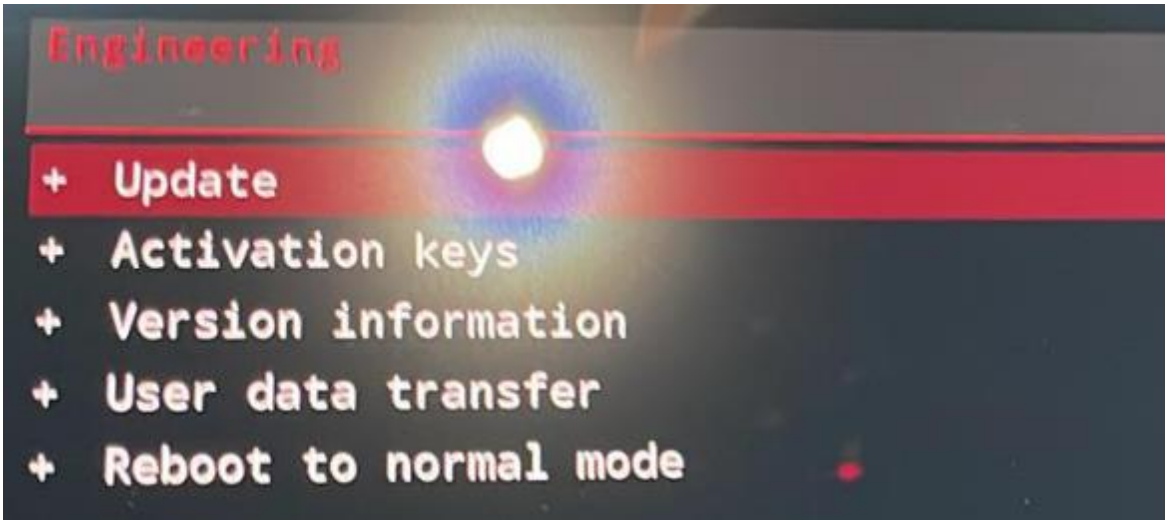
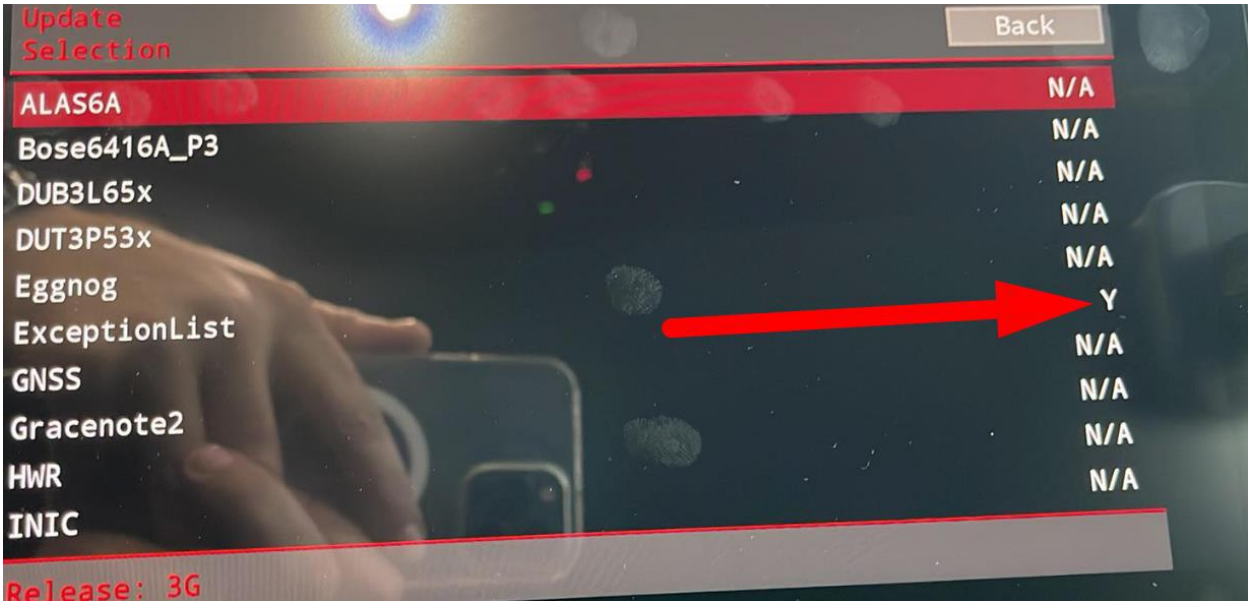
Shell access via challenge method

Update with “Special firmware” which changes public key of challenge. To do that. Hold two fingers in top right corner to enter **SWUP** (**RED**) Mode. Press +

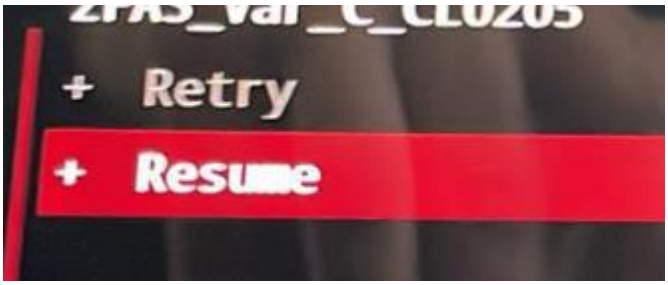
Press **+ Update**



Everything should say **N/A** except **ExceptionList**. It is normal, just scroll down and press **Start update**.



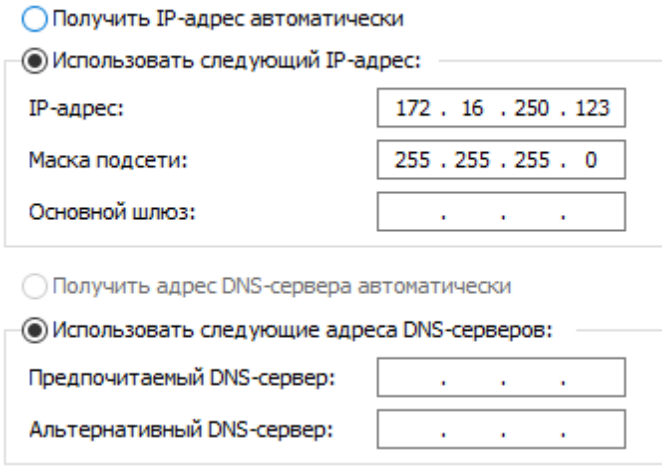
After update finished, press **+ Resume**



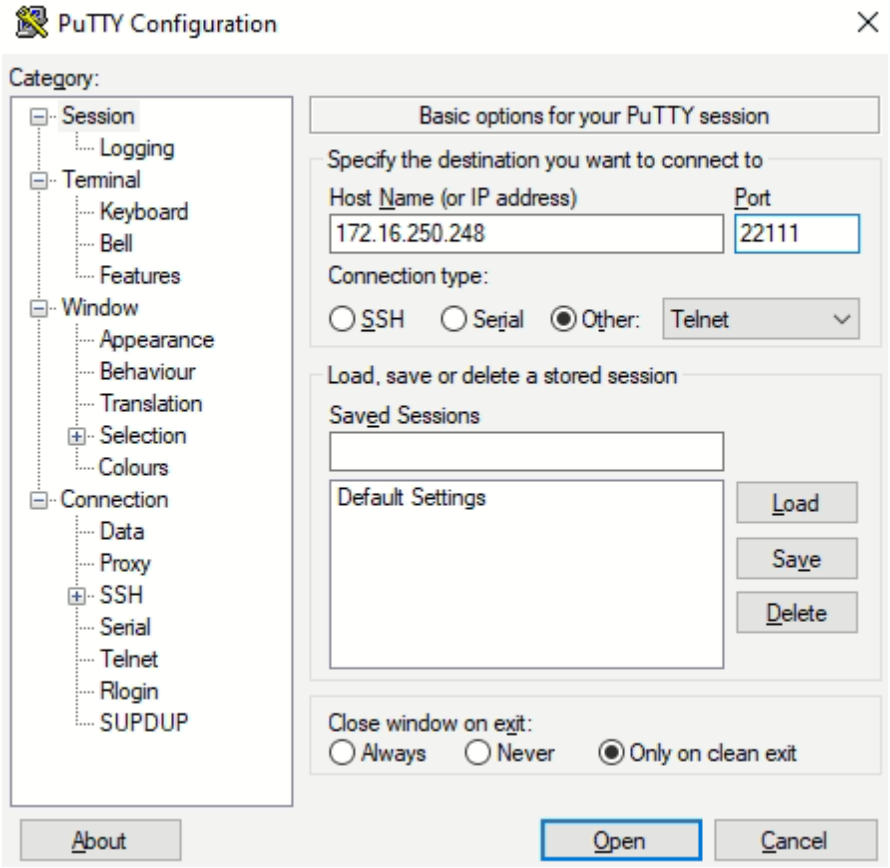
NOTE: ALL CHANGES ON UNIT SHOULD BE DONE IN RED MENU !!! HOLD 2 FINGERS IN TOP RIGHT CORNER, UNIT WILL GO TO RED MENU, ONLY THEN YOU CAN CONTINUE WITH FECS/CONVERSION.

When unit is in **red** menu, connection to unit can be done via D-Link DUB-E100. You need to change IPv4 address and mask to same as Harman uses

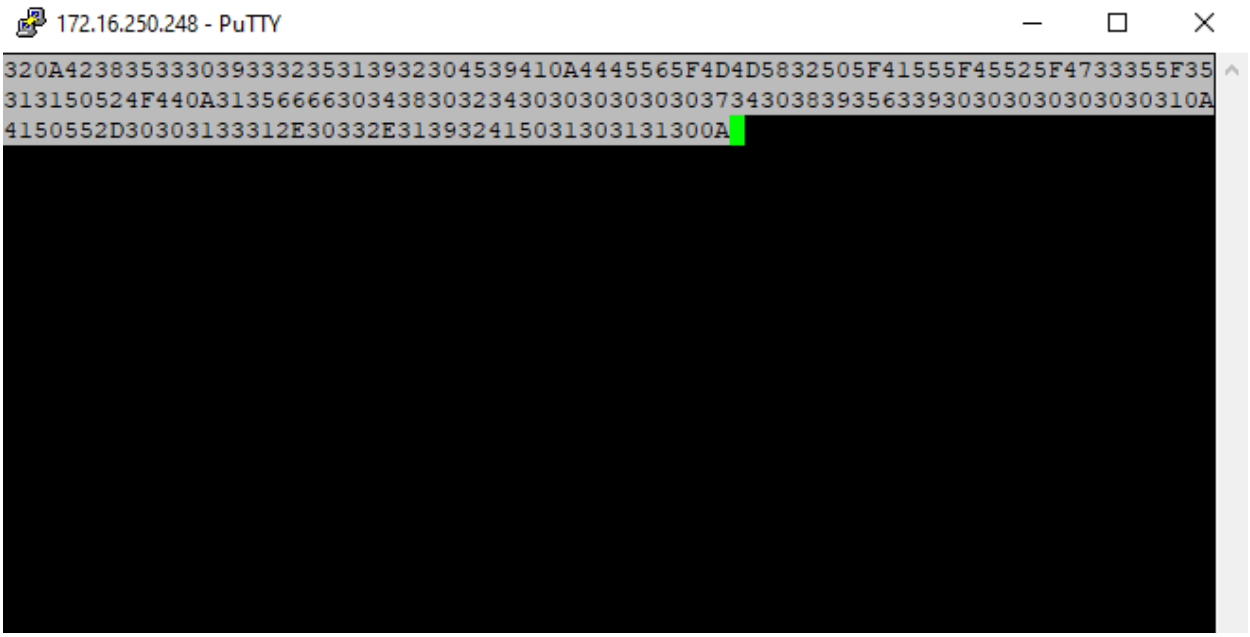
When unit is in **red** menu, connection to unit can be done via D-Link DUB-E100. You need to change IPv4 address and mask to same as Harman uses.



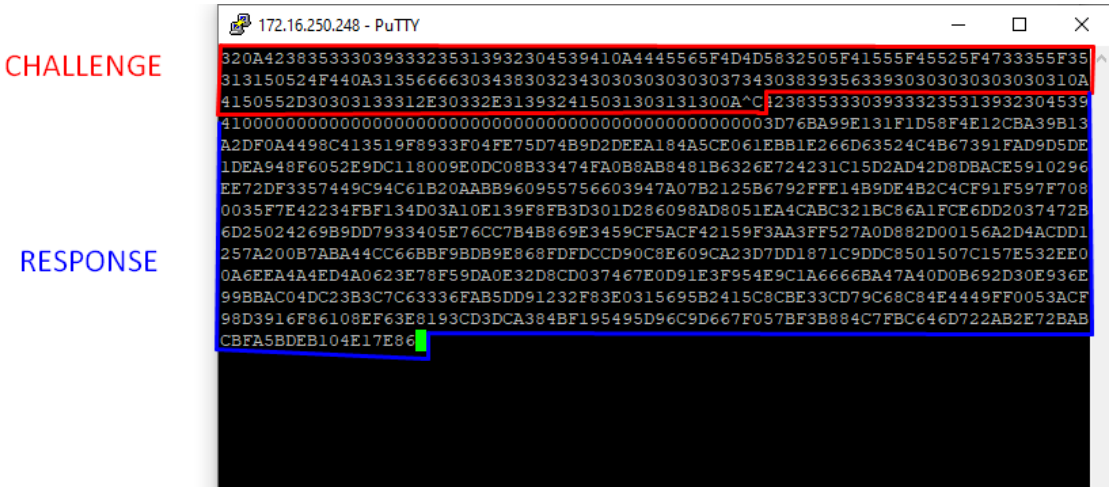
Challenge is on telnet **172.16.250.2.48**:**22111**



Copy **CHALLENGE KEY** and send



Copy **mmx_respnse.**, CTRL + A (Select all), CTRL + C (Copy all) and paste response with right click into **same** putty window!

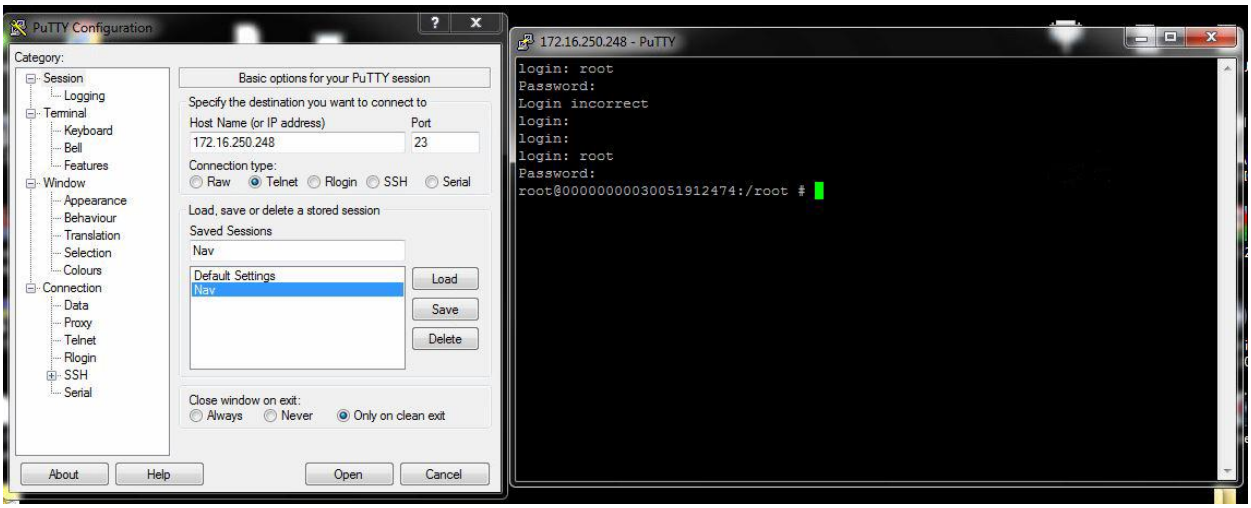


Press Enter. Putty should close.

MMX console	**Telnet**: 172.16.250.248:**23**
Challenge	**Telnet**:172.16.250.248:**22111**

Now you have opened telnet access and can connect with port 23.

Note: If you can't login, you are probably in normal, not in red menu. Go to red menu, and try to login then.



To disable password you need to run these commands:

RUN ALL COMMANDS ONLY FROM RED MENU !!)

mount -t qnx6 /dev/mnanda0t177.2 /mnt/swup

cp /mnt/swup/etc/nopasswd /mnt/swup/etc/passwd

sync

Now, even after reboot, your unit will have no password.

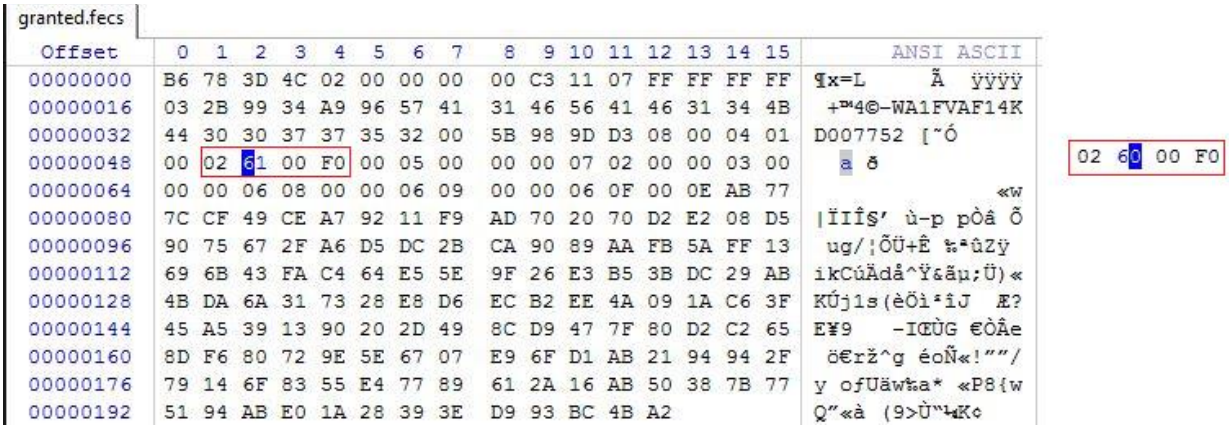
---

backup before modifying or patching any files

mount -a

mount -uw /fs/sdb0/
cat /dev/fs0 > /fs/sdb0/fs0_mib2p
cat /eso/bin/apps/fecmanager > /fs/sdb0/fecmanager
cat /eso/bin/apps/componentprotection > /fs/sdb0/componentprotection
mkdir /fs/sdb0/fec_backup/
cp -f /mnt/persist_new/fec/* /fs/sdb0/fec_backup/

FEC keys Edit on hex:



Put fecmanager and granted.fecs to SD, then login to unit and use commands:

mount -t qnx6 /dev/mnanda0t177.1 /tmp/177.1

mount -t qnx6 /dev/mnanda0t177.2 /tmp/177.2

mount -t qnx6 /dev/mnanda0t177.3 /tmp/177.3

mount -uw /tmp/177.1

mount -uw /tmp/177.2

mount -uw /tmp/177.3

/fs/sdb0/fecmanager

cp -Vf /fs/sdb0/fecmanager /tmp/177.1/eso/bin/apps/fecmanager

chmod 777 /tmp/177.1/eso/bin/apps/fecmanager

cp -Vf /fs/sdb0/fecmanager /tmp/177.2/eso/bin/apps/fecmanager

chmod 777 /tmp/177.2/eso/bin/apps/fecmanager

cp -Vf /fs/sdb0/fecmanager /tmp/177.3/eso/bin/apps/fecmanager

chmod 777 /tmp/177.3/eso/bin/apps/fecmanager

Fec:

rm -f /mnt/persist_new/fec/*.hist

rm -f /mnt/persist_new/fec/*.fecs

cd /mnt/persist_new/fec

cp -Vf /fs/sdb0/granted.fecs /mnt/persist_new/fec/

restart unit hold Power button