

Porta  **SIP™**



Administrator Guide

Maintenance Release 22

Copyright Notice & Disclaimers

Copyright © 2000-2011 PortaOne, Inc. All rights reserved.

PortaSIP Administrator Guide, March 2011

Maintenance Release 22

V.1.22.5

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 4

Hardware and Software Requirements 5

Installation 5

What's New in Maintenance Release 22? 6

Important Upgrade Notes 7

1. System Concepts 10

PortaSIP's Role in Your VoIP Network..... 11

PortaSIP Components..... 13

PortaSIP® Performance 14

Call Handling Rules..... 15

Call Process / Supported Services..... 17

PortaSIP Presence Server..... 26

Instant Messaging..... 27

Call Recording..... 29

Virtual SIP Servers 30

Clustering of PortaSIP Servers 31

Call Flow Scenarios for a PortaSIP Cluster..... 33

Understanding SIP Call Routing..... 37

NAT Traversal Guidelines 38

Auto-provisioning IP Phones 45

PortaSIP and Emergency Services (E911) 48

2. Advanced Features 50

User Authentication 51

IP Centrex Feature Management..... 54

Call Transfer..... 54

Call Forwarding 57

Selective Call Processing..... 62

Call Parking..... 63

Call Barring 65

Paging / Intercom Calls..... 65

SIP Identity..... 66

Support for Privacy Flags 69

Service Announcements via the Media Server 71

NAT Keep-alive..... 72

Keep-alive Call Monitoring..... 73

First Login Greeting 73

SIP TAPI..... 73

Direct Incoming Calls to B2BUA..... 74

VoIP from Vendor Connection..... 74

Legal Call Intercept..... 76

Secure Calling..... 76

Voice VPN Rating..... 76

Voice On-net Rating 77

3. IP Centrex Features 78

4. How to	84
... configure my Cisco gateway to accept incoming SIP calls and terminate them to a telephony network?.....	85
... configure my Cisco gateway to send outgoing calls using SIP?	86
... configure my Cisco gateway for PSTN->SIP service?	87
... support incoming H323 and SIP calls on the same gateway?.....	87
... provide services to and bill a customer who has a SIP-enabled gateway but no authorization capability (e.g. Cisco AS5350)?.....	88
... make all SIP calls to a certain prefix NNN go to my gateway XXX?..	88
... allow my customer to have two phone numbers from different countries which will both ring on the same SIP phone?.....	89
... create an application to handle PSTN->SIP calls on Cisco gateway?89	
... configure SIP phone X made by vendor Y?.....	89
... bill incoming calls from PSTN to SIP using a special rate?	90
... bill using different rate plans for incoming, outgoing and forwarded calls?	90
... provide error messages from the media server in my users' local language.....	91
... calculate how much bandwidth I need for my PortaSIP server?	91
... enable my SIP phone or ATA to be automatically provisioned by PortaSwitch?.....	92
5. Administration / FAQ.....	93
Troubleshooting Common Problems	94
FAQ.....	95
6. Appendices	99
APPENDIX A. Supported SIP RFCs.....	100
APPENDIX B. Cisco GW Setup for PortaSIP (COMEDIA).....	101
APPENDIX C. Client's Sipura Configuration for PortaSIP	101
APPENDIX D. Configuring Windows Messenger for Use as a SIP User Agent.....	103
APPENDIX E. SJPhone Configuration for PortaSIP.....	106
APPENDIX F. SIP Devices with Auto-provisioning.....	108

Preface

This document provides PortaSIP (PortaSwitch) users with the most common examples and guidelines for setting up a VoIP network. The last section of the document answers the most frequent questions users ask after running PortaSwitch for the first time.

Where to get the latest version of this guide

The hard copy of this guide is updated at major releases only, and does not always contain the latest material on enhancements occurring in-between minor releases. The online copy of this guide is always up-to-date, integrating the latest changes to the product. 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**
- Terminal sessions, console screens, or system file names are displayed in fixed width font



The **exclamation mark** draws your attention to important information or actions.

NOTE: Notes contain helpful suggestions about or references to materials not contained in this manual.



Timesaver means that you can save time by performing the action described in the paragraph.



Tips provide information that might help you solve a problem.

Trademarks and Copyrights

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

Hardware and Software Requirements

Server System Recommendations

- One UNIX Server.
- A minimum of 80 GB of available disk space; this space is required for storing various log files
- An i386 processor (Xeon, Opteron) with 64bit support. Additional processor speed is needed for networks with a high call volume.
- At least 4 GB of RAM, 8 GB recommended.
- At least one USB port.

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

<http://www.portaone.com/support/faq/hardware-requirements/hardware-requirements/>

For information about whether particular hardware is supported by Oracle Enterprise Linux from the JumpStart Installation DVD, consult the related document on the Oracle or RedHat website:

<https://hardware.redhat.com/>

Installation

A jumpstart installation DVD is provided for all PortaOne products. This DVD contains installation media for Oracle Enterprise Linux (64-bit version), supplementary packages necessary for convenient system administration and maintenance, and all required software packages. 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**.

What's New in Maintenance Release 22?

This release includes several new features and improvements:

- **Caching Authentication Results** – the SIP proxy in PortaSIP performs caching of registration information if user authentication has been done successfully, so there is no need to send authentication requests to PortaBilling for subsequent registration requests within a relatively short time interval. This allows PortaSIP's capacity to double in terms of registration attempts processed per second, and it protects the system from a “registration storm” (whether unintended or part of a denial-of-service attack).
- **Call Forward Info** – When an incoming call to some account (e.g. account A, representing an external DID) is forwarded to another account (e.g. account B, provisioned on the actual SIP phone) - the visible call forward info feature in PortaSwitch enables to include identification of the forwarder (account A) in the outgoing call information. Thus when user B receives the call, he/she can easily determine the origin of incoming calls and respond accordingly.

Important Upgrade Notes

We try to make the process of upgrading as easy as possible, and to keep our releases backward compatible. Here are just a few things you should remember when upgrading:

- The proxy server is now using a new release of the SIP stack libraries (resiprocate 1.6). Although we have conducted extensive testing in our labs to ensure backward compatibility, customers using older versions of IP phones or IP phones with known SIP RFC compatibility issues are advised to test their phones using a new release of PortaSIP with a staging system – prior to upgrading their production system.
- The “CLD Tech-Prefix” mode of authorization (configured via Call Handling) previously included both tech-prefix and the remote IP address in the authorization ID (so a call arriving from IP address 1.2.3.4 and destination number 567#1234567 would be authenticated using a **567#1.2.3.4** ID). In maintenance release 22, the “CLD Tech-Prefix” mode of authorization will only use the actual tech-prefix (**567#** in our example) as the ID. If you wish to authorize by tech-prefix and IP address – use the “CLD Tech-Prefix and IP” authorization mode, which will authenticate by using a **567#@1.2.3.4** ID (please note the added @ symbol separating the tech-prefix from the IP address). All of your existing call handling rules will automatically change to this authorization mode when the upgrade is performed. And for any accounts that had ID in the form “tech-prefix+IP” (e.g. **123#5.6.7.8**) their ID will automatically be changed to include the @ symbol (becoming **123#@5.6.7.8**).

Handling of incoming calls

Previously, a call made by a customer in your network would only be charged to the account and the customer who originated the call, and the CDR would be stored under that account. If the call was made between two phone lines within your network, it meant that only the caller would see the CDRs. This has been changed since MR21 – so a call coming to an account is always charged to that account and the CDRs for an incoming call are always visible for the recipient of the call, whether the call originated outside the network or from another account within the network.

So how does this change affect you? The difference will only be noticeable in two situations:

- calls made between accounts on your network (e.g. when calls are made within the same IP Centrex, or when a call is made from an

- IP phone belonging to customer A to a phone number belonging to customer B);
- incoming calls from PSTN, when for some reason there was no “VoIP from Vendor” connection configured, and instead the calls were treated as if coming from a “fake” customer account. This is definitely not advisable, so you should consider moving to “VoIP from Vendor” instead.

In MR20, no CDRs were produced for the recipient of the calls in these scenarios, so he was not billed for such incoming calls. In MR21 and later, however, the recipient is billed for these calls.

For the authorization and rating of an incoming call the applicable tariff plan is selected from the rating table based on a combination of the PortaSIP node, which connects the call, and the INCOMING access code. If and only if an entry with the INCOMING access code does not exist, then the applicable rate will be retrieved from the tariff, associated with the default entry (which has an empty access code).

Within that tariff, a rate for the phone number used on the SIP phone is selected. This allows you to apply different rates based on phone numbers distributed to SIP phones. For example, incoming calls to local numbers from the US or Canada are free, incoming calls to UK numbers are charged at \$0.01/minute and incoming calls to toll-free numbers are charged at \$0.03/minute.

If the rating table in your product for IP Centrex / hosted IP PBX services does not contain a separate tariff assignment for incoming calls (an entry with INCOMING access code), and only contains an entry for PortaSIP and an empty access code – this tariff will be used for rating both incoming and outgoing calls. Since the situation when an incoming call is rated according to the rate for outgoing calls will almost certainly produce an incorrect charge – this should be avoided. The proper long-term solution is to add a separate entry (with the INCOMING access code) and the correct tariff for calculating the incoming charges to the list of access points in the product. Keep this in mind when creating a new product on your system after the upgrade.

During the migration from MR20 to MR21 (or a later) release, the list of access points for existing products should be reviewed, taking into consideration the requirements for a separate entry for incoming calls (as described above).

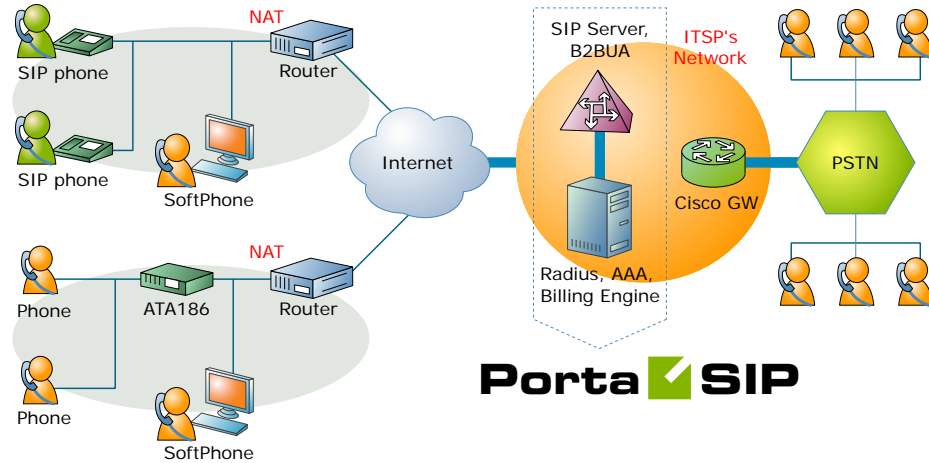
In order to provide backward compatibility, PortaOne offers a migration script that will, during the update process, automatically insert a rate with zero price per minute for a special VOICEONNETIN destination into every existing tariff used to charge your customers. As a result, although the tariff for outgoing calls is still used to charge incoming calls, this

special rate will be used and for both of the scenarios described above a CDR will be produced with a zero charged amount. This will not affect the customer's bill, and so from his perspective everything will work just as it used to.

It is recommended that you perform automated migration, then adjust the configuration by creating a separate tariff for charging incoming calls and adding an extra entry in the product's accessibility list, including the PortaSIP node, the INCOMING access code, and the tariff you just created.

1 . System Concepts

PortaSIP's Role in Your VoIP Network

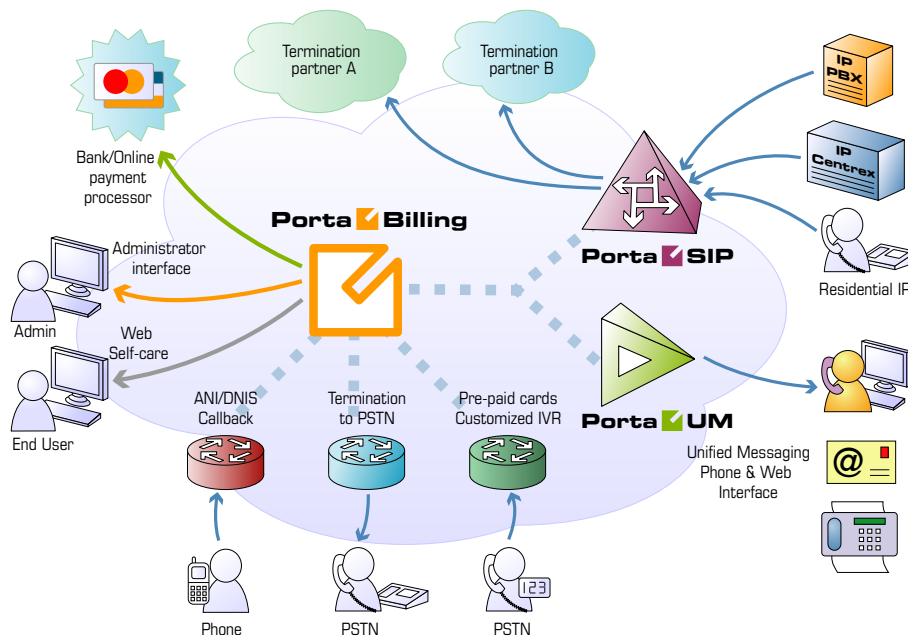


PortaSIP is a call control software package enabling service providers to build scalable, reliable VoIP networks. Based on the Session Initiation Protocol (SIP), PortaSIP provides a full array of call routing capabilities to maximize performance for both small and large packet voice networks.

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 and wholesale traffic exchange services.

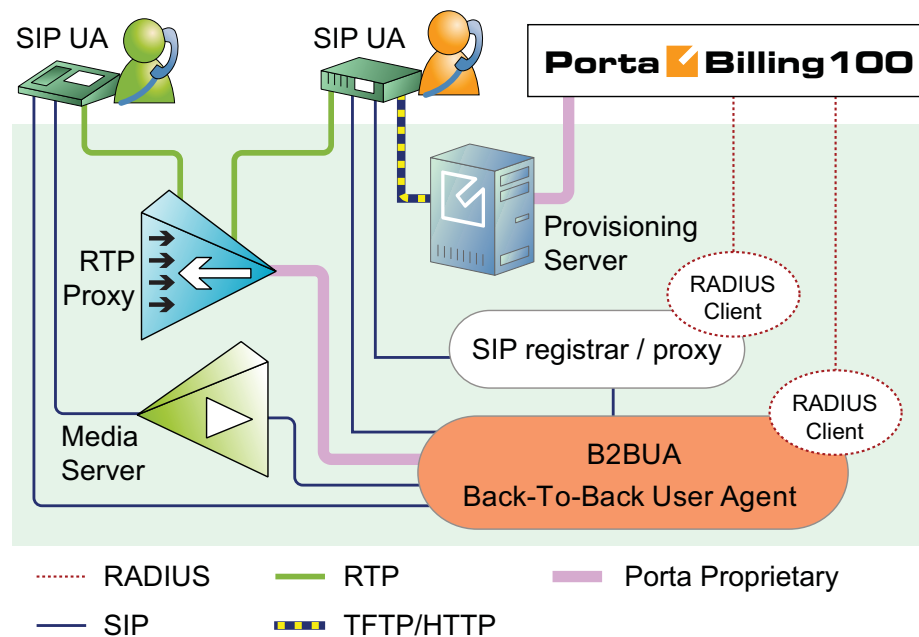
PortaSIP functions



PortaSIP provides the following functionalities:

- SIP registration, allowing SIP phones to use the service from any IP address (static or dynamically assigned)
- Customizable greeting upon successful service activation
- Authorization for all incoming calls
- Customer numbering plans to ensure correct phone number translation
- Facilitation of communication between SIP phones behind a NAT
- Error announcements from the media server
- Automatic disconnect of calls when the maximum credit time is reached
- Automatic disconnect of calls when one of the parties goes offline due to a network outage
- Various IP Centrex features: call waiting, call hold, music on hold, abbreviated dialing, follow-me, etc.
- Fail-over routing (a list of routes arranged according to cost, preference and customer routing plan is supplied by PortaBilling100)
- Forwards calls to the unified messaging service (PortaUM) if a SIP phone is not available

PortaSIP Components



PortaSIP components:

- **SIP Proxy Server:** The SIP Proxy Server performs a number of functions, such as registering SIP telephones, dealing with NAT issues, etc.
- **Back-To-Back User Agent (B2BUA):** The B2BUA SIP-based logical entity can receive and process INVITE messages as a SIP User Agent Server (UAS). It also acts as a SIP User Agent Client (UAC), determining how the request should be answered and how to initiate outbound calls. Unlike a SIP proxy server, the B2BUA maintains the complete call state. Integrating B2BUA with PortaSIP ensures that every call made between endpoints (off-net, on-net, etc.) is authorized, authenticated and billed. The system is also able to provide prepaid services (i.e. to disconnect a call if the account balance falls below zero). Also, B2BUA can automatically disconnect the other call leg if the SIP phone goes offline due to a network problem.
- **RTP Proxy:** The RTP Proxy is an optional component used to ensure a proper media stream flow from one SIP telephone to another when one or both of them are behind a NAT firewall.
- **Media Server:** The Media Server is used to play a number of short voice prompts to an SIP user when an error occurs, such as zero balance, invalid password, and so on.

PortaSIP® Performance

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

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

A PortaSIP server (assuming this is a server which meets the hardware requirements described on www.portaone.com) can process about **20 call attempts per second**. This means that 20 users can start a new phone call on your network each second (and the same amount of users will end their calls during that second). In addition, the PortaSIP server can process 50 registration attempts per second. Assuming that each phone re-registers every 10 minutes on average, this translates to **30,000 simultaneously registered SIP phones**.

How many concurrent calls does that translate into?

Assuming PortaSIP is working in signaling-only mode, this primarily depends on the average call duration (ALOC) and call success rate (ASR). Given an aggregated call processing speed of 20 call attempts per second, an average call duration of 5 minutes, and a call success rate of 50% (the industry norms), this means that 50% of the 20 call attempts per second will succeed. So 10 calls will be connected, while the same amount of previously connected calls will be disconnected. Since the average call duration is 300 seconds, this means that at all times approximately $10 * 300 = 3,000$ calls will be in a “connected” state. Obviously if your ASR or ALOC change, it will 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 stream that has to pass through the server. Voice traffic is extremely sensitive to delays in processing, so using a high-end network adapter is highly recommended.

A single PortaSIP instance can proxy up to **750 concurrent calls**. Note that in order to handle such a high number of proxied calls you must allocate a sufficient amount of bandwidth, since 750 calls using the g729 codec will consume about 48 Mbit/s of bandwidth (for both incoming and outgoing traffic).

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 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 processing 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 be satisfied for each of the following parameters of an incoming call:

- 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 be satisfied 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 a list of call handling rules is defined, PortaSIP starts by evaluating the conditions for the first rule. If they are not satisfied, the conditions for the second rule are evaluated, and so on, until a rule is found where all the conditions are satisfied. The evaluation process stops there, and this rule is used to process 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.

Available call handling scenarios

These include:

- Apply digest authentication (this is the default call handling scenario).
- Use authentication by remote IP.
- Use authentication by 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.

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.

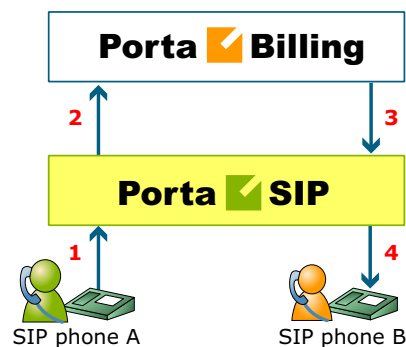
These auto-created rules are displayed on a separate tabs in **the Call Handling** screen, so you can easily distinguish them from the rules, created by administrators.

Call Process / Supported Services

SIP UA <--> SIP UA

An example: a customer purchases our 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:

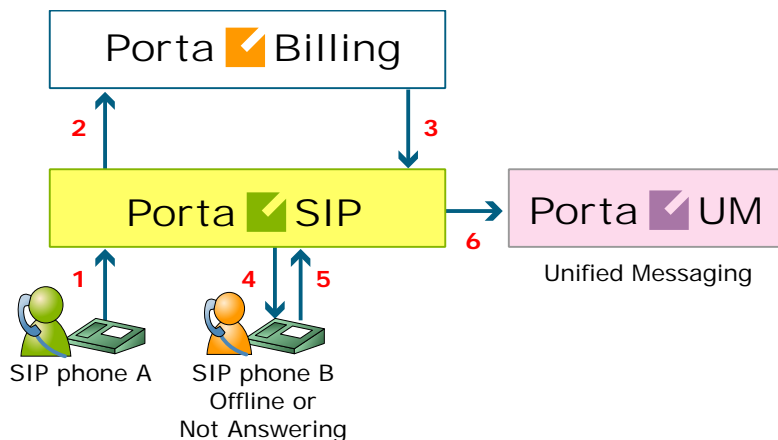
- User A dials user B's number (121). His SIP user agent sends an INVITE request to the SIP server (1).
- The SIP server sends an authorization request to the billing (2).
- Billing performs several operations:
 - Checks that such an account exists, that it is not blocked/expired, that the supplied password 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 (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 dialed number is one of our SIP accounts, if it is currently registered, and what is the NAT status of both SIP phones.

Based on the results of the above operations, billing 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 sends an INVITE to the SIP user agent for user B (4).
- If one of the SIP phones is behind NAT, the SIP server will be instructed by the billing 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.

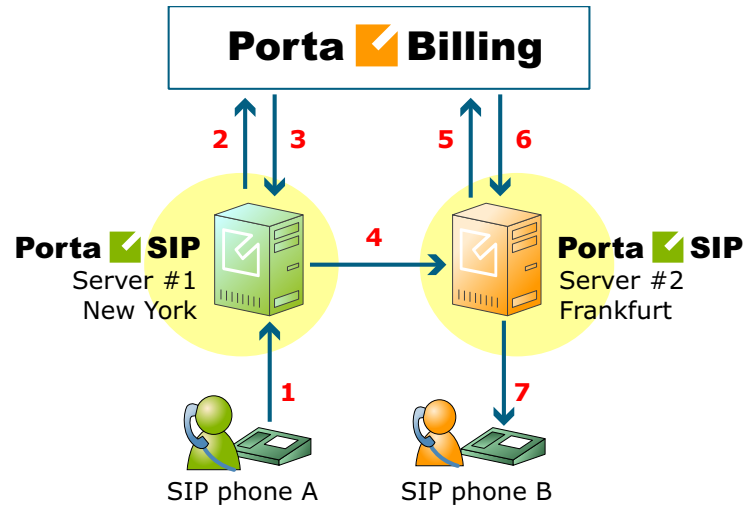
The called party is not online



- User A dials 121 in an attempt to reach user B. His SIP user agent sends an INVITE request to the SIP server (1).
- The SIP server performs authorization in the billing (2). The billing will perform number translation and determine whether the destination number is actually an account.
- The billing checks the registration database, but finds that this account is not online at the moment. If B has unified messaging services enabled, the billing will return routing (3) for this call, which will be sent to the UM gateway. 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 several PortaSIP servers

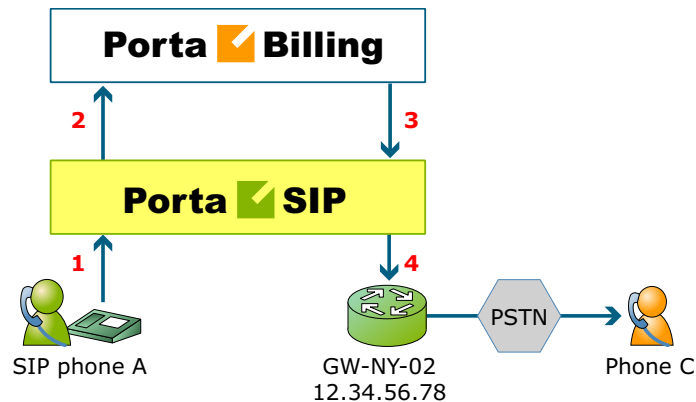
You can use several PortaSIP servers simultaneously for improved reliability or better network utilization. Let's assume you have two PortaSIP servers, the primary one in New York, and a second one installed in Frankfurt. The Frankfurt's PortaSIP serves most of your European customers (i.e. they connect 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 will try to register there if the New York server is down or for some reason inaccessible.



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

- A dials B's number (4981234567). His SIP user agent sends an INVITE request to PortaSIP server #1 (1).
- The SIP server sends an authorization request to the billing (2).
- After all the usual authorization checks, the billing discovers that the dialed number is one of our SIP accounts, but is currently registered to PortaSIP server #2. It instructs the SIP server to route this call to the IP address of PortaSIP #2 (3).
- PortaSIP server #1 sends an INVITE request to PortaSIP server #2 (4).
- Upon receiving this INVITE, PortaSIP #2 sends an authorization request to the billing (5).
- The billing authorizes the call, since it comes from a trusted node, and requests that the call be sent to the locally registered SIP UA (6).
- The SIP server sends an INVITE request to the SIP phone (7).

SIP UA -> PSTN

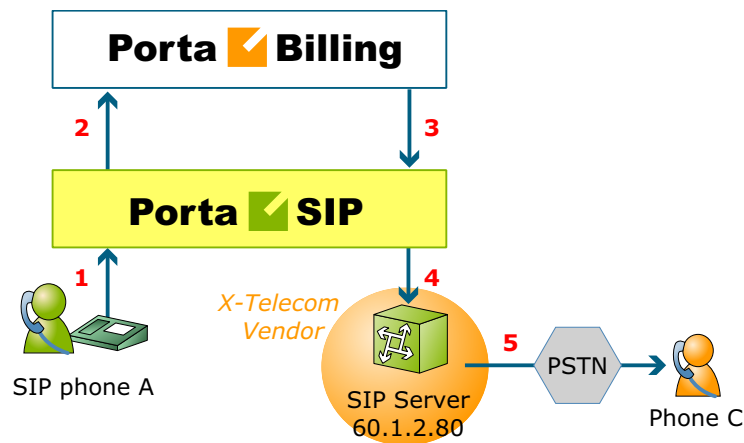


- User A attempts to call his co-worker, user C. C has not been assigned a SIP phone yet, thus he only has a normal PSTN phone number from the 202 area code, and A dials 3001234. A's SIP user agent sends an INVITE request to the SIP server (1).
- The SIP server sends an authorization request to the billing (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).

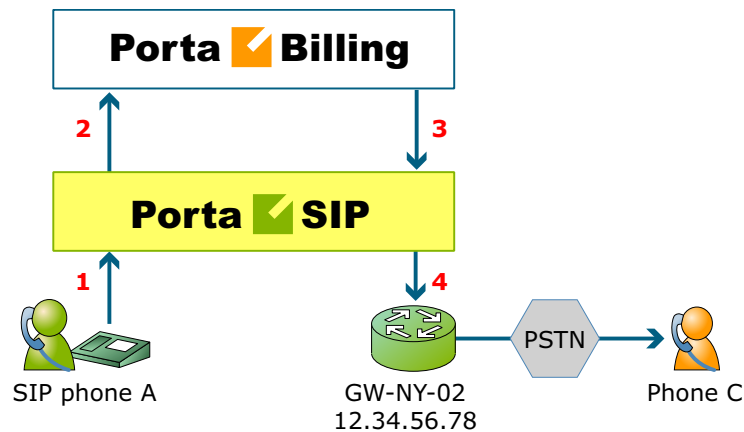
- The SIP server tries to send a call to all routes returned by the billing sequentially, until either a connection is made or the list of routes is exhausted (4).
- When the call is finished, the SIP server sends accounting information to the billing.

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, 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.

Terminating SIP calls to a vendor using telephony

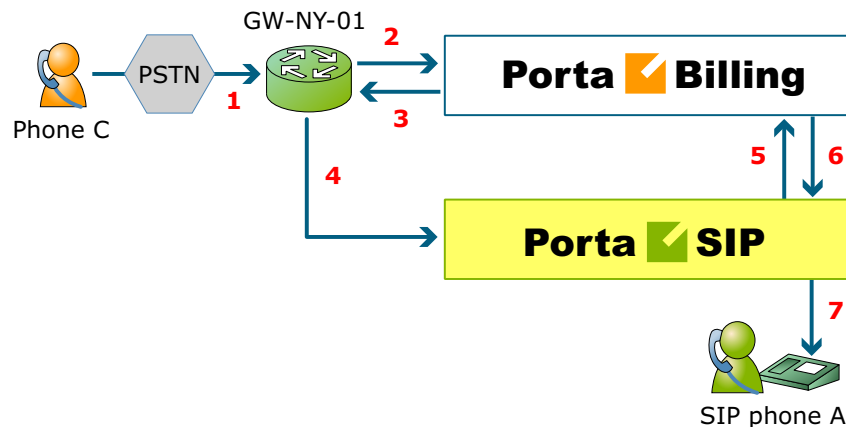


- Let's assume that T1 is connected to Qwest on our gateway **GW-NY-02** in New York, where we are able to terminate calls to the US. This connection would be described as a **PSTN to vendor** connection. The PortaSIP server obtains the address of the GW-NY-02 gateway in the route information.
- The 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. 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.

PSTN -> 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 (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).

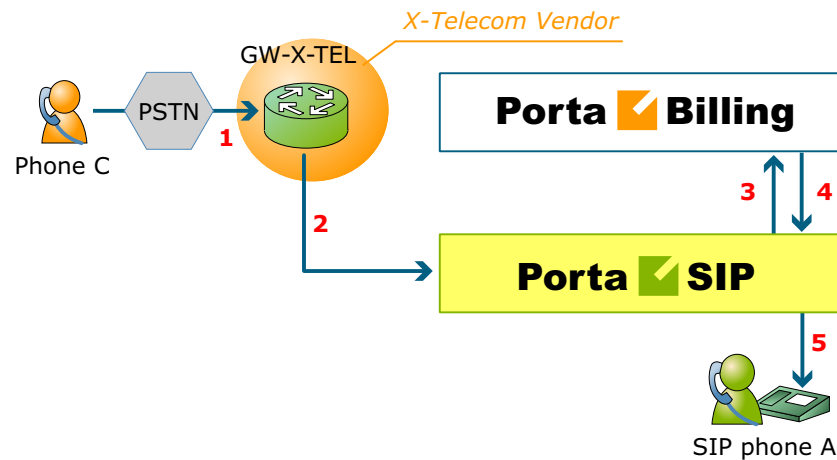
NOTE: The gateway cannot make this call "on behalf" of A, since even if we know A's account ID, we do not know A's password; therefore, such a call will be rejected. In addition, Cisco gateways currently do not support INVITE with authorization.

- 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. 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 -> SIP (via VoIP DID Provider)

In the previous section we discussed traditional PSTN->SIP service, when a call is delivered to your gateway via E1/T1 lines and then forwarded to a SIP phone. Unfortunately, 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”.



- 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 (3).
- The billing 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.

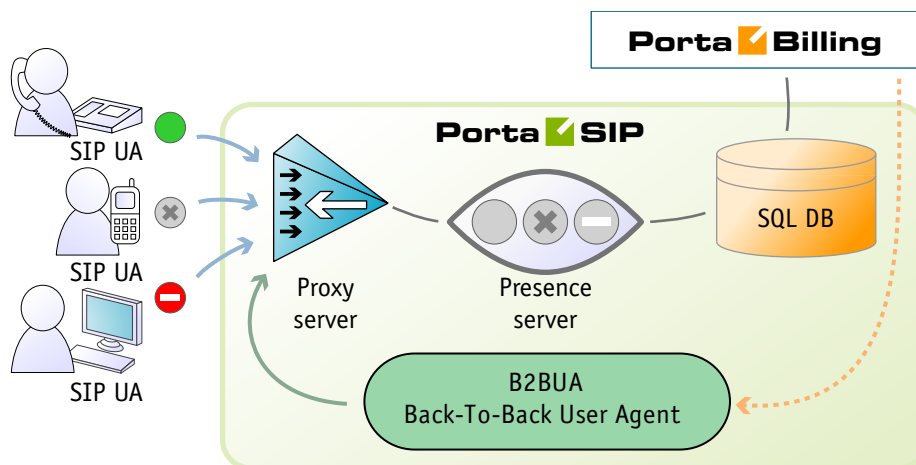
PortaSIP Presence Server

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 nearby a communication device, and so on. 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.

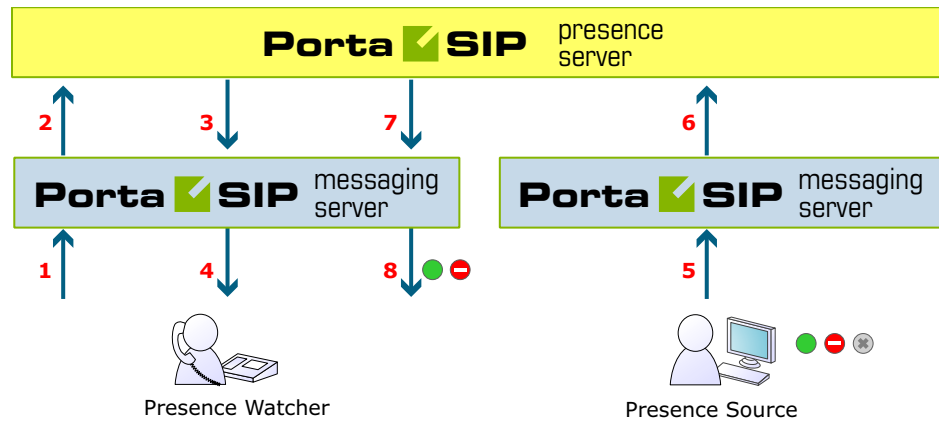
In order to provide such services, i.e. to handle presence requests, a PortaSIP presence server is required. This server is a backend component that interacts with the PortaSIP proxy server and maintains online information for all users registered within your network. It allows SIP user agents to publish/subscribe requests and respond to them, and to generate notifications of changes in presence status.



PortaSIP's presence service can run on the same physical server where the PortaSIP software package is installed.



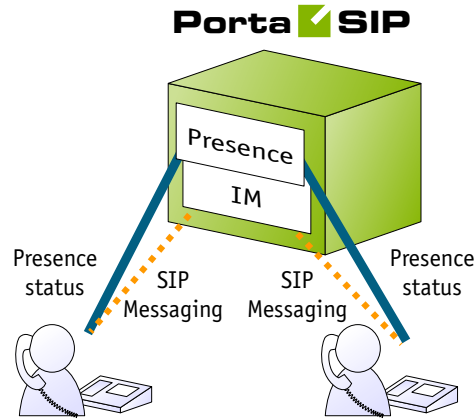
Typically, the whole process functions in the publish/subscribe manner. Presence information is published from a certain source, e.g. mobile phones, laptop computers, PDAs, desktop PCs, or even other application servers. The PortaSIP presence server then sends the combined presence data to all watchers who have subscribed to the presence service for the given user. The presence server merges this information to form a complete overview of the each user's presence information.



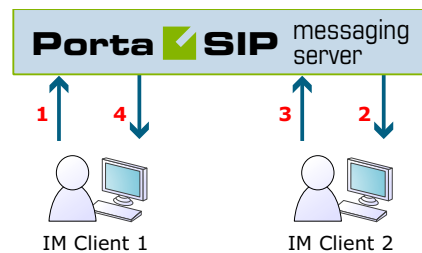
- The SIP user agent sends a SUBSCRIBE request to the PortaSIP proxy server (1); if authorized successfully, the SUBSCRIBE request is forwarded to the PortaSIP presence server (2).
- Based on the results, the PortaSIP presence server sends a notification response (3) via the PortaSIP proxy server (4) back to the user agent.
- The user agent (presentity) sends a PUBLISH request to the PortaSIP proxy server (5); if authorized successfully, the request is forwarded to the PortaSIP presence server (6).
- The presence server sends a NOTIFY request to the PortaSIP proxy server (7), which identifies SIP user agents (watchers) subscribing to presence for the given user, and forwards them a NOTIFY request (8).

Instant Messaging

Instant Messaging (IM) is defined as the exchange of text messages between two users in real time. As a service, IM is always coupled with the presence service (see earlier in this chapter). For example, when a friend comes online, a user can be notified of this and have the option of sending his friend an instant message. Supported by wide range of multimedia clients such as MS Messenger, instant messaging can be easily used to post messages from any computer or mobile device.



PortaSIP includes an advanced messaging module that enables online messaging, server-side message storage for offline users (so they can receive messages later), and the option of maintaining full message history on the server. The messaging module is implemented as an internal part of the PortaSIP proxy server, and enables communication between users by means of SIP MESSAGE packets.



A basic instant messaging flow will look like this:

- 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.
- To make themselves available for contact via a particular SIP user agent, users send a SIP REGISTER message to the PortaSIP proxy.
- Once users have been registered, they can send MESSAGE requests to each other via the PortaSIP proxy.
- When a message reaches its destination, a 200 OK response is returned. (This does not necessarily mean the message has been read by its recipient.)

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.
- 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.

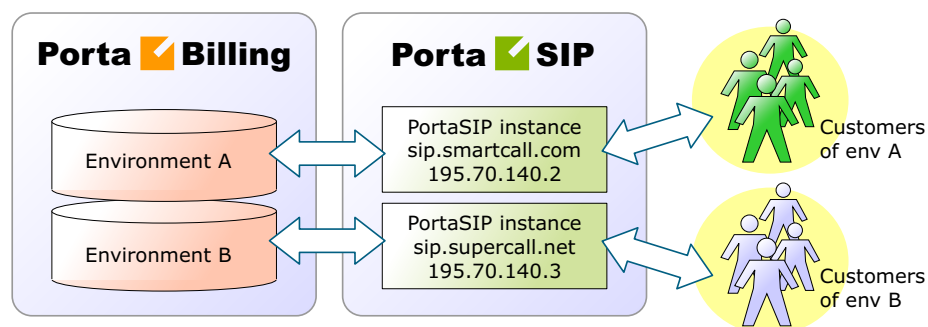
Important notes

- 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 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 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 SIP server side is an extra IP address (IP alias) allocated to that server.

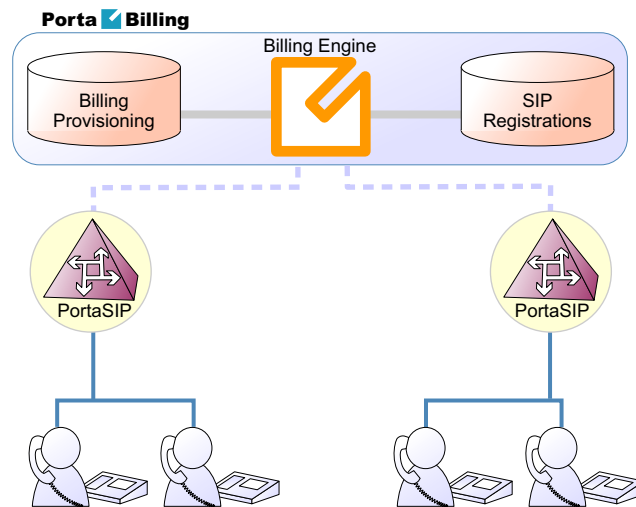


Every virtual SIP server acts as an independent PortaSIP installation.

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.

Clustering of PortaSIP Servers

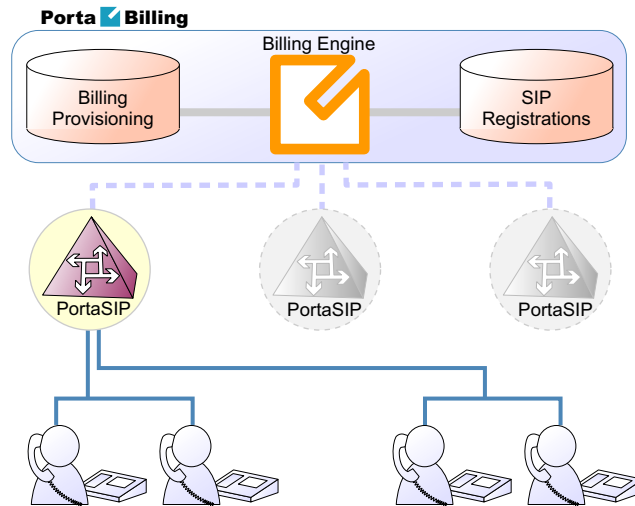
You may also install several physically independent PortaSIP servers and connect all of them to the same virtual environment in PortaBilling100. In this case, several PortaSIP servers (combined in this case into a PortaSIP cluster) communicate with a single central billing, which provides all the required service provisioning information and maintains a global database of SIP phone registrations. A SIP phone user may connect to any of the available PortaSIP servers (only those which are available to him via his product's accessibility, of course). Once a SIP phone is successfully registered to one of the SIP servers, the information is globally available within this PortaSwitch environment.



By installing several independent PortaSIP servers you can achieve two main goals:

- Improve the reliability of your network
- Optimize call flow on your network so as to better utilize the available network infrastructure.

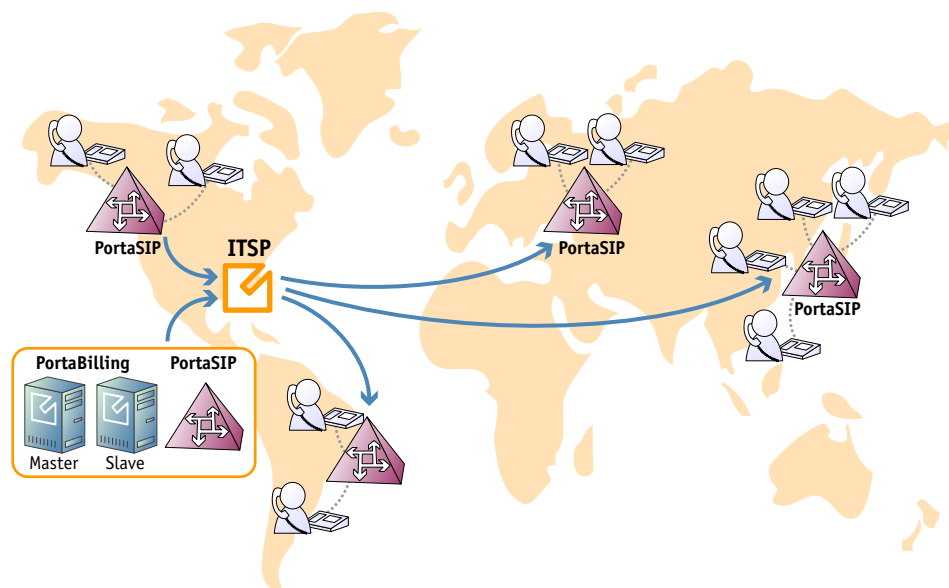
Improved Reliability



Even if one of the SIP servers is down due to network issues or hardware problems, your subscribers can continue using the service via other SIP servers.

Better Network Utilization

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.

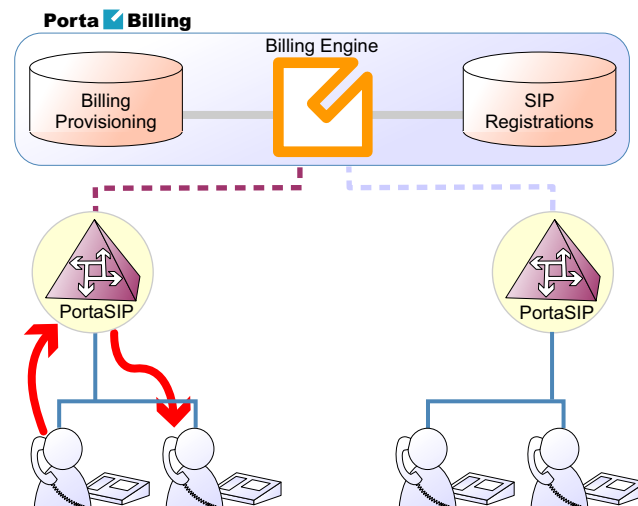


This allows VoIP services to be efficiently provided in a situation which is highly typical for many countries or regions: good, fast Internet connectivity inside the country/region and mediocre connectivity with the rest of the world. For all users inside that region, VoIP traffic (signaling and RTP)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

Call Flow Scenarios for a PortaSIP Cluster

SIP UA <--> SIP UA

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

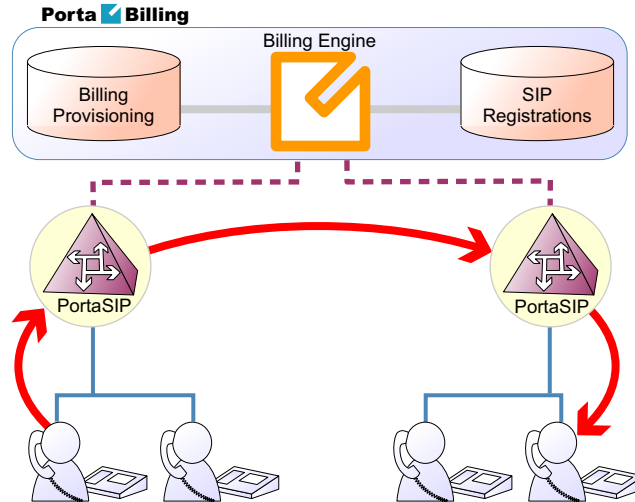


In this case, the call flow is exactly the same as in a situation where only one PortaSIP server is available (discussed earlier in the *SIP UA <--> SIP UA* section).

- PortaSIP receives an incoming call and requests authorization and routing from PortaBilling100.
- 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.

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.

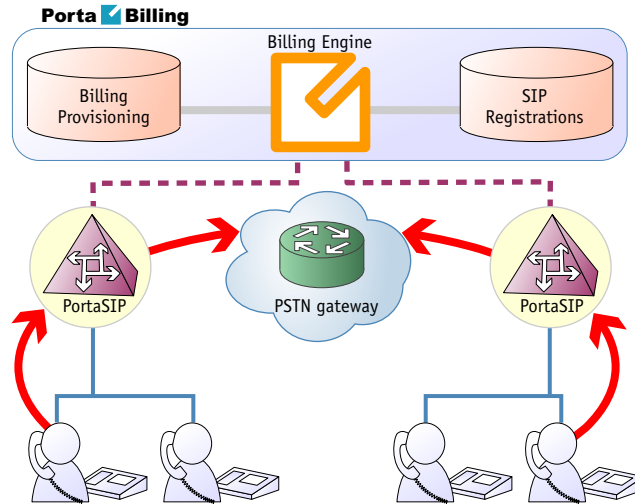


It may be asked why the first (originating) PortaSIP server does not send the call directly to the called SIP phone (since the registration database contains its contact IP:port information)? The answer is that, if the called SIP phone is behind a NAT (and most Internet users are behind a NAT these days),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

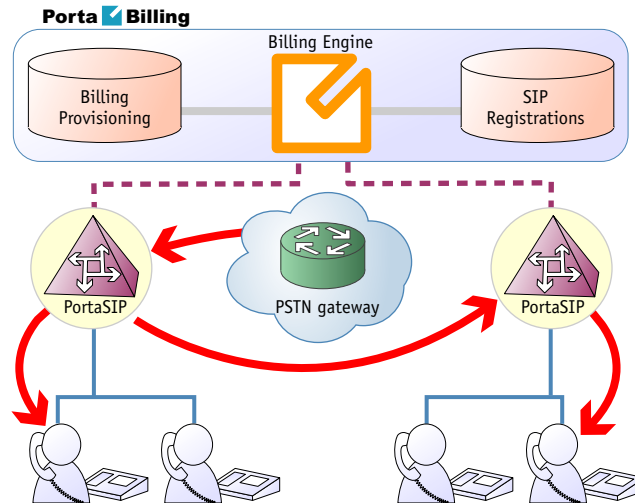
SIP UA -> PSTN

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 -> PSTN calls in the case of a single PortaSIP server.



PSTN -> 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.



SIP Phone Configuration for PortaSIP Cluster

In order to ensure reliable VoIP services, a SIP phone must be able to automatically switch to backup servers, should one of the SIP servers not be available. How does a SIP phone know about alternative SIP servers? There are several options:

1. Program the backup SIP server's IP address into the SIP phones, if this is supported by the IP phone configuration. The main disadvantage of this method is that it only works with certain SIP phone models.
2. Instead of programming the IP address of the SIP server into the SIP phone's config, use a hostname instead (e.g. sip.supercall.com). This name can be set up to resolve to multiple IP addresses of different SIP servers ("DNS round-robin"). However, this may not work if the manufacturer of the SIP phone has employed a simplified approach, so that the phone does not perform DNS resolving if a current SIP server fails.
3. Use the DNS SRV records. These records were designed specifically for the purpose of providing clients with information about available servers (including the preferred order in which individual servers should be used) in a redundant multi-server environment. This method is currently the most flexible and reliable one; see details below.

Using DNS SRV records for multiple PortaSIP proxies – an example

Here we assume that you have two PortaSIP servers available in the main hosting center for your VoIP mysipcall.com service, as well as one backup PortaSIP server in a collocation center in a different city. Your users normally use either one of the "main" servers, and only if they cannot access either of them (e.g. a network problem affecting the entire hosting center) will they go to a backup one.

First of all, your DNS server for the mysipcall.com domain must be configured with DNS A-records for the individual PortaSIP servers:

```
portasip1           IN      A       193.100.3.2
portasip2           IN      A       193.100.3.5
portasip3           IN      A       64.12.63.37
```

After this you may define a SRV record describing the available SIP servers:

```
_sip._udp.proxy    SRV     10      0       5060    portasip1
                   SRV     10      0       5060    portasip2
                   SRV     60      0       5060    portasip3
```

The first two servers have a higher priority (10), so they will be tried first. Also note that DNS SRV allows you to specify which port should be used for communication.

On your SIP phone, you should specify the following:

```
SIP proxy/registrar: proxy.mysipcall.com
Use DNS SRV: yes
DNS SRV Auto Prefix: yes
```

If you do not switch on the "auto prefix" feature, then the SIP proxy address must be entered as `_sip._udp.proxy.mysipcall.com`.

So now, when a SIP phone is switched on, it will first query the DNS database for servers for `_sip_udp_.proxy.mysipcall.com`, receiving a list of recommended servers (`portasip1.mysipcall.com`, `portasip2.mysipcall.com` and `portasip3.mysipcall.com`). After that it will obtain the IP addresses of these servers from the DNS database, and attempt to contact them in sequence until it succeeds.

```
Remote-Party-ID:
<sip:1234@sip.example.com>;party=callid;privacy=full
```

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:

- 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 (PortaUM 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.

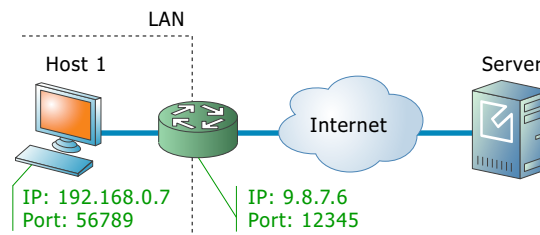
NAT Traversal Guidelines

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.



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).

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.

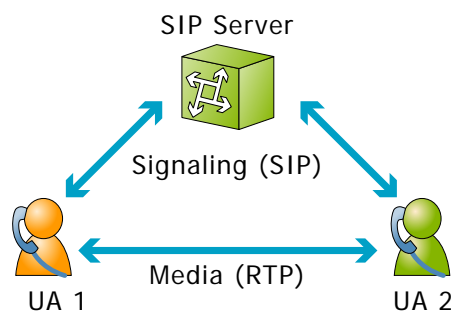
Registering a client which is behind a NAT requires either a registrar that can save the IP:port in its registration information, based on the port and IP that it identifies as the source of the SIP message, or a client that is aware of its external mapped address and port and can insert them into the 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:



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.

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

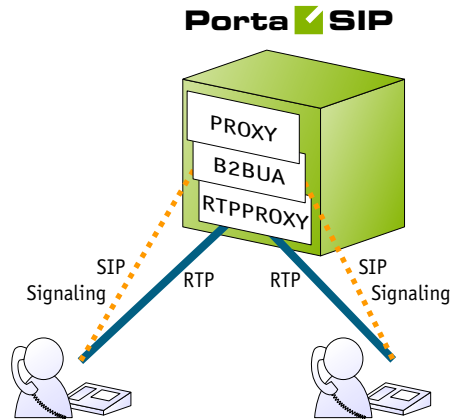
1. A call is made from one SIP UA (SIP phone) to another SIP UA (SIP phone), with both phones on public IP addresses (outside a NAT). In this case, the phones can communicate directly and no RTP proxying is required.
2. A call is made from one SIP UA (SIP phone) to another SIP UA (SIP phone), and at 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 PSTN

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.
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

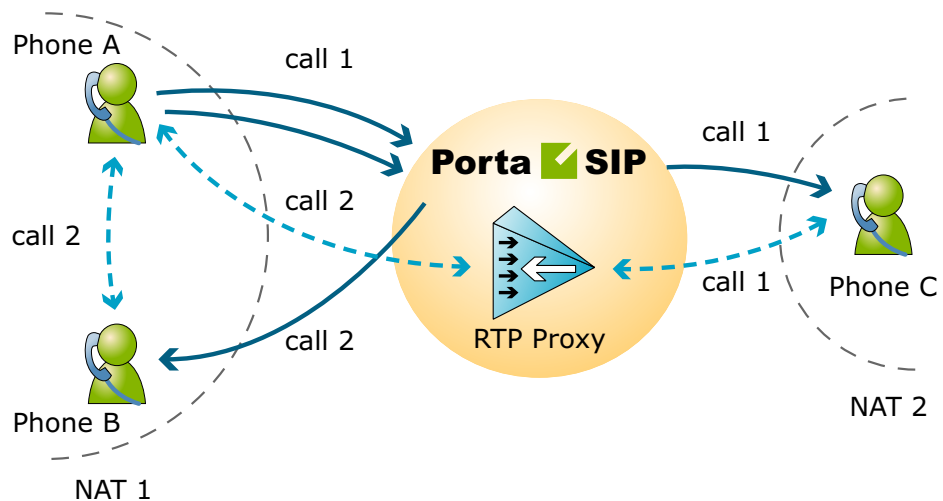
This provides an effective NAT traversal solution according to the RTP proxy method described above. The RTP proxy is fully controlled by PortaSIP, and is absolutely transparent to the SIP phone.



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.

SIP-to-SIP calls



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 SIP-2-SIP calls can be summarized as follows:

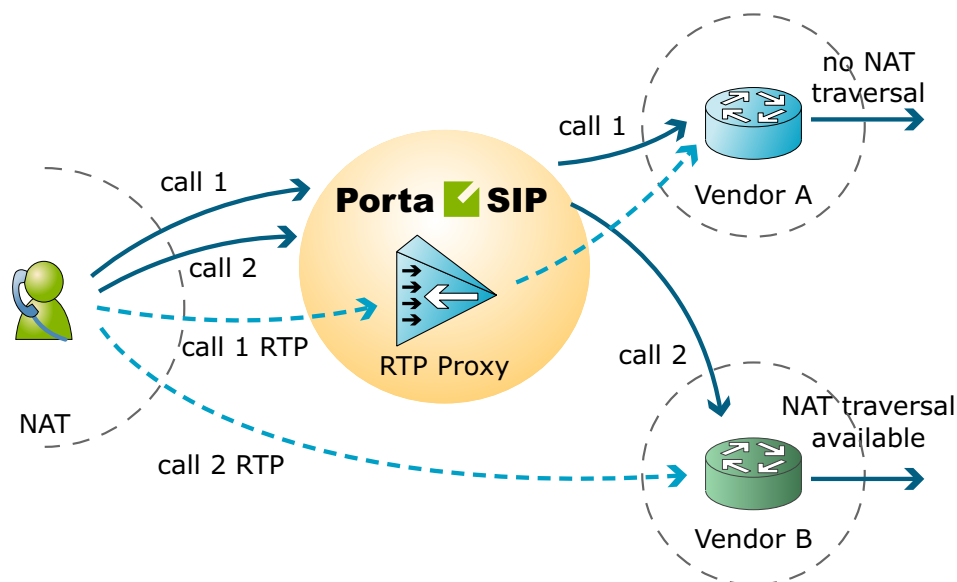
- If both phones are on public IP addresses, do not use an RTP proxy; rather, allow the media stream to go directly between them.
- If both phones are behind the **same** NAT router, do not use an RTP proxy; rather, allow the media stream to go directly between them.
- Otherwise the RTP proxy is used

SIP-to-PSTN or PSTN-to-SIP calls

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 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.

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

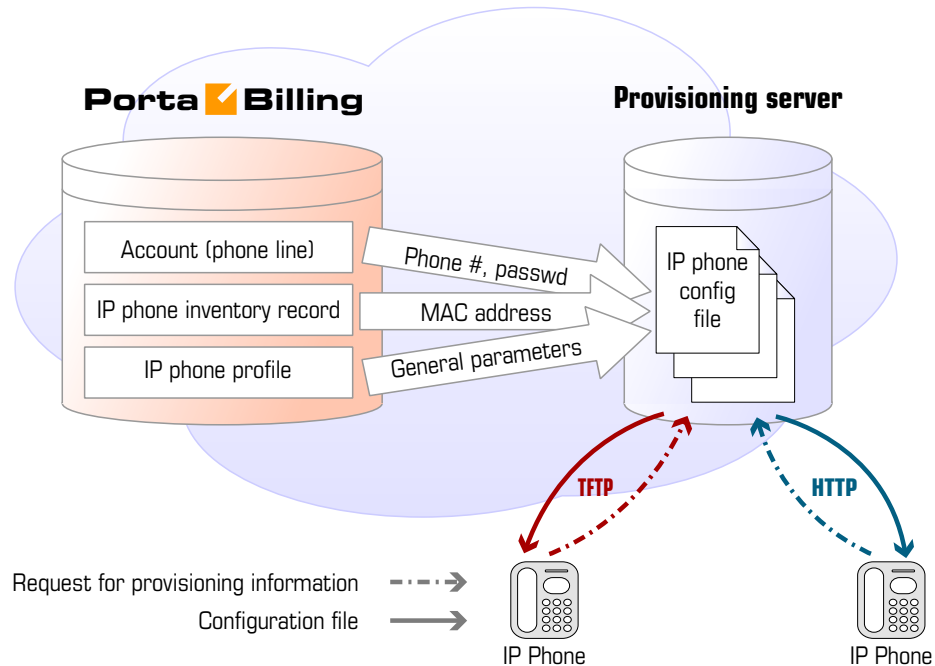
This approach is a fundamentally different one. Instead of attempting to contact an IP phone and change its parameters (pop method), the initiative is transferred to the IP phone itself. The device will periodically go to the provisioning server and fetch its configuration file.

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 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 IP phone 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.

IP Phone Inventory

The IP phone directory 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 IP phone 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 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.

2. Advanced Features

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	b2bus	AAA
server	70.68.0.213	216.231.44.34	216.231.44.34	PortaBilling
time	Sipura/SPA2000-3.1.1.5	PortaSIP	PortaSIP	
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,

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

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).

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.

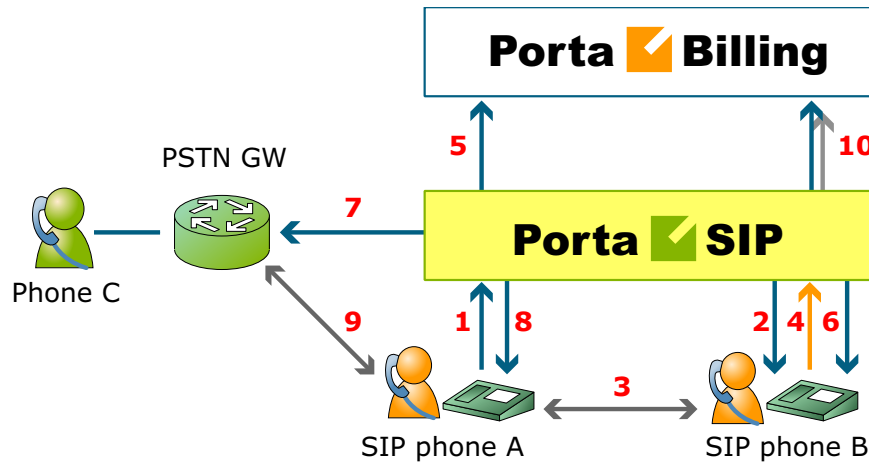
This allows you to define most call feature parameters only once, on the customer level. These will then be automatically propagated to accounts (individual phones).

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 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->PSTN or PSTN->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 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



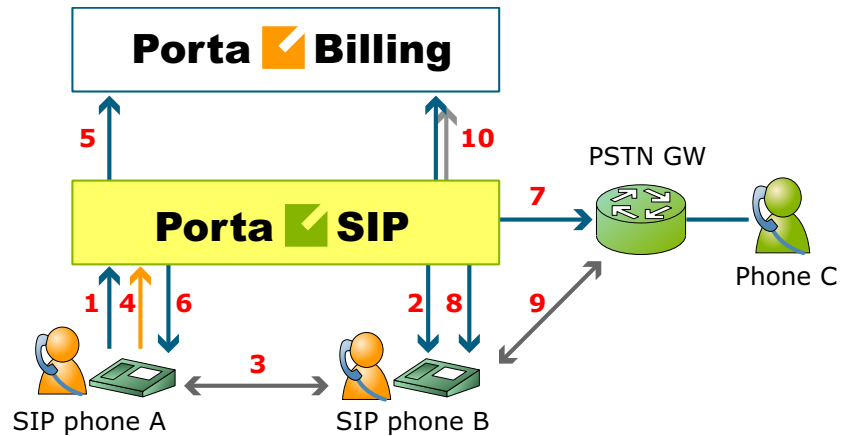
- A dials B’s phone number (1).
- PortaSIP sends the incoming call to B (2); when B answers, the call is established between A and B (3).
- At a certain moment in the conversation, B performs a call transfer (REFER) to C (4).
- PortaSIP intercepts this message and sends an authorization request to PortaBilling 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).
- When either A or C hangs up, the call is terminated, and two accounting records are sent to the billing (10): one is for the A->B call (charged to its originator, A) and the other for the A->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.

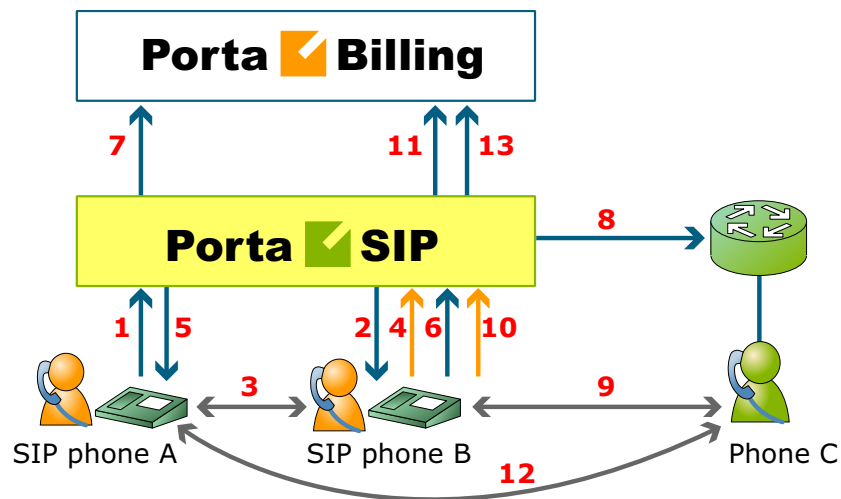
A scenario in which it is the calling party who initiates the transfer (shown below) is nearly identical to that described above for a transfer initiated by the called party.



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

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 two accounting records are sent to the billing (13): one is for the A->B call (charged to its originator, A) and the other for the A->C call (likewise charged to its originator, B).

Call Forwarding

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

- **Forward to CLD** is simple, unconditional forwarding to a different phone number.
- **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.

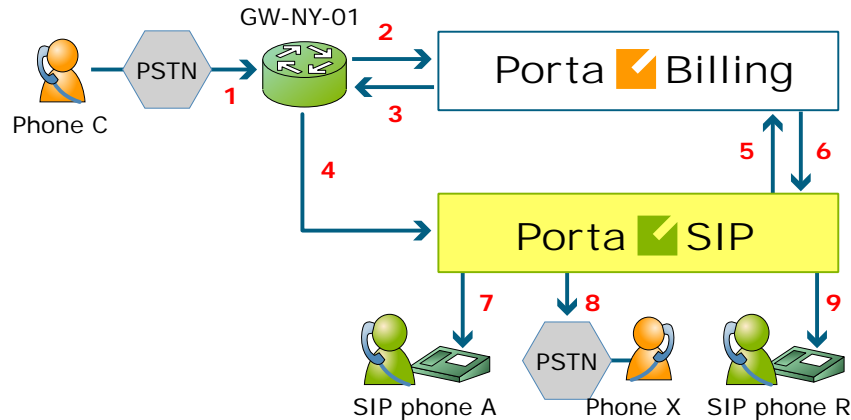
Follow-me services

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.



- 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 (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 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.
- If such a call was completed to follow-me number R, 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 outgoing rates for A).
- 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 A will be charged for call B->R.

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 information. If a customer who buys DIDs from you has two SIP proxies, you need to 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 forwarded calls

From a billing perspective, a forwarded call is treated as two separate calls. Thus, if party A calls party B, and B has follow-me set up for phone number 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 destination C.

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.

Follow-me vs. redirect number

What is the difference between the follow-me and associated number (formerly called "redirect number") properties of an account? While both seem to serve a similar purpose, redirect numbers had several drawbacks:

- Different gateways/applications had different kinds of support for this feature. For instance, the default Cisco debit card application did not support this feature at all.
- Using only a single phone number as a parameter did not permit flexible services.

For this reason, a new, flexible, robust solution was required, and so the call forwarding feature was implemented in PortaSwitch. The redirect number feature is now obsolete, and information in the redirect number field is no longer used by PortaSwitch. PortaBilling still returns the

associated number value in the h323-redirect-number RADIUS attribute for backward compatibility, and so it can still be used by some external applications, e.g. TCL scripts on a Cisco gateway.

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).

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.

Selective Call Processing

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 selective call processing rules in PortaSwitch. When the selective call processing 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). Also, when listing your colleague's phone number (i.e. another phone in your IP Centrex environment), you can enter its short extension number instead of the complete number.
- **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 Period** – 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 processing algorithm

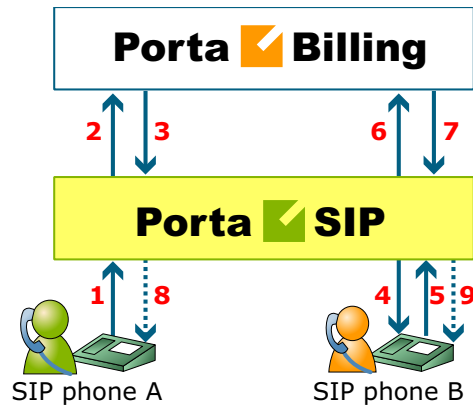
When a new call arrives to PortaSwitch, call information is sequentially checked against all defined call processing rules. The call information (ANI, DNIS and current time) is checked against each rule’s limitations. If at least one of these does not match, the rule is skipped and processing moves on 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.

Call Parking

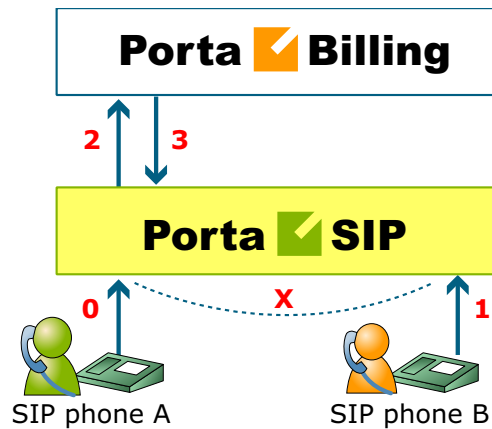
Call parking allows users to put a conversation on hold and then resume it from a different IP phone.

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 requests that this call be parked by dialing a special call parking code (5).
- The dialed code is sent to billing for verification (6). Upon successful approval (7), A is put on hold and hears the music-on-hold melody uploaded by B (8).
- The call parking confirmation message is played to B (9); this message also contains information about the code to retrieve 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).
- 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.

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 customer and account only. 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.

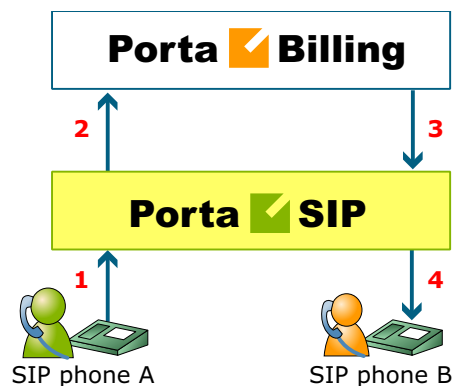
A call barring class covers a specific set of phone numbers that the customer should potentially be denied access to. In this regard, a call barring class is very similar to a destination group. The difference is that while a destination group can only contain pre-defined destination prefixes, a call 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.

Definition of the various call barring classes (such as “Mobiles”, “International”, etc.) is done globally in the **Call Barring** tab under **Company Info**. Barring of a specific class can then be turned on/off for an individual account.

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



- 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 telcos.

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 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:
 - o 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.
 - o 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:

The screenshot shows the configuration page for an account with ID 12065551234. The 'Product' is 'USD - EasyCall' and the 'Balance' is '10.00000 USD'. The 'Service Type' is 'Internet Access' and 'Outgoing Calls' is selected. A dropdown menu for 'Allowed CLI' is open, showing options: 'Customer's default', 'Customer's default', 'Any Number (Do Not Modify)', 'Account ID Only', 'Account ID Or Account Alias', 'Specified Number Only', 'Any Account Of The Same Customer', and 'Any Account Of The Specified Batch'. Other fields include 'Batch', 'Default Valid CLI', 'Display Number', 'Preferred IVR Language', 'Favorite Numbers Enabled', and 'E911'.

- **No restrictions (Do Not Modify)** - Accept and continue relaying any identity value supplied by the remote party. This assumes that the remote party is trusted and assumes full responsibility.
- **Account ID Only** – This is the strictest option; it only allows an identity that is the same as the ID on the account which is already authorized for placing a call.
- **Account ID or Account Alias** – A slightly relaxed version – 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 DID's in addition to his primary number to place outgoing calls using any of these DID's as his identity.
- **Specified Number Only** – The identity will always be set to a specific phone number, stored in the **Default Valid CLI** attribute of the account.
- **Any Account of the Same Customer** – An identity is considered valid if it matches an account ID (or account alias) of any account belonging to this customer. 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. So the supplied identity is fine, as long as it is one of the phone numbers provided for this customer.
- **Any Account of the Specified Batch** – This is a more restrictive option than the one above as it requires that 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 (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 batch.

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:

- **No restrictions (Do Not Modify)** – will allow the remote IP phone or IP PBX to supply any CLI/ANI number.
- **Use the Same Rule** – will apply the same restrictions as the ones placed on the identity information (described above).
- **Fix to Identity CLI** – 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 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.

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. SIP proxy receives the INVITE request and sends an authorization request to the billing.
- 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 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. 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). These files are located in `/usr/local/share/asterisk/sounds`, and you can change them according to your needs. 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, 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.

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 NAT helper 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.
- Therefore, the call will be charged for call duration quite close to the real one.

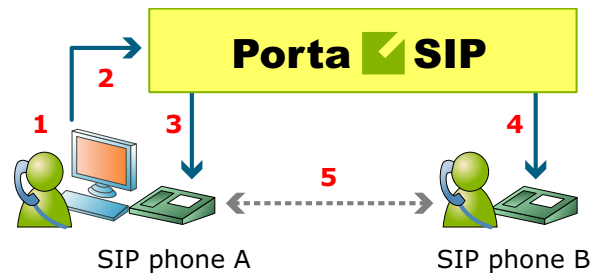
First Login Greeting

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.

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).

Direct Incoming Calls to B2BUA

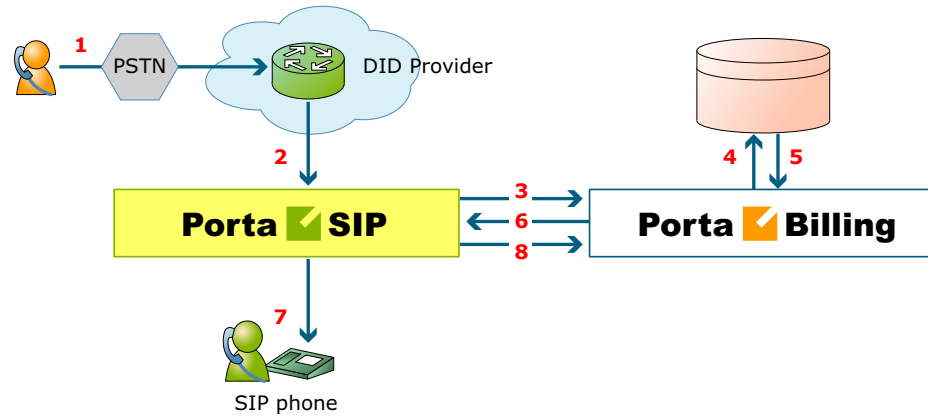
During the life of a VoIP call, PortaSIP and the remote SIP UA exchange various SIP messages. B2BUA is the originator or recipient of these messages, but every message passes through the SIP proxy. This is necessary for several reasons, the most important of them being the fact that the SIP proxy must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

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.

VoIP from Vendor Connection

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 (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 "IP authentication" chapter).
- PortaBilling will check whether this authorization request is related to a "VoIP from vendor" connection (4). In there is no match, it assumed to be a normal call from one of your customers, and the call will then proceed according to the standard algorithm. Otherwise (i.e. if this call is indeed coming via a VoIP from vendor 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.

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 (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

PortaSIP fully supports Secure Real-time Transport Protocol (SRTP) according to RFC 3711, which provides confidentiality, message authentication and replay protection to voice traffic between IP phones.

Voice VPN Rating

The **Voice VPN** (Virtual Private Network) feature provides special handling of calls within a specific IP Centrex environment, typically the telephony system for a certain enterprise. Most of its features (e.g. abbreviated dialing) have 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 countries).

When the **Voice VPN** feature is enabled for a particular customer and a call is made from account A (belonging to this customer) to account B

(belonging to this same customer), PortaBilling will look up the applicable rate not for the actual phone number, but for the special keyword `VOICEVPN`, and use this 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.

Using the `VOICEVPN` 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 **Voice VPN 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.

3. IP Centrex Features

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

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.

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-book or lifts the handset.

This feature is configured on the SIP phone side 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 )
```

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 (choose “Follow-me when unavailable”) 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 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.

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.

Call Park / Call Pickup

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 pickup 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 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 “de-park code”.

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 using the tariff configuration in PortaBilling.

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).

Supported by PortaSwitch.

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.

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.

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.

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 VPN Distinctive Dialing feature.

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.

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.

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 via the follow-me feature.

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.

Supported by PortaSwitch (the actual "message waiting" SIP info packet is originated by PortaUM and relayed by PortaSIP).

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 PortaUM and relayed by PortaSIP), 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 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 simply 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.

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 Processing 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.

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 Processing 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 Processing 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 Abbreviated Dialing 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.

Toll Restriction

Feature description: Blocks a station from placing calls to telephone numbers that would incur toll charges.

Provided using the tariff configuration in PortaBilling.

700/900 Blocking

Feature description: Blocks a station from placing calls to 700 and 900 numbers.

Provided using the tariff configuration in PortaBilling.

4. How to ...

... configure my Cisco gateway to accept incoming SIP calls and terminate them to a telephony network?

Configuration of the Cisco gateway for SIP is not much more difficult than H323. First of all, make sure that the rest of your system is configured properly – that the gateway can place the outgoing calls, and is able to communicate with the billing using RADIUS.

Codecs

First of all, make sure you have set up a list of codecs which are supported by your SIP agents on your GW. Your actual configuration might differ, but here is a good example which should work in most cases:

```
voice class codec 1
  codec preference 1 g723r63
  codec preference 2 g729r8
  codec preference 3 g729br8
  codec preference 4 g723r53
  codec preference 7 g726r16
  codec preference 8 g726r24
  codec preference 9 g726r32
  codec preference 10 g711alaw
  codec preference 11 g711ulaw
  codec preference 12 g723ar53
  codec preference 13 g723ar63
```

SIP agent

Now enable the SIP agent functionality on your gateway. Also enable it on gateways where NAT symmetric traversal is supported, as this will facilitate calls from SIP agents behind the firewall.

```
sip-ua
  nat symmetric check-media-src
```

NOTE: Cisco GWs are currently unable to log in to the SIP server using the REGISTER method.

Dial-peers

Finally, create an SIP-enabled incoming dial-peer:

```
dial-peer voice 100 voip
  incoming called-number .T
  voice-class codec 1
  session protocol sipv2
  dtmf-relay rtp-nte
!
```

Note that this gateway provides no authentication of incoming SIP calls, so that potentially anyone could route calls to you from their SIP server. This is why the recommended configuration is as follows:

```
call application voice remote_ip flash:app_remote_authenticate.tcl

dial-peer voice 100 voip
  incoming called-number .T
  voice-class codec 1
  session protocol sipv2
  dtmf-relay rtp-nte
  application remote_ip
!
```

Thus, every incoming call will be authenticated by the IP address of the remote peer. Since signaling for the SIP call comes from the SIP server, this would be the address of the SIP server. This means that calls coming from your own SIP server will be authenticated by billing, since your SIP server is entered in the system as a trusted node.

... configure my Cisco gateway to send outgoing calls using SIP?

Configuration of the Cisco gateway for SIP is not much more difficult than H323. First of all, make sure that the rest of your system is configured properly – that the gateway can place the outgoing calls, and is able to communicate with the billing using RADIUS.

SIP server parameters

Specify general parameters of the SIP server, such as hostname. You can also refer to the SIP server by its IP address; however, this method will require reconfiguration of each individual gateway if you change the IP address of your SIP server.

```
sip-ua
  aaa username proxy-auth
  sip-server dns:<hostname-of-your-SIP-server>
```

NOTE: Cisco GWs are currently unable to register to SIP servers using the REGISTER method, or to perform proper authorization of an outgoing call using the INVITE method. Therefore, remote IP address authorization is performed by PortaSIP when it detects an incoming call from the Cisco gateway. In order for this authorization to be successful, the gateway should be registered among the PortaBilling nodes.

Dial-peers

Now you can create an SIP-enabled outgoing dial-peer:

```
dial-peer voice 200 voip
  destination pattern .T
  session protocol sipv2
```

```
session target sip-server
!
```

You probably will need an application on the incoming telephony dial-peer to properly authenticate and authorize incoming calls.

... configure my Cisco gateway for PSTN->SIP service?

Obtain a PSTN2SIP application. Create an application and a dial-peer to process incoming PSTN calls:

```
call application voice pstn2sip flash:pstn2sip.tcl
call application voice pstn2sip authenticate-by dnis
call application voice pstn2sip skip-password yes
call application voice pstn2sip authorize yes
call application voice pstn2sip dial-account-id yes

dial-peer voice 100 pots
incoming called-number .T
application pstn2sip
voice-port 0:d
!
```

The example above is for when you receive incoming calls with phone numbers already in E.164. If the number is received in a local format, you will have to use the translate feature in the PSTN2SIP script to convert the number into E.164. For instance, if you receive a US phone number in NANP (area code + phone number), you should add the following command to the application configuration:

```
call application voice pstn2sip translate "/^/1/"
```

Then configure your gateway to send outgoing calls to the SIP server according to the instructions in the previous topic.

... support incoming H323 and SIP calls on the same gateway?

This configuration is supported, as Cisco GW can handle both H323 and SIP calls at the same time. However, please note that Cisco matches an incoming dial-peer by the incoming called number, not by the protocol. Thus, the dial-peer shown below will match both incoming SIP and H323 calls, even if it gives the session protocol sipv2:

```
dial-peer voice 101 voip
description *** Incoming SIP calls
incoming called-number .
```



```
voice-class codec 1
session protocol sipv2
dtmf-relay rtp-nte
fax protocol cisco
```

... 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.

... make all SIP calls to a certain prefix NNN go to my gateway XXX?

Normally it is only possible to use the REGISTER command for user-agents, i.e. for devices which represent a single physical phone. An SIP user agent cannot register with the SIP server and report: “I am going to receive all calls for prefix NNN”. (Cisco 5300 supports the REGISTER command, but this only works for numbers assigned to FXS ports or IP phones). Therefore, if you have a gateway with E1/T1 connected to it and wish to route certain prefixes there for termination, you must define the routing in the billing. To do this, proceed as follows:

- Create a new tariff with the “Routing Ext”.
- When you enter rates into this tariff, two new columns will appear: **Preference** and **Huntstop**. Enter the desired routing preference. (The higher the number, the more desirable this route is. 0 means no route at all.) Turn the huntstop on if you do not wish to use any routes with a lower priority.
- Create a **PSTN to vendor** connection to the vendor, specify the gateway which will handle termination as your **Node**, and select the tariff you have created as the termination tariff.
- Make sure that your gateway is actually configured to accept incoming VoIP calls and send them to telephony for the destinations you plan to terminate.

... 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.

... create an application to handle PSTN->SIP calls on Cisco gateway?

You can create this application yourself according to the functionality description in this guide. An advanced PSTN2SIP application may be purchased from PortaOne, please contact our sales team.

... 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 next section.

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**.
- In the product associated with this account, add an accessibility 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 accessibility 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.

... bill using different rate plans for incoming, outgoing and forwarded calls?

This is done by assigning different access codes to entries in the product's accessibility.

- **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. Although you may specify OUTGOING as an access code, it is recommended that you keep this entry as a “default”, i.e. with an empty access code. Then if further possibilities for different rate plans (e.g. special rating for calls on hold) are added in future releases, this rate plan will be automatically applied to these new entries.

Service Type *	Node	Access Code	Info Digits	Tariff *	Delete
NOT SELECTED	ANY		ANY		
Voice calls	PortaSIP	FOLLOWME		SuperCall - forwarded calls	X
Voice calls	PortaSIP	INCOMING		SuperCall - incoming calls	X
Voice calls	PortaSIP			SuperCall - outgoing calls	X

The information above assumes that PSTN->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 previous topic.

... 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. Upload the files to the PortaSIP server in the /usr/local/share/asterisk/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.

Currently PortaSIP supports the following languages for media announcements:

- English
- French
- Spanish
- Portuguese (Brazilian)

... 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 <http://www.voip-info.org/wiki-Bandwidth+consumption> website provides information regarding bandwidth consumption by voice calls, depending on the codec used.

Do not use the “codec bitrate” in your calculations, but rather an actual bandwidth figure which takes IP headers into account.

For example, if you anticipate a maximum of 60 simultaneous calls with the g729 codec, you will need $31.2\text{Kbps} * 2 * 60 = 3.7\text{Mbps}$. Note that we multiply the “one call bandwidth” not just by the total number of calls, but also by 2, since every call will be coming both in and out of the RTP proxy.

... 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.

5. Administration / FAQ

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
  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

Why can't my debit account initiate 3-way calling using the features of a SIP phone such as Linksys 941?

Since 3-way calling requires 2 simultaneous outgoing SIP sessions from one SIP telephone, debit accounts will be unable to use it, as the first session will lock the account and not allow the second one to go through. Therefore, if you want to enable your clients to use such services, create a credit account for them instead or configure the overdraft protection in PortaBilling in such way, that only a small portion of the funds would be locked at the start of the call.

Does PortaSIP support conferencing?

You can use a 3-way calling feature, available in most SIP phones or ATAs. The full-scale SIP conferencing requires a separate solution – PortaOne provides a dedicated conferencing server as the PortaBridge product.

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.

Can I use PortaSIP with a billing system other than PortaBilling100?

Yes, this is possible. PortaSIP uses the standard Radius protocol to communicate with the billing engine, and its AAA behavior was purposely made very similar to that of Cisco IOS. So it should work with any billing system that supports Radius and can bill Cisco gateways. However, advanced services, such as billing-assisted routing, abbreviated dialing, PortaUM integration, and so on, require support from the billing engine. Detailed specifications of the protocol used to exchange information between PortaBilling100 and PortaSIP are available upon request.

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 Mera Networks www.mera-voip.com), or use one of your 36xx Cisco gateways with the special IOS feature 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 connected the Cisco AS53XX gateway to PSTN in order to send calls from PSTN to my SIP accounts and terminate calls from my SIP accounts to PSTN. How many simultaneous sessions will it be able to handle?

A rule of thumb is that each SIP->PSTN call or PSTN->SIP call will use up one DSP and one timeslot in E1/T1 interface. Therefore, if you have connected your gateway to PSTN using, for example, two E1 ports, and are using both of those ports for SIP<->PSTN, the maximum number of simultaneous calls you will be able to handle will be 60, provided that you have enough free DSPs in the system.

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 (COMEDLA)*, 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 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.

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).

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.

6. Appendices

APPENDIX A. Supported SIP RFCs

- RFC 3261 (“SIP: Session Initiation Protocol”) – supported, with the limitation that the SIP URL domain is ignored in the incoming requests.
- RFC 4566 (“SDP: Session Description Protocol”), RFC 2327 (“SDP: Session Description Protocol”) – supported, with the limitations and relaxations provided for SDP under SIP.
- RFC 3262 (“Reliability of Provisional Responses in the Session Initiation Protocol (SIP)”) – supported.
- RFC 3263 (“Session Initiation Protocol (SIP): Locating SIP Servers”) – supported.
- RFC 3264 (“An Offer/Answer Model with the Session Description Protocol (SDP)”) – only the early model is supported.
- RFC 3265 (“Session Initiation Protocol (SIP)-Specific Event Notification”) – supported in the presence server and emulated in the B2BUA.
- RFC 3323 (“A Privacy Mechanism for the Session Initiation Protocol (SIP)”) – supported in part.
- RFC 3324 (“Short Term Requirements for Network Asserted Identity”), 3325 (Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks”) – supported.
- RFC 3428 (“Session Initiation Protocol (SIP) Extension for Instant Messaging”) – supported.
- RFC 3489 (“STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)”) – supported.
- RFC 3515 (“The Session Initiation Protocol (SIP) Refer Method”) – supported.
- RFC 3581 (“An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing”) – supported.
- RFC 3842 (“A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)”) – supported.
- RFC 3891 (“The Session Initiation Protocol (SIP) "Replaces" Header”) – supported.
- RFC 4244 (“An Extension to the Session Initiation Protocol (SIP) for Request History Information”) – supported.

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**:
 - i. **Proxy** – PortaSIP address (or hostname)
 - ii. **Register** – yes
 - b. in the **Subscriber** information part:
 - i. **Display Name** – your identification (e.g. John Doe; this will be seen by the called party)
 - ii. **User ID** – SIP account ID
 - iii. **Password** – VoIP password for your SIP account
 - iv. **Use Auth ID** – no
5. Submit all the changes and update the SPA configuration.


Sipura Phone Adapter Configuration

Info
System
SIP
Provisioning
Regional
Line 1
Line 2
User 1
User 2
[User Login](#) [basic](#) | [advanced](#)

System Information

DHCP:	Enabled	Current IP:	192.168.0.88
Host Name:	SipuraSPA	Domain:	portaone.com
Current Netmask:	255.255.255.0	Current Gateway:	192.168.0.192
Primary DNS:	192.168.0.192		
Secondary DNS:	207.102.99.66 207.102.99.82		

Product Information

Product Name:	SPA-2000	Serial Number:	88012BA66086
Software Version:	2.0.10(e)	Hardware Version:	2.0.1(0905)
MAC Address:	000E08AB4638	Client Certificate:	Installed

System Status

Current Time:	1/8/2003 14:17:56	Elapsed Time:	4 days and 02:23:13
Broadcast Pkts Sent:	0	Broadcast Bytes Sent:	0
Broadcast Pkts Recv:	560688	Broadcast Bytes Recv:	34980083
Broadcast Pkts Dropped:	0	Broadcast Bytes Dropped:	0
RTP Packets Sent:	3074	RTP Bytes Sent:	120568
RTP Packets Recv:	2341	RTP Bytes Recv:	54292
SIP Messages Sent:	1724	SIP Bytes Sent:	1167889
SIP Messages Recv:	362	SIP Bytes Recv:	166405
External IP:			

Line 1 Status

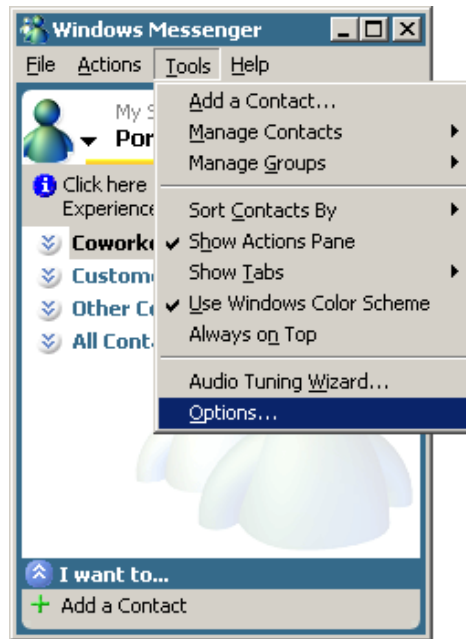
Hook State:	On	Registration State:	Registered
Last Registration At:	1/8/2003 14:07:33	Next Registration In:	2947 s
Message Waiting:	No	Call Back Active:	No
Last Called Number:	16044680035	Last Caller Number:	
Mapped SIP Port:			
Call 1 State:	Idle	Call 2 State:	Idle
Call 1 Tone:	None	Call 2 Tone:	None
Call 1 Encoder:		Call 2 Encoder:	
Call 1 Decoder:		Call 2 Decoder:	
Call 1 FAX:		Call 2 FAX:	
Call 1 Type:		Call 2 Type:	
Call 1 Remote Hold:		Call 2 Remote Hold:	
Call 1 Callback:		Call 2 Callback:	
Call 1 Peer Name:		Call 2 Peer Name:	
Call 1 Peer Phone:		Call 2 Peer Phone:	

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:			
S RTP 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

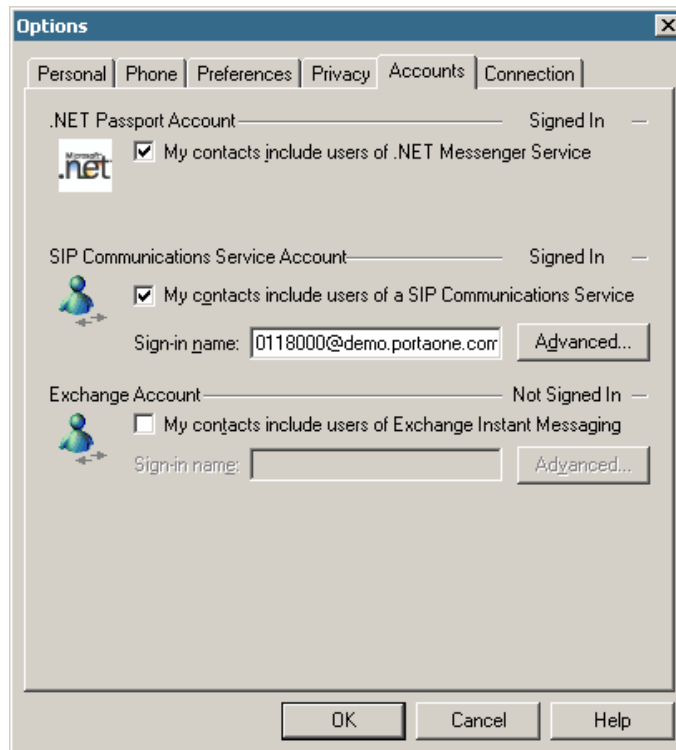
APPENDIX D. Configuring Windows Messenger for Use as a SIP User Agent

The following instructions apply to Windows Messenger version 5.0.

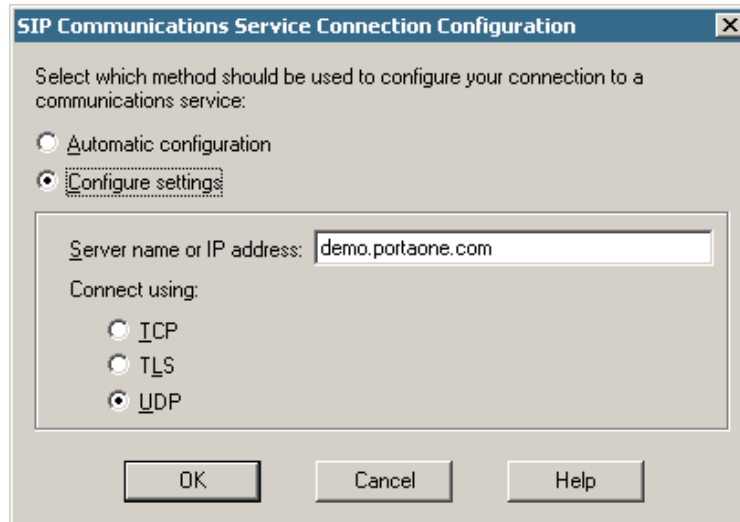
1. Start Windows Messenger, and select “Options...” from the “Tools” menu



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.



- Click the “Configure settings” radio button and enter the “Server name or IP address” using either the IP address of the PortaSIP server or its name in DNS. Make sure that the “UDP” radio button is selected, then click OK.



SIP Communications Service Connection Configuration

Select which method should be used to configure your connection to a communications service:

Automatic configuration

Configure settings

Server name or IP address:

Connect using:

ICP

TLS

UDP

OK Cancel Help

- Sign out and then sign in again. You should see the pop-up dialog below. 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.



Sign In to a SIP Communications Service

Enter your sign-in name, user name, and password to sign in to demo.portaone.com.

Sign-in name:
Example: someone@example.com

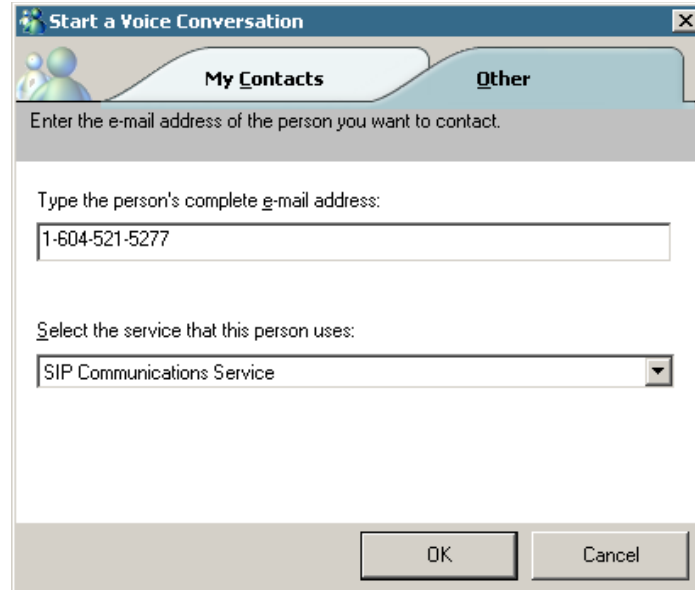
User name:
Examples: domain\username
someone@example.com

Password:

Save my password

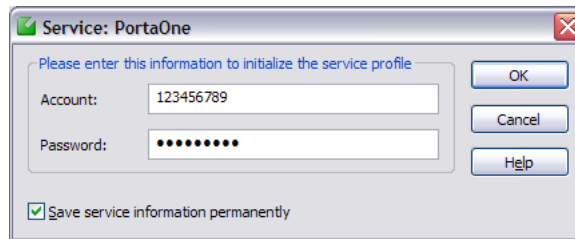
OK Cancel

5. To make a call, click the “Action” item in the main menu, then select “Start Voice Conversation”. Click the “Other” tab, making sure that “Communications Service” is selected in the drop-down Service box, and enter the phone number in the “Enter e-mail address:” field, as shown below. 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 screen will be displayed.



2. Key in the Account ID and password for the PortaSIP and press 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 press “Login...” to change or make corrections to the Account/Password.

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)
- Sipura 1001
- Sipura 2000
- Sipura 2002
- Sipura 2100
- Sipura 3000
- Linksys PAP2
- 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 GXW400x
- GrandStream HT286
- GrandStream HT486
- GrandStream HT488
- GrandStream HT496
- GrandStream HT502
- Thomson TWG850 (only eMTA part)

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.