



## Regesta Smart Web Interface

Teldat-Dm 1003-I

Copyright© Teldat-DM1003-I Version 1.1 Teldat S.A.

## **Legal Notice**

### **Warranty**

This publication is subject to change.

Teldat S.A. offers no warranty whatsoever for information contained in this manual.

Teldat S.A. is not liable for any direct, indirect, collateral, consequential or any other damage connected to the delivery, supply or use of this manual.

# Table of Contents

Chapter 1	Introduction . . . . .	1
1.1	Introduction . . . . .	1
1.2	Local connection to the router . . . . .	1
Chapter 2	Web Interface . . . . .	6
2.1	Structure . . . . .	6
2.2	Info Menu . . . . .	6
2.3	Status Menu . . . . .	7
2.3.1	WWAN-1 Status . . . . .	8
2.3.2	DMVPN connections . . . . .	12
2.3.3	DHCP Clients . . . . .	12
2.3.4	Netstat . . . . .	13
2.3.5	Diagnostics . . . . .	14
2.3.6	PRIME . . . . .	15
2.3.7	SCADA . . . . .	17
2.4	Logs Menu. . . . .	20
2.4.1	WWAN-1 Traces . . . . .	20
2.5	System Menu . . . . .	21
2.5.1	Password . . . . .	21
2.5.2	Settings . . . . .	22
2.5.3	SNMP . . . . .	22
2.6	Nets Menu. . . . .	25
2.6.1	Interfaces . . . . .	26
2.6.2	Networks . . . . .	28
2.6.3	DMVPN . . . . .	31
2.6.4	Wireless WAN Configuration . . . . .	33
2.6.5	DHCP . . . . .	38
2.6.6	Routes . . . . .	40
2.6.7	PRIME . . . . .	43
2.6.8	SCADA . . . . .	45
2.6.9	Virtual Bridges . . . . .	45
Chapter 3	Configuration Recommendations . . . . .	48
3.1	Keepalive mechanism in the tunnels . . . . .	48
3.2	Parameters for carrier changeover . . . . .	49

# Chapter 1 Introduction

## 1.1 Introduction

Regesta Smart routers can be quickly and efficiently booted through web configuration.

The Web Configurator is set up to automate the configuration process based on the router's work scenario. The configuration parameters that can be accessed through the web are those vital for router operations. The remaining parameters, hidden from the user, contain values that are adjusted for optimal operation. The adjustment criterion used is the connection speed to terminals.

## 1.2 Local connection to the router

If no settings have been pre-activated, the default factory settings installed will be enabled. You can access the Web Configurator by connecting the Ethernet cable, supplied with the router, to the WAN port and to the PC that is being used for configuration purposes.



Fig. 1: WAN port in a Regesta Smart router.

The default IP address, accessible from the WAN port, is 192.168.1.1/24. The PC must have an address belonging to the Regesta Smart subnet (192.168.1.0/24).

Once you have made sure the router can be accessed via the IP address, enter the following URL into the web browser:

<http://192.168.1.1>

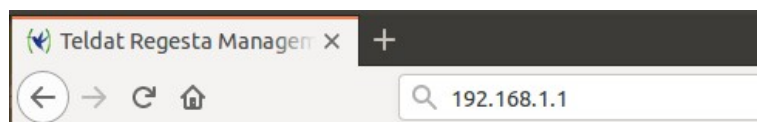



Fig. 2: Accessing the Web Configurator.

If access is correct, the Web Configurator home page is displayed. Its format and the information shown depend on the Regesta Smart model and license.

**Administrator**

User

Password




Add to Favorites 📶 -59 dBm voda ES GSM Online

## Administration

**Wireless Connection**

**Wireless Connection Status**


Online

▶ **As administrator you can:**

- WWAN connection
- DMVPN network
- VLAN configuration
- DHCP server
- NTP client

**Teldat Regesta Smart PRO**

**Overview**

The Regesta Smart PRO model is a rugged equipment with one Gigabit Ethernet port, one Gigabit Ethernet/SFP port and one integrated WWAN interface. Optionally, this model can have a four-port Gigabit Ethernet switch and serial interfaces.

---

**Regesta Smart PRO**


Web Firmware Version: 12.1.0

Fig. 3: Home page of the Regesta Smart PRO with WWAN access technology.

**Administrator**

User

Password




Add to Favorites 📶 -67 dBm voda ES GSM Online

## Administration

**Wireless Connection**

**Wireless Connection Status**


Online

▶ **As administrator you can:**

- WWAN connection
- DMVPN network
- VLAN configuration
- DHCP server
- NTP client

**Teldat Regesta Smart PLC**

**Overview**

The Regesta Smart PLC model is a rugged equipment with one Gigabit Ethernet port, one Gigabit Ethernet/SFP port, one integrated WWAN interface and one PLC interface. Optionally, this model can have serial interfaces.

---

**Regesta Smart PLC**

Web Firmware Version: 12.1.0

Fig. 4: Home page of the Regesta Smart PLC with WWAN access technology.

Fig. 5: Home page of the Regesta Smart LITE with WWAN access technology.

In the bar at the top of the home page, a changing text indicates whether the device may be accessed through WWAN technology or not. If the device cannot be accessed or is not equipped with this technology, an “Offline” information message appears.

Fig. 6: WWAN Access: Coverage quality, carrier, technology and connection status.

Fig. 7: The device is inaccessible or is not equipped with WWAN access technology.

In the middle of the home page, a graph shows the status of the character associated to WWAN access technology (where present in the device). Written information on the characteristics of the Web Configurator and the Regesta Smart model can also be found.

Fig. 8: Home page information – Regesta Smart PRO with WWAN access technology.

### Administration

<p><b>Wireless Connection</b></p> <p><b>Wireless Connection Status</b></p> <p> <b>Offline</b></p> <p>▶ <b>As administrator you can:</b></p> <ul style="list-style-type: none"> <li>- WWAN connection</li> <li>- DMVPN network</li> <li>- VLAN configuration</li> <li>- DHCP server</li> <li>- NTP client</li> </ul>	<p><b>Teldat Regesta Smart PLC</b></p> <p><b>Overview</b></p> <p>The Regesta Smart PLC model is a rugged equipment with one Gigabit Ethernet port, one Gigabit Ethernet/SFP port, one integrated WWAN interface and one PLC interface. Optionally, this model can have serial interfaces.</p>
--	---

Fig. 9: Home page information – Regesta Smart PLC with WWAN access technology.

### Administration

<p><b>Wireless Connection</b></p> <p><b>Wireless Connection Status</b></p> <p> <b>Online</b></p> <p>▶ <b>As administrator you can:</b></p> <ul style="list-style-type: none"> <li>- WWAN connection</li> <li>- DMVPN network</li> <li>- VLAN configuration</li> <li>- DHCP server</li> <li>- NTP client</li> </ul>	<p><b>Teldat Regesta Smart LITE</b></p> <p><b>Overview</b></p> <p>The Regesta Smart LITE model is a rugged equipment with one Gigabit Ethernet port, one Gigabit Ethernet/SFP port and one integrated WWAN interface. Optionally, this model can have serial interfaces.</p>
---	--

Fig. 10: Home page information – Regesta Smart LITE with WWAN access technology.

The rest of the page displays information on the device model and the web firmware version installed.

<b>Regesta Smart PLC</b>	Web Firmware Version: 12.1.0
--------------------------	------------------------------

Fig. 11: Device model and Web firmware version installed.

To access device configuration and monitoring, enter the user and password and click on the “Log in” button. Initially, the device leaves the factory without any defined users.

**Administrator**

**User**

**Password**

Fig. 12: Access with user and password.

Depending on the access level assigned to the logged-in user (*root*, *configuration* or *monitoring*), he/she may be able to access some pages but not others.


<b>Info</b>	Status ▾	Logs ▾	System ▾	Nets ▾	 -69 dBm voda ES WCDMA Online	<b>Logout</b>
-------------	----------	--------	----------	--------	--	---------------

Fig. 13: Access through the “root” level.


<b>Info</b>	Status ▾	Logs ▾	System ▾	Nets ▾	 Offline	<b>Logout</b>
-------------	----------	--------	----------	--------	---	---------------

Fig. 14: Access through the “configuration” level.



Fig. 15: Access through the “monitoring” level.

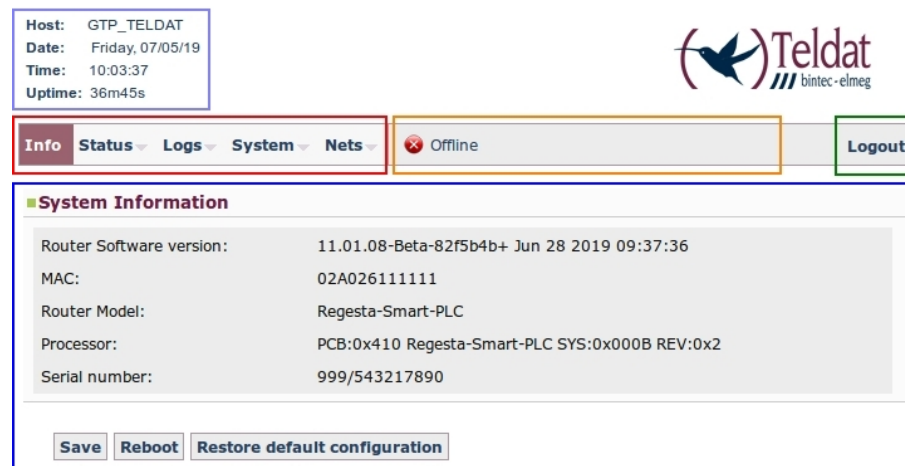


## Chapter 2 Web Interface

### 2.1 Structure

The configuration and monitoring pages have a common structure, described below:

- **Information on the router, date and time** (shown in purple): Displays the name of the router, the date, the time and the time elapsed since the last restart.
- **Main menu** (red): Lets you browse through the different configurator pages.
- **Status bar** (orange): Shows whether the device is accessible through WWAN , whenever this technology is present in the device.
- **Logout** (green): Disconnects the user and redirects him/her to the application's exit page. Here, instructions are given on how to return to the configurator start page.
- **Configuration/monitoring page** (blue): This is the page the user is currently accessing and that allows him/her to configure or monitor the different router characteristics.

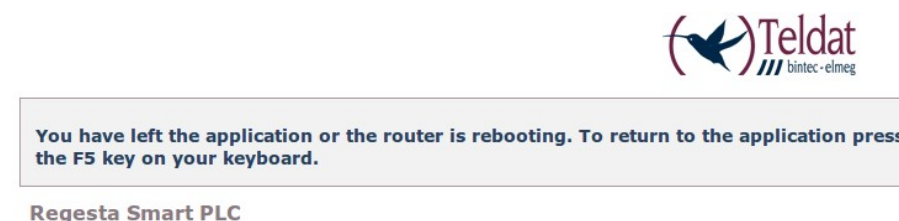


The screenshot shows the Teldat web interface. At the top left, a purple box displays system information: Host: GTP\_TELDAT, Date: Friday, 07/05/19, Time: 10:03:37, Uptime: 36m45s. To the right is the Teldat logo (bintec-elmeg). Below this is a navigation bar with a red 'Info' button, a dropdown menu with 'Status', 'Logs', 'System', and 'Nets', an orange 'Offline' status indicator, and a green 'Logout' button. The main content area is titled 'System Information' and contains a table of router details:

Router Software version:	11.01.08-Beta-82f5b4b+ Jun 28 2019 09:37:36
MAC:	02A026111111
Router Model:	Regesta-Smart-PLC
Processor:	PCB:0x410 Regesta-Smart-PLC SYS:0x000B REV:0x2
Serial number:	999/543217890

At the bottom of the system information section are three buttons: 'Save', 'Reboot', and 'Restore default configuration'.

Fig. 16: Page structure.



The screenshot shows the Teldat application's exit page. At the top right is the Teldat logo (bintec-elmeg). Below it is a grey box with the text: "You have left the application or the router is rebooting. To return to the application press the F5 key on your keyboard." Below this box is the text "Regesta Smart PLC".

Fig. 17: Application's exit page.

### 2.2 Info Menu

Once the user and password have been validated, the following page containing information on the device is displayed.

**System Information**

Router Software version:	11.01.08-Beta-82f5b4b+ Jun 28 2019 09:37:36
MAC:	02A026111111
Router Model:	Regesta-Smart-PLC
Processor:	PCB:0x410 Regesta-Smart-PLC SYS:0x000B REV:0x2
Serial number:	999/543217890

Fig. 18: "Info" page.



#### Note

The "Save," "Reboot" and "Restore default configuration" buttons are only available if the logged-in user has been assigned a "root" or "configuration" access level.

The data shown is as follows:

- **Router Software version:** Router's CIT version.
- **MAC:** Physical Ethernet address.
- **Router Model:** Regesta Smart model.
- **Processor:** Processor.
- **Serial number:** Router's serial number.

There are three buttons at the bottom of the page that execute the following actions:

- **Save button:** Lets you save the changes made in the router configuration.
- **Reboot button:** Lets the user reboot the router from the Web. By clicking on this button, the user is automatically logged out and redirected to the application's exit page.



#### Note

So that changes made in the router configuration through the Web Configurator can activate, you first need to save them via "Save" and then restart the router using "Reboot".

- **Restore default configuration button:** Lets you reestablish the router's default configuration, which automatically restarts for changes to be effective. On reboot, the user is automatically redirected to the application's exit page.



#### Note

If you reestablish the default configuration, you will lose all subsequent changes made to the router's configuration.

From this page, and depending on his/her access level, the user can enter the remaining Web Configurator pages. The following sections describe the configuration/monitoring screens in the order in which they appear in the bar at the top of the page.

## 2.3 Status Menu

This menu allows you to access information regarding several aspects of the router status. This menu varies depending on the Regesta Smart model and its license.

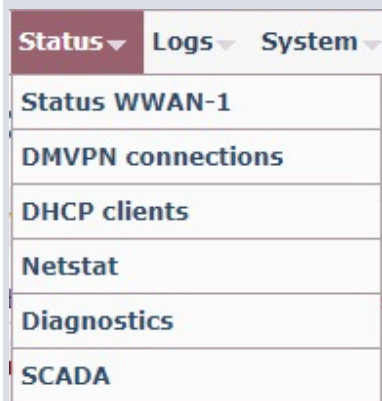


Fig. 19: Status Menu – Regesta Smart PRO with WWAN access technology.

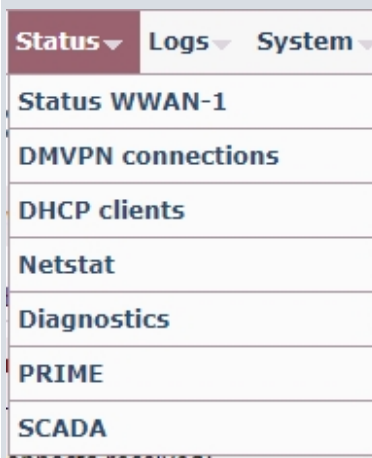


Fig. 20: Status Menu – Regesta Smart PLC with WWAN access technology.

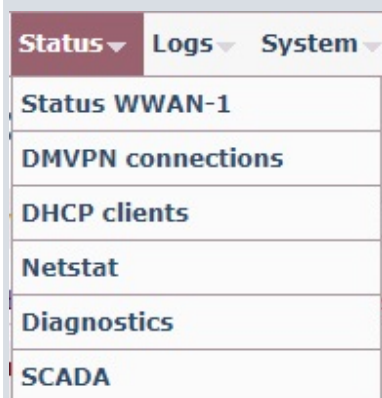


Fig. 21: Status Menu – Regesta Smart LITE with WWAN access technology.

### 2.3.1 WWAN-1 Status

Summarizes the parameters that characterize the cellular interface. This menu option remains hidden in Regesta Smart devices that do not have WWAN technology.

## WWAN-1 Connection Status

### ■ Connection

Register:	Registered
Operator:	21401
Technology:	WCDMA
Level(dBm):	-67

### ■ Cells

	UARFCN	PSC	RSCP(dBm)	ECIO(dB)
Serving Cell:	3062	382	-67	-5
WCDMA Cell #1:	3062	383	-74	-12
WCDMA Cell #2:	3062	376	-77	-15

### ■ Module Information

Manufacturer:	Quectel
Model:	EC25E
Firmware:	EC25EFAR02A08M4G
IMEI:	861107032164981
IMSI:	214019816249846
SIM Card ID	8934569821305399721

### ■ IP Protocol

Assigned IP:	172.17.91.146
--------------	---------------

Fig. 22: Status –WWAN-1 Status.

This page is divided into four sections:

### 2.3.1.1 Connection

Provides information on the status of the radio link and on network registration.

#### ■ Connection

Register:	Registered
Operator:	21401
Technology:	WCDMA
Level(dBm):	-67

Fig. 23: WWAN-1 Status – Connection.

- **Register:** Module's GSM register status in the network.
- **Operator:** Mobile telephony carrier code.
- **Technology:** Type of connection used by the router.
- **Level (dBm):** Signal reception level measured by the module.

### 2.3.1.2 Cells

Displays information on the serving and neighboring cells.



#### Note

It doesn't always show the same information. The latter depends on the type of module and technology used.

### 2.3.1.2.1 Example of 2G Connection

■ Cells						
	Cell ID	PLMN ID	LAC	ARFCN	BSIC	SIGNAL (dBm)
Serving Cell:	13087	21401	17166	102	6	-61 / -60
GSM/EDGE Cell #1:	13115	21401	17166	103	8	-75 / -74
GSM/EDGE Cell #2:	13114	21401	17166	111	6	-73 / -72
GSM/EDGE Cell #3:	13091	21401	17166	117	59	-78 / -77
GSM/EDGE Cell #4:	13116	21401	17166	113	11	-92 / -91

Fig. 24: WWAN-1 Status – Cells (2G Connection).

- **Cell ID:** Serving/neighbor cell in decimal identifier.
- **PLMN ID:** Mobile telephony carrier identifier.
- **LAC (Location Area Code):** Local area code for the serving/neighbor cell in decimal.
- **ARFCN (Absolute Frequency Channel Number):** Channel number selected.
- **BSIC (Base Station Identity Code):** Base station identifier.
- **Signal (dBm):** Signal reception level.

### 2.3.1.2.2 Example of 3G Connection

■ Cells				
	UARFCN	PSC	RSCP(dBm)	ECIO(dB)
Serving Cell:	3062	382	-67	-5
WCDMA Cell #1:	3062	383	-74	-12
WCDMA Cell #2:	3062	376	-77	-15

Fig. 25: WWAN-1 Status – Cells (3G Connection).

- **UARFCN (Absolute Frequency Channel Number):** Channel number selected.
- **PSC (Primary Scrambling Code):** Scrambling code for the serving/neighbor cell.
- **RSCP (dBm):** Power of the signal code received.
- **ECIO (dB):** Chip energy over total power received.

### 2.3.1.2.3 Example of LTE Connection

**Cells**

**LTE Intrafrequency Information**

```

UE is in idle mode
PLMN ID coded: 21401
Tracking Area Code: 0116
Global cell ID in the system information block 04631501
E-UTRA absolute radio frequency channel number of the serving cell: 1501
LTE serving cell ID: 287
Priority for serving frequency: 6
S non-intra search threshold to control non-intrafrequency searches: 6
Serving cell low threshold: 4
S intra search threshold: 54
Cell #1
  Physical cell ID: 287
  Current RSRQ as measured by L1: -11 (dB)
  Current RSRP as measured by L1: -97 (dBm)
  Current RSSI as measured by L1: -65 (dBm)
  Cell selection Rx Level: 27
Cell #2
  Physical cell ID: 285
  Current RSRQ as measured by L1: -16 (dB)
  Current RSRP as measured by L1: -105 (dBm)
  Current RSSI as measured by L1: -79 (dBm)

```

**LTE Interfrequency Information**

```

UE is in idle mode
Cell #1
E-UTRA absolute radio frequency channel number: 6300
Cell Srxlev low threshold: 0
Cell Srxlev high threshold: 14
Cell reselection priority: 4

```

Fig. 26: Status WWAN-1 – Cells (LTE Connection).

### 2.3.1.3 Module Information

Displays information on the module.

**Module Information**

Manufacturer:	Quectel
Model:	EC25E
Firmware:	EC25EFAR02A08M4G
IMEI:	861107032164981
IMSI:	214019816249846
SIM Card ID	8934569821305399721

Fig. 27: WWAN- Status 1 – Module Information.

- **Manufacturer:** Module manufacturer.
- **Model:** Module model.
- **Firmware:** Module's firmware version.
- **IMEI:** Module's International Mobile Equipment Identity.
- **IMSI:** International Mobile Subscriber Identity for the SIM installed in the router.
- **SIM Card ID:** Integrated Circuit Card ID for the SIM installed in the router.

### 2.3.1.4 IP Protocol

Displays the IP address dynamically assigned by the carrier.

■ IP Protocol	
Assigned IP:	172.17.91.146

Fig. 28: Status WWAN-1 – IP Protocol.

## 2.3.2 DMVPN connections

Allow you to monitor the state of the tunnels established with the central routers.

### DMVPN Connection Status

■ Tunnel 1	
Interface:	gre1
Protocol-Address:	11.7.0.1
NBMA-Address:	11.68.80.5
Status:	DOWN

■ Tunnel 2	
Interface:	gre2
Protocol-Address:	11.5.0.1
NBMA-Address:	11.68.80.1
Status:	DOWN

■ Tunnel 3	
Interface:	gre3
Protocol-Address:	11.17.0.1
NBMA-Address:	11.68.80.117
Status:	DOWN

■ Tunnel 4	
Interface:	gre4
Protocol-Address:	11.15.0.1
NBMA-Address:	11.68.80.113
Status:	DOWN

Fig. 29: Status – DMVPN connections.

The information displayed for each tunnel is as follows:

- **Interface:** GRE interface associated to the tunnel.
- **Protocol-Address:** Remote GRE interface address.
- **NBMA-Address:** Public tunnel address at the remote end.
- **Status:**
  - If the tunnel is not configured, the status is: *Not configured*.
  - If the tunnel is configured but not working, the status is: *DOWN*.
  - If the tunnel is configured and working, the status is: *UP*.

## 2.3.3 DHCP Clients

Provides information on client devices that have received an IP address from the Regesta Smart's DHCP server.

## DHCP Leases

■ **Users**

IP Address	MAC Address	Valid From	Valid Till
12.167.5.163	00:2e:d6:33:33	Mon Jul 08 2019 10:42:47	Mon Jul 08 2019 22:42:47

[Refresh](#)

Fig. 30: Status – DHCP Clients.

The information displayed on DHCP clients is as follows:

- **IP Address:** IP address for the connected client.
- **MAC Address:** Physical address for the connected client.
- **Valid From:** Date on which the IP address was given to the client.
- **Valid Till:** Date on which the IP address given to the client times out.

Click on *Refresh* to update the list.

## 2.3.4 Netstat

Displays the following information in table format:

### 2.3.4.1 Interface Statistics

■ **Interfaces Statistics**

Interface	Unicast Pkts Rcv	Multicast Pkts Rcv	Bytes Received	Packets Transmitted	Bytes Transmitted
ethernet0/0	464	2512	351079	416	210416
ethernet0/1	0	0	0	0	0
prime0/0	57	0	2963	16	128
uart1/0	0	0	0	0	0
uart1/1	0	0	0	0	0
cellular1/0	52	0	1334	24	438
cellular1/1	0	0	0	3	580
cellular1/2	0	0	0	0	0
direct-ip1	0	0	0	3	538
direct-ip2	0	0	0	0	0
gre1	0	0	0	3	108
gre2	0	0	0	3	108
gre3	0	0	0	0	0
gre4	0	0	0	0	0
loopback1	0	0	0	0	0
loopback2	0	0	0	0	0
ethernet0/0.14	0	0	0	0	0

Fig. 31: Status – Netstat – Interface Statistics.



### 2.3.4.2 Active TCP connections in the router

#### List of TCP connections

Local Addr	Local Port	Remote Addr	Remote Port	State
0.0.0.0	23	0.0.0.0	0	LISTEN
0.0.0.0	4059	0.0.0.0	0	LISTEN
0.0.0.0	21400	0.0.0.0	0	LISTEN
0.0.0.0	21	0.0.0.0	0	LISTEN
0.0.0.0	80	0.0.0.0	0	LISTEN
192.168.1.1	23	192.168.1.5	59262	ESTAB
0.0.0.0	22	0.0.0.0	0	LISTEN
0.0.0.0	24300	0.0.0.0	0	LISTEN
192.168.1.1	80	192.168.1.5	42569	ESTAB
192.168.1.1	80	192.168.1.5	42570	ESTAB
192.168.1.1	80	192.168.1.5	42571	ESTAB
192.168.1.1	80	192.168.1.5	42572	ESTAB
192.168.1.1	80	192.168.1.5	42573	ESTAB
192.168.1.1	80	192.168.1.5	42574	ESTAB
0.0.0.0	53	0.0.0.0	0	LISTEN

Fig. 32: Status – Netstat – List of TCP connections.

### 2.3.4.3 Interface IP addresses

#### Interface IP Addresses

Interface	IP Address
ethernet0/0	192.168.1.1/24
direct-ip1	dhcp-negotiated - 172.17.4.17/32
direct-ip2	dhcp-negotiated - 0.0.0.0/0
gre1	11.7.6.52/21
gre2	11.5.6.52/21
gre3	11.17.6.52/21
gre4	11.15.6.52/21
loopback1	11.69.80.134/32
ethernet0/0.14	12.167.5.1/24
Special IP Address	
internal-address	0.0.0.0
management-address	11.69.80.134
router-id	0.0.0.0
global-address	11.69.80.134

Fig. 33: Status – Netstat – Interface IP Addresses.

### 2.3.4.4 Active IP routing table

#### Routing Table

Type	Dest net/Mask	Cost	Age	Next hop(s)
stat(2)[0]	0.0.0.0/0	[ 60/1 ]	0	direct-ip1
sbnt(0)[0]	11.0.0.0/8	[240/1 ]	0	none
stat(1)[0]	11.68.80.1/32	[ 60/1 ]	0	direct-ip1
stat(1)[0]	11.68.80.5/32	[ 60/1 ]	0	direct-ip1
dir(0)[2]	11.69.80.134/32	[ 0/1 ]	0	loopback1
sbnt(0)[0]	12.0.0.0/8	[240/1 ]	0	none
dir(0)[1]	12.167.5.0/24	[ 0/1 ]	0	ethernet0/0.14
sbnt(0)[0]	172.17.0.0/16	[240/1 ]	0	none
dir(0)[1]	172.17.4.17/32	[ 0/1 ]	0	direct-ip1
dir(0)[1]	192.168.1.0/24	[ 0/1 ]	0	ethernet0/0

Fig. 34: Status – Netstat – Routing Table.

## 2.3.5 Diagnostics

Executes the *ping* operation to determine whether the device accesses a given IP address. Additionally, you can execute a *traceroute* operation from the device and check the hops needed to reach a certain *router/host*.

## Diagnostics

### Network Utilities

```

PING : 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0. time=667. ms
64 bytes from 8.8.8.8: icmp_seq=1. time=488. ms
64 bytes from 8.8.8.8: icmp_seq=2. time=567. ms
64 bytes from 8.8.8.8: icmp_seq=3. time=527. ms
64 bytes from 8.8.8.8: icmp_seq=4. time=284. ms

---- PING Statistics----
5 packets transmitted, 5 packets received,
0 time out surpassed packets, 0% packet loss
round-trip (ms)  min/avg/max = 284/506/667
GTP_TELDAT IP+
```

```

Press any key to abort.

Tracing the route to 8.8.8.8 [],
Protocol: UDP, 4 hops max, 56 byte packets

 1    0 ms!N    0 ms!N    0 ms!N    11.69.80.134
GTP_TELDAT IP+
```

Fig. 35: Status – Diagnostics – Ping – Traceroute.

## 2.3.6 PRIME

This option on the *Status* menu is only available if we are using the Regesta Smart PLC model.

### PRIME Status

#### Global PRIME Information

PLC Firmware Version: 01.04.03.01-B-M  
 Interface State: UP(4)  
 PRIME Mng State: UP(16)

#### TCP Connections Information

TCP Listen Port: 502  
 Opened Sessions: 0  
 Max Simultaneous Sessions: 0  
 Packets Sent: 0  
 Packets Received: 0

#### Topology Information

BASE NODE									
State	MAC	CHANNEL	LNID	DISC	UP-TIME	CNX-TIME			
Running	02:A0:26:11:11:13	1	0x0000	0	0:00:10	0:00:10			
SERVICE NODES									
Total listed SN: 1									
<ul style="list-style-type: none"> <li>• Terminals: 1</li> <li>• Switches: 0</li> <li>• Disconnec.: 0</li> </ul>									
Level	State	MAC	LNID	SID	LSID	DISC	UP-TIME	%	CNX-TIME
0	terminal	00:15:02:11:11:20	0x0bb9	0x00	0xff	0	0:00:06	60.0	0:00:06

Fig. 36: Status – Prime.

This page allows you to monitor the information on the PRIME interface and system topology. Said information appears structured as follows:

- *Global PRIME information:*

Shows information on the state of the PLC interface and the firmware version running over the PLC module.

#### ■ Global PRIME Information

PLC Firmware Version:	01.04.03.01-B-M
Interface State:	UP(4)
PRIME Mng State:	UP(16)

Fig. 37: Status - Global PRIME Information.

- *TCP connection information:*

Shows information on the TCP connection:

- Port number used.
- Number of open sessions.
- Maximum number of concurrent sessions.
- Packets sent and received.

#### ■ TCP Connections Information

TCP Listen Port:	502
Opened Sessions:	0
Max Simultaneous Sessions:	0
Packets Sent:	0
Packets Received:	0

Fig. 38: Status – Information on TCP Connections.

- *Topology Information:*

This table provides information on the nodes, thus defining the system's topology. There are 2 types of nodes:

- *Base Node:* This is the local node (the router).
- *Service Node:* Remaining nodes (switches and terminals) that make up the system.

### ■ Topology Information

BASE NODE									
State	MAC	CHANNEL	LNID	DISC	UP-TIME	CNX-TIME			
Running	02:A0:26:11:11:13	1	0x0000	0	0:00:10	0:00:10			
SERVICE NODES									
Total listed SN: 1									
<ul style="list-style-type: none"> <li>• Terminals: 1</li> <li>• Switches: 0</li> <li>• Disconnec.: 0</li> </ul>									
Level	State	MAC	LNID	SID	LSID	DISC	UP-TIME	%	CNX-TIME
0	terminal	00:15:02:11:11:20	0x0bb9	0x00	0xff	0	0:00:06	60.0	0:00:06

Fig. 39: Status – Topology Information.

The meaning of some of the columns found above is as follows:

**LNID:** Node identifier belonging to the PRIME network.

**SID:** Located on the Service Nodes list, this identifies the switch the Service Node is connected to. If there is no switch (Service Node is directly connected to the Base Node), the parameter value is 0x00.

**LSID:** Part of the Service Nodes list, it identifies the nodes with a switch role.

**DISC:** Shows the number of disconnections detected.

**UP-TIME:** Total time the node remains connected.

**%:** UP-TIME percentage with respect to the Base Node UP-TIME.

**CNX-TIME:** Period during which the node remains connected in the current session.

## 2.3.7 SCADA

This option on the *Status* menu is only available if we are using the Regesta Smart and we have SCADA interfaces.

## SCADA Status

Network:

**Global information on TCP sessions that affect the interface**

Opened sessions:	1
Current sessions:	1
Disconnects received:	0
Disconnects transmitted:	0

**Traffic in the serial interface**

Bytes sent to the interface:	0
Bytes received from the interface:	0
Packets sent to the interface:	0
Packets received from the interface:	0

**TCP traffic generated by the interface**

Bytes sent over TCP packets:	0
Bytes received over TCP packets:	0
TCP packets sent:	0
TCP packets received:	0

**Information on established TCP sessions wich affect the interface**

State	Remote IP address	Remote port	Establish Time	Origin
ESTAB	192.168.213.157	47593	08:31:55 02/04/20	remote

Fig. 40: Status – Scada

This page allows you to monitor the information on the SCADA interface which has been selected in the selector "Network". Said information appears structured as follows:

- *Global information on TCP sessions that affect the interface:*

Shows information on the state of TCP sessions that affect the interface:

- Opened sessions.
- Current sessions.
- Disconnects received.
- Disconnects transmitted..

**Global information on TCP sessions that affect the interface**

Opened sessions:	1
Current sessions:	1
Disconnects received:	0
Disconnects transmitted:	0

Fig. 41: Status - Global Scada TCP sessions Information.

- *Traffic in the serial interface:*

Shows information about traffic in the serial interface:

- Bytes sent to the interface.
- Bytes received from the interface.
- Packets sent to the interface.

- Packets received from the interface.

#### ■ Traffic in the serial interface

Bytes sent to the interface:	0
Bytes received from the interface:	0
Packets sent to the interface:	0
Packets received from the interface:	0

Fig. 42: Status – Information about Traffic in serial interface.

- *Topology Information:*

This table provides information about TCP traffic generated by the interface:

- Bytes sent over TCP packets.
- Bytes received TCP packets.
- TCP packets sent.
- TCP packets received.

#### ■ TCP traffic generated by the interface

Bytes sent over TCP packets:	0
Bytes received over TCP packets:	0
TCP packets sent:	0
TCP packets received:	0

Fig. 43: Status – TCP traffic generated by the interface.

- *Information on established TCP sessions which affect the interface*

This table provides information on established TCP sessions that affect the interface.

#### ■ Information on established TCP sessions wich affect the interface

State	Remote IP address	Remote port	Establish Time	Origin
ESTAB	192.168.213.157	47593	08:31:55 02/04/20	remote

Fig. 44: Status – Information on established TCP sessions that affect the interface.

The meaning of some of the columns found above is as follows:

*State:* The state of established TCP sessions.

*Remote IP address:* Remote IP address used in the session.

*Remote port:* Remote port used in the session.

*Establish time:* Session established time.

*Origin:* Origin of the session.

## 2.4 Logs Menu

Shows the status evolution for the device's 2G/3G/LTE module. This menu remains hidden in devices that do not have WWAN technology.

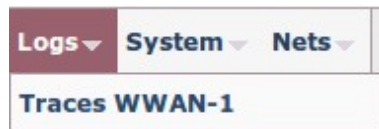


Fig. 45: Logs Menu.

### 2.4.1 WWAN-1 Traces

Displays the information linked to the router's 2G/3G/LTE module.

**Traces WWAN-1**

■ **WWAN-1**

Module Manufacturer:	Quectel
Module Model:	EC25E
Module Firmware:	EC25EFAR02A08M4G

■ **Modem diagnostics**

```

AT+COPS=3,2,+COPS?;+CGREG?;+QTEMP;+CBC
+COPS: 0,2,"21401",0
+CGREG: 2,1,"430E","333A",0
+QTEMP: 38,0,34
+CBC: 0,61,3799

OK
AT+COPS=3,2,+COPS?;+CGREG?;+QTEMP;+CBC
+COPS: 0,2,"21401",0
+CGREG: 2,1,"430E","333A",0
+QTEMP: 38,0,34
+CBC: 0,61,3800

OK
AT+COPS=3,2,+COPS?;+CGREG?;+QTEMP;+CBC
          
```

Modem status

Fig. 46: Logs – WWAN-1 Traces.

This is divided into two sections:

#### 2.4.1.1 WWAN-1

Displays information on the module's type, version and firmware:

■ **WWAN-1**

Module Manufacturer:	Quectel
Module Model:	EC25E
Module Firmware:	EC25EFAR02A08M4G

Fig. 47: WWAN-1 Traces – WWAN-1.

- **Module Manufacturer:** Module manufacturer.
- **Module Model:** Module model.
- **Module Firmware:** Module's firmware version.

### 2.4.1.2 Modem diagnostics

Allows you to monitor the commands sent to the 2G/3G/LTE module and the results by clicking on the "Modem status" button.

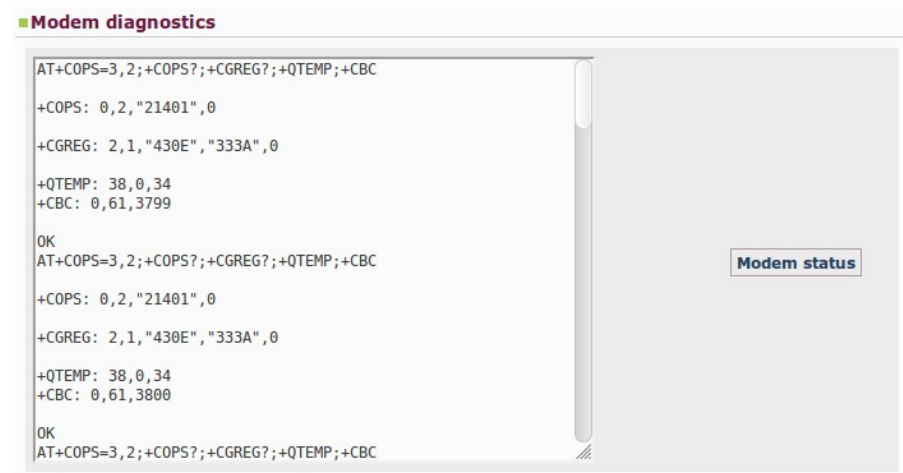


Fig. 48: WWAN-1 Traces – Modem diagnostics.

## 2.5 System Menu

Lets you configure the router's general parameters.



Fig. 49: System Menu.

### 2.5.1 Password

Allows the user to modify the device access password (provided the user has been created in local mode and the AAA feature is disabled in the configuration). To save the changes, you need to enter the password twice and click on the *Apply* button.



Fig. 50: System – Password.

When the logged-in user operates under the "configuration" access level, the previous page will show up differently because said user does not have enough privileges to modify the password.



## System Local Password

### Change Current User Password

Not administrative permission

Fig. 51: System – Password.

## 2.5.2 Settings

Here, you can configure various general system parameters.

### System Settings

#### System Settings

Host Name:  (1-79 characters)

#### Time Settings

NTP Server:  Timezone:

Summer Time:

#### Web Settings

HTTP Port:  (1-65534)

Fig. 52: System – Settings.

### 2.5.2.1 System Settings

System parameters.

- **Host Name:** Router's name.

### 2.5.2.2 Time Settings

Date and time parameter.

- **NTP Server:** NTP server's IP address to synchronize the router's date and time.
- **Timezone:** Hour zone the router is in.
- **Summer Time:** Activate or deactivate summer time.

### 2.5.2.3 Web Settings

Web configuration parameter.

- **HTTP Port:** Web configuration port.

To save the changes made in the configuration, click on *Apply*. To delete the changes specified and recover the data the router had, click on the *Cancel* button.

## 2.5.3 SNMP

Shows the SNMP protocol configuration environment for the sending and receiving of SNMPv1 traps.

## Host Trap Manager Settings

**■ Hosts**

Hosts:

---

**■ Host Configuration**

IP Address:   
 UDP Port:   
 Send Standard Traps:       Send Enterprise Traps:

---

**■ Community Subnet**

Subnets:   
 Subnet IP:       Subnet Mask:

---

**■ Host List**

IP Address	Port	Standard Traps	Enterprise Traps
12.165.2.20	162	Yes	Yes
12.165.2.25	75	No	Yes

---

**■ Subnets List**

Subnet	Mask
12.165.2.0	255.255.255.0

Fig. 53: System – SNMP.

This is divided into the following sections:

### 2.5.3.1 Hosts

Allows you to configure all the *hosts* to which the SNMPv1 traps generated by the device must be sent.

#### 2.5.3.1.1 Adding and configuring a host

To add a new host, carry out the following steps:

- (1) Select the “*New Host*” option from the pull-down menu.
- (2) Specify the following configuration parameters:
  - **IP Address:** IP address of the host where the SNMPv1 traps generated by the device are sent to.
  - **UDP Port:** UDP port where the *host* expects the traps to arrive. Default is 162.
  - **Send Standard Traps:** Enables/disables generic trap sending.
  - **Send Enterprise Traps:** Enables/disables the sending of specific company traps containing Teldat events.
- (3) Click on the *Apply* button.

To cancel the modifications executed, click on *Cancel*.

**■ Hosts**

Hosts:

---

**■ Host Configuration**

IP Address:       UDP Port:   
 Send Standard Traps:       Send Enterprise Traps:

Fig. 54: SNMP – Hosts – Adding and configuring a host.

### 2.5.3.1.2 Editing a host configuration

To execute this, select the host from the pull-down menu and (once you have made any required changes) click on the *Apply* button. This section allows you to modify all data, except for the host IP address.

To cancel the changes you have made and return to the information the device had on said *host*, simply click on the *Cancel* button.

The screenshot shows the 'Hosts' section with a dropdown menu set to '12.165.2.20' and a 'Remove' button. Below it is the 'Host Configuration' section with the following fields:

IP Address:	12.165.2.20	UDP Port:	162
Send Standard Traps:	Yes	Send Enterprise Traps:	Yes

At the bottom right of the 'Host Configuration' section are 'Apply' and 'Cancel' buttons.

Fig. 55: SNMP – Hosts – Editing a host configuration.

### 2.5.3.1.3 Removing a host

To remove a host, first select it from the pull-down menu and then click on *Remove*.

The screenshot shows the 'Hosts' section with a dropdown menu set to '12.165.2.20' and a 'Remove' button.

Fig. 56: SNMP – Hosts – Removing a host.

## 2.5.3.2 Community Subnet

Allows you to define the subnets where SNMP petitions can be executed.

### 2.5.3.2.1 Adding and configuring a subnet

To add a new subnet, select the “*New Subnet*” option from the pull-down menu, indicate its IP address and its subnet mask and click on the *Add* button.

The screenshot shows the 'Community Subnet' section with the following fields:

Subnets:	-- New Subnet --		
Subnet IP:	12.165.2.144	Subnet Mask:	255.255.255.254

An 'Add' button is located at the bottom right of the 'Community Subnet' section.

Fig. 57: SNMP – Community Subnet – Adding a subnet.

### 2.5.3.2.2 Removing a subnet

To remove a subnet, first select it from the pull-down menu and then click on the *Remove* button.

The screenshot shows the 'Community Subnet' section with the following fields:

Subnets:	12.165.2.144	Remove	
Subnet IP:	12.165.2.144	Subnet Mask:	255.255.255.254

An 'Add' button is located at the bottom right of the 'Community Subnet' section.

Fig. 58: SNMP – Community Subnet – Removing a subnet.

### 2.5.3.3 Host List

A list at the end of the page shows the *hosts* that have already been configured. The goal is for the user to view the hosts the device sends traps to more easily.

■ Host List			
IP Address	Port	Standard Traps	Enterprise Traps
12.165.2.20	162	Yes	Yes
12.165.2.25	75	No	Yes

Fig. 59: SNMP – Host List.

### 2.5.3.4 Subnets List

For that same reason, configured subnets from where SNMP petitions can be executed are shown in table format.

■ Subnets List	
Subnet	Mask
12.165.2.144	255.255.255.254

Fig. 60: SNMP – Subnets List.

## 2.6 Nets Menu

Lets you configure the router's network parameters. It is a variable menu whose options depend on the Regesta Smart model being configured and its license.

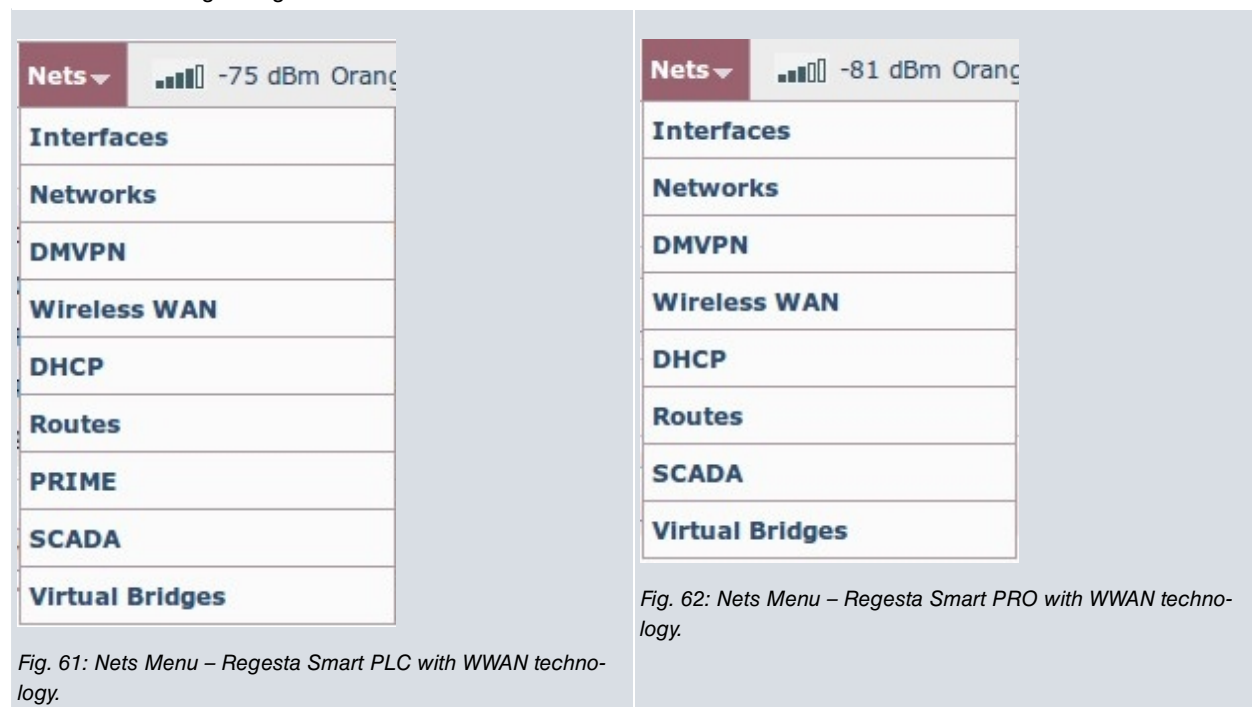


Fig. 61: Nets Menu – Regesta Smart PLC with WWAN technology.

Fig. 62: Nets Menu – Regesta Smart PRO with WWAN technology.



Fig. 63: Nets Menu – Regesta Smart LITE with WWAN technology.

## 2.6.1 Interfaces

Allows the user to create and remove interfaces and subinterfaces. VLAN configuration is only available for Regesta Smart models that have a switch and the corresponding license.

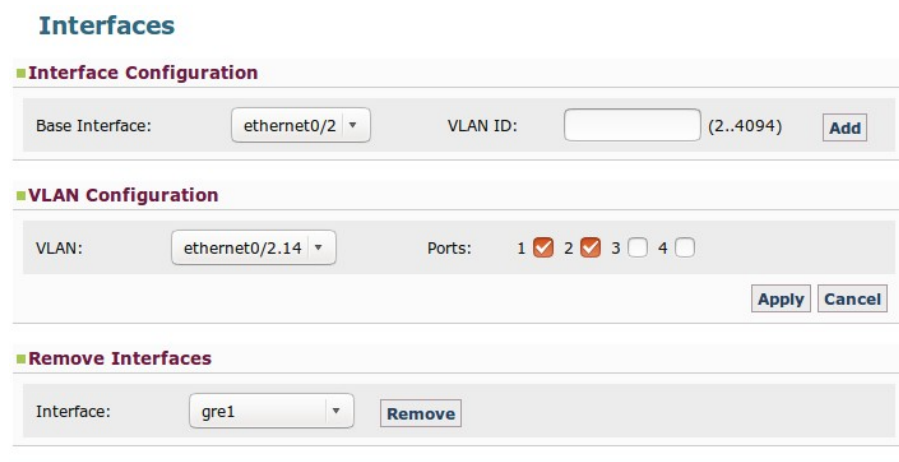


Fig. 64: Nets – Interfaces. Regesta Smart PRO with switch and license.



Fig. 65: Nets – Interfaces. Regesta Smart PRO with switch but without license.

## Interfaces

### ■ Interface Configuration

Base Interface:  GRE Id:

### ■ Remove Interfaces

Interface:

Fig. 66: Nets – Interfaces. Regesta Smart LITE.

## Interfaces

### ■ Interface Configuration

Base Interface:  GRE Id:

### ■ Remove Interfaces

Interface:

Fig. 67: Nets – Interfaces. Regesta Smart PLC.

The page is divided into the following sections:

### 2.6.1.1 Interface Configuration

Through the *Add* button, you can add Ethernet subinterfaces, GRE interfaces and BVI interfaces by selecting the base interface from the pull-down menu and specifying an identifier.

### ■ Interface Configuration

Base Interface:  VLAN ID:  (2..4094)

Fig. 68: Interfaces – Interface Configuration – Ethernet Subinterfaces.

### ■ Interface Configuration

Base Interface:  GRE Id:

Fig. 69: Interfaces – Interface Configuration – GRE interfaces.

### ■ Interface Configuration

Base Interface:  BVI Id:

Fig. 70: Interfaces – Interface Configuration – BVI interfaces.

### 2.6.1.2 VLAN configuration

Allows you to configure VLANs in the device, indicating the interface and ports involved. This option remains hidden in devices that do not have a switch or have a switch but no corresponding license.

#### 2.6.1.2.1 Adding and configuring a VLAN

To do this, select the interface from the pull-down menu, check the ports you wish to associate to the *VLAN* and click on the *Apply* button. To cancel any modifications made, click on the *Cancel* button.

**VLAN Configuration**

VLAN: ethernet0/2.14 ▾ Ports: 1  2  3  4

Apply Cancel

Fig. 71: Interfaces – VLAN configuration – Adding and configuring a VLAN.

### 2.6.1.2.2 Editing a VLAN configuration

Select the interface from the pull-down menu and, once you have made the appropriate changes by checking/unchecking the ports, click on *Apply*.

If you wish to cancel the changes you have made and return to the information the device had on said *VLAN*, simply click on the *Cancel* button.

**VLAN Configuration**

VLAN: ethernet0/2.14 ▾ Ports: 1  2  3  4

Apply Cancel

Fig. 72: Interfaces – VLAN configuration – Editing the configuration for a VLAN.

### 2.6.1.3 Remove Interfaces

Allows you to remove any of the interfaces and subinterfaces created by selecting them from the pull-down menu and clicking on the *Remove* button.

**Remove Interfaces**

Interface: gre1 ▾ Remove

Fig. 73: Interfaces – Remove Interfaces.

## 2.6.2 Networks

Here you can define the IP addresses for each interface and subinterface created on the previous page, as well as for the *loopback* interface. Additionally, you can enable or disable routing traffic (IP) control between local subnets.

## Network Configuration

### ■ Network Settings

Network:	<input type="text" value="ethernet0/0.14"/>	<input type="button" value="Secondary IP Addresses"/>
IP Address:	<input type="text" value="12.167.5.1"/>	
Netmask:	<input type="text" value="255.255.255.0"/>	

### ■ Traffic Control Settings

Enable Routing Traffic Control

### ■ Loopback Settings

IP Address:	<input type="text" value="11.69.80.134"/>	
Netmask:	<input type="text" value="255.255.255.255"/>	

Fig. 74: Nets – Networks.

This page is divided into the following sections:

### 2.6.2.1 Network Settings

Allows you to assign/modify IP addresses for Ethernet interfaces/subinterfaces, GRE interfaces and BVI interfaces (defining up to six secondary IP addresses for each). To view, add, modify or remove these latter addresses, click on the “*Secondary IP Addresses*” button. Once you have configured an interface, click on the *Apply* button to save any changes made.

The *Cancel* button allows you to cancel the changes being specified for an interface. When clicked, the information the device had stored on this interface is shown once more.



**Network Settings**

Network: ethernet0/0.14

IP Address: 12.167.5.1

Netmask: 255.255.255.0

Secondary IP Addresses

**Secondary IP Addresses**

Secondary IP Address	IP Address	Netmask
<input checked="" type="checkbox"/> Secondary IP Address 1:	12.168.20.2	255.255.255.0
<input type="checkbox"/> Secondary IP Address 2:		
<input type="checkbox"/> Secondary IP Address 3:		
<input type="checkbox"/> Secondary IP Address 4:		
<input type="checkbox"/> Secondary IP Address 5:		
<input type="checkbox"/> Secondary IP Address 6:		

Hide

Apply Cancel

Fig. 75: Networks – Networks Settings.

The *Hide* button lets you hide the “*Secondary IP Addresses*” option, but never to disable them.

Also, and if applicable, this section allows you to remove from the configuration the IP address that the device has configured by default in the ethernet0/0 interface. To do this, select this interface from the pull-down menu and click on “*Delete IP Address*”.

**Network Settings**

Network: ethernet0/0

IP Address: 192.168.1.1

Netmask: 255.255.255.0

Delete IP Address

Secondary IP Addresses

Apply Cancel

Fig. 76: Networks – Networks Settings – Removing the default IP address.

### 2.6.2.2 Traffic Control Settings

Allows you to enable or disable routing traffic (IP) control between local subnets, filtering the flow of packets between local interfaces.

**Traffic Control Settings**

Enable Routing Traffic Control

Apply

Fig. 77: Networks – Traffic Control Settings.

### 2.6.2.3 Loopback Settings

There is a special network that isn't associated to any interface. This network is usually used for administrative tasks and is known as *loopback*. In this section, you can define its IP address and network mask.

### ■ Loopback Settings

IP Address:	<input type="text" value="11.69.80.134"/>
Netmask:	<input type="text" value="255.255.255.255"/>

Fig. 78: Networks – Loopback Settings.

## 2.6.3 DMVPN

A DMVPN network is made up of a next-hop server known as a HUB. This has a public IP address, destination for the tunnels that remote devices establish (Regesta Smart) and a private destination IP address for the GRE tunnels necessary to transport the routing protocol.

Each HUB operates in a terminator. The latter can have several available HUBs, operating over different subinterfaces.

On this page, you can configure the GRE tunnel global parameters and the data necessary to configure each HUB that intervenes in the network.

### Dynamic Multipoint Virtual Private Network Configuration

#### ■ Global Tunnel Settings

Recovery Time:	<input type="text" value="300"/>	(0..86400 seconds)
Keepalive Period Reachable:	<input type="text" value="10"/>	(1..36000 seconds)
Keepalive Period Unreachable:	<input type="text" value="20"/>	(2..36000 seconds)
Keepalive Stability Threshold:	<input type="text" value="3"/>	(1..255)
<input checked="" type="checkbox"/> IPsec Mode:	<input type="text" value="Main"/>	
IPsec Preshared-Key:	<input type="text" value="...."/>	(1..32 characters)

#### ■ Hub Settings

Tunnel Interface:	<input type="text" value="gre1"/>
Remote IP Address:	<input type="text" value="11.7.0.1"/>
NHS IP Address:	<input type="text" value="11.68.80.5"/>
Base Interface:	<input type="text" value="direct-ip1"/>
Key:	<input type="text" value="22"/> (0..4294967295)

Fig. 79: Nets – DMVPN.

### 2.6.3.1 Global Tunnel Settings

Configures the general parameters applicable to the GRE tunnel that the Regesta Smart assigns to each configured HUB.

**Global Tunnel Settings**

Recovery Time:  (0..86400 seconds)

Keepalive Period Reachable:  (1..36000 seconds)

Keepalive Period Unreachable:  (2..36000 seconds)

Keepalive Stability Threshold:  (1..255)

IPsec Mode:

IPsec Preshared-Key:  (1..32 characters)

Fig. 80: DMVPN – Global Tunnel Settings.

- **Recovery Time:** Time, in seconds, it takes for traffic to be routed through a lower priority GRE tunnel before reaching a higher priority tunnel, provided the latter is operative. This way, the device can always make use of the carrier with the highest communication quality.
- **Keepalive Parameters:** The *Keepalive* mechanism is used to monitor connectivity with the remote end of the tunnel by sending maintenance packets and checking that a response is received.
  - **Keepalive Period Reachable:** Time, in seconds, between the sending of successive *keepalive* petition packets when responses are received.
  - **Keepalive Period Unreachable:** Time, in seconds, between the sending of successive *keepalive* petition packets when responses stop arriving.
  - **Keepalive Stability Threshold:** Number of consecutive *keepalive* petition packets without response in order to determine lost connectivity with the remote tunnel end.
- **IPsec Mode:** This is the initial IKE protocol phase that authenticates the ends and can be one of two types: *Main* and *Aggressive*. The *Aggressive* mode allows the Regesta Smart devices to be identified by a *pre-shared key* and by a device identifier. This way, pools of devices authenticated through a given *pre-shared key* can be created.

When you select *Aggressive* mode, a box is automatically generated to enter the Key ID identifying the device (Figure 76).

On activating the check-button, you also activate GRE tunnel encryption using IPsec.

IPsec Mode:

IPsec Preshared-Key:  (1..32 characters)

Fig. 81: DMVPN – Global Tunnel Settings – IPsec Mode: Main.

IPsec Mode:

Key ID:  (1..64 characters)

IPsec Preshared-Key:  (1..32 characters)

Fig. 82: DMVPN – Global Tunnel Settings – IPsec Mode: Aggressive.

To store the configuration established for GRE tunnels, click on *Apply*. To cancel the changes made and recover the information that the device had, click on the *Cancel* button.

### 2.6.3.2 Hub Settings

Configures the parameters that define each of the Hubs.

**Hub Settings**

Tunnel Interface:

Remote IP Address:

NHS IP Address:

Base Interface:

Key:  (0..4294967295)

Fig. 83: DMVPN – Hub Settings.

- **Tunnel Interface:** Configured through a pull-down menu, it allows you to configure the local GRE interface operating over the tunnel.
- **Remote IP Address:** Address of the terminator router's GRE interface used by the device to establish the GRE tunnel.
- **NHS IP Address:** HUB address used by the device to establish the tunnel. This address corresponds to the NHS (*Next Hop Server*).
- **Base Interface:** Base interface over which the GRE tunnel is transported. This is a pull-down menu that admits different options depending on the device model, its license and the scenario to configure. In cases where you have WWAN technology, the PPP1/DIRECT-IP1 option corresponds to the protocol established with the carrier assigned to the SIM1, while the PPP2/DIRECT-IP2 option corresponds to the protocol established with the carrier assigned to the SIM2 (whenever there are two SIM cards).
- **Key:** Key used in GRE tunnels to distinguish the tunnel to which a mGRE interface belongs to when there is more than one mGRE interface in a tunnel terminator router. This is not a security key.

To store the configuration set for the HUB, click on *Apply*. To cancel the changes made and recover the information the device had on this HUB, click on the *Cancel* button.



#### Note

Tunnel priority is defined by the GRE interface to which it is associated. As a result, the tunnel associated to the GRE1 interface has greater priority when routing traffic. The tunnel associated to the GRE4 interface has the lowest priority.

## 2.6.4 Wireless WAN Configuration

You may only access this *Nets* menu option when using a model that incorporates WWAN technology. It remains hidden in all other models.

Here, you configure the router's 2G/3G/LTE cellular module interface and define the network's connection parameters.

## Wireless WAN Configuration

### Primary SIM Settings

Phone Number:	<input type="text"/>
PIN Code:	<input type="text" value="****"/>
APN:	<input type="text" value="ac.vodafone.es"/>
APN username:	<input type="text"/>
APN password:	<input type="text"/>
Network mode:	<input type="text" value="UMTS/HSDPA"/>

### Secondary SIM Settings

Phone Number:	<input type="text"/>
PIN Code:	<input type="text" value="****"/>
APN:	<input type="text" value="movistar.es"/>
APN username:	<input type="text"/>
APN password:	<input type="text"/>
Network mode:	<input type="text" value="UMTS/HSDPA"/>

### SIM Changeover Settings

Configure double SIM management

Mode to select the main SIM:

Main Primary SIM

Main Secondary SIM

Sequential Order

Random Order

#### Supervision parameters:

RSCP Threshold:	<input type="text" value="-45"/>	(-113..0) dBm
ECNO Threshold:	<input type="text" value="-3"/>	(-50..5) dB
Threshold Interval:	<input type="text" value="2"/>	(0..180) minutes
Recovery Interval:	<input type="text" value="2"/>	(0..65535) minutes
Registration Criteria Interval:	<input type="text" value="3"/>	(0..180) minutes

Fig. 84: Nets – Wireless WAN (Regesta Smart PLC with one 2G/3G/LTE module).

### 2.6.4.1 Primary SIM Settings

In this section, you can configure the connection parameters associated to the SIM1 card. These parameters are as follows:

- **Phone Number:** Telephone number associated to the SIM card.
- **PIN Code:** The SIM card's PIN code.
- **APN:** Access point name used with the SIM card.
- **APN username:** User name used to access the APN with the SIM card (if there is authentication).

- **APN password:** Password used to access the APN with the SIM card (if there is authentication).
- **Network mode:** Radio network technology the internal module has to use when selecting this SIM.

**Primary SIM Settings**

Phone Number:	<input type="text"/>
PIN Code:	<input type="text" value="****"/>
APN:	<input type="text" value="ac.vodafone.es"/>
APN username:	<input type="text"/>
APN password:	<input type="text"/>
Network mode:	<input type="text" value="UMTS/HSDPA"/>

Fig. 85: Wireless WAN – Primary SIM Settings.

When registering a mobile device, some LTE network operators ask for the equipment to have a certain APN configured with its authentication parameters. If this APN is not configured correctly, registering may not take place or do so incorrectly (preventing data contexts from establishing). Therefore, when selecting the LTE option (or the automatic mode in a module that supports this technology), the following data must be configured:

Network mode:

**LTE configuration**

*The use of this option depends on the network, each carrier decides if this option is necessary or not.*

Registration APN

APN:	<input type="text"/>
Protocol Data Packet type:	<input type="text" value="IP"/>
Authentication type:	<input type="text" value="None"/>
Username:	<input type="text"/>
Password:	<input type="text"/>

Fig. 86: Wireless WAN – Primary SIM Settings - LTE.

### 2.6.4.2 Secondary SIM Settings

In this section, you configure the connection parameters associated to the SIM2 card, which are the same as those for SIM1.

**Secondary SIM Settings**

Phone Number:	<input type="text"/>
PIN Code:	<input type="text" value="****"/>
APN:	<input type="text" value="movistar.es"/>
APN username:	<input type="text"/>
APN password:	<input type="text"/>
Network mode:	<input type="text" value="UMTS/HSDPA"/>

Fig. 87: Wireless WAN – Secondary SIM Settings.

### 2.6.4.3 SIM Changeover Settings

Defines the parameters that set the conditions for a changeover to the backup carrier and the return to the main carrier.

The configurable parameters for carrier changeover vary depending on whether the device runs in automatic mode or has a 2G, 3G or LTE connection.

**SIM Changeover Settings**

Configure double SIM management

**Mode to select the main SIM:**

Main Primary SIM

Main Secondary SIM

Sequential Order

Random Order

**Supervision parameters:**

RSSI Threshold:  (-113..0) dBm

Threshold Interval:  (0..180) minutes

Recovery Interval:  (0..65535) minutes

Registration Criteria Interval:  (0..180) minutes

Fig. 88: Wireless WAN –SIM Changeover Settings with a 2G connection.

**SIM Changeover Settings**

Configure double SIM management

**Mode to select the main SIM:**

Main Primary SIM

Main Secondary SIM

Sequential Order

Random Order

**Supervision parameters:**

RSCP Threshold:  (-113..0) dBm

ECNO Threshold:  (-50..5) dB

Threshold Interval:  (0..180) minutes

Recovery Interval:  (0..65535) minutes

Registration Criteria Interval:  (0..180) minutes

Fig. 89: Wireless WAN –SIM Changeover Settings with a 3G connection.

### SIM Changeover Settings

Configure double SIM management

Mode to select the main SIM:

- Main Primary SIM  
 Main Secondary SIM  
 Sequential Order  
 Random Order

Supervision parameters:

3G	RSCP Threshold:	<input type="text" value="-45"/>	(-113..0) dBm
	ECNO Threshold:	<input type="text" value="-3"/>	(-50..5) dB
	Threshold Interval:	<input type="text" value="2"/>	(0..180) minutes
2G	RSSI Threshold:	<input type="text" value="-45"/>	(-113..0) dBm
	Threshold Interval:	<input type="text" value="2"/>	(0..180) minutes
Recovery Interval:		<input type="text" value="2"/>	(0..65535) minutes
Registration Criteria Interval:		<input type="text" value="3"/>	(0..180) minutes

Fig. 90: Wireless WAN –SIM Changeover Settings when one SIM is configured with a 2G connection and the other with a 3G connection.

### SIM Changeover Settings

Configure double SIM management

Mode to select the main SIM:

- Main Primary SIM  
 Main Secondary SIM  
 Sequential Order  
 Random Order

Supervision parameters:

LTE	RSRP Threshold:	<input type="text" value="-70"/>	(-140..0) dBm
	RSRQ Threshold:	<input type="text" value="-10"/>	(-20..0) dB
	Threshold Interval:	<input type="text" value="2"/>	(0..180) minutes
3G	RSCP Threshold:	<input type="text" value="-45"/>	(-113..0) dBm
	ECNO Threshold:	<input type="text" value="-3"/>	(-50..5) dB
	Threshold Interval:	<input type="text" value="2"/>	(0..180) minutes
Recovery Interval:		<input type="text" value="2"/>	(0..65535) minutes
Registration Criteria Interval:		<input type="text" value="3"/>	(0..180) minutes

Fig. 91: Wireless WAN –SIM Changeover Settings when one SIM is configured with an LTE connection and the other with a 3G connection.

#### 2.6.4.3.1 Mode to select the main SIM

This section indicates which of the two mobile telephone carriers defined acts as main and which as backup. There are four options for this:



	<i>Main Carrier</i>	<i>Backup Carrier</i>
<i>Main Primary SIM</i>	SIM 1	SIM 2
<i>Main Secondary SIM</i>	SIM 2	SIM 1
<i>Sequential Order</i>	The main carrier is sequentially selected on device start up. At this point, the carrier that was last used is marked as the backup carrier.	
<i>Random Order</i>	The main carrier is randomly selected on device start up.	

### 2.6.4.3.2 Supervision Parameters

This section configures the different criteria to be checked before switching carriers.

*Switch parameters independent of the technology used*

- **Recovery Interval:** Specifies the maximum time, in minutes, that the backup SIM is used. After said time, changeover to main SIM takes place.
- **Registration Criteria Interval:** Specifies the maximum time, in minutes, that the interface can remain unregistered. When this interval times out, carrier changeover takes place.

*Switch parameters with a 2G connection*

- **RSSI Threshold:** When the Received Signal Strength Indicator (RSSI) drops below this threshold (value in dBm), the backup interval initiates.
- **Threshold Interval:** Backup interval. Specifies the number of minutes the RSSI spends below the threshold before changeover to the other carrier takes place.

*Switch parameters with a 3G connection*

- **RSCP Threshold, ECNO Threshold and Threshold Interval:** The coverage is provided by RSCP in dBm and by EcNo in dB. When one of these is constantly equal to, or lower than, the values configured for a period entered, in minutes, under the “*Threshold Interval*” field, changeover to another carrier is performed.

*Switch parameters with an LTE connection*

- **RSRP Threshold, RSRQ Threshold and Threshold Interval:** The coverage is provided by RSRP in dBm and by RSRQ in dB. When one of these is constantly equal to, or lower than, the values configured for a period entered, in minutes, under the “*Threshold Interval*” field, changeover to another carrier is performed.

## 2.6.5 DHCP

Allows you to configure the device's DHCP server.

## DHCP Server Configuration

### Global DHCP Settings

DHCP:	<input type="button" value="Enable"/>
Maximum Lease Time:	<input type="text" value="3550w"/> (1s..3550w5d3h14m7s)
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

### Subnet DHCP Settings

Interface:	<input type="text" value="ethernet0/0.14"/>	<input type="button" value="Remove"/>
IP Address:	<input type="text" value="12.167.5.1"/>	
Start Range:	<input type="text" value="12"/> . <input type="text" value="167"/> . <input type="text" value="5"/> . <input type="text" value="150"/>	Network: 12.167.5.0
End Range:	<input type="text" value="12"/> . <input type="text" value="167"/> . <input type="text" value="5"/> . <input type="text" value="170"/>	Broadcast: 12.167.5.255
Router IP:	<input type="text" value="12.167.5.1"/>	
DNS Server:	<input type="text"/>	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

### DHCP - Subnet List

Subnet	Start Range	End Range
ethernet0/0.14	12.167.5.150	12.167.5.170

Fig. 92: Nets – DHCP.

This page is divided into the following sections:

#### 2.6.5.1 Global DHCP Settings

Defines the general parameters for the DHCP server, such as the option to enable/disable the protocol and to indicate for how long addresses are assigned to the devices.

### Global DHCP Settings

DHCP:	<input type="button" value="Enable"/>
Maximum Lease Time:	<input type="text" value="3550w"/> (1s..3550w5d3h14m7s)
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Fig. 93: DHCP – Global DHCP Settings.

#### 2.6.5.2 Subnet DHCP Settings

You can assign specific configuration options to each Ethernet subinterface and to each BVI interface defined in the router so as to define and identify groups of clients. The configurable parameters are:

**Subnet DHCP Settings**

Interface:

IP Address:

Start Range:  .  .  .  
 Network: 12.167.5.0

End Range:  .  .  .  
 Broadcast: 12.167.5.255

Router IP:

DNS Server:

Fig. 94: DHCP – Subnet DHCP Settings.

- **Interface:** Configured through a pull-down menu where you can select the interface to configure.
- **IP Address:** Displays the IP address assigned to the interface selected to warn that it cannot be part of the address interval assigned to DHCP clients.
- **Start Range:** Indicates the initial host number to assign (the lowest) to the subnet. To do this, the address of the selected subnet is indicated.
- **End Range:** Indicates the final host number to assign (the highest) to the subnet. To do this, the broadcast address is indicated.
- **Router IP:** You can specify the client's future default gateway.
- **DNS Server:** Allows you to allocate an available DNS to the client. This parameter is optional.

To store the configuration established for the selected interface, click on *Apply*. To cancel the changes you have made and recover the information the device had, click on the *Cancel* button.

### 2.6.5.3 DHCP – Subnet List

Displays information on all the subnets that have been configured in the device's DHCP server.

**DHCP - Subnet List**

Subnet	Start Range	End Range
ethernet0/0.14	12.167.5.150	12.167.5.170

Fig. 95: DHCP – DHCP Subnet List.

## 2.6.6 Routes

The first section on this page allows the user to install default routes in the device through active tunnels or ppp/direct-ip connections. The second section displays the RIP protocol configuration environment.

## Routes Configuration

### Routes Settings

Enable Default Route by direct-ip Disable ▾  
 Automatic Default Route (ACAT)

Apply

### RIP Settings

Interface: direct-ip1 ▾ Selector: Send ▾ Position: None ▾

Add

### RIP Distribute Subnet

Subnets: -- New Subnet -- ▾

Subnet IP:  Subnet Mask:

Add

### Remove RIP Configuration

Remove RIP Configuration

Remove

### RIP Configuration Interfaces

Interface	Send	Receive
192.168.1.1	none	none
direct-ip1	none	none
direct-ip2	none	none
gre1	rip2-multicast	none
gre2	rip2-multicast	none
gre3	rip2-multicast	none
gre4	rip2-multicast	none
11.69.80.134	none	none
12.167.5.1	none	none

### RIP Configuration Distributed Subnets

Subnet	Mask
12.167.100.0	255.255.255.0
11.69.80.134 (Loopback Address)	255.255.255.255

Fig. 96: Nets – Routes.

### 2.6.6.1 Route Settings

Here, you can decide whether to install default routes in the device through tunnels when these are active (by selecting the *Disable* option and ticking the checkbox) or explicitly add a default route through the ppp/direct-ip connections (by selecting the *Enable* option). If the device cannot offer either option, this section remains hidden.

### Routes Settings

Enable Default Route by direct-ip Disable ▾  
 Automatic Default Route (ACAT)

Apply

Fig. 97: Routes – Routes Settings.

### 2.6.6.2 RIP Settings

Allows you to define what type of RIP packets can be sent and received for each PPP/DIRECT-IP and GRE interface, disable RIP sending, and/or listen in this interface through the *none* option. To do this, use the *Apply* button each time you configure or modify data for an interface.

**RIP Settings**

Interface:  Selector:  Position:

Fig. 98: Routes – RIP Settings.

- **Interface:** Configured through a pull-down menu where you can select the interface you want to configure.
- **Selector:** Here, you can select the type of compatibility you wish to configure for the selected interface: *Send* or *Reception*.
- **Position:** Depending on the option selected in the *Selector* field, we can view one set of options or another:
  - **Send Selector:**
    - **None:** Disables RIP packet sending in the interface.
    - **RIP-2 Multicast:** Version 2 RIP packets are sent using multicast.
  - **Reception Selector:**
    - **None:** Disables RIP listening in the interface.
    - **RIP-2:** Only accepts version 2 RIP packets.

### 2.6.6.3 RIP Distribute Subnet

The different subnets that are going to be broadcast by RIP within the tunnels are defined in this section.

#### 2.6.6.3.1 Adding and configuring a subnet

To add a new *subnet*, select the “*New Subnet*” option from the pull-down menu, indicate its IP address and the subnet mask, and click on *Add*.

**RIP Distribute Subnet**

Subnets:

Subnet IP:  Subnet Mask:

Fig. 99: Routes – RIP Distribute Subnet – Adding a subnet.

#### 2.6.6.3.2 Removing a subnet

To remove a *subnet*, select it from the pull-down menu and click on the *Remove* button.

**RIP Distribute Subnet**

Subnets:

Subnet IP:  Subnet Mask:

Fig. 100: Routes – RIP Distribute Subnet – Removing a subnet.

### 2.6.6.4 Remove RIP Configuration

Allows you to remove all RIP-defined configurations. To execute this, you need to click on the *Remove* button and confirm this action.

### Remove RIP Configuration

Remove RIP Configuration

Fig. 101: Routes – Remove RIP Configuration.

## 2.6.6.5 RIP Configuration

To simplify user tasks, two lists are displayed (at the bottom of the page) with the sending and reception parameters to be used in the interfaces and subinterfaces advertised by RIP within the tunnels.

### RIP Configuration Interfaces

Interface	Send	Receive
192.168.1.1	none	none
direct-ip1	none	none
direct-ip2	none	none
gre1	rip2-multicast	none
gre2	rip2-multicast	none
gre3	rip2-multicast	none
gre4	rip2-multicast	none
11.69.80.134	none	none
12.167.5.1	none	none

### RIP Configuration Distributed Subnets

Subnet	Mask
12.167.100.0	255.255.255.0
11.69.80.134 (Loopback Address)	255.255.255.255

Fig. 102: Routes –RIP Configuration.

## 2.6.7 PRIME

You may only access this *Nets* menu option when using the Regesta Smart PLC model. It allows the user to configure parameters relative to the PLC/PRIME interface.

## PRIME Interface Configuration

### PRIME Settings

Local IP:  Local-port:  (0..65535)

### PLC Signal Settings

PLC-Signal:  Channel number (!):  (1..8)

(!) The channel is only configured if the router's hardware supports multichannel and if the router has PRIME 1.4

### Topology Info Settings

Save Topology Info

Timeout (s):  (10..65535)

File Name Prefix:  (1..20 chars)

File Path:  (1..20 chars)

FTP Server IP:

FTP Server-Port:  (0..65535)

FTP User:  (1..12 chars)

FTP Password:  (1..12 chars)

Fig. 103: Nets - PRIME.

The configurable parameters on this page are as follows:

- *PRIME Settings*: In this section, the local IP and the local port assigned to the interface can be configured.
- *PLC Signal Settings*: Allows you to enable/disable the PLC signal and choose the frequency channel.



#### Note

The channel is only configured if the router's hardware supports multichannel and if the router has PRIME 1.4.

- *Topology Info Settings*: Allows you to configure parameters relative to topology file management. Said file contains the system's topology information (Service Nodes registered in the Base Node) and the configurable features here are:
  - Enable or disable the generation and FTP sending of topology files.
  - Timeout Adjustment. This is the period of file updating (time between save operations).
  - Specify the file name and the path where it is stored.
  - IP address and port number of the FTP server.
  - FTP user and password.

## 2.6.8 SCADA

You may only access this *Nets* menu option when using the Regesta Smart model. It allows the user to configure parameters relative to the SCADA interface.

The console port may not be on the router, in which case we can make it appear after the router has been saved and restarted. When the port is selected, it can be configured as a SCADA interface.

### SCADA Interface Configuration

Network: console port ▼

■ **Network Settings**

Local-IP:

Local-port:  (0..65535)

Driver-type: RS232 ▼

Idle-time:  (0s..2d)

Parity: even ▼

Protocol: modbus-rtu ▼

Speed:  (300..115200)

Fig. 104: **Nets - Scada.**

The configurable parameters on this page are as follows. They can differ depending on the interface configured and the card installed:

- *Local-IP*: In this section, the local IP assigned to the interface can be configured.
- *Local-port*: In this section, the local port assigned to the interface can be configured. The port is 502 by default.
- *Driver-type*: Allows you to configure the type of driver: RS232, RS485-2W or RS485-4W.



#### Note

All options are not always shown. This depends on the card installed.

- *Idle-time*: Allows you to configure the idle-time. It is 0s by default.
- *Parity*: Allows you to configure the parity: even, odd or mask. It is even by default.
- *Protocol*: Allows you to configure the protocol: modbus-rtu or modbus-ascii. It is modbus-rtu by default.
- *Speed*: In this section, the interface speed can be configured. Its value is 2400 by default.
- *Termination-resistor*: Allows you to enable/disable the termination-resistor. It is disabled by default and only appears for configuration if the driver is RS485.

## 2.6.9 Virtual Bridges

Here, the user can create up to a maximum of seven virtual bridges and modify them.



## Virtual Bridges

### Virtual Bridge Configuration

Interface:

---

▶ **Ports Configuration**

Interface:  Port:  (1..254)

---

▶ **Ports List**

Interface	Port	Action
ethernet0/1	1	<input type="button" value="Delete port"/>
ethernet0/2.16	2	<input type="button" value="Delete port"/>

Fig. 105: Nets - Virtual Bridges.

For each BVI interface created on the device, the user can configure a virtual bridge. To do this, the user must first select the BVI interface from the pull-down menu. Once selected, its configuration is automatically displayed on the page.

Interface:

Fig. 106: Virtual Bridges - Virtual Bridge Configuration.

▶ **Ports List**

Interface	Port	Action
ethernet0/1	1	<input type="button" value="Delete port"/>
ethernet0/2.16	2	<input type="button" value="Delete port"/>

Fig. 107: Virtual Bridges - Port List

To add an Ethernet interface/subinterface to a virtual bridge, the user must select it from the pull-down menu, indicate a port number and click on the *Add* button. It is important to know that the same interface cannot pertain to more than one bridge and that the application will warn if this situation occurs. Every time an interface is added, the virtual bridge configuration displayed on the page is automatically updated.

### Ports Configuration

Interface:  Port:  (1..254)

### Ports List

Interface	Port	Action
ethernet0/1	1	<input type="button" value="Delete port"/>
ethernet0/2.16	2	<input type="button" value="Delete port"/>

Fig. 108: Virtual Bridges - Add Interfaces.

The user can also remove a port from the virtual bridge configuration by clicking on the corresponding button. If the virtual bridge remains empty after deleting the port, the application will warn the user and offer the possibility of deleting the virtual bridge as well as its corresponding BVI interface. Every time a port is removed, the virtual bridge configuration displayed on the page is automatically updated.

### Ports List

Interface	Port	Action
ethernet0/1	1	<input type="button" value="Delete port"/>
ethernet0/2.16	2	<input type="button" value="Delete port"/>

Fig. 109: Virtual Bridges - Port List - Remove Port.

## Chapter 3 Configuration Recommendations

### 3.1 Keepalive mechanism in the tunnels

The keepalive mechanism determines the time (T) the device takes to detect a drop in a tunnel. Its value is determined by the “*Keepalive Period Reachable*”, “*Keepalive Period Unreachable*” and “*Keepalive Stability Threshold*” parameters as follows:

$$T = \text{Keepalive Period Reachable} + (\text{Keepalive Period Unreachable} * (\text{Keepalive Stability Threshold} - 1))$$

■ **Global Tunnel Settings**

Recovery Time:	<input type="text"/>	(0..86400 seconds)
Keepalive Period Reachable:	<input type="text"/>	(1..36000 seconds)
Keepalive Period Unreachable:	<input type="text"/>	(2..36000 seconds)
Keepalive Stability Threshold:	<input type="text"/>	(1..255)
<input checked="" type="checkbox"/> IPsec Mode:	Main	▼
IPsec Preshared-Key:	••••	(1..32 characters)

Fig. 110: DMVPN – Global Tunnel Settings.

To determine what values you should select, keep the following in mind:

- **Short T Values**

- **Advantages**

- They allow for a quick detection of drops in tunnel connectivity, thus reducing the time the device remains inaccessible.

- **Drawbacks:**

- The traffic generated by this mechanism isn't application traffic. As a result, the lower the frequency at which these packets are sent, the higher the traffic generated. This hinders communication performance.
    - In low speed channels, if a traffic peak is produced, there is a high possibility *keepalive* packets won't arrive in time and trigger a tunnel drop.
    - They increase the possibility of tunnels being dropped due to small instabilities.

- **Long T Values**

- **Advantages:**

- They reduce the traffic this mechanism generates and, consequently, increase communication performance.
    - Traffic peaks and small connection instabilities do not affect tunnel maintenance.

- **Drawbacks:**

- The device remains inaccessible for a longer period, as it takes longer to detect a drop in the tunnel.

In view of the foregoing, we recommend configuring the mechanism with the following values. This way, a drop in a tunnel will be detected in (approximately) 60 seconds:

Keepalive Period Reachable = 10 seconds between each keepalive transmission.

Keepalive Period Unreachable = 30 seconds between every keepalive transmission in an unreachable state.

Keepalive Stability Threshold = 3 polling packets in an unreachable state are needed for the tunnel to be considered down.

In high speed channels like HSDPA, you can reduce the " *Keepalive Period Unreachable* " parameter without triggering false tunnel drops due to peaks in traffic. However, you must remember that the device can dynamically change the type of cellular network it is connected to at any point.

## 3.2 Parameters for carrier changeover

In a WWAN technology scenario with dual SIM, the switch process from one carrier to another requires a period of time that you must bear in mind when configuring the supervision criteria. Below, we have laid out some guidelines to optimize parameter configuration:

- **Registration Criteria Interval:** Too low a value will trigger continuous switching, since the device will not have enough time to connect to either carrier. To avoid this scenario, we suggest assigning more than 2 minutes.
- **Recovery Interval:** This value must be greater than the one indicated in the previous parameter so that the device has enough time to establish connection with the main carrier before changing over.

### ■ SIM Changeover Settings

Configure double SIM management

#### Mode to select the main SIM:

- Main Primary SIM  
 Main Secondary SIM  
 Sequential Order  
 Random Order

#### Supervision parameters:

RSSI Threshold:	<input type="text" value="-45"/>	(-113..0) dBm
Threshold Interval:	<input type="text" value="2"/>	(0..180) minutes
Recovery Interval:	<input type="text" value="2"/>	(0..65535) minutes
Registration Criteria Interval:	<input type="text" value="3"/>	(0..180) minutes

Fig. 111: Wireless WAN –SIM Changeover Settings.