How to install sngrep on your VoipNow server

`sngrep` is a tool for displaying SIP calls message flows from the terminal of your server. It can be used to display real-time SIP traffic and to process PCAP files (packet captures). Think of it as a specialized `tcpdump` tool designed for VoIP. It's open-source and it's available here.

This knowledge base article assumes advanced knowledge of the Linux command line and familiarity with the SIP protocol.

Step-by-step guide

Here are the steps to take if you want to install `sngrep` on your VoipNow server.

Please note that all commands listed in a code block need to be executed as root.

1. If VoipNow is not installed, perform the installation using the command line installer as instructed here.
2. Install the required software packages so that you can download and compile `sngrep` by running:

```
# yum -y install git libpcap openssl-devel gnutls pcre-devel libpcap-devel ncurses-devel autoconf
automake gcc make
```

3. Download the `sngrep` files.

```
# cd ~
# git clone https://github.com/irontec/sngrep.git
Cloning into 'sngrep'...
remote: Counting objects: 4878, done.
remote: Total 4878 (delta 0), reused 0 (delta 0), pack-reused 4878
Receiving objects: 100% (4878/4878), 4.06 MiB | 1.98 MiB/s, done.
Resolving deltas: 100% (3864/3864), done.
Checking connectivity... done.
```

4. A new folder named `sngrep` containing the source code will be created. Go to that folder.

```
# cd sngrep
```

5. Run the `bootstrap.sh` script.

```
# ./bootstrap.sh
Generating the configure script ...
```

6. Run the `configure` script.

```
./configure
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /usr/bin/mkdir -p
checking for gawk... gawk
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
checking whether make supports nested variables... (cached) yes
checking for style of include used by make... GNU
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking dependency style of gcc... gcc3
checking how to run the C preprocessor... gcc -E
checking for grep that handles long lines and -e... /usr/bin/grep
checking for egrep... /usr/bin/grep -E
checking for ANSI C header files... yes
```

```
checking for sys/types.h... yes
checking for sys/stat.h... yes
checking for stdlib.h... yes
checking for string.h... yes
checking for memory.h... yes
checking for strings.h... yes
checking for inttypes.h... yes
checking for stdint.h... yes
checking for unistd.h... yes
checking minix/config.h usability... no
checking minix/config.h presence... no
checking for minix/config.h... no
checking whether it is safe to define __EXTENSIONS__... yes
checking for gcc... (cached) gcc
checking whether we are using the GNU C compiler... (cached) yes
checking whether gcc accepts -g... (cached) yes
checking for gcc option to accept ISO C89... (cached) none needed
checking dependency style of gcc... (cached) gcc3
checking for g++... no
checking for c++... no
checking for gpp... no
checking for aCC... no
checking for CC... no
checking for cxx... no
checking for cc++... no
checking for cl.exe... no
checking for FCC... no
checking for KCC... no
checking for RCC... no
checking for xlC_r... no
checking for xlC... no
checking whether we are using the GNU C++ compiler... no
checking whether g++ accepts -g... no
checking dependency style of g++... none
checking whether ln -s works... yes
checking for egrep... (cached) /usr/bin/grep -E
checking for pthread_create in -lpthread... yes
checking for pcap_open_offline in -lpcap... yes
checking pcap.h usability... yes
checking pcap.h presence... yes
checking for pcap.h... yes
checking ncurses.h usability... yes
checking ncurses.h presence... yes
checking for ncurses.h... yes
checking for initscr in -lncurses... yes
checking for new_panel in -lpanel... yes
checking for new_form in -lform... yes
checking for new_item in -lmenu... yes




configure:
configure: sngrep configure finished
configure: ========================================================
configure: GnuTLS Support               : no
configure: OpenSSL Support              : no
configure: Unicode Support              : no
configure: Perl Expressions Support     : no
configure: IPv6 Support                 : no
configure: EEP Support                  : no
configure: ========================================================
configure:
checking that generated files are newer than configure... done
configure: creating ./config.status
config.status: creating Makefile
config.status: creating src/Makefile
config.status: creating config/Makefile
config.status: creating doc/Makefile
```

```
config.status: creating tests/Makefile
config.status: creating src/config.h
config.status: executing depfiles commands
```

7. Compile `sngrep` with the `make` command.

```
# make
Making all in src
make[1]: Entering directory `/root/sngrep/src'
make  all-am
make[2]: Entering directory `/root/sngrep/src'
  CC       capture.o
  CC       address.o
  CC       packet.o
  CC       sip.o
  CC       sip_call.o
  CC       sip_msg.o
  CC       sip_attr.o
  CC       main.o
  CC       option.o
  CC       group.o
  CC       filter.o
  CC       keybinding.o
  CC       media.o
  CC       setting.o
  CC       rtp.o
  CC       util.o
  CC       vector.o
  CC       ui_panel.o
  CC       scrollbar.o
  CC       ui_manager.o
  CC       ui_call_list.o
  CC       ui_call_flow.o
  CC       ui_call_raw.o
  CC       ui_stats.o
  CC       ui_filter.o
  CC       ui_save.o
  CC       ui_msg_diff.o
  CC       ui_column_select.o
  CC       ui_settings.o
  CCLD     sngrep
make[2]: Leaving directory `/root/sngrep/src'
make[1]: Leaving directory `/root/sngrep/src'
Making all in config
make[1]: Entering directory `/root/sngrep/config'
make[1]: Nothing to be done for `all'.
make[1]: Leaving directory `/root/sngrep/config'
Making all in doc
make[1]: Entering directory `/root/sngrep/doc'
make[1]: Nothing to be done for `all'.
make[1]: Leaving directory `/root/sngrep/doc'
Making all in tests
make[1]: Entering directory `/root/sngrep/tests'
make[1]: Nothing to be done for `all'.
make[1]: Leaving directory `/root/sngrep/tests'
make[1]: Entering directory `/root/sngrep'
make[1]: Nothing to be done for `all-am'.
make[1]: Leaving directory `/root/sngrep'
```

8. Install `sngrep` with the `make install` command.

```
# make install
Making install in src
make[1]: Entering directory `/root/sngrep/src'
make[2]: Entering directory `/root/sngrep/src'
 /usr/bin/mkdir -p '/usr/local/bin'
  /usr/bin/install -c sngrep '/usr/local/bin'
make[2]: Nothing to be done for `install-data-am'.
make[2]: Leaving directory `/root/sngrep/src'
make[1]: Leaving directory `/root/sngrep/src'
Making install in config
make[1]: Entering directory `/root/sngrep/config'
make[2]: Entering directory `/root/sngrep/config'
 /usr/bin/mkdir -p '/usr/local/etc'
 /usr/bin/install -c -m 644 sngreprc '/usr/local/etc'
make[2]: Nothing to be done for `install-data-am'.
make[2]: Leaving directory `/root/sngrep/config'
make[1]: Leaving directory `/root/sngrep/config'
Making install in doc
make[1]: Entering directory `/root/sngrep/doc'
make[2]: Entering directory `/root/sngrep/doc'
make[2]: Nothing to be done for `install-exec-am'.
 /usr/bin/mkdir -p '/usr/local/share/man/man8'
 /usr/bin/install -c -m 644 sngrep.8 '/usr/local/share/man/man8'
make[2]: Leaving directory `/root/sngrep/doc'
make[1]: Leaving directory `/root/sngrep/doc'
Making install in tests
make[1]: Entering directory `/root/sngrep/tests'
make[2]: Entering directory `/root/sngrep/tests'
make[2]: Nothing to be done for `install-exec-am'.
make[2]: Nothing to be done for `install-data-am'.
make[2]: Leaving directory `/root/sngrep/tests'
make[1]: Leaving directory `/root/sngrep/tests'
make[1]: Entering directory `/root/sngrep'
make[2]: Entering directory `/root/sngrep'
make[2]: Nothing to be done for `install-exec-am'.
make[2]: Nothing to be done for `install-data-am'.
make[2]: Leaving directory `/root/sngrep'
make[1]: Leaving directory `/root/sngrep'
```

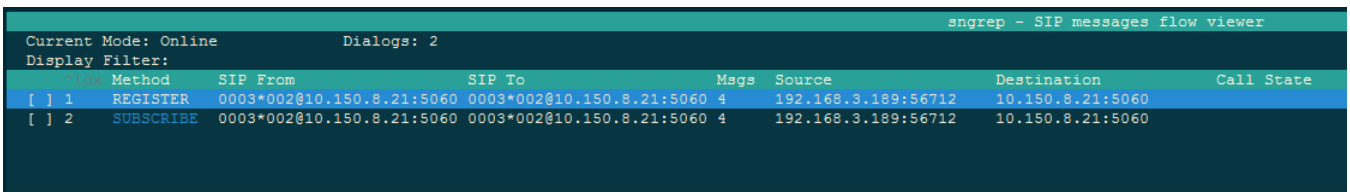
9. `sngrep` is now installed into `/usr/local/bin/sngrep` which should be already in your path. You may launch it with the `sngrep` command:

```
# sngrep
```

After starting `sngrep`, you'll be presented with a text-mode, interactive interface which can be navigated with the arrow keys and quit with the Esc key.

How to make the most of SNGREP

Initialize a softphone which registers to your VoipNow server, and the `REGISTER` and the `SUBSCRIBE` methods sent by the phone will appear in the console right away. You can clear the list of captured messages by pressing the F5 key, as indicated in the legend at the bottom of the screen.



You can move the cursor between the displayed packets using the arrow keys. For details about a specific SIP method, press ENTER. You'll get a graphical flow of the packets exchanged between your phone and the VoipNow server. You may navigate through the flow using the same arrow keys - the selected message details will be displayed on the right of the window.

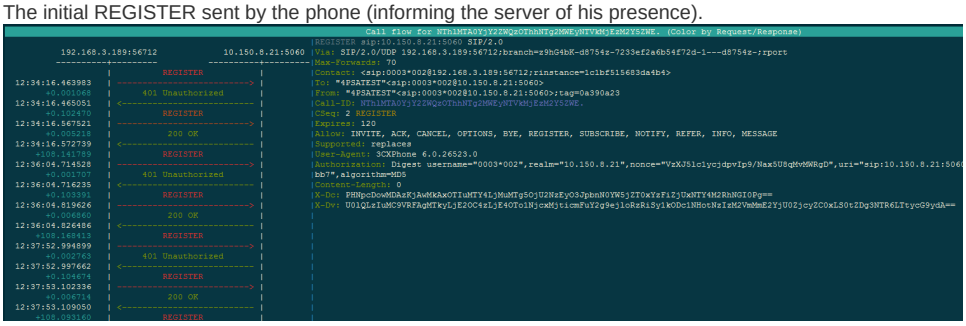
```
                                                                  Call flow for NTh1MTA0YjY2ZWQzOThhNTg2MWEyNTVkMjEzM2Y5ZWE. (Color by Request/Response)
                                                                                                |REGISTER sip:10.150.8.21:5060 SIP/2.0
         192.168.3.189:56712             10.150.8.21:5060                                       |Via: SIP/2.0/UDP 192.168.3.189:56712;branch=z9hG4bK-d8754z-b42c2d6ac977f91c-1---d8754z-;rport
        ---------+---------             ----------+---------                                    |Max-Forwards: 70
                 |          REGISTER               |                                           |Contact: <sip:0003*002@192.168.3.189:56712;rinstance=1c1bf515683da4b4>
 12:34:16.463983 | ------------------------------> |                                           |To: "4PSATEST"<sip:0003*002@10.150.8.21:5060>
       +0.001068 |      401 Unauthorized           |                                           |From: "4PSATEST"<sip:0003*002@10.150.8.21:5060>;tag=0a390a23
 12:34:16.465051 | <------------------------------ |                                           |Call-ID: NTh1MTA0YjY2ZWQzOThhNTg2MWEyNTVkMjEzM2Y5ZWE.
       +0.102470 |          REGISTER               |                                           |CSeq: 1 REGISTER
 12:34:16.567521 | ------------------------------> |                                           |Expires: 120
       +0.005218 |           200 OK                |                                           |Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REGISTER, SUBSCRIBE, NOTIFY, REFER, INFO, MESSAGE
 12:34:16.572739 | <------------------------------ |                                           |Supported: replaces
    +108.141789  |          REGISTER               |                                           |User-Agent: 3CXPhone 6.0.26523.0
 12:36:04.714528 | ------------------------------> |                                           |Content-Length: 0
       +0.001707 |      401 Unauthorized           |                                           |X-Dc: PHNpcDowMDAzKjAwMkAxOTIuMTY4LjMuMTg5OjU2NzEyO3JpbnN0YW5jZT0xYzFiZjUxNTY4M2RhNGI0Pg==
 12:36:04.716235 | <------------------------------ |                                           |X-Dv: U0lQLzIuMC9VRFAgMTkyLjE2OC4zLjE4OTo1NjcxMjticmFuY2g9ejloRzRiSy1kODc1NHotYjQyYzJkNmFjOTc3ZjkxYy0xLS0tZDg3NTR6LTtycG9ydA==
       +0.103391 |          REGISTER               |                                           |
 12:36:04.819626 | ------------------------------> |                                           |
       +0.006860 |           200 OK                |                                           |
 12:36:04.826486 | <------------------------------ |                                           |
    +108.168413  |          REGISTER               |                                           |
 12:37:52.994899 | ------------------------------> |                                           |
       +0.002763 |      401 Unauthorized           |                                           |
 12:37:52.997662 | <------------------------------ |                                           |
       +0.104674 |          REGISTER               |                                           |
 12:37:53.102336 | ------------------------------> |                                           |
       +0.006714 |           200 OK                |                                           |
 12:37:53.109050 | <------------------------------ |                                           |
    +108.093160  |          REGISTER               |                                           |
```

Pressing ENTER again will show the packet in raw mode.

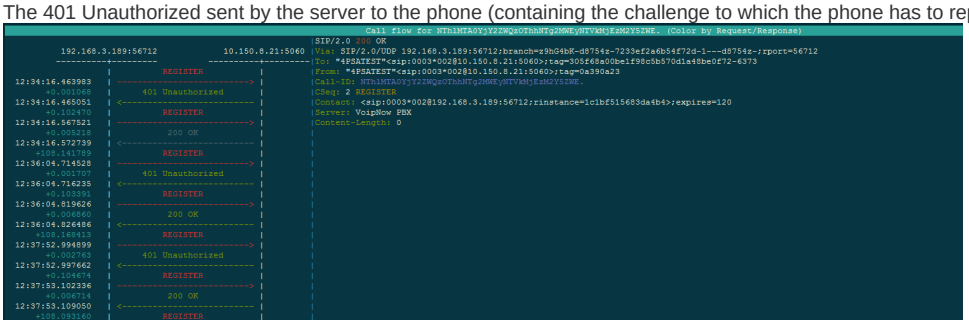
```
2016/05/13 12:34:16.463983 192.168.3.189:56712 -> 10.150.8.21:5060
REGISTER sip:10.150.8.21:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.3.189:56712;branch=z9hG4bK-d8754z-b42c2d6ac977f91c-1---d8754z-;rport
Max-Forwards: 70
Contact: <sip:0003*002@192.168.3.189:56712;rinstance=1c1bf515683da4b4>
To: "4PSATEST"<sip:0003*002@10.150.8.21:5060>
From: "4PSATEST"<sip:0003*002@10.150.8.21:5060>;tag=0a390a23
Call-ID: NTh1MTA0YjY2ZWQzOThhNTg2MWEyNTVkMjEzM2Y5ZWE.
CSeq: 1 REGISTER
Expires: 120
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REGISTER, SUBSCRIBE, NOTIFY, REFER, INFO, MESSAGE
Supported: replaces
User-Agent: 3CXPhone 6.0.26523.0
Content-Length: 0
X-Dc: PHNpcDowMDAzKjAwMkAxOTIuMTY4LjMuMTg5OjU2NzEyO3JpbnN0YW5jZT0xYzFiZjUxNTY4M2RhNGI0Pg==
X-Dv: U0lQLzIuMC9VRFAgMTkyLjE2OC4zLjE4OTo1NjcxMjticmFuY2g9ejloRzRiSy1kODc1NHotYjQyYzJkNmFjOTc3ZjkxYy0xLS0tZDg3NTR6LTtycG9ydA==
```

Here are the 4 stages of a SIP registration:

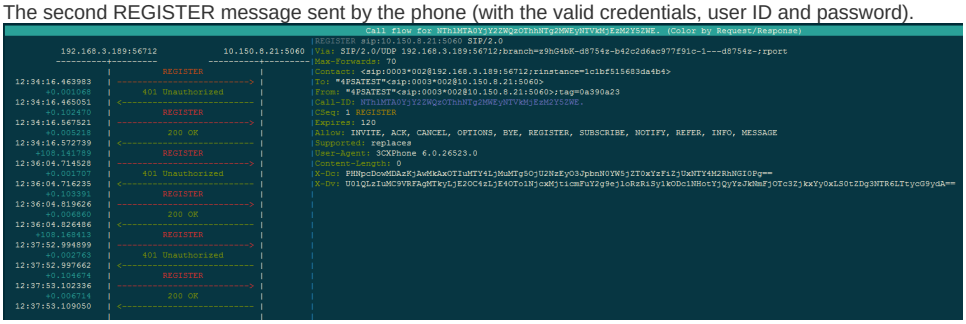
1. The initial REGISTER sent by the phone (informing the server of his presence).



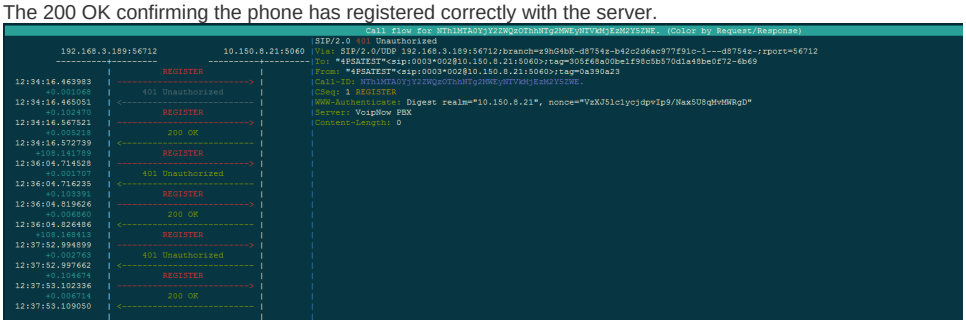
2. The 401 Unauthorized sent by the server to the phone (containing the challenge to which the phone has to reply).



3. The second REGISTER message sent by the phone (with the valid credentials, user ID and password).

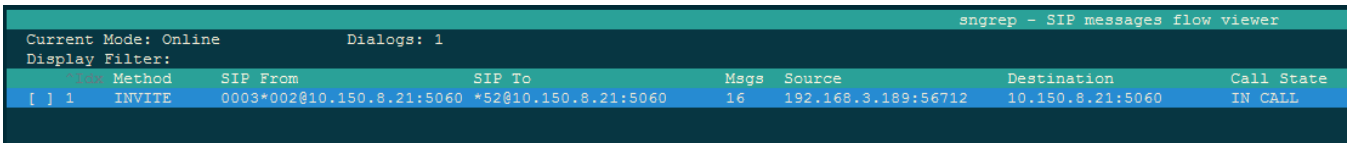


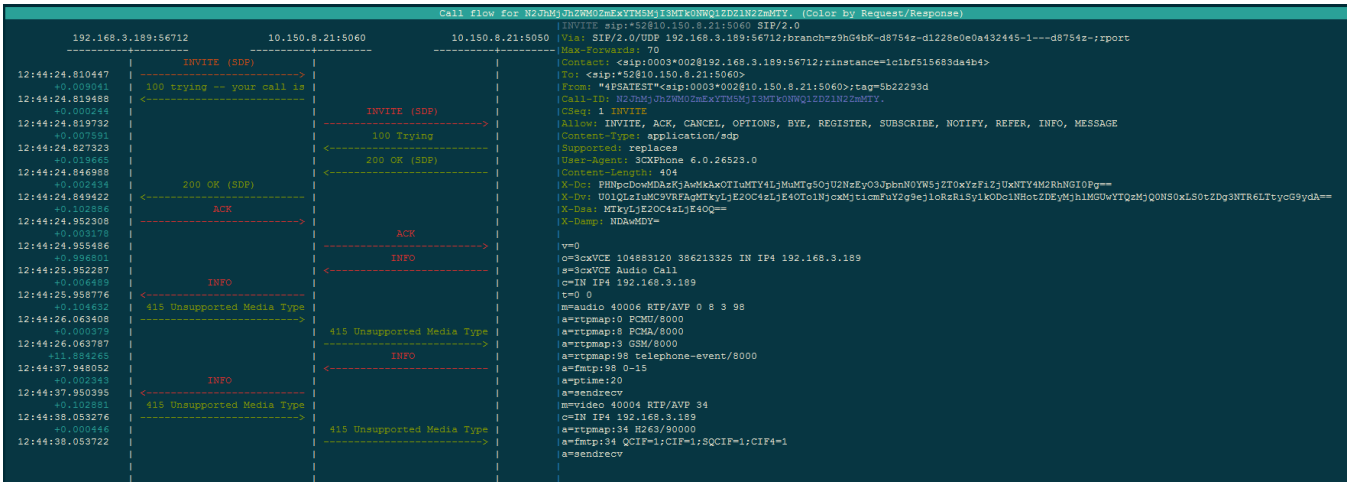
4. The 200 OK confirming the phone has registered correctly with the server.



Place a call to *52 (the echo test) and you'll see the call appear in the list.

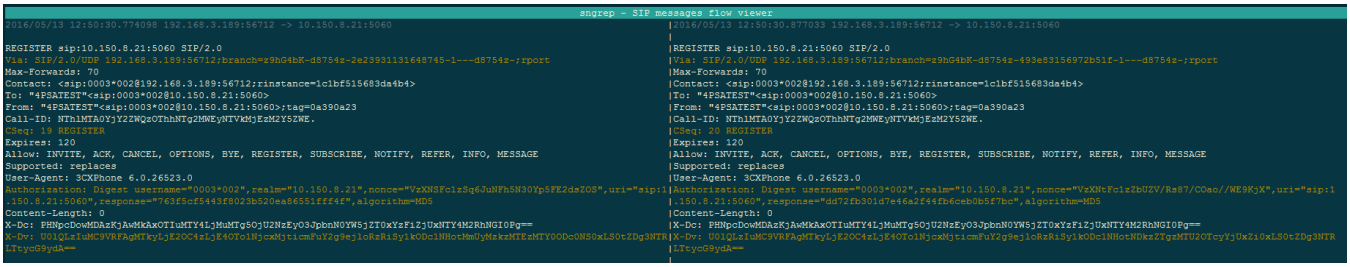
Pressing ENTER will open a call flow diagram illustrating the communication between the phone and the SIP/PBX components of VoipNow.



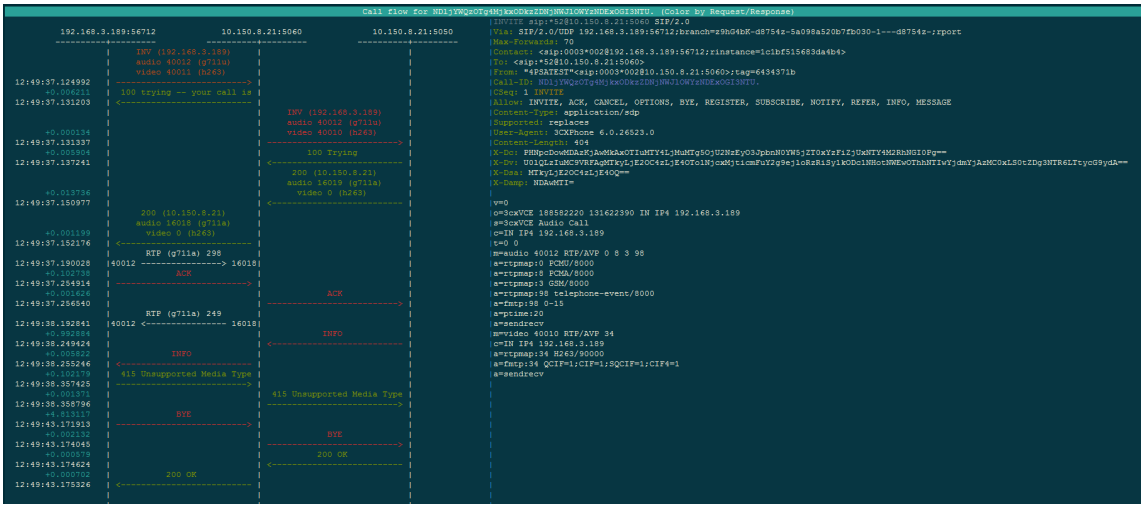


More great SNGREP features

For example, you can compare two SIP packets by checking them with the Space key. Once the second packet is checked, the differences between the two packets will be automatically shown in a separate window.



If you press F2 and F3 in a call flow, you will be able to see SDP and RTP information.



There are more options and features in sngrep, so feel free to explore further. While a bit more cumbersome to use than Wireshark, sngrep can help you quickly debug SIP problems on your server.

Related articles

- How to install sngrep on your VoipNow server
- Primary and secondary server setup for 4PSA DNS Manager
- How to interact with RabbitMQ
- How to Allow 4PSA Access to the Server
- How to do a data migration between two DNSManager servers