FAQ - Wireshark tracing

Valid for:	N610	N670	N870	N870E	Embedded Integrator	Virtual Integrator

Introduction

If needed, you can start a pcap trace on the system direct from your PC.

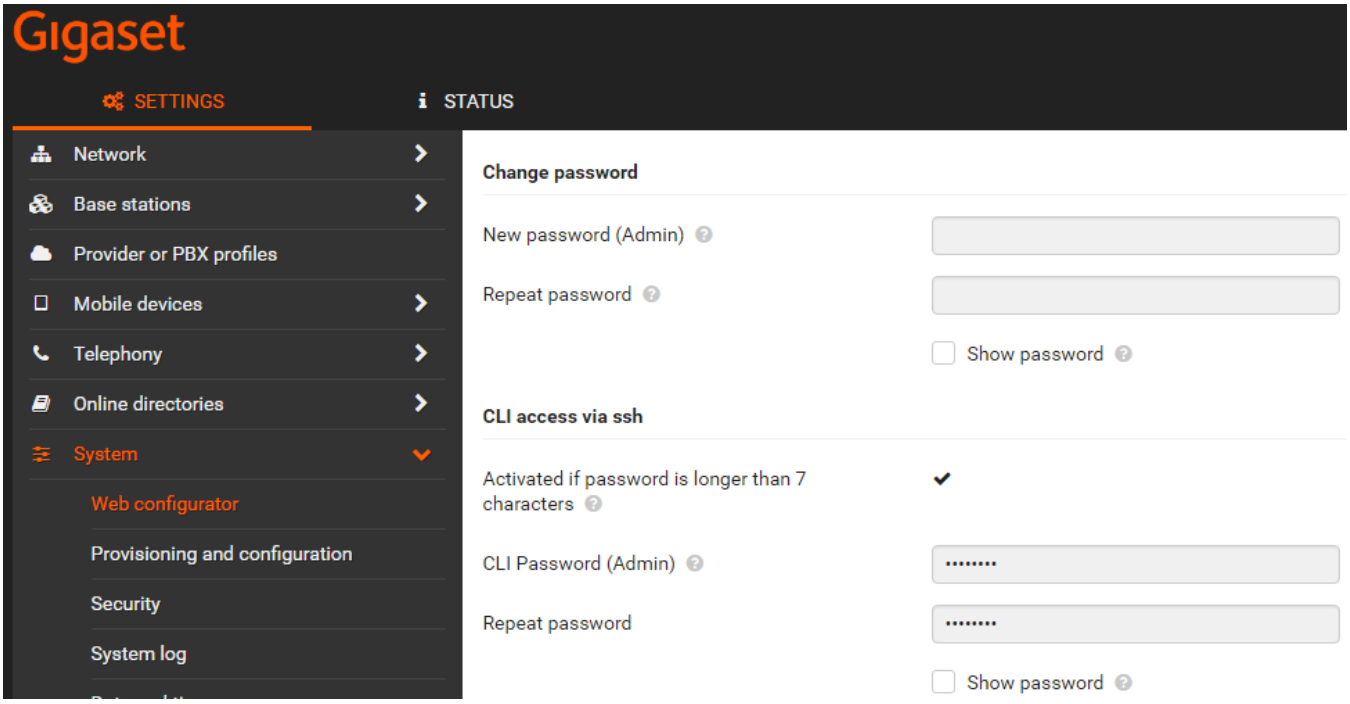
The trace can be made on the:

- DECT Manager + Base + Integrator
- DECT Base

Enable SSH access

First you need to enable SSH access to the system.

Open the web-interface and go to: **SETTINGS - System - Web configurator**.



Enter the Password for the SSH access.

Tools

The trace can be started direct from your PC.

Download this zip file that contains all tools and a batch file you can start direct from your laptop and opens a stream from the N870 to wireshark that is installed on your PC.
If you like to capture trace data from multiple device you may use our tool. Have a look here: FAQ Nx70 - Debugging Tool via cli access

1. Download the zip file.
2. Extract to your PC.
3. Wireshark must be installed on your PC.
4. Start the batch file.
5. Enter the IP address of the N870 device.
6. Enter the SSH Password.
7. Enter the port that you would like to trace or leave empty to trace all traffic.
8. Enter the host that you would like to trace or leave empty to trace all traffic.
9. Enter the Interface you are using or leave empty.

10. Enter the full path to Wireshark. (Press enter for default: C:\Wireshark\Wireshark.exe)
11. Wireshark is started and you can see all traffic from the N870.
12. When connected for the first time the rsa2 key needs to be stored in the cache. Go to the command box and confirm by entering y followed by enter.

The device that has the role DECT Manager + Integrator + Base will send the SIP traffic and RTP if the handset is connected to this device. Always remember that the DECT base where the call is started is sending the RTP to the outside world.

New batch file example:

The batch file must sometimes be changed dependent on the windows version or security on your PC. Also which version of plink and whireshark you use can have an influence on the batch file.

We can only share information when we adjusted the batch file to solve issues caused by the above. We can not support you solving Windows/security /plink issues.

Below is a batch file that is used today by us that works with the N870 software 2.26, latest putty version, Windows 10 and Wireshark 3.0.8

Batch file example

```
@echo off
set ipaddress=
set password=
set interface=
set wire=
set optionshost=
set optionsport=


@echo off

echo.
echo !!! This is used on your own risk !!!
echo.
echo.
echo To use default values (192.168.178.190, cliadmin, any), just press ENTER
echo.
echo Specially for the path to wireshark,
echo it is the easiest to press enter for the standard installation path!
echo (default: C:\Wireshark\Wireshark.exe)
echo.
echo Please enter...
echo Connection:
set /p ipaddress=1. ...IP-address from DECT Manager (for example, 192.168.178.190):
set /p password=2. ...admin-password (for example, Gigaset123):
echo.
echo Options:
set /p optionsport=3. ...the port for tracing (leave empty for ANY):
set /p optionshost=4. ...the host for tracing (leave empty for ANY):
echo.
echo Miscellaneous:
set /p interface=5. ...interface to capture (for example, any):
set /p wire=6. ...the full-path to wireshark:
echo.


if "%ipaddress%"=="" (set ipaddress=192.168.178.190)
if "%password%"=="" (set password=Gigaset123)
if "%interface%"=="" (set interface=any)
if "%wire%"=="" (set wire="C:\Wireshark\Wireshark.exe")
if NOT "%optionshost%"=="" (set optionshost=and host %optionshost%)
if "%optionsport%"=="" (set optionsport=not port 22) else (set optionsport=port %optionsport%)
echo %wire%

%CD%\plink.exe -ssh -pw %password% cli@%ipaddress% "exit"
%CD%\plink.exe -ssh -batch -pw %password% cli@%ipaddress% "sudo /usr/sbin/tcpdump -s0 %optionsport% %optionshost% -w -" | %wire% -k -l -i -
```