



Regesta-PLC

Web Interface Manual

Copyright© Teldat DM479-I Version 1.0 12/2016 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

I	Related Documents	1
Chapter 1	Introduction	2
1.1	Introduction	2
1.2	Local connection	2
Chapter 2	Web Interface	5
2.1	Structure	5
2.2	Information menu	5
2.3	Status menu	6
2.3.1	WWAN-1 Status	6
2.3.2	DMVPN connections	10
2.3.3	DHCP Clients	11
2.3.4	Netstat	11
2.3.5	Diagnostics	12
2.3.6	PRIME	13
2.4	Logs menu.	14
2.4.1	Traces WWAN-1	15
2.5	System menu	16
2.5.1	Password	16
2.5.2	Settings	17
2.5.3	SNMP.	17
2.6	Nets menu.	20
2.6.1	Interfaces	20
2.6.2	Networks	22
2.6.3	DMVPN	24
2.6.4	Wireless WAN Configuration	27
2.6.5	DHCP	33
2.6.6	Routes	35
2.6.7	PRIME	37
Chapter 3	Configuration Recommendations	39

I Related Documents

Teldat Dm478-I

Chapter 1 Introduction

1.1 Introduction

The **Regesta-PLC** router configuration tool provides a quick and efficient start up.

It is a Web Configurator that runs automatically and takes into account the router's work scenario. The configuration parameters, which can be accessed through the web, are those vital to the router operations. The remaining parameters (hidden from the user) aim at optimizing the operating system. To configure them, the connection speed to the terminal is the main factor considered.

1.2 Local connection

If no settings have been pre-activated, the default factory settings installed will be enabled. You can access the Web Configurator by connecting an Ethernet cable, supplied with the router, to any of the LAN ports and to the PC being used for the configuration tasks.

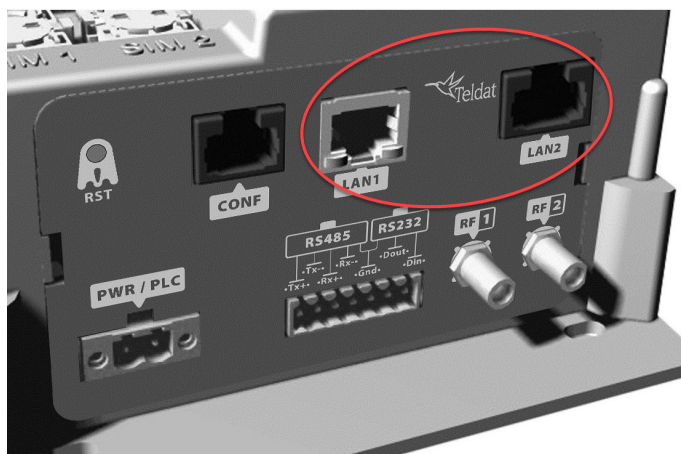


Fig. 1: Regesta PLC connector panel showing the LAN ports

The default IP address (accessible from any switch port) is 192.168.1.1/24. The PC must configure an address belonging to the Regesta-PRO-ER subnet (192.168.1.0/24).

Once you have guaranteed IP access to the router, enter the following URL into the Web browser:

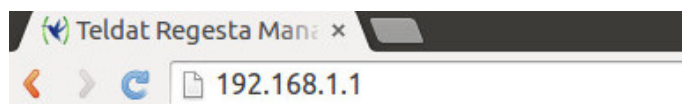



Fig. 2: Accessing the Web Configuration


If router access is correct, the Web configurator home page is displayed.

Administrator

User

Password




Add to Favorites
 -65 dBm 21407 WCDMA Online

Administration

Wireless Connection

Wireless Connection Status

 Online

▶ **As administrator you can:**

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

Teldat Regesta-PLC

Overview

The Regesta-PLC model is a rugged equipment with an integrated PLC module and two LAN ports.

Regesta-PLC 3G 30SN

Web Firmware Version: 5.2.0

Fig. 3: REGESTA-PLC Home page

In the bar at the top of the home page, there is a changing text that indicates whether or not the device may be accessed and through which technology. In the case of the Regesta-PLC, this can only be WWAN. If the device cannot be accessed, an "Offline" information message appears.


 -61 dBm movistar GPRS Online

Fig. 4: WWAN Access: Coverage quality, carrier, technology and connection status


 Offline

Fig. 5: Device is inaccessible

In the middle of the home page, you'll see a graph showing the status of the characters associated to each access technology the device incorporates. Written information can also be found on the characteristics of the Web Configurator and the REGESTA-PLC device.

Administration

<p>Wireless Connection</p> <p>Wireless Connection Status</p> <p style="text-align: center;"> Online</p> <p>▶ As administrator you can:</p> <ul style="list-style-type: none"> - WWAN connection - DMVPN network - VLAN configuration - DHCP server - NTP client 	<p>Teldat Regesta-PLC</p> <p>Overview</p> <p>The Regesta-PLC model is a rugged equipment with an integrated PLC module and two LAN ports.</p>
---	---

Fig. 6: Home page information - REGESTA-PLC with WWAN access.

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

Regesta-PLC 3G 30SN	Web Firmware Version: 5.2.0
----------------------------	-----------------------------

Fig. 7: Device model and the Web firmware version installed

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

Administrator

User

Password **Log in**

Fig. 8: Access with user and password

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


Info	Status ▾ Logs ▾ System ▾ Nets ▾	 -89 dBm Orange HSDPA/HSUPA Online	Logout
-------------	---	---	---------------

Fig. 9: Access through the 'root' level


Info	Status ▾ Logs ▾ System ▾ Nets ▾	 -89 dBm Orange HSDPA/HSUPA Online	Logout
-------------	---	---	---------------

Fig. 10: Access through the 'configuration' level

Info	Status ▾ Logs ▾	 -89 dBm Orange HSDPA/HSUPA Online	Logout
-------------	-------------------------------	---	---------------

Fig. 11: 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 lapsed since the last restart.
- *Main menu* (red): Lets you browse through the different configurator pages.
- *Status bar* (orange): Shows whether or not the device is accessible and through which configuration.
- *Logout*(green): Disconnects the user and redirects him/her to the application disconnection 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 which allows him/her to configure or monitor the different router characteristics.

The screenshot shows the Teldat web interface with several elements highlighted by colored boxes:

- Purple box:** Host: REGESTA-PLC, Date: Friday, 11/11/16, Time: 00:19:14, Uptime: 1m46s
- Red box:** Main menu with items: Info, Status, Logs, System, Nets
- Orange box:** Status bar showing signal strength, -75 dBm, 21407 WCDMA Online
- Green box:** Logout button
- Blue box:** System Information section containing:

Router Software version:	11.00.05.10.03 Nov 8 2016 20:05:37
MAC:	00A0268C0012
Router Model:	Regesta-PLC 3G 30SN 27 201
Processor:	RP_PLC PCB:0x369 CHIP_ID:0x6368 REV:0xB2
Serial number:	879/00109

 Below the table are buttons for Save, Reboot, and Restore default configuration.

Fig. 12: Page structure

2.2 Information menu

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

The screenshot shows the System Information page with the following details:

- System Information**

Router Software version:	11.00.05.10.03 Nov 8 2016 20:05:37
MAC:	00A0268C0012
Router Model:	Regesta-PLC 3G 30SN 27 201
Processor:	RP_PLC PCB:0x369 CHIP_ID:0x6368 REV:0xB2
Serial number:	879/00109
- Buttons: Save, Reboot, Restore default configuration

Fig. 13: 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-PLC model and router license.
- *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 any changes made in the router configuration.
- *Reboot Button*: Lets the user reboot the router from the Web. On clicking on this button, the user is automatically logged out and redirected to the application disconnection page.
- *Restore default configuration Button*: Lets you reestablish the router default configuration, which automatically re-starts for changes to be effective. On reboot, the user is automatically redirected to the application disconnection page.

**Note**

- *For the changes executed in the router configuration via the Web Configurator to activate, you first need to save the changes through the "Save" button and then reboot the router using the "Reboot" button.*
- *If you reestablish the default configuration, you will lose all changes previously made to the router's configuration.*

From this home 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

The *Status* menu allows you to access information on the various aspects of the router status.

Status ▾	Logs ▾	System ▾	N
Status WWAN-1			
DMVPN connections			
DHCP clients			
Netstat			
Diagnostics			
<u>PRIME</u>			

Fig. 14: Menu Status – REGESTA-PLC with 1 2G/3G/LTE module and PRIME technology

2.3.1 WWAN-1 Status

Summarizes the parameters that characterize the cellular interface for module 1.

WWAN-1 Connection Status

■ Connection

Register:	Registered
Operator:	21407
Technology:	WCDMA
Level(dBm):	-69

■ Cells

	UARFCN	PSC	RSCP(dBm)	ECIO(dB)
Serving Cell:	10838	510	-70	-6
WCDMA Cell #1:	10838	310	-77	-13

■ Module Information

Manufacturer:	Sierra Wireless, Incorporated
Model:	MC7304
Firmware:	SW19X15C_05.05.16.02 r21040 carmd-fwbuild1 2014/03/17 23:49:48
IMEI:	356853050599937
IMSI:	214075537088744
SIM Card ID:	8934076100141203330

■ IP Protocol

Assigned IP:	176.81.214.1
--------------	--------------

Fig. 15: Status –WWAN-1 Status

This page is divided into four sections:

(a) *Connection*

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

■ Connection

Register:	Registered
Operator:	21407
Technology:	WCDMA
Level(dBm):	-69

Fig. 16: 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.

(b) *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.

- 2G Connection:

■ Cells							
	MCC	MNC	LAC	CellID	BSIC	ARFCN	RX(-dBm)
Serving Cell:	214	07	b05	82c	98	6	53
Neighbour 1:	214	07	b05	82f	112	550	33
Neighbour 2:	214	07	b05	82b	114	66	35
Neighbour 3:	214	07	b05	82d	52	3	45
Neighbour 4:	214	07	b05	123	70	54	55
Neighbour 5:	214	07	b05	126	2	548	57
Neighbour 6:	214	07	b05	82e	1	542	57

Fig. 17: WWAN-1 Status – Cells (2G Connection)

- 3G Connection:

■ Cells				
	UARFCN	PSC	RSCP(dBm)	ECIO(dB)
Serving Cell:	10838	510	-70	-6
WCDMA Cell #1:	10838	310	-77	-13

Fig. 18: WWAN-1 Status – Cells (3G Connection)

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

- 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 04482e02
E-UTRA absolute radio frequency channel number of the serving cell: 1501
LTE serving cell ID: 89
Priority for serving frequency: 6
S non-intra search threshold to control non-intrafrequency searches: 14
Serving cell low threshold: 4
S intra search threshold: 54
Cell #1
  Physical cell ID: 89
  Current RSRQ as measured by L1: -8 (dB)
  Current RSRP as measured by L1: -90 (dBm)
  Current RSSI as measured by L1: -62 (dBm)
  Cell selection Rx Level: 33
Cell #2
  Physical cell ID: 285
  Current RSRQ as measured by L1: -7 (dB)
  Current RSRP as measured by L1: -88 (dBm)
  Current RSSI as measured by L1: -71 (dBm)

```

LTE Interfrequency Information

```

UE is in idle mode
Cell #1
E-UTRA absolute radio frequency channel number: 3250
Cell Srxlev low threshold: 0
Cell Srxlev high threshold: 20
Cell reselection priority: 7
Cell #2
E-UTRA absolute radio frequency channel number: 6300
Cell Srxlev low threshold: 0
Cell Srxlev high threshold: 4
Cell reselection priority: 5

```

Fig. 19: **WWAN-1 Status – Cells (LTE Connection)**

(c) *Module Information*

Displays information on the module.

Module Information

Manufacturer:	Sierra Wireless, Incorporated
Model:	MC7304
Firmware:	SWI9X15C_05.05.16.02 r21040 carmd-fwbuild1 2014/03/17 23:49:48
IMEI:	356853050599937
IMSI:	214075537088744
SIM Card ID:	8934076100141203330

Fig. 20: **WWAN- Status 1 – Module Information.**

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

- *SIM Card ICC*: Integrated Circuit Card ID for the SIM installed in the router.

(d) *IP Protocol*

Displays the IP dynamically assigned by the carrier.

■ IP Protocol	
Assigned IP:	176.81.214.1

Fig. 21: Status WWAN-1 – IP Protocol.

2.3.2 DMVPN connections

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

DMVPN Connection Status

■ Tunnel 1	
Interface:	gre1
Protocol-Address:	11.4.7.6
NBMA-Address:	11.16.80.6
Status:	UP

■ Tunnel 2	
Interface:	gre2
Protocol-Address:	11.6.7.6
NBMA-Address:	11.16.80.6
Status:	UP

■ Tunnel 3	
Interface:	gre3
Protocol-Address:	11.14.7.6
NBMA-Address:	11.16.80.143
Status:	DOWN

■ Tunnel 4	
Interface:	gre4
Protocol-Address:	11.16.7.6
NBMA-Address:	11.16.80.147
Status:	DOWN

Fig. 22: 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 isn't configured, the tunnel status is: *Not configured*.

- If the tunnel is configured but not operative, the tunnel status is: *DOWN*.
- If the tunnel is configured and operative, the tunnel status is: *UP*.

2.3.3 DHCP Clients

Provides information on client devices that have received IP addresses from the REGESTA-PLC's DHCP server.

DHCP Leases

■ Users

IP Address	MAC Address	Valid From	Valid Till
12.167.5.163	00:2e:d6:33:33	Sat Mar 10 2012 10:20:35	Sat Mar 10 2012 12:35:40
12.167.5.162	00:88:0A:88:11	Sat Mar 17 2012 13:15:20	Sat Mar 10 2012 15:30:25

[Refresh](#)

Fig. 23: Status – DHCP Clients.

The information displayed on the 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

This page displays the following information in table format:

- *Interface Statistics*:

■ Interfaces Statistics

Interface	Unicast Pqts Rcv	Multicast Pqts Rcv	Bytes Received	Packets Transmitted	Bytes Transmitted
ethernet0/0	1761	3055	1034106	1800	921445
ethernet0/1	0	0	0	0	0
atm0/0	0	0	0	0	0
cellular1/0	478	0	35564	239	6011
cellular1/1	116	0	2524	126	8627
ppp1	25	0	438	39	2775
ppp2	31	0	618	57	4356
gre1	0	0	0	116	4176
gre2	0	0	0	116	4176
gre3	0	0	0	100	3600
gre4	0	0	0	100	3600
loopback1	0	0	0	0	0
ethernet0/0.5	0	0	0	0	0
ethernet0/0.19	0	0	0	0	0
ethernet0/0.25	0	0	0	0	0

Fig. 24: Status – Netstat – Interface Statistics.

- *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	80	0.0.0.0	0	LISTEN
0.0.0.0	53	0.0.0.0	0	LISTEN
0.0.0.0	22	0.0.0.0	0	LISTEN

Fig. 25: Status – Netstat – List of TCP connections.

- Interface IP addresses:

■ Interface IP Addresses

Interface	IP Address
ppp1	unnumbered - using global-address (16.1.16.13)
ppp2	unnumbered - using global-address (17.60.12.89)
gre1	12.10.68.2/21
gre2	15.21.168.3/21
gre3	10.2.45.125/21
gre4	14.8.2.67/21
loopback1	17.60.12.89/32
ethernet0/0.5	12.167.5.160/29
ethernet0/0.19	12.167.45.160/29
ethernet0/0.25	12.167.2.32/30
Special IP Address	
internal-address	0.0.0.0
management-address	17.60.12.89
router-id	0.0.0.0
global-address	17.60.12.89

Fig. 26: Status – Netstat – Interface IP Addresses.

- Active IP routing table:

■ Routing Table

Type	Dest net/Mask	Cost	Age	Next hop(s)
del(0)[0]	16.0.0.0/8	[255/16]	200	none
dir(0)[1]	16.1.16.13/32	[0/1]	0	ppp1
del(0)[0]	16.45.67.108/32	[255/16]	210	none
del(0)[0]	11.0.0.0/8	[255/16]	200	none
stat(1)[0]	11.16.80.6/32	[60/1]	0	ppp1
del(1)[0]	11.16.80.143/32	[255/16]	210	none
del(1)[0]	11.16.80.147/32	[255/16]	210	none
sbnt(0)[0]	12.0.0.0/8	[240/1]	0	none
dir(0)[1]	12.167.2.32/30	[0/1]	0	ethernet0/0.25
dir(0)[1]	12.167.5.160/29	[0/1]	0	ethernet0/0.5
dir(0)[1]	12.167.45.160/29	[0/1]	0	ethernet0/0.19
sbnt(0)[0]	17.0.0.0/8	[240/1]	0	none
dir(0)[2]	17.60.12.89/32	[0/1]	0	loopback1

Fig. 27: Status – Netstat – Routing Table.

2.3.5 Diagnostics

Executes a *ping* operation, which can determine if the device accessed 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 10.94.70.1: icmp_seq=0. time=145. ms
64 bytes from 10.94.70.1: icmp_seq=1. time=85. ms
64 bytes from 10.94.70.1: icmp_seq=2. time=96. ms
64 bytes from 10.94.70.1: icmp_seq=3. time=85. ms
64 bytes from 10.94.70.1: icmp_seq=4. time=85. ms

---- PING Statistics----
5 packets transmitted, 5 packets received,
0 time out surpassed packets, 0% packet loss
round-trip (ms)  min/avg/max = 85/99/145
REGESTA_3G_1M IP+
```

```

Press any key to abort.

Tracing the route to: 10.94.70.1 [],
Protocol: UDP, 4 hops max, 56 byte packets

 1   94 ms  99 ms  70 ms   10.94.70.1
Trace complete.

REGESTA_3G_1M IP+
```

Fig. 28: Status – Diagnostics – Ping – Traceroute.

2.3.6 PRIME

This option on the *Status* menu can only be accessed using a REGESTA-PLC model.

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

- *PRIME global 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:	01.03.10.01-B-L
Interfaz State:	UP(4)
PRIME Mng State:	UP(11)

Fig. 29: Status - Global PRIME Information

- *TCP connection information:*

Shows information on the TCP connection:

- Port number used.

- Number of opened sessions.
- Maximum number of concurrent sessions.
- Packets sent and received.

■ TCP Connections Information

TCP Listen Port:	12
Opened Sessions:	0
Max Simultaneous Sessions:	0
Packets Sent:	0
Packets Received:	0

Fig. 30: Status – TCP Connections information

- *Topology Information* :

This table provides information on the nodes, which define the system topology. There are 2 types of nodes:

- Base Node: This is the local node (the router).
- Service Node: Rest of the nodes (switches and terminals) making up the system.

■ Topology Information

BASE NODE									
State	MAC	LNID	DISC	UP-TIME	CNX-TIME				
Running	00:A0:26:8C:00:13	0x0000	0	19:07:18	19:07:18				
SERVICE NODES									
Level	State	MAC	LNID	SID	LSID	DISC	UP-TIME	%	CNX-TIME
0	terminal	40:40:22:68:D4:01	0x00d3	0x00	0xff	1	2:34:28	13	0:01:34

Fig. 31: Status – Topology Information

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

LNID: Node identifier on 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: Located on the Service Nodes list, this 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: Length of time the node remains connected in the current active connection.

2.4 Logs menu

Accesses pages where you can see the evolution of the status for the device's 2G/3G/LTE module.



Fig. 32: Logs Menu – REGESTA-PLC 1 2G/3G/LTE module.

2.4.1 Traces WWAN-1

This page displays the information associated to the router's 2G/3G/LTE module.

Traces WWAN-1

■ WWAN-1

Module Manufacturer:	Sierra Wireless, Incorporated
Module Model:	MC8705
Module Firmware:	T3_5_4_1AP R604 CNSZXD00000155 2013/03/15 10:05:05

■ Modem diagnostics

```

FO;*CNTI=0
+CSQ: 18,99
+COPS: 0,2,"21401",2
+CGREG: 2,1,"430E","007C0C05",2
^SYSINFO: 2,2,0,5,1
*CNTI: 0,HSDPA/HSUPA
OK
AT+RSCP?;+ECIO?;+UPSC?;!GSTATUS?;!GSMINFO?;+USET?;+USET?1
+RSCP:
RSCP: -76 dBm
+ECIO:
Tot Ec/Io: -8.5 dB

```

Modem status

Fig. 33: Logs – Traces WWAN-1.

This is divided into two sections:

(a) *WWAN-1*

Displays information on the type and version of the module and the firmware installed in the device:

■ WWAN-1

Module Manufacturer:	Sierra Wireless, Incorporated
Module Model:	MC8705
Module Firmware:	T3_5_4_1AP R604 CNSZXD00000155 2013/03/15 10:05:05

Fig. 34: Logs – Traces WWAN-1– WWAN-1.

(b) *Modem diagnostics*

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



Fig. 35: Traces WWAN-1 – Modem diagnostics.

2.5 System menu

Lets you configure the router's general parameters.

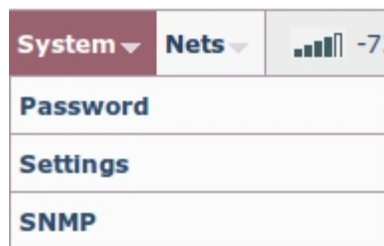


Fig. 36: System Menu.

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.

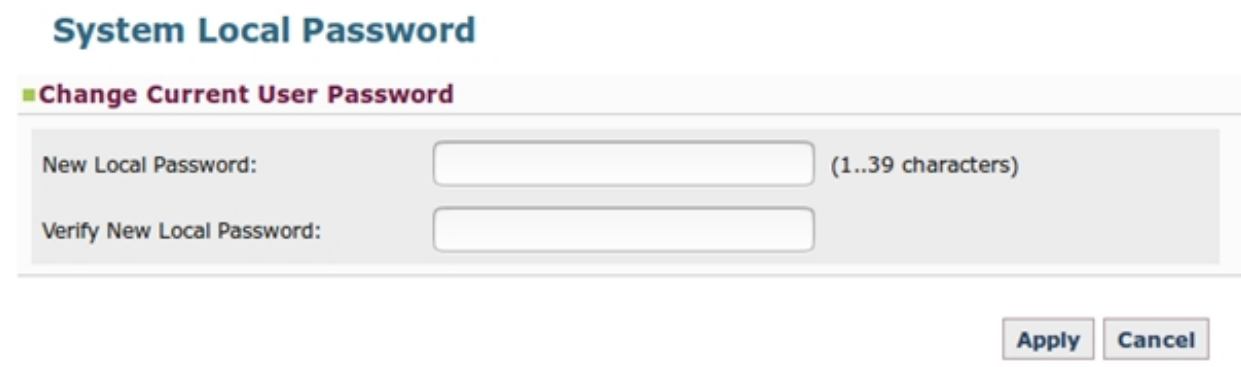


Fig. 37: System – Password.

When a 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. 38: System – Password.

2.5.2 Settings

Here you can configure various general parameters in the system.

System Settings

■ System Settings

Host Name: (1-79 characters)

■ Time Settings

NTP Server: Timezone:

Summer Time:

■ Web Settings

HTTP Port: (1-65534)

Fig. 39: System – Settings.

- *System Settings*

System parameters.

- *Host Name*: Router name.

- *Time Settings*

Date and time parameter.

- *NTP Server*: NTP server IP address to synchronize the router's date and time.

- *Timezone*: Hour zone the router is in.

- *Summer Time*: Activate or deactivate summer time.

- *Web Settings*

Web configuration parameter.

HTTP Port: Web configuration port.

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

2.5.3 SNMP

This page shows the SNMP protocol configuration environment for the sending and receiving of SNMPv1 traps.

Host Trap Manager Settings

Hosts

Hosts:

-- New Host --

Host Configuration

IP Address:

UDP Port:

162

Send Standard Traps:

No

Send Enterprise Traps:

No

Apply

Cancel

Community Subnet

Subnets:

-- New Subnet --

Subnet IP:

Subnet Mask:

Add

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. 40: System – SNMP.

This is divided into the following sections:

(a) *Hosts*:

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

- *Adding and configuring a host*

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

- Select the *New Host* option from the pull-down menu.
- 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.

- Click on *Apply*.

To cancel the modifications, click on *Cancel*.

Hosts

Hosts: -- New Host --

Host Configuration

IP Address: 12.165.2.28 UDP Port: 162

Send Standard Traps: Yes Send Enterprise Traps: No

Apply Cancel

Fig. 41: **SNMP – Hosts – Adding and configuring a host**

- *Editing a host configuration*

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

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

Hosts

Hosts: 12.165.2.20 Remove

Host Configuration

IP Address: 12.165.2.20 UDP Port: 162

Send Standard Traps: Yes Send Enterprise Traps: Yes

Apply Cancel

Fig. 42: **SNMP – Hosts – Editing the configuration for a host.**

- *Removing a host*

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

Hosts

Hosts: 12.165.2.20 Remove

Fig. 43: **SNMP – Hosts – Remove a host.**

(b) *Community Subnet*

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

- *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 subnet mask then click on *Add*.

Community Subnet

Subnets: -- New Subnet --

Subnet IP: 12.165.2.144 Subnet Mask: 255.255.255.254

Add

Fig. 44: **SNMP – Community Subnet – Adding a subnet.**

- *Removing a subnet*

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

Fig. 45: **SNMP – Community Subnet – Removing a subnet.**

(c) *Host List*

There is a list at the end of the page showing 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. 46: **SNMP – Host List.**

(d) *Subnets List*

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

■ Subnets List	
Subnet	Mask
12.165.2.0	255.255.255.0

Fig. 47: **SNMP – Subnets List.**

2.6 Nets menu

Lets you configure the router's network parameters.

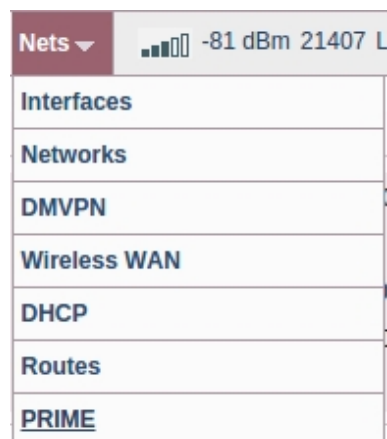


Fig. 48: **Nets Menu – REGESTA-PLC with WWAN and PRIME technologies.**

2.6.1 Interfaces

On this page, the user can create and remove interfaces and subinterfaces (as well as configure VLANs).

Interfaces

Interface Configuration

Base Interface: VLAN ID: (1..10000)

VLAN Configuration

VLAN: Ports: 1 2 3 4 5 6

Remove Interfaces

Interface:

Fig. 49: Nets – Interfaces.

The page is divided into the following sections:

(a) *Interface configuration*

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

Interface Configuration

Base Interface: VLAN ID: (1..10000)

Fig. 50: Interfaces – Interface Configuration –Ethernet Subinterfaces.

Interface Configuration

Base Interface: GRE Id:

Fig. 51: Interfaces – Interface Configuration –GRE Tunnels.

(b) *VLAN configuration*

Allows you to configure VLANs in the device, indicating the interface and the ports that will be members of each of them.

- *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 *Apply*. To cancel any modifications made, click on *Cancel*.

VLAN Configuration

VLAN: Ports: 1 2 3 4 5 6

Fig. 52: Interfaces – VLAN configuration – Adding and configuring a VLAN.

- *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: ethernet0/0.5 Ports: 1 2 3 4 5 6

Apply Cancel

Fig. 53: Interfaces – VLAN configuration – Editing the configuration for a VLAN.

(c) *Remove Interfaces*

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

Remove Interfaces

Interface: gre1 Remove

Fig. 54: 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: ethernet0/0.5

IP Address: 12.167.5.160

Netmask: 255.255.255.248

Secondary IP Addresses

Apply Cancel

Traffic Control Settings

Enable Routing Traffic Control

Apply

Loopback Settings

IP Address: 17.60.12.89

Netmask: 255.255.255.255

Apply Cancel

Fig. 55: Nets – Networks.

This page is divided into the following sections:

(a) *Network Settings*

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

Cancel 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: ethernet0/0.5

IP Address: 12.167.5.160

Netmask: 255.255.255.248

[Secondary IP Addresses](#)

Secondary IP Addresses

Secondary IP Address	IP Address	Netmask
<input checked="" type="checkbox"/> Secondary IP Address 1:	12.167.10.81	255.255.255.252
<input checked="" type="checkbox"/> Secondary IP Address 2:	12.167.11.80	255.255.255.252
<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. 56: Networks – Networks Settings.

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

Additionally, this section allows you to delete the IP address the device has configured by default from the configuration. To do this, select the Ethernet0/0 interface from the pull-down menu and click on *Delete IP Address*.

Network Settings

Network: ethernet0/0 [Delete IP Address](#)

IP Address: 192.168.1.1

Netmask: 255.255.255.0

[Secondary IP Addresses](#)

Fig. 57: Networks – Networks Settings – Removing the default IP address.

(b) *Traffic Control Settings*

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



The screenshot shows a web interface section titled "Traffic Control Settings". It features a single checkbox labeled "Enable Routing Traffic Control" which is checked. An "Apply" button is located in the bottom right corner of the settings area.

Fig. 58: Networks – Traffic Control Settings.

(c) *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.



The screenshot shows a web interface section titled "Loopback Settings". It contains two input fields: "IP Address" with the value "17.60.12.89" and "Netmask" with the value "255.255.255.255". "Apply" and "Cancel" buttons are located in the bottom right corner.

Fig. 59: 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 the remote devices establish (REGESTA-PLC), and a private destination IP address for the GRE tunnels that are necessary to transport the routing protocol.

Each HUB operates in a terminator. The latter can have several HUBs available, 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="5"/>	(1..36000 seconds)
Keepalive Period Unreachable:	<input type="text" value="5"/>	(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="11.4.7.6"/>	
NHS IP Address:	<input type="text" value="11.16.80.6"/>	
Base Interface:	<input type="text" value="ppp1"/>	
Key:	<input type="text" value="11"/>	(0..4294967295)

Fig. 60: Nets – DMVPN.

(a) *Global Tunnel Settings*

Configures the general parameters applicable to the GRE tunnel that the REGESTA-PLC assigns to each configured HUB.

Global Tunnel Settings

Recovery Time:	<input type="text" value="300"/>	(0..86400 seconds)
Keepalive Period Reachable:	<input type="text" value="5"/>	(1..36000 seconds)
Keepalive Period Unreachable:	<input type="text" value="5"/>	(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)

Fig. 61: DMVPN – Global Tunnel Settings.

- *Recovery Time*: Time in seconds in which traffic is 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.

- (a) *Keepalive Period Reachable*: Time in seconds between the sending of successive *keepalive* petition packets when responses are received.
 - (b) *Keepalive Period Unreachable*: Time in seconds between successive the sending of successive *keepalive* petition packets when responses stop arriving.
 - (c) *Keepalive Stability Threshold*: Number of consecutive *keepalive* petition packets without responses to determine that connectivity with the remote tunnel end has been lost.
- *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-PLC devices to be identified by a *pre-shared key*. Thus, 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.

On activating the *check* button, you also activate GRE tunnel encryption using IPSec.

Fig. 62: DMVPN – Global Tunnel Settings – IPSec Mode Main.

Fig. 63: DMVPN – Global Tunnel Settings – IPSec Mode Aggressive.

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

(b) Hub Settings

Configures the parameters that define each one of the Hubs.

Fig. 64: 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 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.

er assigned to the SIM2 (whenever there are two SIM cards). The other possible option, ADSL, is only available when you have a device model with an ADSL interface (this does not apply to Regesta-PLC).

- **Key:** Key used in the GRE tunnels to distinguish which mGRE interface a tunnel corresponds to, in the HUB, 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 has on this HUB, click on *Cancel*.

**Note**

Tunnel priority is defined by the GRE interface it is associated to. This means 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

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

Wireless WAN Configuration

■ Primary SIM Settings

Phone Number:	<input type="text"/>
PIN Code:	<input type="text" value="****"/>
APN:	<input type="text" value="operador1.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="operador2.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="0"/>	(-113..0) dBm
ECNO Threshold:	<input type="text" value="0"/>	(-50..5) dB
Threshold Interval:	<input type="text" value="0"/>	(0..180) minutes
Recovery Interval:	<input type="text" value="0"/>	(0..65535) minutes
Registration Criteria Interval:	<input type="text" value="0"/>	(0..180) minutes

Fig. 65: Nets – Wireless WAN (Regesta-PLC 1 2G/3G/LTE module).



Note

The parameters that determine the changeover conditions between the carriers are only displayed on the page when the device is equipped with a single module.

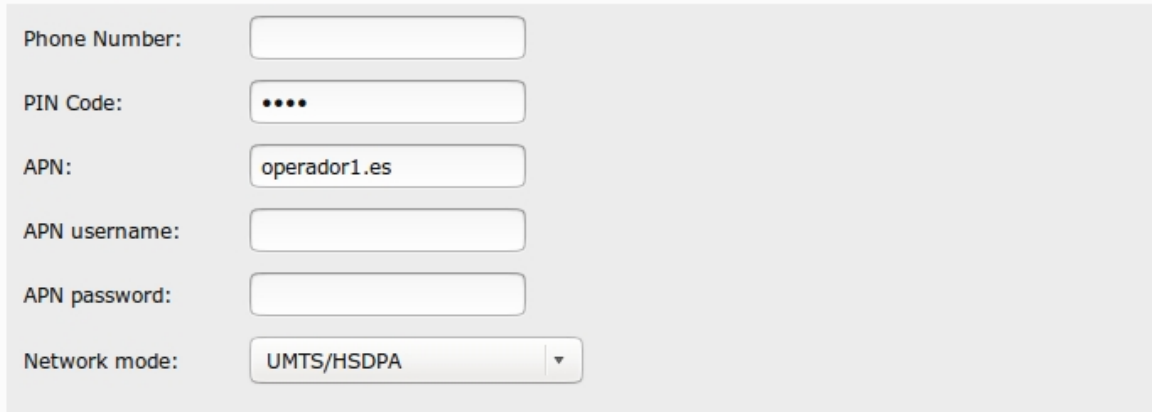
(a) Primary SIM Settings

Configures 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 must use when selecting this SIM.

■ Primary SIM Settings



Phone Number:

PIN Code:

APN:

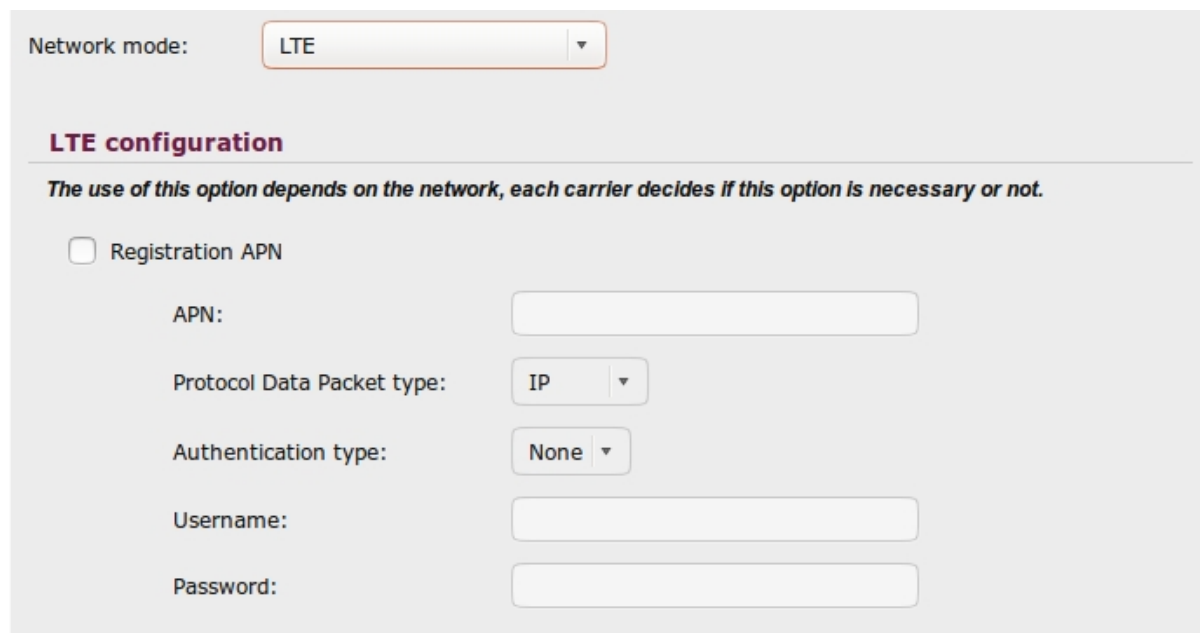
APN username:

APN password:

Network mode:

Fig. 66: Wireless WAN – Primary SIM Settings

When registering a mobile device, some LTE mobile phone carrier networks require that the equipment has 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 can 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:

Protocol Data Packet type:

Authentication type:

Username:

Password:

Fig. 67: Wireless WAN – Primary SIM Settings - LTE.

(b) Secondary SIM Settings

Configures the connection parameters associated to the SIM2 card, which are the same as those for the SIM1.

■ Secondary SIM Settings

Phone Number:	<input type="text"/>
PIN Code:	<input type="text" value="****"/>
APN:	<input type="text" value="operador2.es"/>
APN username:	<input type="text"/>
APN password:	<input type="text"/>
Network mode:	<input type="text" value="UMTS/HSDPA"/>

Fig. 68: Wireless WAN – Secondary SIM Settings.

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

Fig. 69: Wireless WAN –SIM Changeover Settings over 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. 70: Wireless WAN –SIM Changeover Settings over 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="0"/>	(-113..0) dBm
	ECNO Threshold:	<input type="text" value="0"/>	(-50..5) dB
	Threshold Interval:	<input type="text" value="0"/>	(0..180) minutes
2G	RSSI Threshold:	<input type="text" value="0"/>	(-113..0) dBm
	Threshold Interval:	<input type="text" value="0"/>	(0..180) minutes
	Recovery Interval:	<input type="text" value="0"/>	(0..65535) minutes
	Registration Criteria Interval:	<input type="text" value="0"/>	(0..180) minutes

Fig. 71: Wireless WAN –SIM Changeover Settings when a SIM is configured over 2G connection and the other over 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="0"/>	(-140..0) dBm
	RSRQ Threshold:	<input type="text" value="0"/>	(-20..0) dB
	Threshold Interval:	<input type="text" value="0"/>	(0..180) minutes
3G	RSCP Threshold:	<input type="text" value="0"/>	(-113..0) dBm
	ECNO Threshold:	<input type="text" value="0"/>	(-50..5) dB
	Threshold Interval:	<input type="text" value="0"/>	(0..180) minutes
Recovery Interval:		<input type="text" value="0"/>	(0..65535) minutes
Registration Criteria Interval:		<input type="text" value="0"/>	(0..180) minutes

Fig. 72: Wireless WAN –SIM Changeover Settings when a SIM is configured over LTE connection and the other over 3G connection.

- *Mode to select the main SIM*

Indicates which of the two defined mobile telephone carriers is the main and which the 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.	

- *Supervision Parameters*

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) the backup SIM is used (SIM2 card). After said time, switch to main SIM takes place.

Registration Criteria Interval: Specifies, the maximum time (in minutes) the interface can be unregistered. After said time, switch to the other carrier takes place.

Switch parameters with a 2G connection

RSSI Threshold: When the RSSI (Received Signal Strength Indicator) drops below this threshold, in dBm, the backup interval initiates.

Threshold Interval: Backup interval. Specifies the number of minutes with the RSSI below the threshold before changeover to the other carrier takes place.

Switch parameters with a 3G connection

RSCP Threshold, ECNO Threshold & Threshold Interval: Coverage is provided by RSCP in dBm and by EcNo in dB. When one of these is continuously equal or less than the configured values during a time indicated in minutes in the *Threshold Interval* field, changeover to another carrier is carried out.

Switch parameters with an LTE connection

RSRP Threshold, RSRQ Threshold & Threshold Interval: Coverage is provided by RSRP in dBm and by RSRQ in dB. When one of these is continuously equal or less than the configured values during a time indicated in minutes in the *Threshold Interval* field, changeover to another carrier is carried out.

2.6.5 DHCP

This page 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="button" value="ethernet0/0.5"/>	<input type="button" value="Remove"/>
IP Address:	<input type="text" value="12.167.5.160"/>	
Start Range:	<input type="text" value="12"/> . <input type="text" value="167"/> . <input type="text" value="5"/> . <input type="text" value="162"/>	Network: 12.167.5.160
End Range:	<input type="text" value="12"/> . <input type="text" value="167"/> . <input type="text" value="5"/> . <input type="text" value="165"/>	Broadcast: 12.167.5.167
Router IP:	<input type="text" value="12.167.5.160"/>	
DNS Server:	<input type="text"/>	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

DHCP - Subnet List

Subnet	Start Range	End Range
ethernet0/0.5	12.167.5.162	12.167.5.165
ethernet0/0.19	12.167.45.163	12.167.45.165

Fig. 73: Nets – DHCP.

This page is divided into the following sections:

- (a) *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

Fig. 74: DHCP – Global DHCP Settings.

(b) Subnet DHCP Settings

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

■ Subnet DHCP Settings

Fig. 75: 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 selected interface to inform that it cannot form part of the addresses interval assigned to DHCP clients.
- **Start Range:** Indicates the initial host number to assign (the lowest) in the subnet. To do this, the address of the selected subnet is indicated.
- **End Range:** Indicates the final host number to assign (the highest) in the subnet. You are told which one is the broadcast address.
- **Router IP:** You can specify the default Gateway the client will have.
- **DNS Server:** Allows you to specify an available DNS for the client. This parameter is optional.

To store the configuration established for the Ethernet subinterface, click on *Apply*. To cancel the changes you have made and recover the information the device has, click on *Cancel*.

(c) DHCP – Subnet List

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

■ DHCP - Subnet List

Subnet	Start Range	End Range
ethernet0/0.5	12.167.5.162	12.167.5.165
ethernet0/0.19	12.167.45.163	12.167.45.165

Fig. 76: DHCP – DHCP Subnet List.

2.6.6 Routes

The first section on this page allows a user to install default routes in the device through active tunnels or ppp/direct-ip connections (in Regesta-PLC, this is usually *direct-ip*). The second section displays the RIP protocol configuration environment.

Routes Configuration

Routes Settings

Enable Default Route by PPP:

Disable

Automatic Default Route (ACAT)

Apply

RIP Settings

Interface: ppp1

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
ppp1	none	none
ppp2	none	none
gre1	rip2-multicast	none
gre2	rip2-multicast	none
gre3	rip2-multicast	none
gre4	rip2-multicast	none
17.60.12.89	none	none
12.167.45.160	none	none
12.167.2.32	none	none
20.20.20.20 (ATM Address)	rip2-multicast	none
10.18.1.100 (Tunnel Source Address)	none	none
12.167.10.82	none	none

RIP Configuration Distributed Subnets

Subnet	Mask
12.167.10.80	255.255.255.248
17.60.12.89 (Loopback Address)	255.255.255.255

Fig. 77: Nets – Routes.

(a) 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 checking the checkbox) or explicitly add a default router through the ppp/direct-ip connections (by selecting the *Enable* option).

Fig. 78: Routes – Routes Settings.

(b) *RIP Settings*

Allows you to define what type of RIP packets can be sent and what type can be received for each PPP/DIRECT-IP interface, or disable the RIP send 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.

Fig. 79: 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 Multicast*: Only accepts version 2 RIP packets.

(c) *RIP Distribute Subnet*

The different subnets going to be broadcast by RIP are defined in this section.

- *Adding and configuring a subnet*

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

Fig. 80: Routes – RIP Distribute Subnet – Adding a subnet.

- *Removing a subnet*

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

RIP Distribute Subnet

Subnets:

Subnet IP: Subnet Mask:

Fig. 81: Routes – RIP Distribute Subnet – Removing a subnet.

(d) *Remove RIP Configuration*

Lets you remove the configuration defined by RIP that the application automatically generates as you specify the data. To execute this, click on *Remove* and subsequently confirm this action.

Remove RIP Configuration

Remove RIP Configuration

Fig. 82: Routes – Remove RIP Configuration.

(e) *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
ppp1	none	none
ppp2	none	none
gre1	rip2-multicast	none
gre2	rip2-multicast	none
gre3	rip2-multicast	none
gre4	rip2-multicast	none
17.60.12.89	none	none
12.167.45.160	none	none
12.167.2.32	none	none
20.20.20.20 (ATM Address)	rip2-multicast	none
10.18.1.100 (Tunnel Source Address)	none	none
12.167.10.82	none	none

RIP Configuration Distributed Subnets

Subnet	Mask
12.167.10.80	255.255.255.248
17.60.12.89 (Loopback Address)	255.255.255.255

Fig. 83: Routes –RIP Configuration.

2.6.7 PRIME

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

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*: Enables/disables the PLC signal.
- *Topology Info Settings*: Allows you to configure parameters relative to topology file management. Said file contains

the system 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 and save).
- Specify the file name and the path where it is stored.
- IP address and port number of the FTP server.
- FTP user and password.

PRIME Interface Configuration

PRIME Settings

Local IP:

Local-port: (0..65535)

PLC Signal Settings

PLC-Signal:

Topology Info Settings

Save Topology Info

Timeout (s): (10..65535)

File Name Prefix:

File Path:

FTP Server IP:

FTP Server-Port: (0..65535)

FTP User:

FTP Password:

Fig. 84: Nets - PRIME.

Chapter 3 Configuration Recommendations

- *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 in the following way:

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

Dynamic Multipoint Virtual Private Network Configuration

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:	<input type="text"/>	(1..32 characters)

Fig. 85: DMVPN – Global Tunnel Settings.

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

- Short T Values

Advantages:

- They allow for a drop in tunnel connectivity to be detected rapidly, thereby reducing the time the device remains inaccessible.

Drawbacks:

- The traffic generated by this mechanism isn't application traffic. Therefore, the lower the frequency these packets are sent at, the more traffic is generated. Thus, the communication performance is lower.
- 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 that this mechanism is configured 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 keepalive transmission in an unreachable state.

Keepalive Stability Threshold = 3 polling packets in an unreachable state to consider that the tunnel is down.

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

- *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 better configure the parameters:

Registration Criteria Interval: A too low value will mean the device does not have enough time to connect to either of the two carriers, triggering continuous switching. To avoid this, we suggest you assign a time of more than 2 minutes.

Recovery Interval: This value must be greater than that 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: (-113..0) dBm

Threshold Interval: (0..180) minutes

Recovery Interval: (0..65535) minutes

Registration Criteria Interval: (0..180) minutes

Fig. 86: Wireless WAN –SIM Changeover Settings.