



Regesta-PRO-ER Web Interface

Teldat-Dm 478-I

Copyright© Teldat-DM478-I Version 5.1 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	5
2.1	Structure	5
2.2	Info Menu	5
2.3	Status Menu	6
2.3.1	WWAN-1 Status	7
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	ADSL	13
2.4	Logs Menu.	14
2.4.1	Traces WWAN-1	14
2.5	System Menu	15
2.5.1	Password	16
2.5.2	Settings	16
2.5.3	SNMP.	17
2.6	Nets Menu.	19
2.6.1	Interfaces	20
2.6.2	Networks	21
2.6.3	DMVPN	23
2.6.4	Wireless WAN Configuration	26
2.6.5	DHCP.	30
2.6.6	Routes	32
2.6.7	ADSL	35
Chapter 3	Configuration Recommendations	38
3.1	Keepalive mechanism in the tunnels	38
3.2	Parameters for carrier changeover	39
3.3	Configuring ADSL	39

Chapter 1 Introduction

1.1 Introduction

The web configuration is a Regesta-PRO-ER router configuration tool allowing for a quick and efficient start up.

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

1.2 Local connection to the router

The router has default factory settings installed that activate if they haven't done so before. You can access the web configurator by connecting an Ethernet cable, supplied with the router, to any of the switch ports and to the PC being used for the configuration tasks.



Fig. 1: Rear view of the Regesta-PRO-ER router. Switch ports.

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

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

<http://192.168.1.1>

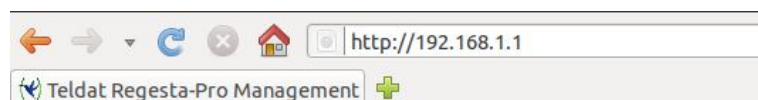



Fig. 2: Accessing the web configuration.

If the router access is correct, the web configurator home page is displayed. The format and the information it shows depend on the types of access technology present in the device.




Administrator
 User
 Password

Add to Favorites -87 dBm Orange HSDPA/HSUPA Online

Administration

Wireless Connection

Wireless Connection Status

 **Online**

As administrator you can:

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


Teldat Regesta-Pro-ER

Overview

The Regesta-Pro-ER model is a rugged equipment with an integrated dual WWAN, ADSL interface and a six-port Fast Ethernet switch.

RegestaPro-ER 1M 2PT 3G IPSEC
Web Firmware Version: 5.1.6

Fig. 3: REGESTA-PRO-ER Home page showing only the WWAN access technology.



Administrator
 User
 Password

Add to Favorites Offline

Administration

ADSL Connection

ADSL Connection Status

 **Offline**

As administrator you can:

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

Teldat Regesta-Pro-ER

Overview

The Regesta-Pro-ER model is a rugged equipment with an integrated dual WWAN, ADSL interface and a six-port Fast Ethernet switch.

RegestaPro-ER 2PT IPSEC ADSL
Web Firmware Version: 5.1.6

Fig. 4: REGESTA-PRO-ER Home page showing only the ADSL access technology.

Fig. 5: REGESTA-PRO-ER Home page showing the WWAN and ADSL access technologies.

In the bar at the top of the home page, there is a changing information text that indicates whether the device may be accessed and through which technology: WWAN / ADSL. If the device cannot be accessed, an “Offline” information message appears.

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

Fig. 7: ADSL Access.

Fig. 8: Device is inaccessible.

In the central part of the home page, a graphic appears showing the status of the characters associated to each of the access technologies present in the device. Written information can also be found on the characteristics of the web configurator and the REGESTA-PRO-ER device.

Fig. 9: Home page information – REGESTA-PRO-ER with WWAN access only.

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



Fig. 10: Device model and the Web firmware version installed.

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

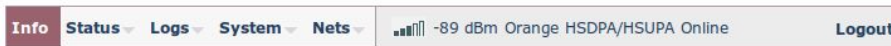
 A rectangular login form with a white background and a thin gray border. At the top left, the word 'Administrator' is written in a bold, dark blue font. Below it, there are two input fields: the first is labeled 'User' and the second is labeled 'Password'. Both labels are in a bold, dark blue font. Below the 'Password' field is a button labeled 'Log in' in a bold, dark blue font.

Fig. 11: 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 or others.



Fig. 12: Access through the “root” level.



Access through the “configuration” level.



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): allows you to browse through the different configurator pages.
- **Status bar** (orange): shows whether the device is accessible and through which technology.
- **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 that allows him to configure or monitor the different router characteristics.

The screenshot shows the Teldat web interface. At the top left, a purple box highlights the system information: Host: REGESTA_3G_1M, Date: Monday, 03/12/12, Time: 17:08:15, Uptime: 10m18s. The Teldat logo is in the top right. Below the logo is a navigation bar with a red box around 'Info', 'Status', 'Logs', 'System', and 'Nets' menus, an orange box around the signal strength and connection status '-93 dBm movistar HSDPA/HSUPA Online', and a green box around the 'Logout' button. The main content area is titled 'System Information' and contains a table with the following data:

Router Software version:	10.08.25.05.05 Mar 7 2012 14:51:08
MAC:	00A0269E003E
Router Model:	RegestaPro-ER 1M 3G IPSEC ADSL 27 20
Processor:	96369RP6xER PCB:0x241 CHIP_ID:0x6368 REV:0xB0
Serial number:	754/00131

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

Fig. 15: Page structure.

The screenshot shows the Teldat application disconnection page. At the top is the Teldat logo. 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 "RegestaPro-ER 1M 3G IPSEC ADSL".

Fig. 16: Application disconnection page.

2.2 Info Menu

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

The screenshot shows the 'Info' page. At the top is the Teldat logo. 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 "RegestaPro-ER 1M 3G IPSEC ADSL". The main content area is titled 'System Information' and contains a table with the following data:

Router Software version:	10.08.25.05.05 Mar 7 2012 14:51:08
MAC:	00A0269E003E
Router Model:	RegestaPro-ER 1M 2G IPSEC ADSL 27 18
Processor:	96369RP6xER PCB:0x241 CHIP_ID:0x6368 REV:0xB0
Serial number:	754/00131

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

Fig. 17: "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-PRO-ER 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:** allows you to save the changes made in the router configuration.
- **Reboot button:** allows the user to reboot the router from the web. On clicking on this button, the user is automatically logged out and 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.

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

**Note**

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

From this home page, and depending on the 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

Allows you to access information on several aspects of the router status. This menu varies depending on the number of 2G/3G/LTE modules the device has and on whether the module has an ADSL interface or not.

Fig. 18: Status Menu – REGESTA-PRO-ER with 1 2G/3G/LTE module and without ADSL.

Fig. 19: Status Menu – REGESTA-PRO-ER without 2G/3G/LTE modules, only ADSL technology.

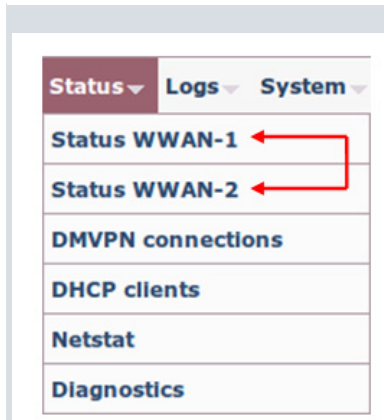


Fig. 20: Status Menu – REGESTA-PRO-ER with 2 2G/3G/LTE modules and without ADSL.

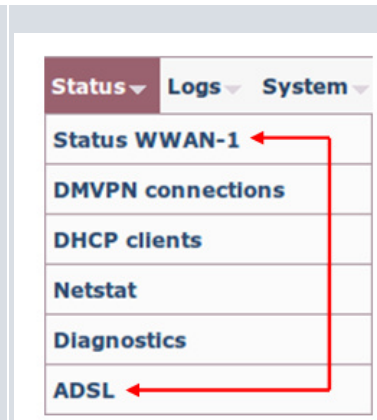


Fig. 21: Status Menu – REGESTA-PRO-ER with 1 2G/3G/LTE module and with ADSL technology.

2.3.1 WWAN-1 Status

Displays a summary on the parameters that characterize the cellular interface for module 1. This menu option remains hidden in REGESTA-PRO-ER devices that do not have WWAN technology.

WWAN-1 Connection Status

■ **Connection**

Register:	Home network
Operator:	21401
Technology:	HSDPA/HSUPA
Level(dBm):	-75

■ **Cells**

	UARFCN	PSC	ECIO(-dBm)	RSCP(-dBm)
Serving Cell:	10713	378	8.5	76
Neighbour 1:	10713	376	11.0	78
Neighbour 2:	10713	382	20.5	87
Neighbour 3:	10713	383	11.5	78

■ **Module Information**

Manufacturer:	Sierra Wireless, Incorporated
Model:	MC8705
Firmware:	T3_5_4_1AP R604 CNSZXD00000155 2013/03/15 10:05:05
IMEI:	353567043227504
IMSI:	214019816249848
SIM Card ID:	8934569821305399747F

■ **IP Protocol**

Assigned IP:	47.59.16.77
--------------	-------------

Fig. 22: Status –WWAN-1 Status.

This page is divided into four sections:

2.3.1.1 Connection

This provides information on the status of the radio link and on network registration.

■ Connection

Register:	Home network
Operator:	21401
Technology:	HSDPA/HSUPA
Level(dBm):	-75

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

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

- **MCC (Mobile Country Code):** Code assigned to Spain within the mobile network (214).
- **MNC (Mobile Network Code):** Carrier code.
- **LAC (Location Area Code):** Local area code for the serving cell/neighbor in decimal.
- **CellID:** Serving cell/neighbor in decimal identifier.
- **BSIC (Base Station Identity Code):** Base station identifier.
- **ARFCN (Absolute Frequency Channel Number):** Selected channel number.
- **RX (-dBm):** Signal reception level.

2.3.1.2.2 Example of 3G Connection

■ Cells

	UARFCN	PSC	ECIO(-dBm)	RSCP(-dBm)
Serving Cell:	10713	378	8.5	76
Neighbour 1:	10713	376	11.0	78
Neighbour 2:	10713	382	20.5	87
Neighbour 3:	10713	383	11.5	78

Fig. 25: 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.

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

2.3.1.3 Module Information

Displays information on the module.

■ **Module Information**

Manufacturer:	Sierra Wireless, Incorporated
Model:	MC8705
Firmware:	T3_5_4_1AP R604 CNSZXD00000155 2013/03/15 10:05:05
IMEI:	353567043227504
IMSI:	214019816249848
SIM Card ID:	8934569821305399747F

Fig. 27: 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 ID:** ID of the SIM installed in the router.

2.3.1.4 IP Protocol

Displays the IP dynamically assigned by the carrier.

■ IP Protocol	
Assigned IP:	47.59.16.77

Fig. 28: Status WWAN-1 – IP Protocol.



Note

In a two-module REGESTA-PRO-ER router, the page corresponding to module 2 is accessible through the WWAN-2 Status menu and contains the same information as for module 1.

2.3.2 DMVPN connections

This page 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. 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 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-PRO-ER device'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

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 the *Refresh* button to update the list.

2.3.4 Netstat

This page displays the following information in table format:

2.3.4.1 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. 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	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. 32: Status – Netstat – List of TCP connections.

2.3.4.3 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. 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)	
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. 34: Status – Netstat – Routing Table.

2.3.5 Diagnostics

This executes the *ping* operation, which can determine if the device accessed a given IP address. Additionally, you can execute the *traceroute* operation from the device and check the hops required to reach a certain *router/host*.

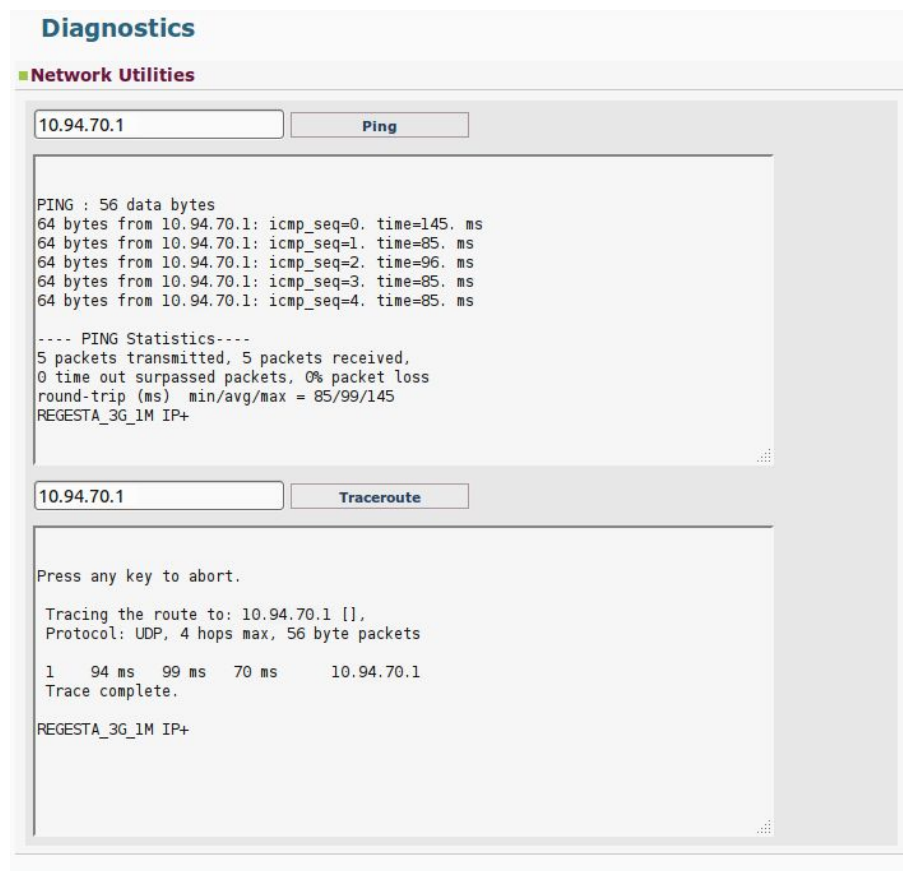


Fig. 35: Status – Diagnostics – Ping – Traceroute.

2.3.6 ADSL

This option on the *Status* menu is only accessible when dealing with a REGESTA-PRO-ER model with an ADSL interface. The option is hidden for all other models.

This page allows you to monitor device synchronization using the DSLAM. The following information appears:

- **Signal Parameters**

- **Operational Mode:** displays the operating mode used to reach synchronization. In cases where there is no synchronization, the “*NOT CONNECTED*” message appears.
- **Noise Margin (dB):** indicates the noise margin measured by the ATU-C (DSLAM) and the ATU-R (REGESTA-PRO-ER).
- **Attenuation (dB):** indicates the subscriber’s loop length. The greater the attenuation, the lower the negotiated Upstream/Downstream rate.
- **Output Pwr (dBm):** displays the transmission power.
- **Attainable Rate (bps):** indicates the maximum rate that can be achieved under current conditions. It does not include the available data speed.

- **Channel Parameters:** displays the Upstream/Downstream rates negotiated in synchronization.

ADSL Status

Signal Parameters

Operational Mode: **ANSI T1.413**

	ATU-C	ATU-R
Noise Margin (dB):	+ 6.0	+22.4
Attenuation (dB):	1.5	0.0
Output Pwr (dBm):	+ 7.3	+11.8
Attainable Rate (bps):	12680000	1192000

Channel Parameters

	Fast channel		Interleaved channel	
	Downstream	Upstream	Downstream	Upstream
Current Transmit Rate (bps):	0	0	7616000	992000

Fig. 36: Status – ADSL.

2.4 Logs Menu

Accesses pages where you can see the evolution of the status for the device's 2G/3G/LTE modules. This menu varies depending on the number of modules present in the device. It remains hidden for those devices that do not have WWAN technology.

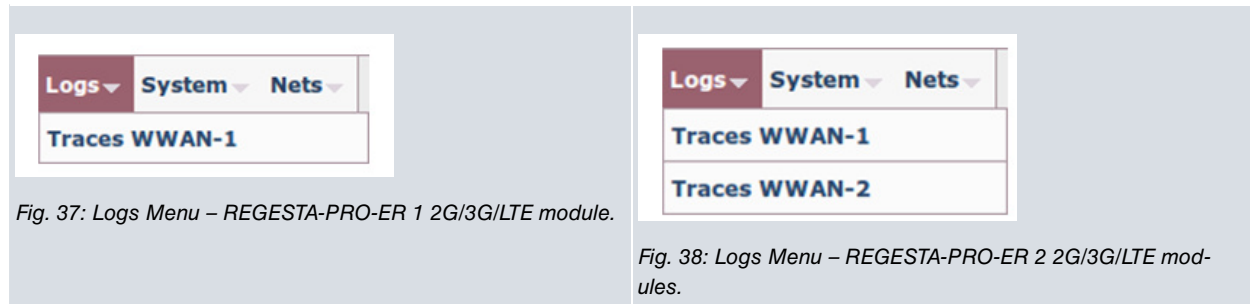


Fig. 37: Logs Menu – REGESTA-PRO-ER 1 2G/3G/LTE module.

Fig. 38: Logs Menu – REGESTA-PRO-ER 2 2G/3G/LTE modules.

2.4.1 Traces WWAN-1

This page displays the information associated to the router's 2G/3G/LTE 1 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. 39: Logs – Traces WWAN-1.

This is divided into two sections:

2.4.1.1 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. 40: Traces WWAN-1 – WWAN-1.

- **Module Manufacturer.**
- **Module Model.**
- **Module Firmware:** Module 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.

■ Modem diagnostics	
<pre> 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,HSOPA/HSUPA OK AT+RSCP?;+ECIO?;+UPSC?;!GSTATUS?;!GSMINFO?;+USET?;+USET?1 +RSCP: RSCP: -76 dBm +ECIO: Tot Ec/Io: -8.5 dB </pre>	<div style="border: 1px solid gray; padding: 2px; display: inline-block;">Modem status</div>

Fig. 41: Traces WWAN-1 – Modem diagnostics.



Note

In a two module REGESTA-PRO-ER, the page corresponding to module 2 can be accessed through the Traces WWAN-2 menu. This contains the same information as for module 1.

2.5 System Menu

Allows you to configure the router's general parameters.

System ▾	Nets ▾	Signal strength: -73
Password		
Settings		
SNMP		

Fig. 42: 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. 43: 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.

Fig. 44: System – Password.

2.5.2 Settings

Here you can configure various general parameters in the system.

Fig. 45: System – Settings.

2.5.2.1 System Settings

System parameters.

- **Host Name:** Router name.

2.5.2.2 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.

2.5.2.3 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 recoup the data the router has, click on the *Cancel* button.

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:

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. 46: 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 executed modifications, click on the *Cancel* button.

The screenshot shows the 'Hosts' configuration interface. At the top, there is a 'Hosts:' section with a dropdown menu currently displaying '-- New Host --'. Below this is the 'Host Configuration' section, which contains four input fields: 'IP Address' (12.165.2.28), 'UDP Port' (162), 'Send Standard Traps' (Yes), and 'Send Enterprise Traps' (No). At the bottom right of the configuration section are 'Apply' and 'Cancel' buttons.

Fig. 47: SNMP – Hosts – Adding and configuring a host.

2.5.3.1.2 Editing a host configuration

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

If you wish 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' configuration interface. The 'Hosts:' section now has a dropdown menu displaying '12.165.2.20' and a 'Remove' button next to it. The 'Host Configuration' section has been updated: 'IP Address' is 12.165.2.20, 'UDP Port' is 162, 'Send Standard Traps' is Yes, and 'Send Enterprise Traps' is Yes. 'Apply' and 'Cancel' buttons are still present at the bottom right.

Fig. 48: SNMP – Hosts – Editing the configuration for a host.

2.5.3.1.3 Removing a host

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

The screenshot shows the 'Hosts' configuration interface. The 'Hosts:' section has a dropdown menu displaying '12.165.2.20' and a 'Remove' button next to it. The rest of the page content is not visible in this specific screenshot.

Fig. 49: SNMP – Hosts – Remove a host.

2.5.3.2 Community Subnet

This section 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' configuration interface. At the top, there is a 'Subnets:' section with a dropdown menu currently displaying '-- New Subnet --'. Below this are two input fields: 'Subnet IP' (12.165.2.144) and 'Subnet Mask' (255.255.255.254). At the bottom right is an 'Add' button.

Fig. 50: 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.

■ **Community Subnet**

Subnets:

Subnet IP: Subnet Mask:

Fig. 51: SNMP – Community Subnet – Removing a subnet.

2.5.3.3 Host List

There is a list at the end of the page showing the *hosts* that have been already configured so that the user can view the *hosts* the device sends the 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. 52: 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.

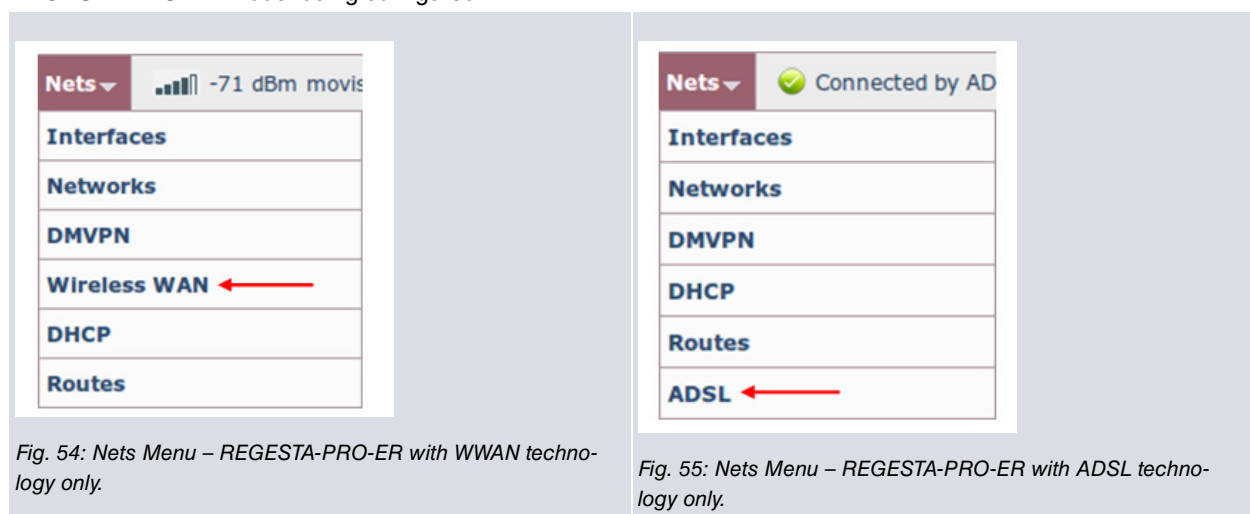
■ **Subnets List**

Subnet	Mask
12.165.2.0	255.255.255.0

Fig. 53: SNMP – Subnets List.

2.6 Nets Menu

Allows you to configure the router's network parameters. It is a variable menu whose options depend on the REGESTA-PRO-ER model being configured.



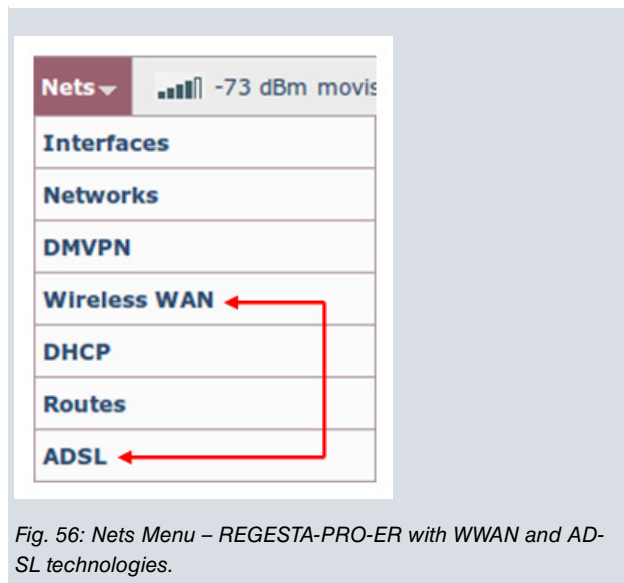


Fig. 56: Nets Menu – REGESTA-PRO-ER with WWAN and ADSL technologies.

2.6.1 Interfaces

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

Fig. 57: Nets – Interfaces.

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 the ATM subinterface (if the device has ADSL technology) by selecting the base interface from the pull-down menu and specifying an identifier.

Fig. 58: Interfaces – Interface Configuration –Ethernet Subinterfaces.

Fig. 59: Interfaces – Interface Configuration –GRE Tunnels.

Fig. 60: Interfaces – Interface Configuration –ATM Subinterface.

2.6.1.2 VLAN configuration

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

2.6.1.2.1 Adding and configuring a VLAN

To do this, select the interface in 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.

The screenshot shows a web interface titled "VLAN Configuration". It features a dropdown menu for "VLAN:" with "ethernet0/0.5" selected. To the right, under "Ports:", there are six checkboxes labeled 1 through 6. Checkboxes 1, 2, and 6 are checked, while 3, 4, and 5 are unchecked. At the bottom right, there are two buttons: "Apply" and "Cancel".

Fig. 61: 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/un-checking the ports, click on the *Apply* button.

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.

The screenshot shows the same "VLAN Configuration" interface. The "VLAN:" dropdown is still set to "ethernet0/0.5". In the "Ports:" section, checkboxes 1, 2, 5, and 6 are checked, while 3 and 4 are unchecked. The "Apply" and "Cancel" buttons are visible at the bottom right.

Fig. 62: Interfaces – VLAN configuration – Editing the configuration for a VLAN.

2.6.1.3 Remove Interfaces

This section 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 the *Remove* button.

The screenshot shows a web interface titled "Remove Interfaces". It features a dropdown menu for "Interface:" with "gre1" selected. To the right of the dropdown is a button labeled "Remove".

Fig. 63: Interfaces – Remove Interfaces.

2.6.2 Networks

Here you can define the IP addresses for each of the interfaces and subinterfaces 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. 64: Nets – Networks.

This page is divided into the following sections:

2.6.2.1 Network Settings

Allow 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 the *Apply* button to save any changes made.

The *Cancel* button gives you the opportunity 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. 65: Networks – Networks Settings.

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

Additionally, this section offers the possibility 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 the “Delete IP Address” button.

The screenshot shows the 'Network Settings' section. It features a dropdown menu for 'Network' set to 'ethernet0/0'. Below it are input fields for 'IP Address' (192.168.1.1) and 'Netmask' (255.255.255.0). A 'Delete IP Address' button is positioned to the right of the network dropdown. At the bottom right, there is a 'Secondary IP Addresses' button.

Fig. 66: Networks – Networks Settings – Removing the default IP address.

2.6.2.2 Traffic Control Settings

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

The screenshot shows the 'Traffic Control Settings' section. It contains a single checkbox labeled 'Enable Routing Traffic Control', which is currently checked. An 'Apply' button is located at the bottom right of the section.

Fig. 67: 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.

The screenshot shows the 'Loopback Settings' section. 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 at the bottom right.

Fig. 68: 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-PRO-ER) 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 of the HUBs that intervene 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. 69: Nets – DMVPN.

2.6.3.1 Global Tunnel Settings

Here, the user configures the general parameters applicable to the GRE tunnel that the REGESTA-PRO-ER 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. 70: 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.
 - **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 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 REGESTA-PRO-ER devices to be identified by a *pre-shared key*

and by a device identifier. 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 (Figure 72).

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

Fig. 71: DMVPN – Global Tunnel Settings – IPsec Mode: Main.

Fig. 72: DMVPN – Global Tunnel Settings – IPsec Mode: Aggressive.

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

2.6.3.2 Hub Settings

In this section, you configure the parameters that define each one of the Hubs.

Fig. 73: 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 option corresponds to the *Point-To-Point* protocol established with the carrier assigned to the SIM1, while the PPP2 option corresponds to the *Point-To-Point* protocol established with the carrier 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.
- **Key:** Key used in GRE tunnels to distinguish the tunnel to which an 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 the *Apply* button. To cancel the changes you have made and recover the information that the device has on this HUB, click on the *Cancel* button.



Note

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

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 cellular interfaces belonging to modules 2G/3G/LTE and you define the connection parameters for the network.

Wireless WAN Configuration

Primary SIM Settings

Phone Number:

PIN Code:

APN:

APN username:

APN password:

Network mode:

Secondary SIM Settings

Phone Number:

PIN Code:

APN:

APN username:

APN password:

Network mode:

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. 74: Nets – Wireless WAN (Regesta-PRO-ER 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.

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="operador1.es"/>
APN username:	<input type="text"/>
APN password:	<input type="text"/>
Network mode:	<input type="text" value="UMTS/HSDPA"/>

Fig. 75: Wireless WAN – Primary SIM Settings.

When registering a mobile device, some operator LTE 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 must be configured:

Network mode:	<input type="text" value="LTE"/>
---------------	----------------------------------

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. 76: 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 the SIM1).

Secondary SIM Settings

Phone Number:

PIN Code:

APN:

APN username:

APN password:

Network mode:

Fig. 77: Wireless WAN – Secondary SIM Settings.

2.6.4.3 SIM Changeover Settings

In this section, you can define 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. 78: 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. 79: 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="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. 80: 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="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. 81: 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 defined mobile telephone carriers is the main one 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.	

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:** Recovery Interval. Specifies the maximum time, in minutes, that the backup SIM is used (SIM2). After this times out, changeover to the main SIM occurs.
- **Registration Criteria Interval:** Specifies the maximum time admitted, in minutes, that the interface can be unregistered. When this interval times out, carrier changeover executes.

Switch parameters with a 2G connection

- **RSSI Threshold:** (Received Signal Strength Indicator). When the RSSI 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 y Threshold Interval:** The coverage is given 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 and Threshold Interval:** The coverage is given by RSCP in dBm and by RSQR 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

Allows you to configure the device's DHCP server.

DHCP Server Configuration

Global DHCP Settings

DHCP:

Maximum Lease Time: (1s..3550w5d3h14m7s)

Subnet DHCP Settings

Interface:

IP Address:

Start Range: . . . Network: 12.167.5.160

End Range: . . . Broadcast: 12.167.5.167

Router IP:

DNS 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. 82: Nets – DHCP.

This is divided into the following sections:

2.6.5.1 Global DHCP Settings

Define 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:

Maximum Lease Time: (1s..3550w5d3h14m7s)

Fig. 83: DHCP – Global DHCP Settings.

2.6.5.2 Subnet DHCP Settings

You can assign specific configuration options to each Ethernet subinterface defined in the router with the aim of defining and identifying groups of clients. The parameters that need to be configured are as follows:

Subnet DHCP Settings

Interface:

IP Address:

Start Range: . . . Network: 12.167.5.160

End Range: . . . Broadcast: 12.167.5.167

Router IP:

DNS Server:

Fig. 84: 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 ad-

addresses interval assigned to the DHCP clients.

- **Start Range:** Indicates the initial host number that is ready to be assigned (the lowest) in the subnet. To do this, the address of the selected subnet is indicated.
- **End Range:** Indicates the final host number that is ready to be assigned (the highest) in the subnet. To do this, the broadcast address is indicated.
- **Router IP:** Enables you to 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 the *Apply* button. To cancel the changes you have made and recover the information that the device has, click on the *Cancel* button.

2.6.5.3 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. 85: DHCP – DHCP Subnet List.

2.6.6 Routes

Allows the user to install default routes in the device (through active tunnels or ppp/direct-ip connections), and then 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. 86: 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 checking the checkbox) or explicitly add a default router through the ppp/direct-ip connections (by selecting the *Enable* option).

Routes Settings

Enable Default Route by PPP:

Disable

 Automatic Default Route (ACAT)

Apply

Fig. 87: Routes – Routes Settings.

2.6.6.2 RIP Settings

Allow you to define what type of RIP packets can be sent and what type can be received for each PPP/DIRECT-IP and GRE 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. 88: 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 the RIP packet sending in the interface.
 - **RIP-2 Multicast:** The 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 in the pull-down menu, indicate its IP address and the subnet mask and click on the *Add* button.

Fig. 89: 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.

Fig. 90: Routes – RIP Distribute Subnet – Removing a subnet.

2.6.6.4 Remove RIP Configuration

This option lets you remove all the configuration defined by RIP (except for the part associated to an ADSL scenario that the application automatically generates as you specify the data). To execute this, you need to click on the *Remove* button and subsequently confirm this action.

Remove RIP Configuration

 Remove RIP Configuration

Fig. 91: 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 the reception parameters to be used in interfaces and the 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. 92: Routes –RIP Configuration.

2.6.7 ADSL

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

On this page, the user can configure the ADSL interface specifying the following parameters:

- **ADSL Scenario:** The REGESTA-PRO-ER can be configured to operate with DSLAM ATM and DSLAM IP devices. The user must specify which scenario is going to be configured and, should the second scenario be selected, the IP address for the second hop in the GRE tunnel routes must be indicated (i.e. the IP address for the DSLAM IP device's ATM interface).
- **WAN IP Address:** The ADSL interface's IP address and the subnet mask are configured here.
- **Open Mode Configuration:** Through a pull-down menu, you can configure the connection standard you are going to use.
- **Alternative Open Modes Configuration:** You can configure up to a maximum of four alternative open modes to use in cases where an error occurs using the previously defined standard connection. There is a pull-down menu for each fallback.
- **Peak Cell Rate Configuration:** You can define the peak rate in Kbps through this parameter.
- **Tunnels Source Address:** This specifies the source IP address for the GRE tunnels.

ADSL Configuration

ADSL Scenario

ATM-DSLAM Scenario

IP-DSLAM Scenario

WAN IP Address

IP Address:

Netmask:

Open Mode Configuration

Open Mode:

Recommended option: "g.dmt.bis-plus"

Alternative Open Modes Configuration

Fallback 1:

Recommended option: "ansi-t1.413"

Fallback 2:

Fallback 3:

Fallback 4:

Peak Cell Rate Configuration

Peak Cell Rate: (1..4194303) kbps

Tunnels Source Address

IP Address:

Fig. 93: Nets –ADSL – DSLAM ATM.

ADSL Configuration

ADSL Scenario

ATM-DSLAM Scenario

IP-DSLAM Scenario

Next Hop IP Address:

WAN IP Address

IP Address:

Netmask:

Open Mode Configuration

Open Mode:

Recommended option: "g.dmt.bis-plus"

Alternative Open Modes Configuration

Fallback 1:

Recommended option: "ansi-t1.413"

Fallback 2:

Fallback 3:

Fallback 4:

Peak Cell Rate Configuration

Peak Cell Rate:

(1..4194303) kbps

Tunnels Source Address

IP Address:

Fig. 94: Nets –ADSL – DSLAM IP.

Chapter 3 Configuration Recommendations

3.1 Keepalive mechanism in the tunnels

Determines the time (T) that 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:

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

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. 95: DMVPN – Global Tunnel Settings.

To find out what values you should select, you need to 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 at which these packets are sent, the higher the traffic generated. Thus, the communication performance is lower.

- In low speed channels (GPRS), if there is a traffic peak, chances are *keepalive* packets are not arriving on time. This causes 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 the communication performance.

- The presence of traffic peaks and small connection instabilities does 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 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 causing false tunnel drops due to peaks of traffic. However, you must remember that the device can dynamically change the type of cellular network it is connected to at any point.

Since ADSL scenarios represent high-speed connections, you can reduce the T value so the device reacts faster to a drop in a tunnel.

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 better configure the parameters:

- **Registration Criteria Interval:** A too lower value will mean that the device does not have enough time to connect to either of the two carriers, thus provoking a situation of continuous switching. To avoid this scenario, 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.

Fig. 96: Wireless WAN –SIM Changeover Settings.

3.3 Configuring ADSL

In any scenario, an inappropriate configuration can mean that the device will not operate correctly. For this reason, we have put forward some recommendations to follow when configuring an ADSL scenario.

- Both the IP address for the ADSL interface, as well as the source IP address for the tunnels (if there are any), are data that must be provided by the ADSL access provider and whose correct configuration is vital to establish the data connection.

Fig. 97: ADSL Configuration – WAN IP Address.

Tunnels Source Address

IP Address	<input type="text"/>
------------	----------------------

Fig. 98: ADSL Configuration – Tunnels Source Address.

- The device's operating environment may include DSLAMs that do not support certain open modes. For this reason, we recommend including fallbacks (alternative open modes in case of error) in the configuration.

Alternative Open Modes Configuration

Fallback 1	<input type="text" value="none"/>	Recommended option: "ansi-t1.413"
Fallback 2	<input type="text" value="none"/>	
Fallback 3	<input type="text" value="none"/>	
Fallback 4	<input type="text" value="none"/>	

Fig. 99: ADSL Configuration – Alternative Open Modes Configuration.