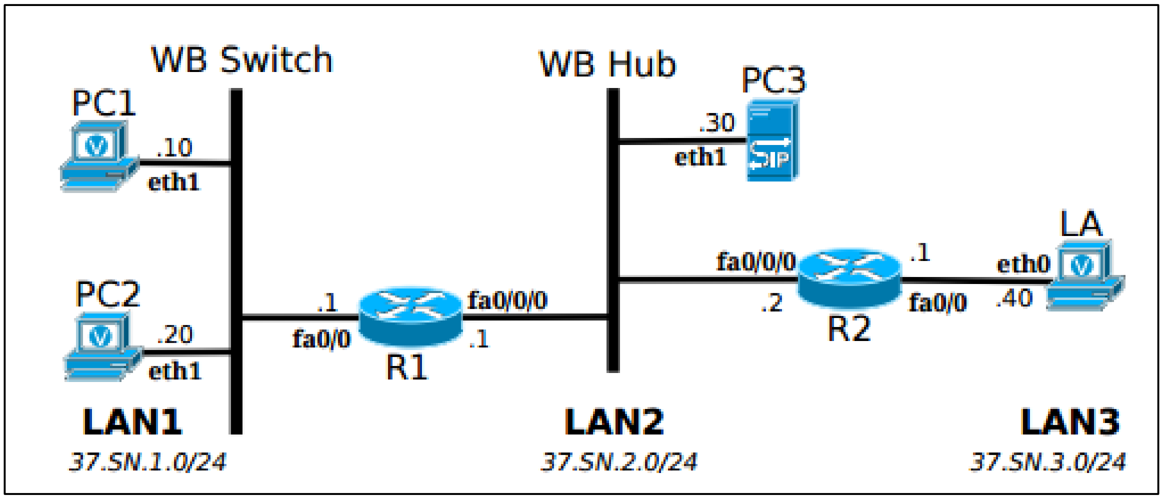
## Experiment 4: Topology

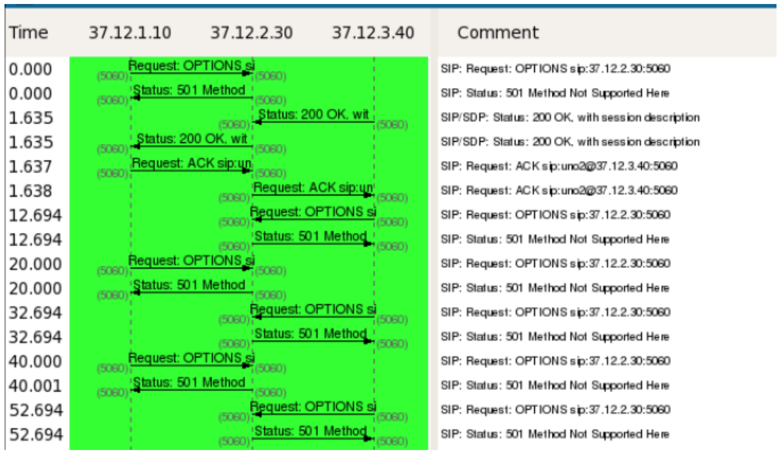



- The devices were connected as shown in the topology above.
- Interface eth0 of PC3 was connected to hub and wireshark was started to capture the traffic between the LANs.
- Static routes were added on PC3 and the routers to achieve complete connectivity and using ping the connectivity was confirmed.

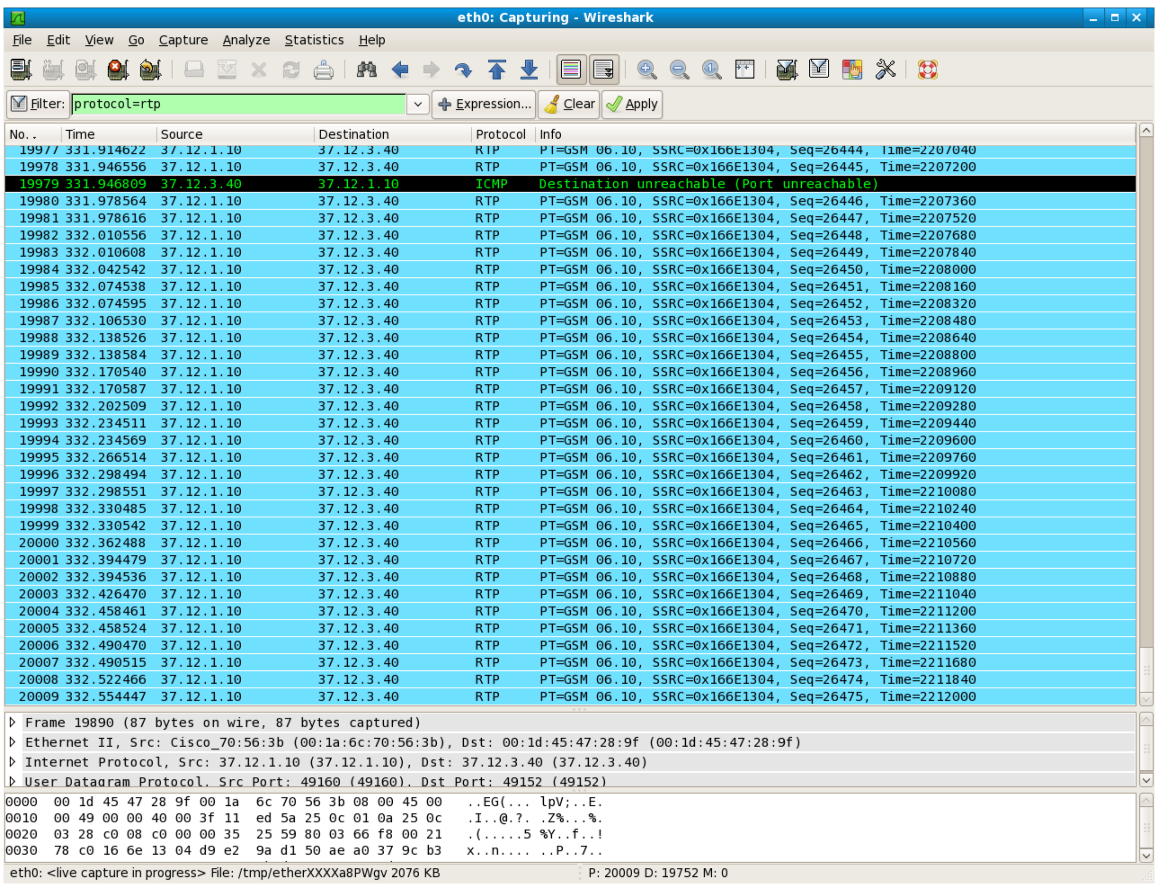
## Experiment 4.1: Direct communication between user agents

- The SJphone user agent was launched on the PC1 and laptop by executing the command sjphone.sh on the Linux command line.
- The name was set by filling the name field.
- The phone was configured to make a PC-PC call using the SIP signaling protocol.
- In the address box of the phone interface of PC1, the complete SIP address of the user to be called was entered in the form <username>@<user agent IP address>, and the call was started by clicking dial.
- We were able to hear the ringtone on the laptop.
- The call connection setup and the teardown can be seen in the wireshark capture below.

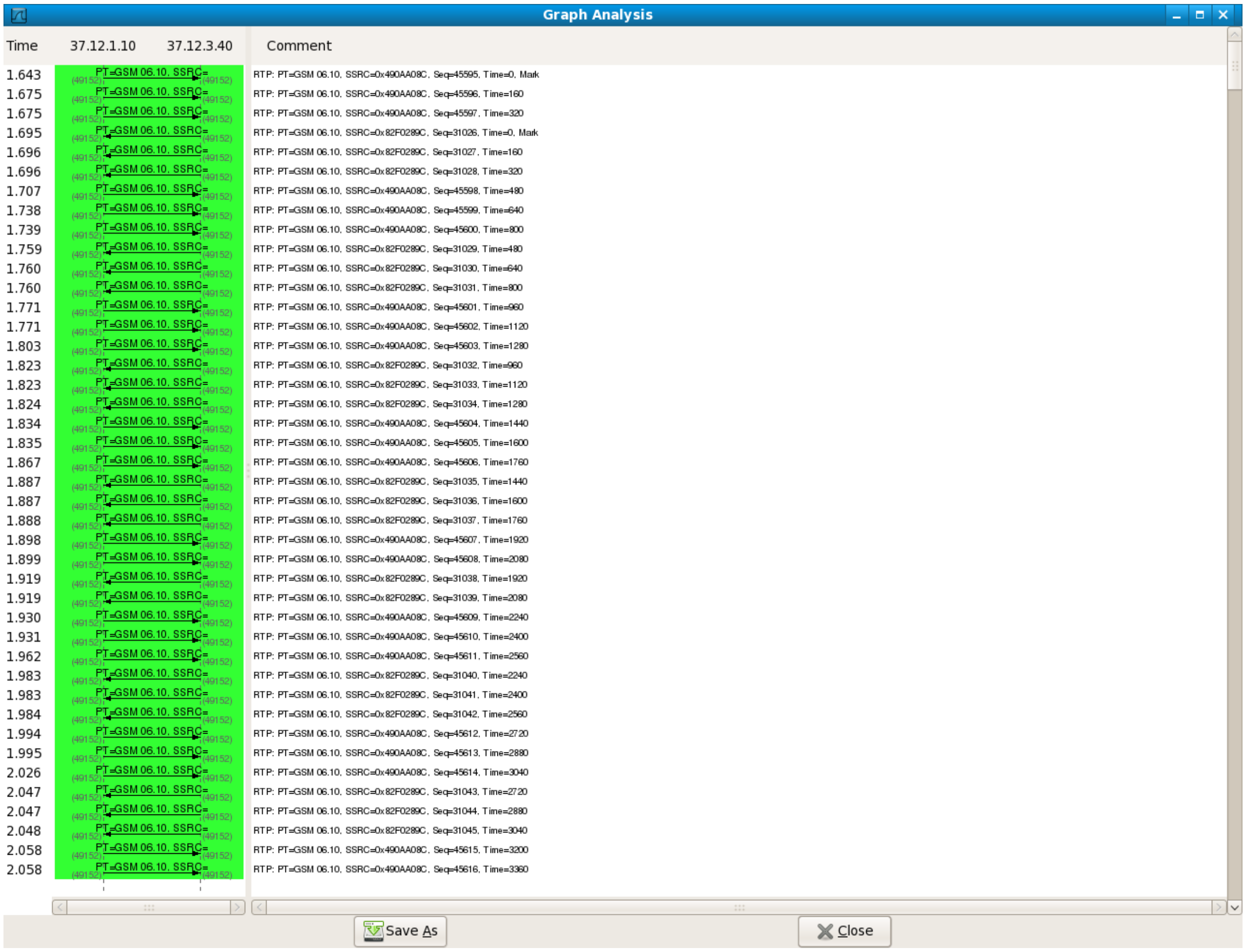
- As we can see, the PC phone @ 37.12.3.40 was called from the PC phone @ 37.12.1.10. And we see the initial call trying, and the ringing phase. Finally, once the call is completed, and the hang-up button is pressed we the BYE messages as well. The flow graph of the same transaction is also shown below.




- From the captures we can see that the port number for the signaling flow is **5060** which is the SIP protocol.
- The voice packets i.e. RTP packets are also shown below.




- The captures show us the voice transactions occurring between the 2 PC phones.
- The similar transactions are shown in the flow graph below.




- From the captures, we can see that the port on which the RTP transaction occurs is **49152**.
- All the SJPhone instances were shutdown.

**Experiment 4.2: Communication via a SIP proxy server**

- Using the following steps, the SIP Proxy server was configured.

```
sudo /etc/init.d/mysqld start
sudo openserdbctl drop
sudo openserdbctl create
cp /etc/openser/openser-nonat.cfg /etc/openser/openser.cfg
```

- The configuration file at /etc/openser/openser.cfg was opened in a text editor. At the listen directive, the part between the colons was changed to the IP address of the SIP proxy server i.e. **37.12.2.30**.
- The openser daemon was started. Ensured that it is working.
- The SIP domain was created using the following steps and SIP users were added using the steps below.

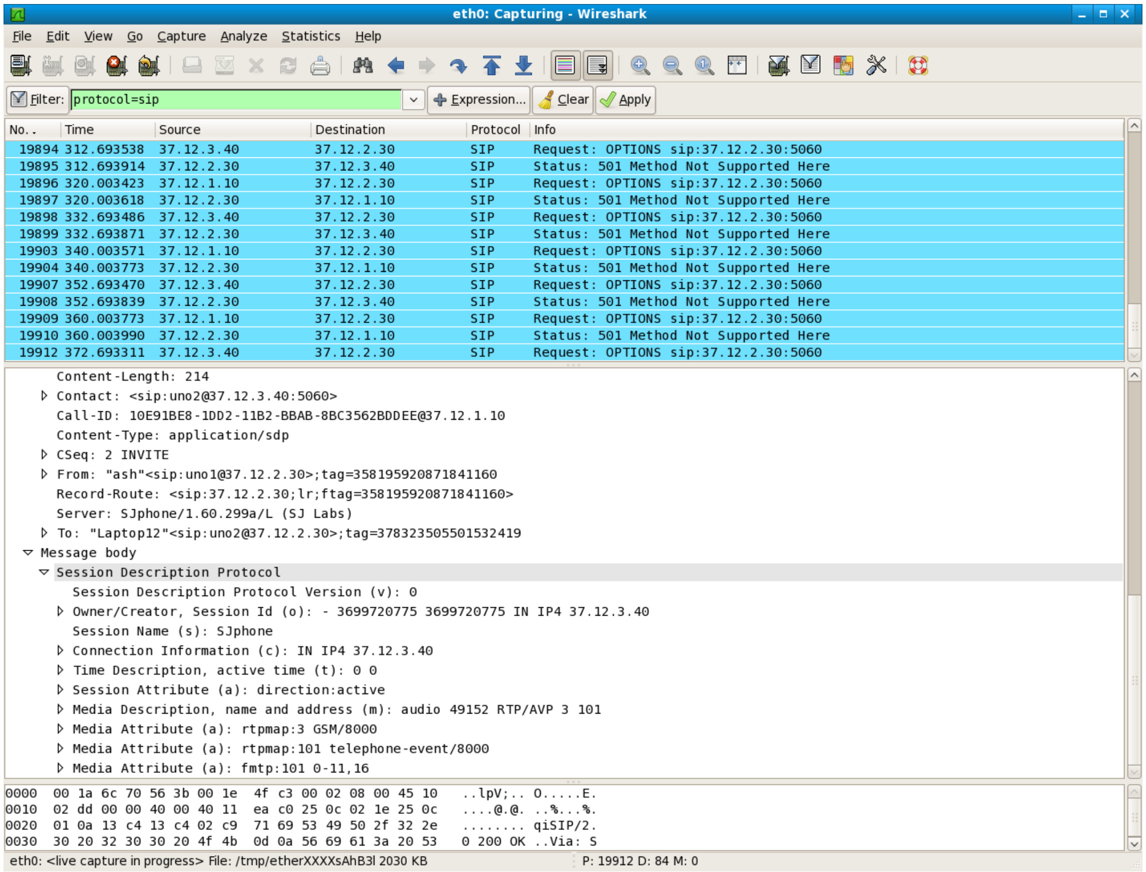
```
sudo openserctl domain add 37.12.2.30
sudo openserctl domain reload
sudo openserctl domain show
sudo openserctl add uno1@37.12.2.30 openserrw uno1@pitt.edu
```

```
sudo openserctl add uno2@37.12.2.30 openserrw uno2@pitt.edu
```

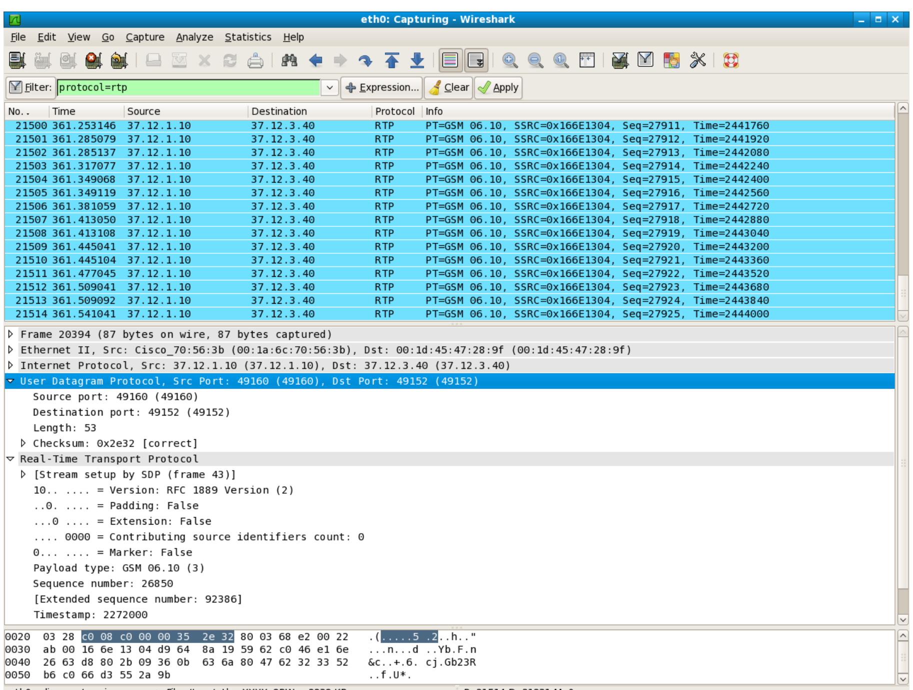
- SJPhone was launched on PC1, and configured to register with SIP proxy server. After the configuration, we were able to see the message “ready to call” which indicates that the user is registered with the SIP proxy server.
- Similar steps were carried out on the SJPhone application on the laptop and it was registered with the SIP proxy server.

```
[team12@netlab-wb2pc3 ~]$ sudo openserctl ul show
Domain:: location table=512 records=2 max_slot=1
        AOR:: uno2
                Contact:: sip:uno2@37.12.3.40:5060 Q=0
                        Expires:: 3557
                        Callid:: B6BA4848-1DD1-11B2-AAB7-BD0D33A5B951@37.12.3.40
                        Cseq:: 2
                        User-agent:: SJphone/1.60.299a/L (SJ Labs)
                        State:: CS_SYNC
                        Flags:: 0
                        Cflag:: 0
                        Socket:: udp:37.12.2.30:5060
                        Methods:: 4294967295
        AOR:: uno1
                Contact:: sip:uno1@37.12.1.10:5060 Q=0
                        Expires:: 3324
                        Callid:: 4F13C162-1DD2-11B2-BBAA-8BC3562BDDEE@37.12.1.10
                        Cseq:: 2
                        User-agent:: SJphone/1.60.299a/L (SJ Labs)
                        State:: CS_SYNC
                        Flags:: 0
                        Cflag:: 0
                        Socket:: udp:37.12.2.30:5060
                        Methods:: 4294967295
```

- Now the call was placed between the 2 user agents registered with the SIP proxy using just the username.
- The connection setup captures are shown. As it can be the calling party is checking with the SIP server **37.12.2.30**. The SIP server in turn places the call to the called party at **37.12.3.40**.
- Also it can be seen in the packet details below, at the end of the call initialization, the SIP server is sending the IP information of the calling party to the called party. And the RTP port **49152** is also shared.
- The RTP transaction occurs directly between the user agents on the IP and port, highlighted in the snapshot above. RTP captures are shown below.



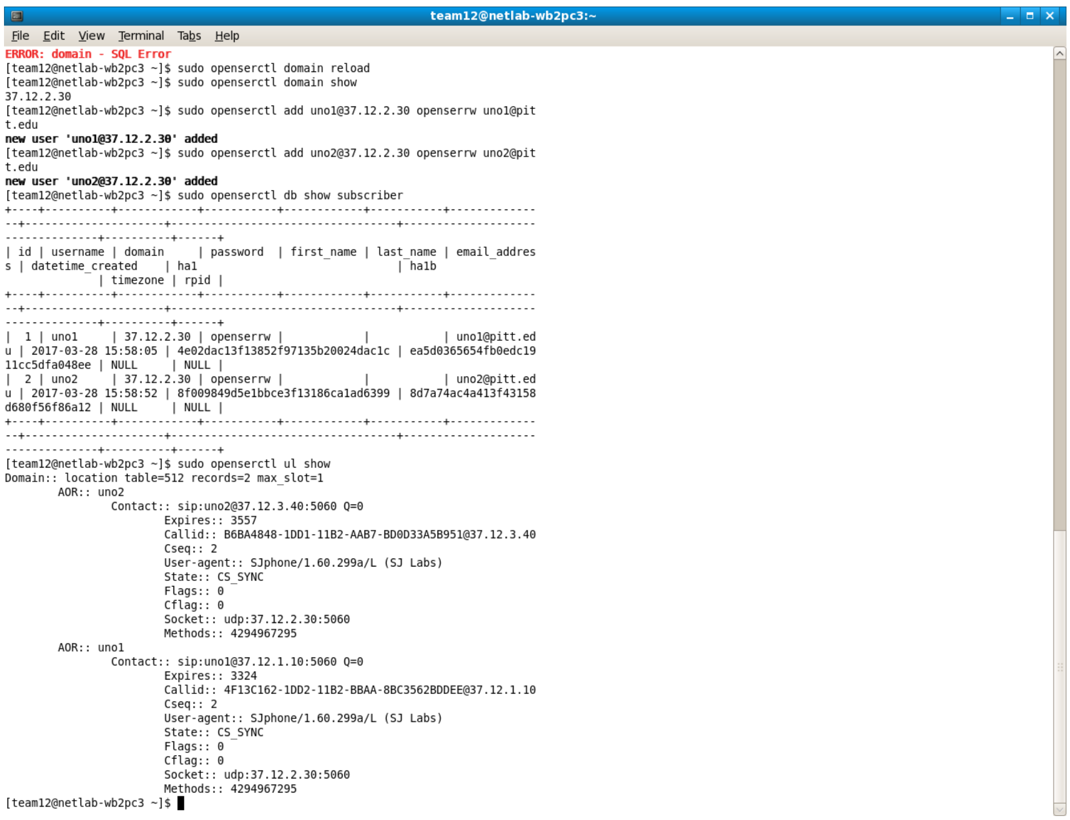

- The RTP transaction occurs directly between the user agents on the IP and port, highlighted in the snapshot above. RTP captures are shown below.



- All the SJPhone instances were closed.

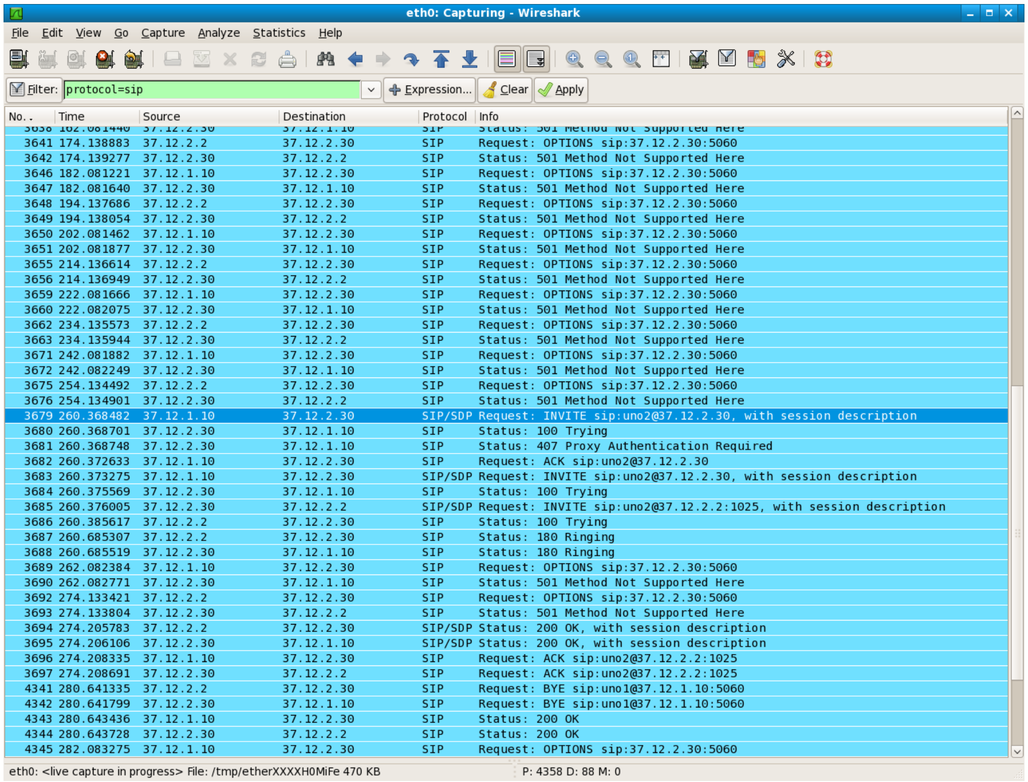
## Experiment 4.3: NAT issues with VOIP Traffic – Router based solution

- The IP addresses on LAN3 were changed to the subnet 10.31.0.0/24.
- On router R2, NAT with overload was configured so that hosts in LAN3 can access the outside world using the public IP of the interface of fa0/0/0 on router R2.
- Confirmed connectivity to LAN1 and LAN2 from LAN3 using ping.
- Wireshark was started on the laptop to monitor eth0.
- SJPhone application was launched on PC1 and Laptop.
- Registered users on the SIP server are shown below.

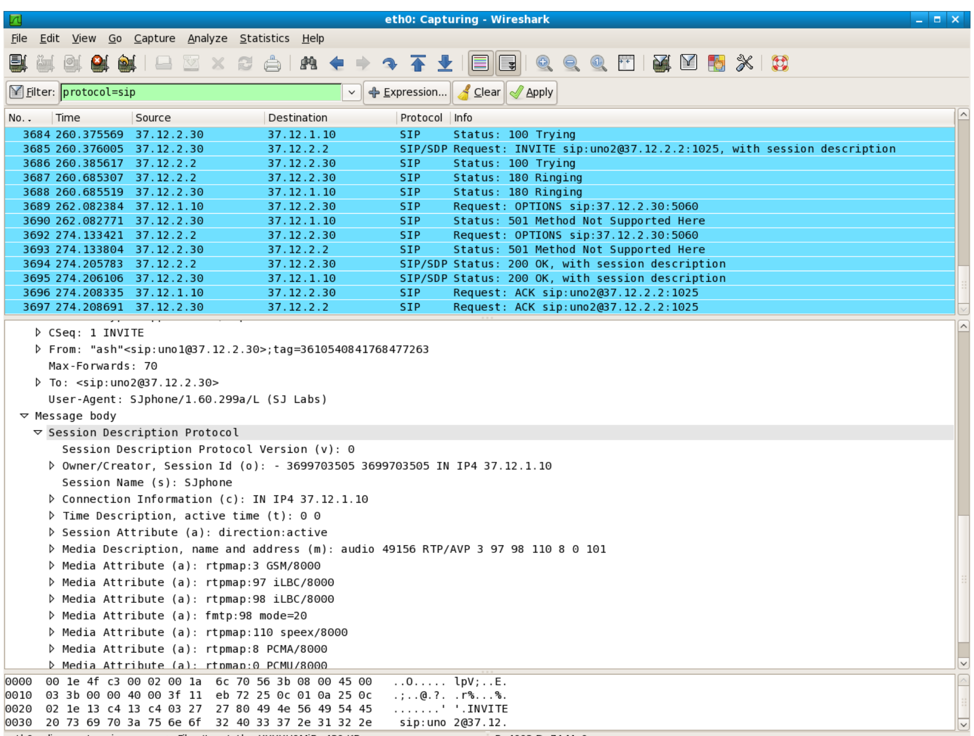


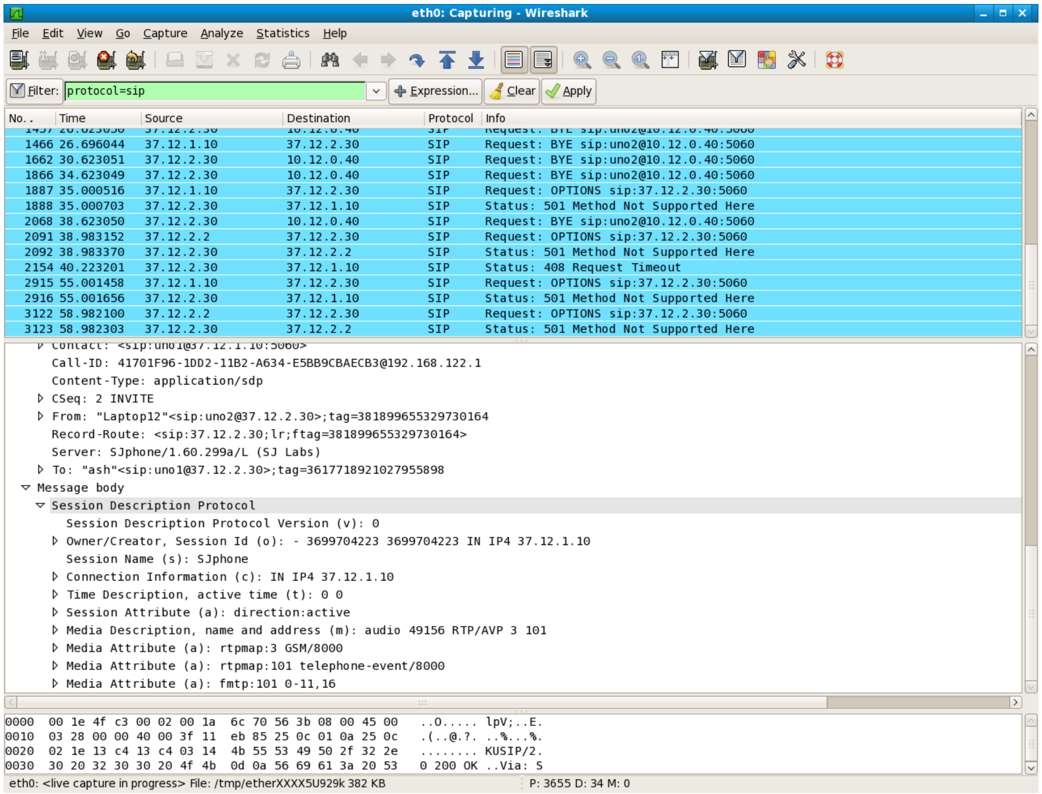
```
team12@netlab-wb2pc3:~
File Edit View Terminal Tabs Help
ERROR: domain - SQL Error
[team12@netlab-wb2pc3 ~]$ sudo openserctl domain reload
[team12@netlab-wb2pc3 ~]$ sudo openserctl domain show
37.12.2.30
[team12@netlab-wb2pc3 ~]$ sudo openserctl add uno1@37.12.2.30 openserrw uno1@pit
t.edu
new user 'uno1@37.12.2.30' added
[team12@netlab-wb2pc3 ~]$ sudo openserctl add uno2@37.12.2.30 openserrw uno2@pit
t.edu
new user 'uno2@37.12.2.30' added
[team12@netlab-wb2pc3 ~]$ sudo openserctl db show subscriber
+----+----------+-----------+----------+-----------+----------+------------
--+---------------------+---------------------------------+-------------------
-------------+---------+-----+
| id | username | domain     | password  | first_name | last_name | email_addres
s | datetime_created    | ha1                              | ha1b
               | timezone | rpid |
+----+----------+-----------+----------+-----------+----------+------------
--+---------------------+---------------------------------+-------------------
-------------+---------+-----+
|  1 | uno1     | 37.12.2.30 | openserrw |            |           | uno1@pitt.ed
u | 2017-03-28 15:58:05 | 4e02dac13f13852f97135b20024dac1c | ea5d0365654fb0edc19
11cc5dfa048ee | NULL     | NULL |
|  2 | uno2     | 37.12.2.30 | openserrw |            |           | uno2@pitt.ed
u | 2017-03-28 15:58:52 | 8f009849d5e1bbce3f13186ca1ad6399 | 8d7a74ac4a413f43158
d680f56f86a12 | NULL     | NULL |
+----+----------+-----------+----------+-----------+----------+------------
--+---------------------+---------------------------------+-------------------
-------------+---------+-----+
[team12@netlab-wb2pc3 ~]$ sudo openserctl ul show
Domain:: location table=512 records=2 max_slot=1
        AOR:: uno2
                Contact:: sip:uno2@37.12.3.40:5060 Q=0
                        Expires:: 3557
                        Callid:: B6BA4848-1DD1-11B2-AAB7-BD0D33A5B951@37.12.3.40
                        Cseq:: 2
                        User-agent:: SJphone/1.60.299a/L (SJ Labs)
                        State:: CS_SYNC
                        Flags:: 0
                        Cflag:: 0
                        Socket:: udp:37.12.2.30:5060
                        Methods:: 4294967295
        AOR:: uno1
                Contact:: sip:uno1@37.12.1.10:5060 Q=0
                        Expires:: 3324
                        Callid:: 4F13C162-1DD2-11B2-BBAA-8BC3562BDDEE@37.12.1.10
                        Cseq:: 2
                        User-agent:: SJphone/1.60.299a/L (SJ Labs)
                        State:: CS_SYNC
                        Flags:: 0
                        Cflag:: 0
                        Socket:: udp:37.12.2.30:5060
                        Methods:: 4294967295
[team12@netlab-wb2pc3 ~]$
```

- Call was started from PC1 to the Laptop. The call was successful as the Cisco 2811 routers are equipped with Application-level Gateway for SIP traffic and they are capable of parsing the SIP registration and apply the necessary NAT-traversal measures.
- The call setup and teardown traffic was captured. Captures are shown below. We can see the INVITE, ACK and the BYE messages.




- ➢ The SDP messages exchanged and the SDP flow on both PC1 and the Laptop are captured and shown below.





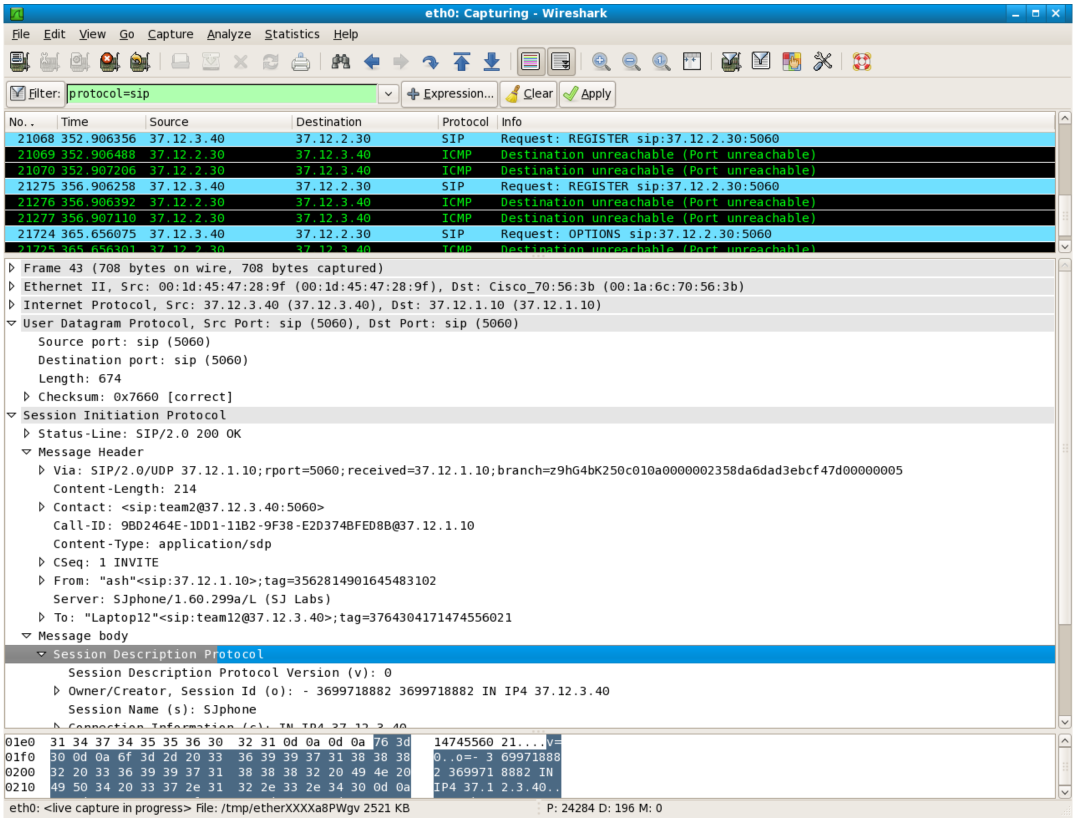

- As it can be seen from the laptop point of view, for SIP messages, it is always communicating with the SIP server and we see the private IP address of the Laptop. Whereas from the PC3 point of view, it observes that the request is coming from the PC1 to the SIP server and the SIP server is forwarding the requests to the public IP of the router R2. It does not know the private IP address of the Laptop. The router takes care of forwarding the messages to the Laptop received from the SIP server.
- All SJPhone instances were closed.

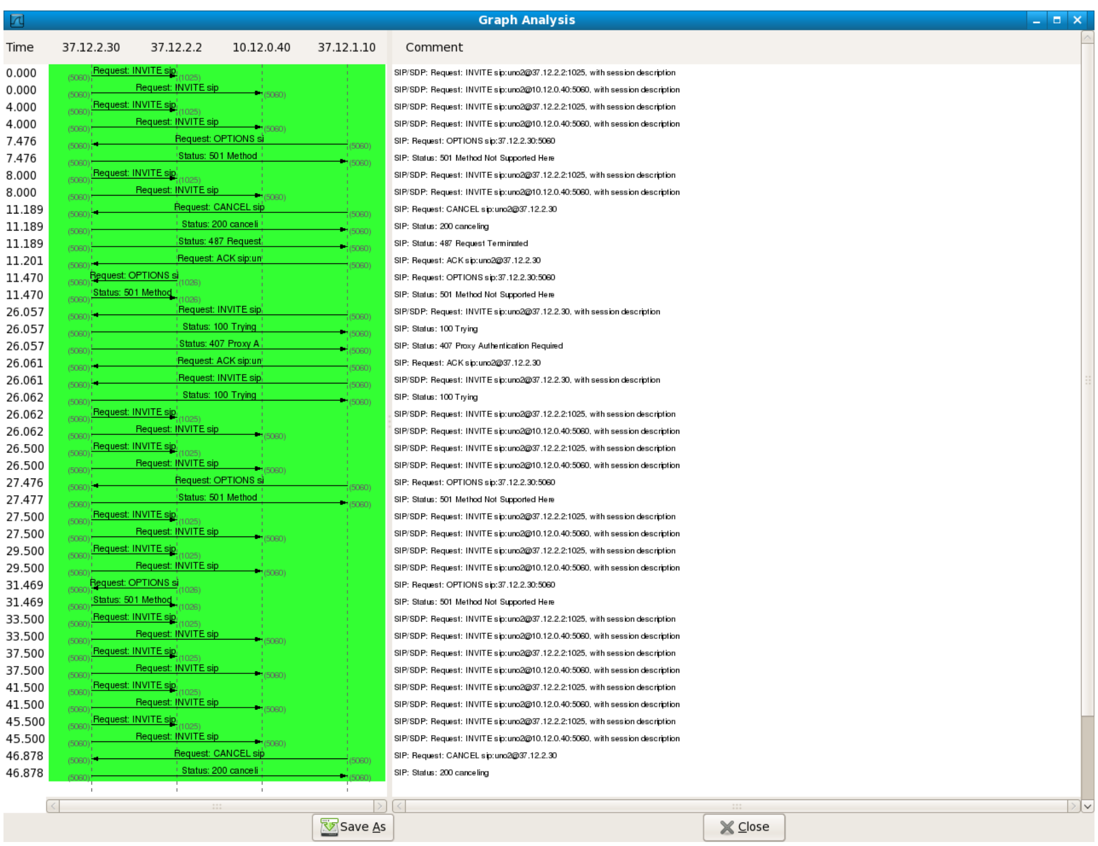
## Experiment 4.4: NAT issues with VOIP traffic – without routers support

- Ensured that on PC3 there are 2 static routes and there is no default gateway set.
- On the router R2, SIP NAT was disabled using the commands given below.

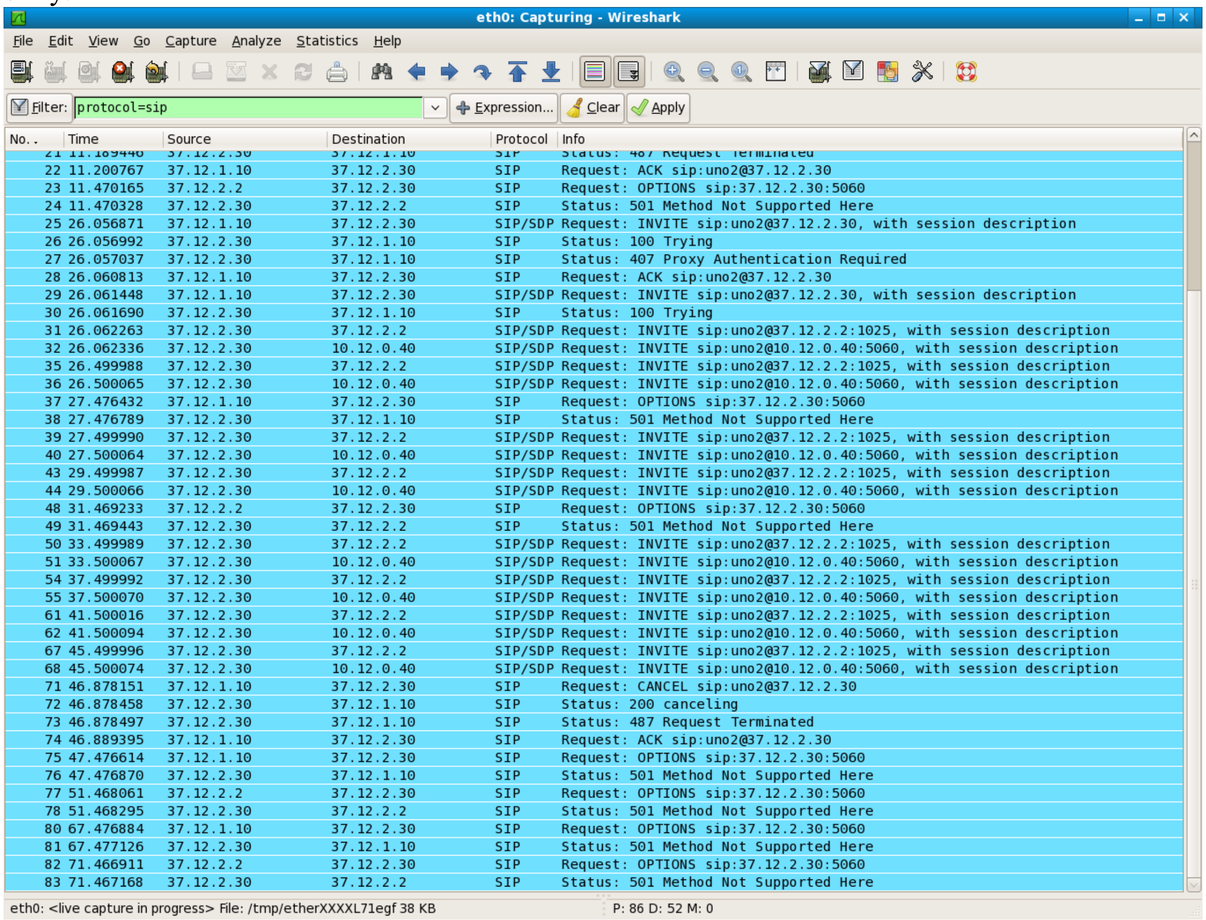
```
no ip nat service sip tcp port 5060
no ip nat service sip udp port 5060
```

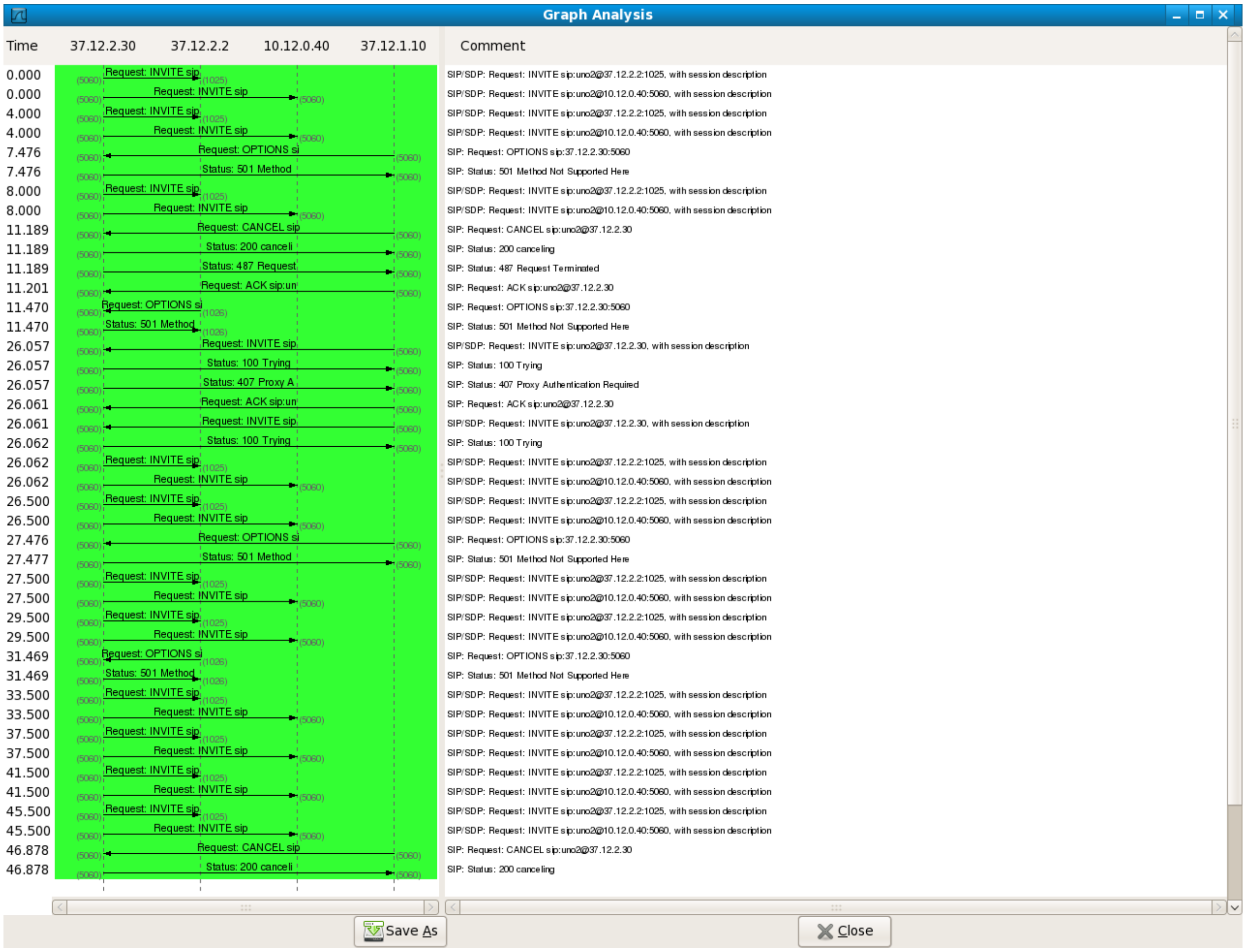
- The NAT translations were cleared on the router.
- The SJPhone instances were launched again and the call was repeated from the PC1 to Laptop.
- This call failed. As it can be seen in the captures below, the PC1 is not able to reach the Laptop now since the SIP NAT was disabled on the router. An ICMP unreachable message is sent back to the PC1.


eth0: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: protocol=sip
Expression... Clear Apply
No. . Time Source Destination Protocol Info
21068 352.906356 37.12.3.40 37.12.2.30 SIP Request: REGISTER sip:37.12.2.30:5060
21069 352.906488 37.12.2.30 37.12.3.40 ICMP Destination unreachable (Port unreachable)
21070 352.907206 37.12.2.30 37.12.3.40 ICMP Destination unreachable (Port unreachable)
21275 356.906258 37.12.3.40 37.12.2.30 SIP Request: REGISTER sip:37.12.2.30:5060
21276 356.906392 37.12.2.30 37.12.3.40 ICMP Destination unreachable (Port unreachable)
21277 356.907110 37.12.2.30 37.12.3.40 ICMP Destination unreachable (Port unreachable)
21724 365.656075 37.12.3.40 37.12.2.30 SIP Request: OPTIONS sip:37.12.2.30:5060
Frame 43 (708 bytes on wire, 708 bytes captured)
Ethernet II, Src: 00:1d:45:47:28:9f (00:1d:45:47:28:9f), Dst: Cisco_70:56:3b (00:1a:6c:70:56:3b)
Internet Protocol, Src: 37.12.3.40 (37.12.3.40), Dst: 37.12.1.10 (37.12.1.10)
User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
Source port: sip (5060)
Destination port: sip (5060)
Length: 674
Checksum: 0x7660 [correct]
Session Initiation Protocol
Status-Line: SIP/2.0 200 OK
Message Header
Via: SIP/2.0/UDP 37.12.1.10;rport=5060;received=37.12.1.10;branch=z9hG4bK250c010a0000002358da6dad3ebcf47d00000005
Content-Length: 214
Contact: <sip:team2@37.12.3.40:5060>
Call-ID: 9BD2464E-1DD1-11B2-9F38-E2D374BFED8B@37.12.1.10
Content-Type: application/sdp
CSeq: 1 INVITE
From: "ash"<sip:37.12.1.10>;tag=3562814901645483102
Server: SJphone/1.60.299a/L (SJ Labs)
To: "Laptop12"<sip:team12@37.12.3.40>;tag=3764304171474556021
Message body
Session Description Protocol
Session Description Protocol Version (v): 0
Owner/Creator, Session Id (o): - 3699718882 3699718882 IN IP4 37.12.3.40
Session Name (s): SJphone
01e0 31 34 37 34 35 35 36 30 32 31 0d 0a 0d 0a 76 3d 14745560 21....v=
01f0 30 0d 0a 6f 3d 2d 20 33 36 39 39 37 31 38 38 38 0..o=- 3 69971888
0200 32 20 33 36 39 39 37 31 38 38 38 32 20 49 4e 20 2 369971 8882 IN
0210 49 50 34 20 33 37 2e 31 32 2e 33 2e 34 30 0d 0a IP4 37.1 2.3.40..
eth0: <live capture in progress> File: /tmp/etherXXXXa8PWgv 2521 KB
P: 24284 D: 196 M: 0


Graph Analysis
Time 37.12.2.30 37.12.2.2 10.12.0.40 37.12.1.10
Comment
SIP/SDP: Request: INVITE sip:uno2@37.12.2.2:1025, with session description
SIP/SDP: Request: INVITE sip:uno2@10.12.0.40:5060, with session description
SIP: Request: OPTIONS sip:37.12.2.30:5060
SIP: Status: 501 Method Not Supported Here
SIP: Request: CANCEL sip:uno2@37.12.2.30
SIP: Status: 200 canceling
SIP: Status: 487 Request Terminated
SIP: Request: ACK sip:uno2@37.12.2.30
SIP/SDP: Request: INVITE sip:uno2@37.12.2.30, with session description
SIP: Status: 100 Trying
SIP: Status: 407 Proxy Authentication Required
Save As
Close

- Now we tried a call from Laptop to PC1. This call was successful because a NAT overload was configured earlier on router R2 and since this connection is originating from inside LAN3 the router will overload the connection to its outside interface IP address and add a NAT translation entry.






- From the captures and the flow graph we can see that the call is successful and there is no ICMP unreachable message sent.
- After a few seconds, the call was ended from the PC1 side. But this call was not terminated on the laptop side because the SIP message is generated from PC1 and sent to SIP server. The SIP server now tries to send this message to the Laptop but since there is no NAT translation entry on the router for the SIP server and since SIP NAT is disabled on the router, it does not allow this message to pass through and hence the Laptop still thinks that the call is still going on.
- In the captures given above we can see once the PC1 sends a BYE message to the SIP server, the SIP server tries to forward that message to the Laptop. But since it is not successful it sends a message back to the PC1 saying that the sending has failed and we see a "send failed" packet.

## Exit Procedures

- Ensured there is one cable connecting each PCx21 port to the DELL switch (ports 1-20).
- Ensured there is one cable connecting port LA111 to the DELL switch (ports 1-20).
- The LNET port is connected to port 19 of the DELL switch.
- The MGT port is connected to port 23 of the DELL switch.
- Nothing else is connected to the switch, hub or router ports.
- Unused cables were put on the cabling rack and all computers were shut down.