

## EHS6T LAN – Enkom Active Oy demo unit at Upseerinkatu 1, 5. floor electrical distribution cabinet



EHS6T LAN  
Has been connected to a Raritan BCM unit (Branch Circuit Monitoring)

The BCM measurement data are read in real time, using the http(s) connection

SIM = a fixed, public IPv4 address (Sonera)

Port forward EHS6T LAN – Raritan BCM

Only Http(s) allowed (port 443)

Firewall settings on the Linux side (OpenWRT)

# EHS6T LAN – Enkom Active Oy demo unit at Upseerinkatu 1, 5. floor electrical distribution cabinet



```
195.165.181.238:1234 - Tera Term VT
File Edit Setup Control Window Help
~SCFG: "URC/Ringline/ActiveTime", "2"
~SCFG: "Userware/Autostart", "1"
~SCFG: "Userware/Autostart/Delay", "0"
~SCFG: "Userware/DebugInterface", "0.0.0.0", "0.0.0.0", "0"
~SCFG: "Userware/DebugMode", "off"
~SCFG: "Userware/Passwd", ""
~SCFG: "Userware/Stdout", "usb1", "", "off"
~SCFG: "Userware/Watchdog", "0"

OK
at i1
Cinterion
EHS6
REVISION 03.001
A-REVISION 00.000.42

OK
at ^sjan=5
~STAM: "a:/JRC-1.56.42.jad", "Java Remote Control MIDlet Suite", "Cinterion", "1.56.42", "1"
~STAM: "a:/SLAE.jad", "SL Agent Module Services", "Genalto M2M GmbH", "2.1.1", "0"

OK
```

```
195.165.181.238:22 - Tera Term VT
File Edit Setup Control Window Help
-rw-r--r-- 1 root root 2478 Sep 28 2015 protocols
drwxr-xr-x 2 root root 71 Mar 11 2016 rc.button
-rw-r-xr-x 1 root root 2407 Sep 28 2015 rc.common
drwxr-xr-x 1 root root 0 Jan 23 15:20 rc.d
-rw-r--r-- 1 root root 140 Mar 11 2016 rc.local
lrwxrwxrwx 1 root root 16 Mar 11 2016 resolv.conf -> /tmp/resolv.conf
-rw-r--r-- 1 root root 6509 Mar 11 2016 ser2net.conf
-rw-r-xr-x 1 root root 5481 Mar 11 2016 ser2netehsfu-0.01.conf
-rw-r--r-- 1 root root 3017 Sep 28 2015 services
-rw----- 1 root root 210 Jan 23 14:32 shadow
-rw----- 1 root root 210 Nov 11 15:19 shadow-
-rw-r--r-- 1 root root 9 Sep 28 2015 shells
-rw-r-xr-x 1 root root 414 Mar 11 2016 snsdl.conf
-rw-r--r-- 1 root root 872 Sep 28 2015 sysctl.conf
-rw-r--r-- 1 root root 154 Dec 21 10:19 sysupgrade.conf
drwxr-xr-x 1 root root 0 Mar 11 2016 uci-defaults
-rw-r--r-- 1 root root 926 Mar 11 2016 vsftpd.conf
-rw-r--r-- 1 root root 9 Mar 11 2016 vsftpd.denied_users

root@OpenWrt:/home/nittari# cat demo
This is a demo user "nittari" that has a
home directory /home/nittari.

root@OpenWrt:/home/nittari#
```

AT-command using Telnet with TeraTerm, port 1234, USB3 at the modem side.

**-unprotected connection**

Linux (OpenWRT) –connection using SSH:lla (Tera Term)  
- User Name, Passphrase and certificate required  
**-protected connection**

Genalto Sensorlogic Module Services

# EHS6T LAN – Enkom Active Oy demo unit at Upseerinkatu 1, 5. floor electrical distribution cabinet

**TLS-protected connection** to Sensorlogic Module Services – Firefox-browser used (monitoring, updates etc.)

The screenshot shows the Gemalto Sensorlogic Module Services web interface. The page title is "3 DEVICES". Below the title, there is a filter bar with "Filter by" set to "My organization", "Supply Voltage (mV)" set to a dropdown, and "Choose condition" set to a dropdown. The main content is a table with 3 columns: "IMEI", "Type", and "Supply Voltage (mV)".

IMEI	Type	Supply Voltage (mV)
357042061238748	EHS6	4150
004401081754919	ELS61-E	3650
004401081024099	EHS6	3980

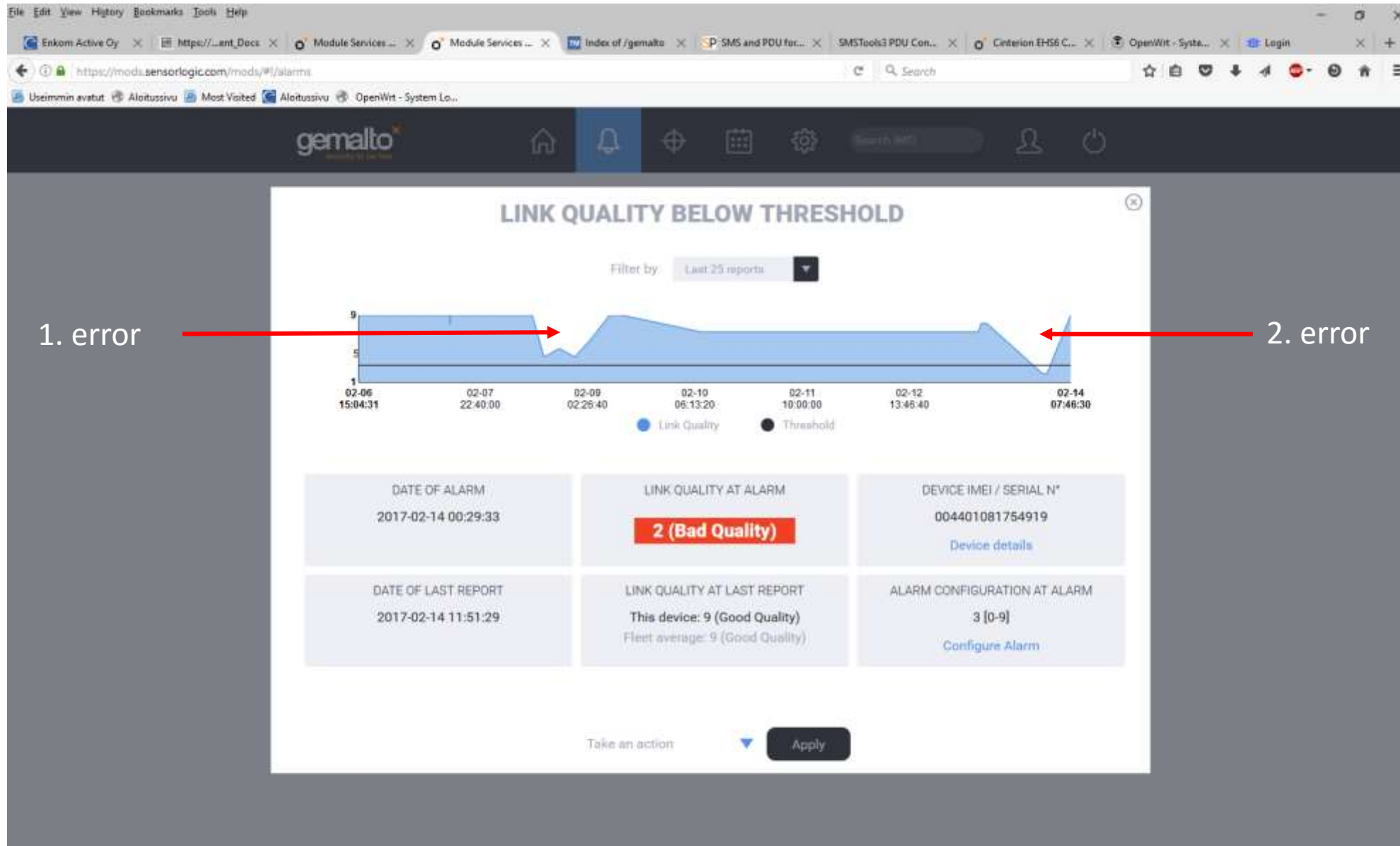
Annotations on the right side of the image:

- A red circle highlights the IMEI "357042061238748" in the first row.
- A red circle highlights the "Supply Voltage (mV)" value "4150" in the first row.
- A red arrow points from the text "Voltage from the EHS6T LAN" to the circled "4150".
- A red arrow points from the text "Voltages from two Gemalto modules, EHS6 and ELS61-E (LTE)" to the "3650" value in the second row.
- A red arrow points from the text "Voltages from two Gemalto modules, EHS6 and ELS61-E (LTE)" to the "3980" value in the third row.

3 of 3 devices displayed

# EHS6T LAN – Enkom Active Oy demo unit at Upseerinkatu 1, 5. floor electrical distribution cabinet

Alarm display – LTE network errors shown



# EHS6T LAN – Enkom Active Oy demo unit at Upseerinkatu 1, 5. floor electrical distribution cabinet

FTP (PASV)-connection with WinSCP, only user/password protection, access limited to one folder only.



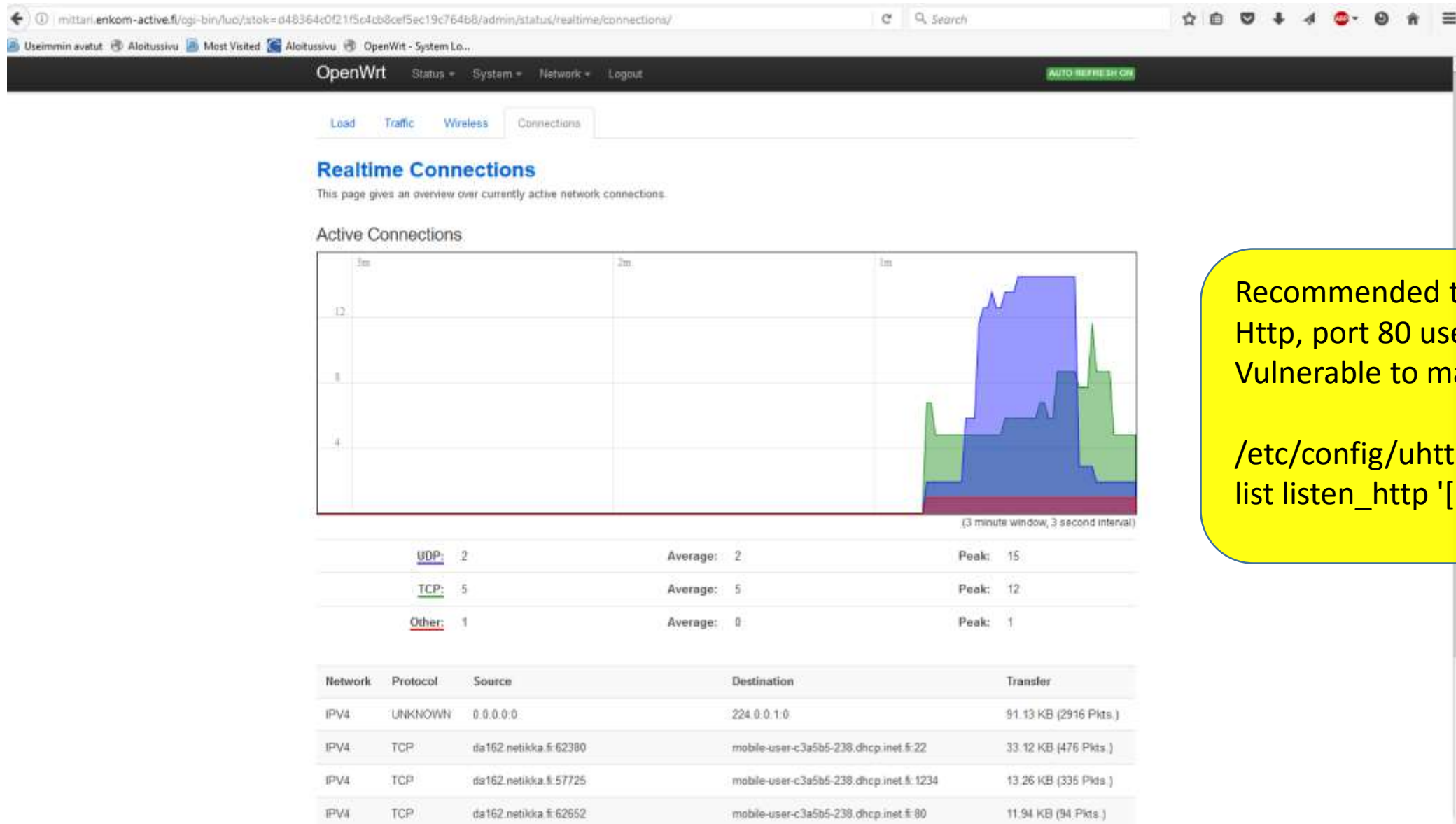
The screenshot shows the WinSCP interface connected to a remote host 'fw@195.164.181.238'. The local pane shows the user's home directory with various folders. The remote pane shows the root directory with two files: 'lokilukukoe' (57 KB) and 'topresults' (8 KB). A red circle highlights these two files, and a red arrow points from them to the text box on the right.

Name	Size	Changed	Rights	Owner
lokilukukoe	57 KB	14.2.2017 13.28	rw-r--r--	0
topresults	8 KB	14.2.2017 13.29	rw-r--r--	0

Files, made and stored on the EHS6T LAN Linux (OpenWRT) environment

# EHS6T LAN – Enkom Active Oy demo unit at Upseerinkatu 1, 5. floor electrical distribution cabinet

OpenWRT optional graphical user interface used using Firefox (not supported but exists 😊)



Recommended to be disabled.  
Http, port 80 used.  
Vulnerable to many attacks.

/etc/config/uhttpd file:  
list listen\_http '[:,]:80'<- delete

# EHS6T LAN – Enkom Active Oy demo unit at Upseerinkatu 1, 5. floor electrical distribution cabinet

Trials to attack to the system each 3..4 minutes. (none successful, all trials through http)

OpenWrt Status System Network Logout

```
Tue Feb 14 13:10:49 2017 authpriv.info dropbear[28332]: Child connection from 221.194.44.195:43241
Tue Feb 14 13:10:55 2017 authpriv.info dropbear[28332]: Exit before auth: Disconnect received
Tue Feb 14 13:10:58 2017 authpriv.info dropbear[28333]: Child connection from 218.65.30.210:10348
Tue Feb 14 13:11:03 2017 authpriv.info dropbear[28333]: Exit before auth: Disconnect received
Tue Feb 14 13:11:24 2017 authpriv.info dropbear[28334]: Child connection from 116.31.116.25:23261
Tue Feb 14 13:11:29 2017 authpriv.info dropbear[28334]: Exit before auth: Disconnect received
Tue Feb 14 13:12:11 2017 authpriv.info dropbear[28335]: Child connection from 218.65.30.210:54341
Tue Feb 14 13:12:18 2017 authpriv.info dropbear[28336]: Child connection from 103.48.80.183:61193
Tue Feb 14 13:12:18 2017 authpriv.info dropbear[28335]: Exit before auth: Exited normally
Tue Feb 14 13:12:25 2017 authpriv.warn dropbear[28336]: Login attempt for nonexistent user from 103.48.80.183:61193
Tue Feb 14 13:12:26 2017 authpriv.warn dropbear[28336]: Login attempt for nonexistent user from 103.48.80.183:61193
Tue Feb 14 13:12:27 2017 authpriv.warn dropbear[28336]: Login attempt for nonexistent user from 103.48.80.183:61193
Tue Feb 14 13:12:28 2017 authpriv.info dropbear[28336]: Exit before auth: Exited normally
Tue Feb 14 13:12:46 2017 authpriv.info dropbear[28337]: Child connection from 116.31.116.25:19258
Tue Feb 14 13:12:51 2017 authpriv.info dropbear[28337]: Exit before auth: Disconnect received
Tue Feb 14 13:13:25 2017 authpriv.info dropbear[28338]: Child connection from 218.65.30.210:45187
Tue Feb 14 13:13:31 2017 authpriv.info dropbear[28338]: Exit before auth: Disconnect received
Tue Feb 14 13:14:08 2017 authpriv.info dropbear[28339]: Child connection from 116.31.116.25:35633
Tue Feb 14 13:14:13 2017 authpriv.info dropbear[28339]: Exit before auth: Disconnect received
Tue Feb 14 13:14:42 2017 authpriv.info dropbear[28340]: Child connection from 218.65.30.210:55187
Tue Feb 14 13:14:53 2017 authpriv.info dropbear[28340]: Exit before auth: Disconnect received
Tue Feb 14 13:15:29 2017 authpriv.info dropbear[28371]: Child connection from 116.31.116.25:20687
Tue Feb 14 13:15:32 2017 authpriv.info dropbear[28372]: Child connection from 81.209.12.162:62380
Tue Feb 14 13:15:35 2017 authpriv.info dropbear[28371]: Exit before auth: Exited normally
Tue Feb 14 13:16:02 2017 authpriv.info dropbear[28427]: Child connection from 218.65.30.210:41330
Tue Feb 14 13:16:07 2017 authpriv.notice dropbear[28372]: Pubkey auth succeeded for 'root' with key md5 20:23:5f:08:1c:70:3e:9f:1d:73:71:4f:f2:6e:52:35 from 81
Tue Feb 14 13:16:09 2017 authpriv.info dropbear[28427]: Exit before auth: Disconnect received
Tue Feb 14 13:16:51 2017 authpriv.info dropbear[28524]: Child connection from 116.31.116.25:36286
Tue Feb 14 13:16:57 2017 authpriv.info dropbear[28524]: Exit before auth: Disconnect received
Tue Feb 14 13:17:17 2017 authpriv.info dropbear[28570]: Child connection from 218.65.30.210:39794
Tue Feb 14 13:17:27 2017 authpriv.info dropbear[28570]: Exit before auth: Disconnect received
Tue Feb 14 13:18:00 2017 authpriv.info dropbear[28652]: Child connection from 81.209.12.162:62466
Tue Feb 14 13:18:09 2017 authpriv.warn dropbear[28652]: User 'fw' has invalid shell, rejected
Tue Feb 14 13:18:12 2017 authpriv.warn dropbear[28652]: User 'fw' has invalid shell, rejected
Tue Feb 14 13:18:15 2017 authpriv.info dropbear[28680]: Child connection from 116.31.116.25:27369
Tue Feb 14 13:18:20 2017 authpriv.info dropbear[28680]: Exit before auth: Exited normally
Tue Feb 14 13:18:22 2017 authpriv.warn dropbear[28652]: User 'fw' has invalid shell, rejected
Tue Feb 14 13:18:24 2017 authpriv.info dropbear[28652]: Exit before auth (user 'fw', 2 fails): Exited normally
Tue Feb 14 13:18:33 2017 authpriv.info dropbear[28708]: Child connection from 218.65.30.210:48078
Tue Feb 14 13:18:40 2017 authpriv.info dropbear[28708]: Exit before auth: Disconnect received
Tue Feb 14 13:19:34 2017 authpriv.info dropbear[28826]: Child connection from 116.31.116.25:42703
```

China  
China  
Vietnam  
China  
Finland 😊  
My own successful SSH-login

- please use non public M2M SIM Cards and own APN if possible
- Protect and encrypt the communication (SSL/TLS/http(s) and certificates)
- close http (port 80)

# EHS6T LAN – Enkom Active Oy demo unit at Upseerinkatu 1, 5. floor electrical distribution cabinet

HTTP(S) connection with Firefox browser to the Raritan voltage/current measurement system

Panel 1 (RK5.1.2.3.4.5BB\_OMA\_NIMI) | Circuit 4 (Asiakas1\_valaistus)

### Circuit Settings

Panel: Panel 1 (RK5.1.2.3.4.5BB\_OMA\_NIMI)  
Name: Asiakas1\_valaistus  
Circuit Type: Line-Neutral  
Circuit Rating: 60 A  
CT Rating: 60 A

Setup Delete Circuit

### Sensors

Type	Value	State
RMS Current	0.11 A	normal
RMS Voltage	235.1 V	
Phase Angle	15.4 °	normal
Active Power	17 W	normal
Reactive Power	5 var	normal
Apparent Power	27 VA	normal
Power Factor	0.65	normal
Displacement Power Factor	0.96	normal
Active Energy	149377 Wh	normal

Reset Active Energy

Real time electricity consumption through an EHS6T LAN terminal