

# SIPp

## SIPp reference documentation

by Richard GAYRAUD [initial code], Olivier JACQUES [code/documentation], Charles P. Wright [code], Many contributors [code]

### Table of contents

1 Foreword.....	5
2 Installation.....	7
2.1 Getting SIPp.....	7
2.2 Stable release.....	7
2.3 Unstable release.....	7
2.4 Available platforms.....	7
2.5 Installing SIPp.....	8
2.6 Increasing File Descriptors Limit.....	9
3 Using SIPp.....	10
3.1 Main features.....	10
3.2 Integrated scenarios.....	10
3.2.1 UAC.....	10
3.2.2 UAC with media.....	11
3.2.3 UAS.....	12
3.2.4 regexp.....	12
3.2.5 branch.....	13

3.2.6 UAC Out-of-call Messages.....	13
3.2.7 3PCC.....	13
3.3 3PCC Extended.....	16
3.4 Controlling SIPp.....	17
3.4.1 Traffic control.....	19
3.4.2 Remote control.....	20
3.5 Running SIPp in background.....	21
3.6 Create your own XML scenarios.....	21
3.6.1 Structure of client (UAC like) XML scenarios.....	30
3.6.2 Structure of server (UAS like) XML scenarios.....	35
3.6.3 Actions.....	36
3.6.4 Variables.....	45
3.6.5 Injecting values from an external CSV during calls.....	46
3.6.6 Conditional branching.....	49
3.6.7 SIP authentication.....	53
3.6.8 Initialization Stanza.....	55
3.7 Screens.....	55
3.8 Transport modes.....	59
3.8.1 UDP mono socket.....	59
3.8.2 UDP multi socket.....	60
3.8.3 UDP with one socket per IP address.....	60
3.8.4 TCP mono socket.....	61
3.8.5 TCP multi socket.....	61
3.8.6 TCP reconnections.....	62
3.8.7 TLS mono socket.....	62

3.8.8 TLS multi socket.....	62
3.8.9 IPv6 support.....	62
3.8.10 Multi-socket limit.....	63
3.9 Handling media with SIPp.....	63
3.9.1 RTP echo.....	63
3.9.2 PCAP Play.....	63
3.10 Exit codes.....	64
3.11 Statistics.....	64
3.11.1 Response times.....	64
3.11.2 Available counters.....	65
3.11.3 Detailed Message Counts.....	66
3.11.4 Importing statistics in spreadsheet applications.....	66
3.12 Error handling.....	66
3.12.1 Unexpected messages.....	66
3.12.2 Retransmissions (UDP only).....	67
3.12.3 Log files .....	67
3.13 Online help (-h).....	68
4 Performance testing with SIPp.....	77
4.1 Advices to run performance tests with SIPp.....	77
4.2 SIPp's internal scheduling.....	77
5 Useful tools aside SIPp.....	78
5.1 JEdit.....	78
5.2 Wireshark/tshark.....	78
5.3 SIP callflow.....	78
6 Getting support.....	79

7 Contributing to SIPp.....79

## 1 Foreword

**Warning:**

This version of the documentation is for SIPp 3.2 branch. To access the latest version of the documentation, go to [this page](#) ( ../doc/reference.html ) .

SIPp is a performance testing tool for the SIP protocol. It includes a few basic SipStone user agent scenarios (UAC and UAS) and establishes and releases multiple calls with the INVITE and BYE methods. It can also reads XML scenario files describing any performance testing configuration. It features the dynamic display of statistics about running tests (call rate, round trip delay, and message statistics), periodic CSV statistics dumps, TCP and UDP over multiple sockets or multiplexed with retransmission management, regular expressions and variables in scenario files, and dynamically adjustable call rates.

SIPp can be used to test many real SIP equipments like SIP proxies, B2BUAs, SIP media servers, SIP/x gateways, SIP PBX, ... It is also very useful to emulate thousands of user agents calling your SIP system.

**Want to see it?**

Here is a screenshot

```

ocadmin@vista:~/sipp
----- Scenario Screen ----- [1-4]: Change Screen --
Call-rate(length)  Port  Total-time  Total-calls  Remote-host
    10 cps(0 ms)   5061      4.01 s      40  127.0.0.1:5060(UDP)


10 new calls during 1.000 s period      16 ms scheduler resolution
0 concurrent calls (limit 30)           Peak was 1 calls, after 0 s
0 out-of-call msg (discarded)
1 open sockets

          Messages  Retrans  Timeout  Unexpected-Msg
INVITE  ----->      40       0        0
    100 <-----      0       0         0
    180 <-----      40       0         0
    200 <----- E-RTD  40       0         0
    ACK  ----->      40       0
          [    0 ms]
    BYE  ----->      40       0        0
    200 <-----      40       0         0

----- [+|-|*|/]: Adjust rate ---- [q]: Soft exit ---- [p]: Pause traffic -----

```

And here is a video (Windows Media Player 9 codec or above required) of SIPp in action:

 [sipp-01.wmv](#) ( images/sipp-01.wmv)

## 2 Installation

### 2.1 Getting SIPp

SIPp is released under the [GNU GPL license](http://www.gnu.org/copyleft/gpl.html) ( <http://www.gnu.org/copyleft/gpl.html> ) . All the terms of the license apply. It is provided to the SIP community by [Hewlett-Packard](http://www.hp.com) ( <http://www.hp.com>) engineers in hope it can be useful.

We receive some support from our company to work on this tool freely, but **HP does not provide any support nor warranty concerning SIPp.**

### 2.2 Stable release

Like many other "open source" projects, there are two versions of SIPp: a stable and unstable release. Stable release: before being labelled as "stable", a SIPp release is thoroughly tested. So you can be confident that all mentioned features will work :)

Note:

Use the stable release for your everyday use and if you are not blocked by a specific feature present in the "unstable release" (see below).

[SIPp stable download page](http://sourceforge.net/project/showfiles.php?group_id=104305) ( [http://sourceforge.net/project/showfiles.php?group\\_id=104305](http://sourceforge.net/project/showfiles.php?group_id=104305))

### 2.3 Unstable release

Unstable release: all new features and bug fixes are checked in [SIPp's SVN](http://sipp.svn.sourceforge.net/viewvc/sipp/sipp/trunk/) ( <http://sipp.svn.sourceforge.net/viewvc/sipp/sipp/trunk/>) repository as soon as they are available. Every night, an automatic extraction is done and the source code of this release is made available.

Note:

Use the unstable release if you absolutely need a bug fix or a feature that is not in the stable release.

[SIPp "unstable" download page](http://sipp.sourceforge.net/snapshots/) ( <http://sipp.sourceforge.net/snapshots/>)

### 2.4 Available platforms

SIPp is available on almost all UNIX platforms: HPUX, Tru64, Linux (RedHat, Debian, FreeBSD), Solaris/SunOS.

A Windows port has been contributed. You can now compile SIPp under Cygwin. A binary package with a Windows installer is also available. Check [the download page](http://sourceforge.net/project/showfiles.php?group_id=104305) ( [http://sourceforge.net/project/showfiles.php?group\\_id=104305](http://sourceforge.net/project/showfiles.php?group_id=104305)) to download it and run SIPp under Windows.

Note:

SIPp works only over Windows XP and will not work on Win2000. This is because of IPv6 support. The Windows installer should prevent someone to install SIPp on Win2000.

## 2.5 Installing SIPp

- On Linux, SIPp is provided in the form of source code. You will need to compile SIPp to actually use it.
- Pre-requisites to compile SIPp are (see [Compilation tips](http://sipp.sourceforge.net/wiki/index.php/Compilation) ( <http://sipp.sourceforge.net/wiki/index.php/Compilation>) ):
  - C++ Compiler
  - curses or ncurses library
  - For authentication and TLS support: OpenSSL >= 0.9.8
  - For pcap play support: libpcap and libnet
  - For distributed pauses: [Gnu Scientific Libraries](http://www.gnu.org/software/gsl/) ( <http://www.gnu.org/software/gsl/>)
- You have four options to compile SIPp:
  - **Without TLS (Transport Layer Security) and authentication support:** This is the recommended setup if you don't need to handle SIP authentication and/or TLS. In this case, there are **no dependencies to install** before building SIPp. It is straight forward:

```
# gunzip sipp-xxx.tar.gz
# tar -xvf sipp-xxx.tar
# cd sipp
# make
```

- **With TLS and [authentication](#) support,** you must have installed [OpenSSL library](http://www.openssl.org/) ( <http://www.openssl.org/>) (>=0.9.8) (which may come with your system). Building SIPp consist only in adding the "ossl" option to the make command:

```
# gunzip sipp-xxx.tar.gz
# tar -xvf sipp-xxx.tar
# cd sipp
# make ossl
```

- **With [PCAP play](#) and without [authentication](#) support:**

```
# gunzip sipp-xxx.tar.gz
# tar -xvf sipp-xxx.tar
# cd sipp
# make pcapplay
```

- **With [PCAP play](#) and [authentication](#) support:**

```
# gunzip sipp-xxx.tar.gz
```



```
# tar -xvf sipp-xxx.tar
# cd sipp
# make pcapplay_oss1
```

**Note:**

To enable [GSL](http://www.gnu.org/software/gsl/) ( <http://www.gnu.org/software/gsl/>) at compile time, you must install GSL and its include files, as well as un-comment the lines in the local.mk file of SIPp distribution. Then, re-compile SIPp.

- On Windows, SIPp is provided both with the source and the pre-compiled executable. Just execute the installer to have SIPp installed.

**Warning:**

SIPp compiles under CYGWIN, provided that you installed IPv6 extension for CYGWIN (<http://win6.jp/Cygwin/>), as well as OpenSSL and libncurses.

- To compile SIPp on Windows with pcap (media support), you must:
  - Copy the [WinPcap developer package](http://www.winpcap.org/devel.htm) ( <http://www.winpcap.org/devel.htm>) to "C:\cygwin\lib\WpdPack"
  - Remove or rename "pthread.h" in "C:\cygwin\lib\WpdPack\Include", as it interferes with pthread.h from cygwin
  - Compile using either "make pcapplay\_cygwin" or "pcapplay\_oss1\_cygwin"

## 2.6 Increasing File Descriptors Limit

If your system does not supports enough file descriptors, you may experience problems when using the TCP/TLS mode with many simultaneous calls.

You have two ways to overcome this limit: either use the `-max_socket` command line option or change the limits of your system.

Depending on the operating system you use, different procedures allow you to increase the maximum number of file descriptors:

- On Linux 2.4 kernels the default number of file descriptors can be increased by modifying the `/etc/security/limits.conf` and the `/etc/pam.d/login` file.

Open the `/etc/security/limits.conf` file and add the following lines:

```
soft nofile 1024
hard nofile 65535
```

Open the `/etc/pam.d/login` and add the following line

```
session required /lib/security/pam_limits.so
```

The system file descriptor limit is set in the `/proc/sys/fs/file-max` file. The following command will increase the file descriptor limit:

```
echo 65535> /proc/sys/fs/file-max
```

To increase the number of file descriptors to its maximum limit (65535) set in the `/etc/security/limits.conf` file, type:

```
ulimit -n unlimited
```

Logout then login again to make the changes effective.

- On HP-UX systems the default number of file descriptors can be increased by modifying the system configuration with the `sam` utility. In the Kernel Configuration menu, select Configurable parameters, and change the following attributes:

```
maxfiles : 4096
maxfiles_lim : 4096
nfiles : 4096
ninode : 4096
max_thread_proc : 4096
nkthread : 4096
```

## 3 Using SIPp

### 3.1 Main features

SIPp allows to generate one or many SIP calls to one remote system. The tool is started from the command line. In this example, two SIPp are started in front of each other to demonstrate SIPp capabilities.

Run sipp with embedded server (uas) scenario:

```
# ./sipp -sn uas
```

On the same host, run sipp with embedded client (uac) scenario

```
# ./sipp -sn uac 127.0.0.1
```

### 3.2 Integrated scenarios

Integrated scenarios? Yes, there are scenarios that are embedded in SIPp executable. While you can create your own custom SIP scenarios (see [how to create your own XML scenarios](#)), a few basic (yet useful) scenarios are available in SIPp executable.

#### 3.2.1 UAC

Scenario file: [uac.xml](#) ( uac.xml.html) ([original XML file](#) ( uac.xml) )

SIPp UAC	Remote
----------	--------

```

(1) INVITE
----->
(2) 100 (optional)
<-----
(3) 180 (optional)
<-----
(4) 200
<-----
(5) ACK
----->

(6) PAUSE

(7) BYE
----->
(8) 200
<-----

```

### 3.2.2 UAC with media

Scenario file: [uac\\_pcap.xml](#) ( uac\_pcap.xml.html) ([original XML file](#) ( uac\_pcap.xml) )

```

SIPp UAC Remote
(1) INVITE
----->
(2) 100 (optional)
<-----
(3) 180 (optional)
<-----
(4) 200
<-----
(5) ACK
----->

(6) RTP send (8s)
=====>

(7) RFC2833 DIGIT 1
=====>

(8) BYE
----->
(9) 200
<-----

```

### 3.2.3 UAS

Scenario file: [uas.xml](#) ( uas.xml.html) ([original XML file](#) ( uas.xml) )

```

Remote          SIPp UAS
| (1) INVITE    |
|----->      |
| (2) 180      |
|-----<      |
| (3) 200      |
|-----<      |
| (4) ACK      |
|----->      |
| (5) PAUSE    |
| (6) BYE      |
|----->      |
| (7) 200      |
|-----<      |

```

### 3.2.4 regexp

Scenario file: [regexp.xml](#) ( regexp.xml.html) ([original XML file](#) ( regexp.xml) )

This scenario, which behaves as an UAC is explained in greater details in [this section](#).

```

SIPp regexp    Remote
| (1) INVITE    |
|----->      |
| (2) 100 (optional) |
|-----<      |
| (3) 180 (optional) |
|-----<      |
| (4) 200      |
|-----<      |
| (5) ACK      |
|----->      |
| (6) PAUSE    |
| (7) BYE      |
|----->      |
| (8) 200      |
|-----<      |

```

### 3.2.5 branch

Scenario files: [branchc.xml](#) ( branchc.xml.html ) ([original XML file](#) ( branchc.xml ) ) and [branchs.xml](#) ( branchs.xml.html ) ([original XML file](#) ( branchs.xml ) )

Those scenarios, which work against each other (branchc for client side and branchs for server side) are explained in greater details in [this section](#).

```
REGISTER ----->
200 <-----
200 <-----
INVITE ----->
100 <-----
180 <-----
403 <-----
200 <-----
ACK ----->
[ 5000 ms ]
BYE ----->
200 <-----
```

### 3.2.6 UAC Out-of-call Messages

#### Warning:

In SIPp 3.2, this feature is only enabled when the -aa (auto-answer) command-line parameter is used.

Scenario file: [ooc\\_default.xml](#) ( ooc\_default.xml.html ) ([original XML file](#) ( ooc\_default.xml ) )

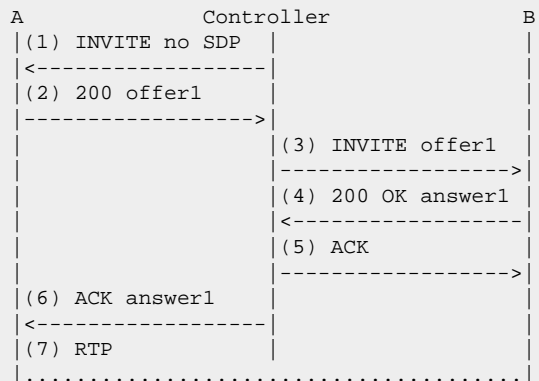
When a SIPp UAC receives an out-of-call request, it instantiates an out-of-call scenario. By default this scenario simply replies with a 200 OK response. This scenario can be overridden by passing the -oocsf or -oocsn command line options.

```
SIPp UAC           Remote
| (1) .*          |
| <-----       |
| (2) 200         |
| ----->       |
```

### 3.2.7 3PCC

3PCC stands for 3rd Party Call Control. 3PCC is described in [RFC 3725](#) ( <http://www.ietf.org/rfc/rfc3725.txt> ) . While this feature was first developed to allow 3PCC like scenarios, it can also be used for every case where you would need one SIPp to talk to several remotes.

In order to keep SIPp simple (remember, it's a test tool!), one SIPp instance can only talk to one remote. Which is an issue in 3PCC call flows, like call flow I (SIPp being a controller):



Scenario file: [3pcc-A.xml](#) ( 3pcc-A.xml.html ) ( [original XML file](#) ( 3pcc-A.xml ) )

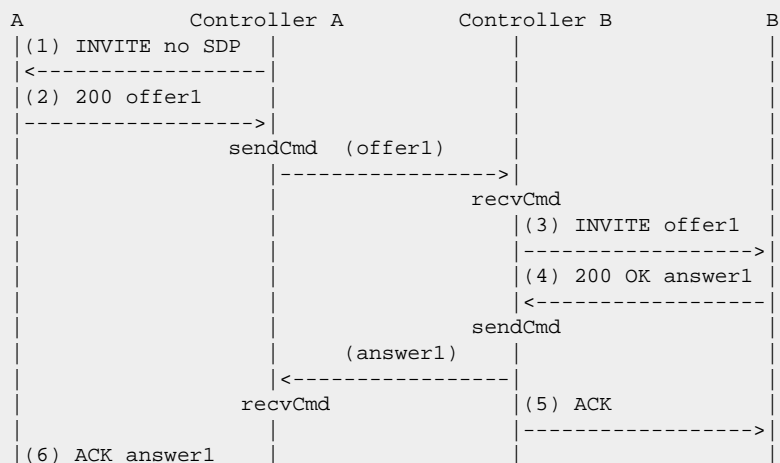
Scenario file: [3pcc-B.xml](#) ( 3pcc-B.xml.html ) ( [original XML file](#) ( 3pcc-B.xml ) )

Scenario file: [3pcc-C-A.xml](#) ( 3pcc-C-A.xml.html ) ( [original XML file](#) ( 3pcc-C-A.xml ) )

Scenario file: [3pcc-C-B.xml](#) ( 3pcc-C-B.xml.html ) ( [original XML file](#) ( 3pcc-C-B.xml ) )

The 3PCC feature in SIPp allows to have two SIPp instances launched and synchronised together. If we take the example of call flow I, one SIPp instance will take care of the dialog with remote A (this instance is called 3PCC-C-A for 3PCC-Controller-A-Side) and another SIPp instance will take care of the dialog with remote B (this instance is called 3PCC-C-B for 3PCC-Controller-B-Side).

The 3PCC call flow I will, in reality, look like this (Controller has been divided in two SIPp instances):



```

|<-----|
| (7) RTP |
|-----|

```

As you can see, we need to pass information between both sides of the controller. SDP "offer1" is provided by A in message (2) and needs to be sent to B side in message (3). This mechanism is implemented in the scenarios through the `<sendCmd>` command. This:

```

<sendCmd>
  <![CDATA[
    Call-ID: [call_id]
    [$1]

  ]]>
</sendCmd>

```

Will send a "command" to the twin SIPp instance. Note that including the Call-ID is mandatory in order to correlate the commands to actual calls. In the same manner, this:

```

<recvCmd>
  <action
    <ereg regexp="Content-Type: .*"
      search_in="msg"
      assign_to="2"/>
  </action>
</recvCmd>

```

Will receive a "command" from the twin SIPp instance. Using the [regular expression](#) mechanism, the content is retrieved and stored in a call variable (\$2 in this case), ready to be reinjected

```

<send>
  <![CDATA[

    ACK sip:[service]@[remote_ip]:[remote_port] SIP/2.0
    Via: SIP/2.0/[transport] [local_ip]:[local_port]
    From: sipp <sip:sipp@[local_ip]:[local_port]>;tag=[call_number]
    To: sut <sip:[service]@[remote_ip]:[remote_port]>[peer_tag_param]
    Call-ID: [call_id]
    CSeq: 1 ACK
    Contact: sip:sipp@[local_ip]:[local_port]
    Max-Forwards: 70
    Subject: Performance Test
    [$2]

  ]]>
</send>

```

In other words, `sendCmd` and `recvCmd` can be seen as synchronization points between two SIPp instances, with the ability to pass parameters between each other.

Another scenario that has been reported to be do-able with the 3PCC feature is the following:

- A calls B. B answers. B and A converse
- B calls C. C answers. C and B converse
- B "REFER"s A to C and asks to replace A-B call with B-C call.
- A accepts. A and C talk. B drops out of the calls.

### 3.3 3PCC Extended

An extension of the 3pcc mode is implemented in sipp. This feature allows n twin sipp instances to communicate each other, each one of them being connected to a remote host.

The sipp instance which initiates the call is launched in "master" mode. The others are launched in "slave" mode. Twin sipp instances have names, given in the command line (for example, s1, s2...sn for the slaves and m for the master) Correspondances between instances names and their addresses must be stored in a file (provided by -slave\_cfg command line argument), in the following format:

```
s1;127.0.0.1:8080
s2;127.0.0.1:7080
m;127.0.0.1:6080
```

Each twin sipp instance must access a different copy of this file.

[sendCmd](#) and [recvCmd](#) have additional attributes:

```
<sendCmd dest="s1">
  <![CDATA[
    Call-ID: [call_id]
    From: m
    [$1]
  ]]>
</sendCmd>
```

Will send a command to the "s1" peer instance, which can be either master or slave, depending on the command line argument, which must be consistent with the scenario: a slave instance cannot have a sendCmd action before having any recvCmd. Note that the message must contain a "From" field, filled with the name of the sender.

```
<recvCmd src="m">
  <action
    <ereg regexp="Content-Type: .*"
      search_in="msg"
      assign_to="2" />
  </action>
```



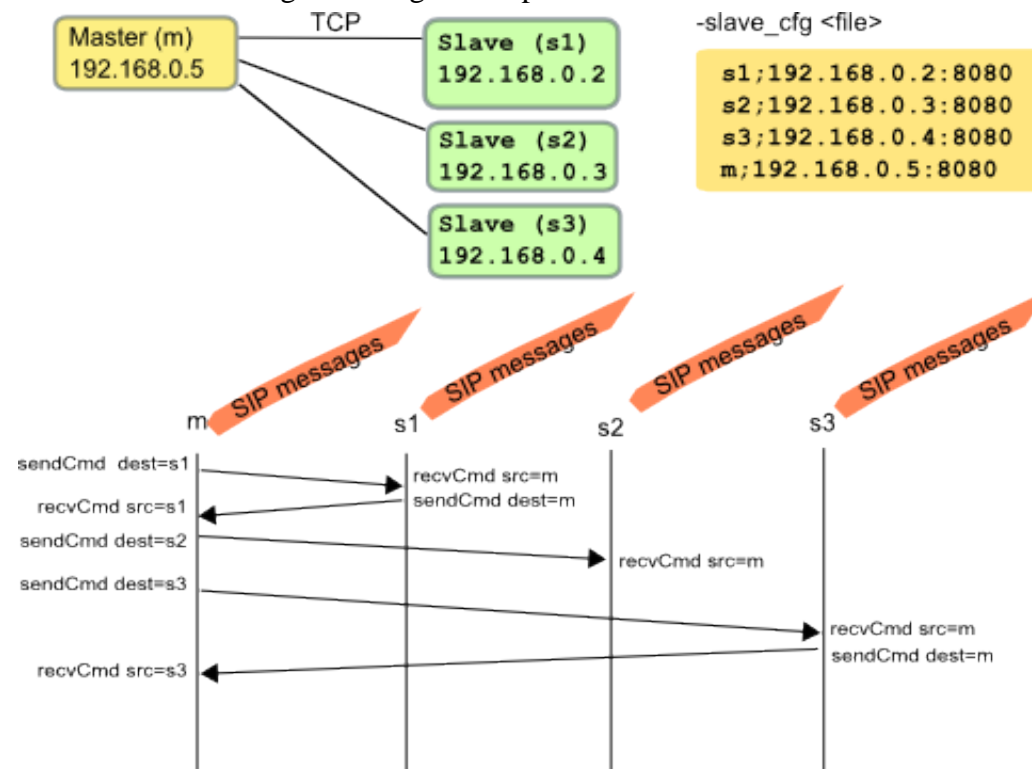
```
</recvCmd>
```

Indicates that the twin command is expected to be received from the "m" peer instance.

Note that the master must be the launched at last.

There is no integrated scenarios for the 3pcc extended mode, but you can easily adapt those from 3pcc.

Example: the following drawing illustrate the entire procedure. The arrows that are shown between SIPp master and slaves depict only the synchronization commands exchanged between the different SIPp instances. The SIP message exchange takes place as usual.



### 3.4 Controlling SIPp

SIPp can be controlled interactively through the keyboard or via a UDP socket. SIPp supports both 'hot' keys that can be entered at any time and also a simple command mode. The hot keys are:

Key	Action
+	Increase the call rate by 1 * rate_scale
*	Increase the call rate by 10 * rate_scale
-	Decrease the call rate by 1 * rate_scale
/	Decrease the call rate by 10 * rate_scale
c	Enter command mode
q	Quit SIPp (after all calls complete, enter a second time to quit immediately)
Q	Quit SIPp immediately
s	Dump screens to the log file (if -trace_screen is passed)
p	Pause traffic
1	Display the scenario screen
2	Display the statistics screen
3	Display the repartition screen
4	Display the variable screen
5	Display the TDM screen
6-9	Display the second through fifth repartition screen.

In command mode, you can type a single line command that instructs SIPp to take some action. Command mode is more versatile than the hot keys, but takes more time to input some common actions. The following commands are available:

Command	Description	Example
dump tasks	Prints a list of active tasks (most tasks are calls) to the error log.	dump tasks
set rate X	Sets the call rate.	set rate 10
set rate-scale X	Sets the rate scale, which adjusts the speed of '+', '-', '*', and '/'.	set rate-scale 10
set users X	Sets the number of users (only valid when -users is specified).	set rate 10

Command	Description	Example
set limit X	Sets the open call limit (equivalent to -l option)	set limit 100
set hide <true false>	Should the hide XML attribute be respected?	set hide false
set index <true false>	Display message indexes in the scenario screen.	set index true
set display <main ooc>	Changes the scenario that is displayed to either the main or the out-of-call scenario.	set display main set display ooc
trace <log> <on off>	Turns log on or off at run time. Valid values for log are "error", "logs", "messages", and "shortmessages".	trace error on

Table 2: List of Interactive Commands

### 3.4.1 Traffic control

SIPp generates SIP traffic according to the scenario specified. You can control the number of calls (scenario) that are started per second. If you pass the `-users` option, then you need to control the number of instantiated users. You can control the rate through:

- Interactive hot keys (described in the previous section)
- Interactive Commands
- Startup Parameters

There are two commands that control rates: `set rate X` sets the current call rate to X. Additionally, `set rate-scale X` sets the `rate_scale` parameter to X. This enables you to use the '+', '-', '\*', and '/' keys to set the rate more quickly. For example, if you do `set rate-scale 100`, then each time you press '+', the call rate is increased by 100 calls and each time you press '\*', the call rate is increased by 1000 calls. Similarly, for a user based benchmark you can run `set users X`.

At starting time, you can control the rate by specifying parameters on the command line:

- "-r" to specify the call rate in number of calls per seconds
- "-rp" to specify the "rate period" in milliseconds for the call rate (default is 1000ms/1sec). This allows you to have n calls every m milliseconds (by using `-r n -rp m`).

#### Note:

Example: run SIPp at 7 calls every 2 seconds (3.5 calls per second)

```
./sipp -sn uac -r 7 -rp 2000 127.0.0.1
```

You can also **pause** the traffic by pressing the 'p' key. SIPp will stop placing new calls and wait until all current calls go to their end. You can **resume** the traffic by pressing 'p' again.

To **quit** SIPp, press the 'q' key. SIPp will stop placing new calls and wait until all current calls go to their end. SIPp will then exit.

You can also force SIPp to **quit** immediately by pressing the 'Q' key. Current calls will be terminated by sending a BYE or CANCEL message (depending if the calls have been established or not). The same behaviour is obtained by pressing 'q' twice.

**Note:**

**TIP:** you can place a defined number of calls and have SIPp exit when this is done. Use the `-m` option on the command line.

### 3.4.2 Remote control

SIPp can be "remote-controlled" through a UDP socket. This allows for example

- To automate a series of actions, like increasing the call rate smoothly, wait for 10 seconds, increase more, wait for 1 minute and loop
- Have a feedback loop so that an application under test can remote control SIPp to lower the load, pause the traffic, ...

Each SIPp instance is listening to a UDP socket. It starts to listen to port 8888 and each following SIPp instance (up to 60) will listen to `base_port + 1` (8889, 8890, ...).

It is then possible to control SIPp like this:

```
echo p >/dev/udp/x.y.z.t/8888 -> put SIPp in pause state (p key)
echo q >/dev/udp/x.y.z.t/8888 -> quit SIPp (q key)
```

**Note:**

All keys available through keyboard are also available in the remote control interface

You could also have a small shell script to automate a serie of action. For example, this script will increase the call rate by 10 more new calls/s every 5 seconds, wait at this call rate for one minute and exit SIPp:

```
#!/bin/sh
echo "*" >/dev/udp/127.0.0.1/8889
sleep 5
echo "*" >/dev/udp/127.0.0.1/8889
sleep 5
echo "*" >/dev/udp/127.0.0.1/8889
sleep 5
echo "*" >/dev/udp/127.0.0.1/8889
sleep 60
```

```
echo "q" >/dev/udp/127.0.0.1/8889
```

To send a command to SIPp, preface it with 'c'. For example: `echo "cset rate 100" >/dev/udp/127.0.0.1/8888` sets the call rate to 100.

### 3.5 Running SIPp in background

SIPp can be launched in background mode (`-bg` command line option).

By doing so, SIPp will be detached from the current terminal and run in the background. The PID of the SIPp process is provided. If you didn't specify a number of calls to execute with the `-m` option, SIPp will run forever.

There is a mechanism implemented to stop SIPp smoothly. The command `kill -SIGUSR1 [SIPp_PID]` will instruct SIPp to stop placing any new calls and finish all ongoing calls before exiting.

When using the background mode, the main sipp instance stops and a child process will continue the job. Therefore, the log files names will contain another PID than the actual sipp instance PID.

### 3.6 Create your own XML scenarios

Of course embedded scenarios will not be enough. So it's time to create your own scenarios. A SIPp scenario is written in XML (a DTD that may help you write SIPp scenarios does exist and has been tested with jEdit - this is described in a later section). A scenario will always start with:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<scenario name="Basic Sipstone UAC">
```

And end with:

```
</scenario>
```

Easy, huh? Ok, now let's see what can be put inside. You are not obliged to read the whole table now! Just go in the next section for an example.

There are many common attributes used for flow control and statistics, that can be used for all of the message commands (i.e., `<send>`, `<recv>`, `<nop>`, `<pause>`, `<sendCmd>`, and `<recvCmd>`).

Attribute(s)	Description	Example
start_rtd	Starts one of the "Response Time Duration" timer. (see <a href="#">statistics section</a> ).	<code>&lt;send start_rtd="invite"&gt;</code> : the timer named "invite" will start when the message is sent.
rtd	Stops one of the 5 "Response Time Duration" timer.	<code>&lt;send rtd="2"&gt;</code> : the timer number 2 will stop when the message is sent.

Attribute(s)	Description	Example
repeat_rtd	Used with a rtd attribute, it allows the corresponding " <b>Response Time Duration</b> " timer to be counted more than once per call (useful for loop call flows).	<send rtd="1" repeat_rtd="true">: the timer number 1 value will be printed but the timer won't stop.
crlf	Displays an empty line <b>after</b> the arrow for the message in main SIPp screen.	<send crlf="true">
next	You can put a "next" in any command element to go to another part of the script when you are done with sending the message. For optional receives, the next is only taken if that message was received. See <a href="#">conditional branching</a> section for more info.	<p>Example to jump to label "12" after sending an ACK:</p> <pre data-bbox="1503 456 2190 922"> &lt;send next="12"&gt;   &lt;![CDATA[       ACK sip:[service]@[remote_ip]:[remote_port] SIP/2.0 Via: ... From: ... To: ... Call-ID: ... Cseq: ... Contact: ... Max-Forwards: ... Subject: ... Content-Length: 0    ]]&gt; &lt;/send&gt; </pre> <p>Example to jump to label "5" when receiving a 403 message:</p> <pre data-bbox="1503 978 2190 1241"> &lt;recv response="100"   optional="true"&gt; &lt;/recv&gt; &lt;recv response="180" optional="true"&gt; &lt;/recv&gt; &lt;recv response="403" optional="true" next="5"&gt; &lt;/recv&gt; &lt;recv response="200"&gt; &lt;/recv&gt; </pre>
test	You can put a "test" next to a "next" attribute to indicate that you only want to branch to the label specified with "next" if the variable specified in "test" is set (through <a href="#">regex</a> for example). See <a href="#">conditional branching</a> section for more info.	<p>Example to jump to label "6" after sending an ACK only if variable 4 is set:</p> <pre data-bbox="1503 1329 2190 1420"> &lt;send next="6" test="4"&gt;   &lt;![CDATA[ </pre>

Attribute(s)	Description	Example
		<pre> ACK sip:[service]@[remote_ip]:[remote_port] SIP/2.0 Via: ... From: ... To: ... Call-ID: ... Cseq: ... Contact: ... Max-Forwards: ... Subject: ... Content-Length: 0  ]]&gt; &lt;/send&gt; </pre>
chance	In combination with "test", probability to actually branch to another part of the scenario. Chance can have a value between 0 (never) and 1 (always). See <a href="#">conditional branching</a> section for more info.	<pre> &lt;recv response="403" optional="true" next="5" test="3" chance="0.90"&gt; &lt;/recv&gt; </pre> <p>90% chance to go to label "5" if variable "3" is set.</p>
condexec	Executes an element only if the variable in the condexec attribute is set. This attribute allows you to write complex XML scenarios with fewer next attributes and labels.	<pre>&lt;nop condexec="executethis"&gt;</pre>
condexec_inverse	If condexec is set, condexec_inverse inverts the condition in condexec. This allows you to execute an element only when a variable is not set.	<pre>&lt;nop condexec="skipthis" condexec_inverse="true"&gt;</pre>
counter	Increments the counter given as parameter when the message is sent. The counters are saved in the <a href="#">statistic file</a> .	<pre>&lt;send counter="MsgA"&gt;</pre> Increments counter "MsgA" when the message is sent.

Table 1: List of attributes common to all commands

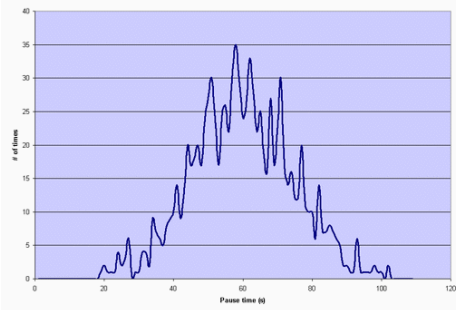
Each command also has its own unique attributes, listed here:

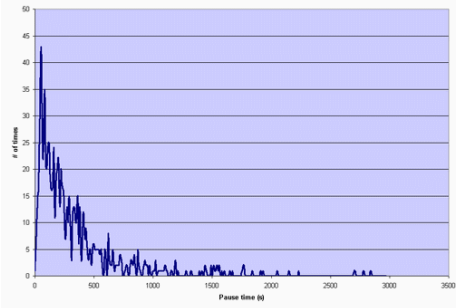
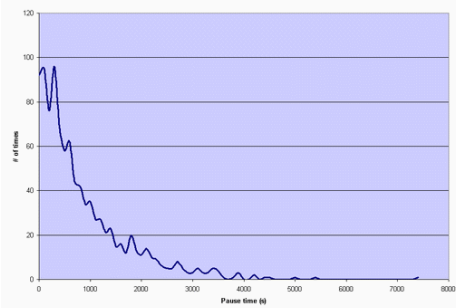
Command	Attribute(s)	Description	Example
<b>&lt;send&gt;</b>	retrans	Used for UDP transport only; it specifies the T1 timer value, as described in SIP RFC 3261, section 17.1.1.2.	<pre>&lt;send retrans="500"&gt;</pre> will initiate T1 timer to 500 milliseconds (RFC3261 default).
	lost	Emulate packet lost. The value is specified as a percentage.	<pre>&lt;send lost="10"&gt;</pre> 10% of the message sent are actually not sent :).

Command	Attribute(s)	Description	Example
	start_txn	Records the branch ID of this sent message so that responses can be properly matched (without this element the transaction matching is done based on the CSeq method, which is imprecise).	<send start_txn="invite">: Stores the branch ID of this message in the transaction named "invite".
	ack_txn	Indicates that the ACK being sent corresponds to the transaction started by a start_txn attribute. Every INVITE with a start_txn tag must have a matching ACK with an ack_txn attribute.	<send ack_txn="invite">: References the branch ID of the transaction named "invite".
<recv>	response	Indicates what SIP message code is expected.	<recv response="200">: SIPp will expect a SIP message with code "200".
	request	Indicates what SIP message request is expected.	<recv request="ACK">: SIPp will expect an "ACK" SIP message.
	optional	Indicates if the message to receive is optional. In case of an optional message and if the message is actually received, it is not seen as a unexpected message. When an unexpected message is received, Sipp looks if this message matches an optional message defined in the previous step of the scenario. If optional is set to "global", Sipp will look every previous steps of the scenario.	<recv response="100" optional="true">: The 100 SIP message can be received without being considered as "unexpected".
	rrs	<b>Record Route Set</b> . if this attribute is set to "true", then the "Record-Route:" header of the message received is stored and can be recalled using the <b>[routes]</b> keyword.	<recv response="100" rrs="true">.
	auth	<b>Authentication</b> . if this attribute is set to "true", then the "Proxy-Authenticate:" header of the message received is stored and is used to build the <b>[authentication]</b> keyword.	<recv response="407" auth="true">.
	lost	Emulate packet lost. The value is specified as a percentage.	<recv lost="10">: 10% of the message received are thrown away.



Command	Attribute(s)	Description	Example
	timeout	Specify a timeout while waiting for a message. If the message is not received, the call is aborted, unless an ontimeout label is defined.	<code>&lt;recv timeout="100000"&gt;</code>
	ontimeout	Specify a label to jump to if the timeout popped before the message to be received.	Example to jump to label "5" when not receiving a 100 message after 100 seconds: <pre>&lt;recv response="100" timeout="100000" ontimeout="5"&gt; &lt;/recv&gt;</pre>
	action	Specify an action when receiving the message. See <a href="#">Actions section</a> for possible actions.	Example of a "regular expression" action: <pre>&lt;recv response="200"&gt; &lt;action&gt; &lt;ereg regexp="([0-9]{1,3}\.){3} [0-9]{1,3}:[0-9]*" search_in="msg" check_it="true" assign_to="1,2"/&gt; &lt;/action&gt; &lt;/recv&gt;</pre>
	regexp_match	Boolean. Indicates if 'request' ('response' is not available) is given as a regular expression. If so, the recv command will match against the regular expression. This allows to catch several cases in the same receive command.	Example of a recv command that matches MESSAGE or PUBLISH or SUBSCRIBE requests: <pre>&lt;recv request="MESSAGE  PUBLISH SUBSCRIBE" crlf="true" regexp_match="true"&gt; &lt;/recv&gt;</pre>
	response_txn	Indicates that this is a response to a transaction that was previously started. To match, the branch ID of the first via header must match the stored transaction ID.	<code>&lt;recv response="200" response_txn="invite" /&gt;</code> : Matches only responses to the message sent with start_txn="invite" attribute.
<b>&lt;pause&gt;</b>	milliseconds	Specify the pause delay, in milliseconds. When this delay is not set, the value of the -d command line parameter is used.	<code>&lt;pause milliseconds="5000"/&gt;</code> : pause the scenario for 5 seconds.

Command	Attribute(s)	Description	Example
	variable	Indicates which call variable to use to determine the length of the pause.	<code>&lt;pause variable="1" /&gt;</code> pauses for the number of milliseconds specified by call variable 1.
	distribution	Indicates which statistical distribution to use to determine the length of the pause. Without GSL, you may use <code>uniform</code> or <code>fixed</code> . With GSL, <code>normal</code> , <code>exponential</code> , <code>gamma</code> , <code>lambda</code> , <code>lognormal</code> , <code>negbin</code> , (negative binomial), <code>pareto</code> , and <code>weibull</code> are available. Depending on the distribution you select, you must also supply distribution specific parameters.	<p>The following examples show the various types of distributed pauses:</p> <ul style="list-style-type: none"> <li><code>&lt;pause distribution="fixed" value="1000" /&gt;</code> pauses for 1 second.</li> <li><code>&lt;pause distribution="uniform" min="2000" max="5000" /&gt;</code> pauses between 2 and 5 seconds.</li> </ul> <p>The remaining distributions require GSL. In general The parameter names were chosen to be as consistent with Wikipedia's distribution description pages.</p> <ul style="list-style-type: none"> <li><code>&lt;pause distribution="normal" mean="60000" stdev="15000" /&gt;</code> provides a normal pause with a mean of 60 seconds (i.e. 60,000 ms) and a standard deviation of 15 seconds. The mean and standard deviation are specified as integer milliseconds. The distribution will look like:</li> </ul>  <ul style="list-style-type: none"> <li><code>&lt;pause distribution="lognormal" mean="12.28" stdev="1" /&gt;</code></li> </ul>

Command	Attribute(s)	Description	Example
			<p>creates a distribution's whose natural logarithm has a mean of 12.28 and a standard deviation of 1. The mean and standard deviation are specified as double values (in milliseconds). The distribution will look like:</p>  <ul style="list-style-type: none"> <li> <p><code>&lt;pause distribution="exponential" mean="900000" /&gt;</code> creates an exponentially distributed pause with a mean of 15 minutes. The distribution will look like:</p>  </li> <li> <p><code>&lt;pause distribution="weibull" lambda="3" k="4" /&gt;</code> creates a Weibull distribution with a scale of 3 and a shape of 4 (see <a href="#">Weibull on Wikipedia</a>)</p> </li> </ul>

Command	Attribute(s)	Description	Example
			<p>( <a href="http://en.wikipedia.org/wiki/Weibull">http://en.wikipedia.org/wiki/Weibull</a>) for a description of the distribution).</p> <ul style="list-style-type: none"> <li>• <code>&lt;pause distribution="pareto" k="1" x_m="2" /&gt;</code> creates a Pareto distribution with k and <math>x_m</math> of 1 and 2, respectively (see <a href="http://en.wikipedia.org/wiki/Pareto_distribution">Pareto on Wikipedia</a> ( <a href="http://en.wikipedia.org/wiki/Pareto_distribution">http://en.wikipedia.org/wiki/Pareto_distribution</a>) for a description of the distribution).</li> <li>• <code>&lt;pause distribution="gamma" k="3" theta="2" /&gt;</code> creates a Gamma distribution with k and theta of 9 and 2, respectively (see <a href="http://en.wikipedia.org/wiki/Gamma_distribution">Gamma on Wikipedia</a> ( <a href="http://en.wikipedia.org/wiki/Gamma_distribution">http://en.wikipedia.org/wiki/Gamma_distribution</a>) for a description of the distribution).</li> <li>• <code>&lt;pause distribution="negbin" p="0.1" n="2" /&gt;</code> creates a Negative binomial distribution with p and n of 0.1 and 2, respectively (see <a href="http://en.wikipedia.org/wiki/Negative_binomial_distribution">Negative Binomial on Wikipedia</a> ( <a href="http://en.wikipedia.org/wiki/Negative_binomial_distribution">http://en.wikipedia.org/wiki/Negative_binomial_distribution</a>) for a description of the distribution).</li> </ul>
	sanity_check	By default, statistically distributed pauses are sanity checked to ensure that their 99th percentile values are less than INT_MAX. Setting <b>sanity_check</b> to false disables this behavior.	<code>&lt;pause distribution="lognormal" mean="10" stdev="10" sanity_check="false" /&gt;</code> disables sanity checking of the lognormal distribution.
<b>&lt;nop&gt;</b>	action	The nop command doesn't do anything at SIP level. It is only there to specify an action to execute. See <a href="#">Actions section</a> for possible actions.	Execute the play_pcap_audio/video action: <pre>&lt;nop&gt;   &lt;action&gt;     &lt;exec play_pcap_audio="pcap/g711a.pcap" /&gt;   &lt;/action&gt; &lt;/nop&gt;</pre>
<b>&lt;sendCmd&gt;</b>	<![CDATA[]]>	Content to be sent to the twin <a href="#">3PCC</a> SIPp instance. The Call-ID must be included in the	<pre>&lt;sendCmd&gt;   &lt;![CDATA[</pre>

Command	Attribute(s)	Description	Example
		CDATA. In 3pcc extended mode, the From must be included to.	<pre>Call-ID: [call_id] [\$1]  ]]&gt; &lt;/sendCmd&gt;</pre>
	dest	3pcc extended mode only: the twin sipp instance which the command will be sent to	<sendCmd dest="s1">: the command will be sent to the "s1" twin instance
<recvCmd>	action	Specify an action when receiving the command. See <a href="#">Actions section</a> for possible actions.	<p>Example of a "regular expression" to retrieve what has been send by a sendCmd command:</p> <pre>&lt;recvCmd&gt;   &lt;action&gt;     &lt;ereg regexp="Content-Type: .*"       search_in="msg"       assign_to="2" /&gt;   &lt;/action&gt; &lt;/recvCmd&gt;</pre>
	src	3pcc extended mode only: indicate the twin sipp instance which the command is expected to be received from	<recvCmd src = "s1">: the command will be expected to be received from the "s1" twin instance
<label>	id	A label is used when you want to branch to specific parts in your scenarios. The "id" attribute is an integer where the maximum value is 19. See <a href="#">conditional branching</a> section for more info.	<p>Example: set label number 13:</p> <pre>&lt;label id="13" /&gt;</pre>
<Response Time Repartition>	value	Specify the intervals, in milliseconds, used to distribute the values of response times.	<ResponseTimeRepartition value="10, 20, 30"/>: response time values are distributed between 0 and 10ms, 10 and 20ms, 20 and 30ms, 30 and beyond.
<Call Length Repartition>	value	Specify the intervals, in milliseconds, used to distribute the values of the call length measures.	<CallLengthRepartition value="10, 20, 30"/>: call length values are distributed between 0 and 10ms, 10 and 20ms, 20 and 30ms, 30 and beyond.
<Globals>	variables	Specify the name of globally scoped variables.	<Globals variables="foo,bar" />.

Command	Attribute(s)	Description	Example
<User>	variables	Specify the name of user-scoped variables.	<User variables="foo,bar" />.
<Reference>	variables	Suppresses warnings about unused variables.	<Reference variables="dummy" />

Table 2: List of commands with their attributes

There are not so many commands: send, rcv, sendCmd, rcvCmd, pause, ResponseTimeRepartition, CallLengthRepartition, Globals, User, and Reference. To make things even clearer, nothing is better than an example...

### 3.6.1 Structure of client (UAC like) XML scenarios

A client scenario is a scenario that starts with a "send" command. So let's start:

```
<scenario name="Basic Sipstone UAC">
  <send>
    <![CDATA[

      INVITE sip:[service]@[remote_ip]:[remote_port] SIP/2.0
      Via: SIP/2.0/[transport] [local_ip]:[local_port]
      From: sipp <sip:sipp@[local_ip]:[local_port]>;tag=[call_number]
      To: sut <sip:[service]@[remote_ip]:[remote_port]>
      Call-ID: [call_id]
      Cseq: 1 INVITE
      Contact: sip:sipp@[local_ip]:[local_port]
      Max-Forwards: 70
      Subject: Performance Test
      Content-Type: application/sdp
      Content-Length: [len]

      v=0
      o=user1 53655765 2353687637 IN IP[local_ip_type] [local_ip]
      s=-
      t=0 0
      c=IN IP[media_ip_type] [media_ip]
      m=audio [media_port] RTP/AVP 0
      a=rtpmap:0 PCMU/8000

    ]]>
  </send>
```

Inside the "send" command, you have to enclose your SIP message between the "<![CDATA" and the "]]>" tags. Everything between those tags is going to be sent toward the remote system. You may have noticed that there are strange keywords in the SIP message, like [service], [remote\_ip], .... Those keywords are used to indicate to SIPp that it has to do something with it.

Here is the list:

Keyword	Default	Description
[service]	service	Service field, as passed in the <b>-s service_name</b>
[remote_ip]	-	Remote IP address, as passed on the command line.
[remote_port]	5060	Remote IP port, as passed on the command line. You can add a computed offset [remote_port+3] to this value.
[transport]	UDP	Depending on the value of <b>-t</b> parameter, this will take the values "UDP" or "TCP".
[local_ip]	Primary host IP address	Will take the value of <b>-i</b> parameter.
[local_ip_type]	-	Depending on the address type of <b>-i</b> parameter (IPv4 or IPv6), local_ip_type will have value "4" for IPv4 and "6" for IPv6.
[local_port]	Chosen by the system	Will take the value of <b>-p</b> parameter. You can add a computed offset [local_port+3] to this value.
[len]	-	Computed length of the SIP body. To be used in "Content-Length" header. You can add a computed offset [len+3] to this value.
[call_number]	-	Index. The call_number starts from "1" and is incremented by 1 for each call.
[cseq]	-	Generates automatically the CSeq number. The initial value is 1 by default. It can be changed by using the <b>-base_cseq</b> command line option.
[call_id]	-	A call_id identifies a call and is generated by SIPp for each new call. <b>In client mode, it is mandatory to use the value generated by SIPp in the "Call-ID" header.</b> Otherwise, SIPp will not recognise the answer to the message sent as being part of an existing call. Note: [call_id] can be pre-pended with an arbitrary string using '///'. Example: Call-ID: ABCDEFGHIJ///[call_id] - it will still be recognized by SIPp as part of the same call.

Keyword	Default	Description
[media_ip]	-	Depending on the value of <b>-mi</b> parameter, it is the local IP address for RTP echo.
[media_ip_type]	-	Depending on the address type of <b>-mi</b> parameter (IPv4 or IPv6), media_ip_type will have value "4" for IPv4 and "6" for IPv6. Useful to build the SDP independently of the media IP type.
[media_port]	-	Depending on the value of <b>-mp</b> parameter, it set the local RTP echo port number. Default is none. RTP/UDP packets received on that port are echoed to their sender. You can add a computed offset [media_port+3] to this value.
[auto_media_port]	-	Only for pcap. To make audio and video ports begin from the value of <b>-mp</b> parameter, and change for each call using a periodical system, modulo 10000 (which limits to 10000 concurrent RTP sessions for pcap_play)
[last_*]	-	The '[last_*]' keyword is replaced automatically by the specified header if it was present in the last message received (except if it was a retransmission). If the header was not present or if no message has been received, the '[last_*]' keyword is discarded, and all bytes until the end of the line are also discarded. If the specified header was present several times in the message, all occurrences are concatenated (CRLF separated) to be used in place of the '[last_*]' keyword.
[field0-n file=<filename> line=<number>]	-	Used to inject values from an external CSV file. See <a href="#">"Injecting values from an external CSV during calls"</a> section. The optional file and line parameters allow you to select which of the injection files specified on the command line to use and which line number from that file.
[file name=<filename>]	-	Inserts the entire contents of filename into the message. Whitespace, including carriage returns and newlines at the end of the line in the file are not processed as with other keywords; thus your file must be formatted exactly as you would like the bytes to appear in the message.
[timestamp]	-	The current time using the same format as error log messages.



Keyword	Default	Description
[last_message]	-	The last received message.
[\$n]	-	Used to inject the value of call variable number n. See <a href="#">"Actions"</a> section
[authentication]	-	Used to put the authentication header. This field can have parameters, in the following form: [authentication username=myusername password=myspassword]. If no username is provided, the value from -s command line parameter (service) is used. If no password is provided, the value from -ap command line parameter is used. See <a href="#">"Authentication"</a> section
[pid]	-	Provide the process ID (pid) of the main SIPp thread.
[routes]	-	If the "rrs" attribute in a recv command is set to "true", then the "Record-Route:" header of the message received is stored and can be recalled using the [routes] keyword
[next_url]	-	If the "rrs" attribute in a recv command is set to "true", then the [next_url] contains the contents of the Contact header (i.e within the '<' and '>' of Contact)
[branch]	-	Provide a branch value which is a concatenation of magic cookie (z9hG4bK) + call number + message index in scenario. An offset (like [branch-N]) can be appended if you need to have the same branch value as a previous message.
[msg_index]	-	Provide the message number in the scenario.
[cseq]	-	Provides the CSeq value of the last request received. This value can be incremented (e.g. [cseq+1] adds 1 to the CSeq value of the last request).
[clock_tick]	-	Includes the internal SIPp clock tick value in the message.
[sipp_version]	-	Includes the SIPp version string in the message.
[tdmmap]	-	Includes the tdm map values used by the call in the message (see -tdmmap option).

Keyword	Default	Description
<b>[fill]</b>	-	Injects filler characters into the message. The length of the fill text is equal to the call variable stored in the <code>variable=N</code> parameter. By default the text is a sequence of X's, but can be controlled with the <code>text="text"</code> parameter.
<b>[users]</b>	-	If the <code>-users</code> command line option is specified, then this keyword contains the number of users that are currently instantiated.
<b>[userid]</b>	-	If the <code>-users</code> command line option is specified, then this keyword contains the integer identifier of the current user (starting at zero and ending at <code>[users-1]</code> ).

Table 1: Keyword list

Now that the INVITE message is sent, SIPp can wait for an answer by using the "[recv](#)" command.

```
<recv response="100"> optional="true"
</recv>

<recv response="180"> optional="true"
</recv>

<recv response="200">
</recv>
```

100 and 180 messages are optional, and 200 is mandatory. **In a "recv" sequence, there must be one mandatory message.**

Now, let's send the ACK:

```
<send>
<![CDATA[

ACK sip:[service]@[remote_ip]:[remote_port] SIP/2.0
Via: SIP/2.0/[transport] [local_ip]:[local_port]
From: sipp <sip:sipp@[local_ip]:[local_port]>;tag=[call_number]
To: sut <sip:[service]@[remote_ip]:[remote_port]>[peer_tag_param]
Call-ID: [call_id]
Cseq: 1 ACK
Contact: sip:sipp@[local_ip]:[local_port]
Max-Forwards: 70
Subject: Performance Test
Content-Length: 0

]]>
```

```
</send>
```

We can also insert a pause. The scenario will wait for 5 seconds at this point.

```
<pause milliseconds="5000" />
```

And finish the call by sending a BYE and expecting the 200 OK:

```
<send retrans="500">
  <![CDATA[

    BYE sip:[service]@[remote_ip]:[remote_port] SIP/2.0
    Via: SIP/2.0/[transport] [local_ip]:[local_port]
    From: sipp <sip:sipp@[local_ip]:[local_port]>;tag=[call_number]
    To: sut <sip:[service]@[remote_ip]:[remote_port]>[peer_tag_param]
    Call-ID: [call_id]
    Cseq: 2 BYE
    Contact: sip:sipp@[local_ip]:[local_port]
    Max-Forwards: 70
    Subject: Performance Test
    Content-Length: 0

  ]]>
</send>

<recv response="200">
</recv>
```

And this is the end of the scenario:

```
</scenario>
```

Creating your own SIPp scenarios is not a big deal. If you want to see other examples, use the `-sd` parameter on the command line to display embedded scenarios.

### 3.6.2 Structure of server (UAS like) XML scenarios

A server scenario is a scenario that starts with a `"recv"` command. The syntax and the list of available commands is the same as for "client" scenarios.

But you are more likely to use `[last_*]` keywords in those server side scenarios. For example, a UAS example will look like:

```
<recv request="INVITE">
</recv>

<send>
  <![CDATA[

    SIP/2.0 180 Ringing
    [last_Via:]
```

```

[last_From:]
[last_To:];tag=[call_number]
[last_Call-ID:]
[last_CSeq:]
Contact: <sip:[local_ip]:[local_port];transport=[transport]>
Content-Length: 0

]]>
</send>

```

The answering message, 180 Ringing in this case, is built with the content of headers received in the INVITE message.

### 3.6.3 Actions

In a "[recv](#)" or "[recvCmd](#)" command, you have the possibility to execute an action. Several actions are available:

- [Regular expressions](#) (ereg)
- [Log something in aa log file](#) (log)
- [Execute an external \(system\), internal \(int\\_cmd\) or pcap\\_play\\_audio/pcap\\_play\\_video command](#) (exec)
- [Manipulate double precision variables using arithmetic](#)
- [Assign string values to a variable](#)
- [Compare double precision variables](#)
- [Jump to a particular scenario index](#)
- [Store the current time into variables](#)
- [Lookup a key in an indexed injection file](#)
- [Verify Authorization credentials](#)
- [Change a Call's Network Destination](#)

#### 3.6.3.1 Regular expressions

Using regular expressions in SIPp allows to

- Extract content of a SIP message or a SIP header and store it for future usage (called re-injection)
- Check that a part of a SIP message or of an header is matching an expected expression

Regular expressions used in SIPp are defined per [Posix Extended standard \(POSIX 1003.2\)](#) ( <http://www.opengroup.org/onlinepubs/007908799/xbd/re.html>) . If you want to learn how to write regular expressions, I will recommend this [regex tutorial](#) ( <http://analyser.oli.tudelft.nl/regex/index.html.en>) .

Here is the syntax of the regexp action:

Keyword	Default	Description
regexp	None	Contains the regexp to use for matching the received message or header. MANDATORY.
search_in	msg	can have four values: "msg" (try to match against the entire message); "hdr" (try to match against a specific SIP header); "body" (try to match against the SIP message body); or "var" (try to match against a SIPp string variable).
header	None	Header to try to match against. Only used when the search_in tag is set to hdr. MANDATORY IF search_in is equal to hdr.
variable	None	Variable to try to match against. Only used when the search_in tag is set to var. MANDATORY IF search_in is equal to var.
case_indep	false	To look for a header ignoring case . Only used when the search_in tag is set to hdr.
occurrence	1	To find the nth occurrence of a header. Only used when the search_in tag is set to hdr.
start_line	false	To look only at start of line. Only used when the search_in tag is set to hdr.
check_it	false	if set to true, the call is marked as failed if the regexp doesn't match. Can not be combined with check_it_inverse.
check_it_inverse	false	Inverse of check_it. iff set to true, the call is marked as failed if the regexp does match. Can not be combined with check_it.
assign_to	None	contain the variable id (integer) or a list of variable id which will be used to store the result(s) of the matching process between the regexp and the message. Those variables can be re-used at a later time either by using '\$n' in the scenario to inject the value of the variable in the messages or by using the content of the variables for <a href="#">conditional branching</a> . The first variable in the variable list of assign_to contains the entire regular expression matching. The following variables contain the sub-expressions matching. Example:  <pre>&lt;ereg regexp="o=([[:alnum:]]*) ([[:alnum:]]*) ([[:alnum:]]*)"       search_in="msg"</pre>

Keyword	Default	Description
		<pre>check_it=i"true" assign_to="3,4,5,8"/&gt;</pre> <p>If the SIP message contains the line</p> <pre>o=user1 53655765 2353687637 IN IP4 127.0.0.1</pre> <p>variable 3 contains "o=user1 53655765 2353687637", variable 4 contains "user1", variable 5 contains "53655765" and variable 8 contains "2353687637".</p>

Table 1: regexp action syntax

Note that you can have several regular expressions in one action.

The following example is used to:

- First action:
  - Extract the first IPv4 address of the received SIP message
  - Check that we could actually extract this IP address (otherwise call will be marked as failed)
  - Assign the extracted IP address to call variables 1 and 2.
- Second action:
  - Extract the Contact: header of the received SIP message
  - Assign the extracted Contact: header to variable 6.

```
<recv response="200" start_rtd="true">
  <action>
    <ereg regexp="([0-9]{1,3}\.){3}[0-9]{1,3}:[0-9]*" search_in="msg" check_it="true" assign_to="1,2" />
    <ereg regexp=".*" search_in="hdr" header="Contact:" check_it="true" assign_to="6" />
  </action>
</recv>
```

### 3.6.3.2 Log a message

The "log" action allows you to customize your traces. Messages are printed in the <scenario file name>\_<pid>\_logs.log file. Any [keyword](#) is expanded to reflect the value actually used.

#### Warning:

Logs are generated only if -trace\_logs option is set on the command line.

Example:

```
<recv request="INVITE" crlf="true" rrs="true">
  <action>
<ereg regexp=".*" search_in="hdr" header="Some-New-Header:" assign_to="1" />
    <log message="From is [last_From]. Custom header is [$1]"/>
  </action>
</recv>
```

You can use the alternative "warning" action to log a message to SIPp's error log. For example:

```
<warning message="From is [last_From]. Custom header is [$1]"/>
```

### 3.6.3.3 Execute a command

The "exec" action allows you to execute "internal", "external", "play\_pcap\_audio" or "play\_pcap\_video" commands.

#### Internal commands

**Internal** commands (specified using int\_cmd attribute) are stop\_call, stop\_gracefully (similar to pressing 'q'), stop\_now (similar to ctrl+C).

Example that stops the execution of the script on receiving a 603 response:

```
<recv response="603" optional="true">
  <action>
    <exec int_cmd="stop_now"/>
  </action>
</recv>
```

#### External commands

**External** commands (specified using command attribute) are anything that can be executed on local host with a shell.

Example that execute a system echo for every INVITE received:

```
<recv request="INVITE">
  <action>
    <exec command="echo [last_From] is the from header received >> from_list.log"/>
  </action>
</recv>
```

### 3.6.3.4 PCAP (media) commands

**PCAP play** commands (specified using `play_pcap_audio` / `play_pcap_video` attributes) allow you to send a pre-recorded RTP stream using the [pcap library](http://www.tcpdump.org/pcap3_man.html) ( [http://www.tcpdump.org/pcap3\\_man.html](http://www.tcpdump.org/pcap3_man.html) ).

Choose **play\_pcap\_audio** to send the pre-recorded RTP stream using the "m=audio" SIP/SDP line port as a base for the replay.

Choose **play\_pcap\_video** to send the pre-recorded RTP stream using the "m=video" SIP/SDP line port as a base.

The `play_pcap_audio/video` command has the following format: `play_pcap_audio="[file_to_play]"` with:

- `file_to_play`: the pre-recorded pcap file to play

#### Note:

The action is non-blocking. SIPp will start a light-weight thread to play the file and the scenario with continue immediately. If needed, you will need to add a pause to wait for the end of the pcap play.

Example that plays a pre-recorded RTP stream:

```
<nop>
  <action>
    <exec play_pcap_audio="pcap/g711a.pcap" />
  </action>
</nop>
```

### 3.6.3.5 Variable Manipulation

You may also perform simple arithmetic (add, subtract, multiply, divide) on floating point values. The "assign\_to" attribute contains the first operand, and is also the destination of the resulting value. The second operand is either an immediate value or stored in a variable, represented by the "value" and "variable" attributes, respectively.

SIPp supports call variables that take on double-precision floating values. The actions that modify double variables all write to the variable referenced by the **assign\_to** parameter. These variables can be assigned using one of three actions: `assign`, `sample`, or `todouble`. For `assign`, the double precision value is stored in the "value" parameter. The `sample` action assigns values based on statistical distributions, and uses the same parameters as a [statistically distributed pauses](#). Finally, the `todouble` command converts the variable referenced by the "variable" attribute to a double before assigning it.

For example, to assign the value 1.0 to \$1 and sample from the normal distribution into \$2:

```
<nop>
  <action>
    <assign assign_to="1" value="1" />
    <sample assign_to="2" distribution="normal" mean="0" stdev="1"/>
    <!-- Stores the first field in the injection file into string variable $3.
```



```

    You may also use regular expressions to store string variables. -->
    <assignstr assign_to="3" value="[field0]" />
    <!-- Converts the string value in $3 to a double-precision value stored in $4. -->
    <todouble assign_to="4" variable="3" />
  </action>
</nop>

```

Simple arithmetic is also possible using the **<add>**, **<subtract>**, **<multiply>**, and **<divide>** actions, which add, subtract, multiply, and divide the variable referenced by **assign\_to** by the value in **value**. For example, the following action modifies variable one as follows:

```

<nop>
  <action>
    <assign assign_to="1" value="0" /> <!-- $1 == 0 -->
    <add assign_to="1" value="2" /> <!-- $1 == 2 -->
    <subtract assign_to="1" value="3" /> <!-- $1 == -1 -->
    <multiply assign_to="1" value="4" /> <!-- $1 == -4 -->
    <divide assign_to="1" value="5" /> <!-- $1 == -0.8 -->
  </action>
</nop>

```

Rather than using fixed values, you may also retrieve the second operand from a variable, using the **<variable>** parameter. For example:

```

<nop>
  <action>
    <!-- Multiplies $1 by itself -->
    <multiply assign_to="1" variable="1" />
    <!-- Divides $1 by $2, Note that $2 must not be zero -->
    <multiply assign_to="1" variable="2" />
  </action>
</nop>

```

### 3.6.3.6 String Variables

You can create string variables by using the **<assignstr>** command, which accepts two parameters: **assign\_to** and **value**. The value may contain any of the same substitutions that a message can contain. For example:

```

<nop>
  <action>
    <!-- Assign the value in field0 of the CSV file to a $1. -->
    <assignstr assign_to="1" value="[field0]" />
  </action>
</nop>

```

A string variable and a value can be compared using the **<strcmp>** action. The result is a double value, that is less than, equal to, or greater than zero if the variable is lexicographically less than, equal to, or greater than the value. The parameters are **assign\_to**, **variable**, and **value**. For example:

```

<nop>

```

```

<action>
  <!-- Compare the value of $strvar to "Hello" and assign it to $result.. -->
<strcmp assign_to="result" variable="strvar" value="Hello" />
</action>
</nop>

```

### 3.6.3.7 Variable Testing

Variable testing allows you to construct loops and control structures using call variables. The **test** action takes four arguments: **variable** which is the variable that to **compare** against **value**, and **assign\_to** which is a boolean call variable that the result of the test is stored in. Compare may be one of the following tests: **equal**, **not\_equal**, **greater\_than**, **less\_than**, **greater\_than\_equal**, or **less\_than\_equal**.

Example that sets \$2 to true if \$1 is less than 10:

```

<nop>
  <action>
    <test assign_to="2" variable="1" compare="less_than" value="10" />
  </action>
</nop>

```

### 3.6.3.8 lookup

The lookup action is used for indexed injection files (see [indexed injection files](#)). The lookup action takes a file and key as input and produces an integer line number as output. For example the following action extracts the username from an authorization header and uses it to find the corresponding line in users.csv.

```

<recv request="REGISTER">
  <action>
    <ereg regexp="Digest .*username=\"([^\"]*)\" search_in="hdr" header="Authorization:" assign_to="junk,username" />
    <lookup assign_to="line" file="users.csv" key="[$username]" />
  </action>
</nop>

```

### 3.6.3.9 Updating In-Memory Injection files

Injection files, particularly when an [index](#) is defined can serve as an in-memory data store for your SIPp scenario. The `<insert>` and `<replace>` actions provide a method of programmatically updating SIPp's in-memory version of an injection file (there is presently no way to update the disk-based version). The insert action takes two parameters: file and value, and the replace action takes an additional line value. For example, to inserting a new line can be accomplished as follows:

```

<nop display="Insert User">
  <action>
    <insert file="usersdb.conf" value="[$user];[$calltype]" />
  </action>
</nop>

```

Replacing a line is similar, but a line number must be specified. You will probably want to use the lookup action to obtain the line number for use with replace as follows:

```
<nop display="Update User">
  <action>
    <lookup assign_to="index" file="usersdb.conf" key="[$user]" />
    <!-- Note: This assumes that the lookup always succeeds. -->
    <replace file="usersdb.conf" line="[$index]" value="[$user];[$calltype]" />
  </action>
</nop>
```

### 3.6.3.10 Jumping to an Index

You can jump to an arbitrary scenario index using the `<jump>` action. This can be used to create rudimentary subroutines. The caller can save their index using the `[msg_index]` substitution, and the callee can jump back to the same place using this action. If there is a special label named `"_unexp.main"` in the scenario, SIPp will jump to that label whenever an unexpected message is received and store the previous address in the variable named `"_unexp.retaddr"`.

Example that jumps to index 5:

```
<nop>
  <action>
    <jump value="5" />
  </action>
</nop>
```

Example that jumps to the index contained in the variable named `_unexp.retaddr`:

```
<nop>
  <action>
    <jump variable="_unexp.retaddr" />
  </action>
</nop>
```

### 3.6.3.11 gettimeofday

The `gettimeofday` action allows you to get the current time in seconds and microseconds since the epoch. For example:

```
<nop>
  <action>
    <gettimeofday assign_to="seconds,microseconds" />
  </action>
</nop>
```

### 3.6.3.12 setdest

The setdest action allows you to change the remote end point for a call. The parameters are the transport, host, and port to connect the call to. There are certain limitations based on SIPp's design: you can not change the transport for a call; and if you are using TCP then multi-socket support must be selected (i.e. `-t tn` must be specified). Also, be aware that frequently using setdest may reduce SIPp's capacity as name resolution is a blocking operation (thus potentially causing SIPp to stall while looking up host names). This example connects to the value specified in the `[next_url]` keyword.

```
<nop>
  <action>
    <assignstr assign_to="url" value="[next_url]" />
    <ereg regexp="sip:.*@([0-9A-Za-z\.\.]+):([0-9]+);transport=([A-Z]+)" search_in="var" check_it="true" assign_to="dummy,host,port,transport" variable="url" />
    <setdest host="[$host]" port="[$port]" protocol="[$transport]" />
  </action>
</nop>
```

### 3.6.3.13 verifyauth

The verifyauth action checks the Authorization header in an incoming message against a provided username and password. The result of the check is stored in a boolean variable. This allows you to simulate a server which requires authorization. Currently only simple MD5 digest authentication is supported. Before using the verifyauth action, you must send a challenge. For example:

```
<recv request="REGISTER" />
<send><![CDATA[

SIP/2.0 401 Authorization Required
[last_Via:]
[last_From:]
[last_To:];tag=[pid]SIPpTag01[call_number]
[last_Call-ID:]
[last_CSeq:]
Contact: <sip:[local_ip]:[local_port];transport=[transport]>
WWW-Authenticate: Digest realm="test.example.com", nonce="47ebe028cda119c35d4877b383027d28da013815"
Content-Length: [len]

]]>
</send>
```

After receiving the second request, you can extract the username provided and compare it against a list of user names and passwords provided as an injection file, and take the appropriate action based on the result:

```
<recv request="REGISTER" />
  <action>
    <ereg regexp="Digest .*username=\"([^\"]*)\"" search_in="hdr" header="Authorization:" assign_to="junk,username" />
    <lookup assign_to="line" file="users.conf" key="[$username]" />
    <verifyauth assign_to="authvalid" username="[field0 line=\"[$line]\"]" password="[field3 line=\"[$line]\"]" />
```

```

    </action>
</recv>

<nop hide="true" test="authvalid" next="goodauth" />
<nop hide="true" next="badauth" />

```

### 3.6.4 Variables

For complex scenarios, you will need to store bits of information that can be used across messages or even calls. Like other programming languages, SIPp's XML scenario definition allows you to use variables for this purpose. A variable in SIPp is referenced by an alphanumeric name. In past versions of SIPp, variables names were numeric only; thus in this document and the embedded scenarios, you are likely to see lots of variables of the form "1", "2", etc.; although when creating new scenarios you are encouraged to assign meaningful names to your variables.

Aside from a name, SIPp's variables are also loosely typed. The type of a variable is not explicitly declared, but is instead inferred from the action that set it. There are four types of variables: string, regular expression matches, doubles, and booleans. All mathematical operations take place on doubles. The `<test>` and `<verifyauth>` actions create boolean values. String variables and regular expression matches are similar. When a string's value is called for, a regular expression match can be substituted. The primary difference is related to the `test` attribute (see [Conditional Branching](#)). If a string has been defined, a test is evaluated to true. However, for a regular expression variable, the regular expression that set it must match for the test to be evaluated to true. Values can be converted to strings using the `<assignstr>` action. Values can be converted to doubles using the `<todouble>` action.

Variables also have a scope, which is one of global to all calls, per-user, or the default per-call. A global variable can be used, for example to store scenario configuration parameters or to keep a global counter. A user-variable when combined with the `-users` option allows you to keep per-user state across calls (e.g., if this user has already registered). Finally, the default per-call variables are useful for copying values from one SIP message to the next or controlling branching. Variables can be declared globally or per-user using the following syntax:

```

<Global variables="foo,bar" />
<User variables="baz,quux" />

```

Local variables need not be declared. To prevent programming errors, SIPp performs very rudimentary checks to ensure that each variable is used more than once in the scenario (this helps prevent some typos from turning into hard to debug errors). Unfortunately, this can cause some complication with [regular expression matching](#). The regular expression action must assign the entire matched expression to a variable. If you are only interested in checking the validity of the expression (i.e. the `check_it` attribute is set) or in capturing a sub-expression, you must still assign the entire expression to a variable. As this variable is likely only referenced once, you must inform SIPp that you are knowingly using this variable once with a Reference clause. For example:

```

<recv request="INVITE">
  <action>
    <ereg regexp="<math>\langle sip:([^\;@]*)</math>" search_in="hdr" header="To:" assign_to="dummy,uri" />
  </action>
</recv>
<Reference variables="dummy" />

```

### 3.6.5 Injecting values from an external CSV during calls

You can use "-inf file\_name" as a command line parameter to input values into the scenarios. The first line of the file should say whether the data is to be read in sequence (SEQUENTIAL), random order (RANDOM), or in a user based manner (USER). Each line corresponds to one call and has one or more ';' delimited data fields and they can be referred as [field0], [field1], ... in the xml scenario file. Example:

```
SEQUENTIAL
#This line will be ignored
Sarah;sipphone32
Bob;sipphone12
#This line too
Fred;sipphone94
```

Will be read in sequence (first call will use first line, second call second line). At any place where the keyword "[field0]" appears in the scenario file, it will be replaced by either "Sarah", "Bob" or "Fred" depending on the call. At any place where the keyword "[field1]" appears in the scenario file, it will be replaced by either "sipphone32" or "sipphone12" or "sipphone94" depending on the call. At the end of the file, SIPp will re-start from the beginning. The file is not limited in size.

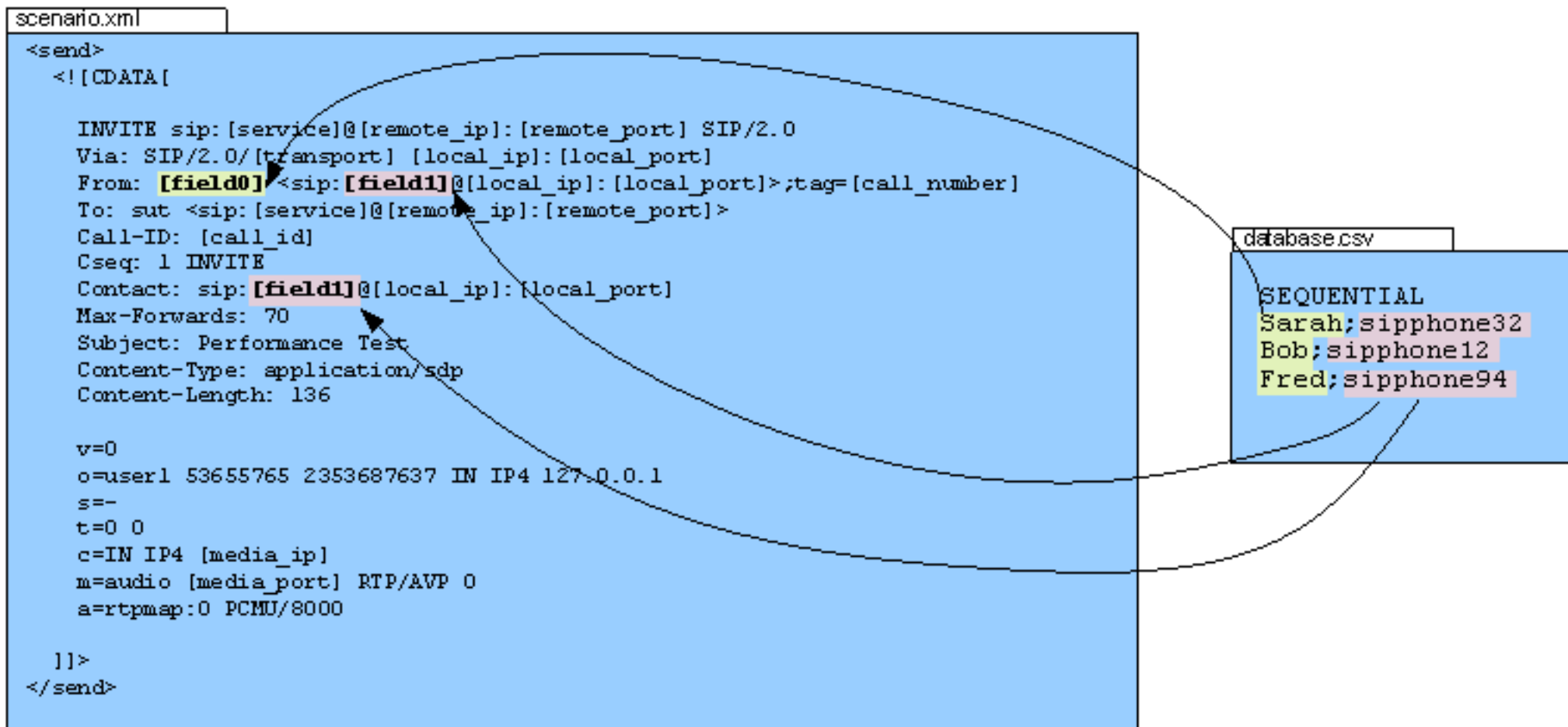
You can override the default line selection strategy with the optional line argument. For example:

```
[field0 line=1]
```

Selects the second line in the file (the first line is line zero. The line parameters support keywords in the argument, so in conjunction with a lookup action it is possible to select values based on a key.

The CSV file can contain comment lines. A comment line is a line that starts with a "#".

As a picture says more than 1000 words, here is one:



Think of the possibilities of this feature. They are huge.

It is possible to use more than one injection file, and is necessary when you want to select different types of data in different ways. For example, when running a user-based benchmark, you may have a caller.csv with "USER" as the first line and a callee.csv with "RANDOM" as the first line. To specify which CSV file is used, add the file= parameter to the keyword. For example:

```
INVITE sip:[field0 file="callee.csv"] SIP/2.0
From: sipp user <[field0 file="caller.csv"]>;tag=[pid]SIPpTag00[call_number]
To: sut user <[field0 file="callee.csv"]>
...
```

Will select the destination user from callee.csv and the sending user from caller.csv. If no file parameter is specified, then the first input file on the command line is used by default.

### 3.6.5.1 PRINTF Injection files

An extension of the standard injection file is a "PRINTF" injection file. Often, an input file will have a repetitive nature such as:

```
USERS
user000;password000
user001;password001
...
user999;password999
```

SIPp must maintain this structure in memory, which can reduce performance for very large injection files. To eliminate this problem, SIPp can automatically generate such a structured file based on one or more template lines. For example:

```
USERS,PRINTF=999
user%03d;password%03d
```

Has the same logical meaning as the original example, yet SIPp only needs to store one entry in memory. Each time a line is used; SIPp will replace %d with the requested line number (starting from zero). Standard printf format decimal specifiers can be used. When more than one template line is available, SIPp cycles through them. This example:

```
USERS,PRINTF=4
user%03d;password%03d;Foo
user%03d;password%03d;Bar
```

Is equivalent to the following injection file:

```
USERS
user000;password000;Foo
user001;password001;Bar
user002;password002;Foo
user003;password003;Bar
```

The following parameters are used to control the behavior of printf injection files:



Parameter	Description	Example
PRINTF	How many virtual lines exist in this file.	PRINTF=10, creates 10 virtual lines
PRINTFMULTIPLE	Multiple the virtual line number by this value before generating the substitutions used.	PRINTF=10,PRINTFMULTIPLE=2 creates 10 virtual lines numbered 0,2,4,...,18.
PRINTFOFFSET	Add this value to the virtual line number before generating the substitutions used (applied after PRINTFMULTIPLE).	PRINTF=10,PRINTFOFFSET=100 creates 10 virtual lines numbered 100-109. PRINTF=10,PRINTFMULTIPLE=2,PRINTFOFFSET=10 creates 10 users numbered 10,12,14,...28.

Table 1: Printf Injection File Parameters

### 3.6.5.2 Indexing Injection files

The `-inindex` option allows you to generate an index of an injection file. The arguments to `-inindex` are the injection file to index and the field number that should be indexed. For example if you have an injection file that contains user names and passwords (as the following):

```
USERS
alice,pass_A
bob,pass_B
carol,pass_C
```

You may want to extract the password for a given user in the file. To do this efficiently, SIPp must build an index for the first field (0). Thus you would pass the argument `-inindex users.csv 0` (assuming the file is named `users.csv`). SIPp will create an index that contains the logical entries `{"alice" => 0, "bob" => 1, "carol" => 2}`. To extract a particular password, you can use the lookup action to store the line number into a variable (say `$line`) and then use the keyword `[field1 line="$line"]`.

## 3.6.6 Conditional branching

### 3.6.6.1 Conditional branching in scenarios

It is possible to execute a scenario in a non-linear way. You can jump from one part of the scenario to another for example when a message is received or if a call variable is set.

You define a label (in the xml) as `<label id="n"/>` Where `n` is a number between 1 and 19 (we can easily have more if needed). The label commands go anywhere in the main scenario between other commands. To any action command (send, receive, pause, etc.) you add a `next="n"` parameter, where `n` matches the id of

a label. **When it has done the command** it continues the scenario from that label. This part is useful with optional receives like 403 messages, because it allows you to go to a different bit of script to reply to it and then rejoin at the BYE (or wherever or not).

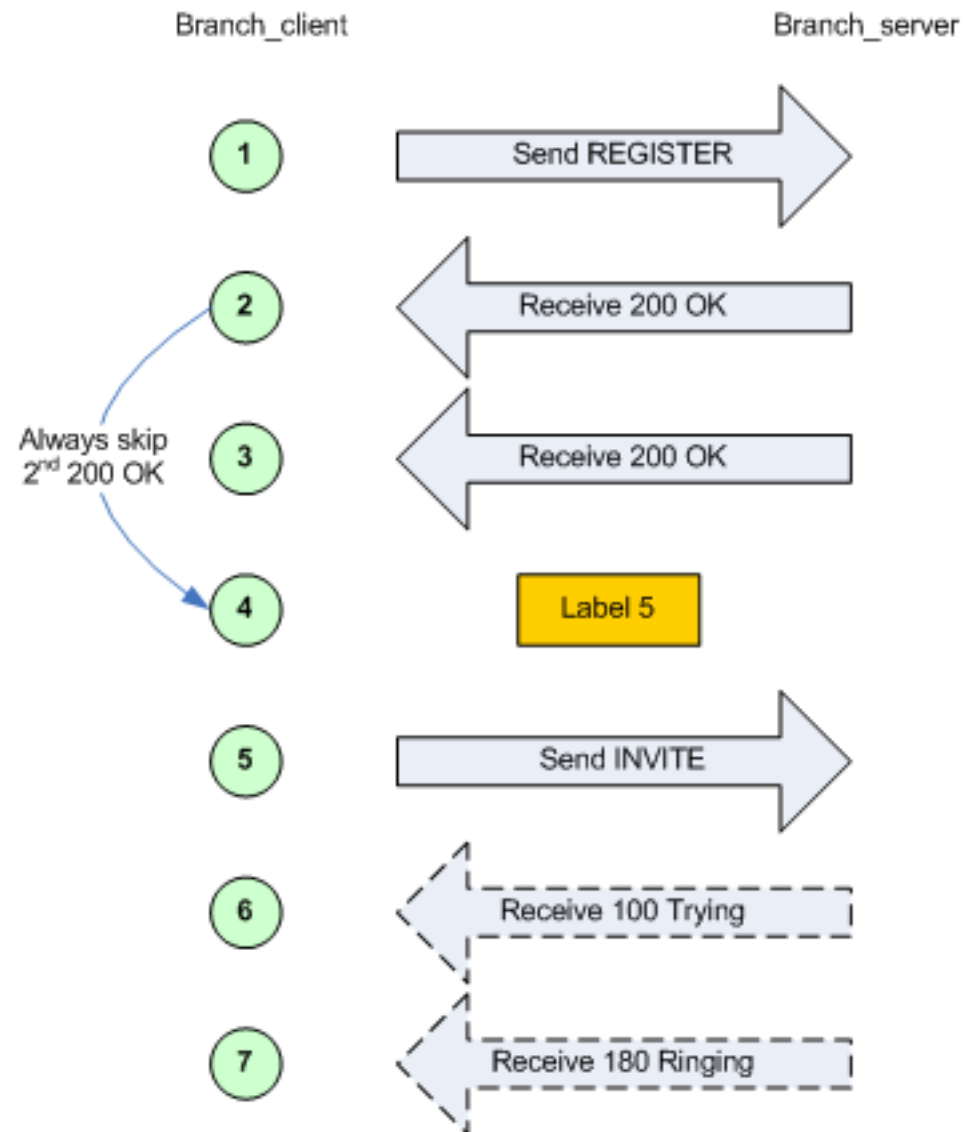
Alternatively, if you add a **test="m"** parameter to the next, it goes to the label only if variable [\$m] is set. This allows you to look for some string in a received packet and alter the flow either on that or a later part of the script. The evaluation of a test varies based on the type of call variable. For regular expressions, at least one match must have been found; for boolean variables the value must be true; and for all others a value must have been set (currently this only applies to doubles). For more complicated tests, see the [<test> action](#).

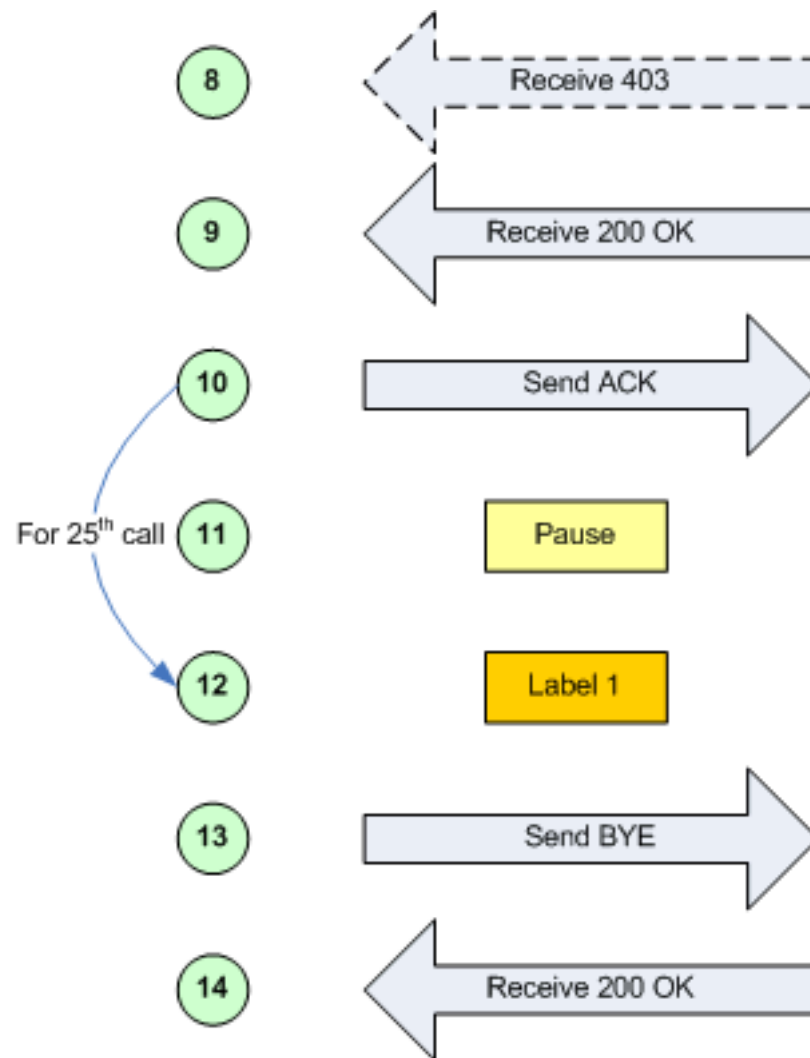
**Warning:**

If you add special cases at the end, don't forget to put a label at the real end and jump to it at the end of the normal flow.

**Example:**

The following example corresponds to the embedded ['branchc'](#) (client side) scenario. It has to run against the embedded ['branches'](#) (server side) scenario.





### 3.6.6.2 Randomness in conditional branching

To have SIPp behave somewhat more like a "normal" SIP client being used by a human, it is possible to use "statistical branching". Wherever you can have a conditional branch on a variable being set (`test="4"`), you can also branch based on a statistical decision using the attribute "chance" (e.g. `chance="0.90"`). Chance can have a value between 0 (never) and 1 (always). "test" and "chance" can be combined, i.e. only branching when the test succeeds and the chance is good.

With this, you can have a variable reaction in a given scenario (e.g.. answer the call or reject with busy), or run around in a loop (e.g. registrations) and break out of it after some random number of iterations.

### 3.6.7 SIP authentication

SIPp supports SIP authentication. Two authentication algorithm are supported: Digest/MD5 ("algorithm="MD5") and Digest/AKA ("algorithm="AKAv1-MD5", as specified by 3GPP for IMS).

#### Warning:

To enable authentication support, SIPp must be compiled in a special way. See [SIPp installation](#) for details

Enabling authentication is simple. When receiving a 401 (Unauthorized) or a 407 (Proxy Authentication Required), you must add `auth="true"` in the `<recv>` command to take the challenge into account. Then, the authorization header can be re-injected in the next message by using `[authentication]` keyword.

Computing the authorization header is done through the usage of the `"[authentication]"` keyword. Depending on the algorithm ("MD5" or "AKAv1-MD5"), different parameters must be passed next to the authentication keyword:

- Digest/MD5 (example: `[authentication username=joe password=schmo]`)
  - **username:** username: if no username is specified, the username is taken from the '-s' (service) command line parameter
  - **password:** password: if no password is specified, the password is taken from the '-ap' (authentication password) command line parameter
- Digest/AKA: (example: `[authentication username=HappyFeet aka_OP=0xCDC202D5123E20F62B6D676AC72CB318 aka_K=0x465B5CE8B199B49FAA5F0A2EE238A6BC aka_AMF=0xB9B9]`)
  - **username:** username: if no username is specified, the username is taken from the '-s' (service) command line parameter
  - **aka\_K:** Permanent secret key. If no `aka_K` is provided, the "password" attributed is used as `aka_K`.
  - **aka\_OP:** OPerator variant key
  - **aka\_AMF:** Authentication Management Field (indicates the algorithm and key in use)

In case you want to use authentication with a different username/password or `aka_K` for each call, you can do this:

- Make a CSV like this:

```
SEQUENTIAL
User0001:[authentication username=joe password=schmo]
User0002:[authentication username=john password=smith]
User0003:[authentication username=betty password=boop]
```

- And an XML like this (the `[field1]` will be substituted with the full auth string, which is the processed as a new keyword):

```
<send retrans="500">
  <![CDATA[
```

```

REGISTER sip:[remote_ip] SIP/2.0
Via: SIP/2.0/[transport] [local_ip]:[local_port]
To: <sip:[field0]@sip.com:[remote_port]>
From: <sip:[field0]@[remote_ip]:[remote_port]>
Contact: <sip:[field0]@[local_ip]:[local_port];transport=[transport]
[field1]
Expires: 300
Call-ID: [call_id]
CSeq: 2 REGISTER
Content-Length: 0

]]>
</send>

```

## Example:

```

<recv response="407" auth="true">
</recv>

<send>
  <![CDATA[

    ACK sip:[service]@[remote_ip]:[remote_port] SIP/2.0
    Via: SIP/2.0/[transport] [local_ip]:[local_port]
    From: sipp <sip:sipp@[local_ip]:[local_port]>;tag=[call_number]
    To: sut <sip:[service]@[remote_ip]:[remote_port]>[peer_tag_param]
    Call-ID: [call_id]
    CSeq: 1 ACK
    Contact: sip:sipp@[local_ip]:[local_port]
    Max-Forwards: 70
    Subject: Performance Test
    Content-Length: 0

  ]]>
</send>

<send retrans="500">
  <![CDATA[

    INVITE sip:[service]@[remote_ip]:[remote_port] SIP/2.0
    Via: SIP/2.0/[transport] [local_ip]:[local_port]
    From: sipp <sip:sipp@[local_ip]:[local_port]>;tag=[call_number]
    To: sut <sip:[service]@[remote_ip]:[remote_port]>
    Call-ID: [call_id]
    CSeq: 2 INVITE
    Contact: sip:sipp@[local_ip]:[local_port]
    [authentication username=foouser]
    Max-Forwards: 70
    Subject: Performance Test
    Content-Type: application/sdp
  ]]>
</send>

```

```

Content-Length: [len]

v=0
o=user1 53655765 2353687637 IN IP[local_ip_type] [local_ip]
s=-
t=0 0
c=IN IP[media_ip_type] [media_ip]
m=audio [media_port] RTP/AVP 0
a=rtpmap:0 PCMU/8000

]]>
</send>

```

### 3.6.8 Initialization Stanza

Some complex scenarios require setting appropriate global variables at SIPp startup. The initialization stanza allows you do do just that. To create an initialization stanza, simply surround a series of <nop> and <label> commands with <init> and </init>. These <nop>s are executed once at SIPp startup. The variables within the init stanza, except for globals, are not shared with calls. For example, this init stanza sets \$THINKTIME to 1 if it is not already set (e.g., by the -set command line parameter).

```

<init>
<!-- By Default THINKTIME is true. -->
<nop>
<action>
  <strcmp assign_to="empty" variable="THINKTIME" value="" />
  <test assign_to="empty" compare="equal" variable="empty" value="0" />
</action>
</nop>
<nop condexec="empty">
  <action>
    <assignstr assign_to="THINKTIME" value="1" />
  </action>
</nop>
</init>

```

### 3.7 Screens

Several screens are available to monitor SIP traffic. You can change the screen view by pressing 1 to 9 keys on the keyboard.

- Key '1': Scenario screen. It displays a call flow of the scenario as well as some important informations.

```

ocadmin@vista:~/sipp.2004-07-05
----- Scenario Screen ----- [1-4]: Change Screen --
Call-rate(length)  Port  Total-time  Total-calls  Remote-host
    190 cps(0 ms)  5061    50.01 s     8586  127.0.0.1:5060(UDP)

190 new calls during 1.000 s period    3 ms scheduler resolution
205 concurrent calls (limit 570)       Peak was 232 calls, after 6 s
0 out-of-call msg (discarded)
1 open sockets

Messages  Retrans  Timeout  Unexpected-Msg
INVITE ----->    8586     0        0
  100 <-----    0         0         0
  180 <-----    8586     0         0
  200 <----- B-RTD  8586     68        0
ACK ----->    8586     68
  [ 1000 ms]
BYE ----->    8381     0         0
  200 <----- E-RTD  8381     0         0

----- [+-|*|/]: Adjust rate ---- [q]: Soft exit ---- [p]: Pause traffic -----

```

- Key '2': Statistics screen. It displays the main statistics counters. The "Cumulative" column gather all statistics, since SIPp has been launched. The "Periodic" column gives the statistic value for the period considered (specified by `-f frequency` command line parameter).



```

ocadmin@vista:~/sipp.2004-07-05
----- Statistics Screen ----- [1-4]: Change Screen --
Start Time           | 2004-07-13 17:24:08
Last Reset Time     | 2004-07-13 17:26:05
Current Time        | 2004-07-13 17:26:06
-----+-----+-----
Counter Name        | Periodic value          | Cumulative value
-----+-----+-----
Elapsed Time        | 00:00:00:999           | 00:01:58:019
Call Rate           | 26.026 cps             | 24.886 cps
-----+-----+-----
Incoming call created | 0                      | 0
OutGoing call created | 26                     | 2937
Total Call created   |                        | 2937
Current Call        | 0                      |
-----+-----+-----
Successful call      | 26                     | 2937
Failed call          | 0                      | 0
-----+-----+-----
Response Time        | 00:00:00:000           | 00:00:00:000
Call Length          | 00:00:00:000           | 00:00:00:000
----- [+-|*|/]: Adjust rate ---- [q]: Soft exit ---- [p]: Pause traffic -----

```

- Key '3': Repartition screen. It displays the distribution of response time and call length, as specified in the scenario.

```

ocadmin@vista:~/sipp.2004-07-05
----- Repartition Screen ----- [1-4]: Change Screen --
Average Response Time Repartition
    0 ms <= n <    1000 ms :          0
  1000 ms <= n <   1040 ms :         385
  1040 ms <= n <   1080 ms :         388
  1080 ms <= n <   1120 ms :         384
  1120 ms <= n <   1160 ms :         382
  1160 ms <= n <   1200 ms :         382
                n >=   1200 ms :         190
Average Call Length Repartition
    0 ms <= n <    1000 ms :          0
  1000 ms <= n <   1100 ms :         946
  1100 ms <= n <   1200 ms :         975
  1200 ms <= n <   1300 ms :         190
  1300 ms <= n <   1400 ms :          0
                n >=   1400 ms :          0
----- [+-|*|/]: Adjust rate ---- [q]: Soft exit ---- [p]: Pause traffic -----

```

- Key '4': Variables screen. It displays informations on actions in scenario as well as scenario variable informations.

```

ocadmin@vista:~/sipp.2004-07-05
----- Variables Screen ----- [1-4]: Change Screen --
Action defined Per Message :
=> Message[3] (Receive Message) - [3] action(s) defined :
    --> action[0] = Type[1] - where[Full Msg] - checkIt[1] - varId[1]
    --> action[1] = Type[1] - where[Full Msg] - checkIt[1] - varId[2]
    --> action[2] = Type[1] - where[Header-Contact:] - checkIt[1] - varId[6]

Setted Variable Liste :
=> Variable[1] : setted regexp{([0-9]{1,3}\.){3}[0-9]{1,3}: [0-9]*}
=> Variable[2] : setted regexp{([0-9]{1,3}\.){3}[0-9]{1,3}: [0-9]*}
=> Variable[6] : setted regexp[.*]
----- [+-|*|/]: Adjust rate ---- [q]: Soft exit ---- [p]: Pause traffic -----

```

### 3.8 Transport modes

SIPp has several transport modes. The default transport mode is "UDP mono socket".

#### 3.8.1 UDP mono socket

In UDP mono socket mode (-t u1 command line parameter), one IP/UDP socket is opened between SIPp and the remote. All calls are placed using this socket. This mode is generally used for emulating a relation between 2 SIP servers.

### 3.8.2 UDP multi socket

In UDP multi socket mode (`-t un` command line parameter), one IP/UDP socket is opened for each new call between SIPp and the remote.

This mode is generally used for emulating user agents calling a SIP server.

### 3.8.3 UDP with one socket per IP address

In UDP with one socket per IP address mode (`-t ui` command line parameter), one IP/UDP socket is opened for each IP address given in the [inf file](#).

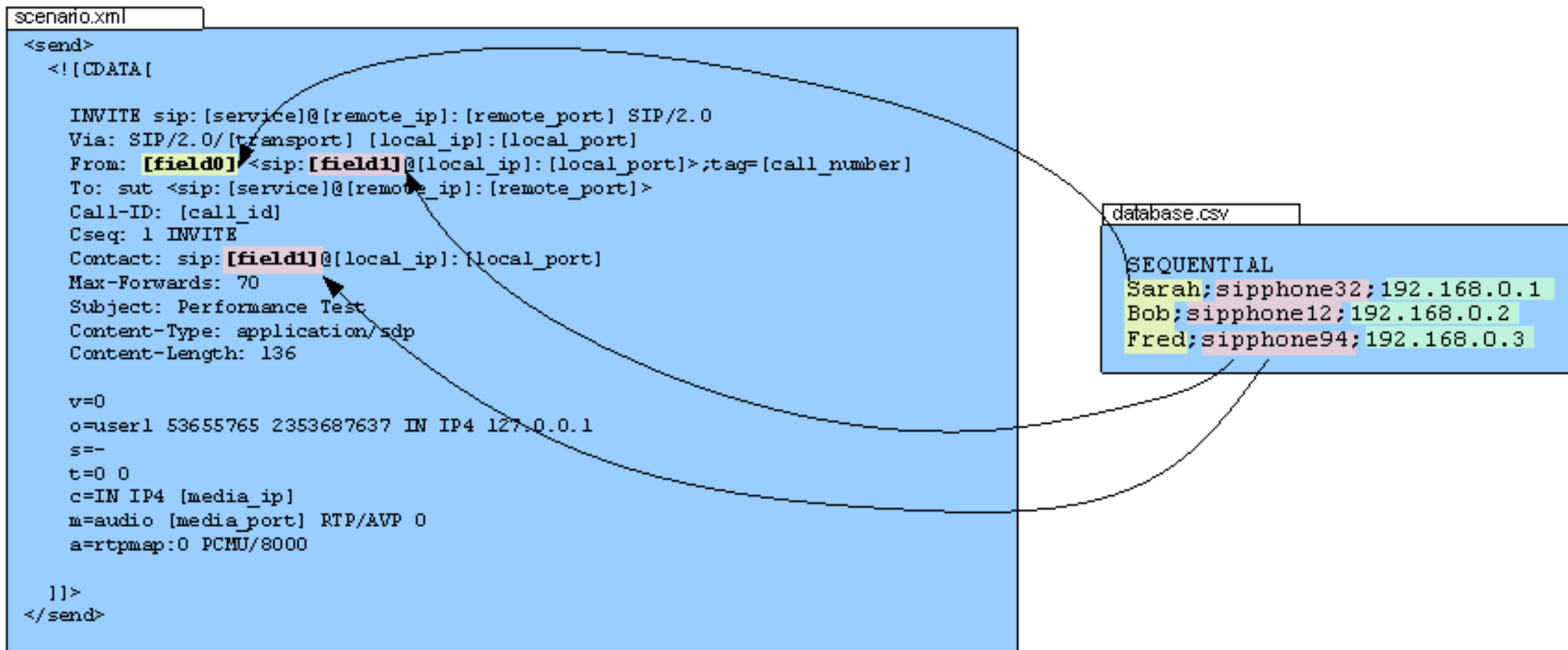
In addition to the "`-t ui`" command line parameter, one must indicate which field in the inf file is to be used as local IP address for this given call. Use "`-ip_field <nb>`" to provide the field number.

There are two distinct cases to use this feature:

- Client side: when using `-t ui` for a client, SIPp will originate each call with a different IP address, as provided in the inf file. In this case, when your IP addresses are in field X of the inject file, then you have to use `[fieldX]` instead of `[local_ip]` in your UAC XML scenario file.
- Server side: when using `-t ui` for a server, SIPp will bind itself to all the IP addresses listed in the inf file instead of using 0.0.0.0. This will have the effect SIPp will answer the request on the same IP on which it received the request. In order to have proper Contact and Via fields, a keyword `[server_ip]` can be used and provides the IP address on which a request was received. So when using this, you have to replace the `[local_ip]` in your UAS XML scenario file by `[server_ip]`.

In the following diagram, the command line for a client scenario will look like: `./sipp -sf myscenario.xml -t ui -inf database.csv -ip_field 2 192.168.1.1`

By doing so, each new call will come sequentially from IP 192.168.0.1, 192.168.0.2, 192.168.0.3, 192.168.0.1, ...



This mode is generally used for emulating user agents, using on IP address per user agent and calling a SIP server.

### 3.8.4 TCP mono socket

In TCP mono socket mode (`-t t1` command line parameter), one IP/TCP socket is opened between SIPp and the remote. All calls are placed using this socket.

This mode is generally used for emulating a relation between 2 SIP servers.

### 3.8.5 TCP multi socket

In TCP multi socket mode (`-t tn` command line parameter), one IP/TCP socket is opened for each new call between SIPp and the remote.

This mode is generally used for emulating user agents calling a SIP server.

### 3.8.6 TCP reconnections

SIPp handles TCP reconnections. In case the TCP socket is lost, SIPp will try to reconnect. The following parameters on the command line control this behaviour:

- **-max\_reconnect**: Set the maximum number of reconnection attempts.
- **-reconnect\_close true/false**: Should calls be closed on reconnect?
- **-reconnect\_sleep int**: How long to sleep (in milliseconds) between the close and reconnect?

### 3.8.7 TLS mono socket

In TLS mono socket mode (`-t 11` command line parameter), one secured TLS (Transport Layer Security) socket is opened between SIPp and the remote. All calls are placed using this socket.

This mode is generally used for emulating a relation between 2 SIP servers.

#### Warning:

When using TLS transport, SIPp will expect to have two files in the current directory: a certificate (`cacert.pem`) and a key (`cakey.pem`). If one is protected with a password, SIPp will ask for it.

SIPp supports X509's CRL (Certificate Revocation List). The CRL is read and used if `-tls_crl` command line specifies a CRL file to read.

### 3.8.8 TLS multi socket

In TLS multi socket mode (`-t 1n` command line parameter), one secured TLS (Transport Layer Security) socket is opened for each new call between SIPp and the remote.

This mode is generally used for emulating user agents calling a SIP server.

### 3.8.9 IPv6 support

SIPp includes IPv6 support. To use IPv6, just specify the local IP address (`-i` command line parameter) to be an IPv6 IP address.

The following example launches a UAS server listening on port 5063 and a UAC client sending IPv6 traffic to that port.

```
./sipp -sn uas -i [fe80::204:75ff:fe4d:19d9] -p 5063
./sipp -sn uac -i [fe80::204:75ff:fe4d:19d9] [fe80::204:75ff:fe4d:19d9]:5063
```

**Warning:**

The Pcap play feature may currently not work on IPv6.

### 3.8.10 Multi-socket limit

When using one of the "multi-socket" transports, the maximum number of sockets that can be opened (which corresponds to the number of simultaneous calls) will be determined by the system (see [how to increase file descriptors section](#) to modify those limits). You can also limit the number of socket used by using the `-max_socket` command line option. Once the maximum number of opened sockets is reached, the traffic will be distributed over the sockets already opened.

## 3.9 Handling media with SIPp

SIPp is originally a signalling plane traffic generator. There is a limited support of media plane (RTP).

### 3.9.1 RTP echo

The "RTP echo" feature allows SIPp to listen to one or two local IP address and port (specified using `-mi` and `-mp` command line parameters) for RTP media. Everything that is received on this address/port is echoed back to the sender.

RTP/UDP packets coming on this port + 2 are also echoed to their sender (used for sound and video echo).

### 3.9.2 PCAP Play

The PCAP play feature makes use of the [PCAP library](http://www.tcpdump.org/pcap3_man.html) ( [http://www.tcpdump.org/pcap3\\_man.html](http://www.tcpdump.org/pcap3_man.html)) to replay pre-recorded RTP streams towards a destination. RTP streams can be recorded by tools like [Wireshark](http://www.wireshark.org/) ( <http://www.wireshark.org/>) (formerly known as Ethereal) or [tcpdump](http://www.tcpdump.org/) ( <http://www.tcpdump.org/>) . This allows you to:

- Play any RTP stream (voice, video, voice+video, out of band DTMFs/RFC 2833, T38 fax, ...)
- Use any codec as the codec is not handled by SIPp
- Emulate precisely the behavior of any SIP equipment as the pcap play will try to replay the RTP stream as it was recorded (limited to the performances of the system).
- Reproduce exactly what has been captured using an IP sniffer like [Wireshark](http://www.wireshark.org/) ( <http://www.wireshark.org/>) .

A good example is the [UAC with media](#) (uac\_pcap) embedded scenario.

SIPp comes with a G711 alaw pre-recorded pcap file and out of band (RFC 2833) DTMFs in the pcap/ directory.

**Warning:**

The PCAP play feature uses pthread\_setschedparam calls from pthread library. Depending on the system settings, you might need to be root to allow this. Please check "man 3 pthread\_setschedparam" man page for details

More details on the possible PCAP play actions can be found in the [action reference section](#).

The latest info on this feature, tips and tricks can be found on [SIPp wiki](http://sipp.sourceforge.net/wiki/index.php/Pcapplay) ( <http://sipp.sourceforge.net/wiki/index.php/Pcapplay> ) .

### 3.10 Exit codes

To ease automation of testing, upon exit (on fatal error or when the number of asked calls (-m command line option) is reached, sipp exits with one of the following exit codes:

- 0: All calls were successful
- 1: At least one call failed
- 97: exit on internal command. Calls may have been processed. Also exit on global timeout (see -timeout\_global option)
- 99: Normal exit without calls processed
- -1: Fatal error

Depending on the system that SIPp is running on, you can echo this exit code by using "echo ?" command.

### 3.11 Statistics

#### 3.11.1 Response times

Response times can be gathered and reported. Response time names can be arbitrary strings, but for backwards compatibility the value "true" is treated as if it were named "1". Each response time can be used to compute time between two SIPp commands (send, rcv or nop). You can start a timer by using the [start\\_rtd](#) attribute and stop it using the [rtd](#) attribute.

You can view the value of those timers in the SIPp interface by pressing 3, 6, 7, 8 or 9. You can also save the values in a CSV file using the -trace\_stat option (see below).

If the -trace\_rtt option is set, the response times are also dumped in the >scenario file name<\_>pid<\_rtt.csv.

Each line represents a RTD measure (triggered by a message reception with a rtd="n" attribute). The dump frequency is tuned by the -rtt\_freq parameter.



### 3.11.2 Available counters

The `-trace_stat` option dumps all statistics in the `scenario_name_pid.csv` file. The dump starts with one header line with all counters. All following lines are 'snapshots' of statistics counter given the statistics report frequency (`-fd` option). When SIPp exits, the last values of the statistics are also dumped in this file.

This file can be easily imported in any spreadsheet application, like Excel.

In counter names, (P) means 'Periodic' - since last statistic row and (C) means 'Cumulated' - since sipp was started.

Available statistics are:

- `StartTime`: Date and time when the test has started.
- `LastResetTime`: Date and time when periodic counters were last reseted.
- `CurrentTime`: Date and time of the statistic row.
- `ElapsedTime`: Elapsed time.
- `CallRate`: Call rate (calls per seconds).
- `IncomingCall`: Number of incoming calls.
- `OutgoingCall`: Number of outgoing calls.
- `TotalCallCreated`: Number of calls created.
- `CurrentCall`: Number of calls currently ongoing.
- `SuccessfulCall`: Number of successful calls.
- `FailedCall`: Number of failed calls (all reasons).
- `FailedCannotSendMessage`: Number of failed calls because Sipp cannot send the message (transport issue).
- `FailedMaxUDPRetrans`: Number of failed calls because the maximum number of UDP retransmission attempts has been reached.
- `FailedUnexpectedMessage`: Number of failed calls because the SIP message received is not expected in the scenario.
- `FailedCallRejected`: Number of failed calls because of Sipp internal error. (a scenario sync command is not recognized or a scenario action failed or a scenario variable assignment failed).
- `FailedCmdNotSent`: Number of failed calls because of inter-Sipp communication error (a scenario sync command failed to be sent).
- `FailedRegexDoesntMatch`: Number of failed calls because of regexp that doesn't match (there might be several regexp that don't match during the call but the counter is increased only by one).
- `FailedRegexShouldntMatch`: Number of failed calls because of regexp that shouldn't match (there might be several regexp that shouldn't match during the call but the counter is increased only by one).
- `FailedRegexHdrNotFound`: Number of failed calls because of regexp with `hdr` option but no matching header found.
- `FailedOutboundCongestion`: Number of failed outgoing calls because of TCP congestion.
- `FailedTimeoutOnRecv`: Number of failed calls because of a `recv` timeout statement.
- `FailedTimeoutOnSend`: Number of failed calls because of a `send` timeout statement.
- `OutOfCallMsgs`: Number of SIP messages received that cannot be associated with an existing call.

- Retransmissions: Number of SIP messages being retransmitted.
- AutoAnswered: Number of unexpected specific messages received for new Call-ID. The message has been automatically answered by a 200 OK Currently, implemented for 'PING' message only.

The counters defined in the scenario are also dumped in the stat file. Counters that have a numeric name are identified by the GenericCounter columns.

In addition, two other statistics are gathered:

- ResponseTime (see previous section)
- CallLength: this is the time of the duration of an entire call.

Both ResponseTime and CallLength statistics can be tuned using [ResponseTimeRepartition](#) and [CallLengthRepartition](#) commands in the scenario.

The standard deviation (STDev) is also available in the log stat file for these two statistics.


### 3.11.3 Detailed Message Counts

The SIPp screens provide detailed information about the number of messages sent or received, retransmissions, messages lost, and the number of unexpected messages for each scenario element. Although these screens can be parsed, it is much simpler to parse a CSV file. To produce a CSV file that contains the per-message information contained in the main display screen pass the `-trace_counts` option. Each column of the file represents a message and a particular count of interest (e.g., "1\_INVITE\_Sent" or "2\_100\_Unexp"). Each row corresponds to those statistics at a given statistics reporting interval.

### 3.11.4 Importing statistics in spreadsheet applications

#### 3.11.4.1 Example: importation in Microsoft Excel

Here is a video (Windows Media Player 9 codec or above required) on how to import CSV statistic files in Excel and create a graph of failed calls over time.

 [sipp-02.wmv](#) ( images/sipp-02.wmv)

## 3.12 Error handling

SIPp has advanced feature to handle errors and unexpected events. They are detailed in the following sections.

### 3.12.1 Unexpected messages

- When a SIP message that **can** be correlated to an existing call (with the `Call-ID:` header) but is not expected in the scenario is received, SIPp will send a CANCEL message if no 200 OK message has been received or a BYE message if a 200 OK message has been received. The call will be marked as failed. If the unexpected message is a 4XX or 5XX, SIPp will send an ACK to this message, close the call and mark the call as failed.

- When a SIP message that **can't** be correlated to an existing call (with the `Call-ID:` header) is received, SIPp will send a BYE message. The call will not be counted at all.
- When a SIP "PING" message is received, SIPp will send an ACK message in response. This message is not counted as being an unexpected message. But it is counted in the "AutoAnswered" [statistic counter](#).
- An unexpected message that is not a SIP message will be simply dropped.

### 3.12.2 Retransmissions (UDP only)

A retransmission mechanism exists in UDP transport mode. To activate the retransmission mechanism, the "send" command must include the "retrans" attribute. When it is activated and a SIP message is sent and no ACK or response is received in answer to this message, the message is re-sent.

#### Note:

The retransmission mechanism follows RFC 3261, section 17.1.1.2. Retransmissions are differentiated between INVITE and non-INVITE methods.

`<send retrans="500">`: will initiate the T1 timer to 500 milliseconds.

Even if retrans is specified in your scenarios, you can override this by using the `-nr` command line option to globally disable the retransmission mechanism.

### 3.12.3 Log files

There are several ways to trace what is going on during your SIPp runs.

- You can log sent and received SIP messages in `<name_of_the_scenario>_<pid>_messages.log` by using the command line parameter `-trace_msg`. The messages are time-stamped so that you can track them back.
- You also can trace it using the `-trace_shortmsg` parameter. This logs the most important values of a message as CSV into one line of the `<scenario file name>_<pid>_shortmessages.log`
- You can trace all unexpected messages or events in `<name_of_the_scenario>_<pid>_errors.log` by using the command line parameter `-trace_err`.
- You can trace the counts from the main scenario screen in `<name_of_the_scenario>_<pid>_counts.csv` by using the command line parameter `-trace_counts`.
- You can trace the messages and state transitions of failed calls in `<name_of_the_scenario>_<pid>_calldebug.log` using the `-trace_calldebug` command line parameter. This is useful, because it has less overhead than `-trace_msg` yet allows you to debug call flows that were not completed successfully.
- You can save in a file the statistics screens, as displayed in the interface. This is especially useful when running SIPp in background mode.

This can be done in different ways:

- When SIPp exits to get a final status report (`-trace_screen` option)
- On demand by using USR2 signal (example: `kill -SIGUSR2 738`)
- By pressing 's' key (if `-trace_screen` option is set)

- If the `-trace_logs` option is set, you can use the `<log>` action to print some scenario traces in the `<scenario file name>_<pid>_logs.log` file. See the [Log action section](#)

SIPp can treat the messages, short messages, logs, and error logs as ring buffers. This allows you to limit the total amount of space used by these log files and keep only the most recent messages. To set the maximum file size use the `-ringbuffer_size` option. Once the file exceeds this size (the file size can be exceeded up to the size of a single log message), it is rotated. SIPp can keep several of the most recent files, to specify the number of files to keep use the `-ringbuffer_files` option. The rotated files have a name of the form `<name_of_the_scenario>_<pid>_<logname>_<date>.log`, where `<date>` is the number of seconds since the epoch. If more than one log file is rotated during a one second period, then the date is expressed as `<seconds.serial>`, where `serial` is an increasing integer identifier.

### 3.13 Online help (-h)

The online help, available through the `-h` option is duplicated here for your convenience

Usage:

```
sipp remote_host[:remote_port] [options]
```

Available options:

```
-v           : Display version and copyright information.

-aa         : Enable automatic 200 OK answer for INFO, UPDATE and
             NOTIFY messages.

-auth_uri   : Force the value of the URI for authentication.
             By default, the URI is composed of
             remote_ip:remote_port.

-base_cseq  : Start value of [cseq] for each call.

-bg         : Launch SIPp in background mode.

-bind_local : Bind socket to local IP address, i.e. the local IP
             address is used as the source IP address. If SIPp runs
             in server mode it will only listen on the local IP
             address instead of all IP addresses.

-buff_size  : Set the send and receive buffer size.

-calldebug_file : Set the name of the call debug file.

-calldebug_overwrite: Overwrite the call debug file (default true).

-cid_str    : Call ID string (default %u-%p@%s). %u=call_number,
             %s=ip_address, %p=process_number, %%=% (in any order).
```

```
-ci          : Set the local control IP address

-cp          : Set the local control port number. Default is 8888.

-d          : Controls the length of calls. More precisely, this
             : controls the duration of 'pause' instructions in the
             : scenario, if they do not have a 'milliseconds' section.
             : Default value is 0 and default unit is milliseconds.

-deadcall_wait : How long the Call-ID and final status of calls should be
             : kept to improve message and error logs (default unit is
             : ms).

-default_behaviors: Set the default behaviors that SIPp will use. Possible
             : values are:
             : - all Use all default behaviors
             : - none Use no default behaviors
             : - bye Send bytes for aborted calls
             : - abortunexp Abort calls on unexpected messages
             : - pingreply Reply to ping requests
             : If a behavior is prefaced with a -, then it is turned
             : off. Example: all,-bye

-error_file   : Set the name of the error log file.

-error_overwrite : Overwrite the error log file (default true).

-f           : Set the statistics report frequency on screen. Default is
             : 1 and default unit is seconds.

-fd          : Set the statistics dump log report frequency. Default is
             : 60 and default unit is seconds.

-i           : Set the local IP address for 'Contact:', 'Via:', and
             : 'From:' headers. Default is primary host IP address.

-inf         : Inject values from an external CSV file during calls into
             : the scenarios.
             : First line of this file say whether the data is to be
             : read in sequence (SEQUENTIAL), random (RANDOM), or user
             : (USER) order.
             : Each line corresponds to one call and has one or more
             : ';' delimited data fields. Those fields can be referred
             : as [field0], [field1], ... in the xml scenario file.
             : Several CSV files can be used simultaneously (syntax:
             : -inf f1.csv -inf f2.csv ...)

-infindex    : file field
             : Create an index of file using field. For example -inf
```

```

users.csv -inindex users.csv 0 creates an index on the
first key.

-ip_field      : Set which field from the injection file contains the IP
                address from which the client will send its messages.
                If this option is omitted and the '-t ui' option is
                present, then field 0 is assumed.
                Use this option together with '-t ui'

-l            : Set the maximum number of simultaneous calls. Once this
                limit is reached, traffic is decreased until the number
                of open calls goes down. Default:
                (3 * call_duration (s) * rate).

-log_file     : Set the name of the log actions log file.

-log_overwrite : Overwrite the log actions log file (default true).

-lost        : Set the number of packets to lose by default (scenario
                specifications override this value).

-rtcheck     : Select the retransmission detection method: full
                (default) or loose.

-m           : Stop the test and exit when 'calls' calls are processed

-mi          : Set the local media IP address (default: local primary
                host IP address)

-master      : 3pcc extended mode: indicates the master number

-max_recv_loops : Set the maximum number of messages received read per
                cycle. Increase this value for high traffic level. The
                default value is 1000.

-max_sched_loops : Set the maximum number of calls run per event loop.
                Increase this value for high traffic level. The default
                value is 1000.

-max_reconnect : Set the the maximum number of reconnection.

-max_retrans  : Maximum number of UDP retransmissions before call ends on
                timeout. Default is 5 for INVITE transactions and 7 for
                others.

-max_invite_retrans: Maximum number of UDP retransmissions for invite
                transactions before call ends on timeout.

-max_non_invite_retrans: Maximum number of UDP retransmissions for non-invite
                transactions before call ends on timeout.

```

```
-max_log_size : What is the limit for error and message log file sizes.

-max_socket : Set the max number of sockets to open simultaneously.
             This option is significant if you use one socket per
             call. Once this limit is reached, traffic is distributed
             over the sockets already opened. Default value is 50000

-mb : Set the RTP echo buffer size (default: 2048).

-message_file : Set the name of the message log file.

-message_overwrite: Overwrite the message log file (default true).

-mp : Set the local RTP echo port number. Default is 6000.

-nd : No Default. Disable all default behavior of SIPp which
     are the following:
     - On UDP retransmission timeout, abort the call by
       sending a BYE or a CANCEL
     - On receive timeout with no ontimeout attribute, abort
       the call by sending a BYE or a CANCEL
     - On unexpected BYE send a 200 OK and close the call
     - On unexpected CANCEL send a 200 OK and close the call
     - On unexpected PING send a 200 OK and continue the call
     - On any other unexpected message, abort the call by
       sending a BYE or a CANCEL

-nr : Disable retransmission in UDP mode.

-nostdin : Disable stdin.

-p : Set the local port number. Default is a random free port
    chosen by the system.

-pause_msg_ign : Ignore the messages received during a pause defined in
                the scenario

-periodic_rtd : Reset response time partition counters each logging
               interval.

-r : Set the call rate (in calls per seconds). This value can
     bechanged during test by pressing '+','_','*' or '/'.
     Default is 10.
     pressing '+' key to increase call rate by 1 *
     rate_scale,
     pressing '-' key to decrease call rate by 1 *
     rate_scale,
     pressing '*' key to increase call rate by 10 *
     rate_scale,
```

pressing '/' key to decrease call rate by 10 \*  
rate\_scale.

If the -rp option is used, the call rate is calculated  
with the period in ms given by the user.

- rp : Specify the rate period for the call rate. Default is 1 second and default unit is milliseconds. This allows you to have n calls every m milliseconds (by using -r n -rp m).  
Example: -r 7 -rp 2000 ==> 7 calls every 2 seconds.  
-r 10 -rp 5s => 10 calls every 5 seconds.
- rate\_scale : Control the units for the '+', '-', '\*', and '/' keys.
- rate\_increase : Specify the rate increase every -fd units (default is seconds). This allows you to increase the load for each independent logging period.  
Example: -rate\_increase 10 -fd 10s  
==> increase calls by 10 every 10 seconds.
- rate\_max : If -rate\_increase is set, then quit after the rate reaches this value.  
Example: -rate\_increase 10 -rate\_max 100  
==> increase calls by 10 until 100 cps is hit.
- no\_rate\_quit : If -rate\_increase is set, do not quit after the rate reaches -rate\_max.
- recv\_timeout : Global receive timeout. Default unit is milliseconds. If the expected message is not received, the call times out and is aborted.
- send\_timeout : Global send timeout. Default unit is milliseconds. If a message is not sent (due to congestion), the call times out and is aborted.
- sleep : How long to sleep for at startup. Default unit is seconds.
- reconnect\_close : Should calls be closed on reconnect?
- reconnect\_sleep : How long (in milliseconds) to sleep between the close and reconnect?
- ringbuffer\_files : How many error/message files should be kept after rotation?
- ringbuffer\_size : How large should error/message files be before they get rotated?
- rsa : Set the remote sending address to host:port for sending



the messages.

-rtp\_echo : Enable RTP echo. RTP/UDP packets received on port defined by -mp are echoed to their sender. RTP/UDP packets coming on this port + 2 are also echoed to their sender (used for sound and video echo).

-rtt\_freq : freq is mandatory. Dump response times every freq calls in the log file defined by -trace\_rtt. Default value is 200.

-s : Set the username part of the request URI. Default is 'service'.

-sd : Dumps a default scenario (embedded in the sipp executable)

-sf : Loads an alternate xml scenario file. To learn more about XML scenario syntax, use the -sd option to dump embedded scenarios. They contain all the necessary help.

-shortmessage\_file: Set the name of the short message log file.

-shortmessage\_overwrite: Overwrite the short message log file (default true).

-oocsf : Load out-of-call scenario.

-oocsn : Load out-of-call scenario.

-skip\_rlimit : Do not perform rlimit tuning of file descriptor limits. Default: false.

-slave : 3pcc extended mode: indicates the slave number

-slave\_cfg : 3pcc extended mode: indicates the file where the master and slave addresses are stored

-sn : Use a default scenario (embedded in the sipp executable). If this option is omitted, the Standard SipStone UAC scenario is loaded. Available values in this version:

- 'uac' : Standard SipStone UAC (default).
- 'uas' : Simple UAS responder.
- 'regex' : Standard SipStone UAC - with regex and variables.
- 'branchc' : Branching and conditional branching in scenarios - client.
- 'branches' : Branching and conditional branching in scenarios - server.

Default 3pcc scenarios (see -3pcc option):

```

- '3pcc-C-A' : Controller A side (must be started after
  all other 3pcc scenarios)
- '3pcc-C-B' : Controller B side.
- '3pcc-A'   : A side.
- '3pcc-B'   : B side.

-stat_delimiter : Set the delimiter for the statistics file

-stf            : Set the file name to use to dump statistics

-t            : Set the transport mode:
  - ul: UDP with one socket (default),
  - un: UDP with one socket per call,
  - ui: UDP with one socket per IP address The IP
    addresses must be defined in the injection file.
  - tl: TCP with one socket,
  - tn: TCP with one socket per call,
  - ll: TLS with one socket,
  - ln: TLS with one socket per call,
  - cl: ul + compression (only if compression plugin
    loaded),
  - cn: un + compression (only if compression plugin
    loaded). This plugin is not provided with sipp.

-timeout       : Global timeout. Default unit is seconds. If this option
  is set, SIPp quits after nb units (-timeout 20s quits
  after 20 seconds).

-timeout_error : SIPp fails if the global timeout is reached is set
  (-timeout option required).

-timer_resol   : Set the timer resolution. Default unit is milliseconds.
  This option has an impact on timers precision. Small
  values allow more precise scheduling but impacts CPU
  usage. If the compression is on, the value is set to
  50ms. The default value is 10ms.

-sendbuffer_warn : Produce warnings instead of errors on SendBuffer
  failures.

-trace_msg     : Displays sent and received SIP messages in <scenario file
  name>_<pid>_messages.log

-trace_shortmsg : Displays sent and received SIP messages as CSV in
  <scenario file name>_<pid>_shortmessages.log

-trace_screen  : Dump statistic screens in the
  <scenario_name>_<pid>_cenaris.log file when quitting

```

```
SIPp. Useful to get a final status report in background
mode (-bg option).

-trace_err      : Trace all unexpected messages in <scenario file
                 name>_<pid>_errors.log.

-trace_calldebug : Dumps debugging information about aborted calls to
                 <scenario_name>_<pid>_calldebug.log file.

-trace_stat     : Dumps all statistics in <scenario_name>_<pid>.csv file.
                 Use the '-h stat' option for a detailed description of
                 the statistics file content.

-trace_counts   : Dumps individual message counts in a CSV file.

-trace_rtt      : Allow tracing of all response times in <scenario file
                 name>_<pid>_rtt.csv.

-trace_logs     : Allow tracing of <log> actions in <scenario file
                 name>_<pid>_logs.log.

-users         : Instead of starting calls at a fixed rate, begin 'users'
                 calls at startup, and keep the number of calls constant.

-watchdog_interval: Set gap between watchdog timer firings. Default is 400.

-watchdog_reset  : If the watchdog timer has not fired in more than this
                 time period, then reset the max triggers counters.
                 Default is 10 minutes.

-watchdog_minor_threshold: If it has been longer than this period between watchdog
                 executions count a minor trip. Default is 500.

-watchdog_major_threshold: If it has been longer than this period between watchdog
                 executions count a major trip. Default is 3000.

-watchdog_major_maxtriggers: How many times the major watchdog timer can be tripped
                 before the test is terminated. Default is 10.

-watchdog_minor_maxtriggers: How many times the minor watchdog timer can be tripped
                 before the test is terminated. Default is 120.

-ap           : Set the password for authentication challenges. Default
                 is 'password'

-tls_cert     : Set the name for TLS Certificate file. Default is
                 'cacert.pem'

-tls_key      : Set the name for TLS Private Key file. Default is
                 'cakey.pem'
```

```

-tls_crl      : Set the name for Certificate Revocation List file. If not
               specified, X509 CRL is not activated.

-3pcc        : Launch the tool in 3pcc mode ("Third Party call
               control"). The passed ip address is depending on the
               3PCC role.
               - When the first twin command is 'sendCmd' then this is
                 the address of the remote twin socket. SIPp will try to
                 connect to this address:port to send the twin command
                 (This instance must be started after all other 3PCC
                 scenarii).
                 Example: 3PCC-C-A scenario.
               - When the first twin command is 'recvCmd' then this is
                 the address of the local twin socket. SIPp will open
                 this address:port to listen for twin command.
                 Example: 3PCC-C-B scenario.

-tdmmap      : Generate and handle a table of TDM circuits.
               A circuit must be available for the call to be placed.
               Format: -tdmmap {0-3}{99}{5-8}{1-31}

-key         : keyword value
               Set the generic parameter named "keyword" to "value".

-set         : variable value
               Set the global variable parameter named "variable" to
               "value".

```

#### Signal handling:

SIPp can be controlled using posix signals. The following signals are handled:

USR1: Similar to press 'q' keyboard key. It triggers a soft exit of SIPp. No more new calls are placed and all ongoing calls are finished before SIPp exits.

Example: kill -SIGUSR1 732

USR2: Triggers a dump of all statistics screens in <scenario\_name>\_<pid>\_screens.log file. Especially useful in background mode to know what the current status is.

Example: kill -SIGUSR2 732

#### Exit code:

Upon exit (on fatal error or when the number of asked calls (-m option) is reached, sipp exits with one of the following exit code:

0: All calls were successful

1: At least one call failed

97: exit on internal command. Calls may have been processed

99: Normal exit without calls processed

-1: Fatal error

Example:

```
Run sipp with embedded server (uas) scenario:
./sipp -sn uas
On the same host, run sipp with embedded client (uac) scenario
./sipp -sn uac 127.0.0.1
```

## 4 Performance testing with SIPp

### 4.1 Advices to run performance tests with SIPp

SIPp has been originally designed for SIP performance testing. Reaching high call rates and/or high number of simultaneous SIP calls is possible with SIPp, provided that you follow some guidelines:

- Use an HP-UX, Linux or other \*ix system to reach high performances. The Windows port of SIPp (through CYGWIN) cannot handle high performances.
- Limit the traces to a minimum (usage of `-trace_msg`, `-trace_logs` should be limited to scenario debugging only)
- To reach a high number of simultaneous calls in multi-socket mode, you must increase the number of filedescriptors handled by your system. Check "[Increasing File Descriptors Limit](#)" section for more details.
- Understand [internal SIPp's scheduling mechanism](#) and use the `-timer_resol`, `-max_recv_loops` and `-up_nb` command line parameters to tune SIPp given the system it is running on.

Generally, running performance tests also implies measuring response times. You can use SIPp's timers (`start_rtd`, `rtd` in scenarios and `-trace_rtt` command line option) to measure those response times. The precision of those measures are entirely dependent on the `timer_resol` parameter (as described in "[SIPp's internal scheduling](#)" section). You might want to use another "objective" method if you want to measure those response times with a high precision (a tool like [Wireshark](#) (<http://www.wireshark.org/>) will allow you to do so).

### 4.2 SIPp's internal scheduling

SIPp has a single-threaded event-loop architecture, which allows it to handle high SIP traffic loads. SIPp's event loop tracks various tasks, most of which are the calls that are defined in your scenario. In addition to tasks that represent calls there are several special tasks: a screen update task, a statistics update task, a call opening task, and a watchdog task. SIPp's main execution loop consists of:

1. Waking up tasks that have expired timers.
2. Running up to `max_sched_loop` tasks that are in a running state (each call is executed until it is no longer runnable).
3. Handling each of the sockets in turn, reading `max_recv_loops` messages from the various sockets.

SIPp executes this loop continuously, until some condition tells it to stop (e.g., the user pressing the 'q' key or the global call limit or timeout being reached).

Several parameters can be specified on the command line to fine tune this scheduling.

- `timer_resol`: during the main loop, the management of calls (management of wait, retransmission ...) is done for all calls, every "timer\_resol" ms at best. The delay of retransmission must be higher than "timer\_resol". The default timer resolution is 1 millisecond, and that is the most precise resolution that SIPp currently supports. If you increase this parameter, SIPp's traffic will be burstier and you are likely to encounter retransmissions at high load. If you have too many calls, or each call takes too long, the timer resolution will not be respected.
- `max_rcv_loops` and `max_sched_loops`: received messages are read and treated in batch. "max\_rcv\_loops" is the maximum number of messages that can be read at one time. "max sched loops" is the maximum number of processing calls loops. These limits prevent SIPp from reading and processing new messages from sockets to the exclusion of processing existing calls, and vice versa. For heavy call rate, increase both values. Be careful, those two parameters have a large influence on the CPU occupation of SIPp.
- `watchdog_interval`, `watchdog_minor_threshold`, `watchdog_major_threshold`, `watchdog_minor_maxtriggers`, and `watchdog_major_maxtriggers`: The watchdog timer is designed to provide feedback if your call load is causing SIPp's scheduler to be overwhelmed. The watchdog task sets a timer that should fire every `watchdog_interval` milliseconds (by default 400ms). If the timer is not serviced for more than `watchdog_minor_threshold` milliseconds (by default 500s), then a "minor" trigger is recorded. If the number of minor triggers is more than `watchdog_minor_maxtriggers`; the watchdog task terminates SIPp. Similarly, if the timer is not serviced for more than `watchdog_major_threshold` milliseconds (by default 3000ms), then a major trigger is recorded; and if more than `watchdog_major_maxtriggers` are recorded SIPp is terminated. If you only see occasional messages, your test is likely acceptable, but if these events are frequent you need to consider using a more powerful machine or set of machines to run your scenario.

## 5 Useful tools aside SIPp

### 5.1 JEdit

JEdit (<http://www.jedit.org/>) is a GNU GPL text editor written in Java, and available on almost all platforms. It's extremely powerful and can be used to edit SIPp scenarios with syntax checking if you put the DTD ([sipp.dtd](http://sipp.sourceforge.net/doc/sipp.dtd) ( <http://sipp.sourceforge.net/doc/sipp.dtd> ) in the same directory as your XML scenario.

### 5.2 Wireshark/tshark

Wireshark (<http://www.wireshark.org/>) is a GNU GPL protocol analyzer. It was formerly known as Ethereal. It supports SIP/SDP/RTP.

### 5.3 SIP callflow

When tracing SIP calls, it is very useful to be able to get a call flow from an wireshark trace. The "callflow" tool allows you to do that in a graphical way: <http://callflow.sourceforge.net/>

An equivalent exist if you want to generate HTML only call flows <http://www.iptel.org/~sipsc/>

## 6 Getting support

You can likely get email-based support from the sipp users community. The mailing list address is [sipp-users@lists.sourceforge.net](mailto:sipp-users@lists.sourceforge.net) (mailto:sipp-users@lists.sourceforge.net) . To protect you from SPAM, this list is restricted (only people that actually subscribed can post). Also, you can browse the SIPp mailing list archive: <http://lists.sourceforge.net/lists/listinfo/sipp-users>

## 7 Contributing to SIPp

Of course, we welcome contributions! If you created a feature for SIPp, please send the "diff" output (`diff -bruN old_sipp_directory new_sipp_directory`) on the [SIPp mailing list](http://lists.sourceforge.net/lists/listinfo/sipp-users) ( <http://lists.sourceforge.net/lists/listinfo/sipp-users> ) , so that we can review and possibly integrate it in SIPp.