SATELLAR DIGITAL SYSTEM
PART II: CENTRAL UNIT
USER GUIDE VERSION 1.5

USER GUIDE

WIRELESS WORLD – LOCAL SOLUTION

SATEL

SATEL

Contents

Important notice

All rights to this manual are owned solely by SATEL OY (referred to in this user guide as SATEL). All rights reserved. The copying of this manual (without written permission from the owner) by printing, copying, recording or by any other means, or the full or partial translation of the manual to any other language, including all programming languages, using any electrical, mechanical, magnetic, optical, manual or other methods or devices is forbidden.

SATEL reserves the right to change the technical specifications or functions of its products, or to discontinue the manufacture of any of its products or to discontinue the support of any of its products, without any written announcement and urges its customers to ensure that the information at their disposal is valid.

SATEL software and programs are delivered ”as is”. The manufacturer does not grant any kind of warranty including guarantees on suitability and applicability to a certain application. Under no circumstances is the manufacturer or the developer of a program responsible for any possible damages caused by the use of a program. The names of the programs as well as all copyrights relating to the programs are the sole property of SATEL. Any transfer, licensing to a third party, leasing, renting, transportation, copying, editing, translating, modifying into another programming language or reverse engineering for any intent is forbidden without the written consent of SATEL.

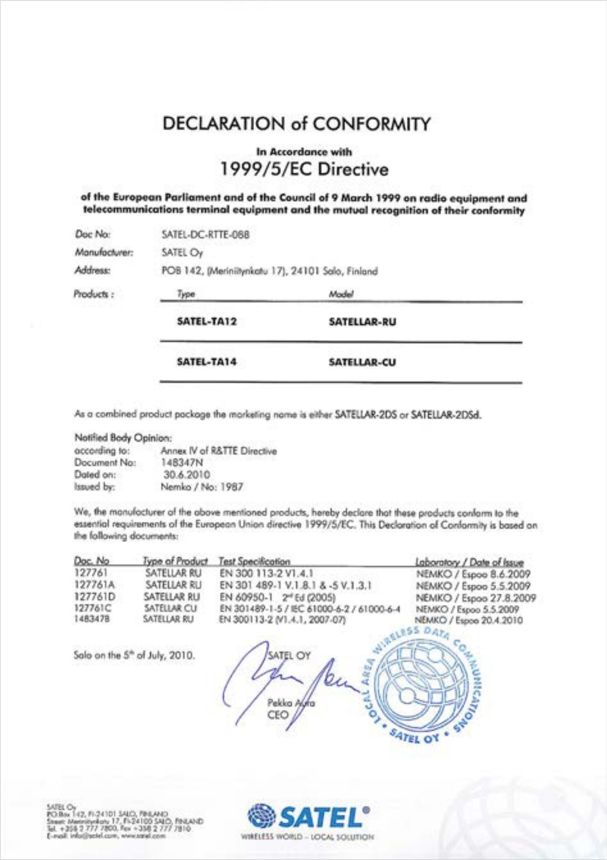
SATEL PRODUCTS HAVE NOT BEEN DESIGNED, INTENDED NOR INSPECTED TO BE USED IN ANY LIFE SUPPORT - RELATED DEVICE OR SYSTEM - RELATED FUNCTION NOR AS A PART OF ANY OTHER CRITICAL SYSTEM AND ARE GRANTED NO FUNCTIONAL WARRANTY IF THEY ARE USED IN ANY OF THE APPLICATIONS MENTIONED.

Salo, Finland 2015

Product conformity

SATELLAR CU

SATEL Oy hereby declares that SATELLAR Central Unit is in compliance with the essential requirements (electromagnetic compatibility and electrical safety) and other relevant provisions of Directive 1999/5/EC. Therefore the equipment is labelled with the following CE-marking.



DECLARATION of CONFORMITY

In Accordance with

1999/5/EC Directive

of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity

Doc No: SATEL-DC-RTTE-088

Manufacturer: SATEL Oy

Address: POB 142, (Meriniitynkatu 17), 24101 Salo, Finland

Products :

Type	Model
SATEL-TA12	**SATELLAR-RU**
SATEL-TA14	**SATELLAR-CU**

As a combined product package the marketing name is either SATELLAR-2DS or SATELLAR-2DSd.

Notified Body Opinion:
according to: Annex IV of R&TTE Directive
Document No: 148347N
Dated on: 30.6.2010
Issued by: Nemko / No: 1987

We, the manufacturer of the above mentioned products, hereby declare that these products conform to the essential requirements of the European Union directive 1999/5/EC. This Declaration of Conformity is based on the following documents:

Doc. No	Type of Product	Test Specification	Laboratory / Date of Issue
127761	SATELLAR RU	EN 300 113-2 V1.4.1	NEMKO / Espoo 8.6.2009
127761A	SATELLAR RU	EN 301 489-1 V.1.8.1 & -5 V.1.3.1	NEMKO / Espoo 5.5.2009
127761D	SATELLAR RU	EN 60950-1 2nd Ed (2005)	NEMKO / Espoo 27.8.2009
127761C	SATELLAR CU	EN 301489-1-5 / IEC 61000-6-2 / 61000-6-4	NEMKO / Espoo 5.5.2009
148347B	SATELLAR RU	EN 300113-2 (V1.4.1, 2007-07)	NEMKO / Espoo 20.4.2010

Salo on the 5th of July, 2010.

SATEL OY

Pekka Aura
CEO

LOCAL AREA WIRELESS DATA COMMUNICATIONS • SATEL OY •

SATEL Oy
PO Box 142, FI-24101 SALO, FINLAND
Street: Meriniitynkatu 17, FI-24100 SALO, FINLAND
Tel. +358 2 777 7800, Fax +358 2 777 7810
E-mail: info@satel.com, www.satel.com

SATEL®
WIRELESS WORLD – LOCAL SOLUTION

Warranty and safety instructions

Read these safety instructions carefully before using the product:

- The warranty will be void if the product is used in any way that is in contradiction with the instructions given in this manual, or if the housing of the radio modem has been opened or tampered with.
- The devices mentioned in this manual are to be used only according to the instructions described in this manual. Faultless and safe operation of the devices can be guaranteed only if the transport, storage, operation and handling of the device is appropriate. This also applies to the maintenance of the products.
- To prevent damage the Central Unit (referred to in this user guide as CU) must always be switched OFF before connecting or disconnecting the serial connection cable. It should be ascertained that different devices used have the same ground potential. Before connecting any power cables the output voltage of the power supply should be checked.
- To be protected against all verified adverse effects the separation distance of at least 44 cm must be maintained between the antenna of SATELLAR radio modems and all persons.

1. Introduction to the SATELLAR product family

SATELLAR is a new generation narrow band radio modem that consists of separate units:

- Central unit (CU)
- Radio units 1W, 5W and 10W (RU)
- Expansion units (XU)

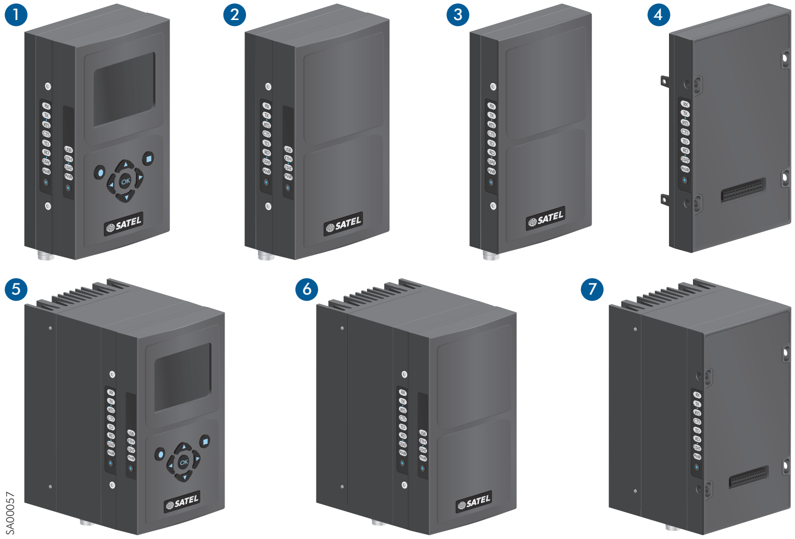


Figure 1.1 SATELLAR product family:

1. SATELLAR-2DS: Central unit (CU) with display and keypad + radio unit (RU), 1 W
2. SATELLAR-2DS: Central unit (CU) without display and keypad + + radio unit (RU), 1 W
3. SATELLAR-1DS: Radio unit (RU), 1 W
4. Expansion unit, to be added between radio and central unit
5. SATELLAR-20DS / -25DS with display:
Central unit (CU) with display and keypad + radio unit (RU), 10 W (-20DS) or 5 W (-25DS)
6. SATELLAR-20DS / -25DS without display:
Central unit (CU) w/o display and keypad + radio unit (RU), 10 W (-20DS) or 5 W (-25DS)
7. SATELLAR-10DS / -15DS: Radio unit (RU), 10 W (-10DS) or 5 W (-15DS)

Using SATELLAR the customer builds an own independent radio data communication network. This document presents the specifications and usage of the CU. The properties of other units are described in the extent, which is necessary to read in order to understand the operation of the CU.

Data communication

SATELLAR operates either as a transparent radio link, essentially replacing a wire, for classic RS-232, RS-485 or RS-422 based protocols, or as a wireless router in an IP-based network. Using SATELLAR many network topologies are possible, everything from a point-to-point connection to a nationwide chain with multiple branches.

Range

With SATELLAR the communication range of a point to point link is typically longer than 10 km in urban conditions (some obstacles in the line of sight), and longer than 20 km in ideal line of sight conditions. The range can be further extended using high gain antennas, booster modules and radio repeaters.

Security

Data security is often a concern when using radio communication. In SATELLAR a 128-bit encryption on the air-interface ensures privacy in the radio network.

Display and keypad

The CU is available with or without a display and keypad. The size of the display is 2.4 ", resolution is 320 x 240 pixels, and the amount of colors is 65k. The keypad has seven buttons: left, right, up, and down arrows, OK button, and two software defined buttons.

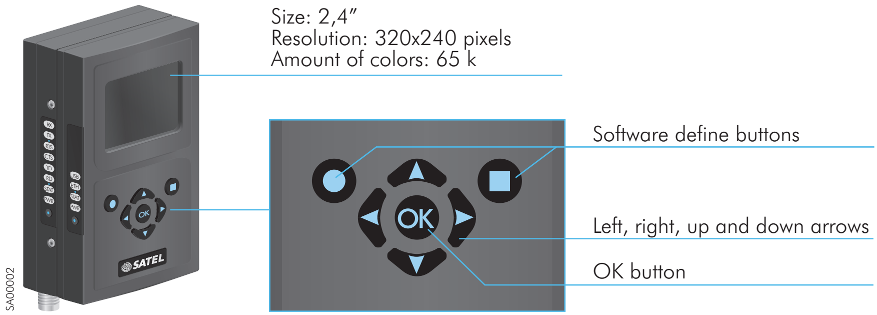


Figure 1.2 Display and keypad

Diagnostics and configuration

Radio modems are often used in applications where reliability and independence are key properties. To support this demand, SATELLAR has built-in diagnostic and remote configuration features.

Local use

The status of the CU can be seen from the LED indicators, which are located on the other narrow side of the unit. More detailed information is available using the graphical user interface with a QVGA display and 7 pushbuttons.

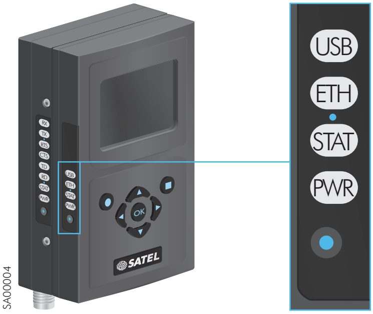


Figure 1.3 The status of the CU can be seen from the LED indicators

Remote use

Once deployed, status monitoring and configuration can be performed using one of the following methods:

1. The SATELLAR CU provides WWW pages for configuration and diagnostic, accessible using IP connectivity (the Ethernet interface of the CU)

2. Using the Windows based SATEL NMS PC software through the serial data interface of the RU, the USB device port of the CU, or TCP/IP port 55555 of the CU. (Check SW availability from SATEL)

SATELLAR can also be accessed over the air by the methods described above.

Flexible and expandable

SATELLAR concept has been designed to be flexible and expandable both in terms of hardware and software functions.

Software

In the RU the modulation method, channel spacing (i.e. air interface data rate), and forward error correction can be selected by changing the modem settings by software. Also the RF output power can be set.

Hardware

Due to the modular mechanical structure of SATELLAR, it is possible to add hardware expansion units. The idea is that this could be done as an update after the initial deployment. At the moment, however, the RU does not support the update. Schedule for this will be informed later.

USB host and device connectors offer a possibility to connect commercially available USB devices like Bluetooth and WLAN modules to the modem or e.g. to show the modem as an external memory device to the PC.

Ruggedized

SATELLAR is constructed of die-cast aluminum to withstand the abuse typical to rough industrial environments. It operates over a wide temperature range and under severe vibration conditions to meet the requirements of vehicular and process industry applications.

1.1 Mounting

SATELLAR can be mounted directly on a flat surface or to a DIN rail. When mounting on the flat surface, two-piece mounting clips can be used. The mounting clips are delivered in the basic sales package. DIN-rail mounting is possible either on the backside of the stack of different SATELLAR Units or on the other narrow side of each unit (the latter case so that the LED indicators remain visible for the user). The DIN-rail mounting clips have to be ordered separately.

NOTE!

1. The equipment must be installed in restricted access location due to high touch temperatures of metal enclosure.
2. The screen of coaxial antenna cable must be grounded to protect from over voltages from outdoor antenna.

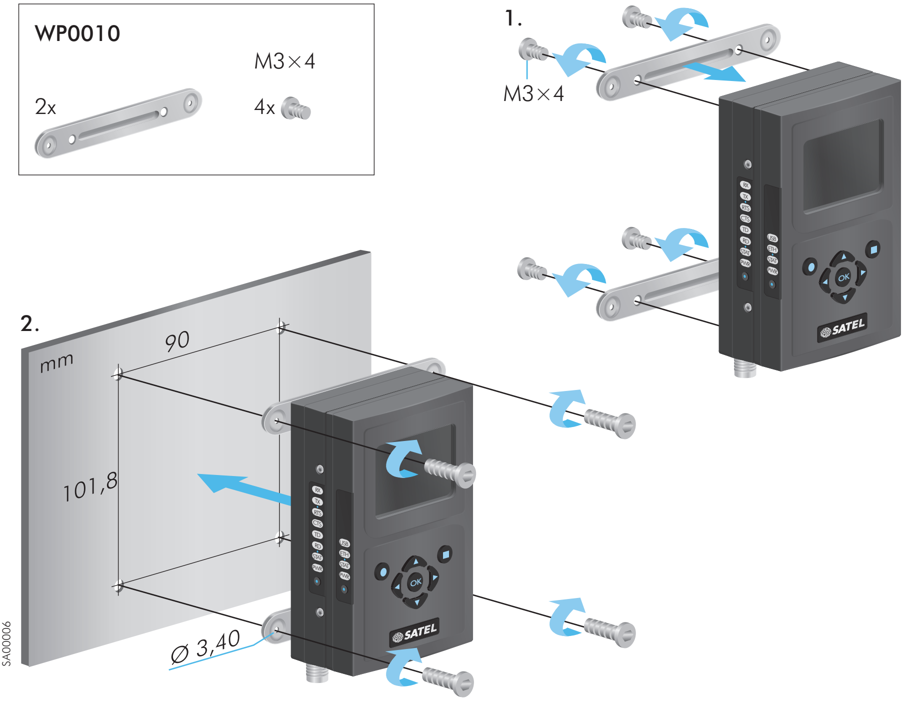


Figure 1.4 SATELLAR-2DS, mounting on flat surface with mounting clips (includes in the delivery)

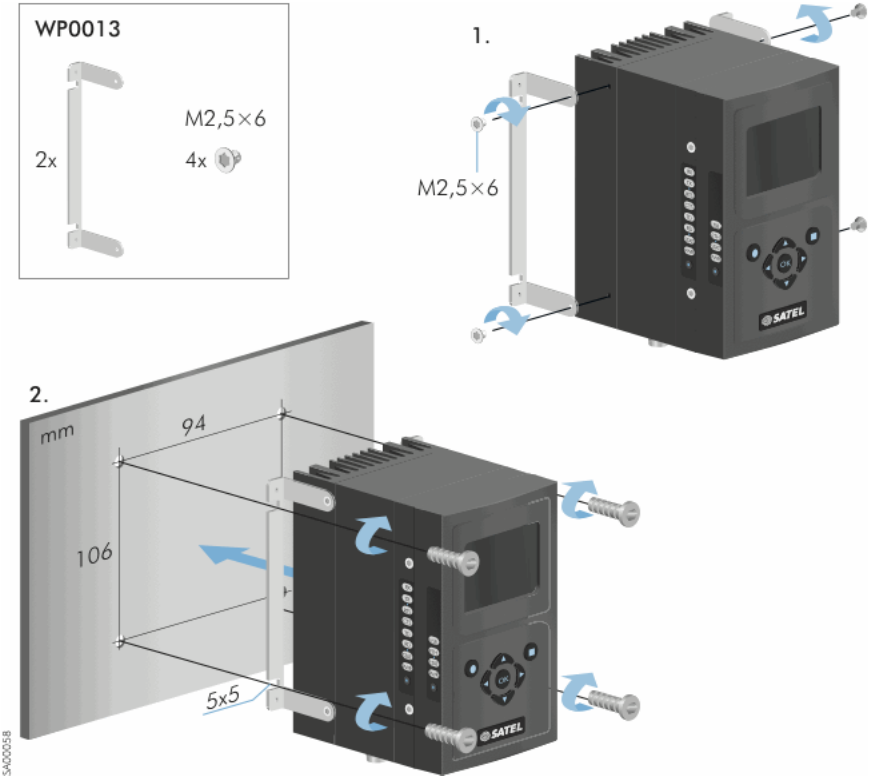


Figure 1.5 SATELLAR-20DS or -25DS, mounting on flat surface with mounting clips (included in the delivery)

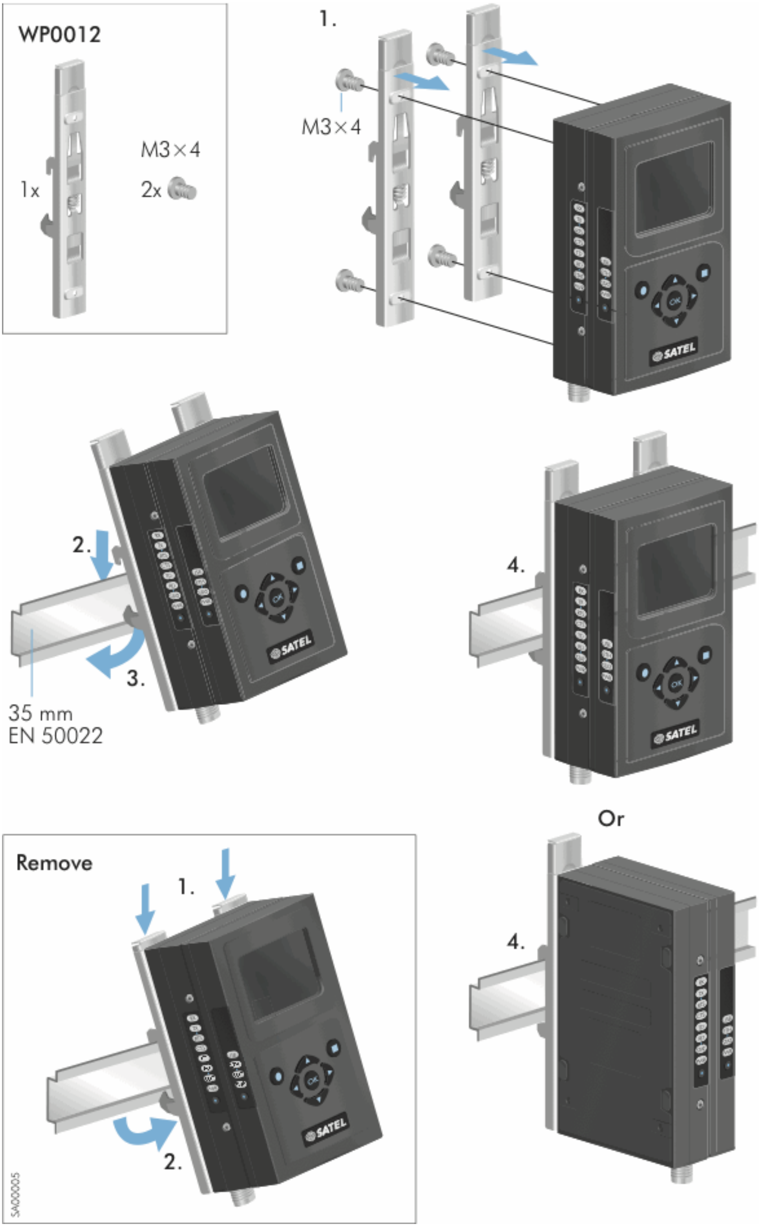


Figure 1.6 SATELLAR-2DS, mounting on the DIN-rail with mounting clips (to be ordered separately)

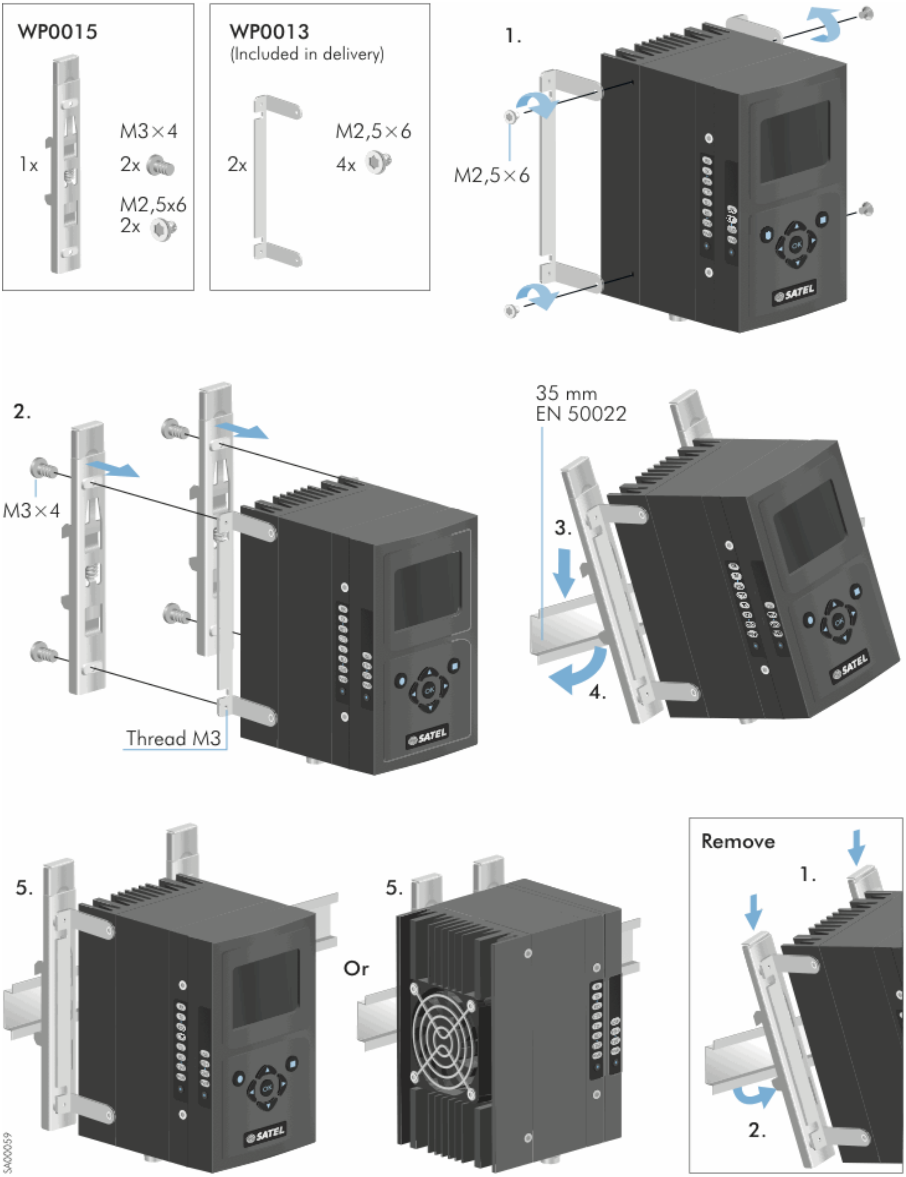


Figure 1.7 SATELLAR-20DS or -25DS, mounting on the DIN-rail with mounting clips (to be ordered separately). Please note that the fan is only in version SATELLINE-20DS.

2. Technical specifications

Electrical

CPU	ARM 9 @ approx. 200 MHz
RAM	64 MB
ROM	128 MB
Display	2.4 ”, 320 x 240 pixel resolution, 65 k colours
Keypad	up, down, left, right, OK (select), and two SW defined keys
Power consumption (no USB device connected)	2.0 W with the display 1.4 W without the display
USB interfaces	USB-host & USB-device USB2.0 high speed
Ethernet interface	10/100 Mbps Ethernet RJ-45 with Auto-MDIX
Start time from power on	For CU/RU combination: 65 s until IP communication works (locally and over the air). 130 s until LCD/GUI works.

Mechanical and environmental

Mechanical dimensions	130 x 21.7 x 76.5 mm
Weight	260 g
Temperature ranges	-25 - +55 deg °C, complies with the standards -30 - +75 deg °C, functional -40 - +85 deg °C, storage
Humidity	< 95 % @ 25 deg °C, non-condensing
Vibration	At least 10 – 500 Hz/5g without degradation in data transfer capability
Shock resistivity	Dropping height 1 m, all directions
IP rating	IP 52
Mounting:	DIN rail (side or back), two piece mounting clip, or directly on flat surface

Standards compliance

Emissions	IEC 61600-6-4
Immunity	IEC 61000-6-2
ESD	IEC 61000-4-2 level 4 for external connections EIC 61000-4-2 level 2 for internal unit-to-unit connector
RoHS	2002/95/EC

Table 2.1 SATELLAR Central Unit technical specifications

3. Typical setup

The figure below shows a typical setup when transferring IP data through the CU. When using the RU together with the CU the recommended minimum distance between the antenna and CU is 2 m in order to avoid degradation of the receiver sensitivity due to interference from the CU.

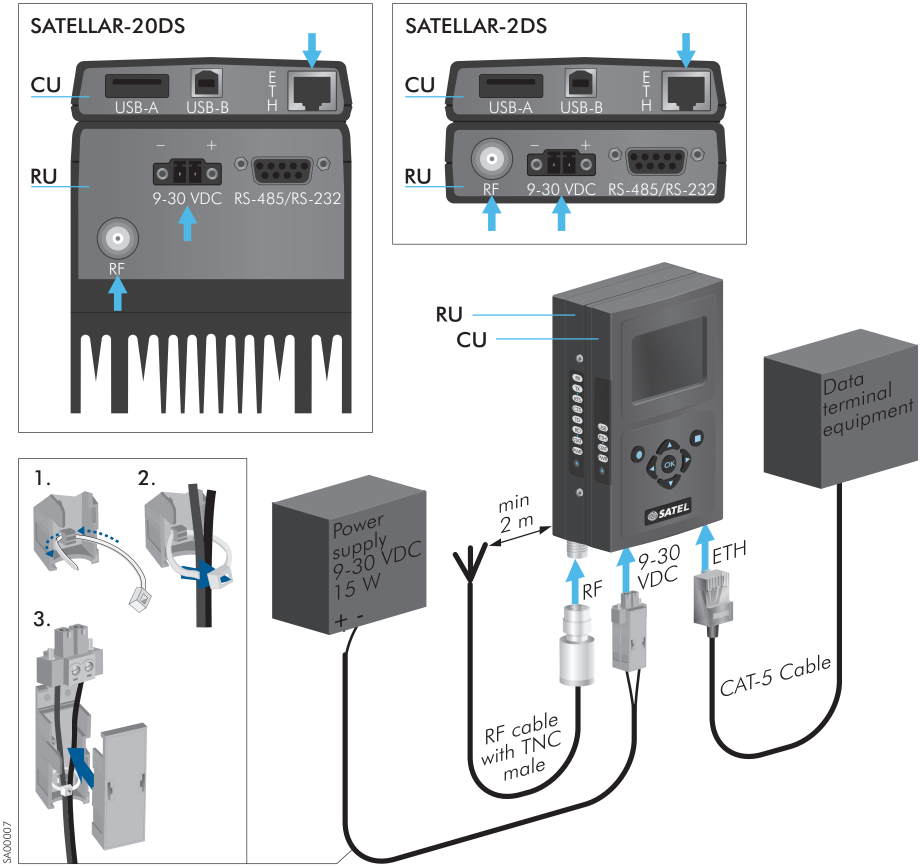


Figure 3.1 Transferring IP data through the CU, cabling

4. Mechanical assembly, modular construction

The expansion unit XU is attached between RU and CU as described in the Figure 4.1.

First remove the CU and RU from each other, see the figure. Take the rubber cover from the unit-to-unit connector of the XU. Modular constraction allows you to connect the expansion unit XU between RU and CU units. Align the tabs of the CU with the mounting holes of the XU and press the units together, and do the same between RU unit and XU+CU units. Finally, tighten the connections with the screws. Now the combination can be mounted either by DIN rail adapters or by a two-piece mounting clip.

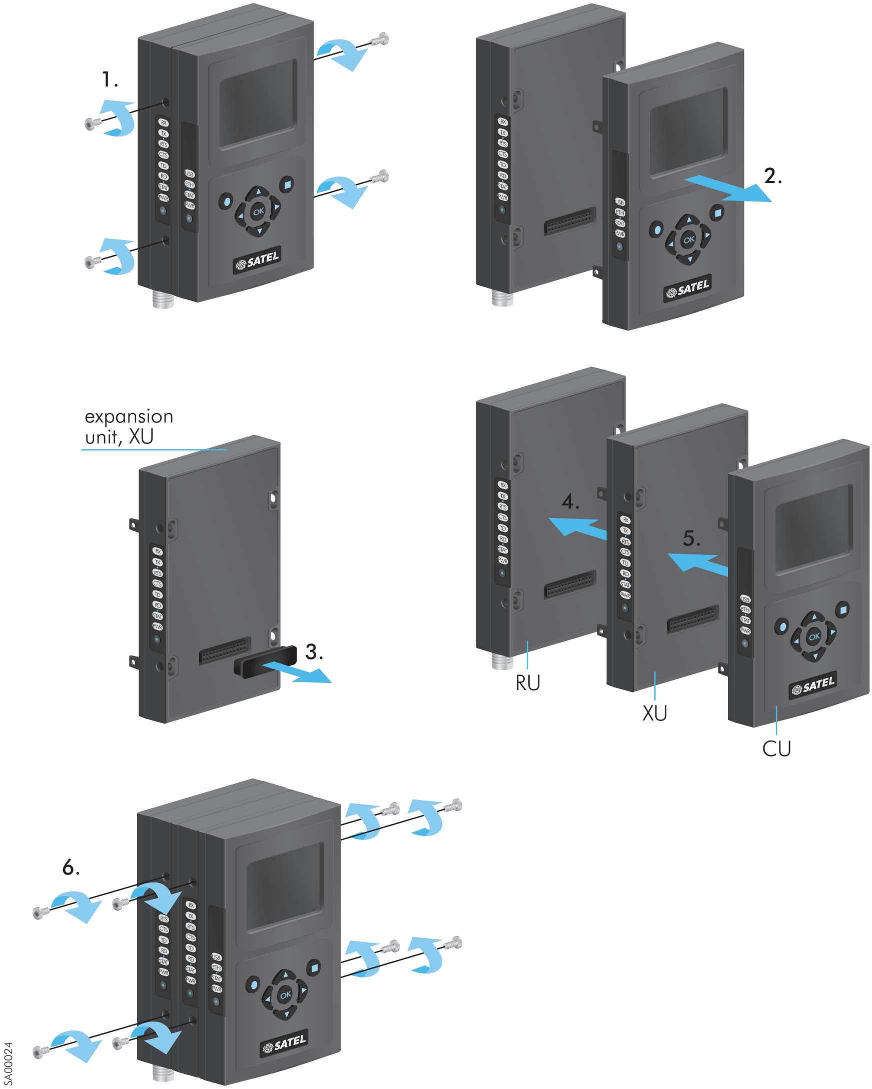
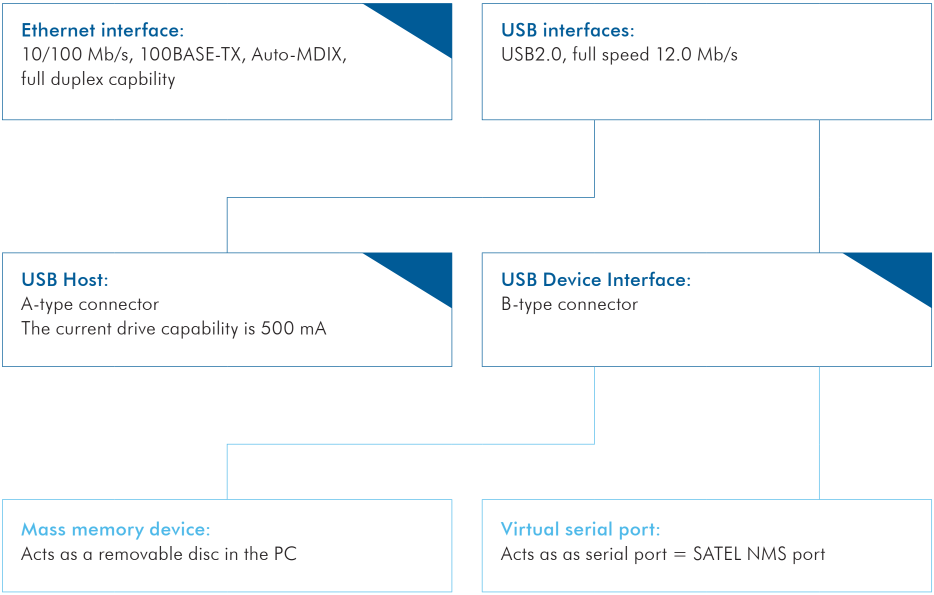


Figure 4.1 Modular construction, mounting of the expansion unit XU

5. Interfaces

The CU offers three data interfaces: Ethernet, USB host and USB device. LED indicator shows the status of the unit and graphical user interface can be used to check and change device settings and to see the diagnostics data.



Ethernet interface:
10/100 Mb/s, 100BASE-TX, Auto-MDIX,
full duplex capbility

USB interfaces:
USB2.0, full speed 12.0 Mb/s

USB Host:
A-type connector
The current drive capability is 500 mA

USB Device Interface:
B-type connector

Mass memory device:
Acts as a removable disc in the PC

Virtual serial port:
Acts as as serial port = SATEL NMS port

Figure 5.1 Three data interfaces: Ethernet, USB host and USB device

5.1 Ethernet

Ethernet interface is 10/100 Mb/s 100BASE-TX with Auto-MDIX and full-duplex capability.

5.2 USB

The USB interfaces support USB2.0 Full Speed (12.0 Mb/s) data rates. Both USB host and device interfaces are available. For USB host the A type connector is used and for USB device the connector is B type. The current drive capability of the USB host interface is 500 mA. The USB device interface has two modes: Mass memory device and Virtual serial port. The mode can be selected in Modem Settings, General category and in addition by the function button as described in chapter 5.5.

In the Mass memory device -mode a PC can be connected to the USB device interface and SATELLAR acts as a Removable Disc in the PC. The removable disk contains copies of system log files, which can be copied to the PC. Update files can be copied to the removable disk and be used in the Firmware Updater (see chapter 8.3). Any other files copied to the removable disk are removed when the cable is disconnected.

In Virtual serial port -mode, the USB port acts as a serial port. When the USB port is connected to a PC, the virtual serial port device is created in the PC. This virtual port appears to windows as a normal serial port: the only difference is that an actual D9 connector is not used. This allows programs to connect to serial ports in order to access the CU via the USB connection.

Windows PC requires a special driver, available from SATEL. The Virtual Serial port acts as a SATEL NMS port, allowing a program such as SATEL NMS PC to be used to change the settings of SATELLAR.

5.3 Diagnostics, monitoring, changing settings

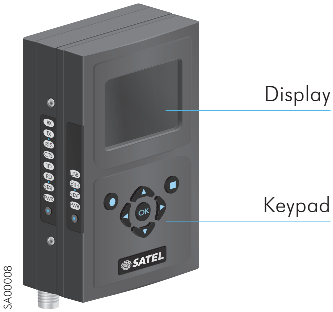
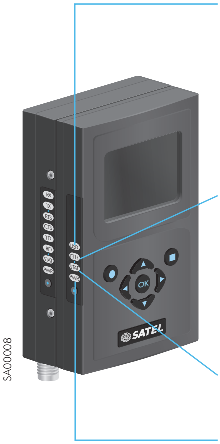


Figure 5.2 Display and keypad

CU equipped with a display and keypad offers an easy way to check or change device settings and see diagnostics information. The same is possible using the Web interface of the CU or SATEL NMS PC SW. Graphical user interface is explained more in chapter 5.6 and the PC SW is described in its own user manual.

5.4 LED indicators

The CU provides four LED indicators that are located on one of the narrow sides of the unit. They are listed and described in the table below.



LED Label	Status	Description
USB	OFF	USB host disabled
	ON	USB host enabled, USB device detected
	Blinking (0.25 s interval)	USB host enabled, no USB device detected
	Blinking (0.50 s interval)	USB device setting override using function button, see chapter 5.5
	Blinking (1.0 s interval)	USB is a mass memory device
ETH	OFF	Ethernet port disabled
	ON	Ethernet port enabled and connected
	Blinking (0.25 s interval)	Ethernet port enabled but not connected or operational
	Blinking (0.50 s interval)	Ethernet port setting override using function button, see chapter 5.5
STAT	ON	Normal operation mode
	Blinking (0.25 s interval)	Device is starting up
PWR	OFF	Device is powered off
	ON	Device is powered on

Table 5.1 LED indicators

NOTE: In normal operation the USB LED indicates the status of the USB host interface. When operating with the function button (chapter 5.5), the USB LED refers to the state changes in the USB device interface.

5.5 Function button

The function button is located below the LED indicators. It is used to control the operation of the USB device and Ethernet interfaces as described below. The CU must be allowed to boot up completely before the button will work.

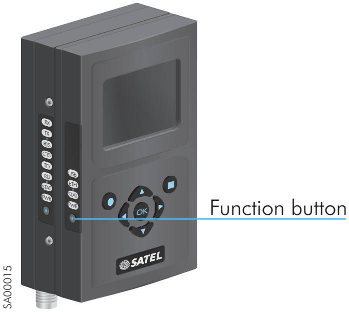


Figure 5.3 Location of the Function button

When the button is pressed for more than a second, all the LEDs turn on indicating the start of the process. The effect depends on how long the button is kept depressed, and is indicated by turning the LEDs off one by one. When the LEDs indicate the desired function, release the button. After the button has been released, press the button once more quickly (less than a second) to finish the operation.

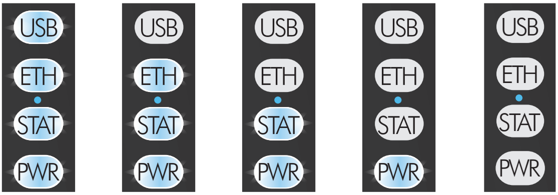


Figure 5.4 LED indications, see the Table 5.2

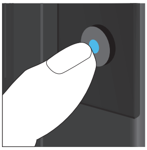
Action	Length of press [seconds]	LED indication		Effect
	1 to 2	All LEDs ON.	● ● ● ●	The USB device and Ethernet interface settings are reset to states defined by user settings.
	2 to 4	The uppermost LED (USB) is switched off.	○ ● ● ●	The USB device setting is changed so that if the user setting is Mass memory device, the setting changes to Virtual serial port and vice versa. Thereafter the USB LED starts to blink until the setting is reset to the original value. Blinking interval is 0.5 seconds if the new device setting is Virtual serial port and 1.0 seconds if the setting is Mass memory device.
	4 to 6	The next lower LED (ETH) is switched off.	○ ○ ● ●	The CU IP address settings are changed. Thereafter the IP address is 192.168.1.1, the net mask is 255.255.255.0, and DHCP is switched to off mode. The ETH LED blinks until the setting is reset to the original value. Blinking interval is 0.5 seconds.
	6 to 8	The next lower LED (STAT) is switched off.	○ ○ ○ ●	No specific operation defined.
	8 to 10	The fourth LED (PWR) is switched off.	○ ○ ○ ○	All the LEDs start to blink rapidly until the MCU restarts. SATELLAR CU then reboots.
	> 10	All LEDs ON.	● ● ● ●	
	> 20	All LEDs turn ON and remain on even if the button is kept down.		The selection process starts from the beginning (11 to 12 seconds counts as 1 to 2 seconds etc.).

Table 5.2 Function button operation

5.6 Graphical user interface

In SATELLAR device equipped with LCD display and keypad, GUI can be used to change settings and access the various applications.

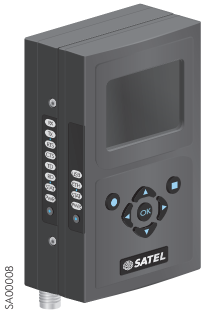
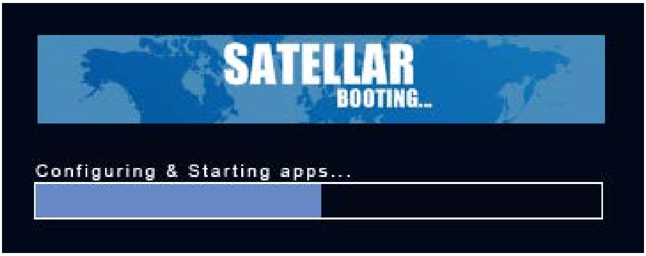


Figure 5.5 Central Unit equipped with LCD display and keypad

5.6.1 Booting screen

This screen is visible while the CU is starting up.



Configuring & Starting apps...

5.6.2 LCD display, information and button menu areas

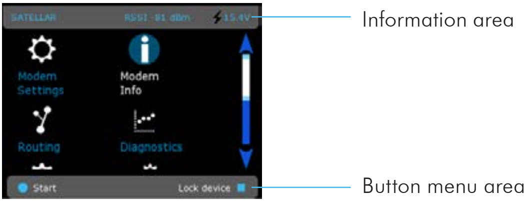


Figure 5.6 Information and button menu areas

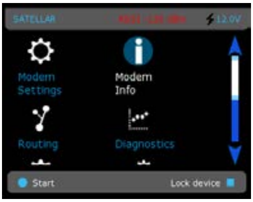


Figure 5.7 Red font indicating a value lower than the defined threshold

The top of the screen is the Information area. The following information is available (From left to right).

- Modem name: Default value is “SATELLAR”. It can be changed in Modem Settings, General category (see chapter 7.1.2).
- Current date and time, if enabled (see chapter 7.1.6)
- RSSI value: The signal level of the last received message. If no message has been received in the last 5 seconds, the value is set to -128. If the reading is lower than the defined minimum threshold value, this value is shown with red font. The threshold can be set in Modems Settings, General category (see chapter 7.1.2).
- Voltage reading. A numeric value or a voltage bar depending on the setting in Modem Settings, General category (see chapter 7.1.2).

On the bottom of the screen is the button menu area operated by software defined keypad buttons. The left (round) button command is displayed on the left bottom corner of the screen and the right (square) button command on the bottom right corner of the screen.

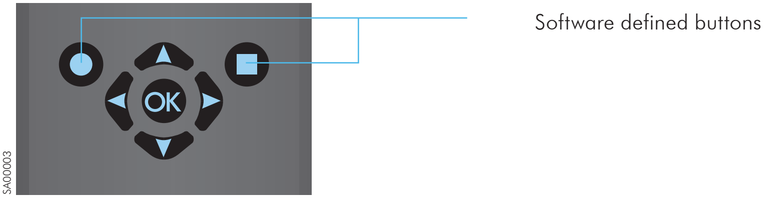


Figure 5.8 Software defined buttons on keypad

5.6.3 Main menu

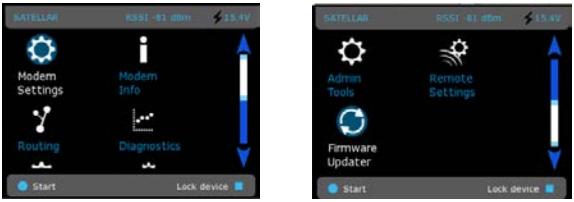


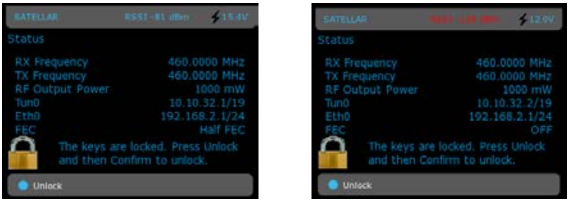
Figure 5.9 Main menu view

This menu screen contains icons which can be used to start the different applications.

- Modem Settings: See chapter 7.1
- Modem Info: See chapter 7.2
- Routing: See chapter 7.3
- Diagnostics: See chapter 8.1
- Admin Tools: See chapter 8.8
- Remote settings: See chapter 8.4
- Firmware updater: See chapter 8.3

To start an application, use the cursor keys to select the icon and press the round button or OK button.

5.6.4 Status screen



```
Status
 RX Frequency        460.0000 MHz
 TX Frequency        460.0000 MHz
 RF Output Power          1000 mW
 Tun0                10.10.32.1/19
 Eth0               192.168.2.1/24
 FEC                      Half FEC
     The keys are locked. Press Unlock
     and then Confirm to unlock.
```

```
Status
 RX Frequency        460.0000 MHz
 TX Frequency        460.0000 MHz
 RF Output Power          1000 mW
 Tun0                10.10.32.2/19
 Eth0               192.168.2.1/24
 FEC                           OFF
     The keys are locked. Press Unlock
     and then Confirm to unlock.
```

Figure 5.10 Status screen view

If “Lock Screen” command is given in main menu, or the defined time passes without keyboard input, the screen goes to the status/lock screen mode.

In this screen some basic status values are displayed.

- RX Frequency
- TX Frequency
- RF Output Power
- Tun0 IP Address
- Eth0 IP Address
- Forward Error Correction (FEC) mode

No input is allowed in this screen, except to unlock the screen. To do this, follow the instruction on screen. If PIN code has been enabled, the correct code must be entered to unlock.

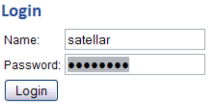
5.6.5 Screen save mode

After a timeout set in Modem Settings, General category (see chapter 7.1.2), the display is turned off. When any button is pressed, the Status screen is displayed and the UI can be unlocked as normal.

5.7 WWW User interface

This interface can be used with a web browser application, such as Mozilla Firefox. The url to access the WWW -page is *http://<modem's IP address>*. By default this is *http://192.168.1.1.* If the current IP address is unknown, it can be forced to 192.168.1.1 by using the function button as explained in chapter 5.5, or using the Graphical user interface, if present. The WWW interface can also be used across the radio link, once routes have been set (see chapter 6). In this case either of the IP addresses defined can be used (both the eth0 and tun0 addresses work).

5.7.1 Login



Login

Name: satellar

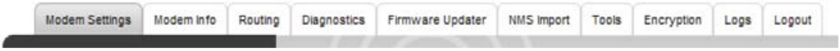
Password: ●●●●●●●●

The first screen of the WWW interface is the login screen. The user name is *satellar* and the default password is *Satel123*. (The password can be changed in settings, see chapter 7.1.2)

You can also log in using the name *admin* and default password is *Satel456*. In this case an additional application called Administration is available, see chapter 8.8.

5.7.2 Main menu

The main menu lists all the "applications" available in the WWW interface. An additional Administration tab is available when logged in with user name *admin* as explained in chapter 5.7.1.

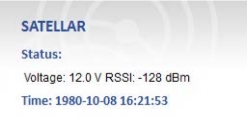


5.7.3 Status area

The area immediately below the main menu shows the name of the radio station (settable in the General Settings category, see chapter 7.1.2). Current status information is also available:

- Voltage
- Received signal strength (RSSI)
- Current system time

More status information may be visible depending on the firmware versions installed.



SATELLAR

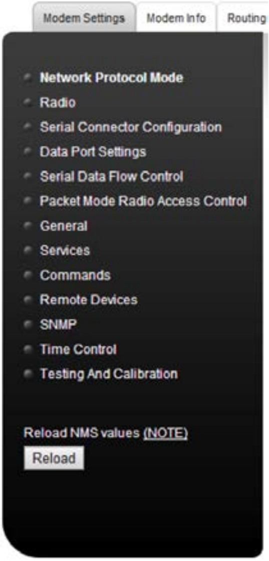
Status:

Voltage: 12.0 V RSSI: -128 dBm

Time: 1980-10-08 16:21:53

5.7.4 Categories list

Once a Main menu application (see chapter 5.7.2) is selected, the categories related to that application are listed in the dark grey area on the left. The category labels can be clicked to open the category page, which contain settings and information related to that category. More details about categories can be found beginning from chapter 7.

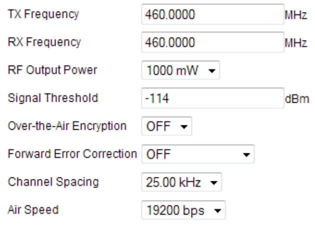


There is also one button in the category area: Reload NMS values. It can be used to force a reload of settings from the RU and CU settings databases to be dipalyed on the WWW User Interface.

Loading operation takes several minutes, so it should only be used if some of the settings seems to be incorrectly displayed.

5.7.5 Category page

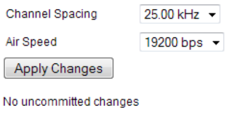
This area to the right of Categories list shows the contents of the currently selected category. It contains settings or other information.



TX Frequency	460.0000 MHz
RX Frequency	460.0000 MHz
RF Output Power	1000 mW
Signal Threshold	-114 dBm
Over-the-Air Encryption	OFF
Forward Error Correction	OFF
Channel Spacing	25.00 kHz
Air Speed	19200 bps

5.7.6 Changing settings

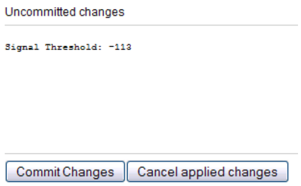
When changing settings in the WWW interface, select first the correct application and category, then change the desired settings found on the category page. Finally click the Apply Changes button.



Channel Spacing	25.00 kHz
Air Speed	19200 bps

No uncommitted changes

Some settings are text or numbers which can be changed by typing, while others are drop down lists, allowing you to select from a few choices. Any changes you make are lost if you change the category or application without clicking the Apply Changes -button.



Uncommitted changes

```
Signal Threshold: -113
```

When the Apply Changes button is clicked, all changes on the current page are added to the list of uncommitted changes. You can then navigate to another page and Apply more changes, which are also added to the list. When you have finished making changes, store and take the new settings into use by clicking the Commit Changes button. You can also discard all applied changes by clicking the Cancel applied changes button. In this case all settings are removed from the list of uncommitted changes and all settings of all units remain as they were.

When Commit Changes is clicked, the CU will store settings into the settings database and the Radio Unit, and restart all necessary Linux processes. Therefore the committing process may take a relatively long time, sometimes up to a minute.

NOTE: If the IP Address has been changed, the browser will be automatically redirected to the new address, but in case the network address part of the IP address has changed, you'll need to modify your computer's IP settings so that it is again in the same LAN as the modem to be able to continue using the WWW interface.

5.8 SATEL NMS

SATEL NMS is a Network Management System. Devices that support SATEL NMS can be configured and monitored using external software provided by SATEL. One such program is SATEL NMS PC. Configuration and monitoring can be performed either locally using a cable, or remotely via a radio link.

The SATELLAR Central Unit supports SATEL NMS, and provides the following features.
Connection options:

- Connect via TCP/IP Port 55555
- Connect via USB Device port when the USB port is in Virtual Serial port mode. (See chapters 5.2 and 7.1.2 for details)
- Remote connection via radio network is available when the routing settings are correctly defined.

Most settings available via the User Interfaces of the CU are also accessible using SATEL NMS. For this purpose, the NMSID (Network Management System IDentifier) as well as Sub-Unit number of each setting is listed in this manual, see chapter 7. The NMSIDs are also used by the NMS Import application (see chapter 8.5).

Note that the NMS Address of the CU is the same as the RMAC Address of the attached Radio Unit. See the Radio Unit user manual for details.

5.9 SSH

SATELLAR's linux command line can be accessed using the SSH protocol. To do this you need a SSH client, such as putty.exe. The user name is *satellar* and the password is *Satel123*.

6. Data transmission

The CU is used to transfer data over the IP protocol. Multiple IP protocols are supported, such as TCP/IP, UDP and ICMP. A prerequisite for wireless IP transmission is that the RU is configured to packet routing protocol mode as explained in the RU user manual.

6.1 Internet protocol

Each CU has an IP address belonging to the Local Area Network (LAN) to which they are connected via their Ethernet interface. Each CU also has another IP address belonging to a second LAN, the SATELLAR RU LAN. This LAN is formed by the radio protocol. These two interfaces are called eth0 and tun0 according to standard Linux naming conventions. The CU acts as an IP router device, routing IP packets between its Ethernet interface (eth0) and the radio network provided by SATELLAR RUs (tun0).

6.1.1 Example

In the Figure 6.1 shown on the next page is presented a network which has three (3) data terminal equipment devices (DTEs) connected to CU through Ethernet. Each CU is connected to a RU, together forming a SATELLAR-2DSd Radio Station (in this case RU type is: 1 W, with display and keypad). In addition there are two standalone RUs acting as repeater stations. Each of the stations has a unique station address (RMAC) which is a number freely selectable in the range of 1 … 4094. The station addresses are used at the radio protocol level when sending messages through the radio path. (The radio protocol is explained in the RU user manual.)

Each DTE belongs to a LAN on the eth0 interface of a SATELLAR. To be able to communicate with each other, IP routing must be correctly configured in each DTE and each SATELLAR.

How the station addresses are used for routing the data through the radio path, is explained in the RU user manual. This is called Packet Routing. For the network topology seen on Figure 6.1 the Packet Routes routing table looks like the following:

Radio unit	Next hop (neighbor)	Addresses behind (remotes)
A	2	3, 4, 5
B	3	1, 2, 5
C	3	1, 2, 4
D	1	-
	3	4, 5
E	2	1
	4	-
	5	-

Table 6.1 Packet Routes routing table for Figure 6.1

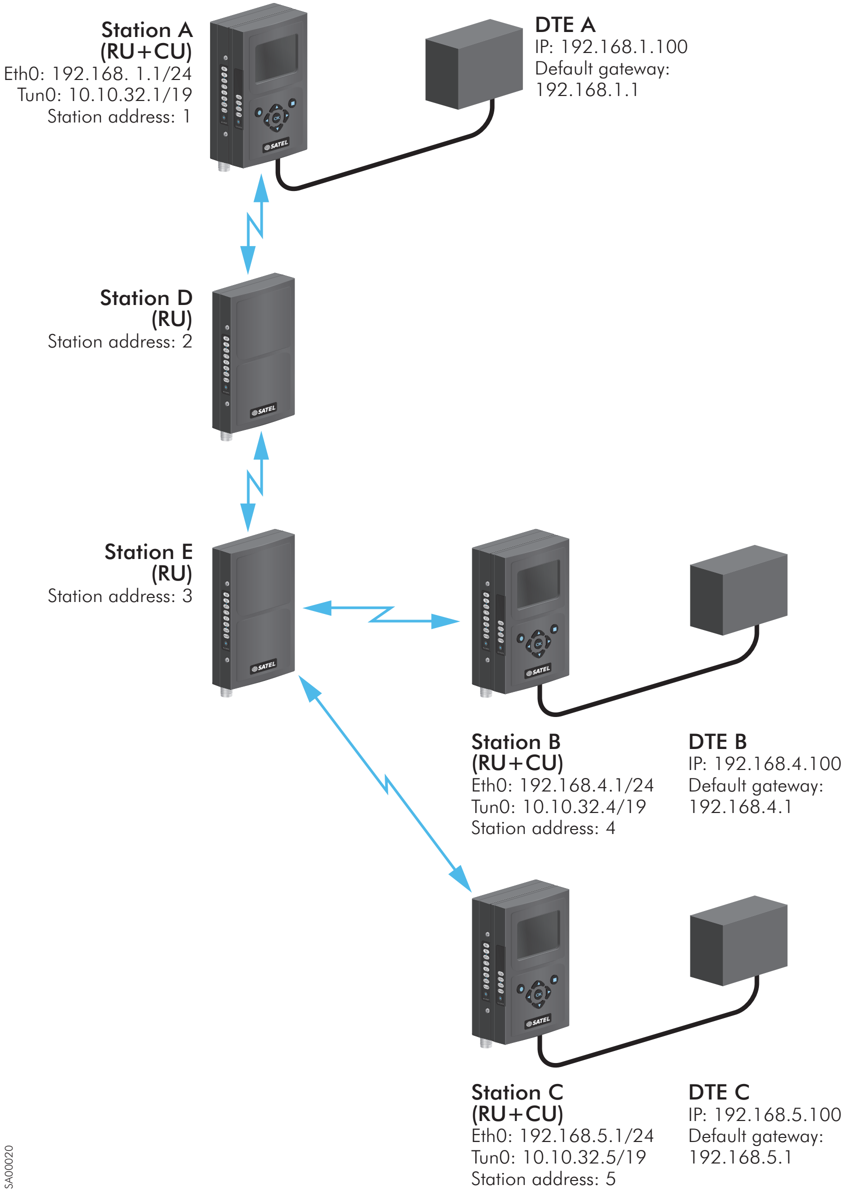


Figure 6.1 Routing example

6.1.2 Forming the tun0 IP address

Whenever the station address (RMAC) of a SATELLAR is changed, the IP address for the tun0 interface is automatically determined: If the station address is X, the tun0 IP address is set to 10.10.32.X, netmask 19.

In case the station address (X) is larger than 254, the tun0 address is of the form 10.10.A.B, where A = 32 + (X / 254), rounded down and B = 1 + (X % 254) [% being the modulus operator]. For example, RMAC 500 translates to tun0 address 10.10.33.247.

In case a subnet with network address 10.10.32.0/19 is already in use in a system, a SATELLAR radio network can be configured to use another tun0 network Base Address. To do this, use the Admin Settings application (see chapter 8.8.2). All modems MUST use the same tun0 Base Address.

6.1.3 Choosing the eth0 IP address

Eth0 IP addresses must be selected according to two rules.

- Each CU's eth0 interface must belong to a different subnet.
- The CU and the corresponding DTE must belong to the same subnet.

Additionally

- It is a good practice to set the CU IP address as 192.168.X.1 where X is the station address (RMAC), if possible.
- The default gateway for the DTE should be the corresponding CU, unless there is another gateway present in the LAN. In this case the routing tables of the gateway must be modified accordingly.

The rules can be clarified with the help of Figure 6.1: Routing example.

The station A has

- Station address (RMAC) 1 → tun0 address is 10.10.32.1
- Eth0 address 192.168.1.1/24 (i.e. subnet mask is 255.255.255.0)
- Therefore DTE A must have an address 192.168.1.X, e.g. 192.168.1.100 and its default gateway must be 192.168.1.1

The station B has

- Station address (RMAC) 4 → tun0 address is 10.10.32.4
- Eth0 address must be chosen so that it belongs to a subnet different from station A, e.g. 192.168.4.1/24
- Therefore DTE B must have an address 192.168.4.X, e.g. 192.168.4.100 and its default gateway must be 192.168.4.1

The station C has

- Station address (RMAC) 5 → tun0 address is 10.10.32.5
- Eth0 address must be chosen so that it belongs to a subnet different from stations A and B, e.g. 192.168.5.1/24
- Therefore DTE C must have an address 192.168.5.X, e.g. 192.168.5.100 and its default gateway must be 192.168.5.1

Stations D and E act only as repeaters without a CU and therefore no local Ethernet connection. So they have no IP addresses – just station addresses.

6.1.4 Setting IP routes

After all the addresses have been set it is still required to define IP routes for each of the CU. Routing data must include the address and net mask of each of the destination subnets (LANs) that need to be reached and the gateway it can be reached through. The gateway address is the tun0 address of the target CU.

For the network in the Figure 6.1 the IP routing tables of each CU equipped station are:

Station	Destination/net mask	Gateway
A	192.168.4.0/24	10.10.32.4
	192.168.5.0/24	10.10.32.5
B	192.168.1.0/24	10.10.32.1
	192.168.5.0/24	10.10.32.5
C	192.168.1.0/24	10.10.32.1
	192.168.4.0/24	10.10.32.4

Table 6.2 IP routing tables for each CU in Figure 6.1

The usage of different addresses and routing tables can be clarified by an example where DTE A wants to send a message to DTE B.

1. The destination IP address, 192.168.4.100, belongs to a subnet different from the source address, 192.168.1.100. The message is therefore routed to the default gateway of DTE A, i.e. to CU of station A.
2. CU of station A recognizes that the destination address belongs to sub network 192.168.4.0 which is reachable through gateway 10.10.32.4. The message is therefore forwarded to tun0 interface which translates the gateway address to the RMAC address, 4 in this case.
3. At this point the packet routing protocol of the RU enters the picture: it reads the destination RMAC address and consults the packet routing table to find out that a message to address 4 must be sent to address 2. (Address of station D).
4. Station A's RU now reserves the radio path using the CSMA/CA algorithm to send the data to station D.
5. Station D receives the data and recognizes that the final destination address is 4. Station D consults its packet routing table and sees that the message to address 4 must be sent to address 3 (station E) and then reserves the radio path to send the message.
6. Station E receives the message and then forwards it to station B (as above) which is the final destination station.
7. The packet routing protocol in station B recognizes that the received data is intended for this station and therefore forwards the data to the CU/tun0 interface.
8. The IP router software component of the CU of station B recognizes that the destination IP address differs from its own IP address but belongs to the same sub network. Therefore it forwards the message to eth0 interface and then the message finally reaches the destination, i.e. DTE B.

6.2 Proxy Arp

Proxy ARP option enables SATELLAR to act as a "Pseudo-bridge" or a hidden router. When this option is enabled, SATELLAR responses with its own MAC address to all ARP (Address Resolution Protocol) requests addressed to a remote network. This causes the other hosts in the same local network to send their packets to the SATELLAR, which then routes those packets according to its configured IP Routes. This behavior makes it look like the hosts on each side of the bridge belong to the same physical network segment (Default=OFF).

6.3 DHCP

The CU supports the DHCP (Dynamic Host Control Protocol) in either Server or Client mode. DHCP can also be set to off, which is the default setting.

In client mode, the CU attempts to contact a DHCP server in the Ethernet subnet to get the eth0 IP address.

In server mode, the CU provides IP addresses to other devices in the Ethernet subnet.
Typically SATELLAR networks are configured with DHCP OFF, because static IP addresses are needed to access remote devices reliably.

7. Settings

The CU has several settings, which affect the operation of the IP routing and other things. The CU can also be used to change the settings of the RU as well as any other units present. There are several interfaces to use when viewing info and changing settings (see chapter 5.6)

The settings are grouped into categories used in the LCD and WWW GUIs. Each setting is also listed with the sub-unit number and NMSID for use with NMS Protocol and NMS Import features. See chapter 5.8 for information about NMSIDs and chapter 8.5 for information about NMS Import.

NOTE: See the settings selection quide at the end of the manual.

7.1 Modem Settings

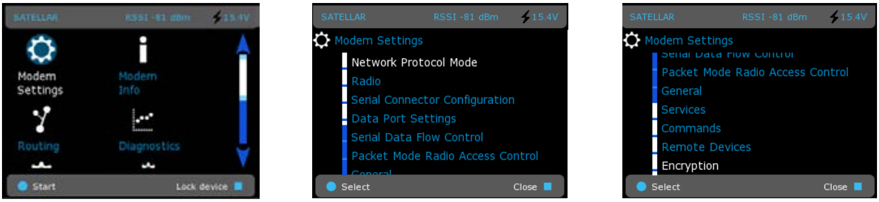


Figure 7.1 Modem Settings by CU: Graphical user interface (GUI/LCD)

7.1.1 Radio Unit Settings categories

For explanation of categories Network Protocol Mode, Radio, Serial Connector Configuration, Data Port Settings, Serial Data Flow Control and Packet Mode Radio Access Control, see the RU user manual chapter 7, subchapters 7.1 through 7.3 respectively.

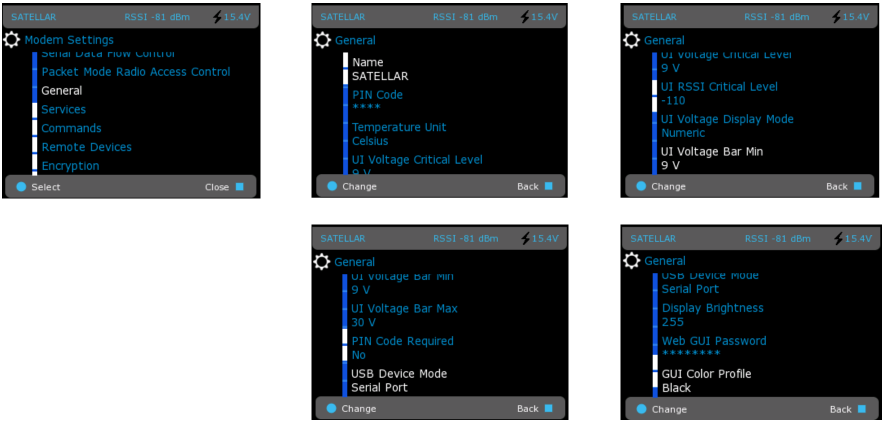
7.1.2 General

These are general and miscellaneous settings of the radio station and CU.

Attribute	Explanation	Sub unit	NMSID
Name	Name of the radio station. This is freely selectable by the user, up to a maximum length of 32 characters. The name can be used to identify the radio station. It is shown in the WWW interface and GUI/LCD screen, for example.	0	1.769

Attribute	Explanation	Sub unit	NMSID
PIN Code	Code to unlock the GUI/LCD Screen of the CU (if present).	1	1.3200
Temperature unit	Fahrenheit, Kelvin or Celsius. Used by the Diagnostics graph for modem temperature.	1	1.3201
UI Voltage Critical Level	When the Voltage reading drops to this level, it is displayed in red in the GUI/LCD and WWW interfaces.	1	1.3202
UI RSSI Critical Level	When RSSI drops to this level it is displayed in red.	1	1.3203
UI Voltage Display mode	Select the way to display voltage in the GUI/LCD: either numeric or as a bar	1	1.3204
UI Voltage Bar Min	If display mode is set to Bar, this Voltage level corresponds to the minimum level of the voltage indicator, i.e. no bars. Value is also used as a minimum threshold for SNMP Voltage. See chapter 8.2 for more details.	1	1.3205
UI Voltage Bar Max	If display mode is Bar, this Voltage level corresponds to Maximum bars	1	1.3206
PIN Code Required	If set to Yes, user must enter PIN code to unlock the GUI/LCD and keyboard.	1	1.3224
USB Device Mode	Choose how the CU will act when connected to a PC: Mass memory or Serial port. See also chapter 7.3.	1	1.3225
Display Brightness	A value from 0 to 255, this setting controls the brightness of the LCD screen's backlight.	1	1.3258
Web GUI Password	Set the password of user "satellar". This affects the WWW password and linux command line login password for this user. The password is case-sensitive. Default password is "Satel123".	1	1.3259
GUI Color profile	Choose a color profile for the GUI/LCD. Default is "Black"	1	1.3261
LCD Timeout	The time in seconds without keys pressed before the LCD (if present) of the CU is powered off.	1	1.3275

Table 7.1 Modem settings, General



General

Name
SATELLAR

PIN Code
****

Temperature Unit
Celsius

UI Voltage Critical Level
9 V

UI RSSI Critical Level
-110

UI Voltage Display Mode
Numeric

UI Voltage Bar Min
9 V

UI Voltage Bar Max
30 V

PIN Code Required
No

USB Device Mode
Serial Port

Display Brightness
255

Web GUI Password
****

GUI Color Profile
Black

Figure 7.2 Modem Settings, General by CU: Graphical user interface (GUI/LCD)

7.1.3 Services

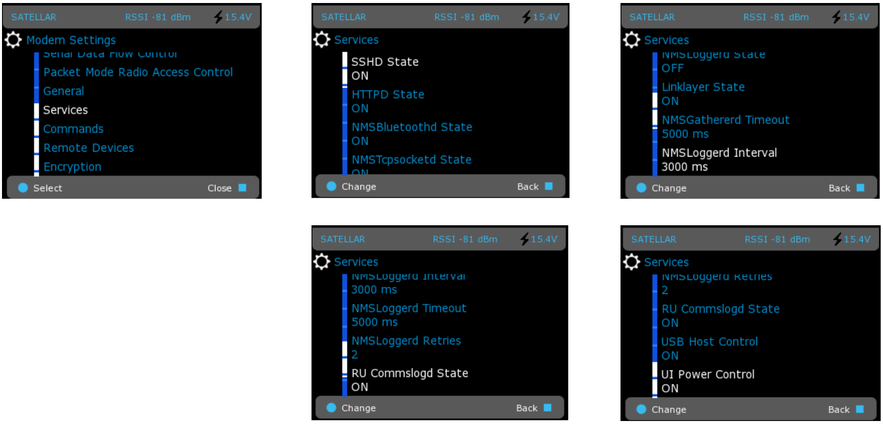
This category can be used to disable unused features of the CU and fine-tune some operational parameters. Usually these settings should not be modified, as some of the settings disable essential services of the device.

Attribute	Explanation	Sub unit	NMSID
SSHD State	Turn the SSH server ON or OFF	1	1.3230
HTTPD State	Turn the Web server ON or OFF. WARNING: If this is turned off, the WWW interface becomes unavailable. It can be turned back on using the GUI/LCD (if present) or SATEL NMS protocol.	1	1.3231
NMSBluetoothd State	Turn ON or OFF the possibility of giving SATEL NMS commands to the device using a wireless Bluetooth serial connection. A supported USB Bluetooth dongle must be connected to the CU. (List of supported devices available separately)	1	1.3232
NMSTcpsocketd State	Turn ON or OFF the possibility of using SATEL NMS commands over a TCP/IP connection to the device. The default TCP port is 55555.	1	1.3233
NMSLoggerd State	This service is required by the diagnostics features. It monitors diagnostic values and stores them in a database, where they can be viewed using the Diagnostics application. If this service is disabled, the status bar RSSI and Voltage readings are also disabled.	1	1.3234
Linklayer State	This feature is required by IP data transfer. WARNING: IF THIS IS DISABLED, NO IP DATA CAN BE TRANSMITTED TO THE RADIO NETWORK. Diagnostics can still be gathered and settings can still be changed.	1	1.3235
NMSGathererd timeout	Time in milliseconds to wait for NMS messages sent to the RU before giving up. It is usually not necessary to modify this value	1	1.3237
NMSLoggerd Interval	How often the Diagnostic values are updated, in milliseconds.	1	1.3238
NMSLoggerd Timeout	Time in milliseconds to wait for diagnostic NMS messages before giving up. In case a CU is set up to monitor other devices in the network (using the “Modem Settings/Remote Devices” settings category), it may become necessary to increase this value if the network is very large.	1	1.3239
NMSLoggerd Retries	Number of times to retry lost diagnostic NMS messages. This value should be kept low to avoid congestion in heavy traffic situations.	1	1.3240
RU Commslogd State	Set logging of NMS messages between the CU and the RU ON or OFF. The log can be viewed in the “Logs” page of the WWW interface.	1	1.3262
USB Host Control	When USB Host Control is OFF, the USB host port power is turned off and no devices can be connected. When the value is ON, the port works normally.	1	1.3269

Table 7.2 Modem settings, Services

Attribute	Explanation	Sub unit	NMSID
UI Power Control	When UI Power Control is ON, the GUI/LCD Screen is turned off after the defined timeout (See Modem Settings/General). When the value is OFF, the screen is always turned off and the device uses less power.	1	1.3274
SNMPD State	Select SNMPD (SNMP Daemon or agent) ON or OFF	1	1.3266
HTTPD IP Address	Binding IP Address for the Web server	1	1.3400
SSHD IP Address	Binding IP Address for the SSH server	1	1.3401
NMSTcpsocketd IP Address	Binding IP Address for the NMS TCP socket	1	1.3402

Table 7.2 Modem settings, Services



SATELLAR RSSI -81 dBm 15.4V
Modem Settings
Serial Data Flow Control
Packet Mode Radio Access Control
General
Services
Commands
Remote Devices
Encryption
Select Close

SATELLAR RSSI -81 dBm 15.4V
Services
SSHD State
ON
HTTPD State
ON
NMSBluetoothd State
ON
NMSTcpsocketd State
ON
Change Back

SATELLAR RSSI -81 dBm 15.4V
Services
NMSLoggerd State
OFF
Linklayer State
ON
NMSGathererd Timeout
5000 ms
NMSLoggerd Interval
3000 ms
Change Back

SATELLAR RSSI -81 dBm 15.4V
Services
NMSLoggerd Interval
3000 ms
NMSLoggerd Timeout
5000 ms
NMSLoggerd Retries
2
RU Commslogd State
ON
Change Back

SATELLAR RSSI -81 dBm 15.4V
Services
NMSLoggerd Retries
2
RU Commslogd State
ON
USB Host Control
ON
UI Power Control
ON
Change Back

Figure 7.3 Modem Settings, Services by CU: Graphical user interface (GUI/LCD)

7.1.4 Commands

This chapter has commands to reset the unit(s) or restore settings to various states, for example to initialize a device to its original status or reboot device.

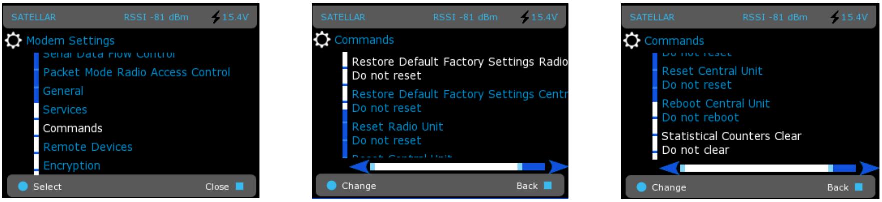
Use only one command at the time and do not to save any other settings at the same time.
Also, refresh NMS values after Radio Unit value restore.

To issue a command, select “Reset” or “Reboot”, for example. The command is sent when settings are committed, as detailed in chapter 5.7.6.

Command	Explanation	Sub unit	NMSID
Restore Default Factory Settings Radio Unit	The RU's settings, including Frequency, Packet routing tables, RMAC etc. are restored to the state they were in when the unit left the factory.	0	1.3085
Restore Default Factory Settings Central Unit	The CU's settings, including IP, routing etc. are restored to the state they were in when the unit left the factory.	1	1.3085
Reset Radio Unit	Resets the Radio Unit. This command is mostly used by NMS Protocol to discard unsaved changes. It is not usually necessary to use this command when configuring the modem using the WWW or LCD user interfaces.	0	1.3090
Reset Central Unit	Resets the Central Unit. This command is mostly used by NMS Protocol to discard unsaved changes. It is not usually necessary to use this command when configuring the modem using the WWW or LCD user interfaces. (Note that despite being called the Reset command, the CU is not actually reset. Only unsaved settings are cleared.)	1	1.3090
Reboot Central Unit	Reboot the CU (by resetting the MCU). The reboot lasts approximately one a minute (see technical specification for accurate values)	1	1.3093
Statistical Counters Clear	Clears (resets to zero) all Radio Unit statistical counters. Statistical counters include the variables whose values increase due to some activity. These variables are Bytes to Radio, Bytes from Radio, Transmitted Packet Count and Received Packet Count. Setting of this patameter to value Clear resets those counters to zero. Note that the value is automatically restored back to do not clear after commit. Reset of values can be observed from Modem Info page values (as soon as the countres are updated).	1	1.3109

Table 7.3 Modem settings, Commands

There are also three buttons at the bottom of the WWW interface page: Reboot RU+CU, Reboot CU and Reboot RU. Select the corresponding button to reboot the CU, RU or both. In this case there is no need to select Apply or Commit buttons, but the reboot happens immediately.



Restore Default Factory Settings Radio
Do not reset

Restore Default Factory Settings Centr
Do not reset

Reset Radio Unit
Do not reset

Reset Central Unit
Do not reset

Reboot Central Unit
Do not reboot

Statistical Counters Clear
Do not clear

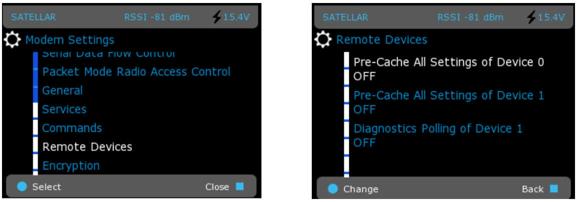
Figure 7.4 Modem Settings, Commands by CU: Graphical user interface (GUI/LCD)

7.1.5 Remote Devices

This controls how the CU diagnostics service (NMSLoggerd) handles remote radio stations. By default, no online remote monitoring is done.

Setting	Explanation	Sub unit	NMSID
Pre-cache All Settings of Device N	(N equals the RMAC address of the radio station). Enable this to have the CU remotely fetch all settings from the remote device. This will cause significant radio traffic. (Not usually recommended)	1	1.3264
Diagnostics Polling of Device N	(N equals the RMAC address of the radio station). Enable this to have the CU monitor the diagnostics values of the remote device. The diagnostics become available in the Diagnostics page. This will cause additional radio traffic which may be significant depending on the size of the network, defined time intervals, timeouts and retries (see chapter 7.1.3) and the number of devices monitored. This setting is not shown, unless at least one Packet Route is defined (see chapter 7.3.1)	1	1.3265

Table 7.4 Modem settings, Remote devices



Pre-Cache All Settings of Device 0
OFF

Pre-Cache All Settings of Device 1
OFF

Diagnostics Polling of Device 1
OFF

Figure 7.5 Modem Settings, Remote devices by CU: Graphical user interface (GUI/LCD)

7.1.6 SNMP

The usage of SNMP is described in chapter 8.2.

7.1.7 Time Control

Control current date and time, time zone and Network Time Protocol (NTP) settings.
Note that SATELLAR does not have battery-backed real time clock hardware, therefore time is not accurately preserved during power off and reboot. Using an external NTP server can help mitigate this.

Time is used mainly for logging purposes and accurate real-time is not essential for the operation of SATELLAR.

Setting	Explanation	Sub unit	NMSID
Time Operation Mode	*No time operation* – default. Other time settings have no effect.	1	1.3282
	Manual time operation. Time and time zone settings are used, NTP settings are not used.		
	NTP Time. Time setting is not used; instead the NTP protocol is used.		
NTP Server Address	Current time is fetched from the defined NTP Server Address. Only works if Time operation mode is set to NTP time.	1	1.3283
NTP Interval	Time is refreshed from the NTP server after the interval defined in this settings has passed. Default is 100 seconds. Please be aware this setting will consume some radio bandwidth if used in remote SATELLARs, therefore very small values are not recommended.	1	1.3284
Time	Current time given in *"YYYY-MM-DD hh:mm:ss"* format. This setting is only taken into use if *Time operation mode* is set to Manual time operation.	1	1.3285
Time Zone	Select time zone. Used in both NTP time and Manual time modes.	1	1.3286
NTP Request Source IP Address	Source IP address of the NTP requests	1	1.3347

Table 7.5 Modem settings, Time control

NTP time setup can be verified from System Messages at Logs sheet.
Successful connection to NTP server generates the line:

```
May 26 08:06:03 (none) user.notice ntpclient: 29279 10391.478 55115.0 20.0 1080364372505324.6
1709.0 0
```

7.1.8 Testing and Calibration

This category contains settings that help testing and calibrating the network.

Setting	Explanation	Sub unit	NMSID
Carrier Test	Activates the carrier test in the radio unit. When the test is on, the RU will transmit a carrier signal continuously with no actual data included. It can be used to measure how well other devices can receive the transmissions. All devices in range operating on the same frequency will be able to measure the RSSI. When the test is on, the radio interface is reserved, because of the constant transmission.	0	1.3074
Carrier Test Timeout	Specifies the duration for the carrier test on seconds. This value can be modified either before starting the carrier test or during the test. If the value is zero, the carrier test will stay on until turned off.	1	1.3094
Fast RSSI scan	When this parameter is set to TRUE, RSSI value in the GUI will update about once per second. (If set to FALSE, the update frequency of RSSI value in the GUI is once per 30 seconds by default). Fast RSSI scan increases CPU usage. Also, other statistics like Voltage and Temperature will not be collected, if Fast RSSI scan is enabled. It is recommended to enable Fast RSSI scan only when a fast update is required for example for antenna alignment or troubleshooting.	1	1.330
RSSI RMAC Address	By default the RSSI displayed in the GUI and the Diagnostics application will show the RSSI measured from the last signal received. If the device is receiving signals from multiple devices, it may be difficult to match the measured RSSI to the corrcet transmitting neighbor. This parameter can be used to force the RSSI measurement to be done only for the messages received from the specific modem only. Value expected for this parameter is the remote device RMAC. If the value is 4096, the RSSI will be measured from any device. Note that RMAC specific RSSI monitoring does not work with Carrier Test, because the RMAC information is not included to test signal by the transmitting modem.	1	1.331

Table 7.6 Modem Settings, Testing and Calibration

7.1.8.1 Example: Using carrier timeout and fast RSSI

In this example there is one master device with several neighbors. The user wants to know how well each of the neighbors can hear the master, and adjust the antennas of the devices that have poor reception. The carrier test is used.

The carrier test is activated in the master device. Also, because the device cannot be accessed remotely, the timeout is set to two hours. Carrier test will automatically stop and normal operation can continue after 7200 seconds.

The following values are set from the GUI:

- Carrier test: ON
- Carrier test timeout: 7200

When the test is on, the user accessess all the remote modems to verify measured RSSI from the GUI. If a poor RSSI value is found from any of the remote devices, the user proceeds to adjust the antenna. By default, the RSSI on the screen updates about once per each 30 seconds. This may not be sufficient for antenna adjustment purposes. Therefore the user makes the RSSI measurement faster by changing the following setting:

- Fast RSSI scan: ON

Now the RSSI measurement updates about once per second, and the user can see the results of the antenna djustment in almost real time. After the antenna has been adjusted, the fast RSSI mode should be turned off:

- Fast RSSI scan: OFF

7.2 Modem Info

This application contains information about the radio station. These values cannot be changed.

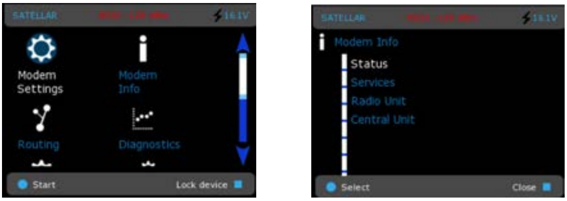


Figure 7.6 Modem Info by CU: Graphical user interface (GUI/LCD)

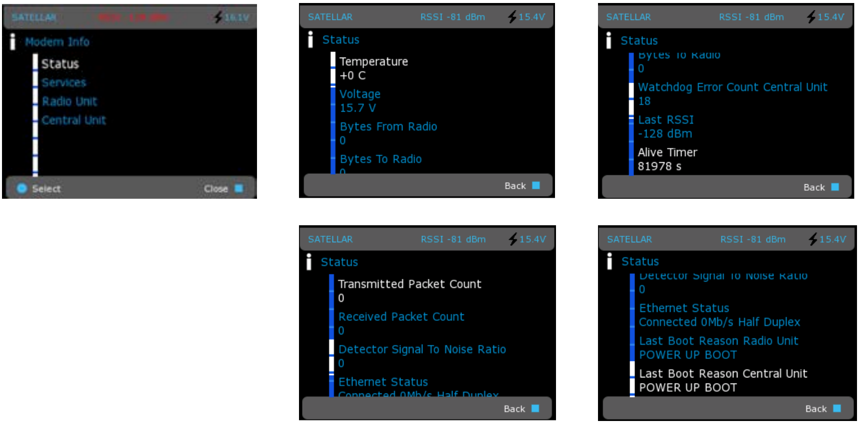
7.2.1 Status

Information about the current general state of the radio station. The values on this page may be refreshed by pressing the F5 Key, or selecting Refresh from a menu, when viewed via the WWW interface on a standard web browser.

Item	Explanation	Sub unit	NMSID
Temperature	Measured inside the RU radio module. See RU user manual for details.	0	1.32
Voltage	Measured by the RU from the voltage input terminals. Precision of the reading is 0.1 Volts, but actual measurement accuracy may vary, see RU user manual for details.	0	1.33

Item	Explanation	Sub unit	NMSID
Bytes From Radio	How much data (including NMS messages) has been received by the RU from radio.	0	1.38
Bytes to Radio	How much data (including NMS messages) has been transmitted by the RU to radio.	0	1.39
Watchdog Error Count CU	Number of reboots the CU’s Watchdog has performed.	1	1.45
Last RSSI	Signal strength of the last received radio message.	0	1.111
Alive Timer	Time in seconds the RU has been running since the last reset.	0	1.113
Transmitted Packet Count	Number of Packet Routing packets transmitted by Radio Unit to the radio since last reset of the RU.	0	1.120
Received Packet Count	Number of Packet Routing packets received by Radio Unit from the radio since last reset of the RU.	0	1.121
Detector Signal To Noise Ratio	Signal to Noise Ratio (SNR) measured by the RU from last received data packet, in decibels (dB).	0	1.122
Ethernet Status	As a result of settings or auto MDI-X negotiation the Ethernet status may change. This item shows the current status. Connected/Not connected, 10 or 100Mb/s, Full or Half duplex.	1	1.3257
Last Boot Reason RU	Reason for the last restart. User command, Watchdog error, Power up etc.	0	9.795
Last Boot Reason CU	Reason for the last restart. User command, Watchdog error, Power up etc.	1	9.795
Temperature Ceiling	Maximum measured temperature since the last reset	0	1.83

Table 7.7 Modem info, Status



SATELLAR RSSI -128 dBm 16.1V
Modem Info
Status
Services
Radio Unit
Central Unit
Select Close

SATELLAR RSSI -81 dBm 15.4V
Status
Temperature
+0 C
Voltage
15.7 V
Bytes From Radio
0
Bytes To Radio
0
Back

SATELLAR RSSI -81 dBm 15.4V
Status
Bytes To Radio
0
Watchdog Error Count Central Unit
18
Last RSSI
-128 dBm
Alive Timer
81978 s
Back

SATELLAR RSSI -81 dBm 15.4V
Status
Transmitted Packet Count
0
Received Packet Count
0
Detector Signal To Noise Ratio
0
Ethernet Status
Connected 0Mb/s Half Duplex
Back

SATELLAR RSSI -81 dBm 15.4V
Status
Detector Signal To Noise Ratio
0
Ethernet Status
Connected 0Mb/s Half Duplex
Last Boot Reason Radio Unit
POWER UP BOOT
Last Boot Reason Central Unit
POWER UP BOOT
Back

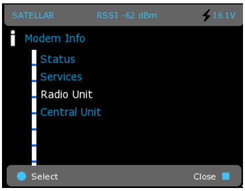
Figure 7.7 Modem info, Status by CU: Graphical user interface (GUI/LCD)

7.2.2 Services

This page shows information on different services running in the CU (see more about the services in chapter 7.1.3). In addition to seeing which services are running, it can also be seen which services have been restarted or have caused the device to reboot recently.

7.2.3 Radio Unit

This page shows information about the RU. See the Radio Unit User Guide for details.



SATELLAR RSSI -62 dBm 16.1V
Modem Info
Status
Services
Radio Unit
Central Unit
Select Close

Figure 7.8 Modem info, Radio unit by CU: Graphical user interface (GUI/LCD)

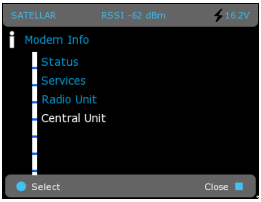
7.2.4 Central Unit

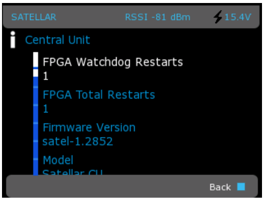
This page shows information about the CU.

Item	Explanation	Sub unit	NMSID
FPGA Watchdog Restarts	Count of restarts the hardware watchdog has performed.	1	1.123
FPGA Total Restarts	Total count of restarts the hardware has performed.	1	1.124
Firmware version	The version of the file system of the CU. This information is needed when updating the firmware using Firmware Updater (see chapter 8.3)	1	1.650
Model	Product model name. Normally this is “Satellar CU”	1	1.772
Ethernet MAC Address	The Media Access Control (MAC) address of the built-in Ethernet interface.	1	1.3210
Kernel version	The version of the Linux kernel of the CU. This information is needed when updating the firmware using Firmware Updater (see chapter 8.3). This is the version of SATELLAR kernel build, not the Linux kernel version it is based on.	1	1.3215
Serial Nbr RW	The serial number of the CU, equal to the one printed on the sticker on the device.	1	9.652
Board 1 *	Hardware information about the PCB.	1	various
Interface board *	Hardware information about the interface board (Ethernet and USB connectors).	1	various

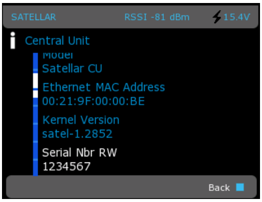
* Exact numbers and names of these items depend on the current HW configuration of the device

Table 7.8 Modem info, Central unit

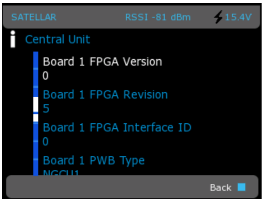




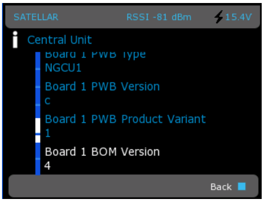
FPGA Watchdog Restarts
1
FPGA Total Restarts
1
Firmware Version
satel-1.2852
Model
Satellar CU



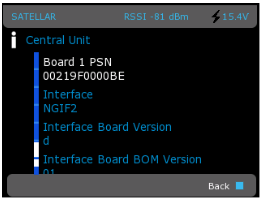
Model
Satellar CU
Ethernet MAC Address
00:21:9F:00:00:BE
Kernel Version
satel-1.2852
Serial Nbr RW
1234567



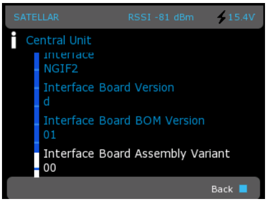
Board 1 FPGA Version
0
Board 1 FPGA Revision
5
Board 1 FPGA Interface ID
0
Board 1 PWB Type
NGCU1



Board 1 PWB Type
NGCU1
Board 1 PWB Version
c
Board 1 PWB Product Variant
1
Board 1 BOM Version
4



Board 1 PSN
00219F0000BE
Interface
NGIF2
Interface Board Version
d
Interface Board BOM Version
01

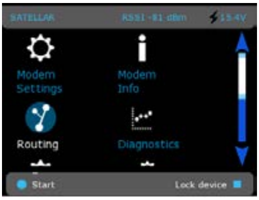


Interface
NGIF2
Interface Board Version
d
Interface Board BOM Version
01
Interface Board Assembly Variant
00

Figure 7.9 Modem info, Central unit by CU: Graphical user interface (GUI/LCD)

7.3 Routing

The routing application allows changing the Packet routing tables, IP settings and routes. This is similar to Modem Settings.



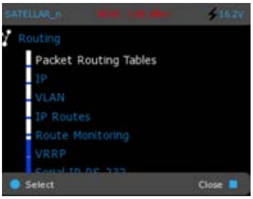


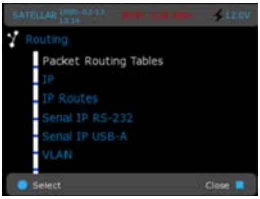
Figure 7.10 Routing by CU: Graphical user interface (GUI/LCD)

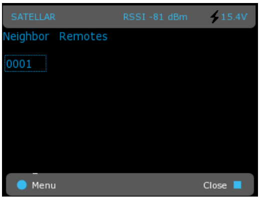
7.3.1 Packet Routing Tables

This category controls the packet routing tables of the RU. The interface is a little different on the GUI/LCD and WWW. In both cases you can:

- Add new packet routes
- View current routes
- Delete selected routes
- Add remote stations to a route
- Delete remote stations from a route

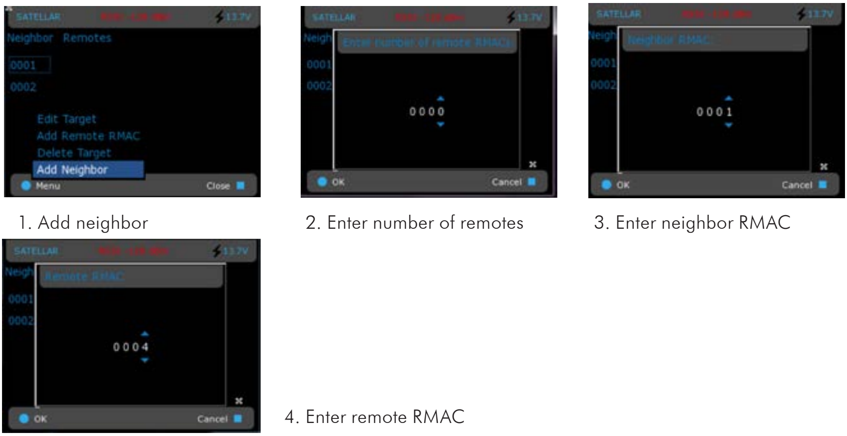
Important terms related to Packet Routing are:
- Neighbor, the RMAC address of a modem behind one radio link
- Remotes, RMAC address of modems behind the specific neighbor





0001

Figure 7.11 Packet routing tables by CU: Graphical user interface (GUI/LCD)



1. Add neighbor

2. Enter number of remotes

3. Enter neighbor RMAC

4. Enter remote RMAC

Figure 7.12 Add new route

It is possible to cancel the procedure at any point and discard the route by selecting Cancel.

Editing of a route is done by highlighting the route that needs to be modified and then selecting Menu -> Edit Target. See the figure "1. Add neighbor".

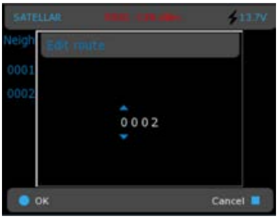


Figure 7.13 Edit route

To add a new remote RMAC address to existing route, highlight the neighbor to which the route is added to and then select Menu -> Add Remote RMAC (see figure "1. Add neighbor"). Next, fill in the RMAC address to be added to the route.

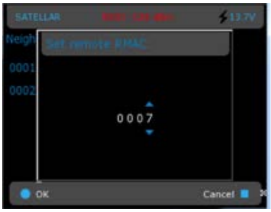
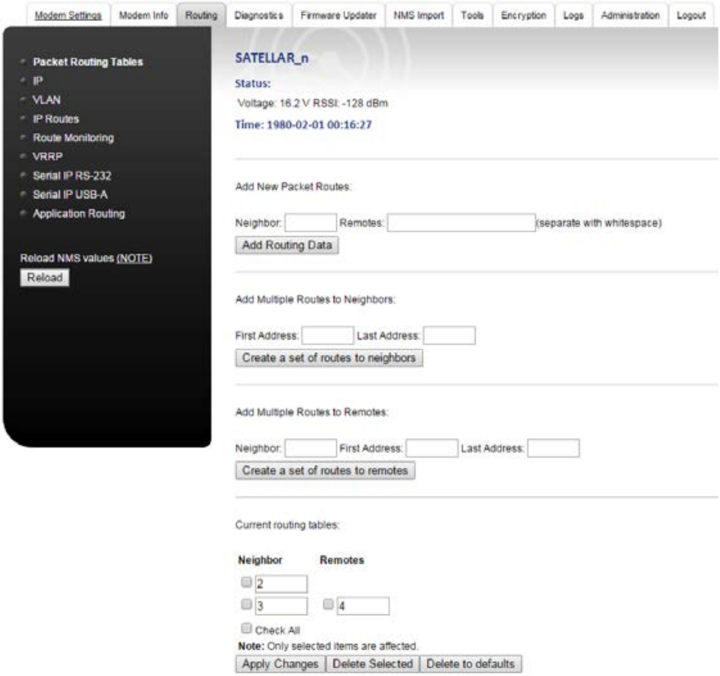


Figure 7.14 Set remote RMAC

To delete a route, highlight the neighbor or remote which needs to be deleted and then select Menu -> Delete Target (see Figure "1. Add neighbor").

Inserted values are pre-validated so in case of invalid input, SATELLAR will show the numbers in red color and proceeding is not allowed until the value is corrected.

Once all needed modifications are done, select Back twice to return to the main menu and you will be prompted to save or discard settings.



SATELLAR_n

Status:

Voltage: 16.2 V RSSI: -128 dBm

Time: 1980-02-01 00:16:27

Add New Packet Routes:

Neighbor: ______ Remotes: ______ (separate with whitespace)

Add Multiple Routes to Neighbors:

First Address: ______ Last Address: ______

Add Multiple Routes to Remotes:

Neighbor: ______ First Address: ______ Last Address: ______

Current routing tables:

Neighbor	Remotes
□ 2	
□ 3	□ 4

□ Check All

Note: Only selected items are affected.

Figure 7.15 Packet routing tables by CU: WWW user interface

With WWW interface, adding new routes is done by entering value for the neighbor RMAC address to Neighbor field and filling in the RMAC addresses of remotes behind this neighbor to the Remotes field. Separate remote RMAC address with whitespace. Apply the defined Packet Route by selecting Add Routing Data. For example, to add a route to neighbor device with RMAC address 2, insert number 2 to Neighbor field and select Add Routing Data button to appl the new packet route.

In case of neighboring modem with RMAC address 3 having modems with RMAC addresses 5 and 6 behind it, add the corresponding route as follows:

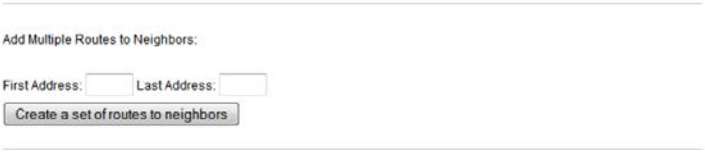
- Insert "3" to Neighbor field
- Fill in "6 5" to Remotes field
- Select Add Routing Data to apply changes.

At GUI the same functionality is achieved by:

- Select Add Neighbor
- Setting number of remote RMACs to 2
- Define the neighbor address to 3
- When asked for remote RMAC value, set the remote RMAC number 5
- When asked for next remote RMAC value, set the remote RMAC number 6

- To delete a route, mark the checkbox next to the route entry and select Delete Selected.
- To modify a route, change any of the values on a row and select on the Apply Changes.

In the WWW interface, Packet Routes can also be created automatically. Multiple routes can be configured with one step by defining a range of addresses. For example, setting the First Address to 5 and the Last Address to 10 creates routes to the following neighbors: 5, 6, 7, 8, 9 and 10. The changes are applied by selecting Create a set of routes to neighbors.

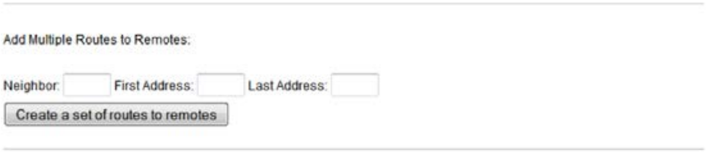


Add Multiple Routes to Neighbors:

First Address: Last Address:

Figure 7.16 Adding multiple routes to neighbors

Multiple remotes can also be added similarly with one step. This is done by setting values to the First Address and Last Address fields. The neighbor that has these addresses behind is defined by setting the correct address to the Neighbor field. The changes are applied by selecting Create a set of routes to remotes. For example, Packet Routes to remotes 6,7,8,9 and 10 via the neighbor 5, is configured by setting address 5 to Neighbor field, number 6 to First Address and number 10 to Last Address field. Selecting Create a set of routes creates routes to remotes from 6 to 10 via the Neighbor 5.



Add Multiple Routes to Remotes:

Neighbor: First Address: Last Address:

Figure 7.17 Adding multiple routes to be reachable via one neighbor

If you have entered an invalid route, SATELLAR will print a red error text and the invalid route is not added.
All applied changes are committed and taken into use by selecting Commit Changes button.
Applied configurations can be reversed by Cancel applied changes.

See RU user manual for more information about packet routing.

In LCD GUI route management has 4 options: Edit Target, Add Remote RMAC, Delete Target and Add New Neighbor.

To add new route:

1. Select Menu -> Add Neighbor
2. Provide the number of remote RMAC addresses for this neighbor. In case adding only neighbor, and no remotes, leave this to zero.
3. Fill in the RMAC address of the neighbor.
4. If number of remotes > 0, then RMAC for each remote is set.

7.3.2 IP

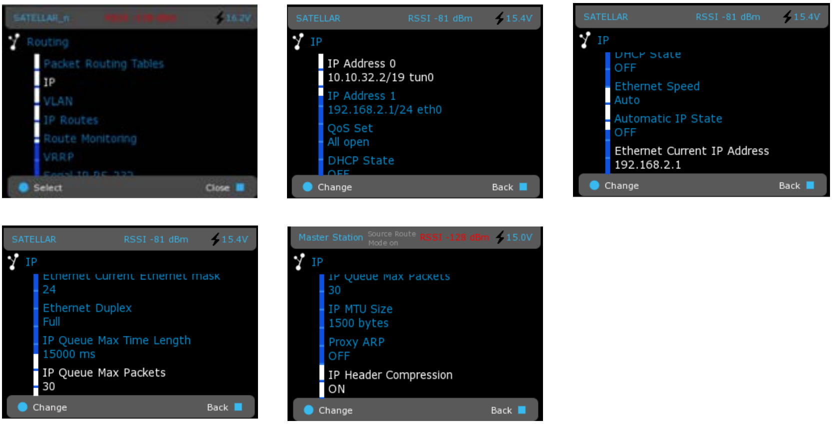
This category contains the Internet Protocol settings.

Setting	Explanation	Sub unit	NMSID
IP Address 0 and 1	One of these is the Tun0 address. This cannot be directly modified. The Eth0 address can be modified.	1	1.3208
QoS set	The functionality controlled by this setting is not finished in the current firmware version. Please ignore it for the time being.	1	1.3227
DHCP State	OFF, Client or Server. Default is OFF. See chapter 6.2 for details.	1	1.3229
Ethernet Speed	Auto, 10 Mbps or 100 Mbps. Some Ethernet devices will not work correctly if speed is set to Auto. In this case select the correct speed using this setting.	1	1.3255
Automatic IP State	OFF or ON. Default is OFF. If set to ON, the eth0 address is set to 172.20.X.1/14, where X equals the RMAC address. In this case, the eth0 IP address cannot be modified until Automatic IP State is set to OFF.	1	1.3263
Ethernet Current IP Address	Show the current eth0 address. If the address has been overridden by the function button as detailed in chapter 5.5, this value is 192.168.1.1, even if the setting on this same page has been set to another value.	1	1.3270
Ethernet Current Ethernet mask	As above, shows the actual netmask in use at this time.	1	1.3271
Ethernet Duplex	Settable to FULL or HALF. Some Ethernet devices require this to be set to Half.	1	1.3276
IP Queue Max Time Length	The IP router of the CU buffers the IP packets going to the radio interface. This setting controls how long individual packets are kept in the buffer before being deleted. See below for more information.*	1	1.3280
IP Queue Max Packets	This setting controls the maximum number of packets in the outgoing IP packet buffer.*	1	1.3281

Setting	Explanation	Sub unit	NMSID
IP MTU Size	MTU=Maximum Transmission Unit. MTU of a communications protocol of a layer is the size (in bytes) of the largest protocol data unit that the layer can pass onwards. The largest number is 1500-byte packet. A larger MTU brings greater efficiency. Large packets increase lag and minimum latency. Corruption of a single bit in a packet requires that the entire packet is retransmitted. Retransmissions of larger packets take longer.	1	1.3317
Proxy ARP	When this option is enabled, SATELLAR responses with its own MAC address to all ARP requests (Address Resolution Protocol) addressed to IP address that actually locates in a remote network. This causes the other hosts in the same local network to send their packets to the SATELLAR, which then routes those packets according to its configured IP Route. Effectively, the Proxy ARP connects to separate physical LAN segments on each side of the radio network to the same IP network. (Default value: OFF).	1	1.3318
IP Header Compression	IP Header Compression reduces the size of headers in TCP/IP connections. It will reduce latency since the transmitted packets will be smaller. The compression algorithm assumes that there is very little packet loss, so the feature should be used only in good-quality point-to-point connections. Lost packets will make the receiver unable to uncompress the received packets, causing extra retransmissions. If there are repeaters in the network, or there is noticeable packet loss, IP Header Compression should not be used.	1	1.3324

* IP Queue handling: When the radio channel is experiencing heavy traffic, IP packets cannot always be sent immediately. They are placed in a queue waiting for the radio channel to become free. (See RU user manual for more information). Note that the radio queue should not be set to too large values, because the TCP/IP protocol will resend IP packets if it has not received a response in time. Too long IP queue will in this case just cause more duplicate packets to be sent, to no useful effect. Also some real-time or near-real-time applications, typically those using the UDP protocol, require packets to be at most a few seconds old, therefore buffering them for tens of seconds is not useful.

Table 7.9 Routing, Internet protocol settings



SATELLAR_n RSSI -128 dBm 16.2V
Routing
Packet Routing Tables
IP
VLAN
IP Routes
Route Monitoring
VRRP
Serial IP RS-232
Select Close

SATELLAR RSSI -81 dBm 15.4V
IP
IP Address 0
10.10.32.2/19 tun0
IP Address 1
192.168.2.1/24 eth0
QoS Set
All open
DHCP State
OFF
Change Back

SATELLAR RSSI -81 dBm 15.4V
IP
DHCP State
OFF
Ethernet Speed
Auto
Automatic IP State
OFF
Ethernet Current IP Address
192.168.2.1
Change Back

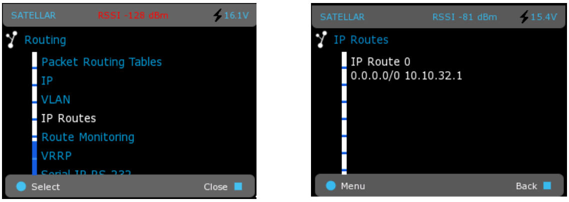
SATELLAR RSSI -81 dBm 15.4V
IP
Ethernet Current Ethernet mask
24
Ethernet Duplex
Full
IP Queue Max Time Length
15000 ms
IP Queue Max Packets
30
Change Back

Master Station Source Route Mode on RSSI -128 dBm 15.0V
IP
IP Queue Max Packets
30
IP MTU Size
1500 bytes
Proxy ARP
OFF
IP Header Compression
ON
Change Back

Figure 7.18 Routing, IP by CU: Graphical user interface (GUI/LCD)

7.3.3 IP Routes

This category allows adding, modifying and removing IP routes. For examples of typical routes, see chapter 6.1.



IP Route 0
0.0.0.0/0 10.10.32.1

Figure 7.19 Routing, IP Routes by CU: Graphical user interface (GUI/LCD)

A short introduction to IP routing

The SATELLAR IP radio network consists of Local Area Networks (LANs) and routers (the SATELLAR CUs). One of the LANs is the radio network, reached through the tun0 interface of each SATELLAR. This LAN is common to all SATELLARs. The other LANs are the Ethernet LANs (reached through the eth0 interface).

A router's defined task is to route IP packets between LANs. To do this, the router needs routing tables which tell it how to reach any other network. Therefore each router must have defined routes to all the LANs.

The task of defining routes is made easier by the concept of default route, also known as default gateway. All IP packets are sent to the default gateway, unless there is a specific route telling otherwise. All IP routes consist of two pieces of information.

- The target *network address* (including netmask)
- The target *gateway address*.

Together these two tell the router that an *IP packet belonging to a certain network (i.e. LAN or subnet) must be sent to a certain gateway*. For example a route defined as 192.168.2.0/24 10.10.32.2, tells that all IP packets which have a destination address that falls under the 192.168.2.0/24 network address (for example 192.168.2.7) must be sent to the gateway 10.10.32.2.

Note that there must also be a return route defined in the other end router back to the original LAN. (Sometimes a default route is enough for this). Typically SATELLARs at remote sites will act as the default gateway for the Ethernet LAN they are connected to.

It is also possible to define multiple routes to one network with redundant routing. For more information see chapter 7.6. The rest of this chapter will focus on single routes to a single destination.

Consider the network in the Figure 7.20. There are four Ethernet LANs (1 through 4), connected by SATELLAR radios (R1 through R4). The radios are connected by a fifth LAN, the radio LAN. LAN 1 is also connected to the internet via a gateway (router, ADSL etc.).

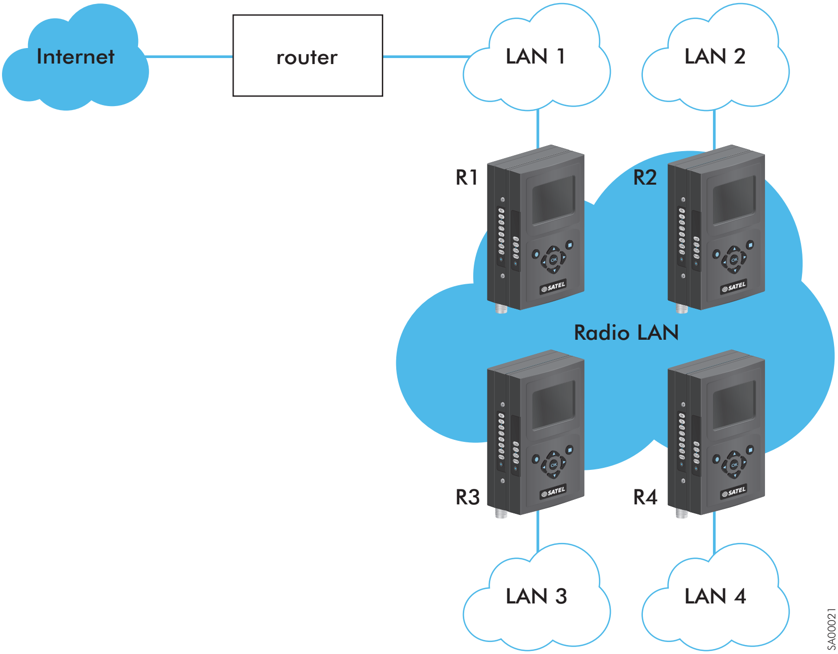


Figure 7.20 IP routing

Before designing the IP routes, we must define the desired connectivity. To keep the amount of routes smaller, we decide that LANs 2, 3 and 4 do not need to have access to each other, because our central station is in LAN 1 and it will receive status messages from sensors connected to the other LANs. The sensors do not need to communicate with each other. LAN 1 must however have access to the internet, so it can be reached from off-site for remote monitoring.

Router	Default gateway	Other routes
router	WAN/internet	LAN 2 via R1 LAN 3 via R1 LAN 4 via R1
R1	router	LAN 2 via R2 LAN 3 via R3 LAN 4 via R4
R2	R1	none
R3	R1	none
R4	R1	none

Table 7.10 Interface routes, see Figure 7.20

(Note that interface routes are omitted for simplicity, as they are automatically added)

The next step is to decide the actual IP address and netmask for each LAN. You also decide which device will be the default gateway of each LAN.

LAN name	network IP address	Netmask	Default gateway
LAN 1	192.168.1.0	24	router
LAN 2	192.168.2.0	24	R2
LAN 3	192.168.3.0	24	R3
LAN 4	192.168.4.0	24	R4
Radio LAN (Automatic)	10.10.32.0	19	R1

Table 7.11 IP address and net mask, see Figure 7.20

Please remember that the Radio LAN (tun0) addresses of each modem are automatically set based on the RMAC addresses (see chapter 6.1.2). If we assume that each RMAC of radios R1…R4 is the same as their number, we get the following IP addresses for the modems:

Device	RMAC address	tun0 IP address	eth0 IP address (suggestion)
router	-	-	192.168.1.1
R1	1	10.10.32.1	192.168.1.2
R2	2	10.10.32.2	192.168.2.1
R3	3	10.10.32.3	192.168.3.1
R4	4	10.10.32.4	192.168.4.1

Table 7.12 IP address, see Figure 7.20

Now we can define the routing tables with actual addresses:

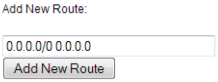
Device	Target network	gateway	notes
router	0.0.0.0/0	<WAN IP address or interface>	Default route is to internet
	192.168.2.0/24	192.168.1.2	LAN 2 via R1
	192.168.3.0/24	192.168.1.2	LAN 3 via R1
	192.168.4.0/24	192.168.1.2	LAN 4 via R1
R1	0.0.0.0/0	192.168.1.1	Default route is via the router to internet
	192.168.2.0/24	10.10.32.2	LAN 2
	192.168.3.0/24	10.10.32.3	LAN 3
	192.168.4.0/24	10.10.32.4	LAN 4
R2	0.0.0.0/0	10.10.32.1	Default route is via the radio network to R1
R3	0.0.0.0/0	10.10.32.1	Default route is via the radio network to R1
R4	0.0.0.0/0	10.10.32.1	Default route is via the radio network to R1
<other devices in the LANs>	0.0.0.0/0	<default gateway of the LAN as defined above>	We omit the details, but in principle each device in LANs 2, 3 and 4 will set the SATELLAR as their default gateway. Devices in LAN 1 use router as their default gateway.

Table 7.13 Routing tables with actual address, see Figure 7.20

To insert these routing tables to the SATELLAR CUs, use the Routing Application, IP Routes category. Note that you also need to change the routing in your other routers to gain full connectivity. In case of demonstrating and testing, the "router" is usually your PC.

Adding routing tables to SATELLAR

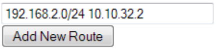
To add a new route with the WWW interface, insert the route in the text area and select Add New Route.



Add New Route:

0.0.0.0/0 0.0.0.0

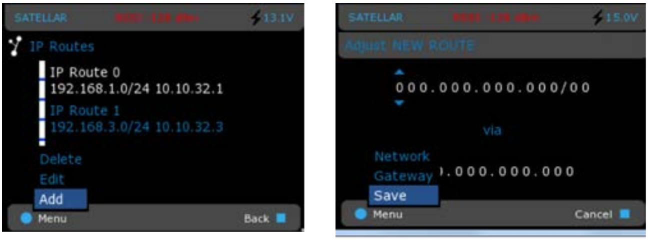
For example, to add a route to LAN 192.168.2.0/24 via the radio address 10.10.32.2, insert this:



192.168.2.0/24 10.10.32.2

You can also define a Metric for each route for redundant routing. See chapter 7.6.

To add a new route in LCD GUI, select Menu -> Add. Then modify destination Network (upper value) and Gateway (lower value). Changing the editing between upper and lower values, or Network and Gateway, is done with selection in Menu: select either Menu -> Network or Menu -> Gateway. When the route is ready, select Save. Alternatively select Cancel to abandon the route.

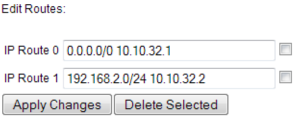


IP Route 0
192.168.1.0/24 10.10.32.1
IP Route 1
192.168.3.0/24 10.10.32.3

Adjust NEW ROUTE
000.000.000.000/00
via
).000.000.000

Figure 7.21 Add and Save new route

To edit existing routes with WWW interface, use the Edit routes functionality. Select apply to apply changes.

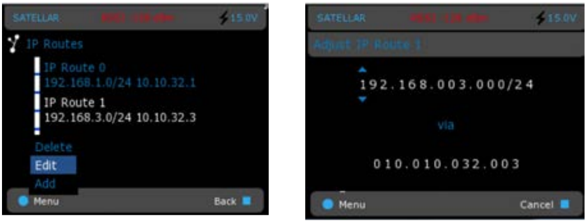


Edit Routes:

IP Route 0 0.0.0.0/0 10.10.32.1 □

IP Route 1 192.168.2.0/24 10.10.32.2 □

To edit IP routes with GUI: In the IP Routes view, highlight the route to edit and select Menu -> Edit.



IP Route 0
192.168.1.0/24 10.10.32.1
IP Route 1
192.168.3.0/24 10.10.32.3

Adjust IP Route 1
192.168.003.000/24
via
010.010.032.003

Figure 7.22 Edit IP routes

With WWW interface, set of IP Routes can also be created automatically, based on the provided parameters. The parameters are used as follows: the parameter Base address, together with Mask, defines the destination network for the first route. The next hop to this network will be the radio network IP address of the neighboring modem provided to the field First Address. For the next automatically created route, the destination network will be the next available network according to the Mask value.

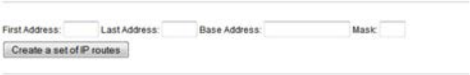
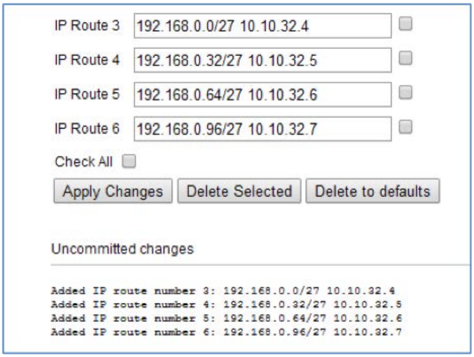


Figure 7.23 Create a set of IP routes

For eaxmple, with the Mask 27, the network size will be 32 addresses. So if the first automatically created route is to network 192.168.0.0/27, the next one will be to 192.168.0.32/27. The next hop for the next route will be the next radio network IP address in sequency. Automatic route creation will be applied further on for the next network and next radio IP address, until the radio network IP address specified in the field Last Address is reached.

Eaxmple 1. Setting “Base Address: 192.168.0.0 Mask: 27 First Address: 4 Last Address: 7” creates routes as presented in the following picture:



IP Route 3 192.168.0.0/27 10.10.32.4 □

IP Route 4 192.168.0.32/27 10.10.32.5 □

IP Route 5 192.168.0.64/27 10.10.32.6 □

IP Route 6 192.168.0.96/27 10.10.32.7 □

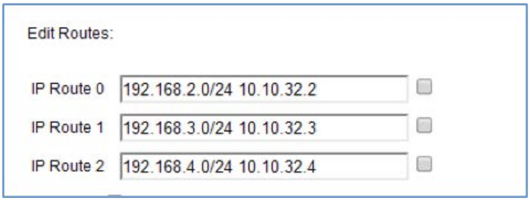
Check All □

Uncommitted changes

```
Added IP route number 3: 192.168.0.0/27 10.10.32.4
Added IP route number 4: 192.168.0.32/27 10.10.32.5
Added IP route number 5: 192.168.0.64/27 10.10.32.6
Added IP route number 6: 192.168.0.96/27 10.10.32.7
```

Figure 7.24 Example 1

Example 2: Setting the following “Base Address: 192.168.2.0 Mask: 24 First Address: 2 Last Address: 3” creates routes as presented in the following picture:



Edit Routes:

IP Route 0 192.168.2.0/24 10.10.32.2 □

IP Route 1 192.168.3.0/24 10.10.32.3 □

IP Route 2 192.168.4.0/24 10.10.32.4 □

Figure 7.25 Example 2

To delete a route with WWW interface, mark the checkbox and select the Delete Selected button. It is also possible to mark checkbox Chek All to select all routes. Deleting all routes at once is not recomended if you have more than 500 routes.

To detele a route with GUI, highlight the correct route and select Menu -> Delete Target.

With the WWW interface, Delete to defaults button deletes all routes from device. This is useful especially with large amount of routes. Note that this action does not ask for confirmation, but the routes are removed immediately.

If you have entered an invalid route, SATELLAR will print a red error text and the invalid route is not added. Finally, remember to click on the *Commit Changes* button, or *Cancel* applied changes if you made a mistake.

7.4 Serial IP

Serial IP is a feature where data coming from serial port is converted to IP packets and set to designated IP address. Correspondingly the received IP packets are converted and forwarded to serial interface. Serial IP configuration handling is divided into two sections for two interfaces:

- RS-232 connection in the radio unit (RU) and
- USB-Serial dongle attached to USB-A port of the central unit (CU).

Central Unit handles all the IP related data traffic and the air interface is IP based. Central Unit is needed for stations using the serial IP (CU, router). Central Unit is not required if the station is acting only as a repeater (no terminal connection).

NOTE! IP routing to the destination is not required if the IP data traffic is not entered to the SATELLAR radio modem via RJ45 connector and the sender target address is defined to be TUN0 address (radio address).

- The IP ports are selectable from port 1 to 65535. There are several ports already in use for various applications (NOTE! Application layer), e.g. http 80, https 443, SSH 21 and 22. Typically ports 1024 - 65535 are reserved for general purpose. EXCEPTIONS: Ports 54441, 54442 and 55555 are reserved for SATELLAR use.
- Due to the IP based data transfer, the transmission delays variate. The SCADA system shall be adjusted according to the SATELLAR Serial IP delays.

7.4.1 Serial IP RS-232 / USB-A

This section includes configurations related to both RS-232 and USB-A interface connection / serial IP functionality.

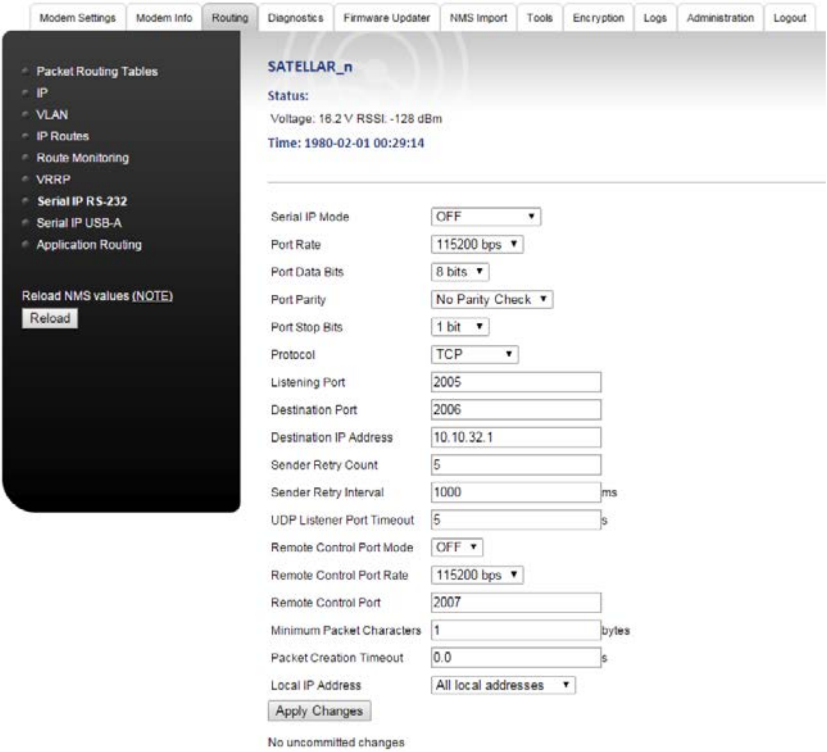
Attribute	Explanation	Sub unit	NMSID
Serial IP Mode	Server – Used in cases where the data transfer is initiated by some remote host. Server cannot open a connection, it can only answer to the request for opening the connection by Client.	1	3287
	Client – Used typically in cases where most of data transfer is initiated by this device. Client sends the request to the Server for the connection to be opened.		
	Send Only - In this mode device is able only to send data to from serial port to defined IP address and port i.e. not able to receive any sending.		
	Receive Only – In this mode device is able to only receive data to defined IP listening port and forward it to serial port .		

Attribute	Explanation	Sub unit	NMSID
	Twoway mode - This mode is meant to be used with TCP. In the other modes TCP can either only originate the connection (Client and Send Only) or listen to incoming connections (Server and Receive Only). In Twoway mode either side can either initiate or listen to connections.		
Port Rate	Rate of serial port – from 1200 to 460800 bps. Default is 19200.	1	3288
Port Data Bits	Serial Port Data Bits - 7 or 8.	1	3289
Port Parity	Serial Port Parity - No Parity, Odd, Even.	1	3290
Port Stop Bits	Serial Port Stop Bits – 1 bit or 2 bits.	1	3291
Protocol	TCP, UDP, Telnet or Bulk Mode. Must be coherent in network.	1	3292
Listening Port	IP Port for listening incoming messages. *	1	3293
Destination Port	IP Port for sending outgoing messages. **	1	3294
Destination IP Address	IP address for sending outgoing messages. **	1	3295
Sender Retry Count	Count for how many times messages are attempted to resent in TCP protocol if send does not succeed. ***	1	3296
Sender Retry Interval	The gap time between resending attempts (in TCP mode) in milliseconds. ***	1	3297
UDP Listener Port Timeout	Timeout for releasing the listener of one connection in UDP mode in seconds. This means that if there is no data received in defined time, connection is closed. New connection can be established at any time again. ****	1	3298
Remote Control Port Mode	Defines whether the RFC 2217 configuration possibility set on or off, default being off.	1	3299
Remote Control Port Rate	Port rate of remote control connection. Default is 115200.	1	3300
Remote Control Port	IP port of configuration.	1	3301
Minimum Packet Characters**	Minimum size of sent IP packets	1	3319
Packet Creation Timeout**	How long to wait for new serial data before creating IP packet	1	3320
Local IP Address	This is the address that remote clients will connect to when connecting to this device. It is also the sending address in case of outgoing traffic.	1	3404

* Parameter is effective when message listening is on (Server, Client, Receive Only).
** Parameter is effective when message sending is on (Server, Client, Send Only).
*** Parameter is effective when message sending is on (Server, Client, Send Only) with TCP protocol.
**** Parameter is effective when message listening is on (Server, Client, Receive Only) with UDP protocol.

Table 7.14 The configurations related to both RS-232 and USB-A interface connection / serial IP functionality

NOTE: The connection will be established only by the Client and only to the device acting in Server mode. Once the connection has been established, the data traffic can be both ways. The connection will be kept open as long as the SATELLAR central units are running. The connection is closed by the Client or the connection is opened to another destination by the Client.



SATELLAR_n

Status:

Voltage: 16.2 V RSSI: -128 dBm

Time: 1980-02-01 00:29:14

Serial IP Mode	OFF ▾
Port Rate	115200 bps ▾
Port Data Bits	8 bits ▾
Port Parity	No Parity Check ▾
Port Stop Bits	1 bit ▾
Protocol	TCP ▾
Listening Port	2005
Destination Port	2006
Destination IP Address	10.10.32.1
Sender Retry Count	5
Sender Retry Interval	1000 ms
UDP Listener Port Timeout	5 s
Remote Control Port Mode	OFF ▾
Remote Control Port Rate	115200 bps ▾
Remote Control Port	2007
Minimum Packet Characters	1 bytes
Packet Creation Timeout	0.0 s
Local IP Address	All local addresses ▾

No uncommitted changes

Figure 7.26 Configuration of Serial IP RS-232 via WWW-interface

7.4.2 Examples

7.4.2.1 Point-to-point

Example “Point-to-point” presents the basic feature and usage of configuration parameters.

Two user devices DTE A and B are connected to SATELLARs via serial port connection and the SATELLARs are configured to have a radio connection.

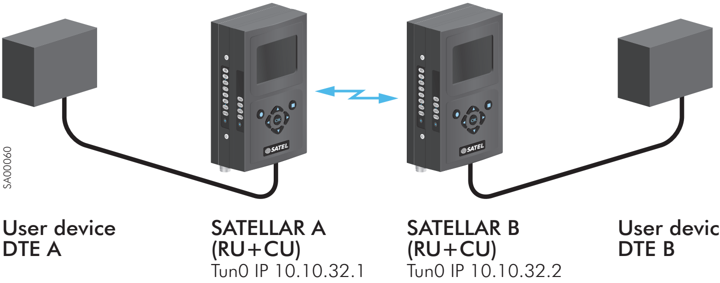


Figure 7.27 Point to point -example

SATELLAR A is having Tun0 IP 10.10.32.1 and SATELLAR B Tun0 IP 10.10.32.2 (can be obtained from screen saver or from Routing – IP category). SATELLAR B is a client which is the side that initiates the connection. It has been configured to listen messages from serial port, to send them to target address and port. SATELLAR A is a server side that has been configured to listen dedicated IP port and to forward messages to serial port. Transmission is always started from client side; it creates the connection between the SATELLARs. There are some differences for this when using UDP, see chapter 7.4.2.5 UDP.

First, the serial port in both SATELLARs must be configured to match the User device configuration. After that, the SATELLAR devices are able to communicate with each others.

Parameter	SATELLAR A	SATELLAR B
Mode	Server	Client
Protocol	TCP	TCP
Listening Port	2005	Irrelevant in this mode
Sending Port	Irrelevant in this mode	2005
Sender Target Address	10.10.32.2	10.10.32.1

Table 7.15 Configuration of SATELLAR a and B devices in Point to point- example

The basic idea is to cross-configure SATELLAR devices to communicate with each other. Protocol can be also UDP as long as it is same in both ends.

7.4.2.2TCP Server

SATELLAR is configured to listen to defined IP Port number and forward data from the port to the serial port (IP to Serial-conversion).

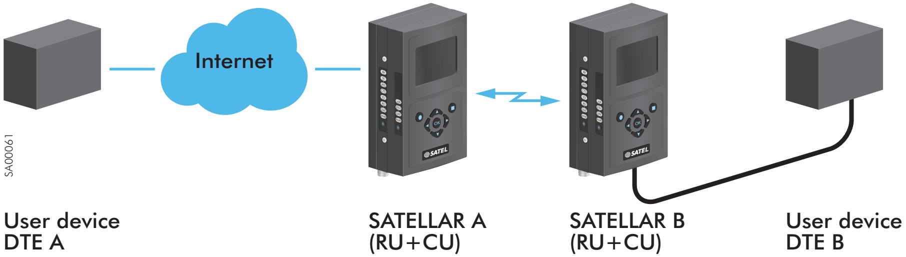


Figure 7.28 TCP Server, conversion from IP to serial port

DTE A

Ethernet IP Address 192.168.1.1
IP Route 192.168.2.0/24 via 192.168.1.2
Application able to send messages to dedicated address
and port configured to send to 192.168.2.10 port 2006

SATELLAR A

Ethernet IP Address 192.168.1.2
RMAC 1 i.e. Tun0 10.10.32.1
Packet Route to 2
IP Route 192.168.2.0/24 via 10.10.32.2

SATELLAR B

Ethernet IP Address 192.168.2.10
RMAC 2 i.e. Tun0 10.10.32.2
Packet Route to 1
IP Route 192.168.1.0/24 via 10.10.32.1
Serial IP configuration as above
Serial port configuration in line with User device DTE B

DTE B

Serial port configuration in line with SATELLAR B

User Device DTE A has an Ethernet IP address 192.168.1.1. SATELLAR B has two IP addresses Tun0 10.10.32.2 and Eth0 192.168.2.10 which both can be used depending on the routing configuration in User device DTE A. Ethernet address is used in this example.

SATELLAR A does not have any Serial IP connection and it is configured to have radio connection with SATELLAR B. User device DTE A must be set to route messages to SATELLAR B via SATELLAR A. In this case SATELLAR A has an IP 192.168.1.2, User device DTE A must have a route 192.168.2.0/24 via 192.168.1.2 and must also have an application able to send messages to dedicated address and port, in this case to port 2006 at 192.168.2.10.

Parameter	SATELLAR B
Mode	Server
Protocol	TCP
Listening Port	2006

Table 7.16 Serial port conficuration of SATELLAR B

Sending of parameters is not necessary, since TCP is capable of sending replies back when connection has been opened.

7.4.2.3TCP Client

In TCP client case whenever data comes from the serial port, the data is buffered and sent to target address. This can be e.g. some on-demand service sending some e.g. log data whenever there is something to send. Setup is similar to server case.

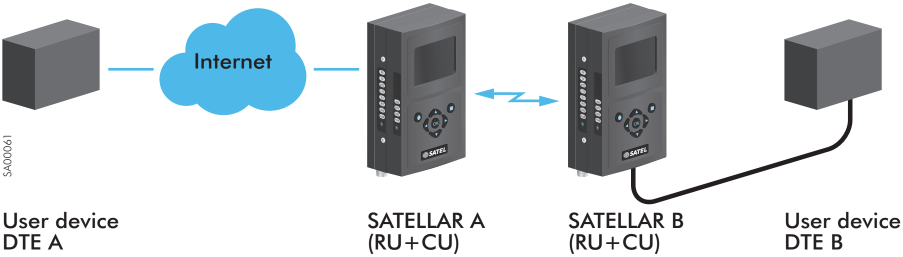


Figure 7.29 TCP Client

DTE A: IP address 192.168.1.1
SATELLAR A: IP address 192.168.1.2
SATELLAR B: IP address 192.168.2.10

User Device DTE A has IP address: 192.168.1.1, SATELLAR A: 192.168.1.2 and SATELLAR B: 192.168.2.10. SATELLARs are configured to have the radio connection and IP routes are configured so that devices are able to communicate with each other i.e. route from User device DTE A to SATELLAR B via SATELLAR A and from SATELLAR B to User device DTE A via SATELLAR A.

User device DTE A must now have an application that opens port listening to messages coming from SATELLAR B. SATELLAR A does not have any Serial IP configuration. SATELLAR B has following serial port configuration, where it is assumed that User Device DTE A has port 2005 open:

Parameter	SATELLAR B
Mode	Client
Protocol	TCP
Sending Port	2005
Sender Target Address	192.168.1.1

Table 7.17 Serial port conficuration of SATELLAR B

7.4.2.4Multipoint-to-point

Multipoint-to-point case can be presented as an extended case of TCP Client.

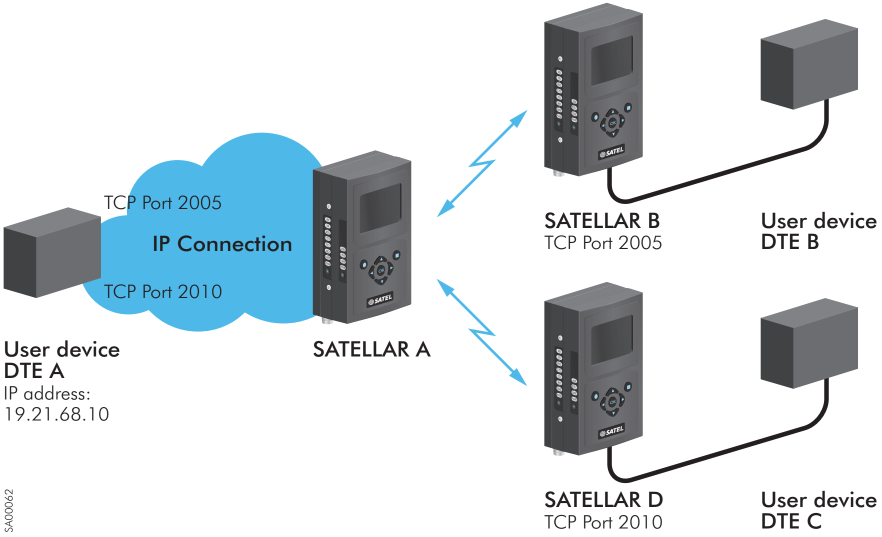


Figure 7.30 Multipoint-to-point -example

In this example the User device DTE A is capable of simultaneously listening to several ports. Both SATELLAR B and SATELLAR C are configured to send messages to User device DTE A, but to different ports. Following configuration is set to SATELLAR B and SATELLAR D, when User device DTE A has IP address 192.168.1.1:

Parameter	SATELLAR B	SATELLAR C
Mode	Client	Client
Protocol	TCP	TCP
Sending Port	2005	2010
Sender Target Address	192.168.1.1	192.168.1.1

Table 7.18 The configuration of SATELLAR B and SATELLAR C

One option for this kind of tasking is serial port virtualizing that can be done e.g. with HW VSP application: **http://www.hw-group.com/products/hw_vsp/index_en.html**

The application creates virtual serial ports which are actually IP addresses and ports i.e. user defines IP address and port combination which then creates a (virtual) serial port to system. By this way different applications can use these connections as serial ports although they are actually IP connections.

7.4.2.5UDP

UDP mode can be used similar to TCP modes with some extension.

In point-to-point case the mode of the device can be either client or server. Due to nature of protocol both devices need to be able to send and receive independent of other device. See chapter 7.4.3 UDP and TCP protocols for more detailed protocol explanation.

Parameter	SATELLAR A	SATELLAR B
Mode	Server	Server
Protocol	TCP	TCP
Listening Port	2005	2006
Sending Port	2006	2005
Sender Target Address	10.10.32.2	10.10.32.1

Table 7.19 Example of point-to-point case

When using UDP in Server mode in generally and some replies are needed to be sent, also the target address needs to be set. This concerns also the Client mode and listening of replies.

Parameter	SATELLAR B
Mode	Server
Protocol	UDP
Listening Port	2006
Sending Port	2005
Sender Target Address	192.168.1.1

Table 7.20 The conficuration of SATELLAR B

7.4.2.6Send or receive only

These features are limited versions of presented features. The example is similar to point-to-point.

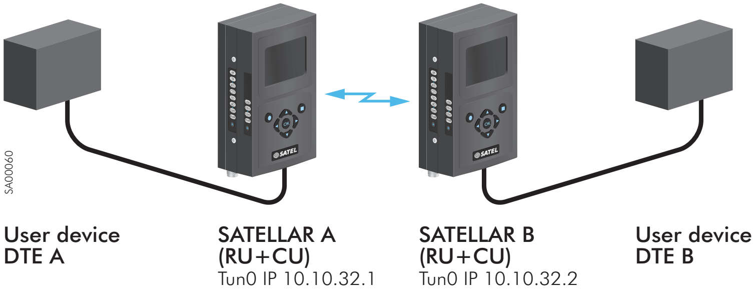


Figure 7.31 Send or receive only -example

SATELLAR A is having Tun0 IP 10.10.32.1 and SATELLAR B Tun0 IP 10.10.32.2. SATELLAR A is configured to send to SATELLAR B and SATELLAR B is configured to listening defined port.

Parameter	SATELLAR A	SATELLAR B
Mode	Send only	Receive only
Protocol	UDP	UDP
Listening Port	Irrelevant in this mode	2006
Sending Port	2006	Irrelevant in this mode
Sender Target Address	10.10.32.2	Irrelevant in this mode

Table 7.21 The conficuration of SATELLAR A and SATELLAR B

The User device DTE A can only send and the User device DTE B can only listen the messages.

7.4.3 UDP and TCP protocols

Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are both based on Internet Protocol (IP) suite. They are used for relaying datagrams - also known as network packets – from the source host to the destination host solely based on the addresses. Packets are structured by Open Systems Interconnection (OSI) model layer principles. OSI model structures packets to different layers and TCP and UDP packets can quite simply be presented with these layers:

- Data link layer: Physical addresses i.e. source and destination MAC addresses
- Internet layer: IPv4 / IPv6 addresses and related header
- Transport Layer: TCP, UDP or similar protocol data (ports etc.) and related header
- Application Layer: Actual user data

Following tables present the structure of data. Data link layer data comes first and in the end there is frame footer. Between the frame data and footer is IP packet data. In IP packet internet layer data is first, then the transport layer i.e. protocol related data and finally actual user data.

Data Link layer

Frame header (8 bytes)	Frame data (14 bytes)	IP + UDP packet (below)	Frame footer i.e. CRC (4 bytes)

IP Packet

bits	0-3	4-7	8-13	14-15	16-18	19-31
0	Version	Internet Header Length	Differentiated Services Code Point	Explicit Congestion Notification	Total Length	
32	Identification				Flags	Fragment Offset
64	Time To Live		Protocol		Header Checksum	
96	Source Address					
128	Destination Address					
160+	Data (UDP Packet)					

UDP Packet

bits	0-7	8 – 15	16 – 23	24 – 31
0	Source Port		Destination Port	
32	Length		Checksum	
64+	Data (actual user data)			

Thus IP + UDP Packet headers are altogether 28 bytes. TCP packet is alike the UDP with some more information in TCP section such as sequence number. TCP header is thus larger (20 bytes) than UDP (8 bytes).

The difference between the protocols is the administration of packets and how the received packets are supposed to be handled. UDP is a not connection based simple transmission model without implicit handshaking dialogues for providing reliability, ordering, or data integrity. Thus, datagrams may arrive out of order, appear duplicated, or go missing without notice. UDP assumes that error checking and correction is either not necessary or performed in the application, avoiding the overhead of such processing at the network interface level. TCP on the other hand is connection based protocol which provides error checking, ordering and general reliability.

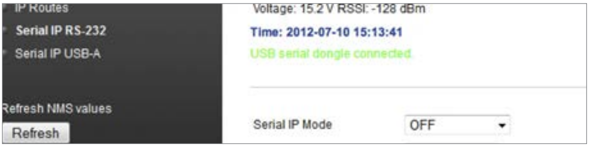
Time-sensitive applications often use UDP because dropping packets is preferable to waiting for delayed packets. Also as described above, the size of headers - i.e. packet overhead - is smaller with UDP which may make difference when the size of actual data is always small. Examples of applications using UDP are DHCP, DNS and voice and video applications. On the other hand, if error correction facilities, ordering and general reliability is needed, an application may use the TCP. Examples of using TCP are HTTP, FTP, SMTP and SSH.

7.4.4 Notes

There are some noticeable issues, which are related to serial IP functionality.

7.4.4.1 USB Serial dongle connection

Availability of USB serial connection is informed with different notes. When USB serial dongle is connected, the following text is shown in the screen: USB serial dongle connected.



Voltage: 15.2 V RSSI: -128 dBm

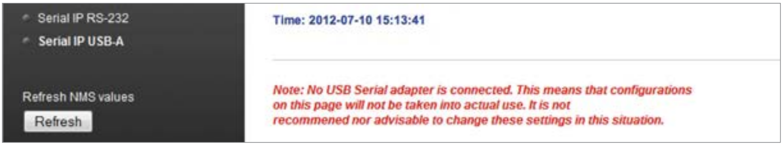
Time: 2012-07-10 15:13:41

USB serial dongle connected

Serial IP Mode OFF

Figure 7.32 USB serial dingle connected

If not connected, then note about interface being not available is shown.



Time: 2012-07-10 15:13:41

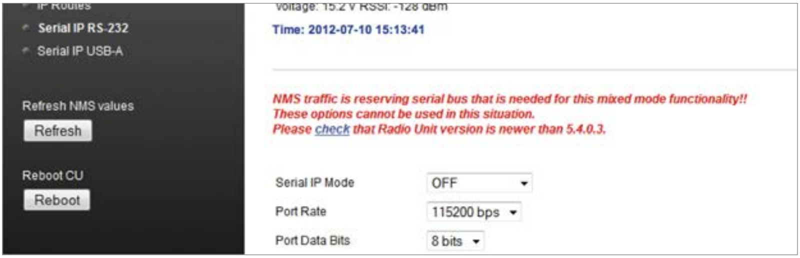
Note: No USB Serial adapter is connected. This means that configurations on this page will not be taken into actual use. It is not recommened nor advisable to change these settings in this situation.

Figure 7.33 USB serial dongle not connected

Please make sure that Serial IP Mode is OFF when USB serial dongle is not connected.

7.4.4.2 RS-232 port availability

In some occasions RS-232 is reserved and cannot be used for Serial IP functionality. Following text is displayed in such occasions.



Voltage: 15.2 V RSSI: -128 dBm

Time: 2012-07-10 15:13:41

NMS traffic is reserving serial bus that is needed for this mixed mode functionality!!
These options cannot be used in this situation.
Please check that Radio Unit version is newer than 5.4.0.3.

Serial IP Mode: OFF
Port Rate: 115200 bps
Port Data Bits: 8 bits

7.4.4.3 Disconnecting USB Serial dongle

When disconnecting the USB Serial dongle the Serial IP Mode must to be set OFF. Detaching the dongle when the mode is not OFF sets the device in to a fault state and may even reboot the device. If the Serial IP Mode is ON, but the dongle is not connected, following warning text is displayed at web UI: USB serial IP mode is on but dongle is not connected!! Pelase set the mode off.

7.4.4.4 Incompatible parameter combinations

There are some parameter combination cases that can make the connection ends incompatible:

– Different protocols: It must be verified that both connection ends have the same protocol. When one connection end uses TCP and other UDP, connection cannot work.
– Compatible modes: If both ends have either send only or receive only mode on, connection does not work as assumed. On the other hand, when using send only on one end and receive only on other end, it must be verified that send only is in the end intended to send data.
– Ports and addresses: Ports and addresses must match in the setup. I.e. the sending target address and port must match with IP address of listener and the port that is opened for listening.

7.5 Virtual Local Area Network (VLAN)

Virtual LAN (VLAN) is a feature that allows a physical LAN network to be devided into separate networks. All devices connected to same VLAN can communicate with each other as if they were connected to the same physical LAN.

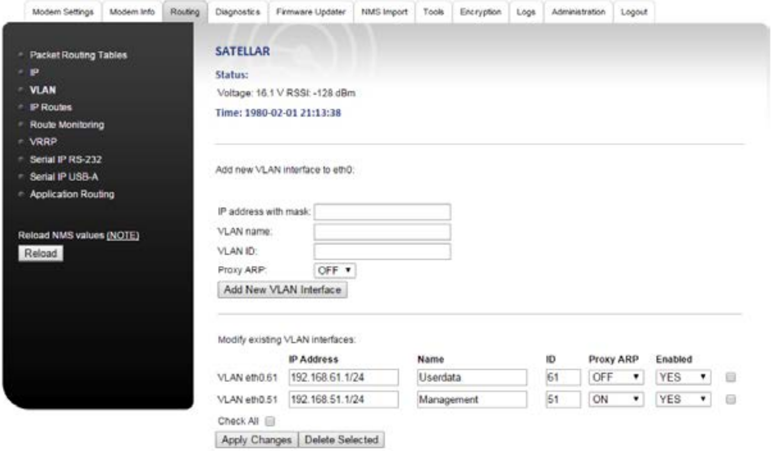
The Vlan operation and functionality is described in the IEEE (Institute of Electrical and Electronics Engineers) standards 802.1q

The SATELLAR supports VLAN in its Ethernet port (eth0). The ethernet interface accepts those ethernet frames that have a VLAN tag matching any of the VLAN IDs configured to SATELLAR. SATELLAR removes any VLAN tag from the accepted frames after receiving them and correspondingly adds VLAN tag with a correct ID to the frames sent out from the VLAN interface. The VLAN information is not carried over the radio and cannot be configured to the radio interface.

7.5.1 VLAN settings

The VLAN settings are available under the Routing menu, at the VLAN page. This applies for both, the GUI on the modem display and the WWW user interface. In the VLAN configuration page, VLAN interfaces can be added, modified or removed.

7.5.1.1 WWW user interface



SATELLAR

Status:

Voltage: 16.1 V RSSI: -128 dBm

Time: 1980-02-01 21:13:38

Add new VLAN interface to eth0:

IP address with mask:

VLAN name:

VLAN ID:

Proxy ARP: OFF ▾

Add New VLAN Interface

Modify existing VLAN interfaces:

	IP Address	Name	ID	Proxy ARP	Enabled	
VLAN eth0.61	192.168.61.1/24	Userdata	61	OFF ▾	YES ▾	□
VLAN eth0.51	192.168.51.1/24	Management	51	ON ▾	YES ▾	□

Check All □

Apply Changes | Delete Selected

The WWW UI is divided into two sections: add new VLAN interface and modify existing VLAN interfaces. To add a new VLAN interface, fill the empty fields with correct values and then select Add new VLAN. The fields have the following definitions:

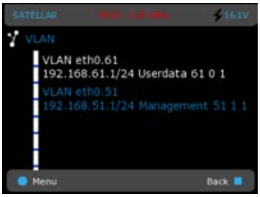
To add a new VLAN interface, fill the empty fields with correct values and then select Add new VLAN. The fields have the following definitions:

Name	Explanation
IP address	The IP address and the net mask of the VLAN interface. The IP address should be unique. The address is given in the same format as the eth0 IP address, for example: 192.168.51.1/24
VLAN name	A descriptive name for VLAN. Must be 1-31 characters long and can contain only alphanumeric symbols. All specified VLANs must have unique names.
VLAN ID	A number from the range 1-4094, identifying the VLAN. Each device connected to the same VLAN network must have the same ID.
Proxy ARP	Enable or Disable Proxy ARP operation for this VLAN interface.

Table 7.22 The conficurations related to creating and modifying VLANs

You can add multiple VLANs. When all desired VLANs have been added, select Apply Changes and Commit Changes as when modifying any other parameter. To delete a VLAN, select the checkbox next to it and choose Delete Selected and Commit Changes.
You have the option to disable a VLAN instead of deleting it completely. The last field in every VLAN is Enabled, that can be set to NO. Remember to Apply and Commit changes. Every VLAN will be enabled by default.

7.5.1.2 GUI

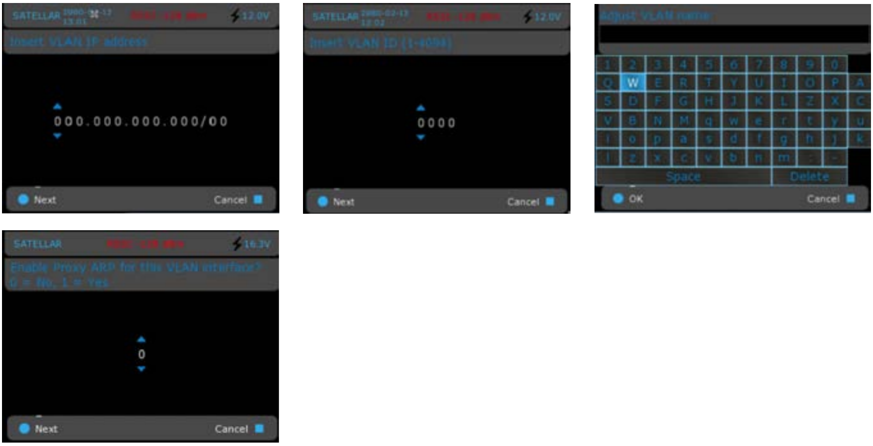


```
VLAN eth0.61
192.168.61.1/24 Userdata 61 0 1
VLAN eth0.51
192.168.51.1/24 Management 51 1 1
```

Figure 7.34 VLAN configuration screen

The following information is displayed for each VLAN interface: The automatically generated name, the IP address and mask, a descriptive name, the VLAN ID, Proxy ARP status (0 indicates that Proxy ARP is off, 1 indicates that Proxy ARP is on for this interface) and if the interface is enabled or not (1 indicates enabled and 0 disabled).

To add a new VLAN interface, select Menu -> Add, which starts a configuration wizard. The wizard will go through three different editors asking to insert the IP address, VLAN ID, Proxy ARP status and the name of the VLAN interface. Refer to the previous section for more detailed explanation of each parameter. In each stage, after inserting the value, select Next to proceed to next step. After you have set valid values to all fields, the new VLAN interface has been created and it appears in the list.



Insert VLAN IP address

000.000.000.000/00

Insert VLAN ID (1-4094)

0000

Adjust VLAN name

Enable Proxy ARP for this VLAN interface?
0 = No, 1 = Yes

0

Figure 7.35 Configuring VLAN interface

To edit an existing VLAN interface, navigate to the corresponding interface and select Menu -> Edit. This launches a wizard, which guides you through editing the interface parameters. The wizard is similar to one used when adding a new VLAN interface. To remove a VLAN, navigate to the respective entry to be removed and select Menu - > Delete.

When finished with adding, modifying or removing VLAN interfaces save the settings by pressing the Back button twice to return to the main menu: you will be prompted to save the settings.

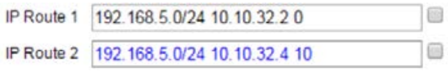
7.6 Redundant Routing

With the SATELLAR it is possible to define multiple routes to one destination, so that if one route fails a secondary route can be used. Redundant routing is required both in the radio interface and Ethernet interface for the end-to-end connection to be fully redundant. Virtual Router Redundancy Protocol (VRRP) is used for Ethernet redundancy and Route Monitoring for radio redundancy.

This chapter is divided into three sections: Section 7.6.1 describes Route Monitoring and radio redundancy. Section 7.6.2 describes VRRP and Ethernet redundancy. Section 7.6.3 describes how to use the two features together to create redundant networks and contains several examples.

7.6.1 Route monitoring

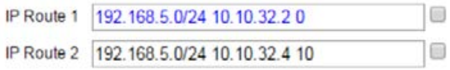
Route monitoring is used if several IP routes are defined to the same destination (see section 7.3.3 for more information about IP routes). If more than one route is defined to one destination, they must have different metric values. Metric is a parameter describing the cost of the route, so a smaller value means a preferred route. For example here are two routes specified to subnetwork 192.168.5.0/24:



IP Route 1 192.168.5.0/24 10.10.32.2 0 ☐

IP Route 2 192.168.5.0/24 10.10.32.4 10 ☐

The number seen after the gateway is the metric. The route using gateway 10.10.32.2 has a smaller metric, so it is used by default. The route currently not in use is marked blue in the WWW interface. Now if the SATELLAR with the address 10.10.32.2 drops off the network, the local device will switch to the alternative route:



IP Route 1 192.168.5.0/24 10.10.32.2 0 ☐

IP Route 2 192.168.5.0/24 10.10.32.4 10 ☐

In those cases, the following warning can also be seen in the WWW UI to inform the user that the primary route is not available:

WARNING: One or more primary IP routes are not in use. See Routing->IP Routes or Logs->Service Messages for more information

Also, the following log entry will appear in the Logs -> Service Messages page:

```
Changing route to 192.168.5.0/24 from 10.10.32.2 to 10.10.32.4
```

The SATELLAR uses ICMP echo messages to determine is the gateway usable or not. The parameters to determine when to switch routes can be seen in table down below:

Item	Explanation	Sub unit	NMSID
Check Interval	How often in seconds a gateway is checked	1	2700
Only Check With Traffic	If set to Yes, routes will only be monitored if there is traffic to that network. This will cause less unnecessary traffic in the network, but on the other hand an unusable route will only be detected the next time any traffic is sent. If set to No, routes will be monitored regardless of traffic. This option should not be used if Only Check With Traffic is set to Yes.	1	2701
Allowed Fail Count	How many times must a gateway fail to respond before being determined unavailable	1	2702
Revert Timer	How often in seconds will a higher priority route be checked to see if it is available again	1	2703
Ping Timeout	The allowed timeout for the ICMP query.	1	2704
Only Monitor Primary	If set to Yes, only the primary route is monitored. When changed to backup route, the primary route will be monitored based on revert timer, and when it answers again the route will revert to it. The backup route(s) will not be monitored, even if they are in use.	1	2705

Table 7.23 Routing, Route monitoring

Every check interval, the local SATELLAR will send a message to the currently used gateway of a network. If the gateway fails to answer more times than the allowed fail count indicates alternative gateways with higher metrics will be pinged. If a working gateway is found, all traffic to the networks will be routed through that gateway.

If the used route is not the primary route, gateways with lower metrics will be contacted regularly. If connection is re-established, traffic is again routed through that device. Revert timer indicates how often routes with lower metrics will be contacted.

Route monitoring quality is a trade-off between time and network traffic. If switching to a secondary route needs to be fast, a lot of extra traffic is generated into the network. Let's say that check interval is 30 seconds and allowed fail count is 3. There are two alternative gateways to one remote network. Then the SATELLAR will notice that a gateway is not working in at most 30 * (3 + 1) = 120 seconds. With those parameters, one monitoring message will be generated every 30 seconds.

If there are multiple remote networks, each with their own alternative gateways, the networks will be checked one at a time every check interval. So if in the previous example there are two remote networks, the SATELLAR will notice that a gateway is not working in at most 30 * (3 + 1) * 2 = 240 seconds. One monitoring message will still be generated every 30 seconds.

7.6.2 VRRP

Virtual Router Redundancy Protocol is a networking protocol that automatically assigns a virtual IP address to one machine in a network. It has been specified in IETF publication RFC 5789 (http://tools.ietf.org/html/rfc5798), VRRP will be described in this section to the extent that is relevant to usage with SATELLAR.

The SATELLAR can use VRRP in its Ethernet interface, either eth0 or any VLAN interface. When multiple SATELLAR devices are in the same Ethernet network, one of them is the master router and the rest of them are backup routers. In addition to its own IP address, the master router has a designated virtual IP address. If the device somehow becomes unusable, if it loses power or radio connectivity for example, the virtual IP address will be assigned to one of the backup routers. Because of this, any other device located in the network can use the virtual IP address as its gateway, and it does not have to know which physical Satellar it is using.

The parameters used to control VRRP can be seen in table down below:

Item	Explanation	Sub unit	NMSID
VRRP State	Is VRRP ON or OFF	1	2710
VRRP Virtual IP Address*	The virtual IP address	1	2711
VRRP Virtual Router ID*	Router ID to identify the router group	1	2712

Item	Explanation	Sub unit	NMSID
VRRP Priority	Priority of the SATELLAR. The highest priority device is the master in normal conditions	1	2713
VRRP Advertisement Interval*	How often in seconds is the status of the virtual router checked	1	2714
VRRP Check Target Radio IP	This is an IP address behind the radio interface that the SATELLAR needs to be able to reach in order to be a master	1	2715
VRRP Interface	Which interface is VRRP used with. The Ethernet interface is eth0, and any VLAN interface is eth0.X where X is the VLAN ID	1	2716
VRRP Check Target Local IP	This is an IP address behind the Ethernet interface that the SATELLAR needs to be able to reach in order to be a master	1	2717
VRRP Virtual RMAC Address	Beta version of a feature, where the RMAC address of the device is changed along with the IP address, to make route monitoring in substations unnecessary. See section 7.6.3.5 for more information.	1	2718

* These parameters must all be the same in one virtual router

Table 7.24 Routing, VRRP

The group of SATELLAR devices in the Ethernet network works as a single virtual router with the virtual IP address as the gateway for every other device. Each device must have the same virtual router ID as well as the advertisement interval.

Each device has a priority, from 2 to 255 (priority 1 is reserved in the Satellar for internal use). The active device with the highest priority is the master at any given time. Every advertisement interval the device sends a multicast packet to all other devices in the network.

If a master router fails to send the advertisement packets, the other devices assume that the master has failed and go into an election process to set the device with the largest priority to be the new master. If a device with a higher priority enters the network at some point, it will be elected as the new master.

There are several reasons for the master to fail. The clearest ones are power failure or disconnection from the Ethernet network. In those cases it is clear that the master stops sending advertisements. But there are also other ways it can fail: if it loses connectivity to the radio network or the Ethernet network. For those cases, it is possible to determine check target IP addresses, which will be checked regularly. Rules from route monitoring (see section 7.6.1) will be used to determine when connectivity is lost. By default the IP addresses are 0.0.0.0, in which case no checking is done.

If the device cannot connect to either of the defined IP addresses, it forces itself to be a backup router and signals the rest of the devices in the network to start an election for a new master.

The status of the VRRP can be seen in the WWW interface, one of the following messages is always displayed at the top of the page when VRRP is on:

- INFO: VRRP is in BACKUP state
- INFO: VRRP is in MASTER state
- INFO: VRRP is in BACKUP state, cannot connect to Target Radio IP
- INFO: VRRP is in FAULT state, cannot connect to Target Local IP
- INFO: VRRP is in FAULT state

More information about the VRRP process can be found in the Logs -> System Messages page by searching for entries from process keep alived.

7.6.3 Building a redundant network

7.6.3.1 Example 1: Redundant master station with one substation

This is perhaps the simplest example of a redundant network. Two data terminal equipment (DTE) devices are connected by SATELLARs. DTE A is connected to SATELLARs R1 and R2 via Ethernet; DTE B is connected to SATELLAR R3.

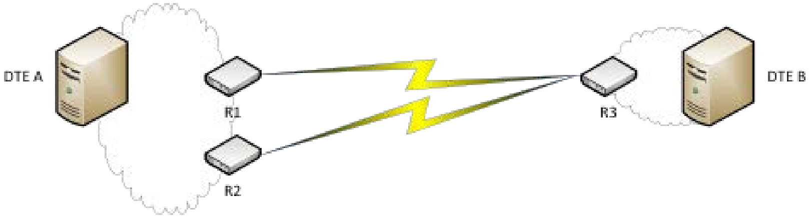


Figure 7.36 Example 1

R1 and R2 have VRRP running. R3 does not have VRRP, but it has two IP routes to DTE A. In this setup, if either R1 or R2 breaks down, traffic will still continue to flow. But if R3 breaks down, traffic will naturally stop.

The devices have the following addresses:

Device	IP Address	RMAC Address
DTE A	192.168.1.100/24	-
R1	192.168.1.1/24	1
R2	192.168.1.2/24	2
R3	192.168.3.1/24	3
DTE B	192.168.3.100/24	-

Both R1 and R2 have radio connectivity to R3. The following VRRP settings will have been changed from their default values:

Setting	R1	R2
VRRP State	On	On
VRRP Virtual IP Address	192.168.1.10/24	192.168.1.10/24
VRRP Virtual Router ID	10	10
VRRP Priority	255	100
VRRP Check Target Radio IP	192.168.3.1	192.168.3.1

R1 has a higher priority, so in normal circumstances it will be the VRRP master and hold the virtual IP address 192.168.1.10/24. Both have defined 192.168.3.1 as the IP address to use, that will determine are radio communications working or not. Other valid IP addresses to use are for example 10.10.32.3 and 192.168.3.100.

DTE A can use the virtual IP address 192.168.1.10 as the gateway to DTE B, it does not need to know which STAELLAR is using the address. DTE B will use 192.168.3.1 as the gateway.

Both R1 and R2 have a normal IP route defined to 192.168.3.0/24 via 10.10.32.3. But R3 will have the following IP routes defined:

- 192.168.1.0/24 via 10.10.32.1, metric 0
- 192.168.1.0/24 via 10.10.32.2, metric 10

So the primary route goes through R1. If something happens to R1, if it is for example powered off or the Ethernet cable is disabled, R2 will become the master and R3 will route all traffic going to DTE A through R2. It uses the default route monitoring parameters, so it will notice if a device is missing in 2-3 minutes. If R1 starts working again, R3 will revert to using R1 again in at most 5 minutes. If R3 stops working traffic will stop, so the network is not fully redundant.

7.6.3.2Example 1: Redundant master station with multiple substations

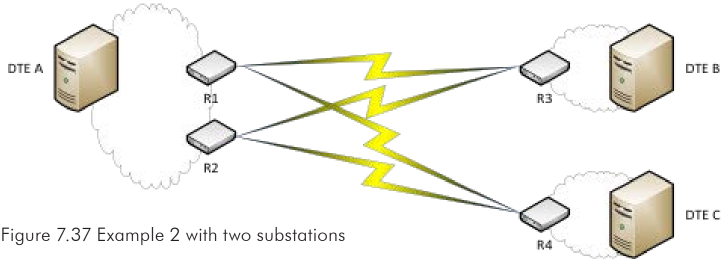


Figure 7.37 Example 2 with two substations

The new devices have the following addresses:

Device	IP Address	RMAC Address
DTE C	192.168.4.100/24	-
R4	192.168.4.1/24	4

This actually changes very little for the other devices. R1 and R2 need to add normal packet and IP routes to R4. The VRRP settings in R1 and R2 can remain unchanged, although there is the option of changing the Check Target Radio IP to that of R4 or DTE C. This will only affect which device will be used to determine if the radio of the VRRP master is working, so generally it is a good idea to select the substation with the best connectivity.

R4 will have the following IP routes defined:

- 192.168.1.0/24 via 10.10.32.1, metric 0
- 192.168.1.0/24 via 10.10.32.2, metric 10

Again, in this setup traffic will continue to flow even if R1 or R2 face some sort of problem.

Using this example, more substations can be added. With every new substation, basically two steps need to be done:

- A route to the new substation needs to be added to R1 and R2
- The new substation needs routes specified to R1 and R2

It should be noted that each new substation adds more extra traffic to the network, since each substation will regularly determine is R1 still usable or not. If the monitoring messages start to hamper the actual traffic in the network, the route monitoring could be made more infrequent. This of course means that the substations will be slower to update the route when needed.

There is also an alternative option: enabling the “Only Check With Traffic” option in Route Monitoring. In those cases the substations will only check the availability of R1 when there is actually any traffic from the substation to 192.168.1.0/24 (this includes replies to messages sent by DTE A, so the substation does not need to generate traffic spontaneously). This will make the network load lighter, but it means that the first time traffic is directed to a substation there will always be a delay before the traffic works.

Note: The device specified to be the Check Target Radio IP for R1 and R2 will always have traffic, because the VRRP master will use it to determine that its radio is working. So in practice the option will have no effect for that substation.

7.6.3.3Example 3: Two fully redundant routes

In this example there are two alternative routes between DTE A and DTE B.

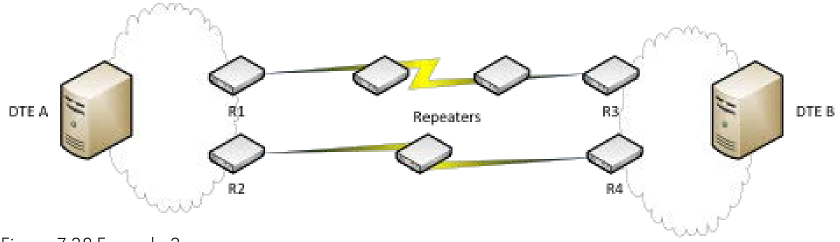


Figure 7.38 Example 3

R1 and R3 will have packet and IP routes defined to each other, as will have R2 and R4. No IP routes with different metric values will be needed. There can be any number of repeaters between either of the two pairs. The two routes should not use common repeaters, because that would cause a single point of failure. The point of this example is to create a network that will work if any one device malfunctions.

The devices have the following addresses:

Device	IP Address	RMAC Address
DTE A	192.168.1.100/24	-
R1	192.168.1.1/24	1
R2	192.168.1.2/24	2
R3	192.168.3.1/24	3
R4	192.168.3.2/24	4
DTE B	192.168.3.100/24	-

All four non-repeater SATELLARs will have VRRP enabled with the following parameters:

Setting	R1	R2	R3	R4
VRRP State	On	On	On	On
VRRP Virtual IP Address	192.168.1.10/24	192.168.1.10/24	192.168.3.10/24	192.168.3.10/24
VRRP Virtual Router ID	10	10	30	30
VRRP Priority	255	100	255	100
VRRP Check Target Radio IP	192.168.3.10	192.168.3.10	192.168.1.10	192.168.1.10

DTE A will have 192.168.1.10 as its gateway and DTE B will have 192.168.3.10. R1 and R3 are the VRRP masters by default.

Now, if R1 or R3 or any repeater between them will stop working, R2 and R4 will become the VRRP masters and traffic will flow through them.

It is possible to add as many networks as one wishes, by adding extra SATELLAR devices.

7.6.3.4Example 4: Fully redundant network

The problem in Example 3 is that if one device on both routes breaks down, traffic will stop. If the two networks are close enough that they do not require repeaters, it is feasible to build a fully redundant network between DTE A and DTE B.

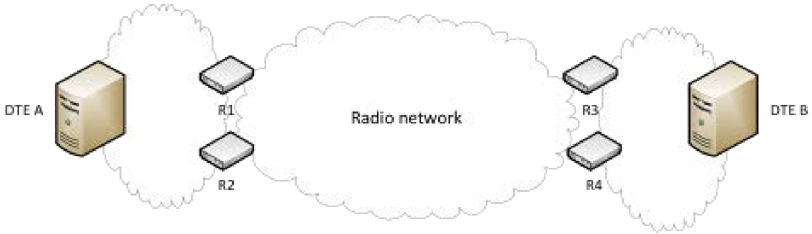


Figure 7.39 Example 4

The VRRP settings and IP addresses can be used directly from Example 3, but the routing will look significantly different. The packet and IP routes will look like this:

Device	Packet routes	IP route 1	IP route 2
R1	3, 4	192.168.3.0/24 via 10.10.32.3, metric = 0	192.168.3.0/24 via 10.10.32.4, metric = 5
R2	3, 4	192.168.3.0/24 via 10.10.32.3, metric = 0	192.168.3.0/24 via 10.10.32.4, metric = 5
R3	1, 2	192.168.1.0/24 via 10.10.32.1, metric = 0	192.168.1.0/24 via 10.10.32.2, metric = 5
R4	1, 2	192.168.1.0/24 via 10.10.32.1, metric = 0	192.168.1.0/24 via 10.10.32.2, metric = 5

So by default traffic will flow through R1 and R3. But if R1 breaks down, traffic from DTE A to DTE B will be routed through R2 to R3. If R3 then breaks down, traffic will flow through R2 to R4. If R1 then comes back up, traffic will flow through R1 to R4. So as long as there is one possible functional route, it will be used.

Now, it is possible to bring repeaters into this case as well, but it significantly increases the number of devices in the network. Adding only one repeater between DTE A and DTE B would create a single point of failure. Adding a repeater between pairs R1-R3 and R2-R4 would revert the case back to Example 3. So to make this case fully redundant with repeaters would require repeaters between pairs R1-R3, R1-R4, R2-R3 and R2-R4, a total of four repeaters on top of the four devices already in the network.

7.6.3.5Example 5: Virtual RMAC Address

Virtual RMAC address can be used to change the RMAC address of the modem along with the IP address. Therefore route monitoring is not needed in other devices, making the switchover much faster. The feature is still experimental.

Let's take Example 2 and change it to use Virtual RMAC Address. The setup has a redundant master device and two substations as seen in Figure 7.Y. This time the devices will have the following addresses (the DTE devices will be exactly the same as in Example 2):

Device	IP Address	RMAC Address
R1	192.168.1.1/24	101
R2	192.168.1.2/24	102
R3	192.168.3.1/24	3
R4	192.168.4.1/24	4

R1 and R2 will have exactly the same IP routes and VRRP parameters as in example 2, but with the following addition:

- Virtual RMAC Address: 1

Both of the substations need only one IP route:

- 192.168.1.0/24 via 10.10.32.1

Route monitoring is not needed, since only the master has tun0 address 10.10.32.1 (RMAC 1) in use. To ensure radio connectivity in all cases, all the substations should have packet routes defined to both the actual RMAC addresses of the master devices, in addition to the virtual RMAC. The packet route tables of the devices would therefore look like this:

Device	PR Neighbors
R1	3, 4
R2	3, 4
R3	1, 101, 102
R4	1, 101, 102

Some restrictions should be kept in mind when configuring a VRMAC address:

- R1 and R2 should not have packet routes to each other
- You should configure and commit all radio settings (RMAC address, PR table etc.) before enabling the VRMAC feature.

7.6.4 Redundancy related SNMP notifications

It is possible to enable sending of notifications for any redundancy related events. Chapter 8.2 presents usage of SNMP in generally and also the functionality of redundancy notification ID at general level. Notifications are sent if this ID has been set to ON and SNMP service is set ON.

Change of the status of VRRP causes different events depending on the case. Simple example is that if backup device notices that master is not present and sets itself as a master, this generates one notification. If the notification has been enabled in both devices, both devices send notification. Route monitoring sends messages simply in case it notices that one device is not responding or that higher priority device responds again. Thus it does not generate several messages for one event.

Both route change and VRRP state change notifications describe the cause of notification and IP of device that has sent it. There are few cases related to these notifications that need to have a clarification.

In case there are radio target IPs defined and master drops to backup since it cannot connect to that device, it generates more notifications. When backup notices that master has changed into backup, it sets itself as a master and then tries to connect to radio target IP (if such has been defined in this device). If the original master is unable to connect to target radio IP since its radio is broken, the new master presumably can connect. But if the remote device has been broken, then either of these two devices cannot connect to it. If notification has been set on at both devices, this case generates 3-4 notifications (master1 is original master and backup1 original backup): master1 to backup2, backup1 to master2, master2 notices that it cannot connect to remote device and sets itself as a backup and then one or the other device sets itself as a master.

In case both VRRP is on and some backup routes are defined, one event may generate several messages. Considering the previously mentioned case where target radio IP device gets broken. Both devices act the same way as in that case but in addition both change to lower priority route which generates one more notification from both. This would mean 6 notifications for this event.

When noticing a bunch of notification in short period (e.g. during one minute) of time, one option is to start from the latest ones since they define the current states of devices. In this case the latest messages are either describing current VRRP states of devices or they are about changing to lower priority route. Nevertheless, these would be the last messages in some order so they would provide the information about current status.

7.7 Application Routing

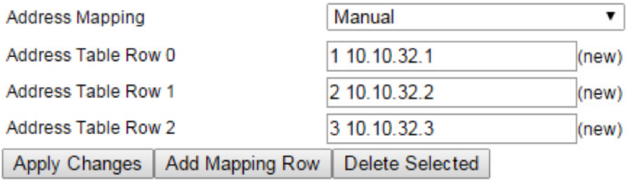
Application Routing allows the SATELLAR to route packets based on the data itself. When the feature is on, incoming packets will be analyzed and then routed to a specific destination based on the data itself. Two protocols are currently supported: DNP3 and Modbus RTU. In both cases, the destination address will be used to determine routing.

There are two options for how the protocol messages are received by the SATELLAR device: either from the serial port or via a TCP connection. When serial connection is used, serial parameters need to be specified as with Serial IP. Same serial port cannot be used as input in Serial IP and Application Routing. Serial IP with RS-232 cannot be set on while that port is used as input in Application Routing. If the TCP connection is used, a listening port needs to be defined.

It also needs to be defined, how the SATELLAR sends the packets over the radio. There are two options: TCP and UDP. In both cases two ports need to be defined: the port of the destination where packets are sent, as well as the port where incoming packets are listened to.

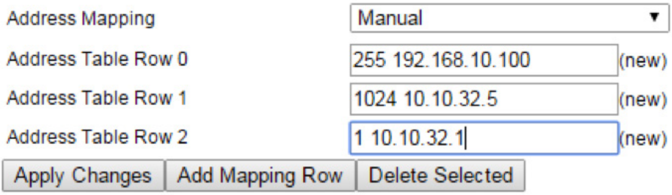
The actual routing is based on the destination address used by the protocol. There are two options on how to translate the protocol address to a radio address. The simpler one is to set Address Mapping to Application Address to RMAC. That means that the destination address will be set directly as the destination RMAC address. So for example if a DNP3 message contains destination address 10, it will be sent to a SATELLAR with RMAC address 10 (IP address 10.10.32.10). So if possible, the RMAC of each Satellar attached to a DTE should have the RMAC address that is same as the protocol address of the DTE it is connected to.

If that setup is not possible, it is also possible to determine the mapping manually by adding address table rows and setting Address Mapping to Manual. Each row contains two elements: first is the protocol address and second is the destination IP address. Rows can be added in the WWW interface with the button Add Mapping Row:



Address Mapping	Manual
Address Table Row 0	1 10.10.32.1 (new)
Address Table Row 1	2 10.10.32.2 (new)
Address Table Row 2	3 10.10.32.3 (new)

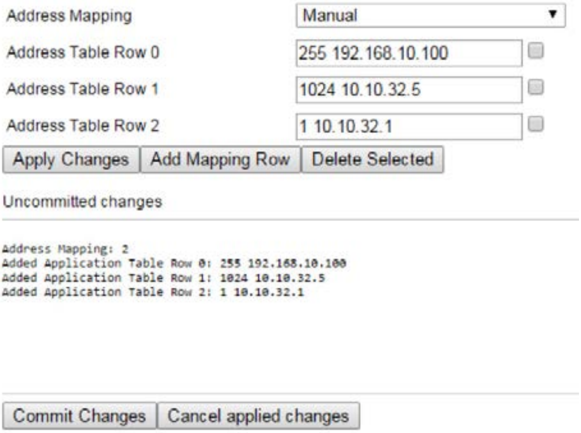
After the rows have been added, each can be edited:



Address Mapping	Manual
Address Table Row 0	255 192.168.10.100 (new)
Address Table Row 1	1024 10.10.32.5 (new)
Address Table Row 2	1 10.10.32.1 (new)

In that example, messages to application address 255 will be routed to 192.168.10.100 etc. After all rows have been edited to be correct, Apply Changes will store the table. Finally selecting Commit Changes will save the table to the device:

7. Settings



Address Mapping: Manual

Address Table Row 0: 255 192.168.10.100 □

Address Table Row 1: 1024 10.10.32.5 □

Address Table Row 2: 1 10.10.32.1 □

Uncommitted changes

```
Address Mapping: 2
Added Application Table Row 0: 255 192.168.10.100
Added Application Table Row 1: 1024 10.10.32.5
Added Application Table Row 2: 1 10.10.32.1
```

To delete a row, select the checkbox next to it and use the button Delete Selected. Commit Changes is required afterwards to finish the removal of the rows.

The settings of application routing are seen down below:

Attribute	Explanation	Sub unit	NMSID
Application Protocol	The used protocol of actual data. The currently supported protocols are DNP3 and Modbus RTU. If the selection is OFF, then no application routing is used.	1	3493
Application Transport Protocol	Where the traffic originates from. TCP and Serial Port are supported at the moment.	1	3494
Application Listening Port	If Application Transport Protocol is TCP, this is the listening port	1	3495
Serial Port	If Application Transport Protocol is serial, this variable lets you choose which serial port to use: RS-232 or USB	1	3498
Port Rate	If Application Transport Protocol is serial, this is the rate of the serial port	1	3499

Port Data Bits	If Application Transport Protocol is serial, this sets the serial port data bits	1	3500
Port Parity	If Application Transport Protocol is serial, this sets the serial port parity	1	3501
Port Stop Bits Port Stop Bits	If Application Transport Protocol is serial, this sets the serial port stop bits	1	3502
Transport Protocol For Substation Data	The protocol used to transmit the data to other SATELLAR devices. TCP and UDP are supported	1	3503
Destination Port For Substation Data	Which port will the data be sent to	1	3504
Listening Port For Substation Data	Which port will listen to replies	1	3505
Application Listening IP Address	This is the binding IP address of the device. Incoming packets must be transmitted to this address and outgoing packets will have this as the source address	1	3506
Address Mapping	Select between manual and automatic address mapping	1	3507
Address Mapping Row (Note: only available in web UI)	If manual address mapping is used, this array holds the mapping. New rows can be added in the WWW interface	1	3520

Table 7.25 Application Routing settings

7.7.1 Example1: DNP3 with TCP, UDP and serial port

In this example, SATELLAR devices are used to enable DNP3 communication between a Supervisory Control And Data Acquisition (SCADA) device and two Remote Terminal Units (RTU). The SCADA is connected to SATELLAR R1 with an Ethernet cable, and the two RTUs to their SATELLARs with a serial cable. SATELLAR R1 has radio connectivity to both R2 and R3, and there can be repeaters between them.

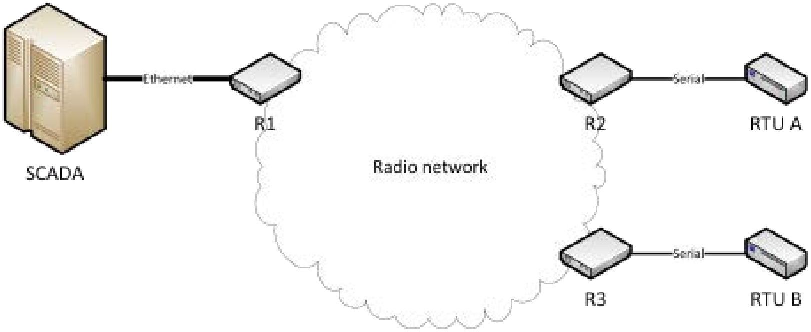


Figure 7.40 Example 1

The devices will have the following addresses:

Device	IP Address	RMAC Address	DNP3 Address
SCADA	192.168.1.100	-	255
R1	192.168.1.1	1	-
R2	192.168.2.1	2	-
R3	192.168.3.1	3	-
RTU A	-	-	2
RTU B	-	-	3

In this topology, R1 is the master device and the other two slave devices. R1 will have a TCP server that listens to DNP3 messages from the SCADA sent over TCP. It will relay those messages as UDP packets to R2 and R3. R2 and R3 will then relay those messages through the serial port to the connected RTU. If RTU A sends a message to the SCADA, it is written to the serial port of R2. R2 will send it as a UDP packet to R1, which will in turn write the message to the SCADA through the open TCP connection. The Application Routing parameters for the three SATELLARs can be seen in table down below. The serial port parameters are not included; they will just be set so that they are the same as in the RTUs.

Device	R1	R2	R3
Application Protocol	DNP3	DNP3	DNP3
Application Transport Protocol	TCP	Serial Port	Serial Port
Application Listening Port	20000	(No effect)	(No effect)
Serial Port	(No effect)	RS-232	RS-232
Transport Protocol For Substation Data	UDP	UDP	UDP

Destination Port For Substation Data	2006	2005	2005
Listening Port For Substation Data	2005	2006	2006
Address Mapping	Application Address to RMAC	Manual	Manual
Address Mapping Row	(empty)	255 192.168.1.1	255 192.168.1.1

Table 7.26 Application Routing Parameters of Example 1

The Application Listening Port of R1 is 20000, so the SCADA needs to open a TCP connection to 192.168.1.1:20000. All SATELLARs must have the same transport protocol, in this case UDP. The master sends to destination port 2006, so both the slaves must have listening port set to 2006. Correspondingly, both slave devices have destination ports 2005 and R1 has listening port 2005.

Both slave SATELLARs have the matching RMAC addresses to the DNP3 addresses of the RTUs, so R1 can use Application Address to RMAC Address Mapping. Messages sent to DNP3 address 2 will be routed first to R2 and then to RTU A. But the SCADA has the address 255, so both slaves need to use manual mapping. They both need just one Address Mapping Row:

255 192.168.1.1

That means that DNP3 messages to destination address 255 will be routed to R1, which will in turn relay the message to the SCADA.

7.7.1.1 Variations to the example 1

The example uses UDP to send the messages over the radio. That is generally recommended, since UDP uses less radio resources than TCP and is also faster. But if a slower but more secure connection is desired, TCP can also be used to transport the messages over the radio. That can be done by simply changing Transport Protocol For Substation Data to TCP in every SATELLAR. Nothing else needs to be changed, either in the SATELLARs or the other devices in the network.

Exactly the same example also works, if every SATELLAR has Modbus RTU selected as the Application Protocol. The SCADA and RTUs must naturally also use Modbus RTU in that case.

In the example above, the RTUs are connected to their respective devices through the serial port. But if they were also connected to the slave devices through Ethernet, then both R2 and R3 would need to change the Application Transport Protocol to TCP and also set a port that the RTUs could use. No other settings need to be changed.

8. Applications

This chapter explains the additional applications available in the CU.

8.1 Diagnostics

This application is used to view graphs of measured diagnostics.

The following Diagnostics graphs are available:

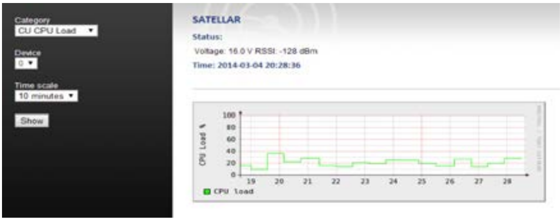
Diagnostic	Explanation
CU RAM Usage	Memory used by all running processes and kernel in the CU.
CU CPU Load	Shows the percentage of CU CPU (MCU) processing power used.
NMS Timeouts	Local RU NMS message timeouts. Values higher than 0 indicate the RU is busy with data traffic and unable to answer all settings or diagnostics NMS messages sent by the CU.
RSSI	Signal strength of all received radio messages.
Temperature	As measured at the RU RF Power Amplifier. See RU User Manual for accuracy and other information.
Voltage	As measured at the RU power in connector. See RU User Manual for accuracy and other information.

Table 8.1 Diagnostics

The diagnostics graphs can be viewed in several different time scales:
- Previous 10 minutes (scale: minutes)
- Previous 1 hour (scale: five minutes)
- Previous 5 hours (scale: hours)
- Previous 24 hours (scale: 6 hours)
- Previous week (scale: days)
- Previous month (scale: weeks)

Diagnostics, except CU load and MEM usage, from remote devices can also be viewed, if remote diagnostics have been turned on (see section 7.1.5).

8.1.1 Diagnostics application in WWW interface



Category: CU CPU Load

Device: 0

Time scale: 10 minutes

Show

SATELLAR

Status:

Voltage: 16.0 V RSSI: -128 dBm

Time: 2014-03-04 20:28:36

In the WWW UI, the diagnostic category, device and time scale can be selected from the ropdown menus on the left. Selecting Show presents the diagnostic data accordingly.

8.1.2 Diagnostics application in the GUI

In the GUI, the diagnostic category is selected by opening the menu item Variable with the left button, and selecting one of the values. A Help text is also available. Similarly, the device menu item is opened with the OK button. The Device menu is used to select which device to show the diagnostics from. The time scale can be changed by pressing the left and right keypad buttons.

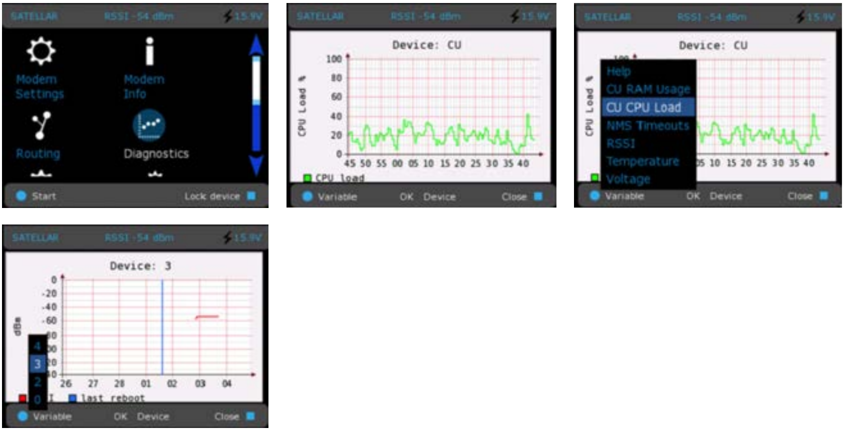


Figure 8.1 Diagnostics by CU: Graphical user interface (GUI/LCD)

8.2 Simple Network Management Protocol (SNMP)

An “Internet-standard protocol for managing devices on IP networks.” It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP is simply a protocol for collecting and organizing information. SNMP itself does not define which information (which variables) a managed system should offer. Rather, SNMP uses an extensible design, where the available information is defined by management information bases .

In typical SNMP uses, one or more administrative computers, called managers, have the task of monitoring or managing devices on a network. Each managed system executes, at all times, a software component called an agent which reports information via SNMP to the manager.

Essentially, SNMP agents expose management data on the managed systems as variables. The protocol also permits active management tasks, such as modifying and applying a new configuration through remote modification of these variables.

An SNMP-managed network consists of three key components:

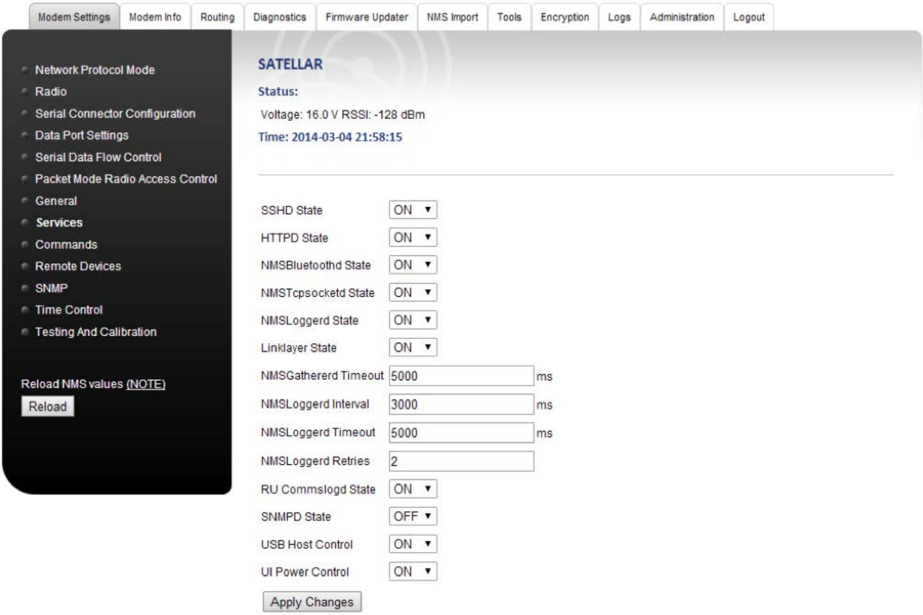
- Managed device
- Agent — software which runs on managed devices
- Network management system (NMS) — software which runs on the manager

Typical radio modem or system monitoring can be RSSI-values, Voltage or Temperature. Setting type configuration consists of IP- or radio parameters.

Status of SNMP application is set similarly to other CU applications in Services category.

Attribute	Explanation	Sub unit	NMSID
SNMPD State	Enable or disable the SNMP functionality. Options are ON and OFF. Default value is OFF.	1	3266

Table 8.2 The settings of SNMP status



Status:
Voltage: 16.0 V RSSI: -128 dBm
Time: 2014-03-04 21:58:15

SSHD State	ON	
HTTPD State	ON	
NMSBluetoothd State	ON	
NMSTcpsocketd State	ON	
NMSLoggerd State	ON	
Linklayer State	ON	
NMSGathererd Timeout	5000	ms
NMSLoggerd Interval	3000	ms
NMSLoggerd Timeout	5000	ms
NMSLoggerd Retries	2	
RU Commslogd State	ON	
SNMPD State	OFF	
USB Host Control	ON	
UI Power Control	ON	

Figure 8.2 Services settings view

8.2.1 SNMP category

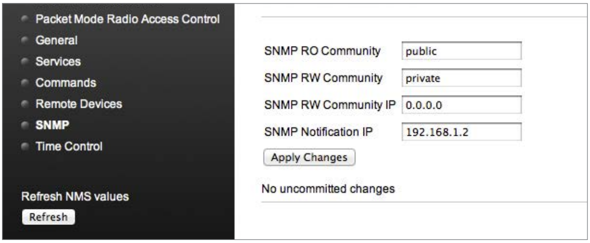
SNMP category includes the settings related to SNMP usage.

Attribute	Explanation	Sub unit	NMSID
SNMP RO Community	Read-only community phrase. Expected password in received SNMP request to grant reading of values. Maximum length is 255 characters. Default RO Community phrase is ‘public’.	1	3241
SNMP RW Community	Read-write community phrase. Expected password in received SNMP requests to grant reading and writing of values. Maximum length is 255 characters. Default RW Community phrase is ‘private’.	1	3242
SNMP RW Community IP	Read-write community IP. Defines the IP address range that is allowed to send read and write requests to this SATELLAR. For example, value 192.168.1.0 allows source addresses from 192.168.1.0 to 192.168.1.1.255. Default value is 0.0.0.0, allowing all addresses.	1	3243
SNMP Notification IP	IP address where the notifications, when available, are sent to.	1	3244
SNMPv3 User Name	Defines the user name of SNMPv3 user. Maximum length is 255 characters and default is ‘User123’.	1	3332
SNMPv3 User Type	Defines whether the user has read-only or read-write access.	1	3333
SNMPv3 USM Security Type*	No Auth – No authentication or privacy used with SNMPv3 communication. Also SNMPv2 access is possible MD5 No Priv – MD5 authentication is used in SNMP communication, no privacy protocol is used. SHA No Priv – SHA Authentication is used in SNMP communication, no privacy protocol is used MD5 DES - MD5 authentication and DES ciphering is used in SNMP communication. SHA DES - SHA authentication and DES ciphering is used in SNMP communication. MD5 AES - MD5 authentication and AES128 ciphering is used in SNMP communication. SHA AES - SHA authentication and AES128 ciphering is used in SNMP communication.	1	3334
SNMPv3 Authentication Passphrase	Password for SNMPv3 authentication. This is used to verify that packet with authentication can be used only ones knowing the password.	1	3335

SNMPv3 Privacy Passphrase	Password for SNMPv3 ciphering. This is used to verify that packet with authentication can be used only ones knowing the password	1	3336
SNMP Listening IP Address	IP address that listens any SNMP request at SATELLAR. As a default it is 0.0.0.0 i.e. it listens the requests from any IP that is available at SATELLAR. It can be set to be e.g. VLAN IP so that SNMP cannot be accessed from other IPs.	1	3337
Notification interval	Interval between the checking of values that are observed for notification. This means that the value that is observed is checked in every interval seconds and compared to related threshold values. Notification is send only when threshold limits are exceeded or undershoot	1	3338
Voltage Notification	Defines is the monitoring of voltage and sending of notifications in case the limits are exceeded or undershoot ON or OFF. Default value is OFF.	1	3339
RSSI Notification	Defines is the monitoring of RSSI and sending of notifications in case the limits are undershoot ON or OFF. Default value is OFF.	1	3340
Temperature Notification	Defines is the monitoring of temperature and sending of notifications in case the limits are exceeded or undershoot ON or OFF. Default value is OFF.	1	3341
SNR Notification	Defines is the monitoring of SNR and sending of notifications in case the limits are undershoot ON or OFF. Default value is OFF.	1	3342
Commit Notification	Defines are the notifications send when any values are committed to Radio or Central Unit. Default value is OFF.	1	3343
Redundancy Notification	Defines are the notifications send for any redundancy related events (VRRP state changes or redundancy caused route switches). More details at chapter 7.6	1	3348

Table 8.3 The settings of SNMP category

* NOTE: This parameter also defines whether the SNMP in generally uses only v3 or both v2 and v3 access. In case any other option than ‘No Auth’ is selected, only v3 access is allowed. In such case also traps are sent with selected SNMPv3 authentication and privacy.



SNMP RO Community	public
SNMP RW Community	private
SNMP RW Community IP	0.0.0.0
SNMP Notification IP	192.168.1.2

No uncommitted changes

Figure 8.3 SNMP settings view

8.2.2 MIB

Management Information Base, MIB, is a database formed by a collection of description files. The MIB database defines the parameters that are available to the SNMP functionality. In the hierarchical name space of the MIB, each parameter is uniquely identified by OID - Object Indetifier.

8.2.2.1 SATELLAR MIB files

External SNMP manager application must have the SATELLAR specific MIB files imported to their MIB, in order to be able to request SATELLAR specific parameters. The SATELLAR specific MIB files are available for download from the SATEL web page www.satel.com. They are also downloadable from the SATELLAR WWW user interface by accessing http://[the SATELLAR IP-address]/mibs. For exmple http://192.168.1.1/mibs. Parameters available to SNMP are basically the same as in GUI or WWW interface. Also, whether the parameter is read-write or read-only, is identical in the SNMP operation and user interfaces. Any text editor can be used to view the contents, but the hierarchical presentation of the parameters is best presented by the MIB browser available in many of the external SNMP applications.

Basic level of hierarchical structure of the SATELLAR MIB contents can be presented as follows:

- satelSATELLARNMS
  - satelSATELLARNMSInfo
    - satelSATELLARNMSInfoRU
    - satelSATELLARNMSInfoCU
  - satelSATELLARNMSSettings
    - satelSATELLARNMSSettingsRU
    - satelSATELLARNMSSettingsCU
  - satelSATELLARNMSRouting
  - satelSATELLARNMSCancelCommit

The branch satelSATELLARNMSInfo contains same parameters as Modem Info category in the WWW interface, satelSATELLARNMSSettings includes same parameters as Modem Settings category in the WWW interface and similarly the satelSATELLARNMSRouting contains same parameters as Routing category in the WWW interface.

8.2.3 Reading and writing values with SNMP

The SNMP monitoring and management protocol is based on Get and Set requests. The external application sends an SNMP Get request to read values and SNMP Set request to write values to SATELLAR parametrs. The available parameters are defined in the MIB and identified uniquely in the MIB and in the request by OID. SATELLAR responses with the queried value or with result of the writing action, again identified by the OID.

Similarly to the GUI or WWW interface operation, after applying changes the configuration must be committed to save the settings. With NSMP, the committing is executed by sending a SNMP Set request with the OID of the satelSATELLARNMSCancelCommit parameter. To commit changes permanently and make them effective, CancelCommit is set to value 1. To cancel changes that are not yet stored CancelCommit is set to 0.

Satellar SNMP settings define whether the SNMP version 2 or SNMP version 3 is available. SNMPv3 USM Security Type parameter defines what SNMPv3 authentication and ciphering method is used, but it also defines whether the SNMPv2 is available or not. If Security Type is set to NoAuth (default), SNMPv2 is available with defined community words and also SNMPv3 is available without authentication or ciphering. When the Security Type is set to any other option, only SNMPv3 with defined parameter settings is available.

8.2.4 SNMP Timeout

Some of the reading or writing actions require more time to complete that others. Espacially commands related to databases, such as routing tables, take longer than accessing a parameter with a single value. Also, SNMP requests sent over the radio interface have longer delay than the request sent over wired IP connection. This has to be taken into account at the external SNMP application sending the requests: most of the SNMP applications have a SNMP Timeout parameter. Increasing the value for timeout in the external application can be used to avoid SNMP connectivity issues with SATELLAR modems.

8.2.4.1 SNMP application examples

NET-SNMP – Console based application for various SNMP usages, such as scripting.

SNMPB - a simple graphical Windows application.

Dude – a simple graphical Windows application.

Spiceworks – a browser-based application.

8.2.5 Notifications (traps)

SNMP also includes the possibility to get notifications - also known as traps - for different events. These are basically messages with different names and possibly some content. One default trap is information about stop and start of SNMP. When SNMP starts, it sends coldStart trap and when it closes down, it sends notification NotifyShutdown. Notifications are sent to IP address that is defined at parameter SNMP Notification IP.

There are several notifications in Satellar that can be enabled. To be able to enable notification, SNMP must be set ON and then each notification is enabled individually. Each notification has user-definable parameters that define when message for the event is sent.

Notification	Definition	Notification Name	Trigger(s)	Message
Voltage Notification	Notifications in case voltage is above maximum, below minimum or returns back from either state	satelNotifyVoltage	Minimum: Modem Settings – General – UI Voltage Critical Level (1.3202) Maximum: Modem Settings – General – UI Voltage Bar Max (1.3206)	Below minimum: "Voltage has dropped to 9.8, it is below set minimum 10.0" Above maximum: "Voltage is now 28.7, it has peaked over the maximum limit 28" Normalized: "Voltage has returned to an acceptable level 14.7"
RSSI Notification	Notifications in case RSSI below minimum (critical) level or returns back to normal level	satelNotifyRSSI	Minimum: Modem Settings – General – UI RSSI Critical Level (1.3203)	Below minimum: "RSSI has dropped to -128, it is below set minimum -110" Normalized: "RSSI has returned to an acceptable level -58"
Temperature Notification	Notifications in case temperature is above maximum level, below minimum level or returns back to normal level from either state		Minimum: Modem Settings – General – Temperature Min (1.3344) Maximum: Modem Settings – General – Temperature Max (1.3345)	Below minimum: has dropped to -10, it is below set minimum 0" Above maximum: "Temperature is now 65, it has peaked over the maximum limit 60" Normalized: "Temperature has returned to an acceptable level 40"
SNR Notification	Notifications in case Detector Signal To Noise Ratio value is below minimum (critical) level or returns back to normal level	satelNotifySNR	Minimum: Modem Settings – General – SNR Critical Level (1.3346)	Below minimum: "SNR has dropped to 10, it is below set minimum 20" Normalized: "SNR has returned to an acceptable level 30"
Commit Notification	Notifies when user commits any Radio or Central Unit value.	satelNotifyCommit		

8.3 Firmware updating

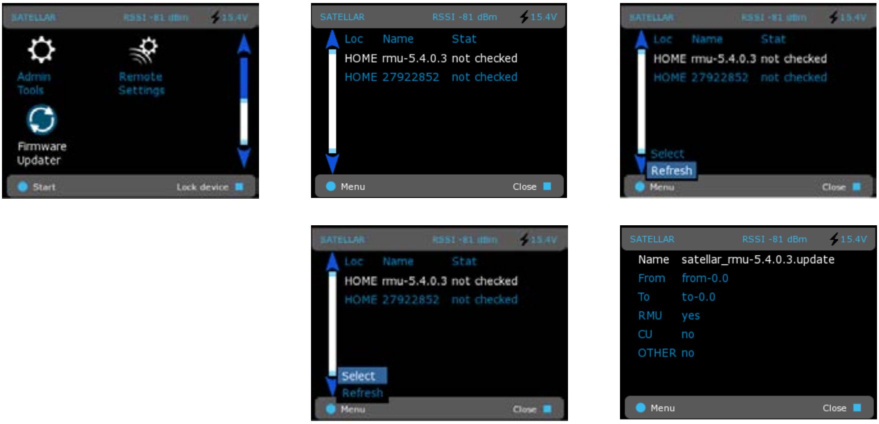
The currently installed firmware version numbers are available in the Modem Info Application, RU and CU categories.

There are three different ways to do the firmware updating:

- to use the firmware updater application in CU by the LCD GUI or in the WWW interface
- to use the USB Stick during boot CU update method
- to use the firmware update over-the-air

8.3.1 Firmware updater application

The Firmware updater application can be used to update the firmware of the RU or the CU. This application is available in the WWW interface and the LCD GUI, but the operation is slightly different. When updating the firmware using Firmware Updater, previous settings are NOT lost, unless the release notes for the new firmware specify differently.



Loc	Name	Stat
HOME	rmu-5.4.0.3	not checked
HOME	27922852	not checked

Name	satellar_rmu-5.4.0.3.update
From	from-0.0
To	to-0.0
RMU	yes
CU	no
OTHER	no

Figure 8.4 Firmware updater by CU: Graphical user interface (GUI/LCD)

8.3.1.1 Choosing the right update file

First you must determine which firmware you are updating. It is possible to update either the RU or the CU firmware.

The RU firmware update file is named “satellar-ru.*x.y.z.w*.update”, where “*x.y.z.w*” is the version number of the new firmware. Simply choose the update file, which has the version number you wish to update to.

The CU firmware update file is named “satellar_xxxxyyyy.update” where xxxx is the old firmware version number and yyyy is the new firmware version number. When updating the CU firmware using Firmware Updater, it is necessary to know the current filesystem version number, so that the correct update file can be chosen. For example, if you need to install a new firmware version satel-2863, and your current filesystem version number is satel-2775, you need an update file named “satellar_27752863.update”. The current firmware version can be seen in Modem Info, CU category.

The CU firmware update file consists of two different files, the kernel image and the filesystem. Due to the relatively large size of the full filesystem image (typically 11 MB), the update includes only the changed parts of the image, so the update file size is kept to a minimum. This is called an incremental, or patch, update.

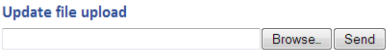
The following table illustrates the different possibilities.

Update file	Example of update file name	Images contained in the update file	Typical size, approximately	Update method
RU update file	satellar_rmu-5.3.0.2.update	RU firmware image.	300 kB	Firmware Updater
CU update file	satellar_27752863.update (typical total size: 4.3 MB)	CU kernel image.	2.4 MB	Firmware Updater
		CU file system incremental upgrade patch.	1.9 MB	

Table 8.4 Choosing the update file

8.3.1.2 Uploading the update file

When you have the correct update file on your computer, open SATELLAR WWW GUI, and go to the Firmware Updater application. Then click on the Browse… button and then locate the file using the window that opens. Then click on Send to transfer the file to SATELLAR CU.



Update file upload

Note that this step is NOT yet the actual update; it is just a file transfer.

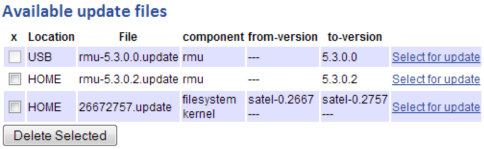
Alternatively, the update file can be placed on an USB memory stick. In the latter case, the file will become visible in the list of Available update files when the memory stick is inserted into SATELLAR's USB port and the web page is reloaded. Allow a few seconds after inserting the stick before reloading the page.

8.3.1.3 Starting the firmware update process

After a file has been uploaded or a USB memory stick containing the file has been inserted, it appears on the list of available update files.

The following image shows that three update files are available:

- A RU update file, eg. version 5.3.0.0, on the USB memory stick
- Another RU update file, eg. version 5.3.0.2, uploaded to the CU
- A CU update file, containing a filesystem patch eg. from version 2667 to 2757 and a kernel image, uploaded to the CU.



Available update files

x	Location	File	component	from-version	to-version	
□	USB	rmu-5.3.0.0.update	rmu	---	5.3.0.0	Select for update
□	HOME	rmu-5.3.0.2.update	rmu	---	5.3.0.2	Select for update
□	HOME	26672757.update	filesystem kernel	satel-0.2667 ---	satel-0.2757 ---	Select for update

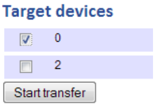
When the file is available, click "Select for update" to start the update process using that file (see chapter 8.3.1.4).

Unneeded files can be deleted from the CU by checking the checkbox in the "x" column and clicking "Delete Selected".

8.3.1.4The firmware update process

The update process is time-consuming, but in case the update is interrupted by a power failure etc, the process can be resumed. The process can also be cancelled at any time.

First the devices to be updated must be selected. Normally choose only device 0 (local device).

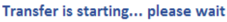


Target devices

☑ 0

□ 2

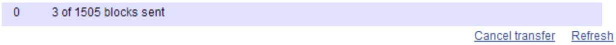
Click the Start transfer -button, and you will get this message:



Transfer is starting... please wait

The progress of update is indicated by a progress bar, which is automatically refreshed with 5-second intervals. The transfer may be cancelled at any time by clicking on “Cancel transfer”, and no harm will be done to the target unit.

When transfer has finished, the RU is restarted and is ready to use.



0 3 of 1505 blocks sent

When updating a CU, it will also be automatically restarted. The restart will take longer than usual; because part of the update process takes place during the booting process. The progress of the update can be seen on the LCD screen. In case no screen is available, the STAT LED blinks while booting and updating is in progress.

The CU firmware update can last up to 10 minutes. Do NOT turn off, restart or reboot the CU during this time. IF the CU is restarted or turned off, the firmware update process fails and the previous firmware version remains in use.

After restart has completed, please check the Firmware versions from Modem Info, RU and CU categories (see chapters 8.5 and 8.4) to see that the Firmware versions have been updated to the new version.

8.3.2 USB Stick during boot CU update method

This method is completely different from the Firmware Updater application. The files used are not .update files; instead they are RAW kernel and/or file system images. The files are placed on a USB Memory Stick and renamed according to the table below. The USB stick is then inserted, and then SATELLAR is rebooted. The update is done automatically during the device boot.

The progress of the update process is displayed on the LCD screen. In case the CU is not equipped with a LCD screen, you can follow the process by the STAT LED. While the STAT LED is blinking, the update is underway.

Image updated	Files needed	File name example	Rename file name to	Approximate duration of update
kernel[1]	kernel image	satel-0.2757_uImage	uImage	5 minutes
	signature file	satel-0.2757_uImage.sig	uImage.sig	
filesystem[2]	filesystem image	satel-0.2757_rootfs.jffs2	rootfs.jffs2	10 minutes or more
	signature file	satel-0.2757_rootfs.jffs2.sig	rootfs.jffs2.sig	

Table 8.5 Update process

[1] Note about kernel update using this method: After the device has booted, it must be restarted again to actually start using the new kernel.

[2] Note about filesystem update using this method: This method removes all files AND settings, including IP settings, stored in the CU. RU settings such as Frequency are not affected. (CU settings can be identified by the sub-unit number “1”). The advantage of this method is that the previous file system version number is not needed; you can update any filesystem version over any other.

8.3.3 Firmware update over-the-air

This chapter explains how the firmware of devices in an installed, running network consisting of SATELLAR 2DS and 20DS devices in Packet routing / TCP/IP mode can be remotely updated.

Both SATELLAR CU and RU firmware can be updated using this method. The method has the following steps:

- Preparation
- Transfer of files
- Update process
- Confirmation

The time taken is dependent on the relatively slow (compared to the size of the update packets) transfer speed over radio. While comparatively slow, the time may still be less than doing the updates by hand, i.e. going to the site physically and doing an USB-memory-stick update. This depends fully on the size and geography of the installed network.

8.3.3.1 Preparation steps

Before starting the firmware update, make sure the following preconditions are fulfilled.

Step 1. Plan the time needed for the update process

You should plan your update process so you know the downtime of the data system beforehand and can proceed with less uncertainty.

Table 1 lists the time needed for some examples. All times are calculated without any other traffic in the radio network. (I.e. data transfer has been stopped)

Air speed	Update file size	Transfer time	Total update time per device (approximate)
38.4 kbps	4.5 MBytes	28 minutes (measured)	50 minutes
38.4 kbps	3.5 MBytes	24 minutes (approximate)	45 minutes
19.2 kbps	4.5 MBytes	45 minutes (approximate)	1 hour 10 minutes
19.2 kbps	300 kB	5 minutes (approximate)	15 minutes

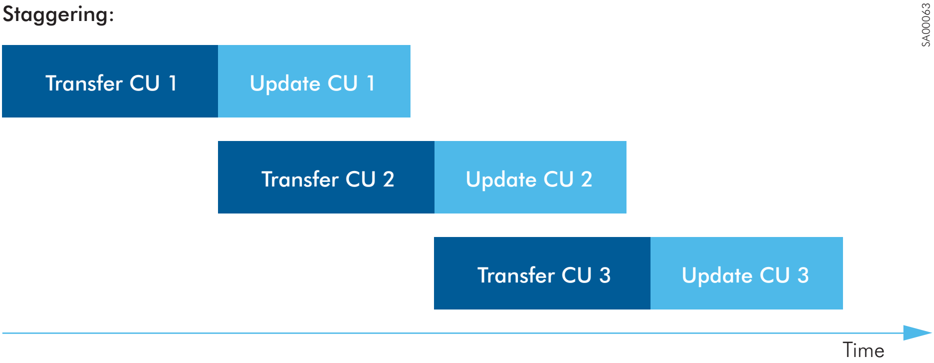
Table 8.6 Update file transmit time examples

Notes about the time needed:

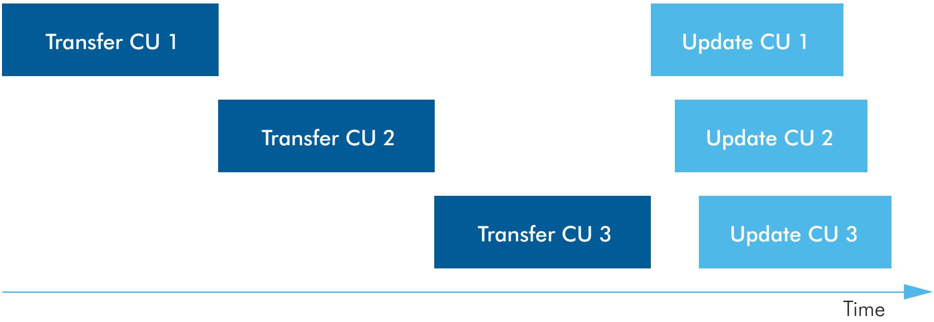
Transmit time is the critical factor. Total time includes data transfer, delays such as using the WWW interface manually, which can be speeded up with a little practice, and the time taken by the CU to actually install the update, a process which is done separately from file transfer. Actually, you can stagger the process by starting the update process in one modem while the update file is being transferred to the next modem. This “staggering” method can save time. Alternatively, transfer all files first (one after the other), then update all modems at once.

Do not start multiple uploads at the same time, as this will cause slower transfer speeds and potentially cause some transfers to fail. (It could be worth trying for overnight transfers, though)

Staggering:



Alternative:



Step 2. Make sure there is a connection to all SATELLAR 2DS and 20DS devices

You need a working TCP/IP connection to all modems. This can be confirmed by opening the WWW setup interface of each remote SATELLAR device by writing the IP address of the device in the address bar of your web browser.

The update is done via the WWW interface of each modem. The HTTP protocol used to control the update and transfer the files is running in the SATELLAR radio network. For this reason the update cannot be done if the Protocol Mode setting in your network is not set to “Packet Routing” or IP connections to all devices do not work for some other reason. You can use either the “radio IP addresses” or the “Ethernet IP addresses” of the Central Units for ping tests and WWW interface access.

If you are using a PC which is connected to other LANs or the Internet at the same time as you are connected to the SATELLAR network, you need to add a temporary IP route to your PC configuration for the purpose of connecting to the SATELLAR network. Assuming your local SATELLAR unit connected via Ethernet has IP 192.168.1.1 and your PC is 192.168.1.2 and this connection is working, you can then use this command in windows to add the temporary route:

First, start cmd.exe using administrator privileges. Then enter the following command:

```
c:\> route add 10.10.32.0 mask 255.255.255.224 192.168.1.1
```

Now you can access all SATELLARs by using their radio IP address, such as 10.10.32.2, 10.10.32.3 etc.

A simpler way is to disconnect the PC from all other networks and set your local SATELLAR unit as the default gateway. This way you don't need to use the ROUTE command.

Step 3. Organize your modems into browser tabs

This is a very useful feature in modern web browsers. If you put each SATELLAR unit's web interface into a separate web browser tab, it is easy to go through the update process. This is also helpful if using the staggering method to save time.

Step 4. Identify the current firmware versions

It is possible that your modems have different firmware versions. When the CU firmware is updated it is important to know what the current version number is. Go to "Modem info, CU" menu (See chapter 7.2.3) in the WWW interface of each of the modems and look at file system version (NMSID 1.650).

For RU firmware, the current version is not important.
If you have different CU firmware versions, it can be helpful to record the version on a piece of paper or excel sheet for easy reference while updating or you could check the version every time using the WWW modem info page.

If you transfer the wrong file to the CU you have just lost 25 minutes or more time, because the wrong update file cannot be used to upgrade the firmware!

Step 5. Gather the needed update files

See CU User Manual chapter 8.2.1 for help identifying the correct files. Make a note which files go into which modems, if your network has different versions currently installed.

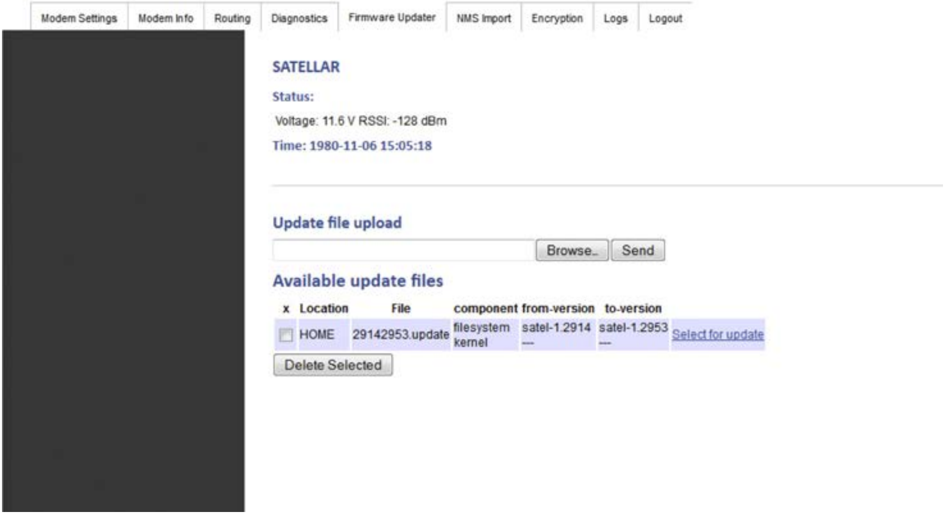
Step 6. Stop all other data traffic

To speed up the file transfer and reduce the risk of transfer errors, it is recommended to stop all other traffic from your radio network while updating.

8.3.3.2 Transferring the files

Actual transfer of the .update file is done exactly as detailed in the chapter 8.2.2. Note that while the file is uploaded, there is no progress indication, other than what is provided by your web browser. Typically uploads are not tracked by web browsers, while downloads have very good progress indicators.

When one upload is complete, this screen appears:



[redacted]

SATELLAR

Status:

Voltage: 11.6 V RSSI: -128 dBm

Time: 1980-11-06 15:05:18

Update file upload

Available update files

x	Location	File	component	from-version	to-version	
□	HOME	29142953.update	filesystem kernel	satel-1.2914 ---	satel-1.2953 ---	Select for update

Figure 8.5 Update file transfer complete

Now you can start the update process as indicated in next chapter, and then start file upload for the next modem.

8.3.3.3 Updating

To start each firmware update, just click on the “Select for update” link text (see Figure 1) as explained in the user manual chapter 8.3.1.3, and follow instructions in chapter 8.3.1.4.
Note especially:

- Select only the target device ‘0’
- Update is done in two stages, “transfer” and “reboot”.
  - Transfer is quick, a minute at most (Do not confuse this with file transfer)
  - Reboot, which can take more than 10 minutes for the CU. (The actual update is done at this stage)

While the firmware is being updated (about 10 minutes for CU firmware), little or no data is being sent or received, so this time can be used for transferring another update file to another modem.

8.3.3.4 Confirming the update

After 10 minutes or so, the web interface should reload automatically. You can also refresh the page manually using your browser (hit F5). Note that the modem is unresponsive while the reboot process in underway.

When the web interface is responding again, go to "Modem Info" and confirm the version number from either the "CU" or "RU" category as appropriate. You should do this step at once for all modems (by going through the browser tabs in order) as the last step of the update process. If any modem does NOT display the new version number, you should:

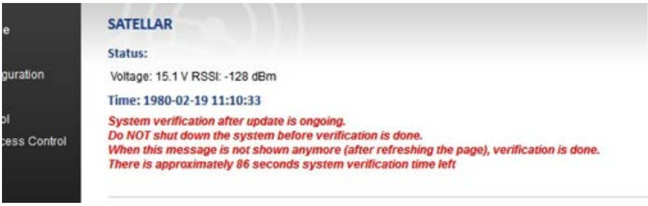
- Refresh the web page (press F5)
- if still old version, reboot the updated device (RU or CU)
- if still old version, retry the update (select for update, also double-check the from version is correct)
- if still old version, confirm the original .update file is valid and re-transmit, effectively doing the whole process again for the affected modem(s).

When all modems are running the new firmware versions, re-start your data traffic.
Updates do not normally change any settings, but if they do, there should be a mention of this in the release notes.

8.3.3.5 Verification of update integrity

When the system has been booted up after the update, a verification process ensures that it is working properly. This will take appr. 2.5 minutes. If the process detects that something is not working correctly, it reverts the system to previously used version. The system shall not be rebooted during the verification process. Rebooting reverts the system to old version too.

Web UI shows the verification state like this:



SATELLAR

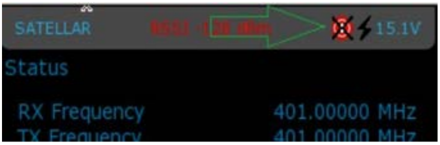
Status:

Voltage: 15.1 V RSSI: -128 dBm

Time: 1980-02-19 11:10:33

System verification after update is ongoing.
Do NOT shut down the system before verification is done.
When this message is not shown anymore (after refreshing the page), verification is done.
There is approximately 86 seconds system verification time left

In GUI there is a do not reboot-icon that indicates the same thing. Green arrow points to this icon:



SATELLAR RSSI -128 dBm 15.1V

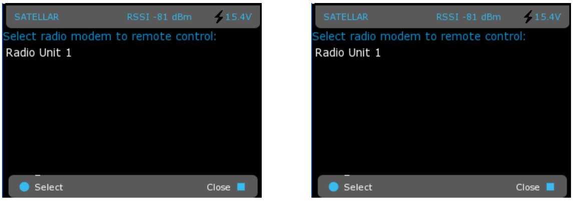
Status

RX Frequency 401.00000 MHz
TX Frequency 401.00000 MHz

In addition to these, STAT and PWR LEDs are blinking simultaneously at a rate of faster (half second) and slower (one second) blinks until the verification is over.

8.4 Remote settings

This application is only available in the LCD GUI. It is used to change settings of a remote SATELLAR, over the air. (The same functionality can be achieved in the WWW interface by contacting the WWW server in the target SATELLAR directly, by using its IP number. Remember that both tun0 and eth0 IP numbers can be used.)



Select radio modem to remote control:
Radio Unit 1

Figure 8.6 Remote settings by CU: Graphical user interface (GUI/LCD)

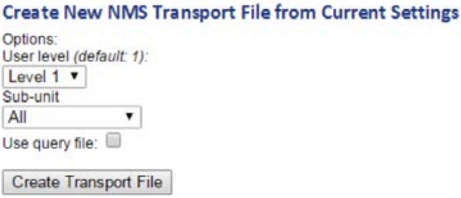
8.5 NMS Import

This application is available in the WWW interface only. It allows to export and import settings as text files. The file is called a NMS Transport file. For example you can export all modem settings into a file and save it to your computer as a backup. You can also edit this file and send it back to the modem, or to another modem. The modified file could contain only one or a few settings, not all settings originally found in the file are needed. This can be used to change the same few settings to multiple modems relatively quickly. (By creating a file with just the settings to be changed, and importing it to all the modems).

8.5.1 Exporting settings from modem

When exporting settings, SATELLAR CU creates a file which contains the settings. The file can then be saved on a computer and kept as a backup, or edited using a text editor and sent back to the modem. The following procedure can be used to export all user settings from a radio station (both CU and RU).

1. Go to the NMS Import Application of WWW GUI. The export section of the page looks like this:



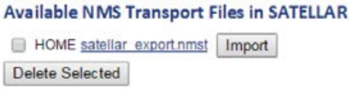
Create New NMS Transport File from Current Settings

Options:
User level *(default: 1)*:
Level 1 ▾
Sub-unit
All ▾
Use query file: □

2. Ignore the query file, User level and sub-unit selections for now. Just select

Create Transport File button. SATELLAR now generates the transport file.

3. The new transport file appears at the top of the page, under Available NMS Transport Files:



Available NMS Transport Files in SATELLAR

□ HOME satellar_export.nmst Import

Delete Selected

4. Click on “satellar_export.nmst” to transport the export file to your computer.

8.5.2 NMS Export advanced features

These optional features are available:

Option	Effect

Query file	If you wish to export only some specific settings, create a text file containing only the NMSIDs, one per row, and use it as the query file. Click Browse to select the file and Upload to send it to the modem.
	Example query file contents:
	`1.398`
	`1.33`
	`1.80`

Use query file	Mark this checkbox to use the query file that was uploaded. The resulting export file will only contain the values of the NMSIDs that were specified in the query file.
User level	Level 1 is the normal level. Sometimes SATEL technical support may request you to export level 5 or 9 settings in case the information is needed to solve a problem. Level 5 or 9 settings cannot be changed.
Sub-unit	Choose All to export both RU and CU settings. Sub-unit 0 exports only RU settings and sub-unit 1 exports only CU settings.

Table 8.7 NMS Export advanced features

8.5.3 The export/import file contents

The transport file is a text file in UNIX format. This means that the windows default text editor ‘notepad.exe’, does not correctly split the text into lines, instead all text appears on one long line. The file should not be edited with an editor which does not support Unix-style text. We recommend using a better text editor, such as ‘Notepad++’ which is freely available on the net.

The file contains a list of NMSIDs, followed by the ‘=’ character and the value assigned to that

NMSID. There are also comment rows, which usually give the name of the following NMSID and possibly the list of valid values.

Example 1:

```
#Address (RMAC)
0:1.398=1
```

The first row is a comment, identified by the '#' character. Everything on comment rows is ignored when importing. This comment tells us that the next NMSID is the address.

The next row begins with a zero, followed by a colon character ':'. The zero indicates the sub-unit is the RU (1 would be CU). Next number is the NMSID, which is '1.398'. After the equal sign '=' is the value, which is 1. The address of the RU is therefore set to 1.

Example 2:

```
#Protocol Mode
#0 = Basic-RX Priority, 1 = Basic-TX Priority, 2 = Basic-Repeater, 6 = Packet Routing
0:1.409=6
```

The two comment rows tell that this is the Protocol Mode setting, and valid choices are 0, 1, 2, or 6. The comment explains what each number means. The actual NMSID row again shows that sub-unit is 0 (RU), the NMSID is '1.409' and the current value is '6'.

8.5.4 Managing export files

You can use transport files as backup to store the settings of devices in your network, so in case you need to replace the hardware, you can just import the saved settings to the new hardware. In this case it is useful to name the transport files to the name of the radio station, for example.

Remember that the file extension must remain as .nmst, otherwise you are free to rename the file. Avoid using special characters in the name.

Another way to use transport files is to create a file containing all the settings, which are common to all modems in your network. Some such settings are RX and TX frequencies (0:1.256 and 0:1.257), bandwidth, airspeed, encryption keys, network ID, TUN Base Address (1:1.3212) etc. These settings must be the same in each modem for the network to work. If you put all these settings in a single file, you can easily import it to all modems, saving time and avoiding errors caused by inputting all the settings by hand.

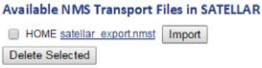
Another use related to the above is to copy some settings from one modem to another. In this case you should carefully edit the file after exporting, removing any settings you do not wish to modify in the target device. For example you might want to create a copy of a modem you have already configured, except for the Address and IP settings, which should remain as they are. In this case remove the relevant rows from the file before importing it to the target modem.
Always be careful of typing errors when editing the file. If any errors appear in the file, the whole import process fails (see next paragraph).

NMS Commands, such as Save User settings, Restore User settings and Reset should NOT be used in a transport file.

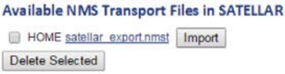
8.5.5 Importing settings to a modem

To send a transport file to the modem follow this procedure:

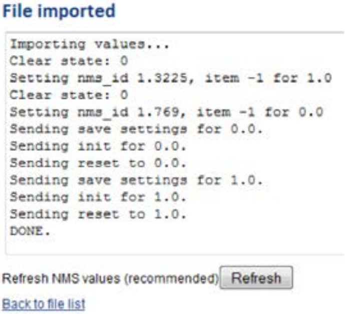
1. Click the Browse… button under the NMS Transport File Upload heading, select your file in the window that opens, and finally select the Upload button.


Available NMS Transport Files in SATELLAR
□ HOME satellar_export.nmst
Import
Delete Selected

2. The file will appear under the Available NMS Transport Files heading. Select on the "Import" button to import the settings.


Available NMS Transport Files in SATELLAR
□ HOME satellar_export.nmst
Import
Delete Selected

3. The importing process result is shown in a text box.



File imported

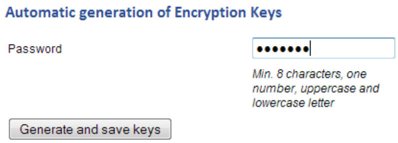
```
Importing values...
Clear state: 0
Setting nms_id 1.3225, item -1 for 1.0
Clear state: 0
Setting nms_id 1.769, item -1 for 0.0
Sending save settings for 0.0.
Sending init for 0.0.
Sending reset to 0.0.
Sending save settings for 1.0.
Sending init for 1.0.
Sending reset to 1.0.
DONE.
```

4. In case of any errors, the process stops and an error message is displayed. The error message will tell which NMS ID caused the error. For example, an error message such as this: "ERROR: Value set of 1.769/-1 for 0.0 failed" means that the NMS ID with the problem was 1.769, and the subunit was 0 (the first number in 0.0 or 1.0 is the subunit). If an error happens, NO values are saved. Fix the error and try again.

8.6 Encryption

The Encryption Application is used to set the encryption keys of the radio protocol of the RU. See the RU User Manual for information about encryption.

You have two choices to input encryption keys. The easiest way is to use a password, and SATELLAR then automatically generates encryption keys from the password. Type your password in the "Password" text field. The web page will show an indicator about how strong the password is. Then click the Generate and save keys button. The same password will always generate the same keys.

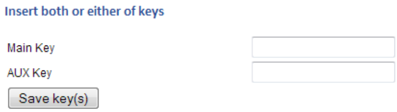


Automatic generation of Encryption Keys

Password ●●●●●●●

Min. 8 characters, one number, uppercase and lowercase letter

The other way to insert encryption keys is to manually insert them. This option is for power users who wish to generate keys themselves.



Insert both or either of keys

Main Key

AUX Key

You can insert either one or both keys at the same time. The key that is left empty is not saved.

Note that as a security measure, the encryption keys or passwords in the device cannot be read back, but you can see a CRC checksum in Modem Info->RU, which can be used to verify if modems have the same keys inserted.

8.7 Logs

Logs are available on the WWW interface only. These can be used to debug problems. If you contact SATEL representative with a problem report, it may be a good idea to include copies of the logs in your report, or SATEL may request you to provide copies.

- Kernel Messages: Linux kernel messages
- System Messages: Linux system messages
- Service Messages: Messages of the SATELLAR Services
- RU NMS Log: internal NMS traffic between the RU and the CU

8.8 Administration

This application contains settings which are not usually needed and have a high possibility of rendering the modem inoperable if they are set into incorrect values.

To access the Administration application in the LCD GUI, select the Admin Tools icon and press Start. This application requires a PIN code.

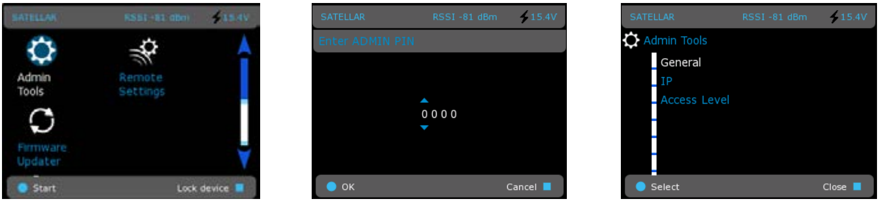


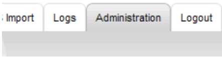
Figure 8.7 Admin tools / Access to Administration applications by CU: Graphical user interface (GUI/LCD)

LCD GUI default pin code	0000

To access Administration application in the WWW User Interface, you need to log out and log in using the admin password.

WWW username	admin
WWW default password	Satel456

After login, the WWW interface has an additional "Administration" tab.

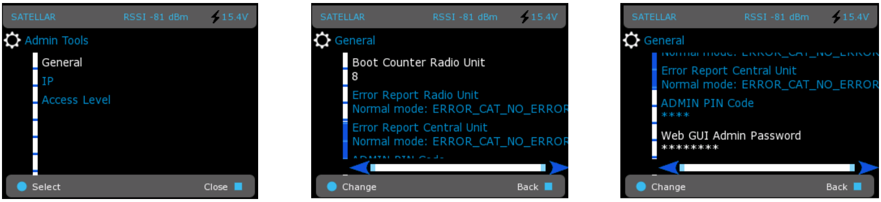


The following setting categories are available in the Administration application.

8.8.1 General

Item	Explanation	Sub unit	NMSID
Boot Counter RU	This value indicates the number of reboots for the RU.	0	1.119
Error Report RU	The currently active error codes. If an internal error caused the unit(s) to reboot, these values will show what caused the error. In case of problems, please send a screen capture of this page to SATEL technical support.	0	1.797
Error Report CU		1	1.797
ADMIN PIN Code	Allows changing the admin pin code.	1	1.3245
Web GUI Admin Password	Allows changing the WWW interface admin password.	1	1.3260

Table 8.8 Admin tools, General



Boot Counter Radio Unit
8
Error Report Radio Unit
Normal mode: ERROR_CAT_NO_ERROR
Error Report Central Unit
Normal mode: ERROR_CAT_NO_ERROR

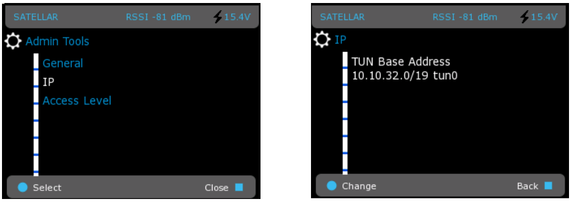
Error Report Central Unit
Normal mode: ERROR_CAT_NO_ERROR
ADMIN PIN Code
****
Web GUI Admin Password
****

Figure 8.8 Admin tools, General by CU: Graphical user interface (GUI/LCD)

8.8.2 IP

Item	Explanation	Sub unit	NMSID
TUN Base Address	This can be used to change the IP Network address of the radio network. It must be the same in all modems of a network. Only change this if your system already uses the 10.10.32.0/19 network. The default is 10.10.32.0/19. For more information, see chapter 6.1.2.	1	1.3212

Table 8.9 Admin tools, IP



TUN Base Address
10.10.32.0/19 tun0

Figure 8.9 Admin tools, IP by CU: Graphical user interface (GUI/LCD)

8.9 Tools

This application contains maintenance, verification and troubleshooting tools.

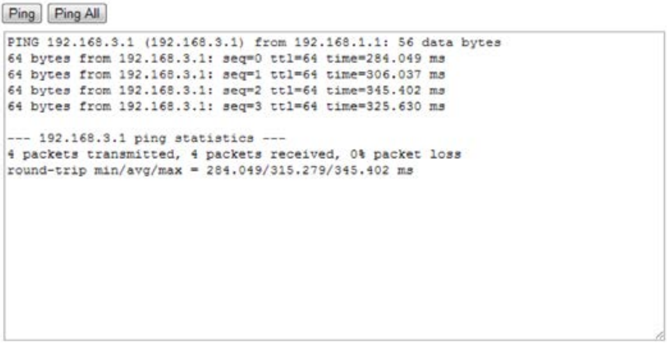
8.9.1 Ping

This tool is used to verify the reachability of a destination IP address with the standard network administration utility ping. It operates by sending echo requests to the destination address and expecting the response back. These requests are used to measure the round-trip time and packet loss. The ping tool in the WWW interface has the following parameters:

Option	Effect
Destination IP address	The IP address that the requests are sent to. The format used is four integers from the range 0-255, separated by dots. For example: 192.168.1.1 10.10.32.1
Source IP address	The source IP address to be sent with the query. It is selected from a drop-down menu containing all the IP addresses of the unit.
Number of pings	Defines how many messages will be sent to the destination address. If left blank, the messages will be sent continuously until “Stop Ping” is selected.
Packet size	Size of the sent message. Useful parameter to adjust to verify the network operation by simulating user data messages of different sizes.
Interval	How often are new ping requests send

Table 8.10 The ping tool in the WWW interface

Ping and Ping All buttons are shown above the output window. When the button Ping is selected, sending the requests with the provided parameters will start. Results calculated based on the received responses will be shown in the output window. The window is refreshed every 5 seconds until the operation is complete. If some of the parameters are invalid, an error message will be displayed.



```
PING 192.168.3.1 (192.168.3.1) from 192.168.1.1: 56 data bytes
64 bytes from 192.168.3.1: seq=0 ttl=64 time=284.049 ms
64 bytes from 192.168.3.1: seq=1 ttl=64 time=306.037 ms
64 bytes from 192.168.3.1: seq=2 ttl=64 time=345.402 ms
64 bytes from 192.168.3.1: seq=3 ttl=64 time=325.630 ms

--- 192.168.3.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 284.049/315.279/345.402 ms
```

Figure 8.10 Ping error message

When Ping All is selected, then the echo requests will be sent to all gateways known to the unit. The gateways are specified in the Routing -> IP Routes. The parameter of destination IP address will be ignored in this case, but all other parameters will be applied.

When the Ping is running, a third button will appear:

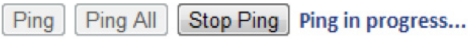


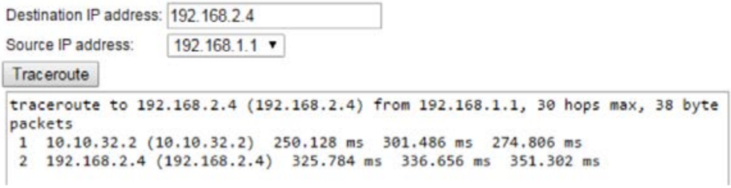
Figure 8.11 Stop Ping -button

When Stop Ping is selected, the currently running Ping operation will be terminated. Leaving the page will not stop the operation. Even if other pages are accessed in the browser, the Ping will still continue running on the background. It will not stop until Stop Ping has been selected.

8.9.2 Traceroute

Traceroute is a network diagnostic tool for displaying the hops taken by the IP packet along the route to the destination. Traceroute also measures and displays round-trip times for each hop. In the resulting listing, the hops are represented by their IP addresses, or if the tool is not able to request information from one of the hops, an asterisk (“*”) will be dispalyed instead. Note that this is not a necessarily an indication of a problem.

There are only two parameters for this tool: the destination IP address and the source IP address. Both have same functionality as with the Ping tool. After the parameters are set, the Traceroute button is selected to start the operation. An example the output of finished traceroute operation:



Destination IP address: 192.168.2.4
Source IP address: 192.168.1.1 ▼

```
traceroute to 192.168.2.4 (192.168.2.4) from 192.168.1.1, 30 hops max, 38 byte
packets
 1  10.10.32.2 (10.10.32.2)  250.128 ms  301.486 ms  274.806 ms
 2  192.168.2.4 (192.168.2.4)  325.784 ms  336.656 ms  351.302 ms
```

Figure 8.12 Output of the finished Traceroute operation

8.9.3 NMS Value

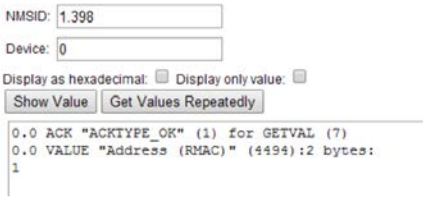
The NMS value tool is used to show the values of individual settings with the help of NMSIDs. See chapter 5.8 for more information about NMSIDs.

The tool has the following options:

Option	Effect
NMSID	The NMSID of the setting to be shown, for example 1.389. Chapter 7 provides a list of available NMSIDs. Multiple NMSIDs can be provided, separated by whitespace. The maximum number of NMSIDs is 30.
Device	The target device to read the NMSID value from: • 0 for local RU • 4096 for local CU • RMAC of the remote device for remote RU • 4096+ RMAC of the remote device for the remote CU
Display as hexadesimal	If this option is selected, the value of the NMSID will be displayed as hexadesimal.
Display only value	If this option is selected, only the returned value will be sown. All other information, for example messaging, will be omitted.

Table 8.11 NMS Value options

Select the button Show Value to start the operation. As a result, the output will appear in the text field. See the following picture for an example output:

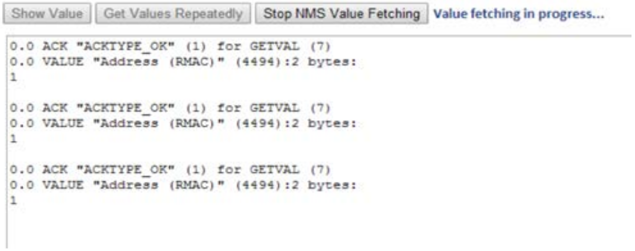


```
0.0 ACK "ACKTYPE_OK" (1) for GETVAL (7)
0.0 VALUE "Address (RMAC)" (4494):2 bytes:
1
```

Figure 8.13 Output of the NMS Value

The result consist of three rows. The first row is an acknowledgement message from the device. The next row contains the name of the parameter that was queried and the size of the value in bytes. The third row contains the actual value. In case of errors, for example if the queried NMSID is unknown, the second row shows an error message and the third row will be omitted.

If the button Get Values Repeatedly is selected, the values will be queried repqtedly, until the button Stop NMS Value Fetching is selected. Leaving the page will not stop the process. The Stop NMS Value Fetching button is also available, when multiple NMSIDs are inserted and the query process is running.



```
0.0 ACK "ACKTYPE_OK" (1) for GETVAL (7)
0.0 VALUE "Address (RMAC)" (4494):2 bytes:
1

0.0 ACK "ACKTYPE_OK" (1) for GETVAL (7)
0.0 VALUE "Address (RMAC)" (4494):2 bytes:
1

0.0 ACK "ACKTYPE_OK" (1) for GETVAL (7)
0.0 VALUE "Address (RMAC)" (4494):2 bytes:
1
```

Figure 8.14 Stop NMS Value Fetching

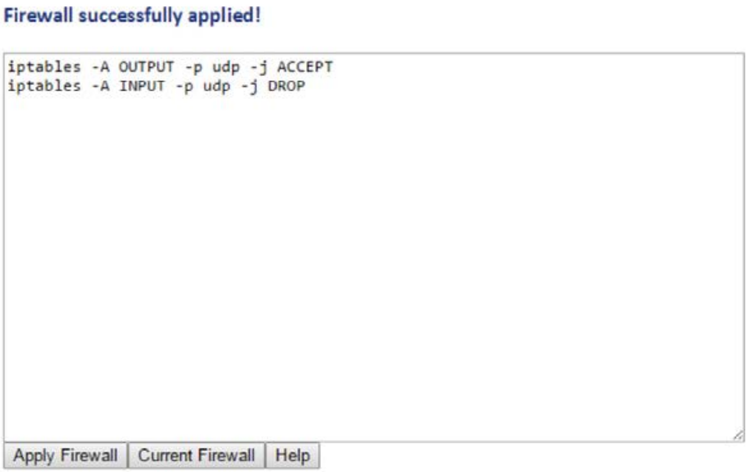
8.9.4 Firewall

This tool is used to set up a firewall to the SATELLAR with the Linux tool iptables. This is a fearure for advanced users, and using it in the wrong way can easily block essential IP traffic. This manual will not explain the usage of iptables itself, more information about the tool can be found at http://www.iptables.org

The tool page in the WWW interface contains one editor window and three buttons. Valid iptables commands may be written into the window, each command on a new line. The commands will be applied when the button "Apply Firewall" is selected.

If the button "Current Firewall" is selected, a new window will open showing the currect firewall rules (if any). The third button "Help" displays the help text of the iptables tool.

An example allowing outgoing but blocking incoming UDP traffic can be seen in the following figure:



Firewall successfully applied!

```
iptables -A OUTPUT -p udp -j ACCEPT
iptables -A INPUT -p udp -j DROP
```

9. Type designation

The label of the CU is located on the back of the CU.

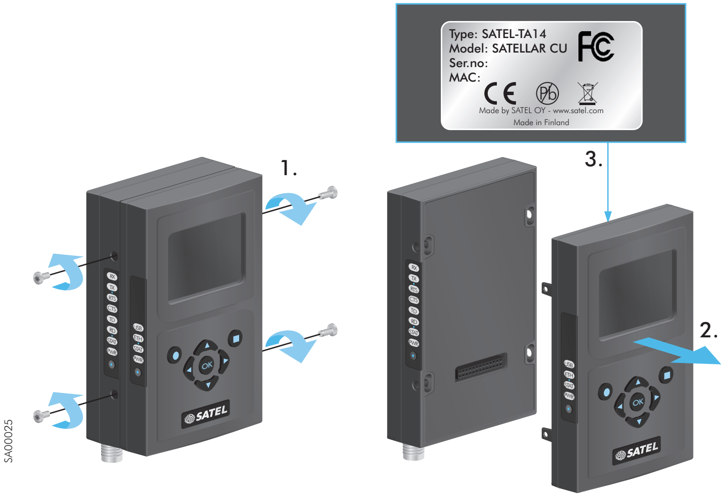


Figure 9.1 Location of the labels in CU

10. Troubleshooting

10.1 Error codes

If the MCU detects an error in operation, it indicates the error state by LEDs in the following way:

At first all the LEDs are switched on for one second. Thereafter all the LEDs are switched off for one second and then an error code is shown for three seconds. This sequence is repeated for approximately one minute or until the MCU is restarted. In some cases the error causes the unit to restart automatically.

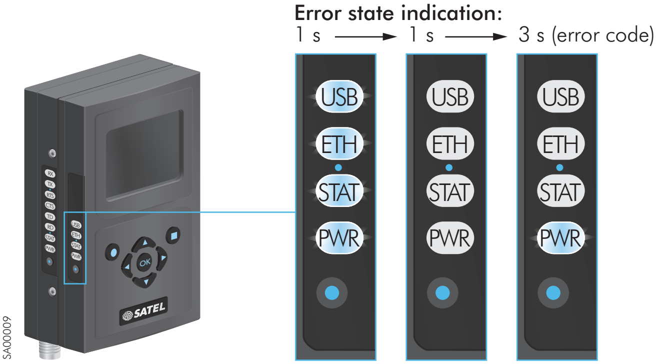


Figure 10.1 Error state and error code indicated by LEDs

For displaying the error codes the four LEDs indicates a binary number, USB LED is the first (MSB) and PWR LED the last (LSB). LED switched on means bit ‘1’. The error codes are the following:

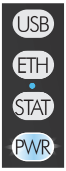
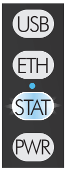
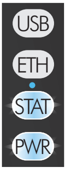
	Binary	Error code	Description
	0001	1	USB over current
	0010	2	USB under voltage
	0011	3	Ethernet interface problem
	0100…1111	4…15	Reserved for future needs
	0000	0	Not used

Table 10.1 Error codes

11. SATEL open source statements

11.1 LGPL and GPL software

This SATEL product contains open source software (OSS), licensed under LGPLv2, GPLv2, GPLv3 and other licenses.

License details for LGPLv2.1 are available from http://www.gnu.org/licenses/lgpl-2.1.html
License details for GPLv2 are available from http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
License details for GPLv3 are available from http://www.gnu.org/licenses/gpl-3.0.html

ALL OPEN SOURCE SOFTWARE used in this software is distributed WITHOUT ANY WARRANTY and is subject to copyrights of one or more respective authors. For more details, see the GPL and LGPL license texts.

11.2 Written offer for LGPL and GPL source code

Where such specific license terms entitle you to the source code of such software, SATEL will provide upon written request via email and/or traditional paper mail the applicable LGPL and GPL source code files via CD-ROM for a nominal fee to cover shipping and media charges as allowed under those respective licenses.

Contact SATEL Technical support for more details: Please visit http://www.satel.com.

12. Settings selection guide

12.1 Modem Settings

Menu	Submenu	Value (* = default)
Network Protocol Mode	NetID	Satel NG * (max 8 characters)
	Address (RMAC)	0001 * (1 - 4093)
	Protocol Mode	Basic-RX Priority Basic-TX Priority Basic-Repeater Packet Routing *
Radio	TX Frequency	460.000000 MHz (Depends on hardware configuration)
	RX Frequency	460.000000 MHz (Depends on hardware configuration)
	RF Output Power	100 mW 200 mW 300 mW 400 mW 500 mW 600 mW 700 mW 800 mW 900 mW 1000 mW *
	Signal Threshold	-114 dBm *
	Over.the-Air Encryption	OFF * / ON
	Forward Error Correction	OFF, Half FEC, Two-thirds FEC
	Channel Spacing	12.50, 25.00 kHz *
	Air Speed	9600, 19200 *, 28800, 38400 bps with 25kHz Channel Spacing
		4800, 9600, 14400, 19200 bps with 12.50 kHz Channel Spacing
Serial Connector Configuration	Radio Unit Port Assignment	NONE MCU UARTS TO SATBUS * DATA UART TO RADIO D9 RD/TD DATA UART TO RADIO D9 RD/TD - NMS TO D9 DTR/DSR DATA UART TO RADIO D9 RD/TD - NMS TO D9 RTS/CTS DATA UART TO RADIO D9 RD/TD - NMS TO SATBUS MCU UARTS TO SATBUS CAN
	DTE Port Physical Communication Mode	RS-232 (with handshaking)
		RS-422, RS-485, FD-RS485 (without handshaking)

Menu	Submenu	Value (* = default)
Data Port Settings	Rate	1200, 2400, 4800, 9600, 19200 *, 38400, 57600 bps
	Data Bits	7, 8 bits *
	Parity	No Parity Check *, Even, Odd
	Stop Bits	1 bit *, 2 bits
Serial Data Flow Control	TX Delay	0 * (0 - 65535)
	CRC	OFF / ON *
	Handshaking CTS Line	Clear To Send, TX buffer state *, RSSI Treshold, Always ON
	Handshaking RTS Line	Ignored *, Flow control, Reception control
	Handshaking CD Line	RSSI treshold *, Data on channel, Always ON
	Pause Length	3 bytes * (3 - 255)
	Maximum Number of Accepted Errors	0 * (0 - 255)
Packet Mode Radio Access Control	Network Topology	Point-to-point *, Repeater, Fast mode
	Retransmissions	OFF / ON *
	Training Sequency Length Back	Full * / Half
	Off Counter	8 * (4 - 63)
General	Name	SATELLAR * (1 - 30 characters)
	PIN Code	0000 * (4 numbers: 0000-9999)
	Temperature Unit	Celsius *, Fahrenheit, Kelvin
	Temperature Min	+0 (-50 - +80 Celsius)
	Temperature Max	+50 (-50 - +80 Celsius)
	SNR Critical Level	0 (0 - 35)
	UI Voltage Critical Level	9 V * (9 - 30 V)
	UI RSSI Critical Level	-110 dBm * (-100 - -118 dBm)
	UI Voltage Display Mode	Numeric * / Bar
	UI Voltage Bar Min	9 * (9 - 30 V)
	UI Voltage Bar Max	30 * (9 - 30 V)
	PIN Code Required	No * / Yes
	USB Device Mode	Serial Port * / Mass Memory
	Display Brightness	255 * (0 - 255)
	Web GUI Password	Satel123 * (8 characters)
	GUI Color Profile	Blue / Black *
	LCD Timeout	2560 s * (1 - 65535 s)

Menu	Submenu	Value (* = default)
Services	SSHD State	OFF / ON *
	HTTPD State	OFF / ON *
	NMSBluetoothd State	OFF / ON *
	NMSTcpsocketd State	OFF / ON *
	NMSLoggerd State	OFF / ON *
	Linklayer State	OFF / ON *
	NMSGathererd Timeout	5000 ms * (1000 - 65535 ms)
	NMSLoggerd Interval	3000 ms * (1000 - 65535 ms)
	NMSLoggerd Timeout	5000 ms * (1000 - 65535 ms)
	NMSLoggerd Retries	2 * (0 - 10)
	RU Commslogd State	OFF / ON *
	SNMPD State	OFF / ON
	USB Host Control	OFF / ON *
	UI Power Control	OFF / ON *
	HTTPD IP Address	All local addresses
	SSHD IP Address	All local addresses
	NMSTcpsocketd IP Address	All local addresses
Commands	Restore Default Factory Settings Radio Unit	Do not reset / Reset
	Restore Default Factory Settings Central Unit	Do not reset / Reset
	Reset Radio Unit	Do not reset / Reset
	Reset Central Unit	Do not reset / Reset
	Reboot Central Unit	Do not reboot / Reboot
	Statistical Counters Clear	Do not clear / Clear
Remote Devices	Pre-Cache All Settings of Device	OFF * / ON
	Diagnostics Polling of Device	OFF* / ON
SNMP	SNMP RO Community	public
	SNMP RW Community	private
	SNMP RW Community IP	0.0.0.0
	SNMP Notification IP	192.168.1.2
	SNMPv3 User name	user123
	SNMPv3 User Type	Read-write* / Read-only
	SNMPv3 USM Security Type	No Auth*/MD5 No Priv/SHA No Priv/MD5 DES/SHA DES/ MD5 AES/SHA AES
	SNMPv3 Authentication Passphrase	pass123word
	SNMPv3 Privacy Passphrase	pass123word
	SNMP Listening IP Address	0.0.0.0
	Notification interval	30 (10-600 s)
	Voltage Notification	OFF* / ON
	RSSI Notification	OFF* / ON
	Temperature Notification	OFF* / ON

Menu	Submenu	Value (* = default)
	SNR Notification	OFF* / ON
	Commit Notification	OFF* / ON
	Redundancy Notification	OFF* / ON
Time Control	Time Operation Mode	No time operation *, Manual time operation, NTP time
	NTP Server Address	192.168.1.1 *
	NTP Request Source IP Address	All local addresses
	NTP Interval	100 s *
	Time	1980-02-01 00:00:00 * (format YYYY-MM-DD hh:mm:ss)
	Time Zone	Greenwhich Mean Time *
		Central European Time (GMT+1)
		East European Time (GMT+2)
		Moscow Time (GMT+3)
		Iran Standard Time (GMT+3:30)
		Iran Daylight Saving Time (GMT+4:30)
		Mauritius Time (GMT+4)
		Afganistan Time (GMT+4:30)
		Pakistan Time (GMT+5)
		Indian Standard Time (GMT+5:30)
		Nepal Time(GMT+5:45)
		Bhutan Time(GMT+6)
		Myanmar Time (GMT+6:30)
		Bangladesh Standard Time(GMT+7)
		China Standard Time(GMT+8)
		Apo Island Time (GMT+8:15)
		Australian Central Western Standard Time (GMT+8:45)
		Japan Standard Time (GMT+9)
		Australian Central Standard Time(GMT+9:30)
		Australian Eastern Standard Time (GMT+10)
		Australian Central Daylight Time (GMT+10:30)
		Vanuatu Time (GMT+11)
		New Zealand Standard Time (GMT+12)
		New Zealand Daylight Time (GMT+13)
		Chatham Island Standard Time (GMT+12:45)
		Chatham Island Daylight Time (GMT+13:45)
		Line Island Time (GMT+14)
		Baker Island Time (GMT-12)
		Samoa Standard Time (GMT-11)
		Hawaiian Standard Time (GMT-10)
		Marquesas Island Time (GMT-9:30)
		Alaska Standard Time (GMT-9)
		Pacific Standard Time (GMT-8)
		Mountain Standard Time (GMT-7)
		Central Standard Time (GMT-6)

Menu	Submenu	Value (* = default)
		Eastern Standard Time (GMT-5)
		Venezuela Standard Time (GMT-4:30)
		Atlantic Standard Time (GMT-4)
		Atlantic Daylight Time (GMT-3)
		Newfoundland Standard Time (GMT-3:30)
		Newfoundland Daylight Time (GMT-2:30)
		Brazilian Standard Time (GMT-3)
		Brazilian Eastern Standard Time (GMT-2)
Testing and Calibration	Carrier Test	OFF* / ON
	Carrier Test Timeout	0 (0 - 65535 s)
	Fast RSSI Scan	OFF* / ON
	RSSI RMAC Address	4096 (1 - 4096)

12.2 Routing

Menu	Submenu	Value (* = default)
Packet Routing Array	see chapter 7.3.1	
IP	IP Address (eth0)	192.168.2.1/24 *
	QoS Set	ignored
	DHCP State	OFF * / ON
	Ethernet Speed	Auto *, 10 Mbps, 100 Mbps
	Automatic IP State	OFF * / ON
	Ethernet Duplex	Full * / Half
	IP Queue Max Time Length	5000 ms * (1 - 65535 ms)
	IP Queue Max Packets	10 * (1 - 65535)
	IP MTU Size	1500 Bytes
	Proxy ARP	OFF * / ON
	IP Header Compression	ON * / OFF
VLAN	see chapter 7.5	
IP Route	see chapter 7.3.3	
Route Monitoring	Check Interval	60 (30 - 65535 s)
	Only Check With Traffic	Yes / No*
	Allowed Fail Count	2 (0 - 65535)
	Only Monitor Primary	Yes / No*
	Revert Timer	300 (0 - 65535 s)
	Ping Timeout	10 (0 - 65535 s)
VRRP	VRRP State	OFF* / ON
	VRRP Virtual IP Address	0.0.0.0/24
	VRRP Virtual Router ID	0* (1 - 255)

	VRRP Priority	100 (2- 255)
	VRRP advertisement Interval	1 (1 - 65535 s)
	VRRP Check Target Radio IP	0.0.0.0
	VRRP Inetrface	eth0
	VRRP Check Target Local IP	0.0.0.0
	VRRP Virtual RMAC	0 (0 - 4095)
Serial IP	Serial IP Mode	OFF*/Server mode/Client mode/Send only/Receive only/ Twoway mode
	Port Rate	1200 bps/2400 bps/4800 bps/9600 bps/19200 bps/38400 bps/57600 bps/115200 bps*/460800 bps
	Port Data Bits	7 bits / 8 bits*
	Port Parity	No Parity Check* / Even / Odd
	Port Stop Bits	1 bit* / 2 bit
	Protocol	TCP*/ UDP/ Telnet/ Bulk Mode
	Listening Port	2005 (1 - 65535)
	Destination Port	2006 (1 - 65535)
	Destination IP Address	10.10.32.1
	Sender Retry Count	5 (0 - 255)
	Sender Retry Interval	1000 (500 - 65535 s)
	UDP Listener Port Timeout	5 (0 - 65535 s)
	Remote Control Port Mode	OFF* / ON
	Remote Control Port Rate	9600 bps/19200 bps/38400 bps/57600 bps/115200 bps*/460800 bps
	Remote Control Port	2007 (1 - 65535)
	Minimum Packet Characters	1 (0 - 255 bytes)
	Packet Creation Timeout	0.0 (0 - 255 s)
	Local Ip Address	All local adresses
Application Routing	Application Protocol	OFF* / DNP3 / Modbus RTU
	Appliaction Transport Protocol	TCP* / Serial Port
	Application Listening Port	20000 (1 – 65535)
	Serial Port	RS-232* / USB-A
	Port Rate	1200 bps/2400 bps/4800 bps/9600 bps/19200 bps/38400 bps/57600 bps/115200 bps*/460800 bps
	Port Data Bits	7 bits/8 bits*
	Port Parity	No Parity Check*/Even/Odd
	Port Stop Bits	Port Stop Bits, 1 bit*/2 bits
	Transport Protocol For Substation Data	TCP / UDP*
	Destination Port For Substation Data	2006 (1 – 65535)
	Listening Port For Substation Data	2005 (1 – 65535)
	Application Listening IP Address	All local addresses
	Address Mapping	Application Address To RMAC* / Manual
	Address Mapping Row**)	1 10.10.32.1
	**) Available only in web UI	

12.3 Administration

Menu	Submenu	Value (* = default)
General	ADMIN PIN Code	0000 * (0000 - 9999)
	Web GUI Admin Password	Satel456 * (8 characters)
IP	TUN Base Address	10.10.32.0/19 *

SATEL Oy
Meriniitynkatu 17, P.O.Box 142
FI-24101 Salo, Finland
Tel. +358 2 777 7800
info@satel.com
www.satel.com

WIRELESS WORLD – LOCAL SOLUTION

SATEL