

Copyright Notice & Disclaimers

Copyright © 2000-2007 PortaOne, Inc. All rights reserved.

PortaSIP Administrator Guide, December 2007

Maintenance Release 16

V.1.16.3

Please address your comments and suggestions to: Sales Department,
PortaOne, Inc. Suite #400, 2963 Glen Drive, Coquitlam BC V3B 2P7
Canada.

Changes may be made periodically to the information in this publication. Such 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	6
What's New in Maintenance Release 16?	6
Important Upgrade Notes	7
1. System Concepts	8
PortaSIP's Role in Your VoIP Network.....	9
PortaSIP Components.....	11
Call Process / Supported Services	12
Separate RTP Proxy Server.....	20
Virtual SIP Servers	21
Clustering of PortaSIP Servers	22
Call Flow Scenarios for a PortaSIP Cluster.....	24
Advanced Features	28
Understanding SIP Call Routing.....	47
NAT Traversal Guidelines	56
Auto-provisioning IP Phones	64
PortaSIP and E911 Services	66
IP Centrex Features.....	68
2. How to	73
... configure my Cisco gateway to accept incoming SIP calls and terminate them to a telephony network?.....	74
... configure my Cisco gateway to send outgoing calls using SIP?	75
... configure my Cisco gateway for PSTN->SIP service?	76
... support incoming H323 and SIP calls on the same gateway?.....	76
... configure my Cisco ATA186 to work with PortaSIP?.....	77
... provide services to and bill a customer who has a SIP-enabled gateway but no authorization capability (e.g. Cisco AS5350)?.....	77
... make all SIP calls to a certain prefix NNN go to my gateway XXX?..	77
... allow my customer to have two phone numbers from different countries which will both ring on the same SIP phone?.....	78
... create an application to handle PSTN->SIP calls?.....	78
... configure SIP phone X made by vendor Y?.....	78
... bill SIP-to-SIP calls?	79
... bill incoming calls from PSTN to SIP using a special rate?.....	79
... bill using different rate plans for incoming, outgoing and forwarded calls?	80
... provide error messages from the media server in my users' local language.....	81
... calculate how much bandwidth I need for my PortaSIP server?	81
... enable my SIP phone or ATA to be automatically provisioned by PortaSwitch?.....	81
3. Administration / FAQ.....	83
Troubleshooting Common Problems	84
FAQ.....	85

PortaSIP Configuration.....	88
4. Appendices	92
APPENDIX A. Tested Routers and NAT Software.....	93
APPENDIX B. Cisco GW Setup for PortaSIP (COMEDIA).....	93
APPENDIX C. Client's Cisco ATA 186 Configuration for PortaSIP.....	93
APPENDIX D. Client's Sipura Configuration for PortaSIP.....	95
APPENDIX E. Configuring Windows Messenger for Use as a SIP User Agent.....	97
APPENDIX F. SJPhone Configuration for PortaSIP.....	100
APPENDIX G. Setting up a Back-to-Back T1/E1 Connection	102
APPENDIX H. SIP Devices with Auto-provisioning	104

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



Caution indicates that the described action might result in program malfunction or data loss.

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.

Hardware and Software Requirements

Server System Recommendations

- One UNIX Server.
- A minimum of 50 GB of available disk space; this space is required for storing various log files
- Intel Xeon or AMD Opteron processor running at 1.8 GHz or greater. Additional processor speed is needed for networks with a high call volume.
- At least 1 GB of RAM, 2 GB recommended.
- At least one USB port.

For information about whether particular hardware is supported by FreeBSD from the JumpStart Installation CD, consult the related document on the FreeBSD website:

http://www.freebsd.org/doc/en_US.ISO8859-1/books/faq/hardware.html

Client System Recommendations

- OS: Windows 95-XP, UNIX or Mac OS
- Browser: Internet Explorer 6.0, FireFox 2.0 with JavaScript enabled.
- Spreadsheet processor (MS Excel)
- Display settings:
 - Minimum screen resolution: 1024 x 768
 - Color palette: 16 bit color (minimum)

NOTE: To view downloaded CSV (Comma-Separated Values) files in Windows, please do the following to match PortaBilling's default list separator: My Computer -> Control Panel -> Regional Settings -> Number -> List Separator type ",".

Installation

In order to simplify installation and support as much as possible, PortaSIP is provided on a jump-start installation CD. This CD contains installation media for FreeBSD (6.1-stable branch with the latest security bug fixes), supplementary packages necessary for convenient system administration and maintenance, and PortaSIP software packages.

PortaSIP installation and configuration are automated and integrated within the main installation process. This allows you to install a completely functional PortaSIP server from scratch in less than 15 minutes!

For detailed installation instructions, please refer to the [PortaSIP Installation Guide](#).

What's New in Maintenance Release 16?

This release includes several new features and improvements:

- Conditional call processing and selective call forwarding.
- Support for SIP TAPI applications (click-to-dial in Microsoft Outlook and others).
- Ability to provide simultaneous ringing on an IP phone and follow-me numbers.
- Ability to use separate network interfaces for SIP signaling and RADIUS communications with billing.
- Ability to install RTP proxy on a separate server for increased performance.

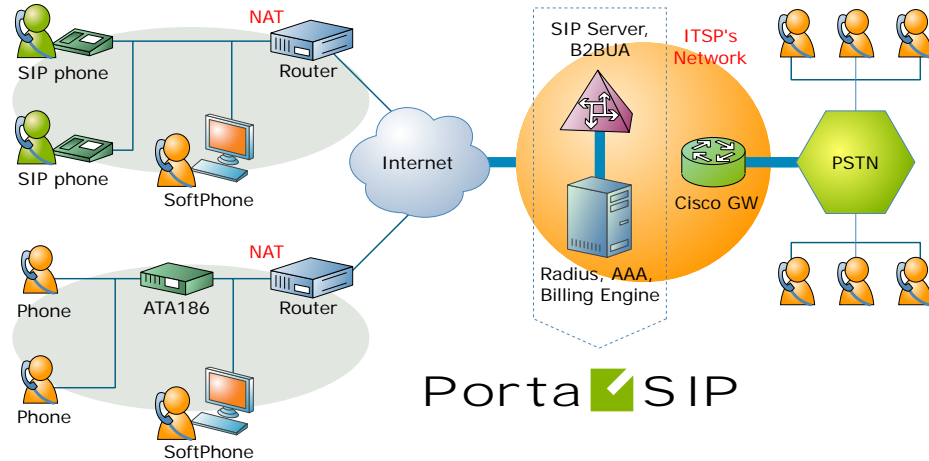
Important Upgrade Notes

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

- Selective call processing was introduced in Maintenance Release 16. When this feature is disabled, incoming calls to an account are processed as usual: i.e. the IP phone rings, call forwarding or follow-me is engaged (if enabled), and, if the call is still not answered, it is forwarded to the user's mailbox. When selective call processing is enabled, however, a new configuration parameter called **Default Action** appears on the **Service Features** tab, right under the **Call Processing Enabled** checkbox. Here you can define how calls should be processed if no call processing rules have been defined, or none of the rule conditions match. This gives you an extra degree of flexibility. Be careful, however, when changing this option from the default value, since the results may then differ from what your customers were used to in previous releases. Also note that the options in the Default Action menu appear only if the corresponding service is switched on; for example, voicemail options will appear only if this account already has UM-enabled status in the database.

1. System Concepts

PortaSIP's Role in Your VoIP Network

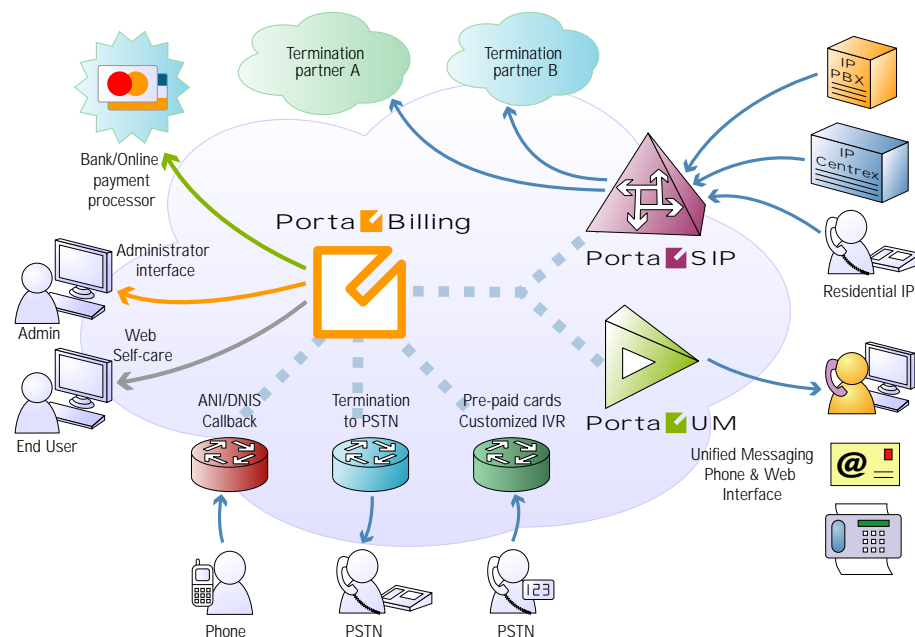


PortaSIP is a call control software package enabling service providers to build scalable, reliable VoIP networks. Based on the Session Initiation Protocol (SIP), PortaSIP provides a full array of call routing capabilities to maximize performance for both small and large packet voice networks.

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.

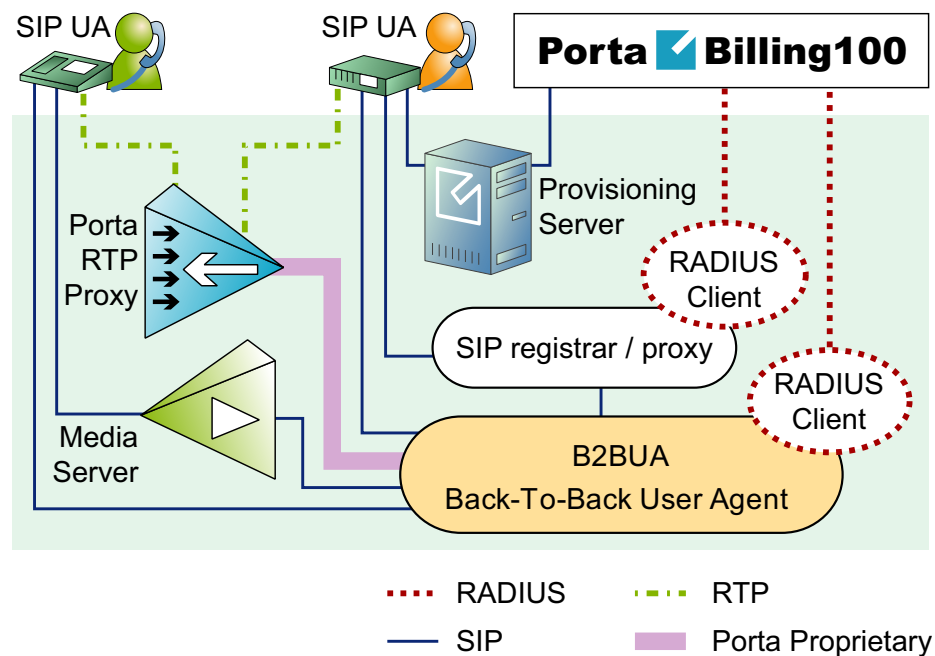
In addition to conventional IP telephony services, PortaSIP provides a solution to the NAT traversal problem and enhances ITSP network management capabilities. It can be used to provide residential, business and wholesale traffic exchange services.

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:

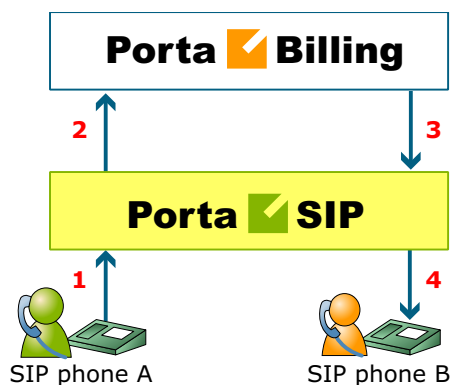
- SIP Proxy Server (SIP Express Router on the diagram): The SIP Proxy Server performs a number of functions, such as registering SIP telephones, dealing with NAT issues, etc.
- Back-To-Back User Agent (B2BUA): The B2BUA SIP-based logical entity can receive and process INVITE messages as a SIP User Agent 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 “Debit” billing (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.

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



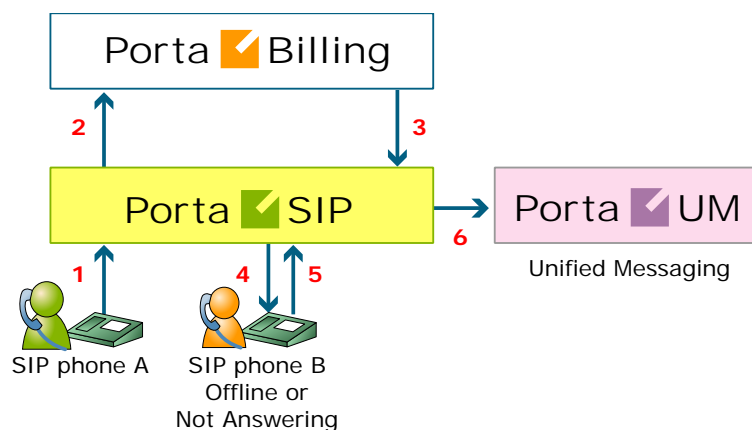
This is the simplest case:

- 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

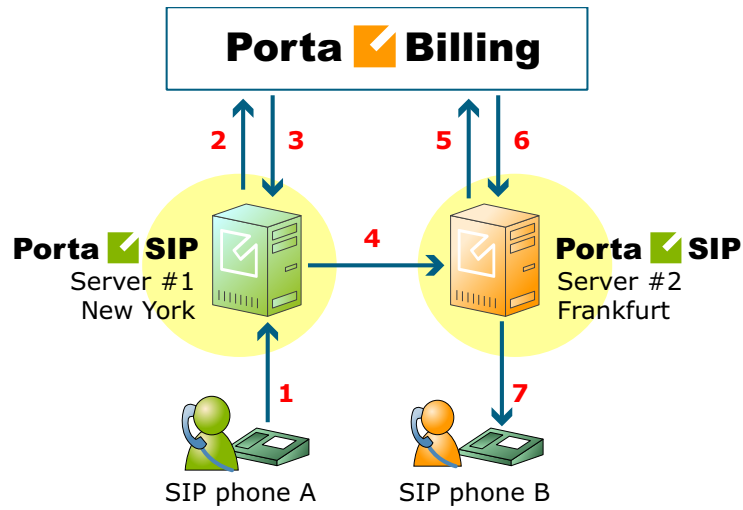


- User A dials 121 in an attempt to reach user B. His SIP user agent sends an INVITE request to the SIP server (1).
- The SIP server performs authorization in the billing (2). The billing will perform number translation and determine whether the destination number is actually an account.
- The billing 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

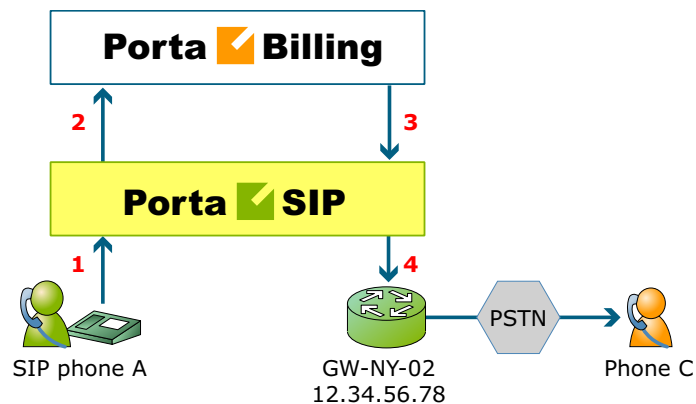
the SIP phone will try to register there if the New York i's server is down or for some reason inaccessible.



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

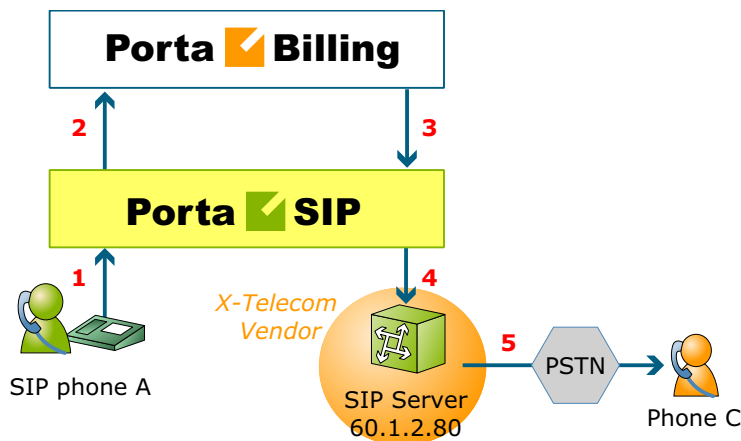


- User A attempts to call his co-worker, user C. C has not been assigned a SIP phone yet, thus he only has a normal PSTN phone number from the 202 area code, and A dials 3001234. A's SIP user agent sends an INVITE request to the SIP server (1).
- The SIP server sends an authorization request to the billing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

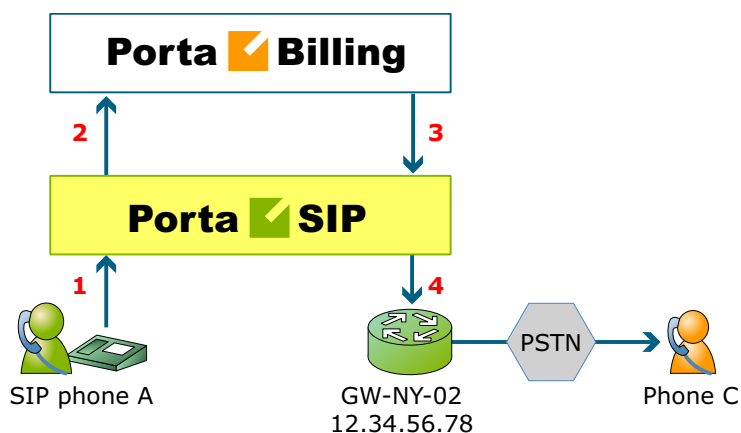
- The SIP server tries to send a call to all routes returned by the billing sequentially, until either a connection is made or the list of routes is exhausted (4).
- When the call is finished, the SIP server sends accounting information to the billing.

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

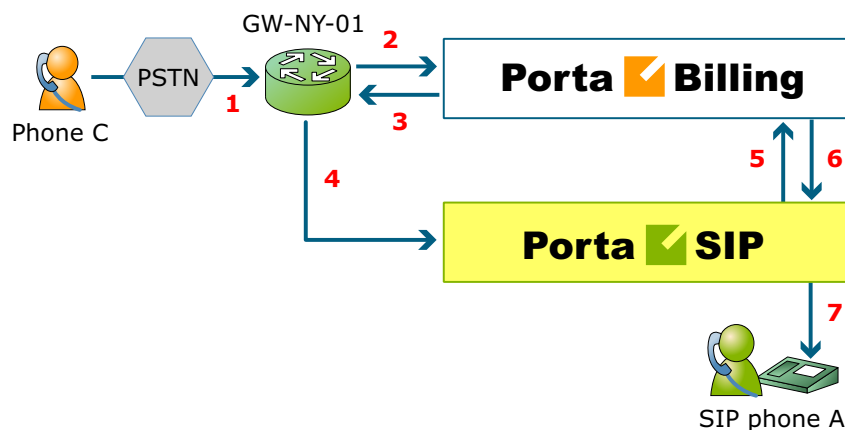


- Let's assume that T1 is connected to Qwest on our gateway **GW-NY-02** in New York, where we are able to terminate calls to the US. This connection would be described as a **PSTN to vendor** connection. The PortaSIP server obtains the address of the GW-NY-02 gateway in the route information.
- The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

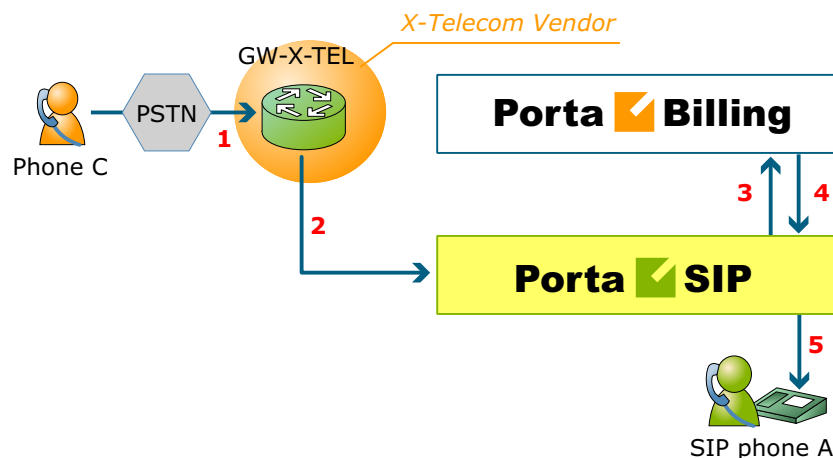
- PortaSIP receives the INVITE, but without authorization information. So the PortaSIP server performs authentication based on the IP address (5), (6). Since this call is made from our trusted node – gateway GW-NY-01 – the call is authorized.
- PortaSIP checks if the SIP user agent of the dialed number (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”.



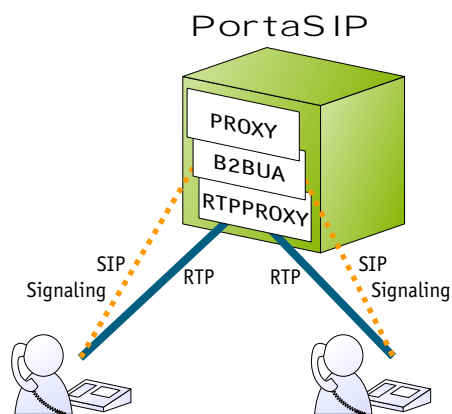
- C wishes to call A on his German phone number. He thus dials A's phone number (since C is in the US, he dials it using the North American format, 0114929876543).
- The call is routed through the telecom network to the gateway of DID consolidator X-Telecom (1).
- X-Telecom in turn forwards this call 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.

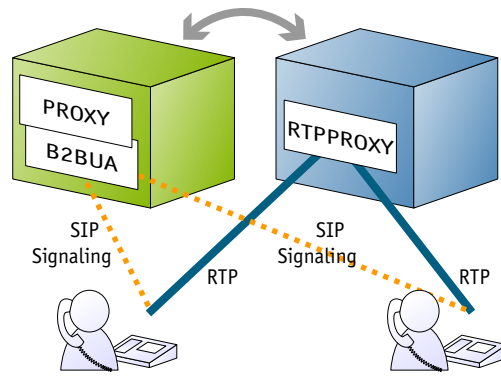
After the call is completed, A is charged for it; also, costs are calculated for the incoming call according to the tariff associated with X-Telecom’s “VoIP from Vendor” connection.

Separate RTP Proxy Server

In the normal scenario, all PortaSIP components reside on the same physical server, so both SIP signaling and RTP media pass through it. Although PortaSIP does not perform transcoding of voice traffic, the many concurrent calls passing through the server still put a certain load on the system, as a result of the huge number of relatively small packets that need to be processed.



Voice traffic is quite different from other types of Internet traffic (e.g. web downloads), as it is very sensitive to packet delays. At any given moment, the system needs to transport packets at a constant speed and with minimum added delay. If a PortaSIP server is loaded with other tasks, this may become difficult. So now you have the option of installing the RTP proxy on a separate server.



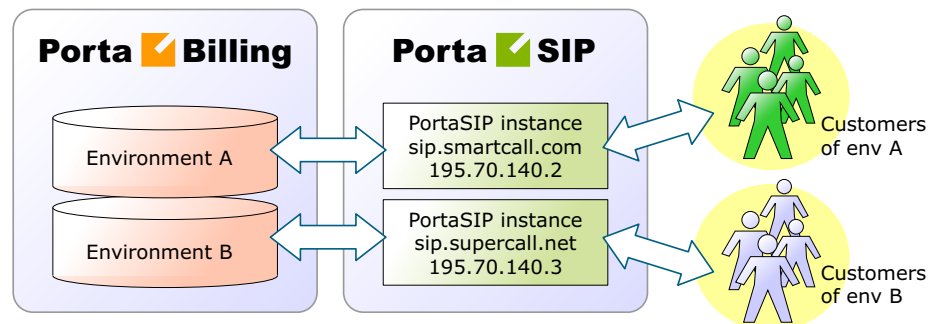
This server is installed next to the PortaSIP server running the SIP proxy and B2BUA. (Since fast and reliable connectivity between the PortaSIP server and the RTP proxy is important, they should be connected by the same Ethernet link.) The RTP proxy will be controlled by B2BUA, so that when a customer tries to make a phone call and proxying is required, B2BUA will give a command to open the ports, and the RTP stream will flow to the server running the RTP proxy.

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 adding an extra IP address (IP alias) and populating the configuration files.



Please contact the PortaOne support team for assistance with this configuration task, since if you configure the network interface on the SIP server improperly it will render all of your SIP services useless.



Every virtual SIP server acts as an independent PortaSIP installation.

The virtual SIP instance resides in the `/var/sipenv-<IP>` directory, where `<IP>` is the IP address allocated to this SIP instance, e.g. for a PortaSIP

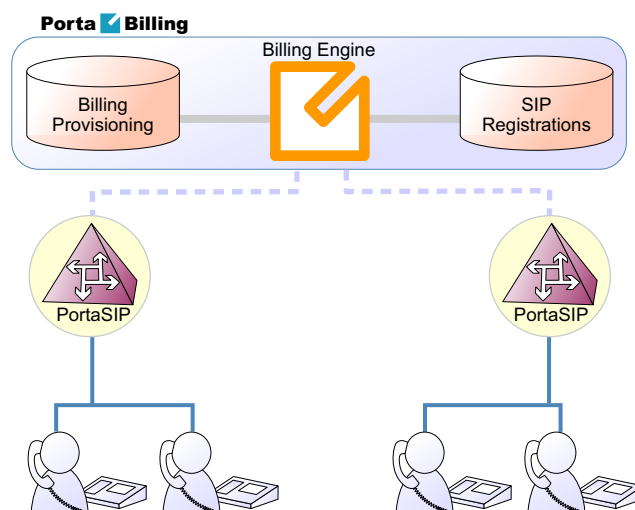
working on IP address 120.34.56.78, it will be `/var/sipenv-120.34.56.78`.

Inside the `sipenv` directory there are several sub-directories, the most important ones being:

- `etc` – this subdirectory contains a master configuration file for the SIP instance and config files for the individual modules
- `log` – PortaSIP log file (`sip.log`) and copies of the log file for previous days are located here

Clustering of PortaSIP Servers

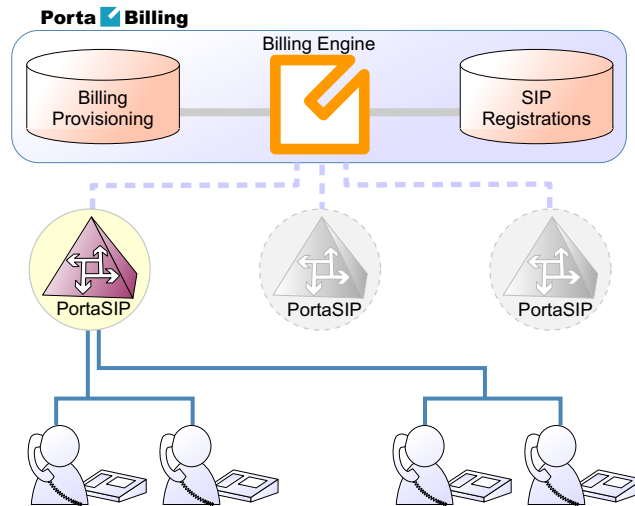
You may also install several physically independent PortaSIP servers and connect all of them to the same virtual environment in PortaBilling100. In this case, several PortaSIP servers (combined in this case into a PortaSIP cluster) communicate with a single central billing, which provides all the required 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.

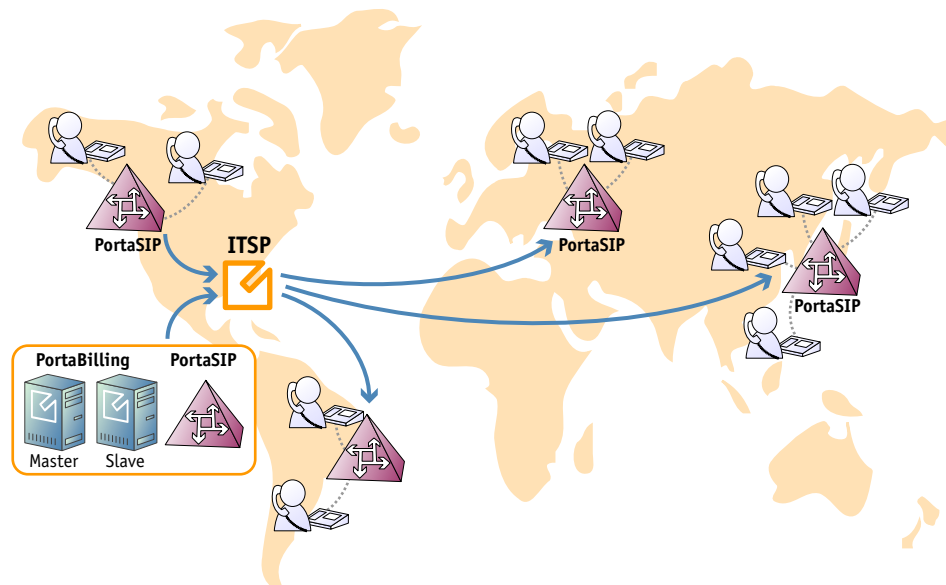
Improved Reliability



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.

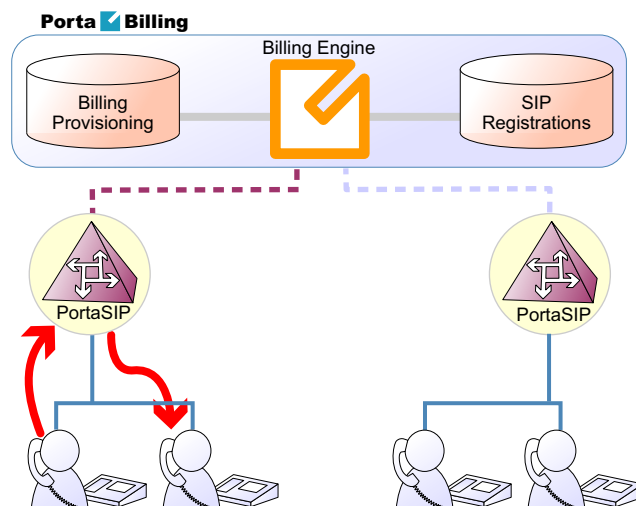


This allows VoIP services to be efficiently provided in a situation which is highly typical for many countries or regions: good, fast Internet connectivity inside the country/region and mediocre connectivity with the rest of the world. For all users inside that region, VoIP traffic (signaling and RTP) 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

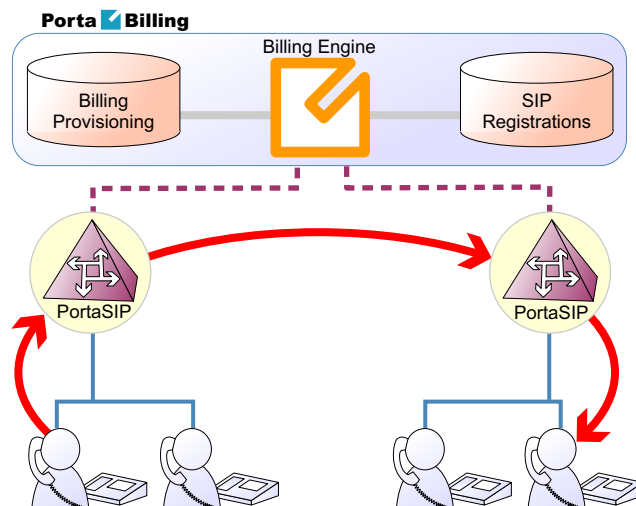


In this case, the call flow is exactly the same as in a situation where only one PortaSIP server is available (discussed earlier in the *SIP UA <--> SIP UA* chapter).

- 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.

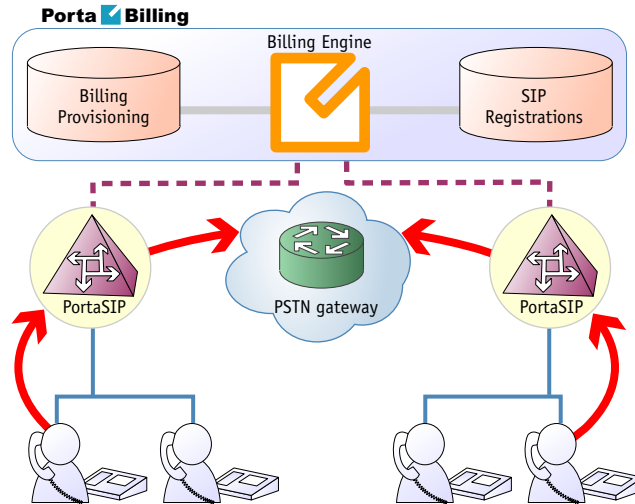


It may be asked why the first (originating) PortaSIP server does not send the call directly to the called SIP phone (since the registration database contains its contact IP:port information)? The answer is that, if the called SIP phone is behind a NAT (and most Internet users are behind a NAT these days),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

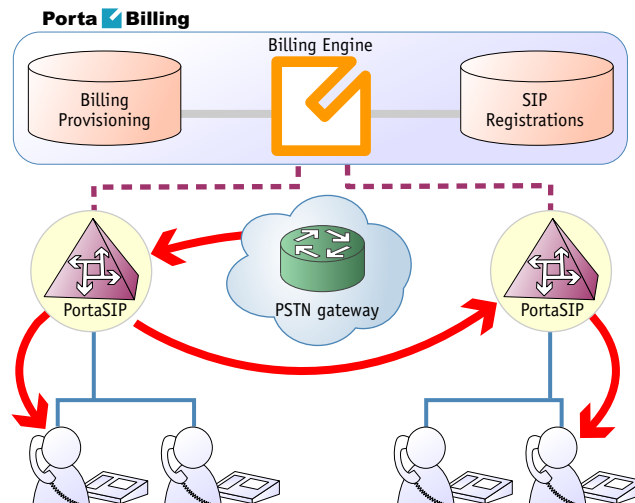
SIP UA -> PSTN

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.

Advanced Features

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.

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 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.

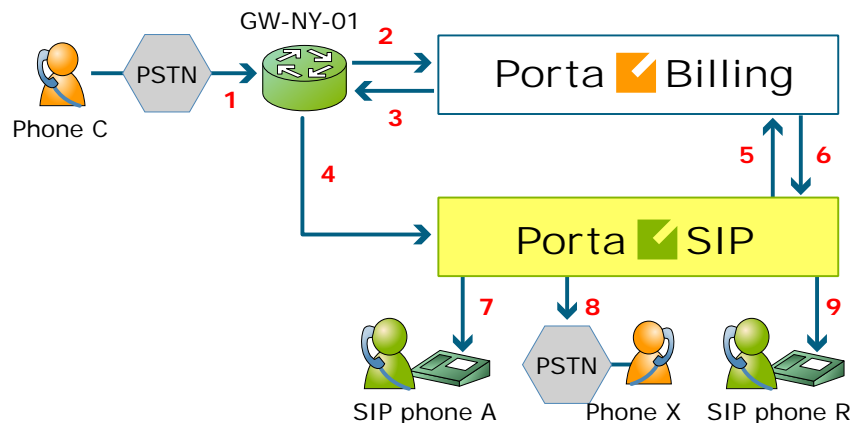
Follow-me services

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 you 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) the remote IP address may only be specified as a value identical to the ID of one of your customer's accounts. If a customer who buys DIDs from you has two SIP proxies, you need only pre-create two accounts whose IDs are identical to their IP addresses. 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 forward them to the correct recipient.

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
- **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
- **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.

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 a 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.

- Any of the SDP fields

By default, the following SIP UAs are considered incapable of digest authentication, so that IP authentication is applied:

- Cisco VoIP gateway (any Cisco gateway running IOS; this does not apply to Cisco ATA 186/188)
- Nextone SBC
- Sonus switch
- Mera SIP-HIT
- Asterisk gateway

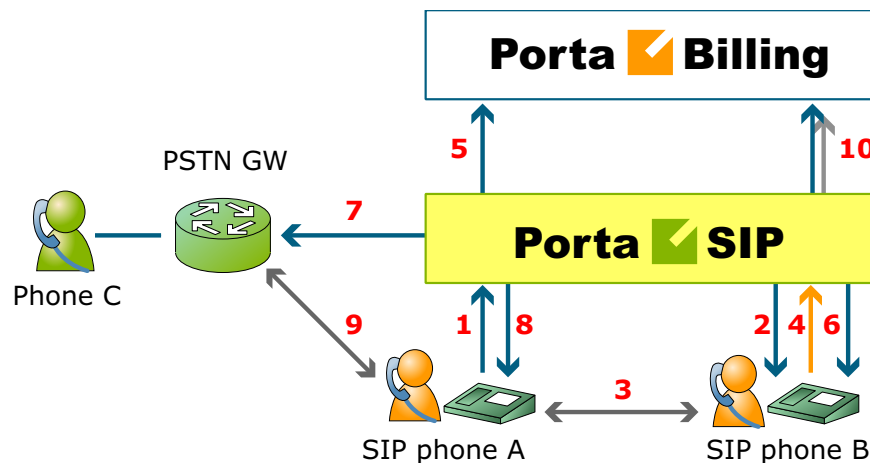
Please ask the PortaOne support team for assistance in adjusting the information in this table to reflect the desired configuration of your network.

PortaSIP-controlled 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



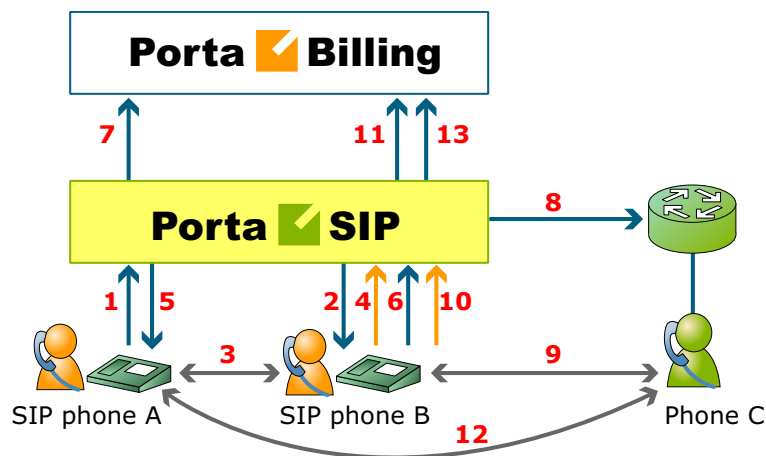
- A dials B's phone number (1).
- PortaSIP sends the incoming call to B (2); when B answers, the call is established between A and B (3).
- At a certain moment in the conversation, B performs a call transfer (REFER) to C (4).
- PortaSIP intercepts this message and sends an authorization request to PortaBilling 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.

Attended transfer

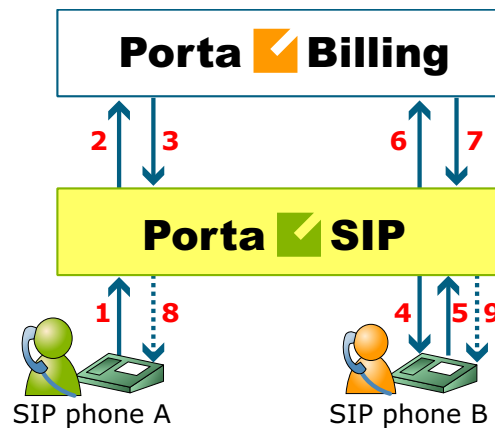


- A dials B's phone number (1).
- PortaSIP sends the incoming call to B (2); when B answers, the call is established between A and B (3).
- B places A on hold (4); PortaSIP provides music on hold for A (5).
- B initiates a new outgoing call to C (6). PortaSIP sends an authorization request to PortaBilling 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 Parking

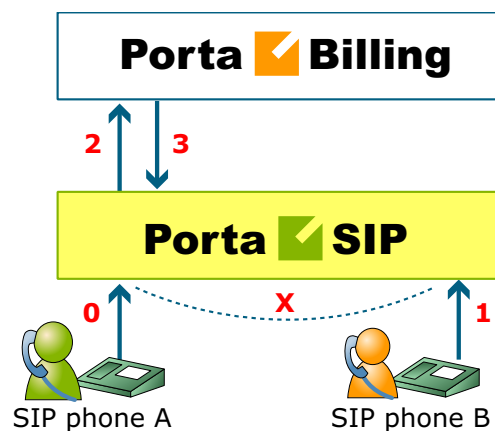
Call parking allows users to put a conversation on hold and then resume it from a different IP phone.

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.

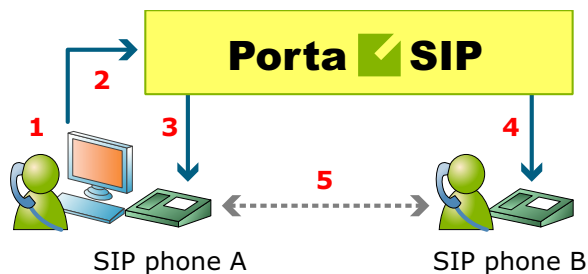
Retrieving a parked call



- 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.

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.

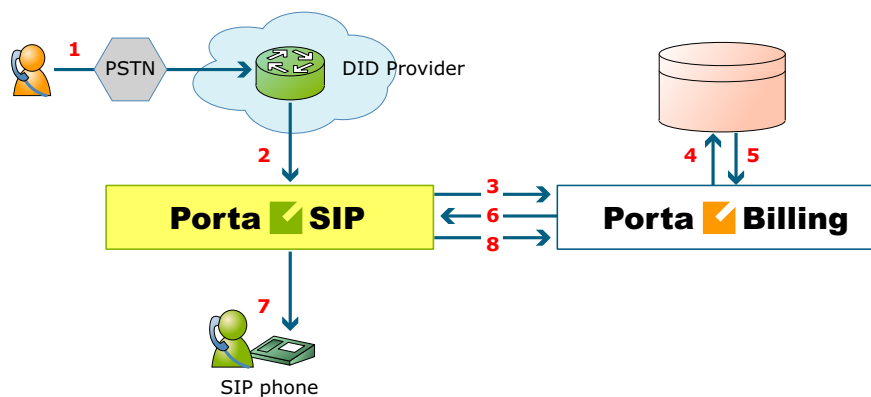
However, if a call arrives from a remote gateway or IP PBX running on a public IP address, NAT traversal is not required, and there is no need to engage the SIP proxy in the SIP message exchange. In this case, B2BUA may accept a direct incoming connection from a remote SIP UA on a public IP address. 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 is 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.

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).

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 name or even his phone number.

In this case, when sending the call to a third-party carrier PortaSIP must present the call information in such a way as to ensure the desired privacy, while at the same time complying with the vendor's requirements regarding mandatory call information.

Unfortunately, there is no single acceptable solution. Some vendors require that you supply them with the actual caller info/caller ID (accompanied by a flag according to the RFCs 3323, 3324 and 3325 that the caller's identity should be hidden from the call's recipient). Other vendors do not have such facilities, and so you must remove the caller info/caller ID from the call information before sending the call to their network. PortaSIP supports both methods; in the vendor's connection configuration you may choose which specific method is to be used for this particular carrier.

EDR	Load	H323	SIP	Remote IP *	Tariff *	RTP Proxying	Transl. Rule	Outgoing Rule	CLI Transl. Rule	Account	Delete
			<input checked="" type="checkbox"/>	210.56.78.1		Always				None	<input type="checkbox"/>
			<input checked="" type="checkbox"/>	210.56.78.1		Clear caller info				30	<input type="checkbox"/>

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 to choose the best route (least-cost routing).

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.

Routing SIP On-net Calls

The SIP server automatically maintains information about all currently registered SIP user agents, so it is able to determine whether a call should be sent directly to a SIP user agent.

Routing Off-net Calls

You can have different vendors for terminating off-net calls. For example, you can terminate calls to the US either to AT&T, via a T1 connected to your gateway in New York, or to a remote gateway from Qwest.

Rate routing parameters

Ordinarily, tariffs define the termination costs for each connection to a vendor. If you create a tariff with the **Routing** type, a few more fields will be added to rates in that tariff:

- **Route category** – you can split this into categories such as “Premium”, “Cheap”, etc. and use these categories in routing plans
- **Preference** – routing priority (0-10), higher values mean higher priority, 0 means do not use this rate for routing at all
- **Huntstop** – signals that no routes with a lower preference should be considered

This allows you to easily manage both termination costs and routing from a single location on the web interface. Thus, when such a routing tariff is associated with a connection, you can send calls for termination to all prefixes for which rates exist in the tariff.

Multiple routes

It is dangerous to have only one termination partner: if it is down, your customers will not be able make any more calls. Normally, you will try to find several vendors and enter their rates into the system. Each connection to a vendor (with routing tariff) will produce one possible route, and PortaBilling will arrange them according to cost or your other preferences.

Routing plans

Routing preferences in the rate allow you to specify that, for example, you would rather send a call to MCI than to T-Systems. However, this decision is “global”, and so will apply to all calls made in your system. But

what if you would like to use MCI first for customer A, while T-Systems should be the first route for customer B, and customer C should be routed to MCI only?

This can be accomplished using routing plans. A routing plan defines the routes for which categories are available, as well as in which order they should be arranged. For instance, in the example above MCI may be assigned as the “Normal” route category and T-Systems as the “Premium” category. After that, three routing plans will be created:

- **Quality** - includes first Premium and then Normal routing categories
- **Ordinary** - includes first Normal and then Premium routing categories
- **Cost-efficient** – includes only Normal routing category

So, depending on which routing plan is assigned to the current customer, the system will offer a different set of routes.

Routing algorithm

The routing principle is simple:

- The SIP server (or MVTS, or some other entity) asks PortaBilling for routing destinations for a given number.
- PortaBilling checks every tariff with routing extensions associated with a vendor connection for rates matching this phone number. In each tariff the best-matching rate is chosen; this rate will define the routing parameters.
- A list of possible termination addresses will be produced (this will include the remote IP addresses for VoIP connections and IP addresses of your own nodes with telephony connections).
- This list will be sorted according to routing plan, routing preference and cost; entries after the first huntstop will be ignored.
- If there are several routes with identical cost/preference, load sharing will be applied, so that each potential route has an equal chance of being the first. Consequently, if your termination carrier provides you with three gateways to send calls to, at the end of the day each gateway will receive approximately the same number of calls (33%).
- A list of these IP addresses (with optional login and password for SIP authentication) will be returned to the SIP server. (To avoid extremely long delays, only a certain number of routes from the beginning of the list are returned; the default is 15, but this can be changed in `porta-billing.conf`).

Route sorting

How exactly does PortaBilling100 arrange multiple available routes?

1. By route category. Only route categories which are included in the routing plan will be used, following the order given in the routing plan.
2. If you have multiple route categories within the routing plan, you can either merge them into the same group by assigning them the same order value, or keep each one separate, with its own order value. Then routes within the same order group for route categories will be arranged according to preference.
3. For routes with the same preference, the system can arrange them according to cost (a comparison is made on the **Price_Next** rate parameter) so that cheaper routes will be among the first ones, or in random fashion.

Does PortaSwitch support LCR?

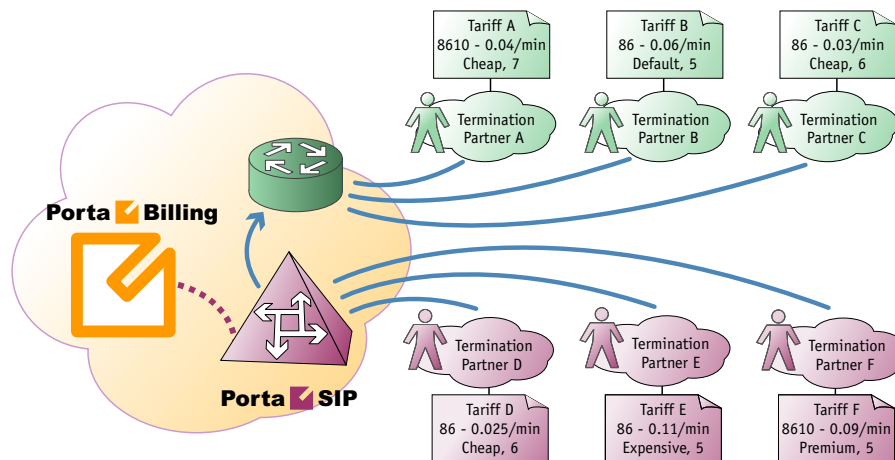
Yes, we support LCR – and much more besides. In fact, “just LCR” is the simplest type of routing PortaSwitch handles. If you decide not to use routing plans (one default plan for everyone) or routing preferences (same preference for all vendors), then the routing decision will be affected solely by the vendor’s cost. Also, PortaSwitch supports a “profit-guarantee” mode for routing. Only those termination carriers who satisfy your conditions for the minimum required profit (e.g. at least \$0.005 each minute) will be chosen.

Compare the two illustrations below. The first one shows simple least-cost routing: all of the available carriers are arranged according to cost. In the second illustration, PortaSwitch routing preferences are used, so that the administrator can re-arrange the routing. In this case, carrier D has been moved down the routing list, while carrier A has been moved up to the top of the list, thus becoming the first route.

Test Dialplan												
										America/Vancouver	porta-root	Help
										Close	Objects	Logout
Phone Number		Routing Plan		Protocol		Date and Time						
8610234567		Default		H323 SIP		YYYY-MM-DD HH:Mi						
				<input type="checkbox"/>		<input checked="" type="checkbox"/>		Search				
#	Destination	Country	Description	Price	Route Category	Preference	Huntstop	Route to	Vendor	Connection	Tariff	
1	86	CHINA	Proper	0.02500 USD	Default	5	N	45.12.158.200	Vendor D	Termination to vendor D	Vendor D	
2	86	CHINA	Proper	0.03000 USD	Default	5	N	ny-gw-01	Vendor C	Termination to carrier C	Vendor C	
3	8610	CHINA	Beijing	0.04000 USD	Default	5	N	ny-gw-01	Vendor A	Termination to carrier A	Vendor A	
4	86	CHINA	Proper	0.06000 USD	Default	5	N	ny-gw-01	Vendor B	Termination to carrier B	Vendor B	
5	8610	CHINA	Beijing	0.09000 USD	Default	5	N	64.67.2.191	Vendor F	Termination to vendor F	Vendor F	
6	86	CHINA	Proper	0.11000 USD	Default	5	N	193.50.123.6	Vendor E	Termination to carrier E	Vendor E	

Test Dialplan											
Phone Number		Routing Plan		Protocol		Date and Time					
861045676		Default		H323 SIP		YYYY-MM-DD HH:MM					
#	Destination	Country	Description	Price	Route Category	Preference	Huntstop	Route to	Vendor	Connection	Tariff
1	8610	CHINA	Beijing	0.04000 USD	Default	6	N	ny-gw-01	Vendor A	Termination to carrier A	Vendor A
2	86	CHINA	Proper	0.03000 USD	Default	5	N	ny-gw-01	Vendor C	Termination to carrier C	Vendor C
3	86	CHINA	Proper	0.06000 USD	Default	5	N	ny-gw-01	Vendor B	Termination to carrier B	Vendor B
4	8610	CHINA	Beijing	0.09000 USD	Default	5	N	84.67.2.191	Vendor F	Termination to vendor F	Vendor F
5	86	CHINA	Proper	0.11000 USD	Default	5	N	193.50.123.6	Vendor E	Termination to carrier E	Vendor E
6	86	CHINA	Proper	0.02500 USD	Default	2	N	45.12.156.200	Vendor D	Termination to vendor D	Vendor D

Routing configuration example



Consider the following example. If you have:

1. A “Standard” routing plan, which includes three route categories: “Default” (order 70), “Cheap” (order 40) and “Expensive” (order 10).
2. Six vendors (A, B, C, D, E, F) with the following rates (prefix, route category, preference, price):
 - a. 8610, Cheap, 7, 0.04
 - b. 86, Default, 5, 0.06
 - c. 86, Cheap, 6, 0.03
 - d. 86, Cheap, 6, 0.025
 - e. 86, Expensive, 5, 0.11
 - f. 8610, Premium, 5, 0.09

then, when a customer with this routing plan makes a call to **8610234567**, the system will arrange the possible routes as follows:

Vendor	Parameters	Comment
B	Default, 5, 0.06	The “Default” route category is first in the route plan
A	Cheap, 7, 0.04	This vendor has the highest preference in the “Cheap” category
D	Cheap, 6, 0.025	This vendor has the same preference as vendor C, but a cheaper per-minute rate

C	Cheap, 6, 0.03	
E	Expensive, 5, 0.11	This is the only vendor in the last route category

(Vendor F was not included in the routing, since his route category is not in the customer's routing plan).

#	Destination	Country	Description	Price	Route Category	Preference	Huntstop	Route to	Vendor	Connection	Tariff
1	86	CHINA	Proper	0.06000 USD	Default	5	N	ny-gw-01	Vendor B	Termination to carrier B	Vendor B
2	8610	CHINA	Beijing	0.04000 USD	Cheap	7	N	ny-gw-01	Vendor A	Termination to carrier A	Vendor A
3	86	CHINA	Proper	0.02500 USD	Cheap	6	N	45.12.156.200	Vendor D	Termination to vendor D	Vendor D
4	86	CHINA	Proper	0.03000 USD	Cheap	6	N	ny-gw-01	Vendor C	Termination to carrier C	Vendor C
5	86	CHINA	Proper	0.11000 USD	Expensive	5	N	193.50.123.6	Vendor E	Termination to carrier E	Vendor E

Fail-over routing

If a route fails (e.g. the remote gateway is not available, or the call could not be completed because no telephony port was available, or there was some other problem on the vendor's side), PortaSIP will automatically try to deliver the call via the next route. If that route fails as well, PortaSIP will try the one after that, and will keep trying until either the call is connected or there are no more routes left.

Number Translation

There are many different phone number formats, some used by your customers, others by your vendors. How to deal with all of them without making mistakes? PortaBilling offers a powerful tool called **translation rules** for converting phone numbers, with several different types depending on customers' needs.

Your network numbering plan

The key to avoiding problems with number formats is to choose a certain number format as the standard for your network and make sure that calls travel on your network only in this format. The ideal candidate for such a format is E.164 (of course it is highly recommended that you use this same format in billing as well). When a call arrives from your customer (with a phone number from a customer-specific number plan), PortaSwitch will convert the number into your network format. It will then travel on your network until it is sent to a vendor for termination. Just before this happens, it can be converted into the vendor-specific format.

Customer-based translation rules

Very often your customer will have his own numbering format, for example, dialing 00 for international numbers, while dialing just the phone number for local calls. Customer-based translation rules allow you to convert a number from a format specific to this particular customer. There is a special dialing rules wizard available to make such configuration easier, so that customers can even do this themselves. Customer-based translation rules have two applications:

- When a number is submitted for authorization, these rules will be applied, with the resulting number used to search rates. Thus, if your customer dials 0042021234567, you can convert it to 42021234567 and find the correct rates for the 420 prefix.
- This number will be returned to the node which requested it.

Connection-based outgoing translation rules

If your vendor requires a special number format (e.g. tech-prefix), it is possible to apply this rule to convert the number. When billing returns a list of routes, the phone numbers for routes for this connection will be converted. This only works for a routing model in which the VoIP node (e.g. PortaSIP) requests billing for routing information. If your gateway uses dial-peers or an external gatekeeper for routing, then you must configure number translation there.

Connection-based translation rules

When the call has been terminated to the vendor in a vendor-specific format, it will be reported to billing in this same format (e.g. 7834#42021234567). Now it is necessary to convert this number to the proper format for billing (4202134567), which may be done using connection translation rules. These rules will be applied to all calls which go through a given connection (even those routed there using dial-peers or other external tools)

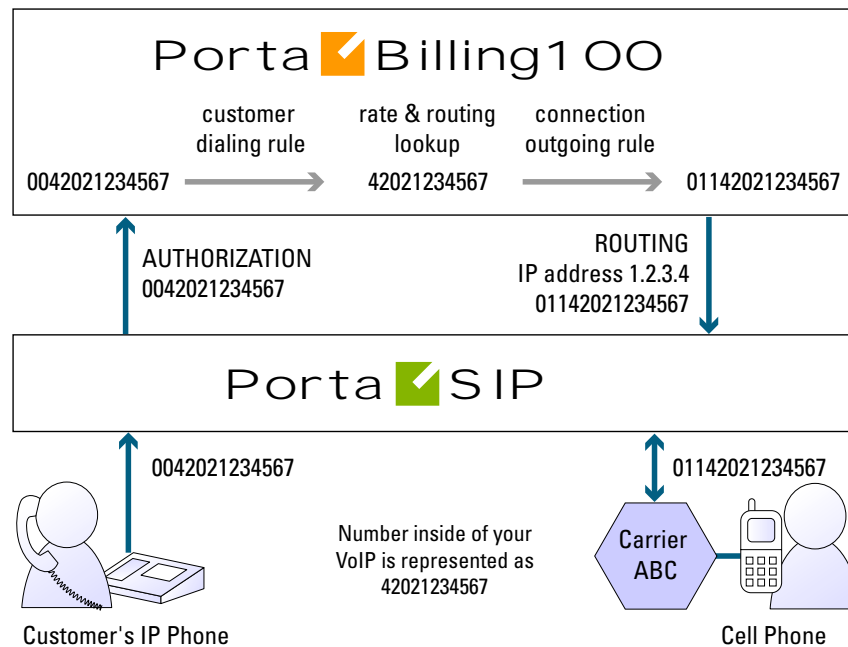
Node-based translation rules

These serve the purpose of converting a number from a custom format used by the customer into billing's internal format during authorization, depending on the gateway. For example, on a gateway in Prague, Czech Republic, there may be the translation rule "strip leading 00", while on a gateway in Moscow, Russia, the rule will be "strip leading 810 or replace leading 8 with 7".

Since customer-based translation rules were introduced, node-based translation has become obsolete. Therefore, a node-based translation rule is applied only if there is no customer-based translation rule defined for a given customer.

Number translation on your network

Below is an illustration of how different translation rules are applied during a call.



1. The customer dials a phone number on his SIP phone. He enters the number in the same format he uses on his conventional phone, i.e. 0042021234567.
2. The number is delivered to the PortaSIP server and translated using the **customer's dialing rule**, which states that the international dialing prefix for this customer is 00. So the number becomes 42021234567 (E.164 format). This number is used to search for the customer's rate for this destination.
3. PortaSIP then requests routing for this number. Carrier ABC is defined for terminating calls to the Czech Republic in PortaBilling. However, this carrier requires the number to be in US dialing format, so the international number must be prefixed by 011. An **outgoing translation rule** `s/^(011)/;` to carrier ABC has been defined, and is now applied to the phone number, with the result 01142021234567. Note that there may be several carriers who can terminate this call, each with its own numbering format. In such a case there will be several alternative routes with different phone numbers.
4. PortaSIP attempts to establish a connection to remote gateway 1.2.3.4 using phone number 01142021234567.
5. After the call is completed, PortaSIP sends an accounting request to PortaBilling, stating that a call to remote gateway 1.2.3.4 has just been completed. PortaBilling finds a connection to vendor ABC with remote IP address 1.2.3.4, and applies the **translation**

rule s/^011//; for this connection in order to convert the number from the vendor-specific format into your billing format. Thus 011 is removed from 01142021234567, and the number becomes 42021234567. PortaBilling searches for the vendor and customer rates for this number and produces the CDRs.

CLI translation rules (off-net calls)

CLI (ANI) is the calling party number (typically programmed on SIP phones). However, due to the reasons described above, this number must be represented in a specific format, depending on the situation. For instance, when your SIP account 12027810003 makes an off-net call to the United States PSTN network, the ANI number must be in the 10-digit format (area code + phone number), i.e. 2027810003. This is accomplished via the “CLI translation rule” property of the vendor’s connection.

CLI translation rules (calls terminated to SIP phones)

Another extremely useful feature of the CLI translation rule is PortaSwitch’s ability to convert the CLI (ANI) number for the incoming call into the customer’s dialing format (activated in the customer’s dialing rules settings). Let’s assume that a customer has a SIP phone with the phone number 12027810003 provisioned to it, and his dialing rules are setup for North America. While out for lunch, he receives three calls:

- From phone number 12027810002 (his colleague)
- From 420298765432 (his customer in the Czech Republic)
- From 12061234567 (his old friend from Seattle)

The ANI (CLI) numbers for all these calls will be converted, so that when he returns from lunch he will see:

- 7810002
- 011420298765432
- 12061234567

Now he can simply hit “redial” on his phone to initiate a call, since these numbers are already in the same format as he would have normally dialed.

Routing SIP On-net Calls

The SIP server automatically maintains information about all currently registered SIP user agents. Thus it is able to determine how to contact a specific SIP user agent if there is an incoming call. In response to the authorization request, the billing engine informs the SIP server that the dialed number is actually a valid SIP account, and that the call should be sent to the SIP user agent. Note that routing the call to a SIP user agent is only one of the possible routes; for instance, a call can be redirected to

follow-me numbers or a unified messaging service if the account is not available online at the moment.

Routing SIP Off-net Calls

You can have different vendors for terminating off-net calls. For example, calls to the US can be terminated either to AT&T, via a T1 connected to your gateway in New York, or by sending the call to a remote gateway from Qwest. You need a tool allowing you to manage routing policies for the different destinations. This tool is extensions routing for tariffs. Tariffs define the termination costs for each connection to a vendor, while extensions routing simply adds a few more fields to the rates in a given tariff. This allows you to easily manage both termination costs and routing from a single location on the web interface. The routing principle is simple:

- The SIP server asks PortaBilling for routing destinations for a number.
- PortaBilling checks every tariff with routing extensions associated with connection to the vendor for rates matching this phone number.
- A list of possible termination addresses will be produced (this will include remote IP addresses for the VoIP connections and IP addresses of your own nodes with telephony connections).
- This list will be sorted according to the routing preference, with entries after the first huntstop being ignored.
- A list of these IP addresses (with optional login and password for SIP authentication) will be returned to the SIP server.

NAT Traversal Guidelines

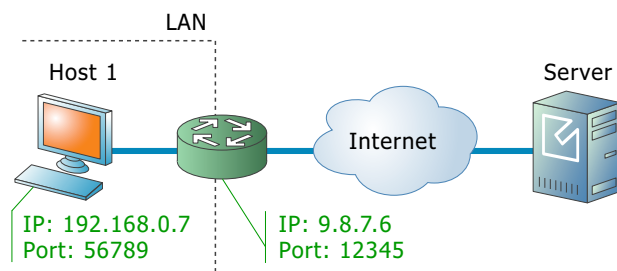
NAT Overview

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.

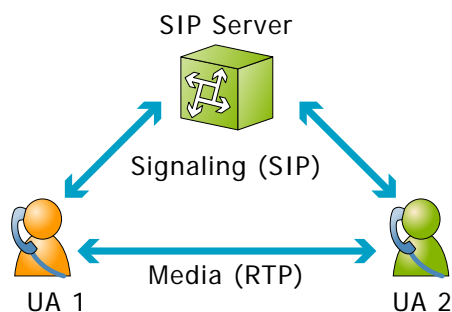
RTP – Media Stream

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.

In appendices A through C you will find a list of tested routers, as well as a typical configuration for Cisco IOS software and Cisco ATA 186 telephones which has been adapted for optimal NAT traversal performance.

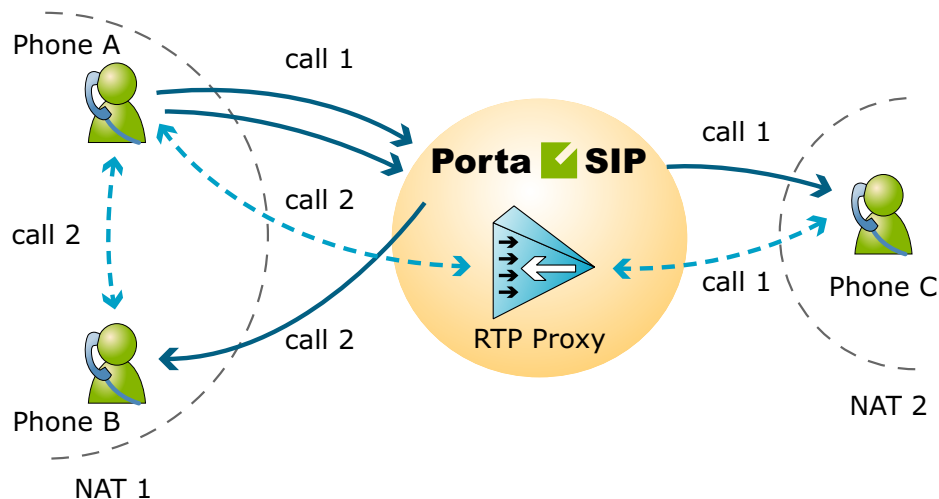
PortaOne RTP Proxy

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 single RTP proxy on an average PC server can support about 5,000 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-to-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

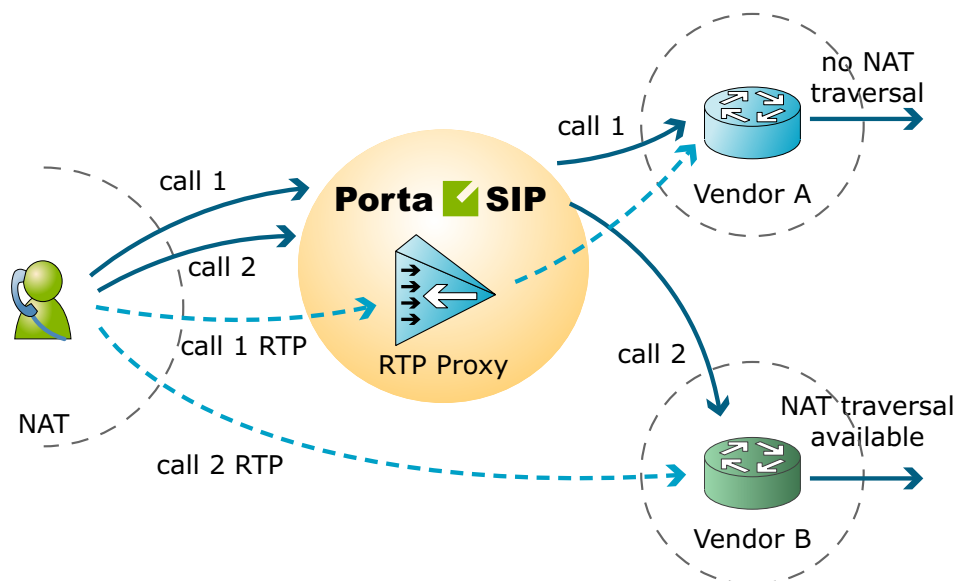
If the called (or calling) party is a remote gateway or remote SIP proxy, its NAT traversal capabilities are described in the PortaBilling configuration under connection properties. The possible values are:

- **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.

All of this is related to the “smart” logic of RTP proxying. Of course, you have control over the RTP proxy's behavior, and may change the default policy; for instance, you may permanently switch the RTP proxy off. See [porta-sip.conf](#) chapter for details on RTP proxy policy configuration.

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.

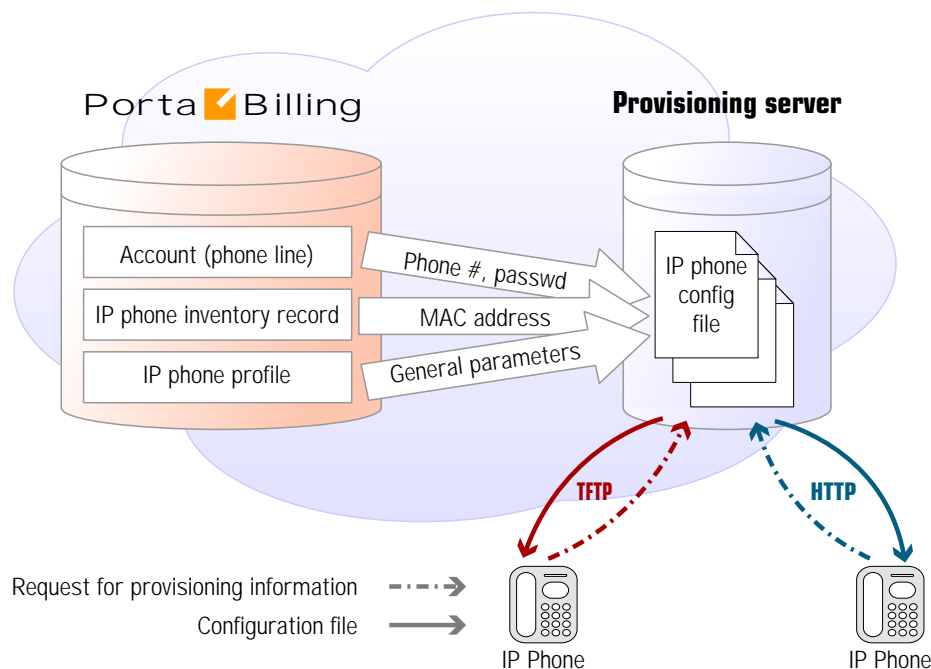
IP Phone Provisioning

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 E911 Services

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.

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.

Automatic Line / Direct Connect ("Hotline")

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

This feature is configured on the SIP phone 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: Alerts the user to incoming calls when the user's line is busy with an established call. Upon hearing the Call Waiting tone, the user can put the current conversation on hold to answer the incoming call.

Supported by PortaSwitch, assuming that the Call Waiting service has been enabled on the IP phone.

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.

Intercom Dialing

Feature description: Allows users to call Centrex extensions by dialing a standard 4-digit code, instead of the entire 7-digit telephone number.

Supported by PortaSwitch via the Abbreviated Dialing feature.

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.

2. 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
```

... configure my Cisco ATA186 to work with PortaSIP?

Perform the initial network configuration of the ATA using the built-in IVR. After your ATA is assigned an IP address, you can go to the web configuration screen at <http://<your-ATA-IP-address>/dev>.

Consult *APPENDIX C. Client's Cisco ATA 186 Configuration for PortaSIP*. For other options not listed in the table below, the default manufacturer value is assumed.

... 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. You just need to create an account for your customer with an account ID identical to the IP address of his gateway. Authentication and billing will be done in the same way as IP-based billing using H323.

... 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. 12027810003) which will be provisioned on his phone, plus some extra accounts (e.g. 4981234567), with the follow-me service on these accounts configured to always go to 12027810003.

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

You can create this application yourself according to the functionality description in this guide. A PSTN2SIP application may be purchased from <http://store.portaone.com>.

... 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 SIP-to-SIP calls?

By default, calls from one SIP account to another are treated as on-net ones, and are therefore not billed. However, if you want to bill your customers for such calls, you can do the following:

- Add the appropriate rate to the tariff associated with the accounts to be charged. For example, if you have SIP accounts with the prefix **078**, then you should add the appropriate rate for destination **078** to the tariff used to charge for outgoing calls.
- Create a special tariff with rates corresponding to the prefixes allocated for your SIP accounts (**078** in the example above). This will be the tariff used to calculate your termination expenses. Since you do not pay anything for such termination, you can enter zero prices for all of the rates.
- Create a new vendor with a descriptive name, for example, “Direct termination to SIP phones”. Add a **VoIP to Vendor** connection to that vendor with the tariff created in the previous step and enter **sip-ua** in the **Remote IP** field.

So now, if a call is made from one SIP phone to another, the originating party will be charged according to the rates you have entered in the customer’s tariff. This call will be counted as terminated to the vendor **Direct termination to SIP phones**, with zero termination cost – but it will still be recorded in the database, so you can easily view statistics for all SIP-SIP calls.

... 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.

Edit	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.

... 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 g720 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 H. 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.

3. 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 Cisco ATA 186 as a reference phone, and the Cisco ATA – 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 Cisco ATA or Sipura to the same network as your SIP phone. If possible, disconnect the SIP phone and use the same IP address for the Cisco ATA / Sipura as was previously used by the third-party SIP phone. Configure the Cisco ATA / Sipura with the same account as was used on your third-party SIP phone.
- Try to make test calls from the Cisco ATA / Sipura.
- 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 Cisco ATA / Sipura 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 Cisco ATA 186?

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.

Does PortaSIP support conferencing?

No. Full-scale SIP conferencing requires a separate software or hardware solution. However, you can make use of the features available in some SIP phones, such as Cisco ATA 186, to allow your clients to set up simple, so-called chain conferences. For more information, please refer to the documentation for each specific SIP phone.

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. In *APPENDIX G. Setting up a Back-to-Back T1/E1 Connection* you will find information on how to set up such a back-to-back connection physically and configure it in Cisco IOS.

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 (COMEDIA)*, there are details on how to configure Cisco IOS and Cisco ATA 186; for other SIP phones or gateways, check the documentation supplied with the device. If you are sure that the codec used for SIP calls is a low-bitrate one (for example, by inspecting the gateway logs), but the quality is still suboptimal, you need to determine where packet loss is occurring in the 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.

PortaSIP Configuration

PortaSIP provides a unified configuration tool. Even if a system consists of several components, using different technologies and configuration methods, you just have to edit one simple configuration file. This master configuration file is then used by PortaOne configuration scripts to manage and provision other modules, e.g. SER, B2BUA, and so on.

porta-sip.conf

This is the only file you need to edit in order to modify PortaSIP parameters. Every row starting with # is considered to be a comment; the other lines will contain VAR:VALUE pairs, separated by a colon (:). This file is created automatically during installation. Thus, assuming you provided correct parameters during installation, you do not have to change anything.



General configuration:

Variable	Description
LADDR	IP address of the SIP environment
SIP_PORT	Port on the SIP server which SIP phones should connect to; value: number (default 5060).
CANONIC_NAME	Fully-qualified domain name for this SIP server (so your customers can use contact information in the form 1234@sip.domain.com)
I_ENV	PortaBilling virtual environment id for this SIP instance (note that this is a numeric ID (<code>i_env</code>) and not the environment name; use the <code>porta-admin.pl</code> utility on the slave server to find the correct value)
RADIUS configuration	
PB_MASTER	IP address of the PortaBilling100 master host
PB_ROUTING_SERVER	IP address of the PortaBilling100 RADIUS server used to process authorization/routing requests (if different from the <code>PB_MASTER</code> above).
PB_REGISTER_SERVER	IP address of the PortaBilling100 RADIUS server used to process registration requests (if different from the <code>PB_MASTER</code> above).
PB_ACCT_SERVER	IP address of the PortaBilling100 RADIUS server used to process accounting requests (if different from the <code>PB_MASTER</code> above).
RAD_KEY	RADIUS secret key for RADIUS requests to the billing; value: string
AUTH_PORT	Port on the RADIUS server to which authentication requests should be sent (1812 by default)
ACCT_PORT	Port on the RADIUS server to which accounting requests should be sent; value: number (1813 by default)
RAD_TIMEOUT	How long the SIP server should wait for a reply from the RADIUS server before retransmit; value: number (3 by default)
RAD_RETRIES	How many retransmit attempts should be made; value: number (5 by default)

Special features configuration:

Variable	Description
FIRSTLOGIN_ENABLE	Activate the first login greeting feature (possible values: 0 or 1)
FIRSTLOGIN_CLI	Appear as CLI (ANI) number on the SIP phone for the first login greeting call; value: E.164 phone number
B2B_KA_A_INTERVAL	If a non-zero value X is provided, this

	enables sending keep-alive requests to the caller party (originating SIP device) every X seconds; zero value disables the keep-alive packets.
B2B_KA_O_INTERVAL	If a non-zero value X is provided, this enables sending keep-alive requests to the caller party (terminating SIP device) every X seconds; zero value disables the keep-alive packets.
SEND_START_ACCT	Send an accounting request to the billing when the call is started; this is necessary if you want to display a list of active calls on the billing's web interface; possible values: 0 or 1
MAX_CREDIT_TIME	Limit maximum call duration for all calls to a specified number of seconds; value: number (-1 means unlimited)
HUNT_STOP	List of SIP error codes which will stop hunting (i.e. trying the next route in the sequence); value: comma-separated list of numbers
REG_EXPIRES_MIN	Minimal interval between registrations in seconds; defaults to 300. This parameter can be used to prevent "hammering" the SIP server with registrations every second or so.
REG_EXPIRES_MAX	Maximum time interval during which the registration will be considered valid, in seconds; defaults to 7200.
ALLOW_ASYMMETRIC	0 or 1; 1 forces an RTP asymmetric flag for any non-NAT UA. The default is 0.
NO_VOICE_REJECTS	0 or 1; if set to 1, prohibits forwarding of SIP UA to a media server for an error announcement if a problem is encountered (e.g. incorrect password or invalid called number). Useful if the PortaSIP instance is working in wholesale traffic exchange mode.
YU_TEL_REMOVE	0 or 1; forces B2BUA to remove options after ';' in the userpart of CLD. Such unusually formatted CLD may be sent by some types of network equipment.
PROCESS_REFERER	0 or 1; do internal processing of REFER requests.

After you have modified the porta-sip.conf file for a certain SIP instance, you must restart that instance:

```
$ sudo /var/sipenv-<ip>/etc/rc.d/sip.sh restart
```

Starting/Stopping PortaSIP Services

If you need to stop all PortaSIP services, then execute the following command:

```
$ sudo /usr/local/erc/rc.d/sip.sh stop
```

This will properly terminate all components. To start PortaSIP, use the following command:

```
$ sudo /usr/local/erc/rc.d/sip.sh start
```

NOTE: Please always make sure that you have stopped services as described above before trying to start them again, since trying to start services when they are already running may render the service inoperable.

4. Appendices

APPENDIX A. Tested Routers and NAT Software

Commodity routers and NAT software bundled with popular operating systems, which attempt to preserve the RTP source port:

1. Linksys BEFSX41
2. Belkin F5D5230-4
3. natd bundled with FreeBSD 4.x and 5.x operating systems
4. iptables bundled with Linux kernel 2.4.x

Commodity routers and NAT software bundled with popular operating systems which do not attempt to preserve the RTP source port:

1. Internet connection sharing software bundled with the Windows XP operating system
2. Netgear RP614

APPENDIX B. Cisco GW Setup for PortaSIP (COMEDIA)

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

APPENDIX C. Client's Cisco ATA 186 Configuration for PortaSIP

UID0	[CLIENT'S ACCOUNT ID (PHONE NUMBER) 1]
PWD0	[CLIENT'S PASSWORD FOR ACCOUNT ID 1]
UID1	[CLIENT'S ACCOUNT ID (PHONE NUMBER) 2]
PWD1	[CLIENT'S PASSWORD FOR ACCOUNT ID 2]
GkOrProxy	[IP ADDRESS OF SERVER RUNNING PORTASIP]
Gateway	0.0.0.0
GateWay2	0.0.0.0
UseLoginID	0
LoginID0	0
LoginID1	0
AltGK	0.0.0.0
AltGKTimeOut	0
GkTimeToLive	300

GkId	.
UseSIP	1
SIPRegInterval	180
MaxRedirect	5
SIPRegOn	1
NATIP	0.0.0.0
SIPPort	5060
MediaPort	[DIFFERENT FOR EACH CLIENT AS DESCRIBED IN THE SETUP GUIDELINES]
OutBoundProxy	0.0.0.0
NatServer	[IP ADDRESS OF SERVER RUNNING PORTASIP]
NatTimer	0x1e
LBRCCodec	0
AudioMode	0x00150015
RxCodec	0
TxCodec	0
NumTxFrames	1
CallFeatures	0xffffffff
PaidFeatures	0xffffffff
CallerIdMethod	0xc0019e60
FeatureTimer	0
Polarity	0
ConnectMode	0xe0400
AuthMethod	0
TimeZone	[SEE CISCO ATA 186 DOCUMENTATION FOR ENTERING CORRECT VALUE]
NTPIP	192.43.244.18
AltNTPIP	131.188.3.222
DNS1IP	0.0.0.0
DNS2IP	0.0.0.0
UDPTOS	0xb8
SigTimer	0x64
OpFlags	0x62
VLANSettings	0x2b
NPrintf	0.0.0.0
TraceFlags	0

The manufacturer's default values are assumed for all options not listed here.

APPENDIX D. 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

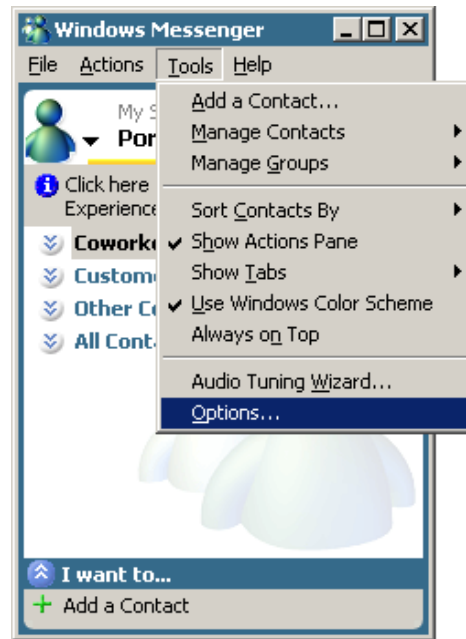
Hook State:	On	Registration State:	Registered
Last Registration At:	1/8/2003 14:07:33	Next Registration In:	2947 s
Message Waiting:	No	Call Back Active:	No
Last Called Number:	16044680035	Last Caller Number:	
Mapped SIP Port:			
Call 1 State:	Idle	Call 2 State:	Idle
Call 1 Tone:	None	Call 2 Tone:	None
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:			
SRTP Private Key:			
Supplementary Service Subscription			
Call Waiting Serv:	yes	Block CID Serv:	yes
Block ANC Serv:	yes	Dist Ring Serv:	yes
Cfwd All Serv:	yes	Cfwd Busy Serv:	yes
Cfwd No Ans Serv:	yes	Cfwd Sel Serv:	yes
Cfwd Last Serv:	yes	Block Last Serv:	yes
Accept Last Serv:	yes	DND Serv:	yes
CID Serv:	yes	CWCID Serv:	yes
Call Return Serv:	yes	Call Back Serv:	yes
Three Way Call Serv:	yes	Three Way Conf Serv:	yes
Attn Transfer Serv:	yes	Unattn Transfer Serv:	yes

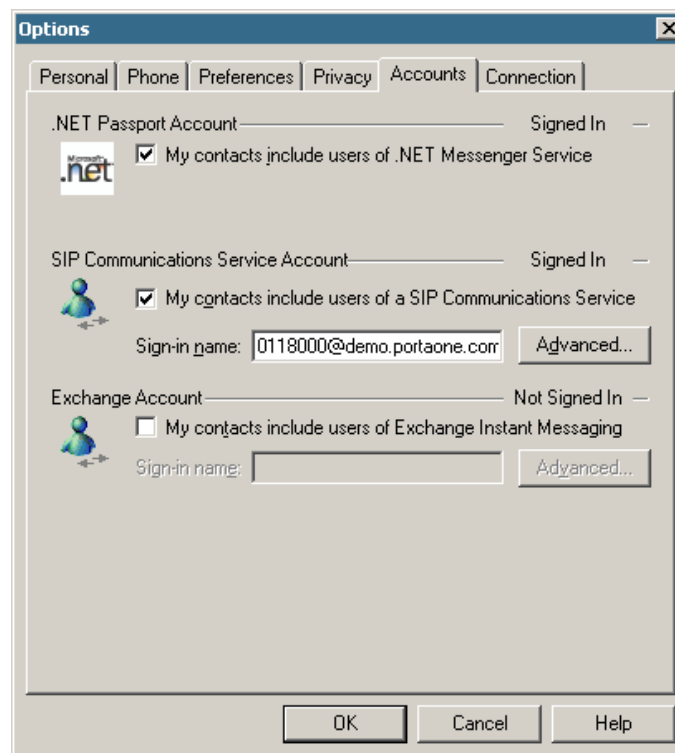
APPENDIX E. Configuring Windows Messenger for Use as a SIP User Agent

The following instructions apply to Windows Messenger version 5.0.

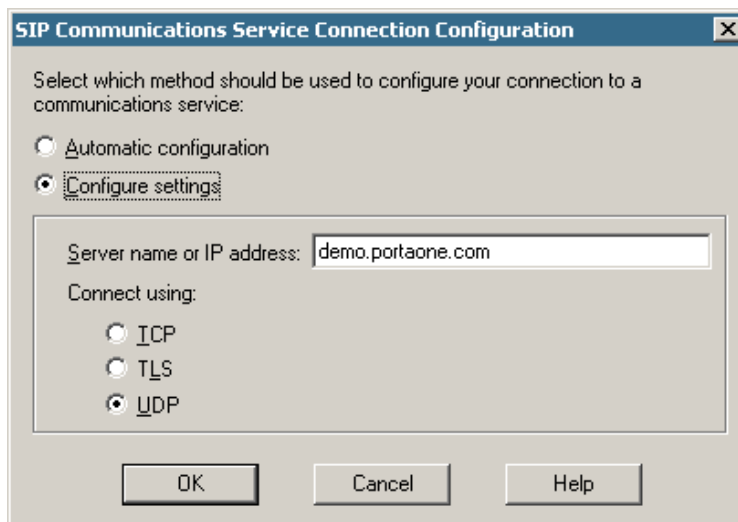
1. Start Windows Messenger, and select “Options...” from the “Tools” menu



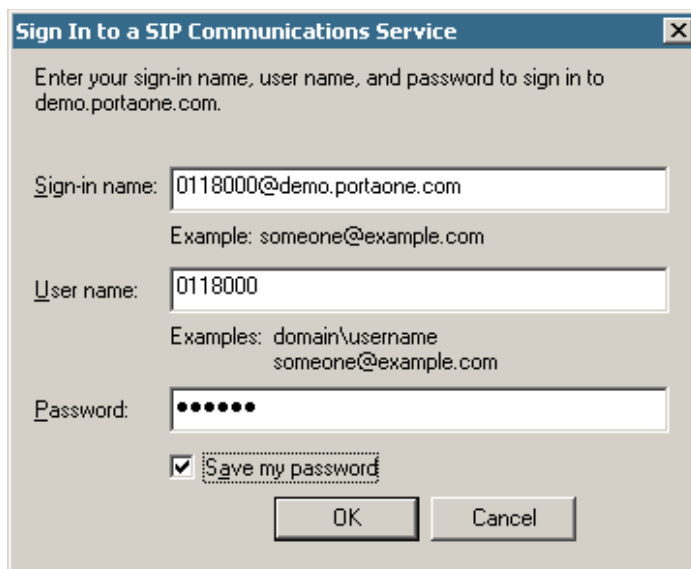
2. Check the “My contacts include users of a SIP Communication Service” check box. Enter your “Sign-in name” as shown, in the form *username@address*, where *username* is the name of the appropriate account in PB and *address* is either the IP address of the PortaSIP server or its name in DNS. Then click the “Advanced...” button.



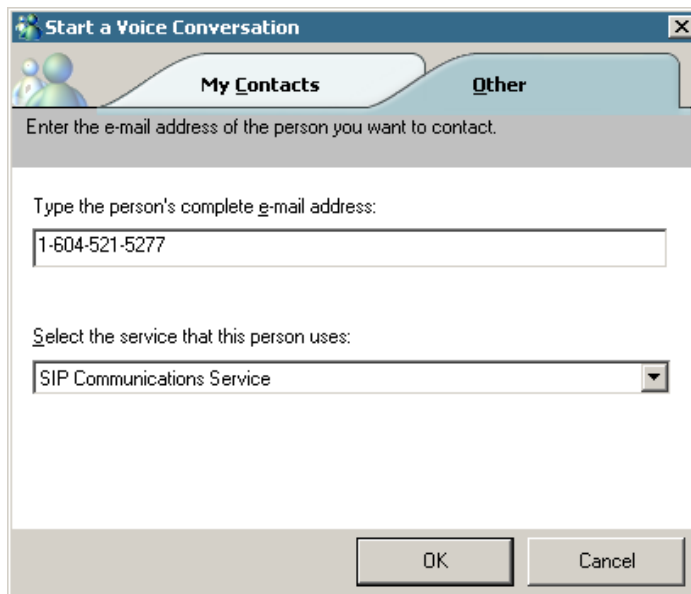
3. Click the “Configure settings” radio button and enter the “Server name or IP address” using either the IP address of the PortaSIP server or its name in DNS. Make sure that the “UDP” radio button is selected, then click OK.



4. 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.

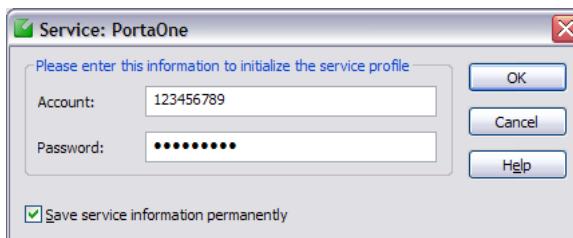


5. To make a call, click the “Action” item in the main menu, then select “Start Voice Conversation”. Click the “Other” tab, making sure that “Communications Service” is selected in the drop-down Service box, and enter the phone number in the “Enter e-mail address:” field, as shown below. Finally, click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



APPENDIX F. 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 G. Setting up a Back-to-Back T1/E1 Connection

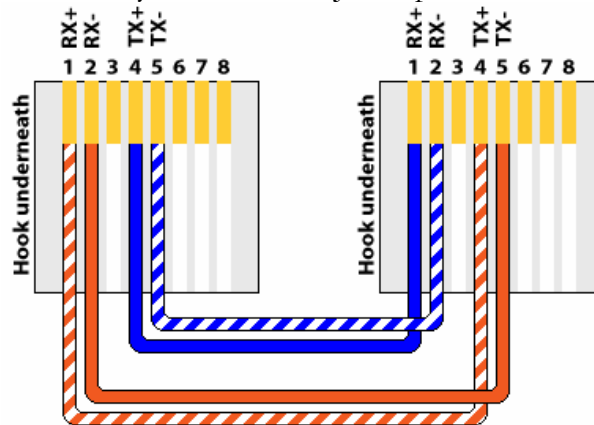
Hardware Setup

In order to make one or more back-to-back connections, you will need to construct one or more RJ-48C cross-over cables using the following table:

T1/E1 CSU/DSU Cross-Over Pinout

From RJ 48C Pin	To RJ 48C Pin
1	4
2	5
4	1
5	2

Make sure you count the RJ-48C pins as shown in the illustration below:



PRI (T1/E1) CrossOver/Loopback Cable

Alternatively, you can order ready-made ones. You can find a number of vendors producing such cables by searching for “RJ-48C cross-over cable” on www.google.com.

Once the cable is ready, plug it into the designated pair of T1/E1 ports in your Cisco AS5300 gateway.

Software Configuration

You also have to configure the T1/E1 interfaces. The sample configuration below is for T1; adjust the time slots for E1:

```
isdn switch-type primary-5ess
!
controller T1 0
framing sf
clock source line primary
linecode ami
pri-group timeslots 1-24
!
controller T1 1
framing sf
clock source line secondary 1
linecode ami
pri-group timeslots 1-24
!
controller T1 2
framing sf
linecode ami
pri-group timeslots 1-24
!
controller T1 3
framing sf
linecode ami
pri-group timeslots 1-24
!
interface Serial0:23
no ip address
isdn switch-type primary-5ess
isdn protocol-emulate network
no cdp enable
!
interface Serial1:23
no ip address
isdn switch-type primary-5ess
no cdp enable
!
interface Serial2:23
no ip address
isdn switch-type primary-5ess
isdn protocol-emulate network
no cdp enable
!
interface Serial3:23
no ip address
isdn switch-type primary-5ess
no cdp enable
```

APPENDIX H. 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 2100
- Sipura 3000
- Linksys PAP2
- Linksys WRT54GP2
- GrandStream HT486
- GrandStream HT496