From Bicom Systems Wiki

Contents

Capturing traffic

Login to the system shell as a root user and execute command that would match the port for traffic you would like to capture:

SIP

Full SIP traffic

```
tcpdump port 5060 -s 0 -w debug.pcap
```

SIP traffic for specific IP address

```
tcpdump -i any port 5060 and host 192.168.1.59 -s 0 -w debug.pcap
```

RTP

SIP + RTP traffic for specific IP address

```
tcpdump -i any host 192.168.1.59 -T rtp -vvvvv -s 0 -w test.pcap
```

NOTE: Please replace IP address so it matches the host you want to perform debugging for (most often that will be your provider IP).

e-mail

SMTP

```
tcpdump -i any port 25 -s 0 -w debug.pcap -vv
```

Analyzing captured traffic

Download the file from PBXware by either using GUI utilities that support connection on port 2020 or using SCP from terminal:

```
scp -P 2020 root@ip.address:/path/to-the/file /destination/folder/on/your/hdd/
```

Download **'Ethereal'** program from 'http: //www.ethereal.com/download.html'

Open your saved file with **'Ethereal'** program and analyze the content.

If you don't have the knowledge to analyze the captured traffic Bicom Systems Support team will be glad to do it for you.

Retrieved from
"http://wiki.bicomsystems.com/HOWTO_Recording_Ethernet_Packets_Using_tcpdump"