C hangs up, the call is terminated and accounting records for two outgoing calls are sent to the billing engine (13): one is the A->B call (charged to its originator, A) and the other is the A->C call (likewise charged to its originator, B).

Attended transfer of forwarded calls by DTMF

Attended transfer by DTMF allows users not only to answer calls forwarded to their mobile phones from their extensions, but also to transfer such calls via DTMF to any extension on the IP PBX just as they do using a SIP phone.

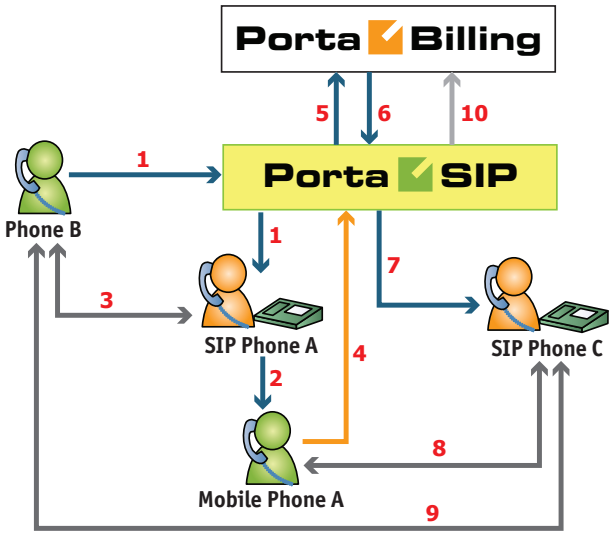
With attended transfer by DTMF enabled, all that users need to do is:

- Dial the special pre-configured transfer code *66, the number of the extension to which the call is to be transferred, and #.
- Make sure that the called party is available and willing to receive the call.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

- Complete the transfer connecting the two parties.

The following diagram illustrates this flow in detail:



- B dials the extension of A (1).
- The call arrives at PortaSIP® and once authorized by PortaBilling® is routed to User A.
- A does not answer, so the call is forwarded to A's mobile number (2).
- A answers the call, and the call is established between B and A (3).
- A realizes that the call is intended for C, and initiates a new outgoing call to C from the mobile phone by dialing *66 followed by C's extension number plus # (4).
- PortaSIP® intercepts the *66 transfer code, collects the extension number, and sends an authorization request to PortaBilling® (5).
- PortaBilling® verifies that A is allowed to transfer calls via DTMF and returns routing to PortaSIP® (6).
- PortaSIP® places B on hold and establishes a call to C (7).
- The call is established between A and C (8). After a short exchange C confirms acceptance of the call from B, whereupon A hangs up to finish the transfer.
- PortaSIP® connects B and C (9).
- When either B or C hangs up, the call is ended and the following accounting information is sent to PortaBilling® (10):
    - A is charged for two call legs, for the incoming call forwarded from B to A's mobile phone, and for the outgoing call from A to C.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

Call Forwarding

PortaSIP supports several call forwarding modes; you can select a specific mode from the **Forward Mode** menu on the **Call Features** tab:

- **Simple Forwarding** is unconditional forwarding to a single phone number, pre-defined by the user.
- **Follow-me** allows you to specify multiple destinations for call forwarding, each of which is active in its own time period. You can also specify that multiple numbers be tried one after another, or that they all ring at the same time.
- **Forward to SIP URI** allows you to specify not only a destination phone number but also an IP address for calls to be forwarded to. This is useful when calls have to be routed directly to an external SIP proxy.
- **Advanced Forwarding** adds a few extra options to those available in **Follow-me** mode, and also allows you to route calls to SIP URI. It thus represents a super-set of all call forwarding capabilities.

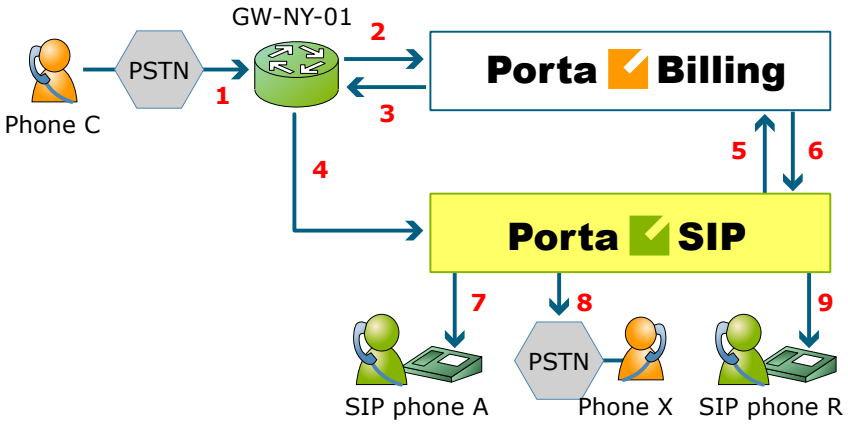
Follow-me services

The follow-me feature allows you to receive calls even if your IP phone is offline at the moment. You can specify several alternative destinations for a single destination number (account). Follow-me is activated when:

- IP phone is offline (not registered).
- IP phone replies with an error code (i.e. the line is currently busy because you are making another call).
- No answer is received within a certain interval (usually 20 seconds) – the phone may be online but nobody answers, or there is a network outage.

For instance, if you do not pick up your IP phone (or the IP phone is unreachable due to a network error) the call would be forwarded to your home phone; if not answered within 30 seconds, it would be forwarded to your mobile phone, and so on. For each of these phone numbers you can define the period when a given phone should be used; for example, calls should be forwarded to your home phone only from 8 in the morning until 9 in the evening.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com



- C wishes to call A. So he dials A's phone number (since C is in the US, he dials it using the North American format, 2027810003).
- The call is routed through the telecom network to gateway GW-NY-01. When the incoming call arrives at the gateway (1), it is processed there in exactly the same way as a normal PSTN->SIP call: the number is transformed, the call is authorized in the billing engine (2), and the timer starts to measure the maximum call time allowed, based on A's current balance (3).
- The call is sent to PortaSIP (4).
- PortaSIP receives the INVITE, but without authorization information. So the PortaSIP server performs authorization in the billing engine based on the IP address, and also requests billing-assisted routing (5).
- PortaBilling® recognizes that the destination is an account with follow-me services enabled, and produces a special list of routes:
    - If the follow-me mode chosen is "When unavailable", then a direct route to the account's SIP UA is included as the first route in the list, with a default timeout.
    - A list of follow-me numbers is produced. If the current time falls outside the specified period for a certain number, it is removed from the list.
    - If the follow-me order is "Random", then the list of phone numbers is shuffled.
    - The maximum call duration is calculated for each follow-me number, based on the balance and rates for the **called** account (A).
    - The resulting list of routes is produced and sent back to PortaSIP (6).

- PortaSIP tries the first route (7); if the call is not connected within the timeout interval, it moves to the next route (8), then to the next one (9), until either the call is put through or no more routes are left.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

- If such a call was completed to follow-me number R (SIP account), then two CDRs will appear in the system: one for the call C->A (charged per the incoming rates for A) and the other for C->R (charged per the incoming rates for R).
- If the call did not originate in the PSTN network, but rather from user B's SIP UA, two CDRs will likewise be generated. B will be charged for call B->A, while R will be charged for B->R (charged per R's incoming rates).

The follow-me service can be recursive. Thus A can forward calls from his SIP phone to B's SIP phone, and B can forward calls to his mobile phone number C. Note that in the case of such a multi-hop follow-me (A->B->C->D->PSTN number), only two CDRs will be produced (similar to a simple follow-me):

- A CDR for the caller (billed to A, A->B).
- A CDR for the forwarder outside the network, i.e. the last SIP account in the follow-me chain (billed to D, A->PSTN).

Simultaneous ringing

You can define a follow-me list with several phone numbers, all of which will ring concurrently. The first one to answer will be connected to the incoming call.

You can also include your own phone number on the list of phone numbers for simultaneous ringing. Your IP phone will then ring together with the other phones (e.g. your home phone or cell phone) and you can answer either one of them. In this case, you are advised to modify the call processing so that it does not include the **Ring** action but starts immediately with **Forward**. Otherwise, the system will first ring only your IP phone, and then ring both your IP phone and all the other phones.

SIP URI forwarding

In traditional call forwarding, you only specify a phone number where calls are sent using the currently available termination partners. This is very convenient for calls terminated to PSTN, since in this case PortaSwitch LCR, profit-guarantee, fail-over and other routing capabilities are engaged automatically. If you provide services such as DID exchange, however, calls must be forwarded directly to a large number of different SIP proxies belonging to your customers. In this case, for every account (DID) you simply define which phone number and IP address all incoming calls should be forwarded to.

In order to protect you from abuse of this service (e.g. a customer tries to set up call forwarding to somebody else's network, then relays a storm of call attempts through your SIP server) it is only possible to use those SIP proxies, which are listed in the **Permitted SIP Proxies** customer

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

information. If a customer who buys DIDs from you has two SIP proxies, you need two list each of those proxies in the **Permitted SIP Proxies** configuration. After that your administrators (or the customer on his self-care pages) will be allowed to use these IPs in the SIP URI.

Billing calls forwarded to an off-net destination

When a call is forwarded to an off-net destination, it is treated as two separate calls from a billing perspective. Thus, if party A (SIP account) calls party B, and B has follow-me set up for off-net destination C, the following will occur:

1. PortaBilling® will check if A is authorized to call B and for how long (based on A's rates and the funds available in A's account).
2. If forwarding is currently active on B's account, PortaBilling® will check if B is authorized to call C and for how long (based on B's rates and available funds).
3. After the call is completed, the two accounts are charged, and CDRs are produced accordingly: one for account A, for a call to destination B, the other for account B, for a call to an off-net destination C.
    - If the call did not originate from SIP account A, but rather from the PSTN network, then two CDRs will likewise be generated. B will be charged for both calls: one for PSTN->B (charged per the incoming rates for B), and another for B->C (charged per the outgoing rates for B).

For A, this call looks like any other call made to B. If B is a number in the US, it will look like a call to the US, and A will be charged according to US rates, even if the call was actually sent to a mobile phone in the Czech Republic. For B, the forwarded call is authorized and billed according to the same rules as a normal outgoing call from this account (or you can apply a different rate plan for forwarded calls). For instance, if B is allowed to make outgoing calls only to US&Canada, and tries to set up a follow-me number to India, the number will not be usable. If multiple follow-me numbers have been defined, each one will be authorized independently. So if B currently has $1 available, and this is enough to make a 5-minute call to the Czech Republic or a 3-minute call to Russia, the call will be automatically disconnected after 5 or 3 minutes, respectively.

Billing calls forwarded to SIP account

Billing for calls forwarded to a SIP account differs from the above case, in which a call is forwarded to an off-net destination.

When a call is forwarded to a SIP account, it is still treated as two separate calls, from a billing perspective, although the logic is different. Let's

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

consider the following example: if account A calls account B, and B has follow-me set up for account C, the following will occur:

1. PortaBilling® will check if A is authorized to call B and for how long (based on A's rates and the funds available in A's account).
2. If forwarding is currently active in B's account, PortaBilling® checks that B is not barred to call C (this restriction can only be based on B's service features such as **Call Barring**, since B's tariff does *not* influence calls forwarded to other SIP accounts) and also if C is authorized to receive the call and for how long (based on C's incoming rates and the funds available in C's account).
3. Then, after the call is completed, the two accounts are charged and CDRs are produced accordingly: one for account A for a call to destination B and the other for account C, for an incoming call from account B.
    - Note that intermediary forwarding accounts (account B in this example) are not charged because they don't actually generate calls and their role (forwarding a call to another SIP account) doesn't involve any costs for the service provider.
    - If the call did not originate from SIP account A, but rather from the PSTN network, two CDRs will likewise be generated. B will be charged for call PSTN->B (charged per the incoming rates for B), while account C will be charged for B->C (per the incoming rates for C).

Forwarding with the original DNIS (CLD)

Very often a company operating an IP PBX would purchase multiple phone numbers, all of which were to be routed to the company (e.g. the main office phone number is in the New York area, but the company also has an 1800 number and a number in the UK for their UK-based sales representative). In general, each additional phone number is provisioned as an account in PortaBilling®, and then a corresponding SIP phone is registered to PortaSwitch® using this account ID to receive incoming calls. But some IP PBXs (e.g. SPA-9000) can only register a single telephone number (account) with the SIP server. In this case, you may set up calls from additional phone numbers to be forwarded to the main account using the follow-me feature. For example, an IP PBX registers to PortaSwitch with account 12061234567; however, DIDs 18007778881 and 4412345678 must also be delivered to the IP PBX. So you would set up accounts 18007778881 and 4412345678 with follow-me to 12061234567. All calls will then be correctly routed to the IP PBX; however, since they all arrive to the IP PBX as calls to 12061234567, calls to different DIDs cannot be distinguished (e.g. if a customer originally dialed the 1800 number, he should be connected to general sales, while if the UK number is dialed the call should be answered by a specific sales team group).

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

In this situation, when defining a forwarding destination you should also activate the **Keep Original CLD** option available in advanced forwarding mode. This will instruct PortaSwitch that the call must be forwarded to destination 12061234567 (in this case, to a registered SIP phone with this number), while the To: in the INVITE message should contain the original DID. The IP PBX will then properly process incoming calls and will forward them to the correct recipient.

Visible call forward info

Ordinarily, when your phone rings, the only information available is the original caller's phone number and, optionally, a caller name. While this works for simple residential calling, where it is always person A calling person B, in an IP PBX scenario there is usually more happening before your IP phone starts to ring. For instance, a secretary answers calls for several companies (Smart Software Design at 18005551234 and Synadyn Corporation at 12065559876), so she needs to greet callers differently depending on which company's number they originally dialed. Similarly, when John is substituting for his colleague, he needs to answer calls to his phone from the sales queue differently from calls forwarded there from the technical support queue. So in a case where calls are being delivered to a phone via an entity such as a huntgroup, external DID or the like, it is obviously important to see not only the original caller's identity (which in many cases is not even very useful) but also information about the entity which forwarded the call.

The visible call forward info feature in PortaSwitch allows users to easily determine the origin of an incoming call and react accordingly. So when account A (representing an external phone number, huntgroup, etc.) in PortaSwitch is configured to forward calls to account B (representing the actual IP phone line), the forwarding is configured to replace "Display Name" information (the description displayed along with the caller's phone number on the phone as it is ringing) with information identifying account A.

Call forwarding from an IP Phone (Endpoint redirection)

The end user may program a "forward to" phone number directly into the phone (many old-style PBX users are accustomed to doing this via feature codes), which will afterwards be returned by the phone in a "302" response to an incoming call request.

PortaSIP® will process a "302" SIP redirect message as if this number were configured in the forward / follow-me settings on the PortaSwitch® web interface (including authorization and charging the user who originated the forward, for the forwarded portion on the call). Advanced settings such as multiple forwarding numbers and time periods are not available for phone-initiated forwarding.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

Note: By design, the "302" redirect does not incorporate authentication, rendering it a potential security risk when used on a public Internet. This is why this feature must be specifically enabled for a customer or account – PortaOne strongly suggests that this be done *only* for those customers who indeed require this feature and are aware of the implications.

Endpoint redirection on IP phones that ring simultaneously

An IP phone that belongs to a particular ring group can forward calls to another phone number that an end user directly enters into their phone.

For example, there are three IP phones that ring at once: phone A, phone B and phone C. Staff member John Doe, who usually answers phone C, wants to receive calls on his own mobile phone. So John Doe enters his mobile phone number directly into the phone as the "forward to" number.

When a call comes to the ring group, phone A, phone B and John Doe's mobile phone begin to ring. The system connects the call to the phone that is picked up first. The other phones stop ringing.

Call Forking

This new feature makes all SIP phones registered on a single account ring simultaneously. Consequently, if an end user owns three SIP phones (e.g. a mobile application on a smartphone, a tablet and a desktop IP phone), he can receive calls to all three devices simultaneously. The same account ID and password can be applied for all end-user SIP phones.

NOTE: Availability of the PortaSIP cluster is mandatory for the call forking feature to work.

To enable call forking on the Configuration server, find the **ClusterSuite** in the **Configuration Tree**, then select **SIPCluster** and choose **ProcessingNode** under it. Select **MUB2bua** among the available groups. Fill in the following fields that control the call forking configuration:

- **call_forking** – Select one of the following options to adjust the sequence in which the SIP phones must ring:
  - **one_by_one** – SIP phones ring in priority sequence (from higher to lower). The end user chooses and assigns the priority in the SIP phone settings;

    NOTE: If priority is not assigned to a SIP phone, then the SIP phone has the lowest priority by default.

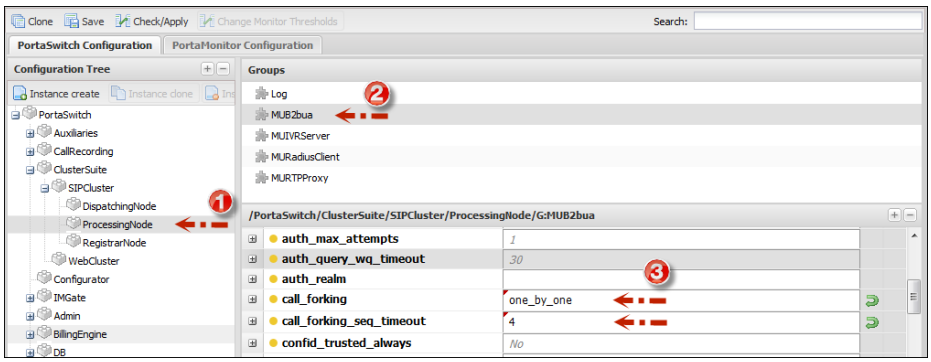
  - **grouped** – SIP phones having equal priority are grouped and ring simultaneously when they are called (from higher to lower priority);

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

- **parallel** – all SIP phones ring simultaneously;
- **disabled** – the last registered SIP phone rings.

NOTE: The time of registration is the time when the last REGISTER request was sent from the SIP phone.

- **call_forking_seq_timeout** – Define the minimum time value (in seconds) during which a SIP phone rings before a call is forwarded to the next SIP phone. This parameter is applied only for the **one_by_one** or **grouped** call forking options.



Using the call forking feature an administrator can easily apply configurations for simultaneous calls to SIP phones for the entire PortaBilling® environment. This significantly simplifies an administrator's work because it does not require the application of more advanced configurations such as **Call Forwarding** and the creation of individual accounts for each SIP phone.

Call Screening

Sometimes incoming calls need to be treated differently: calls from your boss or secretary should reach you on your cell phone even during the weekend, while other calls can just go to voicemail. Calls in the evening hours should go straight to your cell phone (there is no point in ringing your IP phone while you are not in the office), while calls from your ex-girlfriend should always go to voicemail.
All of this can be done using the call screening rules in PortaSwitch. When the call screening feature is enabled for an account (phone line), you can define a set of rules that will be applied to every incoming call. Each rule may include some of the following limitations:

- **From** – Calling number condition. You can specify a list of phone numbers for a caller (ANI or CLI) which satisfy this condition, e.g. you can list extensions for your boss and secretary, your home phone, your wife's cell phone number, and so on. When specifying a phone number, you can enter either the full number or a pattern (e.g. all numbers starting with 1800).

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

- **To** – Called number condition. This can be useful if you have multiple account aliases (or DID numbers) forwarded to your main account. For instance, you may wish to treat incoming calls to your business toll-free number differently from calls to your regular phone number.
- **Time Window** – Call time condition. You can specify limitations regarding the time of day, day of the week, day of the month, or some combination of these. This is ideal for making sure your phone will not ring in the middle of the night.

A rule may contain only some of these limitations (e.g. time), in which case the others will contain a wildcard (e.g. calls from any phone number, or made to any of your DID numbers).

Each rule provides instructions about exactly how a call should be processed. It contains a sequence of one or more of the following actions:

- **Reject** – Simply drop the call without answering it.
- **Ring** – Ring on the current IP phone.
- **Forward** – Redirect to the numbers defined in the call forward / follow-me settings.
- **Voicemail** – Connect the call to this phone's voice mailbox.

When assigning an action to a rule, you will be offered a list containing all the possible combinations based on the currently available features for this account. For instance, the Forward option will be present only if the call forwarding service is currently enabled for the account.

Call screening algorithm

When a new call arrives to PortaSwitch, call information is sequentially checked against all defined call screening rules. The call information (ANI, DNIS and current time) is checked against each rule's limitations. If at least one of these does not match, the rule is skipped and processing moves on to the next one. If there is a match for all three limitations, then the rule's actions are executed and no further rules are processed. If none of the rules matches (or if no call processing rules have been defined), then the default rule is applied, as follows:

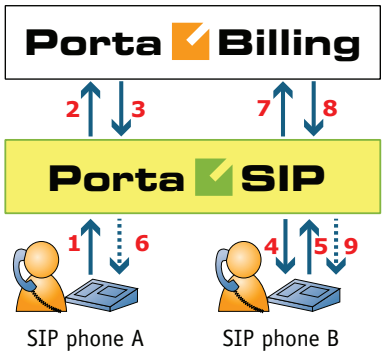
- Ring on the IP phone.
- If not answered within a certain time (defined by the **Timeout** parameter in **Service Features** for the **Voice Calls** service), and if the account has call forwarding enabled, attempt to connect the call to the phone numbers listed there.
- If the call is still not answered and the account has the UM service enabled, forward the call to voicemail; otherwise drop the call.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

Call Parking

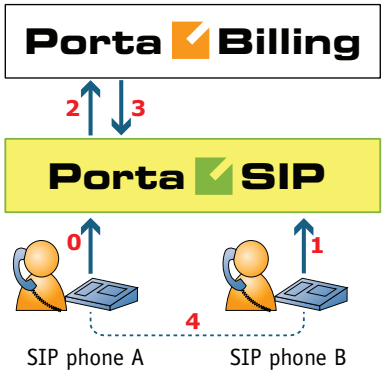
Call parking allows users to put a conversation on hold and then resume it from a different IP phone.

Parking a call



- A dials B's phone number (1).
- An authorization request is sent to PortaBilling® (2); if authorized successfully (3), the call is connected to B (4).
- B parks the call: puts A on hold and then dials a special call parking prefix (5).
- A hears the music-on-hold melody (6).
- The dialed prefix is sent to billing for verification (7).
- Upon successful approval (8), the call parking confirmation message is played to B (9); this message also contains information about the code for retrieving the parked call.

Retrieving a parked call



- A is still connected via call parking (0).
- B dials the retrieval code from any IP phone (1).

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

- An authorization request is sent to PortaBilling® (2), which determines that this is an attempt to retrieve the parked call (3).
- The two call legs (A and B) are joined together (4).

Call Barring

Call barring allows you to prohibit outgoing calls to specific destinations. The main difference between call barring and blocking destinations in a tariff is that the latter applies to all customers using a given tariff plan, while call barring can be activated and configured for an individual account. Also, whereas only the administrator can manage a tariff plan, call barring can be provisioned by end users themselves (e.g. parents prohibiting calls to a dubious premium number on their child's phone, or a small business owner blocking outgoing international calls on a public phone in his café).

When the **Call Barring** service feature is activated, as part of normal call authorization the system checks whether a dialed number matches any pattern specified in the call barring classes. If it does, and if call barring has been activated for that class, the call is rejected.

A call barring class covers a specific set of phone numbers that the customer should potentially be denied access to. In this regard, a call barring class is very similar to a destination group. The difference is that while a destination group can only contain pre-defined destination prefixes, a call barring class operates with a mixture of patterns (e.g. 448% - any number starting with 448) and actual phone numbers (e.g. 44810010099). This lets you fine-tune call barring options without creating excessive destination prefixes.

Definitions of various call barring classes (such as "Mobiles," "International," etc.) are done globally in the **Call Barring Classes** tab of the **Dial Plan** page. Barring of a specific class can then be turned on / off for an individual account.

Customer Sites

A site is a group of customer's accounts that can be conveniently managed as a single entity. For instance, all of the phone lines used in a sales department or in 'office building A' can be joined into a single group. This allows you to apply certain configuration parameters or service restrictions to the accounts in that group. You can limit the combined number of simultaneous calls for all accounts of a particular site. This is useful if, for instance, 'office building A' has limited bandwidth and can only support 30 calls – no more calls will be allowed

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

in order to avoid severe degradation of the sound quality on all calls in progress.

Calls per Second Control

Many ITSPs try to prevent situations in which heavy traffic overloads various components of the VoIP network (for example, because of call centers with auto-dialer software).

To control the amount of traffic that passes through the VoIP network, PortaSwitch® allows the enforcement of the calls per second (CPS) limitation. With the CPS limitation functionality you can restrict the number of dialing attempts that can be made by an endpoint (e.g. a call center PBX) each second. For example, the allowed rate for a call center PBX is defined as 10 CPS. It's possible that at some moment, the call center will send 100 calls per second. As a result, only 10 call initiation requests per second can be processed further, and therefore the other 90 are rejected.

NOTE: The CPS limitation functionality only works if an endpoint is authorized by the IP address or digest username.

In the case of several endpoints using the credentials of a single account, this account's CPS limit is shared by each of these endpoints. That is, the number of dialing attempts made per second by all endpoints cannot exceed the maximum number of dialing attempts defined for the account.

The CPS limitation relies on the Limit Controller component – a part of the PortaSIP® cluster solution. Thus, assuming that the PortaSIP® cluster is configured and running, the logic of processing outgoing calls with the Limit Controller component can be summarized as follows:

- An endpoint attempts to place an outgoing call. The PortaSIP® cluster node receives a new SIP message, detects that this is a new call setup attempt and hence forwards it to the Limits Controller.
- The Limits Controller performs an analysis of the received SIP message: it parses out a caller's IP address and username. Using these attributes, the Limits Controller retrieves the current CPS counter value and configured CPS limit. The Limit Controller then updates the current CPS counter and recalculates the caller's current CPS rate.
- The Limits Controller compares the current CPS rate of the caller and the configured CPS limit. If the CPS counter value is lower than the CPS limit, the Limit Controller relays a positive SIP response and the call is processed further. If the Limit Controller detects that the CPS counter value exceeds the CPS limit, it rejects the call. The Limits Controller always provides a SIP response

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

when it rejects a call to prevent retransmits and the involved components becoming overloaded.

If a PortaSIP® cluster node detects that a newly received message is an in-dialog message, the message will not be sent to the Limit Controller.

Ring-back Tone Generation and Early Media Relying

When an end user places an outgoing call, they expect to hear a ring-back tone in return, to signify that the call is in progress. If the line is quiet, the end user might think the call has failed and might hang up although the call is actually ringing at its destination.

Such situations have been observed when certain VoIP equipment is unable to generate a ring-back tone (for example, due to overload). To ensure that a ring-back tone is delivered to the call originator, PortaSwitch® generates a local ring-back tone.

Let's see how this works in SIP. When a caller makes a call from a SIP user agent, an INVITE request is sent to the called party. When the called party's phone begins to ring, it sends back an 18x Ringing response. The 18x Ringing message may or may not include the Session Description Protocol (SDP) which is used to set up a one-way media stream for conveying RTP media packets with ring-back tone to the caller.

PortaSwitch® analyzes the 18x Ringing message received. If it doesn't contain the SDP, PortaSwitch® immediately generates its own ring-back tone and sends it to the caller. If the 18x Ringing message is received with the SDP, PortaSwitch® waits for the RTP media packets. If they are not received within a predefined timeout, PortaSwitch® generates its own ring-back tone for the caller.

Ring-back tone generation is controlled via the **call_progress_notification**, **call_progress_filter** and **early_media_timeout** service policy options (you can find their description in the table below). Besides ring-back tone generation, these service policy options also control early media relaying. Early media is a powerful aspect of SIP that allows two endpoints (user agents) to communicate before a call is actually established. In terms of SIP this means relaying media prior to 200 OK is sent in response to an INVITE request.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

Option	Description

call_progress_ notification	• **signaling** – This is the default value. PortaSwitch® just re-sends 18x call progress responses and media received from the called party.
	• **audio_rbt** – PortaSwitch® generates a local ring-back tone when:
	  • An 18x Ringing response is received without the SDP.
	  • An 18x Ringing response is received with the SDP, but the RTP media packets are not received within a predefined timeout.
	
	Early media (if provided by the called party) is relayed.
	• **mow** – PortaSwitch® plays the Music on Waiting prompt upon receiving an 182 Queued response without the SDP. The rest of the 18x call progress responses are just re-sent to the called party.

call_progress_ filter	• **full_progress** – This is the default value. PortaSwitch® just re-sends early media and 18x call progress responses received from the called party. • **ringing_only** – PortaSwitch® turns all 18x call progress responses and media from the called party into a 180 Ringing message.
early_media_ timeout	This defines a duration during which PortaSwitch® waits for the RTP media packets upon receiving an 18x Ringing response with the SDP from the called party. If they are not received within the predefined timeout, PortaSwitch® generates its own ring-back tone for the caller.

Let's have a closer look at how a call with ring-back tone generation and early media relaying is established.

1. A caller makes a call from a SIP UA that arrives at the B2BUA. The B2BUA verifies if there is a service policy dynamically matched by the User-Agent header field.
2. The B2BUA sends an authorization request to the billing engine. The billing engine checks if the caller is allowed to send the call to the desired destination and provides the B2BUA with the routing. The authorization response also includes information about the service policies configured for both participants of the call.
3. For each tried route, the B2BUA analyzes the following service policy options:

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

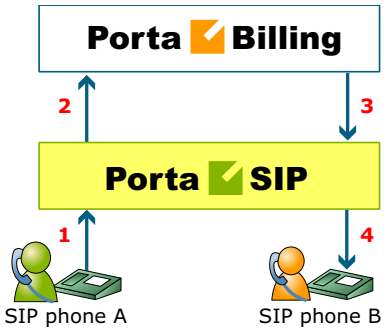
- The **call_progress_notification** option from the dynamically matched service policy.
- The **call_progress_notification** option from the service policy assigned to the Calls from Vendor connection or the authorized account.
- The **call_progress_filter** option from the service policy assigned to the Calls to Vendor connection or the called account.
- The **early_media_timeout** option from the service policy assigned to the Calls to Vendor connection or the called account.

4. The B2BUA receives an 18x call progress response from the called party. The resultant behavior (whether to generate a local ring-back tone or just re-send all 18x call progress responses, relay or prohibit early media) depends on the service policy options configured for both participants of the call. For more detailed information please refer to **APPENDIX G**.
5. The B2BUA starts a new route, without the interruption of the ring-back tone initiated on the previous step.
6. Steps 4 and 5 are repeated for each route tried until 200 OK is received.
7. The B2BUA connects the caller with the called party.

Paging / Intercom Calls

Intercom calls enable users belonging to the same group to use two phones like an on-door speakerphone. When one user dials a special code before the other user's phone number, a two-way audio channel is established automatically. The other user does not need to pick up his handset; instead, speaker-phone mode is activated and both users can now talk to each other. Most VoIP phones with the SIP protocol can be used for intercom calls.

Placing an intercom call



© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

- User A dials an intercom prefix, followed by User B's phone number. His SIP user agent sends an INVITE request to the PortaSIP server (1).
- An authorization request is sent to PortaBilling® (2).
- PortaBilling® performs several operations:
    - Checks that such an account exists and is allowed to use SIP services.
    - Checks whether account B belongs to the intercom group under the same customer.
    - Checks if the account is registered.

  Based on the results of these operations, PortaBilling® sends an authorization response to the PortaSIP server, with a special "auto-answer" trigger (3).
- The PortaSIP server adds the "auto-answer" header to the outgoing INVITE request, and sends the call to SIP user agent B (4).
- The two call legs (A and B) are joined together.
- Speakerphone mode is activated immediately on User B's phone.

SIP Identity

With the growing popularity of VoIP services such as residential VoIP or business SIP trunking, the question of user identity becomes increasingly important, since the only critical piece of identity in a phone call is the caller number (also known as the CLI or ANI), and it is extremely easy to be forged. There is nothing that prevents an IP phone or IP PBX from placing a string into the "From:" SIP header that corresponds to the "Caller number." When one receives a phone call that displays the caller number, for example, as 12065551234 – is it really the person who owns that phone number calling – or is it a fraudulent scam? The question of identity becomes more complex when a call traverses networks of several different service providers. Within this chain, only the first telco (the one the subscriber is directly connected to) can verify the end-user's identity; the other service providers must rely on the information that is provided as a part of the call data – so it is extremely important to know who your trusted contacts are. In many countries, strict regulations govern the responsibilities of service providers in regard to establishing the identities of their customers and passing this information on to the national telephony network or other carriers.

This is why there are several overlapping RFCs and technologies regulating the way the verified identity of the user is passed from one VoIP operator to another. PortaSwitch® supports the most important

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

ones and provides all required tools to conform to the requirements regarding the handling of the user identity.

Trusted Networks

A call is considered as coming from a trusted network if it originates via one of the nodes on your network (it is assumed that this node has already performed the required authorization and established the user's identity, so the provided identity data will be reliable) or if it is coming from an external end-point that has been explicitly marked as trusted.

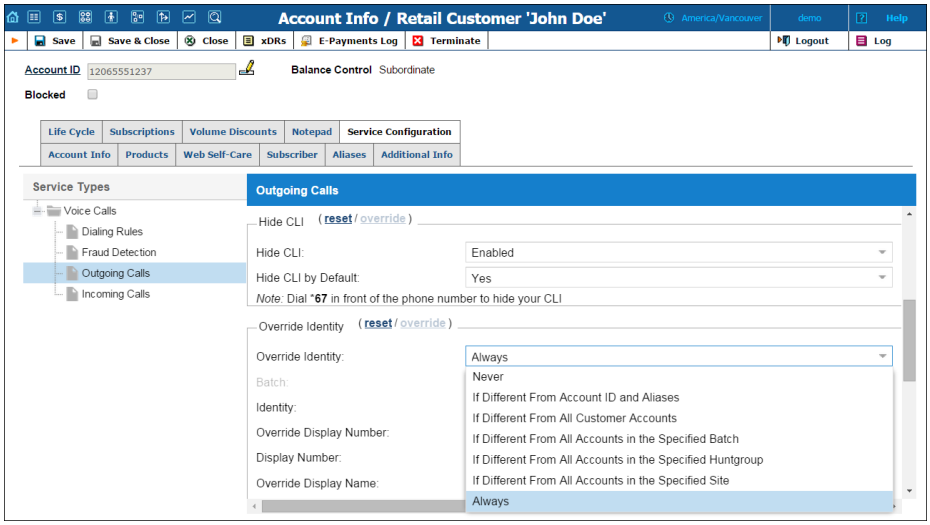
Identity Handling

The process is split into three stages:

1. Extracting the user identity information from the incoming call information based on the incoming network/user trust settings:
    - For requests coming from the trusted network this is done in the following order: if P-Asserted-Identity data is available, then it is used as the identity CLI. Otherwise, if Remote-Party-ID (RPID) data is available, it is used as the identity.
    - When the network is not considered as trusted or neither of the above headers exist, the requested identity is extracted from the P-Preferred-Identity header or as a last resort, from the SIP From: header.
2. Deciding what the user identity should be, based on the user configuration (assigned by the PortaSwitch® administrator – see below) and the data collected during the previous step.
3. Including the required identity data in the outgoing call information, based on the trust status of the user being called or terminating network.

On the PortaSwitch® side, it is possible to set the following conventions for handling identity information:

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com



- **Never** – Accepts and continues relaying any identity value supplied by the remote party. This assumes that the remote party is trusted and undertakes full responsibility for the display number and name supplied.
- **If Different From Account ID and Aliases** – The identity could be the ID of the account that is authorized for the call – or any of the aliases assigned to this account. This allows a customer who is assigned two extra DIDs in addition to his primary number to place outgoing calls using any of these DIDs as his identity.
- **If Different From All Customer Accounts** – An identity is considered valid if it matches an account ID (or account alias) of any of this customer's accounts. This is ideal for SIP trunking types of services, when a customer has his own IP PBX that contains multiple phone lines (extensions) provided on it. The supplied identity is fine as long as it matches one of the phone numbers provided for this customer.
- **If Different From All Accounts in the Specified Batch** – This is a more restrictive option than the one above as it requires that both the account that places the call and the account that matches the supplied identity are from the same batch. This allows you to create "groups" under the same customer. For example, if a UK user makes a call, this call will have an identity that matches any of the customer's UK numbers; if a Canadian user makes a call, the identity used for this call will match any of the customer's Canadian numbers. In this case, all UK and Canadian numbers will belong to their respective batches.
- **If Different From All Accounts in the Specified Huntgroup** – This option requires that the account placing the call and the account that matches the supplied identity come from the same huntgroup. This allows you to fine-tune the identity to be used for calls made by separate departments in your company. For example, calls made by the Sales department will have an identity

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

that matches one of the extensions (phone numbers) from the huntgroup "Sales," while calls made by the Support department will have an identity that matches one of the extensions from the huntgroup "Support."

- **If Different From All Accounts in the Specified Site** – This option requires that the account placing the call and the account that matches the supplied identity come from the same customer site. This allows you to manage the identity for groups of accounts that come from the same customer (within the same IP Centrex environment). For instance, if a customer owns two IP PBXes – a call from PBX A may only have an identity that matches phone numbers associated with PBX A and a call from PBX B may only have an identity that is associated with the phone numbers managed by PBX B. In these cases, each PBX will be represented as a separate customer site.
- **Always** – The identity will always be set to the value defined in the **Identity** field.

Preferred Identity

If an end-point is not trusted, the identity information (P-Asserted-Identity) it supplies will simply be ignored. In this case, the end-point may only suggest the desired identity via the P-Preferred-Identity header. If the desired identity passes all of the validation rules, it can be used as the identity for the outgoing call. After that, the P-Preferred-Identity header is discarded from the outgoing call information and never sent to another IP phone or vendor.

Identity and CLI/ANI Number

Sometimes people think about the VoIP identity as the "caller number" – the number that the party being called will see. This is not true, however – in many cases they can differ. For instance, when a caller requests anonymity (to hide his CLI/ANI number from the party being called) his identity will still be delivered to the telco. This is why in the SIP INVITE message, the identity information is transported in a separate header from the CLI/ANI data that is transported in the SIP From: header.
The "Caller number" value that will be placed in the From: header is controlled by the **Display Number** property. The possible values are:

- **Never** – Will allow the remote IP phone or IP PBX to supply any CLI / ANI number.
- **If Ruled Out by the Identity Constraint** – Will apply the same restrictions as the ones placed on the identity information (described above).
- **If Different from the Used Identity** – Similar to the above, but makes it obligatory for the displayed number to always be the same as the identity CLI, so if a remote party provides a CLI that

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

is valid, but not identical to the identity – it will be replaced with the identity CLI.

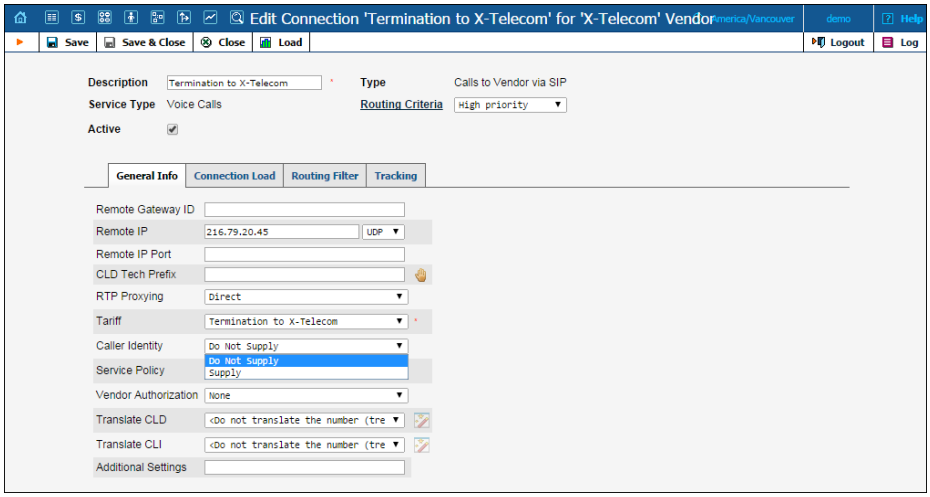
Support for Privacy Flags

A user may sometimes indicate that he wants privacy for a particular outgoing call, i.e. the other party should not see his phone number. This can be done by either activating the privacy settings on the IP phone itself (in this case, the IP phone will include the corresponding RPID header of the SIP INVITE), or by activating the **Hide CLI** feature on the PortaSwitch® side. So when sending the call to a third-party carrier, PortaSIP must show the call information in such a way as to ensure the desired privacy.

Even if an end user requests that his identity be hidden from the called party, some vendors still request that his identification information be sent to them (so they can record this information for various purposes, such as abuse prevention or law enforcement); they will then take care of hiding it from the final recipient.

This actually means that PortaSwitch® must send normal caller information along with a privacy flag that tells the vendor to withhold caller info from the final call recipient.

However, many other vendors do not have the capability to process privacy flags properly. In this case, PortaSwitch® must remove the Caller ID from the call information before sending the call to such a carrier's network. Since a vendor's capabilities in this respect cannot be determined at the time a call is routed to his network, the desired method should be selected in the vendor's connection configuration beforehand. Then the proper method will be used whenever a call with a "privacy" request is sent to that particular carrier.



© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

The basic Caller ID mechanism works much as it does in the case of email. The caller information has a 'From' header field, including the address. For example:

```
From: "John Smith" <sip:1234@sip.example.com>; tag=0099-8877,
```

which means that user John Smith with phone number 1234 is trying to initiate an outgoing call using the 'sip.example.com' server.

When the recipient of a call (the vendor or customer where the call is sent) is marked as "untrusted" (the **Accept/Supply Identity** attribute is set to "No"), PortaSIP replaces the display name in the 'From' field of the outgoing INVITE request ("John Smith" in the example above) with "Anonymous", while the phone number is removed. So the 'From' header field will look like this:

```
From: Anonymous <sip:sip.example.com>; tag=0099-8877
```

Alternatively, if the recipient is marked as trusted, the 'From' field is unchanged; however, an extra header indicating the request for privacy is added to the SIP packet:

```
From: "John Smith" <sip:1234@sip.example.com>; tag=0099-8877,
Privacy: id
P-Asserted-Identity: <sip:1234@sip.example.com>
```

Also, when someone other than the caller uses the PortaBilling® web interface to view call records for calls where privacy has been requested, he will not see the actual phone number.

Service Announcements via the Media Server

A customer might be unable to make a call not only due to network problems, but also for various administrative reasons, for example, if his account is blocked or he does not have enough money on his account. If the end user can be informed of such administrative problems, instead of just being given a busy signal, this will greatly simplify troubleshooting. Here is what would happen in the event that, for instance, an account which is blocked attempts to make a call:

- The customer tries to make a call and sends the INVITE request to PortaSIP®.
- PortaSIP® sends an authorization request to the billing engine.
- PortaBilling® determines that this account is blocked. An authorization reject is returned to the SIP server. In addition to the h323-return-code, a special attribute is sent back to the SIP

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

server. This attribute contains a description of the type of error – in this case, "user_denied".

- The SIP server receives the authorization reject from the billing engine. However, instead of just dropping the call, it redirects the call to the media server, including the error message as a parameter.
- The media server establishes a connection with the SIP UA. It locates a voice prompt file based on the error type and plays it to the user. After this the call is disconnected.

The media server and prompt files are located on the SIP server. So as to avoid dynamic codec conversion, there are three files for each prompt (.pcm, .723 and .729). You can change these files according to your needs, if required.

Here is a list of the currently supported error types:

- **account_expired** – The account is no longer active (expired as per the expiration date or life time).
- **cld_blocked** – There was an attempt to call a destination which is not in the tariff, or is marked as forbidden.
- **cld_dial_error** – A mistake was made when dialing.
- **cld_tmp_unavail** – The account you are trying to contact has configured the incoming call to be dropped, or is out of money.
- **cld_unassigned** – The dialed number is configured to be terminated inside the network, but has not been assigned to any particular user yet.
- **credit_disconnect** – A call is disconnected because the maximum credit time is over.
- **in_use** – This call attempt is blocked because another call from the same debit account is in progress.
- **insufficient_balance** – There are not enough funds to make a call to the given destination.
- **invalid_account** – Incorrect account ID, or account is not permitted to use SIP services.
- **empty_routing** – An outgoing call could not be established because an empty routing list was returned by billing (probably the customer's routing plan is too restrictive).
- **user_denied** – The account is blocked.
- **wrong_passwd** – An incorrect password has been provided.

Every account in PortaBilling® has a "preferred language" property, which defines the desired language for IVRs. The language code (e.g. `ch` for Chinese) assigned to the account is returned from the billing engine, so the media server will first attempt to play a voice prompt for that language. If that prompt does not exist, the default (English) voice prompt will be played.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

NAT Keep-alive

When a SIP phone behind NAT registers to the SIP proxy, the NAT router creates an internal "tunnel" between LAN and WAN, passing all communication for this network connection back and forth between the client and the server. If no packets are sent in either direction over a certain period of time, the NAT router regards the connection as terminated, and removes this "tunnel". If an IP phone behind NAT sends data for this connection, a new "tunnel" will be created and the functionality restored. However, if the SIP server tries to send data (incoming call information) after the NAT "tunnel" has been closed, NAT will reject these packets (since it has no information as to where they should be sent on LAN). This may create problems, because if a NAT router removes a "tunnel" too soon, an IP phone may not receive some incoming calls.

To prevent this situation, PortaSIP includes the NAThelper module, which periodically sends small "ping" packets to registered SIP phones. These packets are small, and so do not create any significant network traffic; but they are sent often enough so that the NAT router keeps the connection open.

Keep-alive Call Monitoring

When a SIP phone goes offline during a phone conversation (e.g. an Internet line is down), the SIP server may not be aware of this fact. So if the remote party does not hang up (e.g. there is an automated IVR, or a problem with disconnect supervision) this call may stay in the "active" state for a long time. To prevent this situation, PortaSIP has a keep-alive functionality.

- Customer A tries to call B, and the call is connected.
- While the call is in progress, PortaSIP periodically sends a small SIP request to the SIP phone.
- If the phone replies, this means that the phone is still online.
- If no reply is received, PortaSIP will attempt to resend the keep-alive packet several times (this is done to prevent call disconnection in the case of an only temporary network connectivity problem on the SIP phone side).
- If no reply has been received following all attempts, PortaSIP will conclude that the SIP phone has unexpectedly gone offline, and will disconnect the other call leg and send an accounting record to the billing engine.
- Therefore, the call will be charged for call duration quite close to the real one.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

First Login Greeting

This feature is not directly related to call processing, but will give your PortaSwitch-based VoIP service a competitive advantage. When a customer unpacks his new SIP phone and connects it to the Internet, the phone will start ringing. When the customer picks up the phone, he will hear a greeting (recorded by you) congratulating him on successfully activating his VoIP service and giving him other important information.

If the customer does not answer the phone (e.g. he has connected his SIP adaptor to the Internet, but has not connected the phone to it yet, and so cannot hear it ringing) PortaSIP will try to call him back later. Of course, after the customer has listened to the message once, his first usage flag is reset, and no further messages will be played.

Voiceover Announcements

Residential VoIP / hosted IP-PBX services initially followed the traditional telephony (POTS) service model: pick up the handset, dial, get connected, and talk.

To make the services even better, PortaSwitch® allows the introduction of additional features to traditional residential VoIP and hosted IP-PBX services that are difficult to provide over traditional telephony. Some of these are:

- Announcing the maximum allowed call duration at the beginning of the call.
- Announcing that the call is about to be disconnected.
- Asking the actual user for authentication by PIN for paid distance calls (for example, if the phone is located in a public place like conference room or hotel hall), etc.

Call flow

- User places an outgoing call to some destination from their IP phone (1).
- The call initiation request is received by PortaSIP® cluster and forwarded to one of the available processing nodes (2).
- The processing node sends an authorization request to PortaBilling® (3).
- PortaBilling® determines that the call must be processed via a special IVR application (as opposed to sending the call directly to the destination) and provides the instruction to forward the call to the Media Server component of the processing node (4).

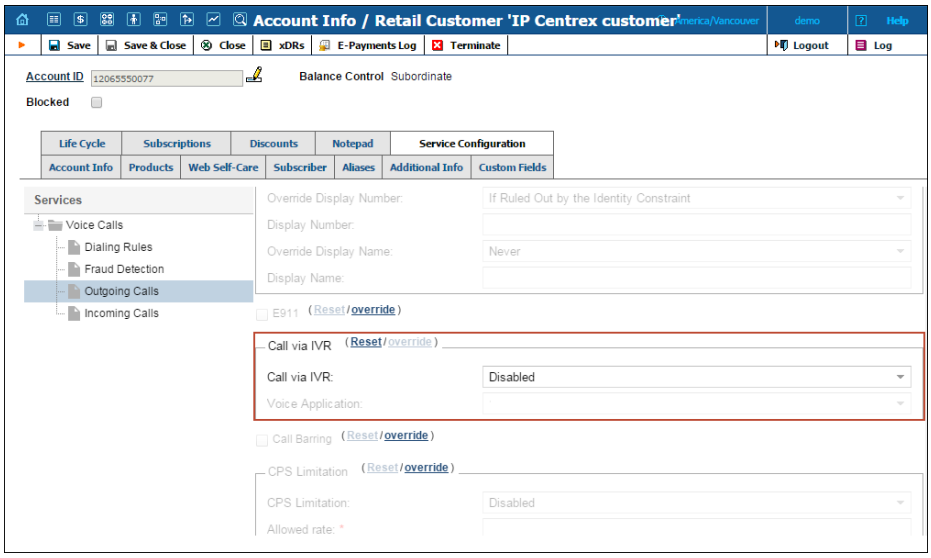
© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

- Upon receiving the call, the Media Server launches the call control application, which establishes a media connection between the user's IP phone and the Media Server (5).
- The call control application sends an additional authorization request to PortaBilling® (6) and receives back the necessary information about the caller, for instance the amount of currently available funds (7).
- The outgoing call is sent again to the dispatching node (8), from where it is routed as any other outgoing call to the final destination using one of the available carriers (9).
- When the call is answered by the called party, the other portion of the media connection is established (10) and the call control application connects the caller and the callee. The media stream still travels via the processing node, so it can intervene at any moment – for instance to announce that the call is about to be disconnected.

Controlling the IVR flow / announcements

The administrator first creates one or more Pass-through IVR applications and configures the options for each application (e.g. whether the maximum allowed call duration should be announced).

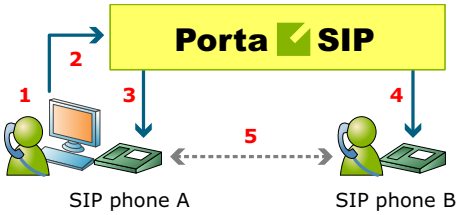
For particular accounts, the administrator configures the **Call via IVR** service feature to control whether the outgoing calls are made in a normal fashion or handled by a media application that would play voice prompts.



© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

SIP TAPI

SIP TAPI is a TAPI driver that enables the SIP click2dial functionality for TAPI applications (like MS Outlook).



- A installs the SIP TAPI driver on his computer (**0**).
- A clicks on the phone icon in his MS Outlook contact list to initiate a call (**1**).
- The SIP TAPI client sends an INVITE to PortaSIP, requesting a call to A's IP phone (**2**), and the IP phone starts ringing.
- A answers his phone (**3**).
- The SIP TAPI client sends a call transfer message to A's phone, requesting an outgoing call to B (**4**).
- B answers his phone, and A and B are connected (**5**).

Please note that SIP TAPI functionality possesses the following idiosyncrasies:

1. The override identity is not supported so the billing engine uses the caller's account ID as a CLI.
2. SIP TAPI supports only default music on hold. Step-by-step instructions for how to configure music on hold in this case can be found in the **Troubleshooting** section of the **Unified PortaSwitch® Handbook Collection.**

Web Call Button

An innovative service that you can now offer using PortaSwitch is web click-to-call. It is intended for customers who are small, medium or large businesses with their own websites, and who use your PortaSwitch for VoIP service. Clicking a special "Call Now" button placed on that website will initiate a call to a pre-determined number (usually the company's call center) directly from the web browser, for a conversation using speakers/microphone.

The end user of the service can be anybody in the world viewing this website, and they make the call free of charge, without the need for a separate IP phone or installing any software on their computer. This is a great competitive advantage for companies looking to find new customers (or maintain their relationship with existing ones) around the world.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

Let's take the example of a tour operator located in Costa Rica which advertises its services on its web page. When a potential customer in the US finds the page via a web search, he may have some additional questions before placing an order. The "traditional" way for him to do this would be to either send an email (which may be too slow) or dial the tour operator's number in Costa Rica (which he may not want or be able to do, since an international call would be too expensive). As a result, it is very likely that being unable to contact the tour operator promptly will lead the customer to keep searching for other alternatives, and so a sales opportunity is lost. One possible solution in this particular situation would be for the tour operator to obtain a US toll-free number which customers can call, but this involves additional costs and only works for specific countries (for instance, a prospective customer from Mexico or Norway would face the same problem as before).

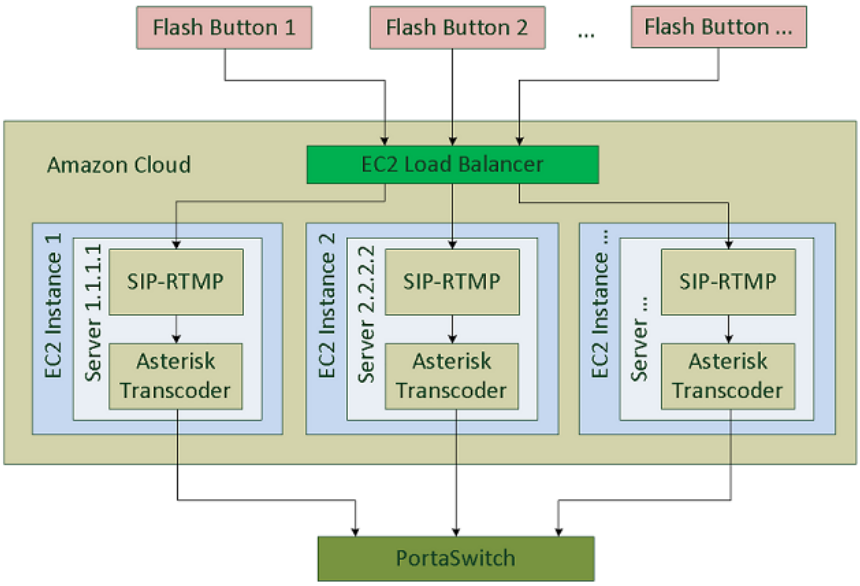
PortaSwitch offers a better alternative: by using a click-to-call control on the website, potential customers can immediately contact the tour operator. This is free of charge for the end user, and there is no cost to the tour operator either (since the call is delivered to their hosted IP PBX environment). So now the tour operator can attract new customers at no extra cost, regardless of where they are located in the world.

Technical details

When the user initiates the call, a Flash applet is launched in his browser. The applet communicates with a voice mediation server using the RTMP protocol. These are servers running in the Amazon Elastic Compute Cloud (Amazon EC2) environment, to minimize hardware costs and allow easy scalability. The voice mediation server then sends a regular SIP call to PortaSwitch, where it is delivered to a pre-determined destination (which may be an auto attendant, a huntgroup, or a phone number provisioned on an IP phone).

There is no call-control program code on the web page visible to the end user, and so there is no possibility of hacking the button to make fraudulent calls (i.e. to a destination other than the one originally intended by the owner of the website).

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com



The code for the button itself is open, under a GPL license (**http://code.google.com/p/siprtmp/**). Asterisk is only required for media transcoding. The streams flow in the following way:

Signal: from Flash plugin (RTMP) via SIP-RTMP (RTMP <-> SIP gateway) to PortaSIP Voip server(SIP rfc 3261)
Media: from Flash plugin (Speex/G.729) via Asterisk (media converter) to SIP client or PortaSIP RTPProxy

Currently, the Flash button can send media using the Speex or G.729 (license required) codecs. Other codecs require transcoding.

Direct Incoming Calls to B2BUA

During the life of a VoIP call, PortaSIP and the remote SIP UA exchange various SIP messages. B2BUA is the originator or recipient of these messages, but every message passes through the SIP proxy. This is necessary for several reasons, the most important of them being the fact that the SIP proxy must perform NAT traversal.

However, if a call arrives from a remote gateway or IP PBX running on a public IP address, NAT traversal is not required, and there is no need to engage the SIP proxy in the SIP message exchange. In this case, B2BUA may accept a direct incoming connection from a remote SIP UA on a public IP address. This is ideal for SIP trunking and similar services. This improvement results in an over 20% decrease in call processing time.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

No special configuration is required on the PortaSIP side, but you should specify your PortaSIP server's port **5061** on your gateway/IP PBX outgoing SIP proxy with IP address.

Incoming Call Delivery to an IP PBX with Dynamic IP Address

When a customer purchases a certain quantity of DID numbers associated with external IP PBX phone lines, all of the DIDs are provisioned as accounts in PortaBilling®. Then the accounts are properly managed and charged for receiving calls.

However, depending on the IP PBX features your customer operates, there are several ways to configure it in PortaBilling® to deliver incoming calls to it from the PortaSIP® server:

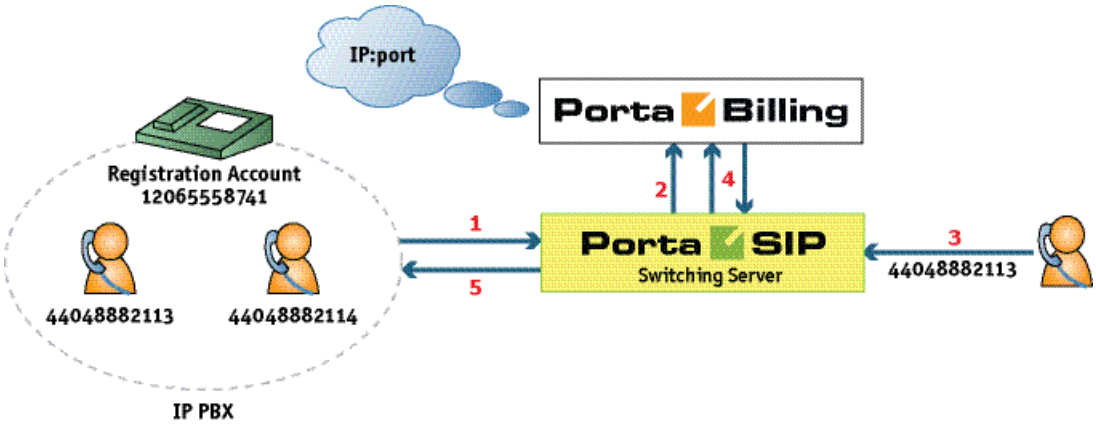
1. The IP PBX registers each phone line separately with its corresponding account on the PortaSIP® server. Then an incoming call to any of the DIDs is routed directly to that number. However, not all IP PBXs support such multiple registrations.
2. In case an IP PBX is located at a static IP address, calls must be delivered to this IP address. Therefore, you can create an account (the **Account ID** can be a DID number used for forwarding calls to the IP PBX) and specify the IP address in the **SIP Static Contact** field. Incoming calls will then be routed to the IP address of the IP PBX and delivered to the corresponding DID. This way each account (i.e. an IP PBX phone line being, as a rule, a DID number) can have its own configuration (e.g. follow-me lists, voicemail, etc.).
3. Usually, however, IP PBXs can only register their main phone lines on the PortaSIP® server. In this case this phone line is provisioned as the registration account (i.e. the account used for registration on the PortaSIP® server) in PortaBilling® and all incoming calls to any of the DIDs are forwarded to this account. This configuration method is frequently used for IP PBXs with dynamic IP addresses.

This last case requires special attention. Using call forwarding for incoming call delivery has some side-effects (it prevents the use of individual forwarding lists for accounts and increases the number of xDRs for a single incoming call). Therefore, it is desirable to directly route all incoming calls to an IP PBX.

This is done by routing incoming calls to an IP PBX with a dynamic IP address via another account (i.e. the registration account). The registration information (`IP:port`) is taken from the registration account and used by

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

the PortaSIP® server to deliver incoming calls to an IP PBX (e.g. a customer has DID number 44048882113 and another one, 12065558741, used as an IP PBX registration account. The IP PBX is registered on the PortaSIP® server with IP address 10.254.302.5. A call to number 44048882113 is delivered to IP address 10.254.302.5).



- When an IP PBX registers with account 12065558741, it sends (1) the REGISTER request to the PortaSIP® server. This request contains the current registration information (`IP:port`) in its SIP contact header.
- The `IP:port` information is taken from the SIP contact header and stored (2) in the database of IP device registrations.
- Someone makes an incoming call (3) to a DID number (44048882113). This call arrives at the PortaSIP® server.
- The PortaSIP® server sends an authorization request to the billing engine. After the usual authorization checks, the billing engine returns the authorization response with instructions to the PortaSIP® server to route this call to the IP PBX (4).
- The PortaSIP® server takes the `IP:port` information (from IP PBX's registration account 12065558741) and routes the call to the IP PBX (5).

Whenever an IP address changes, the IP PBX re-registers with it. Thus, this updated registration information is used for routing incoming calls to the IP PBX on all of the accounts.

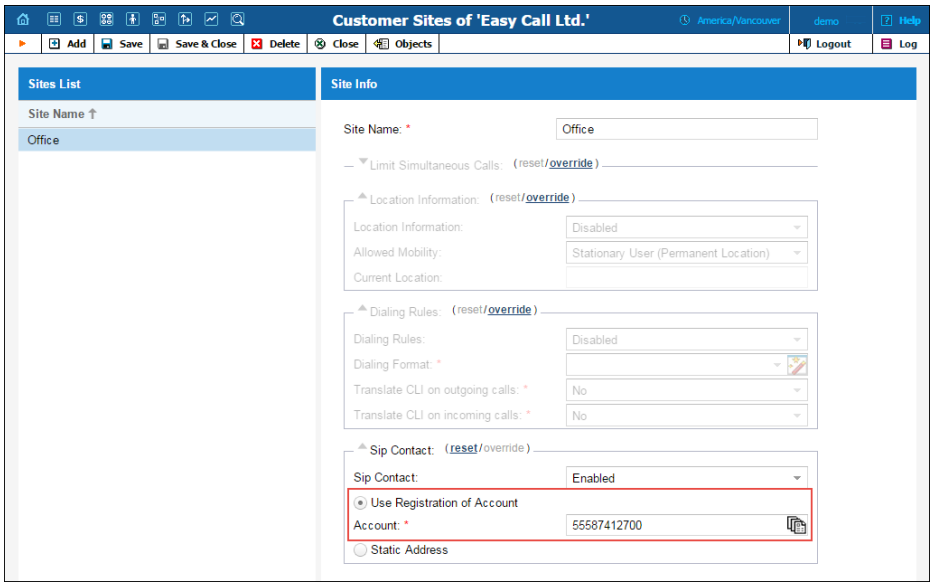
To specify which IP PBX account to use for registration, select it on the customer site. All accounts belonging to this customer site inherit the defined settings.

Consider the following example:

A customer has an IP PBX that uses a dynamic IP address for registration and has 10 DID numbers assigned to it from the range 16045552400 – 16045552409. The administrator configures the IP PBX to register with

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

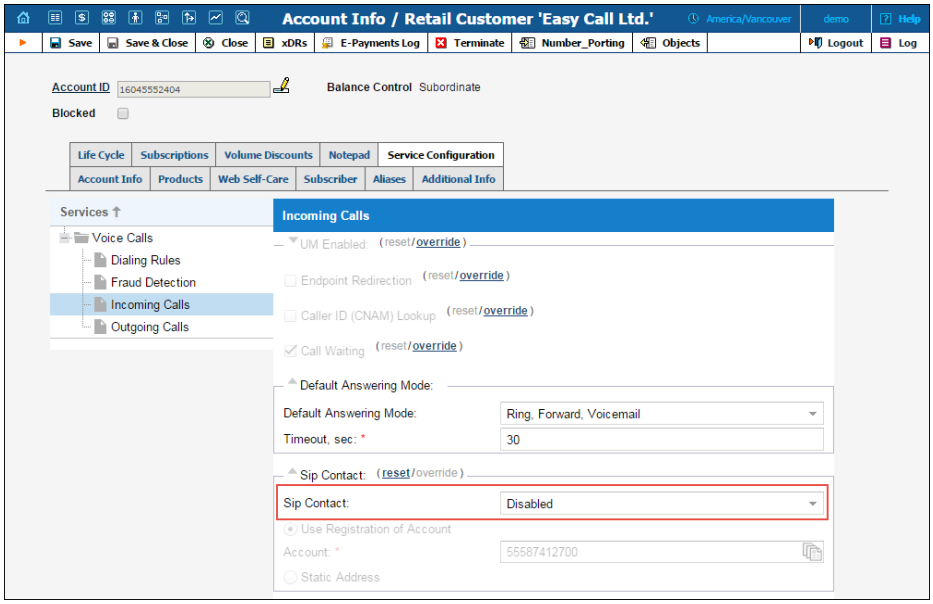
registration account 55587412700 and then creates a customer site for the DID numbers and specifies account 55587412700 in the **Account** field of the **SIP Contact** service feature.



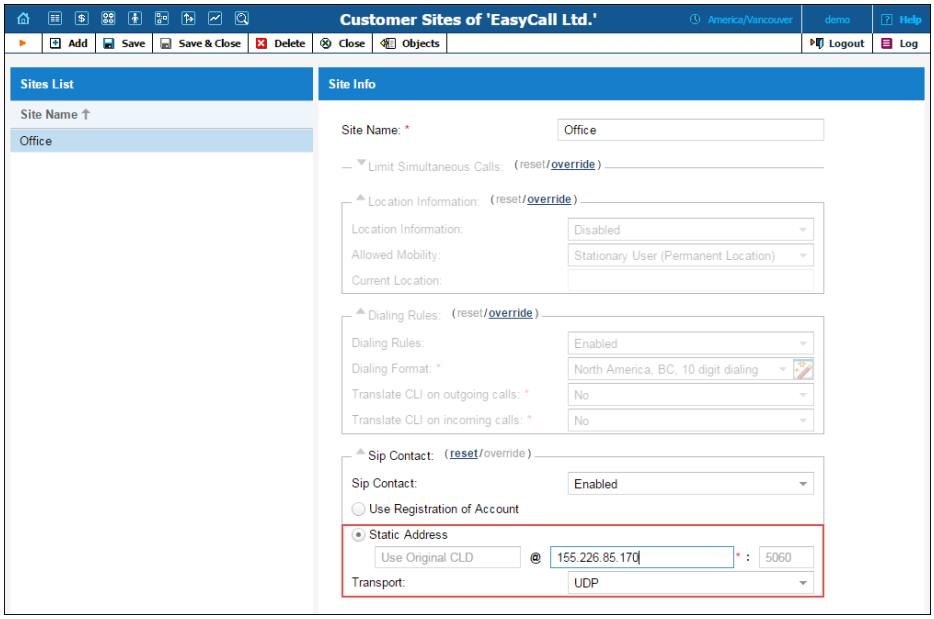
The IP PBX receives IP address 145.163.12.123 from the DHCP server. With this address it registers on the PortaSIP® server by sending a registration request with the SIP contact header 55587412700@145.163.12.123:5060. IP address 145.163.12.123 and port 5060 are taken from the header and saved in the database so that when a call arrives to number 16045552401, it is routed to the following destination 16045552401@145.163.12.123:5060.

Later on the IP PBX is given a new IP address: 20.415.65.4. The IP PBX re-registers with it and sends the new registration request with SIP contact header 55587412700@20.415.65.4:5060 to the PortaSIP® server. Upon successful re-registration, a call arriving at number 16045552401 is now routed to the following destination 16045552401@20.415.65.4:5060.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com



Then suppose the administrator decides to use the number 16045552404 on a separate SIP phone. He disables the SIP contact feature for account 16045552404 and provisions a SIP phone with this account.



Finally, the IP PBX is allocated static IP address 155.226.85.170. The administrator defines the registration with the static address and specifies IP address 155.226.85.170 as a host.

Upon registering the IP PBX, all incoming calls to DIDs are routed to IP address 155.226.85.170:5060.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

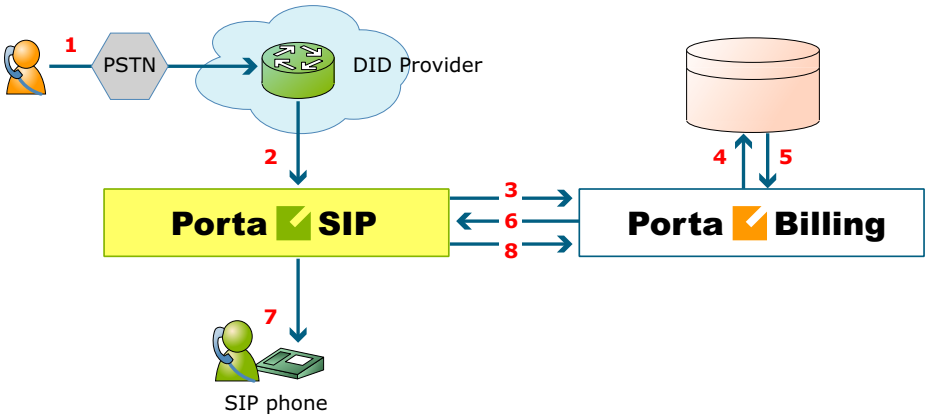
NOTE: When defining that incoming calls for a particular account will be delivered via the registration information of another account, the configuration parameters of the selected account are not considered (e.g. an administrator defines that incoming calls to account 16045552407 will be delivered via account 55587412700. The account 55587412700, in its turn, has a static IP address defined. When someone dials number 16045552407, the system sends the incoming call using the `IP:port` of account 55587412700).

Thus, delivery of incoming calls via the registration information of an account simplifies the configuration of an IP PBX with dynamic IP address, significantly decreasing the administrative load.

ITSPs can provide their customers with SIP trunking services regardless of the way the PBX acquires the IP address for registration.

Calls from Vendor via SIP

In the case of incoming calls from a vendor via IP, there is one further issue: since the call reaches your network via the Internet, potentially anyone could be attempting to send you a call in such a fashion. PortaSwitch must be able to correctly authorize calls coming from your vendors (otherwise these calls will be dropped); yet only calls from a "real" vendor should go through.



- Someone dials a phone number assigned to your customer (1).
- The vendor receives this call from the PSTN network, and sends the call to your PortaSIP server (2).
- PortaSIP sends an authorization request to the billing engine (3), using either a remote IP address or a SIP username as the verification parameter (for more details about these two methods of authentication, see the ***Call Handling Rules*** chapter).
- PortaBilling® will check whether this authorization request is related to a "Calls from Vendor via SIP" connection (4). If there is no match, it assumed to be a normal call from one of your

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

customers, and the call will then proceed according to the standard algorithm.

Otherwise (i.e. if this call is indeed coming via a "Calls from Vendor via SIP" connection), PortaBilling® will compare the username and password supplied in the authorization request with those defined in the vendor account associated with this connection.

- If authentication succeeds (5) (i.e. the call is indeed being sent by your vendor), PortaBilling® will apply the connection's translation rules and check whether the dialed number belongs to one of your accounts (1234). If it does not, the call will be refused (since there has probably been a configuration error, so that the vendor is routing international traffic to your network).
- PortaSIP receives the routing information for the call (6), and so now recognizes that the call should be sent to one of your SIP phones (7). Follow-me, UM parameters and other related information are provided as well. One very important point is that this call will be charged to the account which receives the call.
- After the call is disconnected, the called account is charged for the call (8), and the costs of the call are calculated for the vendor.

Routing Filters

In order for a voice call to be established, the two end-points (IP phones or media gateways) must not only be able to exchange IP packets which contain SIP messages, but also agree on a mutually acceptable way to encode the audio signal for transmission over the IP network (codec). There are many codecs available, with different features in terms of voice quality, compression rate and required processing resources. Some are free, while others require royalty payments. As a result, each device, such as an IP phone, is usually capable of supporting only the limited subset of codecs implemented by the manufacturer.

Normally, at the beginning of a call the calling party announces all the codecs it supports, and then the called party replies back with a list of codecs it is willing to accept, and so the decision is made by the two end-points only. This approach provides great flexibility and, since PortaSwitch does not have to interfere in the audio processing and utilize any codecs on its side, it allows PortaOne to provide you with an unlimited license, without your being responsible for any additional codec royalties. But since the two SIP end-points make the decision regarding the choice of the codec without any consideration of the network infrastructure or other important factors, in some situations their choice may be less than optimal. For instance, SIP phone A may have the G.711 codec as the first preference by default; and if that codec is supported by

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

the other party, it will be chosen for the call. While this is great for a customer A, with high-speed broadband connectivity (G.711 provides sound quality identical to traditional "wired" telephony service, such as ISDN), if customer B attempts to use G.711 with limited bandwidth it will result in severely degraded voice quality and a negative customer experience. Such a customer B should always use a narrow-bandwidth codec such as G.729 to ensure good sound quality.

Thus it becomes increasingly important for the ITSP to actively control the choice of codecs used by the end-points, in order to optimize network performance and avoid negative customer experiences. How is it done?

Routing filters operate with the concept of **call media features**. A call media feature is a property of the call or call media, such as a specific codec, T.38 fax, or the ability to guarantee delivery of the correct CLI (caller identification) to the recipient of the call. Since the caller may have his own set of desired call media features, the main idea is to ensure proper "match-making" between the available carriers, while limiting the caller's choice if required (e.g. the caller may request a video call, but this will be prohibited if he is not authorized to do so).

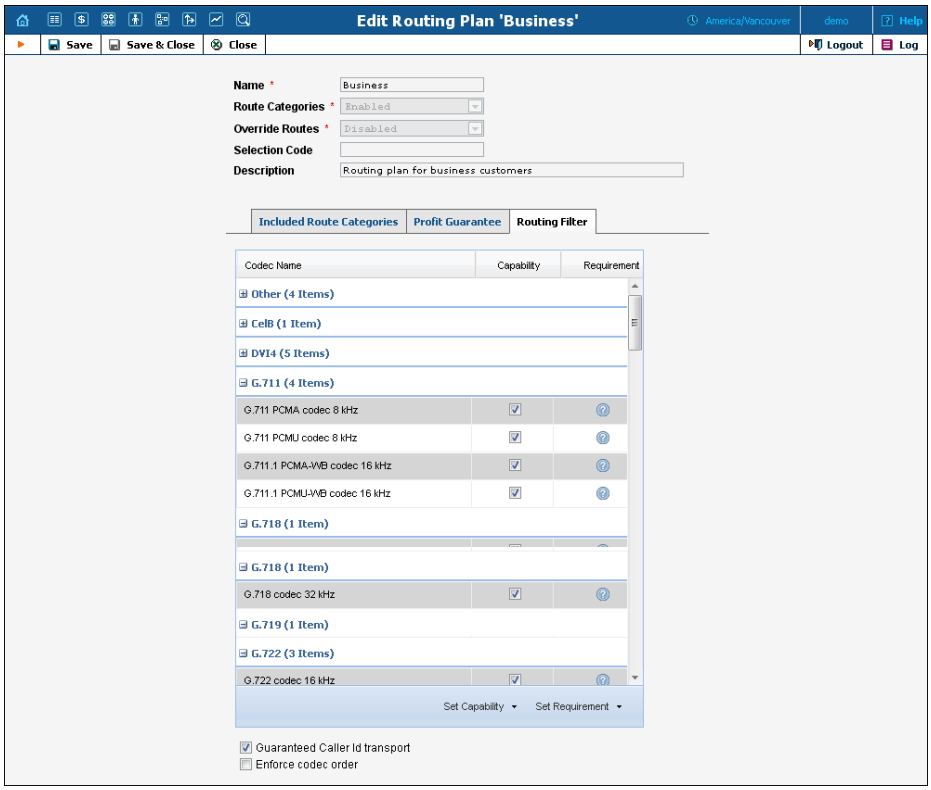
Call Media Regulations

These describe the filters applied to call media features (such as a specific codec or T.38 fax capability), as requested by the calling party. For each feature the PortaSwitch administrator can specify that:

- It is "required" – meaning that the other SIP end-point must have this feature supported in order for the call to be completed.

  For instance, if the "G.729 codec" feature is marked as "required" for an account making a phone call, then only those vendors specifically marked as "guaranteed to support G.729" will be placed in the routing list.
- It is "suppressed" – meaning that PortaSwitch will prevent the use of this particular feature (e.g. G.722 codec) and will not even show the information about this codec in the SIP request when sending an outgoing call to the other end-point.
- It is "not required" – meaning that PortaSwitch does not do any special processing for this feature. It will be included in the outgoing SIP request, and may be used if the other party supports it. This is the default value for any feature.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com



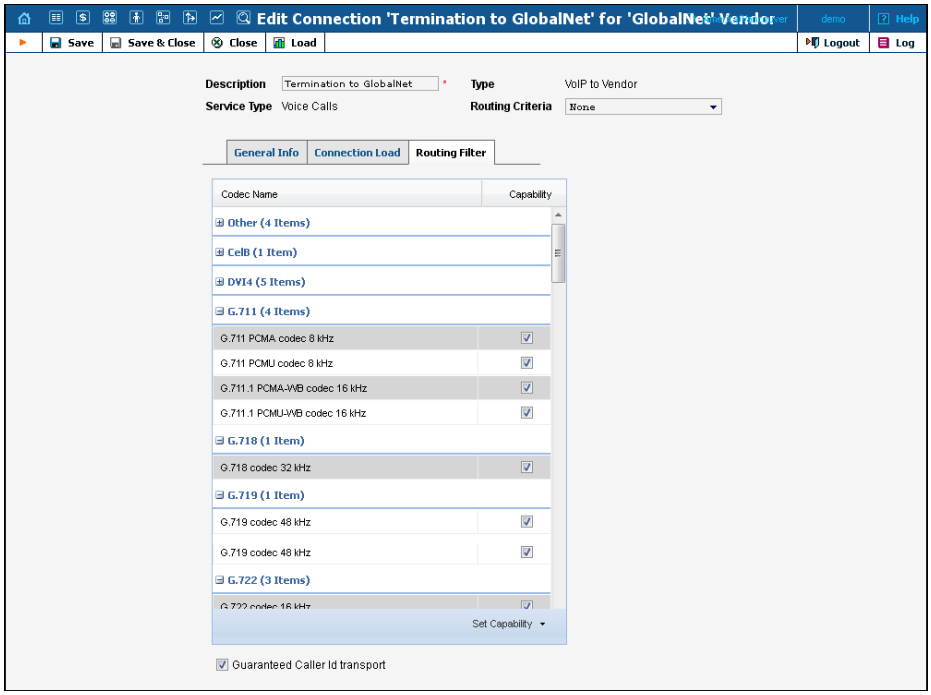
Call Media Capabilities

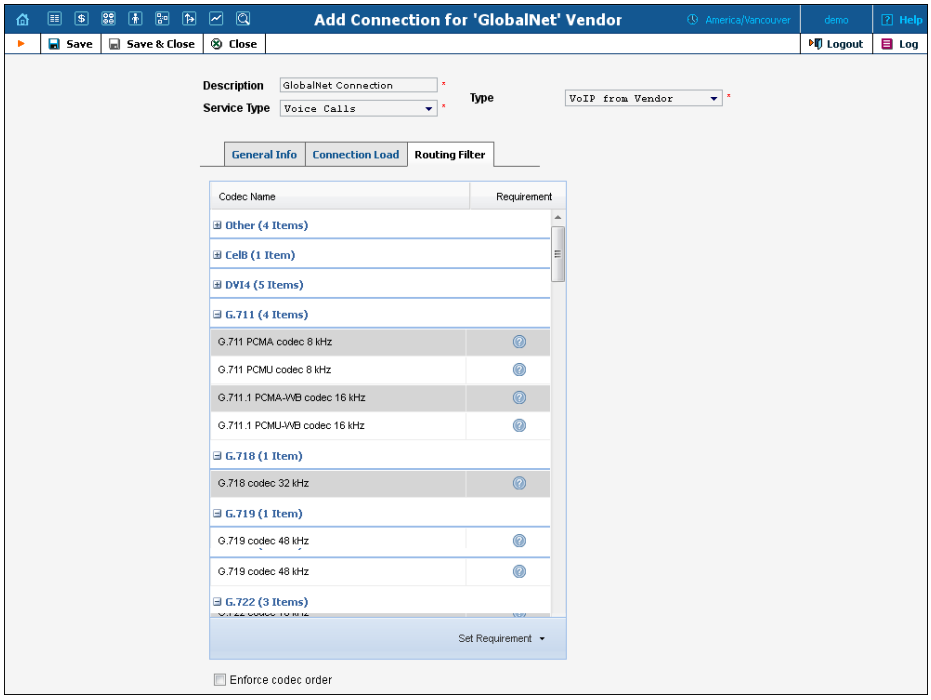
These describe the capabilities of the remote party (such as the gateway of a carrier) and our preferences on using them. For each feature it is specified whether it is:

- Supported – meaning that we know for sure that this equipment supports this feature and are willing to use it.
- Not supported – meaning that this equipment is unable to support this particular feature (e.g. G.723 codec). It could also be our administrator's decision to prohibit it.

  For example, although we do not know whether a vendor's gateway supports the G.722 codec, by marking it as "not supported" we will ensure that, even if the originating end-point shows this codec as available, it will be removed from the codec list sent to the carrier in the SIP call initiation request, and thus never used.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com





Legal Call Intercept

As an ITSP you may be requested to enable law enforcement agencies to monitor a certain subscriber's calls. This may be required in accordance with the Communications Assistance for Law Enforcement Act of 1994

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

(CALEA) or some other law applicable in the country where you provide services.

You can activate the Legal Intercept call feature in PortaBilling® for every account that requires it (obviously, this feature is only accessible from the administrator interface, and is not visible to the end user). When this is done, PortaSIP will be instructed to engage the RTP proxy for every outgoing or incoming call to this account, regardless of other NAT traversal settings, and will produce a complete call recording of the conversation.

The call recordings may then be delivered to the law enforcement agency by any applicable means, or you may even provide real-time access to the location on the PortaSIP server where these files are stored.
In the specific case of CALEA, there are many requirements which an ITSP must comply with, many of them not even related to technical capabilities, but rather purely to administration, e.g. personnel dealing with intercept data must have an appropriate security clearance. So the optimal solution for ITSPs using PortaSwitch is another option described by CALEA, i.e. going via a "trusted third party". At present, PortaSwitch has been successfully tested with the "Just in Time" product from NeuStar's Fiduciary Services.

Secure Calling

By default, PortaSIP communicates with IP phones using the UDP protocol, so the contents of network packets exchanged between the server and endpoints are unencrypted. Therefore, if a third party can receive the packets (e.g. by being connected to the same Ethernet segment and running a network "sniffer" program), it can effectively see who is being called and listen to the whole conversation.

In order to prevent a third party being able to see SIP signaling information (e.g. call parameters such as the destination number), it is possible to use SIP over TLS. In this case, communication between the IP phone and PortaSIP is fully encrypted and cannot be decoded.

In order to ensure that nobody can listen to the actual voice conversation (transmitted as an RTP stream) the two IP phones can be configured to use the Secure Real-time Transport Protocol (SRTP RFC 3711) instead of basic RTP. The phones will then exchange voice data in an encrypted form, with PortaSIP simply passing packets from one phone to another, without analyzing the contents. Naturally, features such as call recording or music on hold will not be available for such conversations, since PortaSIP will not know the decryption key programmed into the IP phones.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

SIP Over TLS

This feature allows communication between an IP phone and PortaSIP® to be encrypted so that it cannot be intercepted. This prevents a third party from being able to see SIP signaling information (e.g. call parameters such as the destination number).

Media Encryption in PortaSwitch®

These days the telecommunications market demands that secure calls be provided. If a user connects to a public WiFi hotspot and establishes a call from his soft phone, it is possible that a third party could intercept and / or listen in on the conversation. Therefore, it is necessary to protect such calls and guarantee their security by means of media encryption.

Another situation might be that a call established from an application that strictly requires media encryption reaches a phone that does not support media encryption.

To handle such cases and enable calls among devices with different capabilities to go through, PortaSwitch® now performs intermediate media encryption. The system can be configured so that:

- PortaSwitch® encrypts the media stream during a call and proxies it to a user's device,
- PortaSwitch® decrypts the media stream received from a user's device before sending it to another party, or
- The media stream is encrypted by phones that use the Secure Real-time Transport Protocol (SRTP RFC 3711) instead of basic RTP. The encrypted media occurs directly among phones or is relayed by PortaSwitch® without decryption (the so-called fully private call).

Let us have a closer look at the possibilities in more detail.

Media Encryption by PortaSwitch®

The key distinction of calls encrypted by PortaSwitch® is that the RTP proxy always mediates the RTP media stream. This provides the RTP proxy with encryption keys, thus making it possible for a calling party's media to be encrypted and then decrypted for a called party and vice versa. More complex call scenarios where a media stream must be encrypted for both call participants and their phones use different key agreement protocols that are also supported.

Consider the following example:

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

John Doe calls his wife Jane from a phone that works only with encrypted media and supports encryption by zRTP. Jane's phone, however, supports only SDES encryption. When the system authorizes the call, it detects that the media must be encrypted for both John and Jane and that the encryption methods differ. During the call, the media stream passes via the RTP proxy which has two sets of encryption keys. This allows PortaSwitch® to receive encrypted media from John's phone, decrypt it with the zRTP encryption keys, encrypt it using SDES encryption keys and send it to Jane's phone.

Fully private calls

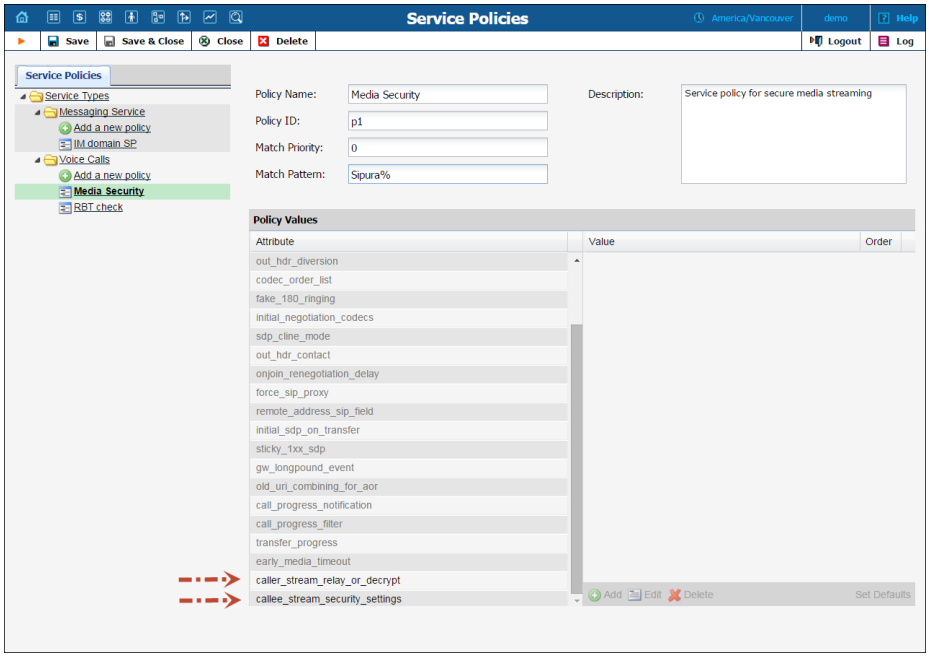
During fully private calls the media stream is solely encrypted by users' phones and delivered directly between these phones. If any of the phones is on a private network and the RTP proxy is involved in the call, it relays the media stream only, without decryption.

When establishing a fully private call, one must remember that:

- Both phones must support the same key agreement protocol;
- Since data is encrypted without the participation of PortaSwitch®, account settings such as call recoding and music on hold are ignored since PortaSwitch® cannot decrypt the media stream.

Whether media encryption by PortaSwitch® is required, and for which call participant: the called party, the calling party or both, is defined by the service policy configuration. The following service policy options: **caller_stream_relay_or_decrypt** and **callee_stream_security_settings** define the security settings for both the calling and called party, respectively.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com



Security settings, however, are applied separately to the calling and called parties. Thus, media stream processing for a calling party can be configured as follows:

- **forced_relay** – PortaSwitch® relays the media stream received from the calling party and ignores the called party's settings. The media features for the account such as music on hold, music on waiting and call recording are not available if the relayed media stream is encrypted;
- **relay_or_decrypt** – This is the default setting. PortaSwitch® relays any type of media stream received from the calling party if it is allowed by the called party's settings. Otherwise, the media stream is encrypted / decrypted;
- **decrypt** – PortaSwitch® always decrypts the media stream received from the calling party.

The following are media stream processing configuration options for the called party:

- **as_caller** – This is the default setting. PortaSwitch® relays any type of stream received from the calling party. The media features for the account such as music on hold, music on waiting and call recording are not available if the relayed media stream is encrypted;
- **decrypted** – PortaSwitch® always decrypts / encrypts the media stream for the called party;
- **sdes** – PortaSwitch® always performs media stream encryption for the called party using the SDES protocol;
- **dtls** – PortaSwitch® always performs media stream encryption for the called party using the DTLS protocol;

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

- **zrtp** – PortaSwitch® always performs media stream encryption for the called party using the zRTP protocol.

The decision to encrypt or relay a particular call depends on the security settings for the call originator. This allows you to fine tune the system for each specific case.

The results of the security setting configuration for both calling and called parties are provided in the table below:

caller_stream_relay_or_decrypt	**callee_stream_security_settings**	**Encryption for the caller device**	**Result**	**Media Features**
forced_relay	decrypted, as_caller, sdes, dtls, zrtp	requested	Caller <-> Relayed via PortaSwitch® or sent directly <-> Callee	No
		no	Caller <-> Relayed via PortaSwitch® or sent directly <-> Callee	Yes
relay_or_decrypt	**as_caller**	requested	Caller <-> Relayed via PortaSwitch® or sent directly <-> Callee	No
		no	Caller <-> Relayed via PortaSwitch® or sent directly <-> Callee	Yes
relay_or_decrypt	decrypted	requested	Caller <-encrypted-> PortaSwitch® <-non-encrypted-> Callee	Yes
		no	Caller <-> Non-encrypted stream relayed via PortaSwitch®<-> Callee	Yes
relay_or_decrypt	sdes, dtls, zrtp	requested	Caller <-encrypted-> (Encrypt 1) PortaSwitch® (Encrypt 2) <-encrypted-> Callee	Yes
		no	Caller <-non-encrypted-> PortaSwitch® <-encrypted-> Callee	Yes
decrypt	as_caller, decrypted	requested	Caller <-encrypted-> PortaSwitch® <-non-encrypted-> Callee	Yes
		no	Caller <-> Non-encrypted stream relayed via PortaSwitch® <-> Callee	Yes

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

decrypt	sdes, dtls, zrtp	requested	Caller <-encrypted-> (Encrypt 1) PortaSwitch® (Encrypt 2) <-encrypted-> Callee	Yes
		no	Caller <-non-encrypted-> PortaSwitch® <-encrypted-> Callee	Yes

The following key agreement protocols are supported:

- SDES;
- DTLS;
- zRTP.

Each key agreement protocol has its own distinctive features yet the general flow is the exchange of cryptographic parameters between a device or an application and the RTP proxy.

Session Description Protocol Security Descriptions (SDES)

When using the SDES key agreement protocol, the exchange of cryptographic parameters is performed during call initiation. The device that uses this key agreement protocol sends a set of randomly generated encryption keys to PortaSIP® with the initial INVITE request. The RTP proxy negotiates one of the keys for media decryption and generates the local encryption key that is then delivered to the device in the confirmation response. These are the keys used for RTP media stream encryption.

When using the SDES key agreement protocol, SIP signaling support over TLS in PortaSwitch® must be enabled and the device's secure SIP signaling must be configured, accordingly.

Datagram Transport Layer Security (DTLS) protocol

The DTLS key agreement protocol is based on the Transport Layer Security (TLS) protocol. During call initiation, the user's device and PortaSIP® exchange IP:port information (just as for a regular RTP session). The negotiated IP:port pair is used to establish a secure DTLS connection which is the TLS over UDP plus special SRTP extension. Once established, it is used to negotiate cryptographic parameters. Those parameters are then used to establish a secure RTP media stream.

zRTP

The zRTP key agreement protocol is similar to the DTLS. PortaSIP® establishes a direct media path to the user's device for the cryptographic

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

parameters exchange. However, it does not require the involvement of signaling when establishing a secure media communication.

After the cryptographic parameters are exchanged, they are used for the RTP media stream encryption.

No matter the method, the encryption keys are unique for each session. This is what eliminates the chance for a call to be intercepted and decrypted.

At present, media stream encryption is only supported for ordinary calls. Support for "complex" calls such as those that involve call pickup, call transfer, etc. will be added in future releases.

PortaSwitch® media stream encryption increases call security and protects users from unwanted interception activities. It allows administrators to manage security settings for accounts, thus making it possible to provide secure calls among phones that have different capabilities.

With this functionality added, PortaSwitch® can be easily integrated with WebRTC applications, thereby increasing the service provider's competitiveness in the market.

Tools for Prevention of VoIP Fraud

PortaSwitch® supports a set of tools to prevent VoIP fraud, i.e. a situation where an attacker uses credentials stolen from a customer's IP PBX or end-point and sends unauthorized voice traffic to your network.

There are two main approaches for distinguishing between the activity of a legitimate user and a hacker:

- Deviation in usage patterns.
- Deviation in the location from which the service is used (geo-IP).

The current version of the fraud protection module in PortaSwitch uses the location deviation method. This enables prevention of the majority of attacks without allowing a single fraudulent call to pass through, so there is zero loss for the service provider (or the customer). We plan to add real-time analysis of usage patterns in the next releases, to allow even better control and proactive prevention of those rare scenarios where location analysis may not yield sufficient results.

Geo-IP Fraud Prevention

If a hacker obtains the valid credentials of one of your customers, he can then send a call from his network using this username and password and

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

even the identification of the SIP phone type. The only piece of information that cannot be easily changed by a hacker is his actual IP address. Although it is not always possible to determine a user's exact location (e.g. street address) from his IP address, information regarding the country and the ISP that owns the IP address (and leases it to the end user) can be determined in the overwhelming majority of cases by using the database of IP address assignments (geo-IP database).

The key element in geo-IP fraud prevention is the assumption that, under normal circumstances, the majority of users will use your service from the same country (and the same region in that country). For instance, a VoIP user in Barcelona, Spain, connects to the Internet via DSL provided by Telefonica. Although his IP address is assigned dynamically by the ISP and may change, the "location" of that address will always point back to Spain. Even if he changes his ISP to Orange, his IP address will still refer to Spain. Usually, larger customers who use SIP trunking services are the primary target for hackers, since they have higher credit limits and are authorized to send larger numbers of simultaneous calls. By using the credentials of such a customer, a hacker can send a significant amount of traffic in a relatively short time period. Fortunately, geo-IP fraud prevention is especially accurate for this type of customer. A residential user may take his SIP phone with him to a different country while on vacation, but it is very unlikely that a company will frequently move their office (and IP PBX) to a different country.

When launching the service, the service provider creates one or more **Geo / Risk Profiles**. Each profile divides the list of all the countries in the world into three zones:

- No Restrictions – A country (or countries) where users intend to use the service. Service usage is allowed without restrictions.
- Suspicious – Countries where it would be unusual (but still possible on a relatively low number of calls) for a customer to use the service without screening. Then any attempt to make an outgoing call from a country listed here will be screened, where he or she must provide additional credentials to prove that this is indeed a legitimate user.

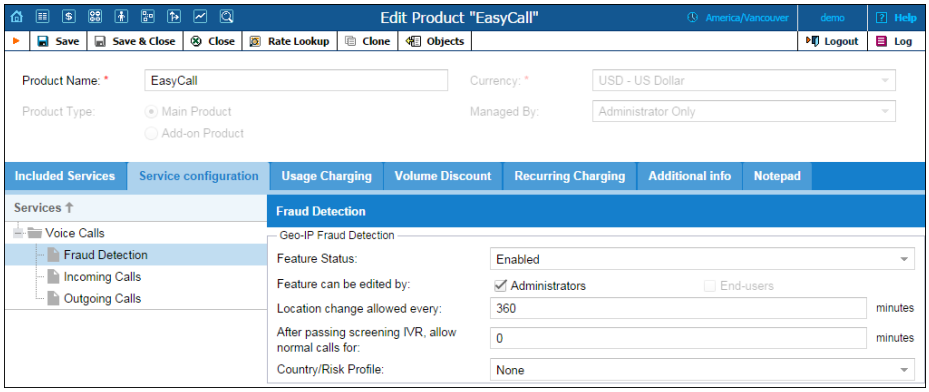
Note: the number of calls that can be made without screening is 5 by default and can be configured on the Configuration Server.

- High-risk – Any usage attempt from these countries will be treated as a potential security breach and immediately screened, where the customer must provide additional credentials to prove that this is indeed a legitimate user.

Naturally, the actual selection will depend on the area where the service provider sells the service and what type of service it is. For instance, an ITSP selling business SIP trunking services in London may define the

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

United Kingdom as the "normal" service location, and everyplace else as restricted, since all of their customers are actually based in the UK. Another ITSP, selling residential VoIP calling via a communication client on a smart phone will define the United Kingdom, France and Spain as normal locations (since they actively advertise their product in these countries and most of their customers are there). In this case, the majority of countries in the world will be listed as "suspicious." Finally, those countries from which the service provider sees an increased amount of hacking attempts will be declared "high-risk."



Next, Geo-IP Fraud Detection can be enabled in individual products, thereby allowing IP verification to be performed for all accounts, using this product. This allows you to apply Geo-IP verification to business and residential VoIP products, and skip it for other products (for backward compatibility or simply because it does not fit the business model, for instance for a service similar to Skype, where users can register and use the service anywhere in the world.

Alerts about suspicious activities

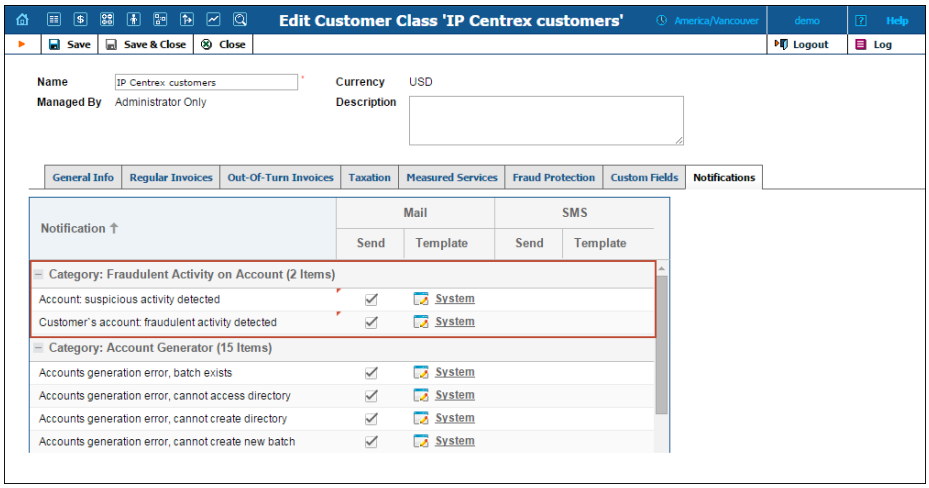
Time is critically important when a fraudulent incident occurs. The sooner one acts, the better chance they have to mitigate possible losses.

PortaSwitch® provides notifications to alert customers whenever the following events take place:

- A call made from a customer's account originates from a high-risk location and is therefore redirected to the screening IVR. The account's status is changed to **Screened**.
- A call made from a customer's account originates from a high-risk location and is therefore immediately rejected. The account's status is changed to **Quarantined**.

To automatically notify your customers about these events, the **Fraudulent Activity on Account** notification templates must be enabled in the customer class.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com



When customers are promptly notified about suspicious activities, they are able to detect fraud early and take necessary protective measures to avoid possible losses.

Country Blacklist

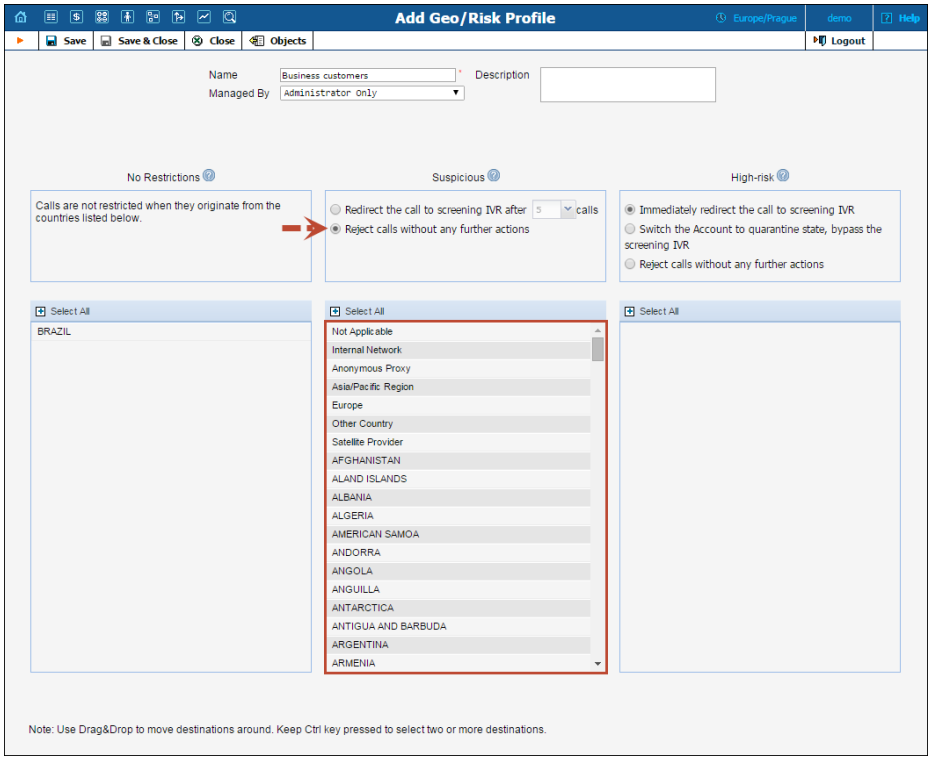
If the service provider wants to block calls originating from countries known for high fraud potential and the screening of calls by means of IVR is unacceptable, the Country blacklist functionality is the one to use.

This functionality immediately drops calls that come from blacklisted countries. While fraudulent calls are rejected, calls originating from trusted countries come through without restrictions.

Consider the following example. A customer who is a wholesale provider is located in Brazil. He wants to allow calls only originating from Brazil and deny calls originating from any other country. As many calls are sent simultaneously, screening calls by means of IVR is not optimal.

For this customer, an administrator configures the Country blacklist to include all countries except Brazil. After a while, a Chinese hacker hacks this customer's account and attempts to send calls to expensive destinations. PortaSwitch® detects that the account is attempting to send calls from a Chinese IP address and since China is present in the Country blacklist, these fraudulent calls are rejected, although calls from Brazil come through without any restrictions.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com



With Country blacklist functionality, service providers can offer more enhanced fraud protection to their customers – including the ability to consistently drop calls that originate from countries with a high fraud risk and to continue sending calls from trusted countries only.

Account Attributes

The default setting for an account is "stationary," meaning that the system expects the account to always be used in the same location. A change of country (location) is immediately considered a potential security breach. The alternative is to mark some accounts as "roaming," in which case, the system allows for a greater number of location changes. This can be useful for customers who travel frequently and use mobile devices to communicate with clients. To reduce the amount of false alerts, a change in location will be considered acceptable in such cases. However, this will make it more difficult to detect actual fraudulent activity.

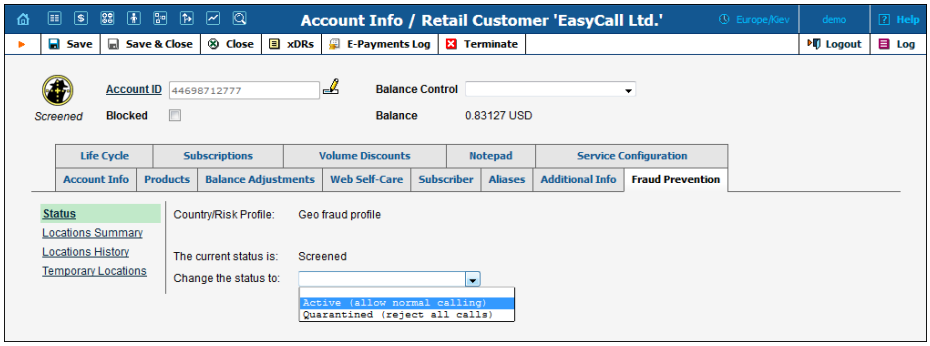
Two additional conditions may be introduced for an account:

- **Screened** – This means that some unusual activity has been detected for this user. An attempt to make an outgoing call will connect the user to a screening IVR, where he or she must provide additional credentials to prove that this is indeed a legitimate user.
- **Quarantined** – This means that after being screened, this account was unable to supply valid credentials and is still generating a large

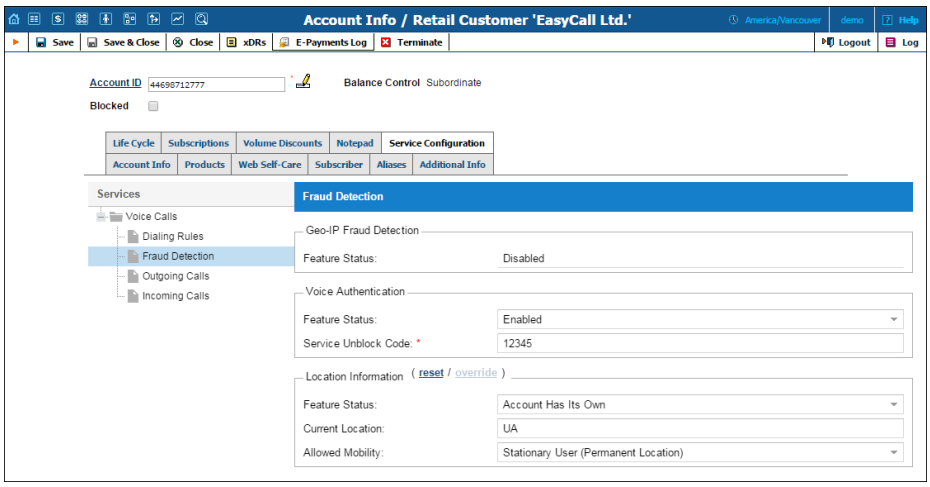
© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

number of call attempts. In order to reduce the load on your network, all such call attempts will automatically be blocked.

Every account is assigned a "default" location. An administrator may override this country selection in order to allow a legitimate user to keep using the service in a country that is otherwise considered "unsafe."



Finally, each account is assigned its own unique "service unblock" code. This is provided to the customer upon sign-up, and can be used later to confirm that a legitimate customer is attempting to make a call, therefore allowing that call from a "suspicious" location.



Call Filtering

For each incoming call, the system analyzes the combination of the account's status, its default location, and the location from which the call is made.

- Any call from a quarantined account is immediately rejected.
- A call from a screened account is redirected to the screening IVR.
- If a call is made by a stationary account but the country of its current location does not match the default country, the call will be screened. If a stationary account does not yet have a default

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

country assigned (e.g. a newly created account), the call is allowed *only* if the current country location is not on the High-risk list.
- For roaming accounts, the call is allowed if the current country location matches the default country, or if the current country location is on the No Restrictions or Suspicious list.
- In all other cases, the call will be screened.

Screening IVR

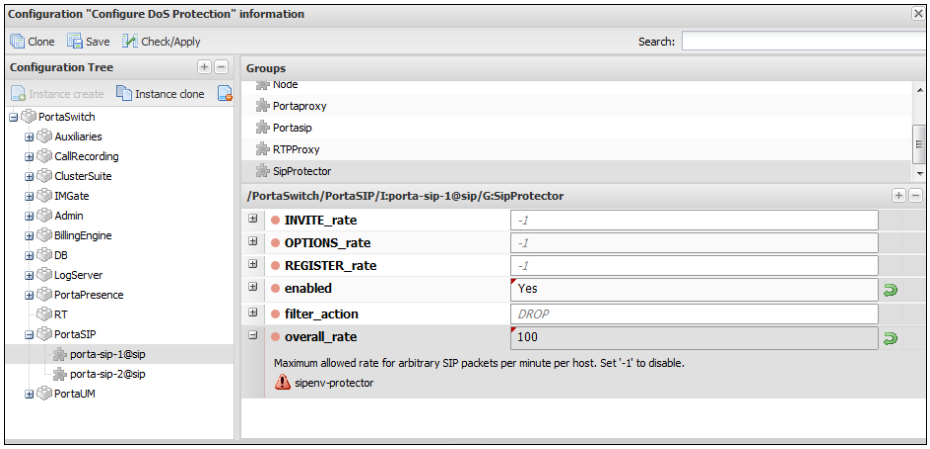
Clearly, blocking outgoing calls on any suspicion will create a negative experience for end users. A genuine customer may take his SIP phone on an overseas trip to see his family, or a businessman may need to make a very important call while transiting an airport in an "unusual" country. The screening IVR is designed to allow legitimate customers to continue making calls in situations where their activity is considered suspicious.

- The screening IVR announces that the user's call cannot be completed because of a potential risk of unauthorized usage.
- It asks the user to re-enter the random 3-digit code he will hear. This is done to confirm that there is a live person on the line. (Hackers often use auto-dialers to test vulnerabilities in a network or generate calls to premium numbers.)
- Then the user must enter the "service unblock" code provided to him when he signed up for the service. If the unblock code is entered correctly, the system will automatically connect the user to the originally dialed number (there is no need to re-enter the number).
- If there are multiple unsuccessful attempts in the screening IVR, the account will be switched to "quarantined" status. This (along with the 3-digit "live human" verification) prevents a hacker from using a script to find the unblock code by "brute force" and continue sending traffic.

Protection from DoS Attacks

Denial-of-Service (DoS) attacks are fairly common in the VoIP world and a service provider must take proactive measures to ensure that service is not affected. The PortaSIP DoS prevention feature utilizes the server's built-in firewall to prohibit network traffic coming from specific IP address once it sends too many requests (beyond the reasonable amount that would be generated by a legitimate SIP phone, proxy or gateway). The management interface for the module is really easy to configure via the Configuration Server web interface.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

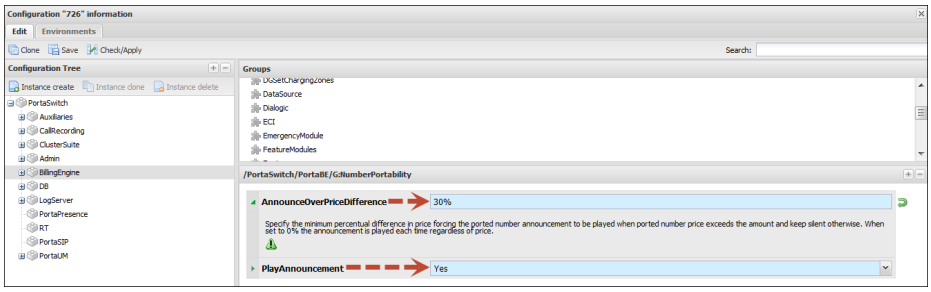


You may configure the maximum amount of SIP requests that will be accepted from every IP phone, or set a limit for INVITE / OPTIONS / REGISTER SIP requests separately. SIP requests that go above the limit can be dropped or logged for future investigation.

You can increase the security of your network and prevent service outages because of a SIP request flood (whether intentional or unintentional.) Future releases of this feature will be improved to provide white lists and message flooding monitoring.

Special Prompt for Calls to Ported Number

With this feature, a prompt is played that signifies a change of price for a call to a ported number if the new price is higher than the old one by a defined percentage.



To set up the configuration, access the **Number Portability** group on the configuration server. By default, the **PlayAnnouncement** feature is off. To activate it, select "Yes" in the corresponding field.

In the **AnnounceOverPriceDifference** field, specify the percentage value to designate the percentage threshold upon which the prompt will be announced.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

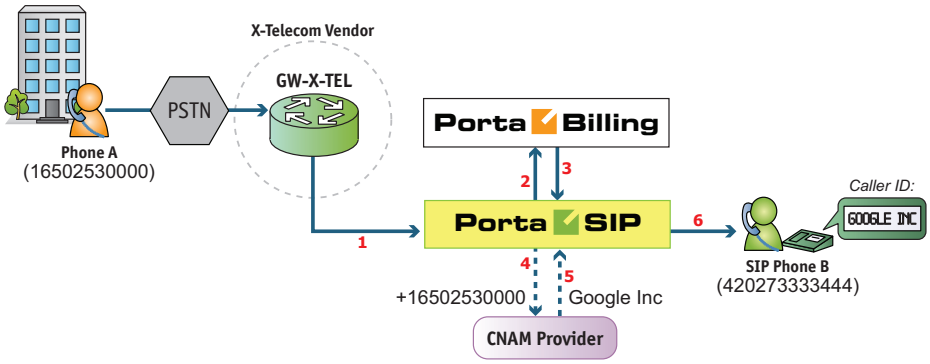
NOTE: By default, the value for the **AnnounceOverPriceDifference** field is "0." This means the announcement is played each time the user calls a ported number, regardless of the price change.

Let's consider the following example: the feature is activated and the value for **AnnounceOverPriceDifference** is 30 percent. An account is making a call to a ported number. During call authorization PortaBilling® detects that the called number has been ported and checks the difference in price for before and after porting. If the difference is within 30 percent, the prompt will not be played; if the difference is greater than the threshold a prompt with a warning will be announced.

Caller ID (CNAM) Lookup

Ordinarily, when somebody calls you, the only caller information available is the caller's phone number. This is often not enough. Sometimes an unwanted call may get through and you may want to avoid the conversation. It is therefore important to see not only the original caller's number but also the caller ID (name and surname, or company name that owns the number).

Integration with a CNAM provider lets you offer the **Caller ID Lookup** feature to your customers so that they can see the caller ID information and respond accordingly. Currently PortaSwitch® is integrated with **OpenCNAM**, which supports numbers from the USA and Canada.



When an incoming call arrives to PortaSIP® (1), it sends an authorization request to the billing engine (2) and checks whether the account receiving the call has the Caller ID Lookup feature enabled (3). If enabled, PortaSIP® sends a request with the caller number to the CNAM provider (4) and receives the caller ID in response (5). The caller ID is then shown on the recipient phone's display (6).

This feature can be enabled for each account on the account's **Service Features** tab. Note that if both caller and the party called are two separate accounts within a specific IP Centrex environment, then a CNAM request

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

will not be made and the caller ID information that is provisioned in PortaBilling® will be shown instead.

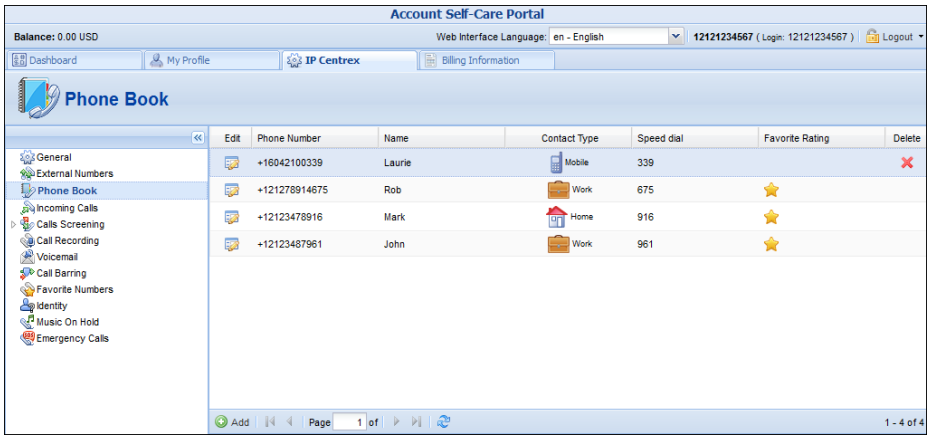
Comfort Ringtone Generation

You may face a situation where some of your vendors do not provide the proper service quality. This causes a high Post Dial Delay which results in discontented customers. To prevent such a negative experience, a "comfort" ringtone can be generated by PortaSwitch as soon as the incoming call is received and while PortaSwitch® performs the actual negotiation with the outgoing carriers. For the caller it will appear as if the call is already being connected to the called party. This functionality may be enabled by defining the corresponding value in the **Service Policies** and can later be assigned at the *account* level.

"Phone Book" for Each Phone Line

The phone book feature allows each account user to maintain their own set of frequently dialed numbers and assign speed dial codes to them. This functionality supplies end users with flexibility, by allowing them to:

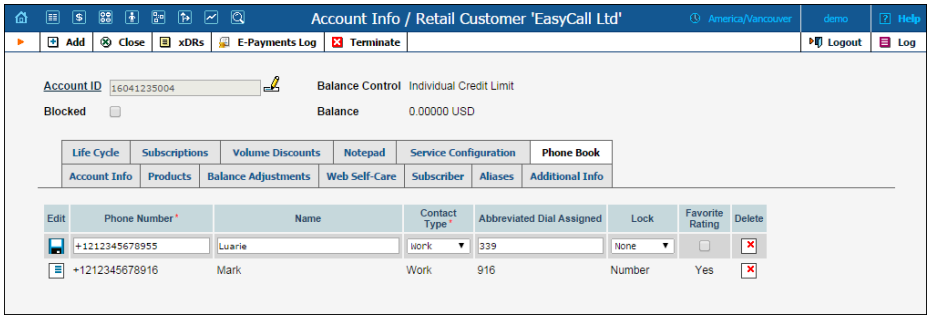
- Maintain their own set of frequently dialed numbers.
- Add, delete and edit their own contacts.
- Assign speed-dial to any entry in the phone book. The maximum short dial length is limited by the administrator.
- Define a list of favorite numbers that will be charged at a special rate. The maximum amount of numbers that an end user can mark as favorite numbers and the patterns used for these favorite numbers are specified by the administrator.



This functionality reduces the amount of work for PortaSwitch administrators:

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

- The administrator can flag any phone book entry as a "favorite" and calls to that number will be charged accordingly. An end user calling this specific number is charged according to a special rate for the FAV destination, defined in the end user's tariff.
- The administrator can "lock" portions of the phone book's information (e.g. an actual phone number) while an end user can still change other attributes. The administrator can fully lock a contact in the phone book (making it impossible for the end user to edit or remove) or partially lock the contact (allowing the end user to change only the name).
- The administrator can limit the speed dial number length by using the **Maximum Short Dial Length** option on the **Service Features** tab.



© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

3. IP Centrex Features

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

This section provides a general overview of various IP Centrex features available in PortaSwitch, as well as their activation and usage. Please note that many of these features are either handled entirely on the IP phone, or require adequate support from it; such cases will be clearly indicated in the feature descriptions. Also, for your convenience we have provided instructions about how a particular feature can be used on an IP phone; these instructions are applicable to Sipura/Linksys devices (1000, 2000, 2100, 3000). For other types of IP phones, please consult the manual provided by the vendor.

Additional Authorization for Toll Calls

Feature description: This feature allows you to perform additional verification of outgoing tolls on international calls. Especially in the case of a single phone being shared among multiple users, this feature enables individual accountability on each user's account.

Supported by PortaSwitch®; See the **Additional Authorization for Toll Calls** handbook for more details.

Alternate Numbers

Feature description: In addition to the user's main phone number, he/she can be assigned multiple alternate phone numbers, all of which will ring on his/her IP phone.

Implemented by assigning additional aliases to the account which represents the main phone line. Each alias is basically a direct inward dialing (DID) number.

Anonymous Call Rejection

Feature description: Automatically reject incoming calls from parties who do not deliver their name or telephone number with the call.

Provided by the IP phone; dial the *77 code to activate this feature, dial the *87 code to deactivate this feature.

Auto Attendant

Feature description: Provides IVR for callers and allows them to navigate among different options by pressing phone keys. Auto attendant capabilities include simple features such as playing a certain voice prompt to an end user or collecting his input, as well as more advanced features such as incoming fax detection or call queues.

See the *Auto Attendant* section in the **PortaSIP® Media Applications Guide** for more details.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

Automatic Line / Direct Connect ("Hotline")

Feature description: Automatically dials a pre-assigned Centrex station's extension number or external telephone number whenever a user goes off-hook or lifts the handset.

This feature is configured on the SIP phone using the dial-plan configuration parameter. For example, the following will implement a Hotline phone that automatically calls 1 212 5551234:

```
( S0 <:12125551234> )
```

The following creates a warmline to a local office operator (1000) after five seconds, unless a 4-digit extension is dialed by the user:

```
( P5 <:1000> | xxxx )
```

Busy Lamp Field (BLF)

Feature description: The BLF service allows monitoring on the physical attendant console of the line status (available, busy, etc.) of individual phone lines in the IP Centrex environment.

This feature is implemented in the presence server; the only thing required from the endpoint is to subscribe to notifications regarding particular phone lines.

Call Logs

Feature description: It shows the most recent calls and call details to an end user. It also provides the ability to listen to recorded calls (if any were recorded).

Supported by PortaSwitch® via the Dashboard feature on the account self-care interface.

Call Forking

Feature description: Allow all SIP phones registered on a single account to ring simultaneously. Consequently, if an end user owns three SIP phones (e.g. a mobile application on a smartphone, a tablet and a desktop IP phone), he can receive calls to all three devices simultaneously. The same account ID and password can be applied for all end-user SIP phones.

Supported by PortaSwitch®. See the *Call Forking* section for more details.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

Call Forwarding

Call Forwarding Always

Feature description: Automatically routes all incoming calls for a given extension to another number (extension, home/mobile phone, etc.).

This feature is implemented by provisioning the call forwarding / follow-me service and setting the **Default Answering Mode** to "Forward Only".

Call Forwarding on Busy

Feature description: Automatically routes incoming calls for a given extension to another pre-selected number when the first extension is busy.

This feature is implemented by provisioning the follow-me service and activating the `Cfwd Busy Serv` supplementary service on the IP phone. Use the *90 code to activate this feature, and *91 to deactivate it.

Call Forwarding to Voice Mail Always

Feature description: Automatically routes all incoming calls for a given extension to voice mail.

This feature is implemented by setting the **Default Answering Mode** to "Voicemail Only."

Call Forwarding to Voice Mail when Busy

Feature description: Automatically routes incoming calls to voice mail for a given extension when that extension is busy.

This feature is implemented by setting the **Default Answering Mode** to "Ring then Voicemail" and then disabling **Call Waiting**.

Call Forwarding to Voice Mail when Call Unanswered

Feature description: Automatically routes incoming calls for a given extension to voice mail after a specified number of rings when there is no answer.

This feature is implemented by setting the **Default Answering Mode** to "Ring then Voicemail."

Call Forwarding on Don't Answer

Feature description: Automatically routes incoming calls for a given extension to another pre-selected number when there is no answer after a specified number of rings.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

This feature is implemented by provisioning the follow-me service (choose "Follow-me when unavailable", then set the ring timeout parameter in follow-me). You may also utilize this feature on the IP phone itself by activating the `Cfwd No Ans Serv` supplementary service. Use the *92 code to activate this feature, and *93 to deactivate it.

Call Forwarding to Multiple Simultaneous Extensions

Feature description: Indicates the number of forwarded calls (originally dialed to the same Centrex extension) which may occur simultaneously.

This feature may be implemented similarly to other call forwarding scenarios, only this time the follow-me service should be provisioned with a simultaneous ring option.

Phone-initiated Forwarding

Feature description: Allows to program a "forward to" phone number directly into the phone, which will afterwards be returned by the phone in a "302" response to an incoming call request.

This feature may be implemented similarly to other call forwarding scenarios, but advanced settings such as multiple forwarding numbers, simultaneous ringing and time periods will not be available for phone-initiated forwarding.

More detailed information about this feature can be found in the *Call forwarding from an IP Phone* section of this document.

Call Me Now

Feature description: Allows an end user to request a call to the user's phone from the service provider's helpdesk (at the expense of the service provider).

See the *Web Callback Trigger* section in the **PortaSIP® Media Applications Guide** for more details.

Call Parking

Feature description: Allows the user to place a call on hold, move to a different location, and then resume the call from any other station in the Centrex by dialing a retrieval code.

Supported by PortaSwitch; in order to use this feature, the customer should define a "call parking prefix" in his call features configuration. Then, when a phone conversation is under way, the user can simply place the call on hold and dial the specified call parking prefix. The dynamically assigned "retrieval code" will be heard; this can be dialed from any phone

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

in the customer's IP Centrex group to retrieve the conversation (i.e. connect the call to that phone). It is also possible to quickly retrieve a call from the original phone by dialing a special "release prefix".

Call Recording

Feature description: Allows the user to record all incoming/outgoing/redirected calls on his phone line, so he can listen to (or download) them from the self-care web portal later on.

Supported by PortaSwitch via the **Call Recording** feature.

Call Recording on Demand

Feature description: Allows the user to start recording a phone conversation after it has already started.

Supported by PortaSwitch via the Call Recording feature. The main requirement for a SIP UA is the ability to send a special SIP INFO request with the header "Record" with "On" and "Off" content. Some phones, such as the SNOM 320/370, already have the appropriate control functionality and do not require extra configuration. In this case, the user presses the "Record" key on the phone and PortaSIP starts recording the call. The user can stop recording by pressing the "Record" key again. Some phones, such as the Yealink SIP-T28P, will need additional configuration (record functionality assigned to a specific button) to support the feature.

Call Restrictions / Station Restrictions

Feature description: Prevents certain types of calls from being made or received by particular stations.

For example, phones in public areas can be blocked from originating calls to external numbers, so as to prevent unauthorized users from incurring toll charges. Phones in certain areas may be blocked from receiving external calls in order to limit employees' ability to take personal calls. A wide variety of restrictions are available, covering incoming calls, outgoing calls, toll restrictions, code restrictions, and differential treatment for internal and external calls.

Provided via the tariff configuration in PortaBilling® or by using the **Call Barring** feature.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

Call Return

Feature description: Allows the user to originate a call to the last party or number that called the user, regardless of whether the user answered the original call or knows the caller's identity.

Provided by the IP phone; dial the *69 code to use this feature.

Call Transfer

Feature description: Transfers an existing call to another party (inside or outside the Centrex group).

PortaSwitch® supports the following transfer types:

- Unattended (blind) transfer
- Attended transfer
- Attended transfer of forwarded calls by DTMF

See the ***Call Transfer*** section for more details.

Call Waiting

Feature description: A feature that allows users to be alerted of one or more calls awaiting connection during a current conversation. Users are normally notified by a short tone on the phone or by use of the caller ID feature. Then, they can answer the second call, while the first one is still on hold.

Control Call Waiting

Feature description: Enables/disables delivery of the call waiting feature to IP phones, allowing administrators to control call waiting for a specific account. This ensures that the feature is supplied only to users who have it activated on the PortaSwitch side (regardless of whether it is enabled on the IP phone itself).

Supported by PortaSwitch®.

Caller ID

Feature description: Allows the user to identify the name and telephone number of a calling party before answering an incoming call.

Supported by PortaSwitch®; the phone must have a display to show the caller ID.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

Caller ID on Call Waiting

Feature description: Allows a caller's name and number to be displayed when the called party is taking another call.

Supported by PortaSwitch®; the phone must have a display to show the caller ID, and the Call Waiting feature must be activated.

Calling Line ID Delivery Blocking

Feature description: Allows an end user to indicate that he wants privacy for a particular outgoing call, i.e. the other party will not see his phone number.

This can be done by either activating the privacy settings on the IP phone itself (in this case, the IP phone will include the corresponding RPID header of the SIP INVITE), or by activating the **Hide CLI** feature on the PortaSwitch side. See the *Support for Privacy Flags* section for more details.

Calling Name Retrieval

Feature description: Allows an end user to see a caller's ID (name and surname, or company name that owns the number) in addition to the original caller's number.

Supported by PortaSwitch®. See the *Caller ID (CNAM) Lookup* section for more details.

Conferencing

Feature description: Allows an end user to create and manage conference bridges for instant meetings.

Supported by PortaSwitch®. See the *Conferencing* section in the **PortaSIP® Media Applications Guide** for more details.

Consultation Hold

Feature description: Calls can be put on hold by depressing the switch-hook or pressing the flash button. After completing the second call, the user is automatically reconnected to the original call on hold.

Supported by PortaSwitch®.

Dialing Rules

Feature description: This allows an administrator or a customer to define a way of dialing phone numbers that is convenient for end users.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

Supported by PortaSwitch®.

The dialing rule wizard can be used to construct correct rules based on the parameters provided, such as country or area code. Alternatively, the dialing rules can be defined by means of regular expressions. This allows administrators to easily manage a network that has many different customer numbering plans.

ANI translation on incoming / outgoing calls

In addition, the dialing rules can translate the CLI (ANI) numbers to / from a vendor-specific format when routing a call to / from a vendor's network. This enables the sending of caller information to a vendor in the format that he requires (e.g. a 10-digit phone number for US callers).

DID (Direct Inward Dialing Number)

See *Additional Authorization* for Toll Calls
Feature description: This feature allows you to perform additional verification of outgoing tolls on international calls. Especially in the case of a single phone being shared among multiple users, this feature enables individual accountability on each user's account.

Supported by PortaSwitch®; See the Additional Authorization for Toll Calls handbook for more details.
Alternate Numbers.

Distinctive Ringing

Feature description: Uses a special ringing pattern to indicate whether an incoming call is from inside or outside the Centrex group.

Supported by PortaSwitch® for the **Ext-to-ext call distinctive ring** feature.

Do Not Disturb

Feature description: The Do Not Disturb (DND) feature allows end users to temporarily disable incoming calls.

Supported by PortaSwitch®. A SIP phone is required to support the DND feature.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

Extension Dialing

Feature description: Allows an end user to dial extension numbers for quickly connecting with phones inside of the same IP Centrex environment.

Supported by PortaSwitch®.

Group Calling Line Identity

Feature description: This service allows a user identity (name and number) to be defined for a group of users.

Supported by PortaSwitch®. See the *SIP Identity* section for more details.

Group Pickup

Feature description: Allows phones in the same IP Centrex environment (all accounts under the same customer) to answer each other's calls by dialing a ***Group Pickup Prefix*** *on their phones.*

Supported by PortaSwitch®.

IP Device / Phone Inventory

Feature description: The IP phone directory allows you to keep track of IP devices (SIP phones or adaptors) that are distributed among your customers.

Supported by PortaSwitch®. See the *CPE Inventory* section for more details.

Multiple Pickup Groups

Feature description: *Allows phone lines in the same IP Centrex environment to be grouped so that phone line owners within the group may answer each other's calls by merely dialing a group call pickup prefix on their phones.*

Supported by PortaSwitch®.

Customers can configure multiple pickup groups on their self-care interfaces. To set up call pickup within huntgroups, the customer first enables the **Group Pickup** option, defines a group call pickup prefix, enables pickup for the required huntgroups and then assigns a primary group (huntgroup) for each extension.

With this functionality it is possible to configure different call pickup scenarios, important for companies with many departments.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

For example, call pickup within a primary group by merely dialing the group pickup prefix, call pickup within a non-primary group by dialing the group pickup prefix and a huntgroup number, directed call pickup of a certain extension by dialing the group pickup prefix and an extension number.

Hunt Groups

Feature description: Allows calls to be redirected to other predetermined lines when the line called is busy. Hunting allows a number of lines to be grouped into a "pool", so that incoming calls are directed to whichever of these lines is available.

Supported by PortaSwitch®; huntgroups are defined on the **Huntgroups** tab in the customer information screen.

Intercom Dialing

Feature description: Allows a receiving phone to auto-answer a call and activate speakerphone mode.

Supported by PortaSwitch®; the Paging / Intercom feature must be activated.

Message Waiting Audible

Feature description: Provides the user with an audible notification - a "stutter" dial tone when messages have been left in the extension's voice mail system.

Provided by the IP phone and supported by PortaSwitch® (the actual "message waiting" SIP info packet is originated by the Media Server and relayed by the Switching Server).

Message Waiting Visual

Feature description: provides the user with a visual indication when messages have been left in the company's voice mail system.

Supported by PortaSwitch® (the actual "message waiting" SIP info packet is originated by the Media Server and relayed by the Switching Server), requires the phone to be able to display the appropriate icon.

Multiple Call Appearances

Feature description: Multiple Call Appearances allow each station to have two or more appearances of the user's primary phone number. Each appearance gives the user the ability to handle one call. Consequently, Multiple Call Appearances allow the user

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

to originate and/or terminate multiple calls simultaneously. Unlike an analog multi-line phone, the station needs only one line (and one phone number) for Multiple Call Appearances. When the user is involved in a call on one call appearance and another call is offered on a different call appearance, the user may use the Caller ID information to decide whether to answer the ringing call appearance or let the call be forwarded to voicemail. To answer the ringing call appearance (or originate a second simultaneous call), the user simple puts the first call appearance on hold. Calls on different appearances can be combined together to form a three-way conference call.

Supported by PortaSwitch® via the follow-me feature. The primary phone number (account) is provisioned on the IP phone, and all the other appearances are created as accounts with the follow-me configured to the primary account.

Music-On-Hold

Feature description: Provides a musical interlude for callers who are waiting on hold.

Supported by PortaSwitch®; every Centrex user can upload his own melody or use the default one for his Centrex environment.

MWI Delivery to an Endpoint

Feature description: This feature allows the Media Server to automatically manage the SIP phone's MWI status so that a user is notified when he has new messages.

Supported by PortaSwitch®. A SIP phone is required to support the message waiting indicator (MWI).

Paging / Intercom Calls (Push To Talk)

Feature description: This allows an end user to dial another user from the same group (customer) when the system requests that the destination VoIP phone automatically answer.

Supported by PortaSwitch®. A SIP phone supports this feature. See the *Paging / Intercom Calls* section for more details.

Selective Call Acceptance

Selective Call Acceptance (SCA) is a telecommunications system feature that allows customers to create a list of phone numbers from which they are willing to accept calls.

Supported by PortaSwitch® via the Call Screening module; every Centrex user can create rules defining a set of phone numbers. If an incoming call matches one of these numbers, the call is accepted; otherwise the call is rejected.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

Selective Call Forwarding

Selective Call Forwarding (SCF) is a telecommunications system feature that allows customers to forward callers from a selected group of numbers to another number.

Supported by PortaSwitch® via the Call Screening module; every Centrex user can create rules defining a set of phone numbers. If an incoming call matches one of these numbers, the call is forwarded to the destination defined in the call forwarding or follow-me settings.

Selective Call Rejection

Selective Call Rejection (SCR) is a telecommunications system feature that allows customers to reject incoming calls.

Supported by PortaSwitch® via the Call Screening module; every Centrex user can create rules defining a set of phone numbers. If an incoming call matches one of these numbers, the call is rejected.

Speed Dialing

Feature description: Allows the user to dial frequently called telephone numbers using an abbreviated speed calling code instead of the entire number.

Supported by PortaSwitch® via the Phone Book feature.

Station Message Detail Recording (SMDR)

Feature description: Allows the corporate telecom manager to receive call detail records on a per-station basis before the monthly telephone bill is even issued. SMDR helps the customer control telephone fraud and abuse, perform accurate cost accounting, and analyze call patterns to identify opportunities for cost reductions.

Supported by PortaSwitch®; call details are available on the PortaBilling® web interface.

Three-way Conferencing (Three-way calling)

Feature description: Allows user to add a third party to an existing conversation forming a three-way conference call.

Supported by PortaSwitch®; SIP phone must support the 3-way calling feature.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

Toll Restriction

Feature description: Blocks a station from placing calls to telephone numbers that would incur toll charges.

Provided via the tariff configuration in PortaBilling® or by using the **Call Barring** feature.

700/900 Blocking

Feature description: Blocks a station from placing calls to 700 and 900 numbers.

Provided via the tariff configuration in PortaBilling® or by using the **Call Barring** feature.

Find more features in the *Supported Services* section of the **PortaSIP® Media Applications Guide**.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

4. Messaging Services

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

Instant Messaging

Instant Messaging (IM) is defined as the exchange of text messages between two users in real time. Supported by a wide range of multimedia clients such as MS Messenger, instant messaging can easily be used to post messages from any computer or mobile device.

IMGate is a constituent component of each PortaSIP® cluster processing node. IMGate enables online messaging and message storage for offline users (so they can receive messages later).

When a MESSAGE request arrives at the PortaSIP® cluster via SIP or SMPP, the dispatching node delivers it to the *active* IMGate.

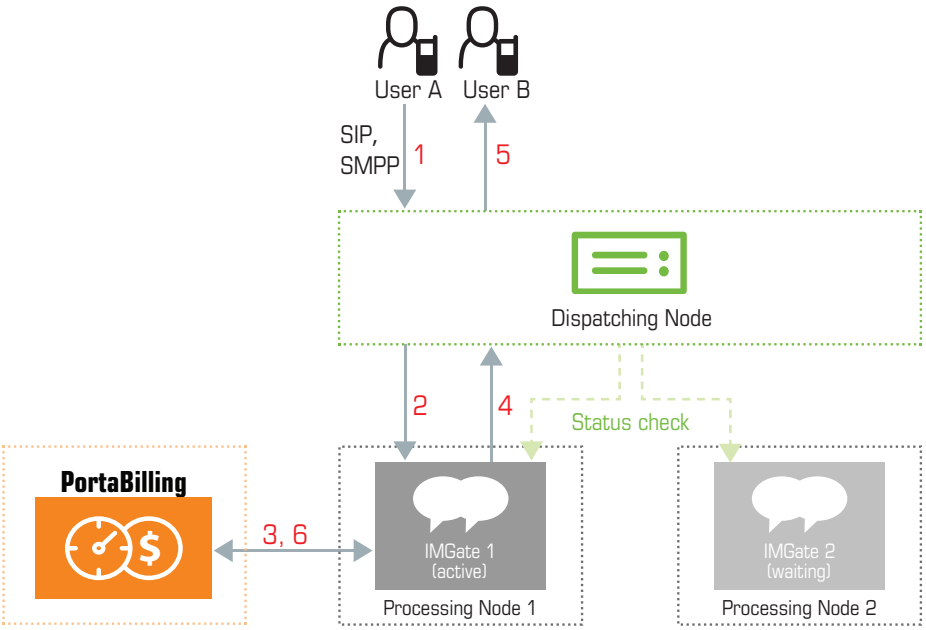
NOTE: To ensure accurate message transfer and delivery, only one IMGate server is active within the PortaSIP® cluster. All other IMGate servers remain in *waiting* mode (ready, but not involved in the work process).

If an active IMGate server becomes unavailable for some reason, the dispatching node activates the next IMGate server to handle MESSAGE request processing.

When an active IMGate server receives a request, it processes the message according to a defined configuration.

Note that a geo-redundancy solution for IMGate will become available in upcoming releases.

A basic instant message flow looks like this:



© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

1. Users connect to PortaSIP with user agents (IM clients). Users are identified by an address (i.e. "John Smith" sip:1234@sip.example.com>) that uniquely defines an individual within PortaSIP.
2. To make themselves available for contact via a particular SIP user agent, users send a SIP REGISTER message to a Registrar.
3. User A sends an instant message. The MESSAGE request arrives at the PortaSIP® cluster dispatching node (**1**).
4. The dispatching node forwards the request to the active IMGate (**2**).
5. IMGate matches the corresponding domain service policy (using a match pattern) that defines how the instant message must be processed.
6. Based on the results, IMGate authorizes the message in the billing engine and receives a routing list for further message delivery (**3**).
7. IMGate checks whether the recipient is registered in the network. If he is, IMGate forwards the message to the dispatching node informing it about the route (**4**). If the recipient's UA is not registered, IMGate stores the message until the recipient's UA sends the REGISTER request to a cluster's processing node.
8. The message is delivered to user B (**5**). When a message reaches its destination, a 200 OK response is returned (note that this does not necessarily mean the message has been read by its recipient).
9. IMGate sends accounting records to the billing engine to charge user A for the outgoing message (**6**).

SMS Message Processing

PortaSwitch® allows the ITSP to offer SMS services (such as instant messaging to mobile users, premium number SMS, SMS campaigns and wholesale SMS) while using an all-IP infrastructure:

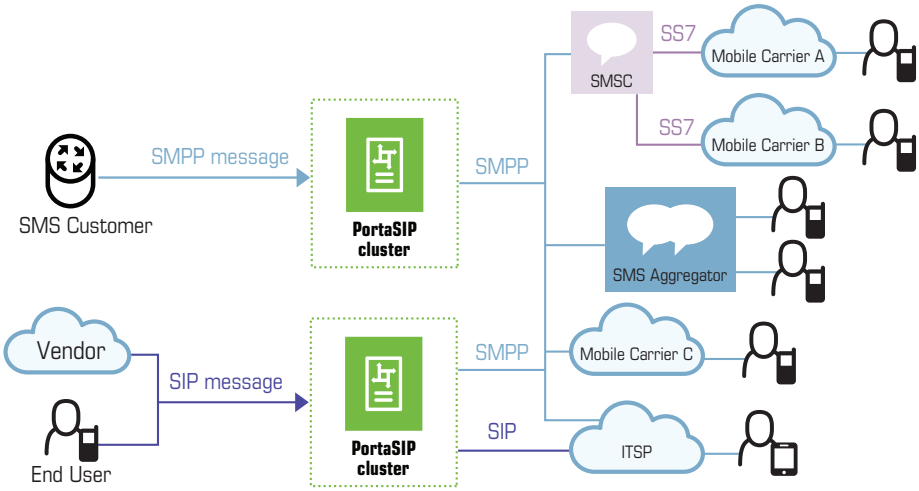
- PortaBilling® performs the authorization, rating and billing for outgoing SMS messages.
- PortaSIP® cluster routes SMS messages to one of the vendors for delivery to a mobile network by using either the industry standard SMPP protocol or the SIP protocol, thus providing fail-over routing.

SMS messages can be routed to the SMSC (short message service center) from **NewNet** and to SMS aggregators using the SMPP protocol.

Also, messages can be routed to other ITSPs using the SIP protocol. For example, if a large fraction of your messaging traffic goes to UK numbers,

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

then it would be to your advantage to connect with a local ITSP (which serves those numbers) to send SMS messages directly, and thereby avoid extra costs.



Note that using either the SMPP or SIP protocol for sending SMSs depends on the configuration of an end-user's instant messenger. This, in turn, determines which messaging vendors' connections (SMPP or SIP) participate in routing.

When sending messages within your network, the SIP protocol is always used.

Future releases will implement rating and billing for incoming SMS messages. With this improvement, everything that is required is in place to provide full-scale SMS messaging services.

Together with instant messaging and voice calls, this feature offers your customers a complete, real-time communication experience.

Step-by-step instructions on how to configure the messaging service can be found in the **Unified PortaSwitch® Handbook Collection**.

Wholesale Messaging

In today's world, instant messages are a powerful and popular tool for marketing and for customer support. For example, call centers that advertise goods often need to broadcast promotional information about

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

sales or reach individual subscribers about special offers. Instant messages are an easy and convenient way to do this.

In wholesale scenario, messages are sent via the SMPP protocol. Upon receiving a message, PortaSIP® cluster authorizes the customer by their IP address and checks whether the customer's product and balance allow messaging. Then the message is forwarded to a vendor. When there are several vendors configured in the system, LCR (least-cost routing) is used allowing a service provider to build an optimal pricing strategy.

Instant Messaging and SMS Combination

Message exchanges can take the form of instant messages or SMS messages or both. As a rule, instant messaging is provided free of charge, while every SMS is authorized and users are charged per message.

The combination of instant messaging and SMS messages allows a user to send either type of message using the same IM application.

Consider the following example:

A user and his friend are both subscribed to an instant messaging service. The user enters his friend's actual phone number 1337225604 (T-Mobile network), and specifies it as a "Mobile" contact type. Then he enters his friend's VoIP number 8789952103 and specifies it as a "SIP" contact type in his instant messenger's contact list. Based on the user's selection, the IM application stores the number 1337225604 as 1337225604@sms and the number 8789952103 as 8789952103@sip.

The user sends an instant message to 8789952103. When the user sends a message to the number 1337225604, he is informed that this message will be sent as an SMS and that he will be charged for it.

The instant messenger determines what type of message to send. Therefore, the IM application is responsible for distinguishing types of contacts and delivering correct contact information to PortaSIP® cluster.

In the case of instant messaging, messages travel within your network (on net messaging) via the SIP protocol; in SMS exchange, messages are sent directly to SMS aggregators via the SMPP protocol.

And how will PortaSIP® cluster know which type of message it is in order to process and deliver it accordingly? The section below provides a description of message delivery specifics.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

Message delivery specifics

The selection of the transport protocol for message delivery is defined by the information contained in the `To:` header of the MESSAGE request. This information is delivered in the format `sip:<number>@<domain>` (e.g. sip:12345@sip.example.com for instant messages and sip:12345@sms.example.com for SMS messages).

When a user sends a message, the MESSAGE request arrives at PortaSIP® cluster. Based on the domain name contained in the `To:` header of the MESSAGE request, the system defines how the request should be processed:

- The system selects a corresponding service policy by matching the domain name taken from the `To:` header with the **match_pattern** value of the domain service policy.
- The selected service policy defines the transport protocol (SIP or SMPP), routing and billing parameters.
- Based on the service policy configuration, PortaSIP® cluster delivers the message via SIP protocol or converts it into an SMPP message and delivers it via the SMPP protocol.

For the instant messenger to pass the correct contact information to the PortaSIP® cluster, the contacts in the instant messenger contact list must be stored with corresponding domains, and PortaBilling® domain service policies must be configured accordingly to match these domains.

To illustrate, let us use the following domains:

- `sip.example.com` for instant messaging.
- `sms.example.com` for SMS delivery.

The instant messenger contact list is then represented as follows: `<number>@sms` – a message to this contact will be sent as an SMS; `<number>@sip` – a message to this contact will be sent as an instant message.

This type of contact representation must be supported by the instant messenger.

Now you have a general idea about contacts formats. You can either customize the instant messenger or develop your own IM application to store users' contacts according to the templates described above.

The configuration of PortaBilling® can be found in the **Unified PortaSwitch® Handbook** collection.

Providing instant messaging and SMS services as a single messaging solution makes you more competitive in the telecommunications market.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

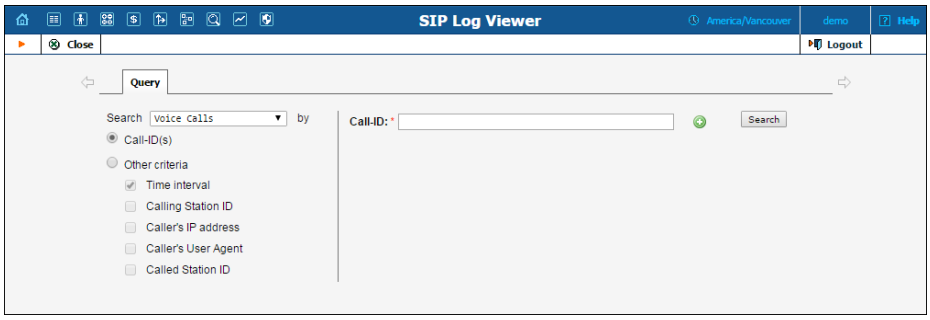
5. Administration

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

SIP Log Viewer

When troubleshooting unsuccessful calls, the administrator needs to have the ability to quickly and efficiently filter a particular call log to find the root of the issue.

This can easily be done with the SIP log viewer functionality, which works with Elasticsearch storage and has a user-friendly web interface.



By default the search is done by Call-ID; however, there is a set of additional search criteria by which a call can be traced. When necessary, several search criteria can be combined into a single search query, thus narrowing the search of a particular call log.

NOTE: To perform an extended SIP log search, configure the **LogServer** and the **Elasticsearch** instances on the configuration server.

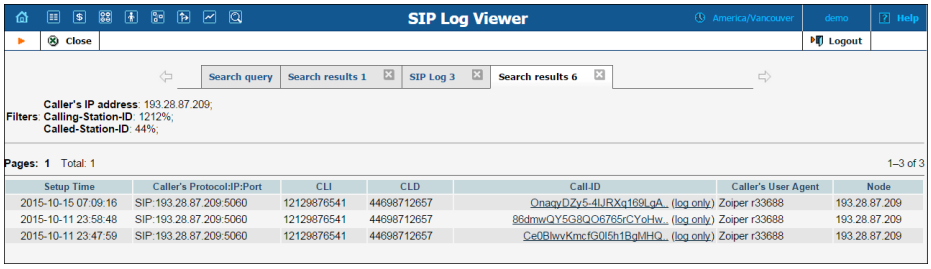
The search criteria available are as follows:

- **Call-ID(s)** – This is the default search criterion. When defined, a call is filtered by its unique ID. If a call consists of several parts (e.g. a callback call), it is possible to define several Call-IDs which will be merged into a single call log. The number of Call-IDs is limited to 5.
- **Time interval** – Filters all call attempts performed within the specified time interval;
- **Calling-Station-ID** – Filters calls in which the originating number (ANI number) is a particular phone number. If a calling number in an incoming call leg was delivered to PortaSwitch® in a local format (e.g. 02065550236), specify it in the same format when tracing the call or use the % pattern to substitute unknown symbols (e.g. %2065550236, 206555% or %206555%);
- **Caller's IP address** – Filters calls that originated from the specified IP address;
- **Caller's User Agent** – Filters calls made from a SIP phone or a dialer application of a particular brand;
- **Called-Station-ID** – Filters calls dialed to a particular number. If an end user dialed a destination number in a local format (e.g.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

02065550236), specify it in the same format when tracing the call or use the % pattern to substitute unknown symbols (e.g. %2065550236, 206555% or %206555%).

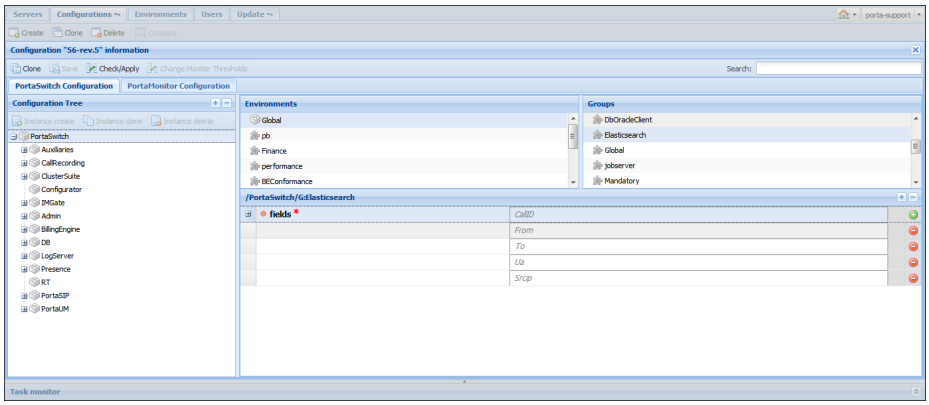
The administrator can perform several call searches at a time by creating several search queries with different search criteria. The results of each query are displayed in a separate tab and contain the specified criteria.



The SIP log viewer functionality speeds up the call log search and improves the troubleshooting process in whole, and log analysis in particular.

Note that it is possible to configure which search parameters can be used in **SIP Log Viewer**. The **ElasticSearch.fields** configuration option contains a list of available search parameters that an administrator can modify via the configuration server web interface. This option is located under the **PortaSwitch** node → **ElasticSearch** group, and can be configured for each virtual billing environment separately.

As soon as one of the search parameters is deleted from the list, it disappears from the admin interface and can no longer be used for searches.



The option can have the following values:

- **CallID** – Call-ID
- **From** – Calling-Station-ID
- **To** – Called-Station-ID

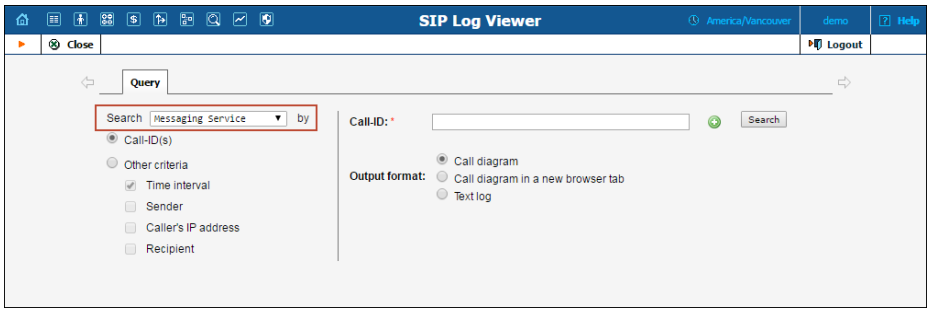
© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

- **Ua** – Caller's User Agent
- **Srcip** – Caller's IP address

When performing a search, the system always uses timestamps (even if the time isn't explicitly specified as a search parameter), and therefore **Time Interval** can't be removed from the search parameter's list.

Message Logs in the SIP Log Viewer

Along with call logs, the administrator can view message logs with the **SIP Log Viewer** tool. The administrator needs to know the Call-ID of a specific message in order to view its log. If the Call-ID is unknown, the administrator can filter message logs by time interval, originating phone number and / or by originating IP address or destination phone number to locate the message log needed.



From the message logs the administrator can obtain the following information:

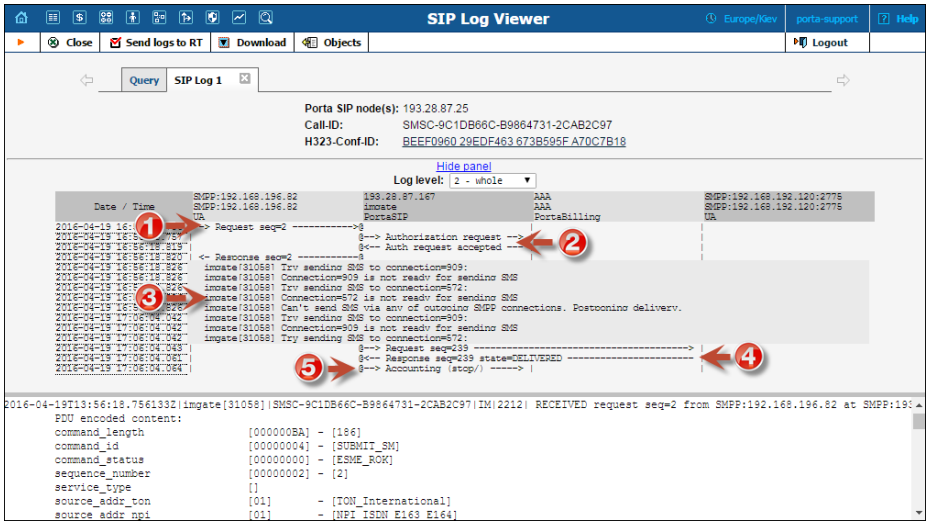
- A matched domain service policy. This policy defines which transport protocol is used for message delivery (SIP or SMPP).
- A routing list for message delivery.
- Routes that have been tried for message delivery.
- The service policy assigned to the vendor connection that is chosen for message delivery.
- A reason for message delivery delay.
- The external services involved in message delivery.

The administrator can view a message log either in plain text or as a message flow diagram. On the message flow diagram the administrator can see the main entities participating in message delivery and the sequence of messages sent among them.

An example of the message flow diagram is shown below. In this scenario, a wholesale provider sends messages via the SMPP protocol. The message arrives at the PortaSIP® cluster from the endpoint (1). The PortaSIP® cluster authorizes the endpoint in the billing engine and receives a routing list for message delivery (2). The IMGate tries the

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

routes returned by the billing engine one by one (3) until a RECEIVED response arrives from the SMSC (short message service center) or the SMS aggregator (4). The IMGate sends accounting records to the billing engine for this message (5).



NOTE: For messages delivered via the SIP protocol, message logs are split into two parts. The first part of the log includes information related to message delivery from the sender to the IMGate and message authorization in the billing engine. The second part of the log includes information related to message delivery from the IMGate to the recipient.

The second part of the log has a different Call-ID. It is provided in the first part of the log as the **Outgoing message call-id** header field.

Having the capability to locate and analyze message logs substantially improves the message troubleshooting process and reduces the time it takes to isolate and fix a problem.

Troubleshooting Common Problems

No or one-way audio during SIP Phone – SIP Phone calls

This problem usually means that one or both phones are behind a NAT firewall. Unfortunately, unless the RTP Proxy is turned on or certain "smart" SIP phones/NAT routers are used, there is no way to guarantee proper performance in such cases (see NAT Traversal section for details).

One-way audio during SIP Phone – Cisco gateway calls

This problem can occur if the Cisco GW is not configured properly. Please check that the GW contains the following in its IOS configuration:

```
sip-ua
```

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

```
nat symmetric check-media-src
```

I have problems when trying to use SIP phone X made by vendor Y with PortaSIP

Unfortunately, not all of the many SIP phones available on the market today fully comply with the SIP standard, especially low-end products. We use Sipura / Linksys 941 as a reference phone, and the Sipura/ Linksys – PortaSIP combination has been thoroughly tested.
If you are unable to get your third-party vendor SIP phone working properly, follow the instructions below:

- Make sure the phone has been configured properly, with such parameters as account ID, password, SIP server address, etc. Consult the product documentation regarding other configuration settings.
- Check the PortaSIP and PortaBilling® logs to ensure that there is not a problem with the account you are trying to use (for example, an expired or blocked account).
- Connect the Sipura / Linksys phone or ATA to the same network as your SIP phone. If possible, disconnect the SIP phone and use the same IP address for the Sipura / Linksys as was previously used by the third-party SIP phone. Configure the Sipura / Linksys with the same account as was used on your third-party SIP phone.
- Try to make test calls from the Sipura / Linksys.
- If you have followed the preceding steps and the problem disappears, then this means your third-party vendor SIP phone is not working according to the standard. Contact the vendor of the SIP phone, and describe the problem.
- If this problem with the Sipura / Linksys persists, contact **support@portaone.com**. Provide a full description of the problem, the ID of the account being used for testing, and the relevant parts of the sip.log and porta-billing.log

FAQ

Which SIP devices can be used with PortaSwitch®?

Any SIP-compatible device should be able to send and receive calls via PortaSwitch®. You need to specify a PortaSIP server's IP address or hostname as well as a SIP username and password for the corresponding PortaBilling® account in the device settings. For additional information you can refer to the list of RFCs supported by PortaSwitch® (Please refer to the *APPENDIX A. Supported SIP RFCs* section of this guide for more details).

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

Does PortaSIP support conferencing?

You can use the 3-way calling feature, available in most SIP phones or ATAs. The full-scale SIP conferencing service is provided by a conference IVR application which is part of the Media Server.

Can you assist me in integrating SIP device X (gateway, media server, conference server, etc.) made by vendor Y with PortaSIP?

Yes, we can; however, you will have to purchase an additional consulting contract. Generally speaking, there should be no compatibility problems between PortaSIP and any standards-compliant SIP device. However, for obvious reasons we only provide detailed setup instructions for the Cisco AS5300 gateway.

I want to terminate my SIP customers to a vendor that only supports H.323 traffic – what should I do?

To do this you need to use a SIP->H.323 protocol converter. Either purchase a dedicated solution, available from a number of vendors (for instance Aloe Systems **www.aloe-systems.com**), or use one of your 36xx Cisco gateways with the special IOS feature called UBE (Universal Border Element), previously called IPIPGW.

In addition to protocol conversion, you may also need convert codecs. This is not possible with IPIPGW, but you can use the Cisco AS53XX gateway by looping one or more pairs of E1/T1 ports on it to allow SIP->ISDN->H323 call flow.

Please note that, in the latter approach, one ongoing session will consume 1 timeslot in each looped E1/T1 (2 total), as well as 2 DSPs. For example, if you have two E1 interfaces connected back-to-back, the maximum number of simultaneous SIP sessions that you will be able to terminate to your H.323 provider will be 30, and each such session will use 2 DSPs.

I have problems with the audio quality of SIP calls, what can I do?

First of all, please make sure that both the user agents and SIP<->PSTN gateway are configured for use of the same low-bitrate codec, such as G.723.

In *APPENDIX B. Cisco GW Setup for PortaSIP (COMEDIA)*, there are details on how to configure Cisco IOS and Cisco ATA 186; for other SIP phones or gateways, check the documentation supplied with the device. If you are sure that the codec used for SIP calls is a low-bitrate one (for example, by inspecting the gateway logs), but the quality is still suboptimal, you need to determine where packet loss is occurring in the

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

media path. To do this, you can use standard network tools such as ping, traceroute and the like. Keep in mind that for SIP UA<->PSTN calls the RTP audio stream flows directly between SIP UA and PSTN GW, while for SIP UA<->SIP UA calls the RTP path depends on whether or not an RTP proxy is enabled. If an RTP proxy is not enabled, the RTP flows directly from one SIP UA to another. Otherwise, each RTP packet sent by one UA goes first to the machine running PortaSIP and is then resent from that machine to another SIP UA.

Can I use IP PBX which only supports the late offer-answer model in conjunction with PortaSIP for SIP trunking services?

PortaSIP® supports the late offer-answer model; therefore these two elements can be connected directly. For more details regarding the supported modes and configuration, see the **Cisco website**.

I tried to register with the SIP server, but my UA says "registered" even if my username or password are incorrect – is there a security breach in PortaSIP?

Of course PortaSIP does not really allow unauthorized clients onto your network. If the SIP UA tries to register using an incorrect username or password, or with an account which is blocked, registration will not succeed. However, UA will still receive registration confirmation (and this is why you see "registered" in the UA). But if you try to make an outgoing call it will be diverted to the media server, where the appropriate message will be played (e.g. "This account does not exist" or "Account is blocked"). This allows SIP registration's troubleshooting to be greatly simplified.

Keep-alive functionality does not work with my XXX brand SIP phone

Your SIP phone must correctly respond to keep-alive re-INVITE requests. If it does not support this functionality, then it may either not reply at all to these requests, or (even worse) assume that this is a new incoming call. If PortaSIP detects that the SIP UA has not answered the first keep-alive (at the very beginning of the call, when the SIP phone should presumably be online), then it assumes that the SIP UA does not support this functionality, and disables keep-alives for this session. In any case, it is recommended to choose a SIP UA which supports re-INVITEs (e.g. Sipura).

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

I do not want to use an RTP proxy (since it will increase the amount of required bandwidth); can I use STUN instead?

The STUN RFC (**http://www.faqs.org/rfcs/rfc3489.html**) states: "This protocol is not a cure-all for the problems associated with NAT". STUN is merely a service that can be installed on a server such as PortaSIP, allowing a STUN-enabled SIP phone to communicate with it and detect the type of firewall it is behind and the public IP address of the NAT router. Thus, a SIP phone may obtain certain information by communicating with a STUN server, but this will not have any effect on the way NAT handles IP packets traveling to or from the phone. In the case of a "cone" firewall, STUN information may help the SIP phone to determine in advance which IP address and port the remote party can use to communicate with it. However, in the case of a "symmetric" NAT this will not work, and so an RTP proxy is still required. Moreover, since this is a relatively new technology many phone vendors have not implemented the STUN functionality in its entirety, or completely correctly.

So, theoretically, STUN may be used in conjunction with PortaSIP's RTP proxy: if a phone detects that it can bypass NAT via STUN, it will act as if it were on a public IP address, and the RTP proxy will not be engaged. Unfortunately, in practice activating STUN only makes matters worse, due to flaws in STUN implementation for IP phones.

Using two different approaches to handling NAT concurrently is the same as adding flavorings (salt, pepper, etc.) to a stew by following several recipes from different cookbooks at the same time: even a slight mix-up will probably result in your adding some of the seasonings twice, while not putting others in at all – and the result will be something which no one can eat.

Currently, one very common problem situation is that where a SIP phone is behind a symmetric NAT and obtains its public IP address from STUN, putting this into the contact information. This confuses the RTP proxy, since PortaSIP regards the SIP phone as being on a public IP address, so that no RTP proxy is used; the result is one-way audio.

So, the simplest answer is: yes. You can use STUN to avoid usage of an RTP proxy in some cases. At the present moment, however, due to unreliable STUN support on the IP phone side, the safest option is to avoid using STUN.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

How many simultaneous voice conversations can be recorded by the combination of a single PortaSIP server and a single server doing the conversion?

Voice conversion is a resource-intensive task, and fully occupies CPU resources while being executed (this is why a dedicated server is required.) A server can efficiently do the number of concurrent conversions which is equal to the total number of its cores, minus one (the remaining core will be used for executing OS tasks, monitoring, transportation of files to be processed and conversion results, etc.). So only one recorded call is converted on each CPU core at a time.

On average, a raw RTP stream which contains the data for a 5-minute call has a size of about 6 megabytes (assuming use of the G711 codec), and its conversion into a 500 kilobyte .wav file takes about 1.5 seconds on a single 3 GHz core.

Assuming that a dedicated server for call recording has a 3 GHz quad-core processor, generally three out of the four cores will be engaged in voice conversion. This server will be able to keep up with 3 * (5 minutes / 1.5 seconds) = 3 * (300 / 1.5) = **600** concurrent calls being recorded on the PortaSIP server. If the number of voice calls being recorded simultaneously exceeds this number (for instance, during peak hours), conversations will still be recorded and the results will be available for end users to download, but with a small delay.

How to ...

... provide services to and bill a customer who has a SIP-enabled gateway but no authorization capability (e.g. Cisco AS5350)?

PortaSIP is able to authenticate incoming calls using the IP address of the remote side. This method ensures that PortaSIP will accept calls from your own gateways, but it can also be used to bill traffic from your customers. In the call scenarios management screen you need to create a new entry, which would activate the “Authorize by IP” application for all calls, coming from this IP address and then create an account for your customer with an account ID identical to the IP address of his gateway.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

... allow my customer to have two phone numbers from different countries which will both ring on the same SIP phone?

You can have an unlimited number of such "extra" phone numbers. Your customer will have one main account (e.g. 12025550003) which will be provisioned on his phone, and extra phone numbers (e.g. 4981234567) will be added as aliases to it. Alternatively you can create extra accounts (e.g. 4981234567), with the follow-me service on these accounts configured to always go to 12025550003.

... configure SIP phone X made by vendor Y?

Obviously, we cannot provide a sample configuration for every possible SIP phone model. Please check the documentation shipped with your device. Essentially, however, you need to configure the following settings:

- **IP address of the SIP proxy** - IP address or hostname of the PortaSIP server.
- **CID** (Caller Identification).
- **Login** and **password** – account ID and password of the corresponding account in PortaBilling®.
- **Preferred audio codec** – depends on your network characteristics; should be compatible with the codec used by other components (e.g. VoIP gateways used for PSTN termination).

In the case of PortaSIP, both the login name and CID should be set to the same value. Set the preferred audio codec to G.723 if your phone supports this. Likewise, enable in-band alerting if your phone supports it, as this will help in situations when the phone is behind a NAT.

... bill incoming calls from PSTN to SIP using a special rate?

The following applies to PSTN->SIP calls, which you receive via a PSTN gateway on your network. For PSTN->SIP calls received directly to your SIP server via VoIP, see the *Special Access Codes* section of this guide.

In order to properly bill a SIP account for such calls, do the following:

- Install a PSTN2SIP application on your Cisco gateway which handles incoming PSTN calls.
- Create an appropriate tariff with the desired rates. For example, if your SIP customer has account **12021234567** and you want to charge him for incoming calls from PSTN to that number, there should be a rate with a prefix matching this number, for example, **1202**.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

- In the product associated with this account, create a rating entry with this PSTN-SIP gateway as the node and the tariff created in the previous step.

Now calls originating from a SIP phone to 1202 numbers will be charged using the tariff associated in the product's Services and Rating list with the PortaSIP node. Calls terminated from the PSTN to the SIP phone will be charged using a different tariff, one associated with the PSTN gateway.

... provide error messages from the media server in my users' local language

First of all, you must record a set of all the required voice prompts (account_expired, cld_blocked and others). Convert them into "raw" format and name the files <original-name>-<language>.sln; for instance, the Chinese version of the "account expired" message will be contained in the file account_expired-ch.sln. Then upload the files to the PortaSIP server in the `/var/lib/porta-sip/sounds/` directory. This will be sufficient to enable the PortaSIP media server to play this voice prompt to SIP phones using g711, GSM and many other popular codecs.

Unfortunately, you cannot perform such online transcoding into the g723 or g729 codec, since in this case you must pay a license fee. A solution is to pre-convert this voice prompt into a g723 or g729 byte stream, store it in a file with the same name (but with the .g723 or .g729 extension), and upload it to PortaSIP. The media server will then use the appropriate file.

... calculate how much bandwidth I need for my PortaSIP server?

The amount of bandwidth required for SIP signaling is insignificant compared to that used by the RTP stream, so the most important task is to correctly estimate your RTP bandwidth needs (of course, this is only applicable if an RTP proxy is used, otherwise the voice stream goes directly between the SIP phone and the remote gateway).

The bandwidth will naturally depend on the codec being used. However, the "codec bitrate" parameter of the codec cannot be used for calculations since it only reflects the actual "useful" data stream. When this data is sent over an IP network it is encapsulated inside of a large number of IP packets (each packet is fairly small since they are sent frequently and do not cause interruptions). In addition to the actual data, each IP packet also contains a header with the information required to route and process the packet.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

In the particular case of voice stream, the amount of actual data in the packet may be equal to or even less than the size of an IP packet header. Since bandwidth is used to transport both the header and the data – the actual amount of consumed bandwidth is higher than the codec's bitrate.

For instance, a g729 codec has 8 Kbps bitrate and requires about 31 Kbps of actual Internet bandwidth. You should remember that the total amount of required PortaSIP® bandwidth is twice the bandwidth required for all calls, since calls originate from both inside and outside the PortaSIP® system.

For example, if you anticipate a maximum of 60 simultaneous calls with the g729 codec, you will need 31.2 Kbps * 2 * 60 = 3.7 Mbps.

You can use a **VoIP Toolbox Bandwidth Calculator** to properly calculate the bandwidth consumption required by voice calls, depending on the codec being used.

... enable my SIP phone or ATA to be automatically provisioned by PortaSwitch?

First of all, you must make sure that your device supports auto-provisioning (see *APPENDIX F. SIP Devices with Auto-provisioning*). Then create the required IP phone profile and enter information about the IP phone into the inventory. Provision the SIP service as described in this manual, and then assign it to an available port on your IP phone in the account info screen for a SIP account.

Enter information about the provisioning server into your IP phone's configuration. In some cases, you may need to restart the IP phone in order to force a configuration update from the provisioning server.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

6. Appendices

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

APPENDIX A. Supported SIP RFCs

- RFC 2833 – "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals" is supported.
- RFC 2976 – "The SIP INFO Method" is supported: the PortaSIP® cluster is able to either resend INFO requests to a remote UA or extract DTMF information if a call scenario requires it.
- RFC 3261 – "SIP: Session Initiation Protocol" is supported with the following limitations:
    - The SIP URL domain is ignored in incoming requests.
    - For non-clustered solutions, in the case of a direct incoming connection from a remote SIP UA to a B2BUA (where the SIP proxy is not engaged in the SIP message exchange), only UDP transport protocol can be used. For the PortaSIP® cluster, TCP and TLS transport protocols are also supported.
    - Dialog forking is not supported when PortaSIP® is a User Agent Client.

- RFC 3262 – "Reliability of Provisional Responses in the Session Initiation Protocol (SIP)" is fully supported.
- RFC 3263 – "Session Initiation Protocol (SIP): Locating SIP Servers" is partially supported with the limitation that NAPTR records are not supported.
- RFC 3264 – "An Offer / Answer Model with the Session Description Protocol (SDP)" is partially supported for a late offer / answer model.
- RFC 3265 – "Session Initiation Protocol (SIP)-Specific Event Notification" is supported in the PortaSIP® cluster.
- RFC 3311 – "The Session Initiation Protocol (SIP) UPDATE Method."
- RFC 3323 – "A Privacy Mechanism for the Session Initiation Protocol (SIP)" is partially supported.
- RFC 3324 – "Short Term Requirements for Network Asserted Identity and 3325 – Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks" are partially supported.
- RFC 3327 – "Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts" is supported.
- RFC 3428 – "Session Initiation Protocol (SIP) Extension for Instant Messaging" is supported.
- RFC 3489 – "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)" is supported.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

- RFC 3515 – "The Session Initiation Protocol (SIP) Refer Method" is partially supported with the limitation that PortaSIP® does not report to the transferring party if the transferred party is unreachable.
- RFC 3550, RFC 1889 – "RTP: A Transport Protocol for Real-Time Applications" are partially supported with the limitation that if the RTP proxy generates the media stream (the actual voice traffic), it does not relay the RTCP packets.
- RFC 3551 – "RTP Profile for Audio and Video Conferences with Minimal Control" is supported, with the following limitation:
    - Not all encodings are supported.

- RFC 3581 – "An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing" is supported.
- RFC 3711 – "The Secure Real-time Transport Protocol (SRTP)" is supported (PortaSIP® passes encrypted packets between the phones and does not perform any encryption).
- RFC 3856 – "A Presence Event Package for the Session Initiation Protocol (SIP)" is supported.
- RFC 3963 – "SIP Extension for Event State Publication" is supported.
- RFC 3891 – "The Session Initiation Protocol (SIP) 'Replaces' Header" is supported.
- RFC 3951, 3952 – "Internet Low Bit Rate Codec (iLBC) and RTP Payload Format for iLBC" is supported for audio playback and for resending RTP streams.
- RFC 4145 – "TCP-Based Media Transport in the SDP" is partially supported.
- RFC 4235 – "An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP)" is supported.
- RFC 4244 – "An Extension to the Session Initiation Protocol (SIP) for Request History Information" is supported.
- RFC 4566, RFC 2327 – "SDP: Session Description Protocol" is supported, with the limitations and relaxations provided for SDP under SIP.
- RFC 4568 – "SDP Security Descriptions for Media Streams" is partially supported – for ordinary calls only.
- RFC 4572 – "Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the SDP)" is partially supported – for ordinary calls only.
- RFC 4961 – "Symmetric RTP / RTP Control Protocol (RTCP)" is supported, provided that PortaSIP® is used to transport the media stream (the actual voice traffic) from one endpoint to another.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

- RFC 5574 – "RTP Payload Format for the Speex Codec" is supported for audio playback and for resending RTP streams between end-points.
- RFC 5763 – "Framework for Establishing a Secure Real-time Transport Protocol (SRTP) Security Context Using Datagram Transport Layer Security (DTLS)" is partially supported – for ordinary calls only.
- RFC 5764 – "DTLS Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)" is partially supported – for ordinary calls only.
- RFC 5806 – "Diversion Indication in SIP" is supported.
- RFC 6189 – "ZRTP: Media Path Key Agreement for Unicast Secure RTP" is partially supported – for ordinary calls only.

APPENDIX B. Cisco GW Setup for PortaSIP (COMEDIA)

```
sip-ua
  nat symmetric check-media-src
```

APPENDIX C. Client's Sipura Configuration for PortaSIP

1. First, you need to know the SPA IP address. Via a touchtone telephone attached to the phone port on the SPA, press the star key four times (****). Then type 110# and the IP address will be announced.
2. Run a Web browser application on the same network as the SPA. Open a session in the SPA by typing http://<spa ip address>/admin/advanced.
3. Choose the specific phone port (click on **Line 1**, **Line 2** or another tab).
4. Provide values for the required parameters, which include:
    a. In **Proxy and Registration**:
        - **Proxy** – PortaSIP address (or hostname).
        - **Register** – **Yes**.
    b. In the **Subscriber** information part:
        - **Display Name** – Your identification (e.g. John Doe; this will be seen by the called party).
        - **User ID** – SIP account ID.
        - **Password** – Service password for your SIP account.
        - **Use Auth ID** – **No**.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

5. Submit all the changes and update the SPA configuration.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

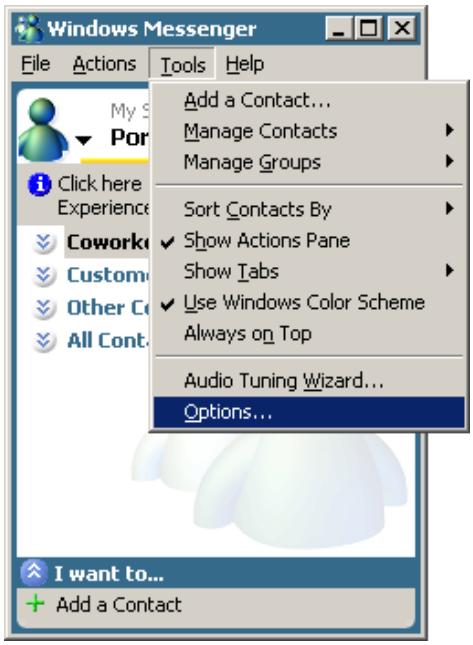
Network Settings			
SIP TOS/DiffServ Value:	0x68	Network Jitter Level:	high
RTP TOS/DiffServ Value:	0xb8		
SIP Settings			
SIP Port:	5060	SIP 100REL Enable:	no
EXT SIP Port:		Auth Resync-Reboot:	yes
SIP Debug Option:	none		
Call Feature Settings			
Blind Attn-Xfer Enable:	no	MOH Server:	
Xfer When Hangup Conf:	yes		
Proxy and Registration			
Proxy:	216.231.44.168	Use Outbound Proxy:	no
Outbound Proxy:		Use OB Proxy In Dialog:	yes
Register:	yes	Make Call Without Reg:	no
Register Expires:	3600	Ans Call Without Reg:	no
Use DNS SRV:	no	DNS SRV Auto Prefix:	no
Proxy Fallback Intvl:	3600		
Subscriber Information			
Display Name:		User ID:	1206001236
Password:	**********	Use Auth ID:	no
Auth ID:			
Mini Certificate:			
SRTP Private Key:			
Supplementary Service Subscription			
Call Waiting Serv:	yes	Block CID Serv:	yes
Block ANC Serv:	yes	Dist Ring Serv:	yes
Cfwd All Serv:	yes	Cfwd Busy Serv:	yes
Cfwd No Ans Serv:	yes	Cfwd Sel Serv:	yes
Cfwd Last Serv:	yes	Block Last Serv:	yes
Accept Last Serv:	yes	DND Serv:	yes
CID Serv:	yes	CWCID Serv:	yes
Call Return Serv:	yes	Call Back Serv:	yes
Three Way Call Serv:	yes	Three Way Conf Serv:	yes
Attn Transfer Serv:	yes	Unattn Transfer Serv:	yes

APPENDIX D. Configuring Windows Messenger for Use as a SIP User Agent

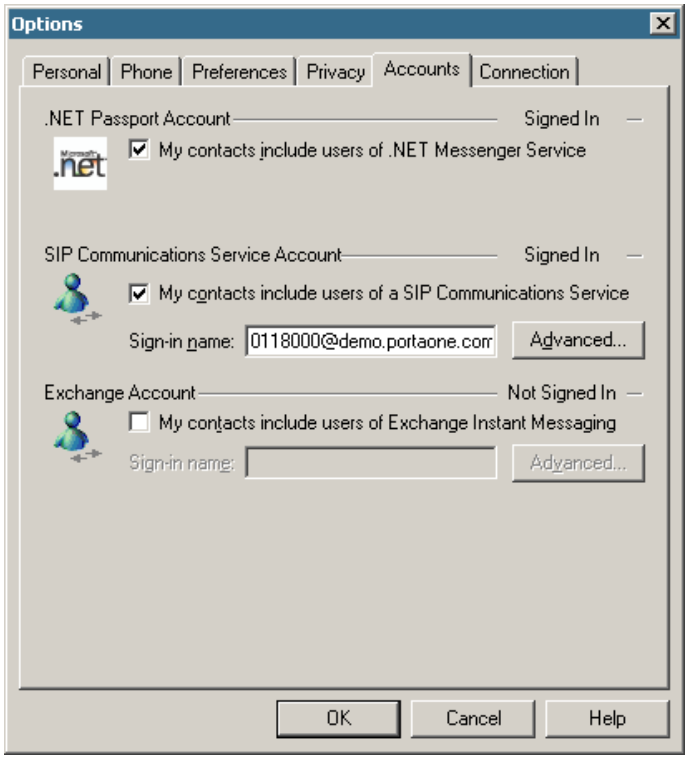
The following instructions apply to Windows Messenger version 5.0.

1. Start Windows Messenger, and select **Options** from the **Tools** menu.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

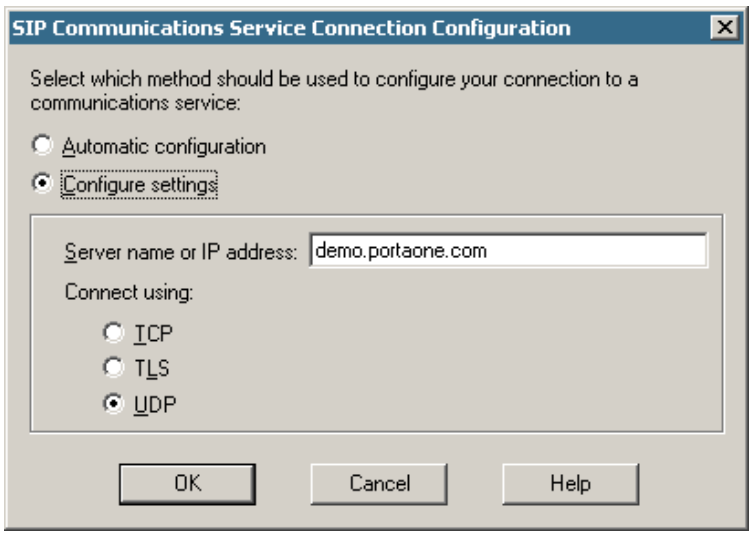


2. Check the **My contacts include users of a SIP Communication Service** check box. Enter your sign-in name as shown, in the form *username@address*, where *username* is the name of the appropriate account in PB and *address* is either the IP address of the PortaSIP server or its name in DNS. Then click the **Advanced** button.

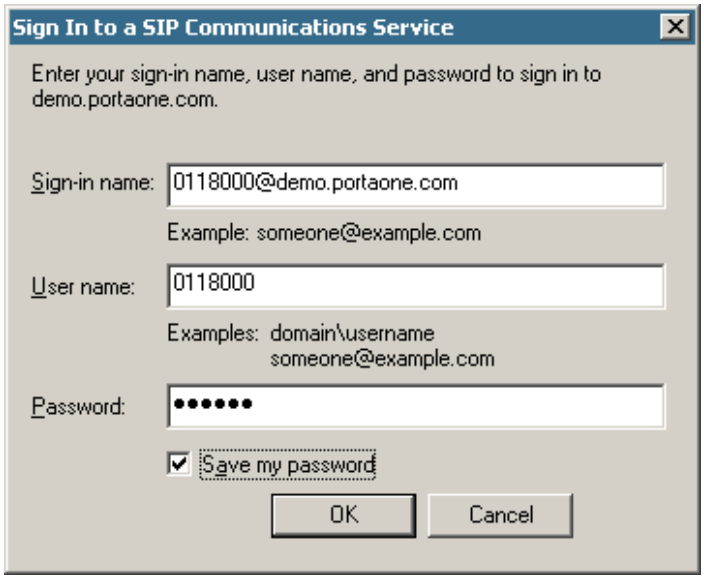


© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

3. Select the **Configure settings** option and enter the IP address of the PortaSIP server or its name in DNS in the **Server name of IP address**. Make sure that the **UDP** option is selected, then click **OK**.

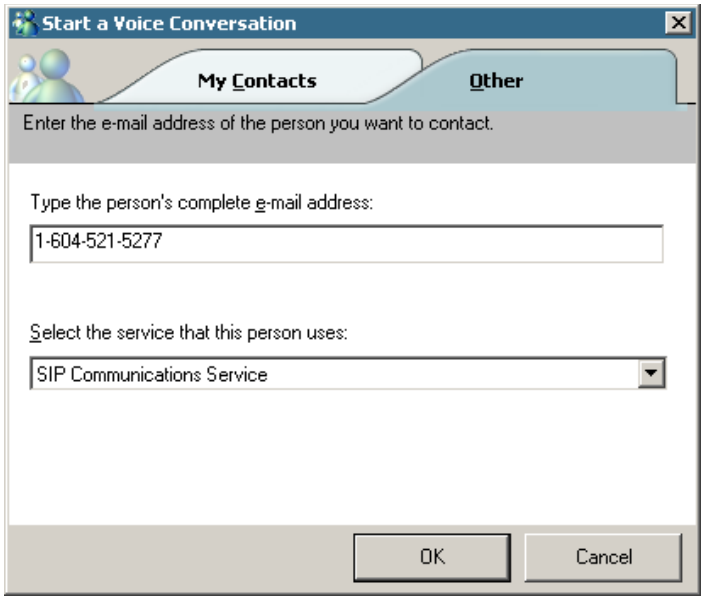


4. Sign out and then sign in again. You should see the dialog box. Fill it in as follows: **Sign-in name** in the form *username@address*, where *username* is the name of the appropriate account in PB and *address* is either the IP address of the PortaSIP server or its name in DNS. Enter the name of the appropriate PB account as the **User Name** and the appropriate account password as the **Password**, then click **OK**. You should now see your status change to online.



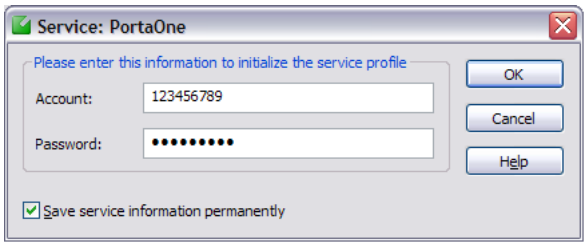
© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

5. To make a call, click **Action** in the main menu, then select **Start Voice Conversation**. Go to the **Other** tab, making sure that **Communications Service** is selected in the **Service** list, and enter the phone number in the **Enter e-mail add**ress field. Finally, click **OK** to place a call.



APPENDIX E. SJPhone Configuration for PortaSIP

1. First, you need to have the SJPhone installed on your machine. After the installation, start the SJPhone software and the following login dialog box will be displayed.



© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

2. Type key in the **Account ID** and password for the PortaSIP and click **OK**. SJPhone display should be similar to the one in the following snapshot, showing the account balance in "Ready to call" state. The phone is ready to be used.

3. Right click on the softphone and click **Login** to change or make corrections to the account / password.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

APPENDIX F. SIP Devices with Auto-provisioning

Currently, PortaSwitch can auto-provision the following SIP phones/ATAs:

- Cisco ATA 186 (firmware versions 2 and 3)
- Cisco SPA-122
- Cisco SPA-504G
- Cisco SPA-8000
- Sipura 1001
- Sipura 2000
- Sipura 2002
- Sipura 2100
- Sipura 3000
- Linksys PAP2 (PAP2T)
- Linksys RTP-300
- Linksys/Sipura SPA-2102
- Linksys SPA-941
- Linksys SPA-942
- Linksys SPA-921
- Linksys SPA-922
- Linksys SPA-3102
- Linksys SPA-962
- Linksys WRT54GP2
- GrandStream DP715
- Grandstream GXP1160
- Grandstream GXP1165
- GrandStream GXP1400/1405
- GrandStream GXP1450
- GrandStream GXP2130
- GrandStream GXP2140
- GrandStream GXP2160
- GrandStream GXV3240
- Grandstream GXV3275
- GrandStream GXW400x
- GrandStream HT286
- GrandStream HT486
- GrandStream HT488
- GrandStream HT496
- GrandStream HT502

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

- GrandStream HT503
- Grandstream HT701
- GrandStream HT702
- Grandstream HT704
- Polycom SoundPoint IP 331
- Polycom SoundPoint IP 335
- Polycom SoundPoint IP 650
- Polycom SoundPoint IP 670
- Polycom SoundPoint IP 5000
- Polycom SoundPoint IP 6000
- RCA Telefield IP110
- RCA Telefield IP160
- RCA Telefield IP170
- RCA Telefield IPX500
- Siemens A580IP
- Thomson TWG850 (only eMTA part)
- Yealink CP860.
- Yealink SIP-T19P
- Yealink SIP-T20P
- Yealink SIP-T21P
- Yealink SIP-T21P E2
- Yealink SIP-T22P
- Yealink SIP-T23G
- Yealink SIP-T23P
- Yealink SIP-T26P
- Yealink SIP-T27P
- Yealink SIP-T28P
- Yealink SIP-T29G
- Yealink SIP-T32G
- Yealink SIP-T38G
- Yealink SIP-T41P
- Yealink SIP-T42G
- Yealink SIP-T46G
- Yealink SIP-T48G
- Yealink T19P E2
- Yealink VP530 IP video phone (firmware version 7x)
- Yealink W52P IP DECT phone
- OneNetUno ATA-171
- Motorola CPEi (Motorola NBBS Device Management Platform is required)
- Fanvil E52
- Fanvil F52

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

- Fanvil E58
- Fanvil C58
- Fanvil E62
- Fanvil C62

We are constantly working to extend the list of supported IP devices. If the IP phone you plan to use is not listed here, please contact us – it may already be scheduled for a future release, or we may include it at your request.

APPENDIX G. Service Policy Configuration for Ring-back Tone Generation and Early Media Relaying

The table below provides information on resultant system's behavior, depending on the service policy options configured for both calling and called parties:

Calling party (Call from Vendor / Account)		Called party (Calls to Vendor / Account)	Resultant behavior
call_progress_ notification	**call_progress_ filter**	**call_progress_ filter**	
signaling	full_progress	full_progress	18x call progress responses are sent to the caller without conversion. Early media (if sent by the callee's SIP UA) is relayed.
audio_rbt	full_progress	full_progress	• 18x response is received without the SDP – The RTP proxy immediately plays the uploaded ring-back media file to the caller. • 18x response is received with the SDP – The RTP media packets are expected. If they

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com

			are not received within a predefined timeout, the RPT proxy plays the uploaded ring-back media file to the caller. Early media (if sent by the callee's SIP UA) interrupts the ring-back tone and is relayed to the caller.
mow	full_progress	full_progress	The RTP proxy plays the Music on Waiting prompt upon receiving a 182 Queued response without the SDP. The rest of the 18x call progress responses are relayed without conversion. Early media (if sent by the callee's SIP UA) interrupts the Music on Waiting prompt and is relayed to the caller.
signaling / mow	full_progress	ringing_only	All 18x call progress responses and media from the called party are passed as a 180 Ringing message to the caller's SIP UA. The Music on Waiting prompt cannot be played.
audio_rbt	full_progress	ringing_only	Upon receiving an 18x response, the RTP proxy immediately plays the uploaded ring-back media file to the caller.
–	ringing_only	–	All 18x call progress responses and media from the called party are turned into a 180 Ringing message.

© 2000–2016 PortaOne, Inc. All rights Reserved. www.portaone.com