REGESTA Web Configuration

Teldat-Dm 452-I

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.

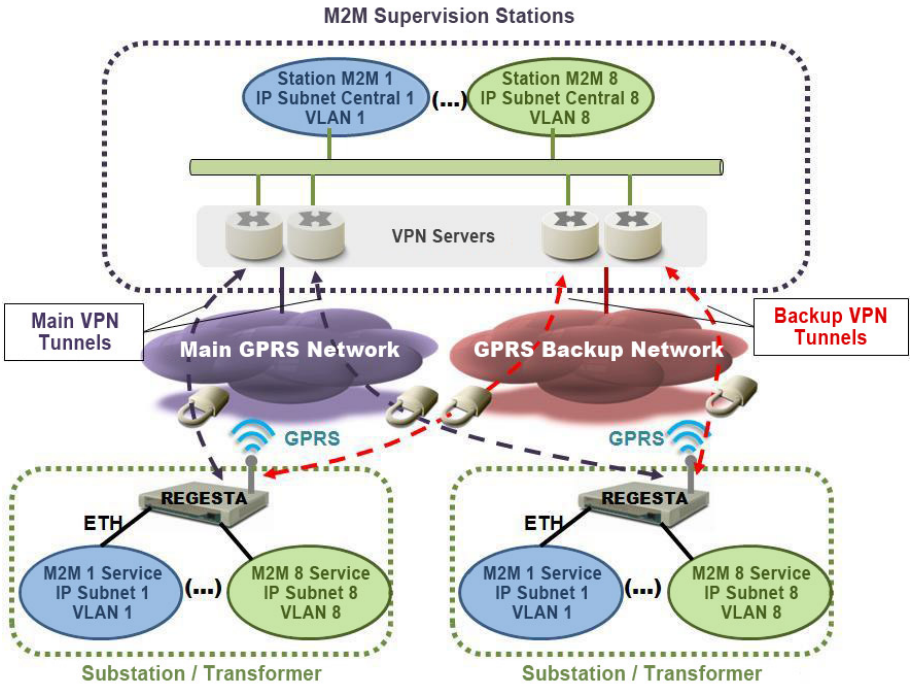
Table of Contents

Chapter 1 Introduction

Web configuration is a configuration tool available in the Regesta device for a quick and efficient start-up.

The web configurator is prepared to automate the configuration taking into consideration the device's work scenario. The essential configuration parameters are accessible through the web. The remaining parameters, hidden from the user, can be adjusted so that the system operates better. The criteria used for this adjustment is the speed of the Regesta connection to the central terminator devices and the speedy detection of connection drops with the terminators.

The application scenario for the Regesta device is as follows:



The Regesta-RP81 device establishes two IPSec+GRE tunnels with the terminator routers through the GPRS carrier in the first option. Both tunnels allow for two DMVPNs to be established (one as main and the other as backup). In cases where the GPRS carrier drops, the device switches to the backup carrier, again establishing two IPSec+GRE tunnels with the terminator routers.

When it comes to the Regesta-RP82, the device maintains GPRS connections with both carriers and establishes two IPSec+GRE tunnels with each carrier respectively. This configuration reduces the device response time in the event of carrier and/or terminal router problems.

Chapter 2 Local connection to the device

The router leaves the factory with a default configuration. Access to the web configurator is carried out by connecting the Ethernet cable, which is supplied with the device, to one of the switch ports and to the PC used for configuration tasks.

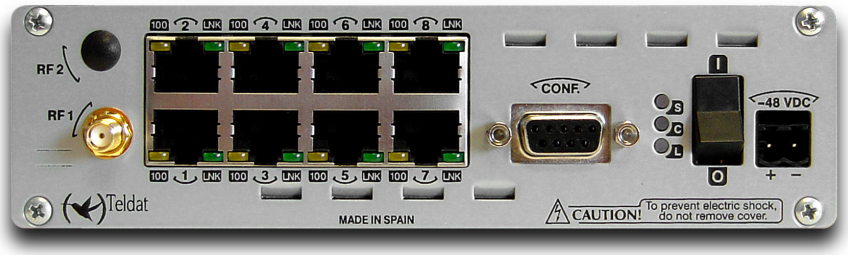


Fig. 2: Regesta RP-81 rear panel. Switch ports.

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 subnet configured (192.168.1.0/24).

Once IP access to the device has been guaranteed, the following URL is entered in a web browser.

http://192.168.1.1

If the access to the device is correct, a screen will appear asking for the user name and the password. The factory settings take “admin” as user and “teldat” as password .

Fig. 3: Login/Password screen.

Once the data has been entered, you can access the main web configurator page.

Chapter 3 Menu Information

This provides the general router information.

Firmware: Device firmware version.

MAC: Ethernet physical address.

Device: Name of the device.

Processor: Processor.

Board: Device hardware.

S/N: Device serial number.

Fig. 4: Main page to access the configuration.

Contains the information needed to enter the device configuration pages. The following sections describe the configuration/monitoring screens in the order in which they appear on the main page access bar.

Chapter 4 Graphs Menu

Shows the different graphics with monitoring information on the GPRS signal level and the incoming and outgoing traffic in the different interfaces.

The interfaces that the device handles are known as:

- *br-<network>*. Each network configured in *Bridged* mode is associated to a bridge interface named *br-<network>*, where *<network>* is the name of the network. E.g. if you configure a network with the name *lan* and type *Bridged*, the associated interface would be called *br-lan*.
- *eth<portid>*. Each switch port has an interface associated with the name *eth<portid>*, where *<portid>* is the identifier for the said port. Port 1 has the interface *eth0* associated, port 2 interface *eth1* and so on.
- *eth<portid>.<vlanid>*. Each VLAN configured in a port has an interface associated named *eth<portid>.<vlanid>*, where *<portid>* is the port identifier and *<vlanid>* is the VLAN identifier.
- *gre<tunnelid>*. Each DMVPN tunnel has an interface associated with the name *gre<tunnelid>*, where *<tunnelid>* is the tunnel identifier.
- *PPP<pppid>.* Each PPP interface has an identifier associated. PPP0 and/or PPP1 interfaces are available in the device.
- *lo*. The loopback interface is known as *lo*.

4.1 GPRS RSSI: RSSI level in the antenna

This graph shows the evolution of the RSSI level in the antenna every 30 seconds.

Note

The RSSI values that are above -93 dBm indicate that the device is located in a good coverage zone. Values between -93 dBm and -104 dBm indicate that the device is located in a low coverage area. Whenever values below -105 dBm appear, the device is in a critical zone where connection to the network cannot be guaranteed.

When it comes to the Regesta-RP81, there is only one GPRS radio interface. Consequently, you can access a single signal level monitoring graph.

When it comes to the Regesta-RP82, there are two GPRS radio interfaces. In this case you have two monitoring graphs, one for each radio interface respectively.

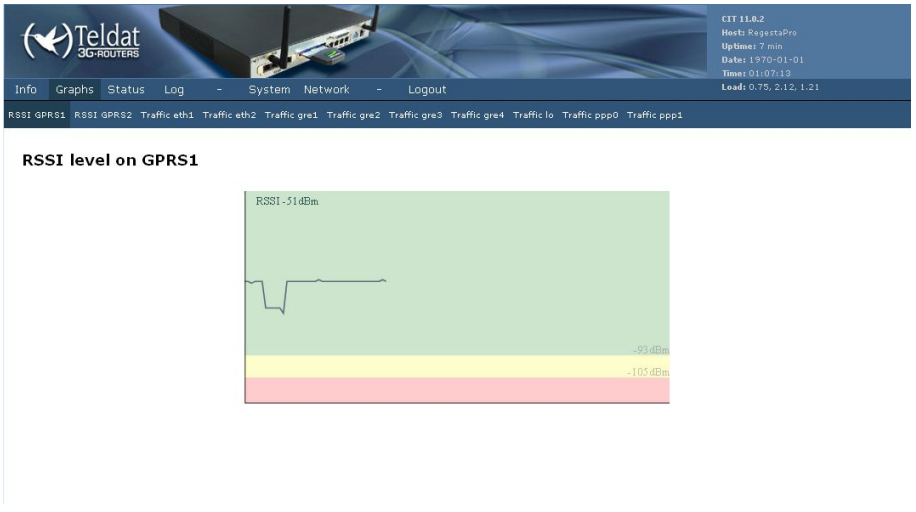


Fig. 5: Monitoring the signal level in the antenna.

4.2 Traffic: Traffic in the interface

Each graph displays information on the traffic being processed by an interface.

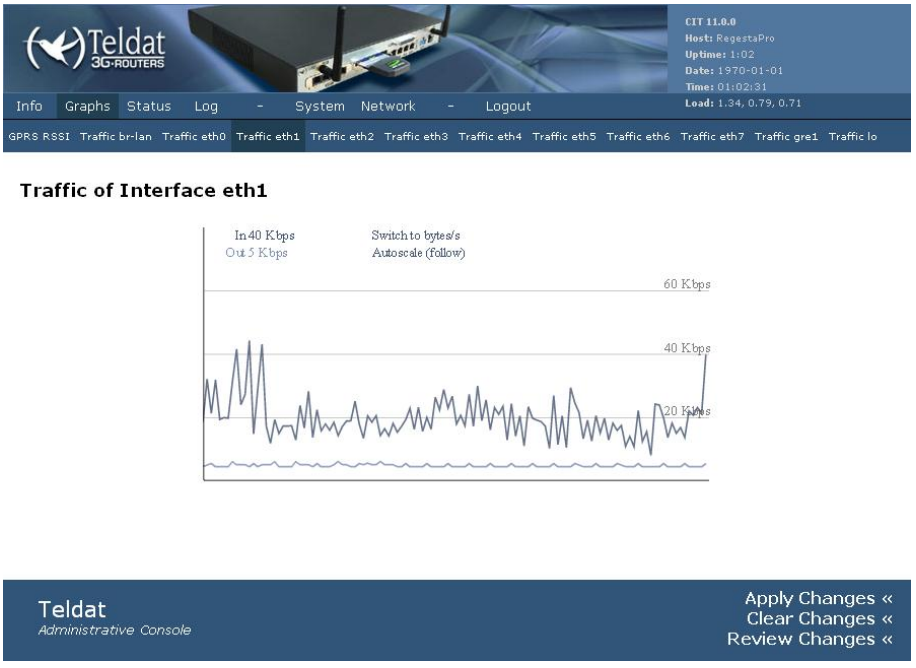


Fig. 6: Traffic entering/exiting through interface eth1.

There are different types of interfaces in the device, each with their corresponding nomenclature. These interfaces are as follows:

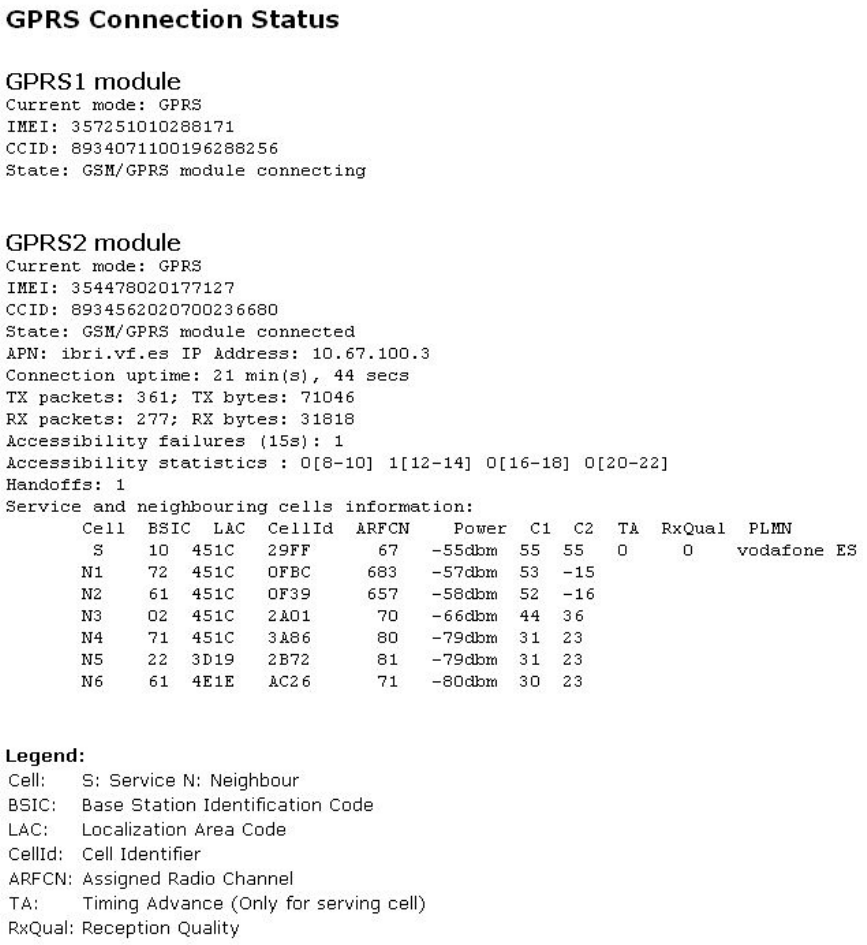
- *br-<network>*. Each network configured in *Bridged* mode is associated to a bridge interface named *br-<network>*, where *<network>* is the name of the network. E.g. if you configure a network with the name *lan* and type *Bridged*, the associated interface would be called *br-lan*. The traffic displayed in this graph corresponds to the packets routed by the device (not those bridged between different bridge ports).
- *eth<portid>*. Each switch port has an interface associated with the name *eth<portid>*, where *<portid>* is the identifier for the said port. Port 1 has the interface *eth0* associated, port 2 interface *eth1* and so on. The traffic displayed in this graph corresponds to the packets entering and leaving through the port in question.
- *eth<portid>.<vlanid>*. Each VLAN configured in a port has an interface associated named *eth<portid>.<vlanid>*, where *<portid>* is the port identifier and *<vlanid>* is the VLAN identifier. The traffic displayed in this graph corresponds to the packets entering and leaving through the port in question, tagged with the VLAN identifier *<vlanid>*.
- *gre<tunnelid>*. Each DMVPN tunnel has an interface associated with the name *gre<tunnelid>*, where *<tunnelid>* is the tunnel identifier. The traffic displayed in this graph corresponds to the packets entering and leaving through this tunnel.
- *lo*. The loopback interface is known as *lo*. This is not associated to any physical interface, and is only used for determined management tasks.
- *ppp<pppid>*. The protocol used to access the GPRS network is PPP. Each GPRS module has a PPP interface associated known as *ppp<pppid>*, where *<pppid>* is the module identifier. The traffic displayed in this graph corresponds to the packets entering and leaving through this module.

Chapter 5 Status Menu

You can access information on the different state aspects of the device through the *Status* menu.

5.1 GPRS

This screen is a summary on the parameters characterizing the GPRS interface.



GPRS Connection Status

GPRS1 module

```
Current mode: GPRS
IMEI: 357251010288171
CCID: 8934071100196288256
State: GSM/GPRS module connecting
```

GPRS2 module

```
Current mode: GPRS
IMEI: 354478020177127
CCID: 89345620207002366 80
State: GSM/GPRS module connected
APN: ibri.vf.es IP Address: 10.67.100.3
Connection uptime: 21 min(s), 44 secs
TX packets: 361; TX bytes: 71046
RX packets: 277; RX bytes: 31818
Accessibility failures (15s): 1
Accessibility statistics : 0[8-10] 1[12-14] 0[16-18] 0[20-22]
Handoffs: 1
Service and neighbouring cells information:
```

Cell	BSIC	LAC	CellId	ARFCN	Power	C1	C2	TA	RxQual	PLMN
S	10	451C	29FF	67	-55dbm	55	55	0	0	vodafone ES
N1	72	451C	OFBC	683	-57dbm	53	-15			
N2	61	451C	OF39	657	-58dbm	52	-16			
N3	02	451C	2A01	70	-66dbm	44	36			
N4	71	451C	3A86	80	-79dbm	31	23			
N5	22	3D19	2B72	81	-79dbm	31	23			
N6	61	4E1E	AC26	71	-80dbm	30	23			

Legend:

Cell: S: Service N: Neighbour
BSIC: Base Station Identification Code
LAC: Localization Area Code
CellId: Cell Identifier
ARFCN: Assigned Radio Channel
TA: Timing Advance (Only for serving cell)
RxQual: Reception Quality

Fig. 7: Summary on the GPRS interface parameters.

- *Current Mode*

  Displays the type of connection used by the device. Regesta only admits GPRS.

- *IMEI*

  International Mobile Equipment Identity for the device's GPRSx module.

- *CCID*

  Integrated Circuit Card ID for the SIM installed in the device.

- *State*

  Displays the state of the device connection to the GPRS network.

  The device can be in one of the following states:

  (1) "GSM/GPRS module Power down",

  (2) "GSM/GPRS module Power up",

  (3) "Initializing GSM/GPRS module",

  (4) "GSM/GPRS module waiting data call",

(5) "GSM/GPRS module connecting",

(6) "GSM/GPRS module connected",

(7) "GSM/GPRS switching to GPRS",

(8) "GSM/GPRS module disconnected",

(9) "GSM/GPRS module halted",

(10) "GSM/GPRS module idle",

- *APN*

  Displays the APN it has connected to and the IP address assigned by the carrier.

- *Connection uptime*

  Time lapsed since the device has connected to the APN and has had an address assigned.

- *TX packets*

  Packets transmitted through the PPP interface assigned to the GPRSx base interface.

- *RX packets*

  Packets received through the PPP interface assigned to the GPRSx base interface.

- *Accessibility failures*

  Number of accessibility failures. An accessibility failure indicates that, during the time configured as “accessibility-ctrl”, the traffic coming from the network supporting the transmitted traffic hasn’t been received.

  This value is significant in Regesta-RP82 devices. In the RP81, an accessibility failure implies a change of carrier (thus causing the failures counter to reset).

- *Accessibility statistics*

  Displays the distribution in the accessibility failures time. The distribution makes sense for values below the “accessibility-ctrl” time.

- *Handoffs*

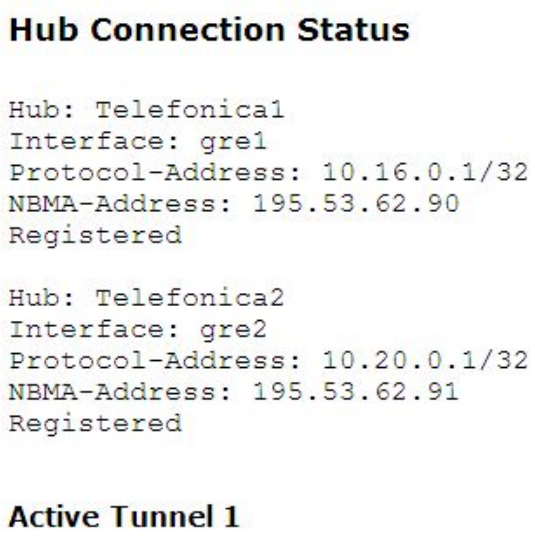
  Number of times a cell change has been produced. A high value means that the device is installed in a border zone between cells. Cell changes can provoke loss of traffic.

- *Service and neighbouring cells information*

  Displays information on the cell providing service and the adjacent ones.

5.2 DMVPN Connections

Monitors the state of the tunnels established with the central routers.



The information available on each tunnel is as follows:

- *Hub*

  HUB name.

- *Interface*

  GRE interface associated to the tunnel.

- *Protocol-Address*

  Address of the remote GRE interface.

- *NBMA-Address*

  Public address of the tunnel at the remote end.

- *Tunnel Status*

  - If the PPP interface over which the tunnel has been established doesn't have the tunnel status established as "Not reachable through base interface".

  - If the PPP interface is established, the possible states are:

    Registered.

    Not Registered.

- Tunnel currently transmitting the traffic.

5.3 SPI

Displays the SPI protocol monitoring (IP Presence Service Protocol)

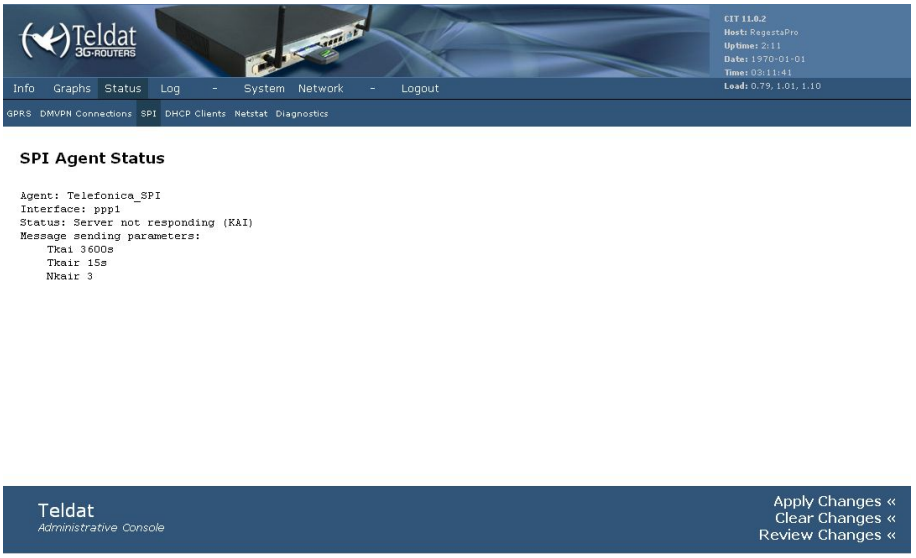


Fig. 9: SPI protocol monitoring.

Currently, this protocol is only available with the Movistar carrier.

5.4 DHCP Clients

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

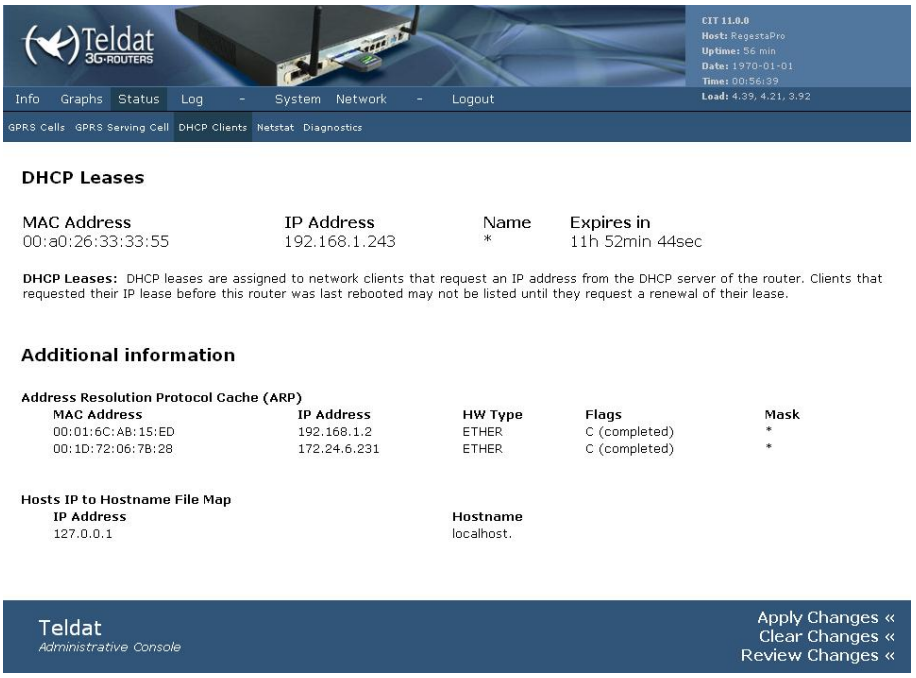


Fig. 10: Monitoring the DHCP protocol.

5.5 Netstat

Summarizes the following information:

- IP addresses assigned to the different device interfaces.
- Interface statistics.
- Device IP routing table.
- Device listening ports.
- List of connections established with the device and their current status.

Netstat

Ethernet/Wireless Physical Connections

```
IP address       HW type     Flags       HW address            Mask     Device
10.67.88.1       0x30a       0x0         0A:43:50:05     *        gre3
10.66.0.100      0x1         0x2         00:01:6C:3C:45:B2     *        eth1
10.67.84.1       0x30a       0x0         0A:43:50:01     *        gre1
10.67.104.1      0x30a       0x2         0A:43:50:71     *        gre2
```

Interfaces Statistics

```
Inter-|   Receive                                                |  Transmit
 face |bytes    packets errs drop fifo frame compressed multicast|bytes    packets errs drop fifo colls carrier compressed
    lo:       0       0    0    0    0     0          0         0        0       0    0    0    0     0       0          0
  eth0:  877584    3482    0    0    0     0          0       226    41056     136    0    0    0     2       0          0
  eth1:       0       0    0    0    0     0          0         0        0       0    0    0    0     0       0          0
  eth2:       0       0    0    0    0     0          0         0        0       0    0    0    0     0       0          0
  eth3:       0       0    0    0    0     0          0         0        0       0    0    0    0     0       0          0
  eth4:       0       0    0    0    0     0          0         0        0       0    0    0    0     0       0          0
  eth5:       0       0    0    0    0     0          0         0        0       0    0    0    0     0       0          0
  eth6:       0       0    0    0    0     0          0         0        0       0    0    0    0     0       0          0
  eth7:       0       0    0    0    0     0          0         0        0       0    0    0    0     0       0          0
  ppp0:    1966      13    0    0    0     0          0         0     7208      50    0    0    0     0       0          0
```

Routing Table

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
10.67.80.113    0.0.0.0         255.255.255.255 UH        0 0          0 ppp1
10.67.80.1      0.0.0.0         255.255.255.255 UH        0 0          0 ppp0
194.224.26.140  0.0.0.0         255.255.255.255 UH        0 0          0 ppp1
10.67.80.117    0.0.0.0         255.255.255.255 UH        0 0          0 ppp1
10.67.80.5      0.0.0.0         255.255.255.255 UH        0 0          0 ppp0
192.168.202.202 0.0.0.0         255.255.255.255 UH        0 0          0 ppp1
192.168.202.1   0.0.0.0         255.255.255.255 UH        0 0          0 ppp0
10.66.128.0     0.0.0.0         255.255.255.128 U         0 0          0 eth2
10.66.0.0       0.0.0.0         255.255.255.128 U         0 0          0 eth1
10.67.88.0      0.0.0.0         255.255.252.0   U         0 0          0 gre3
10.67.84.0      0.0.0.0         255.255.252.0   U         0 0          0 gre1
10.67.108.0     0.0.0.0         255.255.252.0   U         0 0          0 gre4
10.67.104.0     0.0.0.0         255.255.252.0   U         0 0          0 gre2
0.0.0.0         10.67.104.1     0.0.0.0         UG        0 0          0 gre2
```

Router Listening Ports

```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:2601            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:2602            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:53              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:520             0.0.0.0:*
udp        0      0 10.0.98.124:4500        0.0.0.0:*
udp        0      0 10.67.100.3:4500        0.0.0.0:*
udp        0      0 10.67.92.7:4500         0.0.0.0:*
udp        0      0 10.66.0.1:4500          0.0.0.0:*
udp        0      0 10.66.128.1:4500        0.0.0.0:*
udp        0      0 10.67.84.8:4500         0.0.0.0:*
udp        0      0 10.67.104.8:4500        0.0.0.0:*
udp        0      0 10.67.88.8:4500         0.0.0.0:*
udp        0      0 10.67.108.8:4500        0.0.0.0:*
udp        0      0 0.0.0.0:161             0.0.0.0:*
udp        0      0 0.0.0.0:53              0.0.0.0:*
udp        0      0 10.67.100.3:12225       0.0.0.0:*
udp        0      0 0.0.0.0:67              0.0.0.0:*
udp        0      0 10.0.98.124:500         0.0.0.0:*
udp        0      0 10.67.100.3:500         0.0.0.0:*
udp        0      0 10.67.92.7:500          0.0.0.0:*
udp        0      0 10.66.0.1:500           0.0.0.0:*
udp        0      0 10.66.128.1:500         0.0.0.0:*
udp        0      0 10.67.84.8:500          0.0.0.0:*
udp        0      0 10.67.104.8:500         0.0.0.0:*
udp        0      0 10.67.88.8:500          0.0.0.0:*
udp        0      0 10.67.108.8:500         0.0.0.0:*
```

Connections to the Router

```
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 10.66.0.1:80            10.66.0.100:2687        TIME_WAIT
tcp        0      0 10.66.0.1:80            10.66.0.100:2702        TIME_WAIT
tcp        0      0 10.66.0.1:80            10.66.0.100:2672        TIME_WAIT
tcp        0      0 10.66.0.1:80            10.66.0.100:2705        TIME_WAIT
tcp        0      0 10.66.0.1:80            10.66.0.100:2621        TIME_WAIT
tcp        0   1165 10.66.0.1:80            10.66.0.100:2694        ESTABLISHED
tcp        0      0 10.66.0.1:80            10.66.0.100:2701        TIME_WAIT
```

5.6 Diagnostics

Launches a PING operation to assess the manner in which a device accesses a certain IP address. Additionally, from the device, you can execute the TraceRoute operation and check the hops needed to reach a given router/host.

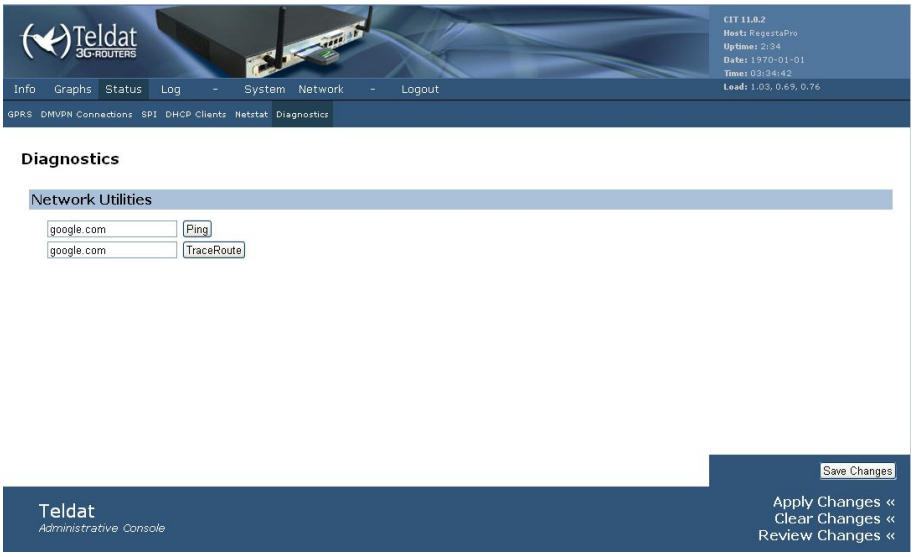


Fig. 14: IP diagnostics screen.

Chapter 6 Log Menu

From the Log menu, you can access pages that provide information on the evolution of the device functionality.

6.1 Syslog

Syslog messages, ordered through protocols, are made up of a set of traces that display the evolution of the device's behavior. The traces available in the device are as follows:

- AT commands.
- PPP protocol.
- GRE protocol.
- IPSec protocol.
- NHRP protocol.

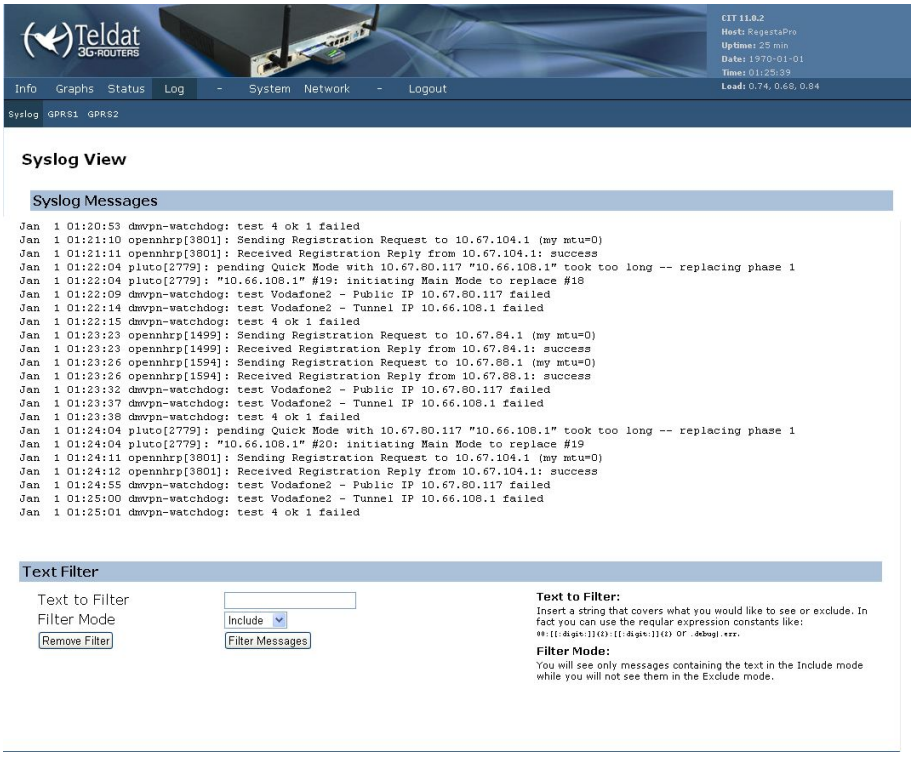


Fig. 15: Syslog in the device.

6.2 GPRS

This page displays the evolution of the connections to the GPRS network over time, indicating the carrier it's connected to and the IP address assigned by the GPRS network. In addition to the connections/disconnections to/from the GPRS network, the state of the connections with the central terminators is also indicated. This information is not lost between device restarts.

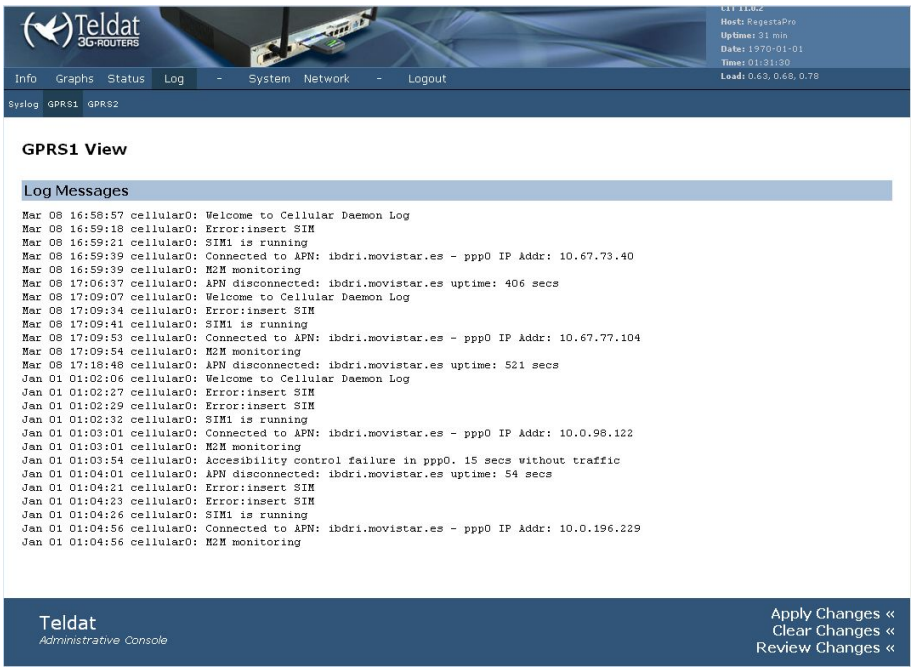


Fig. 16: GPRSx connection log.

Chapter 7 System Menu

Allows you to configure the general router parameters.

7.1 Settings

Configures the general parameters for the system. These are the router name, the time zone and the HTTP port.

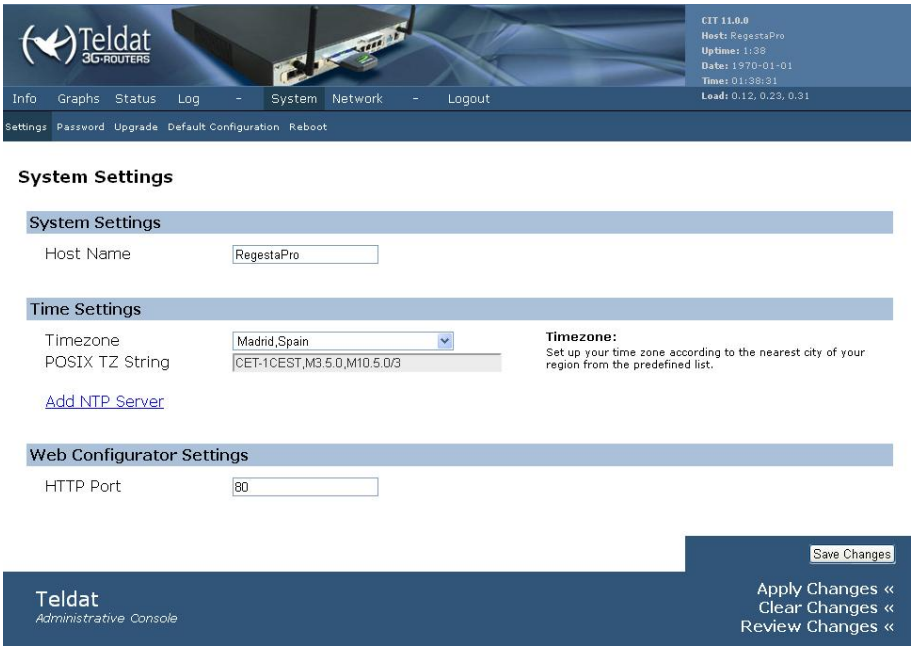


Fig. 17: Device Settings Screen

7.1.1 System Settings

System parameters.

- Host Name. Specifies the name of the device.

7.1.2 Time Settings

Date and time parameters.

- Timezone. Specifies the device time zone.
- Add NTP Server. Adds an NTP server for date and time synchronization

The following options appear for each NTP server that is added:

- NTP Server. Name of the NTP server.
- NTP Server Port.
- Remove NTP Server. Eliminates the NTP server from the list.

7.1.3 Web Configurator Settings

Web configuration parameters.

- HTTP Port. Port used for web configuration.

Note

To modify the configuration, first click on “Save Changes”. This temporarily stores the configuration. For changes to activate, click on the “Apply Changes” option.

7.2 Password

Modifying the password to access the web configuration.

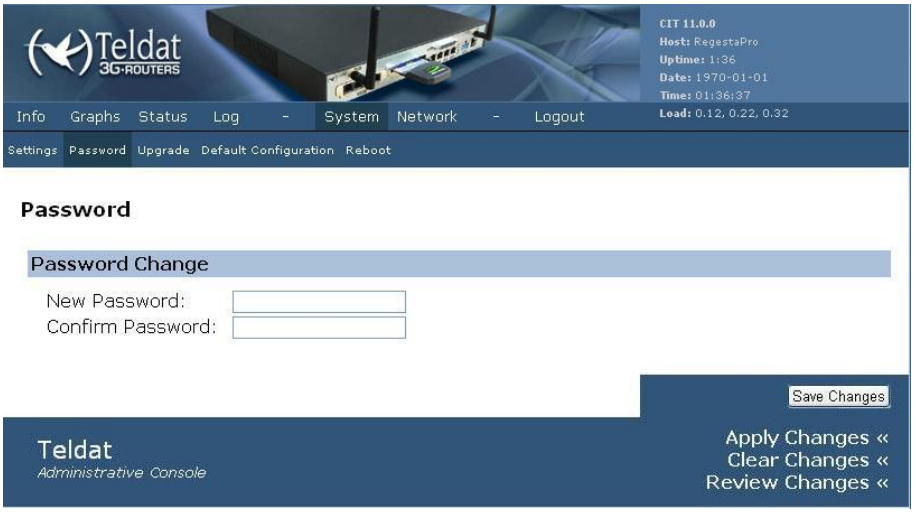


Fig. 18: Screen to change the web access password.

7.3 Upgrade

Upgrading the device firmware.

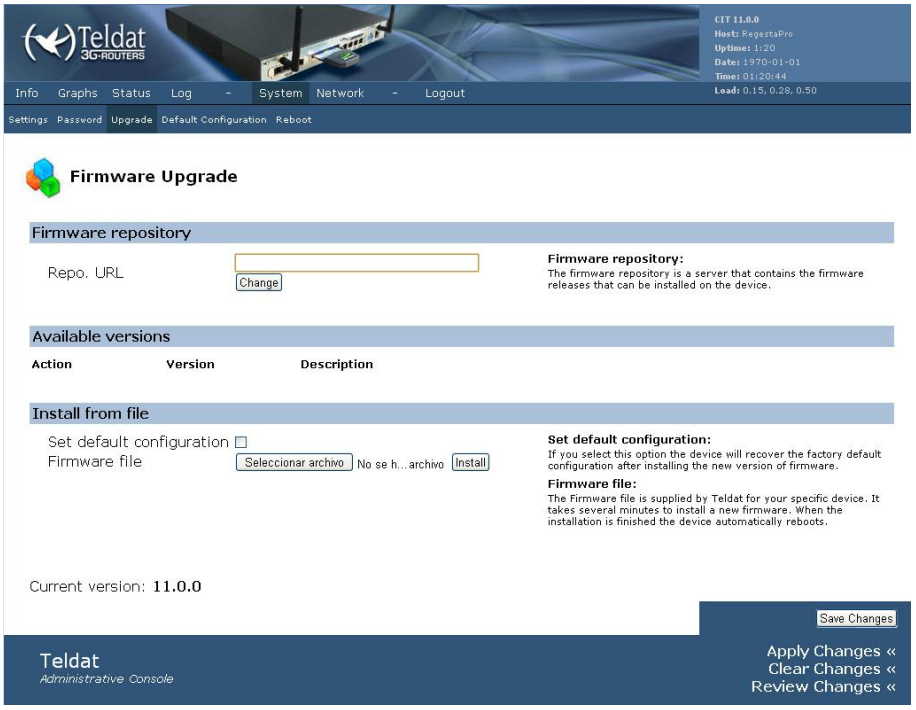


Fig. 19: Updating the software via web.

7.3.1 Install from file

To upgrade the firmware using the file supplied by Teldat, you need to carry out the following steps:

(1) Select the *Set default configuration* option only in cases where you want to delete the configuration and start up the new firmware from the factory configuration.

(2) Select the file containing the new firmware through the *Select file* button.

(3) Start the upgrading process through the *Install* button.

The upgrading process can take various minutes. The device must remain switched on during this process. Once it has finished, the initial web configuration screen reappears.

7.4 Default Configuration

Allows you to reestablish the initial configuration. To do this, click on the *Yes, set default configuration and reboot* button.

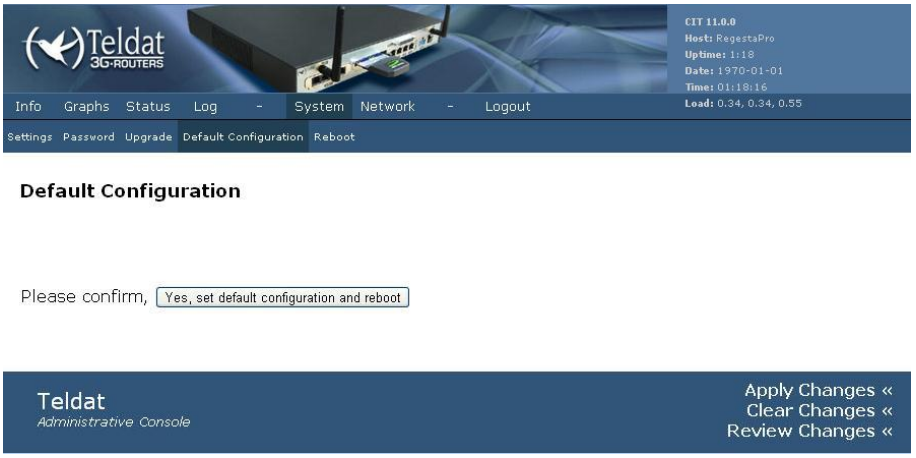


Fig. 20: Confirmation screen for the default configuration.

7.5 Reboot

Allows you to reboot the device. To do this, click on the *Yes, reboot* button.

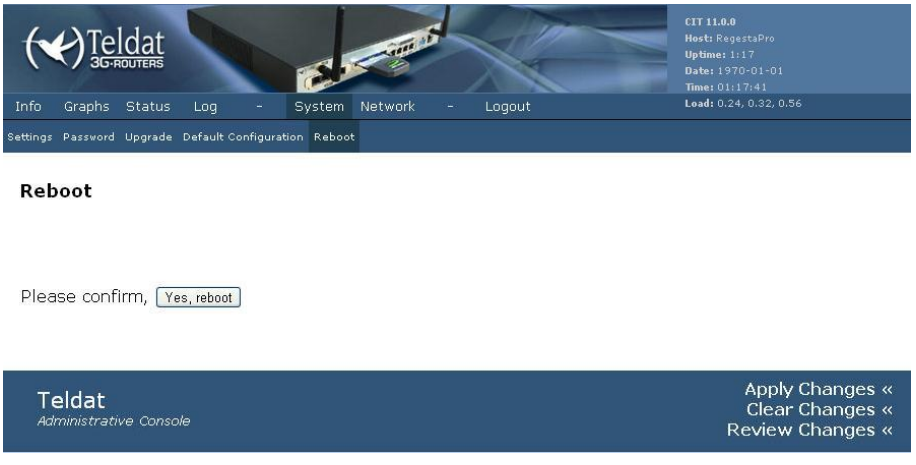


Fig. 21: Confirmation screen for device reboot.

Chapter 8 Network Menu

The Network menu configures all the device network parameters.

8.1 Networks

Configures the device IP networks. These networks are associated to the interfaces on the *Interfaces* page.

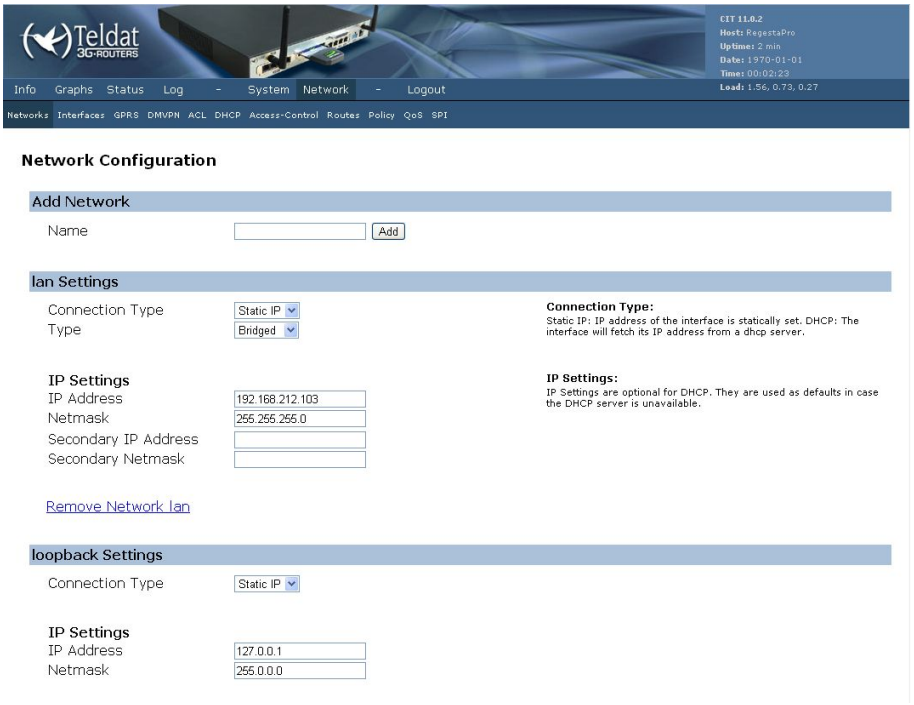


Fig. 22: Configuration screen for the networks.

8.1.1 Adding a network

To add a new network, you need to enter your name in the *Name* box in the section *Add Network* and click on the *Add* button.

8.1.2 Removing a network

To remove a network, use the *Remove Network* link on the section corresponding to said network.

8.1.3 Configuring a network

The parameters that can be configured for a network are as follows:

- *Connection Type: Disabled* .

  Disables the addressing in this network.
- *Connection Type: Static IP* .

  Defines the static IP addressing.
- *Connection Type: DHCP* .

  Defines dynamic addressing by DHCP, so the IP address is requested from a DHCP server.
- *Type: Interface* .

  The network is associated to a single interface.
- *Type: Bridged* .

The network is associated to the wanted interfaces forming a bridge between them.

- *IP Address*.

  Network's main IP address. A network can have various subnets assigned.

- *Netmask*.

  Main IP network mask.

- *Secondary IP Address*.

  New IP address assigned to the network.

- *Secondary Netmask*.

  Mask for the new assigned network.

8.1.4 Loopback Network

There is a special network that does not have an interface associated to it. This network is usually used for administrative tasks and is known as loopback. Here there are options that cannot be configured since there isn't an associated interface.

Note

The local addresses for the GRE tunnels also are configured in the Networks screen. The following image shows you how to configure address 10.67.84.8 as the local address for a GRE tunnel:

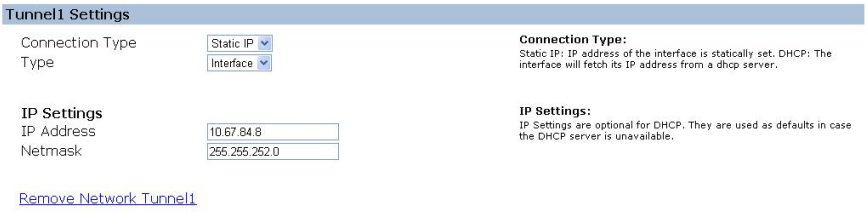


Fig. 23: GRE tunnel: Local configuration.

8.2 Interfaces

This screen is used to associate the defined networks to the device's local interfaces, i.e. Ethernet interfaces and GRE interfaces. You can also create Ethernet subinterfaces.

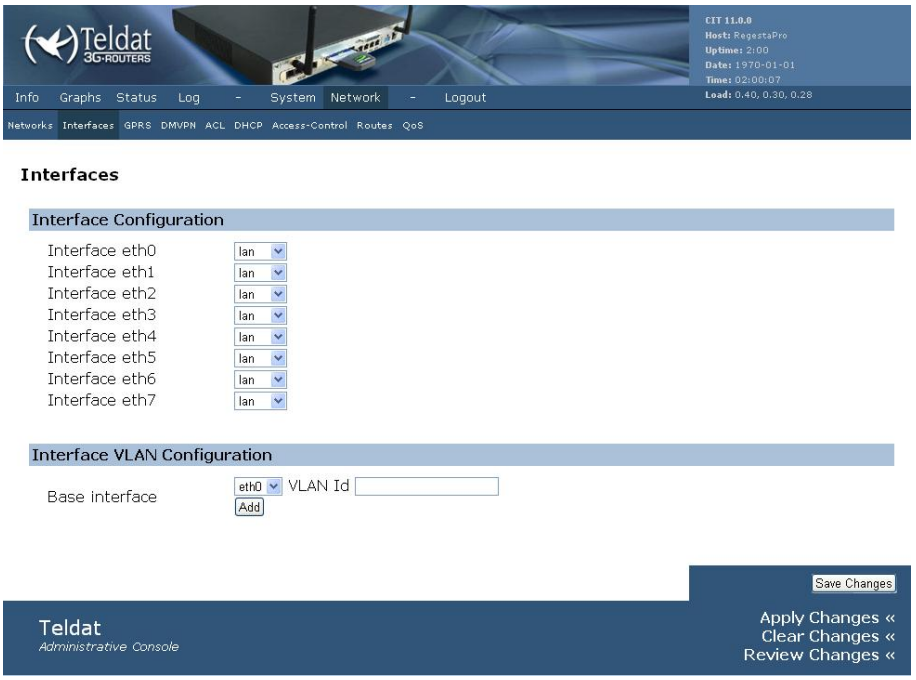


Fig. 24: Configuring the interfaces

8.2.1 Adding a VLAN

The *Interface VLAN Configuration* allows you to add a VLAN to an interface. To do this, you need to select the base interface (eth0 to eth7), enter the VLAN identifier and click on the *Add* button.

8.2.2 Eliminating a VLAN

To eliminate a VLAN from an interface, you need to use the *Remove* link that appears next to the corresponding VLAN subinterface.

8.2.3 Configuring the networks

To associate a network to an interface, you need to select said network from a pull down menu that appears next to the corresponding interface.

If you don't want to associate any network to an interface, select *None* from the pull-down menu. This interface cannot be accessed through IP.

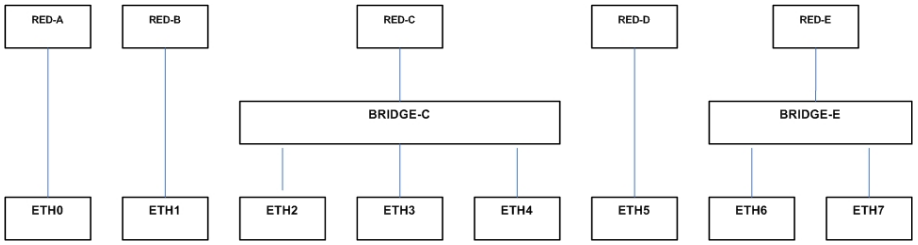
You cannot associate an *Interface* network to more than one interface. Only *Bridged* networks can be associated to more than one interface.

Bridge and interfaces configuration example:

(1) The following networks are defined in the Network screen:
Net-A: Connection Type: *static IP*. Type: *Interface.* IP Address: 1.0.0.1 Mask:255.0.0.0
Net-B: Connection Type: *static IP*. Type: *Interface*. IP Address: 2.0.0.1 Mask:255.0.0.0
Net-C: Connection Type: *static IP*. Type: *Bridge*. IP Address: 3.0.0.1 Mask:255.0.0.0
Net-D: Connection Type: *static IP*. Type: *Interface*. IP Address: 4.0.0.1 Mask:255.0.0.0
Net-E: Connection Type: *static IP*. Type: *Bridge*. IP Address: 10.0.0.1 Mask:255.0.0.0

(2) Networks associated to interfaces:
Eth0 : Net-A Eth4: Net-C
Eth1: Net-B Eth5: Net-D
Eth2: Net-C Eth6: Net-E
Eth3: Net-C Eth7: Net-E

(3) The final result is shown in the following schema:



(4) The devices connected to ports ETH2, ETH3 and ETH4 communicate at layer 2 independently of the IP network configured in NET-C. The BRIDGE-C is made up of 3 internal ports (over which switching is executed) and an internal port (that handles the routing).

(5) The devices connected to ports ETH6 and ETH7 communicate at layer 2 independently of the IP network configured in NET-E. The BRIDGE-E is made up of 3 internal ports (over which switching is executed) and an internal port (that handles the routing).

(6) Devices connected to any switch interface can send and receive traffic through the Regesta if they have IP addressing adjusted to the networks configured in the device. This is a mandatory condition so the Regesta can execute routing.

Port Trunking configuration example.

A port trunking is a port that connects to an Ethernet network and through which VLAN tagged traffic enters and exits. In the Regesta this is configured in the following way.

(1) The ETH0 interface is designed as port trunking. Over this interface you configure as many Ethernet subinterfaces as VLANs sent and received through this port trunking.

(2) You add VLAN-370, VLAN-840 and VLAN-850 over the ETH0 base interface.

(3) Once added, they subsequently appear in the interfaces list on the Interfaces screen.

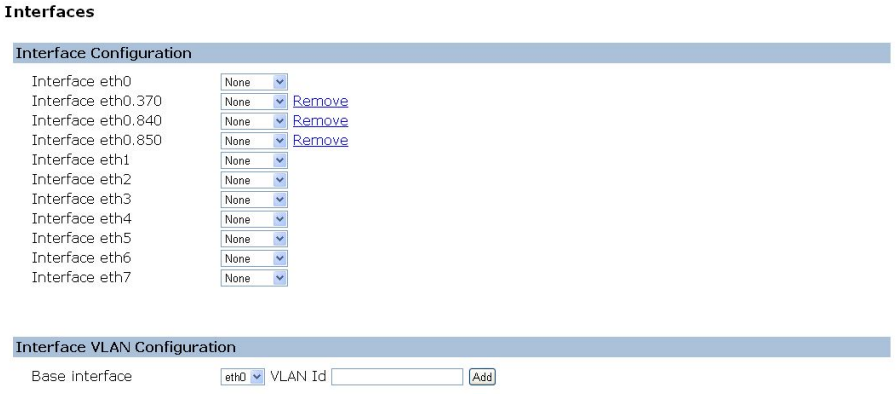
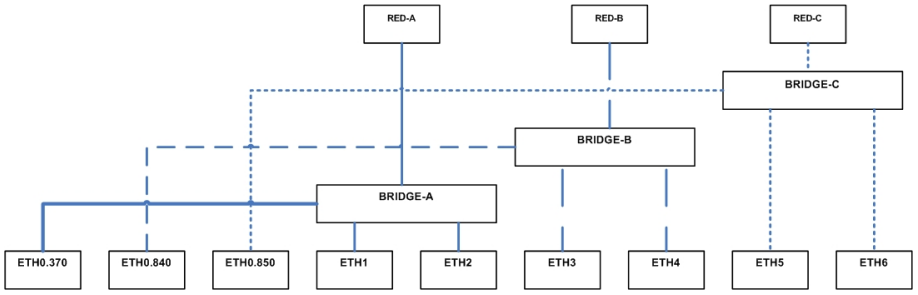


Fig. 26: Configuring Interfaces

(4) The following networks are configured:
Red-A: Connection Type: *static IP*. Type: *Bridge.* IP Address: 1.0.0.1 Mask:255.0.0.0
Red-B: Connection Type: *static IP*. Type: *Bridge*. IP Address: 2.0.0.1 Mask:255.0.0.0
Red-C: Connection Type: *static IP*. Type: *Bridge*. IP Address: 3.0.0.1 Mask:255.0.0.0

(5) Interfaces are associated to networks:
ETH0.370: Red-A ETH0.840: Red-B ETH0.840: Red-C
ETH1: Red-A ETH3: Red-B ETH5: Red-C
ETH2: Red-A ETH4: Red-B ETH6: Red-C

(6) The final result is shown in the following schema:



8.3 GPRS

This is the configuration for the device's two GPRS interfaces, defining the connection parameters to the network and the backup criteria.

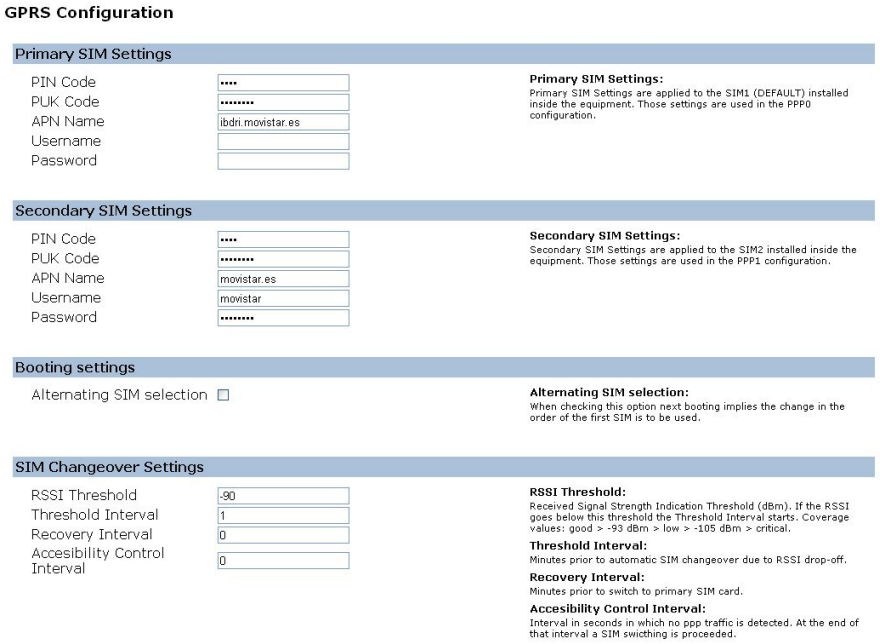


Fig. 28: GPRS interfaces configuration screen.

8.3.1 Primary SIM Settings

Connection parameters associated to the *SIM 1* card (*DEFAULT*). These parameters are as follows:

(1) *PIN Code*.
The PIN code for this SIM card.

(2) *PUK Code*.
The PUK code for this SIM card.

(3) *APN Name*.
The name of the access point used with this SIM card.

(4) *Username*.
The username to access the APN with this SIM card.

(5) *Password* .
Password to access the APN with this SIM card.

8.3.2 Secondary SIM Settings

In this section, the connection parameters associated to *SIM 2* are configured. These are the same as those given for *SIM 1*.

8.3.3 Booting Settings

- Alternating SIM selection

  On selecting this option, the device tries to initially connect to the other carrier (different from the one it was operating with). This option is only available in the Regesta-RP81.

8.3.4 SIM Changeover Settings

Configuration of the parameters that determine the conditions to switch to the backup carrier (SIM2) and return from backup to the main carrier (SIM1).

- *RSSI Threshold*

  The RSSI threshold indicates the intensity of the signal received in the antenna. When the RSSI drops below this threshold (in dBm), a backup period is started.

- *Threshold Interval*

  Specifies the number of minutes that the RSSI can be below the threshold before switching to the other carrier. The option to switch to the other carrier is only available in the Regesta-RP81. When it comes to the RP82, the device disconnects from the APN and attempts to reconnect again.

- *Recovery Interval*

  Specifies the number of minutes that the RSSI can be above the threshold before switching to the main carrier (SIM 1). In cases where this parameter is configured to 0, return to the main carrier does not occur (SIM1). In this case, switch to the main carrier occurs when the RSSI level drops for the duration of the time interval configured in *Threshold Interval*.

  This parameter is only available for the Regesta-RP81.

- *Accessibility Control Interval*

  Time during which absence of incoming traffic forces the device to disconnect from the current carrier. In the case of the RP81, a change of carrier occurs. With the RP82, the device tries to connect once more to the same carrier.

8.4 DMVPN (Dynamic Multipoint Virtual Private Network)

A DMVPN network is made up of a next-hop server known as a HUB, which has a public IP address (the IPSec tunnels' destination). The former is established by the remote device (Regesta) and a private IP address (which is the GRE tunnels destination address), needed to transport the routing protocol. Each HUB operates in a terminator, which can have several available HUBS operating over different subinterfaces.

The next configuration screen displays the general parameters for all the IPSec+GRE tunnels and the data that allows you to configure each of the HUBs that intervene in the network.

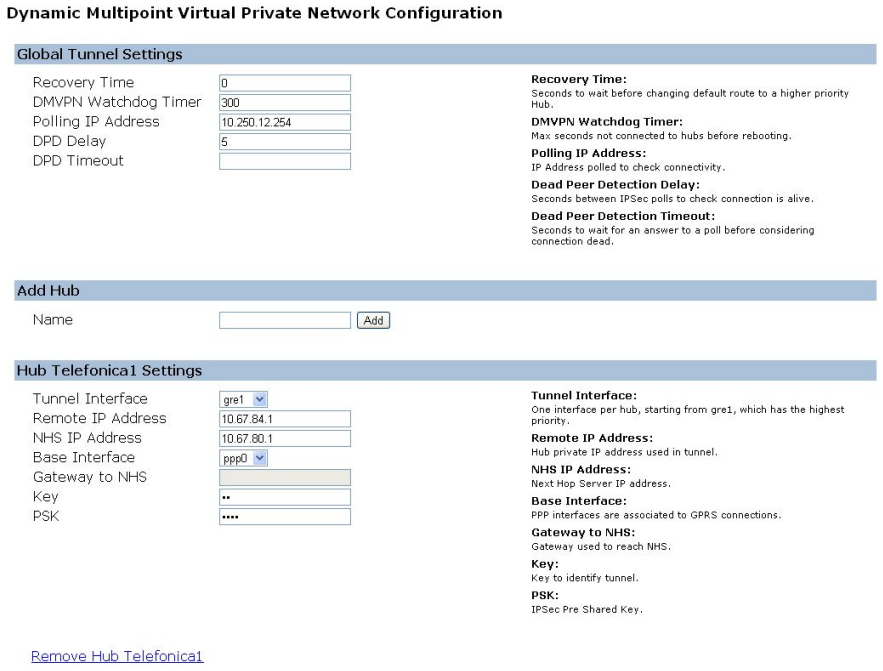


Fig. 29: Configuring the HUBs DMVPN.

8.4.1 Global Tunnel Settings

General parameters applicable to all the IPSec tunnels that the Regesta establishes with each configured HUB:

- *Recovery Time*

  Time in seconds where the traffic is routed through an IPSec tunnel that has less priority before being passed to a higher priority tunnel, if this is operating. The default value is 0. I.e. switching to a higher priority tunnel isn't executed. This situation allows the device to always operate with a carrier that has the highest communications quality.

- *DMVPN Watchdog Timer*

  Timer for the PING watchdog carried out with the IP address configured in the *Polling IP Address* parameter. If this watchdog timer lapses without receiving a response to the PING, the device will reboot. The default value is 0, i.e. polling isn't carried out.

- *Polling IP Address*

  IP address accessible from the Regesta device and to which the device executes PINGs with the aim of detecting global communication problems. The default address is 0.0.0.0, i.e. polling isn't executed.

- *DPD (Dead Peer Detection) Delay*

  Time between IPSec tunnel polls so if the tunnel terminator drops, this can be detected. The default value is 5 seconds and we recommend this is NOT changed.

- *DPD Timeout*

  This parameter is directly related to the *Accessibility Control Interval* parameter, specifically if you don't configure any internal value then it has a value equal to the *Accessibility Control Interval* + 2 seconds. If the *Accessibility Control Interval* is 0, then the DPD timeout has the default value of 20 seconds.

8.4.2 HUB Settings

In this section, we are going to configure the IPSec parameters. In this case, it is a single parameter:

- *Tunnel Interface*

  This is configured through a pull-down menu, enabling you to configure the local GRE interface operating over the IPSec tunnel. The pull-down menu allows you to select interfaces from GRE1 to GRE4.

- *Remote IP address*

mGRE interface term for the terminator router with which the device establishes the GRE tunnel.

- *NHS IP Address*

  HUB address with which the device establishes the IPSec tunnel.

- *Base Interface*

  Base interface over which the IPSec+GRE tunnel is transported. This is a pull-down menu that admits the PPP0 and PPP1 options. PPP0 corresponds to the Point-To-Point protocol established with the carrier assigned to SIM1. PPP1 corresponds to the Point-To-Point protocol established with the carrier assigned to SIM2.

  In addition to the PPP interfaces, it's also possible to establish tunnels over the Ethernet interfaces (such as a scenario with ADSL connections). In this case, the selected Ethernet interface must have a public IP address associated to it which is supplied by the carrier.

- *Gateway to NHS*

  Router's Gateway address that gives the device access to the public network. This address is needed in scenarios with ADSL connections.

- *Key*

  Key used for the GRE tunnels and that allows the HUB to distinguish between all the GRE tunnels connected to it. This is not a security key.

- *PSK*.

  This is the IPSec pre-shared key. This key must match that of the primary and secondary terminator devices.

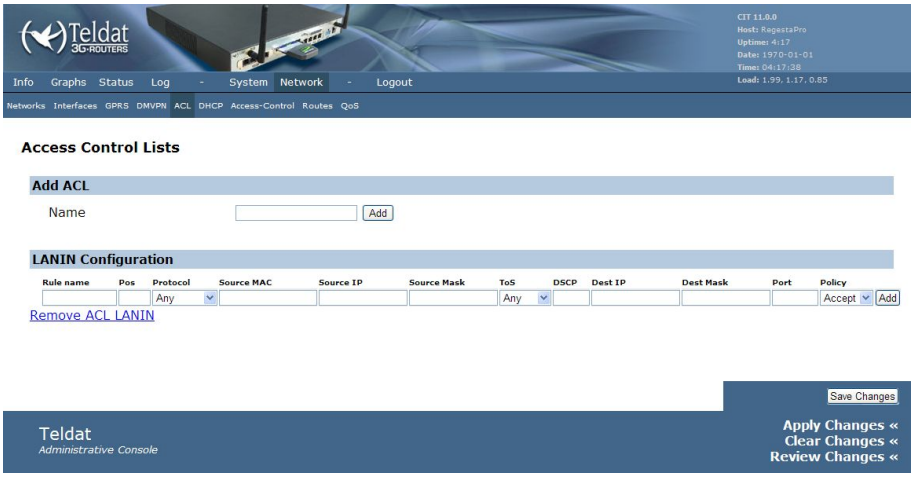
Important

Tunnel priority is defined by the GRE interface to which said tunnel is associated. This means that the tunnel associated to the GRE1 interface has greater priority to transmit traffic. The tunnel associated to the GRE4 interface has the least priority.

8.5 ACL (Access Control List)

Configuring the access control lists.

Access Control Lists are made up of a series of rules that determine which packets are accepted and which ones are dropped. Access Control Lists, or ACL, are configured in the *Access-Control* menu to filter the incoming and outgoing packets.



8.5.1 Adding an ACL

To add a new ACL, you need to enter its name in the *Name* field in the section on *Add ACL*, and then click on the *Add* button.

8.5.2 Removing an ACL

To eliminate an ACL, use the *Remove ACL* link in the section corresponding to said ACL.

8.5.3 Configuring an ACL

An ACL consists of a list of rules that are successively applied until a match is found.

A rule is made up of a name, a priority, a series of match criteria and a policy.

To add a new rule to an ACL you need to enter the parameters in the last line of the corresponding section and click on the *Add* button.

To remove a rule from an ACL, click on the *Remove* link corresponding to said rule.

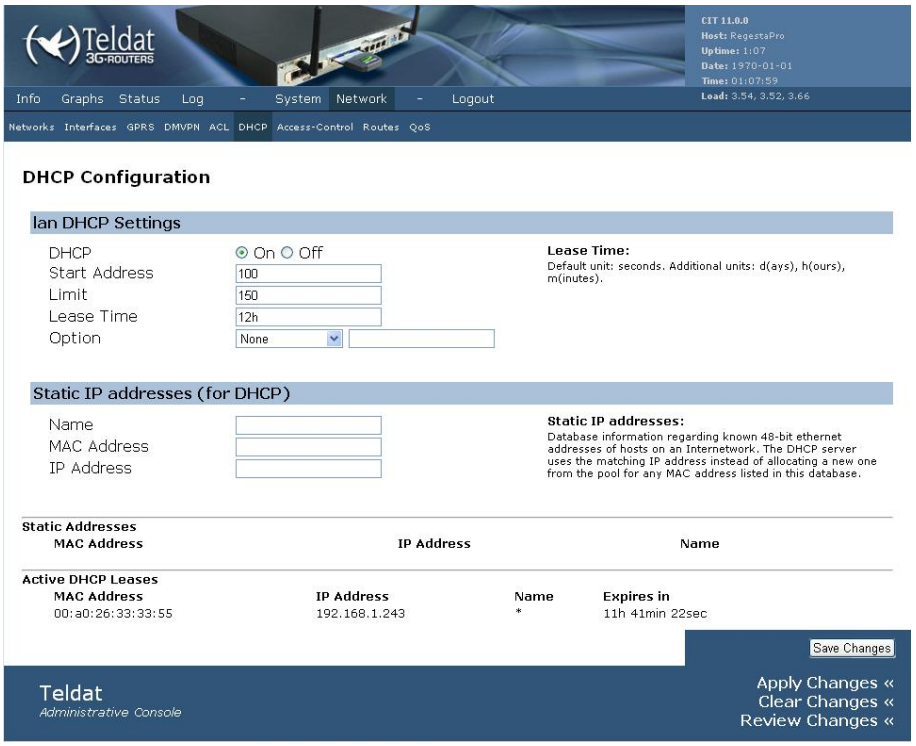
To modify an ACL rule, you need to modify the parameters for said rules and click on the corresponding *Change* button.

The parameters for a rule are as follows:

- *Rule name*. This is an informative field.
- *Pos*. Rule priority. This determines the order in which ACL rules are applied. The rules with the lowest *Pos* number are applied first.
- *Protocol*. Packet protocol. If you select *Any*, this matches any protocol.
- *Source MAC*. Source MAC address. If you leave this field empty, this will match any MAC address.
- *Source IP*. Source network IP address. For this to coincide with any source IP address, you must specify the default network, i.e., *Source IP 0.0.0.0* and *Source Mask 0.0.0.0*.
- *Source Mask*. Source network IP mask. This value is applied together with the *Source IP* mask.
- *ToS*. IP header ToS field. If you select *Any*, this will coincide with any ToS field value. If you select *DSCP*, it will match the value configured in the DSCP parameters.
- *DSCP*. The DSCP value in the IP header ToS field
- *Dest IP*. Destination network IP address. For this to match any destination IP address, you need to specify the default network, i.e. *Dest IP 0.0.0.0* and *Dest Mask 0.0.0.0*.
- *Dest Mask*. Destination network IP mask. This value is applied together with the *Dest IP*.
- *Port*. Port when running the TCP or UDP protocols.
- *Policy*. Policy to apply in matching packets. *Accept* to accept said packets and *Drop* to discard them.

8.6 DHCP (Dynamic Host Configuration Protocol)

Configuring the device DHCP server.



8.6.1 DHCP Settings

In networks with static IP addressing you can enable the DHCP server. The parameters that define its behavior are as follows:

DHCP On/Off. With the *On* option you enable the DHCP server. *Off* disables it.

Start Address. Indicates the number of the initial host to assign (the lowest) address within the network.

Limit. Indicates maximum number of addresses to assign.

Lease Time. Indicates the time an assignment is maintained.

Option None. Corresponds to an empty entry that can be modified to add a new option.

Option Router. Router going to the network (gateway).

Option DNS Servers.

Option Log Server. Syslog Server

Option Time Servers.

Option WINS Server.

Option Bootfile Name. Start-up file name.

Option TFTP Server IP. TFTP server IP address.

8.6.2 Static IP Addresses (for DHCP)

The new static assignments of IP addresses with MAC addresses are configured through the following parameters:

- *Name*. Name of the association.
- *MAC Address*. Network adapter MAC address to which the static IP address is associated.
- *IP Address*. Statically associated IP address.

8.6.3 Static Addresses

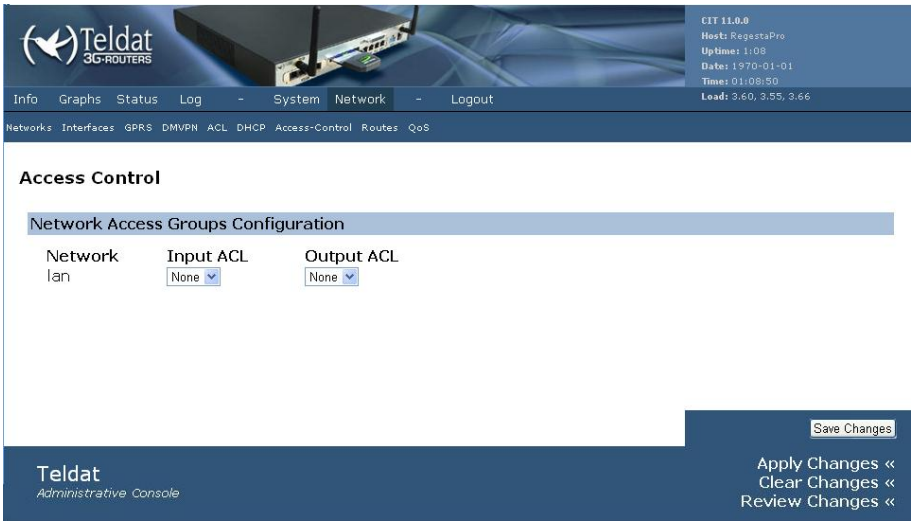
Displays the configured static assignments. This also allows you to delete a static assignment through the corresponding *Remove* link.

8.6.4 Active DHCP Leases

Presents the active leases.

8.7 Access-Control

Establishes access control polices in each of the configured networks.



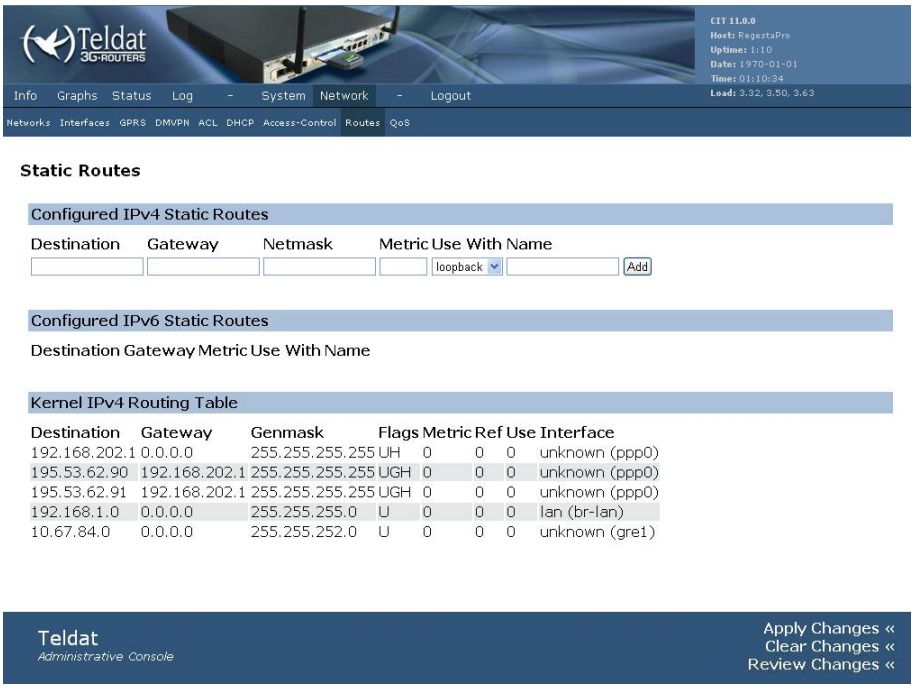
8.7.1 Network Access Groups Configuration

In each configured network there is a possibility of enabling access control policies in both the input and output traffic. These policies use the access control lists configured in the *ACL* page.

- *Input ACL*. This specifies the access control list that must be used to filter the incoming traffic, i.e. the ACL which is applied to each of the packets that reach the device through the corresponding network. The option *None* means that all packets must be accepted.
- *Output ACL*. This specifies the access control list that must be used to filter the outgoing traffic, i.e. the ACL which is applied to each of the packets that are transmitted from the device through the corresponding network. The option *None* means that all packets must be transmitted.

8.8 Routes

This provides access to the configuration and monitoring for static routes. The static routes serve to access local networks that aren't directly connected to the device.



8.8.1 Static Routes

In this section, you can add and delete static routes.

The configurable parameters for a static route are as follows:

- *Destination*. Destination network IP address.
- *Gateway*. IP address for the next hop to reach the destination network.
- *Netmask*. Destination network IP mask.
- *Metric*. Route cost.
- *Use With*. Next hop network.
- *Name*. Route name.

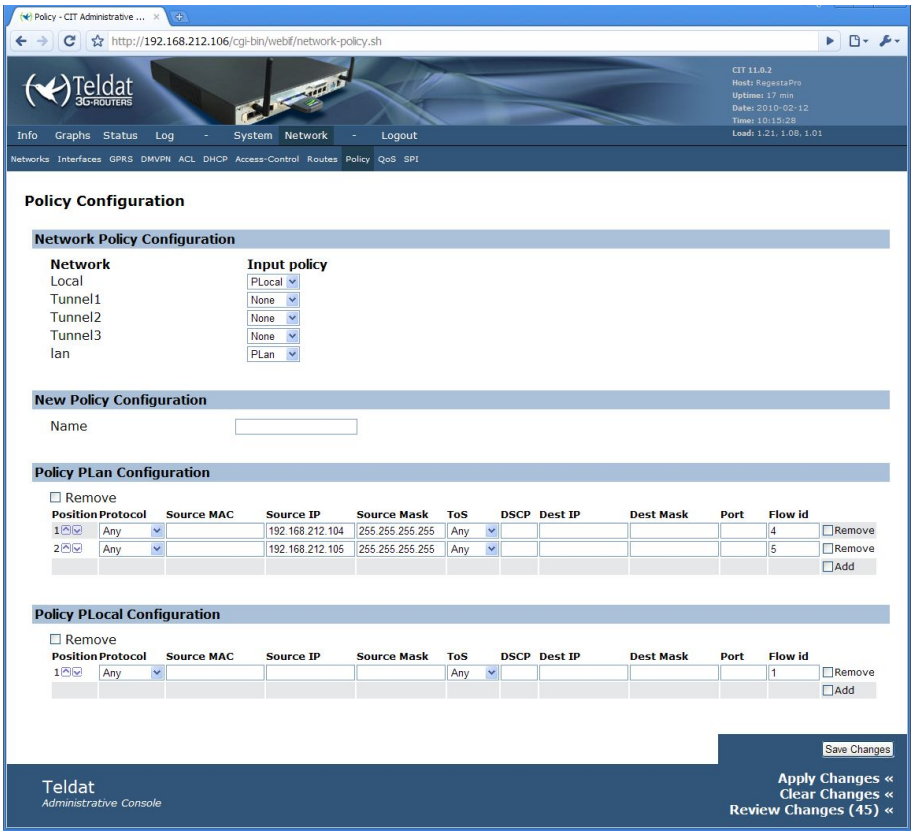
8.8.2 Kernel IPv4 Routing Table

Active routes are shown.

8.9 Policy

Establishes classification policies and flow identification.

Each of the configured networks can be associated to a policy to identify the incoming flows. Once the flows are identified with different marks, these marks can be used in the output interfaces to apply quality of service functions (QoS).



8.9.1 Network Policy Configuration

In each configured network, there is the possibility of enabling flow identification policies in input traffic. The policies must be defined in this same page.

8.9.2 New Policy Configuration

To add a new policy, you need to enter its name (“Name”) and save the changes (“Save Changes”). On reloading the page with the saved changes, a section appears where you can edit the new policy.

8.9.3 Policy <name> Configuration

For each configured policy there is an edit section.

You can remove the policy using the *Remove* box.

A policy is formed by a list of rules ordered by position. These rules are applied to each packet to identify the flow it belongs to. This process consists of applying the configured rules consecutively from the first position until one is found that matches. The packet is then associated to the flow configured in the said rule (“Flow id”).

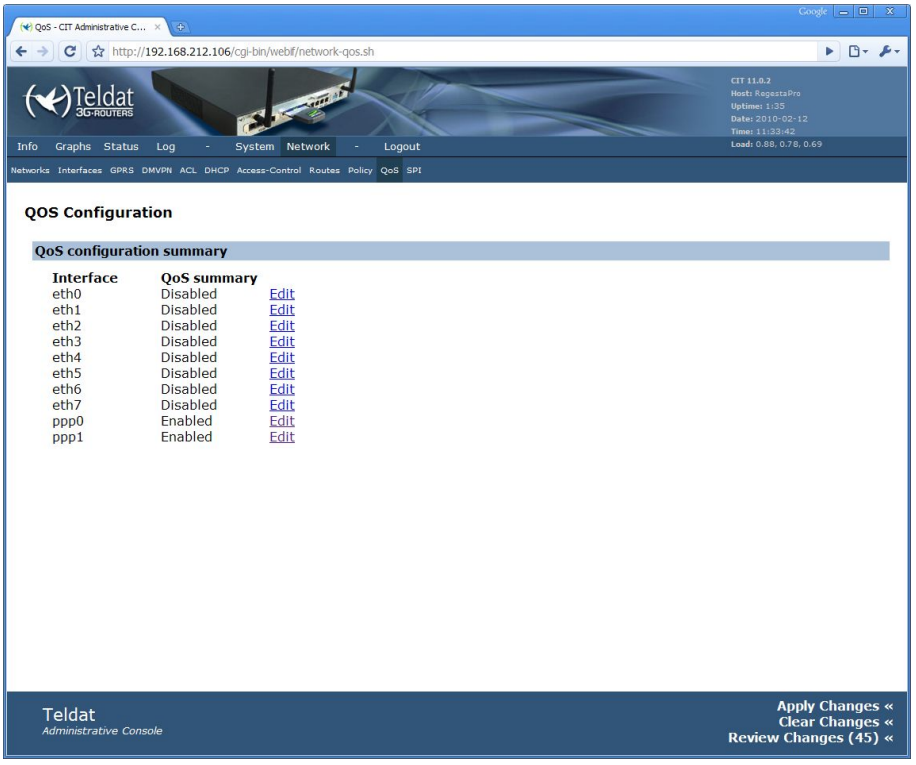
Each rule is made up of the following fields:

- *Position*. Position of the rules within the policy. The rules are applied in the order indicated by this field, beginning with the rule in position 1. You can reposition the rules by using the arrows that appear next to the position number.
- *Protocol*. Packet protocol. If you select *Any*, this will coincide with any protocol.
- *Source MAC*. Source MAC address. If this is left blank, then any MAC address will coincide.
- *Source IP*. Source network IP address. If this is left blank, any source IP address will coincide.
- *Source Mask*. Source network IP mask. This value is applied together with the *Source IP* value. If this is left blank, it takes the host mask (255.255.255.255).
- *ToS*. IP header ToS field. If you select *Any*, this will coincide with any value from the ToS field. If you select *DSCP*, this will match the value configured in the *DSCP* field.
- *DSCP*. The DSCP value in the IP header ToS field.

- *Dest IP*. Destination network IP address. If this is left blank, any destination IP address will coincide.
- *Dest Mask*. Destination network IP mask. This value is applied together with the *Dest IP* value. If this is left blank, it takes the host mask (255.255.255.255).
- *Port*. Destination port in cases where there are TCP or UDP protocols.
- *Flow id*. Flow identifier to associate to the matching packets.
- *Remove*. Removes this rule from the policy.
- *Add*. Adds a new rule to the policy. To add more rules, you need to save the configuration (“Save Changes”).

8.10 QoS (Quality of Service)

Configuring the quality of service to administer the bandwidth in the interfaces.

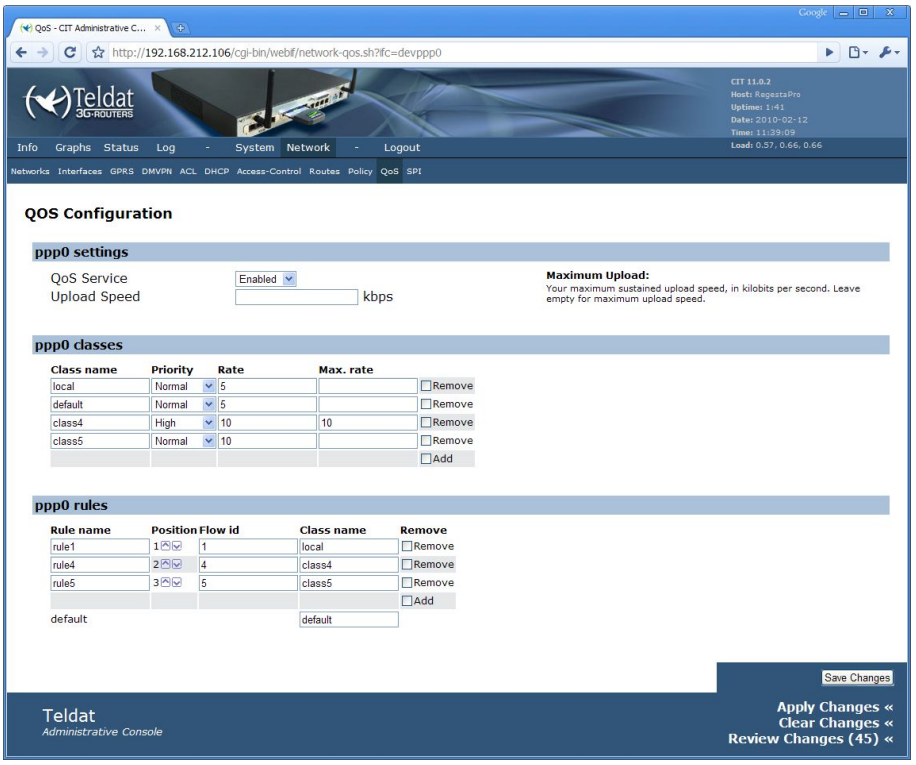


The quality of service (QoS) criteria is applied in the physical output interfaces. These interfaces are Ethernet ports and the PPP links associated to the GPRS connections.

8.10.1 QoS configuration summary

Displays a table indicating whether the quality of service (QoS) function is enabled or not for each interface.

Through the Edit link you can access the quality of service configuration page for the corresponding interface.



The configuration page for the quality of service in an interface is divided into three sections. These allow you to configure global parameters for the interface, traffic classes and rules.

8.10.2 <Interface> settings

You can configure the following parameters in this section:

- *QoS Service*. Allows you to enable or disable the quality of service function in the interface. If this is disabled, no control is carried out over the traffic transmitted by the interface. If it is enabled, the traffic transmitted by the interface is adjusted to the criteria configured in this page.
- *Upload Speed*. Maximum transmission rate in kilobits per second (Kbps). If this is left blank, then the interface transmission speed isn't limited.

8.10.3 <Interface> classes

The traffic transmitted by the interface is split into classes. For each class, a priority is configured and a bandwidth and rate limit are assigned.

The classes are displayed in a list with the following fields:

- *Class name*. This is an administrative field.
- *Priority*. Strict class priority. Classes with greater priority have preference over classes with lower priority when sharing the bandwidth. This means that the bandwidth for the first interface is assigned to the "Real time" priority classes, whilst the remaining bandwidth is assigned to classes with "High", "Normal" and "Low"priority.
- *Rate*. Bandwidth assigned to the class in kilobits per second (Kbps). The bandwidth available for priority classes is proportionally shared depending on this field. E.g. suppose we have 3 classes with Normal priority: Class A with Rate 5, class B with Rate 5 and class C with rate 10. In this configuration class A receives 25% of the available bandwidth for Normal priority, class B another 25% and class C 50%.
- *Max. rate*. Maximum transmission rate for the class in kilobits per second (kbps). If this is left blank, a specific limit isn't established for the class (meaning it competes for all the bandwidth available).
- *Remove*. Removes this class.
- *Add*. Adds a new class. To add more classes you need to save the configuration ("Save Changes").

8.10.4 <Interface> rules

In order to determine the class to which each packet transmitted through the interface is assigned to, a list of rules is used. The rules are consecutively applied in the indicated order (i.e., from the first position onwards) until a rule that matches is found and the packet is associated to the class configured in said rule (“Class name”). The last rule (“default”) indicates what class the packets that do not match any rules will be assigned to.

Each rule consists of the following fields:

- *Rule name*. This is an administrative field.
- *Position*. Indicates the order in which the rules are applied to each packet, beginning with position 1. The rules can be repositioned through the arrows that appear next to the position number.
- *Flow id*. The rule that matches packets that have been associated with this “Flow id”. The packets are associated with a Flow id based on the configuration in the Policy page.
- *Class name*. This is the class the packets which match this rule are assigned to.
- *Remove*. Removes this rule.
- *Add*. Adds a new rule. In order to add a new rule you must save the configuration (“Save Changes”).

8.11 SPI (IP Presence Service)

This protocol belongs to the Spanish carrier Telefónica. It allows devices connected to the GPRS network to periodically send information on the GPRS connection state to a server. The server maintains the connection state for the devices from which it receives polls from.

This protocol is incorporated in the Regesta device, although it’s only operative when the device is connected to the Movistar carrier.

The time values and the number of restarts configured are the values that the protocol initially uses in its contact with the server. Once this contact is established (the server responds to the initial polls), the device receives from the server some new time values and number of restarts.

The configuration screen is shown below:

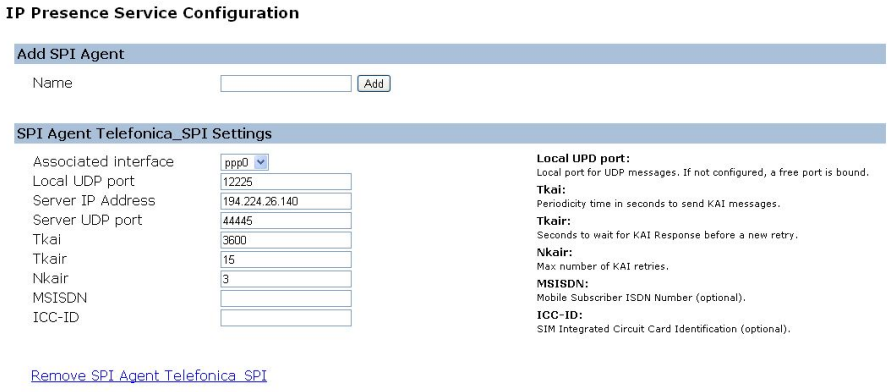


Fig. 37: SPI protocol Configuration Screen.

Configuration parameters:

- *Associated interface*

  Base interface over which the SPI protocol is transmitted. The interface is selected through a pull-down menu using the PPP0 or PPP1 options.

- *Local UDP port*

  Source port for the SPI protocol packets. Default is 12225.

- *Server IP Address*

Server IP address where the SPI protocol packets are sent.

- *Server UDP port*

  Port in the server that listens to the SPI protocol packets. Default is 44445.

- *Tkai*

  Interval between polls (KAI packets) until a response has been received from the server.

- *Tkair*

  Timeout interval for the initial polls (KAI packets).

- *NKair*

  Maximum number of initial poll packet retransmissions (KAI packets).

- *MSISDN*

  Telephone number associated to the SIM. If this parameter is left blank, the SPI protocol can get it from the server.

- *ICC-ID*

  Integrated Circuit Card ID for the SIM installed in the device. If this parameter is left blank, the SPI protocol will get it directly from the SIM

Chapter 9 Logout Menu

Describes the disconnection process from the web.

As the basic HTTP authentication is stored in the browser, you cannot automatically disconnect. You need to close your browser first. However, if you are using Firefox, you can simply use the *Clear Private Data* option.