

snom
VoIP-phones

snom 4S

STUN Server
Version 2.0

User Manual



snom 4S

STUN Server 2.0

snom 4S STUN Server Version 2.0 User Manual

1. Edition 2002

© 2002 snom technology Aktiengesellschaft. All Rights Reserved.

This document is supplied by snom technology AG for information purposes only to licensed users of the snom 4S STUN server 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.



SIP in the Home Network

With the increasing importance of SIP, customers are asking for working solutions that can be used in home networks. Home users carrying their VoIP phone home get frustrated if they can't make phone calls like they can surf the Internet. This endangers the success of VoIP in the mass market.

Because of the limited range of Internet Version 4 addresses, users need to use private addresses in their installations. Unfortunately, SIP and the media transport protocol RTP assumes that addresses are visible in the public Internet but network address translations (NAT) violates these rules.

The next generation Internet protocol version 6 solves these problems. Also, UPnP is a good way to control the behaviour of NAT gateways. However in today's networks, these protocols are most of the time not available. Going to the superstore shows that today's phones have to deal with NAT.

STUN (which stands for simple traversal of UDP through NAT) is a pragmatic approach to solving this problem. It is not limited to SIP, it could also be used for other UDP based protocols. STUN can deal with existing equipment the best way in a sense that nothing has to be changed on the user network side.

The price for STUN is an increased network traffic. If a phone keeps a port open every 60 seconds, it generates a keep-alive traffic of roughly 50,000 packets per month with a total of circa 3 MB network traffic.

In some cases, STUN cannot establish connections. In these cases, TURN could solve this problem. However, TURN needs to "mirror" all traffic including the media streams, which increases the delay and makes VoIP a hard-to-enjoy experience. However, for applications that focus on instant messaging, TURN could be a good solution.

We hope that you can leverage your network with our STUN server!

Christian Stredicke, snom technology AG

Table of Contents

SIP in the Home Network	5
1 How It Works	8
1.1 The NAT Algorithm.....	8
1.2 Failure Example without STUN.....	9
1.3 How STUN Addresses the Problem	9
1.4 Filling the Gaps with TURN.....	10
1.5 Reliability and Scalability	11
2 Windows Installation.....	12
2.1 Installing.....	12
2.2. Deinstalling	13
3 Linux Installation	14
3.1 Automatic starting under SuSe Linux.....	14
3.2 RedHat.....	15
4 Setup.....	16
4.1 Command Line Arguments.....	16
4.2 Using the Web Server	16
4.4 Web Browser	18
4.5 Version	20
5 Maintenance	21
5.1 Log File.....	21
5.2 Statistics.....	22
A References	24
B Log Messages	25



1 How It Works

1.1 The NAT Algorithm

There are many description of NAT [1, 2]. Although it causes a lot of trouble, it is widely used outside of North America and in home installations where only one IP address is available.

In short words, NAT is a table indicating which port of an IP address goes to which private IP address. Symmetrical NAT also remembers for which destination the port has been opened. The internal table of a NAT gateway could look like this:

Port	Private Address	Timeout	Remote Address
1965	192.168.0.4:53	34 s	62.155.70.43:53
43245	192.168.1.54:1324	112 s	130.149.5.2:654
...			

The NAT gateway will execute the following algorithm (full cone algorithm):

- If it receives a packet from the private network, it will search the source address in the table and re-send the packet using the local port and reset the timeout to a default value (e.g. 120 s). For example, if it receives a packet from 192.168.0.4:53, it will use port 1965.
- If the source address cannot be found, it will allocate a new entry.
- If it received a packet from the public network, it will search the destination port in the table and forward it to its destination. For example, if it receives a packet on port 43245, it will forward it to 192.168.1.54:1324.
- If the port cannot be found, the packet is discarded.

The default timeout is typically in the minute region. When there is no traffic on a port, the port is closed automatically. This keeps the list clean.

If the NAT is symmetrical, it will take the Remote Address into account during comparisons. This makes the NAT gateway more reliable for security, however causes problems with VoIP traffic. See the discussion below.



1.2 Failure Example without STUN

When a VoIP phone is behind NAT, it typically tries to send a REGISTER request to the SIP proxy, which is located in the public network. The REGISTER request could look like this:

```
REGISTER sip:sip-operator.com SIP/2.0
Via: SIP/2.0/UDP 192.168.198.243:5060
From: <sip:120@sip-operator.com;user=phone>
To: <sip:120@sip-operator.com;user=phone>
Call-ID: 1322580783@192.168.198.243
CSeq: 25 REGISTER
Contact: <sip:120@192.168.198.243:5060;user=phone
;transport=udp>;expires=3600
Content-Length: 0
```

According to the NAT algorithm, the NAT gateway allocates a new UDP port table entry and forwards the packet. The proxy will receive the packet and try to send it back to address 192.168.198.243 port 5060. However, because this is a private address, this will fail and the reply never reaches the user agent.

Moreover, even if the proxy would be “clever” enough to send it back to the address where it received the packet from, the NAT gateway would close the port after a few minutes and when somebody calls, there will be no way of alerting the user agent. So the problem needs to be addressed in a different way.

1.3 How STUN Addresses the Problem

The core idea behind STUN is putting a “mirror” into the public network. This mirror can be used to see how a device looks like from the public Internet point of view.

There are different kinds of reflection:

- Send the packet back using the same port and IP address where it has been received on the STUN server;
- Send the packet back from a different address.

Initially, the user agent needs to know what kind of NAT it is behind. Therefore, it tries to receive a packet directly from the STUN server. If this fails, there is obviously no way to establish communication to the public Internet and the user agent must give up. If it receives a packet, it can take a look at the identity it

has on the outside world. If it is exactly the same identity is has already stored a local address, it is in the public Internet already and there is no need to use STUN any more. If it has changed, the phone now knows that it is behind NAT and which IP address and port it can use for the outside communication.

If it is behind NAT, it needs to know if the NAT gateway is restrictive and performs the symmetrical NAT algorithm. Therefore, it sends another packet to the STUN server asking to return it from a different address. If this packet finds its way back to the user agent, NAT is not restrictive and the user agent can not start operating. If the packet does not find its way back, the NAT cannot be used directly for VoIP communication. In this case, TURN might help (see below).

Now that the phone knows its identity, it may send the REGISTER packet to the registrar:

```
REGISTER sip:sip-operator.com SIP/2.0
Via: SIP/2.0/UDP 213.43.24.64:23656
From: <sip:120@sip-operator.com;user=phone>
To: <sip:120@sip-operator.com;user=phone>
Call-ID: 1322580783@192.168.198.243
CSeq: 26 REGISTER
Contact: <sip:120@213.43.24.64:23656;user=phone;
        transport=udp>;expires=3600
Content-Length: 0
```

The proxy can then register the contact and send the message back to the indicated destination, so that the NAT gateway forwards the packet to the user agent client.

1.4 Filling the Gaps with TURN

In case of symmetric NAT the situation is not completely hopeless. Setting up a mirror for the required channels on the STUN server can solve the problem.

When a client has determined a symmetrical NAT, it can set up a mirror with the following steps:

- First it allocates a mirror port on the STUN server. This is done by sending a TURN request to the STUN port. The response contains the port number.
- It then sends a packet to the allocated port on the STUN server. This sets up a new port on the NAT gateway. The response to the request contains the port number on the NAT gateway as well as the binding duration of that



port on the STUN server.

It must be said here that the TURN approach has several drawbacks. First, it adds an additional route element into the network path. This can double the network delay and increases the overall network traffic. Additionally, it makes the STUN server stateful which makes scalability and redundancy much more difficult. This is especially a problem for media, where network delay is very important and the network traffic can be significant.

1.5 Reliability and Scalability

Network elements can fail. In such an event, it should be possible to continue services with different servers. STUN and the snom STUN server provides the following mechanisms for this:

- Finding the first STUN server. This is the job of the STUN client which is responsible to switch to a different server if the current server is not responding.
- Dispatching STUN requests to different IP address servers. The snom STUN server allows using several secondary STUN servers (for the change IP address request) in a round robin fashion. If one of these servers fail, the according packet will get lost; however because STUN requires message repetition, other messages will be routed to servers that are available and one of them will respond.

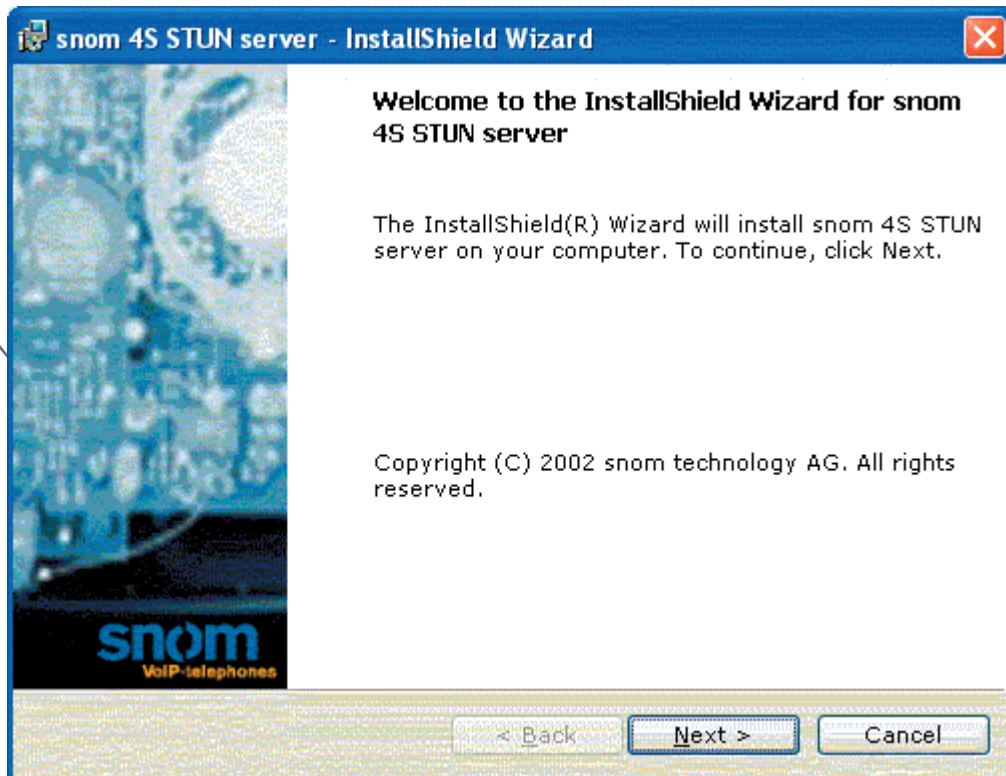
These mechanisms can also be used for scaling the network. Simply take several STUN servers and advertise them via DNS SRV. This will balance the load over the network.

2 Windows Installation

Before you reinstall the software on Windows, you need to uninstall the last version before. See paragraph 2.2 for uninstalling the software on Windows.

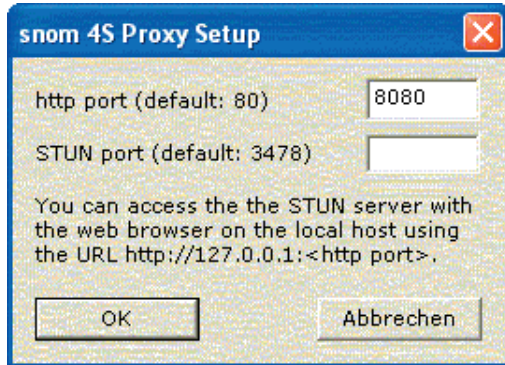
2.1 Installing

Start installing the snom 4S STUN server by double clicking on the image that you have received with the software. After the welcome screen (see below) you need to accept the license agreement and enter your personal information. Select the installation directory and the installation type.





We recommend installing all available files including the documentation so that you have easy access to all necessary information. At the end of the installation, you need to specify the HTTP and STUN port. This is important information as this is required for the further setup and maintenance.



If your computer already runs another web server, you must specify another port than 80 (the default HTTP port). Remember the port number, as you need to use it for accessing the STUN server later.

After the installation finishes, you are asked to reboot the system. After a reboot you should be able to access the STUN server as described in chapter 4.

If you want to avoid restarting, you can access the services manager of the Windows operating system and manually start the snom STUN server.

2.2. Deinstalling

Deinstalling the software requires two steps. First, stop the STUN service in the services section of your computer. Then go to the software page of your computer. Select the snom 4S STUN server and click on the deinstall button.

3 Linux Installation

If you just want to try the STUN server, manual starting should be sufficient. Load the tarball to a directory of your choice and start the server with the command "stund". You may use the command line arguments shown in the next chapter.

3.1 Automatic starting under SuSe Linux

If you want the STUN server to be started automatically after a reboot, you need to set up some files as root.

```
$ su -
```

Uncompress the tarball into the location where you want to keep the STUN server. We recommend linking that directory to a name which does not contain a version number for later updates.

```
# export STUN_DIR=/root/stund
# export STUN_VERSION=snom_stund-i386-linux-2.0
# cd /root
# tar xvfz $STUN_VERSION.tgz
# ln -s $STUN_VERSION stund
```

Copy or link the proxy executable to /usr/sbin/stund.

```
# cd /usr/sbin
# ln -s $STUN_DIR/stund stund
```

Copy or link the startup script stund-suse.sh to /etc/init.d/stund

```
# cd /etc/init.d
# ln -s $STUN_DIR/stund-suse.sh sip-proxy
```

Link the startup script to /etc/init.d/rc[23].d/[SK]20stund (in total 4 links).

```
# ln -s stund rc2.d/S20stund
# ln -s stund rc3.d/S20stund
# ln -s stund rc2.d/K20stund
# ln -s stund rc3.d/K20stund
```

Link /usr/sbin/rcstund to /etc/init.d/stund

```
# ln -s stund /usr/sbin/rcstund
```

Set up the variable START_STUND to "yes" in the /etc/rc.config

Set the necessary options in the STUND_OPTS variable. You should assign the desired html port for the STUN server with the --html_port option and the location where the



configuration will be saved with the `-config` option.

```
#  
# Start the snom 4S SIP proxy (part of the rc.config file)  
#  
START_STUND="yes"  
STUND_OPTS="--html-port 5070 -config /root/stund.txt"
```

You can then try to start the server with the command `rcstund start`. Check with the `ps` command if you can see the process and open a web browser to see if the STUN server is up and running. Reboot the system and check if after the reboot the STUN server was started automatically. You can then continue with the installation using the web browser. Reboot again to check if the configuration has been saved.

```
# rcstund start  
# ps auxww | grep stund  
# sync; reboot; exit
```

3.2 RedHat

The rc script suitable for use on RedHat systems can be found in the installation as `stund-redhat.sh`. It will work correctly with the `chkconfig` cmd with the `--add` option for the RedHat init process to man the daemon.

4 Setup

4.1 Command Line Arguments

The Linux version can be started from the command line. The following options are available:

- `--log <n>`: Set the log level to *n*, which must be an integer number between 0 and 9. 0 means that only the most urgent messages are put into the log, 9 means that even just informative messages find their way into the log.
- `--html-port <n>`: Set the html-port. You can then access the embedded web server of the STUN server on this port. The default value is 80 (the default http port).
- `--no-daemon`: Don't fork a background process. If this option is not present, the STUN server forks a background process that disconnects from the console and works in the background. If the option is present, the program runs as normal user application and you can see the log messages on the terminal.
- `--config <file>`: Tell the server which configuration file to use to store the configuration information. Normally, this is "stund.txt". However, if you are starting several STUN server in the same network, it makes sense to store their configuration information in different configuration files. This is the option that allows this.
- `--version`: Print the version of the STUN server. This is helpful for diagnosis.

4.2 Using the Web Server

The STUN server is controlled via an embedded web server. During setup and/or start you had to specify a html port. Please start a web browser and enter the address of the machine where the STUN server is running. Unless you use the default port 80, you need to specify the http port with a colon after the address. Some browsers require the full URI including the "http", so a sample address could look like "http://stun.mycompany.com:5062" if you specified port 5062.

You should see a window like this:



You can access the different web pages with pull down menus which should appear at the top line of the browser. If your browser does not support JavaScript, you can use the links shown in the tree in the middle of the screen or you can also enter the web page name directly.

4.3 Licensing

The snom STUN server needs to be unlocked before it can be used. To do this, please go to the "Licensing" menu (license_en.htm). You should have received a license key with this product, if not you can request a license key from <mailto:support@snom.de>. Please make sure that the proposed IP address is correct and copy the license code into the License key-field. When requesting a full license please provide the IP address you want the STUN server on.

snom 4S STUN server

Current license type: Demonstration

License Setup

Please enter the IP address of the STUN server, if this is not already filled out correctly.
If you don't have a license key, please contact support@snom.de.

IP address:	<input type="text" value="217.115.141.99"/>
License key:	<input type="text" value="snom-stund-dem-12-sep-2002-"/>

After entering the required information and pressing “Save”, you can see the current license type. It can be “Demonstration” or “Licensed”. The demonstration key expires after 30 days (indicated in the key), so please make sure that you get a full license before this demo key expires.

4.4 Web Browser

After starting the STUN server, you need to set up a few things. Go to “General Setup” in the administration menu (admin_en.htm). You see a dialog like this:



Server Settings

Other STUN server:	<input type="text" value="stun2.abc.org:5062 stun3.abc.org"/>
STUN port 1:	<input type="text" value="5062"/>
STUN port 2:	<input type="text" value="5063"/>
Default binding duration (TURN):	<input type="text" value="600"/>
Log Level (0-9):	<input type="text" value="5"/>
Web interface:	
HTTP port:	<input type="text" value="5070"/>
HTTP user:	<input type="text" value="admin"/>
HTTP password:	<input type="password" value="••••••"/>
HTTP password (confirm):	<input type="password" value="••••••"/>

The fields have the following meaning:

Other STUN server: This is a space separated list of the STUN servers that should be used for answering the “changed IP address” request. You may use DNS names here; however for the sake of efficiency you might want to use IP addresses directly. The servers are used in a round robin fashion, which means after sending one request to the first server, the next request will go to the second server and so on. Message repetitions don’t change this algorithm, so that message repetitions of one change IP requests go to different hosts. This is necessary because one of these hosts could be down and in that case the other hosts can answer the request.

STUN port 1: This is the primary STUN port where messages are received on. This is the port you need to tell your STUN clients.

STUN port 2: This port is used for answering the “change port” requests. The STUN server does not read requests from this port, so you should not use this port for your STUN clients.

Default binding duration: When allocating a TURN port, the server needs a timeout value after this binding is removed. A value of 600 s is reasonable as most of the NAT gateways remove their bindings before 10 minutes. Making

this value bigger increases the number of bound port on the STUN server when many TURN allocation requests have to handled.

Log Level: The log level must be an integer number between 0 and 9. 0 means that only the most urgent messages are put into the log, 9 means that even just informative messages find their way into the log.

HTTP port: The port where the web server expects requests. If you can access the web server, there is usually no need to change this value. If you change this value, you should remember this value as it is hard to find out on which port the web traffic is expected. If you change and forget this value you might have to reinstall the STUN server.

HTTP user and password: To protect the access to the STUN server, you may specify a username and a password (which has to be entered twice for safety). Subsequent requests will only be allowed if you enter this username/password pair.

4.5 Version

You can check which exact version you are using by going to the “Version” menu of the web server ([info_en.htm](#)). This web page also includes information about the license.

5 Maintenance

5.1 Log File

All log messages that are lower or equal to the current log level are written to the internal log. You can see this log in the "Status/Logfile" menu (log_en.htm).

snom 4S STUN server

Logfile

```
[8] Tue Aug 13 15:30:48 2002: Received pdu from 217.230.186.106:29508
00 01 00 08 2b 8c 53 0c 00 03 00 04 00 00 00 00
[8] Tue Aug 13 15:30:48 2002: Send response to 217.230.186.106:29508
[8] Tue Aug 13 15:31:22 2002: Received pdu from 217.230.186.106:29265
00 01 00 08 37 a3 de b1 00 03 00 04 00 00 00 00
[8] Tue Aug 13 15:31:22 2002: Send response to 217.230.186.106:29265
[8] Tue Aug 13 15:31:38 2002: Received pdu from 217.230.186.106:29508
00 01 00 08 25 66 1d f1 00 03 00 04 00 00 00 00
[8] Tue Aug 13 15:31:38 2002: Send response to 217.230.186.106:29508
[8] Tue Aug 13 15:32:12 2002: Received pdu from 217.230.186.106:29265
00 01 00 08 06 8c b4 e0 00 03 00 04 00 00 00 00
[8] Tue Aug 13 15:32:12 2002: Send response to 217.230.186.106:29265
[8] Tue Aug 13 15:32:28 2002: Received pdu from 217.230.186.106:29508
00 01 00 08 7b 7c 97 c0 00 03 00 04 00 00 00 00
[8] Tue Aug 13 15:32:28 2002: Send response to 217.230.186.106:29508
[8] Tue Aug 13 15:33:03 2002: Received pdu from 217.230.186.106:29265
00 01 00 08 28 37 8a 2d 00 03 00 04 00 00 00 00
[8] Tue Aug 13 15:33:03 2002: Send response to 217.230.186.106:29265
[8] Tue Aug 13 15:33:19 2002: Received pdu from 217.230.186.106:29508
00 01 00 08 46 7c 32 bb 00 03 00 04 00 00 00 00
```

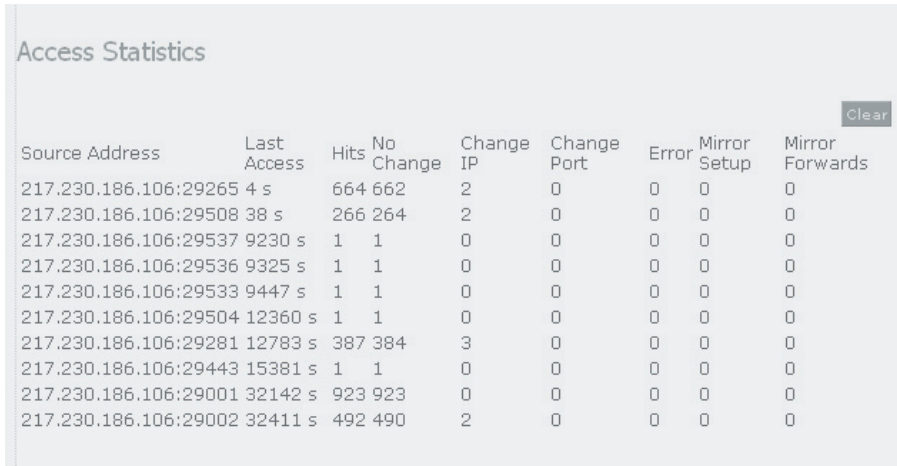
All log messages start with the log level in brackets. The date after the log level is given in GMT. The log messages are explained in the appendix.

Log messages are kept in a first in/first out fashion. At most 200 messages are kept in that buffer. This avoids an overflow of messages and makes sure that you can keep the STUN server running without running out of memory or disk space.

You can clear the log by pushing the “Clear” button.

5.2 Statistics

To see what is going on you can go to the “Status/Statistics” page of the server ([stat_en.htm](#)). You find a table sorted after the time of the last access.



Access Statistics

Source Address	Last Access	Hits	No Change	Change IP	Change Port	Error	Mirror Setup	Mirror Forwards
217.230.186.106:29265	4 s	664	662	2	0	0	0	0
217.230.186.106:29508	38 s	266	264	2	0	0	0	0
217.230.186.106:29537	9230 s	1	1	0	0	0	0	0
217.230.186.106:29536	9325 s	1	1	0	0	0	0	0
217.230.186.106:29533	9447 s	1	1	0	0	0	0	0
217.230.186.106:29504	12360 s	1	1	0	0	0	0	0
217.230.186.106:29281	12783 s	387	384	3	0	0	0	0
217.230.186.106:29443	15381 s	1	1	0	0	0	0	0
217.230.186.106:29001	32142 s	923	923	0	0	0	0	0
217.230.186.106:29002	32411 s	492	490	2	0	0	0	0

The first column (*Source Address*) shows you where the requests of this row came from. You can see the IP address and the port after the colon.

The *Last Access* tells you, when the last packet from that source arrived at the server. The unit for this column is seconds. This important information can be used to see the active hosts. Hosts that did not send packets for more than approximately two minutes are probably not available through their NAT gateway, because the NAT gateway timeout has closed the shown ports.

The total number of *Hits* from that address is shown in the next column. This is simply the sum of all detail information shown in that row.

The *No Change* row shows how many requests did not request an IP address change. Typically, keep-alive messages are of that kind. High numbers in this field indicate that a host is active and tries to keep its address reserved.

The *Change IP* field shows the number of requests for response with a changed IP address. A value greater than zero indicates that the host behind this address tried to find out what kind of NAT it is behind.



The *Change Port* field shows the number of requests for a response from a different port. This type of message is requested only in cases when the STUN clients needs to find out what kind of restrictions it has.

The number of *Error* messages show how many messages could not be processed by the server. To see what the reason for the failure is, you should see the Log.

Whenever a TURN mirror is allocated, the *Mirror Setup* number is incremented. For plain STUN, this field is always zero.

The number of forwarded packets on a mirror is shown in the *Mirror Forwards* field. The number in this field can be significant for mirrors that forward media. Forwarding a voice conversation adds 50 packets per seconds to this field.

The demonstration license limits the number of entries to 10. The full license keeps the last 100 least recently used entries.

To reset the statistics, push the "Clear" button.

A References

- [1] M. Hasenstein, "IP network address translation", 1997, <http://www.sude.se/~mha/linux-ip-nat/diplom/nat.html>
- [2] K. Egevang, P. Francis, „The IP Network Address Translator (NAT)“, IETF 1994, RFC1631
- [3] J. Rosenberg, J. Weinberger, C. Huitema, R. Mahy: „STUN - Simple Traversal of UDP Through Network Address Translators“, Internet Draft, Internet Engineering Task Force. Work in progress.
- [4] J. Rosenberg, J. Weinberger, C. Huitema, R. Mahy: „ Traversal Using Relay NAT (TURN)“, Internet Draft, Internet Engineering Task Force. Work in progress.

B Log Messages

The following log messages are defined:

- 1001: The internal web server could not evaluate a server side include.
- 1002: A port binding has been removed. This happens when the binding is not refreshed by the client.
- 1003: A port binding could not be found. This is an internal error and should not happen.
- 1004: The STUN server received a response. Normally, the server receives only requests. Responses are ignored.
- 1005: The STUN server received a unknown message type. The message is ignored.
- 1006: The STUN server received a message. This log message is informational.
- 1007: The destination of a mirror has been set. This is an informational message.
- 1008: A request with a wrong length count has been received. The processing of the message will continue.
- 1009: A message for a unknown Internet protocol family has been received. This will be typically IPv6, which is not supported in this version.
- 1010: A unknown type has been received that cannot be ignored. The message is discarded.
- 1011: A message repetition for a port allocation has been received. This message is just informational.
- 1012: Allocating new port for TURN mirror. This is informational.
- 1013: No more port could be allocated on the STUN server (out of resources).
- 1014: A change IP request cannot be answered because no other STUN server has been specified.
- 1015: Informational information about the sending of request to a different STUN server.
- 1016: The server specified in the alternative STUN server list can not be resolved. The current version of the STUN server only supports DNS A, other DNS types cannot be resolved.
- 1017: Send a response to the host shown in the log entry. This log message is purely informational.
- 1018: The response address could not be set. This should not happen, as all addresses which have been received should be reachable. If this log message occurs, there is probably a misconfiguration of the routing in the host.
- 1019: A response is being sent from a different port. This message is informational.
- 1020: Same as 1018, but for the secondary STUN port.
- 1021: A TURN mirror has been removed. This is informational.
- 1022: The license check failed. The entered license code is not correct.
- 1023: The operating system gave a fundamental error with the sockets. This should not happen.

- 1024: Information about the reading of the configuration file.
- 1025: The hostname cannot be resolved. Resolving the hostname is necessary to determine the IP address.
- 1026: Initial start up message.
- 1027: The HTTP port could not be opened. Neither the specified port nor one of the port 5068 and on could be opened.
- 1028: The primary STUN port could not be opened.
- 1029: The secondary STUN port could not be opened.
- 1030: A web file could not be found. This should not happen.
- 1031: The Windows WINSOCK interface could not be opened.
- 1032: A Windows registry element could not be read. This could indicate that the user does not have enough permissions to run a service.
- 1033: A Windows registry element could not be written. This could indicate that the user does not have enough permissions to run a service.
- 1034: A Windows registry element could not be deleted. This could indicate that the user does not have enough permissions to run a service.





<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