Capture TCPDumps

TCP Dump

1. If we want to get a TCP Dump of everything on port 5060 we can use the following command. This will create a file called capture.pcap in the tmp directory of everything on port 5060. If the file is bigger than 50MB it will start another file.
    - tcpdump -s0 -w/tmp/capture.pcap -C50 udp and port 5060

2. If we wanted to limit it to a specific IP address, like a phone or SIP carrier, we could do:
    - tcpdump -s0 -w/tmp/capture.pcap -C50 udp and port 5060 and host 129.33.194.122

3. To easily view the SIP transaction, load the PCAP into wireshark and goto Telephony -> VoIP Calls. Then select the session you want to look at and click "Flow." If you've captured the RTP traffic (Option: **-T rtp**), you may be able to play the audio of the call as well.

4. Run tcpdump in the background from a screen session so you can disconnect while it runs. This also tags the file name with the host name and timestamp.
    - screen -dm tcpdump -s0 -w/tmp/capture-dep`hostname -s`-`date +%Y%m%d-%H%M%Z`.pcap -C150 udp and port 5060

Running the commands:

1) Log into the server using SSH protocol
2) Run the command as shown in the above section. eg: "tcpdump -s 0 -i any -w sip-trace.pcap"
3) Reproduce the issue. This means make or receive a call.
4) Stop the tcpdump using CTRL+C
5) Log into the server using WINSCP and download the file "sip-trace.pcap"

Zip up and send in the sip-trace.pcap file (ensure it is zipped) along with the full details of which call the issue occurred on. Ensure you provide the called number, calling number and how many times that number was called in the trace.

Following explains the parameters used:

-i Select interface that the capture is to take place on, this will often be an Ethernet card or wireless adapter but could also be a VLAN interface. Not always required if there is only one network adapter.

-s0 Unlimited size of the packet to capture

-w Saves the file to the current folder

> **Ports**
>
> Remember to use the correct port when capturing packets. By default CHAN_SIP runs on port 5160 and PJSIP runs on port 5060

Ending the 'screen' session in order to stop capturing.

If you decided to run *tcpdump* in the background using a screen session you can end this session with the following steps.

1) Retrieve the name of the screen with the following command:

- screen -ls

This may be the result

```
There is a screen on:
        11523..uc-87161439      (Detached)
1 Socket in /var/run/screen/S-root.
```

2) Attach (enter) your session to the *screen* session running the following command (Keep in mind the screen session is named *11523..uc-87161439*)

- screen -x 11523..uc-87161439

3) Finish the screen with the keys CTRL+C

After that you will be redirected to your SSH session.