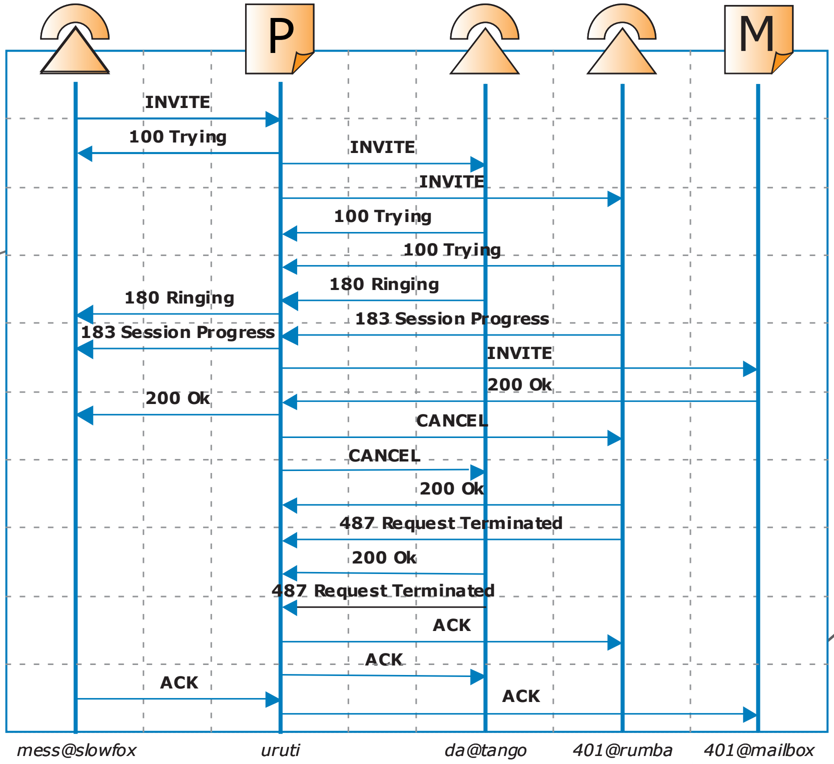
snom
VoIP-phones

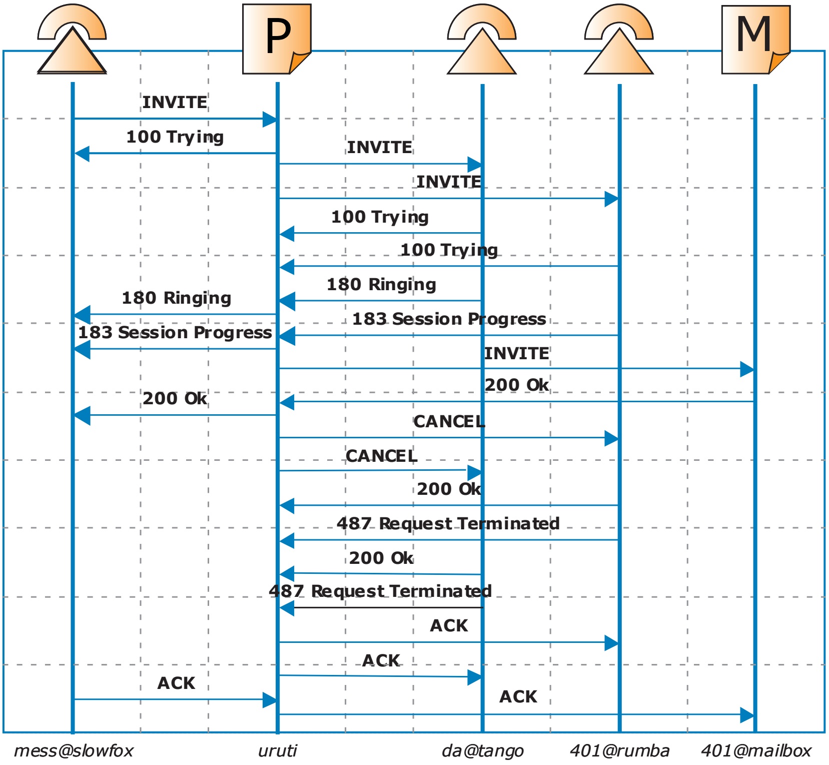
snom 4S



SIP Registrar/Proxy 2.14

User Manual

snom 4S



SIP Registrar/Proxy 2.14

snom 4S Registrar Proxy Version 2.14 User Manual

4. Edition 2002

This document is supplied by snom technology AG for information purposes only to licensed users of the snom 4S registrar proxy and is supplied on an “AS IS” basis, that is, without any warranties whatsoever, express or implied.
Information in this document is subject to change without notice and does not represent any commitment on the part of snom technology AG. The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license agreement. It is against the law to copy or use this software except as specifically allowed in the license. 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 snom technology AG.

Welcome to snom 4S !

SIP is becoming more and more accepted in the area of VoIP. Many companies are working on SIP solutions and making great products that will make telephony much easier and better. However, a easy to use and affordable SIP proxy is hard to get at the moment. But SIP telephony without a proxy makes no sense. That is why we are making this simple and straightforward proxy available.

snom 4S stands for "snom soft switch for small and medium enterprises". That means, the snom 4S proxy was designed for environments handling up to 1000 users with normal traffic. In environments where you need more features and better scalability, we would be happy to refer you to other companies offering carrier grade and feature-rich proxies that solve these problems.

This product is a proxy/registrar which means this software is responsible for locating users. Features like Follow me and group calling are therefore supported; however media services like mailbox and music on hold are not part of the software. You should use a media server for this.

Interoperability is important to us. We have tried to stick to the SIP standard as well as possible and tested the phones of other vendors. We hope that this will help to build up a flourishing VoIP telephone industry in which the products of the different vendors work together like the products in the computer industry do today. We believe that having a choice is good for you and therefore good for us.

This manual gives you a brief introduccion to VoiP and SIP, explains the installation process for Windows and Linux and shows how to run the SIP proxy. For additional snom 4S information, please visit our Web site at **http://www.snom.de** and if you have any comments and suggestions about snom 4S, please contact us through snom technology AG's support link Web site. We would appreciate your feedback.

We hope that this SIP proxy helps you get VoIP up and running!

Thank you and....

have fun using the snom 4S!

Sincerely,

Dr. Christian Stredicke Managing Director	Nicolas Peter-Pohland Managing Director

T

Table of Contents

snom 4S • SIP

Registrar/Proxy 2.14

Voice over Internet Protocol

Today there is a wide choice of different switched network products. Telephones have now been being built for more than a century, and their technology is well-understood and proven. Why choose a different technology?

Modern communication infrastructures transport much more than just one application: email, http, files, instant messages, videos, music, so it is only natural to include voice in the list of applications and use one infrastructure for all of them.. Voice is a real time application. Sending voice over the Internet Protocol is called "VoIP". The delay between sending a packet to the network and receiving it needs to be minimal and constant and this makes specific demands on this application.

Most network equipment can already fulfil this real time requirement. Virtually all switches currently on sale support a VLAN with different priorities in the network, and the vast majority of higher layer network equipment supports some means of transporting packets with different qualities (DiffSrv). The LAN usually supports a bandwidth of 100 MBit/s, which is more than enough to allow voice to flow through the network, and adherence to a certain set of rules ensures that this bandwidth is enough to supply superior telephone quality. The Internet backbone's ability to transport large loads is increasing on a daily basis, and global communications are now ruled by the Internet.

Why SIP?

There has been a "protocol war" regarding the "best" way to set up a phone call. In the mid 90s, H.323 was the first attempt to unify the VoIP industry under a common standard,and move the world of telephony into the computer industry, using most of the methods known from ISDN. Seen however, from today's perspective, the resulting technology was far too complex, so products based on this technology did not work well together. The late introduction of "supplementary services" (H.450.x) not only introduced another level of complexity, but was also simply too late.

By the late 90s, the Session Initial Protocol (SIP) had been proposed (RFC 2543[1]). SIP follows the paradigms of the Internet, and is built upon the same principles used by http and email. Moreover, it has found an enthusiastic community of researchers and developers who like the idea of applying Internet technology to real time communications. More and more applications are being put into SIP, telephony being just one of them.

So far more than 150 drafts have been proposed for extending the SIP protocol. All kinds of solutions are being addressed in these documents, and the highly dynamic field of this new real time communication technology is resulting in evolutionary pressure to find the best common denominator.

Most of the “big players” have jumped on the SIP train. Microsoft Messenger is based on SIP and industry giant Cisco offers SIP extensions to most of their products. International organizations like ETSI host SIP interoperability events, and next generation mobile technology will be integrated with, if not based on, SIP.

Open Standards

Open standards define the rules of the game. Interoperability allows customers to choose between the products of different vendors and opens up competition below the system level. This can be advantageous for the customer, as the computer hardware industry has shown.

Many vendors therefore advertise their usage of an “open standard”, defining this term as “we make the way our standard works public”. However, this cannot really be called “standard” if only one vendor is using it. The disadvantage is that customers still have a limited choice of products they can buy.

There is no one objective definition of an open standard. However, something approaching an open standard could be reached if a significant number of vendors offered products using the same standard, giving customers the possibility of combining products to create a system. SIP is just such a standard.

What You Can Expect and What Not

Telephony is more than making calls from A to B. SIP supports all kinds of transfers, call parking and call picking, user searches (Follow-me), mailbox support, and all the other features known from traditional telephony. In addition to this, telephones can now indicate their willingness to receive calls and the probability of finding a specific user.

You can call a PSTN number from a SIP phone just as you did ten years ago. The network will usually be set up to terminate these calls on a gateway which translates the packet stream into a switched network signal. You can also dial email-like numbers like “sip:fred.flintstone@megaportal.com ”, and you can reach your sales team under the same telephone number and email address.

Internet telephony is still a “best effort” communications technology and does not always necessarily support the quality of transport telephony requires. If you are placing a phone call over the public Internet, there is no guarantee that a packet will be transported within a reasonable time. Usually there is acceptable quality, but it may happen that calls suddenly break off, that there is significant delay, or that packet loss causes stuttering. It is important that users know what to expect: Cell phone users know that driving through a tunnel may break the call, and Internet telephony users must be aware that talking for free may compromise call quality.

snom 4S • SIP

Registrar/Proxy 2.14

The SIP Architecture

User Agents

In a SIP network, the phones[2] make up most of the brain power, unlike traditional telecoms equipment which can not scale so well:

- they play and record audio,
- they compress and uncompress the digital audio,
- they do echo compensation,
- they compensate for packet jitter and packet loss,
- they look for the destination,
- they retrieve their configuration information,
- they keep track of phones that offer a call pickup,
- they publish their state upon request,
- they determine and publish the probability of finding somebody,
- they terminate one or more identities,
- they redirect calls when nobody picks up,
- they are part of a virtual LAN,
- they search address books (LDAP),
- they search internet addresses (DNS A, DNS SRV),
- they usually include a web server,
- they send an receive instant messaging information,
- they publish network management information (SNMP),
- they behave like normal computers on the network (DHCP, DNS).

Phones are also called "user agents" and behave in a client/server manner (somebody being the user agent client, UAC and somebody the user agent server, UAS). In SIP, there is no conceptual difference between a hard phone and a soft phone. The snom 100 VoIP phone or Microsoft Messenger are examples of this kind of system.

Registrars

When dialling a number, the final destination is usually unknown. There needs to be a network service that tells where a number can be found. The registrar fulfils this role for a specific realm, which is typically bound to a DNS address.

User agents register with a registrar. When a request for the user agent arrives at the registrar, it redirects the request to the location that was previously stored in the internal database.

Proxies

Proxies forward requests and help the user agent carry out its tasks. Stateless proxies just forward messages and serve as a “hop” on the path from a user agent client to a user agent server. The rules for hopping may depend on all kinds of rules, e.g. traversing NAT using a stateless proxy.

Stateful proxies keep a list of pending requests. This way proxies can forward requests to different destinations at the same time. When the responses come back from the destinations, the proxy merges the responses, determines the best result and passes it down to the user agent that sent the request (UAC). The snom 4S proxy is a stateful proxy.

Media Server

Strictly speaking, the media server is just a special kind of user agent. Typically it is able to deal with several calls at the same time and is a located on a PC or workstation.

The media server has the following tasks:

- Implement mailbox function. When a user is absent, the user agent of the stateful proxy redirects the call to the mailbox, so that the caller may leave a message. The owner of the mailbox calls the mailbox directly to listen to messages.
- Implement music on hold. Using a fat client, all kinds of music tastes can be played with highest possible quality.
- Implement call parking. Calls can be parked on the media server until a user picks the call for processing. In the meantime, the caller can enjoy the music on hold, using DTMF keys to select his favourites.
- Implement conferencing services. Three or more persons dial into the conference server, which mixes the audio streams for each participant and also notifies them of participants joining and leaving the conference. The conference server also checks the credentials of participants joining the conference. The snom 4s is an example of this technology.

Gateways

From a SIP perspective, the gateway is also just a user agent. Instead of playing the audio stream on a speaker, it sends it to the PSTN network and instead of getting voice from a microphone it retrieves signals from the switched network.

There are three kinds of gateways; PSTN, proxy signalling and NAT gateways.

Depending on the nature of the gateway, it may serve one, two, four, thirty, sixty or more channels at the same time.

Other gateways may translate the signal to existing H323 networks or other proprietary technology networks. These gateways are sometimes called signalling gateways. snom does not produce SIP gateways. Examples of such gateways are manufactured by Cisco, Mediatrix, Sonus and Vegastream. The snom 4s gateway is a SIP NAT gateway software enabling Linux computers to be SIP-aware.

snom 4S ● SIP

Registrar/Proxy 2.14

The snom 4S Solution Framework

snom has set up a SIP-based solution targeted at small and medium sized installations. This solution may be installed on Windows® as well as on Linux computers. The registar proxy is the core part of this framework.

Proxy

The snom 4S registrar proxy is a SIP registrar and proxy with the following features:

- Stateful forking. Requests are forked to one or more destinations and the responses are filtered before passing them back to the user agent client.
- Sequential forking: Users are searched according to the probability that was provided with the registration.
- Full functionality: All SIP methods are supported, that includes transfers, call parking, call picking, notifications, instant messaging and other SIP features.
- Dial plan: You can set up dial plans that will determine whether specific users may call specific destinations, whether numbers are complete, or whether numbers are to be redirected to one or more gateways.
- Authentication: You can force clients to authenticate their identity.
- NAT handling: Requests leaving the private network may be redirected to a NAT gateway.
- Support of path registrations. This way user agents may register with a path that may contain proxies that must be passed.
- Failure recovery: Even after a reboot, the proxy keeps the state of the registrations.
- TCP and UDP transport layer support: Both unreliable and reliable transport layers are supported.[3]
- Web Access: The proxy can be managed remotely via a web browser.
- Interoperability: The proxy is interoperable with the SIP equipment of

other vendors; you are not limited to snom products.[4]

SIP NAT Gateway

The snom 4S Network Address Translation (NAT) gateway is a stateless proxy that transports SIP messages between private and public networks. This makes it possible to share one public Internet address amongst several SIP elements. The NAT gateway supports:

- Forwarding of RTP packets. Both incoming and outgoing packets may be forwarded by the NAT gateway. The SDP attachments of SIP messages are patched according to the local ports. This allows usage of the NAT gateway together with a firewall.

- Path registrations. Registration messages passing the proxy are tagged with the proxy path.

- Default destination: Packets destined for the NAT gateway may be forwarded to a fixed address. This way a publicly accessible proxy may reside inside a private network.

- PPPoE device support. In Linux, the NAT gateway automatically detects the public IP address and changes the address when the PPPoE device changes the IP address.

- Assignment of RTP port range. To comply with available firewalls, a range of ports may be assigned.

- Codec preference reordering. The available codecs are reordered according to their bandwidth requirements. This reduces the bandwidth used when talking over the NAT gateway and makes usage in DSL environments easier.

- Linking to Linux ipchains. This way packets destined at SIP port 5060 can be redirected to the NAT gateway without setting up the user agents in the private network.

Media Server

There are situations when there is nobody available to handle a call. In these cases the media server helps out.

- Mailbox. When nobody picks up a call, the caller can leave a message on a mailbox. The owner of the mailbox receives notification on his phones and an email with voice mail as an attachment.

- Music on hold. When a call is put on hold, the waiting party can listen to some music or announcements. Calls can also be parked on a music on hold server.

- Conferencing services. When more than two people want to talk in a telephone conference, the media server can introduce new participants, ask for pass codes, and mix the audio streams in such a way that participants do not hear themselves.

- Error explanations. When something goes wrong, the media server explains what it was .

snom 4S • SIP

Registrar/Proxy 2.14

Installation

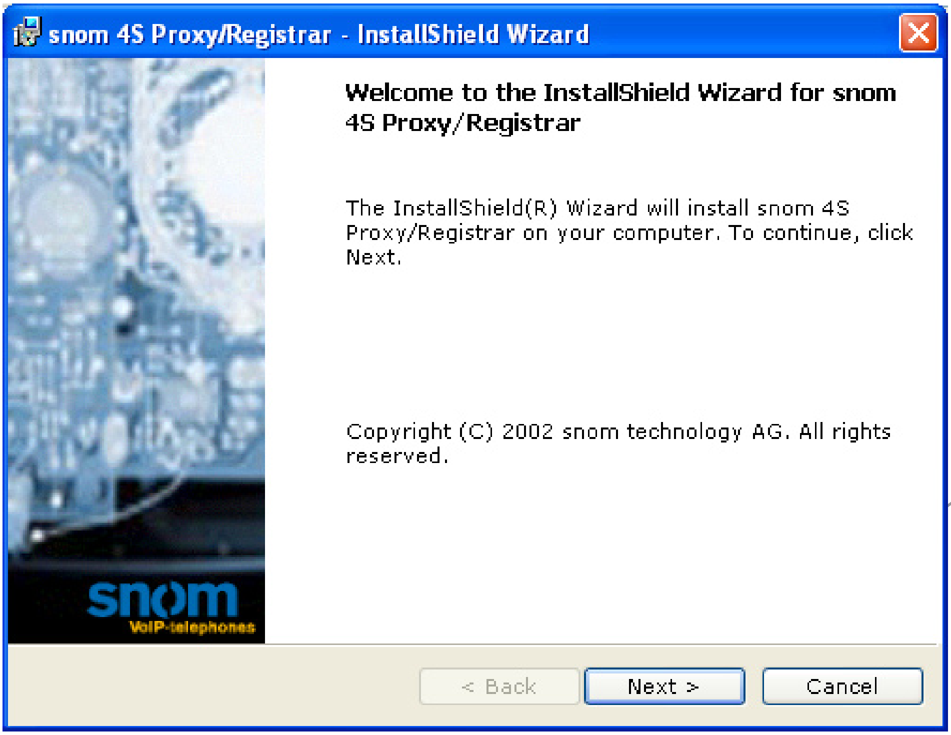
Windows

Tip: If you are doing an update, you need to stop and uninstall the old proxy first (see below).

After double clicking on the setup executable, the installations program starts up (see fig. 2-1). Press Next to begin the installation.

FIGURE: 4-1

Installation Program



snom 4S Proxy/Registrar - InstallShield Wizard

Welcome to the InstallShield Wizard for snom 4S Proxy/Registrar

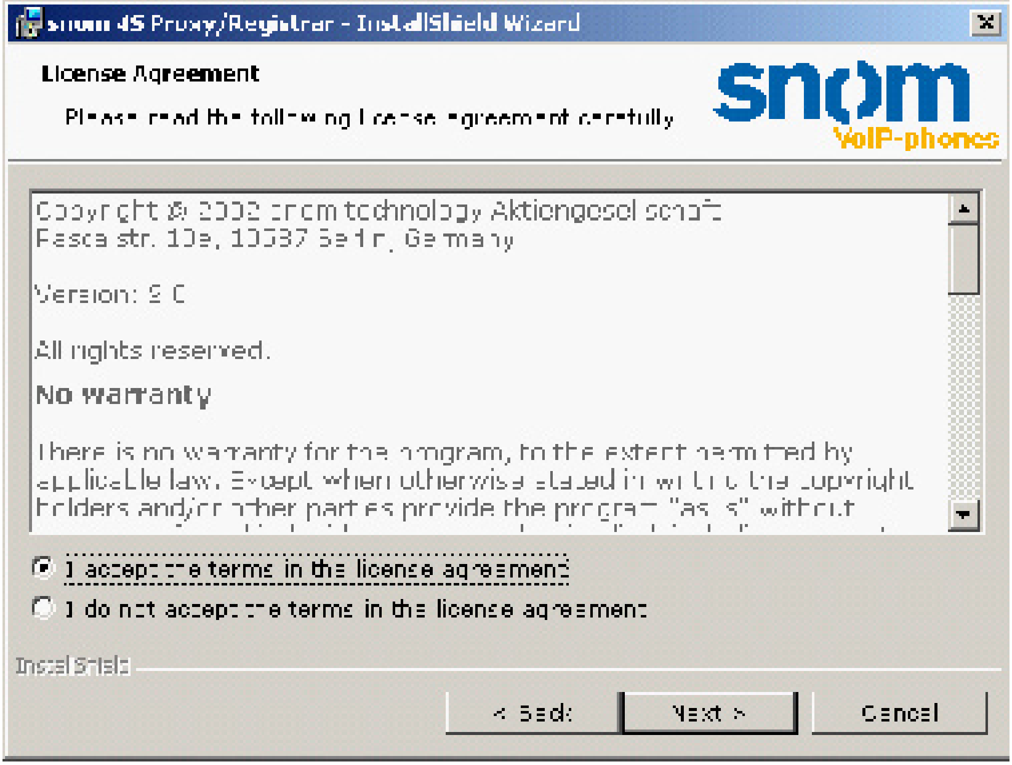
The InstallShield(R) Wizard will install snom 4S Proxy/Registrar on your computer. To continue, click Next.

Copyright (C) 2002 snom technology AG. All rights reserved.

At the beginning of the installation the setup program asks you to accept the license conditions. Please read them carefully, then select the “accept” button and press “next” to accept the conditions. If you decline, the installation will be aborted.

FIGURE: 4-2

License Agreement



snom 4S Proxy/Registrar - InstallShield Wizard

License Agreement

Please read the following license agreement carefully

Copyright © 2002 snom technology Aktiengesellschaft
Pascalstr. 10a, 10587 Berlin, Germany

Version: 2.0

All rights reserved.

No warranty

There is no warranty for the program, to the extent permitted by applicable law. Except when otherwise stated in writing the copyright holders and/or other parties provide the program "as is" without

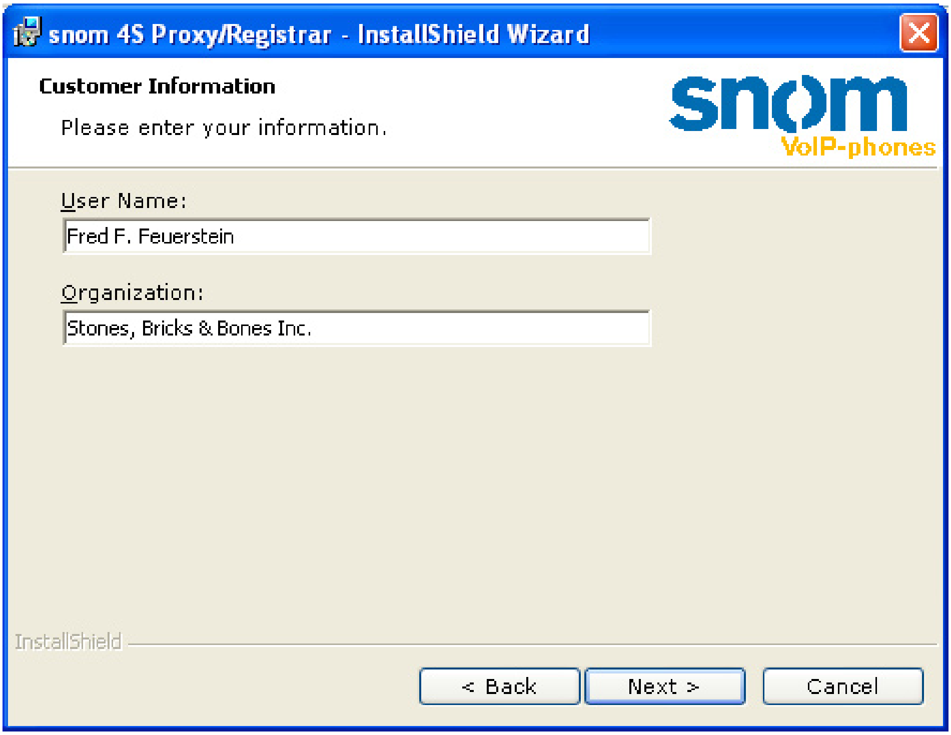
● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

After accepting the license agreement, the next screen asks you to enter your personal information. Enter your name and the name of organization.

FIGURE: 4-3

Customer Information



snom 4S Proxy/Registrar - InstallShield Wizard

Customer Information

Please enter your information.

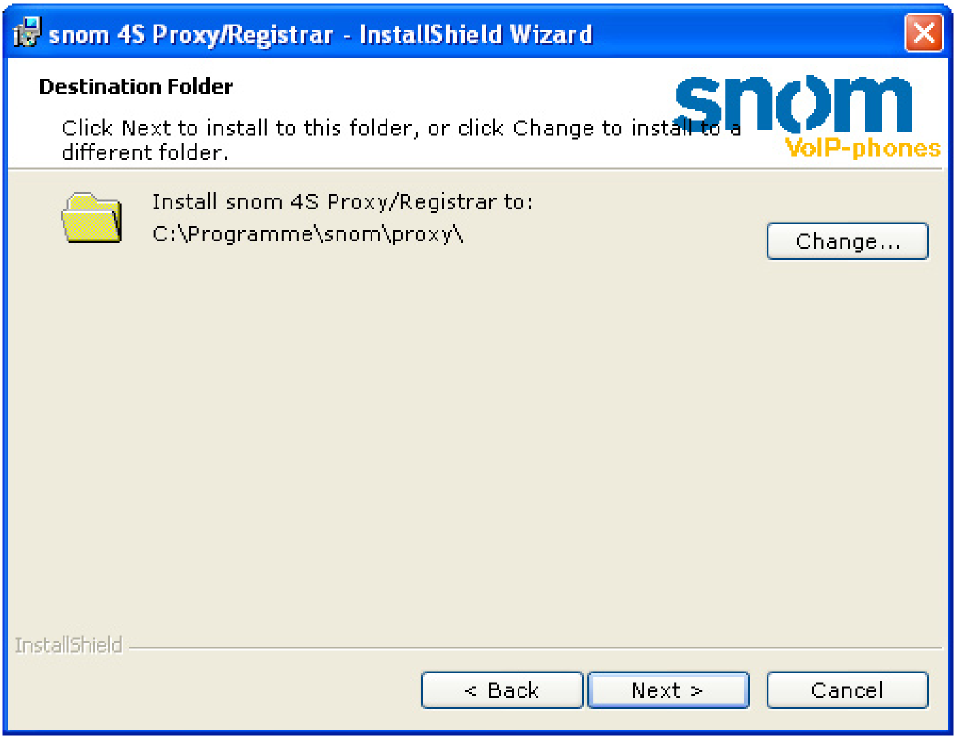
User Name:
Fred F. Feuerstein

Organization:
Stones, Bricks & Bones Inc.

You can then select the location where the proxy's files will be put. The installation program proposes a reasonable location but if you want to you can change it. After this, the installation asks you for the location where the registration information will be put. This directory needs write access and will contain the information for registered users. The installation program proposes a location relative to the proxy installation directory, but it might be useful to specify a different location for this, e.g. a temporary directory. It is important that the directory exists; the proxy will not create this directory.

FIGURE: 4-4

Destination Folder



snom 4S Proxy/Registrar - InstallShield Wizard

Destination Folder

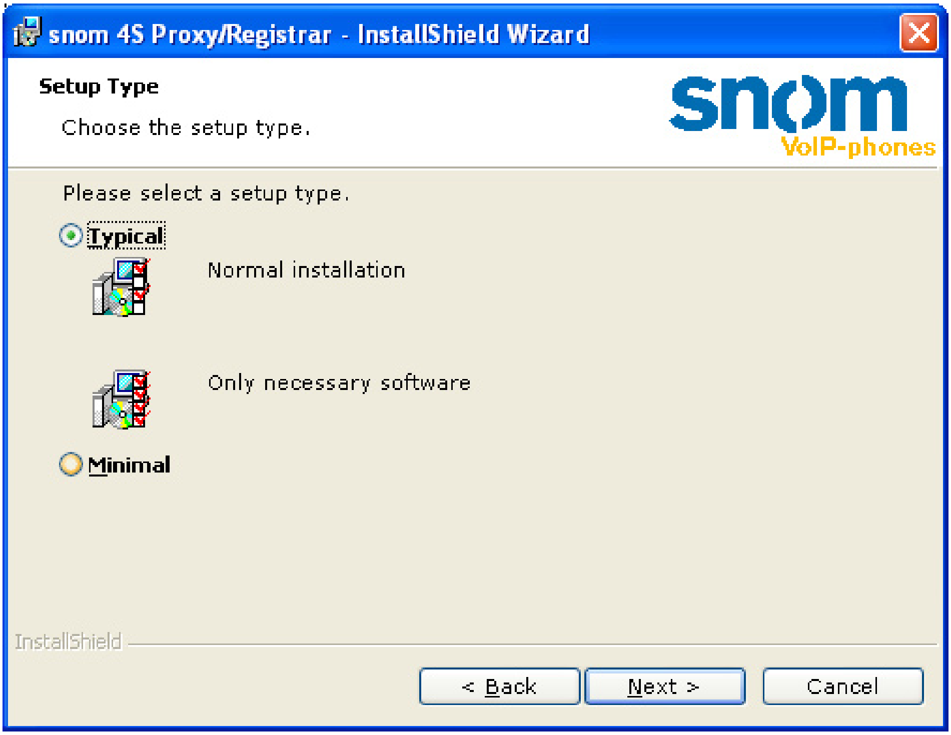
Click Next to install to this folder, or click Change to install to a different folder.

Install snom 4S Proxy/Registrar to:
C:\Programme\snom\proxy\

In the next step you can select the installation type. We recommend using the Typical installation. If you select Minimal, the documentation is not installed.

FIGURE: 4-5

Set up type



snom 4S Proxy/Registrar - InstallShield Wizard

Setup Type

Choose the setup type.

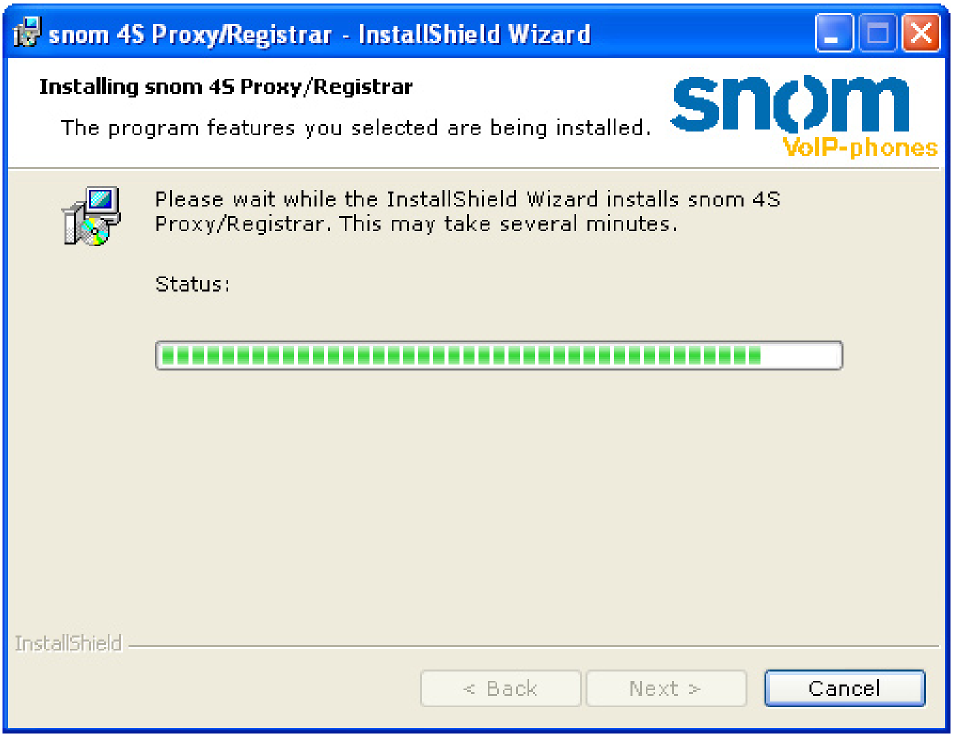
Please select a setup type.

● Typical — Normal installation

○ Minimal — Only necessary software

FIGURE: 4-6

Confirmation Screen



snom 4S Proxy/Registrar - InstallShield Wizard

Installing snom 4S Proxy/Registrar

The program features you selected are being installed.

Please wait while the InstallShield Wizard installs snom 4S Proxy/Registrar. This may take several minutes.

Status:

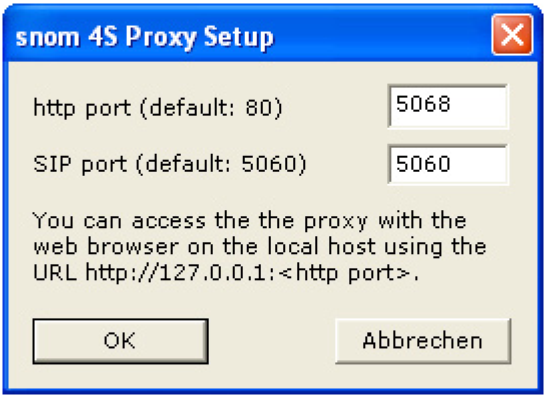
Before the installation finishes, you need to define on which ports the proxy will operate. This is important because otherwise it will be hard for you to find the right port.

The http port defines where the web server of the proxy can be accessed. The default port for web servers is 80, and if you are not running any other web services on the computer, port 80 is a good choice. Otherwise, choose a free port and write the port number down somewhere so you don’t have to search for it. If you don’t fill in any data or cancel the dialog, port 80 will be used.

The SIP port defines where the SIP traffic is expected. This will be port 5060 in most cases and you should change this port only if you know exactly how the proxy can be addressed with a different port number.

FIGURE: 4-7

Entering Ports



snom 4S Proxy Setup

http port (default: 80) 5068

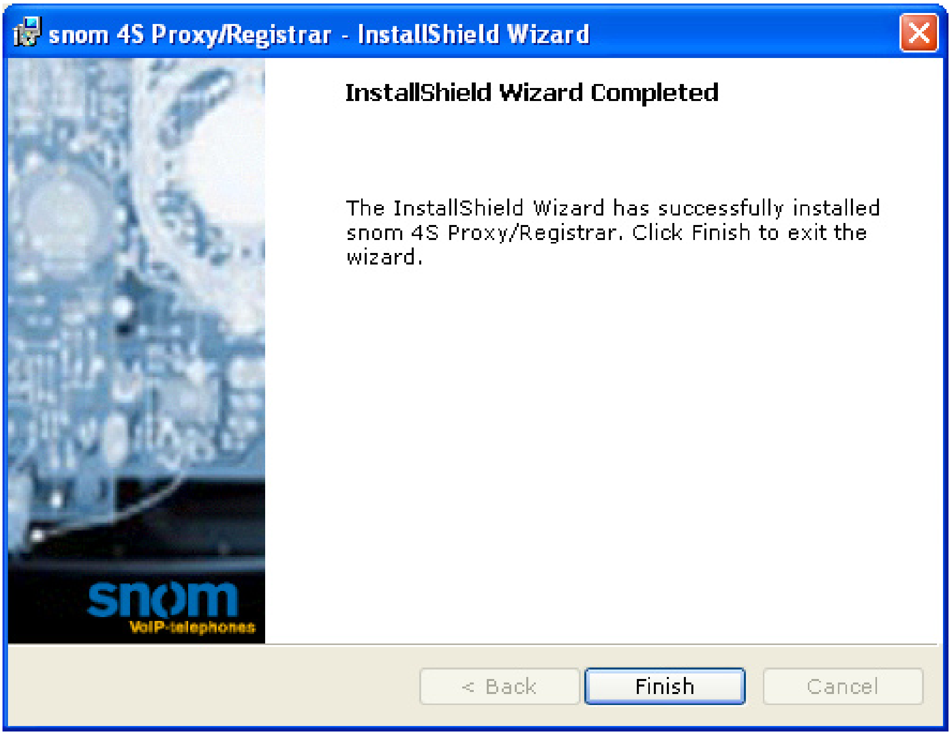
SIP port (default: 5060) 5060

You can access the the proxy with the web browser on the local host using the URL http://127.0.0.1:<http port>.

After finishing the setup wizard, check that the proxy is running. If you do not want to reboot your system (because it is running other critical applications), you can also manually start the service in the services section of the Windows control interface.

FIGURE: 4-8

Installation Completed



snom 4S Proxy/Registrar - InstallShield Wizard

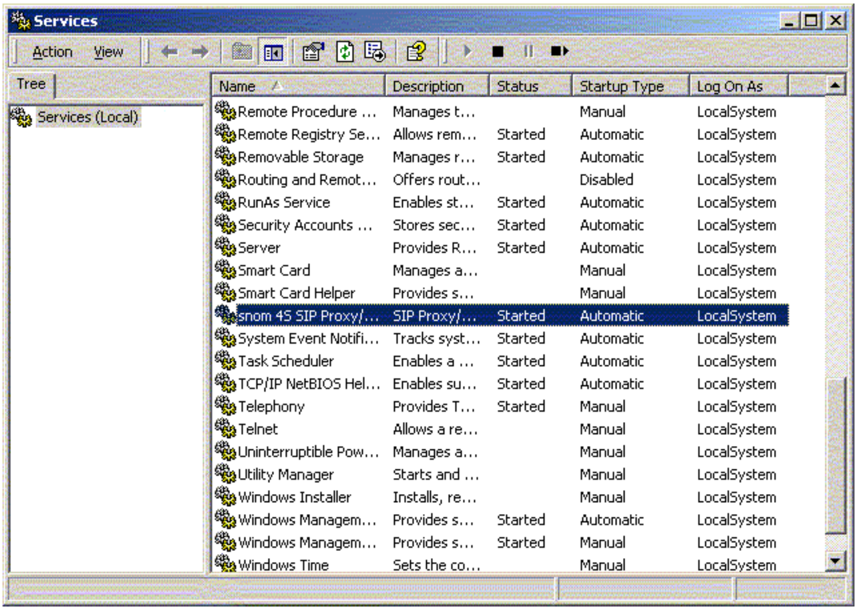
InstallShield Wizard Completed

The InstallShield Wizard has successfully installed snom 4S Proxy/Registrar. Click Finish to exit the wizard.

Check that the installation has been successful by checking the Services field of Windows. Open the services Window and look for "snom 4S SIP Proxy/Registrar". The status should be "Started". If this is not the case you should invoke the proxy by selecting "start". In this case, we recommend rebooting the system to make sure that the proxy is running after the reboot.

FIGURE: 4-9

Service Window

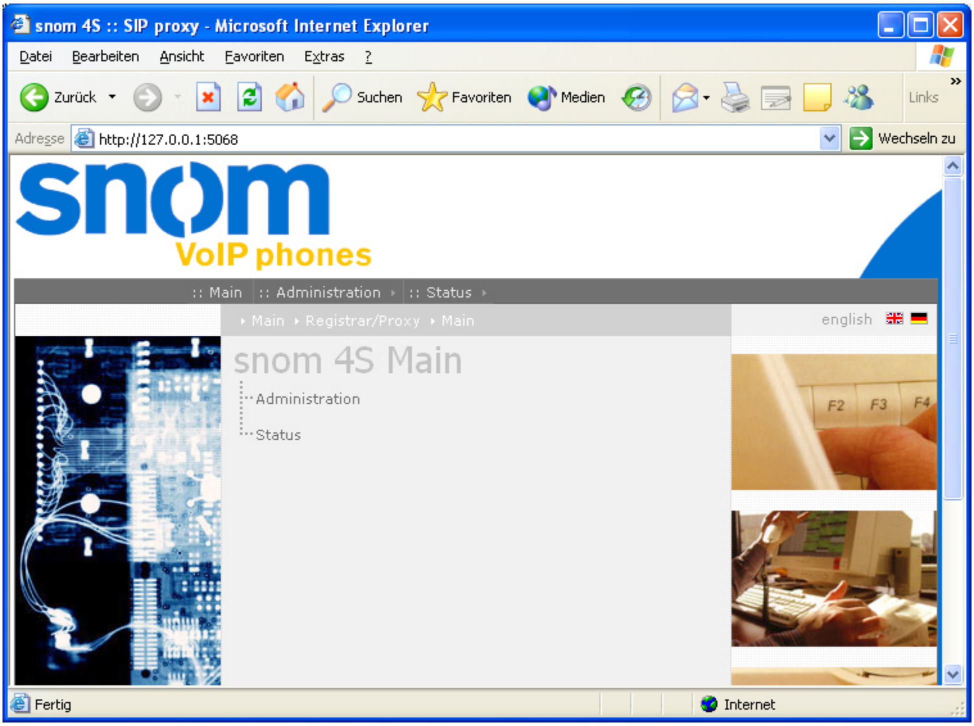


Name	Description	Status	Startup Type	Log On As
Remote Procedure ...	Manages t...		Manual	LocalSystem
Remote Registry Se...	Allows rem...	Started	Automatic	LocalSystem
Removable Storage	Manages r...	Started	Automatic	LocalSystem
Routing and Remot...	Offers rout...		Disabled	LocalSystem
RunAs Service	Enables st...	Started	Automatic	LocalSystem
Security Accounts ...	Stores sec...	Started	Automatic	LocalSystem
Server	Provides R...	Started	Automatic	LocalSystem
Smart Card	Manages a...		Manual	LocalSystem
Smart Card Helper	Provides s...		Manual	LocalSystem
snom 4S SIP Proxy/...	SIP Proxy/...	Started	Automatic	LocalSystem
System Event Notifi...	Tracks syst...	Started	Automatic	LocalSystem
Task Scheduler	Enables a ...	Started	Automatic	LocalSystem
TCP/IP NetBIOS Hel...	Enables su...	Started	Automatic	LocalSystem
Telephony	Provides T...	Started	Manual	LocalSystem
Telnet	Allows a re...		Manual	LocalSystem
Uninterruptible Pow...	Manages a...		Manual	LocalSystem
Utility Manager	Starts and ...		Manual	LocalSystem
Windows Installer	Installs, re...		Manual	LocalSystem
Windows Managem...	Provides s...	Started	Automatic	LocalSystem
Windows Managem...	Provides s...	Started	Manual	LocalSystem
Windows Time	Sets the co...		Manual	LocalSystem

After making sure the proxy is running, you should connect to the proxy to a web browser. In order to do this, you can connect to the address of the local computer (http://127.0.0.1:8080 if you are running the web browser on the same machine). If the http port is already occupied by other programs, the proxy will try to use ports 5068, 5069, 5070 and so on. It is important that you connect to the proxy to a web browser, because that is the only way to control the proxy.

FIGURE: 4-10

Initial snom 4S Screen

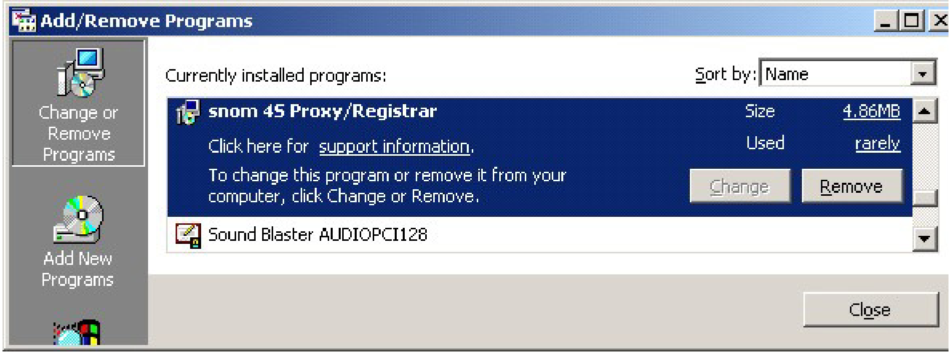


Uninstalling in Windows

To uninstall the proxy, first stop it in the services window. Then go to the Software Window and click on “remove” for snom 4S proxy Server.

FIGURE: 4-11

Uninstalling in Windows



Add/Remove Programs

Currently installed programs:

Sort by: Name

snom 4S Proxy/Registrar — Size 4.86MB

Click here for support information. — Used rarely

To change this program or remove it from your computer, click Change or Remove.

Sound Blaster AUDIOPCI128

Linux

Manual Starting

If you just want to try the proxy, it should be enough to start the proxy manually. Load the tarball to a directory of your choice and start the proxy with the command “proxy”. You can use the command line arguments shown in the next chapter. You don‘t need to have root permissions to run the proxy in this mode, normal user rights are enough.

Automatic Starting

If you want the proxy to be started automatically after a reboot, you need to set up some files as a root. Make sure that you are logged in as root and go to the directory where you want to put the proxy. This directory will have subdirectories for the different proxy versions and for registrations. It typically also contains the configuration information.

```
cd /usr/local

mkdir snom-proxy

cd /usr/local/snom-proxy
```

Extract the files from the tarball:

```
su -

cd /usr/local

tar xvfz ~/snom_sip_proxy-i386-linux-2.14.tgz

cd snom_sip_proxy-i386-linux-2.14
```

The tarball includes a shell script with the name install.sh which sets up the neccessary files and links for you.

```
./install.sh
```

The file /etc/rc.config (for SuSu Linux) and /etc/init.d/functions (for RedHat) are appended with the variable „START_SIP_PROXY“ and the SIP_ PROXY_OPTS variable is set to a value depending on the html port that you specify. You can edit the file and modify the value.

The installation script will install a command rcsip-proxy. rcsip-proxy start starts the proxy while rcsip-proxy stop terminates the proxy process.

After the installation you should see that the proxy is running. Open a web browser to see if the proxy is up and running. Reboot the system and check whether the sip proxy was started automatically after the reboot. You can then continue with the installation using the web browser. Stop and restart the proxy with the rcsip-proxy command to check whether the configuration has been saved.

After several installations, the directory could look like this:

```
lrwxrwxrwx 1 root root      30 Aug 24 11:42 proxy -> snom_sip_proxy-i386-linux-2.12
-rw------- 1 root root    1472 Aug 22 16:17 proxy.txt
lrwxrwxrwx 1 root root      57 Aug 24 11:42 proxy_manual.pdf -> snom_sip_proxy-i386-linux-2.12/
snom 4S SIP Proxy-2.12.pdf
drwxr-xr-x 2 root root   73728 Aug 24 11:56 registrations
drwx--x--x 3 root root    4096 Jul 19 15:04 snom_sip_proxy-i386-linux-2.10
-rw------- 1 root root 3900938 Jul 19 15:04 snom_sip_proxy-i386-linux-2.10.tgz
drwx--x--x 3 root root    4096 Aug 12 14:09 snom_sip_proxy-i386-linux-2.11
-rw------- 1 root root 3902694 Aug 12 14:09 snom_sip_proxy-i386-linux-2.11.tgz
drwx--x--x 3 root root    4096 Aug 24 11:41 snom_sip_proxy-i386-linux-2.12
-rw------- 1 root root 3903533 Aug 24 10:32 snom_sip_proxy-i386-linux-2.12.tgz
```

To update a version, copy the latest tarball into the directory and run the install script of the new version. It will automatically shut down the old proxy and run the new one. This takes less than a second and all registered users will be still registered. Even ongoing phone call will continue as the proxy keeps only little state information about ongoing calls (however ongoing calls will not go to the call log). Typically, users will not observe the updating process.

snom 4S • SIP

Registrar/Proxy 2.14

Registering Phones

As an example, we show you here how to register a snom 100 VoIP phone and a Microsoft Messenger with the proxy.

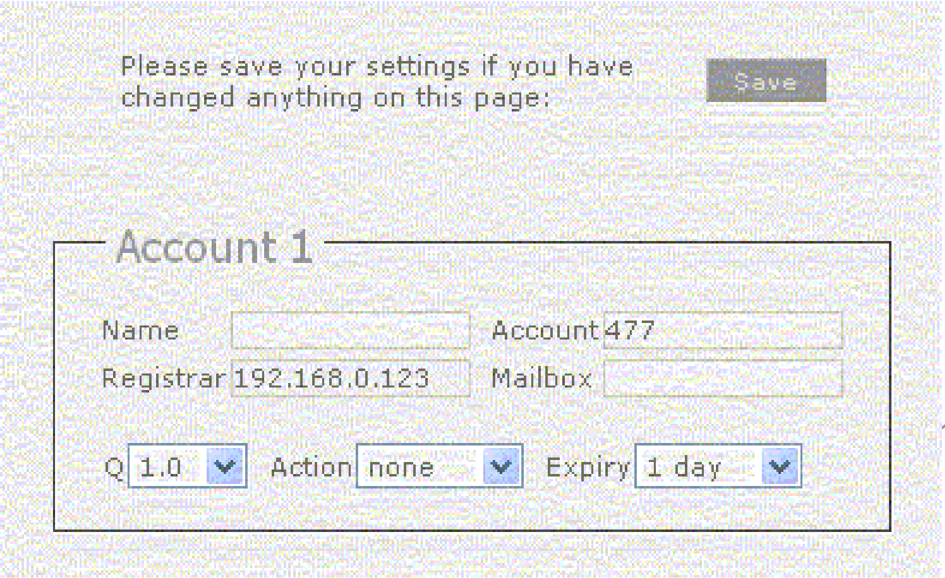
Important: Before you can try this on your proxy, you need to set up the proxy. See Chapter 6 on how doing this.

snom 100 Registration

We assume here that the proxy has the address 192.168.0.182. This address could of course also be a DNS name, but in this example we want to use explicit IP addressing. The phone is behind NAT and has a NAT gateway located at 192.168.0.1.

FIGURE: 5-1

Registering snom VoIP phone



Please save your settings if you have changed anything on this page:

Account 1

Name

Account 477

Registrar 192.168.0.123

Mailbox

Q 1.0

Action none

Expiry 1 day

All we need to do is fill in the Name, the Account and the Registrar information. Because we are behind NAT, we also need to provide the outbound proxy (see the information on NAT gateway).

Looking at the trace of the phone, we see the request going to the proxy and the response coming from the proxy:

Sent to udp:192.168.0.1:5060 at Wed, 31 Dec 1969 21:25:22:458 GMT:

```
REGISTER sip:snomag.de SIP/2.0
Via: SIP/2.0/UDP 192.168.0.11:5060;branch=z9hG4bK-
9jodhbwsu13y
Max-Forwards: 70
From: “Theo Test” <sip:test@snomag.de>
To: “Theo Test” <sip:test@snomag.de>
Call-ID: 00004c4165c8-7tbzmqd51asz@192.168.0.11
User-Agent: snom100-1.11g
CSeq: 10 REGISTER
Route: <sip:192.168.0.1;lr>
Contact: <sip:test@192.168.0.11:5060;line=1>;q=0.7
Expires: 86400
Content-Length: 0
```

Received from 192.168.0.1:5060 at Wed, 31 Dec 1969 21:25:22:614 GMT:

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.0.11:5060;branch=z9hG4bK-
9jodhbwsu13y
From: “Theo Test” <sip:test@snomag.de>
To: “Theo Test” <sip:test@snomag.de>
Call-ID: 00004c4165c8-7tbzmqd51asz@192.168.0.11
Contact: <sip:test@192.168.0.11:5060;line=1>
CSeq: 10 REGISTER
Date: Sun, 9 Jun 2002 18:19:54 GMT
Expires: 3600
Content-Length: 0
```

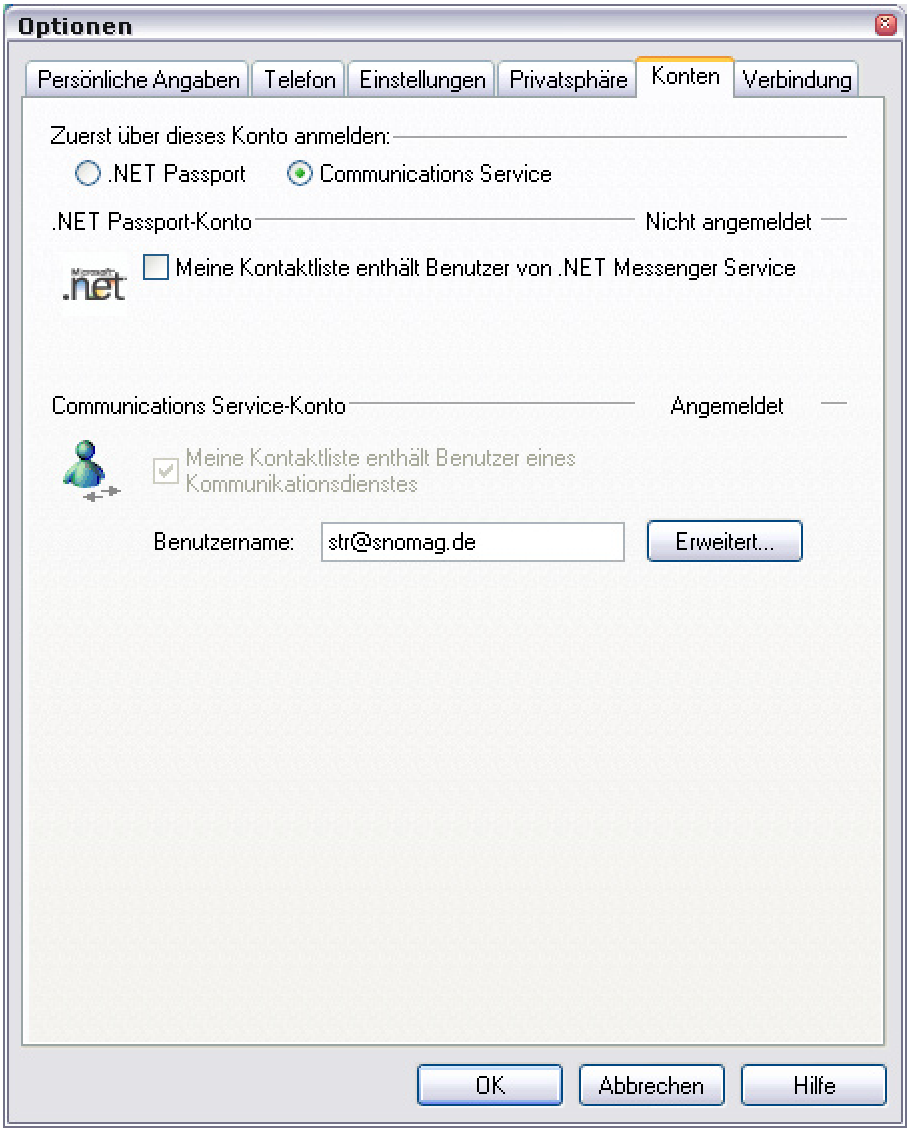
Microsoft Messenger Registration

Microsoft Messenger supports SIP from Version 4.6 ongoing. To register the messenger with a snom proxy, you need to carry out the following steps:

- Open Microsoft Messenger
- Go to Extras/Options
- In the Tab Accounts select communication services and enter the URL that you want to be registered with, e.g. fred.feuerstein@snomag.de.

FIGURE: 5-2

Microsoft Messenger Registration



Optionen

Persönliche Angaben | Telefon | Einstellungen | Privatsphäre | Konten | Verbindung

Zuerst über dieses Konto anmelden:

○ .NET Passport ● Communications Service

.NET Passport-Konto — Nicht angemeldet

□ Meine Kontaktliste enthält Benutzer von .NET Messenger Service

Communications Service-Konto — Angemeldet

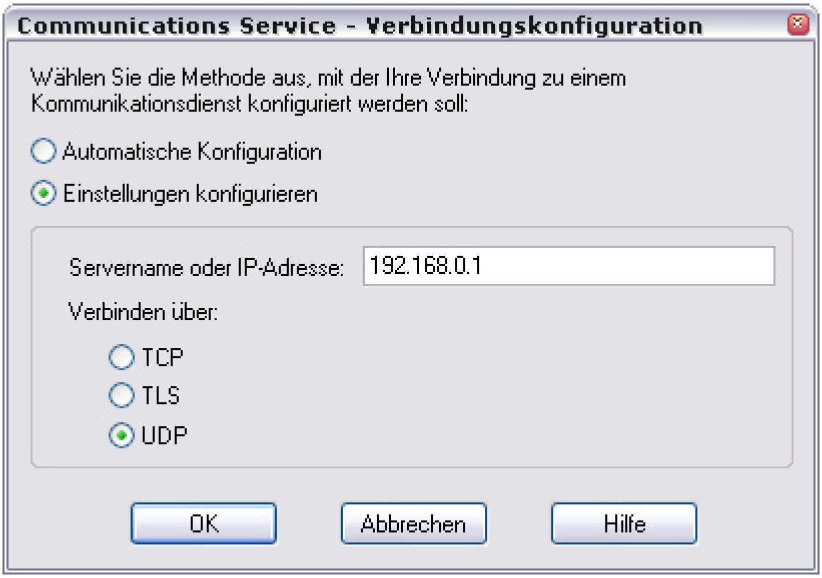
☑ Meine Kontaktliste enthält Benutzer eines Kommunikationsdienstes

Benutzername: str@snomag.de

- If you need an outbound proxy, you can enter this information when you click on Advanced. Select UDP transport mechanism and set the Servername of IP address to the address of the outbound proxy.

FIGURE: 5-3

Outbound Proxy



Communications Service - Verbindungskonfiguration

Wählen Sie die Methode aus, mit der Ihre Verbindung zu einem Kommunikationsdienst konfiguriert werden soll:

○ Automatische Konfiguration

● Einstellungen konfigurieren

Servername oder IP-Adresse: 192.168.0.1

Verbinden über:

○ TCP

○ TLS

● UDP

If you go to the trace page of the proxy, you can see the registration messages:

```
REGISTER sip:snomag.de SIP/2.0
Path: <sip:217.88.123.51;lr>
Max-Forwards: 70
Via: SIP/2.0/UDP 217.88.123.51;branch=7bd0c34ce79c7c00ac6f2
9345595fd6a
Via: SIP/2.0/UDP 192.168.0.182:10379
From: <sip:str@snomag.de>;tag=494c7662-e8dd-4358-95e1-
2721f10cee48
To: <sip:str@snomag.de>
Call-ID: 2cfe99b4-3e65-42c0-b87a-465a7a04069d@192.168.0.182
CSeq: 1 REGISTER
Contact: <sip:192.168.0.182:10379>;methods=”INVITE,
MESSAGE, INFO, SUBSCRIBE, OPTIONS, BYE, CANCEL, NOTIFY,
ACK”
User-Agent: Windows RTC/1.0
Expires: 1200
Event: registration
Allow-Events: presence
Content-Length: 0
```

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 217.88.123.51;branch=7bd0c34ce79c7c00ac6f2
9345595fd6a
Via: SIP/2.0/UDP 192.168.0.182:10379
From: <sip:str@snomag.de>;tag=494c7662-e8dd-4358-95e1-
2721f10cee48
To: <sip:str@snomag.de>
Call-ID: 2cfe99b4-3e65-42c0-b87a-465a7a04069d@192.168.0.182
Contact: <sip:192.168.0.182:10379>
CSeq: 1 REGISTER
Date: Sun, 9 Jun 2002 18:28:20 GMT
Expires: 1200
Content-Length: 0
```

You then can make your first test call.

The snom 4S Proxy/Registrar supports presence and instant messaging with the Microsoft Messenger. Just enter the contact that you would like to see; the proxy will handle the traffic to the registered Microsoft Messenger client.

Important: Turn loose routing off when using the Microsoft Messenger. This is done by default.

snom 4S • SIP

Registrar/Proxy 2.14

General Concepts

Some general concepts need to be explained before you set up the proxy.

Security

When a request arrives at the proxy, it may trigger actions requiring security measures.

Examples include:

- dialling numbers that cost money,
- avoiding anonymous calls, and
- avoiding attacks like hanging up calls without being involved.

The principle for authenticating requests in SIP resembles the mechanism used for http, called challenging. It can be illustrated like this:

- The user agent wants something from the proxy and sends a request to the proxy.

- The proxy says “thank you, but in order to do this please answer the following question”. The proxy keeps a list of questions that are open and discards them after a timeout.

- The user agent checks if it can answer the question. If it can, it sends a new request that contains the question; if it can not it gives up.

- The proxy checks if the answer is correct and corresponds to an open question. If that is the case, the request passes; if not the proxy generates another question.

The answer depends on the realm, the username and the password stored in the proxy and in the user agent. By looking at the answer, it is not possible to find out anything about the password or username.

The setup process is important in ensuring security. When you use a web browser to set up usernames and passwords, this information is transported without security over the network. You should therefore follow the following guidelines:

- Using a password on web interfaces does not help, because the data transported is not encrypted using this mechanism. If you open a web page that contains the password, it will also be transported over the network without encryption.

- The realm and the usernames are no big secret. But make sure that passwords are not sent over insecure parts of the network. On a phone, you can set up the password using the phone keyboard, for the proxy you can use the loop back device 127.0.0.1 for the setup process, if you are logged on the proxy host.

Reliabilty

Proxy failure

It is a fact of life that computer systems can crash. Some precautions can limit the damage. The general approach to address failure is to use redundancy. If one computer fails for one day a year, two might fail only for a couple of minutes.

SIP supports redundancy with the “DNS SRV” model. Behind a DNS address there may be several IP addresses, each of them pointing to a different proxy. If one fails, the user agent goes to the next proxy and the service goes on.

Terminal Failure

When a terminal fails (because of power failure, network disconnection or other events), the other side might not get a disconnection message. This can be a problem for media server and billing programs. For this purpose, the session can be periodically refreshed. This is called "Session Timer". Depending on the refresh rate of the timer, the timing, for billing purposes for example, can be made very accurate.

Transport Layer

SIP today uses UDP as main transport layer. Unfortunately, it is perfectly legal that UDP packets get lost on their way to the destination. Because of this, the SIP programs must retransmit their UDP messages until they receive a feedback that the message has been received by the other party.

This can cause problems when large packets are being transmitted. In most networks, large UDP packets are split up into several smaller packets, which are transmitted independently and which have their own individual chance of getting lost. To avoid this, the latest SIP standard recommends using a different transport layer for this, TCP. The snom 4S proxy supports both transport layers and automatically detects whether an old SIP device cannot handle TCP packets.

State

The snom 4S SIP proxy handles "stateful" information. This is information that needs to be stored somewhere until another event happens. This information primarily affects registrations, as they might be refreshed only after hours or even days. It is therefore important to store this information in a safe place which will be stable even after a crash or reboot. The use of redundancy to make file systems more resilient is a proven solution in these cases.

There are several solutions available here, and the snom 4S builds upon these mechanisms. Registrations may be stored in a safe place, and stateful information may be recovered by reading it from the file system.

Other stateful information is less critical. When forking a request, there needs to be some state information about the fork. However, because this information usually has a scope of only a few seconds, this information is not stored in a separate database. In a case of a reboot, the complete system will recover fast enough.

Overlap Dialling

When a telephone user dials a number, she or he does not have to press enter to start the call in a traditional telephone system. There are two ways to achieve this with the snom 4S:

- Where the length of a telephone number can be determined by a simple rule, a dial plan is used. When the entered number matches a set of pattern, the dialling process is triggered. This is typically the case in USA.

- Where the length of a telephone number cannot be determined beforehand, the network responds with “number incomplete” if more digits are needed to start the call. This mechanism is called overlap dialing.

The same problem occurs when the user enters a SIP URL. Even if the URL contains alphanumeric characters, overlap dialling can be done in SIP. For this the response code 484 was defined in the SIP standard. The proxy responds with this error code when the number detected could not be completed by the PSTN gateway or by the proxy.

Sequential Forking

Forking means that a user may be registered several times and the proxy searches the user on all locations.

For non-INVITE requests (not initiating a call), the proxy just sends the packet to all destinations and waits until all parties have sent a response or a success response arrives.

For INVITE requests (initiating a call) the proxy searches the user according to the probability. Users that registered with a high probability are called first, and then users with a lower probability. When users have the same probability, they are called at the same time, this is called parallel forking. When users have different probabilities, they are called in a row, this is called sequential forking.

When the proxy receives a 3xx response (redirect), it handles them in a special way. If there are other requests pending, it determines the destinations that are provided with the 3xx response and puts them on the list. This is done using the probability of the underlying registrations, and redirected contacts may have an even lower probability.

If the 3xx response for the only pending request, the proxy passes the response through to the request client. The client itself then takes care of the redirection. This is important in cases where a call from a PSTN gateway comes in and should be redirected to a PSTN number. The gateway then does not have to pass the call through the proxy, it can immediately redirect the call on the PSTN level. This does not work however, if the call is redirected to more than one PSTN number, in which case the call will have to go through VoIP.

In many environments, users are registered with a high probability and the mailbox is registered as well, but with a low value. Even if the phone is switched off, the proxy will redirect the call to the mailbox after a timeout.

Network Address Translation

One of the biggest problems with the Internet version 4 is that it has a limited address range. IP V4 defines 32 bits for addresses, which were distributed according to a geographic scheme at a time when the success of the Internet protocol was hard to envision. Regions like Europe or Asia in particular, did not receive enough numbers to connect every network element with its own IP address. Because of this, in many installations several computer and network elements have to share one IP address. They do this by using different ports of the address. An IP packet may go to one of 65,535 ports, making up roughly 16 bits and extending the internet address to about 48 bits.

The computer that owns the IP address is called the network address translation (NAT) gateway. This computer has one "real" IP address (called public IP address) and a private IP address that is visible only to the computers that share the public IP address in a private network. The internet society has defined a specific address space that is used as private IP addresses (192.168.x.x, 10.x.x.x and 172.[16-31].x.x).

The NAT gateway keeps a list of ports and associated private IP addresses. Whenever a packet arrives at the NAT from the public Internet, the NAT gateway looks into the list and forwards the packet to the associated computer and port. When a packet arrives from a private address, the NAT forwards it to the Internet and keeps an association between the private address and the port used for the forwarding. In this way the association table can be set up. There are hundreds of other ways to set up and maintain the NAT table. The mechanism is often combined with a firewall that inspects packets during the forwarding process.

The Internet Protocol V6 solves the NAT problem in a different way. They simply use many more bits to identify a host, but this is much harder to implement and maintain, so NAT is still more popular.

Routing

SIP messages flow from a user agent (the user agent client, UAC) through a number of proxies to another user agent, the user agent server (UAS). This creates a path, the “routing path” that needs to be remembered for further messages. For instance, if a proxy wants to carry out billing, it needs to see all messages between the user agents to determine how long the call took.

To do this, a proxy can insert a header into requests that indicates that it would like to stay in the routing path in future requests. Unfortunately, the first proposals for doing this did this in a complicated way that can cause problems under certain circumstances. For this reason, “loose routing”, a new and better way of routing messages was developed. The snom 4S supports both routing methods.

snom 4S • SIP

Registrar/Proxy 2.14

Configuration

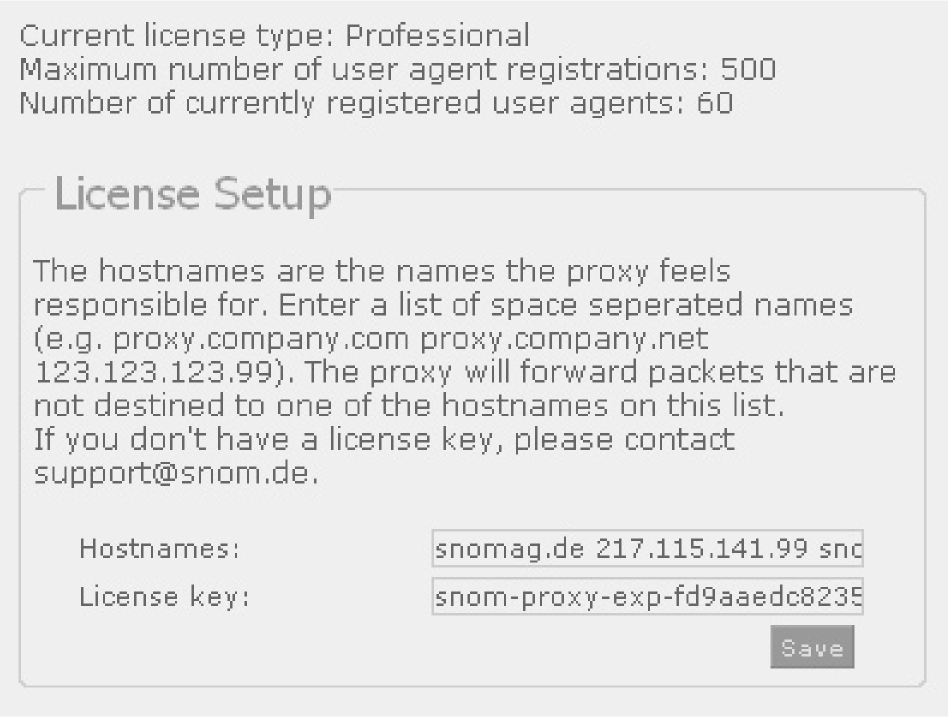
The proxy can easily be set up via a web browser. To access the proxy, just enter the name of the computer where the proxy is running. If you have configured the proxy to use a port other than 80, you will need to append the URL with a colon and the port number, e.g. “http://proxy.mycompany.com:5069”. You can access the different menu items of the proxy by moving the mouse over the top level menu items “Administration” and “Status”. Move the mouse over the pop-up menu items and click on the item you want to select.

Licensing

Before you start operation, you need to set up the licensing part of the proxy. To do this, go to the Administration/Licensing web page and enter the host names, the IP addresses of the proxy (if not proposed correctly) and the license key that you received with the software. If you don’t have a license key, contact mailto:support@snom.de for one. After saving this page, the license type and the number of currently registered users is displayed on top of the page.

__FIGURE: 7-1__

Licensing



Current license type: Professional
Maximum number of user agent registrations: 500
Number of currently registered user agents: 60

License Setup

The hostnames are the names the proxy feels responsible for. Enter a list of space seperated names (e.g. proxy.company.com proxy.company.net 123.123.123.99). The proxy will forward packets that are not destined to one of the hostnames on this list.
If you don't have a license key, please contact support@snom.de.

Hostnames: snomag.de 217.115.141.99 snc

License key: snom-proxy-exp-fd9aaedc8235

Hostnames

You need to enter a list of names that the proxy feels responsible for. When a packet arrives at the proxy, the proxy checks the given hostname against the list you enter in this field.

Typically, this name contains a list of all fully qualified DNS names for the host (e.g. „rumba.company.com sip.company.com company.com company.net"). The list may also contain addresses which can only be located via DNS SRV. This is very helpful in situation when you want to run you mail, www and sip server on different machines but they should share the same name (e.g. company.com is the root domain, but the sip server is running on sip.company.com).

You should also include the IP address of the proxy, because many user agents need to register with the IP address of the proxy.

Using the local host name (like tango) is normally not helpful as this hostname cannot be resolved by DNS. If you do not plan to locate the SIP server via DNS, you should just put in your IP address here.

License Key

Enter the License Key into this field. The key depends on the list of host names and the license type.

After pushing the save button, the web client should show the license type and the menus for the license type become available.

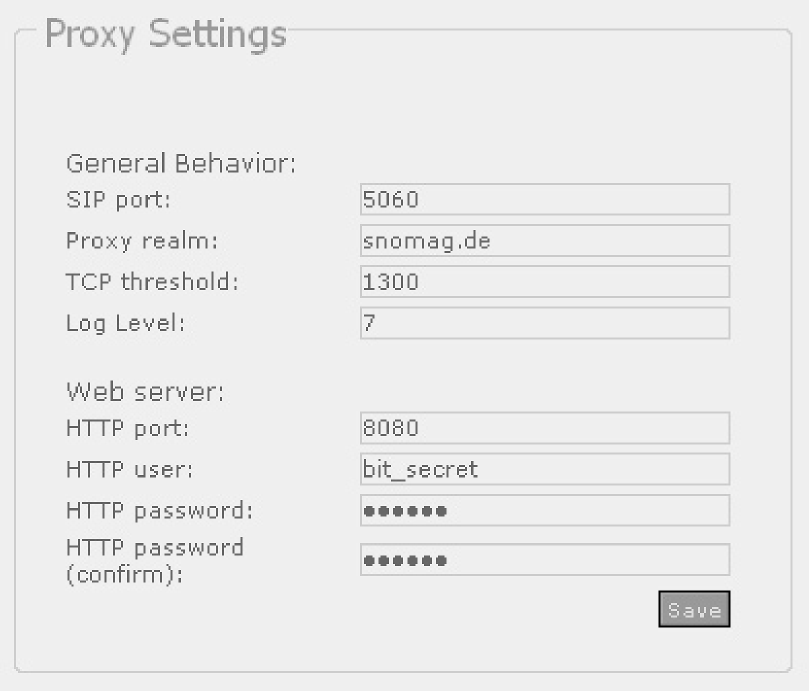
If the web client shows „not licensed‟, please send the list oh hostnames and the IP addresses to mailto:support@snom.de.

General Settings

There are a number of general settings that you should set up in the beginning. To do this, go to the Administration/Settings menu item.

FIGURE: 7-2

General Setup



Proxy Settings

General Behavior:

SIP port:	5060
Proxy realm:	snomag.de
TCP threshold:	1300
Log Level:	7

Web server:

HTTP port:	8080
HTTP user:	bit_secret
HTTP password:	●●●●●●
HTTP password (confirm):	●●●●●●

SIP Port

The SIP port defines where the proxy expects SIP traffic. Typically, this will be port 5060.

If you use a different port, you should make sure that all clients use that port too. This can be done by appending the port to the URL explicitly or by using DNS SRV (see below).

Proxy realm

When the proxy challenges users for authentication (see above), it needs a proxy realm to do so. The clients search the list of possible user names and passwords according to this realm value. If there is only proxy, the default value should be set to “snom”, but if packets might run over several proxies, you should choose a more unique value like “SIP proxy on mycompany.com”.

Remember that these values need to be set up on the user agents that you plan to use with the proxy as well.

TCP threshold

SIP uses both reliable and non-reliable transport layers. The snom proxy version 2.14 supports UDP and TCP transport layers.

When the proxy needs to send a request, it has to make a decision which transport layer to use. The TCP threshold value is compared against the packet length. If it is less that the threshold value, the proxy uses UDP, otherwise TCP. If you want the proxy to use only UDP, you can enter a large number here (e.g. 1000000); if you want the proxy to use only TCP, enter a 1 here.

The recommended value for this field is 1300. Using this value, a UDP packet can be sent within one Ethernet frame without fragmentation.

Log Level

The log level defines how many messages get to the log. If you are only interested in the most important messages, you can set this to 0. If you want to see any possible log message, set this field to 9.

The log is kept internally within the proxy. After a certain number of log entries have been reached, the oldest entries are removed from the log, so that there is no danger of memory overflow from files getting too large.

HTTP port

The http port is used to contact the web server of the proxy. If you can see the configuration page, you have found the right port. However, sometimes you might want to change the port number to a different value (e.g. to install the mailbox). In this case, enter the desired port number here, and restart the proxy.

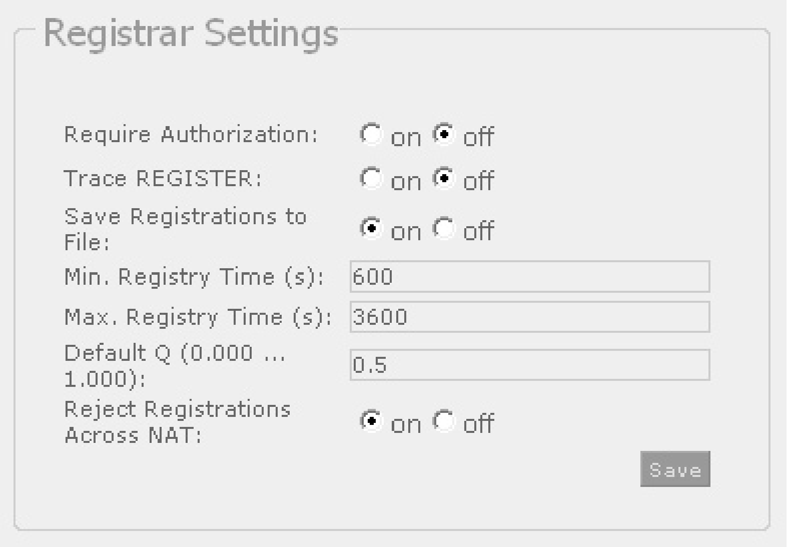
HTTP User and Password

To protect the access to the web server, you can set up a user name and a password for the web server. Remember that this provides only basic security, as the content of the web page is transmitted without encryption over the network and the passwords can easily monitored by network specialists. However, it avoids everybody easily accessing the proxy.

Registration

FIGURE: 7-3

Registration Screen



Registrar Settings

Require Authorization: ○ on ● off

Trace REGISTER: ○ on ● off

Save Registrations to File: ● on ○ off

Min. Registry Time (s): 600

Max. Registry Time (s): 3600

Default Q (0.000 ... 1.000): 0.5

Reject Registrations Across NAT: ● on ○ off

Require Authorization

If the flag is set to "on", all registration requests for the proxy are challenged for authentication. This means that unknown users can not register on the proxy. If the flag is set to "off", only known users are challenged, that means the proxy is open for registration. The list of users is discussed below.

Trace REGISTER

Tracing REGISTER messages in the proxy trace is sometimes undesirable, because it just fills up the trace. If you turn this flag to "off", REGISTER messages and their associated replies are only traced in the Registered Users window (behind the link, see below).

Save Registrations to File

If you turn this flag on, the registrations are stored in the registrations directory (see crash recovery above). The directory name is set up during installation.

Min and Max registration time

User agents register for a specific amount of time. If a user agent does not refresh a registration before this time, the registration is silently discarded. The registration time may be limited to a minimum and maximum time.

Limiting the minimum registration time avoids too many refreshes which cause network overhead. Limiting the maximum registry time reduces the danger of a user agent being unreachable for a longer period of time.

Typical values for minimum and maximum times are 30 seconds and 7200 seconds (two hours).

Default Q

When a user agent registers with the proxy, it should indicate the probability with which the contact can be found at this address. This value control the sequence in which the proxy searches for a user (see sequential forking) For instance a mailbox would register with the proxy with a low probability; a softphone would reregister with a lower probability value when the screen saver goes on.

In this field you can define which value should be taken if no such value has been specified. The value must be in the range between 0.0 and 1.0. A good value is 0.5 or 1.0.

Reject Registrations Across NAT

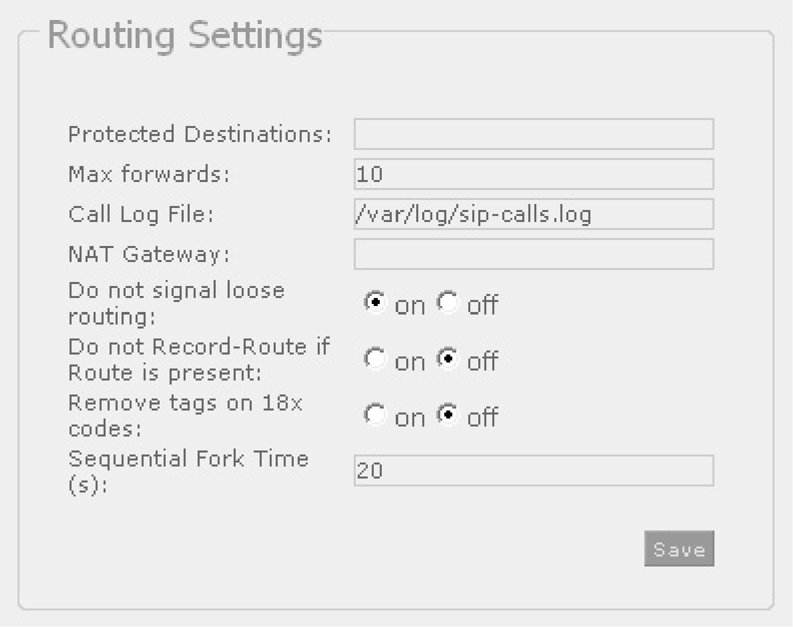
When a user agent registers, it provides a contact and a path that tell the registrar how the user agent can be reached. If the packet goes through NAT-aware equipment, the proxy will get not only the private address but also the qay to get there (see the Path header).

When a user agent from a private address registers without a path at a public address, the registration will fail in most cases. Unfortunately, the registration is shown in the list of registered users, but the registration response never made it back to the user agent. This annoying effect can be avoided by turning the flag on. The proxy will then not accept private IP address registrations if they have a public address and if there is no path provided with the registration. Instead it will write a log entry.

Routing

FIGURE: 7-4

Routing Screen



Routing Settings

Protected Destinations:

Max forwards: 10

Call Log File: /var/log/sip-calls.log

NAT Gateway:

Do not signal loose routing: ● on ○ off

Do not Record-Route if Route is present: ○ on ● off

Remove tags on 18x codes: ○ on ● off

Sequential Fork Time (s): 20

Protected Destinations

When the proxy needs to forward a request, it first checks this field for protected destinations. If one of the destinations match the requested URL, the proxy first challenges the client for authentication.

The protected destinations are seperated by space and contain a pattern according to the rules described in the Dial Plan (see below).

Typically, you want to protect access to the PSTN (because this requires payment). For example, if your PSTN gateways are located at 192.168.0.248 and 192.168.0.249 and the dial plan starts using the PSTN gateway after 4 digits, you would enter a pattern like „sip:$$$$%@~ sip:$$$$%@192.168.0.24[8-9]“. The first pattern makes sure that every request that would be redirected to the PSTN gateway is challenged, the other patterns make sure that direct access to the PSTN gateway is challenged.

If you leave the field blank, the proxy will forward any packet without challenging. If you enter just „*", the proxy will challenge every request.

Max Forwards

Messages in SIP may hop over a number of proxies, and sometimes the path contains loops. Sometimes the loops are endless, and in these situations the criterion for rejecting a message is to look at the number of hops the request has done so far.

This setting controls how many hops a request can make before it is rejected as an endless loop. 70 is the default value; in many environments you can significantly lower this value.

Call Log File

Calls may be logged to a file. If you enter a file name here, the proxy will try to append a line for every call that went through the proxy. See Call Log File Format below for the content of this file.

NAT Gateway

Other calls need to pass through a network address translation (NAT) gateway or a firewall. The criterion for this is when the proxy is in a private network address space and the destination is a public address.

The NAT gateway setting has the same format as the PSTN gateway setting.

Do not signal loose routing

Although loose routing is mandatory for new SIP equipment and is compatible with the old routing method ("strict routing"), some equipment can still cause headaches. You can use the old-style routing by turning this flag on. If you know your equipment does not have a problem with loose routing, turn the flag off. If in doubt, it is better to turn this flag on.

Do not Record-Route if Route is present

Some old equipment does not like to see both recorded routing elements and an already available route path in the SIP header at the same time. In these cases it might help to switch this flag on; however the price of this is that the proxy is probably not in the route of future requests any more. This means you will not be able to see a proper call log even if the phone calls have been successfully made.

Remove Tags on 18x

Some equipment cannot handle different To-tags coming from forking INVITE requests. If you turn this flag on, the To-tags on 18x replies are removed before they are passed down to the user agent client. Typically you will not need to turn this flag on.

Sequential Forking Time

The proxy needs to schedule the sending of INVITE requests. This is done by looking at the user with the highest probability for the call and scaling the other users according to this probability and the sequential forking time. This setting defined the time between the first ringing of a user agent and the maximum time in seconds until the last user agent rings.

For example, if there are three users for number “abc” with the probabilities 0.9, 0.5 and 0.1 and the sequential forking time is 30 seconds, the contact with probability will ring immediately, the contact with probability 0.5 after 30 x (0.9 – 0.5) / 0.9 = 13 s and the contact with probability 0.1 after 27 s. If someone picks up the call, the others will stop ringing immediately.

User Administration

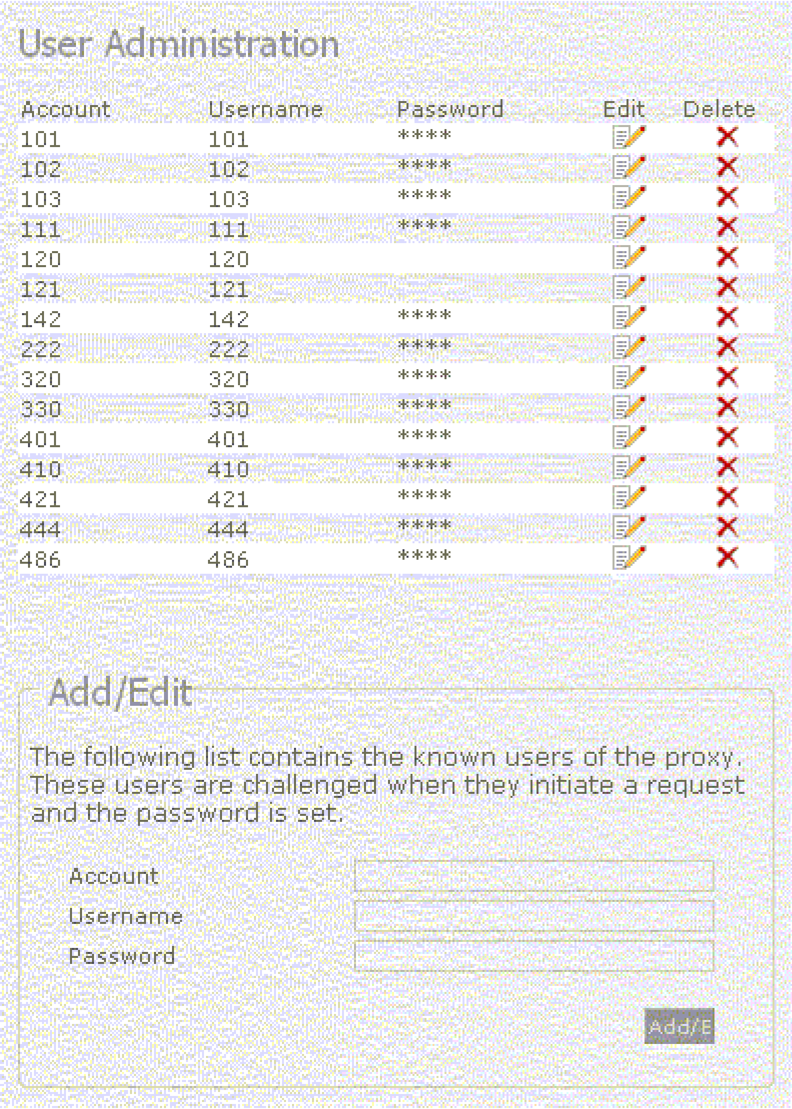
The “well-known” users of the proxy may be challenged on registration and on forwarding requests. This way you can ensure that users are really who they claim to be, and give them special rights (e.g. to make international calls).

User accounts can easily be set up with the web browser. Just go to “User Administration” and add new users. To delete users, click on the delete button of the respective user.

The user account is the part that occurs in the URL. The “user name” and the “password” are requested during authorization. They should be kept in a secure place and set up on the local machine, avoiding the sending of passwords over the network.

FIGURE: 7-5

User Account



User Administration

Account	Username	Password	Edit	Delete
101	101	****	✎	✕
102	102	****	✎	✕
103	103	****	✎	✕
111	111	****	✎	✕
120	120		✎	✕
121	121		✎	✕
142	142	****	✎	✕
222	222	****	✎	✕
320	320	****	✎	✕
330	330	****	✎	✕
401	401	****	✎	✕
410	410	****	✎	✕
421	421	****	✎	✕
444	444	****	✎	✕
486	486	****	✎	✕

Add/Edit

The following list contains the known users of the proxy. These users are challenged when they initiate a request and the password is set.

Account	
Username	
Password	

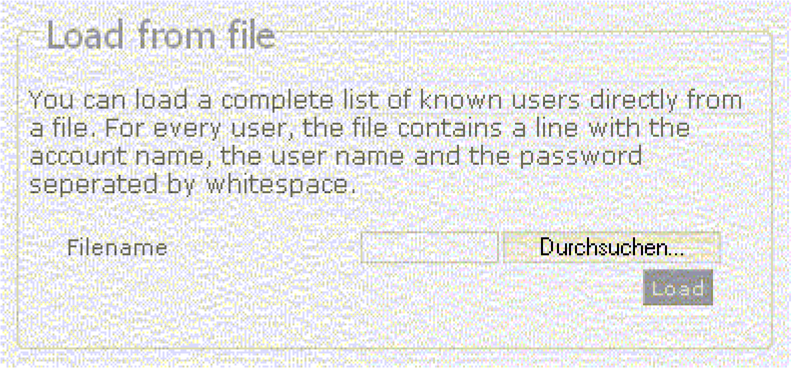
To load a large number of users at one, you may use the “Load from File” feature. The file that you select there needs to be in a simple ASCII format as follows.

Each line describes a user. The first entry defines the account, the second the username and the third the password. The entries are seperated by whitespace. Comment lines can be set up by using a ‚#‛ at the beginning of the line.

Loading accounts from a file erases all accounts that have been set up so far.

FIGURE: 7-6

Load Accounts



Load from file

You can load a complete list of known users directly from a file. For every user, the file contains a line with the account name, the user name and the password seperated by whitespace.

Dial Plan

How it works

The dial plan is a flexible way to tell the proxy what to do with calls that do not go to a registered user. The algorithm for checking the dial plan is simple:

- Determine the source user/group by looking at the “From” header of the request (take only a look at the URL provided there)
- Determine the destination by looking at the request URL
- Go through the dial plan and take the last match found as result (if there is no match, allow the request).

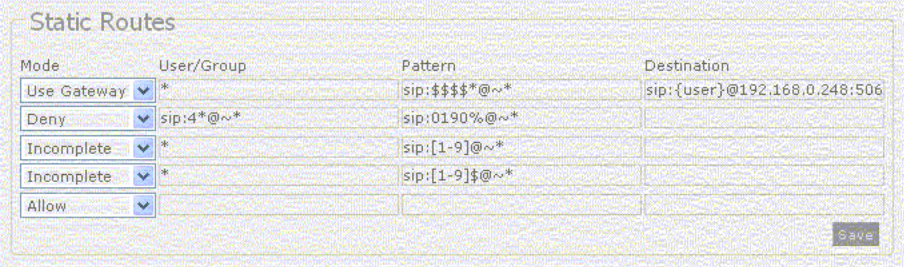
Checking the user/group limits the pattern to a specific list of users. This way you could, for example, grant the sales people the right to make international calls, while everybody else is limited to local calls. Looking at the destination you can find out if the call is local, international, going to the boss, and so on.

The matching process is done using the following “wildcards”:

- ‘?’ matches any character as long as there is one.
- ‘$’ matches a E164 number (0-9, #, * and also + and -).
- ‘*’ matches any character multiple times, even if there is no character.
- ‘%’ matches E164 numbers multiple times, even if there is no digit.
- ‘~’ matches one of the hostnames of the proxy.
- ‘=’ matches the PSTN gateway.
- ‘[a-z]’ matches a character range (in this example from a to z).

FIGURE: 7-7

Static Routes



Static Routes

Mode	User/Group	Pattern	Destination
Use Gateway	*	sip:$$$$*@~*	sip:{user}@192.168.0.248:506
Deny	sip:4*@~*	sip:0190%@~*	
Incomplete	*	sip:[1-9]@~*	
Incomplete	*	sip:[1-9]$@~*	
Allow			

The comparison process <u>includes</u> the sip identifier at the beginning of the URL.

The action can be one of the following:

- “Allow” tells the proxy to use this number as is.
- “Deny” tells the proxy to forbid this number (error code 403 Forbidden).
- “Incomplete” tells the proxy to signal that more digits are expected.
- “Use Gateway” directs the call to the provided URL pattern, typically a PSTN gateway.
- “Not Found” triggers the proxy to send a “404 Not Found” error code.

The destination pattern may include some special variables:

user[:[*start*][:[*length*]]]: The username of the destination. If the start position is present, a substring starting at position start is taken. If the length parameter is present, only length characters are copied.

host: The host name of the destination.

port: The port of the destination. If no port is available, the default port (5060) is used.

cport: The port of the destination preceded wit a colon. If no port is present, this variable returns the empty string.

parm: The parameter list of the destination.

head: The headers of the destination.

url: The complete destination url.

A typical destination pattern could be „sip:{user:1}@192.168.0.248:5060“. In this example, the first digit of the dialled number is removed and send to a PSTN gateway.

The proxy checks all rules of the dial plan. This has the effect that the **last matching rule** will be executed, not the first one.

Example 1: Setting up overlap dialling

In this example, the proxy should try to use the PSTN gateway when more than three digits have been dialled. Otherwise, the number should be marked as “incomplete”.

Rule	Mode	User/Group	Pattern	Destination
1	Use Gateway	*	sip:$$$$%@~*	sip:{user}@gw
2	Incomplete	*	sip:$@~*	
3	Incomplete	*	sip:$$@~*	
4	Incomplete	*	sip:$$$@~*	

Rule 1 tells to use the PSTN gateway where at least four digits are available and the called proxy is the local proxy. The star behind the tilde matches port numbers which might be part of the URL. This can be left out when all attached SIP devices use the latest SIP draft for generating URLs. The destination will be the dialled number plus the string “@gw”, which would be the gateway in this installation.

Rules 2 through 4 match destinations with 1 to 3 digits. They are marked as “incomplete”, giving the user the chance to enter more digits.

Example 2: North American Dial Plan

This example is suitable for a proxy located in the USA.

Rule	Mode	User/ Group	Pattern	Destination
1	Incomplete	*	*	
2	Use Gateway	*	sip:911*@~*	sip:911@gw1
3	Use Gateway	*	sip:[1-9]$$$$$$@~*	sip:{user}@gw2
4	Use Gateway	*	sip:0[1-9]$$$$$$$$$@~*	sip:{user}@gw2
5	Use Gateway	*	sip:00%@~*	sip:{user}@gw2

Rule 1 defaults all calls (not for registered users) to "incomplete". Rule 2 redirects all emergency calls to the gateway number one, which could be connected a local analog line. Rule 3 redirects local calls (7 digits not starting with 0) to the second gateway; rule 4 does this for national calls (a prefix of 0 indicates a national call). International calls start with two 0s and get redirected in any case to the gateway; this works only if the gateway is able to generate incomplete responses.

Example 3: Do not allow cell phone numbers to certain users

In this example, only certain users may call cell phone numbers (400-499 and 101). This example makes sense if the users 101 and 400-499 are listed in the "well known" user list in the User Management list. This example is for Germany.

	Mode	User/Group	Pattern	Destination
1	Incomplete	*	sip:$@~*	
2	Incomplete	*	sip:$$@~*	
3	Use Gateway	*	sip:$$$%@~*	sip:{user}@gw
4	Deny	*	sip:01$$$$$$$$$%@~*	
5	Use Gateway	sip:4$$@~*	sip:01$$$$$$$$$%@~*	sip:{user}@gw
6	Use Gateway	sip:101@~*	sip:01$$$$$$$$$%@~*	sip:{user}@gw

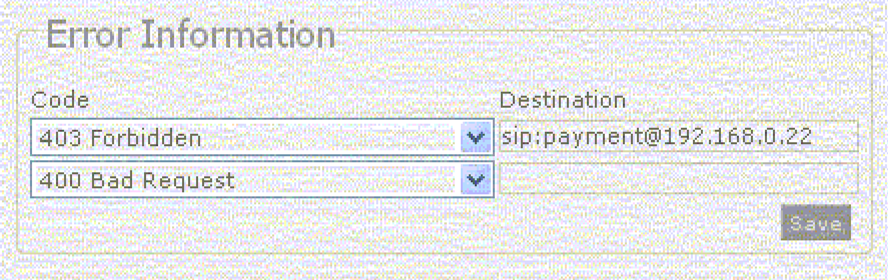
Rules 1-3 redirects call to the gateway if at least three digits are available. Rule 4 defines an exception to this rule if the number starts with 01 and has at least 11 digits (like 01721234567). These numbers are denied for all users, and rules 5 and 6 define the exception to this rule: users 400-499 and user 101 is allowed to place these calls.

Error-Information

Should something go wrong, a telephone system usually generates error reports. In many cases the exact error messages are visible at the protocol level, but the user does not get more than a busy tone. SIP offers improved error information to users. The error information may be on a web page (e.g. http://www.company.com/error-explanations/err_404.htm), but it may also be a SIP URL. While most VoIP phones can not display http content, they can place a call to an announcement server that reads out the error message. This means that the system is much smarter than traditional telephone systems. You can even customize the announcements according to your special requirements.

FIGURE: 7-8

Error Information



Error Information

Code: 403 Forbidden — Destination: sip:payment@192.168.0.22

Code: 400 Bad Request — Destination:

You can simple set up the error information redirection by selecting the approriate error type and enter the destination that should be put into the response. If you leave the destination empty, there will be no error indication for this code.

The following error codes are available:

400 Bad Request	This is a generic error which is not explained in detail.
401 Unauthorized	The request needs authentication; usually the user agent will try again automatically. If they don't have the right credentials, it can inform the user that they need these credentials.
402 Payment Required	The call requires payment.
403 Forbidden	The call is forbidden, this may be because the proxy's dial plan says so or because other network elements think so.
404 Not Found	The destination cannot be found.
405 Method Not Allowed	The destination was found, but does not support the request type.
406 Not Acceptable	There was an unacceptable parameter; this is a generic error message.
407 Proxy Authentication Required	This is like 401.
408 Request Timeout	The destination did not respond at all. Probably it has been switched off.
410 Gone	The destination is switched on, but the requested account is not there.
413 Request Entity Too Large	The request was too large for the destination hardware.
414 Request-URI Too Long	Similar to 413.
415 Unsupported Media Type	The parties are unable to negotiate a common media standard.

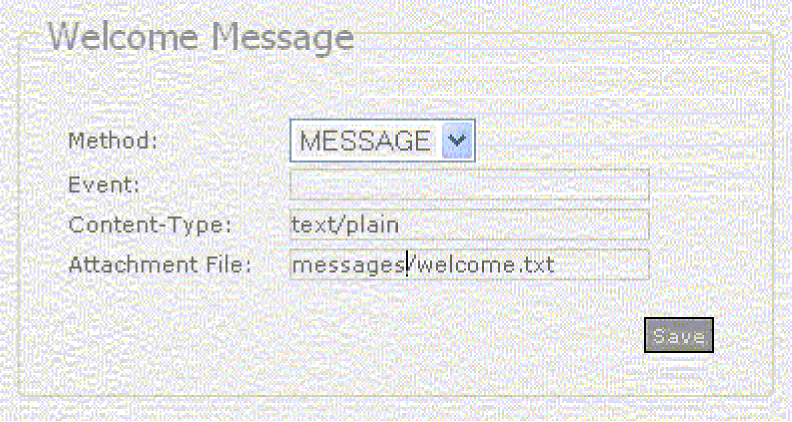
416 Unsupported URI Scheme	The destination is not able to handle the requested URI scheme, e.g. sips:
420 Bad Extension	The caller requested a feature not available at the destination.
421 Extension Required	The destination needs a feature not supported by the caller.
423 Interval Too Brief	There was trouble negotiating the expiry time of a request.
480 Temporarily Unavailable	The requested destination is temporarily unavailable and more detailed information is not available.
481 Call/Transaction Does Not Exist	The request refers to a request which is unknown at the destination.
482 Loop Detected	The request could not be forwarded properly.
483 Too Many Hops	Same as 482.
484 Address Incomplete	The address is incomplete, more digits are required to complete the call.
485 Ambiguous	There were several possibilities for finding the destination, and the destination was not able to determine which one should be the destination.
486 Busy Here	The destination is busy.
487 Request Terminated	The request has been terminated by a CANCEL or BYE request.
488 Not Acceptable Here	Cannot be accepted; this is a fairly generic message.
491 Request Pending	There is another request pending, so the current request cannot be processed.
493 Undecipherable	The message attachment could not be decoded.
500 Server Internal Error	This is a generic network failure message.
501 Not Implemented	The destination does not implement the requested feature.
502 Bad Gateway	The errot came from another network element; this is also quite a generic error message.
503 Service Unavailable	The service is currently not available.
504 Server Time-out	There was no response from a network element.
505 Version Not Supported	There is a problem with the SIP version used.
513 Message Too Large	The message is too large to be processed.
600 Busy Everywhere	There is really a big problem and something for the system administrator.
603 Decline	A network element refuses to work at this time.
604 Does Not Exist Anywhere	The requested resource does not exist anywhere.
606 Not Acceptable	Some aspects of the SDP record are not acceptable, e.g. bandwidth or addressing style. This is also something for your network administrator.

Welcome Message

When a new user signs in, the proxy may send him or her a welcome message. This is a nice feature that informs users about the operators capabilities or downloads operator images onto the phones. When the location of the attachment file changes, the proxy notifies all registered users about the change.

FIGURE: 7-9

Welcome Message



Welcome Message

Method: MESSAGE

Event:

Content-Type: text/plain

Attachment File: messages/welcome.txt

The proxy allows two method for notifying users, message and notify. Notify is typically used for sending media attachments, message is the instant message notification style (which is compatible with most popular equipment). While notify requires a event-type, message usually does not require an event-type. The content-type indicates the type of the attachment. The attachment file points to the location of the file what should be sent to the users.

DNS

What is DNS?

The domain name system (DNS) is a powerful mechanism to make internet addresses human-readable. “www.snom.de” is much easier to remember than 192.67.198.4. But there are also other reasons to use DNS:

If the underlying address changes, the user does not have to change all the addresses in his or her address book. If the address is often used, it can redirect the requests to several servers (server farm) for load balancing. If one server in a server farm fails, another server can continue the operation

One of the key features of SIP is that your email can be the same as your telephone number; your marketing department and your friends will love it.

Setup DNS

Using DNS has two sides: Finding someone with DNS and being found with DNS.

Finding somebody with the proxy is easy. All you need to do is set up the DNS on your computer correctly and the proxy will talk to the DNS server directly to find addresses.

Hint: Both Windows and Linux offer standard DNS functions which are not enough for SIP DNS resolving. Therefore, the proxy contains its own DNS implementation that caches the entries on a private list. The Windows version retrieves the DNS address from the registry, while the Linux version reads out the respective /etc file.

To be found you need the correct DNS server configuration. If you only have one proxy running and you do not plan to use redundancy, all you need to do is make your host known in this DNS server.

To use the DNS searching support, you need to define entries for "_ sip._udp" and "_sip._tcp" for your domain and assign weights and probabilities to the different hosts that serve these services. A configuration file for Linux might look like this:

```
$TTL 1D
anycom.de.      IN SOA  fox.anycom.de.   hostmaster.snom.de. (
                        2002050111      ; serial
                        1D              ; refresh
                        2H              ; retry
                        1W              ; expiry
                        1D )            ; minimum

                IN NS   fox
                IN NS   ns2.nameserver121.com.
                   MX   10 mail.anycom.de.

_sip._tcp.anycom.de.    IN SRV  0 5 5060 sip-server.anycom.de.
                        IN SRV  0 1 5060 test.anycom.de.
                        IN SRV  1 5 5060 www.anycom.de.
_sip._udp.anycom.de.    IN SRV  0 5 5060 sip-server.anycom.de.
                        IN SRV  0 1 5060 test.anycom.de.
                        IN SRV  1 5 5060 www.anycom.de.

localhost       IN A            127.0.0.1
ns              IN A            232.145.142.95
anycom.de.      IN A            232.145.142.95
test            IN A            232.145.142.95
www             IN A            232.145.142.96
sip-server      IN A            232.145.142.97
```

In this example, there are three choices for accessing the proxies for anycom.de. The first two, (sip-server.anycom.de and test.anycom.de) have the weight 0, and as long as one of them is up they will be contacted. Only if both of them are down, will the service go to www.anycom.de. The probability of contacting sip-server is 5/6, the probability of contacting 1/6, as the preference sum is 6. That means that most of the load goes to sip-server.

snom 4S • SIP

Registrar/Proxy 2.14

Maintenance

8

Once the proxy is up and running, you will probably want to take a look on what is going on. There are several pages that give you detailed information about the proxy's state.

Registered Users

To see which users are registered at the proxy, you can go to Status/ Registered Users. You will see a list of the users sorted by account name and probability. On top you see the current time in Greenwich Mean Time (GMT).

The columns have the following meaning:

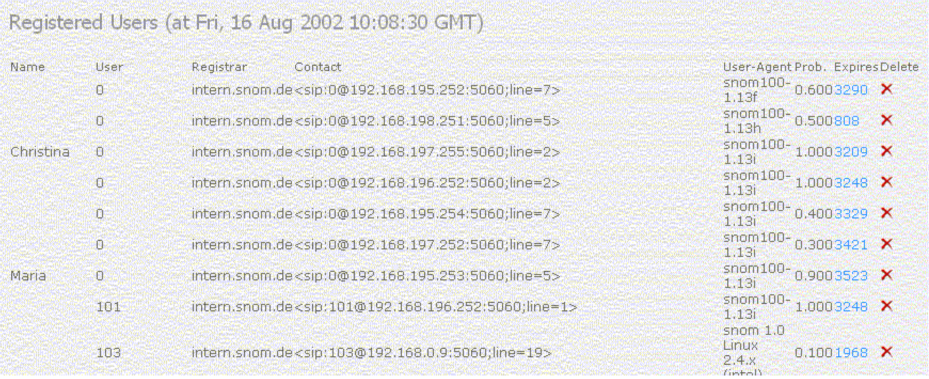
- **Name:** The name of the user as given in the registration.
- **User:** The account that is used as identification in the proxy. This corresponds to the "telephone number" of the user within the proxy realm.
- **Registrar:** The registrar the user registered on. This is one of the names listed in the hostnames.
- **Contact:** This field has two components. One is the path used to route requests to the destination, the other the contact where the user can be reached. The path is optional.
- **User-Agent:** The user agent identification tells the proxy if a license is required.
- **Probability**: The probability of the registration. Users are searched according to their probability.

- **Expires:** The expiry time in seconds. If you click on the link behind this number, you get to the SIP message trace that is associated with the registration.

- **Delete:** If you click on the symbol, the registration is removed. This is helpful if you want to manually remove a registration (otherwise you would have to wait until it expired).

FIGURE: 8-1

Registered Users



Registered Users (at Fri, 16 Aug 2002 10:08:30 GMT)

Name	User	Registrar	Contact	User-Agent	Prob.	Expires	Delete
	0	intern.snom.de	<sip:0@192.168.195.252:5060;line=7>	snom100-1.13f	0.600	3290	✕
	0	intern.snom.de	<sip:0@192.168.198.251:5060;line=5>	snom100-1.13h	0.500	808	✕
Christina	0	intern.snom.de	<sip:0@192.168.197.255:5060;line=2>	snom100-1.13i	1.000	3209	✕
	0	intern.snom.de	<sip:0@192.168.196.252:5060;line=2>	snom100-1.13i	1.000	3248	✕
	0	intern.snom.de	<sip:0@192.168.195.254:5060;line=7>	snom100-1.13i	0.400	3329	✕
	0	intern.snom.de	<sip:0@192.168.197.252:5060;line=7>	snom100-1.13i	0.300	3421	✕
Maria	0	intern.snom.de	<sip:0@192.168.195.253:5060;line=5>	snom100-1.13i	0.900	3523	✕
	101	intern.snom.de	<sip:101@192.168.196.252:5060;line=1>	snom100-1.13i	1.000	3248	✕
	103	intern.snom.de	<sip:103@192.168.0.9:5060;line=19>	snom 1.0 Linux 2.4.x (intel)	0.100	1968	✕

Call Logs

Condition for Logging a Call

A call is logged when the following conditions are met:

1. The proxy received an INVITE and forwarded the request successfully.
2. Then the proxy received a 2xx class code on this INVITE. This defines the start time of the call.
3. The proxy receives a 2xx code on a BYE for this call. This defines the end time of the call.

A call gets into the call log as soon as the start time and the end time have been determined. The number of open calls is limited to 500 calls; so if more than 500 calls have been started but not finished, the proxy cannot close a call and the call will not appear in the call log. This is to limit the amount of memory used for call logging.

Call Logs in the Web Interface

To see the calls that went through the proxy you can go to the call log page. The call log has the following fields:

- **Date/Time:**

  The date and time when the call started (in GMT).

- **Duration:**

  The duration of the call in hours, minutes and seconds.

- **From:**

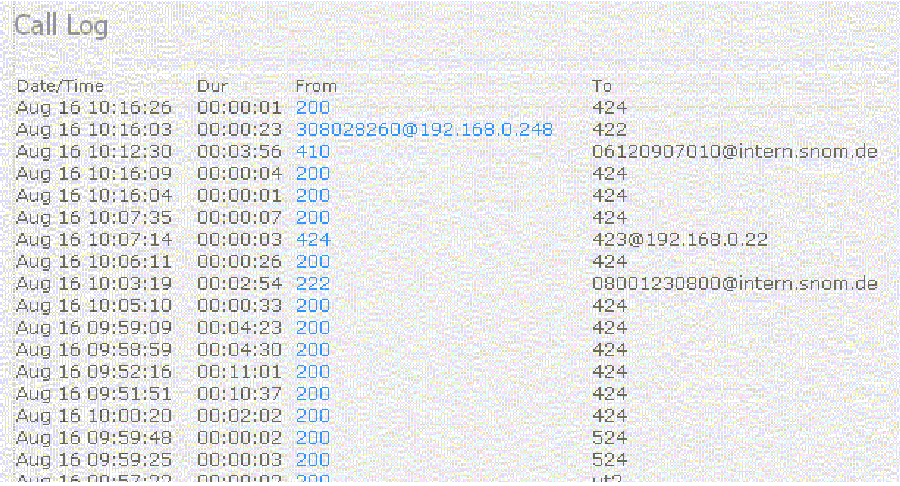
  The originator of the call. If you click on the originator, you see all SIP packets that were involved in this call.

- **To:**

  The call's destination.

FIGURE: 8-2

Call Logs



Call Log

Date/Time	Dur	From	To
Aug 16 10:16:26	00:00:01	200	424
Aug 16 10:16:03	00:00:23	308028260@192.168.0.248	422
Aug 16 10:12:30	00:03:56	410	06120907010@intern.snom.de
Aug 16 10:16:09	00:00:04	200	424
Aug 16 10:16:04	00:00:01	200	424
Aug 16 10:07:35	00:00:07	200	424
Aug 16 10:07:14	00:00:03	424	423@192.168.0.22
Aug 16 10:06:11	00:00:26	200	424
Aug 16 10:03:19	00:02:54	222	08001230800@intern.snom.de
Aug 16 10:05:10	00:00:33	200	424
Aug 16 09:59:09	00:04:23	200	424
Aug 16 09:58:59	00:04:30	200	424
Aug 16 09:52:16	00:11:01	200	424
Aug 16 09:51:51	00:10:37	200	424
Aug 16 10:00:20	00:02:02	200	424
Aug 16 09:59:48	00:00:02	200	524
Aug 16 09:59:25	00:00:03	200	524
Aug 16 09:57:22	00:00:02	200	ut2

The call log stores only the last 100 calls and discards older calls. The call log is only reliable in so far as the involved network elements follow the loose routing of the proxy. If network elements violate this rule, the packets do not flow through the proxy and the proxy is not able to determine the length of the call.

Please remember that the call log is sensitive information and should not be accessible to unauthorized persons. See the comments on security in this manual.

Pending Calls

Similar to the finished calls the proxy keeps a list about the not-finished calls. Because in SIP, a failure code like 401 does not mean the end of this call, the proxy does not differentiate between ongoing calls and failed calls. Therefore, all non-finished calls are kept in the list of „pending calls".

The web server displays the pending calls in the same fashion as the finished calls. If you want to see the packet history associated with the calls, just click on the link shown in the web interface.

Call Log File Format

A line in the call log file has the following format:

```
[Start time]: [Seconds] [Duration] [From] [To]
```

The start time is separated by a colon from the rest, so that it is easier to parse the log file automatically. The date itself has the format Weekday Month Date Time Year, with the time in the format hour:minutes:seconds. An example would be "Fri Jul 5 16:17:06 2002".

The duration of the call is given in seconds.

The from and to addresses are taken from the From: and To: URL in the headers of the INVITE packet. If the hostname in the URL match the hostname the proxy is responsible for, they are stripped from the URL. This makes the log easier to read.

SIP Message Flow

Should a problem occur, a look at the messages that went though the proxy can be very helpful. If you go to the Trace web page, a list of the last messages appears on the screen.

The list has the following elements:

- **Type:**

  The type indicates whether the packet was received (R) or transmitted (T). By clicking on the symbol you get a list of all packets that have the same call-ID as the packet.

- **Source/Destination:**

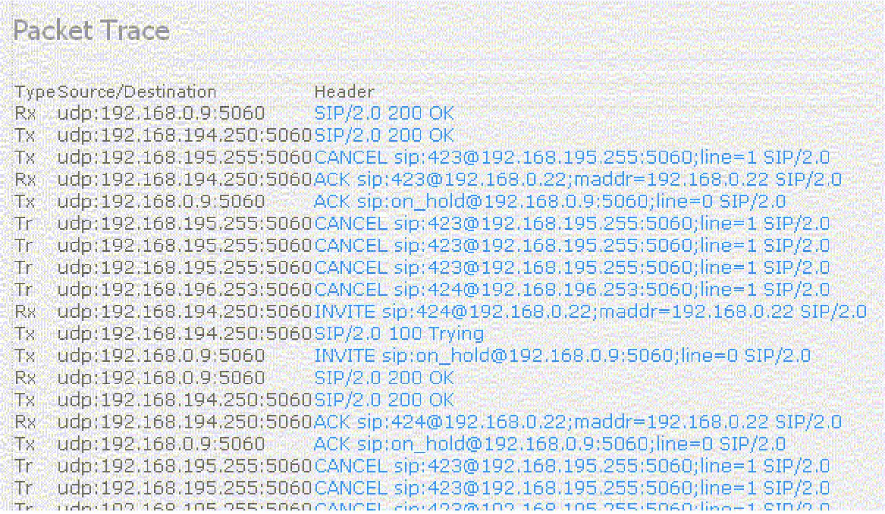
  Here you can see which transport layer (UDP or TCP) was used, the IP address of the source or destination, and the port that was involved.

- **Header:**

  Here you can see the first line of the SIP message.

FIGURE: 8-3

Trace Web Page



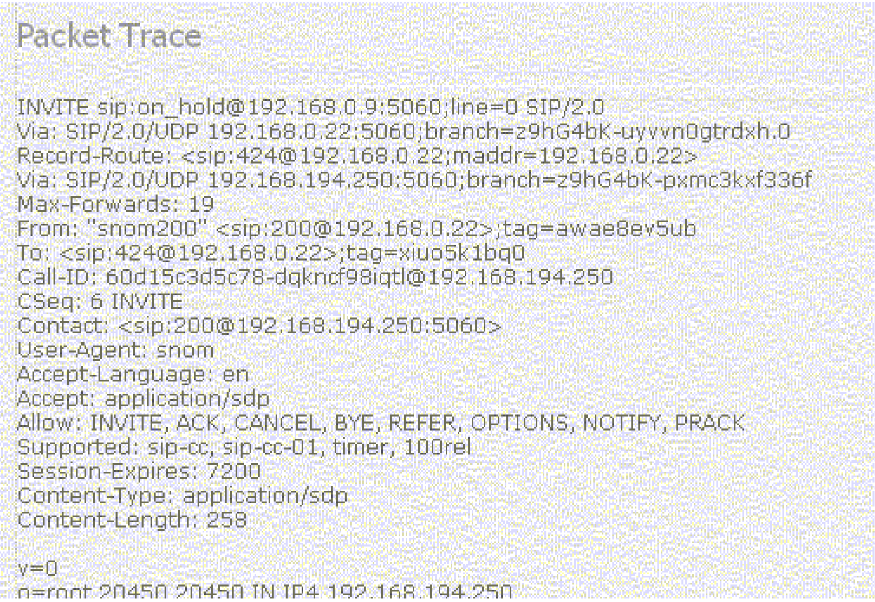
Packet Trace

```
TypeSource/Destination          Header
Rx   udp:192.168.0.9:5060       SIP/2.0 200 OK
Tx   udp:192.168.194.250:5060SIP/2.0 200 OK
Tx   udp:192.168.195.255:5060CANCEL sip:423@192.168.195.255:5060;line=1 SIP/2.0
Rx   udp:192.168.194.250:5060ACK sip:423@192.168.0.22;maddr=192.168.0.22 SIP/2.0
Tx   udp:192.168.0.9:5060       ACK sip:on_hold@192.168.0.9:5060;line=0 SIP/2.0
Tr   udp:192.168.195.255:5060CANCEL sip:423@192.168.195.255:5060;line=1 SIP/2.0
Tr   udp:192.168.195.255:5060CANCEL sip:423@192.168.195.255:5060;line=1 SIP/2.0
Tr   udp:192.168.195.255:5060CANCEL sip:423@192.168.195.255:5060;line=1 SIP/2.0
Tr   udp:192.168.196.253:5060CANCEL sip:424@192.168.196.253:5060;line=1 SIP/2.0
Rx   udp:192.168.194.250:5060INVITE sip:424@192.168.0.22;maddr=192.168.0.22 SIP/2.0
Tx   udp:192.168.194.250:5060SIP/2.0 100 Trying
Tx   udp:192.168.0.9:5060       INVITE sip:on_hold@192.168.0.9:5060;line=0 SIP/2.0
Rx   udp:192.168.0.9:5060       SIP/2.0 200 OK
Tx   udp:192.168.194.250:5060SIP/2.0 200 OK
Rx   udp:192.168.194.250:5060ACK sip:424@192.168.0.22;maddr=192.168.0.22 SIP/2.0
Tx   udp:192.168.0.9:5060       ACK sip:on_hold@192.168.0.9:5060;line=0 SIP/2.0
Tr   udp:192.168.195.255:5060CANCEL sip:423@192.168.195.255:5060;line=1 SIP/2.0
Tr   udp:192.168.195.255:5060CANCEL sip:423@192.168.195.255:5060;line=1 SIP/2.0
Tr   udp:192.168.195.255:5060CANCEL sip:423@192.168.195.255:5060;line=1 SIP/2.0
```

By clicking on the header line, you get the whole packet:

FIGURE: 8-4

Trace Whole Packet



Packet Trace

```
INVITE sip:on_hold@192.168.0.9:5060;line=0 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.22:5060;branch=z9hG4bK-uyvvn0gtrdxh.0
Record-Route: <sip:424@192.168.0.22;maddr=192.168.0.22>
Via: SIP/2.0/UDP 192.168.194.250:5060;branch=z9hG4bK-pxmc3kxf336f
Max-Forwards: 19
From: "snom200" <sip:200@192.168.0.22>;tag=awae8ev5ub
To: <sip:424@192.168.0.22>;tag=xiuo5k1bq0
Call-ID: 60d15c3d5c78-dqkncf98iqtl@192.168.194.250
CSeq: 6 INVITE
Contact: <sip:200@192.168.194.250:5060>
User-Agent: snom
Accept-Language: en
Accept: application/sdp
Allow: INVITE, ACK, CANCEL, BYE, REFER, OPTIONS, NOTIFY, PRACK
Supported: sip-cc, sip-cc-01, timer, 100rel
Session-Expires: 7200
Content-Type: application/sdp
Content-Length: 258

v=0
o=root 20450 20450 IN IP4 192.168.194.250
```

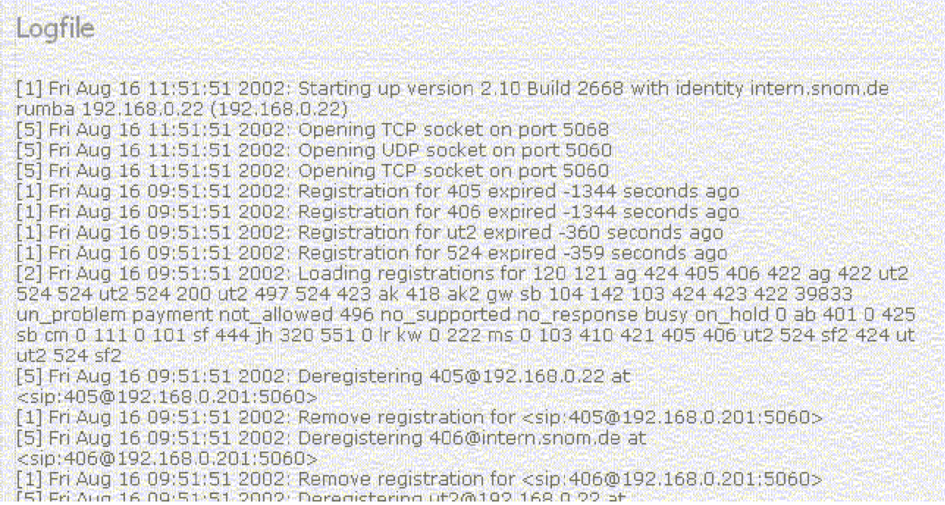
The proxy actually keeps more messages than are displayed on this list. This is necessary because it may take some time until the user clicks on a specific packet and the proxy does not know when the old packets are no longer needed. If you have a lot of packets flowing through the proxy, it might be that older packets are no longer available. However, the packets are kept in the call flow analysis log and on the registration page.

Logging

If you want to see the log file, just go to the Log file menu item. To clear the log, go to the bottom and click on “Clear”.

FIGURE: 8-5

Logging



Logfile

```
[1] Fri Aug 16 11:51:51 2002: Starting up version 2.10 Build 2668 with identity intern.snom.de
rumba 192.168.0.22 (192.168.0.22)
[5] Fri Aug 16 11:51:51 2002: Opening TCP socket on port 5068
[5] Fri Aug 16 11:51:51 2002: Opening UDP socket on port 5060
[5] Fri Aug 16 11:51:51 2002: Opening TCP socket on port 5060
[1] Fri Aug 16 09:51:51 2002: Registration for 405 expired -1344 seconds ago
[1] Fri Aug 16 09:51:51 2002: Registration for 406 expired -1344 seconds ago
[1] Fri Aug 16 09:51:51 2002: Registration for ut2 expired -360 seconds ago
[1] Fri Aug 16 09:51:51 2002: Registration for 524 expired -359 seconds ago
[2] Fri Aug 16 09:51:51 2002: Loading registrations for 120 121 ag 424 405 406 422 ag 422 ut2
524 524 ut2 524 200 ut2 497 524 423 ak 418 ak2 gw sb 104 142 103 424 423 422 39833
un_problem payment not_allowed 496 no_supported no_response busy on_hold 0 ab 401 0 425
sb cm 0 111 0 101 sf 444 jh 320 551 0 lr kw 0 222 ms 0 103 410 421 405 406 ut2 524 sf2 424 ut
ut2 524 sf2
[5] Fri Aug 16 09:51:51 2002: Deregistering 405@192.168.0.22 at
<sip:405@192.168.0.201:5060>
[1] Fri Aug 16 09:51:51 2002: Remove registration for <sip:405@192.168.0.201:5060>
[5] Fri Aug 16 09:51:51 2002: Deregistering 406@intern.snom.de at
<sip:406@192.168.0.201:5060>
[1] Fri Aug 16 09:51:51 2002: Remove registration for <sip:406@192.168.0.201:5060>
[5] Fri Aug 16 09:51:51 2002: Deregistering ut2@192.168.0.22 at
```

snom 4S • SIP

Registrar/Proxy 2.14

More Information

Release Notes

Version 2.14

- Deregistering of clients with the * symbol
- Deregistered contacts are not shown in the contact list

Version 2.13

- Introduction of pending call list

Version 2.12

- Simplified installation for Linux

Version 2.11

- Fixed problem with DNS CNAME
- Tagging on ACK for non 2xx responses was missing
- Handling of ACK for proxy generated error responses was buggy
- IP address is read out automatically, the proxy polls for IP address changes

Version 2.10

- Fixed DNS usage
- Users can now be uploaded from an asci file that contains the account, username and password as space seperated lines
- Settings have been split up into licensing, general admin, routing and registering
- Web interface had a bug that added a ‚\0‘ character after .js files (netscape browser complained about this)
- Users can now explicitly route pattern to specific destinations (see web page for dial plan), e.g. sip:{user}@192.168.0.248:5060
- User search has been made faster ans now scales well

Version 2.03

- Fixed bug where the proxy in strict router mode generated errorneous messages

Version 2.02

- License checking sometimes generated „unlicensed" in demo mode

Version 2.01

- Linux version now spawns process if in daemon mode
- Parsing of SIP URLs without angle brackets sometimes gave problems, the assignment of parameters has been clarified according to RFC.
- New feature welcome sends notifications to new registered users. This feature can be used to send text and images.

The following issues are open or pending:

- Manually stopping the proxy in Windows Service Manager works, but does not signal the service manager that it has finished. The user needs to click on cancel. Shutdown of the whole system also works.
- TLS transport layer needs to be supported.
- When the user does not have sufficient administration rights, the proxy does not register it. This can be a problem when the proxy needs to be restarted, as the registration information may not be saved; however in this case the proxy recovers after the maximum registry time.
- HTTP port setup: The http port of the proxy must be entered during setup. If the desired port 80 is not available, the proxy tries port 5068, 5069 and on. This behaviour needs to be optimized in future releases.
- Where traffic is heavy, the call log may miss a call. This happens when the number of open calls exceeds the proxy's capacity limit (200 calls) and the opened call did not receive a 200 Ok on BYE. Making the call log safe requires usage of session timer in the proxy.
- Authentication for the web server is only Basic. This limits the security of the web access.
- DNS NAPTR is not supported. Only DNS SRV and DNS A are used.
- All time statements refer to GMT. This should be changed to local time in some cases, for billing purposes for example.

Standards

The standards used for this proxy are open in the sense than not only snom is using them. Feel free to take a look at the underlying standards.

General web page for standards: http://www.ietf.org/internet-drafts
SIP working group drafts: http://www.softarmor.com/sipwg/drafts and www.softarmor.com/sipping/drafts
SIP standard used for this manual: http://www.ietf.org (RFC 3261)
Path extension for registering clients: www.softarmor.com/sipwg/drafts/draft-

willis-sip-path-08.txt

Other useful information

General Information: http://iptel.org
Windows Messenger: http://www.microsoft.com/WindowsXP/pro/techinfo/planning/networking/windowsmessenger.asp
snom home page: http://www.snom.de

Footnotes

[1] This standard is now obsolete. Many products currently on the market are compatible with this obsolete RFC. You should be aware of this when buying SIP technology.

[2] Also known as “user agents” or terminals

[3] TLS is not supported in the current version

[4] According to the draft RFC3261

Index

snom
VoIP-phones

http://www.snom.de

snom technology AG
Pascalstr. 10e
D-10587 Berlin
Germany

Tel: +49-(0)30-39833-0
sip: info@snomag.de
mailto: info@snom.de

snom technology USA
Crestside Dr.
Coppell, Texas 75019
USA

Tel: +1-972-740-5078
sip: usa@snomag.de
mailto: usa@snom.de