

SIP-PBX
Manual
Version 2.0.1

pbxnsip

© 2007 pbxnsip Inc.

All Rights Reserved. This document is supplied by pbxnsip Inc. No part of this document may be reproduced, republished or retransmitted in any form or by any means whatsoever, whether electronically or mechanically, including, but not limited to, by way of photocopying, recording, information recording or through retrieval systems, without the express written permission of pbxnsip Inc.

pbxnsip Inc reserves the right to revise this document and make changes at any time and without the obligation to notify any person and/or entity of such revisions and/or changes. Product specifications contained in this document are subject to change without notice.

Comments are welcome. Please send them by email to wiki@pbxnsip.com.

Version: 2.0.1

Preface

A SIP-based PBX is a fairly complex product. So is the documentation. We decided to use a popular content-management system (MediaWiki) to maintain the documentation of the PBX.

This „printed“ manual is a snapshot of this online documentation. It contains most of the relevant documentation of the version 2.0.1 of the PBX. However, it is almost impossible to keep all changes updated in a single document. Therefore, we ask you to visit our online version at <http://wiki.pbxnsip.com> in case you need additional or updated information. More information can be found at our home page <http://www.pbxnsip.com>.

We hope that you enjoy the product, it makes your business more productive and it makes it easy for you to install and maintain a SIP-based telecommunication infrastructure.

The pbxnsip team.

Contents

1	Installation and Quick Start	9
1.1	Downloading and Installation of the Software	9
1.2	Logging in	9
1.3	Verifying that the System is ok	11
1.4	Configuring your PBX	11
1.5	Connecting Devices to the PBX	13
1.6	Changing Your Passwords	14
1.7	Next Steps	14
1.8	System Sanity Check	14
1.8.1	Ports.....	15
1.8.2	Permissions	15
1.8.3	Automatic Restart.....	15
1.8.4	SIP Traffic.....	15
2	Installing the IP-PBX Appliance.....	15
2.1	Installation	15
2.2	Logging into the system	16
2.2.1	Determining the IP address of the system.....	16
2.2.2	Logging into the system with secure shell	16
2.2.3	Logging in by the web interface	16
2.3	Changing system parameters	17
2.3.1	PSTN gateway setup	18
2.3.2	DID setup.....	18
2.3.3	Gain	18
2.3.4	Restart.....	18
2.4	Software updates	19
2.5	Changing the SIP port.....	19
3	User Manual	19
3.1	Basic Calling	19
3.1.1	Dialing an Internal Number.....	20
3.1.2	Dialing an Outside Number	20
3.1.3	Receiving Incoming Calls	20
3.2	Mailbox	20
3.2.1	Leaving Mailbox Messages	20
3.2.2	First Call to Your Mailbox	21
3.2.3	Picking Up Mailbox Messages	21
3.2.4	Main Mailbox Menu	22
3.2.5	Logging into your Mailbox	22
3.2.6	Forwarding Messages per Email	22
3.3	Call Forwarding	23
3.3.1	Call Redirection	23
3.3.2	Do Not Disturb.....	23
3.4	Redial and Call Return.....	24
3.5	Parking, Pickup and Transfer	24
3.5.1	Call Pickup.....	24
3.5.2	Call Park and Retrieve	24

3.5.3	Attended and Unattended	25
3.5.4	Transfer with *77	25
3.5.5	Transferring or Calling Directly to Voice Mail	25
3.6	Caller-ID Treatment	26
3.7	Call Data Record.....	26
3.8	Recording Prompts	26
3.9	Call Mixing.....	27
3.9.1	Call Barge-In	27
3.9.2	Call Teach-Mode	27
3.9.3	Call Listen-In	27
3.10	Hot Desking.....	28
3.10.1	Purpose	28
3.10.2	Logging In.....	28
3.10.3	Logging Out.....	28
3.10.4	Limitations	28
4	Login	28
5	System Administrator.....	30
5.1	Localization	30
5.1.1	Web Interface	31
5.1.2	Voice Interaction	31
5.1.3	Ring Tones.....	32
5.1.4	Time Zones	32
5.2	SIP Security.....	33
5.2.1	Why is security an issue?	33
5.2.2	How does it work?	33
5.2.3	Is SDES supported, if yes in which versions?	33
5.2.4	Is MIKEY supported, if yes in which versions?	34
5.2.5	In the context of TLS, briefly how the certificates are managed?	34
5.2.6	How can I provision phones in a secure way?	34
5.2.7	What is (in terms of technology) "security end-to-end"?	34
5.3	Overall System Settings	35
5.3.1	General	35
5.3.2	Administrator Login	35
5.3.3	Appearance	35
5.3.4	Performance	36
5.3.5	SIP Settings.....	37
5.4	Product Licensing	38
5.4.1	Installing a License	39
5.4.2	Licenses Policy	39
5.4.3	Features.....	39
5.5	Port Setup.....	40
5.5.1	HTTP	40
5.5.2	SIP.....	41
5.5.3	RTP	41
5.5.4	SNMP.....	42
5.5.5	TFTP.....	42

5.5.6	Call Managing Port.....	43
5.6	SNMP.....	43
5.6.1	Purpose	43
5.6.2	Setup	44
5.6.3	Available Object Identifiers	44
5.6.4	Example	45
5.6.5	Log Messages	45
5.7	Prepare an Extension for Plug and Play.....	45
5.7.1	Binding to a MAC address	45
5.7.2	Password Provisioning	46
5.7.3	Other relevant settings.....	47
5.8	Log Setup.....	47
5.8.1	General Logging	47
5.8.2	Specific Events.....	48
5.8.3	SIP Logging	49
5.8.4	Email	50
5.9	Loading of a Certificate	50
5.9.1	Purpose	50
5.9.2	Format.....	51
5.10	Music on Hold	52
5.10.1	Purpose	52
5.10.2	Files	52
5.10.3	Audio Input	52
5.10.4	RTP Stream	52
5.10.5	Setup	53
5.10.6	Editing	53
5.11	Changing the Appearance.....	54
5.11.1	Motivation	54
5.11.2	Unlocking the web page	55
5.11.3	Changing the Appearance.....	55
5.11.4	Providing your own content.....	56
5.12	Domains	56
5.12.1	Domain Listing.....	57
5.12.2	Create a Domain	57
5.12.3	Edit a Domain	58
5.13	Status.....	58
5.13.1	System Status	58
5.13.2	Log Access	59
5.13.3	Call Log.....	61
5.13.4	Active Calls.....	61
5.14	Recording	61
5.14.1	Recording to File	62
5.14.2	Recording to a SIP URI.....	62
6	Domain Administration	63
6.1	Settings	63
6.1.1	Default Values.....	63

6.1.2	Email Settings.....	66
6.1.3	Feature Codes.....	67
6.1.4	Address Book.....	71
6.2	Accounts	74
6.2.1	Existing Account List	74
6.2.2	Creating New Accounts.....	75
6.2.3	Extension	77
6.2.4	Auto Attendant.....	84
6.2.5	Conferencing	88
6.2.6	Hunt Group	89
6.2.7	Agent Group	91
6.2.8	Calling Card	95
6.2.9	Paging	96
6.2.10	Service Flag.....	98
6.2.11	IVR Node.....	100
6.3	Trunks	102
6.3.1	Existing Trunk List	102
6.3.2	Trunk Settings.....	103
6.3.3	Inbound Calls on Trunk.....	107
6.3.4	Outbound Calls on Trunk	109
6.3.5	CO Lines	110
6.4	Dial Plans	112
6.4.1	Dial Plan List.....	112
6.4.2	Dial Plan	112
6.4.3	ENUM	116
6.5	Status.....	118
6.6	General Topics	119
6.6.1	Park and Pickup.....	119
6.6.2	Dialog Permissions.....	119
6.6.3	Wildcard Patterns	120
6.6.4	IP Address List.....	120
7	User Mode	122
7.1	General User Settings	122
7.2	User Redirection Settings.....	124
7.3	User Mailbox Settings.....	125
7.4	User Email Settings	126
7.5	User Instant Message.....	127
7.6	Mailbox View.....	128
7.7	Missed Call List	128
7.8	Personal Call Log	129
7.9	Address Book.....	129
7.10	User Status	130

1 Installation and Quick Start

1.1 Downloading and Installation of the Software

The software can be downloaded from <http://www.pbxnsip.com/downloads.php>. Please select the operating system that you are using. If you are not experienced with Linux, we strongly recommend to use the Windows installation image. You may move the setup to a Linux computer later if you like.

If you are using the embedded appliance, please see Installing the IP-PBX Appliance.

1.2 Logging in

In order to configure the PBX, you need a web browser. The PBX uses http sessions to keep track of the context that the user is in. In order to set up such a contact, you need to log in.

To get a login prompt, just enter the address of the web server of the PBX. By default, this will be port 80, which is the default port of the system. If you want to log on to the local system, just use the address <http://localhost>.

The PBX also supports the secure transport https. If you use this transport layer, the data between the PBX and the web browser is transported using the secure https protocol. The PBX will usually offer a certificate that will cause an alert on the local web browser. Please ignore the alert or add it to the trusted certificates of your web browser. To log on to the secure connection, use a login prompt like "<https://localhost>". By default, the PBX will run the service on port 443, but during the installation you may put it on any other port that you like.



Please note that for secure communication, you should use a certificate for your domain. Otherwise, you might have to accept the warnings from the web browser about the certificate.



pbxnsip [About](#)

Login

Please enter your login information:

Account:

Password:

Login Type: ▼

Remember login information.

Copyright © 2005-2007 pbxnsip Inc. All rights reserved. See the license agreement for more information.

There are three ways to log in. The first way is to log in as system administrator. In this mode, you have access to all resources of the PBX. There is exactly one system administrator mode. Because of this, you should make sure that the login information is kept in a safe place. The second mode is to log in as domain administrator, where you can only make changes within a specific domain. The third mode is the user mode, where you can change only the settings for the selected extension.

By default, the login name for the administrator mode is "admin" and the password is empty.

If you check the "Remember login information" mark, the PBX will send a permanent cookie to the web browser. This cookie can be used next time to skip the login screen and directly move to the first page after login.

If the PBX could not allocate the port that you specified as http port, you need to locate the port number. This situation can happen for example if another web service already took the port. In these situations you can use the Windows command line command "netstat -a -p" to locate the process and find out which TCP ports it has allocated. Usually you are then able to log in. The first thing that you should do then is select another port that is available, so that after a restart the PBX will be able to allocate the specified port.

1.3 Verifying that the System is ok

Usually the installation should be working smoothly. However, if you are already running SIP processes on the system, you might have conflicts on the SIP ports (5060/5061) and/or on the HTTP/HTTPS port. If you are experiencing trouble, please check our section on System Sanity Check.

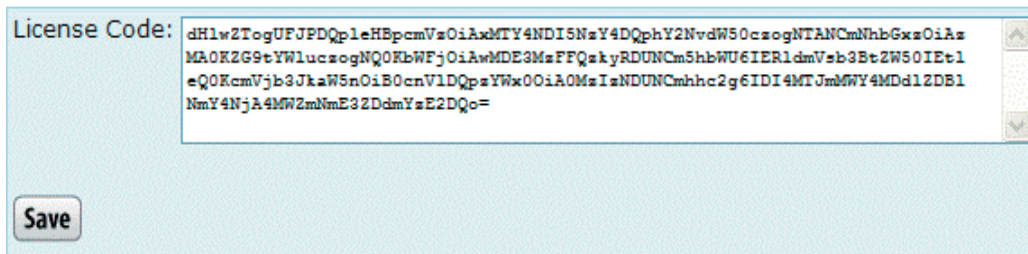
1.4 Configuring your PBX

After you have logged in, you first need to set up the license code. In order to do this, you must be logged in as system administrator. Go to the Settings tab and select License. Enter your license code into the License Code field and push the Save button.

License

Please enter your license code here.

You can get licenses from the [online](#) store. On this link you will also be able to receive demo license codes.



License Code: dH1w2TogUFJPDQp1eHBpcmVzOiAxdMTY4NDI5NzY4DQphY2NvdW50czogNTANCmVhbGxzOiAxMAOKZG9tYWluczogNQ0KbWFjOiAwdDE3MzFFQskYRDUNCm5hbWU6IERldmVsb3BtZW50IEt1eQ0KcmVjb3JkaW5nOiB0cmVldQpsYWx0OiA0MzIsNDUNCmhhc2g6IDI4MTJmMmY4MDd1ZDB1NmY4NjA4MmZmNmE3ZDdmYsE2DQo=

Save

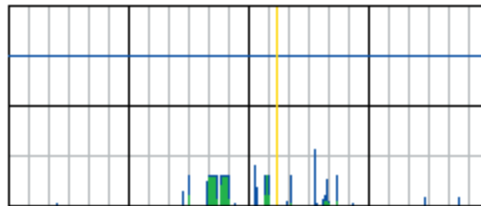
To verify that your code is correct, go to the Status tab. There you should see the License Status and the expiration date. You will also find other useful information like the version number and the routing table that the PBX identified on your system.

System Status Overview

Please use the information on this web page when you address the support.

License Status: Call Center 100
License Duration: 94 days
Version: 2.0.0.1601 (Unix)
Working Directory: /pbxnsip_head
eth0 204.11.192.2 204.11.192.0 255.255.255.248
eth1 204.11.192.3 204.11.192.0 255.255.255.248
IP Addresses: lo 127.0.0.1 127.0.0.0 255.0.0.0
default 204.11.192.2
MAC Addresses: 000255FA92ED 000255FA92EE
Calls: 42359/2311 (CDR: 2398)
Uptime: 145 11:33:59

Media CPU Usage:



In order to get a reasonable first configuration for the PBX, you can use the wizard on the pbxnsip web page. Just go to <http://www.pbxnsip.com/configurator/wizard.php>. Select how many extensions you would like to set up (you must have enough licenses for that). If you are using a PSTN gateway, you just need to enter the IP address of the PSTN gateway into the field that opens when you select "yes" in the PSTN radio button.

We also provide pre-configured configuration information for a few ITSP. If your ITSP is on the list, you just need to enter your customer number and (optionally) your password. If you don't like to enter your password here, you can enter that password later directly in the web interface of your PBX.

The screenshot shows the 'Configuration Wizard' page. At the top left is the 'pbxnsip' logo. Below it is a teal header bar. The main heading is 'Configuration Wizard'. A paragraph explains that the wizard generates a link for copying into the PBX configuration input field, and that the old configuration will be overwritten. Below this is a form with three fields: 'How many extensions should be set up?' with a dropdown menu showing '30 (40-69)', 'Are you using a PSTN gateway?' with radio buttons for 'Yes' (selected) and 'No', and 'Select an Internet Telephone Service Provider' with a dropdown menu showing 'No ITSP'. A 'Send' button is located below the form. A 'Note' section states that the password entered will be visible during configuration. Below the note is a link to an email form for missing ITSPs. At the bottom of the page is a copyright notice: 'Copyright © 2005-2006 pbxnsip Inc. | Home | Disclaimer | Privacy | Imprint'.

After hitting the send button, the web browser will provide you with a URL with the necessary parameters. Copy this URL, then go back to the PBX web interface and go to the system administrator settings tab, and select the License tab again. Below the license code you will find the field "URL" in the Request Configuration section of the page. Paste the URL into that field and hit the Save button.

The PBX will then download the configuration from the pbxnsip web page, erase the existing configuration and replace it with a pre-configured configuration.

In order to verify to configuration, you should click on the Domains tab and go to the localhost domain. If you click on Accounts, you should be able to see that there have been accounts set up.

If you want to enter the password for your ITSP now, just click on the Trunks tab and select the ITSP trunk. Then you will find a password field, where you have to enter your password twice. Hit the Save button and the trunk then should register with your ITSP.

1.5 Connecting Devices to the PBX

After your PBX is up and running, you should register a SIP phone to the PBX. Please refer to the Interoperability Pages to see your specific device.

When your phone is registered, just call *97. You should hear a prompt that welcomes you to your mailbox. If you like, you can record your name there and start using the PBX.

1.6 Changing Your Passwords

When you install the PBX, there are no passwords set up.

- You should set the password for the system Administrator. You find this setting in the administrator mode, Settings.
- You should also consider setting passwords for the extensions. In order to do that, you need to go the domains, select your domain, click on Accounts and then on the extension that you want to set up. Then you will find a password field, where you have to enter the password twice and then hit the save button.

If you want to log in as domain administrator, you can change the permission for that extension. In contrast to the system administrator, there may be several accounts that have the permission to act as domain administrator, even within one domain. The first time when you log in, there is only the system administrator account available.

To log in as domain administrator, you must enter the username and domain name in the "user@domain" form and enter the password, for example "123@test.com". If you have just one domain, you may omit the domain name after the "@" sign. If you have more than one domain and omit the domain name, the system will automatically append a "@localhost" behind the account name.

The domain administrator password is the same as the SIP password for that account.

1.7 Next Steps

After you have initially set up your PBX, you should register more extensions and try outbound and inbound calls. Check out the reference manual on how to set up additional accounts for conferencing, customize the auto attendant, define outbound DID numbers and other useful things.

Once that you are finished with your setup, you should go back to the administrator mode and fine out where your configuration data is stored. You find this information in the Status window. Just ZIP the whole directory and store it in a safe place. If you loose or corrupt the configuration, you can always replace the current configuration with this snapshot.

1.8 System Sanity Check

There are a few things that you can check after installation:

1.8.1 Ports

The PBX uses several ports for the communication with web browsers, SIP devices, DNS, TFTP and other protocols. You can use the "netstat" command both in Linux and Windows to see which ports the process uses.

Sometimes there is a conflict of ports. For example, if there is already another program occupying the SIP port (e.g. a soft phone). In this case you need to close the soft phone and restart the service.

Other typical conflicts are the usage of the HTTP port. Usually you can easily resolve that conflict by running the PBX web server on another port. In order to do this, stop the PBX service and change the working directory of the shell to the working directory of the PBX. Then you can start the PBX with the argument "--http-port 8080". Make sure that you can access the web server. Also make sure that the used ports in the web interface show the same port.

1.8.2 Permissions

You also must make sure that the PBX has the permission to write the working directory of the PBX. Typically, this is no problem. But you should check that the working directory contains folders like "users", "extensions" and so on.

Please also make sure that the directory "recordings" exists; otherwise you will have problems with the recording of audio files (e.g. mailbox messages).

1.8.3 Automatic Restart

In Windows, you can use the service manager to make sure that the service is always running. In order to do this, open the service manager and exit the pbxnsip service. There is a tab which explains what should be done when the service fails. Make sure that the service is restarted on the first attempt.

Check the Task Manager for the "pbxctrl.exe" process. This process should be running only once; if it runs several times you have probably started it several times by accident.

1.8.4 SIP Traffic

Try to register a phone and make a phone call to a number like *97. You should hear the PBX playing back an audio file.

2 Installing the IP-PBX Appliance

2.1 Installation

On the back of the system you find the following connectors:

Four FXO ports. Connect these ports to the FXO ports of your PSTN provider.

LAN port. Connect this port to your local area network.

WAN port. This port is currently not used.

- Music on hold input. You can provide life music on hold music by connecting this port to a radio or CD player. Use a standard audio jack.
- Paging output. This port may be connected to a paging system. The system will then be able to send media to this port when a special number is being dialed.
- Power. Please use only the provided power supply. During installation, you should leave the power turned off.

On the front side of the box you find several LED.

- The power LED lights up right after you turn the power on.
- The LAN and WAN led are flickering when there is traffic on the respective port.
- The FXO port led light up when there is a call active on the respective line.

After making sure that all ports are connected correctly, you should turn the power on. The boot process takes about one minute.

2.2 Logging into the system

2.2.1 Determining the IP address of the system

Before you can access the system, you need to find out what the IP address of the box is. By default, you must use a DHCP server to assign an IP address to the system. Later, you can manually assign a fixed IP address to the system.

If you have access to the DHCP server, you may locate the IP address from the log file of the server.

You may also call the PBX and enter the special code "*#4723#" to get the IP address if the box. This works only if you have a box which has this feature code setup by default.

2.2.2 Logging into the system with secure shell

You may log into the system by using secure shell. The username must be "root" and the default password is "root123". Because this password is not very secure and the root user has access to all resources on the system, we strongly recommend changing this password after setting the system up. You can do this using the passwd command.

2.2.3 Logging in by the web interface

To configure the PBX, you should use the web interface. Please see the general information on how to use the web interface to set the system up.

2.3 Changing system parameters

Ethernet eth0:

Address Type:

DNS Server:

DNS Server 1 (e.g. 1.2.3.4)

DNS Server 2 (e.g. 1.2.3.5)

Internal PSTN Gateway:

Internal IP Address of PBX

Internal IP Address of PSTN Gateway

Internal SIP Port of PSTN Gateway

Internal MoH Port

Internal Paging Port

Internal PSTN Gateway RTP Port Start

Internal PSTN Gateway RTP Port End

DID on FXO Port 1

DID on FXO Port 2

DID on FXO Port 3

DID on FXO Port 4

Input Gain

There is one special web page for this edition of the PBX. It can be found in the system administrator mode in the Settings tab under the "IP Setup" item and it has the following parameters. IP address setup

- The address type determines if you want to use DHCP or a fixed IP address. Although it is convenient it use DHCP, you should make sure that the IP address does not change after a reboot of the system (unless your IP phones can deal with this fact). Usually is avoids a lot of problems if you assign a fixed IP

address to the system. If you can, you should do this on your DHCP server by binding the MAC address of the PBX to a fixed IP address. If this is not possible, you should select an IP address which is not automatically assigned by the DHCP server. In this case, you need to provide the IP address (e.g. 192.168.1.2), the net mask (e.g. 255.255.255.0) and the IP gateway (e.g. 192.168.1.1).

- If you are using DHCP, you usually automatically provision the DNS server with the IP address provisioning. If you don't use DHCP, you must manually enter the DNS server that you want to use.

The IP address setup changes only after a reboot.

2.3.1 PSTN gateway setup

The PBX has a built-in PSTN gateway that operates as separate system. Only the setup part is specific to the PBX. The operation is the PSTN gateway changes only after a reboot.

- The PSTN gateway has its own IP address. You can choose an IP address like 1.1.1.1 for the internal interface of the PBX for this purpose, and assign an IP address of 1.1.1.2 for the PSTN gateway.
- The same applies for the SIP port, where a port 5062 is a convenient choice.
- You also need to select port numbers for the built-in music on hold stream generator (2042 is a good choice) and the internal paging output device (2040 is a good choice here).
- The RTP ports for the internal PSTN gateway must not overlap with any other ports in the system. A port range from 2048 to 2096 is a reasonable choice.

2.3.2 DID setup

When a call reaches the system, the PBX needs to know which DID has been called. This information is important for the internal call routing and the for the call logging. You may enter the 10-digit number here if your PSTN operator typically uses 10-digit codes. Otherwise, you might choose the 11-digit code which includes the leading "1". If you have a port unconnected leave the field empty. If you enter a number, the PBX assumes that the port is available for outbound calls.

2.3.3 Gain

The gain setup is very important for a good audio quality. Please do not change the amplification on the IP phone to compensate for low or high gain, because this has negative effects for internal calls and for calls that go to the mailbox. The gain value of 0 is reasonable for many installations. If you should have a long cable, you may choose to increase the gain.

2.3.4 Restart

If you did any changes on this web page, you need to restart the system.

2.4 Software updates

Software updates require that you log in using the secure shell login mechanism. The system is internally using a standard Linux distribution, so that most of the software upgrade instructions also apply to the software upgrade instructions for this box. If you just need to upgrade the PBX, you can perform the following steps:

1. First stop the PBX process. You can determine the PBX process number with the command "ps -auxww".
2. Get the new image with the command wget. You need to know the location of the image in the internet, e.g. "wget http://www.pbxnsip.com/download/pbxctrl-tecom-2.0.1.1624".
3. Restart the system with the command "sync;reboot;exit".

2.5 Changing the SIP port

If you are able to use DNS SRV, it does make sense to change the standard SIP port from 5060 to something else. This makes it a little bit more difficult for attackers to locate your PBX port and send junk traffic to that port.

If you want to do that, you need to do the following steps:

- Change the port setting in the Port settings in the administrator mode. After that you need to reboot, so that the PBX picks the change up.
- Then you must save the IP Setup again (also in administrator mode), so that the FXO driver settings are updated. Those settings also contain the SIP port of the PBX, and this port also needs to be updated. After saving them, you need to reboot your box again.

3 User Manual

This section will show you how to use the pbxnsip PBX with a standard Voice over IP-phone. Although the usage of different phones varies significantly, you can use most of the features of the PBX in a similar way.

The access codes shown in this manual are the default codes. Your system administrator may assign different codes for the available features. In that case, you should receive a list of the functional feature codes.

Many phones require that you press the Ok button (like on the cell phone) to start a call; other phones may accept pressing the pound (#) key or a check mark key instead. However, for the usage of the PBX that does not make any difference.

3.1 Basic Calling

Making phone calls using an IP-PBX is not much different from traditional telephone systems.

3.1.1 Dialing an Internal Number

To call another extension, just dial the number. For example, if you want to reach extension 123 - just enter "123" and start the call.

There are several services that your PBX System Administrator may have programmed for you (like auto attendant and conference mixing) that can also be reached by dialing an extension number.

3.1.2 Dialing an Outside Number

To dial an outside number, just enter the number that you want to reach. Please note that your system administrator may require a prefix before the number that you want to dial (for example "9"). On some VoIP phones, you may have a dial plan that automatically dials the number without requiring that you press the start key.

The PBX allows the administrator to assign an outside dial plan to each user. Depending on company policy, this feature may be used to restrict certain extensions from placing outside calls or from placing calls to expensive numbers.

If you are not in your office and your company has a strict telephone bill policy, you might want to tell the PBX that you want to bill an outgoing call to your extension number. This feature is useful if you are located in a room that has no permission to place outside calls, for example a kitchen. You must dial *91 to use this feature. The system will prompt you for your extension number, your access code and the destination number.

3.1.3 Receiving Incoming Calls

Incoming calls are usually indicated with a ring tone. Calls from another extension sound different than calls from an outside line (depending on the phone model that you are using).

You should see the Caller-ID on your phone. If the Caller-ID is in your personal address book or in the domain's address book, the PBX will insert the name of the caller.

3.2 Mailbox

3.2.1 Leaving Mailbox Messages

When a user is not available, the voice mail system may pick up the call. In this case the caller will hear an announcement indicating that he/she may leave a message after the tone. If the extension did not record a name, the PBX will spell the extension number.

After leaving the message, the caller can simply hang up (the message will be delivered) or the caller can press the pound sign to access the standard message option features.

In this case the caller has three options:

- If an operator number is available, pressing "0" will send the message and connect the caller with the operator.
- Pressing "1" will delete the message. If the caller presses the "2" option after that he can leave a new message; otherwise no message will be sent.
- Pressing "2" will give the caller the opportunity to record a new message.
- Pressing "3" will make the message as urgent.

If the mailbox is full, the caller will hear an announcement that makes this clear. If the mailbox is full, but there are saved messages, the PBX will make room for a new message by deleting the oldest saved message.

3.2.2 First Call to Your Mailbox

The system administrator may assign a mailbox to your account. The mailbox will pick up messages when you are not available. The message will either be stored for telephone retrieval or forwarded as email.

To go to the voicemail system, you just dial *97 or your extension number.

The first time you call your mailbox, you will have the opportunity to record your name and a personal greeting. This name recording will be used in announcements to callers. If you choose not to record your name, your extension number will be recited to callers. You may record your name later at any time.

3.2.3 Picking Up Mailbox Messages

If you have a voice message in your mailbox and the message has not been forwarded to you by email, your phone should indicate that a message is waiting for you Message Waiting Indication (MWI).

Usually this is a blinking LED light. Depending on your phone type, you may be able to press the message retrieval button, which is just a shortcut for dialing the mailbox number (for example *97). The system will automatically start reading out your messages.

During message playback the following keys are available:

- "1" will start reverse playback like on a tape recorder. If pressed again, the reverse playback will be faster.
- "2" will stop/resume playback.
- "3" will start fast forward the playback. If pressed again, the playback will be faster.
- "4" will read the message again (without envelope information).
- "5" will read the message again, including the "envelope information". This means the time and caller will be included in the message announcement.
- "6" can be used to move the message into another mailbox. The PBX will ask for an extension number and after a verification move the message to another

mailbox.

- "7" will delete the message and move to the next message.
- "8" will leave the mailbox and call the number that has left the message (if that number is not an anonymous number). The PBX will prompt for verification, pressing a star will get the user back to the message readout.
- "9" will save the message in the mailbox.
- "0" will play a help text

After all your messages are played, you will hear the main menu for our voice mailbox.

3.2.4 Main Mailbox Menu

From the main mailbox menu you can listen to your messages; change the access code (Mailbox PIN) for your voice mail; or record your name or record a personal greeting.

- "1" will read new and saved messages.
- "2" makes it possible to change the PIN code for the mailbox
- "3" will ask for a new name recording
- "4" will ask for a new personal greeting message.
- "*" will start dialing a star code. For example, this way you can record a new announcement for the auto attendant of the office while you are in your mailbox (e.g. from a cell phone while you are traveling).

3.2.5 Logging into your Mailbox

When calling your mailbox from a different phone you will hear the mailbox announcement. The PBX assumes that you are someone who might want to leave a message. To retrieve your voice mail, just enter your access code (Mailbox PIN). If the code matches, the system will start reading out messages.

Usually a voice mailbox is set up without an access code. In this case you must call from your extension into the mailbox (by simply dialing your extension or *97). You can follow the main menu instructions to set up the access code if you choose to have one. Using an access code is normally advised.

3.2.6 Forwarding Messages per Email

If your system administrator has set the PBX up with your email address, you may choose to have your voicemail forwarded to your email. To turn this feature on, call *95. Ask someone to leave a message on your mailbox to check that the forwarding works. If there are problems, ask your administrator to check the email address and the settings for the email server.

Call *96 to disable the email forwarding.

3.3 Call Forwarding

3.3.1 Call Redirection

There are several events that may trigger the redirection of an incoming call. The PBX differentiates between the following cases:

- **Always:** All incoming calls are forwarded. For example, this can be used when you are away and a colleague is answering your phone or when you want to redirect all calls to your cell phone.
- **No answer:** Calls are redirected after a certain time when the extension does not pick up. Typically, you use this to redirect incoming calls to an assistant or to your secondary phone in case that you are not sitting next to your telephone
- **Busy:** Calls are forwarded if the extension is busy. Typically you will program this number to redirect calls to a team assistant or to a colleague. This way incoming calls are answered when you are busy on another call.

To turn the "call forward always" on, dial *71. You will hear an announcement that asks you to enter the call forwarding number. Enter the number and press the pound key (#). The system will repeat the number and then hang up. If you want to change the forwarding number just call *71 again.

Alternatively you can turn on "call forward always" by dialing the *71 code plus the redirection number and then starting the call. This has the advantage that you can check the number on the display of your phone.

To disable "call forward always" dial *72. You will hear an announcement saying call forwarding has been turned off.

Programming "call forwarding on busy" works in a similar way. Dial 73 to turn it on and program the forwarding number. Like with the other codes, you can also put the number directly behind the star (*) code.

Dial *74 to turn "call forward on busy" off. To turn "call forward on no answer" on, dial *75. Like with the other codes, you can also put the number directly behind the star code (*). Your system administrator has set the time limit at which un-answered calls are forward. Please contact your system administrator if you want to change this value.

To disable the "call forward on no answer", dial *76.

3.3.2 Do Not Disturb

Do Not Disturb (DND) is similar to the call forward already described in the previous section. However, the typical case is that you temporarily don't want to be disturbed (for example, because you have a meeting). To turn DND on, dial *78.

To turn DND off, dial *79.

If you are a member of a hunt group, the call forwarding conditions for your extension will not apply when the hunt group is called. But if you turn DND on, even

calls that go to the hunt group will leave your phone silent.

Most VoIP phones have a button that acts in a similar way. However this DND function might not be available or might not work as reliably as setting DND for your phone on the PBX.

DND can be overridden by a person that has the DND override permission. Typically this is a secretary who should be able to call the boss, even if he is on DND.

3.4 Redial and Call Return

To redial the last number called, just dial *66.

Call Return (*69) will dial the number of the last call that you missed. The number will be available until you establish a call to that number. This will prevent you from calling back the same person twice.

If you reach an external mailbox the system will believe that the call was established successfully and clear the number. If you reach a mailbox of another extension on your PBX system, the call return number will not be cleared and you will be able to try to reach that extension later by dialing the call return code. The PBX will only store a call return number for calls that contain a valid caller-ID.

Please also note that if you have several telephones that share the same extension number, these devices will share the same redial and call return number.

3.5 Parking, Pickup and Transfer

3.5.1 Call Pickup

As a general rule, you can pick up a call that is ringing at any other extension by dialing *87.

Your telephone system administrator may have configured your PBX with a more strict pickup policy. In that case, you will only be able to pick up calls directed toward members of a hunt group to which you belong. For example, if incoming calls normally first ring extension 501 for a few seconds, then 502 for a few seconds, and then your extension, you will be able to pick up a call to that hunt group while it is ringing extension 501 or while it is ringing 502.

3.5.2 Call Park and Retrieve

While in many cases you may dispose of a call by transferring it to a specific extension, in certain situations you will want to "park" a call so that it can be picked up by an unspecified extension.

Parking a call so that it may be picked up by any extension is a two-step process. First put the call on hold; then, dial *85 to park the call. You will hear an announcement that the call has been parked. At that point, the call can be picked up by any extension that dials *86.

Again, your telephone system administrator may have configured your PBX with a more strict pickup policy. In that case, you will specify a group to which you are parking the call (*85610 for example for group 610). Any member of that group can then pick up the parked call by dialing *86.

3.5.3 Attended and Unattended

If your telephone has a transfer button, the PBX will receive the transfer signal and switches the call to the provided destination. There are generally two types of transfer. The simplest transfer is called a "blind" transfer. The other type is often referred to as an "attended" or a "consultative" transfer. In an attended transfer, you speak with the party to whom the call will be transferred to ensure that the call is wanted. In a blind transfer, you simply transfer the call with no knowledge of whether the person called will be available to take the call.

To initiate a "blind" transfer, just press the transfer button on your phone and dial the extension to which you are transferring by pressing the extension number keys and the call start key.

To initiate an attended transfer, first put the caller on hold (using the hold button on the phone); then dial the number to which you will transfer the call. If the person on the receiving end of your call is prepared to take the call you can just press the transfer key and the call that is on hold will be transferred. You do not have to press the hold button to free the call. If the person is not available to take the call, you can press the hold key to reclaim the call and discuss the caller's options with him or her.

3.5.4 Transfer with *77

Many mobile devices do not have options to transfer calls. However they are able to put a call on hold. The PBX supports blind transfers for such devices in the following way:

- Put the call that should be transferred on hold;
- Then dial *77 followed by the destination number.

Then the PBX will put the call off hold and redirect it to the destination.

Please notice that a blind transfer does not check if the call will be connected. If the number is busy, does not exist or just does not pick up, the PBX will not send automatically the call back.

3.5.5 Transferring or Calling Directly to Voice Mail

If your PBX System Administrator has enabled a prefix (normally "8") to enable you to call a voice mailbox directly, you can "blindly" transfer a call to someone's voice mail by pressing the transfer key, then that mailbox prefix key, followed by the extension number and the call start key. Of course you can also call any person's voice mailbox directly by similarly pressing the mailbox prefix key followed by the extension number and the call start key.

3.6 Caller-ID Treatment

Caller-ID's are usually telephone numbers. By providing your caller-ID to the party that you are calling, the called party may be able to look you up in an address book, initiate a callback, or just see who is calling.

Sometimes you want to reject calls that come from callers whose Caller ID does not reveal their identity. Most VoIP systems use the name "anonymous" in the caller-ID in such a case. To treat these calls, dial *88. If you have set the call forwarding on busy condition, the PBX will forward anonymous calls to that destination (for example, your assistant). This way, you can make sure that anonymous calls get screened first before you take the call. If you have not set the call forward on busy, the system will play an announcement to the caller that tells him that the call can not be taken because of the blocked Caller-ID.

To allow anonymous calls again, dial *89.

If you want to place a call without showing your caller-ID, dial *67. You will hear an announcement that the caller-ID will be blocked for all future calls.

To enable your caller-ID again, dial *68. Please note that the caller-ID will always be presented for internal calls.

3.7 Call Data Record

Sometimes you receive a call from someone that you have to call back. If your system administrator has set up your extension with your email address, instead of asking the person on the phone to spell the phone number and scribble it down on a notepad, you can direct the PBX to send you an email with the call details.

To receive a "data record", dial *63 after the call. The system will send you an email with the Caller-ID, the duration of the call and the time of the call.

3.8 Recording Prompts

The attendant and the agent group support the recording of customized greetings. You can record those greetings from any telephone in your network.

Consult the system administrator manual if you want to restrict the extensions that are allowed to record greetings.

In order to record a greeting, dial *98 followed by the account number (e.g. *98123 if 123 is the number of your auto attendant). The PBX will prompt you for your new prompt. If you just want to delete the old prompt and use the standard prompt, press the star key during the announcement.

The agent group has up to ten announcements. The announcement with the number 0 is the initial announcement; the announcements 1 to 9 are placed in a loop. In order to record those announcements, you need to dial *98 + the group number + * + the announcement number (for example, *98123*4 to record

announcement 4 in the account 123).

3.9 Call Mixing

One of the benefits of the PBX architecture is that existing calls can be interrupted and monitored.

All three modes, and especially the listen in mode, are severely affecting the privacy of the calls on the PBX. Therefore, those modes are only available to extensions that are specifically allowed to use those features. In the permissions tab of the respective extension, the domain or system administrator has to enable the features. Please consult corporation and government regulations if turning these features is allowed in your environment. Illegal listening to phone calls is a severe crime, and system administrators must be aware about that.

To see which calls are active, you can monitor the extension's state of the state of a CO-line. For example, you can do this by using the LED key of a SIP phone with the associated display.

3.9.1 Call Barge-In

In call barge in, two persons that are talking to each other are put into a kind of conference with a third person. Typically, this third person is a secretary reminding ("saving") the boss about another appointment. Both parties will hear the third person come into the call ("knock knock") and both parties will be able to hear what the third person has to say. The existence of the barge in call depends on the existence of the underlying conversation.

In order to barge into a call, dial *81 followed by the extension number that you would like to interrupt, then press dial.

3.9.2 Call Teach-Mode

In teach mode, only one side of the call can hear the third party. This is typically useful in a call center when a trainer wants to give tips to a new agent, so that the customer does not know about the teacher in the background. This mode is also sometimes called whisper mode, because the agent's phone must have a real good echo cancellation so that the customer does not hear some background echo.

In order to start the teach mode, dial *82 followed by the extension number that should hear your voice, and then press dial.

3.9.3 Call Listen-In

The listen mode is similar, but completely stealth mode. The two persons talking to each other are not notified about the listen in and cannot hear what the third person says on the phone (e.g. breathing).

In order to start listening to calls, dial *83 followed by the extension number that you would like to monitor.

3.10 Hot Desking

3.10.1 Purpose

"Hot Desking" (see for example http://en.wikipedia.org/wiki/Hot_desking) makes it possible that employees temporarily or permanently change the routing of all their calls to a specific physical device. Then all calls to that extension, also as part of the hunt group or agent group, get routed to that extension.

Hot Desking means that the person takes ownership on the phone. That means that outbound calls from this phone will show his caller-ID. It is not expected that other significant inbound traffic goes to the originally registered extension. This fact suggests that offices use "virtual" and "real" extension numbers:

- "Real" extension numbers are used for employees with a fixed location (e.g. switch board, management)
- "Virtual" extensions don't have any registrations. They are just used for routing calls to a specific user. They use real extension numbers that are not assigned to any other person, so that there is no conflict between identities on a specific physical device.

In cases when an employee just wants calls to his extension being routed to a colleague's office, it is better to use the unconditional redirection feature of the PBX. This feature must be turned on before the user leaves his office.

3.10.2 Logging In

When you want to log in, enter the Hot Desking star code (typically "*70"). The PBX will prompt for the extension number and the PIN code for that extension number and acknowledge the Hot Desking with a "the service is active now".

3.10.3 Logging Out

In order to log out, you just need to call the Hot Desking star code from a location that is currently registered as hot desk or from the phone that holds a registration for extension in question. The PBX will answer with a "the service is inactive now".

3.10.4 Limitations

Hot Desking has limitations. Because the configuration of the device does not change during Hot Desking, you will not be able to move telephone preferences (like ring tones, address book programming, etc.) to another desk.

4 Login

You can use a standard web browser for the communication with the PBX. Where ever inside or outside of your network you can connect to the web port of the PBX, you can log in to the PBX. The PBX uses http sessions to keep track of the context that the user is in. The session identifier is stored as a temporary cookie in

your web browser. Usually those cookies are allowed today, if that is not the case you need to allow it.

To get a login prompt, just enter the address of the web server of the PBX. By default, this will be port 80, which is the default port of the system. If you want to log on to the local system, just use the address `http://localhost`.

The PBX also supports the secure transport `https`. If you use this transport layer, the data between the PBX and the web browser is transported using the secure `https` protocol (see the documentation on `https` in the Internet). The PBX will usually offer a certificate that will cause an alert on the local web browser. Please ignore the alert or add it to the trusted certificates of your web browser. To log on to the secure connection, use a login prompt like `https://localhost`. By default, the PBX will run the service on port 443, but during the installation you may put it on any other port that you like.



pbxnsip [About](#)

Login

Please enter your login information:

Account:

Password:

Login Type: ▼

Remember login information.

Copyright © 2005-2007 pbxnsip Inc. All rights reserved. See the license agreement for more information.

There are three ways to log in. There is a selection box where you can tell the system how you want to log in. If you choose "automatic", then the PBX will first try to log you in as system administrator, if that is not possible it will try domain administrator, and if that does not work it will try to log you in as user.

The first way is to log in as system administrator. In this mode, you have access to all resources of the PBX. There is exactly one system administrator mode. Because of this, you should make sure that the login information is kept in a safe

place. By default, the login name is "admin" and the password is empty.

The second way to log in is as domain administrator. In contrast to the system administrator, there may be several accounts that have the permission to act as domain administrator, even within one domain. The password in this mode is the password for this extension, which is the same as the SIP password (but not the PIN code).

To log in as domain administrator, you must enter the username and domain name in the "user@domain" form and enter the password, for example "123@test.com". If you have just one domain, you may omit the domain name after the "@" sign. If you have more than one domain and omit the domain name, the system will automatically append a "@localhost" behind the account name.

The domain administrator flag is used to control the permissions of the extension. If the flag is set to true, the web interface will accept the user's login (same as their extension registration) and allow them to change the settings of the domain.

The third mode to log you in is the user mode. The login for this is similar to the domain administrator mode, but you are just taken to a different web page and you can make only changes in your account's realm.

If the PBX could not allocate the port that you specified as http port, you need to locate the port number. This situation can happen for example if another web service already took the port. In these situations you can use the Windows command line command `netstat -a -p` to locate the process and find out which TCP ports it has allocated. Usually you are then able to log in. The first thing that you should do then is select another port that is available, so that after a restart the PBX will be able to allocate the specified port.

5 System Administrator

5.1 Localization

Version 2 is in general independent from languages. This makes it possible that new languages can be added without having to change the code of the program.

There are a few exceptions to this rule. The first exception is that the PBX automatically falls back to US-English when a requested resource is not available in the specified language. Therefore, it is a good idea to install the US-English files in any case.

The second exception is the spelling of numbers and dates. By default, all numbers and dates are spelled with the English number ordering. Only for German, there are several changes. As more languages are being added to the system, this will be improved in future releases.

5.1.1 Web Interface

The web interface is generally language independent. The content is UTF-8 encoded, which makes it easy to use characters which are not on the core ASCII char set.

For every supported language, the PBX needs a file called lang_xx.xml, where xx is replaced with the language code (e.g. en, de, fr, sp). This file is being read after startup of the PBX process. It has a XML-encoded content which looks like this:

```
<?xml version="1.0" encoding="utf-8"?>
<language name="de">
  <file>
    <item id="yes">Ja</item>
    <item id="no">Nein</item>
    <item id="on">An</item>
    <item id="off">Aus</item>
  </file>
  <file name="dom_accounts.htm">
    <item id="name_ext">Durchwahl</item>
    <item id="name_aa">Automatische Vermittlung</item>
  </file>
</language>
```

The name attribute of the language tag indicates which language is being defined. It should be the same as the xx in the filename of the XML file.

For every file that exists in the web server, there should be an entry with the name "file", which lists the used texts in that page. The name of the web page must be indicated with attribute "name". If the attribute is missing, the PBX will use that item as a fallback, which can be used in all web pages (useful for often used items like "yes" or "no").

The XML file for US-English is available on demand and can be used as template.

5.1.2 Voice Interaction

The PBX uses voice prompts in many application areas, for example in the mailbox and the auto attendant. The necessary files are located in the working directory of the PBX in a directory with the name audio_xx. The PBX checks during startup, which directories are available and then determines which languages are installed.

In order to add a new language, you need to have the voice prompts. The files must have 8-kHz sampled WAV files in uncompressed audio format. You can use either u-law encoded files (8 bits per sample) or linear-encoded bytes (16 bits per sample).

If you want to record another language, please contact us for access to the

list of needed prompts.

5.1.3 Ring Tones

Almost every country has its own ring tones. Those ring tones are also stored in the `audio_xx` directory. The PBX determines after startup, which tones are installed.

If you want to install a new ring tone, you must provide the files "ringback.wav" and "busy.wav".

5.1.4 Time Zones

The PBX is able to deal with several time zones at a time. This makes it possible, that every user can select his home time zone, so that for example mailbox messages are read out with the time zone of the user. The PBX also uses the time zone information during the provisioning of the phones, so that the phone will also use the time zone of the user.

In order to make this happen, the PBX needs a time zone configuration file, which is encoded in XML and looks like this:

```
<?xml version="1.0" encoding="utf-8"?>
<timezones dict="timezones.xml">
  <zone name="AKDT">
    <description>Alaska Time Zone</description>
    <gmt_offset>-32400</gmt_offset>
    <dst_offset>3600</dst_offset>
    <dst_start_day_of_week>1</dst_start_day_of_week>
    <dst_start_month>4</dst_start_month>
    <dst_start_time>02:00</dst_start_time>
    <dst_start_week_of_month>1</dst_start_week_of_month>
    <dst_stop_day_of_week>1</dst_stop_day_of_week>
    <dst_stop_month>10</dst_stop_month>
    <dst_stop_time>02:00</dst_stop_time>
    <dst_stop_week_of_month>Last</dst_stop_week_of_month>
  </zone>
  <zone name="CST">
    <description>China, Taiwan</description>
    <gmt_offset>28800</gmt_offset>
  </zone>
</timezones>
```

The name of the time zones is reflected in the `lang_xx.xml` file, where the translated name of the time zone can be found. The description tag is used for fallback purposes.

A timezone must have the usual entries for GMT offset and the daylight savings information (see http://en.wikipedia.org/wiki/Daylight_saving_time). If a time zone has no daylight savings, those tags can be left out.

Unfortunately, the system file in Windows and Linux do not provide enough information to allow plug and play information. If you would like to add a time zone, please let us know. We will add more time zones in upcoming releases.

5.2 SIP Security

5.2.1 Why is security an issue?

Users expect that their phone calls are kept private. Listening to phone calls without permission from a public authority is illegal, and there are frequently cases in the press when this rule is being violated. Unfortunately, there are methods that make it possible to redirect packets in the local area network, for example to a desktop PC (ARP attacks). While you had to get physical access to the cable for TDM-based PBX, you can do this by installing a sniffer tool on your PC.

To address this problem, SIP uses the secure transport layer (TLS), which is also used for web-based security. TLS is based on SSH 3.0. The encryption of the voice packets uses a different standard, SRTP. SRTP is based on AES with at least 128 bit. This should be "pretty private", even if someone is able to relay the packet via PC in the network.

5.2.2 How does it work?

When a phone registers, it establishes a secure connection to the PBX. This security negotiation may take a few seconds—there is some heavy number crunching involved. But the registration period is not time critical, because the user is not aware of this delay.

After the secure connection between the phone and the PBX is established, either the phone or the PBX may initiate a call. The call-related information like caller-ID will be private between the PBX and the phone, because the information is exchanged using the existing secure connection. This call setup is fast, as the necessary security information has already been negotiated during the registration process.

The keys for the SRTP can now also be exchanged in a secure way. Like the caller-ID, this information is invisible to someone listening on packets in the network.

During the call, the PBX will receive SRTP packets, decrypt them, and send them out on the other side of the call. If the other side of the call is also using SRTP, the PBX will encrypt the RTP traffic using the key that has been negotiated with this side. This is called "SRTP transcoding". Because the PBX does have the security context for both calls, it is able to record the call, even if both sides are using secure media.

5.2.3 Is SDES supported, if yes in which versions?

SDES stands for "Session Description Protocol Security Descriptions for Media Streams". The SDES standard is used to exchange the keys between the phone and

the PBX (see for example <http://en.wikipedia.org/wiki/SDES>). The pbxnsip PBX supported SDDES right from the beginning. SDDES is not a RFC (<http://tools.ietf.org/html/rfc4568>).

5.2.4 Is MIKEY supported, if yes in which versions?

No, this is not supported. The reason is that MIKEY comes with a high implementation effort and it seems that most implementers prefer SDDES.

In the context of SRTP, what happens if the IP-phone supports authentication tag but with length less than 80-bit (as described in RFC3711)?

According to SDDES, the MAC must be either 4-byte or 10-byte. We support both modes. The negotiation happens in SDDES.

5.2.5 In the context of TLS, briefly how the certificates are managed?

You can upload a standard certificate into the PBX. Currently we support only one certificate for one domain that might change in further releases. We do not check the certificates of the clients, as usually they use self-signed certificates (DHCP).

5.2.6 How can I provision phones in a secure way?

The provisioning phase is a very critical phase, because during that time passwords have to be put into the phones and it must be made sure that no one captures the password on the network. Using a secure connection for the provisioning solves the problem of keeping the password secure, but it requires that the phone authenticates itself (otherwise any client can retrieve the password).

There are three methods for provisioning secure passwords:

- The PBX does not provision passwords with the plug and play mechanism. While you can use the plug and play for all other parameters, you must put the passwords either through a secure web server connection on the phone or you manually enter the password in the user interface of the phone.
- The PBX provisions the password only once. All other requests for the configuration file will skip the password information. The domain administrator may set or reset the flag for an extension manually if a new phone needs to be provisioned or if a specific extension should be blocked from automatic provisioning.
- The PBX always provisions the password. This most is very convenient, but not very secure.

5.2.7 What is (in terms of technology) "security end-to-end"?

That is a security policy enforcement triggered by the use of a "sips" URI. If the phone sends this scheme, the PBX will establish a call on the other side of the B2BUA only if the other side is secure. Trunks can be marked as exception, as

practically there are only very few secure PSTN gateways able to support TLS/SRTP. Please note that this features must be specifically enabled.

5.3 Overall System Settings

5.3.1 General

The "Audio Language", the "Tones", the "Web Language" and the "Timezone" determine which language is being used for the speech, the tones and the web interface. For more information, see Localization.

General:	
Audio Language:	German ▾
Tones:	English ▾
Web Language:	English ▾
Timezone:	Central Europe ▾

5.3.2 Administrator Login

It is very important that the login as system administrator is protected. Therefore, you should set a reasonable safe password for the administrator login. The password is stored in a hashed format, so that there is no way of reading the password from the Global Configuration File.

By default, the username is "admin" and there is no password.

Adminstrator Login:	
Username:	admin
Password:	●●●●●●●●
Password (repeat):	●●●●●●●●

5.3.3 Appearance

The "Default CDR listing" size tells the system how many CDR records to display on the web interface. This setting should avoid that the user gets too many CDR on the display at a time.

The "Keep CDR Duration" setting defines how long the CDR are kept in the database. By default, this setting is 14 days. The duration is expressed in time unit. A time unit may seconds (put a 's' behind the number), minutes (put an 'm' behind the number), hours (put a 'h' behind the number) or days (put a 'd' behind the number). An example would be "10d", meaning that the CDR are kept for ten days.

The "SOAP Trusted IP" and the "SOAP CDR URL" are only available if the license key contains a SOAP flag. See SOAP for more information.

Most SIP phones do not have a recording button. In order to have the recording feature also available for those devices, you may define DTMF keys that start and stop recording. The keys must be one character and can be 0-9, * and #. Recording is triggered only on connected calls. Please be aware that the other side may hear the tone and that this feature might have side effects on other features, for example when you are calling an external mailbox and use the keys for navigating. The "Recording Location" defines where calls are being recorded. For more information about Recording, see the page Recording.

Appearance:	
Default CDR listing size:	<input type="text" value="30"/>
Keep CDR Duration (smhd):	<input type="text" value="14d"/>
SOAP Trusted IP:	<input type="text" value="localhost"/>
SOAP CDR URL:	<input type="text"/>
Record On Key (e.g. *):	<input type="text"/>
Record Off Key (e.g. #):	<input type="text"/>
Record Location:	<input type="text" value="\$r/rec-\$d-\$t-\$i-\$u-\$n.wav"/>

5.3.4 Performance

The "Maximum Number of Calls" setting defines how many calls the system allows at the same time. Because every call takes a certain portion of the available CPU, allowing too many calls will affect the quality of all ongoing calls. By limiting the number of calls on the CPU, you can reject calls that would otherwise potentially degrade the overall performance. On modern PC, you may have hundred or more calls running on one computer; however on embedded system you will probably have much less CPU power and the probability that you are running out of CPU power is much higher.

The "Maximum Duration of Call Recording" sets an upper limit to call recordings. This setting is important because recording files might become very large and can cause problems with the system performance. There is another setting that limits the recording of a mailbox message, which is a domain setting.

In a SIP environment, the registrar determines how long a user agent may be registered. Short registration times have a negative impact on the performance, but make sure that the user agents stabilize quickly after they lost connection to the PBX. The "Minimum Registration Time" and the "Maximum Registration Time"

settings are used to define the lower and upper limit for the registration time. Typical values are in the range of a few minutes up to several hours. The settings use seconds as the unit.

If the registering user agent is behind NAT, the PBX uses the settings "UDP NAT Refresh" and "TCP/TLS NAT Refresh". The PBX registers agents that use the UDP transport layer only for a short time, so that the user agents will reregister quickly and keep the NAT bindings alive this way. Typically the settings for UDP should be in the range from 15 to 45 seconds, while TCP/TLS connection don't need to refresh the bindings so often, a value of a few minutes are ok in most situations.

The "Maximum call duration" settings set the upper limit for the call duration. By default the setting is two hours, but you might make it longer if you have long phone calls. This setting is good to keep your call list clean, for example if one mailbox talks to another mailbox.

Performance:	
Maximum Number of Calls:	<input type="text"/>
Maximum Duration of Call Recording (s):	<input type="text" value="600"/>
Minimum Registration Time:	<input type="text" value="30"/>
Maximum Registration Time:	<input type="text" value="60"/>
UDP NAT Refresh:	<input type="text" value="30"/>
TCP/TLS NAT Refresh:	<input type="text" value="60"/>
Maximum call duration:	<input type="text" value="7200"/>

5.3.5 SIP Settings

SIP specifies for certain headers a short form. Short headers have the advantage to save some space in the messages, which reduce the overall probability that you run into problems with maximum message size in UDP. Although it is very simple to support this, some devices are not able to deal with the short headers. Therefore, the PBX offers both short and long headers. In order to maximize interoperability, the default value for Use Short SIP Headers is long; if you are running into UDP packet fragmentation problems (message size above 1492 bytes), you should switch to the short header form.

SIP also has it's own multicast group. Usually a SIP device knows where to send the requests; however during boot-up and configuration, a user-agent might want to locate the PBX with a multicast request. Therefore, the PBX offers the setting Listen to sip.mcast.net. If this setting is turned on and you are using user-agents with the multicast detection feature, you can just plug the devices into the

network and they will get their configuration information automatically.

In hosted environments, the service provider might want to set the trunks up and hide this feature from his customers. If Allow domain admin to change trunks is set to "no", then the domain administrators can see their trunks only in the dial plan, but are not able to make changes to the trunks.

When the PBX starts a call, that same call may come back to the PBX, creating a loop. This is a dangerous situation, because it might initiate the same call again and again, ending up in many calls that take a lot of resources. Therefore, the PBX must detect such a loop. In environments where an external SIP proxy routes the call from one PBX domain to another, a simple loop back detection based on the call-id is too pessimistic. Therefore, in such environments you might want to allow such calls and turn the loop back detection off.

When a user presses a key on the telephone, the PBX must be able to understand that key press. In telephony system, this mechanism is typically called DTMF (see <http://en.wikipedia.org/wiki/DTMF>). In VoIP, DTMF should usually be sent via the out-of-band method (RFC2833), which makes it easy and failsafe for the PBX to detect those tones. However, there are sometime devices, which are not supporting this method. In this case, the PBX must decode and analyze the media stream and perform this detection. This is erroneous and costs additional CPU performance. It is strongly recommended not to use this feature and to replace devices which do not support out-of-band with devices that do.

In environments where the service provider controls the PBX from a centralized location, the setting "Remote SIP management" is used to allow the provider to send commands to the PBX (for example, for re-reading the configuration). By default this setting is off, but if you are using such an environment this setting needs to be turned on.

SIP Settings:

Use Short SIP Headers:	<input type="radio"/> Short <input checked="" type="radio"/> Long
Listen to sip.mcast.net:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Allow domain admin to change trunks:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Loopback detection:	<input checked="" type="radio"/> On <input type="radio"/> Off
Inband DTMF detection:	<input type="radio"/> On <input checked="" type="radio"/> Off
Remote SIP management	<input type="radio"/> On <input checked="" type="radio"/> Off

5.4 Product Licensing

The PBX offers several options for product licensing.

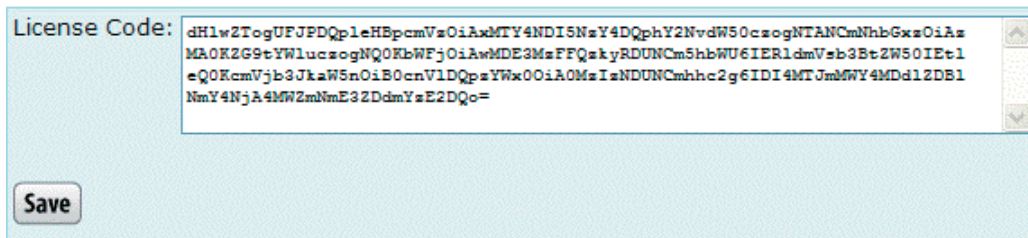
5.4.1 Installing a License

After you received the license code, just copy the license code into the "License Code" field and hit the "Save" button.

License

Please enter your license code here.

You can get licenses from the [online](#) store. On this link you will also be able to receive demo license codes.



The screenshot shows a web form with a text input field labeled "License Code:". The field contains a long alphanumeric string: dH1w2TogUFJPDQp1eHBpcmVzOiAxMTY4NDI5NzY4DQphY2NvdW50czogNTANCmNhbGxzOiAxMAOKZG9tYW1uc2ogNQ0KbWFjOiAwMDE3MzFFQzkyRDUNCm5hbWU6IERldmVsb3BtZW50IEt1eQ0KcmVjb3JkaW5nOiB0cnVldQpsYWx0OiA0MzIzNDUNCmhhc2g6IDI4MTJmMjY4MDdlZDBlNmY4NjA4MjZmNmE3ZDdmYsE2DQo=. Below the input field is a "Save" button.

5.4.2 Licenses Policy

Licenses can be permanent or temporarily. If you buy a license, they are typically permanent; for demonstration licenses, we usually provide temporary keys.

It is pbxnsip's license policy to bind licenses to the addresses of a specific host. Therefore, you need to provide us the address of the host that you want to use with the PBX.

- MAC addresses are generally used to uniquely identify a computer. For CPE installations, MAC addresses must be used.
- IP addresses are used in hosted environments where it is difficult to license specific MAC addresses (server farms and redundancy).

5.4.3 Features

The license generator can have the following parameters:

- calls <number>: Limit the number of calls. A call can consist of several legs, for example during hunt group forking. The number of calls may be limited by the performance check. The default is no limit.
- accounts <number>: Limit the number of accounts. A account is anything that shows up in the Accounts/Show list (including CO-lines).
- domains <number>: Limit the number of domains. If not set, unlimited.
- extensions <number>: Limit the number of extensions. If not set, unlimited.
- attendants <number>: Limit the number of attendants. If not set, unlimited.
- callingcards <number>: Limit the number of callingcards. If not set, unlimited.

- hunts <number>: Limit the number of hunts. If not set, unlimited.
- hoots <number>: Limit the number of paging groups. If not set, unlimited.
- srvflags <number>: Limit the number of service flags. If not set, unlimited.
- ivrnodes <number>: Limit the number of IVR nodes. If not set, unlimited.
- acds <number>: Limit the number of agent groups. If not set, unlimited.
- conferences <number>: Limit the number of conferences. If not set, unlimited.
- colines <number>: Limit the number of CO-lines. If not set, unlimited.
- trunks <number>: Limit the number of trunks. If not set, unlimited.
- soap <bool>: Specify if SOAP is allowed (default false).
- barge <bool>: Specify if call barge in/teach in/listening is allowed (default false).
- secure <bool>: Allow sips calls (default false).
- cdr <bool>: Allow sending of CDR via SOAP (default false).
- lowrate <bool>: Enable the use of the lowrate codec (default false).
- recording <bool>: Enable the use of the recording feature (default false).
- name <text>: A describing name for this license. This name is shown in the status web page.
- expires <time>: The date in number of seconds from 1970.

The key contains a hash over the features and the private key of the PBX key generator for cryptographic security of the key. The key is based64-encoded for easier transportation during the licensing process.

Technically, all features can be controlled seperately. In most cases, licenses will be offered in a package that contains a predefined feature set.

5.5 Port Setup

On this Ports web page you can control which networking resources the PBX utilizes to communicate with the outside IP world.

When specifying ports, you can list the ports that you may bind to. You may either just specify a port number or you may explicitly specify the IP address and the port (separated by a colon, for example "192.168.1.2:8080"). In general, you may bind to more than one socket. The addresses must be separated by spaces. If you don't want to use the service, leave the field empty. If you change the port binding, you need to restart the PBX service.

5.5.1 HTTP

The http and https ports are used for the communication between the build-in web server and the web browser. The http port is used for insecure, but lightweight communication; the https port is used for secure, but a little bit more expensive communication.

By default, the http port is 80, the https port is 443. If you are running another service on your host or you want to gain some additional security, you may change these ports to any other available port.

If you cannot reach the system on any port, please use the netstat command to locate the ports that have been allocated by the system (see the operating system documentation how to use this program). If it all does not help, you must either reinstall the system or change the settings ip_http_port and ip_https_port in the Global Settings File.

HTTP:	
HTTP Port:	<input type="text" value="80"/>
HTTPS Port:	<input type="text" value="443"/>

5.5.2 SIP

The SIP ports are used for insecure and secure SIP communication. By default, the system chooses port 5060 for sip and 5061 for sips. The PBX opens a UDP port and a TCP server port for the insecure communication and a TCP port for the secure communication.

If you are to set your DNS records up, you should set three records (assuming that you are operating the domain "test.com"):

- _sip._udp.test.com must point to sip port (UDP)
- _sip._tcp.test.com must point to the sip port (TCP)
- _sips._tcp.test.com must point to the sips port (TLS)

You can repeat the setup for every domain that you want to operate on the system.

SIP:	
SIP UDP Ports:	<input type="text" value="5060"/>
SIP TCP Ports:	<input type="text" value="5060"/>
SIP TLS Ports:	<input type="text" value="5061"/>

5.5.3 RTP

The RTP ports are used for sending and receiving media. You must specify a reasonable port range so that you have enough ports for all open calls.

Most user agents send RTP media data from the same port where they

expect to receive data. This is useful when a user agent sends media from behind NAT. The PBX can use this mechanism to establish a two way media path, even if the user agent is not able to determine its public IP address for media and is behind NAT.

Some user agents use different ports for sending and receiving. Although they will not be able to operate behind NAT, they are within the scope of the IETF standards. To be able to be compatible with these devices, the PBX has flag called "Follow RTP". By default, this flag is set to "on". If you have trouble with devices that use different ports for sending and receiving, try to turn this flag off. Please note that some of the troublesome devices also have a flag to turn the usage of different ports off.

Please note that you can control this behavior also on trunk level. If only a specific trunk has this problem, you should use this setting only on the trunk level.

RTP:	
Port Range Start:	<input type="text" value="49152"/>
Port Range End:	<input type="text" value="64512"/>
Follow RTP:	<input checked="" type="radio"/> on <input type="radio"/> off

5.5.4 SNMP

The SNMP port setting defines on which port the PBX will listen for SNMP requests. By default, this port is on port 161.

The SNMP trusted addresses lists the IP addresses that may send SNMP requests. If this setting is empty, the PBX will not accept any SNMP requests. Whenever a request is being rejected, the PBX writes a log message.

For more details, see the SNMP chapter.

SNMP:	
SNMP Port:	<input type="text" value="161"/>
SNMP Trusted Addresses:	<input type="text"/>

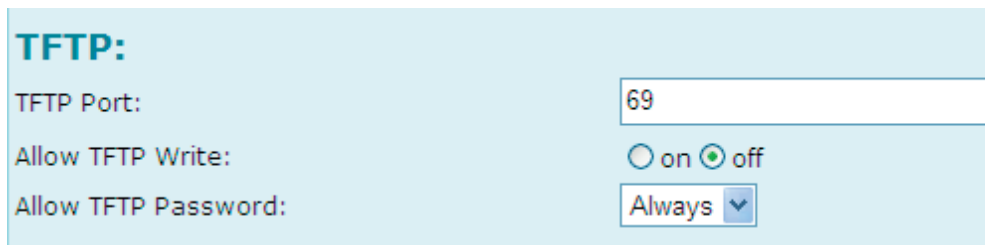
5.5.5 TFTP

The TFTP ports are used for provisioning purposes. Many SIP devices use tftp for automatic configuration. See Automatic Provisioning for more details on this topic. This port is on port 69 by default.

Some devices write log files using tftp. You may enable this with the "Allow TFTP Write" flag. Please notice that this feature makes it possible that users may write files that affect other devices and this may introduce system instability and security concerns. We recommend using this feature only for troubleshooting, if necessary. The uploaded file can also be seen in the log file.

The "Allow TFTP Password" setting can have those values (see also SIP Security and Prepare an Extension for Plug and Play):

- "Always" means that the PBX will always place the passwords into the provisioning files.
- "Once" means that the PBX first checks if the password flag for the respective account is already set, and if not it sends the password; then sets the flag.
- "Never" means that the PBX does not provision passwords.



The screenshot shows a configuration panel for TFTP. It has a light blue background and a title 'TFTP:'. Below the title are three settings: 'TFTP Port:' with a text input field containing '69'; 'Allow TFTP Write:' with two radio buttons, 'on' and 'off', where 'off' is selected; and 'Allow TFTP Password:' with a dropdown menu showing 'Always'.

5.5.6 Call Managing Port

The call managing port is able to provide external tools with information about incoming calls and allows external tools to start calls. The port uses a proprietary interface. If you leave this setting empty the PBX will not open the port. Currently, the tool from Calling Circles uses this port.

5.6 SNMP

5.6.1 Purpose

The simple network management protocol (SNMP) is a widely used protocol for checking what's going on in your network. When you run the PBX, you probably also want to see statistics about the usage and get alarms when something goes wrong.

There are many tools available for SNMP. For example, you can use the Linux command line argument `snmpget` or you can use the Windows commercial tool PRTG Traffic Grapher. Depending on the feature set, you may get SMS or email when something goes wrong. You can use those tools also to monitor other devices in your network, for example SIP phones.

The PBX does not send traps, it only supports GET in SNMP version 1. Though this is very simple, it is supported by all tools. Sending traps has only little value, as the process monitors itself and for example cannot send a trap in the case of a fatal event.

5.6.2 Setup

The setup of SNMP on the PBX side is very simple. Essentially, you have to perform two steps:

Select the port on which the SNMP server should listen. By default, this would be port 161, but on a host that runs other SNMP services as well you might want to choose another port.

Tell the PBX from which addresses to accept SNMP requests. You find the setting "SNMP Trusted IP Addresses" for this. Enter the IP addresses (separated by a space) or the IP address range here. The PBX will accept requests only from these addresses. The format is in the IP Address List format.

The setup of your SNMP tools varies from tool to tool. Because the PBX does not offer a standard set of values (such as CPU temperature, disk space etc.), the setup is a little bit more difficult than the setup of a standard sensor.

5.6.3 Available Object Identifiers

A readable parameter is described by its object identifier (OID). Please enter the OID in your tool and select appropriate names for them. Also make sure that the IP address of the host running the SNMP tool matches the setup that you gave the PBX in the "SNMP Trusted IP Addresses" setting. The PBX does not support "snmpwalk" or other tools that automatically describe the abilities of the PBX. You must enter these settings manually.

The following table describes the available OID. An absolute value describes the current state on the PBX, the value might go up and down. Relative values only go up and accumulate the values.

OID	Description	Absolute	Unit
1.3.6.1.4.1.25060.1.1	Call Objects	Yes	Calls
1.3.6.1.4.1.25060.1.2	Registrations	Yes	Registrations
1.3.6.1.4.1.25060.1.3	Messages	Yes	Minutes
1.3.6.1.4.1.25060.1.4	Call Attempts	No	Calls
1.3.6.1.4.1.25060.1.5	Successful Calls	No	Calls
1.3.6.1.4.1.25060.1.6	Media CPU load	Yes	Value 0..100

Please note that the OID was changed from 1.3.6.1.2.1.2.1.x to 1.3.6.1.4.1.25060.1.x in version 1.5.

The "Call Objects" just shows the number of call objects that have been allocated inside the PBX. Note that usually there are at least two call objects for a regular call, and during call forking you might have even more. This object will give you a good overview on the internal resource usage of the PBX.

The "Registrations" object shows how many extensions are actively

registered with the PBX. This object gives you a good overview on how many active users the system has.

The "Messages" object shows you how many voicemail messages the system currently has stored. Note that when you do Email-forwarding, the messages are not stored on the PBX.

The "Call Attempts" object is useful to measure the Busy Hour Call Attempts (BHCA) number. This number is useful when you want to see where the limits of your system are. The BHCA number is an important performance number of traditional PBX. Feel free to compare the BHCA value of your modern CPU to the value of an old-style hardware PBX.

The "Successful Calls" object is similar to the "Call Attempts", but it measures the number of successful calls. The number is increased when the call terminates. The number can be used to determine the busy hour call performance of the system. Please note that on this software PBX, not only the call establishment takes resources. The call traffic itself also causes significant traffic, especially when the CPU has to do codec translation.

5.6.4 Example

If you use `snmpget`, you can get the status of the PBX with a command like this:

```
# snmpget -v 1 -c public 192.168.1.103 .1.3.6.1.4.1.25060.1.3
SNMPv2-SMI::enterprises.25060.1.3 = INTEGER: 4
```

5.6.5 Log Messages

If you receive SNMP: Received unknown object identifier the SNMP tool tries to get an object identifier that does not exist. Some tools try various object identifiers by default, which is not a reason for concern.

5.7 Prepare an Extension for Plug and Play

5.7.1 Binding to a MAC address

Whenever you want to use plug and play for an extension, you need to tell the PBX about that.

The PBX identifies a device by its MAC address (see for example http://en.wikipedia.org/wiki/MAC_address). When a device supports plug and play, it includes its MAC address in the request for configuration information. The PBX uses three ways to find the extension(s) that match this MAC address:

- If you explicitly specify a MAC address for an extension, then the PBX will associate that extension with that device. You can specify only one MAC address per extension. However, you can use the MAC address in more than one extension. Then the PBX will try to assign more than one extension to that device. It depends on the device if it supports more than one registration.

- In many cases it is inconvenient to enter the MAC addresses for devices. Therefore, the PBX accepts two wildcards for the provisioning. The star symbol ('*') is used for the permanent assignment mode. The PBX will wait until a user agent requests a configuration from the PBX. If that user agent has no configuration assigned to a specific account, it will search for permanent assignments and remember the MAC address of this user agent for this account. The next time when the same user agent boots up it will receive the same extension number and no other user agents will receive that extension number.
- The other mode is temporarily assignment. This mode is indicated by a question mark symbol ('?'). The PBX will search a "free parking slot". An extension is available for plug and play if no other user agent is registered to that extension. That means it will not remember that the user agents was assigned with the extension. The next time when the user agent boots up it might receive another extension number.

5.7.2 Password Provisioning

For complete plug and play, it is desirable to provide the passwords along with the other configuration data. However, this possibility may open a security hole. The PBX has practically not way to authenticate the device. For example, if another user in the network requests the same configuration information, the PBX would provide the same configuration again. The MAC address as key to the configuration data is a very weak protection – many devices use the MAC address in regular SIP requests.

Therefore, the PBX offers three modes:

- "Always" means that the PBX will always place the passwords into the provisioning files. That means everyone who know the MAC address in the network can get the configuration data for a device, including the password. This mode is acceptable in trusted environment, for example small offices or home offices.
- "Once" means that the PBX first checks if the password flag for the respective account is already set, and if not it sends the password; then sets the flag. This mode is useful, when the administrator sets the devices and has control over the time when the device is being provisioned. If the device uses https as protocol for transporting the configuration data, this mechanism is secure.
- "Never" means that the PBX does not provision passwords. This is obviously a safe mode. If the user has the possibility to enter the password on the device (e.g. on the keyboard), this will give the system a good security, while still being reasonable simple for end users.

If the administrator uses the "once" mode and the provisioning of a password fails, this is an indication that someone else retrieved the password by accident or by purpose. In this case the administrator should reset the flag for the extension and choose a new password.

5.7.3 Other relevant settings

There are some more relevant settings that you should consider when performing plug and play:

- The time zone is usually automatically provisioned on the devices. Make sure that you have chosen the right time zone for the system, domain or the extension.
- The dial plan can also be provisioned for some devices. Especially for customers in the North American Numbering Plan can benefit from this feature, as they (usually) don't have press the "Send" button on the phone to start calls.
- Some profiles also provision star codes. For example, the code to retrieve the voicemail can be sent to the device. Make sure that the codes are set up correctly.
- The address book can also be provisioned for some devices. If you want to provide a domain or extension address book, you should set this up before starting the phones. If you do changes in the address book, you need to restart the devices so that they pick the changes up. Some devices support real-time access to the PBX, where a restart is not necessary.
- Some devices support provisioning of the busy lamp field (BLF). You can monitor other extensions, but you can also monitor the status of the hunt group, the agent groups, the CO-lines, conferences and other account types. In order to do this, you need to specify the "List of extensions to watch" in the user mode for an extension. Check the Dialog Permissions state of the account that you want to watch to make sure that the PBX allows the subscription.
- The PBX also supports the provisioning of the number of lines for an extension. Some phones use this information for defining the layout of the buttons.

5.8 Log Setup

5.8.1 General Logging

When you install the system, you want to see how it works and how the PBX interprets the input to the system. Logging is a powerful mechanism to track the activity of the system.

For this purpose, the PBX keeps a list of log messages in memory and if you enter a filename it writes a copy of the log messages to the file system.

The Log Level determines which log messages are put into the log. The range is between 0 and 9. If you select level 0 you will see only the most important messages, if you select level 9 you will see all available log messages of the system. Please note that choosing log level 9 creates additional load for the system and may create huge log files.

The Log Length determines the length of the internal log message buffer. This buffer is used to show the log messages in the web interface (see below).

If you set a Log Filename, the system will write the log messages to the filename which you provide. If you put a dollar sign into the log filename, the system will replace the dollar sign with the current day. This will make sure that the log files don't get too big over time. Please don't forget to delete old log files from time to time, so that your file system does not get overloaded with too much logging information.

One of the first log messages that you will see is the working directory. If the Log Filename does not contain a path, the system will write the log file into that directory. You can specify the directory during the installation process.

Warning! Don't forget to lower the log level once the system is running. Especially when you write the log messages into a file, you will sooner or later get a hard disk full error, which is a quite severe situation because the PBX will then not be able to save runtime data.

General Logging:
Log Level (0-9):
Log Length:
Log Filename:

5.8.2 Specific Events

You can enable or disable logging on a subsystem level. The following subsystems are available:

Log general events: These events are of general interest, for example information about the working directory.

- Log SIP events: Events in this module relate to the SIP traffic of the PBX.
- Log media events: The PBX reports events about media processing, for example a one-way audio RTP timeout.
- Log IVR events: This module logs events about processing user input, for example in the auto attendant or the mailbox.
- Log email events: If you want to troubleshoot the email server interaction, you should turn this module on.
- Log http events: This flag controls if events in the internal http server should be logged.
- Log registration events: When a device registers or deregisters, it appears in this module.
- Log SNMP events: SNMP events occur when an external SNMP agent requests information from the PBX.
- Log trunk events: Log events that are related to the trunks, for example when a

trunk registers the first time.

- Log SOAP events: This subsystem deals with SOAP input and output.
- Log TFTP events: In this module you will find events that have to do with the built-in tftp server and plug and play-related information.

Specific Events:

Log general events:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Log SIP events:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Log media events:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Log IVR events:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Log email events:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Log http events:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Log registration events:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Log SNMP events:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Log trunk events:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Log SOAP events:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Log TFTP events:	<input checked="" type="radio"/> Yes <input type="radio"/> No

5.8.3 SIP Logging

When the PBX receives or sends a SIP packet, it determines if the packet will be logged and which log level this event will have.

- REGISTER packets deal with the registration of extensions or trunks. If you are not interested in the registration traffic, set this setting to "off".
- SUBSCRIBE/NOTIFY deals with message waiting indications and LED state and other used subscriptions.
- OPTIONS are sometimes used to keep the SIP connection alive. In this case you will see a lot of those requests.
- All other packets usually belong to an ongoing call (e.g. INVITE, CANCEL, ACK, BYE).

The watch list filters the SIP packets by it's IP address. Just list the IP addresses you are interested in the "Watch List (IP)" field (you may use subnet mask) and define the log level in the "Watch List Log Level". This feature is useful when you have a specific device that you want to watch in the PBX's log.

SIP Logging:

Log REGISTER: Yes No

Log SUBSCRIBE/NOTIFY: Yes No

Log OPTIONS: Yes No

Log Other Messages: Yes No

Log Watch List (IP):

Log Watch List:

5.8.4 Email

The PBX is able to send notifications for certain events. Currently, the only event is the daily report of the system performance. This email is sent daily after midnight and it contains a chart about the CPU usage of the last day.

In order to use this feature, you need to provide the "From" address that is used for sending the email. The "Account" and "Password" is used for SMTP authentication purposes, the SMTP server will be used for sending the email. The recipients of the performance email must be separated with a semicolon.

Email:

"From" Address (e.g. "PBX" <pbx@domain.com>)

5.9 Loading of a Certificate

5.9.1 Purpose

Certificates are used to indicate your communication partner that you are really the one that you claim to be. This is done using a third party that certifies

your identity and issues you a certificate. The certificate comes for a domain name. Usually those certificates are used for web services; however the same certificates can also be used for SIP services.

By using a certificate you defend your installation against DNS redirection attacks. An attacker might get control over a DNS server (which you don't operate) and redirect all requests to his server. He then might be able to present the same certificate that you have, but he does not have the private key that you used when you requested the certificate from the trusted third party. Therefore, he will not be able to establish secure communication. This way the user agent can check if the host that he contacted is really the desired host and deny the connection if the public and the private keys do not match.

You can provide only one key to the PBX. That means for secure communication, you can operate only one domain in a secure way.

In order to provide the key, just enter the ASCII string that you received from the trusted party, copy it into the text field and push the "Save" button. The PBX will then present this certificate to http and sip connection that require secure communications.

5.9.2 Format

The format of the certificate must be base64-encoded. You must include the private key and the certificate in the upload. Please note that uploading the private key this way might be intercepted by an intruder. You can minimize this risk by using the localhost address from the local machine.



5.10 Music on Hold

5.10.1 Purpose

"Music on Hold" (MOH) is used in several places. The name originally comes from the music that is played when an extension put a caller on hold to avoid silence in the line. For more information, see for example http://en.wikipedia.org/wiki/Music_on_hold.

The PBX uses MOH when a call is being put on hold and when a caller is waiting in an agent group. There can be several sources for music on hold; these sources can be used in parallel and can be used in different locations. Because these sources are system-wide available, they are part of the administrator settings. The music on hold can be selected on domain level. See the domain mode for more information.

5.10.2 Files

The PBX can use one or more files for MOH. These files are read by the PBX on demand and played in an endless loop mode.

The files must be in 8 kHz sampling frequency and they should be in 16 bit per sample signed format. The format must be mono WAV. You may also use other formats (u-law and GSM), but these formats will have less audio quality and require more CPU performance.

The files are loaded only once. However, you should be careful, because long files will be read into memory; long files can easily take a lot of memory. As a rule of thumb, every minute of the file will take about one MB of memory space.

5.10.3 Audio Input

In Windows, the PBX supports additionally the reading from the audio input jack. This is a very convenient way to connect a CD, MP3 player or a radio to the PBX. The disadvantage of this method is that you can have only one external music source.

You can also internally loop the audio output of the local computer back to the audio input of the computer. With this trick, you can use any MP3 player running locally to provide a large number of MP3 files. However, we recommend keeping an eye on the memory usage of the MP3 player, as some players have memory leaks and slowly consume the memory of the computer.

5.10.4 RTP Stream

Streaming RTP data becomes a popular way of providing music from external sources. Just like with a telephone conversation, the PBX receives the audio data in a standard RTP stream. There are several external tools available that are able to generate a compliant RTP stream. Because the PBX can have several RTP streams, you can use this method to generate different music on hold sources for the

system.

The RTP stream must use G.711 encoding. There is no SIP signaling involved in this method and the PBX does not send any RTP data back.

5.10.5 Setup

In order to create a new MOH source, you must enter a name for the new source and select the type of the new source. If the type is "File", you need to specify the name of the file. This file must be in the "audio_moh" directory of the PBX (you must manually place the file there).



Name:	<input type="text" value="Classical Music"/>
Type:	<input type="text" value="File"/>
Filename:	<input type="text" value="classic.wav"/>

For the type "RTP Stream" you must specify on which port the PBX should listen for RTP input (for example, "42000"). This port must be available on the system. If you change the setting, you might need to restart the PBX service, so that the change takes effect.

For the type "Wave Input" there is no additional information required.

5.10.6 Editing

If you want to change a setting, you can just click on one of the links shown above the form. The PBX then will fill out the fields with the settings for the respective source. After making changes, you need to press the "Save" button. If you want to delete the source, click on the delete button. If you want to create a new source, you can use the clear button.

Music on Hold Sources

Please specify the available music on hold sources. These sources can be used independently in the domains of the system.

Available Sources

[Classical Music](#)

[File moh.wav](#)

[Wave Input](#)

Name:	<input type="text" value="Classical Music"/>
Type:	<input type="text" value="RTP Stream"/>
Port Number:	<input type="text" value="6000"/>
<input type="button" value="Save"/> <input type="button" value="Delete"/> <input type="button" value="Clear"/>	

5.11 Changing the Appearance

5.11.1 Motivation

Many users of the pbxnsip PBX would like to change the view of the PBX in such a way, that their company logo and name is used on the web interface and the SIP messaging of the PBX.

In order to address this problem, the PBX has a web page where several customization settings can be set. By default, this page is invisible. By performing some special steps, this page can be unlocked, so that the necessary changes can be made from the web interface.

Please note that pbxnsip does not waive any copyrights on the product by providing this mechanism.

Appearance:

Web Page Width:	<input type="text" value="780"/>
Login Text:	<input type="text" value="pbxnsip"/>
Footer Message:	<input type="text" value="Copyright &copy; 2005-2007 pb"/>
Web Link:	<input type="text" value="http://www.pbxnsip.com"/>
Logo Link:	<input type="text" value="img/main_logo.gif"/>
User-Agent String:	<input type="text" value="pbxnsip-PBX"/>
Lock Appearance:	<input checked="" type="radio"/> Locked <input type="radio"/> Unlocked

5.11.2 Unlocking the web page

The web page is locked when the setting "oem_lock" in the Global Configuration File is set to true. After a fresh installation this is the default. In order to unlock the web page, you need to stop the PBX, manually change the value to "false" and then restart the PBX.

5.11.3 Changing the Appearance

After unlocking the page, you need to log in as administrator and go to the settings/appearance web page. On this page you will see the following settings:

Web Page Width ("web_width"): This setting controls the default width of a web page. 780 is a reasonable value, but depending on the customers PC equipment you might want to make it smaller or larger.

Login Text ("app_login_text"): This text is displayed

Footer Message ("app_footer"): This text is displayed on the bottom of every web page as a copyright hint. It is followed by the text "All rights reserved. See the license agreement for more information".

Web Link ("app_link"): This link is inserted in several places of the web page. For example, the online manual link is based on this link. You must have the images for edges of the design relative to this path. The easiest way to get this working is to try a link and then use the web browser to identify the path to the missing images.

Logo Link ("app_logo"): This is the relative link to the logo image on the top left of the menu navigation bar. The size of this image must be 132x33 pixels. The logo link is the link relative to the http root. You might consider using an absolute

path (including the http scheme). A template image is available on the online Wiki.

User-Agent String ("app_user_agent"): This string is used when creating SIP messages.

When changing the settings, those settings should take effect immediately. You might have to invalidate the browser cache by pushing the reload button on the web browser. You can continue changing the settings until you are confident with the result. Then you can lock the page by changing the radio button to locked state and saving the web page.

5.11.4 Providing your own content

You can put your own content into the html directory. That directory does not exist in the beginning; you must create it first in the working directory of the PBX (where other directories like users, trunks, etc are). Within that directory, you may create another directory img, and in that directory you may put the images that are used. Regarding the content, the best way is to save a page (including the referenced images) and see what images and files are being loaded. If you are interested in a complete customization, you need to contact pbxnsip.

5.12 Domains

Before you can start to use the PBX, you must set up at least one domain. By default, the PBX will create a domain called "localhost" for you.

A domain is like an email domain. It groups a number of users. These users are able to call each other without going through a trunk. Additional features like call pickup can be configured and might have additional restrictions. If you can, you should set up your DNS accordingly, so that users from other domains can find the group by standard DNS name resolution.

You may have several names for a domain (domain alias). One of these names will be the "primary" (canonical) name for the domain. The PBX will use that name whenever it has to generate a name for the domain.

In the profession version of the product, domains may have a limited number of accounts. This feature is necessary for hosted environments, where you want to make sure that customers are not using more accounts than you have sold to them.

The domain that has the name "localhost" (or an alias name "localhost") has a special function. It will match all requests that cannot be matched to a domain name in the domain list. This makes it possible to run the PBX on changing IP addresses without changing the name of the domain and significantly simplifies the setup of the PBX in environments where only one domain is needed.

Domain names may be IP version 4 addresses. Especially when you cannot change DNS, you might want to assign such a name to a domain. However, you must be sure that the host is always running on that IP address, if you are assigning IP addresses by DHCP you have to be careful with this method.

You may mix IPv4 names with DNS addresses. You may also later rename the domain names and reassign the primary domain name.

5.12.1 Domain Listing

To see which domains are available on the system, click on the "Show List" link in the navigation bar.

The web interface lists the available primary and alias domain names and shows the primary domain name in the second column. If you click on the link behind the primary domain name, you will be redirected to the domain context. The Users column shows how many accounts (extensions, hunt groups, etc) are used in the domain. If you click on the edit button, you may change the primary and alias names of the domain as well as other features of the domain.

If you click on the delete button, you delete the alias for the domain. If the name was the primary name, the system will pick randomly another primary name for the domain. If you delete the last name of the domain, the system will ultimately delete the domain and the data that was associated with it.

Current Domains

This list shows the currently available domains on this system. Please note that setting up the domains on this system does not mean that you automatically set up the necessary DNS records. By clicking on the domain link button, you will move into domain mode. Please be careful clicking the delete button, because all domain data will be lost.

Alias	Domain	Users	Edit	Delete
domain1.com	domain1.com	25		
domain2.com	domain2.com	0		
sip.domain2.com	domain2.com	0		

5.12.2 Create a Domain

To create a new domain, you must choose a Primary Name for the domain. You may pick additional alias names and enter them, separated by spaces, into the Alias Names field.

Domain Information:

Primary Name:	<input type="text" value="domain2.com"/>
Alias Names:	<input type="text" value="sip.domain2.com"/>
<input type="button" value="Create"/>	

5.12.3 Edit a Domain

You may specify how many accounts a domain may have. This feature is important if you rent a piece of the PBX to your customers, and want to make sure that they stay within their negotiated limit of accounts. The same applies to the setting "Maximum Number of Extensions" and to "Maximum Number of Calls".

Domain Information:

Primary Name:	<input type="text" value="domain2.com"/>
Alias Names:	<input type="text" value="sip.domain2.com"/>
Maximum Number of Accounts:	<input type="text" value="100"/>
Maximum Number of Extensions:	<input type="text" value="70"/>
Maximum Number of Calls:	<input type="text" value="10"/>

5.13 Status

5.13.1 System Status

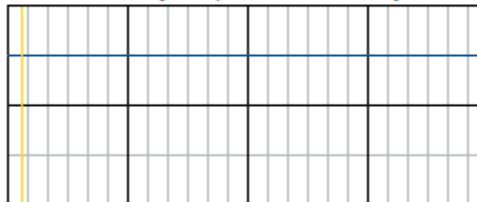
The system status gives you an overview about the state of the PBX.

System Status Overview

Please use the information on this web page when you address the support.

License Status:	Development Key
License Duration:	2 days
Version:	2.0.0.1608 (Win32)
Working Directory:	d:\runtime
IP Addresses:	127.0.0.1 172.20.25.101
MAC Addresses:	001731EC92D5
Calls:	0/0 (CDR: 18)
Uptime:	0 01:38:43 (8MB/2047MB 41%)

Media CPU Usage:



The "License Status" shows the descriptive text of your license. If this field is empty, you do not have a license. The "License Duration" shows you how long the license will last.

The "Version" tell you what version your are running and what operating system.

The "Working Directory" line shows you where the PBX expects the audio and table data. If you want to backup your data, you should copy the data in this directory.

The "IP Addresses" helps you to understand which identities the PBX uses for the outside communication. The PBX first checks on which interface it will send a packet, and then changes it's identity accordingly in the SIP packet. This feature makes it possible to run the PBX on hosts that talk to the public Internet and the private Intranet at the same time without the need for an application layer NAT gateway.

The "MAC Addresses" are used for licensing purposes. The PBX lists the MAC addresses that it could find on this system. Every time that you load the status web page, the system refreshes that table. This is important when you turn adapters on and off (e.g. wireless, VPN).

The "Calls" entry tells you how many successful/unsuccessful calls were made on the system after restart. The CDR number in brackets shows you how many CDR entries the PBX keeps internally for listing purposes. If this number grows too large, you should consider making the Keep CDR Duration shorter.

The "Uptime" line gives you information how long the system is running. The line format is days followed by HH:MM:SS. In Windows, you will also find additional information about the memory usage.

The "Media CPU Usage" field shows you the usage of the CPU over the last 24 hours. The graph shows the ratio between waiting and processing of the media thread of the PBX. This number is a good indication how well the CPU was able to keep the real-time requirements for processing media. The blue line shows the CPU load when new calls are being rejected because of performance problems. The yellow line shows you where the log is currently writing into the graph. The green fields show you the average load (averaged over a period of six minutes), and the blue lines above the green fields show you the peak usage of the CPU (averaged over a period of three seconds).

In the domain mode, you will see only a short version of this page.

5.13.2 Log Access

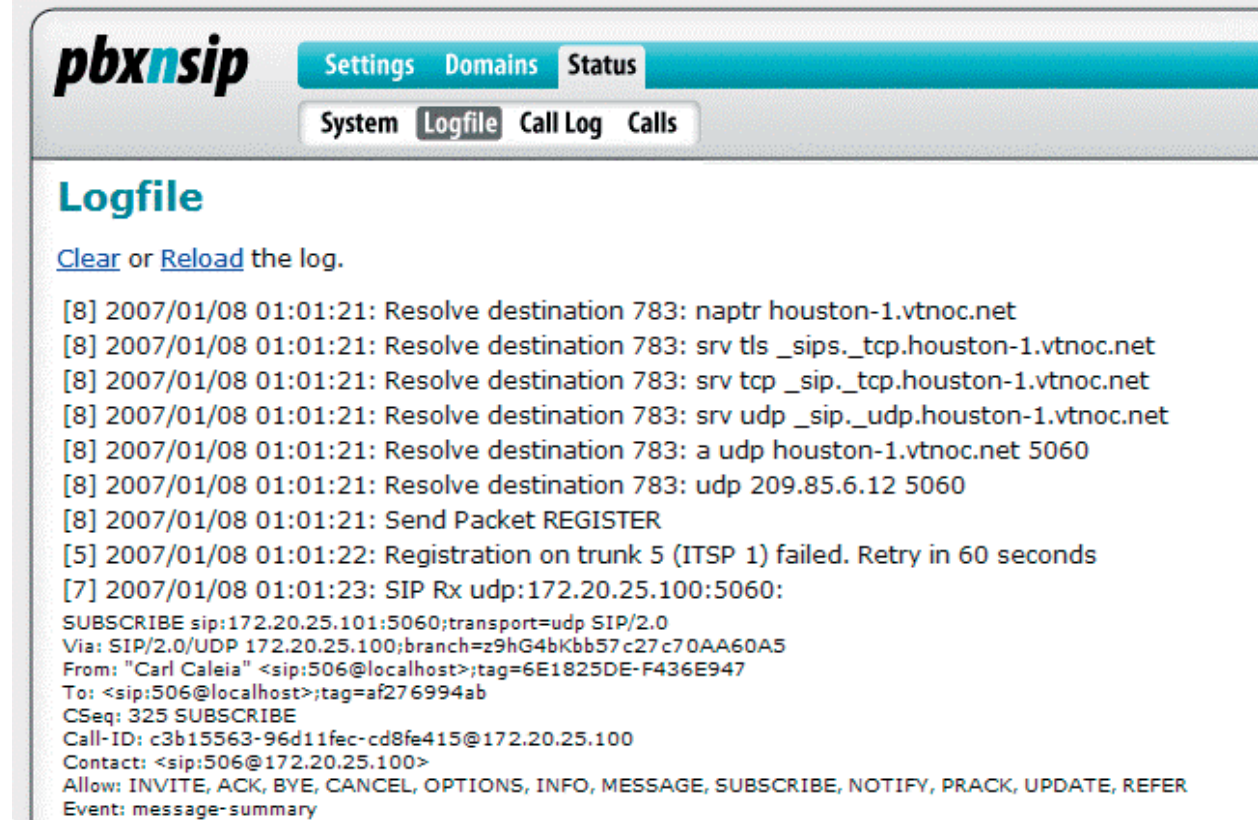
The log file contains a list of the most recent log entries. It is actually not a file; it is an internal list of the last messages. The number of the messages that are shown to you here is a setting that was discussed in the Settings section.

For every log entry, the PBX shows the time when the message was generated and the log level. For SIP packets and in some other situations, the PBX attaches the respective content to the log message, so that the formatting gets easier. If messages are being repeated, the PBX reports just the number of

repetitions.

You may clear or reload the logfile with the links that are presented on the page.

If you want to trace a longer context, you should write the log messages to a file and use a standard text editor to go through the messages. Also, when reporting trouble, try to make a snapshot of the log messages that help to find the problem.



The screenshot shows the pbxnsip web interface. At the top left is the pbxnsip logo. To its right is a navigation bar with tabs for Settings, Domains, and Status. Below this is another row of tabs for System, Logfile, Call Log, and Calls. The Logfile tab is selected. The main content area is titled "Logfile" and contains a link to "Clear or Reload the log." followed by a list of log entries. The entries show SIP registration attempts and a successful SUBSCRIBE message.

```
[8] 2007/01/08 01:01:21: Resolve destination 783: naptr houston-1.vtnoc.net
[8] 2007/01/08 01:01:21: Resolve destination 783: srv tls _sips._tcp.houston-1.vtnoc.net
[8] 2007/01/08 01:01:21: Resolve destination 783: srv tcp _sip._tcp.houston-1.vtnoc.net
[8] 2007/01/08 01:01:21: Resolve destination 783: srv udp _sip._udp.houston-1.vtnoc.net
[8] 2007/01/08 01:01:21: Resolve destination 783: a udp houston-1.vtnoc.net 5060
[8] 2007/01/08 01:01:21: Resolve destination 783: udp 209.85.6.12 5060
[8] 2007/01/08 01:01:21: Send Packet REGISTER
[5] 2007/01/08 01:01:22: Registration on trunk 5 (ITSP 1) failed. Retry in 60 seconds
[7] 2007/01/08 01:01:23: SIP Rx udp:172.20.25.100:5060:
SUBSCRIBE sip:172.20.25.101:5060;transport=udp SIP/2.0
Via: SIP/2.0/UDP 172.20.25.100;branch=z9hG4bKbb57c27c70AA60A5
From: "Carl Caleia" <sip:506@localhost>;tag=6E1825DE-F436E947
To: <sip:506@localhost>;tag=af276994ab
CSeq: 325 SUBSCRIBE
Call-ID: c3b15563-96d11fec-cd8fe415@172.20.25.100
Contact: <sip:506@172.20.25.100>
Allow: INVITE, ACK, BYE, CANCEL, OPTIONS, INFO, MESSAGE, SUBSCRIBE, NOTIFY, PRACK, UPDATE, REFER
Event: message-summary
```

5.13.3 Call Log

Call History

Start	From	To	Duration
2007/01/05 08:37:52	Sharon Houle (520@localhost)	Sharon Houle (520@localhost)	00:48 M
2007/01/05 08:45:33	Paul McCabe (512@localhost)	Christian Stredicke (222@localhost)	
2007/01/05 08:46:05	Paul McCabe (512@localhost)	Christian Stredicke (222@localhost)	01:28 M
2007/01/05 09:29:14	Sharon Houle (520@localhost)	12128428819	02:48
2007/01/05 09:32:14	Sharon Houle (520@localhost)	Paul McCabe (512@localhost)	05:45
2007/01/05 09:38:30	Sharon Houle (520@localhost)	Jonathan Greenwood (500@localhost)	00:08 M
2007/01/05 09:39:14	Sharon Houle (520@localhost)	12128428819	01:35
2007/01/05 09:49:41	Jesse Fleming (523@localhost)	19789020869	00:09
2007/01/05 09:51:40	4612128428819@66.193.176.35	Sharon Houle (520@localhost)	00:33 M
2007/01/05 09:52:35	Sharon Houle (520@localhost)	12128428819	01:22
2007/01/05 09:55:05	Sharon Houle (520@localhost)	Paul McCabe (512@localhost)	02:55
2007/01/05 09:58:35	Sharon Houle (520@localhost)	12128428819	00:01
2007/01/05 10:00:16	Sharon Houle (520@localhost)	12128428819	02:47

The call log shows the last calls that were made on the system, independently from the domain. You will see the start date, the source and destination, the account that will be charged to a call and the duration of the call, if the call connected. The length of the log is set in Appearance.

The start time for unconnected calls is the time when the call was initiated. For calls that actually connected, the connection time will be used.

The "To" and "From" headers are copied as they are. For calls that run over trunks that use registration, this might be annoying, because the PBX will use the identity of the trunk in the "From" field. However, for such calls it will display the account that initiated that call in the Charge column. Note that in the case of call redirect and transfer the PBX will charge the account that initiated there direction and transfer. In these cases you will see several CDR in the log; one for the initial call and another one for the transfer or redirect call.

For calls that were redirected to the mailbox, the PBX adds a "M" flag. For calls that were redirected to an external number, the PBX adds a "E".

5.13.4 Active Calls

In the calls menu, you will see which calls are currently active on the system.

You will see when the call started, the source and destination and the call state. The state may be early or connected.

The page will automatically refresh after ten seconds.

5.14 Recording

The PBX 2.0 supports several ways of recording calls:

- It is able to record selected calls to the file system. Those files are recorded in

compress format using the GSM codec at 13.2 kbit/s (approximately 100 KB per minute).

- Alternatively, calls can be sent to a real-time recording station. This is done using a standard SIP call. By using the SIP standard, the PBX can be connected to a large number of recording devices, including soft phones for listening in or recording solutions that support SIP.
- The user may also initiate a recording by pressing the record button on the phone.

The user-initiated recording, which was supported in the 1.x version, does currently not support the sending of the WAV file. Because such files can get large, we are currently investigating alternative ways of providing recording information.

5.14.1 Recording to File

When recording to a file, the PBX needs to know the location where to place the file. The WAV file itself contains only the recorded conversation; there is no ancillary information (caller-ID, IP-Addresses etc.) embedded in the WAV file. However, by using variables in the recording file name, you may provide information:

- "\$r" is replaced with the recording directory, which is "recordings".
- "\$i" is used to indicate the direction of the call. The PBX substitutes an "i" for incoming calls, and a "o" for outgoing calls.
- "\$u" is being replaced with the canonical (primary) name of the extension.
- "\$n" is replaced with the calling party number.
- "\$m" is replaced with the domain name.
- "\$d" is replaced with the date of the call in the format "20071220" (no spaces or dashes in between).
- "\$t" is replaced with the time of the call in the format "134349" (no spaces or dashes in between).
- "\$\$" is replaced with a single "\$" symbol.

The default recording name is "\$r/rec-\$d-\$t-\$i-\$u-\$n.wav".

5.14.2 Recording to a SIP URI

When you specify a recording name with a sip scheme (e.g. "sip:record@192.168.1.2"), the PBX will initiate a call to that location. The other side of the call can either accept the call or it can send an error code if it does not wish to record this call. In this case, the associated resources for the recording call are released.

If the call connects, the PBX will encode the data in the selected codec type. Please be aware that in any case, the PBX must decode the monitored media streams, because otherwise it would not be able to mix the two streams together. This might mean a significant increase in CPU load that you should keep in mind.

6 Domain Administration

6.1 Settings

6.1.1 Default Values

Default Values:

Default Dial Plan:	Standard International ▾
Default IVR Language:	English ▾
Tone Language:	English ▾
Web Language:	English ▾
Music on Hold Source:	File moh.wav ▾
Timezone:	Default Time Zone ▾
Default PnP Dialplan Scheme:	North America (3-digit extensions [5-7]xx) ▾
Voicemail Timeout:	30
Voicemail Size:	4
Maximum Voicemail Duration:	
Voicemail PIN Digits:	4
Require Entering Mailbox PIN:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Mailbox Escape Account (when caller presses 0):	
Mailbox Direct Dial Prefix:	8
External Voicemail System:	
Mailbox Explanation Prompt:	<input checked="" type="radio"/> Always <input type="radio"/> Not on personal recording
Call Forward On No Answer Timeout:	10
Speed Dial Prefix:	
Address Book Matching:	<input type="radio"/> Include Domain <input checked="" type="radio"/> Just Number
Pickup Policy:	<input type="radio"/> Strict <input checked="" type="radio"/> Loose

6.1.1.1 Default Dial Plan

Most of the accounts in a domain will use a default dial plan. In this case, you will not specify a specific dial plan. Instead, you can specify which dial plan should be used for accounts where no special dial plan has been provisioned. This can be done in the "Default Dial Plan" selection box.

6.1.1.2 Default IVR Language, Tone Language and Web Language

The default language for the system is set up in the administrator mode (see Overall System Settings). If you want to override that setting for the active domain, you may do this with this setting. See Localization for more details on language support.

6.1.1.3 Music on Hold Source

You need to specify which music on hold is being used for the active domain. This source will be used in waiting queues and when an extension puts a call on hold or parks a call on a park orbit. See Music on Hold for more information.

6.1.1.4 Timezone

The default time zone for the system is set up in the administrator mode (see Overall System Settings). If you want to override that setting for the active domain, you may do this with this setting. See Localization for more details on time zones.

6.1.1.5 Default PnP Dialplan Scheme

The automatic provisioning is able to provision a dial plan for selected user agents (see Plug and Play for details. The final decision for the used scheme is being made based on the dial plan of the extension. See Dial Plan Schemes for more information on how to set up dial plans for provisioning.

6.1.1.6 Voicemail Timeout

If you don't specify a value for a specific user but enable the mailbox, the Voicemail Timeout defines how long the PBX will wait until it redirects the call to the mailbox. A reasonable value for this is 20 seconds, but depending on the activity in your office you might change that value.

6.1.1.7 Voicemail Size

The Voicemail Size determines how many messages can be stored in a voicemail box. Again, you can override this value per user, but it is good to have a reasonable default. Twenty is a good default number.

6.1.1.8 Maximum Voicemail Duration

In addition to the maximum duration for a recording, you may specify how long a mailbox message may be. This setting makes it easier to plan memory size for mailbox messages. Typically, a mailbox message should not be longer than two minutes. The unit for the setting is seconds.

6.1.1.9 Voicemail PIN Digits

When you create an extension, you can leave the PIN field empty. Then nobody will be able to access the mailbox with a pin, only a user that registers with

the extension credentials is able to go to the mailbox. However, if a user wants to set up the PIN, you must tell the PBX how many digits a PIN must have. Typically, a PIN consists of four or five digits, but you can pick any number larger than one.

6.1.1.10 Require Entering Mailbox PIN

Calling your mailbox should be simple. Depending on your office layout, it might be easy for coworkers to use a phone without authorization and listen to voicemail messages. Therefore, the administrator can decide if the mailbox should first ask for the PIN code before reading out messages.

6.1.1.11 Mailbox Escape Account

If the Mailbox Escape Account setting is set, a user who hits the mailbox may press the "0" key to get to the account that you specify here. The number may be an internal number or a external number.

6.1.1.12 Mailbox Direct Dial Prefix

If you want to call directly into a mailbox, you may put this direct dial prefix in front of the extension number. This is useful when calling from your cell phone into the auto attendant or when you want to leave a voicemail message for your coworker. Typically, this prefix is a "8".

6.1.1.13 External Voicemail System

Sometimes you don't want to use the built-in mailbox. There are several specialized external voicemail systems available which accept calls from a SIP PBX and provide functions like voicemail to email, calendar functions and much more. For example, you can use Microsoft Exchange for this purpose.

The setting contains the telephone number that should be dialed. You can include replacement fields which are used in the Caller-ID representation for outbound calls (see Outbound Calls on Trunk). The dial plan for the called extension will decide which trunk will be used to initiate the call.

6.1.1.14 Mailbox Explanation Prompt

If a user records a personalized message, the PBX may say after this prompt another message that explains that the caller may now leave a message. Some people like this and others don't, therefore we made the behavior of the PBX a setting. If you set the Mailbox Explanation Prompt, the mailbox will explain the caller's options after the playback of the personal recording. For the standard greetings, the PBX will always explain the options.

6.1.1.15 Call Forward On No Answer Timeout

Sometimes the PBX has to redirect a call after a timeout. The setting "Call Forward On No Answer Timeout" tells the PBX how many seconds to wait before performing the timeout action.

6.1.1.16 Speed Dial Prefix

If you are calling a speed dial number from the address book, you usually run into the problem that you need to put a prefix (like "9") in front of the address book number, so that the call gets routed as an external call. The Speed Dial Prefix solves this problem.

6.1.1.17 Address Book Matching

When you set up the address book, you may specify a speed dial number along with the address book entry. The setting Speed Dial Prefix is used to complete the number in case that a user dials a speed dial number. This is necessary in system setups that require a prefix (e.g. "9") for an outside line.

6.1.1.18 Pickup Policy

The pickup policy is explained in Park and Pickup.

6.1.1.19 SOAP External Call

This setting is only visible if your license key contains a SOAP key. In this setting you can put the address of the application server that is used to determine if calls are allowed to go to an external number. See SOAP for more details.

6.1.2 Email Settings

Email Settings:

From (e.g. Joe Average <ja@domain.com>):	<input <abc@test.com>"="" abc\"="" type="text" value="\"/>
Account (e.g. user1):	<input type="text" value="abc@test.com"/>
Password (e.g. secret):	<input type="password" value="....."/>
SMTP Server (e.g. smtp.domain.com):	<input type="text" value="smtp.test.com"/>

The PBX is able to send emails on different occasions. It uses SMTP (SMTP=Simple Mail Transfer Protocol) and POP3 (POP=Post Office Protocol) to talk to the email server. POP3 is only used for authentication purposes, the PBX will not download messages from the email server; it will just send messages. Most operators today offer the usage of "ESMTP", which stands for Enhanced SMTP. This protocol includes the authentication, so that you don't have to use a POP3 server. Please contact your email-provider to check if these protocols are supported.

The "From" field is copied into the message as the originator of the message. You should put a "display name" and an email address there, please use corner

brackets around the email address to make it clear to the email server what the display name is and what the email address is. An example for this setting is "PBX <pbx@test.com>". Please notice the quotes around the name.

The SMTP server is the address of your SMTP server. You may use DNS names here, and the PBX will use DNS A record lookup to locate the server. If you put a colon followed by a port number behind the name, the PBX will contact the specified port on that host; otherwise it will use the default port.

6.1.3 Feature Codes

Feature codes are traditionally used by users to control the PBX. When the first PBX was invented, there was nothing like a web interface where you could set up your preferences, so the designers decided to define a specific number space for controlling the behavior of the PBX. Traditionally, these codes start with a star symbol followed by one or two digits. The IP PBX emulates this behavior, so that users can use the IP phone just like a PBX extension phone.

6.1.3.1 Call Park

Extensions may hold or park a call. When a call is hold, only the extension can pick the call up again; when the call is parked other extensions may pick up the call as well. Holding is done by pushing the hold button on the extension, most SIP user agents support this feature with a special key or a soft key. Parking a call will redirect the call to a park orbit. Even if you disconnect the extension the call will stay there until someone picks the call up or the caller disconnects.

Every hunt group and extension has its own park orbit. The name of the orbit is the same as the name of the account.

Usually user agents don't have a special key for parking a call. If they have, this key will essentially redirect the call to the park orbit with a blind transfer. Therefore, extension may generally park a call by a blind transfer to the park orbit. However, PBX users are used to star codes that perform the transfer to the park orbit.

In SIP, a user agent will first put the call on hold before it can send a star code. Sending the star code is executed in a new call that has the destination of the star code (e.g. <sip:*85@test.com>). When the PBX receives such a call, it will search the last call that this extension received or initiated and will perform the blind transfer of that call to a matching park orbit. It will then play an announcement that the call has been parked and hang up.

If the extension subscribes for the LED status information, it will light up the respective LED after the call has been parked on the park orbit.

6.1.3.2 Call Park Retrieve

After a call has been parked, there must be a way to retrieve the call from the park orbit. The retrieve code will go through the list of park orbits of the user

and pick up the first park orbit where a call has been parked.

Note that park orbits may have more than one call parked. In this case the park orbit acts as waiting queue. The call park retrieve will pick the first call in the orbit, so that the callers will leave the queue after the first-in-first-out principle.

See Park and Pickup for more information.

6.1.3.3 Call Pickup

Call pickup searches for unconnected calls and redirects them to the extension. The other extension that might be ringing will be canceled. The typical case for call pickup is when a colleague is temporarily not available, but you want to take the call.

The PBX searches first the hunt groups where the extension is a member for a call that can be picked up. If no call was found, it tries the extension's park orbit. If the user specifies the park orbit after the pickup code, the PBX will search only the indicated park orbit. However, the extension must be member of a hunt group, where the pickup destination is also a group member. This is necessary to protect unauthorized call pickups.

More information on parking and pickup can be found in Park and Pickup.

6.1.3.4 Call Return

Call Return will dial the last number that has been missed. This function is useful for SIP devices that don't keep a list of missed calls (e.g. ATA). Most SIP devices with a display have this function built-in, and the user may see the caller-ID in the screen before returning the call.

The call return function stores only one number. When the extension makes a call that gets connected, the call return number is cleared. This makes sure that a number is called only once, and users can dial the call return code without talking to the same number again.

6.1.3.5 Redial

The Redial is similar to call return, but it does not call the last incoming number, it calls the last dialed number again. The redial number is never deleted, users can redial numbers even if the call established. The redial number and the call return numbers are stored independently.

6.1.3.6 Transfer

Some devices do not have a transfer button. For examples, when using ATA there is usually no way to initiate a transfer except dialing a special code. The transfer code initiates a blind transfer of the last call on hold to the provided destination. The destination must be entered directly behind the star code.

6.1.3.7 Call Forward

There are three events that may trigger the forwarding if a call:

All means that the call is forwarded always, independently of an event. Busy means that a call is forwarded if the extension is busy. The busy condition must be returned by the device, the PBX does not check the internal state for the busy condition. This makes it possible to handle the busy condition if several devices register for the same extension number. When several extensions are used, the busy condition checks if all devices are busy.

No Answer means that no device picked up after a certain timeout. The timeout is a domain setting that can be overwritten by an extension setting.

There are six star codes to handle the call forwarding. Three codes are used to enable the call forwarding condition. If the user dials this star code, the PBX will prompt the user for the redirection number.

The other codes are used for turning the redirections off. When the user dials these star codes, the user will hear a prompt that the feature has been deactivated.

6.1.3.8 Block CID

By default, the PBX will try to present the caller-ID on outgoing calls. Sometimes, users don't want to show the extension number. By using the block CID code the PBX will try to hide the CID on all subsequent calls until the user deactivates the blocking.

Calls from one extension to another extension will always show the caller-ID.

6.1.3.9 Block Anonymous Calls

When the PBX receives a call where the caller-ID is neither an extension number nor consists of a valid caller-ID, it will assume that this is an anonymous caller ID. A call-ID is treated as valid when it consists only of the characters 0-9. It may have a '+' character in the beginning.

By default, the PBX will allow anonymous calls. However, some users don't like to receive such calls. When the feature is enabled, those calls are rejected with a IVR prompt which explains that the caller-ID could not be identified and the user accepts only calls with a valid caller-ID.

6.1.3.10 DND

Do Not Disturb (DND) is used to temporarily reject all incoming calls for all devices registered with this extension. The two star codes are used to turn DND on and off.

DND also applies to hunt groups. If a member of a hunt group has set its extension number to DND, the hunt group will skip that extension. This is a different to redirect all, which will not redirect calls from a hunt group.

Many SIP devices have a dedicated DND button. Most implementations handle DND locally on the device. However, when this function is used, the DND applies only to the specific device and not to the extension and it usually does not survive reboot cycles.

6.1.3.11 Agent Login and Logout

Agents can explicitly login and logout for agent groups. Their extension stays registered and is dialable independently from the agent login status. The status applies to all agent groups of the extension.

6.1.3.12 Go To Voicemail

This star code is just a quick way to get to the mailbox.

6.1.3.13 Intercom

By using the Intercom prefix, you can directly call another extension. The other phone is asked to pick up immediately and to establish a two-way audio conversation.

Intercom is different from Paging in the way that Intercom is two-way, one-to-one communications while paging is one-way, one-to-many communications.

6.1.3.14 Record

If you want to record the prompt for an auto attendant, an agent group or an IVR node, you can use the Record star code. The PBX differentiates three cases:

- **Attendant:** The digits behind the code identify the auto attendant and will record the announcement for the account (e.g. dial *98123 to record the announcement for auto attendant 123).
- **IVR Node:** The digits behind the code identify the IVR Node and will record the announcement for the account.
- **Agent Group:** The code needs two arguments. The first argument identifies the queue, and the second argument the prompt. The arguments are separated with a star symbol. The first prompt with index 0 is the welcome prompt; it will not be repeated and it will be played for all callers, no matter if they have to wait or not. The other prompts with the index 1-9 will be repeated in a loop and are only played while the caller has to wait in the loop.

6.1.3.15 Clear Voice Message Indicator

When the user dials this star code, the PBX will delete the Message Waiting Indicator (MWI) on the extensions. Usually it should not be possible to clear the MWI indicator manually, but if the extension just does not want to listen to the mailbox and keep the MWI indication silent, this star code will turn the indicator off.

6.1.3.16 Send Voicemails

When the PBX records a mailbox message, it may store it locally or it may send it via email to the user. Please note that sending a voicemail message per email requires that you have properly set up the email address of the user and of the domain. With the activation and deactivation of this feature you toggle between the methods.

6.1.3.17 Customer Originated Trace

This useful feature sends the call details of the last calls to the email account of the extension. Instead of writing down the number on a notepad, the user can instead send him an email that contains all the information.

The PBX will include a link to the last number. If you click on this link, the PBX will prompt you for your username and password. Please enter your username in the form "user@domain". If your browser supports saving the login information, the next time when you click on such a link to dial a number you will immediately initiate the call to that destination.

This feature works only with user agents that support the REFER mechanism outside of existing dialogs. Check out your phone if it is able to support this feature. On some phones, you have to press "Ok" or lift up the handset in order to acknowledge the dialing of the number. The remote initiation of a call is a security-sensitive topic, as it might turn your phone into a microphone. Therefore, you must authenticate yourself during the initiation of the call and you may have to acknowledge the initiation of the call.

6.1.3.18 Add White List, Add Black List

These codes are used to store the last caller in the "white" or "black" list. It is a convenient way of keeping the address book updated with useful information for further communications. See White and Black List for more details.

6.1.4 Address Book

6.1.4.1 Purpose

The address book stores associations of numbers with names, speed dial entries and types.

Numbers are generally telephone numbers. The PBX does not support SIP URI numbers in the address book. Numbers may contain readability characters. The PBX internally converts the numbers into purified numbers, so that matches with other numbers become more easy and consistent. If your domain has selected a specific dial plan scheme (for example, North American dial plan), the PBX also internally automatically converts the number into a consistent presentation. If the PBX requires that a name must be presented as one string (for example, in the SIP display name), it will automatically put a space character between the first and the last name if both names are not empty.

Names consist of the first name and the last name. The purpose of this separation is to make searches easier; sometimes the user searches for first and sometimes for the last name. Otherwise the PBX treats the names transparently. Names should be encoded in UTF-8 format. The web browser usually performs the necessary conversions, so that the end user does not have to deal with this problem.

6.1.4.2 Speed Dial

The speed dial entry is a two-digit star code (for example, *12). The range should be in the lower feature code range, so that they do not overlap with the other feature codes that are available on the system. If there is an overlap, the speed dial numbers have a higher priority.

Speed dial numbers are useful if you want to store numbers that you are using frequently, especially if your telephone does not support an address book. Used in the domain mode, they also might be useful to hide the number that is being dialed (however, that kind of security is very weak).

6.1.4.3 Black List and White List

An address book entry also has a type flag. This flag can be set to "white", "black" or unset. If it is "white", that address book entry is on the white list, if it is black, it is on the black list. The white list usually contains the contacts that are trusted and therefore get a preferred treatment. The black list usually contains the list of contacts that are known and unwanted. For example, it makes sense to put a family member's number on the white list, while the caller-ID of an aggressive sales person might end up in the black list.

If that flag is set to "white", the number is part of the white list. That means, when a caller has the type "white", he will never be intercepted by the auto attendant to record the name.

Callers on the white list are allowed to receive a call back when the extension becomes available.

If a caller is on the black list, the behavior of the PBX depends on the settings of the user for anonymous call treatment. If the caller should be blocked, then the PBX will block that call. Otherwise the PBX will always ask the person to leave his name before calling the extension.

Callers on the black list will also not be allowed to camp on an extension.

6.1.4.4 Personal Address Book

The address book entries in the personal address book are only visible to the user.

To see the personal address book, you must be logged in as user in the web interface of the PBX. In this screen, you can edit and delete address book entries by clicking on the edit and delete button.

pbxnsip Settings Lists Status Help Logout
Mailbox Missed Call Log Address Book

Personal Address Book

This list shows your personal address book. Please be careful when setting speed dial numbers. Use the asterisk sign in front of the number and be sure that you don't overlap a feature code. Please be careful clicking the delete button, because the entry will be permanently deleted.

Number	First Name	Last Name	Speed Dial	Edit	Delete
011-43-234-4223423	Frederick	Steinman	*13		
212-243-2323	Marc	Kelvin	*12		
515-423-5434	Maria	McKenna			
978-994-4985	Karl	Kloß			

Create New Entry:

First Name:

Last Name:

Number:

Speed Dial:

Contact Type: Regular Contact

Copyright © 2005-2007 pbxnsip Inc. All rights reserved. See the license agreement for more information.

If you want to add an address book entry, you can manually add this entry from the web interface. You may also load a CSV-file into the system (see below).

You can also add a number to the address book by dialing the black list and white list star code. If the number does not exist, the PBX will automatically create an address book entry for this number.

6.1.4.5 Domain Address Book

The domain address book entries are visible to all members of the domain. That means they can search the domain address book and calls coming to that domain will automatically see the name of the calling party.

All names in a domain are automatically included in names searches in the domain.

You can also use the address book to indicate which DID number has been dialed. If you add an address book entry that matches the specific DID, the PBX will add the display name to the caller-ID, and the phone then can display the text associated with the caller-ID.

6.1.4.6 Address Book Import

Most address management programs support the export of a CSV (comma separated value) file. The PBX can read this format, if the below guidelines are kept.

The field separator must be a semicolon.

- The first column must contain the first name; the second column must contain the last name.
- The third column must have the number. The number must have numeric characters. The characters "-", "(", ")", " " (space), "/" and "." are ignored and may be included for readability. The first character may be a '+', so that global telephone numbers may be used. For example, the numbers "(978) 543 6545" and "+49 (30) 386-12345" are valid numbers, while the text "WIRELESS CALLER 9785436534" is not a valid number.
- The fourth column may have a speed dial number. The number must contain a star character in the beginning. If the star code was already used by another entry, the PBX will clear the other star code entry during the import process.
- The text must be encoded in UTF-8 format.

Because the number must have numeric characters, it is ok if the first contains the field description. For example, most programs use a name like "Number" to identify the column, and because that name is not a phone number the system will not include that row in the address book.

The following example shows an address book that can be imported:

```
First Name;Last Name;Number;Speed Dial
Fred;Feuerstein;(978) 123 4567
Carl;Clever;(212) 324 4334;*12
Franky;Fahrenheit;(515) 234 3334
"A;B;C";;(123) 543 3453
```

6.2 Accounts

6.2.1 Existing Account List

The list of accounts shows all available accounts in the domain. The list will show the name, the type and some status information. By clicking on the edit button, you can edit the details of the account. If you click the delete button, you will delete that name of the account and if that was the last name for the account, you will ultimately delete the account.

[1-8](#) [9-16](#) [17-24](#) [25-25](#)

Account	Type (Name)	Status	Edit	Delete
509	Extension (Norman Bardsdales)			
510	Extension (Kevin Kleinmann)			
511	Extension (Doris Dunkingdong)			
512	Extension (Elisa Evergreen)			
513	Extension (Francica Frankenstein)			
514	Extension (Gregory Grumble)			
701	Service Flag	Set		
706	Conference			

* User has administrative permissions for this domain

If you have several names for an account, it will be shown in the list several times. The primary name will be shown in brackets behind the alias name. An asterisk behind the name means that this account has administrative rights for that domain.

The type field shows the type of the account. If you have an extension, it will also show the display-name of that account in brackets. On some user agents, you will see a link for the registration in brackets. This link will take you directly to the web interface of that user agent. The status column will then show how many registrations are available for that account and if the extension has voice mail.

6.2.2 Creating New Accounts

6.2.2.1 General

Before you can use an account, you must first create it. In order to do this, click on the create button in the accounts menu in the domain mode.

When you create an account, you must select what type it will be. The type can not be changed later.

Every account may have several names. One name is the primary name and the other names are the alias names. Please enter the names in the Account Names field. If you use a space between the names, the PBX will set up several accounts for you. If you use a slash between the names, you will set up one account with different alias names. For example, "123/theo 124/fred" will set up two accounts, the first with the names "123" and "theo" and the second with the names "124" and "fred".

A good username is a name that consists only of the letters 0-9, a-z and '+', '-', '_' and '.'. If you want to use PSTN-like numbers, you should use only names with 0-9. However, it does not hurt to create alias names that contain alphanumeric letters like in emails, for example like "joe.average" or "ja". All account names must be lowercase. The PBX changes input automatically to lower case.

Username may start with the special prefix "tel:". This has a special meaning. Accounts with this name have a global scope in the PBX. This is useful to do DID Routing.

6.2.2.2 Creating Extensions

Account Type:

Dial Plan:

Plug and Play:

	Number	First Name	Last Name	Password	Email
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

When you select the extension type, you will be able to add up to ten accounts in one go. You can not only define the account name, you can define also the most important settings for those accounts right during the creation.

First of all, you can select which dial plan those extension will have. If you want to use the default dial plan, you can just leave this selection box unchanged.

If the accounts should be assigned by an automatic plug and play mechanism, you can select either permanent or temporary assignment modes. See Prepare an Extension for Plug and Play for more details on this topic.

6.2.2.3 Creating Other Types

Account Type:	Auto Attendant ▾
Account Names (e.g. "123/f.feuerstein"):	<input type="text"/>
<input type="button" value="Create"/>	

Creating other types does not offer any additional parameters. You need to edit the account's parameter later by selecting them from the Existing Account List.

6.2.3 Extension

When you click the edit extension link, the menu bar will show some more links: Settings, Redirection, Registration and Events.

6.2.3.1 Identity

Identity:	
Primary Name:	<input type="text" value="509"/>
Alias Names:	<input type="text"/>
First Name (e.g. John):	<input type="text" value="Norman"/>
Last Name (e.g. Smith):	<input type="text" value="Bardsdales"/>
Email Address (e.g. abc@company.com):	<input type="text"/>
Cell phone number:	<input type="text"/>
Password:	<input type="password" value="....."/>
Password (retype):	<input type="password" value="....."/>
Dial Plan:	Domain Default ▾
Timezone:	Default Time Zone ▾

In the settings tab, you may define the fundamental settings for that account.

Here you can change the primary and alias names for that account. Use white space to separate the different alias names. The names must follow the naming guidelines described in the section about creating an account.

The name ("First Name", "Last Name") will be used whenever the PBX creates a canonical representation of the extension. This is the case when the

extension starts a call or when an email is sent to the extension user. Here you can fill in any string that you like.

The email address is used in cases when the PBX wants to send an email to the extension user. This setting must have the form username@domain.

The "Cell Phone Number" is used in different places, see Cell Phone Integration on this topic.

The "Password" is used for authenticating the user. If the password is set, the PBX will challenge SIP user agents on requests and it will use that password if the user tries to log into the web interface as domain administrator.

The Dial Plan selection box assigns one of the available dial plans to that user. Because dial plans are assigned on user basis, the domain administrator can control the rights of the user to place outside calls.

Every extension may have its own "Timezone". The time zone is used for mailbox timestamps and for automatic provisioning of the extension's user agents.

6.2.3.2 Mailbox

Mailbox:
Mailbox Enabled: on off
Mailbox Timeout (sec):
PIN (e.g. 1234):
PIN (repeat):
Maximum Number of Messages:
Voicemail Handling:
Send Email for missed calls: on off
Announcement Mode:
Allow Access for Extensions:

You can enable or disable the mailbox for that user with the Mailbox Enabled flag. The Mailbox Timeout will override the domain settings for the duration after which the mailbox will be used. The Mailbox PIN is used to authenticate the user, e.g. when the user is calling his mailbox from another extension or an outside line. You can use any number of digits for this setting, but we recommend four or five digits.

The Maximum Number of Messages will override the domain settings on how many messages can be stored in this mailbox.

The voicemail handling will select the way a mailbox message will be delivered. You can choose between storage on the system (which is the default) and sending via email. If you send the voicemail messages via email, the messages are not kept on the system. You should check that email forwarding is working by making a test call.

The announcement mode contains three modes. The "Anonymous Announcement" mode is the default mode if the user has not recorded his name. If the name has been recorded and the user selects the name mode, the "Name Announcement" can be used. The third mode "Uploaded Announcement" uses a completely customized recording, which may be recorded with the recording star code. The announcement must be loaded into the account by the "Announcement" setting and it must be in 8 kHz sampling frequency, mono, 16 bits/sample format.

If you want to allow other extensions to use the mailbox, you may list those extensions separated by space in the setting "Allow Access for Extensions". This feature makes it possible to set up a group mailbox, for example for a hunt group.

6.2.3.3 Redirection

Disturb:
Anonymous Call Treatment:
DND: on off

Destinations:
Hot Desking at:
Call Forward All:
Call Forward Busy:
Call Forward No Answer:
Call Forward No Answer Timeout (sec):
Mailbox Escape Account (overrides domain setting):

Recording:
Record incoming calls from hunt group: on off
Record incoming calls from agent group: on off
Record incoming calls from extension: on off
Record outgoing calls to internal numbers: on off
Record outgoing calls to external numbers: on off

The setting "Anonymous Call Treatment" describes how anonymous calls to the extension are handled. The following options are available:

- The "no special treatment" mode turns this feature off and sends all calls directly to the extension.
- The mode "reject call" will inform the caller that the extension does not accept anonymous calls. Calls will not be put through to the extension.
- The mode "pretend to be busy" also does not put the call through, but does not tell the caller why. The PBX will not offer camp on.
- The mode "ask for name" will prompt the caller for the name and then put him on hold while calling the extension. After reading out the recorded name, the extension may decide what to do with the call. Either the call can be accepted, or it can be sent to the mailbox or it can be rejected.

- The mode "ask for name even if the caller-id is present" will always ask for recording the name, even if the caller-id is available. Only callers which are on the white list are directly put through.

Please note that internal calls are never anonymous.

The DND and redirection settings are already explained under the star code section.

Hot Desking is described in a separate page Hot Desking.

The redirection tab controls how and when calls get redirected when this extension is called. These settings are also directly accessible to the user through the star code interface of the PBX. If the user uses the star code interface, he does not need administrative rights. By changing it on the web interface, the administrator can change the setting for any extension.

The "mailbox escape account" is described in the Domain Settings. The recording settings are described in Recording.

6.2.3.4 Registrations

User Agent Setup:

Trusted IP Addresses:

Bind to MAC Address:

Password has been used for provisioning: yes no

Parameter 1:

Parameter 2:

Lines:

Dialog Permissions:

Log Register Expiry:

The registrations web page is used to control the registrations for that account.

You may register one or more devices for one extension. When an extension is called, the PBX will call all registered extensions in parallel. The first extension that picks the call up will get the call and the other extensions will receive a cancel message.

If you enter something into the trusted IP address field, the PBX will only

accept registrations from the indicated IP addresses. You can list the allowed IP addresses separated by space. To indicate subnets, use a slash and the number of significant bits behind it (e.g. 192.168.2.0/24).

If you want to bind this registration to a specific user agent, you may enter the MAC address in the "Bind to MAC Address" setting (for example 00c01254f3dc) or use the "?" or "*" symbols which are described under the "Create" section above.

If you choose to provision passwords only once, the PBX keeps a flag for this purpose. Sometimes, it is necessary to send the password again, and in this case the administrator needs to reset the flag manually. That is the purpose of the setting "Password has been used for provisioning".

The settings "Parameter 1" and "Parameter 2" can be used in different places as generic, extension-related parameters. For example, the parameters can be used when presenting outgoing Caller-ID.

The "Lines" parameter is used during provisioning to tell the phone how many line keys it should allocate (whenever applicable). Also, if the parameter is set, the PBX limits the number of calls that this extension can have on the PBX. If there is a call active, the PBX will not page that extension and it will also not perform intercom calls to that extension.

The setting "Dialog Permissions" is described in Dialog Permissions.

Sometimes it is hard to track down registration problems. Therefore, the domain administrator can specify a log level for registration log messages specifically for an extension. This makes it easier to find out when an extension loses registrations temporarily.

Type	Contact	Device	Expires	Reboot
REGISTER	<sip:504@192.168.10.232:2051;line=m2q3d9yb>;flow-id=1;q=1.0;+sip.instance="<urn:uuid:4e890c44-dd88-4e6b-915b-e40672957b23>"	snom300/6.2.3	67	check-sync

Click [here](#) to clear the registrations.

Add Contact:

Save

Below the Edit button you will see the current registrations for that account, if there are any. The list will show the registered contact address (as indicated in the registration message), how long the contact is registered and the registration type. If the registration has the type "REGISTER", it is a standard registration for receiving calls. Other registrations are for specific event types, for example message waiting indications.

Sometimes it is useful to clear all registrations. In order to do this, use the link at the bottom the page. Please don't forget to refresh the registration from the user agent, so that you are able to call it.

You may also send a reboot request to the phone by clicking in the "check sync" link. This way, you don't have to use the web interface of the device or even go to the phone to reboot it (for example to read new configuration data). Please note that not all user agents support this method.

If you want, you can manually add a registration. The meaning of this feature is discussed in a separate page Manual Registration.

6.2.3.5 Permissions

Administration Permissions:

Domain Administrator: on off

Override DND: on off

The domain administrator can grant certain permissions to an extension.

- If the "Domain Administrator" flag is set, the extension has the right to log in as domain administrator and do changes in the domain.
- If the "Override DND" flag is set, the account has the right to call an extension, even if that extension is currently on DND. Please note that this applies only to DND which is set on the PBX; if you set DND locally on the user agent, the PBX has no way to call that phone.

6.2.3.6 Instant Message

Destination:

Message:

You can send an instant message (IM) from the PBX web interface. The PBX will send the message to all accounts that you list in the address field. This is a very simple way to send a message from an account which has no IM-capable devices registered to it.

6.2.4 Auto Attendant

6.2.4.1 Purpose

The auto attendant can be seen as a simple receptionist that helps to connect the incoming caller with an extension. This may include searching for the name, entering the extension number, protecting certain extensions and redirecting calls to external numbers.

All calls to extensions go through the auto attendant. When the PBX already knows the number, it just skips the prompts and goes directly to the phase when the account number is called.

The attendant does not use the SIP redirection mechanism. It starts a new call and passes the media through the PBX. This approach has several advantages, for example the caller can cancel the call and try another extension.

Until one of the destinations answers with a ring back message, the auto attendant plays comfort noise to the caller. This emulates the behavior of the old analog system and indicates the caller that the call is still active. Upon arrival of the ring back message, it changes the tone to a ring back tone.

When calling an extension, the caller has the possibility to press the star key while the extensions are ringing. In this case, it cancels all calls and prompts for another number.

The logic for handling DND and call forwarding is explained in the section about the star code handling (feature codes in the domain administration).

6.2.4.2 Identity

Identity:	
Primary Name:	<input type="text" value="555"/>
Alias Names:	<input type="text" value="info"/>

The identity settings are the same as the settings for the extension identity, see Extension Identity.

6.2.4.3 Behavior

Behavior:

Extension Input:

Say Name: No Yes

Accounts that cannot be called:

Accounts that may record a message:

Dial Plan for outbound calls:

Second Language:

Dialog Permissions:

WAV File*:

When the user enters an extension number, the auto attendant has to determine when it should try to go to an extension. The following modes are available:

- "When Extension Matches" checks after every digit if the digit sequence matches an existing account. If this is the case, it will call that extension. This mechanism is useful when you use accounts with varying name length, however it might be annoying if the caller tries a non-existing number.
- "After 1/2/3/4/5 Digit Input" will count the number of digits and after the right number has been entered it will try to go to the account that has been entered. If that account does not exist, it will play an announcement.
- The "User Must Hit Pound" mode waits until the user hits the pound sign. This mode is useful in variable-length scenarios, where you explicitly tell the user to terminate the input.

If you turn the "Say Name" setting on, the PBX will play an announcement that repeats the user input, or, if the user recorded the extension name, will play back the user name.

The "Accounts that cannot be called" setting lists the accounts that are disabled for redirection. This setting is useful if you want to exclude incoming callers from using conference accounts or to dial VIP numbers. You can use Wildcard Patterns in this list.

To set up the auto attendant prompt, you have two choices. The first choice is to use the Record star code (described in the feature code section). This possibility is useful when the secretary wants to recording on her own or when that announcements may change often. In this case, you might want to list the "Accounts that may record a message" using a list of Wildcard Patterns.

The second choice is to may load a prerecorded WAV file into the system. Please use a standard recording tool to record the message and make sure that you

are using 8 kHz sampling frequency, mono 16-bit recording format. This choice is useful when you want to a studio recording or you want to deploy a recording into several accounts.

If the auto attendant redirects calls to a trunk, it needs a dial plan to do this. You may select the dial plan with the setting "Dial Plan for outbound calls". This dial plan will only be used if there is no account that can be charged for this call (for example, in night mode); otherwise it will use this account's dial plan.

The auto attendant supports environments with two languages. If you select a second language, the auto attendant will determine if the call already has a call assigned. This can for example be the case if the call went through a previous auto attendant or an extension calls the auto attendant. If there is no language assigned, it will first ask the caller for the language and then continue the dialog in that language.

Dialog Permissions are described in Dialog Permissions.

6.2.4.4 Timeout Handling

Timeout Handling:

Redirect Number:	<input type="text" value="520"/>
Timeout (s):	<input type="text" value="20"/>
Hangup Timeout:	<input type="text"/>

When the user does not enter any information for a certain time, you may redirect the call to another account. In order to do this, specify the time in seconds and the account name in the settings "Redirect Number" and "Timeout (s)".

If the user does not enter anything, you also might want to terminate the call. This feature is useful when the PSTN gateway has problems detecting that the call was already hung up. Then the setting "Hangup Timeout" may help to clear the call relatively quickly.

6.2.4.5 Night Service

Night Service:

Service Flag Account:	<input type="text"/>
Night Service Number:	<input type="text"/>

As in other accounts, you may redirect calls to the auto attendant to another account depending on the time of day or other events. This service is called "night service" and is used in conjunction with the Service Flag. If you want to use the night service feature, please set up a service flag and specify where you want to

redirect the service during the night.

6.2.4.6 Dial By Name

Dial By Name:

Input that triggers name search:

Start Search:

If you want to offer the "Dial by Name" feature in the auto attendant, you need to enter a pattern that triggers the name search. If you are using a three digit extension code, 411 is a nice example. This mechanism searches only extensions that have their name set.

The setting "Start Search" tells the PBX how many digits it should read until it starts the search. If there are several matches after a timeout or further entries will not get a unique result, the PBX will list the available matches in a menu. The caller may always cancel the search with the star key.

6.2.4.7 Direct Destinations

Direct Destinations:

User Input:		Destination:
<input type="text" value="1"/>	Sales	<input type="text" value="511"/>
<input type="text" value="0"/>	All other inquiries	<input type="text" value="520"/>
<input type="text"/>	No playback	<input type="text"/>
<input type="text"/>	No playback	<input type="text"/>
<input type="text"/>	No playback	<input type="text"/>
<input type="text"/>	No playback	<input type="text"/>
<input type="text"/>	No playback	<input type="text"/>
<input type="text"/>	No playback	<input type="text"/>
<input type="text"/>	No playback	<input type="text"/>
<input type="text"/>	No playback	<input type="text"/>

Save

You can specify direct destinations. When the user enters the destination, the PBX will call the provided number. The input can be one digit or it can be several digits. The destination can be an internal number such as an extension or

conference room, or it can be an external number.

The PBX has some prerecorded announcements that will be read out along with the direct destination. This makes it much easier to set up an auto attendant that explains the available choices to the caller.

If you want that the auto attendant does not offer direct dialing of extensions, enter a "*" into the setting "Accounts that cannot be called".

6.2.5 Conferencing

6.2.5.1 General

The conference account is a simple conference mixer. It can not compare to the dedicated conference solutions that support white boarding, video, speaker management and so on. However, you can easily establish conferences with a reasonable number of participants.

To enter a conference, you just have to dial the conference account number. The number is also available from a trunk, and you can go into a conference through the auto attendant.

If you want to bring someone into a conference, you can establish a call to the participant as a regular call and then blind transfer the call into the conference account.

6.2.5.2 Settings

Identity:	
Primary Name:	<input type="text" value="714"/>
Alias Names:	<input type="text"/>
<hr/>	
Authentication:	
Dialog Permissions:	<input type="text"/>
Pin:	<input type="text"/>

The identity settings are the same as the settings for the extension identity, see Extension Identity.

The conference account offers a PIN as a simple abuse protection mechanism. If you don't set the PIN, everyone can go into the conference room. Otherwise, callers are asked for the PIN before they enter the conference. Be sure to tell your conference participants the PIN, especially before you blind transfer them into conference.

Dialog Permissions are described in Dialog Permissions.

6.2.6 Hunt Group

6.2.6.1 Purpose

A hunt groups forks a call sequential and parallel in order to locate an extension that can pick up an incoming call. If extension picks the call up, the hunt group will redirect the call to another account or an external number.

The typical use case is a central number that is being called in a company with the receptionist, secretaries and assistants on the different stages of the hunt group.

6.2.6.2 Settings

Identity:	
Primary Name:	<input type="text" value="708"/>
Alias Names:	<input type="text"/>
Name (e.g. Group 1):	<input type="text" value="Group1"/>

The hunt group names may be changed after the creation just like you can change the name of an extension (settings "Primary Name" and "Alias Names"). See the documentation about the Extension Identity.

Stages:	
Stage 1: Extensions	<input type="text" value="502 503"/> Duration <input type="text" value="10"/>
Stage 2: Extensions	<input type="text" value="501 502 503"/> Duration <input type="text" value="10"/>
Stage 3: Extensions	<input type="text"/> Duration <input type="text"/>

The hunt group supports three stages. On each stage you can list the extensions that should ring during the stage and set the duration of that stage. If you don't need a stage, leave the fields empty. In these three stages, just list the extension numbers, separated by spaces. The duration of the stage must be specified in seconds.

If all extensions of a stage should be unavailable, the PBX will immediately move to the next stage. If an extension rings both on the old and the new stage, the PBX will just let this phone keep on ringing.

Behavior:

Final Stage	<input type="text" value="708"/>
Ring Melody:	<input type="text" value="Custom 2"/>
To-Header:	<input type="text" value="Group name"/>
Additional Members of the Group	<input type="text" value="504"/>
Dial Plan for outbound calls:	<input type="text" value="Standard International"/>
Dialog Permissions:	<input type="text"/>

If all stages fail and the setting "Final Stage" is set, the hunt group will go to this destination. In contrast to the other stages, in this stage you can use only one number. Typically this destination will be an auto attendant that will ultimately give the caller the possibility to get someone on the phone. But the destination can also be an external number; therefore the hunt group has a selection field for the "Dial Plan for outbound calls" that should be used for outside calls.

You may select a ring melody that is used for the hunt group. Phones that support the SIP Alert-Info header will change their ring tones, so that you can hear by the tone that the hunt group is being called.

When a phone rings because of a call from a hunt group, the called person wants to know who is calling. There are three modes available:

- "Called Number" displays which number was called. This is typically the hunt group, but for redirected calls it can also be another number.
- "Group Name" always uses the group name of the hunt group, even if the call has been redirected to this group.
- "Group name with called number" shows both strings concatenated.

The setting "Additional Members of the Group" is used to list other extensions that are intrinsically allowed to pick up calls for this hunt group. They are never called directly.

Dialog Permissions are described in Dialog Permissions.

Night Service:

Service Flag Account:	<input type="text" value="714"/>
Night Service Number:	<input type="text" value="19786544543"/>

If you like to use "Night Service", you must define a "Service Flag" first. The hunt group will use the status of the service flag to determine where to send the call. If the flag is set, the hunt group will redirect the calls directly to the "Night Service Number", which can be an internal account or an external number.

6.2.7 Agent Group

6.2.7.1 Purpose

You may use an Agent Group to queue the incoming calls and dispatch them automatically to a list of agents. Typical scenarios are sales and support teams which have a homogeneous skill profile. The members of this group are called "agents".

Within one agent group, there may be at most one call in ring back state. All other calls are queued until the ringing call gets connected and at least one agent is or becomes available. Even if there are several agents available, the queue will have only one caller in the ringing state.

The agent group keeps track which extensions are busy and which agents are available. When an agent becomes available, the PBX automatically takes the next waiting call out of the queue, rings the agents and puts the call in ring back state.

Agents can be logged in or out. If they are logged out, the PBX will not dispatch calls to an agent group to them, but it will include them in regular calls and calls to hunt groups.

6.2.7.2 Settings

Identity:	
Primary Name:	<input type="text" value="709"/>
Alias Names:	<input type="text"/>

The Agent Group names may be changed after the creation just like you can change the name of an extension (settings "Primary Name" and "Alias Names"). See the documentation about the Extension Identity.

Behavior:	
Agents	<input type="text" value="503 504"/>
Ring Melody:	<input type="text" value="External Call"/>
Redirection timeout (s):	<input type="text" value="30"/>
Redirection target:	<input type="text"/>
Dialog Permissions:	<input type="text"/>
Accounts that may record a message:	<input type="text" value="501 502"/>
Gap between announcements (s):	<input type="text" value="20"/>
Agent recovery time (s):	<input type="text" value="2"/>
Call rate limitation (e.g. 2/10)	<input type="text" value="5/5"/>
Dial plan for outbound calls:	<input type="text" value="Domain Default"/>

The agents must be extensions and must be listed (separated by space) in the "Agents" setting.

You may leave the "Agents" setting also empty. In this case, you must manually pull the waiting callers out of the queue, for example by calling the call pickup star code. This mode is useful when your agents are more important than the callers and it should be the agents.

The "Ring Melody" specifies what melody should be used when a call comes in for this agent group.

If a caller leaves a queue, this is no guarantee that the call will be connected. For example, none of the selected agent picks up the phone. To resolve these situations, you may specify a "Redirection timeout (in seconds)" and a "Redirection target". The target may be any dial able number according to the dial plan of the group (see "Dial plan for outbound calls "). The PBX will then redirect the call to the provided number.

When callers are in the queue, they hear music on hold mixed with announcements. The PBX reduces the volume before playing an announcement and increases when it is finished. You may choose music on hold source in the domain settings.

To record an announcement, just dial the recording code followed by another star and the announcement number. For your convenience, you will find these codes at the bottom of the account page. You may specify which accounts may record announcements with the setting "Accounts that may record a message" as a list of Wildcard Patterns. If you leave this setting is empty, all extensions will have this permission.

You may record up to ten announcements. The announcement number "0" is always played when a caller enters the queue, regardless of the number of callers waiting in the queue ("welcome message"). The other announcements "1"- "9" are played in a round-robin fashion.

The "Gap between announcements (s)" tells the PBX how many seconds the PBX should wait between the announcements.

In large agent groups, it is problematic to call all agents at the same time. Therefore, the PBX allows the limitation of calls per second in the setting "Call rate limitation". The syntax for this setting is how many agents are being called in what time period. For example, 2/10 means it will call two (more) agents in ten seconds intervals.

When an agent finished a phone call, it is annoying if the agent gets a new phone call right after the termination of the last call. Sometimes it is even problematic because the SIP phone will not accept an additional call while the last one is being shut down. Therefore, the PBX has a setting called "Agent recovery time". It will make sure that the agent has at least the provided time for recovering from the previous call. In busy call centers, you might make this a short value like two seconds, if you want to give the agent the chance to make some quick notes, you might choose a longer value like one minute (60 seconds). Also, the agent has the opportunity to log out during this time.

Dialog Permissions are described in Dialog Permissions.

6.2.7.3 User Input

User Input Handling	
Key 0:	<input type="text"/>
Key 1:	<input type="text"/>
Key 2:	<input type="text"/>
Key 3:	<input type="text"/>
Key 4:	<input type="text"/>
Key 5:	<input type="text"/>
Key 6:	<input type="text"/>
Key 7:	<input type="text"/>
Key 8:	<input type="text"/>
Key 9:	<input type="text"/>

When the caller is in the queue, he may leave the queue and move to another destination by pressing a key. You just need to specify the destination to enable this feature.

6.2.7.4 Night Service

Night Service:
Service Flag Account:
Night Service Number:

If you like to use "Night Service", you must define a "Service Flag" first. The agent group will be the status of the service flag to determine where to send the call. If the flag is set, the agent group will redirect the calls directly to the "Night Service Number", which can be an internal account or an external number.

6.2.7.5 SOAP Interface

SOAP Interface:
Queue Status URL:
Agent becomes available URL:

If you want to use external logic to control the queue behavior, you might want to use the SOAP settings. Please see the SOAP web page about this topic.

6.2.7.6 Agent log-in and log-out

When an agent does not want to receive calls, he should call the DND star code. It is not recommended to use the local DND button on the phone, because the PBX will then try to send the call to the agent and put the call into the ringing state.

6.2.7.7 Queue Status

Currently in queue 709

From	To	State	Time
2125648534	704	Waiting	0:15
9785445645	704	Waiting	1:53
7144534534	704	Waiting	2:15
4154534536	704	Waiting	5:54
6546465454	704	Waiting	8:23
9784564569	704	Ringing	10:43
2124324237	704	Connected	12:12
4545645645	704	Connected	13:24

The web interface has a queue status tab which lists the callers in the queue. This list is refreshed every ten seconds. Some call centers display this web screen on a projector in the room, so that all agents can see how busy the queue is.

6.2.8 Calling Card

6.2.8.1 Purpose

The calling card account makes it possible to place outbound calls from the PBX without being logged in as extension. For example, if you are traveling and you want to place a call to an international number, you might call into the PBX, enter your extension number, your PIN code and then you can place an outbound call from the PBX. The call will show up in the call log under your account. Typically, this way you can save a lot of money for expensive international cell phone calling and you can present the caller ID of your office.

The calling card account can also be used with an external database, so that you can provide this service also to customers who buy a prepaid or postpaid calling card from you. Typically they dial into a free of charge-number which goes into the calling card account. The PBX uses the SOAP interface to talk to an external application server which manages the calling cards and the amount of money which is left in them. When the call is over, the PBX will report the call duration to the server.

6.2.8.2 Settings

Identity:
Primary Name:
Alias Names:

The calling card names may be changed after the creation just like you can

change the name of an extension (settings "Primary Name" and "Alias Names"). See the documentation about the Extension Identity.

Behavior:

Dial Plan:

Caller-ID: Show Block

Dialog Permissions:

Every outgoing call on the PBX needs to use a dial plan. If the PBX uses the SOAP interface for placing outbound calls, it needs to know which dial plan to use. If the PBX uses the internal database, it uses the dial plan of the selected extension.

The setting "Caller-ID" determines whether to show the caller-ID on outgoing calls. If the caller-ID is shown and the call is started on behalf of a known extension, it will use the caller-ID associated with that extension. If the SOAP interface is being used, the PBX will show the caller-ID of the calling card account.

Dialog Permissions are described in Dialog Permissions.

6.2.8.3 Application Server

Application Server:

Number of digits for calling card ID

6.2.9 Paging

6.2.9.1 Purpose

Paging means a one-way audio communication from one caller to a potentially large group of listeners. Typical applications include supermarkets, hospitals or trains. You may have several paging groups on one PBX that addresses different audiences. For example, you might have one paging account that calls a specific floor of the building, and you might have another group that pages the whole building.

Intercom is a potentially two-way communication between two participants. Intercom is controlled by the feature codes Intercom. In the previous version of the PBX, those two features were both in the paging group. In this version, they have been separated.

There are two ways to implement paging. The first way establishes regular calls to the paging recipients by using standard SIP calls (indicating that the call

should be immediately connected by auto answer). This method works with most available SIP phones and there is also special equipment available that works as an overhead paging speaker. However, when the paging groups become bigger, it puts a lot of performance load on the PBX CPU.

Therefore the PBX offers a second paging mode, which just sends the RTP traffic to a predefined RTP IP address. Typically this is an IP multicast group. Phones and other overhead paging equipment will subscribe to that multicast group and go to paging mode as soon as they receive RTP traffic on this port. Using this method, you can build up very large paging groups with hundreds and thousands of speakers distributed in the organization.

6.2.9.2 Identity

Identity:	
Primary Name:	<input type="text" value="713"/>
Alias Names:	<input type="text"/>

The paging account names may be changed after the creation just like you can change the name of an extension (settings "Primary Name" and "Alias Names"). See the documentation about the Extension Identity.

6.2.9.3 Unicast Mode

Members:	
Streaming Mode	<input type="text" value="Unicast (SIP)"/>
Destination:	<input type="text" value="501 502 503 504"/>
Source:	<input type="text" value="502"/>
Display Name:	<input type="text" value="PA"/>
Dialog Permissions:	<input type="text"/>

In unicast mode, you can list the destination extension numbers in the setting "Destination". Please be careful with the paging group size. The PBX must initiate a call to all of the listed extensions, and this may take significant CPU and bandwidth resources. Unicast paging is not limited to the local area network; all extensions that are connected to the PBX can be paged, no matter where they are located.

You must list the extensions that are allowed to page this group in the setting "Source". If you want to give access to all extensions, you may put a star into that field.

The "Display Name" will be used as the source of the call, so that the SIP phones will show this text in the display during the paging.

Dialog Permissions are described in Dialog Permissions.

6.2.9.4 Multicast Mode

Members:	
Streaming Mode	Multicast <input type="button" value="v"/>
Destination:	224.0.1.75:1234
Source:	*
Dialog Permissions:	

In multicast mode, you must specify one IP address in the form x.x.x.x:n (IP address with port). You can use only one IP address. You can either specify a regular IP address or a multicast address (for more information about multicast, see http://en.wikipedia.org/wiki/IP_Multicast).

The meaning of the "Source" and the "Dialog Permission" are the same as in unicast mode.

6.2.10 Service Flag

6.2.10.1 Purpose

The Service Flag account type is a simple account that is used to indicate a condition to the PBX. The service flag is for example useful to indicate if a hunt group or an auto attendant should be active or not (night service).

A service flag is independent from other accounts. That means you can use one service flag for several accounts, like auto attendants and hunt groups.

The service flag can be controlled manually or automatically. In manual mode, you need to call the service flag number to change its state. The PBX will then play back an announcement about the new state.

In automatic mode, the PBX will use a fixed scheme to turn the flag on and off. See the description below on how to do this.

You can subscribe to the state of a service flag. This way, your phones can display if the service is active or not. Typically, you can put the state of a service flag on a LED key. From the phone point of view, the service flag is like an extension.

6.2.10.2 Settings

Identity:	
Primary Name:	<input type="text" value="701"/>
Alias Names:	<input type="text"/>
Description:	
Mode	<input type="text" value="Day/Night"/> ▼
Display Name	<input type="text" value="Night Mode"/>
Dialog Permissions:	<input type="text"/>
Monday	<input type="text" value="9:00-12:30 1:00P-5:00P"/>
Tuesday	<input type="text" value="9:00-12:30 1:00P-5:00P"/>
Wednesday	<input type="text" value="9:00-12:30 1:00P-5:00P"/>
Thursday	<input type="text" value="9:00-12:30 1:00P-5:00P"/>
Friday	<input type="text" value="9:00-12:30 1:00P-3:00P"/>
Saturday	<input type="text"/>
Sunday	<input type="text"/>
Holiday	<input type="text" value="12/24 12/31"/>

The identity settings are the same as the settings for the extension identity, see Extension Identity. The "Display Name" is just used in the web interface and serves as a comment on the purpose of the service flag.

The "Extensions that may change status" lists, separated by space, the accounts that may change the status of the service flag. You may use wildcard patterns here, for example 9* would allow all extensions that start with a 9 to change the status of the service flag. If you leave this setting empty, all accounts may change the status of the flag. This setting is only visible in manual mode.

The "Dialog Permissions" are described in a separate page; see Dialog Permissions.

In the Day/Night mode, it will automatically change the status of the code. For every day, you need to list the times when the service is active. Every segment must be separated by a space. The service times are using the format HH:MM-HH:MM, you may use the symbol "P" for PM or use the 24-hour format. For example, "9:00-12:30 1:00P-5:00P" would mean that the service is active between 9 AM and 12:30 PM and between 1 PM and 5 PM.



Please note that there must be no space before and after the dash symbol for a time entry (e.g. "9:00-14:00" instead of "9:00 - 14:00").

Holidays are written in the format Month/Day, you may also use any number of holidays (for example, "12/24 12/25 12/26"). Use a space to separate the holiday dates. Holidays repeat every year, if you have a holiday that happens only on a specific year, you need to change that setting for every year.

6.2.11 IVR Node

6.2.11.1 Purpose

When caller hits an IVR node, the PBX will playback the prompt for that IVR node and the user can enter DTMF digits that determine where the PBX will continue processing input. Usually you use that feature as an "entry door" into the system where you decide what to do with a caller. For example, you can ask for a customer number, then ask an external application server what to do with that customer and then route the customer to one of the waiting queues.

If you define a dialog, that dialog may consist of a number of IVR nodes. Each node plays one prompt and asks one specific question to the user. For example, the first prompt may ask you what language you prefer and then dispatch you into two different node systems for two different languages.

This IVR Node mechanism is very flexible. You can either process the input internally in the PBX or use an external application server to decide where to go. In the simplest case, you just do a static routing depending on the user input, without consulting the external server.

The IVR Node account collects user input according to the list of ERE expressions that was entered in the "Match List" of the node.

6.2.11.2 Recording a Message

There are two ways to get a message into an IVR node.

- Either you record the message directly into the node by using the record star code followed by the account number (e.g: *98123 for recording the prompt for account 123). This method is suitable for quick setup and for changing messages.
- The other method is to use WAV files. This way, you can record and edit your message and then later load it into the system. If you use this method, you can set up professional IVR dialogs.

IVR messages are always static. It is not possible to generate dynamic content.

6.2.11.3 Settings

Identity:

Primary Name:

Alias Names:

Settings:

WAV File*:

DTMF Match List:

From-based routing match list:

To-based routing match list:

SOAP URL:

Accounts that may record a message:

Dialog Permissions:

* When uploading a WAV file, please use 8 kHz Mono, 16 bit files. Note that you can also record a message by dialling *98712.

The identity settings are the same as the settings for the extension identity, see Extension Identity. Dialog Permissions are described in Dialog Permissions.

To record an announcement, just dial the recording code followed by another star and the announcement number. For your convenience, you will find these codes at the bottom of the account page. You may specify which accounts may record announcements with the setting "Accounts that may record a message" as a list of Wildcard Patterns. If you leave this setting is empty, all extensions will have this permission.

When the caller enters a digit, the PBX appends that digit to the input for that IVR node. The input string is cleared when the IVR node is being called (also when coming from another IVR node). When the IVR node audio announcement ends, the PBX acts as if the user entered a "E" DTMF digit.

The "DTMF Match List" contains a list of match patterns that are checked. The list elements are separated by space. Each pattern contains of two fields. The fields are separated by any character that does not occur anywhere else in the string, for example "!". The first field contains the extended regular expression and the second field the replacement. The field has the same meaning as the fields in the dial plan. The second field contains the destination.

The destination may be any dial able number. If the number requires a dial plan, the default dial plan of the domain will be used. If the destination field is empty and the pattern matches, the PBX will disconnect the call.

A simple replacement where the caller enters "0" and is sent to extension "500" would be "!0!500!". An example pattern that waits until a user has entered three digits and then returns the three digits would look like this: "!^(0-9){3}\$!\1!".

The other two fields, "From-based routing match list" and "To-based routing match list" are used in the beginning. If there is a match with the "From" or the "To"-header of the call, then the IVR node immediately switches the destination without playing the WAV file. This way, you can implement flexible routing schemes.

If no SOAP URI is specified in the account, the PBX will take the output of the pattern matching as the name of the account to switch to. If the SOAP URI is available, it will pass the destination to the application for further decision what to do with it. See Linking External Application Server to an IVR Node for more information about the SOAP processing.

6.3 Trunks

6.3.1 Existing Trunk List

6.3.1.1 Purpose

Trunks are used to receive or send calls to devices that are not registered with the PBX. The name trunk comes from the idea that there is a physical connection between the PBX and the external device, like it used to be with traditional PBX.

In general, there are three types of trunks:

- Registrations. The PBX registers somewhere else and itself like an extension. This model is typically used when you have an account with an Internet Service Provider and you use this account for terminating your traffic. In this model, the PBX uses the number of the registration as caller-ID, regardless what extension is actually using the trunk. You can use this mode if the service provider supports SIP soft- or hard phones.
- Gateway. The gateway model does not register; it just sends the traffic to the destination. In this model, the PBX uses the caller-ID of the PBX to indicate the extension that initiates an outgoing call (if that extension did not turn block caller-ID on). This model is typically used with customer premises PSTN gateway hardware.
- Proxy. The proxy model is similar to the gateway model. The difference is the way anonymous calls are made and how the proxy represents its own domain. As the name suggests, the proxy model assumes that you are talking to a SIP proxy, while the gateway model assumes that you are talking to a SIP user agent. However, the two models are quite similar.

Trunks are usually in scope of a domain. But you can also make a trunk visible in all domains. For example, if you want to share a PSTN gateway amongst all domains, you would set up a trunk in a separate domain and make it visible to all domains.

6.3.1.2 Existing Trunks

Name	Status	Edit	Delete	Action
External Voicemail				
ITSP 1	404 Not found (Registration failed, retry after 60 seconds)			REGISTER

New Trunk:

Name:

Type:

In the trunk list, you can see which trunks are available in the current domain. If the trunk is a registration, the PBX will show the registration status. To force a re-registration of this trunk, you may click on the register link.

To delete a trunk, you may click on the delete icon. To edit the details of a trunk, you can click on the edit icon.

At the bottom of the page you find a form for creating a new trunk. Trunk names may include alphanumeric characters and space. The system assigns a number to each trunk, so that it is ok if different domains choose the same name for a trunk.

6.3.2 Trunk Settings

6.3.2.1 Name and Type

Name:

Type:

After you have created a trunk, you may change the name and the type. The name must consist of alphanumeric characters and may contain spaces. The trunk type can be selected by a selection box.

6.3.2.2 General Parameters

Display Name:	<input type="text" value="6783979403"/>
Account:	<input type="text" value="6783979403"/>
Domain:	<input type="text" value="sipconnect-fca.atl0.cbeyond.net"/>
Username:	<input type="text" value="6783979403"/>
Password:	<input type="password" value="....."/>
Password (repeat):	<input type="password" value="....."/>
Outbound Proxy:	<input type="text" value="houston-1.vtnoc.net"/>
CO Lines:	<input type="text"/>
Dialog Permissions:	<input type="text"/>
Codec Preference:	<input type="text"/>
STUN Server:	<input type="text"/>
Keepalive Time:	<input type="text"/>
Strict RTP Routing:	<input type="radio"/> on <input checked="" type="radio"/> off
Avoid RFC4122 (UUID):	<input type="radio"/> on <input checked="" type="radio"/> off
Accept redirect:	<input checked="" type="radio"/> on <input type="radio"/> off

The "Display Name", the "Account" and the "Domain" are used to construct the address that the PBX registers. The account must be a valid SIP account identifier and the display name is used for display purposes. For example, the display name could be "Test Account", the account "test-account" and the registrar "test.com". Then the PBX would register "Test Account" <sip:test-account@test.com>.

The "Username" and the "Password" are used for authentication purposes. Some registrars use a different username for authentication; therefore the PBX includes this field as well. The password needs to be entered twice, so that accidental wrong entries can be detected.

The "Outbound Proxy" defines where requests of this trunk will be sent. If this setting is set, it will always send requests to this other address. Otherwise, the dial plan replacement field will determine where the request is being sent. However, in most cases it is better to use the outbound proxy field to make things clear.

The outbound proxy field follows the definitions of RFC 3263 ("Locating SIP Servers"). In a nutshell, you may use the DNS name for a SIP server. If you put a colon with the port number behind the name, you use only DNS A resolution.

Otherwise, the PBX will try DNS NAPTR and DNS SRV first.

The "CO-Lines" and "Dialog Permissions" settings are discussed separately in CO Lines.

If the "Codec Preference" setting is set, the PBX will use a different codec preference on this trunk. Valid codecs are "0" (G.711 u-law), "8" (G.711 a-law), "18" (G.729), "2" (G.726) and "3" (GSM). You may list the preferred codecs. The PBX will try to negotiate the first codec. If you specify only one codec, you might end up with transcoding of the speech.

Some internet service providers still require that you present a public IP address when you want to use their service. Although this way of registering and using a SIP service is quite problematic, the PBX offers a setting that uses an external STUN server to allocate a public IP address.

You can use the "STUN Server" setting in the following ways to resolve an address:

- If you just provide a DNS name, the PBX will try to locate a DNS SRV record for the STUN server. Only if that record does not exist, it will use a DNS A record
- If you explicitly specify the port number behind the DNS name for the STUN server, the PBX will only perform a DNS A lookup for the STUN server address.
- If you just provide an IP address, it will use that IP address. If you don't provide a port number, the PBX will use the default STUN port number (3478).

We recommend not to use this feature and consider a different ITSP if they do not support registrations from behind NAT.

If you specify a "Keep-Alive" time, the PBX will resend the STUN requests after the provided keep-alive time. If you use the keep-alive time setting without a STUN server, the PBX will ignore the registration time from the registrar and re-register after the provided time. This is sometime necessary when providers don't use proper solutions for keeping bindings alive.

The setting "Strict RTP Routing" is necessary, because the IETF allows that RTP traffic send ports may be different from RTP receiving ports. Because this is extremely NAT-unfriendly, today most implementations use the same port number for sending and receiving RTP. However, some gateways still insist on strict IETF compatibility. In this case you need to turn this setting on.

If your registrar does not support UUID (RFC 4122), it usually ignores this unknown additional information. However, some SIP implementations are not able to deal with UUID. In this case, they will report a "Bad Request" to indicate that they were not able to process the request. We added the option "Avoid RFC4122 (UUID)" to explicitly suppress the UUID in REGISTER requests. The UUID is used to indicate that a registration replaces another registration; this is useful to avoid double registration after a restart of the system.

The setting "Accept redirect" is necessary if your trunk should respect

redirect codes. By default, this introduces significant security risks, because the PBX cannot determine if these redirects introduce additional costs (redirection to expensive numbers). Therefore, you should turn this flag on only if you are sure that your service provider does not abuse this feature.

6.3.2.3 Outbound Settings

Prefix:	<input type="text"/>
Visible in all dial plans:	<input type="radio"/> yes <input checked="" type="radio"/> no
Explicit Remote-Party-ID:	<input type="text"/>
Privacy Indication:	<input type="text" value="No Indication"/>
Failover Behavior:	<input type="text" value="No failover"/>
Is Secure:	<input type="radio"/> yes <input checked="" type="radio"/> no

If you have a block of caller-ID for outbound calls, you may just put a number in front of the extension number ("Prefix"). This is typically the case in European installations. For example, if you put a "0049228123456" in this setting, calling from extension "123" will result in the caller-ID "0049228123456123".

You may decide if this trunk should be visible also in other domains. If you turn the setting "Visible in all dial plans" on, this will be the case.

The setting "Explicit Remote-Party-ID" and "Privacy Indication" are discussed in Outbound Calls on Trunk.

When the trunk receives an error code, it may send the call back to the dial plan and continue the matching process. This is useful when this trunk is just a "trial" to place the call, for example when several PSTN gateways are available for terminating the call and one gateway does not accept any more calls. Another example is when you first try to route the call via a peer-to-peer call using ENUM or other location methods and only if such resolution does not result in a connection fall back to a PSTN call. The setting allows three behaviors:

- Never failover. That is the default behavior. In this case, the caller will receive the error code as the result of the call attempt.
- On all error codes. In this case, all error codes will trigger the failover process. Note that also call redirect will be treated as a error code, as the redirection destination can easily be abused to route calls though expensive routes.
- Only 5xx error codes. This will trigger failover only when a 5xx or 6xx class error code is being received. PSTN gateways typically return 5xx class error codes when all channels are in use, and using this mode you can switch to the next PSTN gateway only in this case, while a caller busy will not trigger the failover.

The Is Secure flag is available in the professional version and is used to indicate that outbound calls on this trunk can be treated as secure calls. For

example, when the trunk goes to a local PSTN gateway you might decide to treat this call as a secure call. In the professional version, incoming calls with the sips scheme ask the PBX to ensure that the call should be kept secure end-to-end.

6.3.2.4 Inbound Settings

Extension:	<input type="text"/>
Ringback:	<input type="radio"/> Message 180 <input checked="" type="radio"/> Media

The setting "Extension" is discussed in the section Inbound Calls on Trunk.

The "Ringback" feature was introduced to deal with network operators that are obviously not able to deal with early media. Using the 180 Message simplifies the signaling in forking calls scenarios, however, it means additional delay when the called party picks the handset up and the first samples on the conversion may not be transported. We strongly recommend leaving the flag to the Media state, which is default and ask the operator to fix their problems with early media.

6.3.3 Inbound Calls on Trunk

6.3.3.1 How the PBX identifies the trunk

When a new call is requested from the PBX, it must find out if the call is being initiated from a known extension or from a trunk. It does this in the following way:

- If the Request-URI contains the line parameter, it is clear which trunk is called. The line parameter is set by the PBX when the trunk is registered. The support of the line parameter must be supported by RFC-compliant components. Most SIP devices today are RFC compliant, so that you usually do not have a problem if the parameter is present. However, for gateways and proxies this method is not possible, therefore the PBX must continue searching the trunk if the line parameter is not present.
- The PBX determines to which IP addresses and ports a trunk may send requests. This is done by a recursive DNS-resolution of the outbound proxy of that trunk. The outbound proxy is used as "inbound proxy" as well. The PBX then tries to find trunks with the following priority:
 - o The incoming call matches a domain name of the trunk and a IP address and port of the outbound proxy of that trunk
 - o The incoming call matches a domain name of the trunk and a IP address of the outbound proxy of that trunk
 - o The incoming call matches a IP address and port of the outbound proxy of that trunk
 - o The incoming call matches a IP address of the outbound proxy of that trunk
 - o The incoming call matches a domain name of the trunk

The domain name "localhost" matches any domain name presented in the Request-URI, as usual.

If the From-header identifies an extension on the PBX, the trunk identification will be cancelled and the PBX assumes that the call comes from that extension, no matter if the extension is registered on the perceived IP address or not.

6.3.3.2 How the PBX identifies the extension

After the trunk has been identified, the PBX must determine where to send the call inside the domain. For this purpose, the PBX uses the setting "Extension" in the trunk. The PBX writes a log with the message "Trunk sends call to ..." into the log file (log level 5). There are two modes for this job. The simple mode just looks the extension up and the extended mode uses patterns to identify the destination.

6.3.3.2.1 Simple Mode

In the simple mode, the extension is just the user-part of the Request-URI. For example, if you want to send all calls on this trunk to a specific auto attendant, just put the name of the account into the extension setting.

If you set tel: alias to an account, you can easily set up the necessary information to map an extension to a DID. For example, an extension might have a primary name of "123" and an alias name of "tel:8124353423".

6.3.3.2.2 Extended Mode

In the extended mode, the extension setting must consist of the following four parts in the form <delimiter> <pattern> <delimiter> <replacement> [<delimiter> [<flag> [<delimiter> [<default>]]]] (for example, ![0-9]{7}([0-9]{3})!\1!). The parts must be separated by any unique character which is not used elsewhere in the setting string (for example, an exclamation mark).

- The "pattern" is an extended regular expression which is matched against the user part of the Request-URI (or the To-header if you use the t flag below). This pattern uses the same mechanism as the dial plan.
- The "replacement" tells the PBX which extension to dial. It also uses the same mechanism as the dial plan. Typically it will reference matches from the pattern with \1.
- The flag tells the PBX whether to look into the Request-URI ("u") or into the To-header ("t"). The default is "u". Some Internet service providers provide the destination information in the To-header, although SIP recommends to use the Request-URI. Please note that you cannot just put two delimiters without anything in between, therefore if you want to specify a default you must use either the "u" or the "t".
- If the PBX cannot find the extension, you may specify a default extension. This extension must exist and it will be chosen in case that the replacement pattern does not produce an existing extension.

Please note that you may have more than one expression. The PBX will try to match the expressions until it finds a match. If no match is being found, the default extension of the last pattern will be used.

6.3.3.2.3 Locating Global Extensions

After the extension was identified, the PBX might find out that the extension is actually in a different domain than the trunk is. This can happen if the extension has a tel: name. In this case the call will be taken into the destination's extensions domain.

6.3.3.3 Examples

- The first example is common in Europe. You want to strip the main number of the PBX and use the remaining numbers to identify the extension. If the extension is not found, you send it to the auto attendant. The example assumes that the number starts with 7 digits (e.g. 0228123) and that the auto attendant is located at 100: `"![0-9]{7}([0-9]*)!\1!t!100"`.
- The second example always uses the last 4 digits of the number, no matter how long it is: `"!([0-9]{4}$)\1!t!100"`. This example assumes that the number of digits is always the same.
- In a typical US office, you send all calls to an auto attendant. Then the value for the extension is very simple: Just use the string "100" if the auto attendant is located on account 100.
- If you are using tel: alias names for accounts, you can leave the Extension field just empty and just match the DID number to a tel: alias.

6.3.4 Outbound Calls on Trunk

6.3.4.1 Caller-ID Presentation

When you place an external call, the PBX will try to present your caller-ID. In SIP, the caller-ID is presented in additional headers that differ from the From-header. The reason is that the ITSP must know which account stands behind the ANI, so that the billing goes to the right account.

Usually you want to use a two or three digit extension number and provide a ten or eleven digit ID when you place an outbound call. In that case, you would choose the short digit code as primary extension number and the tel:-alias (e.g. "tel:12121234567") as one of the alias names.

6.3.4.2 Explicit Remote-Party-ID

In the trunk, there is a setting called Explicit Remote-Party-ID. You can put into this setting whatever you would like to present as the caller-ID. If you just put a number there, the PBX will automatically copy the domain name from the From-header.

In addition to that, you can include special characters that will be replaced

with dynamic content:

- '1' will insert the first user parameter from the account
- '2' will insert the second user parameter from the account
- 'u' will insert the canonical user name of the caller
- 'a' will insert the first tel:-alias of the account
- '\$' will insert a dollar sign

For example, you can use the string "\$a" if you are using tel:-alias names for inbound account identification. Then the PBX will automatically use that identification for outbound calls. If you explicitly want to specify the ANI for every account, you can use one of the two account parameters.

You can specify a list of possible Explicit Remote-Party-ID (separated by space). Then the PBX will try to expand the first, and if that fails, it will move on to the next and so on. For example, if you want to try the first tel:-alias and then fall back to a hard coded ANI, then you could use the pattern "\$a 12121212121".

6.3.4.3 Interoperability Issues

There are several methods to indicate the ANI. These methods originally had the purpose to deal with anonymous callers that want to hide their true identity in the From header, therefore you find these settings in the "Privacy Indication" indication.

- RFC 3325 is the IETF standard for this purpose. It uses the header "P-Preferred-Identity" which explicitly states which identity to use. The support for this standard by the ITSP is good and getting better every day.
- There is an old proposal by Cisco Systems called "Remote-Party-ID" from a time when there was no agreed standard. It is still quite popular and if the RFC method does not work, sure worth a trial.
- Some operators do a mix of the RFC 3325 method and their own interpretation of the standard. Use the "RFC3325, but don't hide" method only if your operator tells you to do so.
- By default, the PBX does not present the ANI. Therefore, you must select either of the above methods in order to have this feature working.

If you would like to use ENUM for routing outbound calls, please see ENUM for more information.

6.3.5 CO Lines

6.3.5.1 Purpose of CO-Lines

In TDM-based PBX, there were a number of physical lines connecting the PBX with the public telephone network. These lines were called "CO-lines".

It is interesting to see what calls are active on the CO-lines. Over the centuries that PBX have been used, office users got used to CO-lines and they do

expect at least the same behavior from a modern SIP-based PBX.

In SIP, there are no more physical cables used to connect the PBX with the outside world. However, it is still interesting to see which calls are active between the PBX and the outside world. Therefore, the pbxnsip emulates the behavior of the TDM-based PBX.

CO-lines are associated with trunks. Each trunk may have several CO-lines. Because users can subscribe to the state of the CO-lines, their name must be unique in the domain like for all other accounts.

For example, you can set up four CO-lines on Trunk1 with the name "co1 co2 co3 co4" and more CO-lines on Trunk2 with different names like "co5 co6 co7 co8" (the list of CO-lines must be separated by space). The PBX will reject names for the CO line that are already used by accounts or other CO-lines in the same domain. The CO-lines are listed in the account list, because they share the same namespace.

6.3.5.2 Limiting inbound and outbound traffic

Having a limited number of CO-lines can be used to limit the number of calls that can be assigned to a trunk. When the CO-line setting is used, the PBX will reserve one of the line for each call. When all lines are in use, the PBX will reject further calls that would use the CO-line.

Sometimes it makes sense to reserve lines exclusively for inbound or outbound traffic. If you put a "i" behind the line name, the PBX will use that line only for inbound traffic (e.g. "line1:i"); if you put a "o" behind the line name, the PBX will use that line only for outbound traffic. If there is no attribute set after the colon, the line will be available for inbound or outbound traffic.

6.3.5.3 Monitoring CO-Lines

In most small offices, transfers are being done by parking and picking up calls from lines. In order to be able to do this, it is necessary to display on the phones which call is on which CO-line.

From a PBX point of view, the status of a CO-line is similar to the status of an extension: It may be idle, connected, ringing, on hold or there might be a call being parked. Therefore, the mechanisms to see the status of a CO line are similar to the mechanisms to see the status of an extension. This implies that the name of the CO-line must not clash with the name of an extension or any other account on the system.

In order to see the CO-line status, the user agent needs to subscribe to the status of the CO-line. See the description of the phones on how to do this.

6.4 Dial Plans

6.4.1 Dial Plan List

6.4.1.1 Purpose

Each domain may have zero, one or more dial plans. Dial plans are used when an extension dials a number that is not available on the local PBX. You can assign the dial plan per extension. This gives you the possibility to assign different permissions to the extensions. For example, you might want to have a "Local" dial plan that handles only local calls and an "International" dial plan with permission to make international calls.

Dial plans are not used to control the PBX. For this purpose, each domain has a list of star codes.

6.4.1.2 Create Dial Plan

Name	Edit	Delete
Only emergency calls		
Only local calls		
Standard International		

New Dial Plan:

Name:

To create a dial plan, just enter the name in the creation box in the "Show List" link for the dial plans. The name may be any descriptive name; you may include spaces and capital letters.

The list shows the available dial plans. If you want to delete a dial plan, click on the delete symbol and all dial plan data will be lost. If you click on the edit button, you can set up the details of the dial plan.

6.4.2 Dial Plan

6.4.2.1 Edit Dial Plan

The dial plan consists of four components:

- The preference is used to sort the dial plan entries. When the PBX searches a matching entry in the dial plan, it will take the entry with the lowest preference value. You may use the same preference value for several entries; in this case

the PBX will pick one of the entries for you.

- The Trunk setting defines which trunk is used for the call.
- The pattern setting is matched against the destination of the call. See below for the description of the matching algorithm.
- The replacement is used in the To-header as well as in the Request-URI. See the description below.

Pref Trunk		Pattern	Replacement
100	PSTN Gateway		
100	PSTN Gateway	911	
110	PSTN Gateway	9978xxxxxxx	
120	PSTN Gateway	9xxxxxxxxxx	
130	ITSP	9011*	

Save

6.4.2.2 Simple Dial Plan

In most of the cases, you can use simple patterns.

- Literals. If you want to match a specific number (e.g. 911), just put that number there. The literal will be the first match in the expression.
- Prefixes. If you want to match a specific prefix, put that prefix there with a star behind it. For example, "9*" would match all numbers that start with a 9. The prefix will not be part of the match, only the string matched by the * will be the match of the first expression.
- Fixed patterns. If you use a "x" in a pattern, the PBX will treat it as a wildcard for 0-9. For example, 978xxxxxxx will match any number with the area code 978.

If you use the simplified expression, you don't have to specify a replacement. The PBX will automatically put a "sip:\1@\r;user=phone" as the replacement. There is also a simplified replacement. If you put a prefix in front of a star, the PBX will insert that prefix before the match. For example, "1*" will put a "1" in front of the match.

Examples:

- Pattern "91*" and replacement "1*": If the input is "919781234567@domain.com", the output will be "19781234567@domain.com"
- Pattern "978xxxxxxx" and no replacement: If the input is "9781234567@domain.com", the output will be "9781234567@domain.com"
- Pattern "911|411" and no replacement: This will match input "911@domain.com" and "411@domain.com".
- Pattern "xxxxxxx" and a replacement of "234xxxxxxx" will insert the area code

of 234 to the 7 digit number and input "234xxxxxxx@domain.com"

6.4.2.3 Regular Expression Matching

The regular expression matching algorithm is a very flexible algorithm that follows the NAPTR algorithm of RFC 2915. For an exact description, please refer to this document.

The pattern string of the dial plan is surrounded by a "^" and a "\$" (to make sure that the whole string is matched". The PBX uses the username and the hostname. The port number, parameters and the scheme are not included for the comparison.

If there is a match, the PBX will generate the resulting destination from the replacement string. The string may include references to matching groups in the pattern string. These matches are referred by the group number (starting with 1). Additionally, the matching string 'r' may be used to insert the registrar name.

Technically, that is the description of the algorithms. The example in the next section will make the algorithms more understandable.

To delete a dial plan entry, just clear the pattern and the replacement and press the Edit button.

6.4.2.4 Examples

6.4.2.4.1 Typical dial plan

A typical example is the string `([0-9]*)@.*` as pattern and `sip:\1@\\r;user=phone` as the replacement. The pattern string has one group `[0-9]*`, which is referred in the replacement string as `\1`. That means, if the pattern is matched against the value `2121234567@test.com`, it will store `2121234567` in the first group and the result will be `sip:2121234567@test.com;user=phone` (the `user=phone` indicates the recipient that the number is a telephone number).

6.4.2.4.2 A very simple dial plan

In many cases, you just want to route all numbers that start with a "9" to an outside trunk. This can be done easily just by using the pattern `"9*"`; you don't need to fill anything into the replacement field (the PBX does that automatically).

Pref Trunk		Pattern	Replacement
100	LAN PSTN Gateway		
200	LAN PSTN Gateway	9*	
<input type="button" value="Save"/>			

6.4.2.4.3 Dial plan with prefix in front of the number

If you use a pattern like "1*" in the replacement field, the PBX will automatically put a "1" in front of the match which it found in the pattern field. In the case when you use the pattern "9*" and dial the number 92121234567, the PBX will automatically convert that into a 12121234567.

6.4.2.4.4 A dial plan example for North America

If you use the PBX in the fixed-length dial pal of North America, you may use a dial plan like the one below.

Pref Trunk		Pattern	Replacement
100	LAN PSTN Gateway		
200	LAN PSTN Gateway	9[911 411]	
250	WAN ITSP	9011*	011*
300	LAN PSTN Gateway	91xxxxxxxxxx	1*

Save

The first pattern matches the emergency number and the service number explicitly and sends it to the local gateway. It is a good idea to have an entry for these important numbers, so that they don't accidentally get routed to the wrong gateway.

The second pattern matches all international numbers and sends them to a special trunk, which is supposed to save you costs for international calls.

The third pattern deals with all domestic calls. We use the fixed-length pattern here, to that the PBX can actually tell when this number is complete.

You could add another pattern like 91978xxxxxxx and send those calls to another trunk if you have negotiated a flat rate with your local PSTN service provider.

6.4.2.4.5 Sending star codes on a trunk

In this case you need to fall back to the good old extended regular expressions:

Pref Trunk		Pattern	Replacement
100	LAN PSTN Gateway		
200	LAN PSTN Gateway	*([0-9]*)@.*	sip:*11@ld;user=phone

Save

The pattern matches pattern that start with a star symbol followed by any number of digits. The replacement then inserts the star again and puts the dialled

number behind the star. Alternatively, you could include the star symbol in the match group of the pattern and then you would not have to put the star in the replacement.

6.4.3 ENUM

6.4.3.1 Purpose

ENUM (see for example <http://en.wikipedia.org/wiki/ENUM>) is used to locate a service in the Internet by using a telephone number. Typically, this service is voice communication.

There are several ENUM trees available in the Internet. Several countries started ENUM trials with numbers that are publicly available. Therefore, it makes sense to be able to use different ENUM trees apart from the official e164.arpa tree.

The PBX supports ENUM by adding a special flag when resolving a SIP URI. If the parameter "enum" is set to "true" while routing a packet, the PBX will apply the RFC 2916 algorithm to the packet.

6.4.3.2 Setup

First, you need a trunk that is used for routing ENUM requests. This trunk should be a gateway trunk with no outbound proxy set. You may use other features like trunk failover as you like.

Name:	ENUM Trunk
Type:	SIP Gateway
Domain:	
Username:	
Password:
Password (repeat):
Outbound Proxy:	
CO Lines:	
Dialog Permissions:	
Codec Preference:	
Strict RTP Routing:	<input type="radio"/> on <input checked="" type="radio"/> off
Accept redirect:	<input type="radio"/> on <input checked="" type="radio"/> off
Prefix:	
Visible in all dial plans:	<input type="radio"/> yes <input checked="" type="radio"/> no
Explicit Remote-Party-ID:	
Privacy Indication:	RFC3325
Failover Behavior:	No failover
Is Secure:	<input type="radio"/> yes <input checked="" type="radio"/> no
Extension:	100
Ringback:	<input type="radio"/> Message 180 <input checked="" type="radio"/> Media

In order to use this trunk, you need to make a entry into the dial plan. This dial plan must insert the enum parameter in the replacement URI. The domain name of the URI will be used for the ENUM root location. For example, you can use the string "sip:\1@e164.org;enum=true" in the replacement field. It will use the root domain "e164.org".

Pref Trunk	Pattern	Replacement
100 ITSP 1		
100 ENUM Trunk	*	sip:\1@e164.org;enum=tru

PnP Scheme: Domain Default

6.4.3.3 Example

In this example, you can see the log messages when dialling a number on an ENUM trunk:

```
[5] 2006/10/10 11:25:37: Dialplan: Match 9420222745121@localhost to
<sip:420222745121@e164.arpa;enum=true> on trunk ENUM
[8] 2006/10/10 11:25:37: Converting phone 420222745121 into 1.2.1.5.4.7.2.2.2
.0.2.4.e164.arpa
[8] 2006/10/10 11:25:37: Resolve destination 414: enum 1.2.1.5.4.7.2.2.2.0.2.
4.e164.arpa
[8] 2006/10/10 11:25:37: DNS: Add dns_naptr 1.2.1.5.4.7.2.2.2.0.2.4.e164.arpa
100 50 u E2U+sip !^.*$!sip:echo@nic.cz! (ttl=3600)
[8] 2006/10/10 11:25:37: Resolve destination 414: enum 1.2.1.5.4.7.2.2.2.0.2.
4.e164.arpa
[8] 2006/10/10 11:25:37: Resolve destination 414: url sip:echo@nic.cz
[8] 2006/10/10 11:25:37: Resolve destination 414: naptr nic.cz
[8] 2006/10/10 11:25:37: DNS: Add dns_naptr nic.cz (ttl=3600)
[8] 2006/10/10 11:25:37: Resolve destination 414: naptr nic.cz
[8] 2006/10/10 11:25:37: Resolve destination 414: srv tls _sips._tcp.nic.cz
[8] 2006/10/10 11:25:38: DNS: Add dns_srv _sips._tcp.nic.cz (ttl=3600)
[8] 2006/10/10 11:25:38: Resolve destination 414: srv tls _sips._tcp.nic.cz
[8] 2006/10/10 11:25:38: Resolve destination 414: srv tcp _sip._tcp.nic.cz
[8] 2006/10/10 11:25:38: DNS: Add dns_srv _sip._tcp.nic.cz (ttl=3600)
[8] 2006/10/10 11:25:38: Resolve destination 414: srv tcp _sip._tcp.nic.cz
[8] 2006/10/10 11:25:38: Resolve destination 414: srv udp _sip._udp.nic.cz
[8] 2006/10/10 11:25:38: DNS: Add dns_srv _sip._udp.nic.cz 100 100 sip.nic.cz
5060 (ttl=1800)
[8] 2006/10/10 11:25:38: Resolve destination 414: srv udp _sip._udp.nic.cz
[8] 2006/10/10 11:25:38: Resolve destination 414: a udp sip.nic.cz 5060
[8] 2006/10/10 11:25:38: DNS: Add dns_a sip.nic.cz 217.31.204.193 (ttl=1800)
[8] 2006/10/10 11:25:38: Resolve destination 414: a udp sip.nic.cz 5060
[8] 2006/10/10 11:25:38: Resolve destination 414: udp 217.31.204.193 5060
[8] 2006/10/10 11:25:38: Send Packet INVITE
[6] 2006/10/10 11:25:38: SIP Tx udp:217.31.204.193:5060:
```

6.5 Status

The status information in the domain is similar to the status of the system. Please see the status description for the system.

6.6 General Topics

6.6.1 Park and Pickup

6.6.1.1 What happens when a call is being parked?

When a user parks a call, he disconnects himself from a call and puts the call onto a park orbit. The other side of the call then hears music on hold.

Parking a call is different from holding a call. In some systems, call hold behavior is called exclusive parking because only the user that holds or parks the call can retrieve the call. In SIP-based system it is better to use the term parking for the (non-exclusive) parking of a call and the term holding for a (exclusive) hold of a call because SIP was designed this way.

Every extension and every hunt group has a park orbit where several calls can be parked. When a user parks a call, he can explicitly specify where a call should be parked (e.g. *85111 parks the call on the park orbit of extension 111). If the user does not specify where the call should be parked, the call will be parked on the orbit of the extension that initiates the park operation.

6.6.1.2 Determining which call is being picked up

In most cases it is possible that there are several calls parked at the same time. This makes it necessary to define an algorithm that determines which call should be picked up. Additionally, it is also necessary to check if the caller has the permission to retrieve the call. For example, if the secretary parked an important customer on the orbit of the boss extension, not everybody should have the right to pick that call up -- accidentally or on purpose.

The PBX checks for call in the following sequence:

If the user explicitly specifies the orbit from which the call should be retrieved, then the PBX will retrieve a call that is on that orbit.

Then the PBX will check if a call was parked on the orbit of the calling extension.

After that the PBX will determined to which hunt groups the user belongs.

If a call was parked on the hunt group parking orbit the PBX will retrieve that call.

If a call was parked on the orbit of one of the hunt group members, the PBX will get that call. Starting with version, the PBX will also pick up calls from all other orbits, if the pickup policy flag is set accordingly.

6.6.2 Dialog Permissions

User agents may subscribe for the dialog state of any extension in the domain. The dialog state is typically used to control a LED on a hard phone, or list

the ongoing call on a soft phone display. By default, there is no restriction on who may subscribe to which account. However, there are cases when you want to limit the permissions to do that.

Every account has a field called dialog permissions. This field lists the extensions that may subscribe to the state of the account. If the field is empty, everyone may subscribe. Otherwise it lists the accounts that may subscribe to the state of that account. You may use Wildcard Patterns to match more than one account (e.g. 4* to allow all extensions that start with a 4).

6.6.3 Wildcard Patterns

The wildcard patterns are a simple way to match a pattern in the PBX. This pattern matching scheme is pretty simple and not as powerful as the extended regular expression (ERE) pattern matching. However, it solves most of the problems.

The wildcard pattern matching is used for example in the following places:

- Checking the permission who is allowed to page a Paging.
- The Dialog Permissions in every account use it.
- The permission to record a message in the Agent Group, IVR Node or Auto Attendant.
- The permission to change the status of a Service Flag.

The following wildcards are available:

- A '*' matches any string (with any length).
- A '?' matches any character (length one).
- A '\$' matches a single digit (length one).
- A '%' matches any number (multiple digits or empty string)
- A range enclosed in '[' and ']' matches that range.
- A '\' matches the following character.

Examples. The following examples show typical usages of the wildcard patterns.

- The pattern "9*" matches any thing starting with a 9.
- The pattern "*9" matches anything ending with a 9.
- The pattern "11[02]" matches the patterns 110 and 112.

6.6.4 IP Address List

The PBX uses in several places lists of IP addresses. This list consists of any number of strings, separated by a space. There are three forms that you can use:

- A single IP addresses in the form dots-and-number notation. For example, "192.168.23.34".
- If you want to specify a range of addresses use the form Adr/Bits, where bits is

a number indicating how many bits of the IP address should be considered. For example, the string "192.168.2.0/24" would match addresses 192.168.2.0 until 192.168.2.255.

- If you want to specify the local host, just enter the string "localhost".

The PBX does not perform a DNS resolution of the addresses.

7 User Mode

7.1 General User Settings

The screenshot shows the 'General settings for account 501' page in the pbxnsip web interface. The page has a teal header with the pbxnsip logo and navigation links: Settings, Lists, Status, Help, and Logout. Below the header is a sub-menu with tabs: General (selected), Redirection, Mailbox, Email, and Instant Message. The main content area contains a form with the following fields:

First name (e.g. John):	<input type="text" value="Jim"/>
Last name (e.g. Smith):	<input type="text" value="Smith"/>
Password:	<input type="password" value="....."/>
Password (repeat):	<input type="password" value="....."/>
PIN (e.g. 1234):	<input type="text" value="...."/>
PIN (repeat):	<input type="text" value="...."/>
Cell phone number:	<input type="text" value="9786362341"/>
When calling the extension:	<input type="text" value="Don't call cell phone"/>
Timezone:	<input type="text" value="Default Time Zone"/>
IVR Language:	<input type="text" value="Default System IVR Language"/>
Web Language:	<input type="text" value="Default System Web Language"/>
List of extensions to watch (* for all):	<input type="text" value="502 503"/>
Limit own visibility to this list:	<input type="text"/>
Upload a picture (BMP format):	<input type="text"/> <input type="button" value="Durchsuchen..."/>
Block outgoing caller-ID:	<input checked="" type="radio"/> no <input type="radio"/> yes

At the bottom left of the form is a button. At the bottom of the page is a copyright notice: Copyright © 2005-2007 pbxnsip Inc. All rights reserved. See the license agreement for more information.

The settings "First name" and "Last name" store the display name of the extension. This name will be used for internal calls. Phones that are able to display the names will show it on the screen. These names will also be searched by the auto attendant if the caller chooses the dial by name feature.

The "Password" is used for SIP and HTTP traffic. It should be reasonable safe;

just a few digits of digits will not be enough. However, it is up to the user to choose a safe password. When the user enters a new password, the current HTTP session will stay valid until the next login. Permanent cookies will be invalidated on the next login.

The "PIN" is used in several dialogs of the PBX, for example when entering the mailbox. Although it is also possible to do brute force attacks on PIN codes, it takes more time to perform such attacks. We recommend using at least 5 digits, so that an attacker has at least 100,000 combinations to choose from.

The "Cell phone number" is associated with the extension. When someone tries to call the extension directly, the PBX may include that number in the list of devices that is being called. The setting "When calling the extension" controls if and when the cell phone is being called. For more information, see Cell Phone Integration for more information.

The "Timezone" tells the PBX in which time zone the user is. This setting is used for example in the mailbox (reading out timestamps), but it is also used when the PBX generates configuration files for attached phones.

The "IVR Language" settings controls which language the user prefers. This is setting is used for example, when the user calls the mailbox or when the caller calls into the PBX from the associated cell phone.

The "Web Language" is used when the user logs into the web interface of the PBX. This setting is also used when emails are sent to the user.

The "List of extensions to watch" is used for automatic generation of the configuration files of the phones. The PBX will try to put the listed extensions into the settings for the phone. This setting depends on the used device. For this setting you can use Wildcard Patterns. For example, if you use just a star, the PBX will try to put all extensions of the domain into this list.

If the "Limit own visibility to this list" is set, the PBX allows only the listed users to watch the extension. It also uses Wildcard Patterns.

If you upload a picture in the "Upload a picture" setting, the PBX will automatically insert a SIP header that can be used by SIP phones to show the picture of the extension. This is similar to the display name of the extension, with the difference that in addition of a text a picture is rendered. The picture must be in BMP format that the endpoint understands.

The setting "Block outgoing caller-ID" is used when making outbound calls. If the setting is set to "yes", the PBX will ask the gateway or SIP provider to hide the Caller-ID for this call.

7.2 User Redirection Settings

Do not disturb: on off

Incoming anonymous calls: Pretend to be busy

Hot Desking at:

Call forward all calls to:

Call forward calls when busy to:

Call forward on no answer to: 9784353234

Call forward no answer timeout: 15 sec

Save

The "Do not disturb" (DND) settings is used to keep the user from incoming calls. If this setting is turned on, then this extension will not receive incoming calls. Only extensions that have the permission to override DND will be able to call the extension. However, the extension can a all times place outbound calls.

The setting "Incoming anonymous calls" controls how incoming calls to the extension are treated. This setting does not affect calls that come from a hunt or agent group or internal calls.

- The "no special treatment" mode turns this feature off and sends all calls directly to the extension.
- The mode "reject call" will inform the caller that the extension does not accept anonymous calls. Calls will not be put through to the extension.
- The mode "pretend to be busy" also does not put the call through, but does not tell the caller why. The PBX will not offer camp on.
- The mode "ask for name" will prompt the caller for the name and then put him on hold while calling the extension. After reading out the recorded name, the extension may decide what to do with the call. Either the call can be accepted, or it can be sent to the mailbox or it can be rejected.
- The mode "ask for name even if the caller-id is present" will always ask for recording the name, even if the caller-id is available. Only callers which are on the white list are directly put through.

The "Hot Desking" setting is described in the separate page Hot Desking.

There are several ways of doing call forwarding.

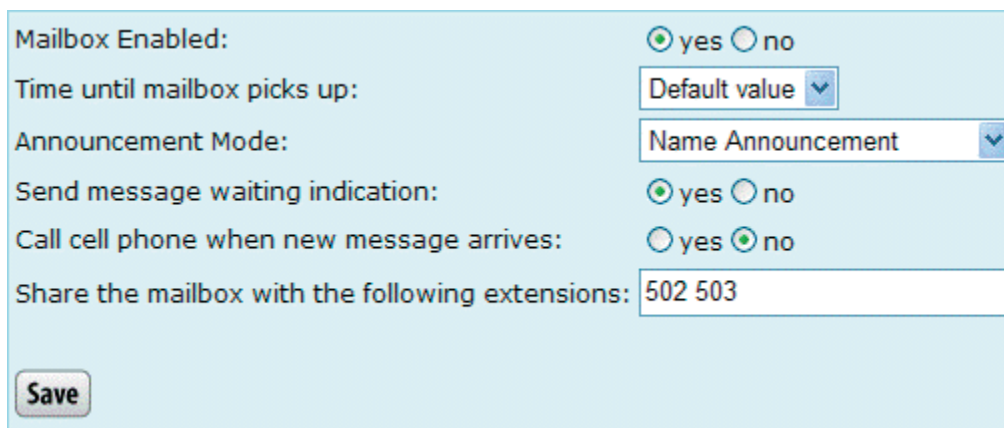
- If you want to temporarily redirect all calls to another extension you can use the "Call forward all calls" setting. This setting affects only calls that are going directly to the extensions. If the extension is part of a hunt group or an agent

group or the call origins from a paging group, the call is not being redirected.

- The "Call forward calls when busy" forwards calls only when the extension is busy. This condition is either true if the phone itself signals it is busy or the "Lines" parameters has been set for the extension and this number has been reached (see Registrations).
- The Call forward on no answer" kicks in when the phone rings, but there is no answer. The waiting time is defined in the domain and can be overridden by a user setting ("Call forward no answer timeout"). If the mailbox picks up earlier, this setting has no effect; if the call is being redirected, the mailbox timeout is cancelled.

All redirection settings can have one number, either internal or external. If the call is being redirected to an external destination, the PBX will use the dial plan of the extension for placing this call and it will charge the extension for this call.

7.3 User Mailbox Settings



The screenshot shows a web form for mailbox settings. It includes the following fields and controls:

- Mailbox Enabled:** Radio buttons for yes and no.
- Time until mailbox picks up:** A dropdown menu currently showing "Default value".
- Announcement Mode:** A dropdown menu currently showing "Name Announcement".
- Send message waiting indication:** Radio buttons for yes and no.
- Call cell phone when new message arrives:** Radio buttons for yes and no.
- Share the mailbox with the following extensions:** A text input field containing "502 503".
- Save:** A button at the bottom left.

The user may decide if the mailbox should be enabled or not. For this purpose, the web page offers the setting "Mailbox Enabled".

As with the redirection setting, the user may override the default setting until the PBX redirects the call to the mailbox. This can be done in the setting "Time until mailbox picks up".

The "Announcement Mode" can have the following values:

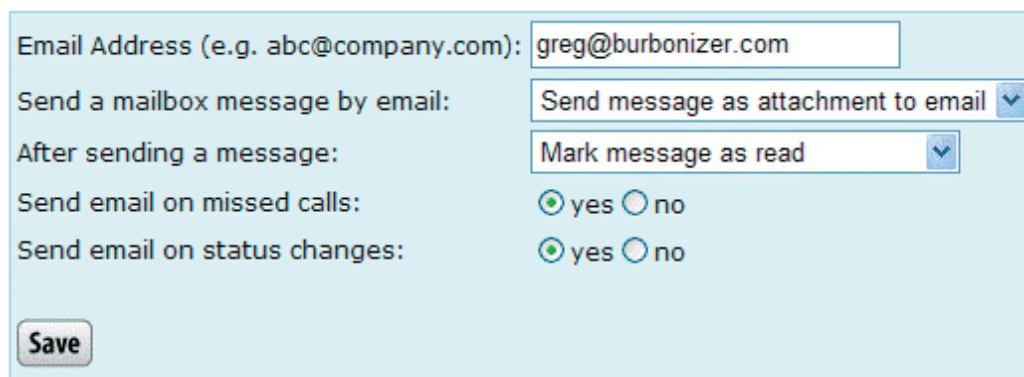
- If the user selects the "Anonymous Announcement" mode, the PBX will just read out the number of the extension.
- If the user selects "Name Announcement" the PBX will play back the recorded name of the extension, if present.
- The setting "Personal Announcement" will read out the recorded announcement of the extension, if present.

If the PBX should send a notification to registered phones, the setting "Send message waiting indication" must be turned on.

If the PBX should call the cell phone after a message has been recorded, the setting "Call cell phone when new message arrives" needs to be turned on. The PBX will charge the extension for this call.

If the mailbox should be shared with other extensions, those extensions can be listed (separated by space) in the setting "Share the mailbox with the following extensions". If the mailbox does not require a PIN code, those extensions can directly dial into the mailbox and listen to messages. Those extensions will also receive the message waiting indication, if the sending has been activated and the phones register for MWI events.

7.4 User Email Settings



Email Address (e.g. abc@company.com): greg@burbonizer.com

Send a mailbox message by email: Send message as attachment to email

After sending a message: Mark message as read

Send email on missed calls: yes no

Send email on status changes: yes no

Save

The setting "Email Address" tells the PBX where to send email messages. The domain administrator must enable Email, so that this setting actually enables sending out emails.

The setting "Send a mailbox message by email" defines how the PBX sends emails out:

- "Send emails without attachments" will just send a notification to the user by email. The voicemail message itself is not sent and must be retrieved either through the web interface or by calling the mailbox. This mode has the advantage that the emails are relatively short; this way it is a useful feature when using mobile devices that support reading emails.
- "Send message as attachment to email" will also send an email, but put the voicemail itself as attachment to the email. This is a good choice if you are using email during the whole day and you are using a personal computer for processing emails.
- "Do not send an email" is a good choice if you are just using your SIP phone to receive voicemail messages.

You can decide what you want to do with the message after an email has been sent. "Keep the message as new message" will keep the message in your mailbox and it will count as a new message. This mode has the potential danger that your mailbox eventually might become full. If you choose the mode "Mark

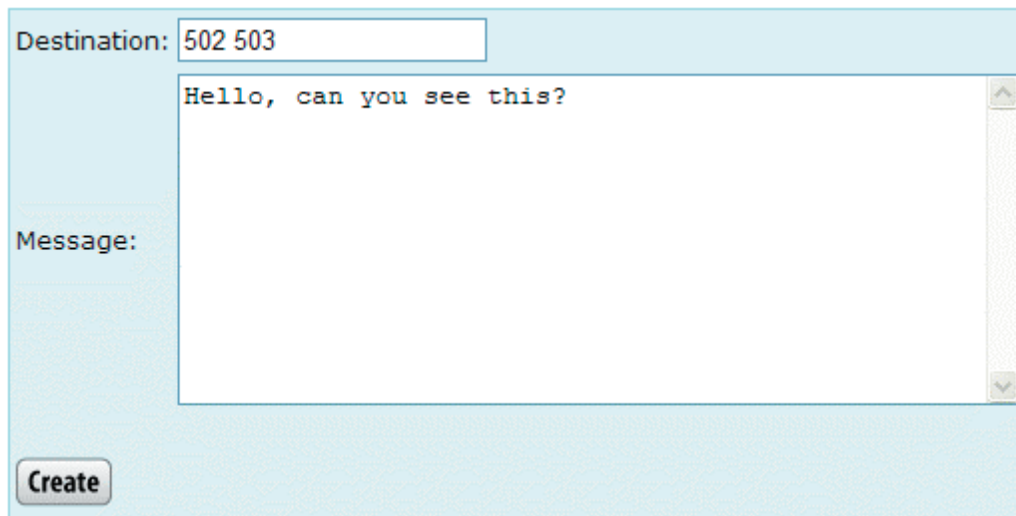
message as read", the PBX will still keep the message in your mailbox, but when the mailbox is becoming full, it will drop the oldest message to make room for a new message and your mailbox will not become full. However, in this mode most SIP phones will not turn on their message waiting indicator (because only new messages trigger this behavior). If you decide to "Delete the message", the PBX will delete the message after sending the email. This keeps your mailbox clean, but the system relies on a reliable transport of the voicemail.

If you want to receive emails when you miss a call, turn the setting "Send email on missed calls" on. The PBX will send this email only if the call went directly to your extensions; calls to a hunt group or agent group do not count.

The PBX can also send you emails when your status changes "Send email on status changes". This email is being sent when the DND status or the redirection changes.

7.5 User Instant Message

Usually you would use a SIP endpoint to send instant messages (IM) to another extension. However, most of the SIP devices do not support that feature today. Therefore, the PBX offers a possibility to do that from the web interface.



Destination: 502 503

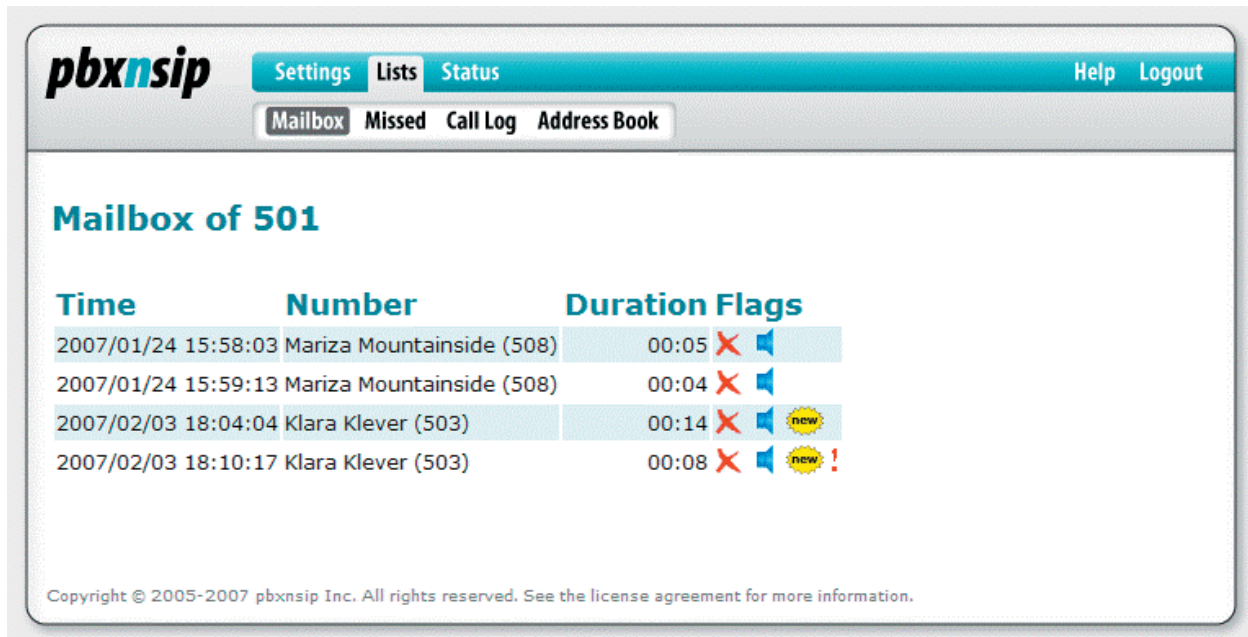
Message: Hello, can you see this?

Create

Sending an IM is simple. Just enter the destinations in the "Destination" field and the text that you want to send in the "Message" field, then click on the "Create" button. You can send the message to more than one destination by listing the extensions separated by spaces. The PBX will then send the message to all registered devices for the extensions that you selected.

The PBX will tell you how many messages have been sent in total.

7.6 Mailbox View



Time	Number	Duration	Flags
2007/01/24 15:58:03	Mariza Mountainside (508)	00:05	X [speaker]
2007/01/24 15:59:13	Mariza Mountainside (508)	00:04	X [speaker]
2007/02/03 18:04:04	Klara Klever (503)	00:14	X [speaker] new
2007/02/03 18:10:17	Klara Klever (503)	00:08	X [speaker] new!

The mailbox page shows you the content of the mailbox. It contains the following information:

- The "Time" is the time stamp when the message was recorded. The time is shown in the time zone of the extension that received the message.
- The "Number" shows the Caller-ID and, if available, the name of the person who left the message.
- The "Duration" shows how long the message is. The format is "minutes:seconds".

The "Flags" field shows several icons:

- The delete icon can be used to delete the message.
- The loudspeaker icon will download the message as WAV file and offer this file for playback on the web browser.
- The "New!" symbol indicates that the PBX keeps that message as unread.
- The red exclamation mark message indicates that the caller marked this message as urgent.

7.7 Missed Call List

The missed call list shows what calls were attempted to the current extension, but did not connect. If there were display-names available, the PBX will show them in the list. The "Time" column shows when the call was started.

The PBX offers click-to-dial by clicking on the number listed on the web page. The PBX will call the extension and ask it to acknowledge the click-to-dial initiation. The call resulting from the click-to-dial will be charged to the extension.

The length of the list is set by the domain administrator. The PBX has only a specified context in which it keeps the necessary records for the call list feature.

7.8 Personal Call Log

Call list for 501

Time	From	To	Duration
2007/01/24 14:14:45	501	Mariza Mountainside (508)	00:04
2007/01/24 14:15:23	Mariza Mountainside (508)	501	00:03
2007/01/24 14:18:39	Mariza Mountainside (508)	501	00:08
2007/01/24 14:18:51	Mariza Mountainside (508)	501	00:02
2007/01/24 14:48:00	501	501	00:23
2007/01/24 14:52:14	Mariza Mountainside (508)	501	
2007/01/24 14:59:03	501	*	00:00
2007/01/24 14:59:07	501	*	00:02
2007/01/24 15:58:15	501	501	00:13
2007/01/24 15:59:24	501	501	00:39
2007/01/24 16:00:09	501	501	00:22
2007/01/26 11:38:06	501	Mariza Mountainside (508)	00:02
2007/01/26 13:56:21	Mariza Mountainside (508)	501	
2007/01/26 14:12:43	Mariza Mountainside (508)	501	

The call list shows what calls were made from or to the current extension. If there were display-names available, the PBX will show them in the list. If the call was not connected the duration will be empty. Otherwise, it will show the duration in minutes and seconds. The "Time" column shows when the call was started.

The PBX offers click-to-dial by clicking on the number listed on the web page. The PBX will call the extension and ask it to acknowledge the click-to-dial initiation. The call resulting from the click-to-dial will be charged to the extension.

The length of the list is set by the domain administrator. The PBX has only a specified context in which it keeps the necessary records for the call list feature.

7.9 Address Book

For the description of the address book, please refer to the section on address book above.

7.10 User Status

Status for extension 501

Do not disturb:	false
Agent logged in:	true
Hot Desking at:	
Call forward all destination:	
Call forward busy destination:	
Call forward on no answer:	
Timeout for call forward on no answer:	
Timeout for mailbox:	
Call redial:	"Mariza Mountainside" <sip:508@localhost>
Call return:	"Klara Klever" <sip:503@localhost>

The user status page shows essential information about the state of the account.

You can see the settings for call redirection, the current state of do not disturb (DND), and the last number that have been dialed or received from that extension.

