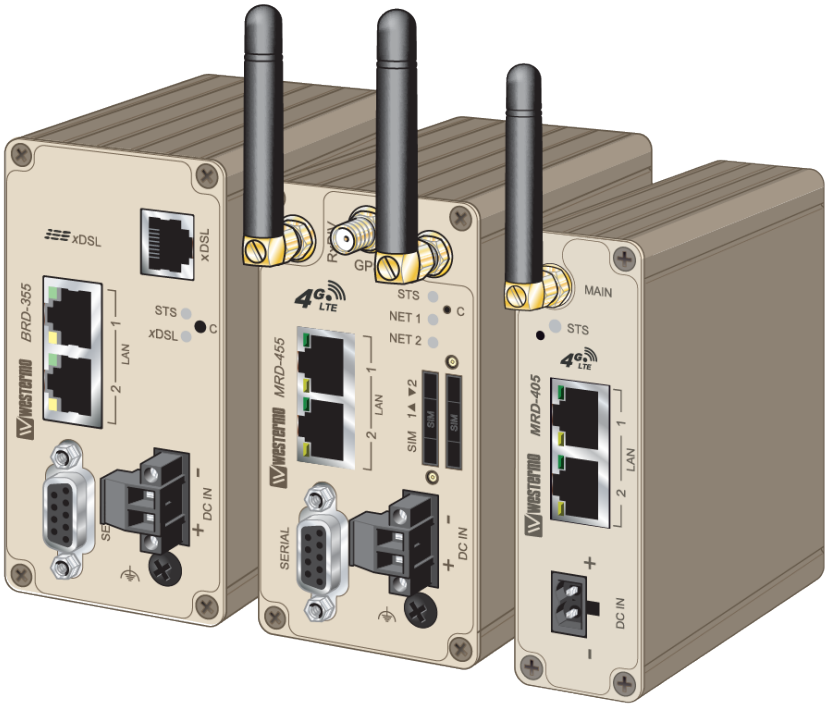
Management Guide
6623-3210

WESTERMO

Management Guide



3G / 4G / xDSL

Industrial Routers

www.westermo.com

©Westermo Teleindustri AB

Documentation Control

Generation Date: September 29, 2017

Legal Information

The contents of this document are provided ”as is”. Except as required by applicable law, no warranties of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose, are made in relation to the accuracy and reliability or contents of this document. Westermo reserves the right to revise this document or withdraw it at any time without prior notice.

Under no circumstances shall Westermo be responsible for any loss of data or income or any special, incidental, and consequential or indirect damages howsoever caused.

More information about Westermo can be found at the following Internet address: http://www.westermo.com

Contents

1 Introduction **1**

1.1 Document Structure . . . 1
1.2 Differences between devices running MRX . . . 1
1.3 Conventions Used . . . 1
1.4 Manual Updates . . . 1
1.5 Default Configuration . . . 1

2 Accessing the Web Interface **2**

2.1 Computer Settings . . . 2
2.2 Windows PC Network Settings . . . 2
2.3 Connecting to the Web Server . . . 6

3 Web Page Layout **8**

3.1 Page Layout . . . 8
3.2 Menu Structure . . . 8
3.3 Symbols . . . 13

4 Status **14**

4.1 Alarms . . . 14
4.2 Wireless . . . 16
4.3 DSL . . . 19
4.4 Local Area Network (LAN) . . . 22
4.5 Virtual Private Network (VPN) . . . 24
4.6 Generic Routing Encapsulation (GRE) . . . 25
4.7 Serial Server . . . 27
4.8 General Purpose Input / Output (GPIO) . . . 28
4.9 System Log . . . 29

5 System **30**

5.1 Administration . . . 30
5.2 System Configuration . . . 31
5.3 Backup & Upgrade . . . 34
5.4 System Information . . . 37
5.5 Syslog . . . 38
5.6 Power . . . 40
5.7 General Purpose Inputs and Outputs (GPIO) . . . 42
5.8 Location using GPS . . . 48

6 Wireless **51**
6.1 Wireless Network . . . 52
6.2 Packet Mode Configuration . . . 57
6.3 Connection Management . . . 65
6.4 Circuit Switched Data (CSD) Mode . . . 68
6.5 SMS . . . 77

7 DSL **88**
7.1 Configure the DSL Network . . . 88
7.2 VDSL Configuration . . . 89
7.3 ADSL Configuration . . . 96
7.4 Connection Status . . . 105
7.5 Connection Management . . . 106

8 Network **110**
8.1 LAN Interface . . . 110
8.2 Configuring the DHCP server . . . 113
8.3 Loopback Interface . . . 114
8.4 Domain Name System (DNS) . . . 114
8.5 Generic Routing Encapsulation (GRE) . . . 117
8.6 Network Diagnostics . . . 118

9 Routing **119**
9.1 Default and Static Routes . . . 119
9.2 Dynamic Routing . . . 125
9.3 Virtual Router Redundancy Protocol (VRRP) . . . 125
9.4 Policy Routing . . . 129
9.5 Quality of Service Routing . . . 133

10 Firewall **140**
10.1 Firewall Setup . . . 140
10.2 Access Control . . . 142
10.3 DoS Filters . . . 143
10.4 Custom Filters . . . 144
10.5 Port Forwarding . . . 149
10.6 Custom NAT . . . 152
10.7 MAC Address Filtering . . . 157

11 Virtual Private Network (VPN) **162**
11.1 Internet Protocol Security (IPsec) VPN . . . 162
11.2 Secure Sockets Layer (SSL) VPN . . . 187
11.3 PPTP and L2TP . . . 193
11.4 Multiple VPN Tunnels . . . 196
11.5 Certificate Management . . . 197

12 Serial Server **207**

12.1 Selecting a port function . . . 207
12.2 Common configuration options . . . 209
12.3 Raw TCP Client/Server . . . 210
12.4 Raw UDP . . . 212
12.5 Modem Emulator . . . 214
12.6 DNP3 IP-Serial Gateway . . . 218
12.7 Modbus IP-Serial Gateway . . . 221
12.8 Telnet (RFC 2217) Server . . . 222
12.9 PPP Server . . . 224
12.10 PPP Dial-Out Client . . . 226
12.11 Phone Book . . . 228

13 Management **244**

13.1 Events . . . 244
13.2 SNMP . . . 248
13.3 DNP3 . . . 257
13.4 SMS . . . 262
13.5 Email . . . 267

1 Introduction

This manual describes the functionality and management features of the MRX operating system which is used in the MRD and BRD production range of modem / routers.

1.1 Document Structure

The first section of the document describes the configuration interface and how to access it. The second section contains specific information for configuring the device.

1.2 Differences between devices running MRX

Not all devices support all features described in this manual. This is usually hardware dependant, for example a Wireless (3G/LTE) device will not include an DSL interface, so the DSL chapter will not be relevant.

1.3 Conventions Used

This manual uses the following typographical conventions:

Italic: Used for emphasising new terms when first introduced.

`www.example.com.au`: Used to display URLs (Web addresses).

Menu ▷ Sub-menu: Used to illustrate menu navigation.

The manual uses the following icons:

Indicates a reference to further information. This may include other documents or information available online.

Indicates a tip, suggestion, or general note relating to the occupying text.

Indicates the text of an SMS.

Indicates a warning or caution relating to the occupying text.

1.4 Manual Updates

Improvements and updates to this manual will be made available on the Westermo website `www.westermo.com`. There you will also find, further product documentation including application notes, user guides, and other support information.

1.5 Default Configuration

Unless otherwise stated the manual assumes the configuration of the unit is in the factory default state. If the modem has been previously configured it may be necessary to perform a configuration reset to return the the configuration to the default state, prior to configuring the device. The procedure to perform a configuration reset is described in the manual for the particular model.

2 Accessing the Web Interface

This section describes how to connect to the web interface of the unit to be configured. As all configuration is performed via the web interface establishing a connection to the web interface is the first step in configuring the device.

The web interface can be accessed from any interface which supports TCP/IP and provides support for both the HTTP and HTTPS protocols. The description which follows describes accessing the web interface via the Ethernet interface. It is also possible to access the web interface via the wireless interface however to do this the firewall will need to be configured to allow incoming connections.

For best results it is recommend that a modern web browser be used with JavaScript enabled. The web interface makes use of JavaScript although it is possible to use a browser with JavaScript disabled not all functionality will be supported.

Due to security issues and lack of support for web standards Internet Explorer 6 is not recommend. Although the web interface supports IE6 not all features are fully supported.

2.1 Computer Settings

In order to view the web pages a computer with a fixed IP address, on the same sub-net as the unit to be configured, will need to be connected to one of the LAN ports.

- The default IP settings of the unit are:
  - IP Address: 192.168.2.200
  - Netmask: 255.255.255.0
- The recommended IP settings for the PC used to configure the unit are:
  - IP Address: 192.168.2.220
  - Netmask: 255.255.255.0
  - Default Gateway: 192.168.2.200
  - Primary DNS: 192.168.2.200

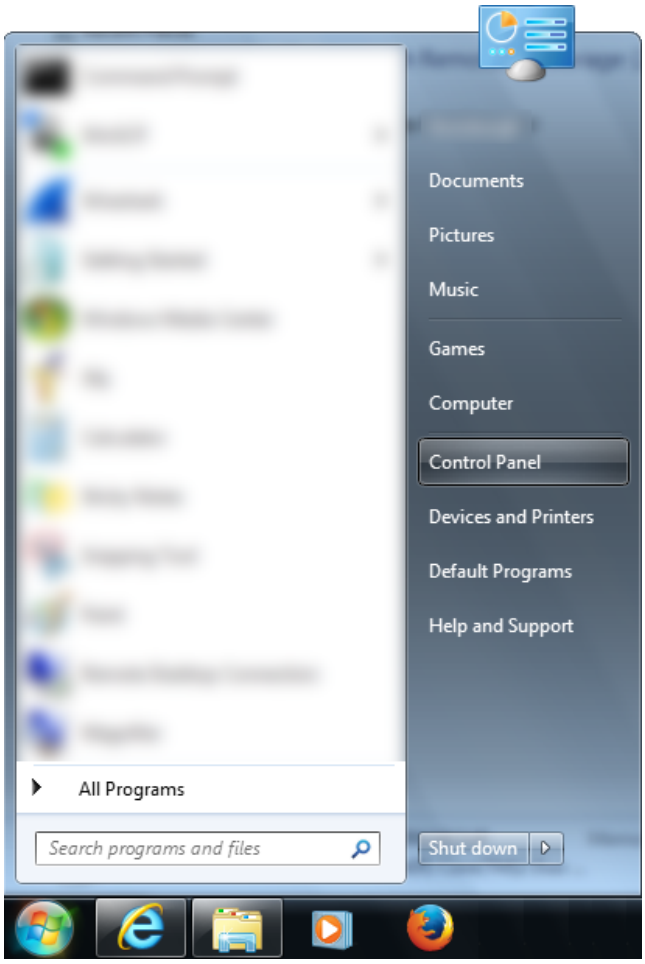
Although it is possible to connect the unit to be configured directly to a Local Area Network (LAN) it is recommend that the network configuration as described in this section be performed prior to doing so.

2.2 Windows PC Network Settings

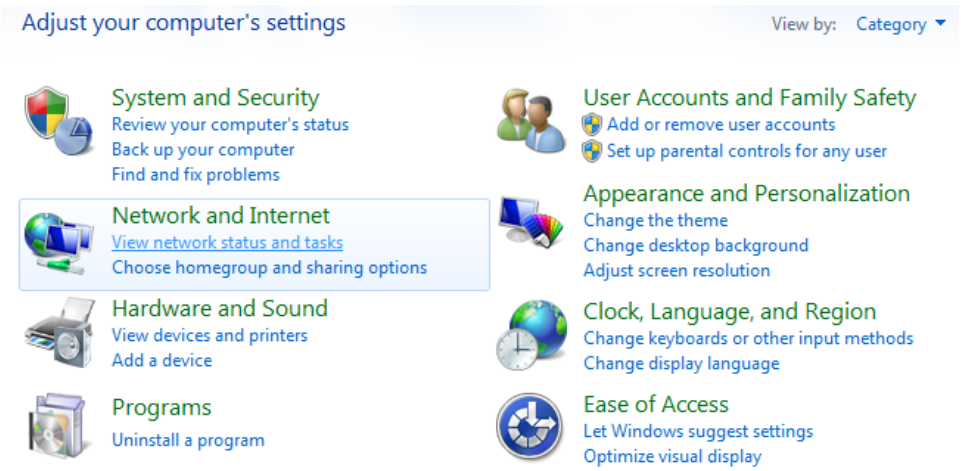
The following describes how to configure the network settings of a Windows PC with the IP settings listed above.

This procedure will change the network settings of the Windows PC, if the PC is connected to a network the connection should be removed before performing the changes. To restore the network settings of the PC record the current settings at Step 7 in the following procedure, then once configuration of the unit has been completed use the recorded values at Step 7 to restore the Windows PC network settings.

1. Open the Control Panel by selecting *Start* ▷ *Control Panel.*

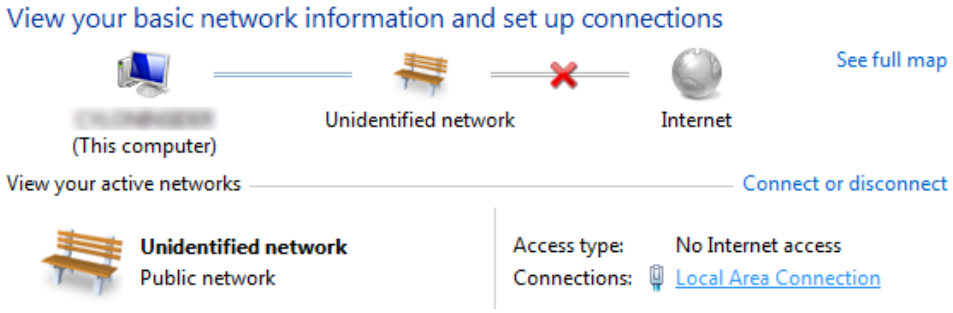


2. The Control Panel will be displayed.



3. Under the section titled **Network and Internet** click the link *View network status and tasks*.

4. The Network Sharing window will be displayed. Click the link *Local Area Connection* which is in the section titled View your active networks.



5. The *Local Area Connection Status* dialogue box will be displayed, as shown on the left of Figure 1, click the *Properties* button.

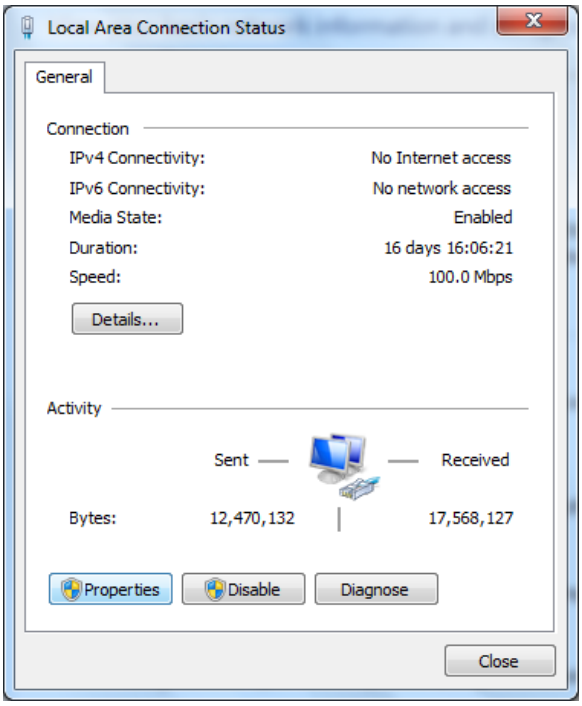


Figure 1: Local Area Connection Status and Properties dialogue boxes.

6. The Local Area Connection Properties dialogue box, as shown on the right of Figure 2, will be displayed. Click on *Internet Protocol (TCP/IP)* to highlight it and then click the *Properties* button.

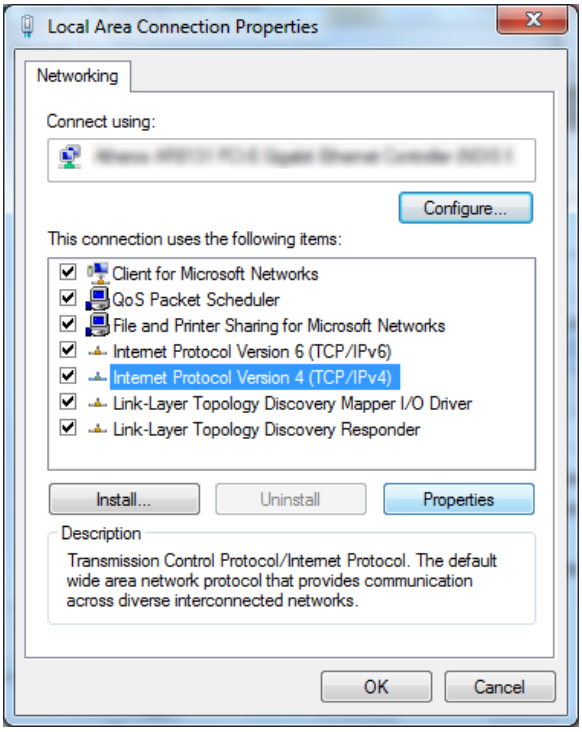


Figure 2: Local Area Connection Status and Properties dialogue boxes.

7. The Internet Protocol (TCP/IP) Properties dialogue box, change the settings to match those shown in Figure 3, and then click “OK”

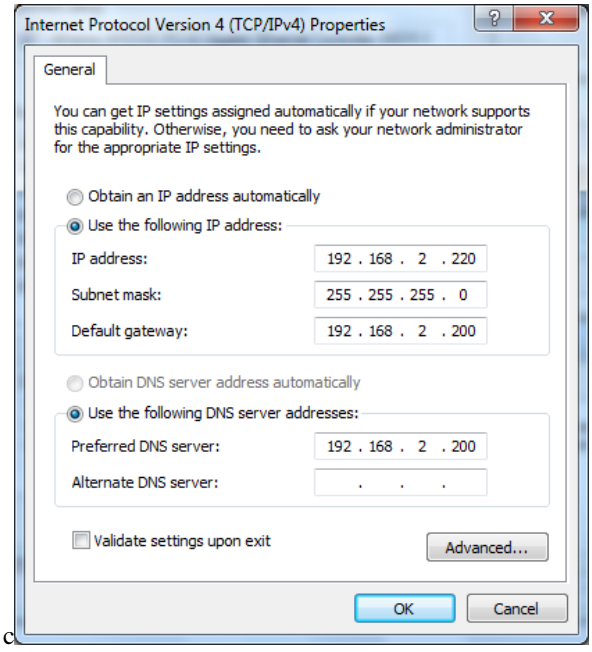


Figure 3: Internet Protocol (TCP/IP) Properties dialogue box showing the recommended IP settings.

If a web browser was open prior to making the network changes, then it will need to closed and re-started before attempting to connect.

2.3 Connecting to the Web Server

- Open a web browser on the PC and browse to the default IP address for the unit as shown:

- A login box similar to Figure 4 will pop up. If the box fails to display, re-check the cable connections to the unit and the IP address settings of the PC.

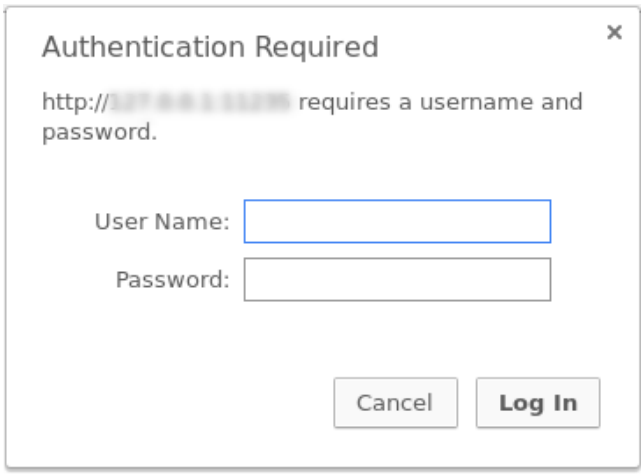


Figure 4: Web login box

- Enter the following login details:
  - User Name: admin
  - Password: westermo
- The Status summary page will be displayed, it will be similar to Figure 5.

Note: As the unit has not yet been configured it is likely that some faults will be indicated.

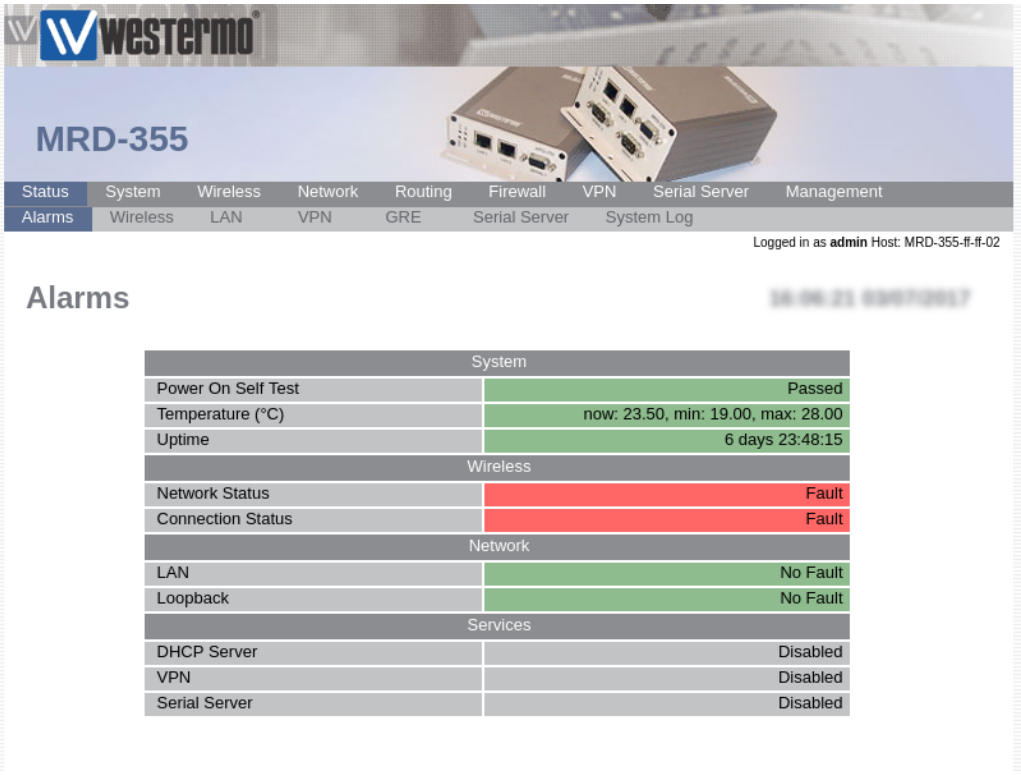


Figure 5: Status summary

3 Web Page Layout

This chapter describes the web page layout and menu structure. The pages are arranged in functional groups accessible via the main menu. For each main menu a number of sub-menu pages provide access to specific information and setting. When a main menu item is select the first sub-menu page is automatically displayed.

This section does not described how to connect to the web interface of the device. For information on connecting to the web server of the device refer to Section 2

3.1 Page Layout

To illustrate the page layout the Status web page is shown in figure 6, this is first page to be displayed when a connection to the web server is established. At the top of the page, below the header section, is the menu which consists of two rows of tabs. The top row is the main menu, the sub-menu tab row is directly under the main menu. The main menu tabs are used to select a group of related pages and the sub-menu is used to select a page within that group. When a main menu tab is selected the sub-menu option tabs will change allowing individual pages within the group to be selected.

Below the menu is the page title. The title indicates the selected page. Below the title is the page body. This section will contain information and/or configuration settings for the selected function.

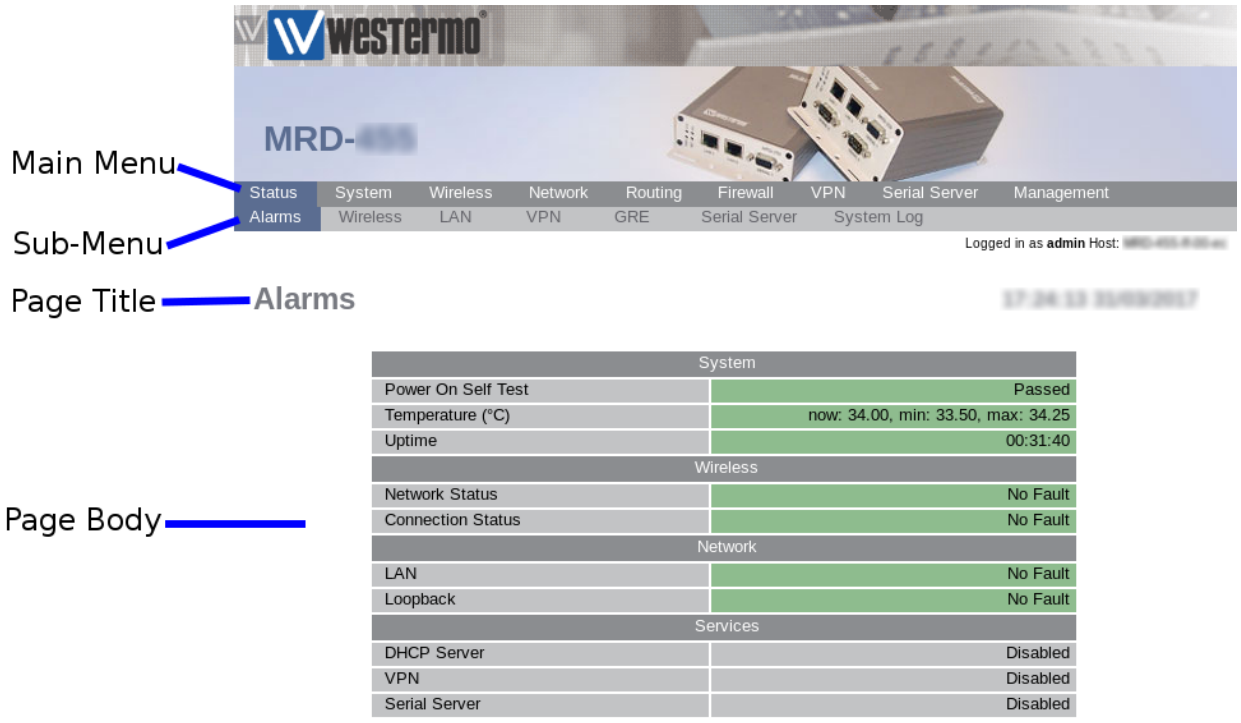


Figure 6: Web Page structure

When a menu item is referenced in the manual it is in the form: Menu ▷ Sub-Menu. For example: Status ▷ Alarms would refer to the Status / Alarms page shown in Figure 6.

3.2 Menu Structure

The section provides a brief description for each of the main menu tabs and for each sub-menu tab.

Not all items listed will be available on all models. For example GPIO will only be displayed for models which have GPIO hardware.
Where possible the most complete menu is shown. Where there are differences in the menus then each alternative will be shown.

3.2.1 Status

The Status tab is used to report the current operating status of the unit.

Figure 7: Status menu - Wireless version.

Figure 8: Status menu - Wireless version with GPIO.

Figure 9: Status menu - DSL version.

Alarms A summary of the alarm status.

Wireless Reports the status of the wireless connection. (Refer to Figures 7 and 8)

DSL Reports the status of the DSL connection. (Refer to Figure 9)

LAN Information on the LAN settings

VPN Reports the status of any active VPNs

GRE Reports the status of any active GRE tunnels

Serial Server Provides and overview of the Serial Server and serial ports.

GPIO Reports state of I/O and sets states of outputs. (Refer to Figure 8)

System Log A log of the system messages.

3.2.2 System

The System tab provides system level information and configuration settings.

Figure 10: System menu

Administration Set host-name, configure the NTP connection, change passwords, set timed re-boot and reboot the modem.

Backup & Upgrade Backup and restore the configuration, upgrade the firmware.

Information Reports model number, serial number, firmware versions, MAC address and wireless IMEI & IMSI.

Syslog Remote syslog settings.

Power Configure the power controller for automatic power shut-down and start-up.

GPIO Configure the digital I/O.

Location GPS configuration.

3.2.3 Wireless

The Wireless tab provides access to the wireless settings.

Figure 11: Wireless menu

Network Operating mode, frequency band selection and SIM card PIN settings.

Packet Mode Profile management and selection, connection state selection.

Connection Management Connection establishment and maintenance options.

Circuit Switched Mode Circuit Switched Data (CSD) mode selection and configuration.

SMS SMS triggers and access control.

3.2.4 DSL

The DSL tab provides access DSL settings, this includes the VDSL and ADSL settings and the options for setting the operating mode.

Figure 12: DSL menu

Network The line and interface general settings.

VDSL The settings for VDSL operation.

ADSL The settings for ADSL operation.

Connection Management The connection management settings.

3.2.5 Network

The Network tab is used to access the Local Area Network (LAN), Dynamic Host Configuration Protocol (DHCP) and DNS settings.

Figure 13: Network menu

LAN LAN and DHCP settings.

Loopback Loopback interface settings.

DNS Manual and Dynamic DNS settings.

GRE Generic Routing Protocol settings.

Diagnostics Verify network connectivity with Ping and Traceroute.

3.2.6 Routing

Routing support includes static and dynamic routing as well as policy and Quality of Service (QoS) based routing. Routing options are accessed via the Routing tab.

Figure 14: Routing menu

Default & Static Define the default route and static routes.

Dynamic Dynamic routing options.

VRRP Configure the Virtual Routing Redundancy Protocol.

Policy Define policy based routes.

QoS Quality of Service (QoS) options and define QoS routes.

3.2.7 Firewall

The Firewall tab allows configuration of the firewall settings which include the definition of port forwards and packet filters.

Figure 15: Firewall menu

Setup Enable NAPT, stateful packet inspection and connection tracking options.

Access Control Define which modem services can be accessed from the wireless interface and VPN tunnels.

DoS Filters Define with Denial of Service filters are enabled.

Custom Filters Define and edit custom packet filters.

Port Forwards Define and edit port forwards.

Custom NAT Define and edit custom Network Address Translation rules.

MAC Filters LAN MAC Address filtering options.

3.2.8 VPN

The VPN tab provides access to the configuration for the SSL, IPsec, PPTP and L2TP VPNs.

Figure 16: VPN menu

IPsec VPN Enable and configure IPsec VPN tunnels.

SSL VPN Enable and configure SSL based VPN (OpenVPN).

PPTP & L2TP Enable and configure PPTP and L2TP VPN tunnels.

Certificate VPN certificate management.

3.2.9 Serial Server

The Serial Server tab is used to access the configuration options for the serial server and each of the available serial ports.

Figure 17: Serial Server menu

Port Setup Configure the serial server port function and configuration options for each of the available serial ports.

Phone Book Modem dial string phone book management.

3.2.10 Management

The Management tab provides access to the management settings.

Figure 18: Serial Server menu

Events Configure the actions taken when an event occurs.

SNMP Configure SNMP parameters.

DNP3 Configure the internal DNP3 outstation.

Email Email server configuration.

3.3 Symbols

The following symbols are used on the web pages:

Edit Icon. Click this icon to edit the indicated setting.

Delete Icon. Click this icon to delete a setting.

OK Button. Click this button to accept a change.

Update Button. Click this button to save changes.

Reset Button. Click this button to reset the values on the page to the values prior to editing.

Choose File Button. Click to choose a file from the local operating system.

Upload Button. Click this button to upload a file to the unit.

Next Button. Click this button to move to the next page in a multiple page configuration.

Back Button. Click this button to move back a page in a multiple page configuration.

4 Status

The Status pages provide information on the operating state of the unit. These pages will assist in ensuring the unit is operating correctly and if it is not working correctly provide assistance in diagnosing the problem.

The status pages do not refresh automatically. In order to see the current status of a displayed value it may be necessary to refresh the page. This is especially the case for a value which is changing, this could be the case at any time but in particular at start up.

To access the status pages click Status on the main menu a page similar to the one shown in Figure 20 will be displayed.

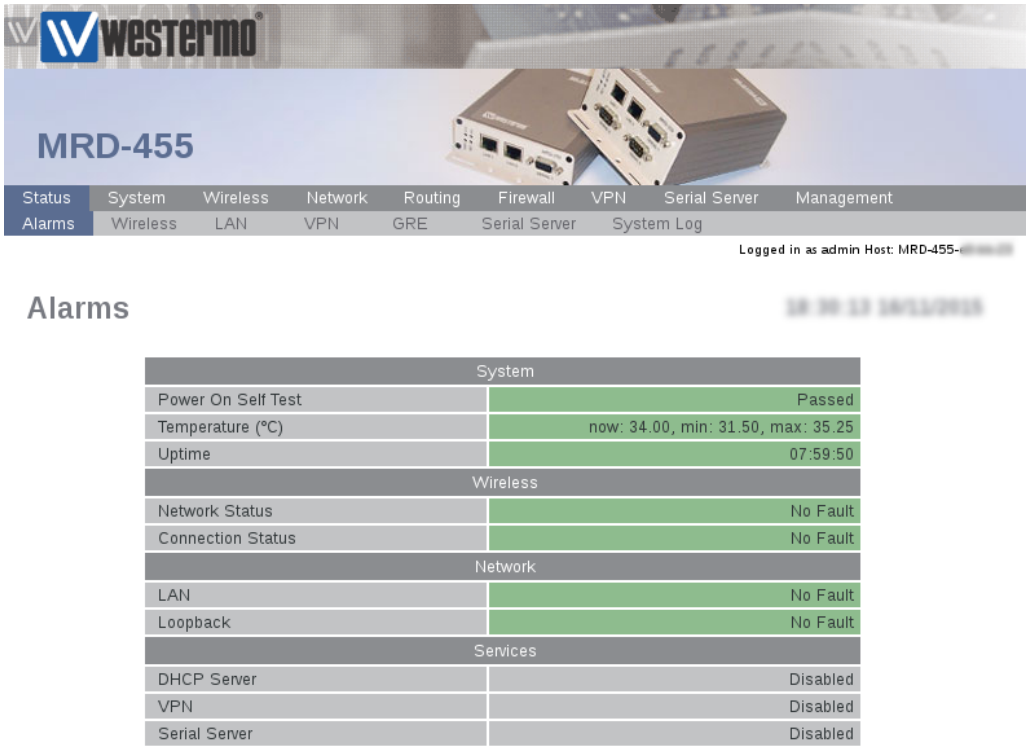


Figure 19: Main status page.

4.1 Alarms

The Status Alarms page is the first page displayed default page once connected to the device, it can also be selected at any time by clicking Status ▷ Alarms. This page provides a summary of the state of the operating services. A service which is operating correctly will be highlighted green, a service with any error will be highlighted red, services not enabled will be shown with a grey background.

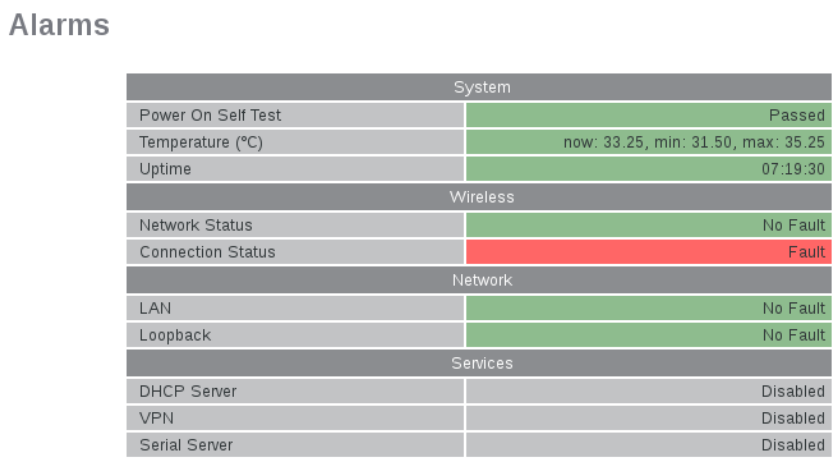


Figure 20: Alarms status page for a Wireless unit, showing Wireless connection status fault.

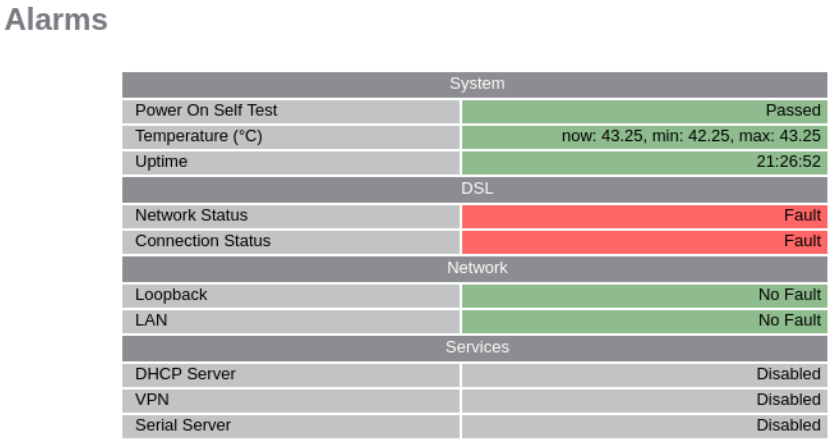


Figure 21: Alarms status page for an DSL unit, showing a connection status fault.

The page is divided into sections representing the status of system level services, the Wireless or DSL interface, LAN interfaces and other services. If a fault is indicated further information can be obtained from the corresponding status page. For example in Figure 20 a fault is indicated for Connection Status in the Wireless section, further information on the fault can be obtained by selecting the Status ▷ Wireless page. Details are shown in the next section.

4.1.1 System

Power On Self Test Indicates the result of the self testing done during the boot sequence. An error would usually indicate a hardware fault and the unit should be returned for service.

Temperature Indicates the current, minimum and maximum operating temperatures.

Uptime Indicates the current running time.

4.1.2 Wireless

Network Status Indicates the current wireless network connection status. This indicates if the unit has established a connection to the network.

Connection Status Indicates the current wireless packet or circuit switched data (CSD) connection status.

Further information can be obtained from the Status ▷ Wireless page.

4.1.3 DSL

Network Status Indicates the current line connection status. This indicates if the unit has established a connection to the DSLAM.

Connection Status Indicates the current packet connection status.

Further information can be obtained from the Status ▷ DSL page.

4.1.4 Network

LAN Indicates the status of the Local Area Network (LAN).

Loopback

Further information can be obtained from the Status ▷ LAN page.

4.1.5 Services

DHCP Server Indicates the status of the Dynamic Host Configuration Protocol (DHCP) server. Further information can be obtained from the Status ▷ LAN page.

VPN Indicates the status of the any Virtual Private Networks. Further information can be obtained from the Status ▷ VPN page.

Serial Server Indicates the status of the Serial Server. Further information can be obtained from the Status ▷ Serial Server page.

4.2 Wireless

The Wireless status page (Status ▷ Wireless) provides details of the current operating state of the wireless interface. The page displayed will depend on the wireless operating mode, Figure 22 shows the page for packet mode, while Figure 23 for Circuit Switched Data (CSD) mode. For information on the different wireless operating modes refer to Section 6.

4.2.1 Network Status

The network status section is common for both modes of wireless operation.

Network Registration Indicates the network registration state.

RF Level (RSSI) Provides an indication of the RF Level or Received Signal Strength Indication (RSSI). The RSSI is a number out of 30 which gives and indication of signal received level. The actual received level is also indicated as a value in dBm.

Bit Error Rate (BER) Indicates the Bit Error Rate or BER of the received signal.

Active SIM Indicates the active SIM. Only relevant for models for more than one SIM.

Provider Indicates the network service provider name and service, the location ID and the cell ID.

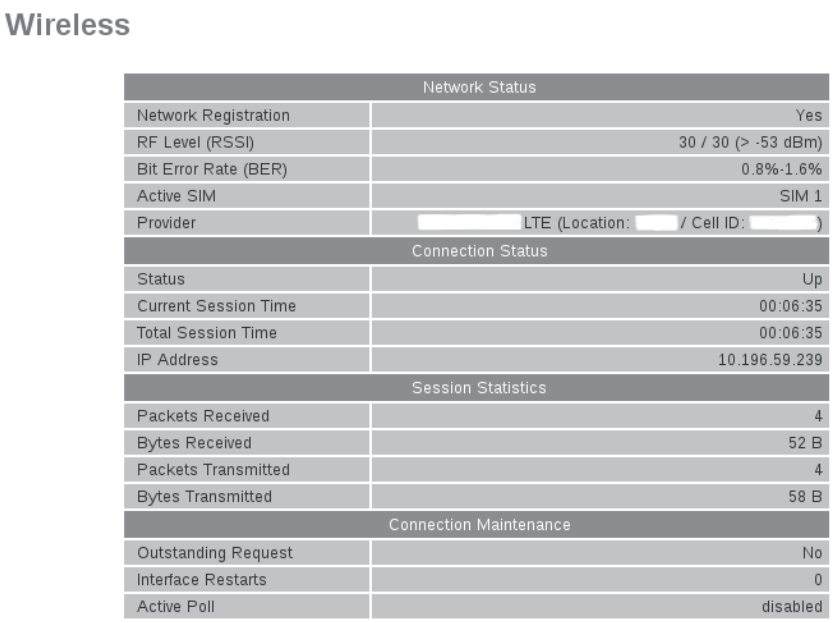


Figure 22: Wireless status page for packet mode.

4.2.2 Connection Status (Packet Mode)

Status The packet connection status. The indication will be 'Up' if the interface is connected or 'Down' if it is not.

Current Session Time Time the current packet session has been active.

Total Session Time The total packet session time since boot.

IP Address The wireless IP address

4.2.3 Session Statistics (Packet Mode)

This section shows the number of data packets and bytes received and transmitted for the session.

Packets Received The total number of packets received.

Bytes Received The total number of bytes received.

Packets Transmitted The total number of packets transmitted.

Bytes Transmitted The total number of bytes transmitted.

4.2.4 Connection Management (Packet Mode)

This section indicates the status of connection management. For details on the configuring connection management for the wireless interface refer to Section 6.

Outstanding Request Indicates if a poll request is outstanding. Will report 'No' if all polls have been answered.

Interface Restarts Indicates the number of times connection management has re-started the wireless interface.

Active Poll Indicates if active polling is enabled. This value is dependant on the settings.

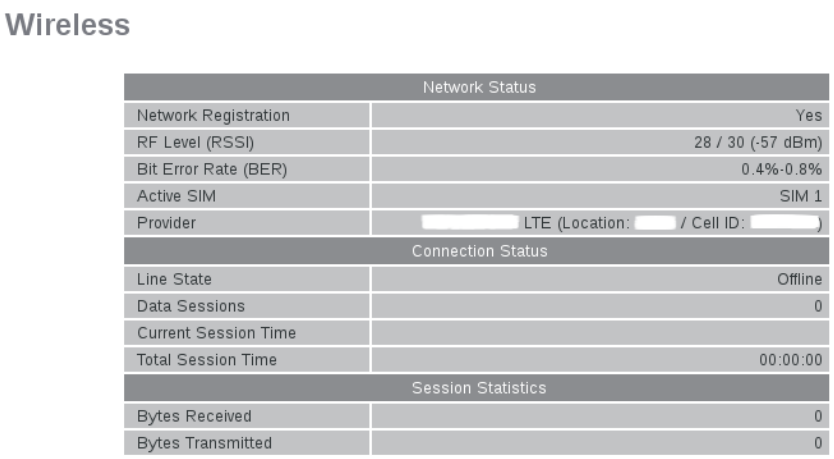


Figure 23: Wireless status page for Circuit Switched Data (CSD) mode.

4.2.5 Connection Status (CSD Mode)

Line State The current status of the connection either *offline* or *connected*.

Last Dial Result The result of the last dial attempt.

Data Sessions The number of successful connections.

Current Session Time Time the current connection has been active.

Total Session Time The total time of all connections since boot.

4.2.6 Session Statistics (CSD Mode)

This section shows the number of data packets and bytes received and transmitted for the session.

Bytes Received The total number of bytes received.

Bytes Transmitted The total number of bytes transmitted.

4.2.7 Connection Status Fault

Continuing the fault example from Section 4.1, Figure 24 shows a Connection Status error for a packet mode connection. The error is due a configuration error, indicating that the wireless packet mode settings need to be checked. For details on the configuring the wireless interface refer to Section 6.

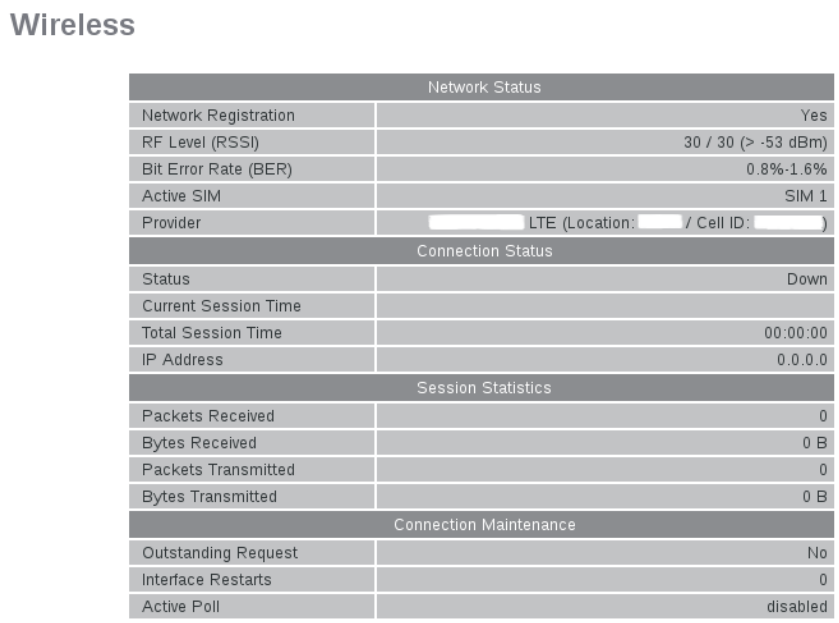


Figure 24: Wireless status page for packet mode displaying a connection error.

4.3 DSL

The DSL status page (Status ▷ DSL) provides details of the current operating state of the DSL interface. For information on configuring the DSL interface refer to Section 7 on page 88.

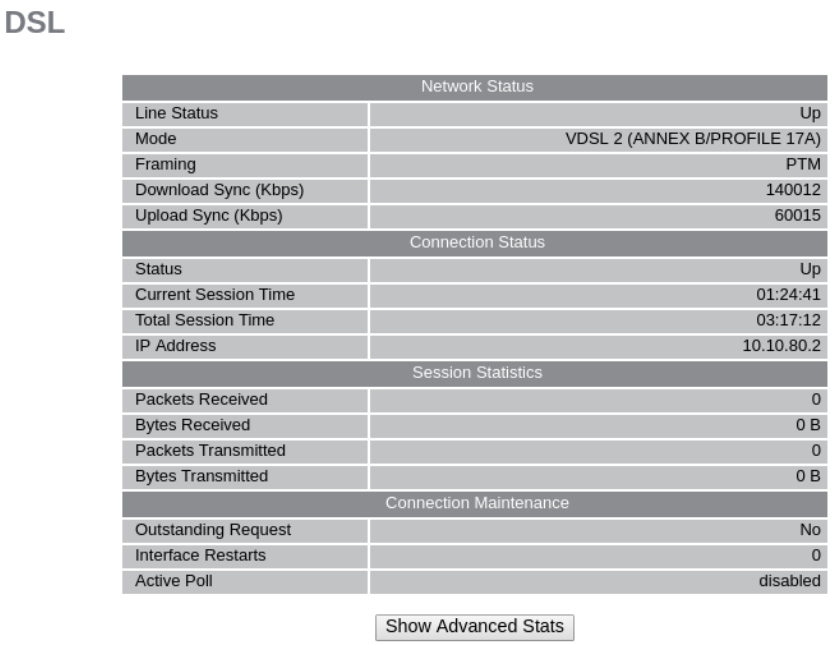


Figure 25: ADSL status page.

4.3.1 Network Status

The section provides information on the status of the ADSL line connection.

Line_Status Indicates the line connection state. When a connection has been established with a DSLM this will be indicated with Up.

Mode Indicates the connection type. For example ADSL, ADSL2+, VDSL it will also indicate the ANNEX and Line profile of the connection.

Framing The framing type of the connection.

Download Sync (Kbps) Indicates the download sync speed in kilobits per second (Kbps).

Upload Sync (Kbps) Indicates the upload sync speed in kilobits per second (Kbps)

4.3.2 Connection Status

The connection status provide details of any packet connections.

Status The packet connection status. The indication will be 'Up' if the interface is connected or 'Down' if it is not.

Current Session Time The time is since the connection was established

IP Address The IP address provided for the connection.

4.3.3 Session Statistics

This section shows the number of data packets and bytes received and transmitted for the session.

Packets Received The total number of packets received.

Bytes Received The total number of bytes received.

Packets Transmitted The total number of packets transmitted.

Bytes Transmitted The total number of bytes transmitted.

4.3.4 Connection Management

This section indicates the status of connection management. For details on the configuring connection management for the DSL interface refer to Section 7.

Outstanding Request Indicates if a poll request is outstanding. Will report 'No' if all polls have been answered.

Interface Restarts Indicates the number of times connection management has re-started the wireless interface.

Active Poll Indicates if active polling is enabled. This value is dependant on the settings.

4.3.5 Advanced Connection Statistics

To access the advanced DSL connection statistics click the Show Advanced Stats button. The page has 2 sections, the first is the line statistics as shown in figure 26, second table contains the Signal Status statistics, Framing details and counters for both upstream and downstream, as shown in figure **??**.

4.3.6 Line Status

This section provides details of the line level connection.

DSL

Line Status	
Line Status	Up
Channel	Fast
Power State	L1

Figure 26: DSL Line Status section of the Advanced Statistics page.

Line Status The current status of the line.

Channel The channel type

Power State The power state.

4.3.7 Advanced Statistics

This section, shown in Figure 27,provides detailed statistical information for the downlink and uplink data. It is divided in 3 sections each of which is described below:

Advanced Statistics		
	Down	Up
Signal Status		
Trellis	On	On
SNR Margin (dB)	119.0	110.0
Line Attn (dB)	23.0	24.0
Signal Attn (dB)	1023.0	1023.0
Pwr (dBm)	107.0	120.0
Sync (Kbps)	140012	60015
Max Sync (Kbps)	161452	66823
PTM Framing		
Bytes	340	340
Frames	4	4
OOS	0	0
Errors	0	0
Discard Packets	0	0
Discard Packets	0	
Counters		
Super Frames	52739	52738
Super Frame Errors	11	6
RS Words	815347201	0
RS Correctable Errors	0	0
RS Uncorrectable Errors	0	0
HEC Errors	34	0
Total Cells	3179048167	1362664307
Data Cells	121	8
Dropped Cells	34	
Total ES	4	4
Total SES	0	0
Total UAS	52	52

Figure 27: DSL Advanced Statistics.

Signal Status: This section provides details of downlink and uplink data lines.

SNR (dB) The Signal to Noise Ratio for the line.

SNR Margin (dB) The noise margin above the minimum required for the indicated sync rate.

Line Attn (dB) The attenuation of the line.

Signal Attn (dB) The signal attenuation.

Pwr (dBm) The receive (downlink) or transmit (uplink) power level.

Sync (kbps) The current data rate at which the connection is synchronised, reported in kilobits per second.

Max (kbps) The maximum theoretical data rate calculated for the line, reported in kilobits per second.

PTM Framing:

Bytes The number of bytes sent or received

Frames The number of frames sent or received.

OOS Out Of Sync.

Errors The number of errored frames.

Discard _Packets The number of discarded packets due to error.

Counters:

Super Frames Traditionally, a superfame consists of 24 frames contiguously transmitted together. In ADSL, a superframe consists of 68 adsl frames plus a synchronisation frame. The ADSL modem generates 4000 frames per second. The global duration of an ADSL superframe is 17ms.

Super Frame Errors Count of the Super Frames received which had an error. This is similar to CRC error.

RS Words Count of the total number of Reed-Solomon code words transmitted/received.

RS Correctable Errors The number of Reed-Solomon code words with correctable errors. Reed-Soloman is a method of Forward Error Correction and therefore a count of data successfully recovered. See FEC.

RS Uncorrectable Errors The number of Reed-Solomon code words that had uncorrectable errors. Reed-Soloman is a method of Forward Error Correction. Uncorrectable Errors are those that are too severe to be corrected by FEC.

HEC Errors Header Error Check/Correction
Count of HEC Errors. HEC is a type of CRC error check which has been performed on the header of an ATM cell, but 1 bit errors can be corrected. This count is usually where HECs have been uncorrected and have been discarded. If these errors are too high within a short period of time it will slow throughput... and could even lead to connection instability. See Out Of Cell Delineation.

Total Cells The total number of ATM cells.

Data Cells The total number of ATM cells containing data.

Dropped Cells The total number of ATM cells dropped due to error.

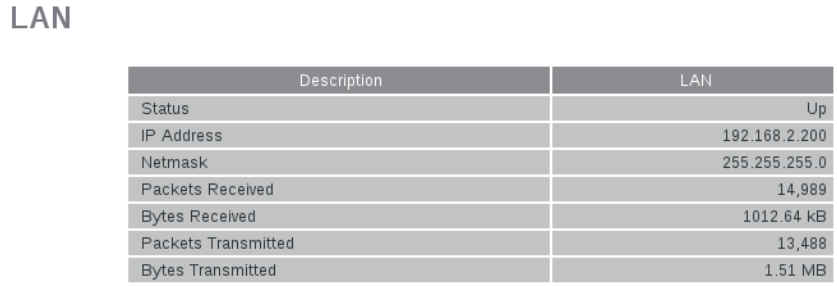
Total ES The number of errored seconds. A one second period of time in which either one or more coding violations occurred OR at least one Loss of Signal events occurred. Its not unusual to see occasional ES.

Total SES The number of Serverly Errors Seconds. A Severely Errored Second is a one second period which contains 30% or more errored blocks OR several other events such as one or more Out Of Frame (OOF) error.

Total UAS Unavailable seconds. Ten consecutive SES's will trigger a UAS event, and will remove the path from use. The path will become usable again after 10 consecutive seconds with no SES.

4.4 Local Area Network (LAN)

The Local Area Network (LAN) status page (Status ▷ LAN) provides details of the current operating state of the LAN or Ethernet interface. A second section displaying DHCP lease information will be shown if the DHCP server has been enabled. For LAN settings refer to Section 8 on page 110.



LAN

Description	LAN
Status	Up
IP Address	192.168.2.200
Netmask	255.255.255.0
Packets Received	14,989
Bytes Received	1012.64 kB
Packets Transmitted	13,488
Bytes Transmitted	1.51 MB

Figure 28: LAN Status page.

4.4.1 LAN Statistics

Provides information of the LAN interface. Refer to figure 28

Status The status of the interface.

IP Address The IP address if the interface

Netmask The netmask of the interface

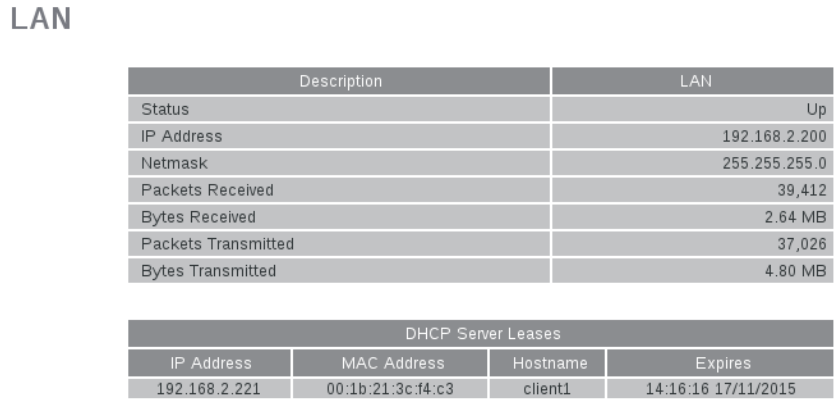
Packets Received The total number of packets received.

Bytes Received The total number of bytes received.

Packets Transmitted The total number of packets transmitted.

Bytes Transmitted The total number of bytes transmitted.

4.4.2 DHCP Server Leases



LAN

Description	LAN
Status	Up
IP Address	192.168.2.200
Netmask	255.255.255.0
Packets Received	39,412
Bytes Received	2.64 MB
Packets Transmitted	37,026
Bytes Transmitted	4.80 MB

DHCP Server Leases			
IP Address	MAC Address	Hostname	Expires
192.168.2.221	00:1b:21:3c:f4:c3	client1	14:16:16 17/11/2015

Figure 29: LAN Status page with DHCP lease information.

The DHCP Server Leases section will only been shown if the DHCP server has been enabled. If the server has been enabled the LAN Status page will be similar to that shown in figure 29.

IP Address The assigned IP address.

MAC Address The MAC address of the device which requested the lease.

Hostname The reported host-name of the device which requested the lease.

Expires The lease expiry time.

4.5 Virtual Private Network (VPN)

The Virtual Private Network (LAN) status page (Status ▷ VPN) provides details of the current operating state of any configured Virtual Private Network (VPN). For VPN settings refer to Section 11 on page 162.

4.5.1 IPsec Connection Status

Provides information on the state of any IPsec connections. Refer to figure 30

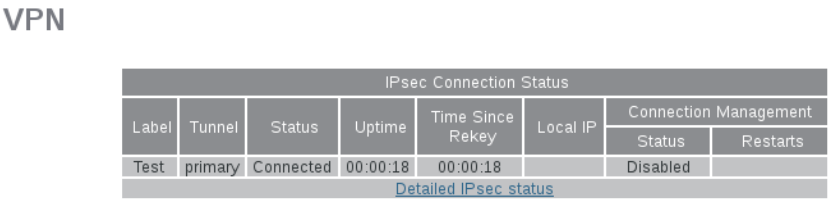


Figure 30: VPN Status page showing IPsec connection status.

Label The name given to the particular tunnel

Tunnel The tunnel type either Primary or Secondary.

Status The connection status. When connected will report 'Connected'.

Uptime The time since the connection was established.

Time Since Rekey The time since the last re-key.

Local IP The local IP address if configured.

Connection Management Status The current state of connection management.

Restarts The number of connection management initiated re-starts.

4.5.2 Detailed IPsec Status

To display detailed logs of the IPsec connection click the link 'Detailed IPsec status' below the status table. The log will be similar to that shown in figure 31.

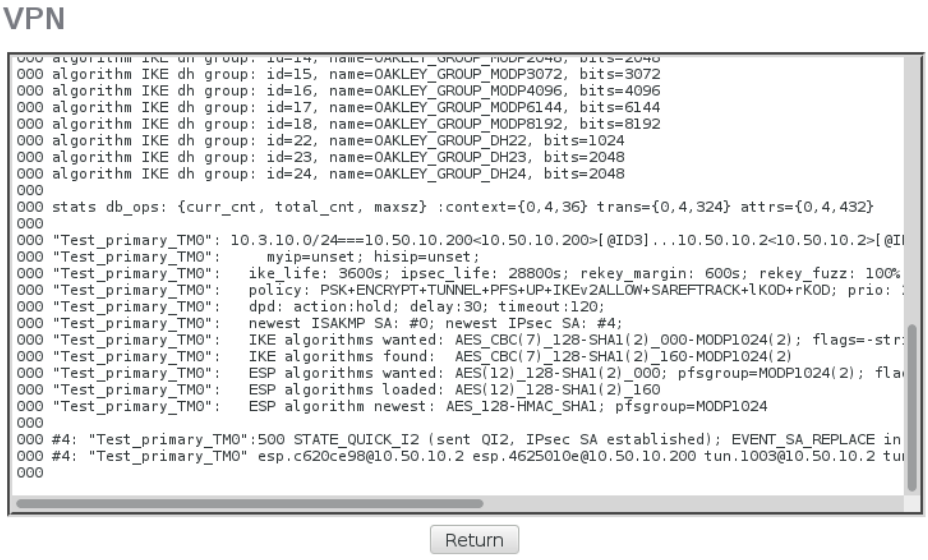


Figure 31: Detailed IPsec connection status.

4.5.3 SSL Connection Status

Provides information on the state of any SSL VPN connections. Refer to figure 32

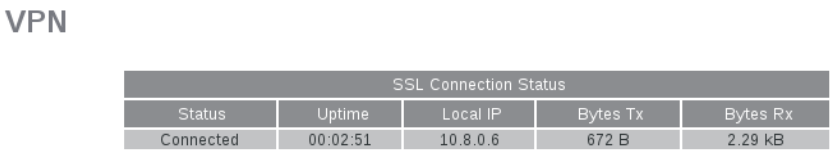


Figure 32: VPN Status page showing SSL connections status .

Status The connection status. When connected will report 'Connected'.

Uptime The time since the connection was established.

Local IP The local IP address.

Bytes Tx The number of bytes transmitted.

Bytes Rx The number of bytes received.

4.5.4 IPsec & SSL Connection Status

If both IPsec and SSL VPN connections are configured both be displayed as shown in figure 32

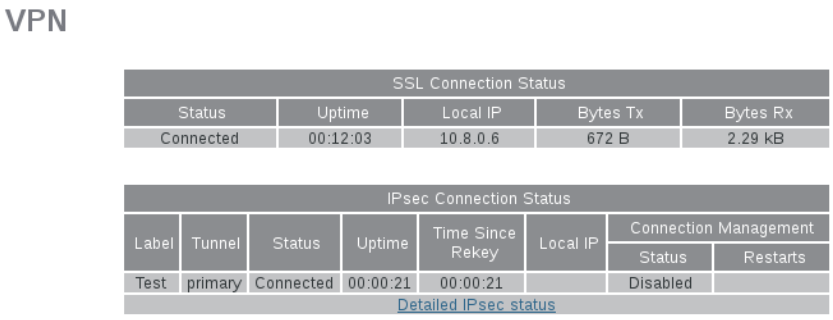


Figure 33: VPN Status page showing both IPsec and SSL connection status.

4.6 Generic Routing Encapsulation (GRE)

The Generic Routing Encapsulation (GRE) status page (Status ▷ GRE) provides details of the current operating state of any configured GRE tunnels. For GRE settings refer to Section 8.5 on page 117.

4.6.1 GRE Tunnel Details

The first section provides details for all configured GRE tunnels. The tunnel label is listed at the top of the column. In figure 34 the details of the tunnel labelled 'gre1' are shown.

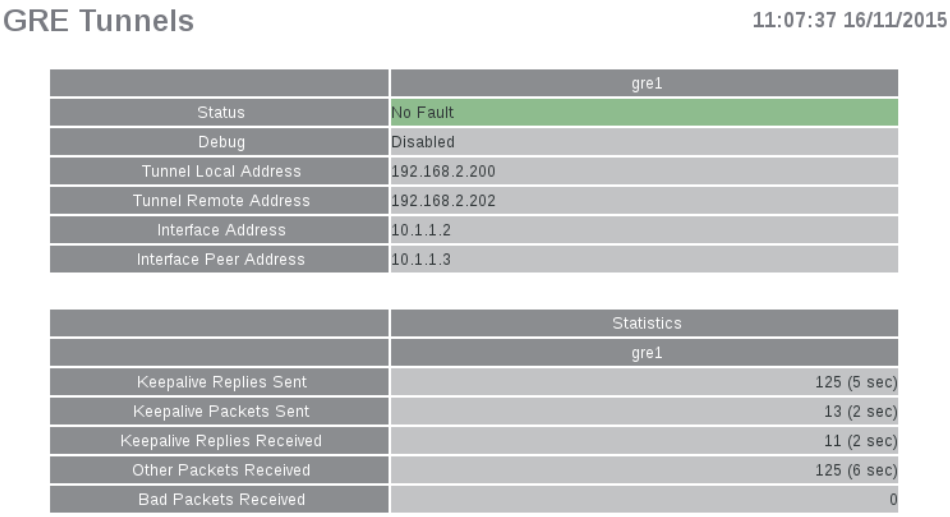


Figure 34: GRE Status page.

Status The operating status of the tunnel. When established and operating correctly will display 'No Fault'.

Debug The debug state either Enabled or Disabled.

Tunnel Local Address The local IP address of the tunnel.

Tunnel Remote Address The remote IP address of the tunnel.

Interface Address The IP address of the interface over which the tunnel will be established.

Interface Peer Address The IP address of the remote interface over which the tunnel will be established.

4.6.2 GRE Tunnel Statistics

The section section of the table details the statistics of the configured GRE tunnels.

Keepalive Replies Sent The number of keep-alive replies sent in response to keep-alive packets received.

Keepalive Packets Sent The number of keep-alive packets sent to the remote interface.

Keepalive Replies Received The number of keep-alive replies received in response to keep-alive packets sent.

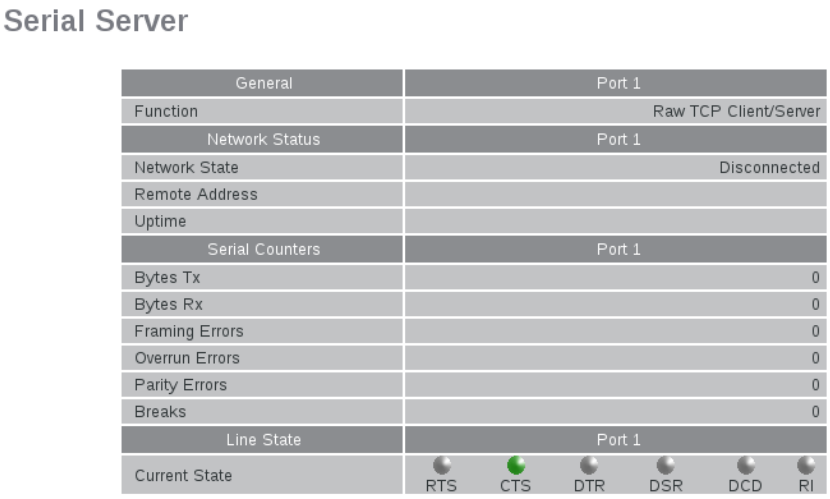
Other Packets Received The number of packets received excluding keep-alive packets.

Bad Packets Received The number of errored packets received.

4.7 Serial Server

The Serial Server status page (Status ▷ Serial Server) provides details of the current operating state of any serial ports configured to work with the serial server. For Serial Server settings refer to Section 12 on page 207.

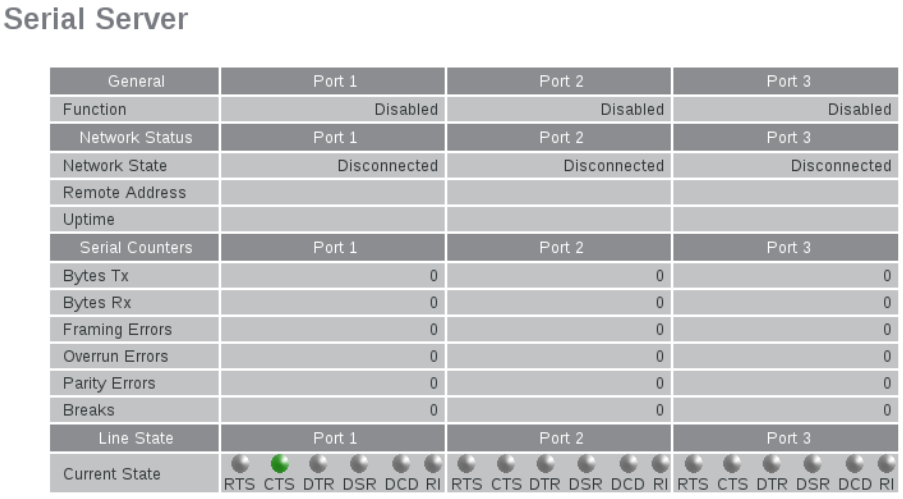
The status page contains 1 column for each serial port of the unit, Figure 35 shows the page for a unit with 1 serial port and 36 shows the page for a unit with 3 serial ports.



Serial Server

General	Port 1
Function	Raw TCP Client/Server
Network Status	**Port 1**
Network State	Disconnected
Remote Address	
Uptime	
Serial Counters	**Port 1**
Bytes Tx	0
Bytes Rx	0
Framing Errors	0
Overrun Errors	0
Parity Errors	0
Breaks	0
Line State	**Port 1**
Current State	RTS CTS DTR DSR DCD RI

Figure 35: Serial Server Status page for unit with 1 serial port.



Serial Server

General	Port 1	Port 2	Port 3
Function	Disabled	Disabled	Disabled
Network Status	**Port 1**	**Port 2**	**Port 3**
Network State	Disconnected	Disconnected	Disconnected
Remote Address			
Uptime			
Serial Counters	**Port 1**	**Port 2**	**Port 3**
Bytes Tx	0	0	0
Bytes Rx	0	0	0
Framing Errors	0	0	0
Overrun Errors	0	0	0
Parity Errors	0	0	0
Breaks	0	0	0
Line State	**Port 1**	**Port 2**	**Port 3**
Current State	RTS CTS DTR DSR DCD RI	RTS CTS DTR DSR DCD RI	RTS CTS DTR DSR DCD RI

Figure 36: Serial Server Status page for unit with 3 serial ports.

General Function Configured function of the port.

Network Status Network State Operating state of the port, either Connected or Disconnected.

Remote Address The IP address of the connection

Uptime The time since the connection was established.

Serial Counters Bytes Tx The number of bytes transmitted since the connection was established.

Bytes Rx The number of bytes received since the connection was established.

Framing Errors The number of receiver framing errors.

Overrun Errors The number of receiver overrun errors.

Parity Errors The number of receiver parity errors.

Breaks The number of receiver breaks.

Line State **Current State** Report of the current state of all signal lines. The indicator is green when asserted and grey when de-asserted.

RTS Ready To Send

CTS Clear To Send

DTR Data Terminal Ready

DSR Data Set Ready

DCD Data Carrier Detect

RI Ring Indicate.

4.8 General Purpose Input / Output (GPIO)

The General Purpose Input / Output (Status ▷ GPIO) provides details of the current operating state of any GPIO for the device. Figure 37 is an example of the GPIO status page. For GPIO settings refer to Section 5.7 on page 42.

GPIO

GPIO Inputs					
Index	Label	Enabled	State	Toggles	Closed time
1	Input-1	Yes	Closed	2	00:00:28
2	Input-2	Yes	Closed	2	00:00:28
3	Input-3	Yes	Open	0	00:00:00
4	Input-4	Yes	Closed	2	00:00:28
5	Input-5	Yes	Closed	2	00:00:28
6	Input-6	Yes	Open	0	00:00:00
7	Input-7	Yes	Closed	2	00:00:28
8	Input-8	Yes	Closed	2	00:00:28

GPIO Outputs					
Index	Label	Enabled	State	Toggles	Closed time
1	Output-1	Yes	Closed	2	00:00:11
2	Output-2	Yes	Closed	2	00:00:11
3	Output-3	Yes	Closed	2	00:00:11
4	Output-4	Yes	Open	0	00:00:00
5	Output-5	Yes	Open	0	00:00:00

Figure 37: GPIO Status page.

4.8.1 GPIO Inputs

Provides information on the current state and past closures of the GPIO inputs.

Index The number of the input starting at 1 for the first input.

Label The configured label for the input.

Enabled The current state of the input either Yes (Enabled) or No (Disabled).

State The current state of the input either Closed (Active) or Open.

Toggles The number of times the input has toggled to the closed state.

Closed time The total accumulated time for which the input has been closed.

4.8.2 GPIO Outputs

Provides information on the current state and past closures of the GPIO inputs.

Index The number of the output starting at 1 for the first output.

Label The configured label for the output.

Enabled The current state of the output either Yes (Enabled) or No (Disabled).

State The current state of the output either Closed (Active) or Open.

Toggles The number of times the output has toggled to the closed state.

Closed time The total accumulated time for which the output has been closed.

4.9 System Log

The system log provides a list of messages from various services. The messages are time and date stamped. The page will display up to 1,000 lines of the log file. As the logs are persistent once the unit has been operating long enough for the log to contain at least 1,000 lines the page will consistently display 1,000 lines.

Figure 38 is an example of the System Log page.

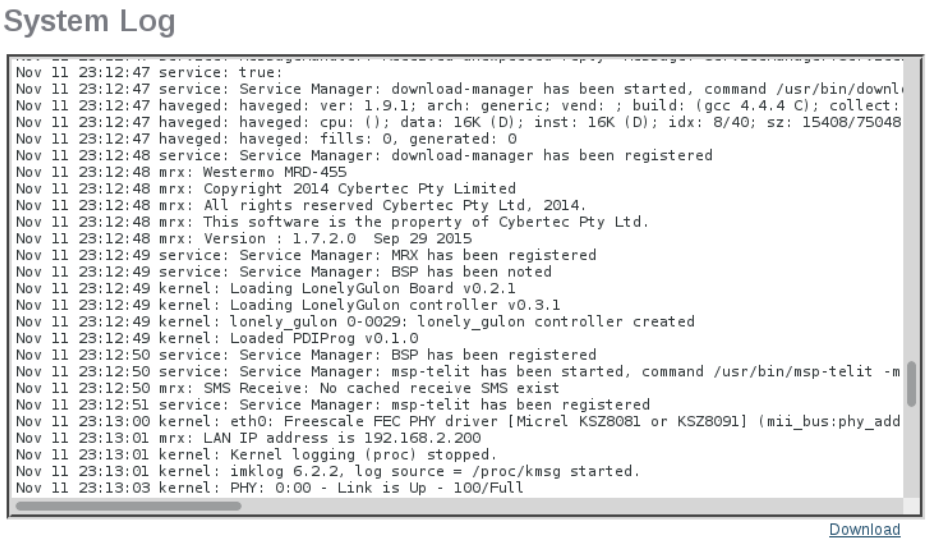


Figure 38: System Log page.

4.9.1 System Log Download

The system log can be downloaded from the unit as a plain text file by clicking the link 'Download' at the bottom right of the page. The downloaded file will be up to 1 Mbyte in size. Due to the way in which the log files are rotated once the unit has been operating for some time to downloaded file will be between 500 Kbytes and 1 Mbyte in size.

5 System

The System tab section provides configuration options and access to features to related to the administration and system level configuration of the unit. Options which can be configured include:

- Host-name for the device.
- Time and Date settings.
- Edit users and passwords
- RADIUS server.
- Shut-down and re-boot.
- Save and restore the device configuration.
- Update the device firmware.
- View device information, serial number, MAC address etc.
- Power controller.
- General Purpose Input and Output (GPIO).

The System pages are accessed by clicking System on the main menu.

5.1 Administration

The main *Administration* page is the default page and will be displayed when System is selected from the main menu. It can also be selected by the menu combination System ▷ Administration at any time. A page similar to that shown in figure 39 will be displayed.

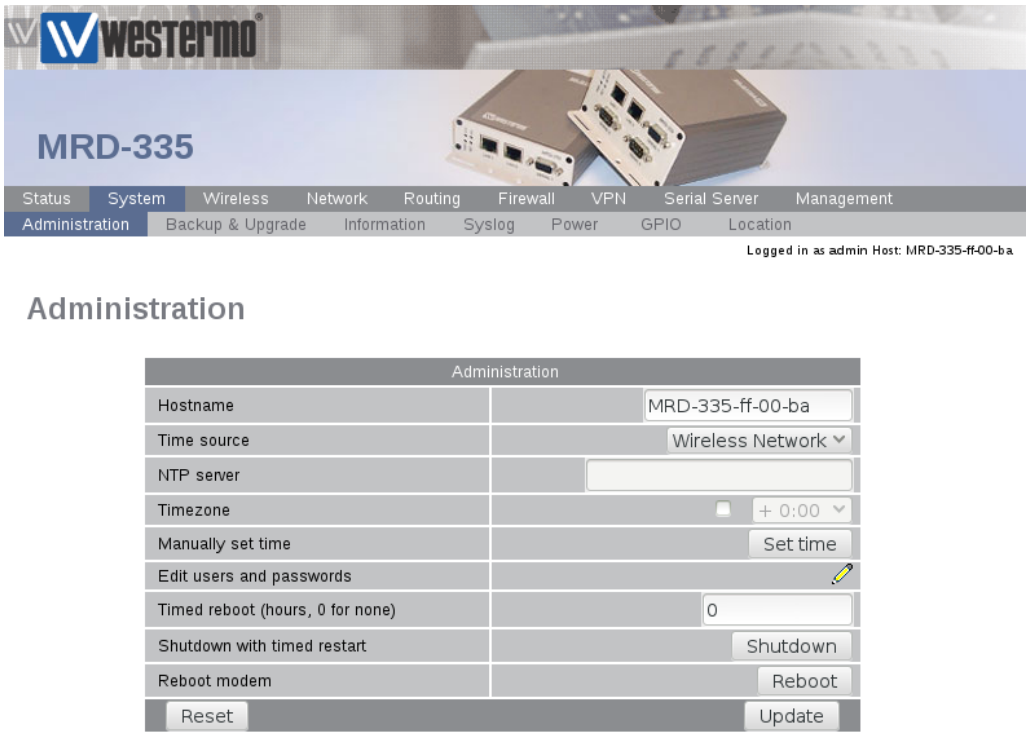


Figure 39: System Administration page.

5.2 System Configuration

The System configuration options are accessed from the main System Administration page. Figure 40 is an example of the page.

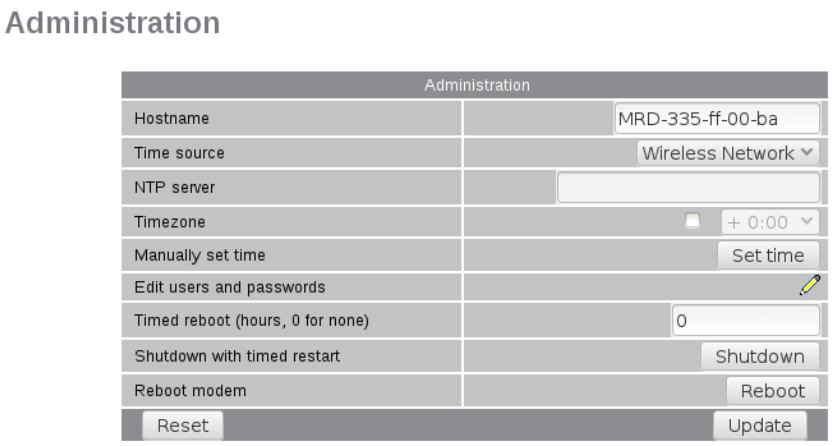


Figure 40: The main System Administration configuration page.

5.2.1 Setting the system host-name

The host-name for the modem can be set in the **Hostname** field. The host-name is limited to 32 characters and can only contain letters 'a' through 'z' and 'A' through 'Z', digits '0' through '9' and hyphens '-', no other symbols, punctuation characters, or white space are permitted. The host-name is displayed on this page, reported via SNMP and used in system-generated SMS messages.

The default host-name is 'SMMMM-xx-xx-xx ' where:

MMMM is the model number; and

xx-xx-xx is the last 3 octets of the unit's MAC address.

As this host-name is based on the MAC address of the unit it will be unique.

5.2.2 Selecting the Time Source

Time Source The time source is selected from the 'Time source' drop-down box. The selections are:

Wireless Network Use the 3G/4G connection for the time source. (Default)

NTP Network Time Protocol

Manual The time and date are set manually with no external time synchronisation.

If the default option of Wireless Network is selected no further configuration is required, if either of the other options is selected further configuration will be required.

5.2.3 Using the Network Time Protocol (NTP)

The time source may be configured to read the current time from a network time server using the NTP protocol. To enable NTP, select **NTP** from the Time source drop-down box and then enter the IP address or host-name of an NTP server in the text field. To correctly adjust the time from the NTP server to the local time zone, the **Timezone** must be set. Select the appropriate number of hours for the time zone in which the unit will be operating, from the drop-down list.

5.2.4 Manual Setting of the time and date

To manually set the time select **Manual** from the Time source drop-down box and then click the Set time button, a pop-up box will be displayed similar to that shown in Figure 41. Adjust the time and date to the desired settings and click the Set button to save.

Figure 41: Manually setting the time and date.

When the time source is set to Manual no external synchronisation will be performed. This means the internal Real Time Clock (RTC) could drift and so not report the correct time. If the unit is left un-powered for such time as the RTC power source is lost the time settings will also be lost.

5.2.5 Editing users and passwords

To change the passwords used for modem access or to enable RADIUS authentication, click the icon in the **Edit users and passwords** field. A page similar to that shown in Figure 42 will be displayed.

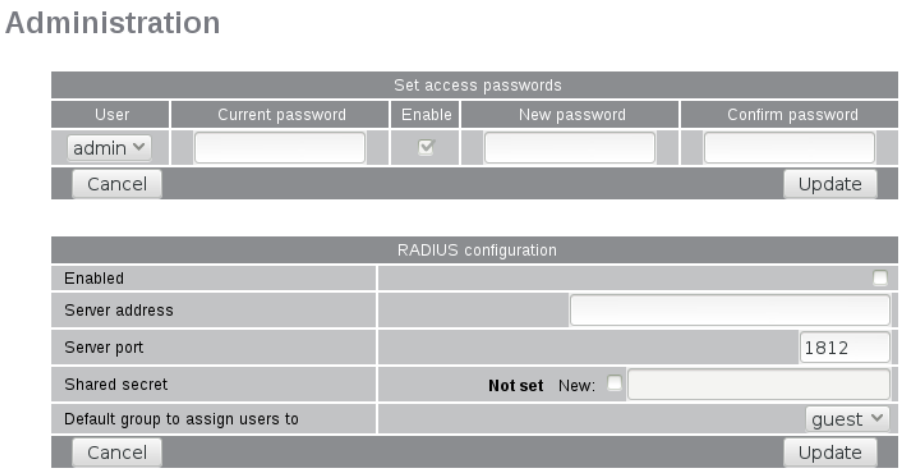


Figure 42: Administration page to change user passwords and to configure RADIUS.

5.2.5.1 Changing basic user passwords

There are two users, each with different access levels:

admin The admin user can view and change the configuration of the modem and view the status.

guest The guest user can view the configuration and status of the modem. This user is disabled by default.

The admin user is enabled by default. The guest user is not enabled by default, to enable the guest ensure the Enable check-box is checked.

The passwords for both users are set using the **Set access passwords** table.

To change a user's password, use the drop-down box in the **User** column to select the appropriate user. Then, enter the **Current password** for the user, followed by the **New password**, repeated to avoid errors in the **Confirm password** field.

To enabled the guest user check the **Enabled** check-box.

Click the Update button to confirm and save the changes.

5.2.5.2 Configuring RADIUS authentication

User credentials can also be authenticated against a RADIUS server. The fields below need to be correctly configured to enable this feature. The RADIUS server administrator will be able to provide the necessary information.

RADIUS Configuration Enabled Set this field to enable RADIUS authentication.

Server address Enter the IP address of the RADIUS server.

Server port Enter the IP port of the RADIUS server. This is normally 1812 or 1645.

Shared secret This is a password that is used to encrypt traffic sent to the RADIUS server. To set this field, click the **New** check-box and enter the secret in the text field.

Default group to assign users to If the RADIUS server fails to provide information regarding the access level of a newly authenticated user, the default set in this field will be used.

RADIUS attribute Service-Type (6) is used to determine the access level of a user. A user with Service-Type set to Administrative-User (6) will be granted the **admin** access level. A user with Service-Type set to NAS-Prompt (7) will be granted the **guest** access level.

Click the Update button to confirm and save the changes.

5.2.6 Setting a timed reboot

In some applications, it may be desirable for the unit to re-boot at a timed interval. To enable this feature, enter a time (in hours) in the **Timed reboot** field. Once the modem has run for the number of hours entered, it will reboot and start the system again. To disable this feature, set the field to 0.

The use of the timed reboot feature is not recommended. The device continuously monitors the operating conditions and network status, if a fault is detected corrective action is taken in order to re-establish network connections. Using the connection management features details in Section 6 will provide a more reliable and stable solution.

5.2.7 Shutdown

A shut-down can be initialised by clicking the Shutdown button, this is recommended before removing power. A shut-down will disconnect the device from any network to which it is connected, terminated all processors and close all connections, the power supplies will then be turned off. The complete shut-down will take approximately 2 minutes. The power will remain off for approximately 1 minute, during this time the power can safely be removed. After this time if the power is still connected the device will start up again and resume normal operation.

It is recommended to shut-down the unit using the method described before removing the power.

5.2.8 Rebooting the modem

A re-boot can be initiated by clicking the Reboot button and then confirming the action when the pop-up dialogue box that appears. The reboot will take around 75 seconds.

The power supplies remain on during a reboot, this differs from a shut-down where the power supplies are turned off.

5.2.9 Update & Reset

After completing configuration changes, click the Update button to confirm and save the changes, or click the Reset button to clear any changes.

5.3 Backup & Upgrade

This section describes how to save the current modem configuration, restore a saved configuration and update the firmware.

To access the Backup & Upgrade options select System ▹ Backup & Upgrade. The Backup & Upgrade page will be displayed as shown in figure 43.

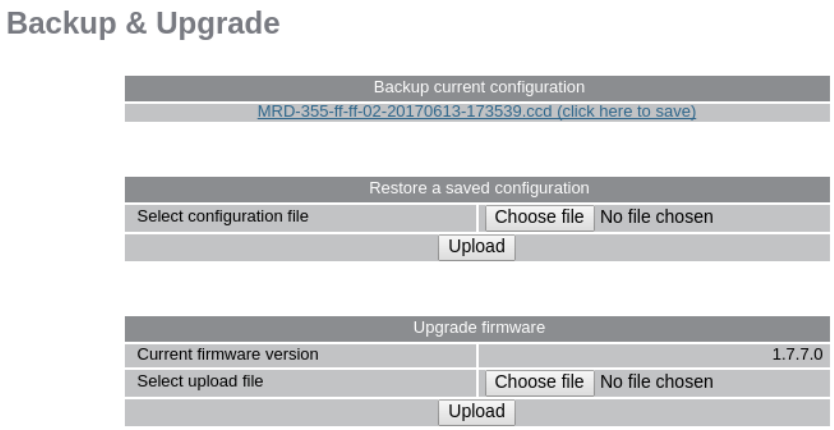


Figure 43: Backup and Upgrade page

5.3.1 Backing up the current configuration

The configuration can be downloaded and saved as a file, this file can then be used to restore the configuration of the unit at some later time or used to configure multiple units with the same configuration.

To save the current configuration click on the link in the section titled **Backup current configuration**. A pop-up box similar to that shown in figure 44 will be displayed. Select **Save to Disk** and click **OK.** Select a suitable location to save the file.

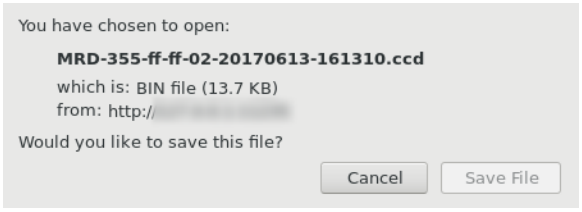


Figure 44: Saving the configuration

The file-name is in the format <Host-name>-<Date>-<Time>.ccd where:

Host-name is the host-name for the unit. Refer to Section 5.2.1 for details.

Date is the current date in the format YYYYMMDD where:

YYYY is the year
MM is the month
DD is the day

Time is the time in the format HHMMSS, where:

HH is the hour
MM is the minute
SS is the seconds

.ccd is the file type. (Configuration file).

The file-name for the configuration file is set when the page is first loaded and will remain as long as the page is not refreshed. The file-name will be updated each time the page is refreshed.

5.3.2 Restoring a saved configuration

To restore a configuration, click the Choose file button in the section titled **Restore a saved configuration.** Select the configuration file, which will then be shown in the text box, as shown highlighted in figure 45. Click the Upload button to transfer the file to the unit.

Once the upload is complete, the unit must be rebooted immediately so the restored configuration can take affect. The details for performing a reboot can be found in Section 5.2.8 above.
Do not make any changes to configuration prior to rebooting.

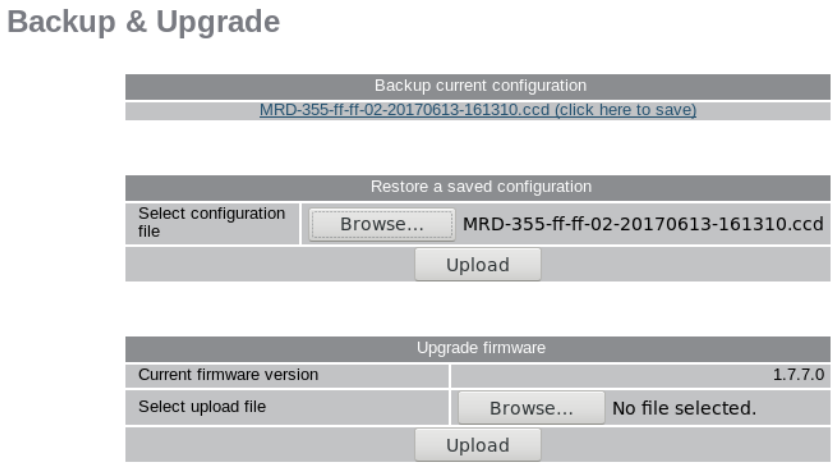


Figure 45: Restore configuration

5.3.3 Upgrading the modem firmware

The firmware can be upgraded via the web interface. To upgrade the firmware, click the Choose file button in the section titled **Upgrade firmware** then navigate to and select the upgrade file. Once selected, the file-name will display as shown highlighted in Figure 46.

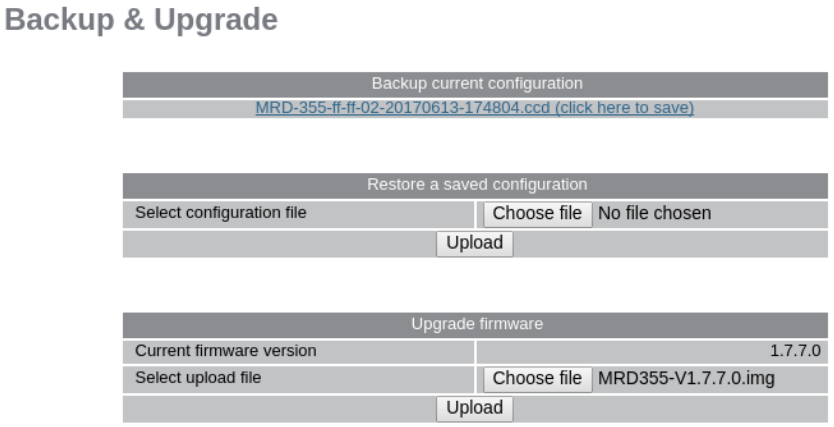


Figure 46: Select firmware upgrade file

To initiate the upload of the file click the Upload button, the file will now be uploaded. The upload may take from several seconds to several minutes depending on the speed of the link the upgrade file is transferred over. When the upload is complete, information on the upgrade file will be displayed, as shown in Figure 47. At this point the upgrade can be cancelled by clicking the Cancel Upgrade button.

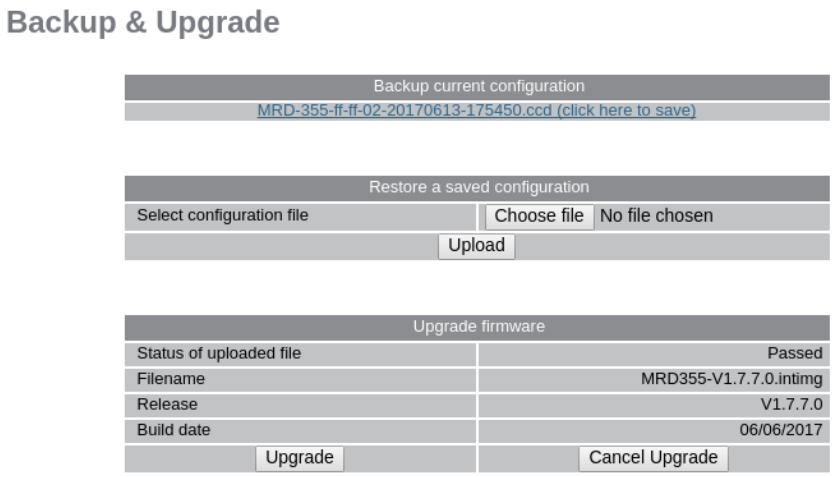


Figure 47: Upload the upgrade file

To proceed with the upgrade click the Upgrade button. The page will change to that shown in figure 48. The firmware upgrade will now proceed.

The upgrade will take several minutes to complete after which time the unit will reboot. During this time the power to the must not be removed.
If power is removed during this time the unit may not re-boot.

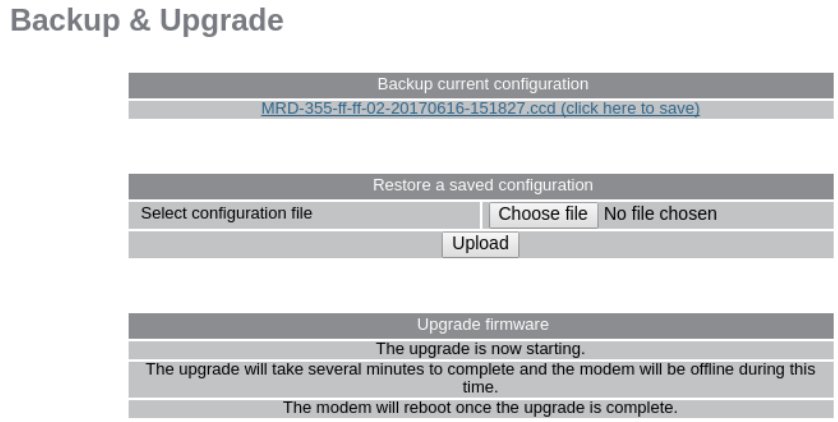


Figure 48: Upload the upgrade file

Once the firmware upgrade has completed the unit will re-boot and the web pages will again be accessible.

5.4 System Information

System Information is accessed by selecting System ▸ Information. An example of the System Information page is shown in figure 49. The first section of the page lists the model and serial number of the unit, plus the firmware and boot loader version. The second part of the page lists the LAN MAC address the IMEI of the wireless module and the wireless IMSI.

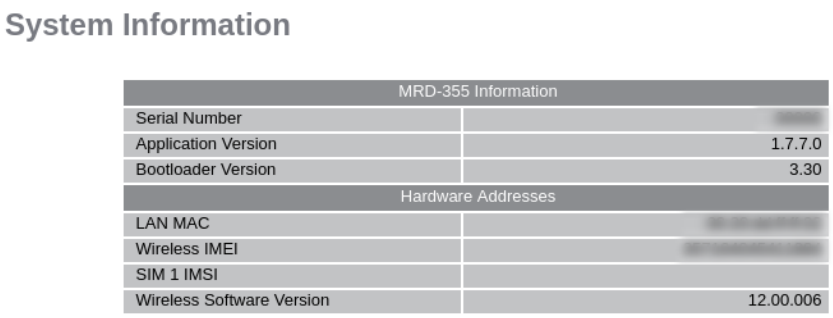


Figure 49: System Information page

5.4.1 Unit Information

The first section of the page lists the following information:

Model The model number of the unit.

Serial Number The serial number of the unit.

Application Version The application firmware version currently installed.

Bootloader Version The bootloader firmware version currently installed.

5.4.2 Hardware Addresses

The second part of the page lists the hardware address of the unit as follows:

LAN MAC The LAN Media Access Control (MAC) address assigned to the Ethernet port of the device.

Wireless IMEI The International Mobile Station Equipment Identity (IMEI) number of the wireless interface.

SIM n IMSI. The International mobile subscriber identity (IMSI) read from the SIM card.

Wireless Software Version The wireless (or RF) firmware version currently installed.

The SIM IMSI will only be listed if an SIM is inserted and can be accessed. If the unit supports more than one SIM then the IMSI for the active SIM will be reported.

5.5 Syslog

Syslog allows the logs to be sent to a remote system for storage an analysis. The Syslog page is accessed by selecting the menu System ▹ Syslog. A page similar to that shown in Figure 50 be shown.

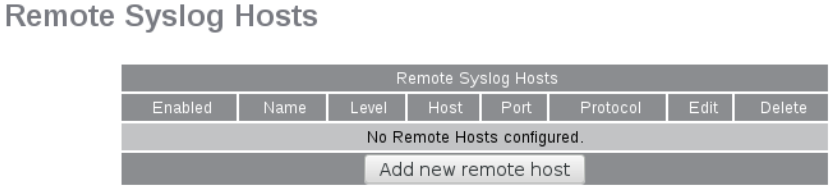


Figure 50: The default Syslog page

5.5.1 Adding a Remote Syslog Host

To add a remote Syslog host click the Add new remote host button, a page similar to that shown in figure 51 will be displayed.

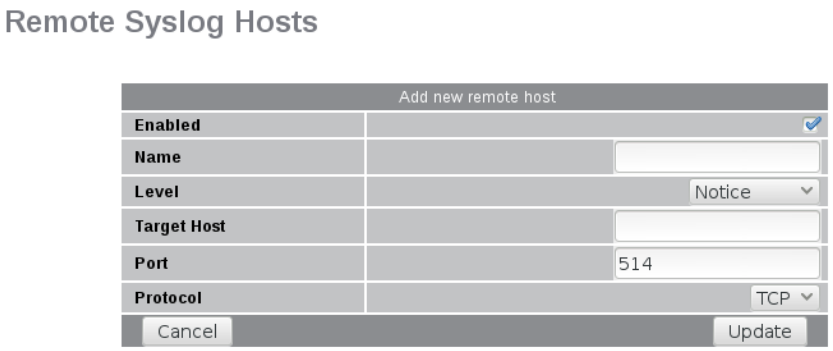


Figure 51: Add a remote Syslog host

To add a new host the following fields are required:

Enabled Check to enable Syslog to this remote host.

Name The name or label for this remote syslog.

Level The logging level. The logging levels are:

Info Lowest level, includes informational messages. This level may generate a large number of messages.

Notice (Default)

Warning

Error

Critical

Alert

Emergency The highest level, emergency messages only. Very few messages at this level.

Target Host The IP address or host-name of the remote Syslog server.

Port The TCP/IP port to use for the connection.

Protocol Select the protocol to use for the connection, either UDP or TCP (Default)

Once complete click 'Update' To save the changes.

The lower the logging level the higher the number of log messages.

5.5.2 Example of Adding a Remote Syslog Host

In this example a new remote host will be configured with the details shown in figure 52.

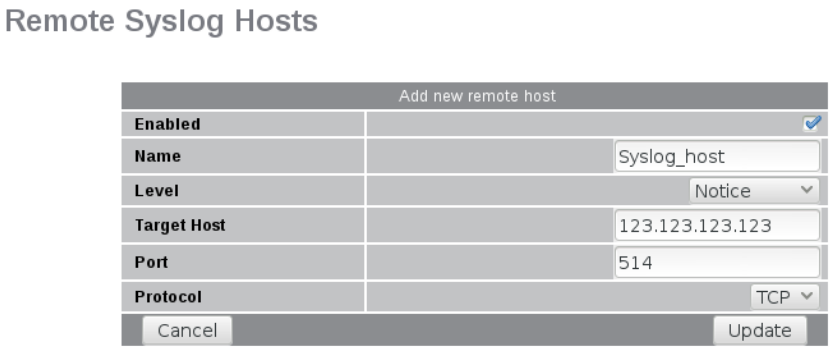


Figure 52: Add a remote Syslog host

After clicking the Update button, the main Syslog page is shown again with the new remote Syslog host listed, as shown in figure 53.

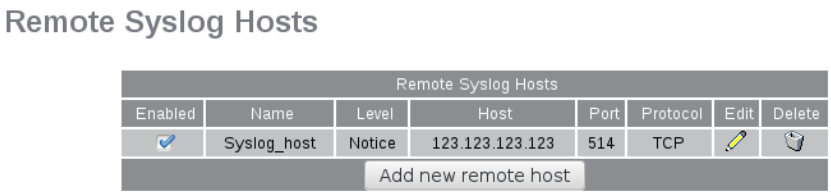


Figure 53: Main Syslog page showing new remote host.

Additional hosts may be added by following the same procedure.

5.5.3 Editing Remote Syslog Host

To edit a Remote Syslog host click the icon beside the entry in the table. The details for the entry will be displayed in a page the same as for the add remote Syslog host. The details can be modified and saved by clicking 'Update'

5.5.4 Deleting a Remote Syslog Host

To delete a Remote Syslog host click the icon beside the entry in the table. A confirmation dialogue will appear, click 'OK' to delete or 'Cancel' to cancel the deletion.

5.6 Power

The power controller may be used to power the unit on and off at specified times. By using the power controller the power consumption can be greatly reduced at times when a network connection is not required. The power controller options are on System ▹ Power page, which is shown in Figure 54.

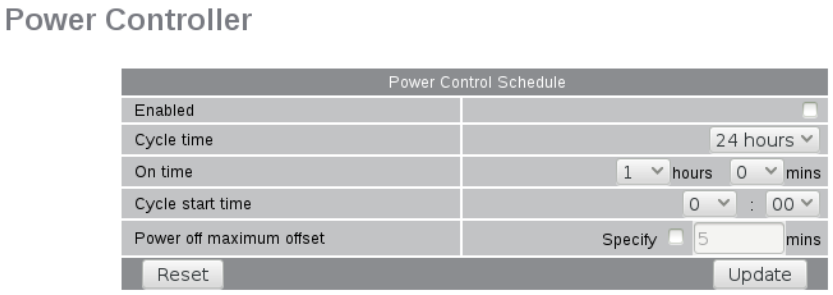


Figure 54: The Power Control Schedule configuration page.

For the power controller to work correctly power must be maintained to the unit at all times. During the *power off* times the power consumption will drop to approximately 10mA. This power is required to maintain the timer circuitry which determines when the unit should again be *powered on*. If during an *power off* time the power is removed from the unit the timer count is lost. When power is re-applied the unit will boot as normal, the timer will be re-initialised and determine if it should remain powered on or enter the *power off* state.

5.6.1 Configuring Power Control Schedule

The configuration options are:

Enabled Enable the power controller be checking the box.

Cycle time Selected the required cycle time from the drop-down list.

On time Select duration for which the power is on.

Cycle_start_time Select the time, offset from start of the cycle, at which the power is turn on.

Power off maximum offset If enable specifies an offset time which is applied if the unit re-powers prior to the scheduled power on time.

The controller works on the basis of a cycle, the duration of the cycle can be set for a maximum of 24 hours to a minimum of 30 minutes. Irrespective of the cycle duration the first cycle begins at midnight subsequent cycles begin straight after the previous cycle. For example if the cycle time is set to 6 hours, the first cycle starts at 12:00am, the second at 06:00am, the third at 12:00pm, the forth at 6pm and so on.

The period for which the unit is powered is set as the *on time* this time can be set to a maximum of 5 minutes less then the cycle time. If this value is set to 0 in will default to the maximum on time of 5 minutes less than the cycle time. The time at which the powered duration begins relative to the start of the cycle is specified as the *cycle start time*. For example if the *On time* is set to 30 minutes and the *Cycle start time* is set to 1 hour the unit will be off for the first hour of the cycle, it will then be powered on for 30 minutes and then remain off for the rest of the cycle.

Once the configuration has been completed click the Update button to save and commit the changes.

5.6.2 Power Control Schedule Example

Example 1

The unit is required to powered on at 2:00am and again at 2:00pm for a duration of one hour.

As there are two *power on* times per day the cycle time required is 12 hours. The *On time* is 1 hours and the *Cycle start time* is 2 hours. The required settings are shown in Figure 55.

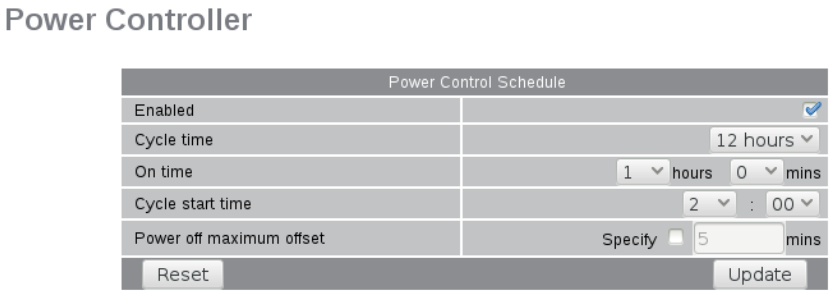


Figure 55: Power Control Schedule configuration example

Example 2

The unit is required to be power on from 5:45am to 6:15am each day. If the power to the unit fails and is return at 5:30am or later it is to remain on until normal power off time.

In this example as the unit is only powered once per day the *Cycle time* required is 24 hours. The *On time* is the duration from the *power on* time and the *power off* time which is 30 minutes. The *Cycle start time* is 5 hours and 45 minutes which is the time from midnight to the power on time. The *Power maximum offset* is enable and the time set to 15 minutes. The configuration is shown in Figure 56.

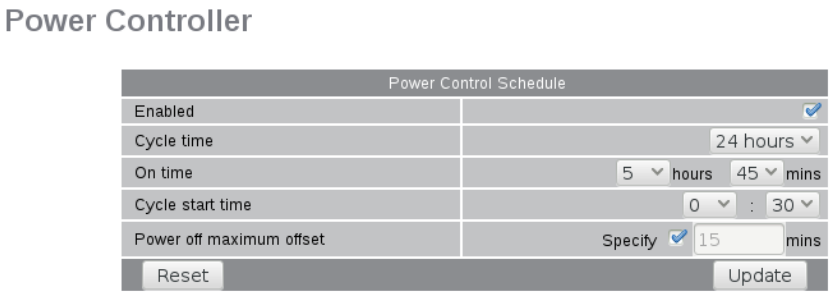


Figure 56: Power Control Schedule configuration example.

5.7 General Purpose Inputs and Outputs (GPIO)

The General Purpose Inputs and Outputs (GPIO) provide a way in which to monitor and control external devices. The inputs may be used to trigger events such as sending an SMS, email or SNMP trap. The outputs can be changed as a result of an event such as the receipt of an SMS. The GPIO options are on System ▹ GPIO page, which is shown in Figure 57.

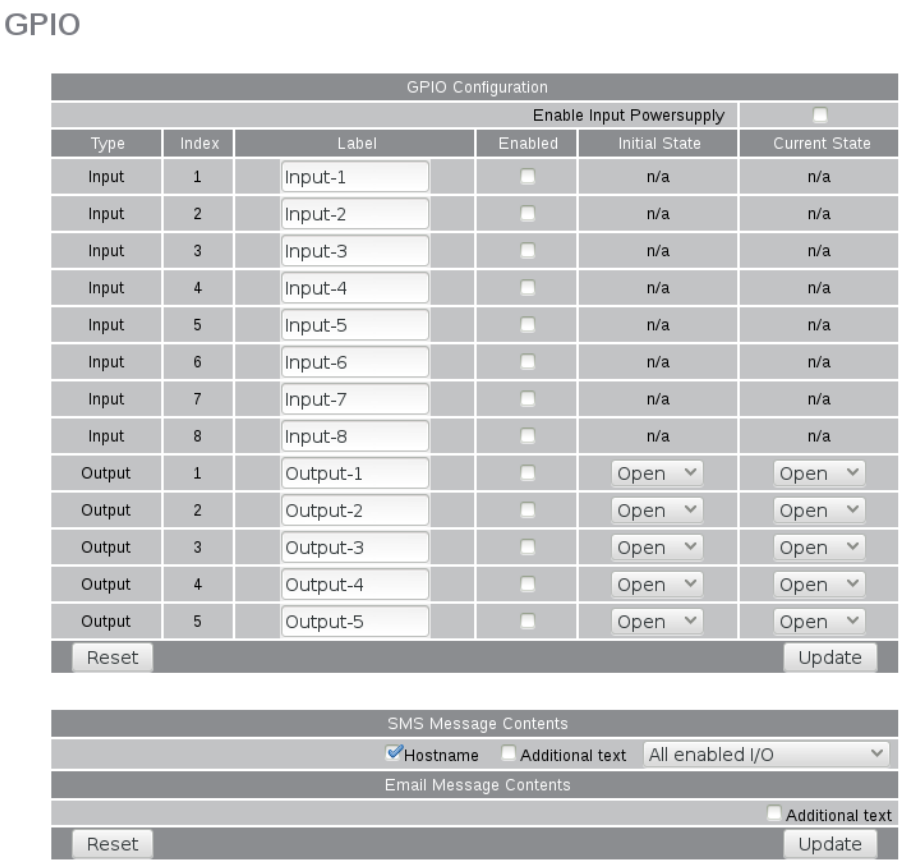


Figure 57: The GPIO configuration page.

5.7.1 GPIO Configuration

The GPIO Configuration of the page is used to configure the individual inputs and outputs.

Enable Input Power Supply Check this box to enable the power supply to power the input circuitry. This is required if the inputs are to work as closed contacts. If the inputs will be triggered with a voltage input this power supply can remain off.

The options within the table are:

Type This field describes the I/O type and is one of:

Input The I/O is an input.

Output The I/O is an output.

Index This is the index of the I/O and is referenced for each type. This index matches the hardware index for the I/O.

Label A text label for the I/O.

Enabled Check to enable reporting of the Input or Output.

Initial State This is the initial state the output will transition to when the unit powers up or re-boots. This field is not applicable for inputs. The state can either be:

Open The output is in the open or off state.

Closed The output is in the closed or on state.

Initial State This is the initial state the output will transition to when the unit powers up or re-boots. This field is not applicable for inputs. The state can either be:

Open The output is in the open or off state.

Closed The output is in the closed or on state.

Once the configuration has been completed click the Update button to save and commit the changes.

The state of the outputs when the unit is powered off and when it commences the boot process will be open. The default state will be applied during the boot sequence. This means that if an output is set to a default state of Closed then it will initially be Open then transition to Closed during power up.

When the unit is powered off or in low power mode, refer to Section 5.6 on page 40 the outputs will be in the Open state.

5.7.2 General Configuration

The general configuration is used to configure the way in which the unit will respond to an I/O event. The options are:

SMS Message Contents Should an input or output cause an SMS event to be generated, the values set in these fields determine the contents of the message. The values are:

Hostname Check to include the unit host-name in the message

Additional text Check to include additional text to be included in the message. When checked a text box will be appear containing the additional text to include in the message, as shown in figure 58. To add or edit text click the icon beside the text box, an example is shown in figure 59.

When to Send Drop-down box with options for when to send and what to include in message. Select from:

No I/O No I/O state included in the message

I/O that generated event Only the state of input or output which generated the event will be included in the message.

All enabled I/O The state of all enabled inputs and outputs will be included in the message.

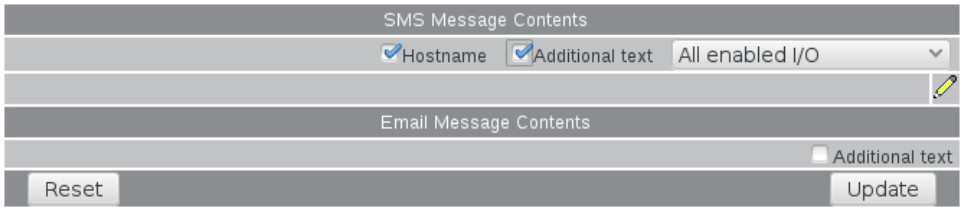


Figure 58: The add additional text to an GPIO message.

5.7.2.1 Example of Additional SMS Text

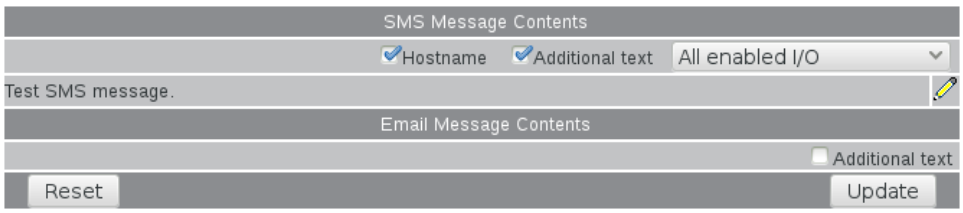


Figure 59: Text added to the add additional text for an GPIO message.

Email Message Contents Should an input or output cause an SMS event to be generated, the values set in these fields determine the contents of the message. The values are:

Additional text Check to include additional text to be included in the message. When checked a text box will be appear containing the additional text to include in the message, as shown in figure 60. To add or edit text click the icon beside the text box, an example is shown in figure 61.

Figure 60: The add additional text to an GPIO message.

5.7.2.2 Example of Additional Email Text

Figure 61: Text added to the add additional text for an GPIO message.

5.7.3 GPIO Example

In this example the two inputs will be enabled and labelled as *Door Alarm* and *Temp Alarm* to represent alarm inputs. The host name will be enabled and the Extra text field set to *Test site*. This configuration is shown in Figure 62 on the following page.

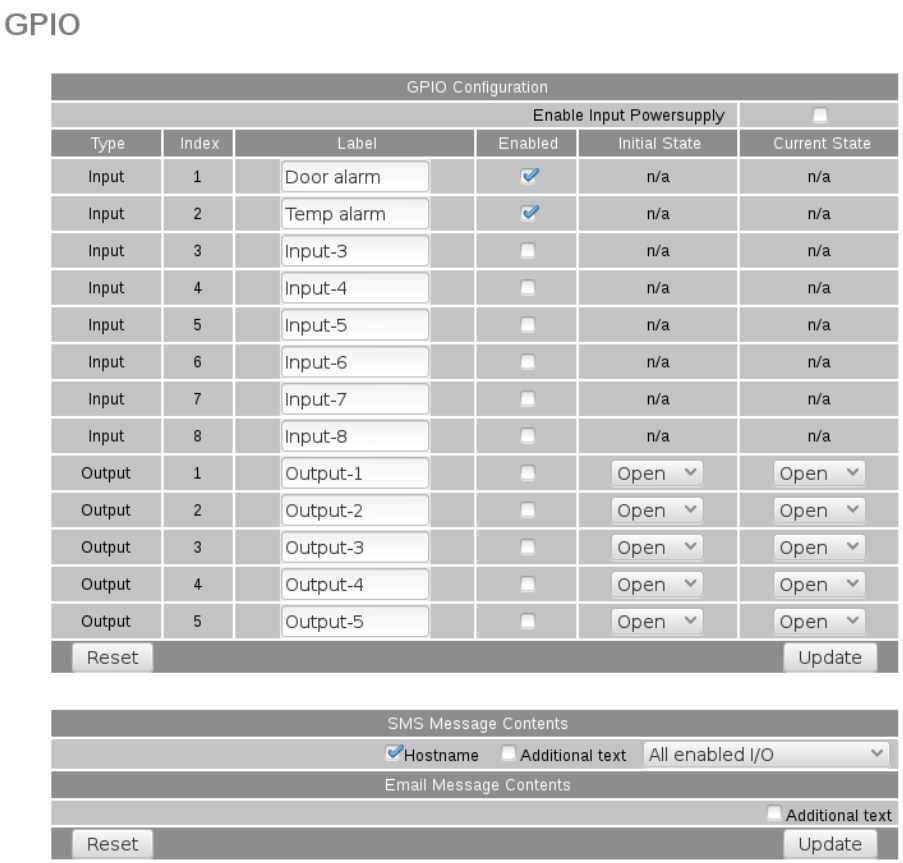


Figure 62: The GPIO configuration example.

To enable an SMS and email to be sent on this trigger SMS and email events need to be configured in the management configuration. For details on Management refer to 13 on page 244. Figure 63 shows both Input 1 and Input 2 have been enabled to send an SMS when the alarm contacts are closed.

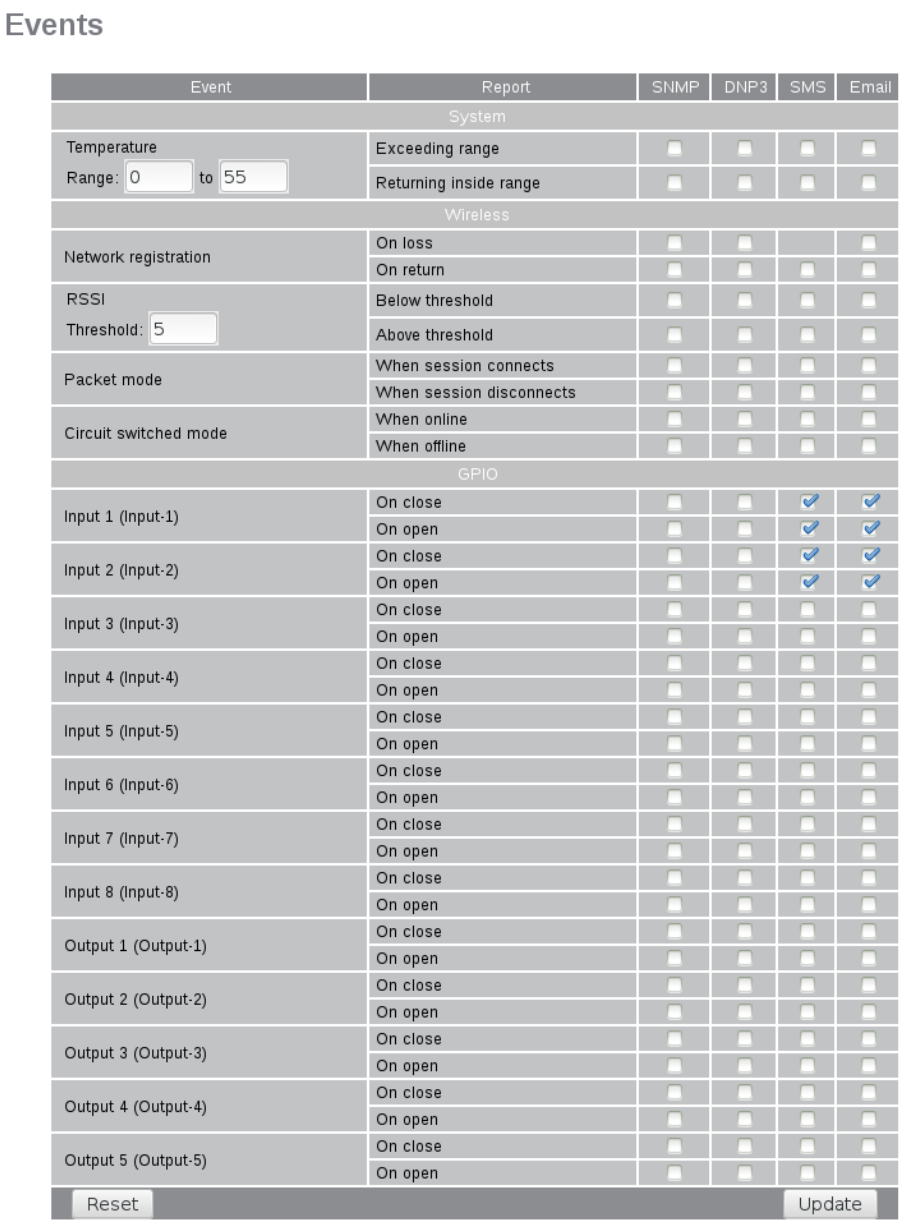


Figure 63: The GPIO SMS event configuration example.

If the alarms inputs are now closed the following SMSes end emails will be sent:

First the Input-1 the *Door alarm* is closed:

<host>: Test site: Door alarm=closed, Temp alarm=open

Hostname: <host>
Uptime: 00:21:44
System time: Sun Jun 25 17:21:17 2017
User message:
Test Email message.
Door alarm: Closed
Temp alarm: Open

And now the Input-1 the *Temp alarm* is closed:

<host>: Test site: Door alarm=open, Temp alarm=closed

Hostname: <host>
Uptime: 00:23:39
System time: Sun Jun 25 17:23:12 2017
User message:
Test Email message.
Door alarm: Open
Temp alarm: Closed

5.8 Location using GPS

The Location page provides access to the GPS configuration. The Location page is accessed by selecting the menu System ▷ Location. A page similar to that in Figure 64 will be shown.

GPS functionality requires a GPS antenna to be connected to the unit. Refer to the GPS section of the manual for the model being configured for details.

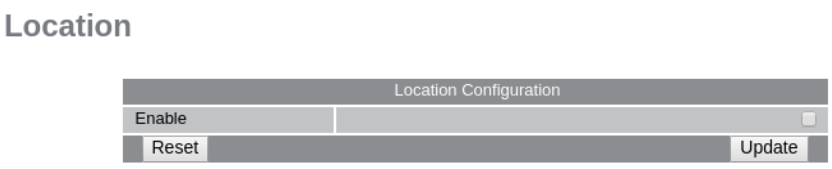


Figure 64: The default Location page.

To enabled GPS check the Enable check-box. The page will expand to show the configuration options as shown in Figure 65 on the next page.

Enabling GPS functionality will increase power consumption. To minimise the power consumption either configure for a manual poll and only update occasionally or set the Periodic fix interval to be a large value.

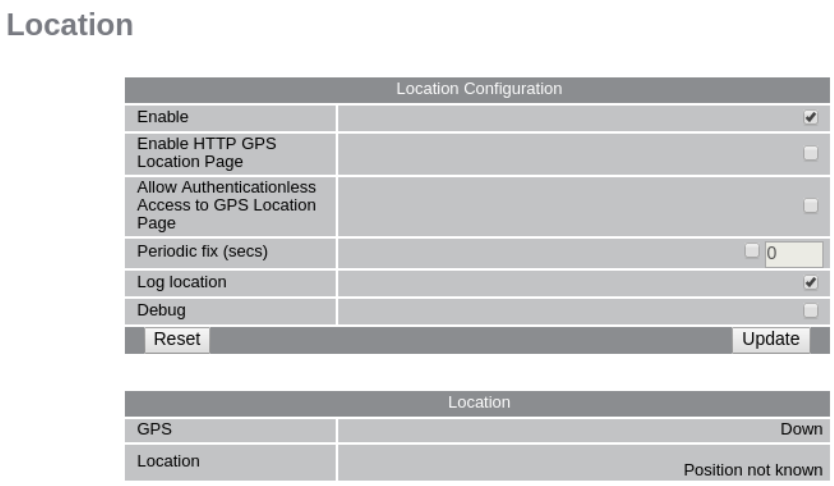


Figure 65: The Location page with GPS enabled.

5.8.1 Location Configuration

Enable Check to enable GPS functionality

Enable HTTP GPS Location Page Enable a web page containing the location data as text.

Allow Authenticationless Access to GPS Location Page Allow access to the location data without authentication.

Periodic fix (secs) Specify the time interval at which to obtain a GPS location fix. A value of 0 (default) means no poll.

Log location Log the location when a GPS fix is acquired.

Debug Enable debugging messages.

Once any changes have been made to the configuration click the Update button the save the changes, only then will GPS be enabled. A page similar to that shown in Figure 66 on the following page be shown.

5.8.2 Location

GPS Will report:

Down When GPS is not Enabled.

Locate (Button) When GPS is enabled.

Location Will report:

Position not known While attempting to acquire a GPS fix.

Co-ordinates and Time-stamp Once a fix has been obtained.

The Locate button will not be displayed until the GPS settings have been saved by clicking the Update button.

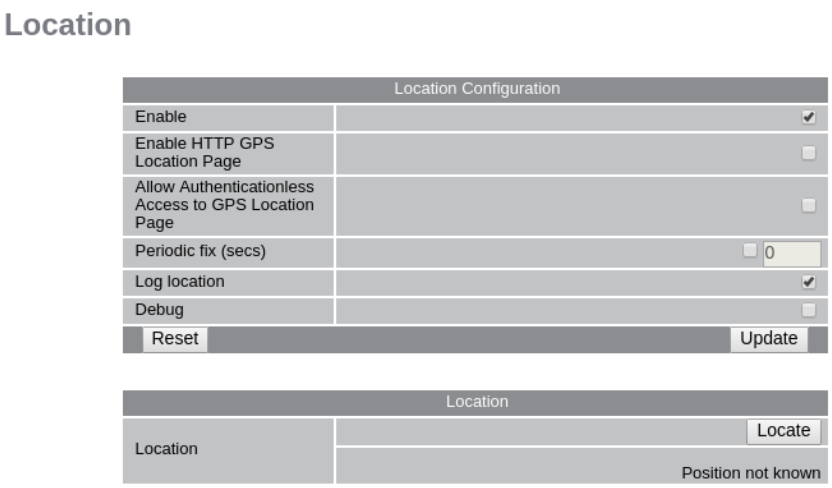


Figure 66: The Location page with GPS configured but no location yet determined.

To obtain a GPS fix click the Locate button. Once the location has been determined it will appear in the location table, as shown in figure 67.

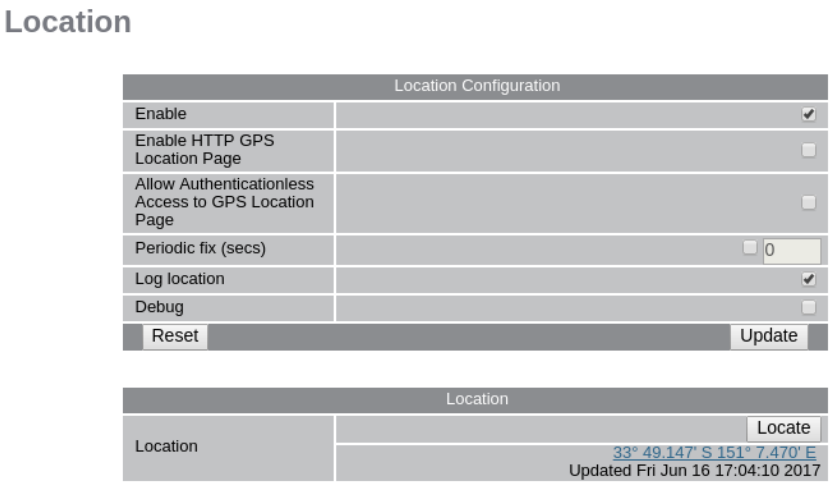


Figure 67: The Location page showing a location.

The location will be written to the log if this option has been enabled. It will appear similar to that shown:

Jun 16 17:04:10 msp: Location: 33 Degrees 49.147’ S 151 Degrees 7.470’ E
Jun 16 17:04:10 msp: Location: 33 Degrees 49.147’ S 151 Degrees 7.470’ E

6 Wireless

This section describes the GSM / 3G / 4G Wireless interface configuration options and settings. Two modes of operation are supported packet mode and Circuit Switched Data (CSD) mode, the configuration settings for each will be described.

The subsections of the configuration are:

- Network - Configure the mode of operation, selecting the frequency band of operation and setting the SIM PIN.
- Packet mode - Configuration of the packet mode settings.
- Circuit switched mode - Configuration of the circuit switched data mode settings.
- SMS - Configure the Short Message Service (SMS) options and settings.

The Wireless configuration page is accessed by selecting the **Wireless** tab from the main menu. When selected the page similar to that shown in Figure 68 will be displayed.

Figure 68: Main Wireless page.

6.1 Wireless Network

The Wireless Network options are used to set the operating mode, select the frequency band of operation and set the SIM PIN. To display the Wireless Network page select Wireless ▷ Network from the menu. The page shown will differ slightly between models, 69 is an example from an LTE unit and 70 is an example from a 3G unit.

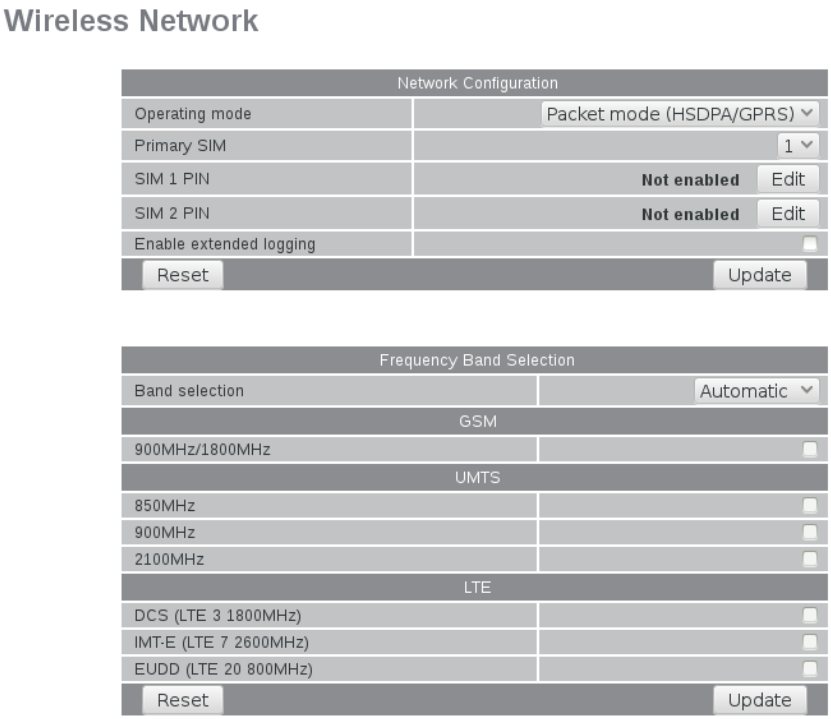


Figure 69: Wireless Network configuration, LTE models

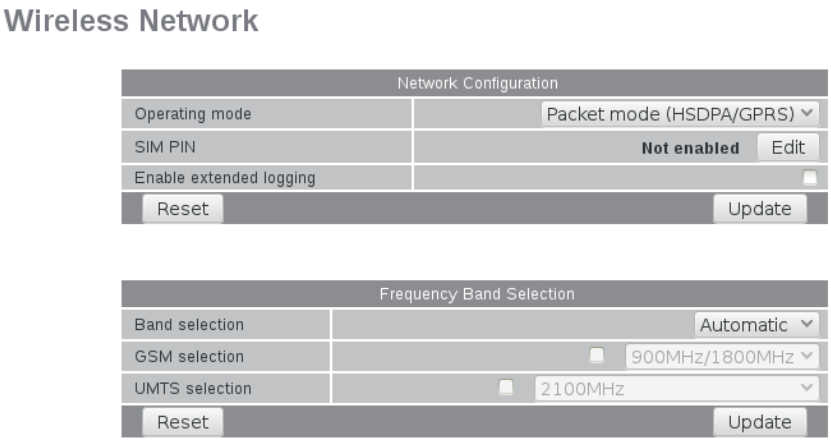


Figure 70: Wireless Network configuration, 3G models

6.1.1 Network Configuration

Operating mode Set the operating mode of the wireless interface. Three modes of operation are supported for the wireless interface, the options are:.

Packet mode In packet mode the unit acts as a TCP/IP modem and router, this is the standard and recommended mode of operation. The majority of the functions and services will only be available when operating in this mode. The modem connects to the provider's network and is allocated an IP address. Data can be routed between the LAN ports and the Wireless port. The Serial Server is used to transport serial data over the packet interface.

Circuit switched mode Circuit Switched Data mode is similar to a traditional dial-up modem. It is mainly intended for the transport of serial data. Connections are established by dialling into the modem using a PSTN modem or dialling out a call via AT commands on the serial port.

Disabled The wireless interface is shut-down. No data connections are possible over the wireless interface, this includes SMS.

Primary SIM Use to select the primary SIM on models which have the option of installing more than one SIM. The SIM selected will be the first used when attempting to establish a network connection.

SIM n PIN Indicates if a PIN has been set for the relevant SIM. Click Edit to set the pin, details are shown in the following section. On models with the option of installing more than one SIM a line for each SIM will be present, the PIN for each SIM will need to be set.

Enable extended logging Check to enable extended logging for the wireless interface. This option is useful if connection problems are encountered.

Click the Update button to save and commit changes.

6.1.2 Setting the SIM card PIN

The SIM card may have a PIN associated with it. If PIN checking is enabled on the SIM then in order to access the SIM, the PIN will need to be set. To set the SIM PIN click the Edit button in the **SIM PIN** row for the relevant SIM. A dialogue box as shown in Figure 71 will be displayed.

Figure 71: Add SIM PIN dialogue

By default the PIN is not enabled, to enable it check the check-box. The dialogue box change to include additional fields as shown in figure 72.

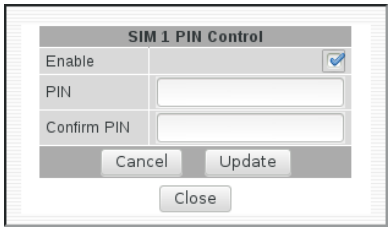


Figure 72: SIM PIN Enabled.

Enter the PIN into both the PIN and Confirm PIN text boxes as shown in Figure 73, the PIN digits will not be shown. The presence of a digit will be indicated by a '●'

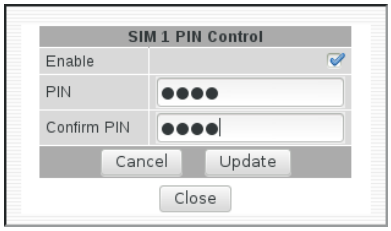


Figure 73: Entering the SIM PIN.

Click the Update button to save and commit changes.

The PIN will only be saved if the two PINs entered match. If the PINs entered do not match an error will be indicated.

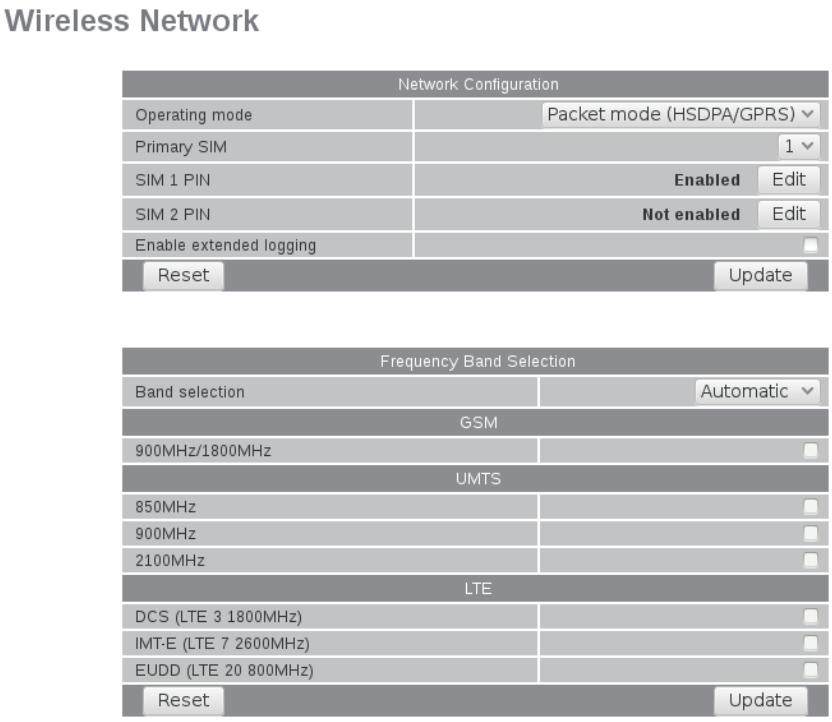


Figure 74: Wireless Network with SIM 1 PIN Enabled.

To change or delete a PIN click the Edit button, a dialogue box as shown in figure 75 will be shown. To disable the PIN un-check the Enable check-box, edit the PIN click the icon and to delete the PIN click the icon.

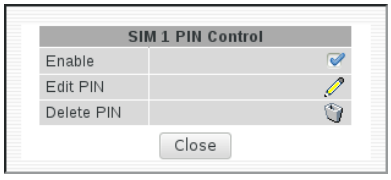


Figure 75: SIM PIN edit dialogue

Disabling the PIN will not delete it, it can be re-enabled at a later time without re-entering the PIN. To disable and remove the PIN click the icon.

6.1.3 Selecting the operating frequency bands

Depending on the model the unit is capable of operating on several frequency bands across LTE (4G), UMTS (3G) and GSM.

The band selection is slightly different for LTE (4G) and 3G models. Some models allow each individual band to be selected, other models only allow bands to be selected in groups. The settings for each type are provided.

The default setting is Automatic which means all supported frequency bands are enabled. When powered on the unit is power up it will start to search for available networks, LTE models will first try LTE (4G) then UMTS (3G) and finally GSM while 3G units will try 3G first then GSM. The process will continue until the unit is able to register with a network provider.

In some cases, it may be desirable to limit the frequency bands that are searched. For example, if the network provider only has an 850Mhz UMTS network then the time to register and connect will be reduced if this is the only band searched.

The default setting of Automatic is the best for most applications. It allows for fall-back options should the main network be unavailable.

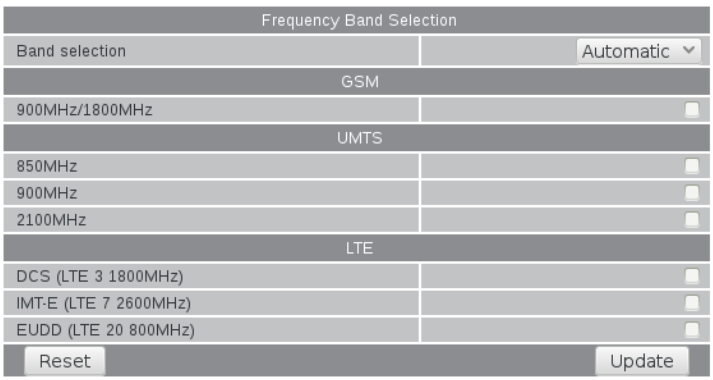


Figure 76: Frequency Band Selection - LTE models.

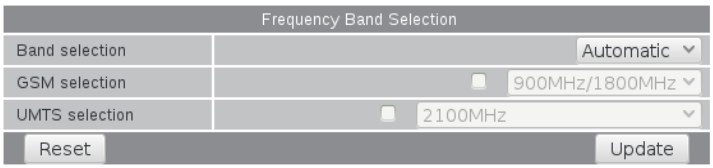


Figure 77: Frequency Band Selection - UMTS models.

The following band selection options are available:

Automatic Search all supported frequency bands. This is the default and recommended setting.

GSM Only Lock to GSM and search all supported GSM bands.

UMTS_Only Lock to UMTS (3G) and search all supported UMTS bands.

LTE Only Lock to LTE (4G) and searhc all supported LTE bands.

Specify Select specific supported frequencies across from LTE, UMTS and GSM.

LTE Models When specify is selected individual LTE, UMTS and GSM bands can be select by checking the check-box associated with the desired band. An example is shown in Figure 78.

UMTS Models When specify is selected bands can be selected in groups:

GSM Selection Check the check-box to enable and select the desired band group from the drop-down box.

UMTS Selection Check the check-box to enable and select the desired band from the drop-down box.

Once changes have been made to the frequency bands click the Update button to save and commit changes or click the Update button to cancel any changes and return to the previous settings.

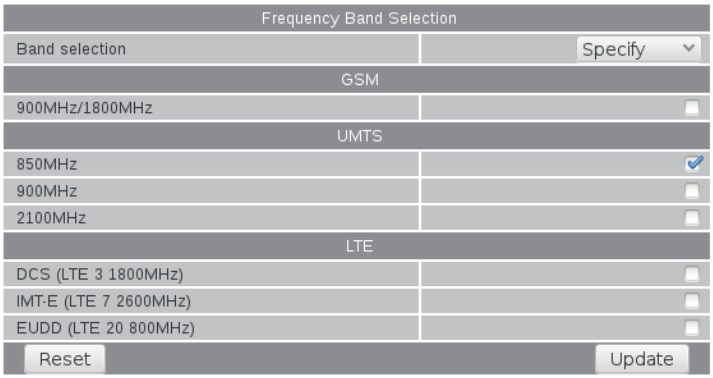


Figure 78: Specifying frequency bands.

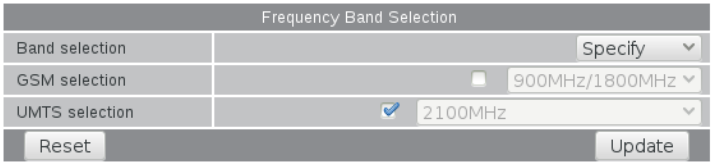


Figure 79: Specifying frequency bands

Care should be taken when changing the frequency bands as doing so will initiate a re-start of the wireless interface. This means that any current wireless connection will be disconnected and then the wireless connection will be re-established. This could result in interruption of data flow.
In particular care should be taken when changing the band selection over the wireless interface as this will result in a disconnection from the device.

6.2 Packet Mode Configuration

Before the modem can establish a packet connection, the details of the connection must be set up in a connection profile. This section details the process of adding, editing and deleting a connection profile. While most configurations will only need one configuration profile, multiple profiles are supported.

To access the packet mode configuration, select Wireless ▷ Packet Mode from the menu. The screen shown in Figure 80will be displayed.

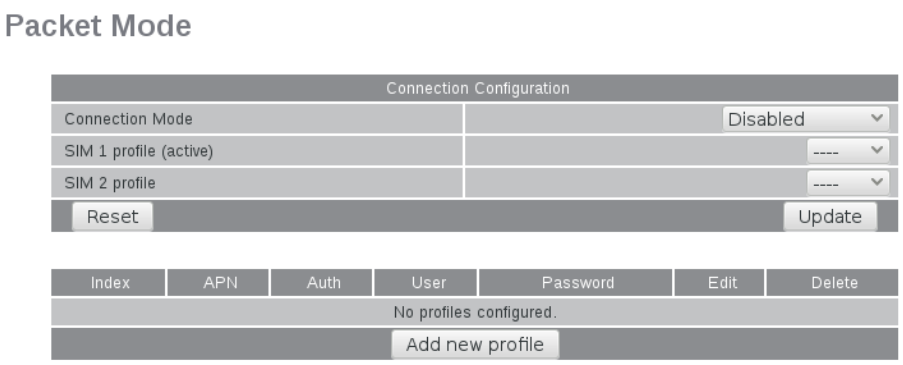


Figure 80: Wireless Interface Packet mode settings

6.2.1 Connection Configuration

By default packet mode is disabled and no profiles are configured.

Connection Mode **Disabled** Packet connections are disabled.

Always Connect Establish and maintain a packet connection.

Automatic Establish a connection only when VRRP master. In order for this to function VRRP must also be configured, for details refer to section 9.3 on page 125

SIM n profile Select the profile for the corresponding SIM. The options are:

Index Select the index of a defined profile. Refer to next section on how to add connection profiles.

Via AT The unit is configured to operate in modem emulation mode and the profile details will be provide via an AT command. Refer to the Serial Server section for details on configuring Modem Emulation.

Click the Update button to save and commit changes.

6.2.2 Adding Connection Profiles

To add a new profile, click the Add new profile button, the add entry page will display as shown in Figure 81.

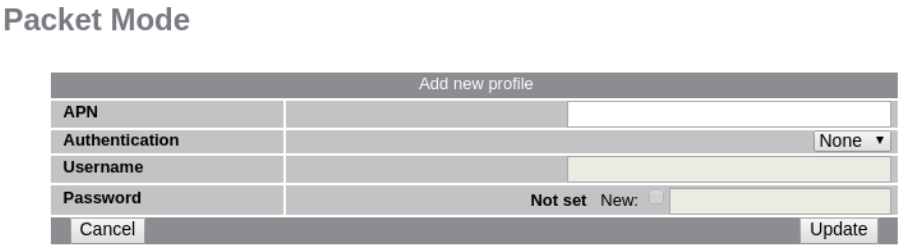


Figure 81: Adding a new profile

The settings required are listed below:

APN This is the name of the network provider's Access Point Name (APN).

Authentication For connections requiring a user-name and password to connect, this field sets the authentication protocol used:

None No authentication is performed.

PAP The Password Authentication Protocol is used.

CHAP The Challenge-Handshake Authentication Protocol is used.

Username For connections with **PAP** or **CHAP** selected for authentication, this is the user-name the modem will use to authenticate.

Password For connections with **PAP** or **CHAP** selected for authentication, this is the password the modem will use to authenticate. In order to set a password click the check box marked **New** then enter the password in the adjacent text field. The password is visible as it is being typed so that it can be checked for errors prior to being set. Once set the password will no longer be visible.

The network provider will specify the required settings for completing a connection profile. The provider may not supply a user-name and password if network authentication is not required. In this case set the **Authentication** to **None**. The only required field is the APN.

Once the profile has been entered click the Update button to save and commit changes.

6.2.3 Example of Adding a Connection Profile

In this example a profile will be added with the following details:

APN apn_string

Authentication CHAP

Username username

Password password

To add a new profile, click the Add new profile button, the add entry page will displayed, add the details as shown in Figure 82

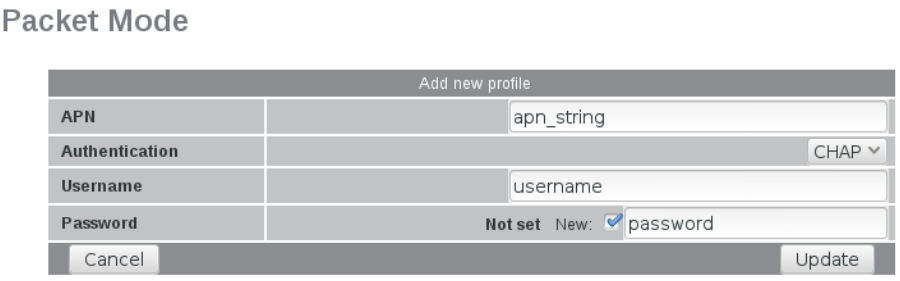


Figure 82: Profile added and selected

Click the Update button to save and commit changes.

The page will revert to the standard packet mode page and the profile will be listed in the profiles table as shown in Figure 83.

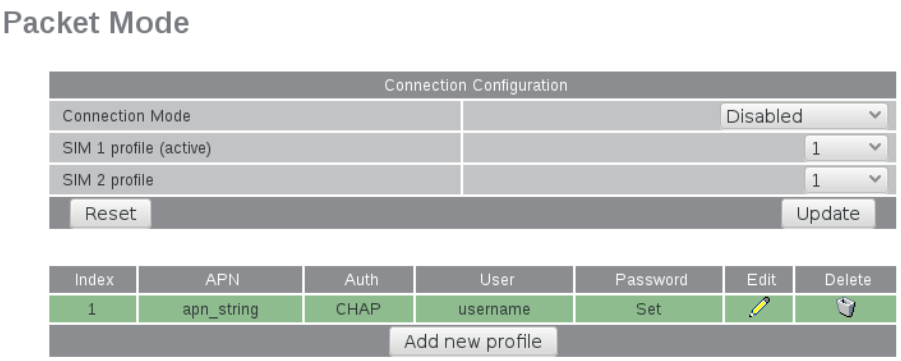


Figure 83: Profile added and selected

As no profiles were previous selected the new profile will automatically be associated with all available SIMs. If more profiles are added the SIM index can be changed.

6.2.4 Enabling a wireless connection

To complete the configuration of the wireless connection, the connection needs to be enabled. This is done by setting the **Connection Mode**. The connection options available are:

Connection Mode Disabled Packet connections are disabled.

Always Connect Establish and maintain a packet connection.

Automatic Establish a connection as required.

Always Connect is generally the best option.

Once the setting has been selected click the Update button to save the change to the connection state. Once the state has been set, the modem will attempt to establish a connection.

Figure 84 shows an example of a completed packet mode configuration.

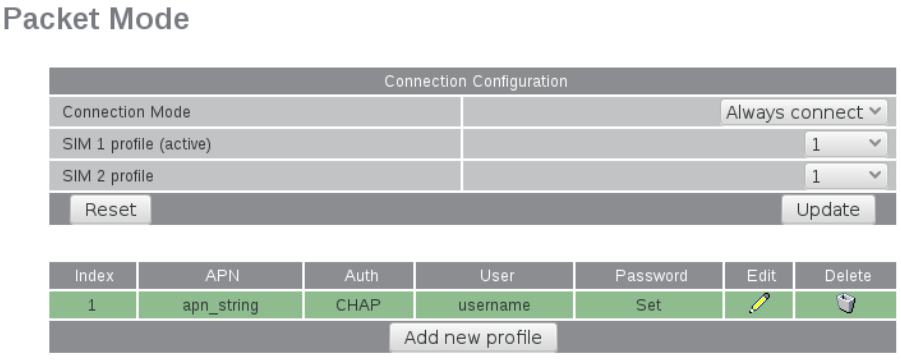


Figure 84: Completed wireless configuration

6.2.5 Adding Further Profiles

Additional profiles may be added by following the same process as above. Figures 85 and 86 show the result of adding a second profile. Notice that the profile with Index 1 is highlighted green as it is the currently selected profile.

Figure 85: Adding a second profile.

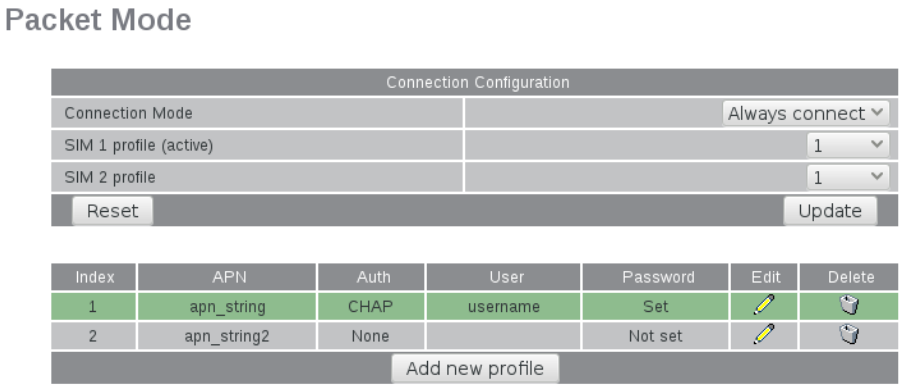


Figure 86: List of profiles now listing 2 profiles.

To change the selected profile select the required index number from the Current profile drop down box in the Connection Configuration section and click Update. The page will update and the selected index will now be highlighted. Figure 87 is an example with the second profile added above selected.

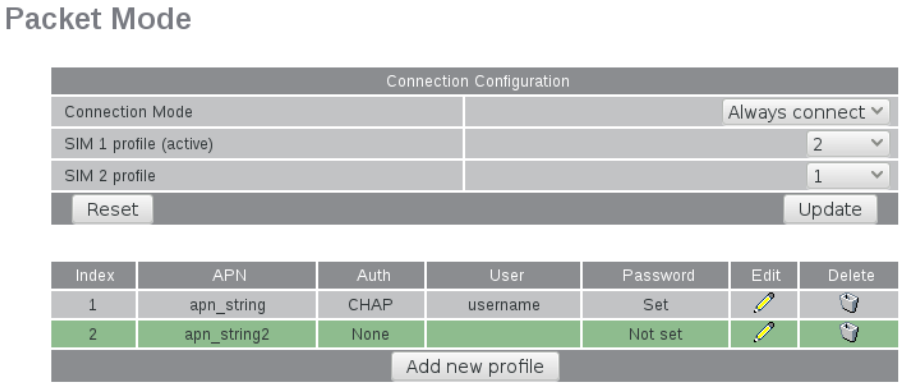


Figure 87: Second profile selected.

For models with more than one SIM the highlighted profile will be for the Active SIM. In the example shown in Figure 87 the Active SIM is SIM 1 and the selected profile for SIM 1 is Index 2 so the profile with Index 2 is highlighted.

6.2.6 Editing a profile

To edit an existing profile click on the icon located in the **Edit** column for the profile to be edited. Complete the changes to the profile then click **Update** to commit the changes. Figure 88illustrates editing of the second profile, in this example the authentication is changed from None to PAP and a Username and Password are added. The updated profile list is shown in Figure 89.

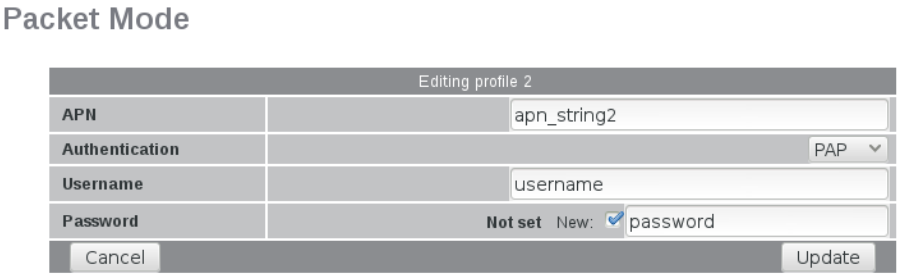


Figure 88: Editing the second profile.

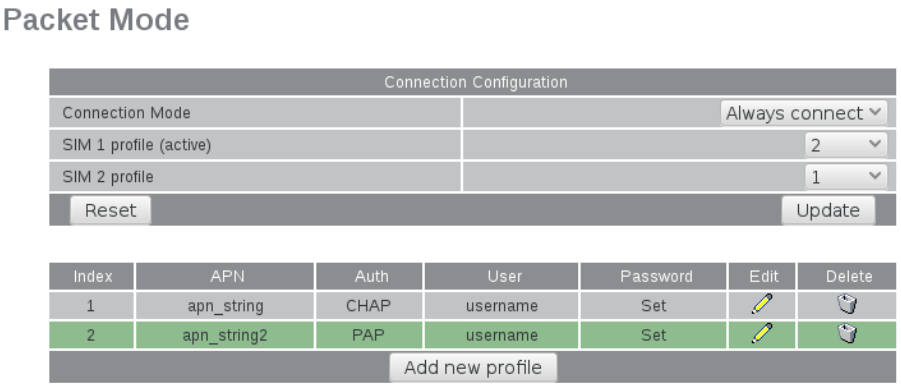


Figure 89: Profile list after editing the second profile.

6.2.7 Deleting a profile

A profile can be deleted by clicking the icon located in the **Delete** column for the profile to be deleted. Click **OK** to confirm the deletion. Figure 90 the process of deleting a profile. In this example the second profile has been deleted. After click OK the updated profile list appears as shown in Figure 91

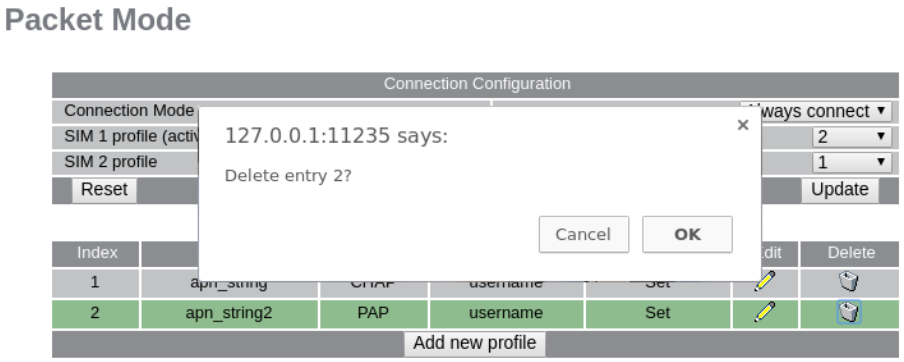


Figure 90: Deleting the second profile.

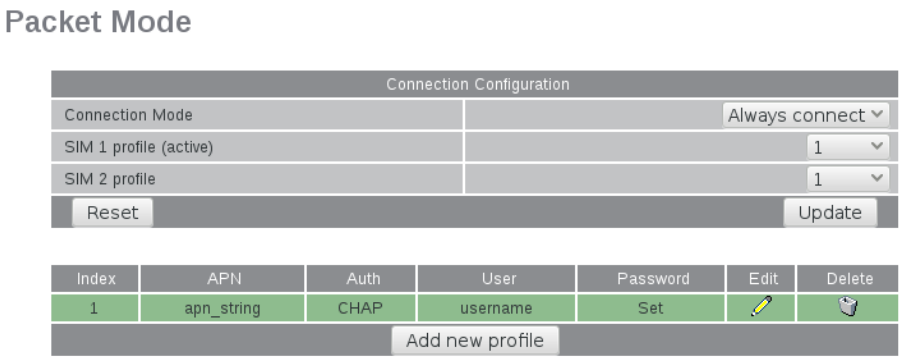


Figure 91: Profile list after deleting the second profile.

As the selected profile for SIM 1 was deleted, the index was automatically set to index 1. This is because an valid profile will always be associated with a SIM where possible.

6.2.8 Checking the status of the connection

To check the status of the connection select **Status** from the main menu and **Wireless** from the sub-menu. The wireless status page will be displayed which will look similar to that shown in Figure 92. The status of the connection will change as the modem connects to the network. The status will change through *Checking, Connecting* and finally *Connected* as a connection is established. To see the value changing the page will need to be refreshed.

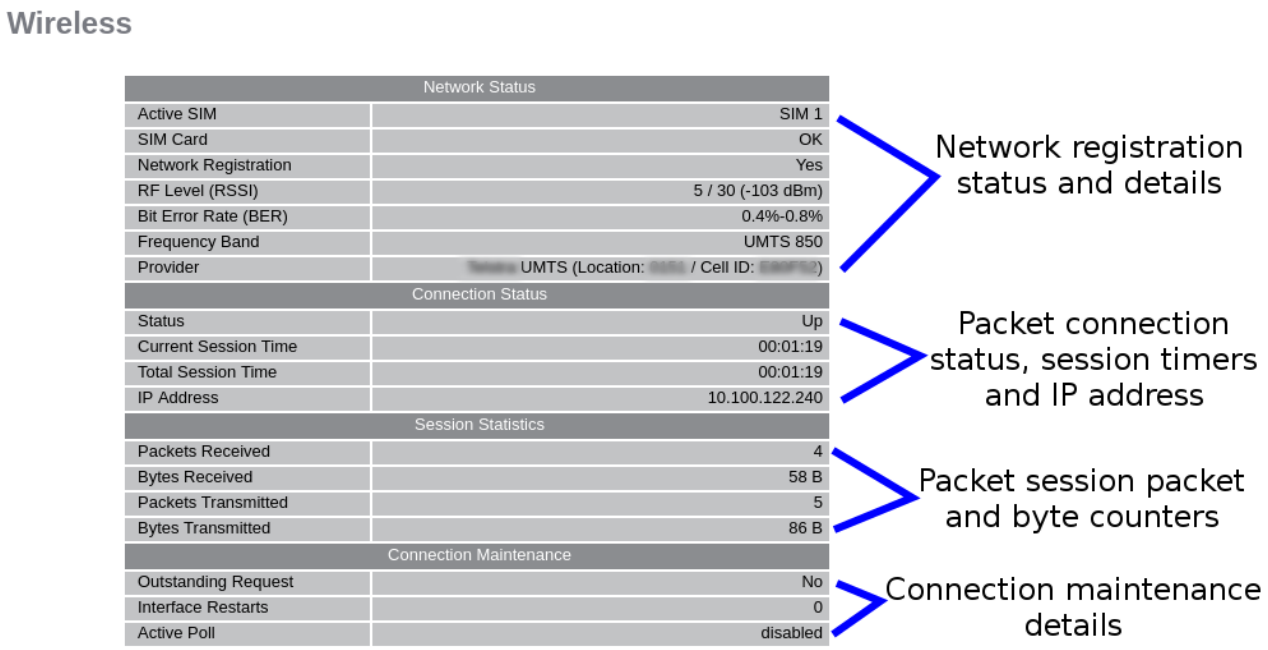
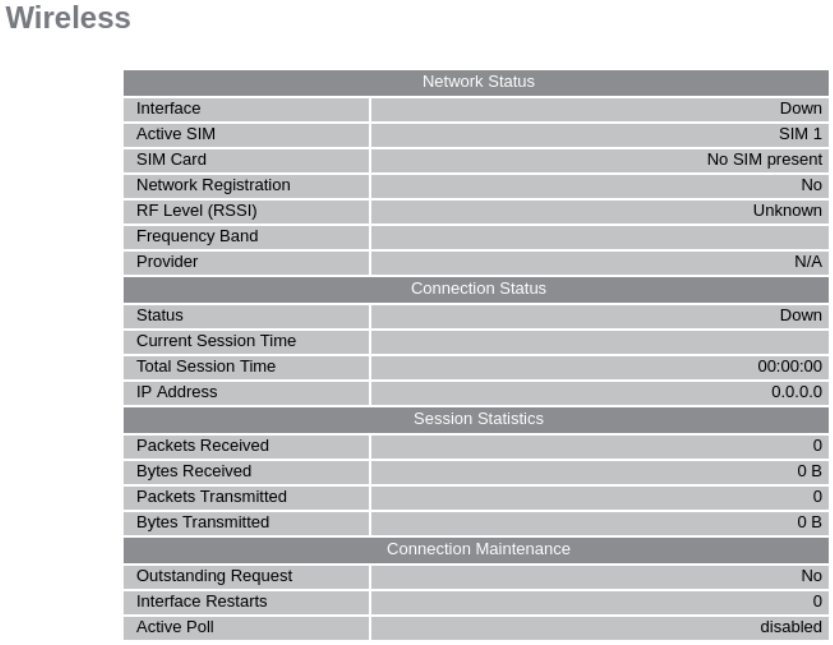


Figure 92: Wireless Status page

The section tiled **Network Status** details the quality of the service available from the wireless network.

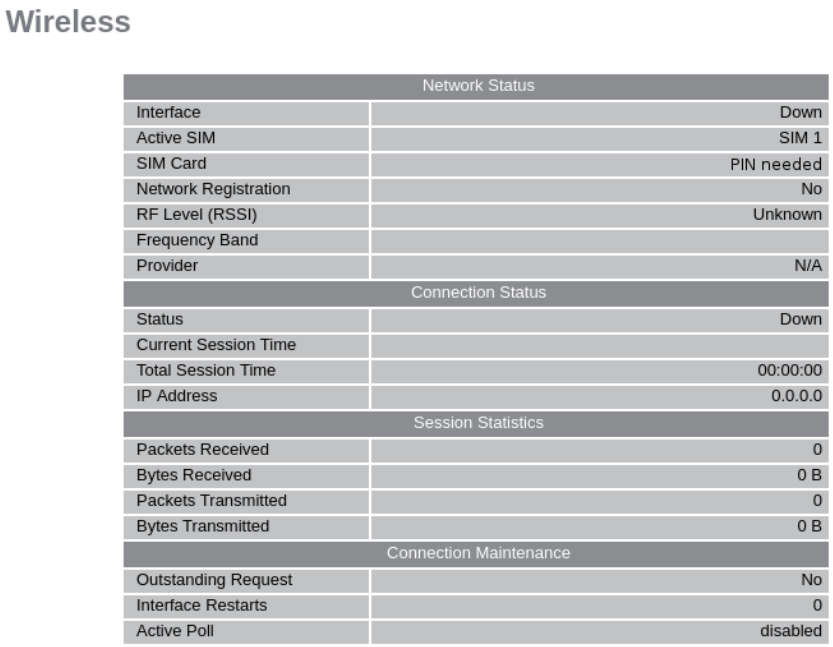
- The **SIM Card** field will only be shown if an error with the SIM card has been detected, and will be reported as **Absent or faulty** or **PIN needed** as shown highlighted in Figures 93 and 94.
    - If the SIM card fault is reported, possible causes include:
        - The SIM card has not be inserted correctly. Refer to the manual for the model being configured, for details on how to insert the SIM card.
        - The SIM card pin number has not been entered or is incorrect. Refer to section 6.1.2 on page 53, for details on entering the SIM card PIN.



Wireless

Network Status	
Interface	Down
Active SIM	SIM 1
SIM Card	No SIM present
Network Registration	No
RF Level (RSSI)	Unknown
Frequency Band	
Provider	N/A
Connection Status	
Status	Down
Current Session Time	
Total Session Time	00:00:00
IP Address	0.0.0.0
Session Statistics	
Packets Received	0
Bytes Received	0 B
Packets Transmitted	0
Bytes Transmitted	0 B
Connection Maintenance	
Outstanding Request	No
Interface Restarts	0
Active Poll	disabled

Figure 93: Wireless Status page showing a SIM Absent fault.



Wireless

Network Status	
Interface	Down
Active SIM	SIM 1
SIM Card	PIN needed
Network Registration	No
RF Level (RSSI)	Unknown
Frequency Band	
Provider	N/A
Connection Status	
Status	Down
Current Session Time	
Total Session Time	00:00:00
IP Address	0.0.0.0
Session Statistics	
Packets Received	0
Bytes Received	0 B
Packets Transmitted	0
Bytes Transmitted	0 B
Connection Maintenance	
Outstanding Request	No
Interface Restarts	0
Active Poll	disabled

Figure 94: Wireless Status page showing a SIM PIN required fault.

- The **Network Registration** field indicates if actively registered to the wireless network. No connection is possible without registration.
  - If the network registration field is **No**, possible causes include:
    - Poor signal strength. Check the antenna is properly connected and experiment with different locations to achieve a higher RF Level.

  - Problem with the SIM card. Ensure the SIM card fitted correctly and is currently enabled with the network provider.
  - The SIM card is not correctly enabled with the network provider. Verify with the provider that the SIM is currently active.

- The **RF Level** indicates the current strength of received signal from the network, with a maximum of 30. Any level over 10 should provide acceptable connection speeds.

The section titled **Connection Status** shows the statistics for the current connection.

- If the **Status** item doesn't show **Connected**, verify the following:
  - **Connection state** is **Always connect** in the packet mode configuration.
  - If the **Status** field always shows **Connecting...**, a problem with the APN, user-name or password is likely. Check that the values these settings with the network provider. Refer to Section 6.2.2 for details on how to enter these values and create a profile.
- The remaining fields list the length of time connected, IP address allocated by the network and data counters. All of this information will reset if a connection is restarted, except the *Total Session Time* field, which will accumulate across all sessions.

6.3 Connection Management

The purpose of connection management is to create and maintain reliable connections that can detect errors and recover as quickly as possible. The connection management is divided in two areas:

Connection establishment Determines how the modem manages the establishment of a connection to the network.

Connection_management Determines how the modem manages the connection to the network once established.

To access the connection management options, select Wireless ▷ Connection Management fom the menu. The connection management page as shown in figure 95 will be displayed.

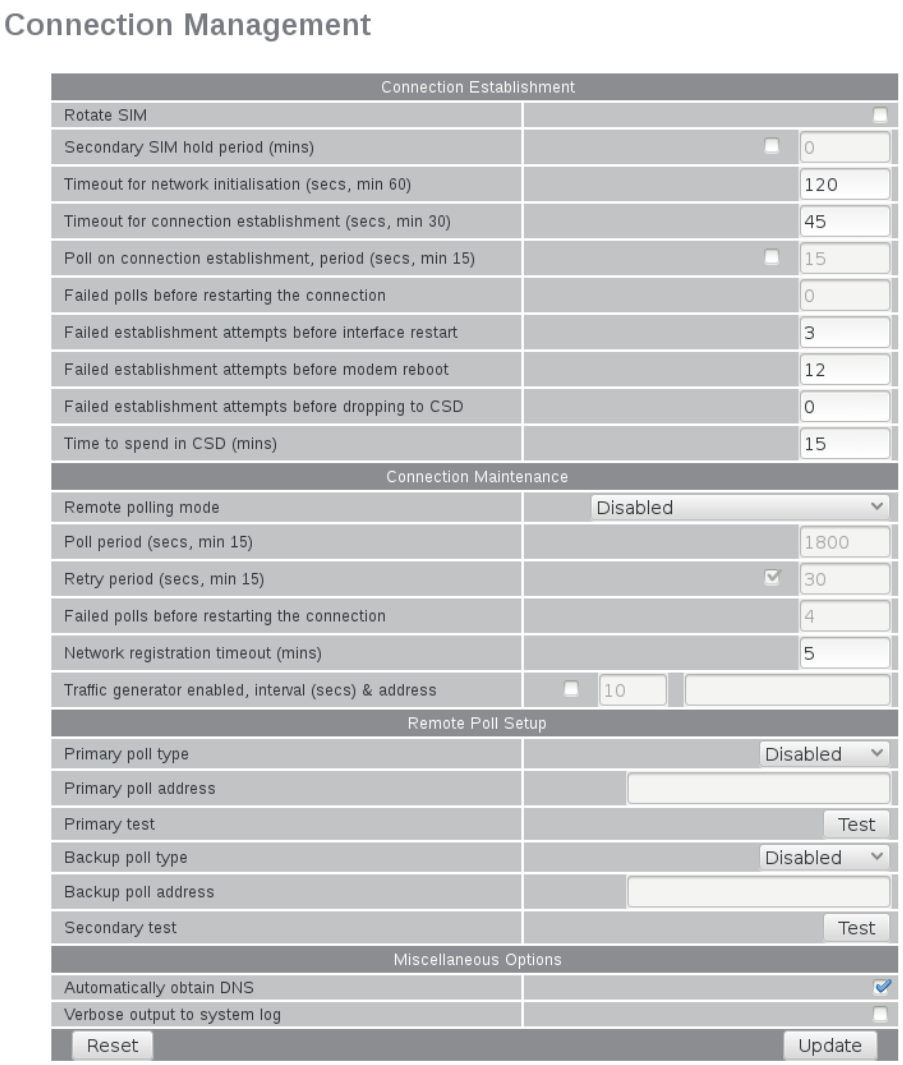


Figure 95: Wireless connection management

6.3.1 Connection Establishment

The connection establishment options are used to set the parameters for initial connection to a provider's wireless network. The options are:

Rotate SIM Check to cycling through to the next available SIM should the connection fail to be established. Option only present on models with more than one SIM.

Secondary SIM hold period (mins) Check to enable a hold time for the secondary SIM and then specify the number of minutes to hold. If the enabled when the secondary SIM is selected it will stay connected using that SIM for the hold time and then try to establish a connection using the primary SIM. Option only present on models with more than one SIM.

Timeout for network initialisation Specify the maximum time in seconds to allow for a network initialisation. The minimum value accepted is 60 Seconds, the default value is 120 seconds.

Timeout for connection establishment Specify the maximum time in seconds to allow for a connection to be established. The minimum value accepted is 30 Seconds, the default value is 45 seconds.

Poll on connection establishment Check to enable and specify the poll re-try period, the minimum value is 15 seconds. If enabled a remote poll will be completed before the connection is considered successful. The purpose of this option is to ensure that not only has a network connection been established but also that end-to-end connectivity exists. The modem does this by polling a remote server using IMP (Ping) or a TCP socket connection. Should the poll fail, the modem retries at the specified interval for the number of polls specified in **Failed polls before restarting the connection**. If this option is enabled then the **Remote Poll Setup** must be enabled and configured correctly.

Failed polls before restarting the connection Set the number of failed polls before the connection is considered to have failed to establish. A value of 0 disables poll on connection establishment. This option is only available when **Poll on connection establishment** enabled.

Failed establishment attempts before interface restart Specify the number of failed connection attempts before restarting the wireless interface. Set this value to *0* to disable.

Failed establishment attempts before modem reboot Specify the number of failed connection attempts before re-booting. Set this value to *0* to disable.

Failed establishment attempts before dropping to CSD Specify the number of failed connection attempts before switching to Circuit Switched Data (CSD) mode. Set this value to *0* to disable the fail-over to CSD feature.

Time to spend in CSD Specify a time in minutes to remain in CSD mode before reverting to packet mode and attempting to establish a connection. This value value is only used if the **Failed establishment attempts before dropping to CSD** option is set to a value greater than *0*.

6.3.2 Connection Maintenance

The connection maintenance refers to the tests employed to determine if a valid network connection is available. Should the connection maintenance test fail then attempts will be made to re-establish the connection.

The following options control connection maintenance:

Remote polling mode Specify the connection maintenance operating mode. Four modes are supported:

- **Disabled** Connection maintenance is disabled. (Default)
- **Poll at fixed interval** Poll the servers specified in the **Remote Poll Setup** at the interval specified.
- **Poll if Rx idle for interval** Only poll the servers specified in the **Remote Poll Setup** when no data has been received from the wireless interface for the specified interval.
- **Reconnect if Rx idle for interval** Monitor the receive data and reconnect if no data has not been received by the wireless interface for the specified interval. This mode is a good choice for configurations that already employ polling traffic, such as when using the SSL VPN or IPsec VPN with dead peer detection.

Poll period Specify the time interval in seconds between polls. Minimum value of 15 seconds.

Retry period Specify the time in seconds to retry the poll after a failed poll. Minimum value of 15 seconds.

Failed polls before restarting connection Specify the number of failed polls to declare the link failed and to re-start the establishment process.

Network registration timeout Specify the time in minutes the time-out for network registration attempt after a polling failure.

Taffic generator enabled, interval & address Check to enable the traffic generator, and specify the time interval between data packets and the address to which to send the packets. The traffic generator is used to generate transmit data, it sends a data packet at the specified interval without expecting a response.

6.3.3 Remote Poll Setup

The remote poll set-up is used to specify the poll type to use and the address of the server to poll. A primary and backup server may be specified. The backup server will be used if the primary server cannot be contacted. The options for each poll are:

Primary Poll type Specify the poll type. The options are:

Disabled The poll is disabled.

Ping (ICMP) Ping the specified address.

TCP Socket Establish a TCP socket to the specified address and port number. The connection will be terminated as soon as successfully opened.

Primary Poll address Specify the address of the primary server to poll. The format used depends on the poll type:

Ping (ICMP) Enter an IP address or host-name, eg 192.168.1.1 or www.exampledomain.com

TCP Socket Enter an IP address or host-name followed by a colon and the TCP port number, for example 192.168.1.1:80

Primary test Click the test button to test the poll.

Backup Poll type Specify the poll type. The options are:

Disabled The poll is disabled.

Ping (ICMP) Ping the specified address.

TCP Socket Establish a TCP socket to the specified address and port number. The connection will be terminated as soon as successfully opened.

Backup Poll address Specify the address of the primary server to poll. The format used depends on the poll type:

Ping (ICMP) Enter an IP address or host-name, eg 192.168.1.1 or www.exampledomain.com

TCP Socket Enter an IP address or host-name followed by a colon and the TCP port number, for example 192.168.1.1:80

Backup test Click the test button to test the poll.

6.3.4 Miscellaneous Options

Automatically obtain DNS Check to enable the use of the received DNS server addresses when a connection is established as the DNS server for all look-up requests. If disabled (un-checked) a DNS server should be entered manually, refer to the Domain Name System (DNS) Section 8.4 for details.

Verbose output to system log Check to enable sending of verbose connection information to the system log. As the size of the system log is limited, this option should only be enabled if connection problems are experienced.

Click the Update button to save and commit changes.

6.4 Circuit Switched Data (CSD) Mode

Circuit Switched Data (CSD) mode works in similar manner to a traditional dial-up modem. Connections are established by dialling into the modem or by dialling out to another modem (PSTN or 4G/3G/GSM). Unlike packet mode, where data is carried over in packets over IP networks, circuit switched mode transports serial data through the telephone network. Typically CSD offers much lower data rates than packet mode (CSD rates are around 9600bps).

The configuration for CSD mode is accessed by selecting Wireless ▷ Circuit Switched Mode, the main CSD configuration page is shown in figures 96 and 97.

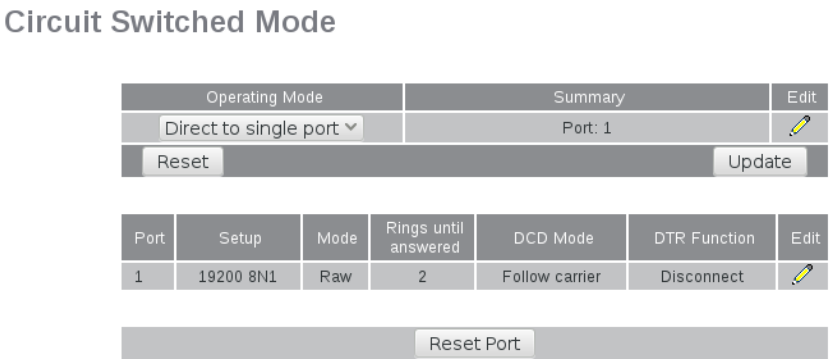


Figure 96: Circuit switched configuration

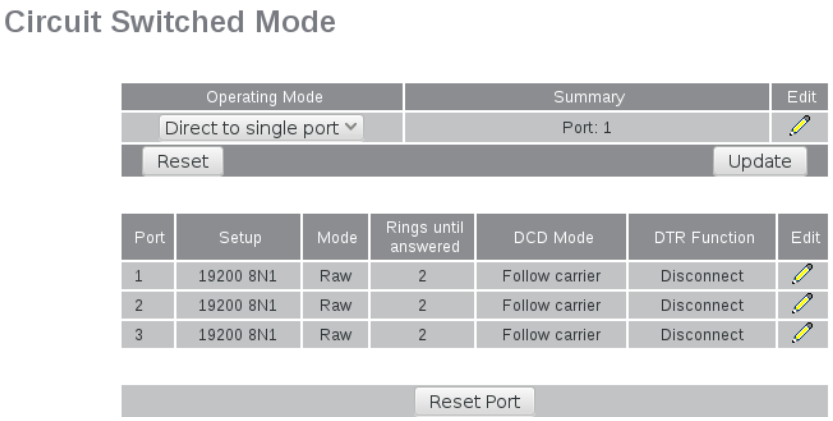


Figure 97: Circuit switched configuration

The number of serial Ports listed is model dependent. Figure 96 shows the Circuit Switch Mode page for a model with 1 serial port while 97 shows the page for a 3 port model.

The Operating mode can be configured for one of four different CSD operating modes:

Direct to single port This is the simplest mode and most like a traditional dial-up modem. An AT command interface is provided at a single selected serial port. This port can then be attached to a device (eg. PLC) which expects to be connected to a basic dial-up modem. The device is able to 'dial-out' using standard AT commands. If an incoming call is received, the modem will indicate this to the device which is able to answer the incoming call again using standard AT commands.

Multiplexed mode The multiplexed mode allows any one of the available serial ports or the PPP server to be selected at the time of connection. This is achieved through having a virtual console to which the initial connection is made. The caller can then issue a command to select a port. Once selected, all data will be directed to the selected port.

PPP server In this mode the unit acts as a PPP remote access server. After dialling in, an IP connection is established between the modem and the calling computer using the Point-to-Point Protocol (PPP). Once the PPP connection has established, all of the packet services of the modem, including the web server and serial server, can be accessed.

PPP dialout In this mode the units acts as a PPP client and will connect or dial a remote PPP server. After dialling, an IP connection is established between the modem and the server. Once this connection has been established, all of the packet services of the modem, including the web server and serial server, can be accessed.

6.4.1 Setting serial port parameters

Where the chosen CSD operating mode is **Direct to single port** or **Multiplexed mode**, it will be necessary to configure the parameters of the serial ports to match the devices attached to the modems. This configuration is set in the lower table on the CSD configuration page. To begin editing a port's set-up, click the icon in the row for that port. The port editing page will display as shown in Figure 98.

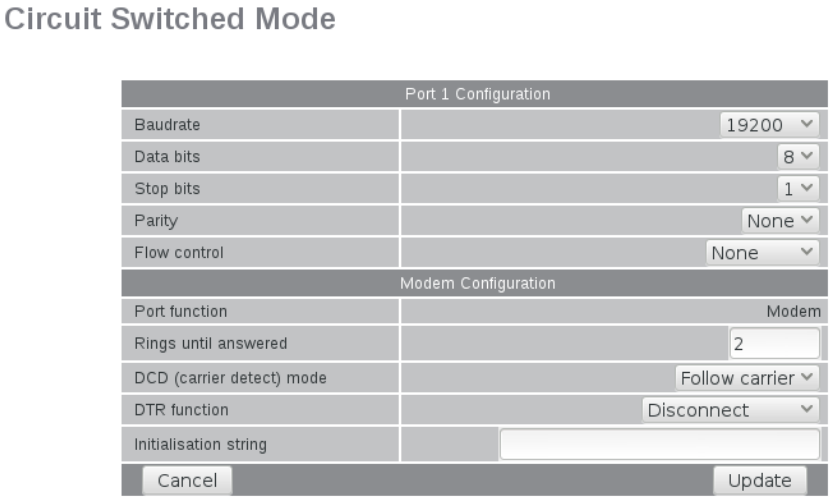


Figure 98: Editing serial port configuration.

For each port, the following parameters can be set:

Port n Configuration Baudrate The port can be configured for any standard baud rate from 300 baud to 230400 baud.

Data bits The port can be configured for operation with 5 to 8 data bits.

Stop bits The port can be configured for operation with 1 or 2 stop bits.

Parity The port can be configured for none, odd or even parity.

Flow control The serial server port can be configured for the following modes:

None No flow control is enabled.

Hardware The port will use the RTS and CTS handshake lines to control the flow of data.

Software The port will use XON/XOFF software flow control. The XOFF character is hex 0x11. The XON character is hex 0x13.

Both The port will use both hardware and software flow control.

Modem Configuration Port function When the CSD operating mode is **Multiplexed**, each serial port can be selected to function as follows:

Modem The modem will generate an AT command interface at the serial port. A device attached to the port can use standard AT commands to dial and receive calls.

Raw No AT command interface will be generated at the serial port. When the port is selected from the virtual console, a transparent data pipe is created between the serial port and the wireless port.

Rings until answered For ports configured for **Modem** mode, this field determines the default number of rings the modem will wait before automatically answering a call. This is equivalent to setting the ATS0 S-Register in a conventional modem.

DCD mode For ports configured for **Modem** mode, this field determines the default state of the Data Carrier Detect (DCD) handshaking line. The following modes are supported:

Always on Regardless of the online state of the port, the DCD line will be active (equivalent to AT&C0).

Follow carrier The DCD line will be active when the port is in the online state (equivalent to AT&C1).

DTR function For ports configured for **Modem** mode, this field determines the default response of the modem to changes in the Data Terminal Ready (DTR) handshaking line. The following modes are supported:

Ignore The port will ignore changes to the state of DTR (equivalent to AT&D0).

Command mode If the DTR line transitions from the active to inactive state while the port is on online data mode, the port will drop to AT command mode (equivalent to AT&D1).

Hangup If the DTR line transitions from the active to inactive state while the port is on online data mode, the port will terminate the current call (equivalent to AT&D2).

Initialisation string Enter and initialisation string if require.

Click the Update button to save and commit changes. The main Circuit Switch Mode page will again be displayed.

6.4.2 Configuring for direct to single port mode

To select direct mode, in the upper table, set the **Operating mode** to **Direct to single port** and click the Update button to save and commit changes.

On models with more than one serial port, it may be desired to change the port that is selected for direct mode. To do this, click the icon in the upper table. The port selection page, as shown in Figure 99 will be displayed. Select the desired port from the drop-down box and click **Update** to set the change.

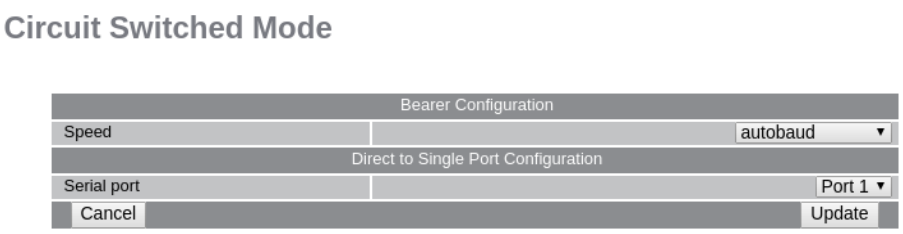


Figure 99: Setting the direct mode port

6.4.3 Configuring for multiplexed mode

Multiplexed mode allows a remote user to dial in to the modem and select the port they wish to communicate with. Whereas **Direct to single port mode** fixes the port to be selected, multiplexed mode allows the selection to be made dynamically. This is suited to applications where multiple devices are attached to the modem's serial ports.

Furthermore, the PPP server (refer to Section 6.4.4 on page 73) is also available as one of the multiplexer selections. This allows applications that normally only use serial data to dial in to the modem and create an IP connection to access modem's web server should any configuration changes need to be made.

Once a call is established in multiplexed mode, the modem will issue the following prompt:

```
CT Mux >
```

This indicates the modem is waiting for a port selection. To select a port, issue the command:

```
PORT=n<CR>
```

where n is the port number and <CR> is a carriage return. The PPP server is selected using the command:

```
PORT=PPP<CR>
```

For applications where the prompt text may interfere with serial protocols, it can be disabled using the **Menu visibility** option.

The multiplexer can support multiple port selections in a single call. Once a port has been selected, it can be deselected by issuing a special command sequence called the disconnect sequence. When received, this will cause the multiplexer to drop back to the menu prompt. An example disconnect sequence is

<2 seconds delay>???<2 seconds delay>

The delay and character used in the disconnect sequence are configurable.

To select multiplexed mode, in the upper table of the Circuit Switched Data page, set the **Operating mode** to **Multiplexed** and click **Update** to set the change. The display will update to be similar to that shown in Figure 100, the summary data will provide a summary of the multiplexed mode settings.

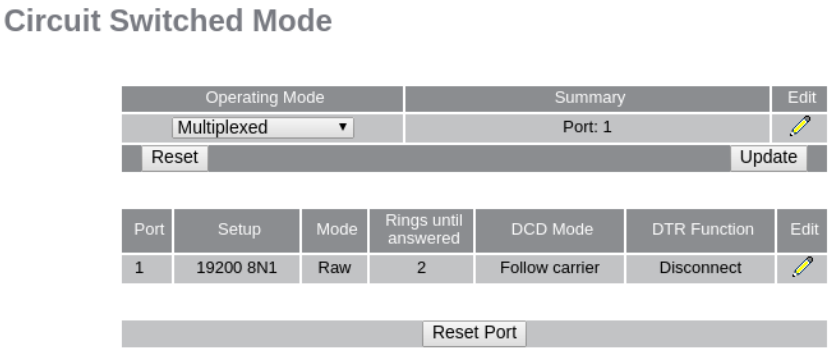


Figure 100: Setting the direct mode port

To configure multiplexed mode, click the icon in the upper table. The multiplexed mode configuration page, as shown in Figure 101 will be displayed.

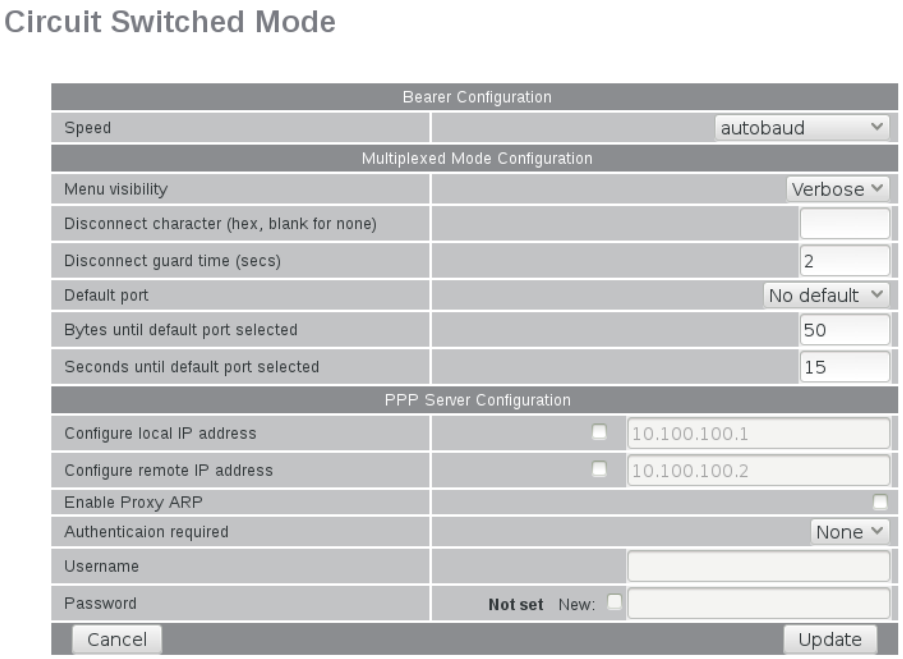


Figure 101: Configuring multiplexed mode

The following options can be configured for multiplexed mode:

Bearer Configuration Speed Choose the operating baud rate for the connection to the wireless network. The default and recommended setting is autobaud. This will automatically set the baud rate.

Changing the baud rate value for the wireless connection usually has not affect. Connection problems may occur if the baud rates do not match. It is for this reason the recommended setting is autoboud.

Multipled Mode Configuration Menu visibility Depending on the application, it may not be desirable to have the multiplexer present menu prompts to the remote modem. This field controls the display of menus:

Verbose The modem will send prompts and status updates to the remote user.

Silent No prompts will be displayed.

Disconnect character This field determines the character used in the disconnect sequence discussed above. The default is a question mark (?), which is entered as 3f hex. To disable the disconnect feature, clear all text in this field.

Disconnect guard time This field determines the idle time around the disconnect sequence discussed above. The value entered is in seconds.

Default port In some applications, it may be desirable to have one of the multiplexer's ports selected automatically if no valid PORT= command has been received within a specified amount of time or specified number of bytes. This dropdown box selects the default port.

Bytes until default port selected Where **Default port** is not set to **No default**, this field determines the number of bytes before the default port is selected.

Seconds until default port selected Where **Default port** is not set to **No default**, this field determines the seconds that can elapse before the default port is selected.

PPP Server Configuration Local IP address Check to enable and enter an IP address. This is the IP address the modem will have in the PPP connection. The address entered should be in IPv4 decimal dotted notation (eg. 10.100.100.1).

Remote IP address Check to enable and enter an IP address. This is the IP address the modem will allocate to the connection PPP client. The address entered should be in IPv4 decimal dotted notation (eg. 10.100.100.1) and must be different to the **Local IP address**.

Enable Proxy ARP Check to enable. Proxy ARP is a technique by which a device on a given network, in this case the modem, answers the ARP queries for a network address that is on a different network, in this case the network of the remote IP address.

Authentication required This fields sets the required level of authentication for remote users connecting to the modem. Available options are:

None No authentication will be required.

PAP Authentication will be required using the PAP protocol.

CHAP Authentication will be required using the CHAP protocol.

Username Where **Authentication** is not set to **None**, this is the user-name a remote user will be required to authenticate with.

Password Where **Authentication** is not set to **None**, this is the password a remote user will be required to authenticate with. To set the password, click the **New** checkbox and enter the password in the adjacent field.

Click **Update** to save any changes.

6.4.4 Configuring for PPP server mode

To select PPP server mode, in the upper table of the Circuit Switched Data page, set the **Operating mode** to **PPP server** and click **Update** to set the change. The display will change to that shown in Figure 102, notice the port list is no longer displayed. As the connection to the modem is now over a packet based PPP connection the ports must be accessed via the Serial Server. For details on the Serial Server refer to section 12 on page 207.

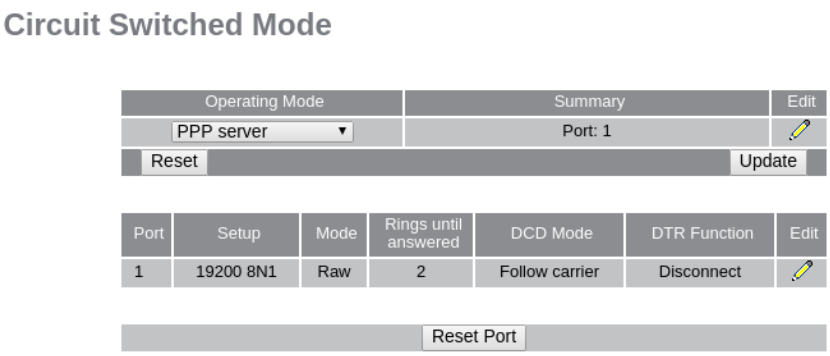


Figure 102: PPP server configuration

To configure PPP server mode, click the icon in the upper table. The PPP server configuration page, as shown in Figure 103 will be displayed.

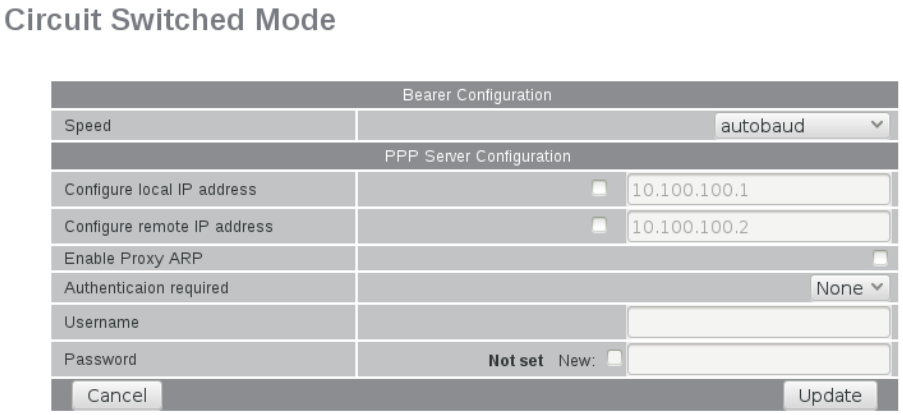


Figure 103: PPP server configuration

The following options can be set for PPP mode:

Bearer Configuration **Speed** Choose the operating baud rate for the connection to the wireless network. The default and recommended setting is autobaud. This will automatically set the baud rate.

Changing the baud rate value for the wireless connection usually has not affect. Connection problems may occur if the baud rates do not match. It is for this reason the recommended setting is autoboud.

PPP Server Configuration **Local IP address** Check to enable and enter an IP address. This is the IP address the modem will have in the PPP connection. The address entered should be in IPv4 decimal dotted notation (eg. 10.100.100.1).

Remote IP address Check to enable and enter an IP address. This is the IP address the modem will allocate to the connection PPP client. The address entered should be in IPv4 decimal dotted notation (eg. 10.100.100.1) and must be different to the **Local IP address**.

Enable Proxy ARP Check to enable. Proxy ARP is a technique by which a device on a given network, in this case the modem, answers the ARP queries for a network address that is on a different network, in this case the network of the remote IP address.

Authentication required This fields sets the required level of authentication for remote users connecting to the modem. Available options are:

None No authentication will be required.

PAP Authentication will be required using the PAP protocol.

CHAP Authentication will be required using the CHAP protocol.

Username Where **Authentication** is not set to **None**, this is the user-name a remote user will be required to authenticate with.

Password Where **Authentication** is not set to **None**, this is the password a remote user will be required to authenticate with. To set the password, click the **New** checkbox and enter the password in the adjacent field.

Click the Update button to save and commit changes.

6.4.5 PPP Dial-out

To select PPP dialout mode, in the upper table of the Circuit Switched Data page, set the **Operating mode** to **PPP dialout** and click **Update** to set the change. The display will change to that shown in Figure 102, notice that as with to PPP server the port list is no longer displayed. As the connection to the modem is now over a packet based PPP connection the ports must be accessed via the Serial Server. For details on the Serial Server refer to section 12 on page 207.

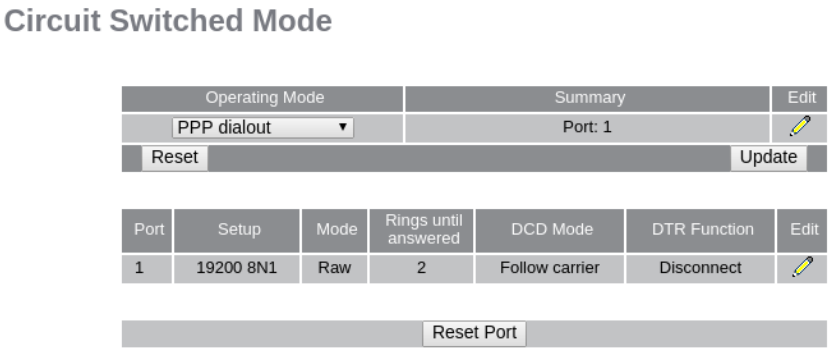


Figure 104: PPP dialout configuration.

To configure PPP server mode, click the icon in the upper table. The PPP dialout configuration page, as shown in Figure 105 will be displayed.

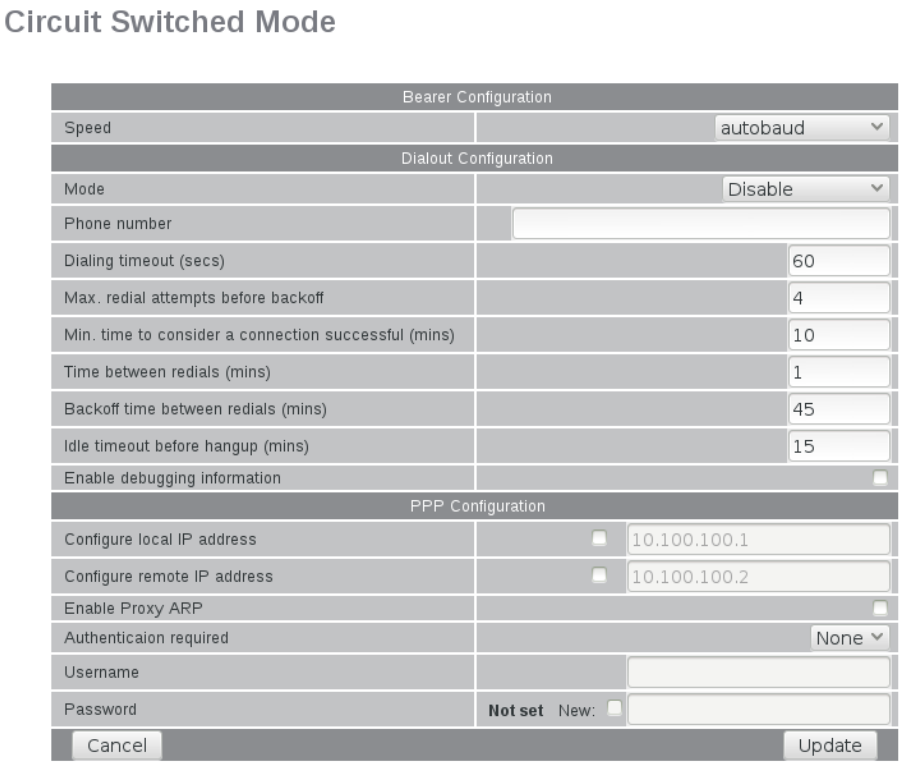


Figure 105: PPP dialout configuration.

The following options can be set for PPP Server dialout configuration:

Bearer Configuration Speed Choose the operating baud rate for the connection to the wireless network. The default and recommended setting is autobaud. This will automatically set the baud rate.

Changing the baud rate value for the wireless connection usually has not affect. Connection problems may occur if the baud rates do not match. It is for this reason the recommended setting is autoboud.

Dialout Configuration Mode This fields sets the operating mode. Available options are:

Disable Disable dial out.

Manual The connection is controlled manually by clicking the Connect and Disconnect buttons which are added to the Circuit Switch Data page when this mode is selected.

On demand The connection is made when data is sent to the interface.

Always connect The connection is permanently established.

Care should be taken when selected the operating mode as incorrect setting could result in excessive data charges.

Phone number The number to call.

Dialing timeout The time in seconds to wait for a connection after dialling.

Max. redial attempts before backoff Set the number of failed dialling attempts after which the time between dialling will be increased. This back-off prevents continuously dialling at a fast rate possibly incurring large call costs.

Min. time to consider a connection successful The minimum connection time in minutes which is considered a successful connection.

Time between redials The time in minutes to wait after a failed dial attempt before redialling.

Backoff time between redials The time in minutes to wait to redial after the back-off count has been reached.

Idle timeout before hangup The connection is considered idle when no data has been transmitted or received for this time in minutes. Once the idle time is reached the connection will be terminated.

Enable debugging information If enabled debugging information is written to the log. This can assist in diagnosing connection problems.

PPP Server Configuration Local IP address Check to enable and enter an IP address. This is the IP address the modem will have in the PPP connection. The address entered should be in IPv4 decimal dotted notation (eg. 10.100.100.1).

Remote IP address Check to enable and enter an IP address. This is the IP address the modem will allocate to the connection PPP client. The address entered should be in IPv4 decimal dotted notation (eg. 10.100.100.1) and must be different to the **Local IP address**.

Enable Proxy ARP Check to enable. Proxy ARP is a technique by which a device on a given network, in this case the modem, answers the ARP queries for a network address that is on a different network, in this case the network of the remote IP address.

Authentication required This fields sets the required level of authentication for remote users connecting to the modem. Available options are:

None No authentication will be required.

PAP Authentication will be required using the PAP protocol.

CHAP Authentication will be required using the CHAP protocol.

Username Where **Authentication** is not set to **None**, this is the user-name a remote user will be required to authenticate with.

Password Where **Authentication** is not set to **None**, this is the password a remote user will be required to authenticate with. To set the password, click the **New** check-box and enter the password in the adjacent field.

Click the Update button to save and commit changes.

6.5 SMS

SMS triggers provide a mechanisim to report and change the state of the unit. For example change the Wireless operating mode, reboot the modem and request a status summary. Each SMS trigger can individually be enabled and disabled and the text trigger can be defined for each trigger. Access control is provided to control which numbers have access to the SMS triggers.

To access the SMS Triggers select Wireless ▷ SMS a page similar to that shown in Figures 106 and 106 will be displayed, the second figure is for a model with GPIO and includes GPIO SMS triggers.

Figure 106: SMS Triggers configuration page.

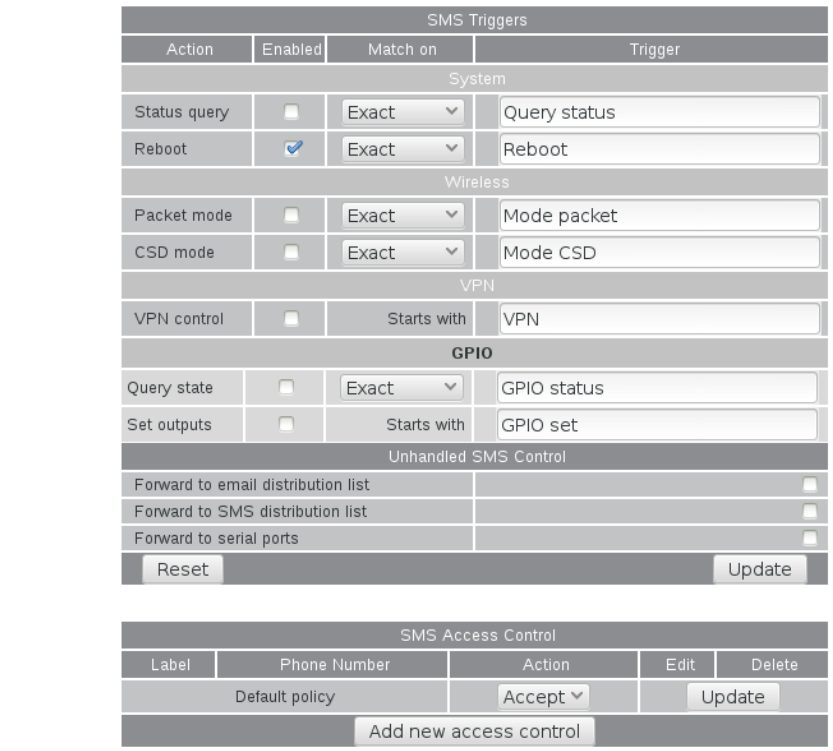


Figure 107: SMS Triggers configuration page for a model with GPIO.

6.5.1 Trigger configuration

The fields below, found in the **SMS Triggers** table, configure an individual trigger:

SMS Triggers Action The SMS actions are separated into several sections, the number of sections varies with each model. The actions are available:

System Status query Query the current state. An SMS will be returned providing current status information.

Reboot Initiate a reboot.

Wireless Packet mode Switch to packet mode.

CSD mode Switch to Circuit Switched Data (CSD) mode.

VPN VPN control Start, stop and re-start VPNs. The VPN command has 2 parameters, action and tunnel and is of the form "VPN <action> <tunnel>". The parameters are:

Action: start Start then specified tunnel.

stop Stop the specified tunnel.

restart Stop and then start the specified tunnel.

Tunnel: All Apply the action to all configured tunnels.

SSL Apply the action to only the SSL VPN.

<label> Apply the action only to the tunnel with the specified label.

GPIO General Purpose Input and Outputs (GPIO).

Query state Report the current state of the Inputs and Outputs.

Set outputs Set the state of the outputs. The output is referenced by its index number, only referenced outputs will change. The form of the command is: "GPIO set <index>=<o/c>" where:

o Sets the output <index> to Open.

c Sets the out <index> to Closed.

Enabled Set this checkbox to enable the trigger.

Match on This value determines how an incoming SMS will be searched to find a match for this trigger. The following match modes can be used:

Exact The trigger will match if the content of the SMS is identical to the **Trigger** field.

Contains The trigger will match if the content of the SMS contains the **Trigger** field.

Starts with The trigger will match if the content of the SMS starts with the **Trigger** field.

Trigger This is the text that will be used, in conjunction with the **Match on** field, to determine whether an SMS is for this trigger.

Unhandled SMS Control Set the action for SMS which do not match any of the enabled triggers. Options:

Forward to email distribution list Forward the SMS as an email to all the address contained in the email distribution list.

Forward to SMS distribution list Forward the message to all of the numbers listed in the SMS distribution list

Forward to serial ports Message will be sent to any serial ports configured in modem emulation mode.

Click the Update button to save and commit changes.

6.5.2 SMS Access control

When the modem receives an SMS, it also receives the phone number which sent the message. The SMS Access control allows source phone numbers to be verified to ensure the sender is authorised to access the modem.

Each access control is specified by setting a phone number and an associated action. The action for each control can be:

Drop Messages from the phone number will be dropped and not processed by the modem.

Allow Messages from the phone number will be accepted and processed by the modem.

The default policy determines the action to be taken when no specific access control matches a phone number. The default policy is **Allow**, however, this can be set to **Drop** for stricter level of control.

6.5.2.1 Setting the default policy to allow

This example describes setting the default policy to **Allow** then adding an entry to blacklist a particular number.

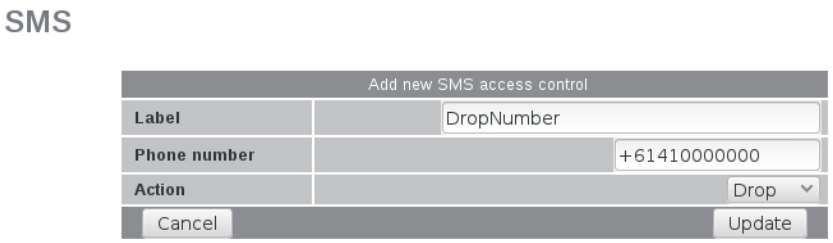


Figure 108: SMS Triggers reject entry

1. In the section titled **SMS Access Control** set the **Action** for the **Default policy** to **Accept**.
2. Click **Update** to set the changes.
3. Click the **Add new SMS access control** button.
4. In the entry form, (Figure 108) enter:
   (a) A label for the new entry.
   (b) Enter the phone number (this should be entered with the full country prefix eg. +61410000000).
   (c) Set the **Action** to **Drop**.
5. Click the **Update** button to set the changes.
6. Repeat the steps above to add further numbers.

When complete the page will include the number to be dropped, as shown in figure 109.

Figure 109: SMS Triggers number to drop added

6.5.2.2 Deleting an Entry

To delete an entry click the the icon a dialogue box similar to that shown in Figure x will be displayed. Click the OK button to remove the entry.

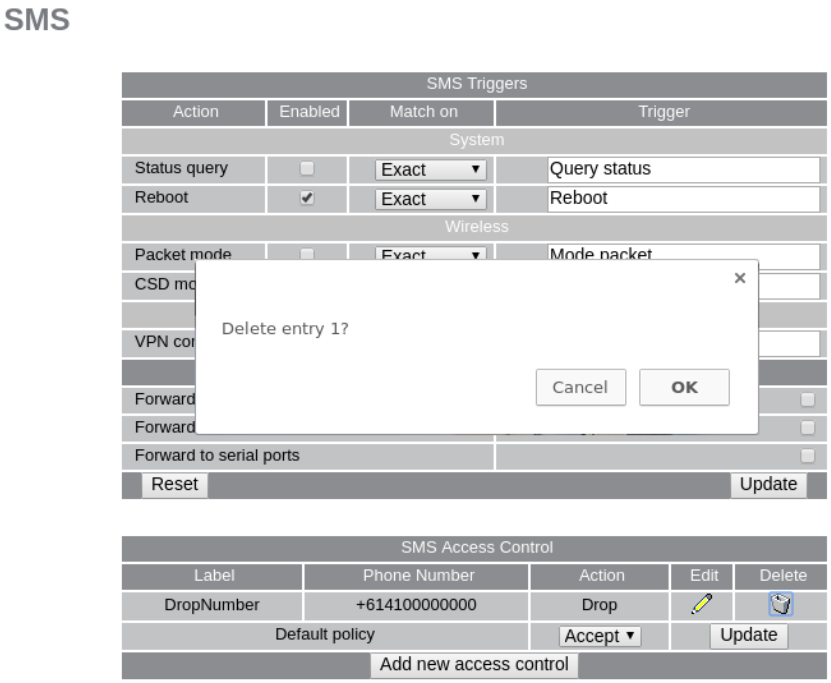


Figure 110: Deleting the Drop entry.

Figure 111: The Drop entry has been deleted.

6.5.2.3 Setting the default policy to drop

This example describes setting the default policy to **Drop** then adding an entry to allow a specific number.

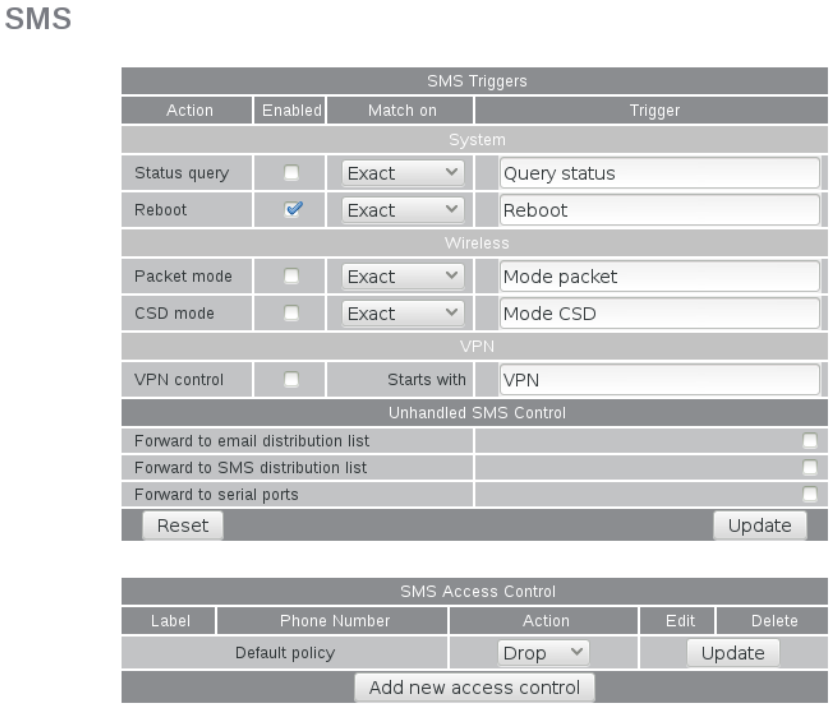


Figure 112: SMS access control default policy set to Drop.

1. In the section titled **SMS Access Control** set the **Action** for the **Default policy** to **Drop**.
2. Click **Update** to set the changes. The page will look similar to that shown in Figure 112
3. Click the **Add new SMS access control** button.
4. In the entry form (Figure 113) enter:
   (a) A label for the new entry.
   (b) Enter the phone number (this should be entered with the full country prefix eg. +61410000000).
   (c) Set the **Action** to **Allow**.
5. Click the **Update** button to set the changes.
6. Repeat the steps above to add further numbers.

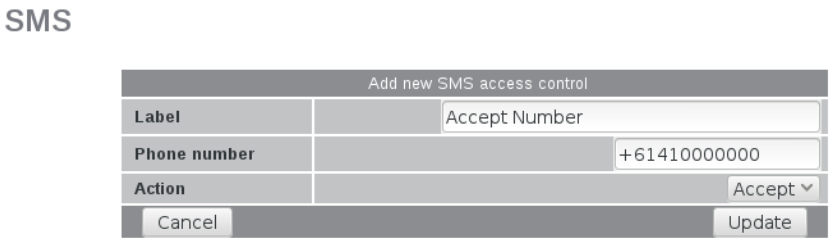


Figure 113: SMS Triggers accept entry

When complete the page will include the number to be accepted, as shown in figure 114.

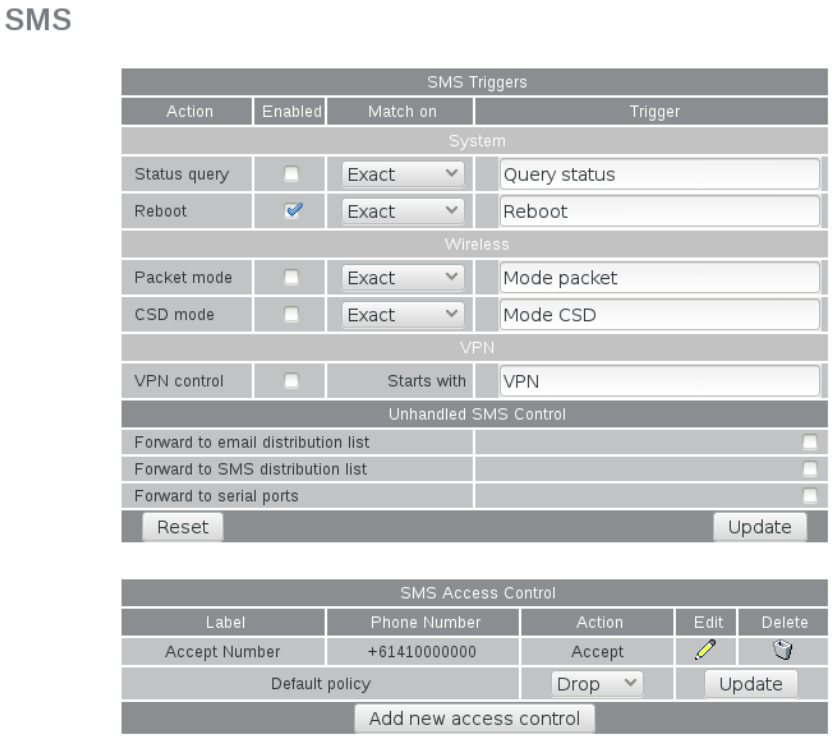


Figure 114: SMS Triggers number to accept added

6.5.2.4 Editing an Entry

To edit an entry click the icon and compete the edits. Click the Update button to save and commit changes.

6.5.3 SMS Examples

The examples listed below will all use the same configuration of the SMS triggers which is shown in Figure 115. A Model with GPIO has been used so that examples of the GPIO can be demonstrated. All SMS are sent from a standard mobile to the phone number of the SIM installed in the unit.

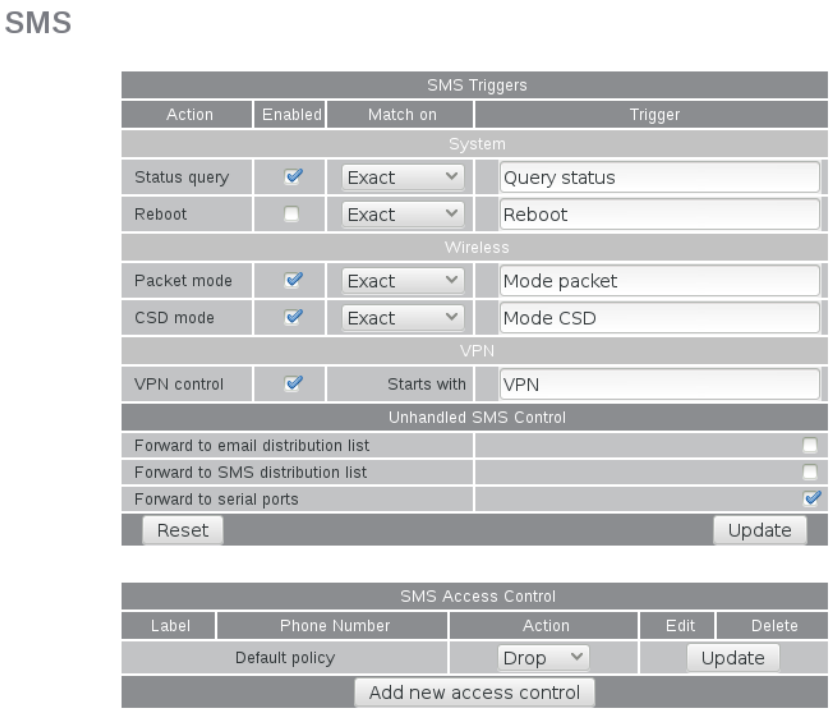


Figure 115: SMS Example configuration.

6.5.3.1 Status Query

The status query SMS is issued as follows:

Query status

The modem responds with:

Host:S2000-ff-ff-00, Uptime:14003399, Temp:37.25, RSSI:20, Mode:Pkt, State:Connected (10.192.168.23), LAN:Up (10.10.10.10)

The meaning of the fields within the message are:

Host The host name of the responding unit.

Uptime The up time in seconds.

Temp The current temperature in Celsius.

RSSI The current Receive Signal Strength Indicator (RSSI) reading.

Mode The current operating mode, either packet (Pkt) or Circuit Switched Data (CSD)

State The state of the connection. If the connection mode is packet the wireless IP address is also displayed.

LAN The state and if active the IP address of the LAN.

6.5.3.2 Reboot

In this example the unit will be rebooted.

The reboot SMS is issued as follows:

Reboot

A shut-down sequence will be initiated and the unit will reboot. This will take approximately 5 minutes during which time the unit will be disconnected from the wireless network and not accessible.

6.5.3.3 Wireless Mode

In this example the unit will be switched from packet mode to circuit switched data mode and back to packet mode. From the Status query example above the unit is currently in packet mode so the first SMS will be to switch to CSD mode.

The Wireless mode SMS is issued as follows:

Mode CSD

Now to check the mode a Query status message is sent:

Query status

The modem responds with:

Host:S2000-ff-ff-00, Uptime:14005447,
Temp:37.25, RSSI:20, Mode:CSD,
State:Offline, LAN:Up (10.10.10.10)

To switch back to packet mode another Wireless SMS is sent:

Mode packet

Again to check the mode a Query status message is sent:

Query status

The modem responds with:

Host:S2000-ff-ff-00, Uptime:14005664, Temp:37.25, RSSI:20, Mode:Pkt, State:Connected (10.192.168.32), LAN:Up (10.10.10.10)

6.5.3.4 VPN Control

The VPN control SMS is issued as follows:

VPN restart ALL

This SMS command will restart all enabled VPNs.

To restart only the VPN labelled test the following SMS command would be issued:

VPN restart test

6.5.3.5 GPIO

Two GPIO SMS commands are available the first reports the status of all inputs and outputs while the second provides output control.

To report the GPIO status the following SMS command is issued:

GPIO status

The response will be similar to:

S2000-ff-ff-00:Input-1=disabled, Input-2=disabled, Output-1=disabled, Output-2=disabled

In this case all of the inputs and outputs are reported as disabled. If the inputs and outputs are now enabled and the SMS GPIO status command is re-sent the following response is received:

S2000-ff-ff-00:Input-1=open, Input-2=open, Output-1=open, Output-2=open

To change the state of the voluptuous to closed the following command is sent:

GPIO set 1=c 2=c

An status message can now be sent to check on the result:

GPIO status

The response will be similar to:

S2000-ff-ff-00:Input-1=open, Input-2=open, Output-1=closed, Output-2=closed

The state of the two outputs has changed from “open” to “closed”.

7 DSL

The section explains the procedure for configuring the DSL interface in order to establish an ADSL or VDSL connection.

To access the configuration page for the DSL interface, click on the *DSL* tab of the main menu. The DSL Network configuration page will be displayed as shown in Figure 116.

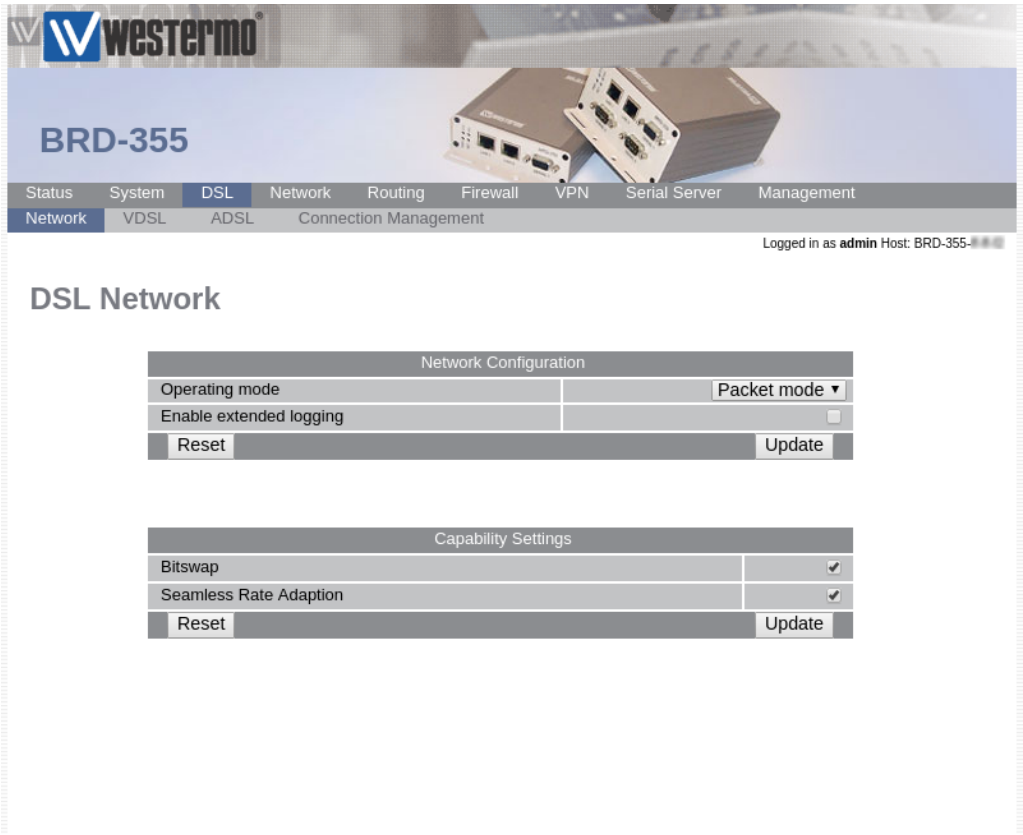


Figure 116: DSL main configuration page.

7.1 Configure the DSL Network

The DSL Network options are used to set the operating mode, and capability settings. To display the DSL Network page select DSL ▷ Network from the menu. When selected the page similar to that shown in Figure 117 will be displayed.

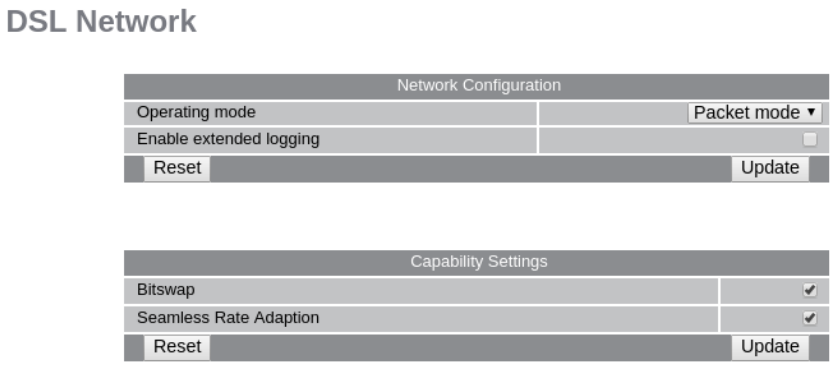


Figure 117: DSL-Network.

7.1.1 Network Configuration

The configuration options are:

Operating mode Set the operating mode of the DSL interface. Two modes of operation are supported, select from:

Packet mode In packet mode the unit acts as a TCP/IP modem and router, this is the standard and recommended mode of operation.

Disabled The DSL interface is shut-down. No data connections are possible over the DSL interface.

Enable extended logging Check to enable extended logging for the DSL interface. This option is useful if connection problems are encountered.

Click the Update button to save and commit changes. Click the Reset button to revert to the original settings.

7.1.2 Capability Settings

The configuration options are:

Bitswap Bit swap process enables the connection to either change the number of bits assigned to each individual sub-channel or if necessary increase the power level whilst still maintaining the data flow. If bit-swapping were not enabled, and a noise burst were to prevent a sub-channel being able to transmit its allocated number of bits the connection would lose sync and would need to re-train.

Seamless Rate Adaption is a feature whereby the data transmission rate is adjusted in real-time in order to adapt to changing line and network conditions in order to avoid dropping the connection. Data transmission is maintained while during the rate changes.

Click the Update button to save and commit changes. Click the Reset button to revert to the original settings.

7.2 VDSL Configuration

To access the VDSL configuration, select DSL ▷ VDSL Mode from the menu. The screen shown in Figure 118will be displayed.

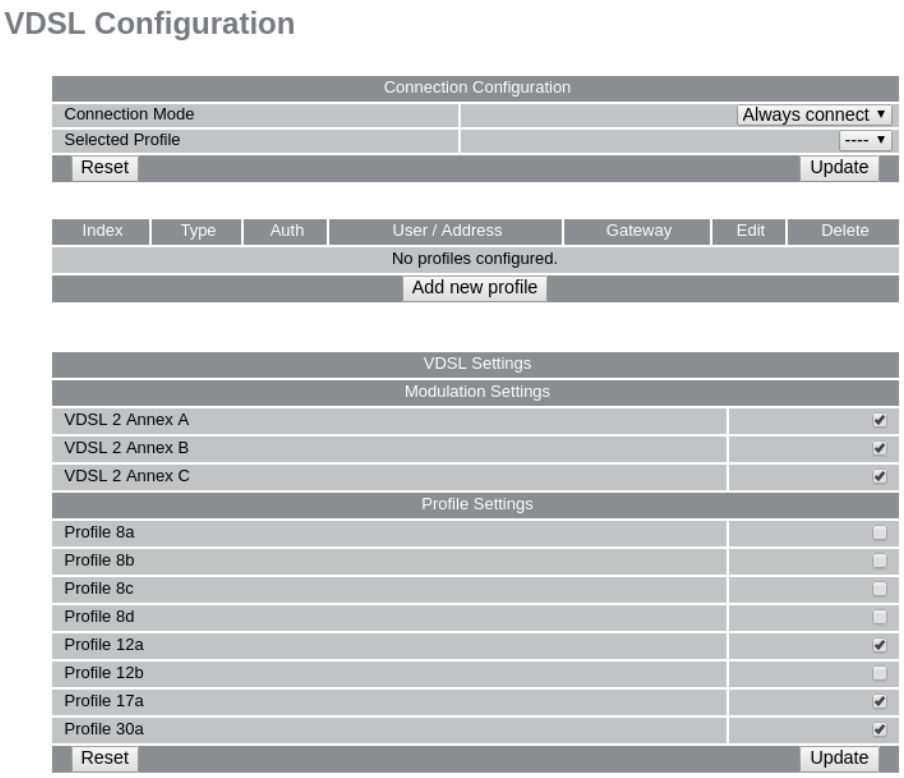


Figure 118: Main VDSL Configuration page.

7.2.1 Connection Configuration

The first section of the page is for the Connection Configuration. In order for the modem to be able to establish an VDSL connection, the details of the connection must be set up in a connection profile. This section details the process of adding, editing and deleting a VDSL connection profile. While most configurations will only need one configuration profile, multiple profiles are supported. Once the profile or profiles have been configured one can be selected as the active profile.

By default packet mode is disabled and no profiles are configured. The options are:

Connection Mode **Disabled** Packet connections are disabled.

Always Connect Establish and maintain a packet connection.

Automatic Establish a connection only when VRRP master. In order for this to function VRRP must also be configured, for details refer to section 9.3 on page 125

Profile Select the index of a defined profile. Refer to next section on how to add connection profiles.

Click the Update button to save and commit changes. Click the Reset button to revert to the original settings.

7.2.2 Profile Management

To add an VDSL profile click the Add new profile button, the Add New Profile page as shown in Figure 119 will be displayed.

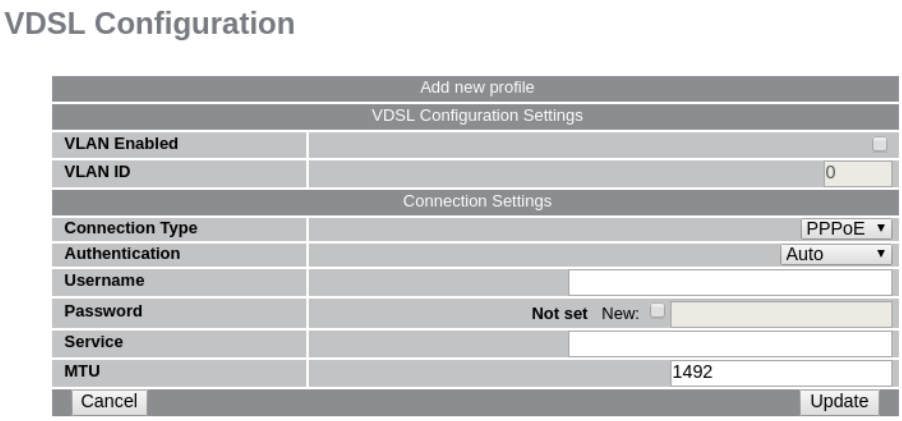


Figure 119: Add new VDSL profile

The profile contains the details for connecting to a particular VDSL service.

The network provider will specify the required settings for completing a connection profile. The provider may not supply a user-name and password if network authentication is not required. In this case set the **Authentication** to **None**.

The first section relates to VLAN settings for the DSL connection, and is common to all connection types. The options are:

VDSL Configuration Settings **VLAN Enabled** Check to enable VLAN over the DSL interface.

VLAN ID Enter the VLAN ID for use over the DSL interface.

The options within the second section listed under the title Connection Settings will changed depending on the selected connection type. The first step is to select the connection type from the drop-down list, the options are:

Connection Type

PPPoE Point to Point Protocol over Ethernet is a method of encapsulating PPP frames within Ethernet frames.

IPoE Internet Protocol over Ethernet is a method of encapsulating IP datagrams with Ethernet frames without using PPPoE.

Bridged Creates a direct connection between the LAN (Ethernet) interface and the DSL interface.

Once The connection type has been selected refer to the appropriate section below for the relevant settings.

Connection Type: PPPoE Refer to figure 120

Authentication For connections requiring a user-name and password to connect, this field sets the authentication protocol used:

None No authentication is performed.

PAP The Password Authentication Protocol is used.

CHAP The Challenge-Handshake Authentication Protocol is used.

Auto (Default) The authentication protocol is automatically determined.

MS-Chap The Microsoft version of the Challenge-Handshake Authentication Protocol (CHAP) is used.

Username For connections where the Authentication is not set to None, this is the user-name the modem will use to authenticate.

Password For connections where the Authentication is not set to None, this is the password the modem will use to authenticate. In order to set a password click the check box marked **New** then enter the password in the adjacent text field. The password is visible as it is being typed so that it can be checked for errors prior to being set. Once set the password will no longer be visible.

Service The service string.

MTU Setting for the Maximum Transmission Unit of the DSL interface.

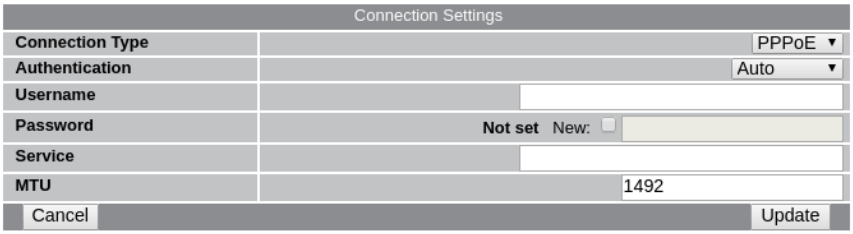


Figure 120: Add new VDSL profile with connection type PPPoE

Once the profile has been entered click the Update button to save and commit changes. Click the Cancel button to abort adding the new profile.

Connection Type: IPoE Refer to figure 121

Address Mode: Static Set a static address IP address for the DSL interface:

Address The IP address for the interface.

Netmask The netmask for the interface.

Gateway The gateway address for the interface.

DHCP The IP address settings for the interface will be set dynamically.

MTU Setting for the Maximum Transmission Unit of the DSL interface.

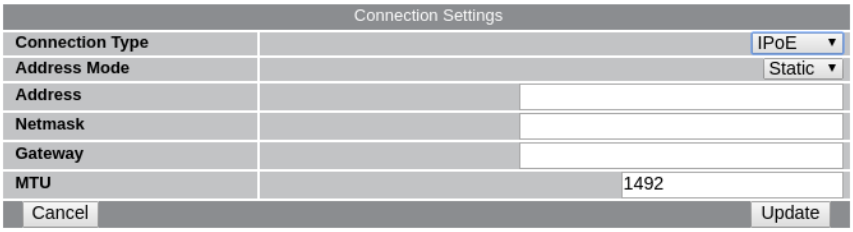


Figure 121: Add new VDSL profile with connection type IPoE

Once the profile has been entered click the Update button to save and commit changes. Click the Cancel button to abort adding the new profile.

Connection Type: Bridged Refer to figure 122

No settings required for bridged mode.

Figure 122: Add new VDSL profile with connection type bridged.

7.2.3 Example of Adding a VDSL Profile

In this example a profile will be added with the following details:

VLAN: Enabled

VLAN ID: 100

Connection Type: IPoE

Address Mode: Static

Address: 10.10.80.2

Netmask: 255.255.255.0

Gateway: 10.10.80.1

MTU: 1492

To access the VDSL configuration, select DSL ▷ VDSL Mode from the menu, a page as shown in Figure 118will be displayed. Assuming no profiles have been configured the profiles section of the page will be as shown in figure 123.

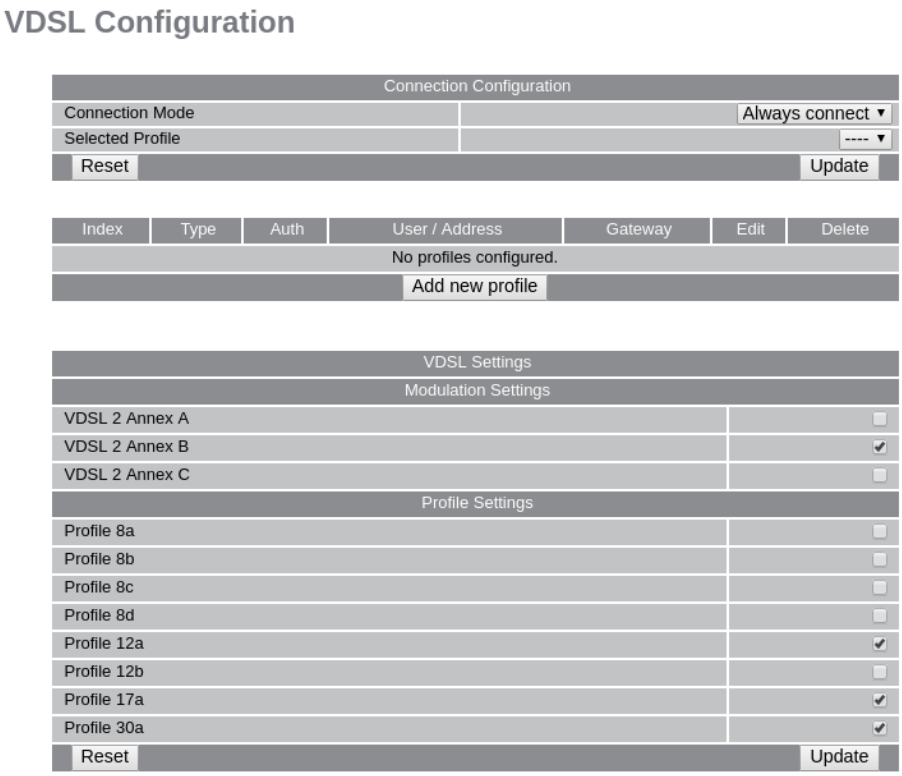


Figure 123: VDSL with no profiles.

To add an VDSL profile click the Add new profile button, the Add New Profile page as shown and the details as listed above can be entered as shown in in Figure 119.

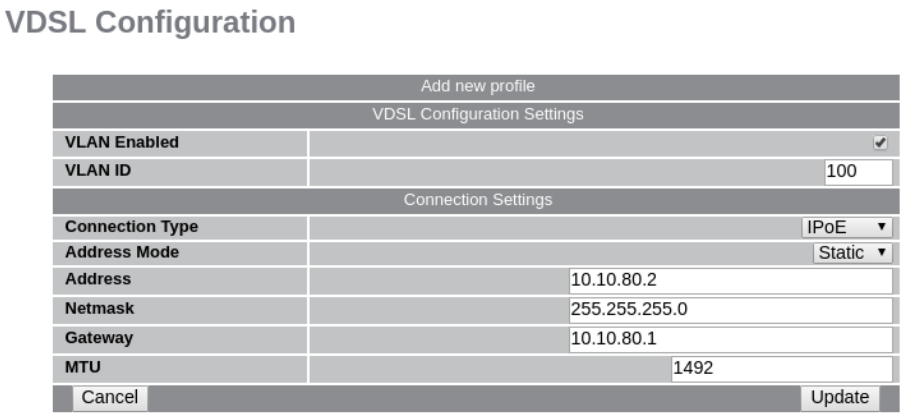


Figure 124: Example of adding a VDSL profile configuration.

Once the profile has been entered click the Update button to save and commit changes.
The VDSL page will be shown again, and the new profile will be included in the profiles list, as shown in figure 125.

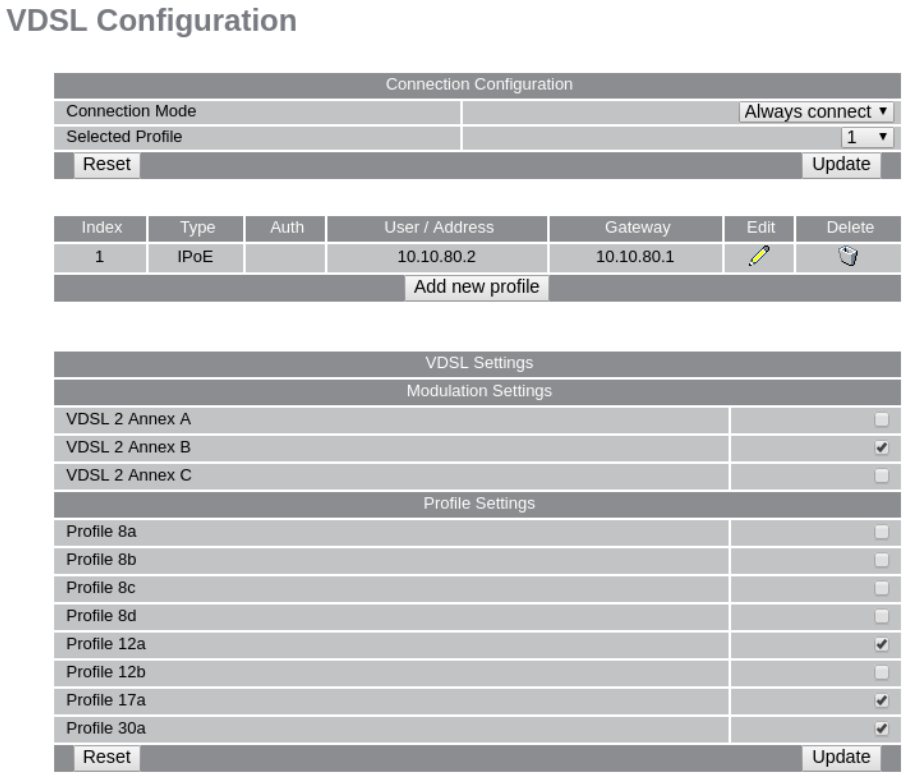


Figure 125: Main VDSL page with newly added profile.

Within the Connection Configuration section the profile should be selected as the active profile. To enable the connection change the Connection Mode from Disabled to Always connect.

7.2.4 Example of Editing a VDSL Profile

To edit an existing profile click on the icon located in the **Edit** column for the profile to be edited. A page similar to add profile page, which includes the details for the profile will be displayed.

The edit profile page for the profile entered in the example above are shown in Figure 126.

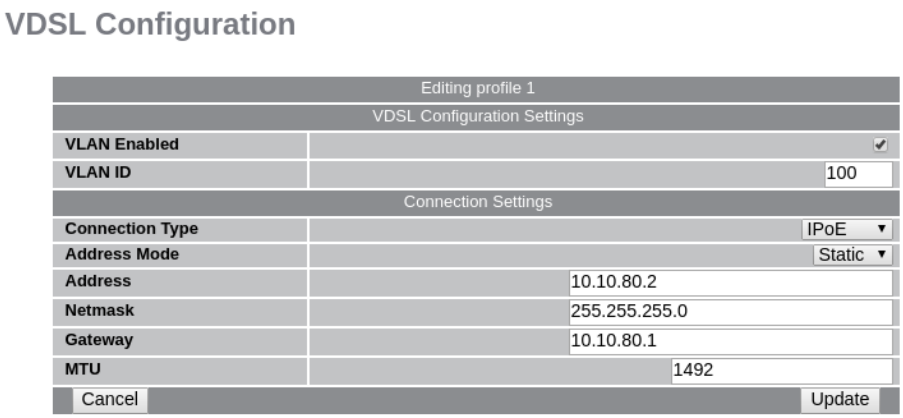


Figure 126: Edit VDSL profile example.

Once the profile has been entered click the Update button to save and commit changes. To abort the changes and leave the profile unchanged click the Cancel button.

7.2.5 Example of Deleting a VDSL Profile

A profile can be deleted by clicking the icon located in the **Delete** column for the profile to be deleted. A dialogue box will shown requesting confirmation of the deletion, Click the OK button to proceed with the deletion or click the Cancel button to abort the deletion. Figure 127 illustrations the deleting a profile entered in the example above.

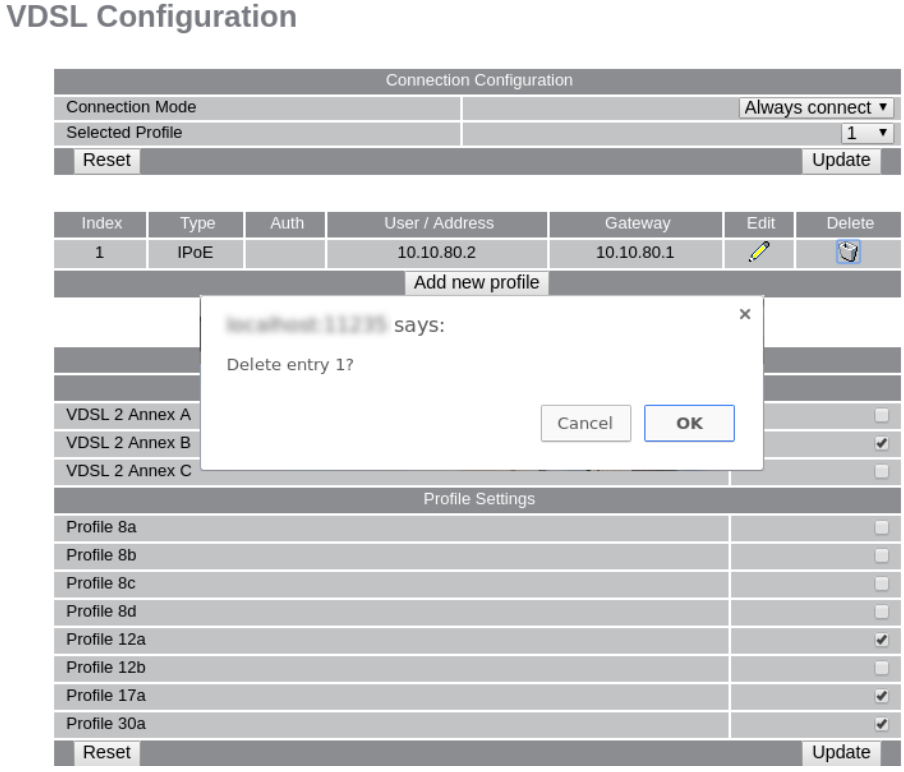


Figure 127: Deleting a VDSL profile.

After confirming the deletion of the profile the main VDSL will be shown and will be similar figure 128.

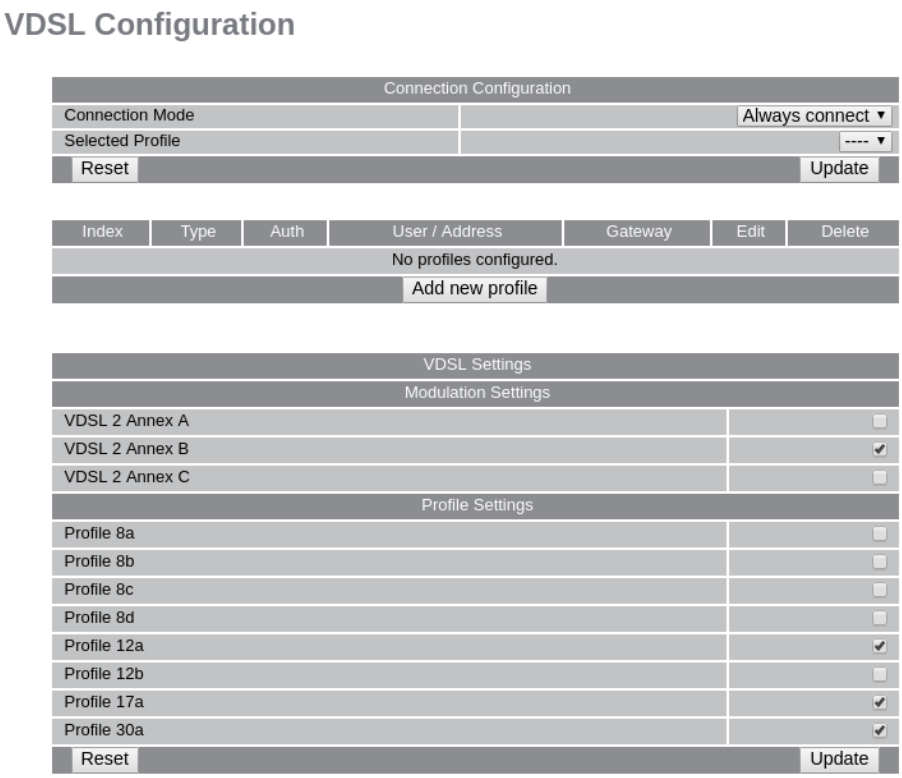


Figure 128: Profile list after deleting the VDSL profile.

7.3 ADSL Configuration

To access the ADSL configuration, select DSL ▷ ADSL Mode from the menu. The screen shown in Figure 129will be displayed.

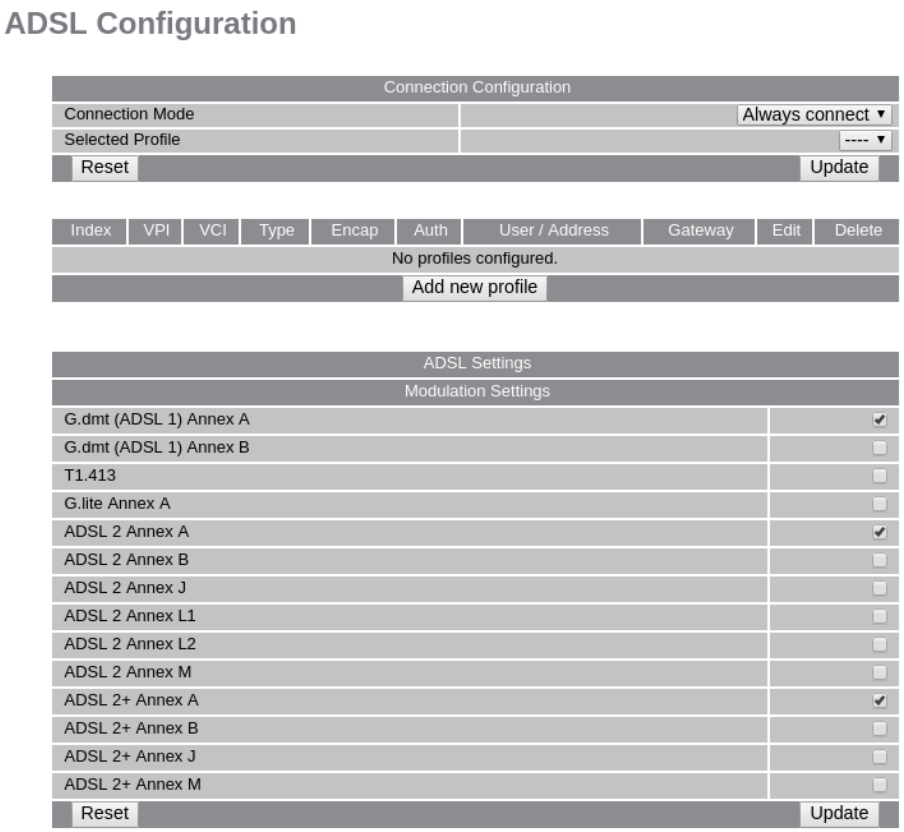


Figure 129: Main ADSL Configuration page.

7.3.1 Connection Configuration

The first section of the page is for the Connection Configuration. In order for the modem to be able to establish an ADSL connection, the details of the connection must be set up in a connection profile. This section details the process of adding, editing and deleting a ADSL connection profile. While most configurations will only need one configuration profile, multiple profiles are supported. Once the profile or profiles have been configured one can be selected as the active profile.

By default packet mode is disabled and no profiles are configured. The options are:

Connection Mode **Disabled** Packet connections are disabled.

Always Connect Establish and maintain a packet connection.

Automatic Establish a connection only when VRRP master. In order for this to function VRRP must also be configured, for details refer to section 9.3 on page 125

Profile Select the index of a defined profile. Refer to next section on how to add connection profiles.

Click the Update button to save and commit changes. Click the Reset button to revert to the original settings.

7.3.2 Profile Management

To add an ADSL profile click the Add new profile button, the Add New Profile page as shown in Figure 130 will be displayed.

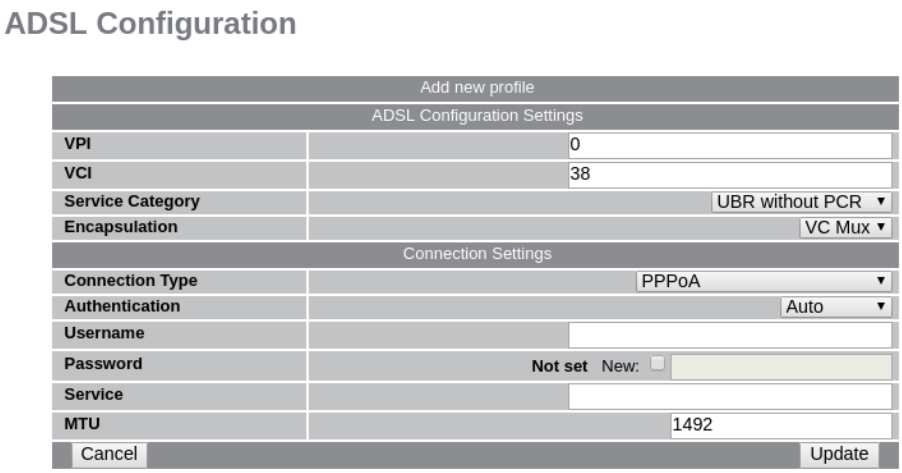


Figure 130: Add new ADSL profile

The profile contains the details for connecting to a particular ADSL service.

The network provider will specify the required settings for completing a connection profile. The provider may not supply a user-name and password if network authentication is not required. In this case set the **Authentication** to **None**.

The first section relates to the settings for the DSL connection, and is common to all connection types. The options are:

ADSL Configuration Settings **VPI** Virtual Path Identify.

VCI Virtual Circuit Identifier.

Service Category The ATM forum-defined service category. Options:

UBR without PCR Unspecified Bit Rate without Peak Cell Rate (PCR)

UBR with PCR Unspecified Bit Rate with Peak Cell Rate (PCR)

PCR Peak Cell Rate. The maximum allowable rate at which cells can be transported along a connection.

CBR Constant Bit Rate, for ATM virtual circuits requiring a static amount of bandwidth.

PCR Peak Cell Rate. The maximum allowable rate at which cells can be transported along a connection.

Non Realtime VBR Non-Real-Time Variable Bit Rate (nrt-VBR)

PCR Peak Cell Rate. The maximum allowable rate at which cells can be transported along a connection.

SCR Sustainable Cell Rate. A calculation of the average allowable, long-term cell transfer rate on a specific connection.

MBS Maximum Burst Size. The maximum allowable burst size of cells that can be transmitted contiguously on a connection.

Realtime VBR Real-Time Variable Bit Rate (rt-VBR)

PCR Peak Cell Rate. The maximum allowable rate at which cells can be transported along a connection.

SCR Sustainable Cell Rate. A calculation of the average allowable, long-term cell transfer rate on a specific connection.

MBS Maximum Burst Size. The maximum allowable burst size of cells that can be transmitted contiguously on a connection.

Encapsulation Select the mechanism for identifying the protocol carried in ATM Adaptation Layer 5 (AAL5) frames. Options:

LLC Logical Link Control.

VC MUX Virtual Circuit Multiplexing.

The options within the first section listed under the titled Add new profile will changed depending on the selected connection type. The first step is to select the connection type from the drop-down list, the options are:

Connection Type

PPPoA Point to Point Protocol over Asynchronous Transfer Mode (ATM) is a method of transporting PPP frames over ATM.

PPPoE Point to Point Protocol over Ethernet is a method of encapsulating PPP frames within Ethernet frames.

MAC Encapsulated Routing Is a method of encapsulating Ethernet frames for transfer over ATM.

IPoE Internet Protocol over Ethernet is a method of encapsulating IP datagrams with Ethernet frames without using PPPoE.

Bridged Creates a direct connection between the LAN (Ethernet) interface and the DSL interface.

Once the connection type has been selected refer to the appropriate section below for the relevant settings.

Connection Type: PPPoA Refer to figure 131

Authentication For connections requiring a user-name and password to connect, this field sets the authentication protocol used:

None No authentication is performed.

PAP The Password Authentication Protocol is used.

CHAP The Challenge-Handshake Authentication Protocol is used.

Auto (Default) The authentication protocol is automatically determined.

MS-Chap The Microsoft version of the Challenge-Handshake Authentication Protocol (CHAP) is used.

Username For connections where the Authentication is not set to None, this is the user-name the modem will use to authenticate.

Password For connections where the Authentication is not set to None, this is the password the modem will use to authenticate. In order to set a password click the check box marked **New** then enter the password in the adjacent text field. The password is visible as it is being typed so that it can be checked for errors prior to being set. Once set the password will no longer be visible.

Service The service string.

MTU Setting for the Maximum Transmission Unit of the DSL interface.

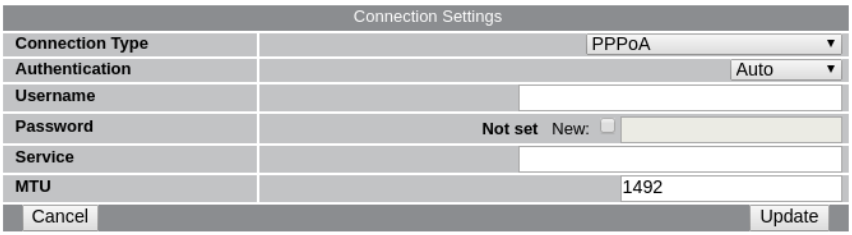


Figure 131: Add new ADSL profile with connection type PPPoA

Once the profile has been entered click the Update button to save and commit changes. Click the Cancel button to abort adding the new profile.

Connection Type: PPPoE Refer to figure 132

Authentication For connections requiring a user-name and password to connect, this field sets the authentication protocol used:

None No authentication is performed.

PAP The Password Authentication Protocol is used.

CHAP The Challenge-Handshake Authentication Protocol is used.

Auto (Default) The authentication protocol is automatically determined.

MS-Chap The Microsoft version of the Challenge-Handshake Authentication Protocol (CHAP) is used.

Username For connections where the Authentication is not set to None, this is the user-name the modem will use to authenticate.

Password For connections where the Authentication is not set to None, this is the password the modem will use to authenticate. In order to set a password click the check box marked **New** then enter the password in the adjacent text field. The password is visible as it is being typed so that it can be checked for errors prior to being set. Once set the password will no longer be visible.

Service The service string.

MTU Setting for the Maximum Transmission Unit of the DSL interface.

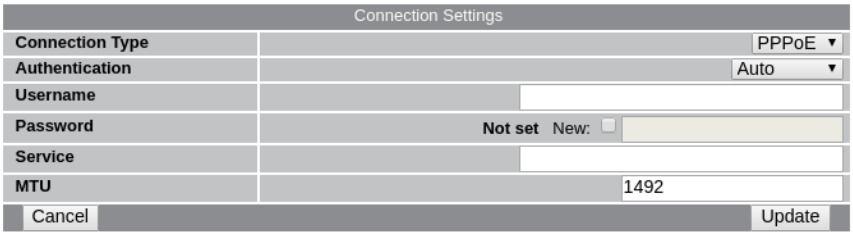


Figure 132: Add new ADSL profile with connection type PPPoE

Once the profile has been entered click the Update button to save and commit changes. Click the Cancel button to abort adding the new profile.

Connection Type: MAC Encapsulation Routing (MER) Refer to figure 133

Address Mode: Static Set a static address IP address for the DSL interface:

Address The IP address for the interface.

Netmask The netmask for the interface.

Gateway The gateway address for the interface.

DHCP The IP address settings for the interface will be set dynamically.

MTU Setting for the Maximum Transmission Unit of the DSL interface.

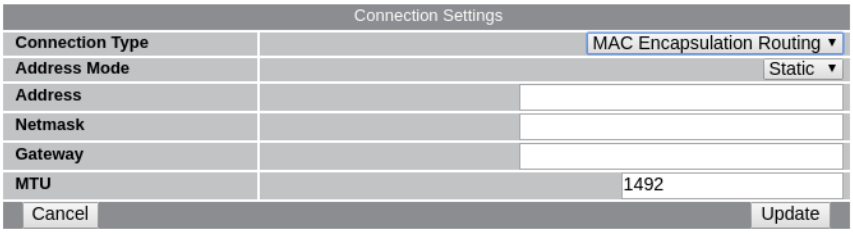


Figure 133: Add new ADSL profile with connection type MAC Encapsulation Routing.

Once the profile has been entered click the Update button to save and commit changes. Click the Cancel button to abort adding the new profile.

Connection Type: IPoA Refer to figure 134

Address The IP address for the interface.

Netmask The netmask for the interface.

Gateway The gateway address for the interface.

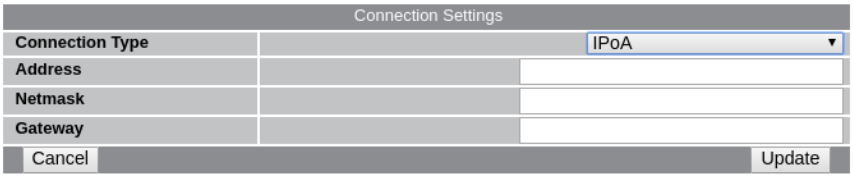


Figure 134: Add new ADSL profile with connection type IPoA

Once the profile has been entered click the Update button to save and commit changes. Click the Cancel button to abort adding the new profile.

Connection Type: Bridged Refer to figure 135

No settings required for bridged mode.

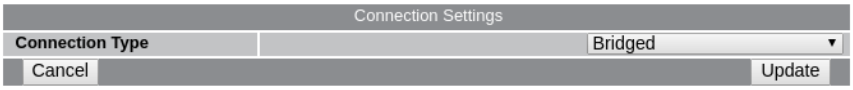


Figure 135: Add new ADSL profile with connection type bridged.

7.3.3 Example of Adding an ADSL Profile

In this example a profile will be added with the following details:

ADSL Configuration Settings:

VPI: 8

VCI: 35

Service Category: UBR without PCR

Encapsulation: LLC

Connection Settings:

Connection Type: MAC Encapsulation Routing (MER)

Address Mode: Static

Address: 10.10.80.2

Netmask: 255.255.255.0

Gateway: 10.10.80.1

MTU: 1492

To access the ADSL configuration, select DSL ▷ ADSL from the menu, a page as shown in Figure 129will be displayed. Assuming no profiles have been configured the profiles section of the page will be as shown in figure 136.

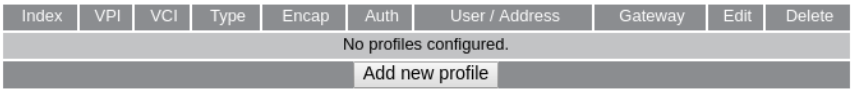


Figure 136: ADSL with no profiles.

To add an ADSL profile click the Add new profile button, the Add New Profile page as shown and the details as listed above can be entered as shown in in Figure 119.

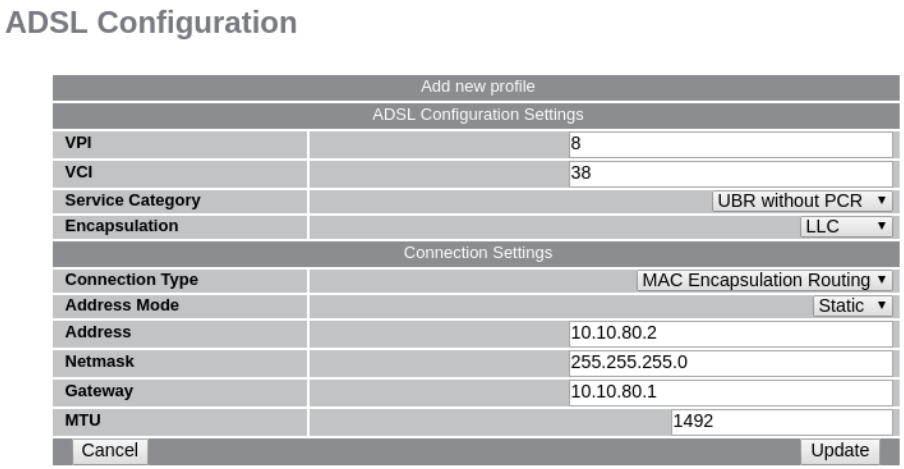


Figure 137: Example of adding an ADSL profile configuration.

Once the profile has been entered click the Update button to save and commit changes.

The main ADSL page will be shown again, and the new profile will be included in the profiles list, as shown in figure 138.

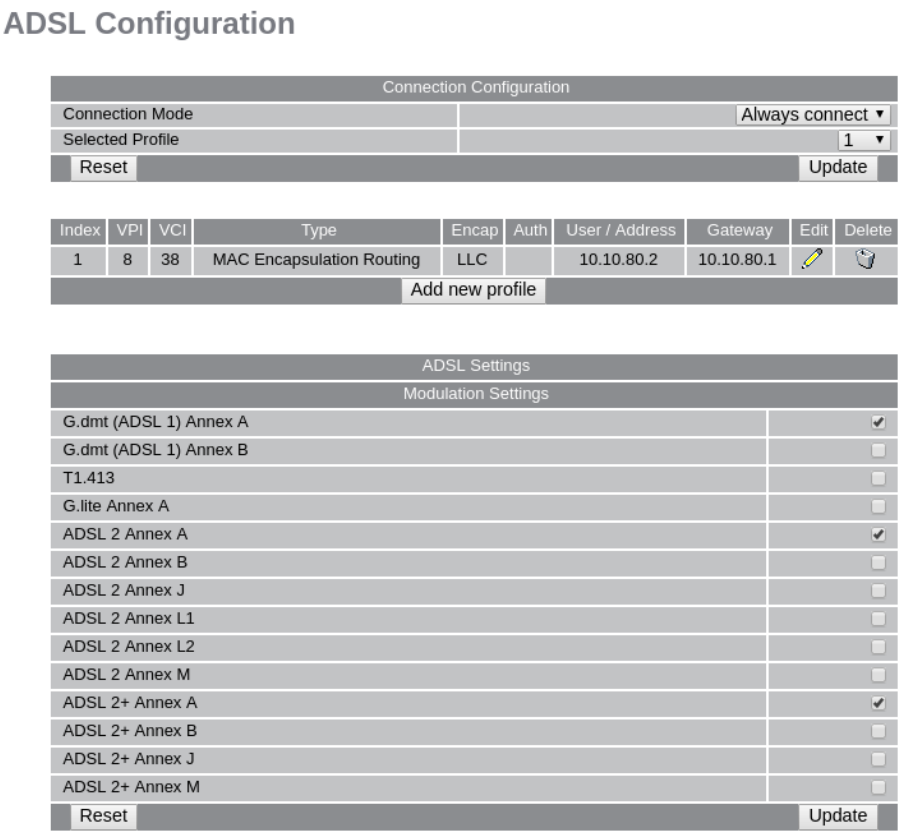


Figure 138: Main ADSL page with newly added profile.

Within the Connection Configuration section the profile should be selected as the active profile. To enable the connection change the Connection Mode from Disabled to Always connect.

7.3.4 Example of Editing an ADSL Profile

To edit an existing profile click on the icon located in the **Edit** column for the profile to be edited. A page similar to add profile page, which includes the details for the profile will be displayed.

The edit profile page for the profile entered in the example above are shown in Figure 139.

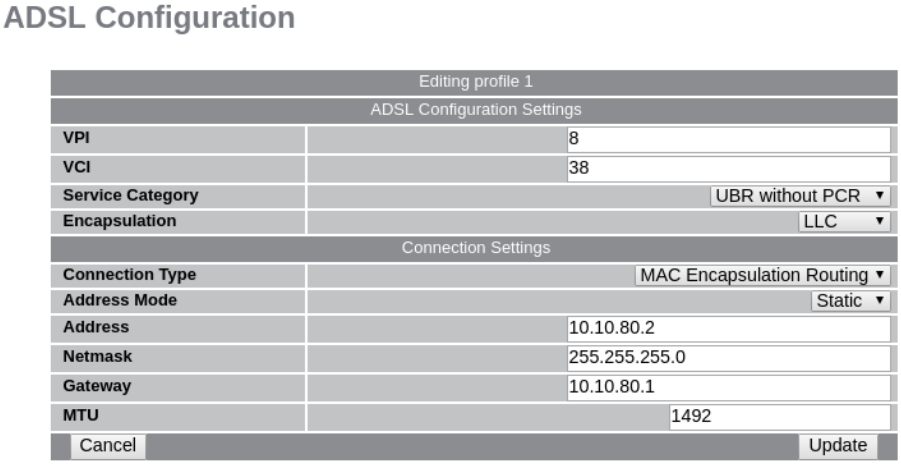


Figure 139: Edit an ADSL profile example.

Once the profile has been entered click the Update button to save and commit changes. To abort the changes and leave the profile unchanged click the Cancel button.

7.3.5 Example of Deleting an ADSL Profile

A profile can be deleted by clicking the icon located in the **Delete** column for the profile to be deleted. A dialogue box will shown requesting confirmation of the deletion, Click the OK button to proceed with the deletion or click the Cancel button to abort the deletion. Figure 140 illustrations the deleting a profile entered in the example above.

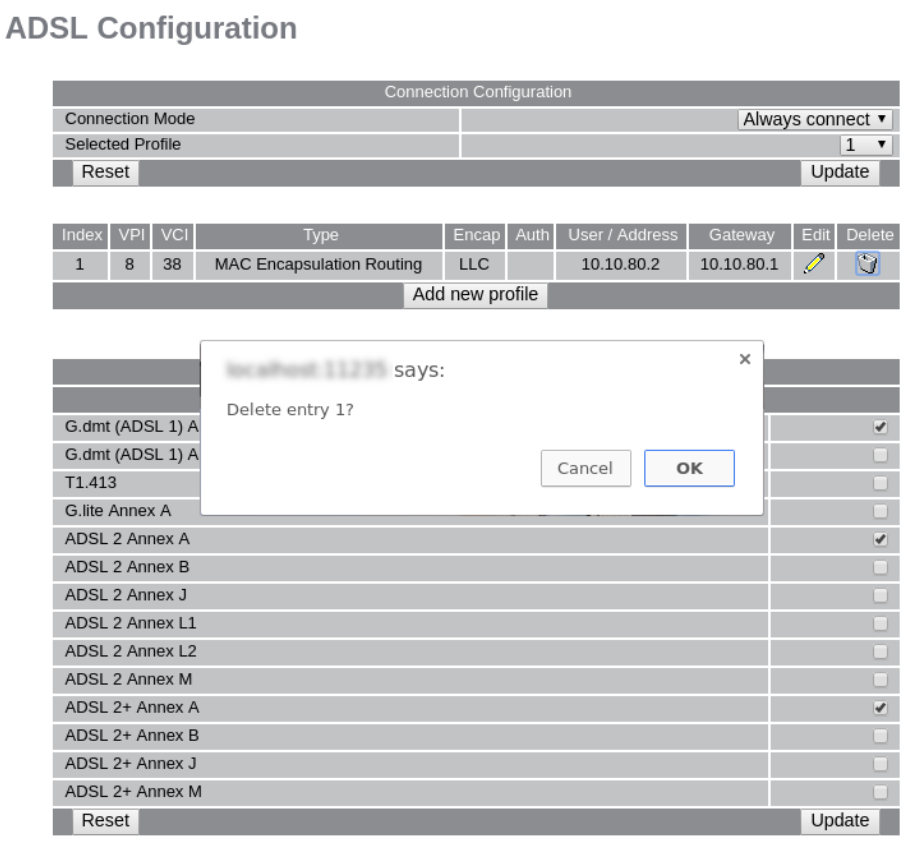


Figure 140: Deleting an ADSL profile.

After confirming the deletion of the profile the main VDSL will be shown and will be similar figure 141.

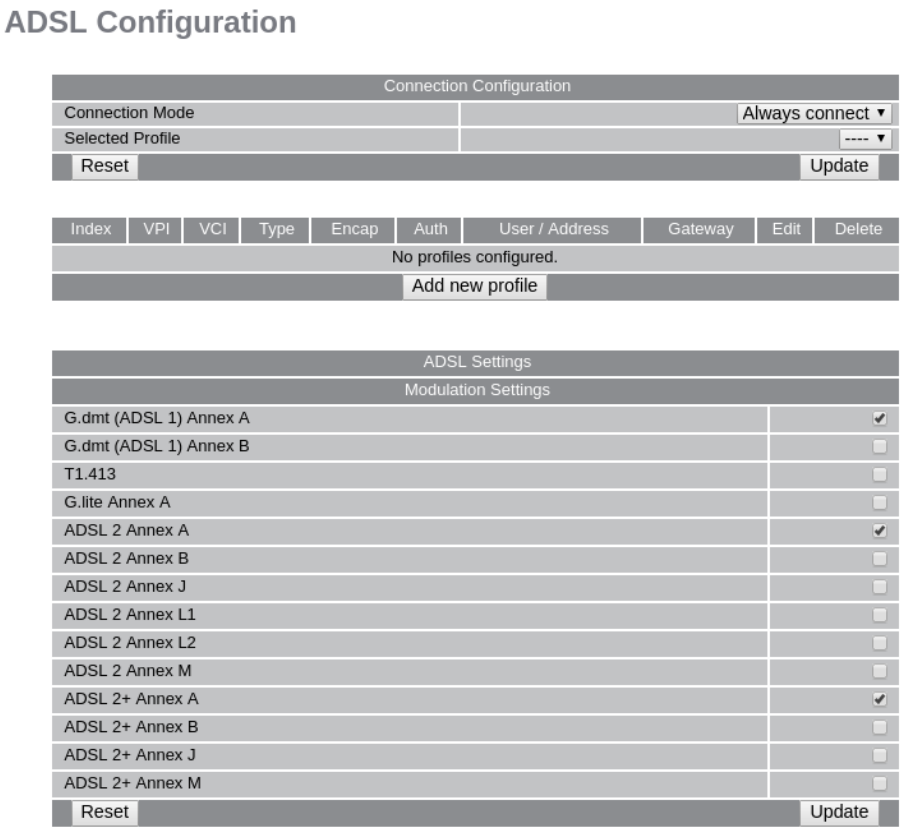


Figure 141: Profile list after deleting the ADSL profile.

7.4 Connection Status

To check the status of the connection select Status ▷ DSL from the menu, the DSL Staus page will be shown similar to that shown in Figure 142. The Network Status reports on the DSL Synchronisation status, once the connected has synced it will report Up. The connection Status reports on the packet or data connection status, once established this will report Up. For full details on the DSL status page including the Advance Status refer to Section **??** on page ??.

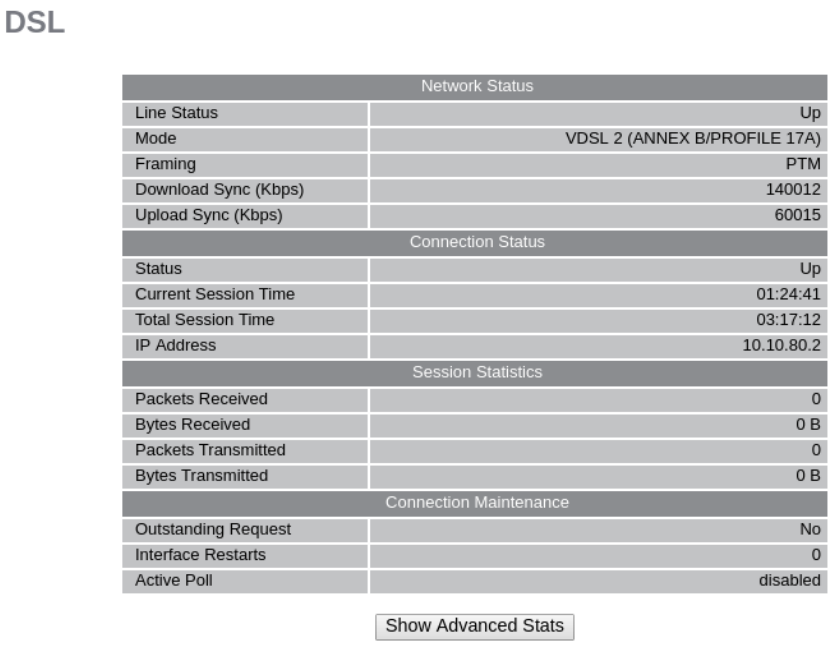


Figure 142: DSL Status page.

With the DSL connection established the Status Alarms page should now indicate no faults as shown in Figure 143.

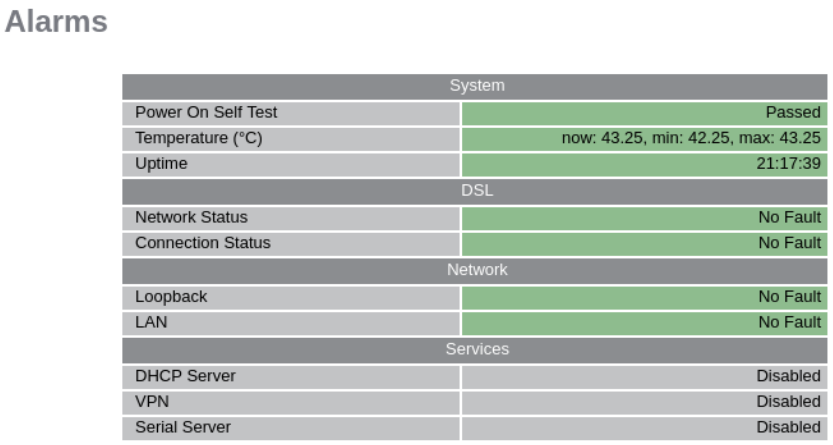


Figure 143: Status Alarms page.

7.5 Connection Management

The purpose of connection management is to create and maintain reliable connections that can detect errors and recover as quickly as possible. The connection management is divided in two areas:

Connection establishment Determines how the modem manages the establishment of a connection to the network.

Connection_management Determines how the modem manages the connection to the network once established.

To access the connection management options, select DSL ▷ Connection Management from the menu. The connection management page as shown in figure 144 will be displayed.

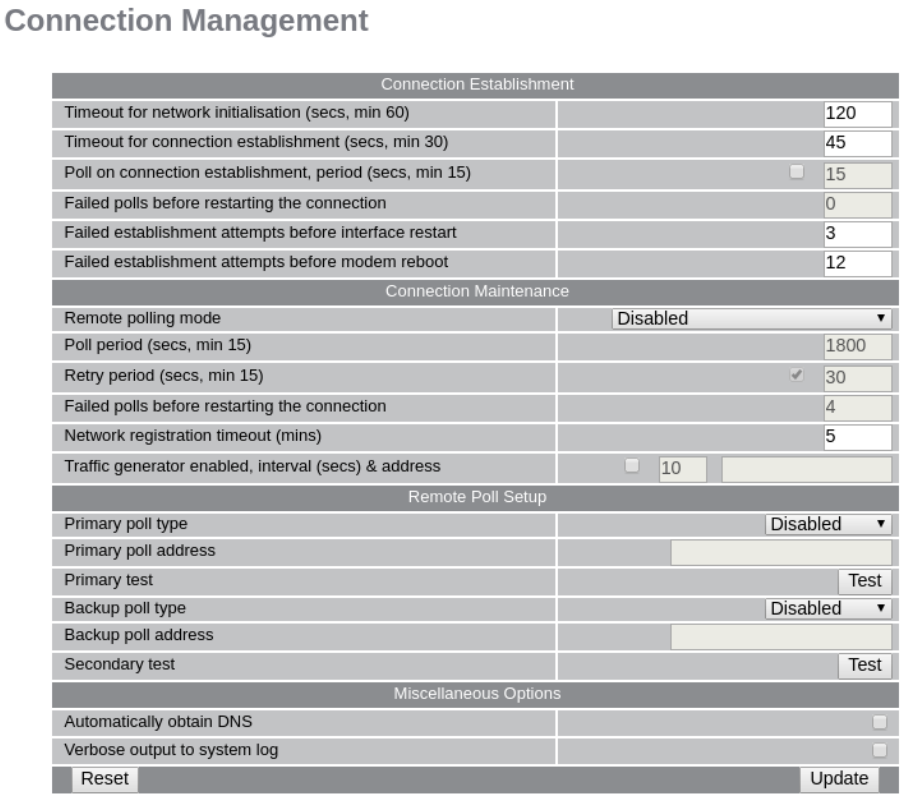


Figure 144: DSL connection management

7.5.1 Connection Establishment

The connection establishment options are used to set the parameters for initial connection to a provider's wireless network. The options are:

Timeout for network initialisation Specify the maximum time in seconds to allow for a network initialisation. The minimum value accepted is 60 Seconds, the default value is 120 seconds.

Timeout for connection establishment Specify the maximum time in seconds to allow for a connection to be established. The minimum value accepted is 30 Seconds, the default value is 45 seconds.

Poll on connection establishment Check to enable and specify the poll re-try period, the minimum value is 15 seconds. If enabled a remote poll will be completed before the connection is considered successful. The purpose of this option is to ensure that not only has a network connection been established but also that end-to-end connectivity exists. The modem does this by polling a remote server using IMP (Ping) or a TCP socket connection. Should the poll fail, the modem retries at the specified interval for the number of polls specified in **Failed polls before restarting the connection**. If this option is enabled then the **Remote Poll Setup** must be enabled and configured correctly.

Failed polls before restarting the connection Set the number of failed polls before the connection is considered to have failed to establish. A value of 0 disables poll on connection establishment. This option is only available when **Poll on connection establishment** enabled.

Failed establishment attempts before interface restart Specify the number of failed connection attempts before restarting the wireless interface. Set this value to *0* to disable.

Failed establishment attempts before modem reboot Specify the number of failed connection attempts before re-booting. Set this value to *0* to disable.

7.5.2 Connection Maintenance

The connection maintenance refers to the tests employed to determine if a valid network connection is available. Should the connection maintenance test fail then attempts will be made to re-establish the connection.

The following options control connection maintenance:

Remote polling mode Specify the connection maintenance operating mode. Four modes are supported:

Disabled Connection maintenance is disabled. (Default)

Poll at fixed interval Poll the servers specified in the **Remote Poll Setup** at the interval specified.

Poll if Rx idle for interval Only poll the servers specified in the **Remote Poll Setup** when no data has been received from the wireless interface for the specified interval.

Reconnect if Rx idle for interval Monitor the receive data and reconnect if no data has not been received by the wireless interface for the specified interval. This mode is a good choice for configurations that already employ polling traffic, such as when using the SSL VPN or IPsec VPN with dead peer detection.

Poll period Specify the time interval in seconds between polls. Minimum value of 15 seconds.

Retry period Specify the time in seconds to retry the poll after a failed poll. Minimum value of 15 seconds.

Failed polls before restarting connection Specify the number of failed polls to declare the link failed and to re-start the establishment process.

Network registration timeout Specify the time in minutes the time-out for network registration attempt after a polling failure.

Taffic generator enabled, interval & address Check to enable the traffic generator, and specify the time interval between data packets and the address to which to send the packets. The traffic generator is used to generate transmit data, it sends a data packet at the specified interval without expecting a response.

7.5.3 Remote Poll Setup

The remote poll set-up is used to specify the poll type to use and the address of the server to poll. A primary and backup server may be specified. The backup server will be used if the primary server cannot be contacted. The options for each poll are:

Primary Poll type Specify the poll type. The options are:

Disabled The poll is disabled.

Ping (ICMP) Ping the specified address.

TCP Socket Establish a TCP socket to the specified address and port number. The connection will be terminated as soon as successfully opened.

Primary Poll address Specify the address of the primary server to poll. The format used depends on the poll type:

Ping (ICMP) Enter an IP address or host-name, eg 192.168.1.1 or www.exampledomain.com

TCP Socket Enter an IP address or host-name followed by a colon and the TCP port number, for example 192.168.1.1:80

Primary test Click the test button to test the poll.

Backup Poll type Specify the poll type. The options are:

Disabled The poll is disabled.

Ping (ICMP) Ping the specified address.

TCP Socket Establish a TCP socket to the specified address and port number. The connection will be terminated as soon as successfully opened.

Backup Poll address Specify the address of the primary server to poll. The format used depends on the poll type:

Ping (ICMP) Enter an IP address or host-name, eg 192.168.1.1 or www.exampledomain.com

TCP Socket Enter an IP address or host-name followed by a colon and the TCP port number, for example 192.168.1.1:80

Backup test Click the test button to test the poll.

7.5.4 Miscellaneous Options

Automatically obtain DNS Check to enable the use of the received DNS server addresses when a connection is established as the DNS server for all look-up requests. If disabled (un-checked) a DNS server should be entered manually, refer to the Domain Name System (DNS) Section 8.4 for details.

Verbose output to system log Check to enable sending of verbose connection information to the system log. As the size of the system log is limited, this option should only be enabled if connection problems are experienced.

Click the Update button to save and commit changes.

8 Network

This section describes the configuration of the network and LAN settings. This includes setting the IP Address of the Ethernet ports, configuring the DHCP server and the DNS settings. The main Network configuration page is accessed by clicking the Network tab, a page similar to that shown in figure 146 will be shown.

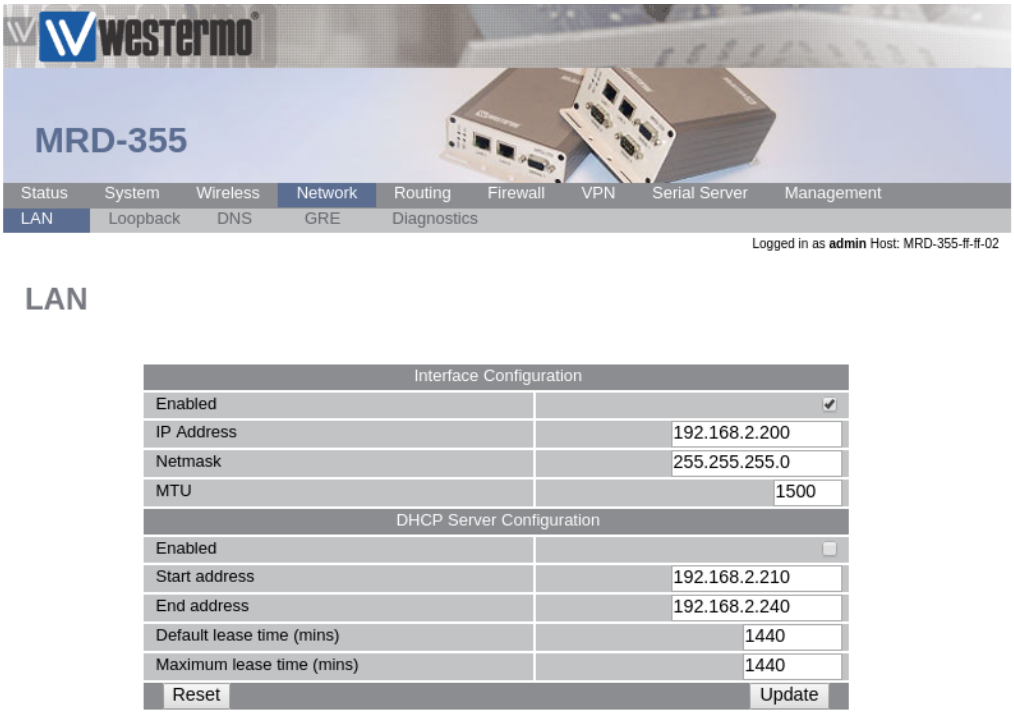


Figure 145: Main Network settings page.

8.1 LAN Interface

The LAN Interface refers to the Ethernet ports of the unit. To access the LAN Interface settings select Network ▷ LAN. Figure 146 is an example of the LAN settings page.

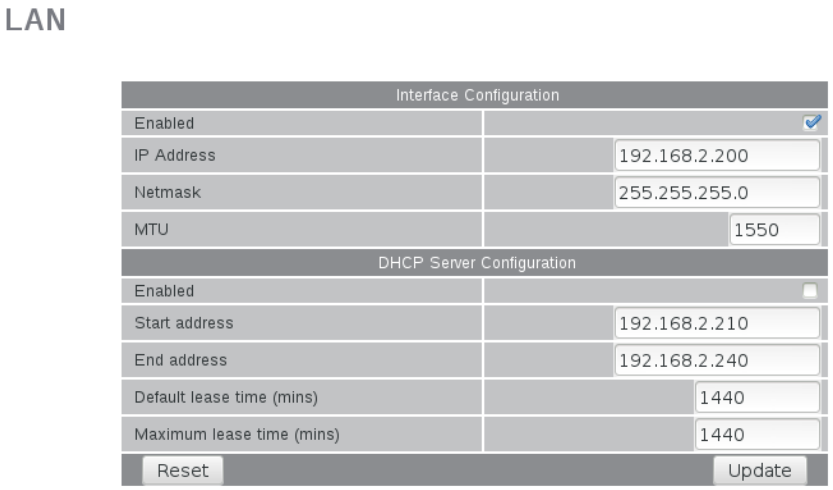


Figure 146: LAN Interface configuration

8.1.1 LAN Interface Configuration

The LAN IP address is the address used to access the modem via the LAN (Ethernet) interface.

The configuration options are:

IP Address The assigned to the LAN (Ethernet) interface.

Netmask The netmask assigned to the LAN interface.

MTU The Maximum Transmission Unit (MTU) of the LAN interface.

The default IP settings are:

IP Address 10.10.10.10

Netmask 255.255.255.0

MTU 1500

The Maximum Transmission Unit (MTU) for Ethernet II framing is 1500. This is standard framing used by most IP over Ethernet implementations. For this reason it is recommended that this value is not be changed from the default value of 1500 except where the sub-net differes from standard.
If uncertain do not change the MTU value from the default of 1500.

8.1.2 Changing the IP settings of the LAN Interface

The network settings are contained in the **Interface Configuration** table (as shown in Figure 146).

To change the IP settings:

1. Ensure that the check-box for **Enabled** is set.
2. Enter the new IP address for the LAN interface in the **IP Address** box.
3. Enter the new netmask in the **Netmask** box.
4. Click the Update button to save and commit changes.

5. A redirect message will appear in the browser similar to that show in figure 147, the browser will then be directed to the new IP address and the Network ▷ LAN will be shown.

Figure 147: LAN Interface redirect message.

If the redirect does not happen automatically, enter the new IP address into the web browser, it will also be necessary to login again due to the IP address change. For details on accessing the web pages and logging into the unit refer to Section 2 on page 2.

8.1.3 Disabling the LAN Interface

By default the LAN interface is enabled, however, for installations where the LAN ports are not required once initial configuration is complete, the ports can be disabled.

If the LAN ports are disabled then access to the web configuration pages will only be available via the wireless interface (if the the firewall settings allow access to the web server, for details on the Firewall configuration refer to Section 10 on page 140).

To disable the LAN Interface:

1. Unset the **Enabled** check-box.
2. A warning dialogue box will be displayed (similar to Figure 148), warning that once the change has been committed the LAN interface will not be accessible.
3. Click the OK button.
4. Click the Update button to save and commit changes.

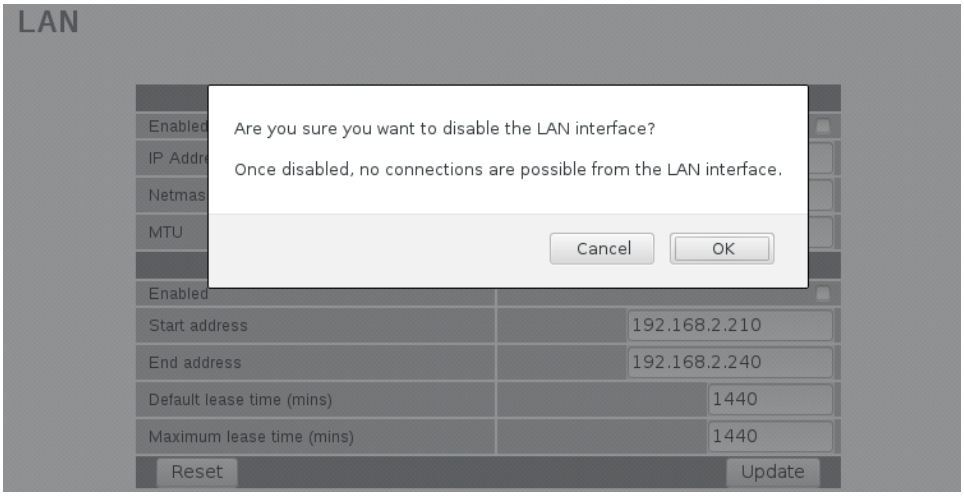


Figure 148: LAN Interface disable warning

The LAN interface will now be disabled.

To re-enable the LAN ports without accessing the web interface, it will be necessary to perform a factory reset of the unit. This will clear all the configuration settings to the factory default settings and the LAN ports will be enabled. Refer the manual for the model being configured for details on how to perform a factory reset.

8.2 Configuring the DHCP server

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides devices connected on a Local Area Network (LAN) with an IP address and other related configuration information such as the subnet mask and default gateway.

The default configuration of the DHCP server will serve IP addresses in the range 10.10.10.100 through 10.10.10.200 to requesting devices connected to the LAN interface. If the default IP address of the unit hasn't been changed this may be a suitable configuration and only enabling DHCP is required.

Should the configuration need to be change, the relevant fields are explained below:

Enabled Set the check-box to enable the DHCP server.

Start address The first IP address in the pool allocated by the DHCP server. This address must be on the same subnet as the LAN IP address.

End address The last IP address in the pool allocated by the DHCP server. This address must be on the same subnet as the LAN IP address and greater than the **Start address**.

Default lease time This field configures the default lease time given to clients. The value entered is in minutes.

Maximum lease time This field configures the maximum lease time given to clients. The value entered is in minutes.

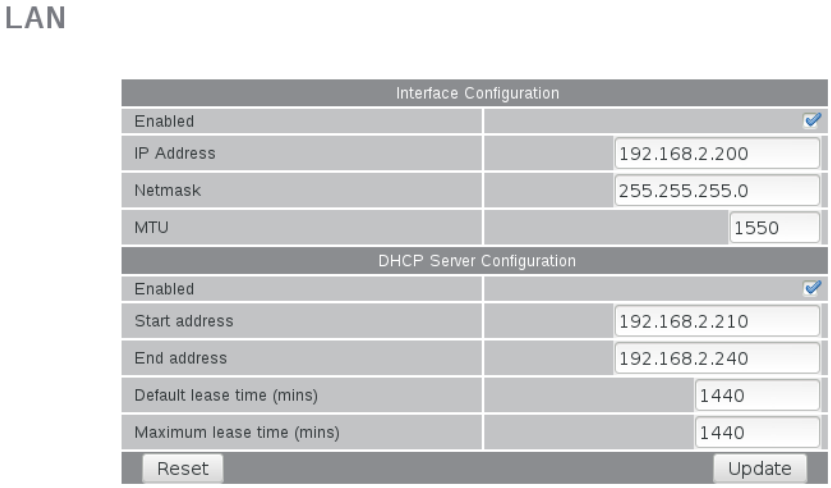


Figure 149: DHCP configuration

Click the Update button to save and commit changes.

The DHCP server will start and devices may start to request IP addresses. Any DHCP leases granted will be listed on the Status ▷ LAN page, refer to Section 4.4.2 on page 23 for details.

8.3 Loopback Interface

The loopback interface is a virtual interface which means it is an interface not associated with any hardware or network. Once configured the loopback interface address does not change, this is distinct from a physical interfaces which could be disabled or the address changed. To access the loopback interface settings select the Network ▷ Loopback page. The Loopback setting page is shown if figure 150.

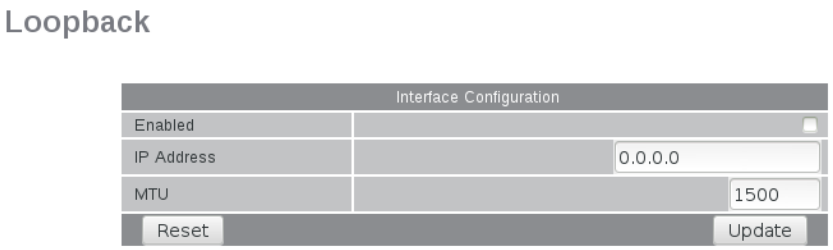


Figure 150: Loopback interface configuration.

8.3.1 Loopback Interface Configuration

Enabled Check to enable the loopback interface.

IP Address The IP address of the loopback interface.

MTU The Maximum Transmission Unit (MTU) of the loopback interface.

Click the Update button to save and commit changes.

8.3.2 Example Loopback Interface Configuration

An example Loopback interface configuration, with IP address of 10.10.10.123 is shown if figure 151.

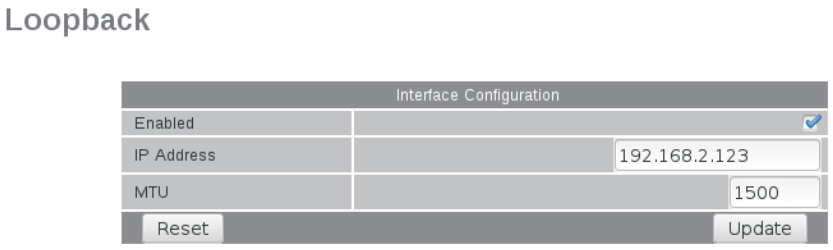


Figure 151: Example Loopback interface configuration.

8.4 Domain Name System (DNS)

The Domain Name System (DNS) is used to resolve domain names to IP addresses. DNS proxy, manual DNS configuration and a dynamic DNS client are all supported. To access the DNS settings select the Network ▷ DNS page. The DNS settings page is shown if figure 152.

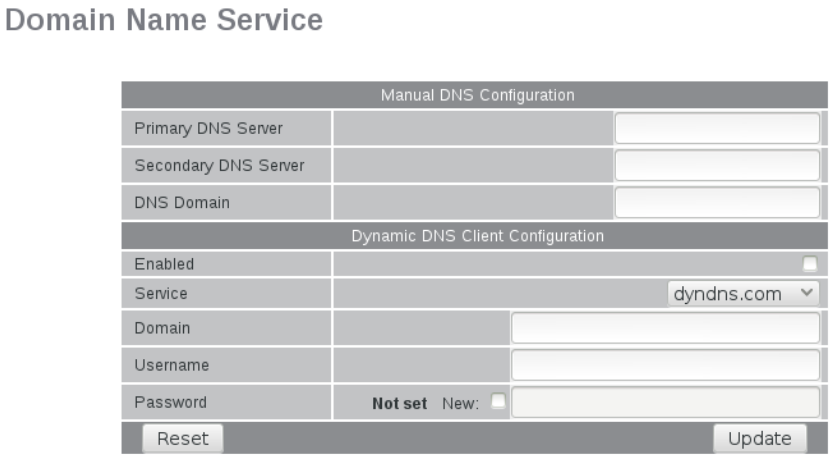


Figure 152: Domain Name Service (DNS) configuration

8.4.1 DNS Proxy

The Dynamic Name System (DNS) proxy allows clients to use the unit as a DNS proxy server. A DNS proxy improves domain lookup performance by caching previous lookups. When a DNS query is resolved by the DNS proxy, the result is stored in the device's DNS cache. The cached result is then used to resolve subsequent queries from the same domain which minimises data over the wireless network and avoids the delay due to network latency.

The cached results have an associated time-to-live (TTL) timer, when the TTL expires the entry will be purged from the cache. The DNS proxy also simplifies configuration of LAN clients, as they only need configure the IP address of the DNS proxy the DNS server. If the DHCP server has been enabled (refer to section 8.2 on page 113) then any device that connected to the LAN interface which requests an IP address from the DHCP server will also be given the IP address of the DNS proxy to use as the DNS server.

8.4.2 Manual DNS Configuration

In the majority of cases, the unit will automatically receive DNS server addresses when establishing a network connection over the WAN interface. In the majority of cases this will be the best DNS server to use.

Should it be necessary to override these values and manually enter DNS server addresses, the alternative DNS server addresses can be entered in the **Manual DNS Configuration** table. The configuration options are:

Primary DNS Server This is the IP address of the first DNS server to be queried. The value entered should be in IPv4 decimal dotted notation.

Secondary DNS Server This is the IP address of the secondary DNS server to be queried. The value entered should be in IPv4 decimal dotted notation.

DNS Domain This domain will be appended to requests without a domain name. It is useful for resolving client names on the LAN.

Click the Update button to save and commit changes.

8.4.3 Dynamic DNS Client Configuration

Dynamic DNS is a system which allows the domain name data held in a name server to be updated in real time. The most common use for this is in allowing an Internet domain name to be assigned to a device with a dynamic IP address.

If the wireless service the modem connects to allocates the modem a public, dynamic IP address, it may be possible to use a dynamic DNS provider to update the address of the modem in the DNS system. Once this address is registered, other hosts with Internet access can reach the modem at the domain name.

Drop-down Option	Provider
dyndns.com	http://www.dyndns.com/
no-ip.com	http://www.no-ip.com/
zoneedit.com	http://zoneedit.com/
easydns.com	http://www.easydns.com/

Table 1: Dynamic DNS providers

Not all wireless providers allocate public IP addresses. Addresses in the range 10.0.0.0 - 10.255.255.255, 172.16.0.0 - 172.31.255.255 and 192.168.0.0 - 192.168.255.255 are not public addresses and will most likely not be suitable for use with dynamic DNS.

Some wireless providers do not allow inbound connections at all, so even though the dynamic DNS client will connect and register the IP address provided to the unit, all attempts to connect to that IP address will fail.

In order to use the dynamic DNS feature, it is first necessary to register at a dynamic DNS provider. The supported providers are listed in table 1.

Once registration is complete, the fields of the **Dynamic DNS Client Configuration** table must be completed. The fields are explained below.

Enabled Set this check-box to enable dynamic DNS updating.

Service Select the appropriate service from the list.

Domain Enter the name of the domain allocated by the dynamic DNS provider.

Username Enter the user-name for the account with the dynamic DNS provider.

Password Enter the password for the account with the dynamic DNS provider.

Click the Update button to save and commit changes.

Figure 153 shows an example DynDNS configuration.

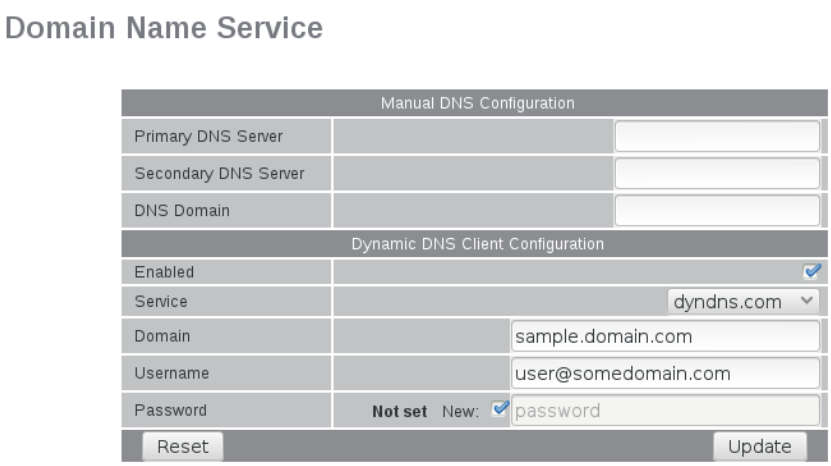


Figure 153: Dynamic DNS Client configuration

8.5 Generic Routing Encapsulation (GRE)

Generic Routing Encapsulation (GRE) is a tunnelling protocol which can encapsulate a wide variety of network layer protocol packet types within a virtual point-to-point link over an IP network. To access the GRE configuration page select Network ▷ GRE a page similar to that shown in Figure 154 will be displayed. This page lists all currently configured tunnels.

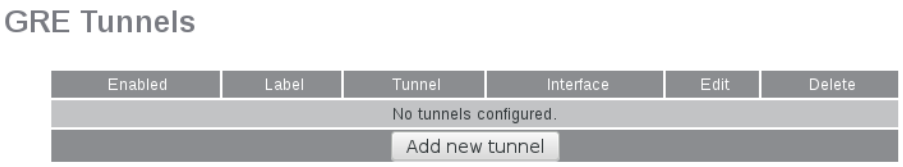


Figure 154: GRE Configuration.

To add a new GRE tunnel click the Add new tunnel button and a page similar to that shown in Figure 155 will be displayed.

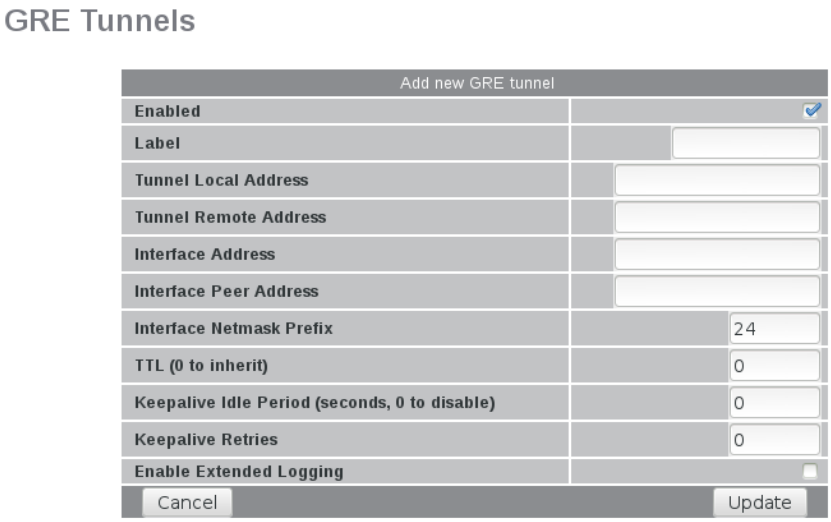


Figure 155: Add a GRE tunnel.

The available options are:

Label The name or label associated with the tunnel.

Enabled Check to enable this particular tunnel.

Remote Address The IP address to which the tunnel is to connect.

Local Address The local address to which the tunnel terminates.

Tunnel Address The address of the tunnel interface.

Peer Address

TTL Time To Live value.

Click the Update button to save and commit changes.

8.6 Network Diagnostics

Ping and Traceroute are two commonly used tools for analysing packet flows and diagnosing network issues. Ping and traceoute requests can be generated via the web interface. To access the diagnostic tools, select Network ▷ Diagnostics. Figure 156 illustrates the available options. The top section is used to select the test type and enter the host name or IP address. The results are presented in the box below.

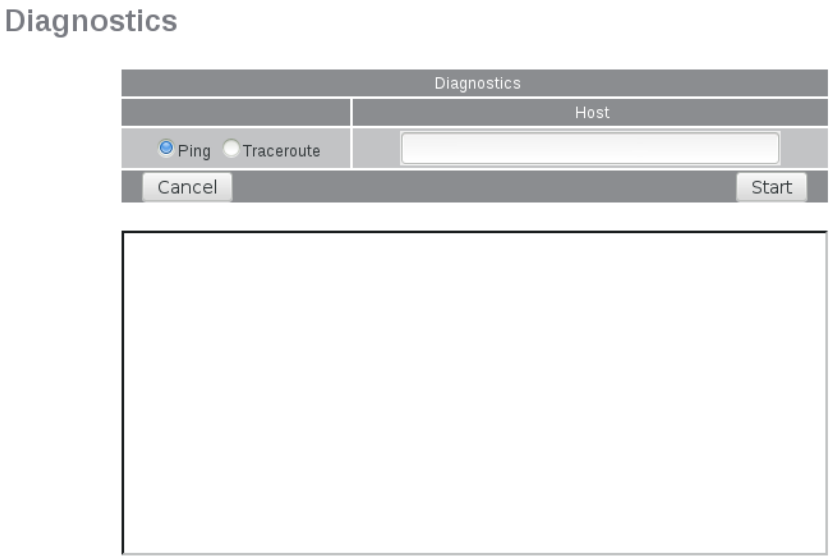


Figure 156: Network diagnostics.

To initiate a test, select **Ping** or **Traceroute** as appropriate and enter a host-name or IP address in the **Host** field. Click the Start button to begin the test. The web page will refresh every 3 seconds until the test completes. A test can be cancelled or the result box cleared by clicking the Cancel button.
Figure 157 is an example of a completed ping test.

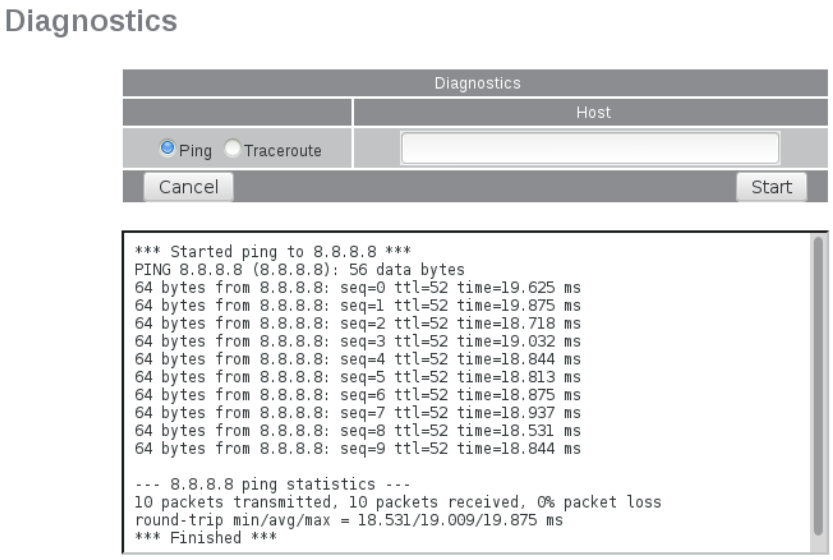


Figure 157: Network diagnostic test

9 Routing

The routing configuration determines how packets arriving from the different interfaces will be delivered to their destination. The routing options are accessed by clicking *Routing* on the main menu, the screen will appear similar to that shown in Figure 158.

Figure 158: The main routing page.

9.1 Default and Static Routes

The Default & Static Routes are the default routing page and can also be accessed by selecting Routing ▷ Default & Static. Figure 158 illustrates the Default & Static Routes page with no routes configured.

9.1.1 Default route

The default route is the network route used when no specific route exists for an IP packet's destination address. All the packets for destinations not defined in the routing table are sent to the default route. This route will lead to another router for further routing.

In the default configuration the Primary default gateway is via the wireless interface (**WLS**). In the majority of situations there will be no need to change this setting. A Secondary default gateway can also be configured which will be used in the event of the interface specified as the Primary default gateway being unavailable.

Figure 159: The Default and Static Routes configuration page

To change the default route select an option from the drop-down list. The possible interfaces include:

WLS Wireless interface.

SSL VPN The SSL VPN interface. This option is only valid if an SSL VPN has been configured. Refer to Section Virtual Private Network (VPN) for details.

WLS CSD The wireless circuit switched data interface. This option is only valid if the unit is operating in Circuit Switched Data (CSD) mode and the PPP server has been enabled.

Serial n The serial port, where n is the number of the port. This option is only valid if the serial port is configured to operate in one of the PPP modes.

Custom Use the IP address entered in the adjacent field.

Once the required default route has been selected click the Update button to save the change.

To configure a Secondary default gateway check the check-box to enable the Secondary default gateway then select an option from the drop-down list. The possible interfaces are the same as listed above for the Primary default gateway. Once the required default route has been selected click the Update button to save the change.

9.1.2 Static routes

Static routes are manually entered routes which direct certain traffic over a network in a fixed or static way. Static routes may be useful for creating exceptions to the default route or for working in complex LAN environments where the configuration is known and consistent.

The diagram in Figure 160 shows a scenario where static routes can be used. In the example, in addition to the 10.10.10.0 subnet the unit is attached to, there is a further subnet (10.10.20.0) reachable via the router at 10.10.10.200. Without a static route, the modem would not know how to handle packets for the 10.10.20.0 subnet and would send them to the default route. With a static route, packets will be correctly forwarded to the router at 10.10.10.200.

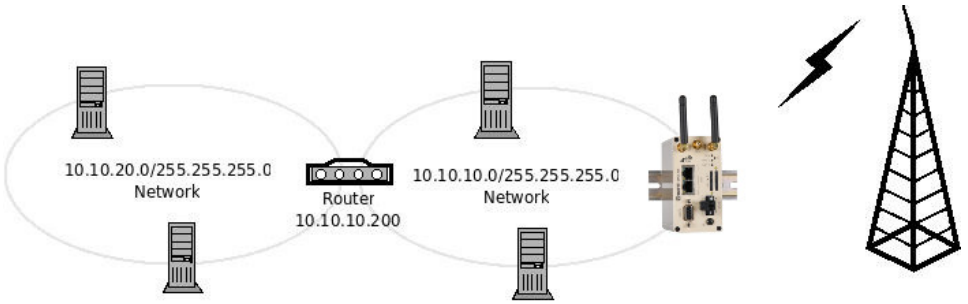


Figure 160: Static routing example

9.1.3 Static route options

The static route options are shown when the Add new static route button is clicked or an existing route is edited. The static route options will be displayed as shown in Figure 161.

Figure 161: Static route options

The following options can be set for each static route:

Enabled Set the enabled check box to have the route installed. A route can be temporarily disabled by un-checking this box.

Target address This is the network or host the static route will target.

Netmask This is the network mask to apply to the static route. The mask entered should be in IPv4 decimal dotted notation. For a host-only route, the netmask is 255.255.255.255.

Gateway Determines the gateway that packets whose destination addresses matched the target address will be routed to. The gateway can be one of the following:

WLS Wireless interface.

SSL VPN The SSL VPN interface. This option is only valid if an SSL VPN has been configured. Refer to Section Virtual Private Network (VPN) for details.

WLS CSD The wireless circuit switched data interface. This option is only valid if the unit is operating in Circuit Switched Data (CSD) mode and the PPP server has been enabled.

Serial n The serial port, where n is the number of the port. This option is only valid if the serial port is configured to operate in one of the PPP modes.

Custom Use the IP address entered in the adjacent field.

Metric The metric is used to determine whether one route should be chosen over another, where both routes are possible. The packet will be directed to the route with the lowest metric.

Insert this entry at position Determines where this entry will be inserted in the list of static routes.

9.1.4 Adding a new static route

From the Default & Static Route page click the Add new static route button, the Add new static route page will be displayed.

An example of adding a new static route is shown in Figure 162. In this example, a new route is to be created that routes all traffic for the 10.10.20.0 subnet via the router at address 10.10.10.200.

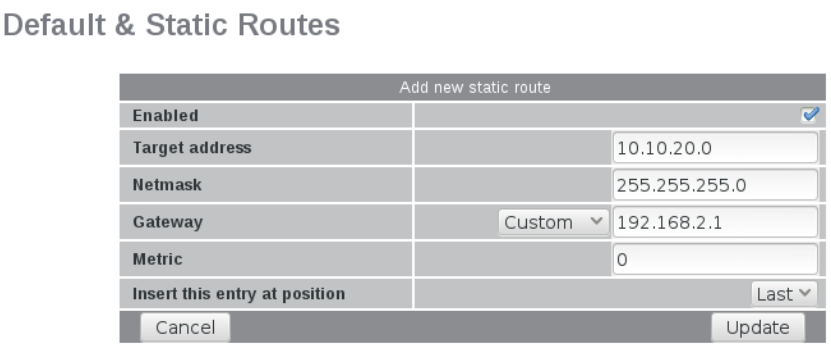


Figure 162: Adding a new static route

To save the new route click the Update button.

The main Default & Static Route page will again be shown with the new route listed, as shown in Figure 163.

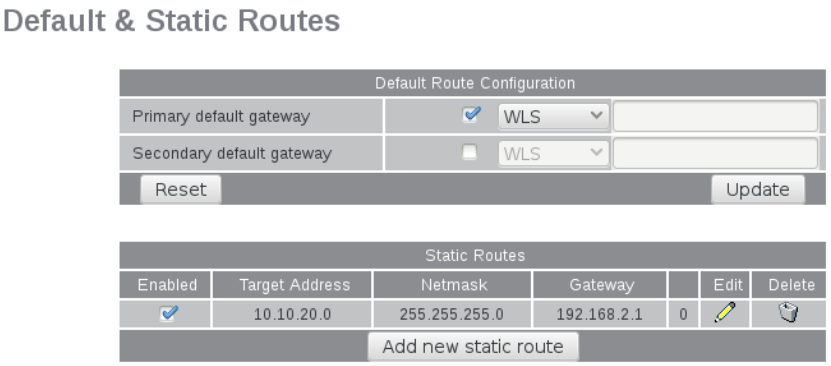


Figure 163: The static route page with a single route

To add a second route, again click the Add new static route button.

In the example shown in Figure 164, a route is created which all route all packets destined for the host 192.168.2.100 via the SSL VPN.

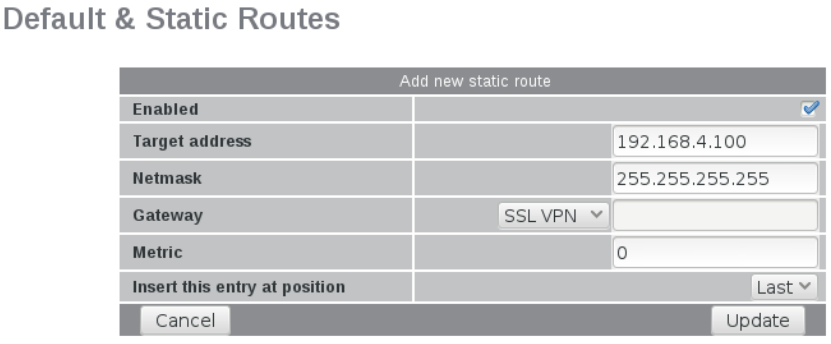


Figure 164: Adding a new static route

To add the route click the Update button.

The main page will again be shown with the new route added, as seen in Figure 165.

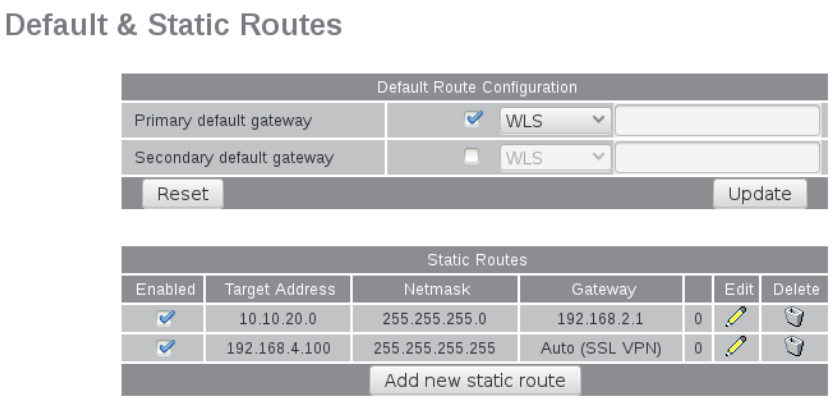


Figure 165: The static route table with two routes

For the route in this example to work a VPN will need to be configured and established. For details on configuring Virtual Private Networks (VPN) refer to Section 11 on page 162

9.1.5 Editing a static route

A static route can be edited by clicking the icon in the **Edit** column of the route to be changed. Once clicked, the details of the route will display in the same table as shown when adding a new route.

As an example, to edit the second route, click the icon in the second row of the table. A page similar to the Add new route page will be displayed, but now showing the details of route 2. Changes to route to the host 192.168.2.200 are shown in Figure 166.

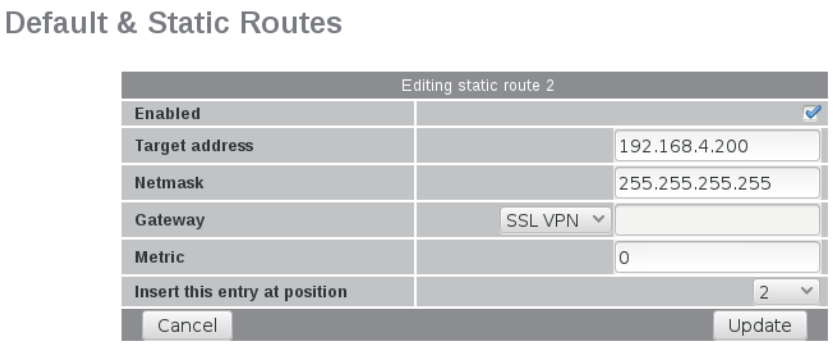


Figure 166: Editing a static route

To save the changes click the Update button or to lose any changes click the Cancel button.

The main page will again be displayed as shown in Figure 167, with the changes for route 2 added to the table.

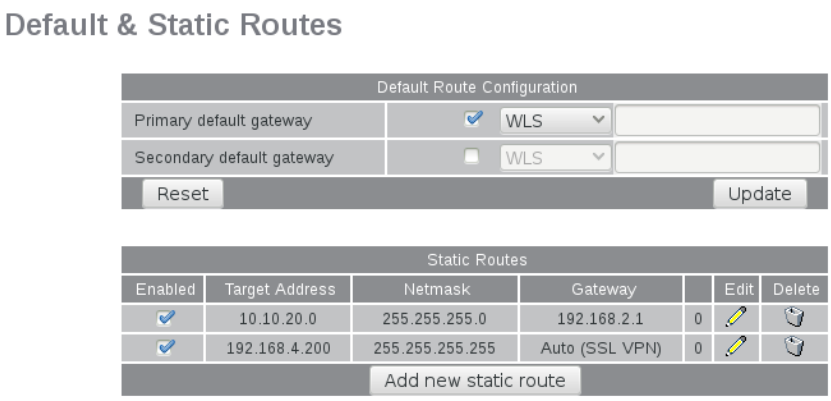


Figure 167: The main route table after editing route two

9.1.6 Deleting a static route

A static route can be deleted by clicking the icon in the **Delete** column of the route to be deleted. A warning box will be displayed. Click the OK button to confirm the deletion or click the Cancel button to prevent the route from being deleted.

For example, to delete route two from the table shown in Figure 167, click the icon in row two of the table. A warning box will now be displayed, as shown if Figure 168. Click the OK button to confirm the deletion of the route.

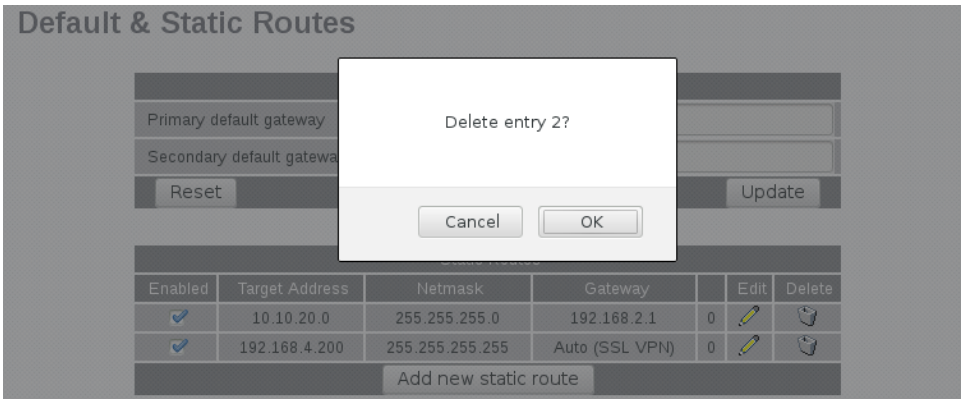


Figure 168: Deleting a static route

The route table will be displayed with the route removed, as shown in Figure 169.

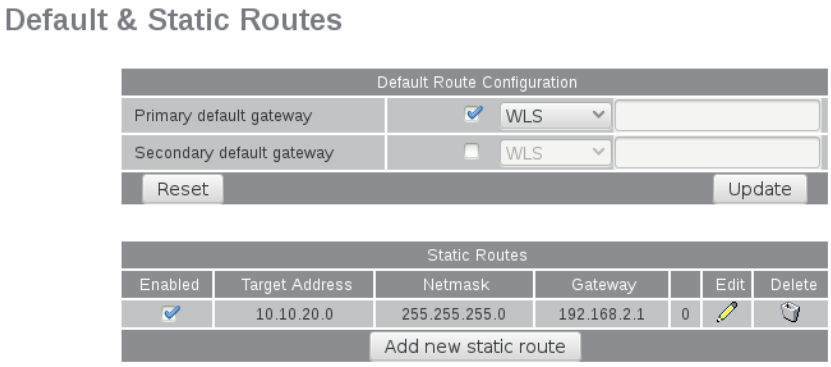


Figure 169: Static route table with route 2 removed

9.2 Dynamic Routing

9.2.1 Routing Information Protocol (RIP)

The Routing Information Protocol (RIP) is a protocol for exchanging routing information with neighbouring routers. RIP is a dynamic routing protocol used in local and wide area networks and is supported in many routers. To access the dynamic routing page, select Routing ▷ Dynamic a page similar to that shown in Figure 170 will be displayed.

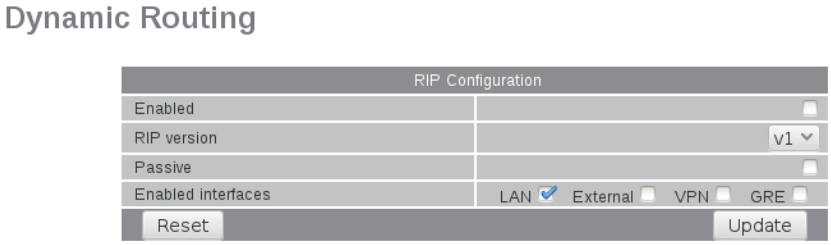


Figure 170: Dynamic routing

9.2.2 Enabling RIP

The RIP function is enabled in the **RIP Configuration** table. The description below explains the fields:

Enabled When set, the dynamic routing function will be enabled.

RIP Version This field determines the protocol version of RIP to be used. Select the version to match that used by neighbouring routers.

Passive When set, packets received on the LAN interface will not be actively broadcast.

Enabled interfaces Select the interfaces for which RIP will be enabled. More then one interface may be selected.

Click the Update button to save and commit the changes.

9.3 Virtual Router Redundancy Protocol (VRRP)

9.3.1 Description

The Virtual Router Redundancy Protocol (VRRP) is designed to increase the availability of the default gateway servicing hosts on a subnet. VRRP is a standardised protocol defined in RFC 3768. Vendors such as Cisco include implementations in their router products.

VRRP achieves redundancy by creating a “virtual gateway”. At any time, only one of the VRRP-enabled routers functions as the virtual gateway. The virtual gateway address is configured into hosts on the local network as their default gateway. VRRP routers take part in elections to decide who will become the master router. The master router then assumes the IP address of the virtual gateway and becomes the path for network traffic.

Figure 171 shows a two modem set-up using VRRP. Router A and Router B communicate via multicast messages to determine who will be the master router. As Router A has higher priority it will become the master in preference to Router B. Should Router B detect that Router A is no longer functioning, it will assume the role of the master router. Once Router A returns, it becomes the master again.

The time for Router B to detect that Router A has failed is determined by the advertising interval. The advertising interval determines how frequently the master router notifies other routers of its state. If Router B is not notified of the status of Router A for more than 3 times the advertising interval, Router B will assume the failure of Router A and become the master. The advertising interval can be set to a low value (as short as 1 second), however, the lower the value, the greater the volume of broadcast traffic on the local network.

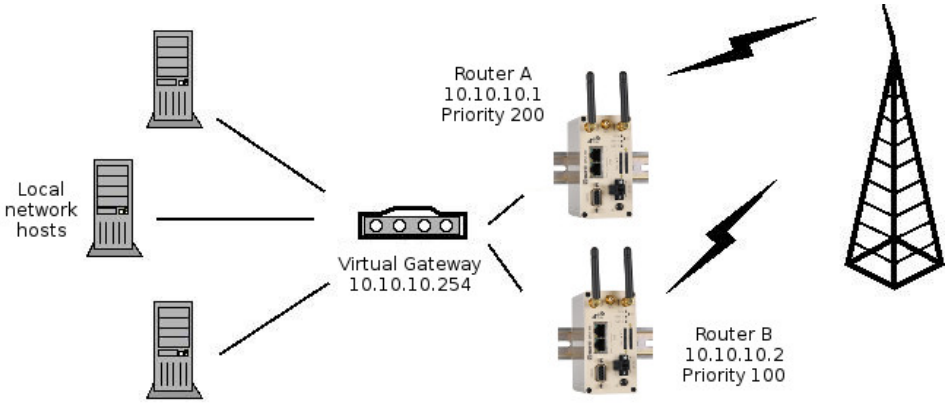


Figure 171: VRRP network scenario

To access the VRRP configuration, select Routing ▷ VRRP a page similar to that shown in Figure172 will be displayed.

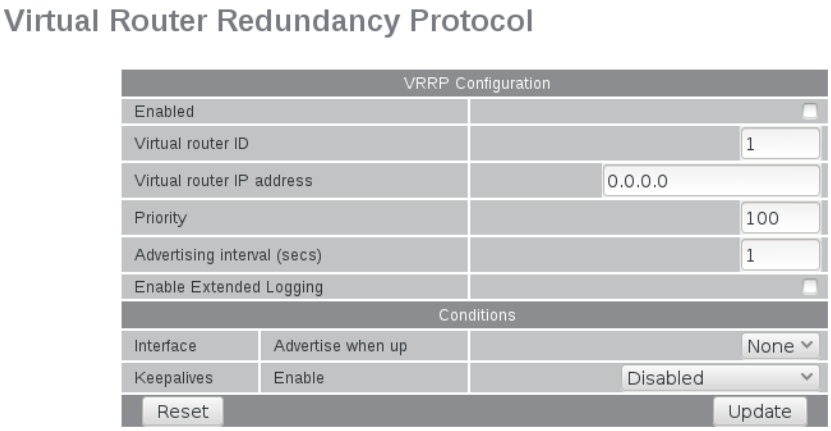


Figure 172: VRRP configuration

9.3.2 VRRP Configuration

The following fields need to be configured to enable VRRP:

VRRP Configuration Enabled When set, the VRRP function will be enabled.

Virtual router ID The virtual router ID (VRID) is common to all physical routers that are part of the same virtual router group. Set this field to match the ID used by the virtual group.

Virtual router IP address This is the IP address of the virtual gateway. It is common to all physical routers in the same virtual router group.

Priority This field determines how highly this router will rank in elections for a new master. A router with a higher priority will be chosen in preference to a router with lower priority. The valid range of priorities is 1 to 254.

Advertising interval (secs) This field determines the frequency with which the router will multicast its status to other router while it is the master. The value entered is in seconds.

Enable Extended Logging Check to enable verbose logging. Normally only used for debugging and system set up.

Conditions **Interface-Advertise when up** When an interface is selected the VRRP function will be disabled until the interface is connected and available. This prevents the unit from becoming the master router when no onward connection is available.

Keepalives-Enable Keep-alives are used to ensure the gateway service is available. Keep-alives can be enabled by selecting Poll at fixed interval. When selected (refer to Figure173) the following configuration options will appear:

Poll Period (secs) The polling period in seconds.

Retry Period (secs) Check box to enable re-tries if initial poll fails, the text box is for the re-try time in seconds.

Maximum failed polls The maximum number of failed polls.

Estimated detection (secs) The estimated minimum and maximum time for a failure to the detected.

Poll The poll type either ICMP (Ping) or TCP Socket and the remote address to poll.

Click the Update button to save and commit the changes.

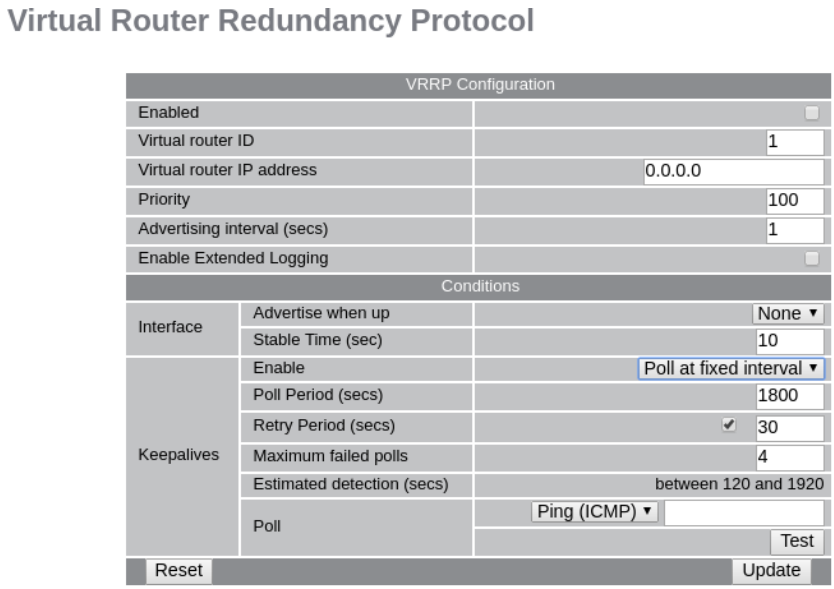


Figure 173: VRRP configuration with polling options shown.

Once enabled, VRRP will change the MAC address of the LAN interface. This may make the internal web server temporarily unavailable until the change in address has propagated.

9.3.3 VRRP Configuration Example

This example will describe the VRRP configuration for the two modems described in the network diagram of Figure 171 on the previous page. As the two devices are in the virtual router group the majority of the settings are the same. The exception is the priority which must be higher for Router A as it is to be the master. The settings for each device is listed below and shown in Figure 174 for Router A and Figure 175 for router B.

VRRP Configuration **Enabled** Checked to enable.

Virtual router ID Set to 1 (the default).

Virtual router IP address Set to the IP address 10.10.10.254

Priority Router A set to 200 and Router B set to 100 (the default).

Advertising interval Set to 1 second (the default).

Enable Extended Logging Disabled (not checked) for both devices.

Conditions **Interface-Advertise when up** Set to the wireless interface WLS

Keepalives-Enable Poll at fixed interval

Poll Period (secs) 1800

Retry Period (secs) Check to enable re-tries and set the retry time for 30 seconds

Maximum failed polls Set maximum number of poll failures to 4

Estimated detection (secs) Calculated

Poll Set poll type either Ping (ICMP) and the remote address to poll as 192.168.0.2.

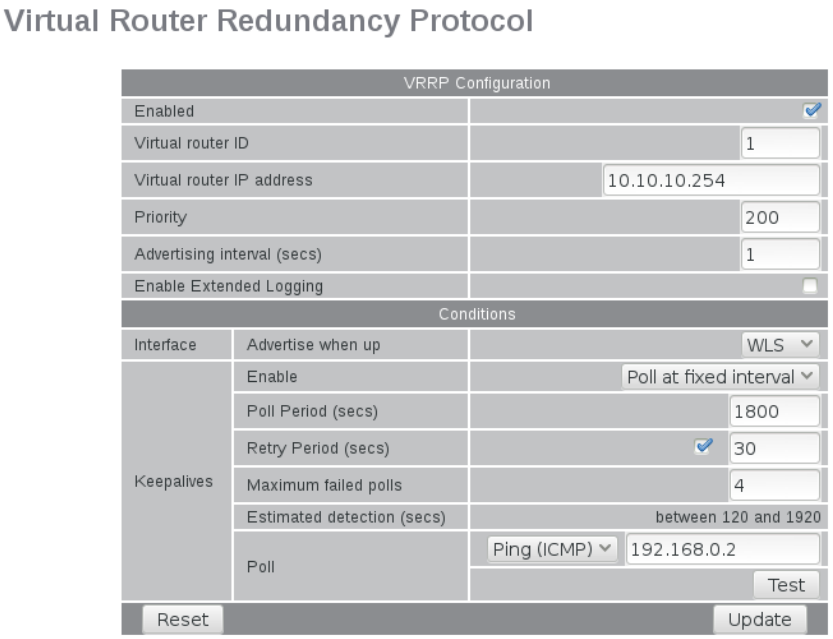


Figure 174: VRRP configuration for Router A

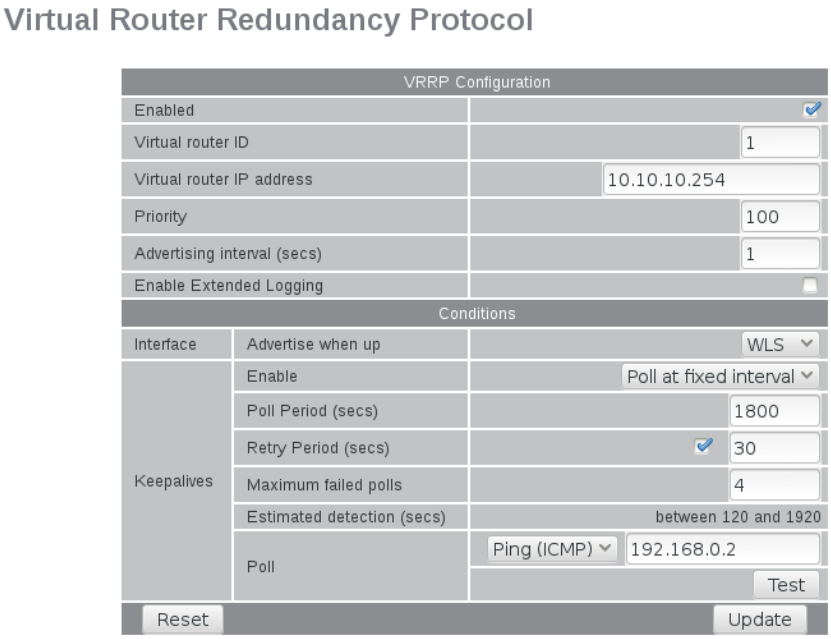


Figure 175: VRRP configuration for Router B.

9.4 Policy Routing

9.4.1 Description

Policy routing is an advanced routing feature that allows packets to be routed based on which of the modem's network interfaces they arrive on, the protocol type or the source or destination address. Conceptually a policy route is similar to a static route, but, as a policy route can match on more attributes than a packet's destination address, they allow for greater flexibility.

To access the policy route configuration, select Routing ▷ Policy a page similar to that shown in Figure 176will be displayed.

Figure 176: Policy route options

9.4.2 Policy route options

The policy route options are shown when the **Add new policy route** button is pressed or an existing route is edited. The policy route options will be displayed as shown in Figure 177.

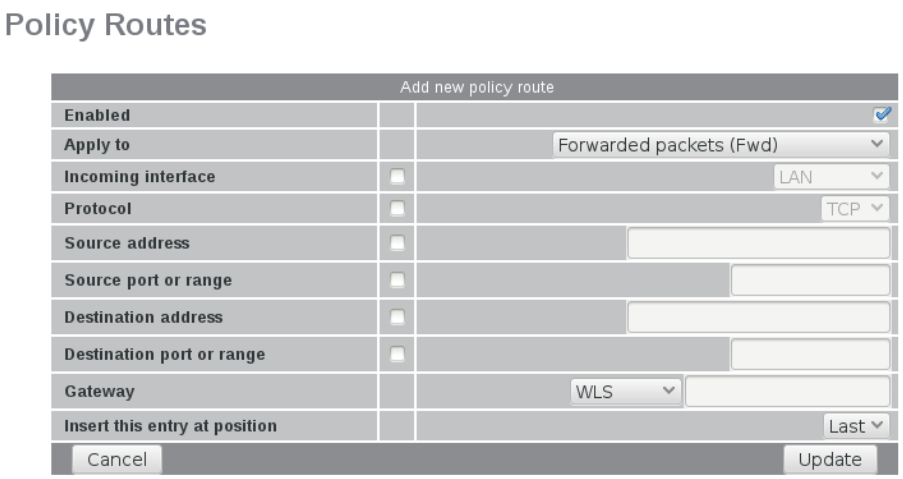


Figure 177: Policy route options

The following options can be set for each policy route:

Enabled Set the enabled check box to have the route installed. A route can be temporarily disabled by un-checking this box.

Apply to Policy routes can be applied at two separate points in the modem:

- **Forwarded packets.** The route will be applied to packets that are received from one network interface and then routed out another network interface.
- **Locally generated packets.** The route will be applied to packets generated by one of the modem's internal services.

Incoming interface If selected, packets will be matched based on the network interface they have been received on. Note that this can't be applied to **Locally generated packets** as they have been generated by the modem itself.

Protocol If selected, packets will be matched based on their protocol type. Note that if you wish to match on source or destination ports, the protocol must be set to **TCP** or **UDP**.

Source address If selected, either a single address (for example, 172.16.1.132) or a subnet range (for example, 172.16.0.0/24) can be entered. Only packets matching this source address will have the filter applied to them.

Source port or range If selected, packets will be matched based on their TCP or UDP source port. Either an individual port (for example, 443) or a range of ports (80-143) can be entered.

Destination address Similar to the **Source address**, but instead matching on the destination address.

Destination port or range Similar to the **Source port or range,** but instead matching on the destination port.

Gateway Determines the gateway that packets who meet all of the matching criteria for the route will be routed to. The gateway can be one of the following:

WLS Wireless interface.

SSL VPN The SSL VPN interface. This option is only valid if an SSL VPN has been configured. Refer to Section Virtual Private Network (VPN) for details.

WLS CSD The wireless circuit switched data interface. This option is only valid if the unit is operating in Circuit Switched Data (CSD) mode and the PPP server has been enabled.

Serial n The serial port, where n is the number of the port. This option is only valid if the serial port is configured to operate in one of the PPP modes.

Custom Use the IP address entered in the adjacent field.

Insert this entry at position Determines where this entry will be inserted in the list of policy routes.

9.4.3 Adding a new policy route

From the main Policy Route page click the Add new policy route button. This will select the Add new policy route page. An example of adding a new policy route is shown in Figure 178. In this example, a new route is to be created that routes all outgoing mail traffic (SMTP, TCP port 25) received from the LAN interface via the gateway at address 10.10.10.1.

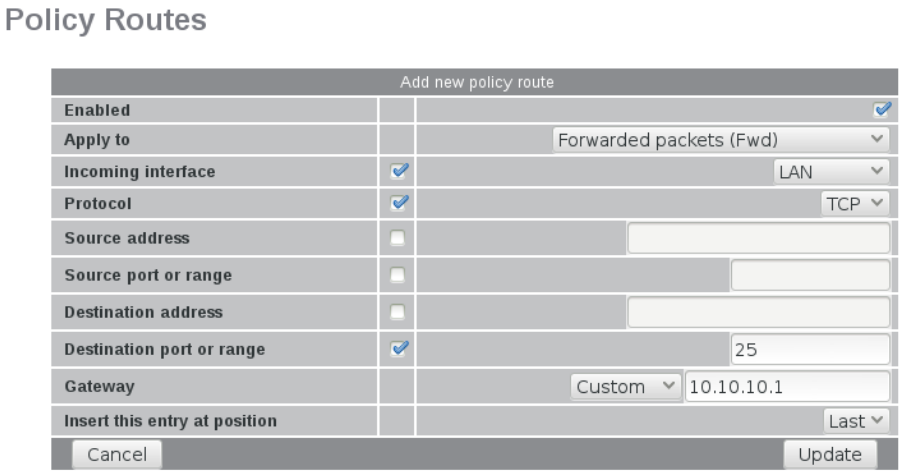


Figure 178: Adding a new policy route

It can be seen in the example that in the centre column, **Incoming interface**, **Protocol** and **Destination port or range** are checked. This indicates these are the matching criteria that will be applied to packets. All criteria that are unchecked will be ignored.

To save the new route click the Update button. The main Policy Route page will again be shown with the new route listed, as shown in Figure 179.

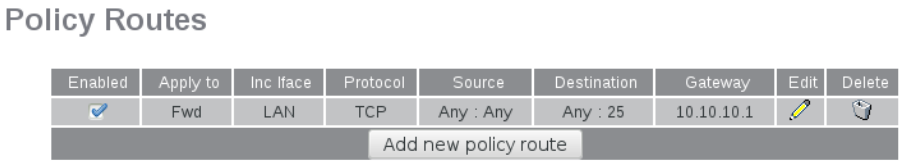


Figure 179: The policy route page with a single route

To add a second route, again click the Add new policy route button. In the example shown in Figure 180, a policy route is created which will route all packets received from the LAN interface, from IP address 10.10.10.50 via the SSL VPN. Again notice that in the centre column, **Incoming interface** and **Source address** are checked. This indicates these are the matching criteria that will be applied to packets. All criteria that are unchecked will be ignored.

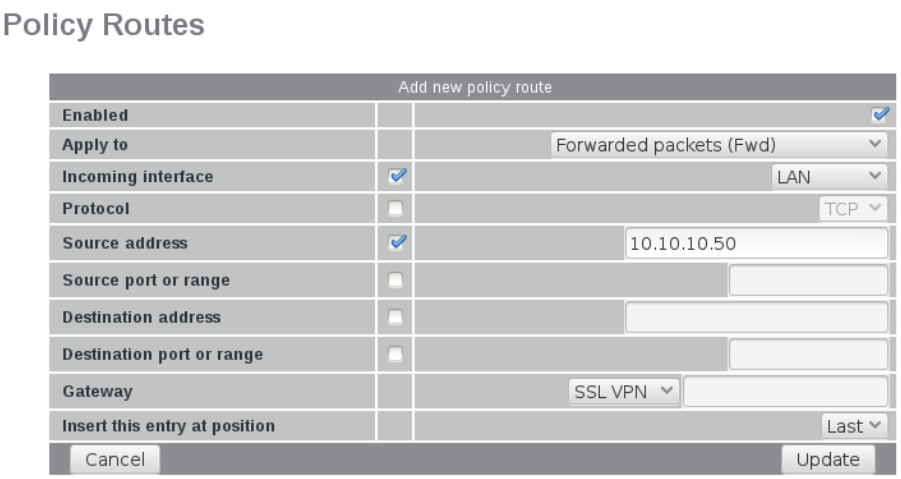


Figure 180: Adding a second policy route

To add the route click the Update button. The main page will again be shown with the new route added, as seen in Figure 181.

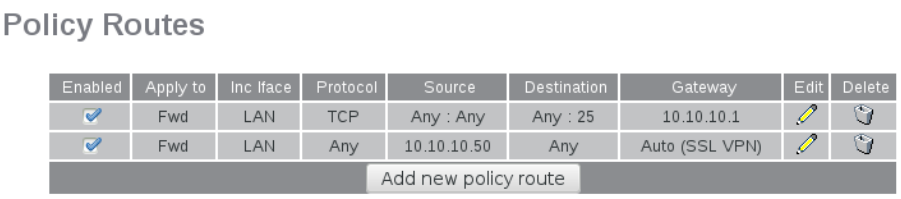


Figure 181: The policy route table with two routes

9.4.4 Editing a policy route

A policy route can be edited by clicking the icon in the **Edit** column of the route to be changed. Once clicked, the details of the route will display in the same table as shown when adding a new route.

As an example, to edit the second route, click the icon in the second row of the table. Changes that add destination address matching to the criteria are shown in Figure 182.

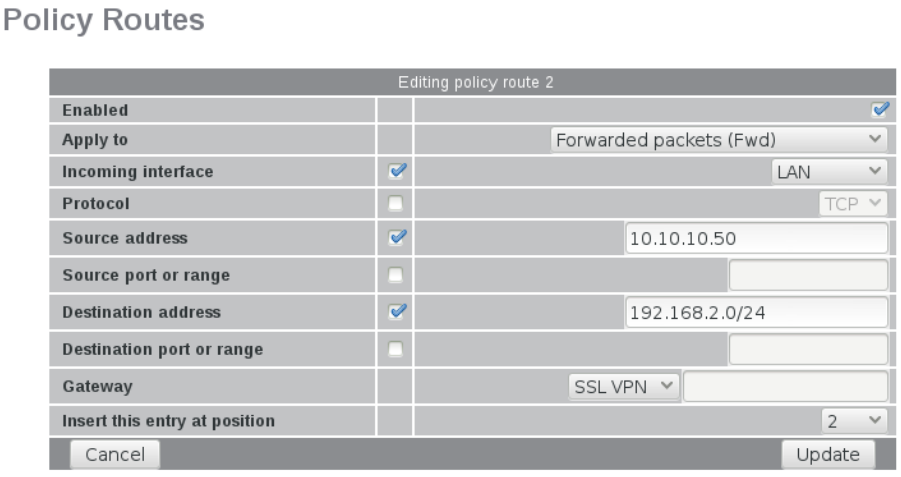


Figure 182: Editing a policy route

To save the changes click the Update button or to lose any changes click the Cancel button. The main page will again be displayed as shown in Figure 183, with the changes for route 2 added to the table.

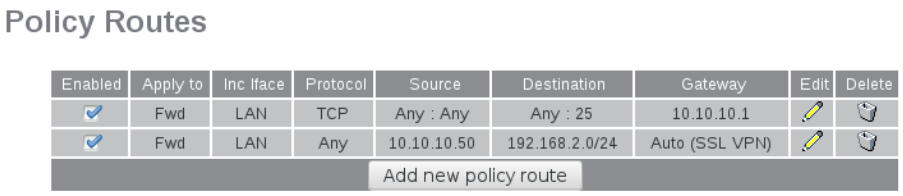


Figure 183: The main route table after editing route two

9.4.5 Deleting a policy route

A policy route can be deleted by clicking the icon in the **Delete** column of the route to be deleted. A warning box will be displayed. Click the OK button to confirm the deletion or click the Cancel button to prevent the route from being deleted.

For example, to delete route two from the table shown in Figure 183, click the icon in row two of the table. A warning box will now be displayed, as shown if Figure 184. Click the OK button.

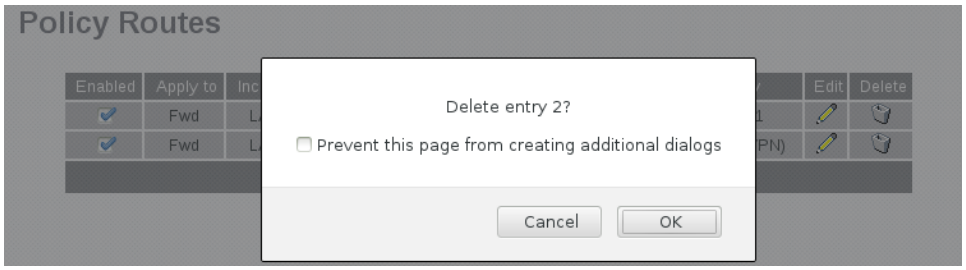


Figure 184: Deleting a policy route

The route table will be displayed with the route removed, as shown in Figure 185.

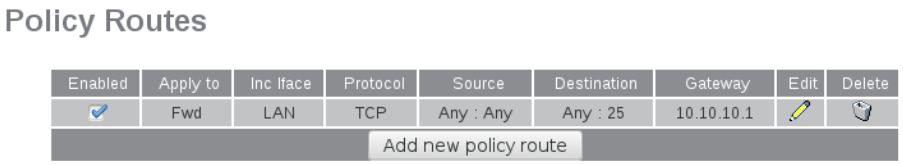


Figure 185: Policy route table with route two removed

9.5 Quality of Service Routing

9.5.1 Description

For bandwidth intensive applications, such as live video or Voice-over-IP (VOIP), it may be desirable to have certain types of traffic prioritised for transmission out the Wireless interface in preference to other traffic. For example, live video packets are more time critical than outgoing email and should be prioritised as such.

The QoS implementation works by dividing the outgoing queue to selected interface into three queue levels:

- High (minimum 60% of bandwidth)
- Standard (minimum 30% of bandwidth)

- Low (minimum 10% of bandwidth)

Where a queue is not using all of its available bandwidth, queues below will expand their bandwidth to ensure full link utilisation. For example, if there is currently no high priority traffic queued, standard traffic will be able to use up to 90% of the available bandwidth.

Configuring the QoS function is performed in two steps:

- Setting the basic options (enabling QoS and setting the available bandwidth)
- Configuring multiple rules to classify packets into the three different priority queues.

To access the QoS configuration, select Routing ▷ QoS a page similar to that shown in Figure 186 will be displayed.

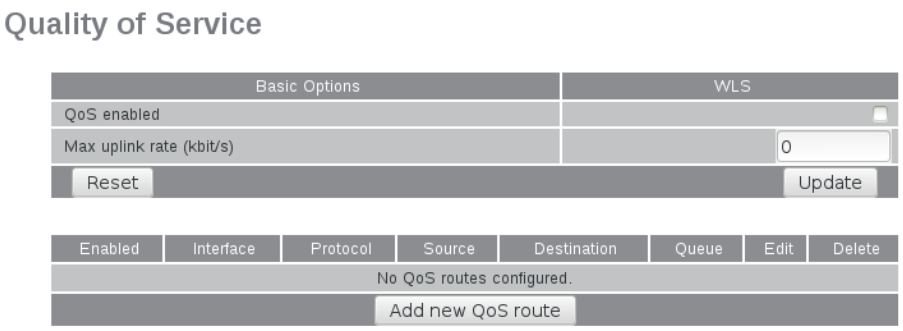


Figure 186: Quality of Service

9.5.2 Basic QoS options

To enable the QoS feature, the following fields must be set:

QoS enabled When set, QoS is activated for the indicated interface.

Max uplink rate Set this to the maximum bit rate attainable for the indicated interface. It is important that this value be correct, as it will be used to determine the bandwidth allocations for each priority level.

It may be necessary to test the interface to determine the maximum bandwidth. This value could vary between installations.

Ccick the Update button to save and commit the changes.

9.5.3 Basic QoS Configuration

As an example of how to complete the basic QoS configuration, assume the maximum uplink bandwidth is 350kbits/sec. QoS would then be set with the following values:

QoS enabled check to enable QoS

Max uplink rate Set to 350.

Figure 187 illustrates the settings for this example.

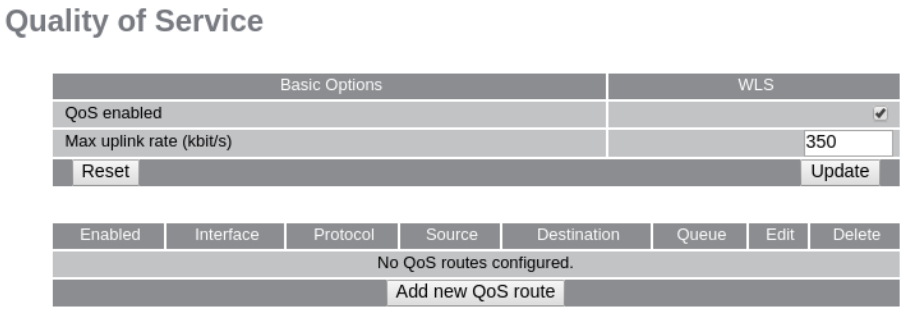


Figure 187: Quality of Service configuration with the uplink rate set.

9.5.4 QoS route options

The QoS route options are shown when the Add new QoS route button is clicked or an existing route is edited by clicking the icon in the **Edit** column of the route to be changed . The QoS route options will be displayed as shown in Figure 188.

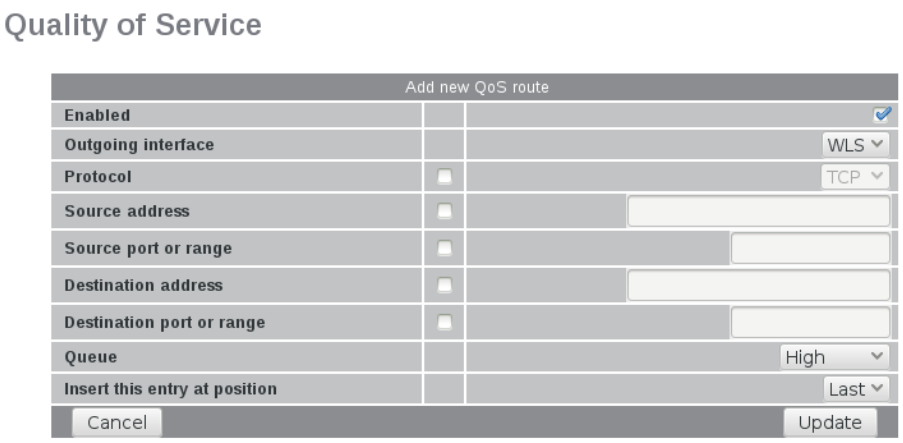


Figure 188: QoS route options

The following options can be set for each QoS route:

Enabled Set the enabled check box to have the route installed. A route can be temporarily disabled by un-checking this box.

Protocol If selected, packets will be matched based on their protocol type. Note that if you wish to match on source or destination ports, the protocol must be set to **TCP** or **UDP**.

Source address If selected, either a single address (for example, 172.16.1.132) or a subnet range (for example, 172.16.0.0/24) can be entered. Only packets matching this source address will have the route applied to them.

Source port or range If selected, packets will be matched based on their TCP or UDP source port. Either an individual port (for example, 443) or a range of ports (80-143) can be entered.

Destination address Similar to the **Source address**, but instead matching on the destination address.

Destination port or range Similar to the **Source port or range,** but instead matching on the destination port.

Queue Sets the priority queue that packets who meet all of the matching criteria for the route will be assigned to.

Insert this entry at position Determines where this entry will be inserted in the list of QoS routes.

9.5.5 Adding a new QoS route

From the main QoS Route page click the Add new QoS route button. This will select the Add new QoS route page. An example of adding a new QoS route is shown in Figure 189. In this example, a new route is to be created that classifies all traffic from the host 10.10.10.95 with TCP source port 80 to the high priority queue.

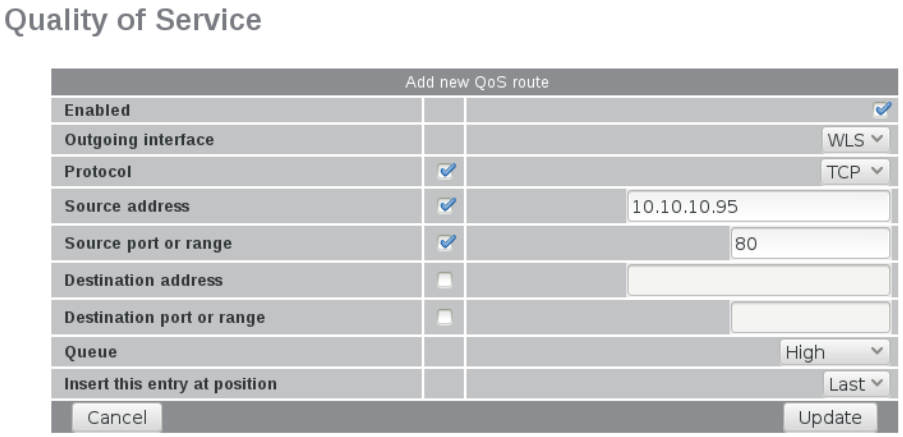


Figure 189: Adding a new QoS route

It can be seen in the example that in the centre column **Protocol** and **Source address** and **Source port or range** are checked. This indicates these are the matching criteria that will be applied to packets. All criteria that are unchecked will be ignored.

To save the new route click the Update button. The main QoS Route page will again be shown with the new route listed, as shown in Figure 190.

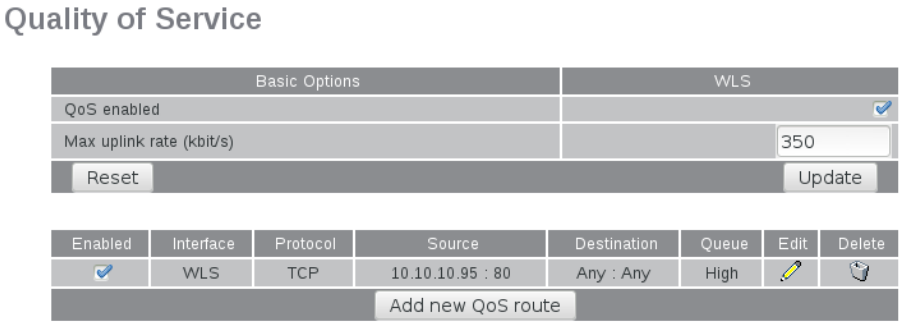


Figure 190: The QoS route page with a single route

To add a second QoS route, again click the Add new QoS route button. In the example shown in Figure 191, a QoS route is created which will classify all packets destined for an SMTP email server (TCP port 25) to the low priority queue. Again notice that in the centre column, **Protocol**, **Destination address** and **Destination port or range** are checked. This indicates these are the matching criteria that will be applied to packets. All criteria that are unchecked will be ignored.

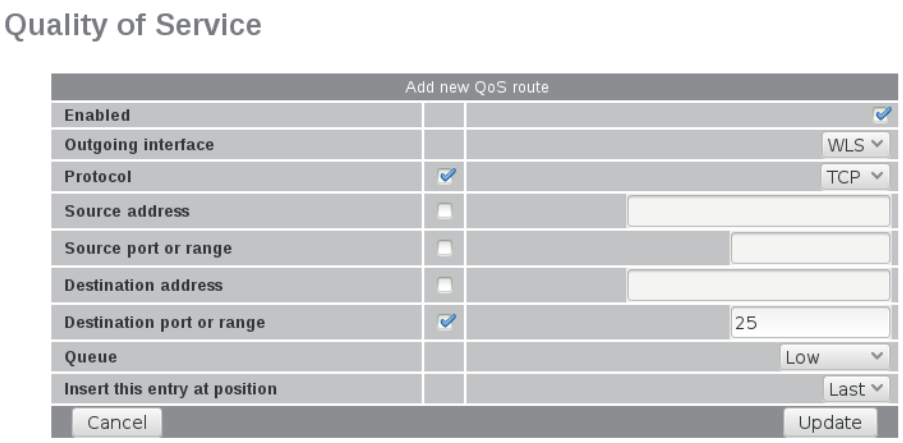


Figure 191: Adding a new QoS route

To add the route click the Update button. The main page will again be shown with the new route added, as seen in Figure 192.

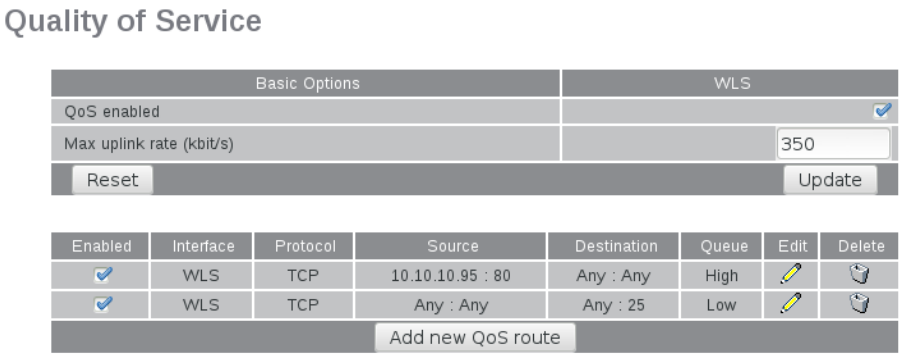


Figure 192: The QoS route table with two routes

9.5.6 Editing a QoS route

A QoS route can be edited by clicking the icon in the **Edit** column of the route to be changed. Once clicked, the details of the route will display in the same table as shown when adding a new route.

As an example, to edit the second route, click the icon in the second row of the table. A page similar to the Add new route page will be displayed, but now showing the details of route 2. Changes that add destination address matching to the criteria are shown in Figure 193.

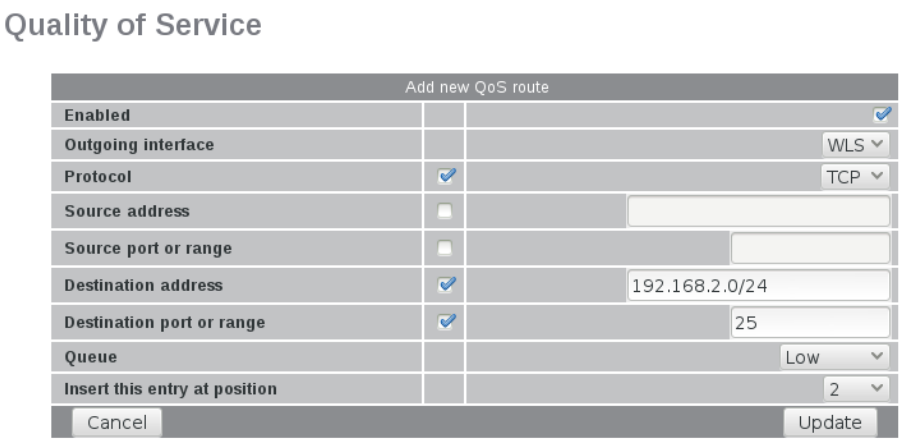


Figure 193: Editing a QoS route

To save the changes click the Update button or to lose any changes click the Cancel button. The main page will again be displayed as shown in Figure 194, with the changes for route 2 added to the table.

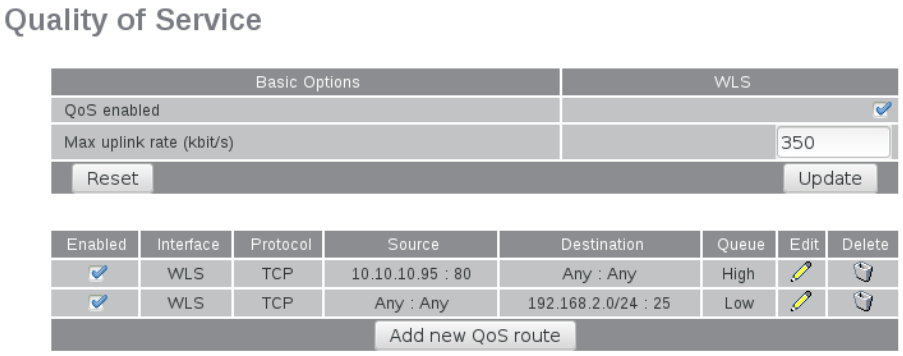


Figure 194: The main route table after editing route two

9.5.7 Deleting a QoS route

A QoS route can be deleted by clicking the icon in the **Delete** column of the route to be deleted. A warning box will be displayed. Click the OK button to confirm the deletion or click the Cancel button to prevent the route from being deleted.

For example, to delete route two from the table shown in Figure 194, click the icon in row two of the table. A warning box will now be displayed, as shown if Figure 195. Click the OK button to confirm.

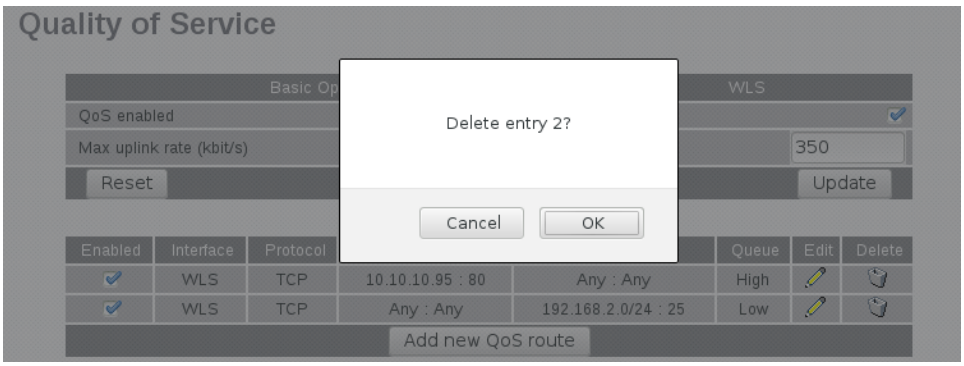


Figure 195: Deleting a QoS route

The route table will be displayed with the route removed, as shown in Figure 196.

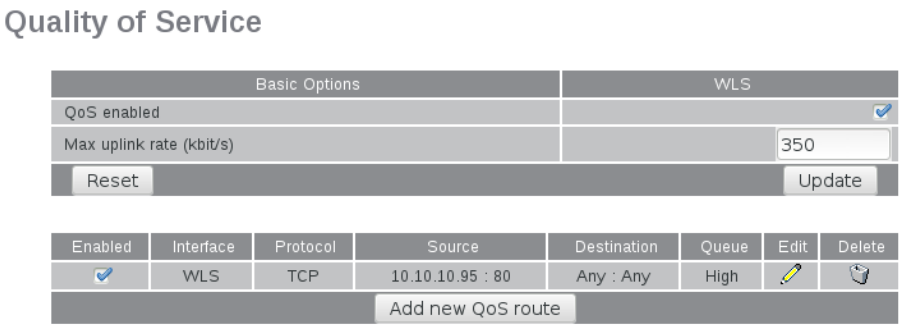


Figure 196: QoS route table with route two removed

10 Firewall

The Stateful Packet Inspection (SPI) Firewall controls the connections from the wireless port to the LAN ports and to the modem itself. The firewall can be used to limit the connections that can be established to or via router. For example, if the router is only to be used for serial communications then the firewall can be set-up to only allow connections through to the serial server (which connects to the serial ports).

The firewall configuration is accessed by selecting the **Firewall** tab from the main menu. When selected the page shown in Figure 197 will be displayed.

Figure 197: Main Firewall page

10.1 Firewall Setup

The firewall configuration is accessed by selecting the Firewall ▹ Setup from the menu. When selected the page will provide the basic configuration details for the firewall as shown in Figure 198.

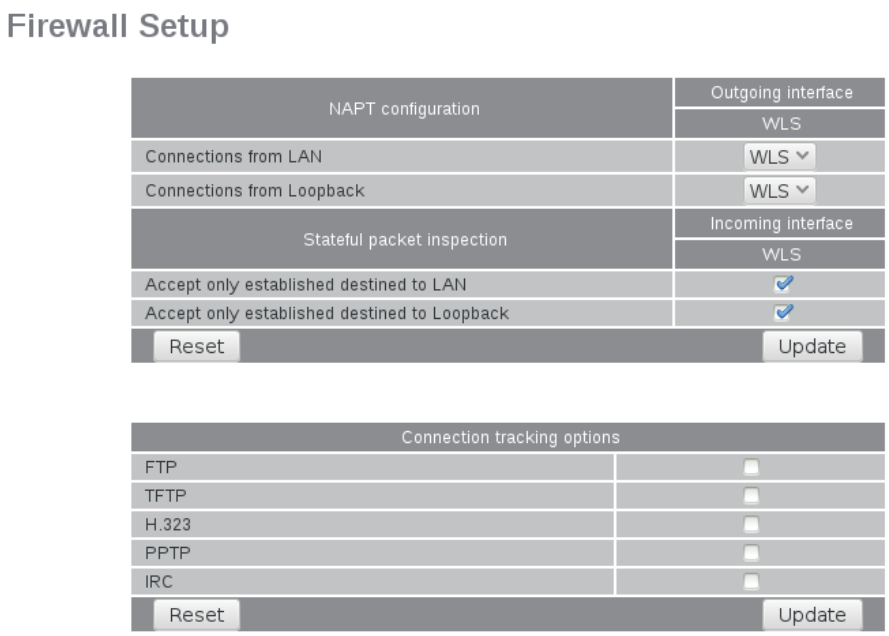


Figure 198: Basic firewall configuration

10.1.1 Network Address and Port Translation (NAPT)

As connection pass from the LAN or Loopback interface and out the WAN (wireless or ADSL) port, the firewall can perform Network Address and Port Translation (NAPT). When set, this option will cause the firewall to substitute the address of the WAN port for the source address of connections received from the LAN or Loopback interface. This is most useful where the LAN or Loopback is a private network and the WAN port has a public address.

In some cases, for example, if connected to an IP WAN that supports direct routing to the LAN network, it may be desirable to disable the NAPT function. This will allow clients on the LAN to be directly addressed without the need for port forwards.

To disable NAPT, un-check the **Connections from LAN** and/or **Connections from Loopback** check-boxes and click the Update button to save and commit the changes.

10.1.2 Stateful Packet Inspection (SPI)

The firewall can function in Stateful Packet Inspection (SPI) mode. When enabled, the firewall will track the state of each connection passing through it (for example, TCP streams) and only allow packets belonging to a known connection to enter from the WAN port. In most cases, SPI should be enabled for greater security. When disabled, the firewall will allow all incoming packets from the WAN port to be forwarded through.

In some cases, for example, if connected to an IP WAN that supports direct routing to the LAN network, it may be desirable to disable the SPI function. This will allow clients on the LAN to be directly addressed without the need for port forwards.

To disable Stateful Packet Inspection (SPI), un-check the **Accept only established destined to LAN** and/or **Accept only established destined to Loopback** check-boxes and click the Update button to save and commit the changes.

10.1.3 Connection tracking options

The firewall can be configured to provide connection tracking and NAT support for a number of additional protocols. The protocols are listed in table 2. To enable support for a protocol, click the check-box for the protocol and click the Update button to save and commit the changes.

Protocol	Description
FTP	Adds support for active mode File Transfer Protocol
TFTP	Adds support for the Trivial File Transfer Protocol
H.323	Adds support for the H.323 voice and video-conferencing protocol
PPTP	Adds support for the Point-to-point Tunnelling Protocol
IRC	Adds support for the Internet Relay Chat protocol

Table 2: Firewall Connection tracking options

10.2 Access Control

10.2.1 Description

The Access Control page allows configuration of the firewall to allow or deny access to internal services of the modem from the wireless port and VPN tunnels. By default, the firewall will block access from the wireless port to all internal services such as the web server, and allow access to all internal services from the VPN tunnels. In certain situations it may be desired to enable access to some services from the wireless port or to disable access to some services from the VPN tunnels, by changing the settings on this page.

The port numbers for internal services are the standard port numbers for the service type, for example, port 80 is used for the web server. It is possible to change the port number for a particular service. This may be a requirement if a conflict exists with a particular port or service.

To access the Access Controls, select the Firewall ▷ Access Control from the menu. When selected the page will show the access control details for the firewall as shown in Figure 199.

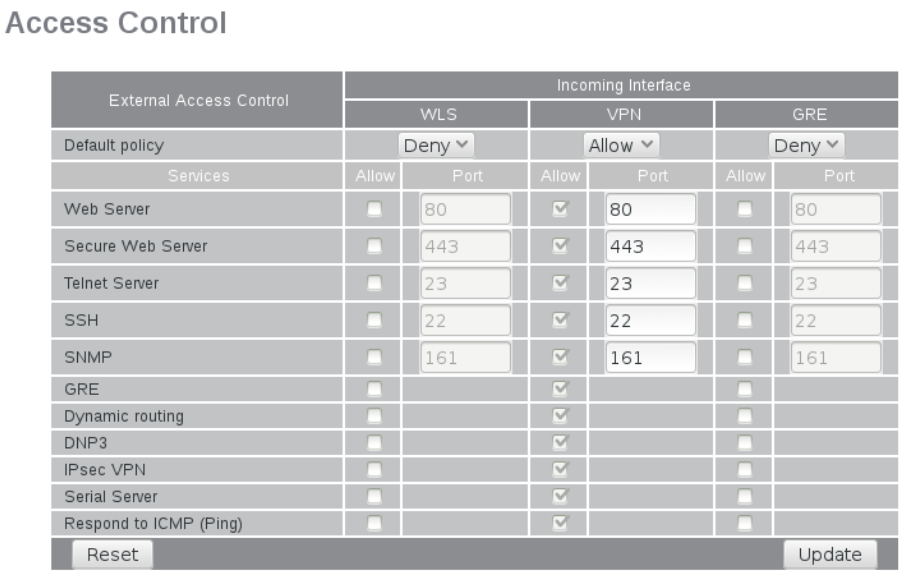


Figure 199: Firewall access control options

10.2.2 Accessing modem services from the WAN port or VPN tunnels

The External Access table provides controls for which services can be accessed from the WAN (Wireless and ADSL) interface and VPN tunnels. By default, the modem will block all requests received on the WAN interface and allow all requests received from VPN tunnels.

There are several modes for determining which services can be accessed:

No access All incoming requests are dropped. Set the **Default policy** set to **Deny** and check no boxes in the **Allow** column.

Restricted access Incoming requests for particular services will be allowed. Set the **Default policy** to **Deny** and check the boxes for the desired services in the **Allow** column.

Full access All incoming requests allowed. Set the **Default policy** to **Allow**.

To change the port number for a service, change the entry in the **Port** column for the given service. For example, to change the web server to port 8080 on the wireless port, enter 8080 in the WLS column on the Web Server row.

It is recommended to only enable services which are required for normal operation of the unit. If a service is required for configuration or testing only allow access when required then remove the access. This serves to improve security and avoid possible additional connections and resulting increase in data.

Click the Update button to save and commit changes or click the Reset button to clear the changes.

10.3 DoS Filters

10.3.1 Description

A denial of service attack (DoS attack) is an attempt to render a network device unavailable to intended users. The most common method of attack involves saturating the target device with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. The intention of DOS attacks is to cause the targeted device to reset or consume resources to such a level that it is unable to provide the intended service. A consequence of such an attack is that even if the device is able to handle the large number of communications requests, the bandwidth over the communications channel used for the attack may be completely consumed, potentially preventing legitimate connections to the targeted device.

The firewall has filters that can detect and drop packets that may be part of a Denial of Service (DOS) attack, for example, TCP packets with invalid header information. Options to enable and disable these filters can be found on DoS Filters page.

10.3.2 Enabling the Denial of Service filters

The Filter Description table provides a number of DOS filters, as shown in Figure 200. The filters can be applied to packets received from the LAN port, the wireless port (WLS), and from any VPN tunnel by checking the boxes in the appropriate column.

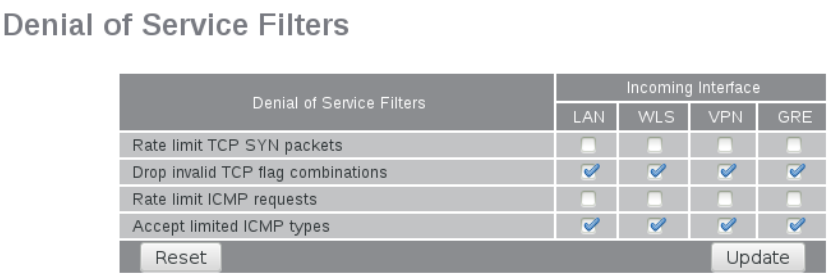


Figure 200: Firewall DoS filter options

The function of each filter is described below:

Rate limit TCP SYN packets This will limit the number of new TCP connection requests (SYN packets) allowed from the given interface. The rate will be limited to 5 per second.

Drop invalid TCP flag combinations Some DOS attacks will send packets that present an invalid combination of TCP flags which may cause problems for some operating systems. The filter will packets with invalid combinations received on the given interface.

Rate limit ICMP requests This will limit the number of ICMP requests (for example, ping requests) allowed from the given interface. The rate will be limited to 5 per second.

Accept limited ICMP types The types of ICMP packets that are accepted will be limited to types 0, 3, 8 and 11.

Click the Update button to save and commit changes or click the Reset button to clear the changes.

It is important to note that although the firewall will drop the packets as described the packets are still received over the WAN interface. This means that the WAN interface still may become saturated due to the number of packets received and there will possibly be excessive data charges. If an excessive number of packets are received the issue may need to be raised with the provider.

10.4 Custom Filters

10.4.1 Description

Custom Filters allow new rules to be added to the firewall to allow or deny specific packets. Packets can be matched based on which of the modem's network interfaces they arrive on or will leave on, the protocol, the source or destination address.

Some example custom filters are:

- A filter than only allows traffic from a particular host on the WAN to access through to the LAN ports.
- A filter that drops all traffic from a particular host on the WAN.

To select the Custom Filters page select Firewall ▷ Custom Filters, page similar to that shown in Figure 201 will be displayed.

Figure 201: Custom Filter main page with no filters configured

10.4.2 Custom filter options

To add a new custom filter click the Add new custom filter button, the custom filter options will be displayed as shown in Figure 202. The same options page is displayed when a custom filter is edited by clicking the icon in the **Edit** column of the filter to be edited.

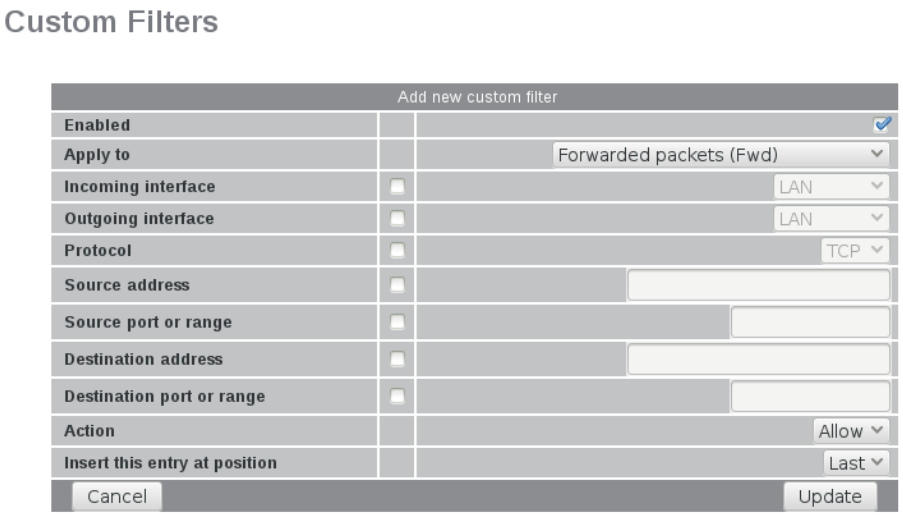


Figure 202: Adding a new custom filter

The following options can be set for each custom filter:

Enabled Set the enabled check box to have the rule installed in the firewall. A rule can be temporarily disabled by un-checking this box.

Apply to Custom filters can be applied at three separate points in the modem:

Forwarded packets. The filter will be applied to packets that are received from one network interface and then routed out another network interface.

Locally destined packets. The filter will be applied to packets destined for the modem's internal services.

Locally generated packets. The filter will be applied to packets generated by one of the modem's internal services.

Incoming interface If selected, packets will be matched based on the network interface they have been received on. Note that this can't be applied to **Locally generated packets** as they have been generated by the modem itself.

Outgoing interface If selected, packets will be matched based on the network interface they will be transmitted on. Note that this can't be applied to **Locally destined packets** as they will be received by the modem itself.

Protocol If selected, packets will be matched based on their protocol type. Note that if you wish to match on source or destination ports, the protocol must be set to **TCP** or **UDP**.

Source address If selected, either a single address (for example, 172.16.1.132) or a subnet range (for example, 172.16.0.0/24) can be entered. Only packets matching this source address will have the filter applied to them.

Source port or range If selected, packets will be matched based on their TCP or UDP source port. Either an individual port (for example, 443) or a range of ports (80-143) can be entered.

Destination address Similar to the **Source address**, but instead matching on the destination address.

Destination port or range Similar to the **Source port or range,** but instead matching on the destination port.

Action Determines what action on packets who meet all of the matching criteria for the filter. Options:

Deny The packet will be dropped.

Allow The packet will be passed.

Insert this entry at position Determines where this entry will be inserted in the list of custom filters.

Click the Update button to save and commit changes or click the Cancel button to cancel the addition or edit.

10.4.3 Adding a new custom filter

From the main Custom Filters page click the **Add new custom filter** button. This will select the Add new custom filter page. An example of adding a new custom filter is shown in Figure 203. In this example, a new filter is to be created to allow packets received via the wireless port, from IP address 112.112.112.112 and destined to the LAN network.

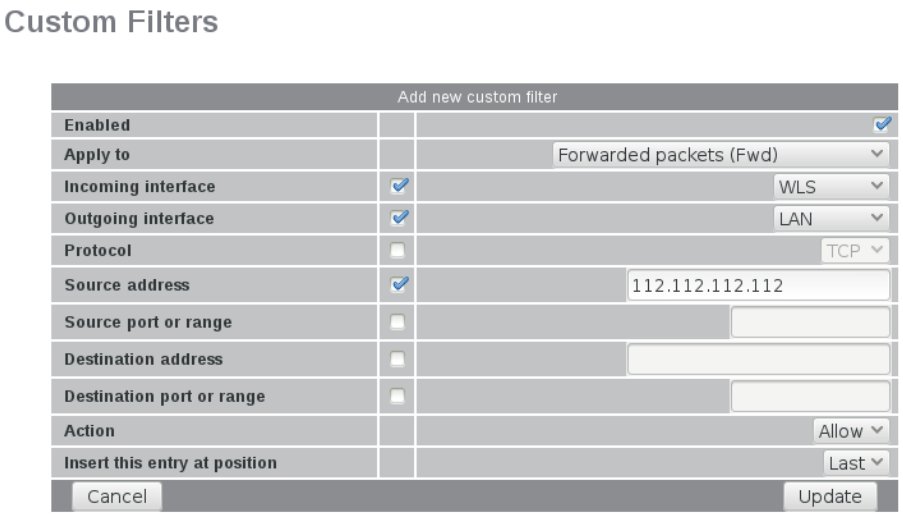


Figure 203: Adding a new custom filter

It can be seen in the example that in the centre column, **Incoming interface**, **Outgoing interface** and **Source address** are checked. This indicates these are the matching criteria that will be applied to packets. All criteria that are unchecked will be ignored.

To save the new filter click the Update button. The main Custom Filter page will again be shown with the new filter listed, as shown in Figure 204.

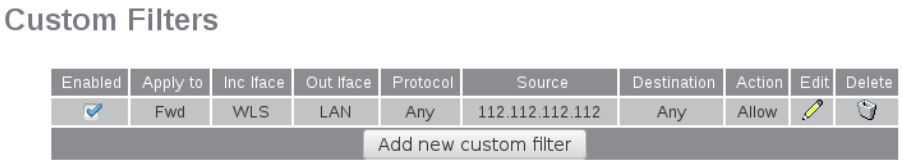


Figure 204: The custom filter page with a single filter

To add a second filter again click the **Add new custom filter** button. In the example shown in Figure 205, a custom filter is created which will deny packets received from the LAN port, from IP address 211.211.211.211 and destined to the wireless network. Again notice that in the centre column, **Incoming interface**, **Outgoing interface** and **Source address** are checked. This indicates these are the matching criteria that will be applied to packets. All criteria that are unchecked will be ignored.

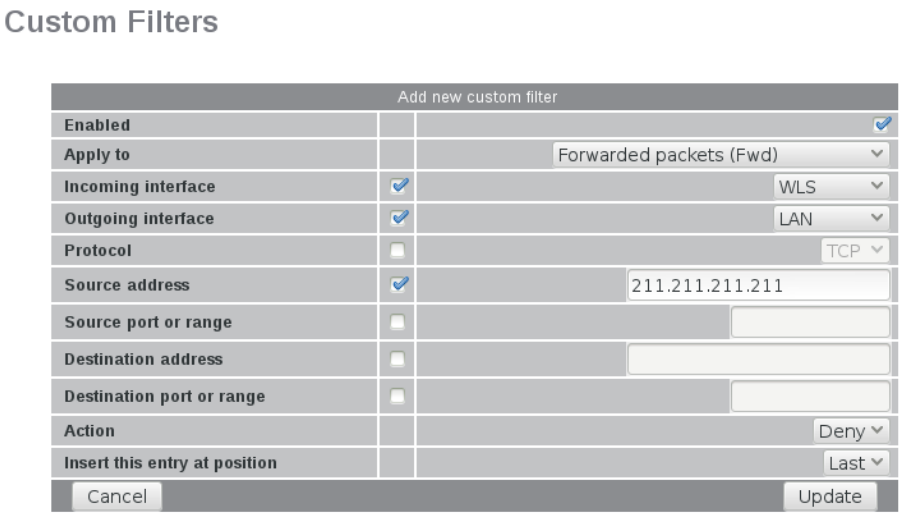


Figure 205: Adding a new custom filter

To add the filter to the filters table click the Update button, the main page will again be shown with the new filter added, as seen in Figure 206.

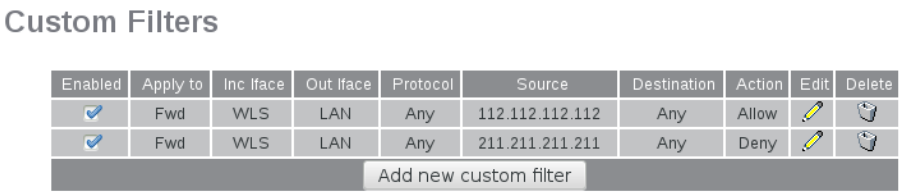


Figure 206: The custom filter table with 2 filters

10.4.4 Editing a custom filter

A custom filter can be edited by clicking the icon in the **Edit** column of the filter to be changed. Once clicked, the details of the filter will display in the same table as shown when adding a new filter.

As an example, to edit the second filter, click the icon in the second row of the table. A page similar to the Add new filter page will be displayed, but now showing the details of filter 2. Changes that add protocol and port number matching to the criteria are shown in Figure 207.

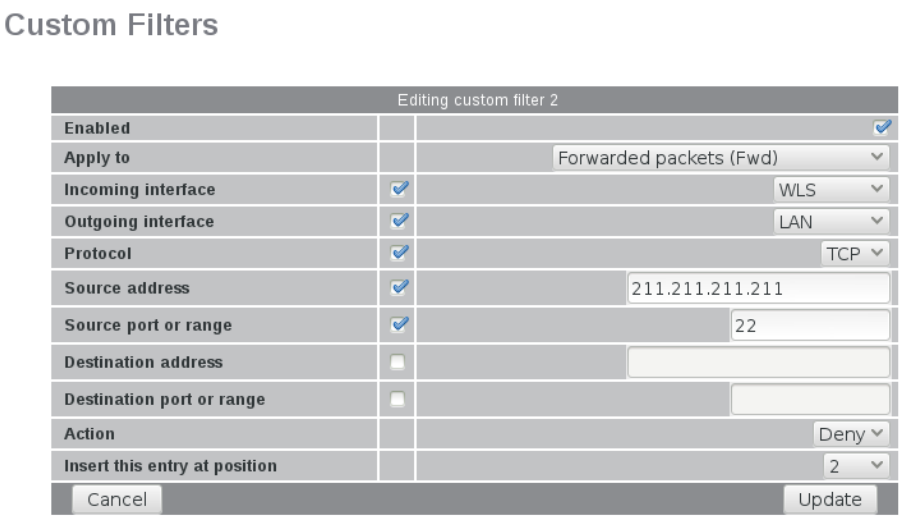


Figure 207: Editing a custom filter

To save the changes click the Update button or to lose any changes click the Cancel button. The main page will again be displayed as shown in Figure 208, with the changes for filter 2 added to the table.

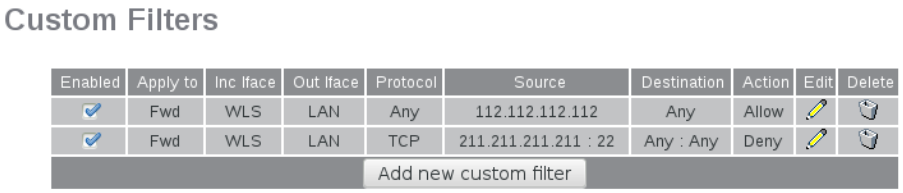


Figure 208: The main custom filter table after editing filter 2

10.4.5 Deleting a custom filter

A custom filter can be deleted by clicking the icon in the **Delete** column of the filter to be deleted. A warning box will be displayed. Click **OK** to confirm the deletion or **Cancel** to prevent the filter from being deleted.

For example, to delete filter 2 from the table shown in Figure 208, click the icon in row 2 of the table. A warning box will now be displayed, as shown if Figure 209. Click **OK** to confirm.

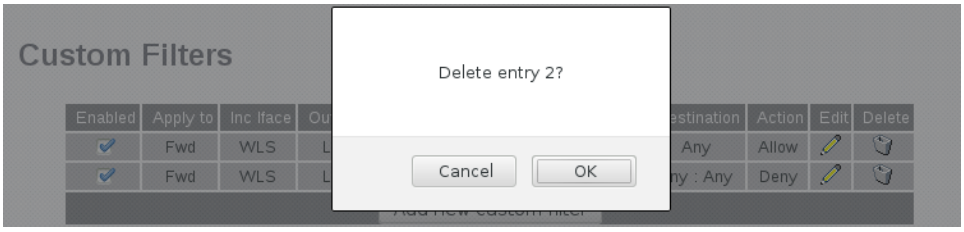


Figure 209: Deleting a custom filter

The filter table will be displayed with filter removed, as shown in Figure 210.

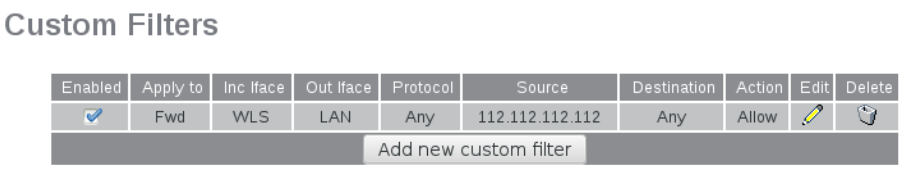


Figure 210: Custom filter table with filter 2 removed

10.5 Port Forwarding

10.5.1 Description

Port forwarding rules alter the destination address (and optionally the destination port) of packets received on the WAN or VPN interfaces of the modem. Port forwards can be used to forward specific services (e.g. HTTP) to a private machine on the LAN network without needing to expose the entire private machine to the public network.

To access the port forward configuration page, select select Firewall ▷ Port Forwards, a page similar to that shown in Figure 211 will be displayed.

Figure 211: Port forward page with no port forwards configured

10.5.2 Port forward options

To add a new port forward click the Add new port forward button, the port forward options will be displayed as shown in Figure 212. The same options page is displayed when a port forward is edited by clicking the icon in the **Edit** column of the port forward rule to be edited.

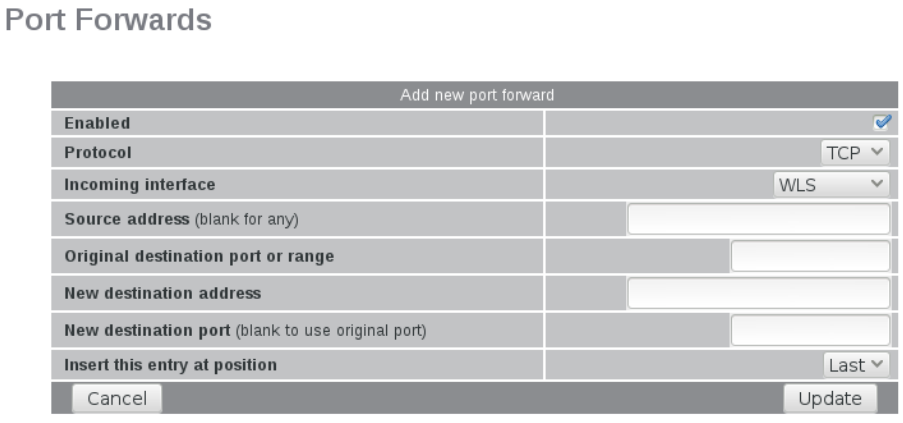


Figure 212: Page to add a Port forward

The following options can be set for each port forward:

Enabled Set the enabled check box to have the rule installed in the firewall. A rule can be temporarily disabled by un-checking this box.

Protocol The modem is able to forward TCP, UDP, GRE, ESP and AH. Most forwards will be either TCP or UDP. Select the appropriate protocol from the list.

Incoming interface Select the interface that the packets to be forwarded on will arrive (in this case, WLS, the wireless port, is selected).

Source address For greater security, the source addresses that the forward will be applied to can be limited. In this field, either a single address (for example, 172.16.1.132) or a subnet range (for example, 172.16.0.0/24) can be entered.

Original destination port or range This is the port number (80 in the example) but can also be a range (entered as, for example, 120-150) that the firewall will match on to forward to the new destination address.

New destination address This is the IP address of the server to forward to (10.10.10.50 in the example).

New destination port In addition to changing the destination address, it is also possible to change the destination port. To do so, enter the port in this field. This field can be left blank to keep the port the same.

Insert this entry at position Determines where this entry will be inserted in the list of port forwards.

Click the Update button to save and commit changes or click the Cancel button to cancel the addition or edit.

10.5.3 Adding a new port forward

From the main port forwards page, click the Add new port forward button. This will select the Add new port forward page. An example of adding a new port forward is shown in Figure 213. In this example a new port forward is created to forward from port 80 of the wireless port to a HTTP server at address 10.10.10.50.

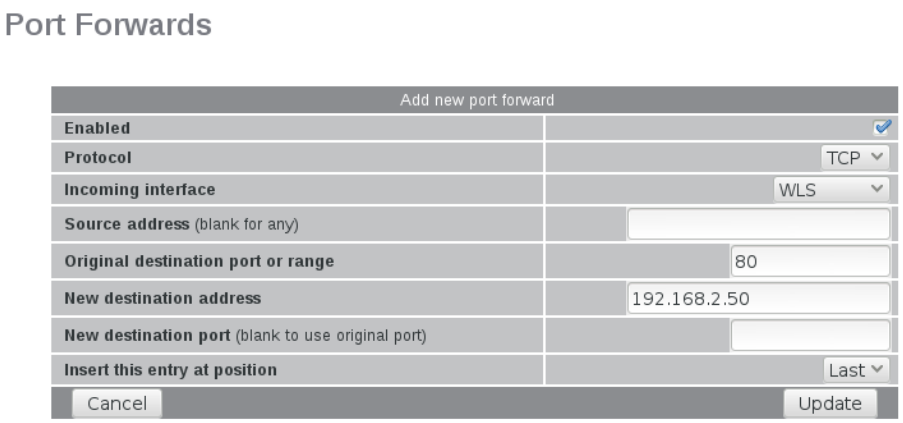


Figure 213: Adding a port forward

Click the Update button to save and commit the new port forward. The port forward table will be updated to include the new port forward as shown in Figure 214.

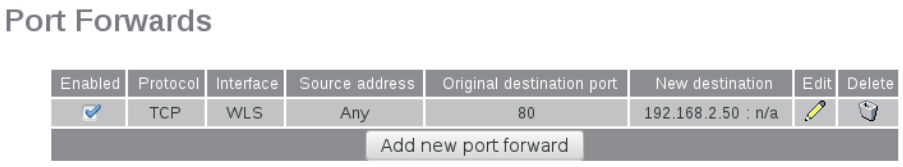


Figure 214: The port forward page with a single port forward

To add a second port forward click the Add new port forward button. In the example shown in Figure 215, a port forward is created which forward packets received for IP address 112.112.112.112 on port 2200 of the wireless port to LAN IP address 10.10.10.72.

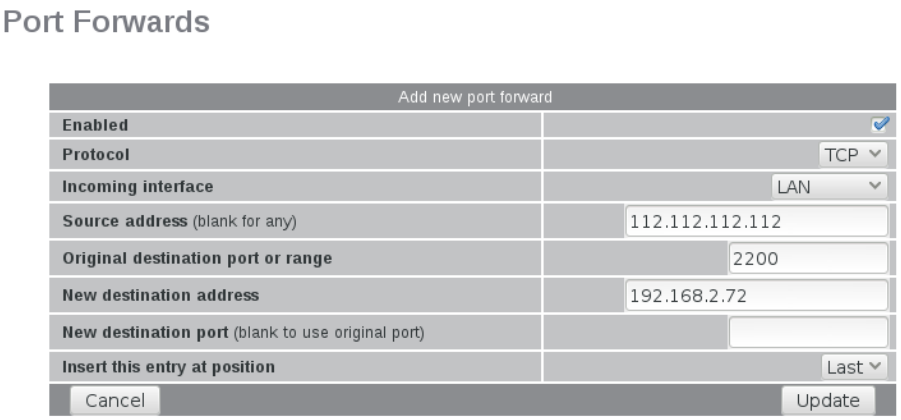


Figure 215: Adding a second port forward

To add the new port forward to the port forward table click the Update button. The main page will again be shown with the new port forward added, as seen in Figure 216.

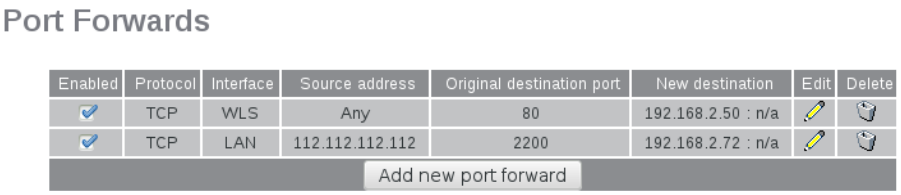


Figure 216: The port forward page with a two port forwards

10.5.4 Editing a port forward

A port forward can be edited by clicking the icon in the **Edit** column of the port forward to be changed. Once clicked, the details of the port forward will be displayed in the same table as when creating a new port forward.

As an example, to edit the second port forward in the port forward table, click the icon in the second row of the table. A page similar to the Add new port forward page will be displayed but will show the details of port forward 2. Changes were made so the destination is now port 22 as shown in Figure 217.

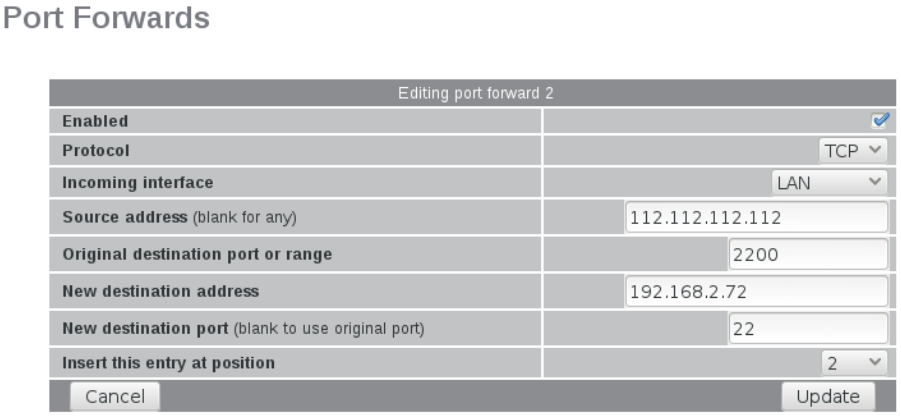


Figure 217: Editing a port forward

To save the changes, click the Update button or to lose changes click the Cancel button. The main page will again be displayed as shown in Figure 218, with the changes for port forward 2 added to the table.

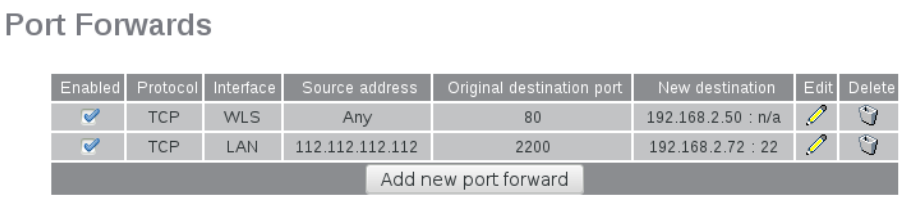


Figure 218: Main port forward page with revised port forward

10.5.5 Deleting a port forward

A port forward can be deleted by clicking the icon in the **Delete** column of the forward to be deleted. A warning box will be displayed. Click **OK** to confirm the deletion.

For example, to delete port forward 2 from the table shown in Figure 218, click the icon in row 2 of the table. A warning box will now be displayed as shown if Figure 219. Click the OK button.

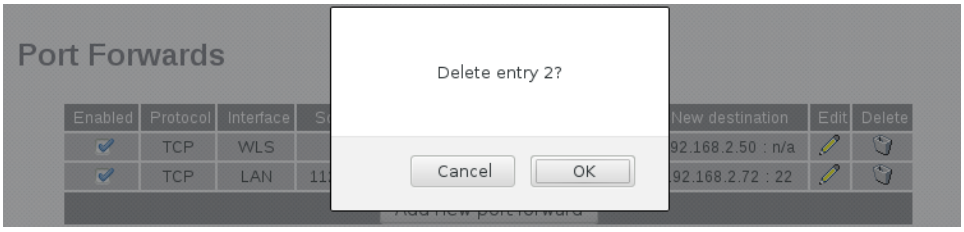


Figure 219: Deleting a port forward

The port forward table will be displayed with the port forward removed, as shown in Figure 220.

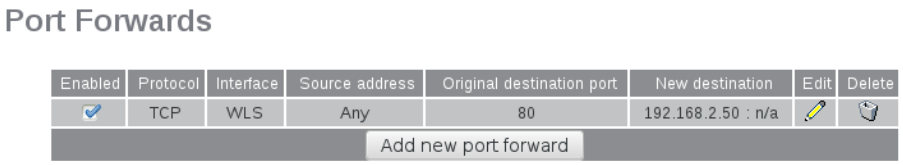


Figure 220: Port forward table of deleting a port forward

10.6 Custom NAT

10.6.1 Description

Custom NAT allow new rules to be added to the firewall to carry out Network Address Translation (NAT) that is different to the usual NAT provided by the firewall. Packets can be matched based on which of the modem's network interfaces they arrive on or will leave on, the protocol, the source or destination address. The packets can have Source-NAT (SNAT) applied, where the source address is altered, or Destination-NAT (DNAT) applied, where the destination address is altered.

Some example custom NATs are:

- Source-NAT on all packets being transmitted out a VPN tunnel.
- Destination-NAT to redirect packets to a host on the LAN.

To access the Custom NAT configuration page, select Firewall ▷ Custom NAT, a page similar to that shown in Figure 221 will be displayed.

Figure 221: Main custom NAT page, with no custom NAT entries in the table

10.6.2 Custom NAT options

To add a custom NAT rule click the Add new custom NAT button, the custom NAT options will be displayed as shown in Figure 222. The same options page is displayed when a custom NAT is edited by clicking the icon in the **Edit** column of the NAT rule to be edited.

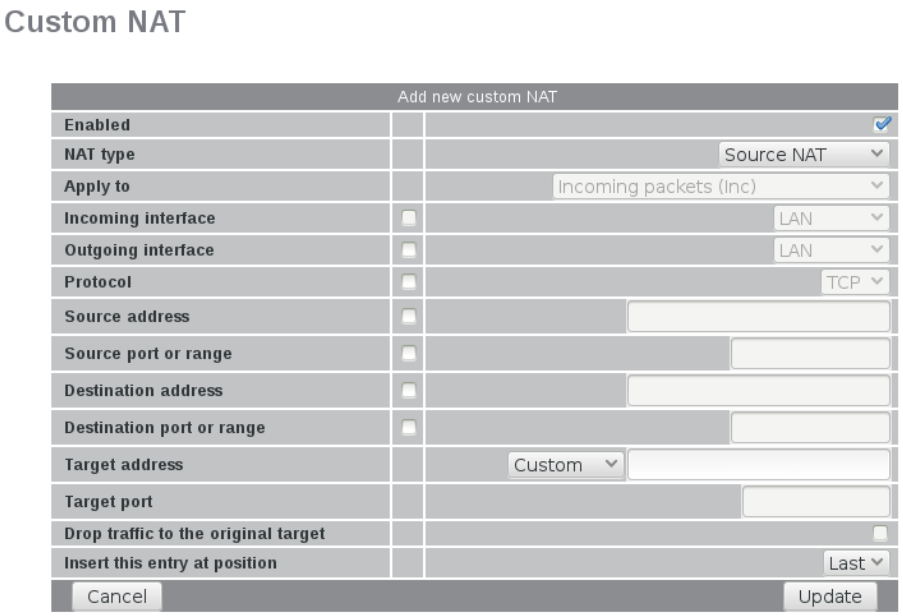


Figure 222: Add new Custom NAT page

The following options can be set for each custom NAT:

Enabled Set the enabled check box to have the rule installed in the firewall. A rule can be temporarily disabled by un-checking this box.

NAT Type Determines the type of NAT the entry will perform. Options:

Source NAT Source NAT changes the source address in IP packet and may also change the source port.

Destination NAT Destination NAT changes the destination address in IP packet and may also change the destination port.

1:1 Provides a one-to-one translation of IP addresses. This type of NAT is also know as Basic NAT

Apply to When entering a destination NAT, there are two places the NAT can be applied:

Incoming packets The rule will be applied to packets received from the modem's network interfaces.

Locally generated packets The rule will be applied to packets generated by an internal service.

Incoming interface If selected, packets will be matched based on the network interface they have been received on. Note that this can only be applied to a **Destination NAT** on **Incoming packets**.

Outgoing interface If selected, packets will be matched based on the network interface they will be transmitted on. Note that this can only be applied to a **Source NAT.**

Protocol If selected, packets will be matched based on their protocol type. Note that if you wish to match on source or destination ports, the protocol must be set to **TCP** or **UDP**.

Source address If selected, either a single address (for example, 172.16.1.132) or a subnet range (for example, 172.16.0.0/24) can be entered. Only packets matching this source address will have the filter applied to them.

Source port or range If selected, packets will be matched based on their TCP or UDP source port. Either an individual port (for example, 443) or a range of ports (80-143) can be entered.

Destination address Similar to the **Source address**, but instead matching on the destination address.

Destination port or range Similar to the **Source port or range,** but instead matching on the destination port.

Target address This is the address that the NAT rule will apply to packets. When set to **Custom**, any IP address can be entered in the text box. If an interface is selected from the drop-down box, the current address of that interface will be applied to packets.

Target port For rules that specify either the TCP or UDP protocol, it is possible to also alter the port number. If no change of port number is desired, this field can be left blank.

Insert this entry at position Determines where this entry will be inserted in the list of custom NAT rules.

Click the Update button to save and commit changes or click the Cancel button to cancel the addition or edit.

10.6.3 Adding a new custom NAT

From the main custom NAT page click the Add new custom NAT button. This will select the Add new custom NAT page. An example of adding a new custom NAT is shown in Figure 223. In this example, a new custom NAT is created which will source NAT packets outgoing on the SSL VPN interface to the IP address of the SSL VPN.

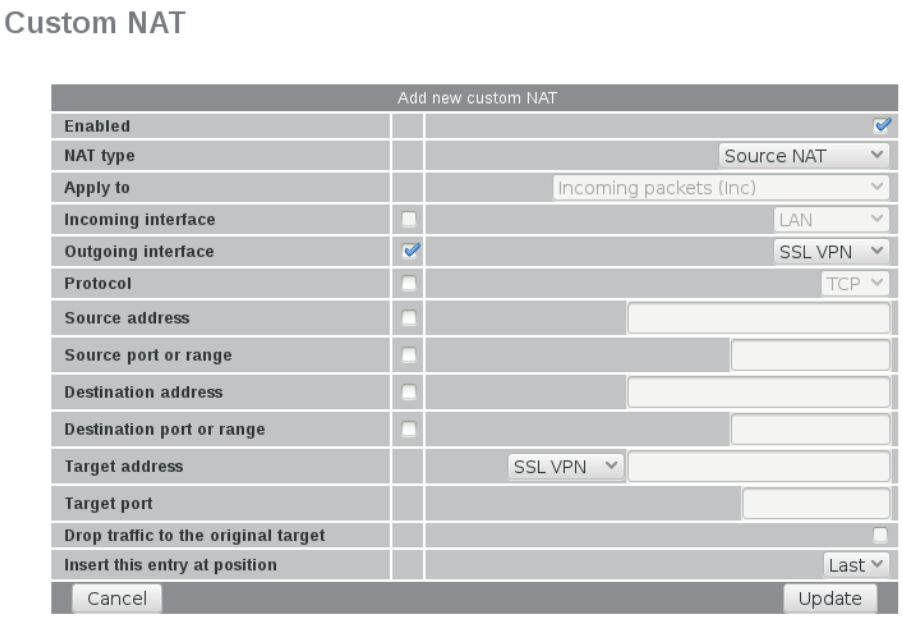


Figure 223: Adding a custom NAT

It can be seen in the example that in the centre column only **Outgoing interface** is checked. This indicates these are the matching criteria that will be applied to packets. In this case, all packets outgoing on the SSL VPN will be source NAT'd.

Click the Update button to save and commit new custom NAT rule. The custom NAT table will be updated to include the new custom NAT as shown in Figure 224.

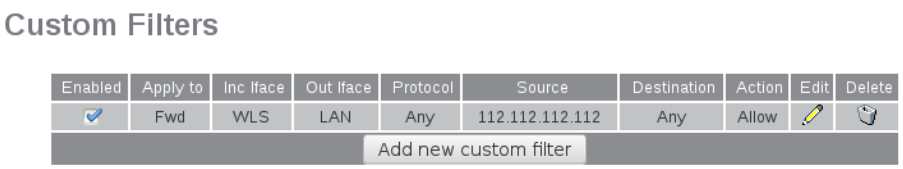


Figure 224: Main custom NAT page showing new custom NAT added to the table

To add a second custom NAT again click the Add new custom NAT button. In the example shown in Figure 225, a destination NAT is created for packets destined for the wireless port.

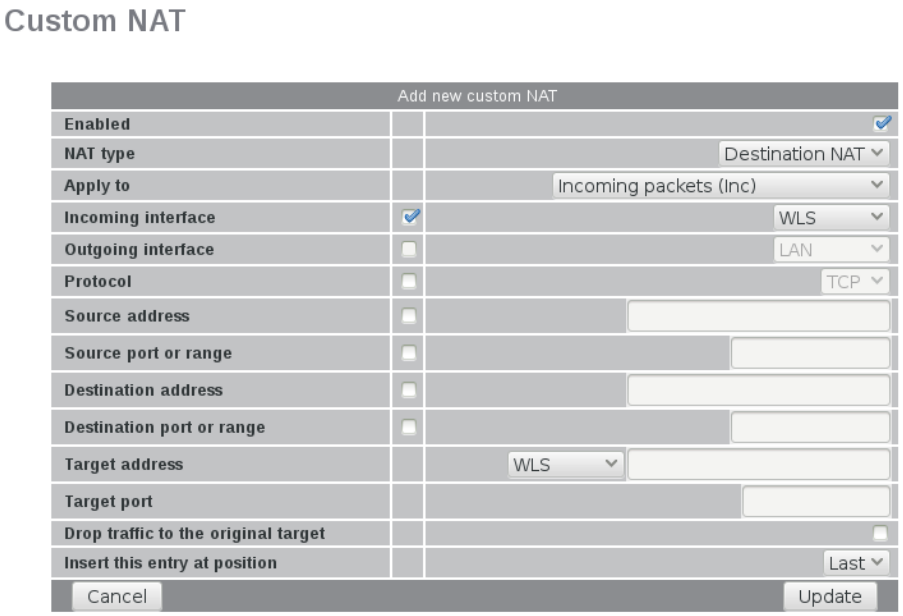


Figure 225: Adding a custom NAT

To add the new custom NAT lick the Update button. The main page will again be shown with the new custom NAT added, as seen in Figure 226.

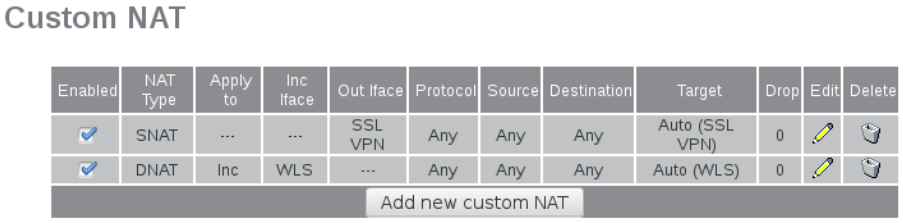


Figure 226: Main custom NAT page showing new custom NAT added to the table

10.6.4 Editing a custom NAT

A custom NAT can be edited by clicking the icon in the **Edit** column of the filter to be changed. Once clicked, the details of the custom NAT will be displayed in the same table as when creating a new custom NAT.

As an example, to edit the second custom NAT in the Custom NAT table shown in Figure 226, click the icon in the second row of the table, A page similar to the new custom NAT page will be displayed but with the details of custom NAT 2. To set the protocol for the custom NAT to be UDP, changes were made as shown in Figure 217.

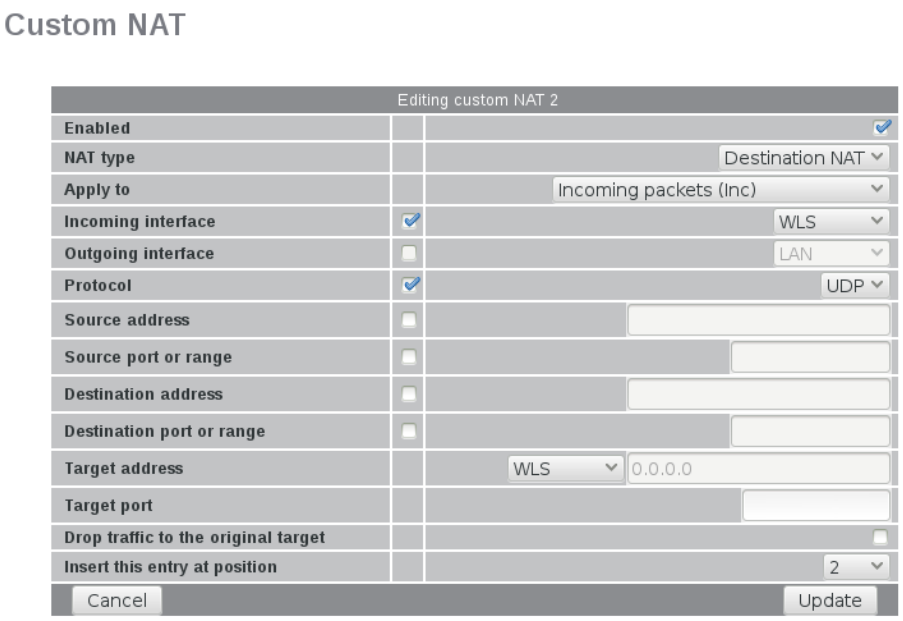


Figure 227: Editing a custom NAT

To save the changes click the Update button or to lose the changes click the Cancel button. The main page will again be displayed as shown in Figure 228, with the changes for custom NAT 2 added to the table.

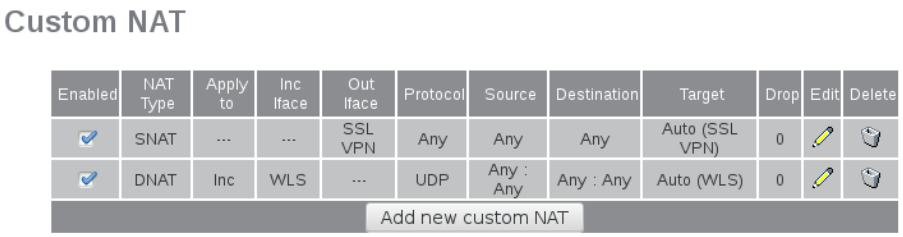


Figure 228: Main custom NAT page with revised custom NAT 2

10.6.5 Deleting a custom NAT

A custom NAT can be deleted by clicking the icon in the **Delete** column of the NAT to be deleted. A warning box will be displayed. Click **OK** to confirm the deletion.

For example, to delete custom NAT 2 from the table shown in Figure 228, click the icon in row 2 of the table. A warning box will now be displayed as shown if Figure 219. Click the OK button.

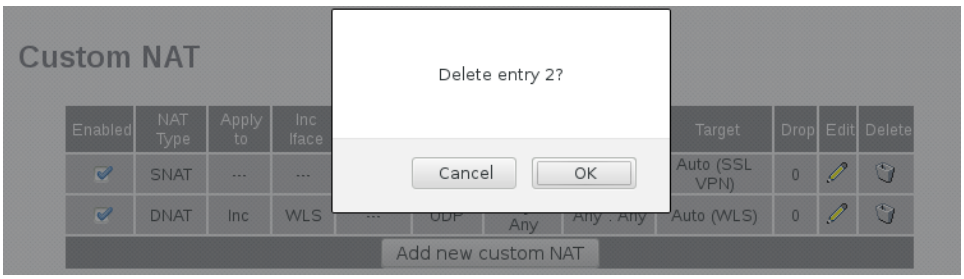


Figure 229: Deleting a custom NAT

The custom NAT table will be displayed with the custom NAT removed, as shown in Figure 220.

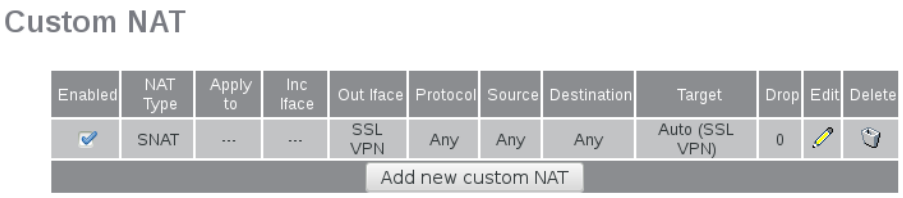


Figure 230: Custom NAT table after deleting a custom NAT

10.7 MAC Address Filtering

10.7.1 Description

The firewall supports Media Access Control (MAC) address filtering. A unique MAC address is assigned to every Ethernet device, this address can be filtered to either allow or deny a device access to a device or network.

While providing a network with a level of protection, MAC Filtering can be circumvented by scanning the network for a valid MAC and then changing the MAC address of the attacker's machine to a validated one. For this reason if access to the LAN interface is to be restricted MAC address filtering should not be used as the only form of security.

To access the MAC Address Filters configuration page, select Firewall ▷ MAC Filters, a page similar to that shown in Figure 231 will be displayed.

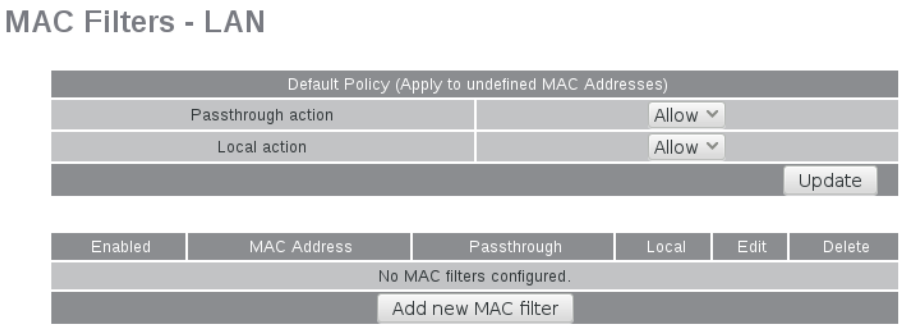


Figure 231: MAC Address filters main page.

10.7.2 Default policy

The default policy sets the action to be taken for all MAC addresses not listed in the MAC address table. The options for this are *Allow* and *Deny*. If the default policy is to be set to Deny it is recommended this is done after the Allow rules have been added so as to prevent accidental lock-out.

Care should be taken when configuring MAC Filters to ensure the computer being used to configure the device is not denied access if as likely it is connected to the LAN interface. When changing filters it is recommended to first add a specific filter to allow access to the computer being used for configuration. If after configuration is complete the rule is no longer required it can be deleted.
If the computer used for configuration is denied access the it will be necessary to perform a factory reset of the device. This will clear all the configuration settings to the factory default settings and the LAN ports will be enabled.

If the access via the LAN interface is restricted then access to the web configuration pages may be available via the wireless interface if the firewall settings allow access.

Passthrough action Action for packets destined for the WAN interface. Options:

Allow All non-matching MAC addresses accepted.

Deny All non-matching MAC address dropped.

Local action Action for packets destined for a service on the device. Options:

Allow All non-matching MAC addresses accepted.

Deny All non-matching MAC address dropped.

Click the Update button to save and commit changes.

10.7.3 Adding a MAC Filter

To add a MAC filter click the Add new MAC filter button, the MAC filter options will be displayed as shown in Figure 222. The same options page is displayed when a MAC filter is edited by clicking the icon in the **Edit** column of the MAC filter to be edited.

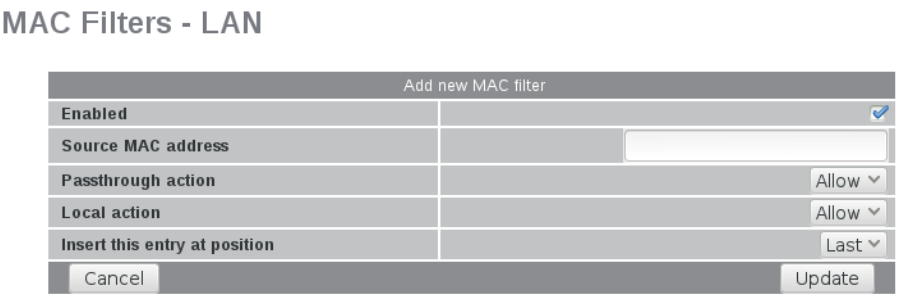


Figure 232: Adding a MAC address filter.

The options are:

Enabled Set to make active the filter. A filter can be disabled by un-checking this box.

Source MAC address The MAC address on which the filter will be applied.

Passthrough Action The action to be applied for pass-through, the options are:

Allow Packets with matching MAC address will be pass-through to the WAN interface.

Deny Packets with matching MAC will be denied access to the WAN interface.

Local Action The action to be applied for local services the options are:

Allow Packets with matching MAC address will be passed to the local services.

Deny Packets with matching MAC will be denied access to the local services.

Insert this entry at position Determines where this entry will be inserted in the list of MAC address filters.

Click the Update button to save and commit changes.

10.7.4 Example MAC Address Filters

On the MAC Address Filter page click the Add new MAC filter button. This will select the Add new MAC Filter page. In this example, shown in figure 233 a new MAC filter will be added to allow MAC address 00:11:22:33:44:55 both pass-through and local access.

Figure 233: Example of adding an MAC filter.

Once the details have been entered click the Update button to save the new MAC filter.

The MAC filter table will be updated to include the MAC filter rule as shown in Figure 234.

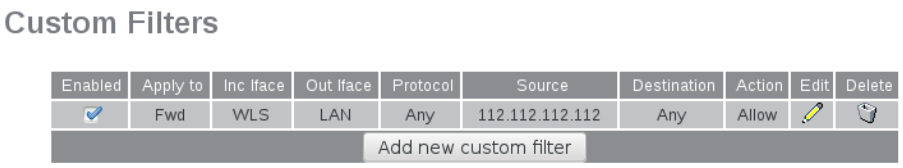


Figure 234: MAC filter table with new rule added.

To add a second MAC filter again click the Add new MAC filter button. In the example, shown in Figure 235, a MAC address filter has been added to allow MAC address 55:44:33:22:11:00 again with pass-through and local access.

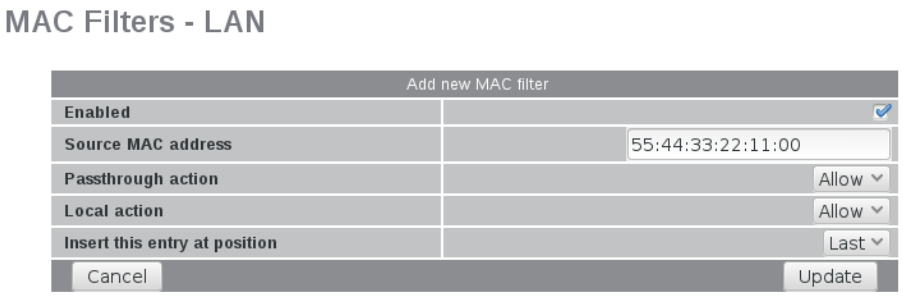


Figure 235: Adding a MAC Filter rule.

To add the new MAC filter click the Update button. The main page will again be shown with the new MAC filter rule added, as seen in Figure 236.

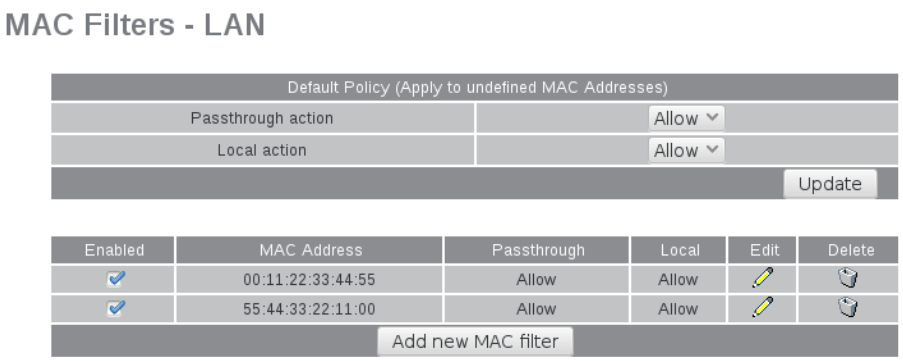


Figure 236: MAC address table with new rule added

10.7.5 Editing a MAC Filter

A MAC Filter can be edited by clicking the icon in the **Edit** column of the filter to be changed. Once clicked, the details of the MAC Filter will be displayed in the same way as when creating a new MAC Filter.

As an example, to edit the second MAC Filter in the MAC Filter table shown in Figure 236, click the icon in the second row of the table, A page similar to the new MAC Filter page will be displayed but containing the details of MAC Filter 2. To change the Local Action for this rule to Deny, changes were made as shown in Figure 217.

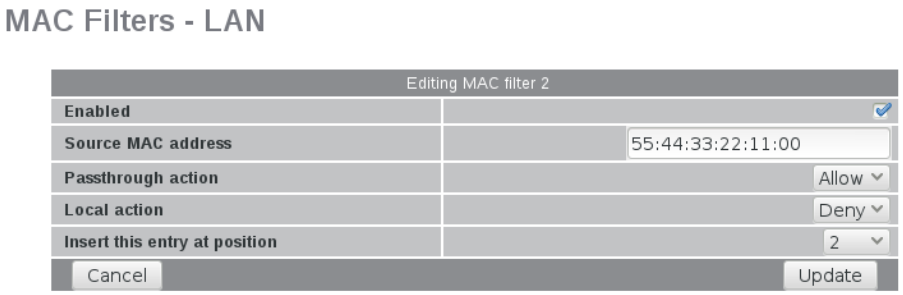


Figure 237: Editing a MAC Filter

To save the changes click the Update button or to lose the changes click the Cancel button. The main page will again be displayed as shown in Figure 238, with the changes for MAC Filter 2 added to the table.

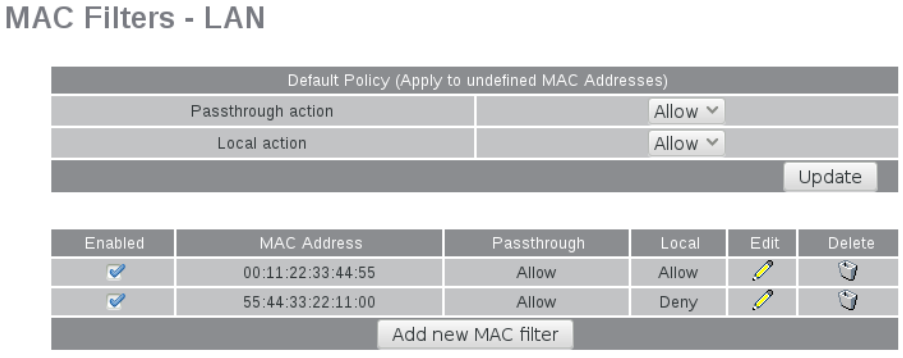


Figure 238: MAC Filter table after changes to MAC filter 2.

10.7.6 Changing the default Policy

In the previous example the second MAC address filter denied access to the local services, however the default policy is to allow access to all MAC addressed which means the deny rule will not work. In order to correct this set the default

action will need to change to Deny. In addition the first rule is an allow rule, so in order for this rule to be effective the default pass-through also needs to be set to Deny. This shown in Figure 239.

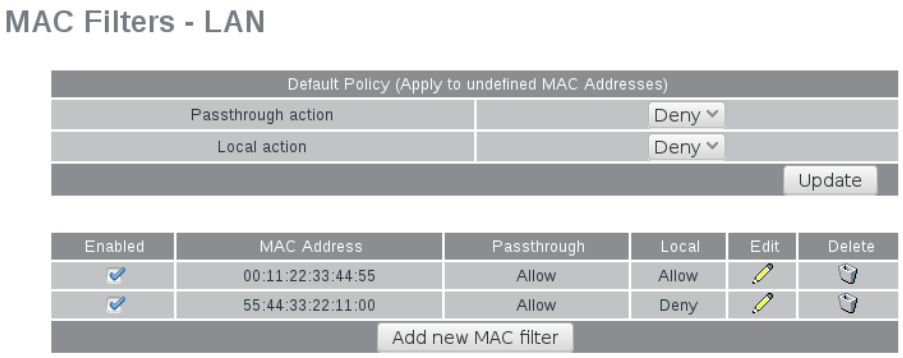


Figure 239: MAC Filter page with default action set to deny.

10.7.7 Deleting an MAC Address Filter

A MAC Filter can be deleted by clicking the icon in the **Delete** column of the MAC Filter to be deleted. A warning box will be displayed. Click the OK button to confirm the deletion.

For example, if it were decided not to allow pass-through in rule 2 the rule could be changed or the same result could be achieve by removing the rule. To delete MAC Filter 2 from the table shown in Figure 239, click the icon in row 2 of the table. A warning box will now be displayed as shown if Figure 240. Click the OK button.

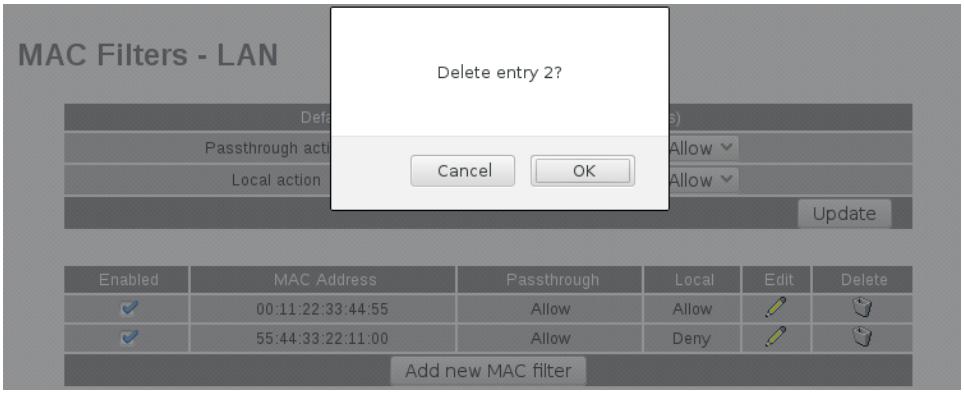


Figure 240: Deleting a MAC Filter.

The MAC Filter table will be updated with the MAC Filter removed, as shown in Figure 220.

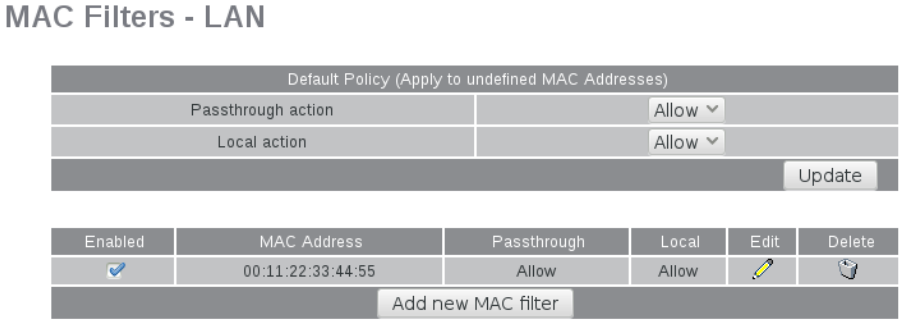


Figure 241: MAC Filter table after deleting a MAC Filter.

11 Virtual Private Network (VPN)

A virtual private network (VPN) is a communications network tunnelled through another, usually insecure network. Generally the secured communications network is tunnelled through the wireless interface and then over the Internet or private network to a VPN-capable router or server. Support is provided for IPsec, SSL and PPTP/L2TP based VPNs and multiple VPN tunnels can be configured to operate simultaneously.

The main VPN page is accessed by clicking VPN on the main menu, the page displayed will be similar that shown in figure 242.

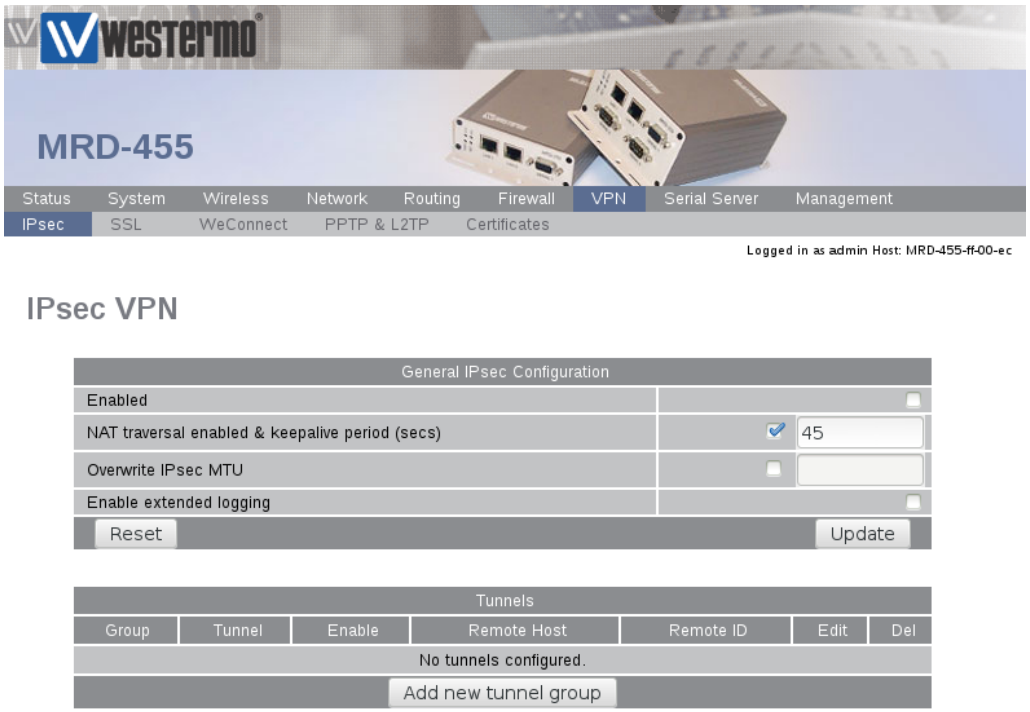


Figure 242: The main VPN page.

11.1 Internet Protocol Security (IPsec) VPN

Internet Protocol Security (IPsec) is a suite of standards and protocols for securing Internet Protocol (IP) communications by authenticating and/or encrypting each IP packet in a data stream. Also included within IPsec are protocols for cryptographic key establishment. IPsec protocols operate at the network layer (layer 3 of the OSI model). This means that it can be used for protecting layer 4 protocols, including both TCP and UDP, the most commonly used transport layer protocols. Using strong encryption and public key cryptography IPsec can secure data links over public networks which would otherwise be insecure.

IPsec is a framework which is built in to various security products from companies such as Cisco and Juniper to provide end-to-end security. IPsec functionality has been tested for interoperability with the Cisco implementation of IPsec know as *Cisco IOS IPsec*.

11.1.1 General IPsec configuration

To access the IPsec VPN configuration page click VPN ▷ IPsec VPN the page shown in Figure 243 will be displayed. The page contains general IPsec configuration options at the top and a list of configured tunnels at the bottom.

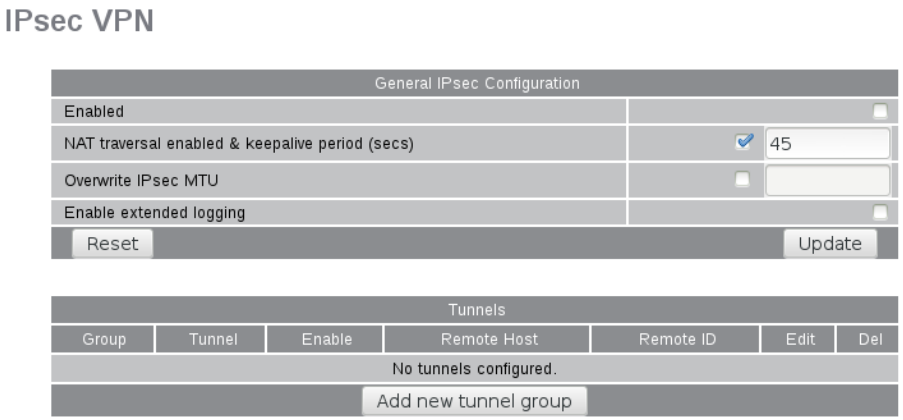


Figure 243: IPsec based VPN main page

The first table contains the **General IPsec configuration** settings. The options are:

Enabled Check the box to enable the IPsec VPN. Default is disabled.

NAT traversal enabled & keepalive period (secs) Check box to enable NAT Traversal and set the keepalive time.

NAT Traversal When passing through a Network Address Translator (NAT) an IP packet is modified in such a way that is incompatible with Internet Protocol Security (IPsec). NAT-Traversal protects the original IPsec encoded packet by encapsulating it within another layer of UDP and IP headers. If the wireless interface is allocated a dynamic and private IP address then the connection to the Internet will be via a Network Address Translator (NAT). This will require the use of NAT-Traversal for IPsec to establish a connection.

Keepalive Period NAT keepalives are used to keep the dynamic NAT mapping alive during a connection between two peers. NAT keepalives are UDP packets with an unencrypted payload of 1 byte. Although similar to dead peer detection (DPD), NAT keepalives are different. DPD is used to detect peer status, while NAT keepalives are sent if the IPSec entity did not send or receive a packet in a specified period of time.

Overwrite IPsec MTU Maximum Transmission Unit (MTU) is the size (in bytes) of the largest packet which can be sent over the IPsec tunnel. Leave the checkbox un-checked and the value blank to use the default setting. To change the MTU check the checkbox and enter the value.

Enable extended logging Check to enable extended logging for the wireless interface. This option is useful if connection problems are encountered.

Click the Update button to save and commit changes.

The second table shows a summary of all configured tunnels. The next section details adding tunnels.

11.1.2 Adding an IPsec tunnel

To add an IPsec tunnel click the Add new tunnel group button. This will display the first of several pages used to configure the IPsec VPN tunnel. The first page is the Tunnel Configuration shown in Figure 244.

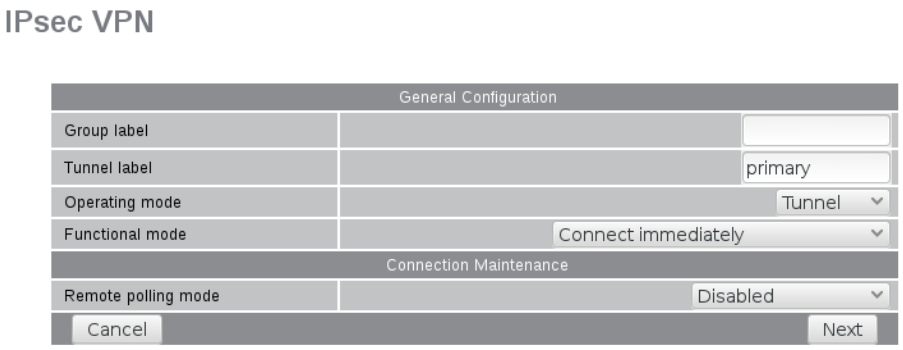


Figure 244: IPsec tunnel configuration

General Configuration IPsec general configuration is the first stage in adding a new IPsec tunnel. The options are as follows:

Group_label Provide a label for the tunnel group. This is used as a reference and is particularly useful when more than one tunnel is configured. This label is required even if there is only 1 tunnel in the group.

Tunnel label Set the label or name for the tunnel within the group. This is used to distinguish between tunnels for example 'primary' and 'secondary'

Operating mode Select the operating mode of the IPsec tunnel from the following options:

Tunnel Tunnel mode encapsulates the entire IP packet to provide a secure connection between two gateways. In tunnel mode the payload, the header and the routing information are all encrypted, and then encapsulated into a new IP packet. This mode is generally used to create a VPN.

Transport Transport mode provides a secure connection between two hosts. Only the payload of the IP packet is encrypted.

Functional mode Select the functional mode of the IPsec tunnel from the following options:

Connect immediately The tunnel will be initiated, that is it will attempt to establish a connection with a remote responder.

Responder or Connect on demand Wait for and respond to incoming connections or if no active connection, establish a connection to a remote server.

Connection Maintenance IPsec connection maintenance options:

Remote polling mode Disabled No remote polling

Poll_at_fixed_interval Enable polling, the following options will appear when selected:

Poll period Specify the time interval in seconds between polls. Minimum value of 15 seconds.

Retry period Check to enable and specify the time in seconds to retry the poll after a failed poll. Minimum value of 15 seconds.

Failed establishment polls before restarting connection Specify the number of failed establishment polls to declare the connection down and to re-start the establishment process.

Failed polls before restarting connection Specify the number of failed polls to declare the connection down and to re-start the establishment process.

Poll type Specify the poll type. The options are:

Ping (ICMP) Ping the specified address.

TCP Socket Establish a TCP socket to the specified address and port number. The connection will be terminated as soon as successfully opened.

Poll address Specify the IP address to poll.

Once configuration is complete on this page click the Next button to move to the next page.

11.1.2.1 Physical Layer Configuration

The second page is the **Physical Layer Configuration** page, the options on the page will depend on the functional mode selected, Figure 245 shows the options for the initiator mode while Figure 246 shows the options for the responder mode.

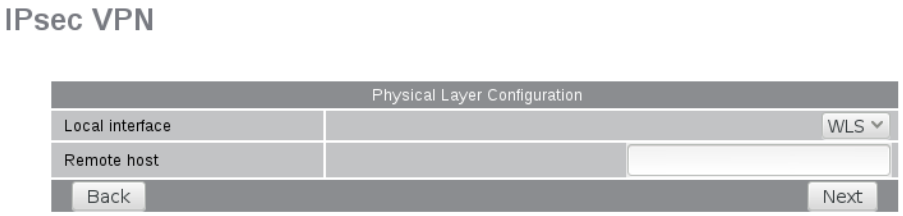


Figure 245: IPsec physical configuration initiator mode.

The options for physical layer configuration when configured as an initiator are as follows:

Local interface Select the interface over which to create the tunnel. The drop-down box will show all of the available options for the device. Possible options are:

WLS The wireless interface.

DSL The DSL interface

LAN The local Ethernet interface. If the option is selected an addition option will appear:

Local Gateway (Nexthop) Enter the gateway or next hop address.

Remote host Provide the address of the remote host to which a connection should be established.

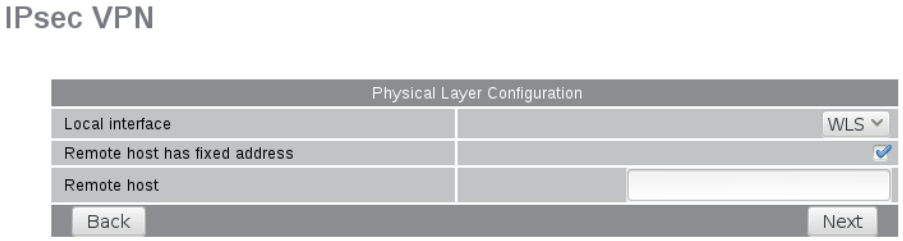


Figure 246: IPsec physical configuration responder mode.

The options for physical layer configuration when configured as a responder are as follows:

Local interface Select the interface over which to create the tunnel. The drop-down box will show all of the available options for the device. Possible options are:

WLS The wireless interface.

DSL The DSL interface

LAN The local Ethernet interface. If the option is selected an addition option will appear:

Local Gateway (Nexthop) Enter the gateway or next hop address. Refer to figure 247 as an example of the responder page with the local interface set to LAN.

Remote host Provide the address of the remote host to which a connection should be established.

Remote host has fixed address Check if the remote host has a fixed address.

Remote host The address of the remote host from which to expect connections. This option will only be available if the Remote host has fixed address has been checked.

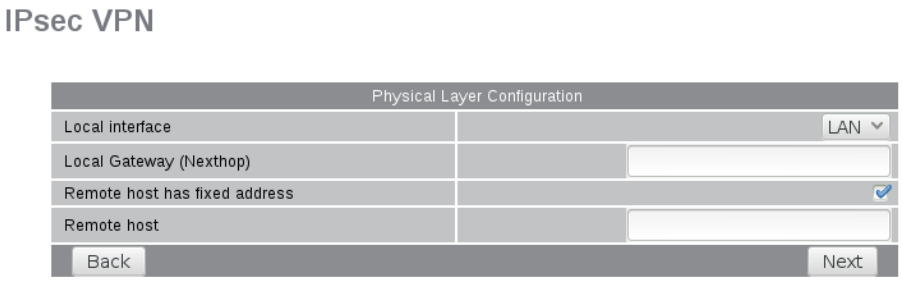


Figure 247: IPsec physical configuration responder mode with LAN interface set as the local interface.

Once configuration is complete on this page click the Next button to move to the next configuration page.

11.1.2.2 Phase 1 Configuration

The Phase 1 Configuration is used to set the parameters for the first phase of IPsec Key Exchange (IKE). The first phase is a set-up phase in which the two hosts agree on how to exchange further information securely. The Phase 1 Configuration page is shown in Figure 248.

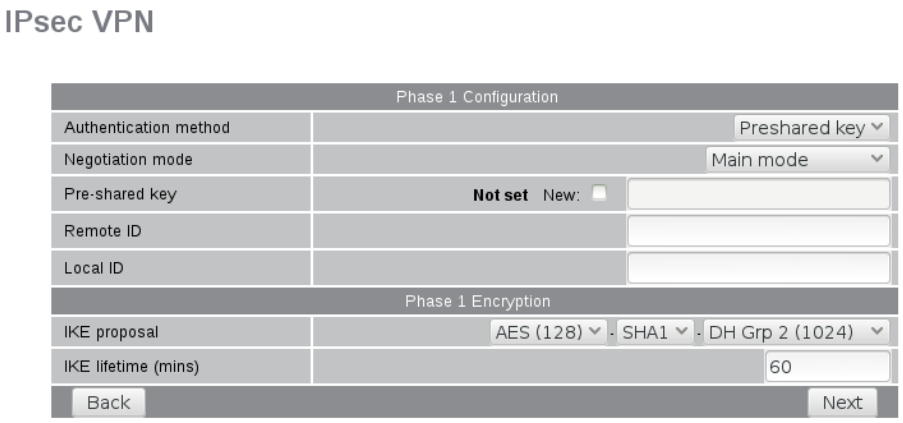


Figure 248: IPsec Phase 1 configuration with Pre-Shared Key selected.

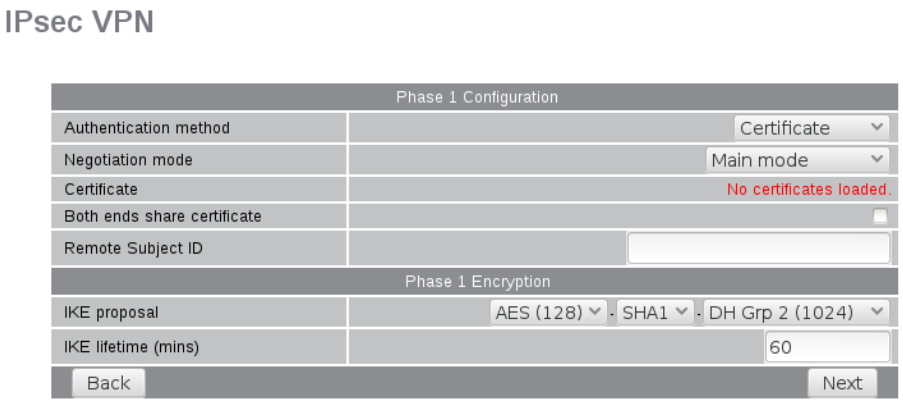


Figure 249: IPsec Phase 1 configuration with certificates selected.

The options for Phase 1configuration are:

Authentication method Select the authentication method from the drop-down list. The options are:

Pre-shared key The Pre-Shared Key (PSK) is a key value which is entered into each host and is used for authentications

Certificate A certificate is an electronic document containing a public key and a digital signature.

Negotiation mode Select the negotiated mode from the drop-down list, the options are:

Main mode Main mode provides identity protection for the hosts initiating the session. Main mode cannot be used with pre-shared keys and name-based IDs.

Aggressive mode Aggressive mode is quicker to establish a connection than Main mode but provides no identity protection. Aggressive mode can be used when there is Network Address Translation (NAT) on the connection between hosts.

Preshared key_options The following options are available when the authentication method is set to Preshared key:

Pre-shared key This field is used to enter the Pre-Shared Key if this method of authentication was selected. To enter a new key check the box and enter the key in the text field. During key entry the key will be in clear-text, once the page is updated the key will no longer be visible. The text immediately prior the check-box will indicate if a key has been **Set** or **Not set**.

Certificate Select the certificate to use if Certificate authentication has been selected. For information on how to enter certificates refer to Section 11.5 Certificate Management.

Remote ID The remote ID is used to ensure the remote host is in fact the expected remote IPsec entity. The remote ID can take a number of forms:

IPv4 The remote party will present a standard IP address (eg 123.123.123.123) as its ID. Enter the IP address in this field.

FQDN Fully Qualified Domain Name. The remote party will present a full hostname as its ID. Enter the name in this field. Note that hostnames must be able to be resolved through DNS.

FQUN Fully Qualified User Name. The remote party will present a name of the form joe@some.place.com or @ipsec.server.com as its ID. The domain of this name does not have to be resolvable. Enter the name in the field, including the '@' symbol.

Distinguised Name Where certificate based authentication is used, the Distinguished Name or Subject string of the certificate must be entered in this field, preceded by an '@' symbol

Local ID The local ID determines how the modem will identify itself to the remote party. The local ID can take a number of forms:

IPv4 The local ID will be a standard IP address (eg 123.123.123.123). Enter the IP address in this field.

FQDN Fully Qualified Domain Name. The local ID will present a hostname as its ID. Enter the name in this field. Note: host-names must be able to be resolved through DNS.

FQUN Fully Qualified User Name. The local ID is a name of the form joe@some.place.com or @ipsec.client.com. The domain of this name does not have to be resolvable. Enter the name in the field, including the '@' symbol.

Certification options The following options are available when the authentication method is set to Certificate:

Certificate Select the certificate to use, for information on how to enter certificates refer to Section 11.5 Certificate Management.

Both ends share certificate Check to indicate yes.

Remote Subject ID The subject ID of the remote certificate. This option is only available if the certificates are not shared.

11.1.2.3 Phase 1 Encryption

The second part of the Phase 1 configuration is the encryption type to be used. The options are:

IKE proposal is a set of parameters for Phase 1 IPSec negotiations. The parameters are encryption algorithm, authentication algorithm and the Diffie-Hellman group.

Encryption Algorithm Select the encryption algorithm from the drop-down list. The options are:

AES (128) 128 bit Advanced Encryption Standard (AES).

AES (256) 256 bit Advanced Encryption Standard (AES).

3DES Triple Data Encryption Standard (3DES).

DES Data Encryption Standard (DES).

Authentication Algorithm Select the authentication mode from the drop-down list. The options are:

MD5 Message-Digest algorithm 5.

SHA1 Secure Hash Algorithm.

Diffie-Hellman Group is a cryptographic protocol which allows two parties to establish a shared secret key over an insecure network without the parties having any prior knowledge of the other party. Select the Diffie-Hellman Group from the drop-down list. The options are:

DH Grp 1 (768) The 768 bit Diffie-Hellman group.

DH Grp 2 (1024) The 1024 bit Diffie-Hellman group.

DH Grp 5 (1536) The 1536 bit Diffie-Hellman group.

DH Grp 14 (2048) The 2048 bit Diffie-Hellman group.

IKE lifetime (mins) Specify the IKE lifetime in minutes. Default is 60 minutes.

Once configuration is complete on this page click the Next button to move to the next configuration page.

11.1.2.4 Phase 2 Configuration

Phase 2 establishes the IPsec Security Associations (SA) parameters in order to establish an IPsec tunnel. Phase 2 has a single mode called Quick mode that starts after IKE has started a secure tunnel in phase 1. Quick mode is also used to re-negotiate a new IPsec SA when the current IPsec SA lifetime expires. The default Phase 2 configuration page is shown in Figure 250 while Figure 251 shown the options available when Xauth is enabled..

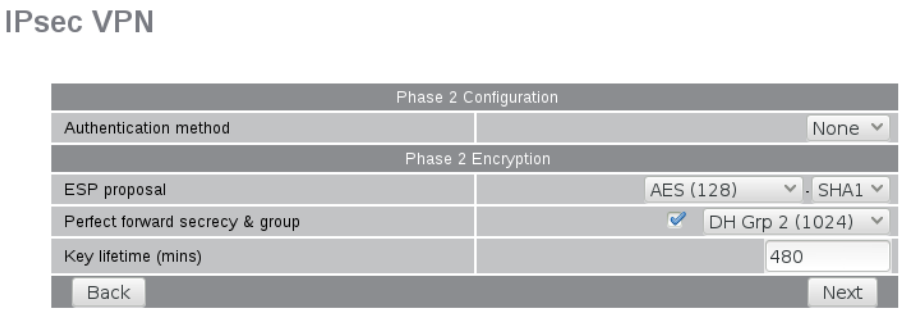


Figure 250: IPsec Phase 2 configuration.

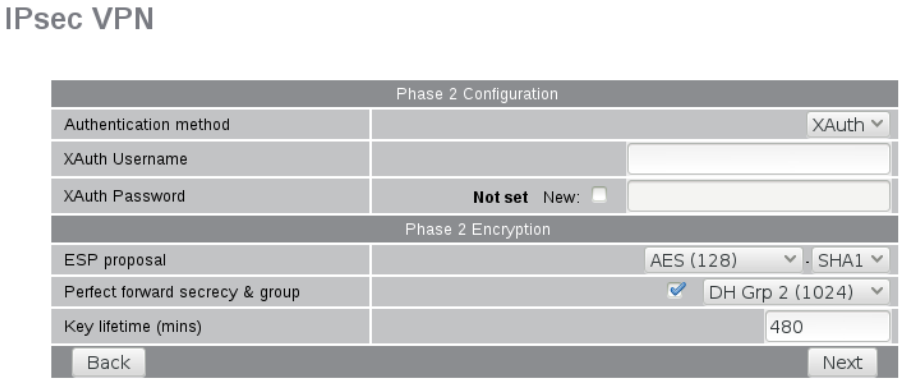


Figure 251: IPsec Phase 2 configuration with Xauth enabled.

The phase 2 options are:

Authentication method Select the extended authentication method, the options are:

None No extended authentication.

XAuth provides an additional level of authentication by allowing the IPSec gateway to request extended authentication from remote users, thus forcing remote users to respond with their credentials before being allowed access to the VPN.

XAuth username This field is used to enter the XAuth user-name if this method of authentication was selected.

XAuth password This field is used to enter the XAuth password if this method of authentication was selected. To enter a new password check the box and enter the password in the text field. During key entry the key will be in clear-text, once the page is updated the key will no longer be visible. The text immediately prior the check-box will indicate if a key has been **Set** or **Not set**.

11.1.2.5 Phase 2 Encryption

The phase 2 encryption options are:

ESP proposal Encapsulating Security Payload (ESP) is used to encrypt the data transmitted in IP datagrams. The proposal establishes the Encryption algorithm and Authentication protocol to use.

Encryption Algorithm Select the encryption algorithm from the drop-down list, the options are:

AES (128) 128 bit Advanced Encryption Standard (AES).

AES (256) 256 bit Advanced Encryption Standard (AES).

3DES Triple Data Encryption Standard (3DES).

Blowfish (128) 128 bit blowfish.

Blowfish (256) 256 bit blowfish.

Authentication Algorithm Select the authentication algorithm from the drop-down list, the options are:

MD5 Message-Digest algorithm 5.

SHA1 Secure Hash Algorithm.

Perfect forward secrecy & group In an authenticated key-agreement protocol using public key cryptography, such as Diffie-Hellman key exchange, perfect forward secrecy (PFS) is the property that ensures a session key derived from a set of long-term public and private keys will not be compromised if one of the private keys is compromised in the future.

Perfect forward secrecy Check to enable perfect forward secrecy.

Diffie-Hellman Group Select the Diffie-Hellman Group from the drop-down list, the options are:

DH Grp 1 (768) The 768 bit Diffie-Hellman group.

DH Grp 2 (1024) The 1024 bit Diffie-Hellman group.

DH Grp 5 (1536) The 1536 bit Diffie-Hellman group.

DH Grp 14 (2048) The 2048 bit Diffie-Hellman group.

Key lifetime (mins) Key lifetime in minutes. Default 480 minutes.

Once configuration is complete on this page click the Next button to move the next page.

11.1.2.6 Tunnel Options

Tunnel options are for configuring how the tunnel renegotiates a connection.

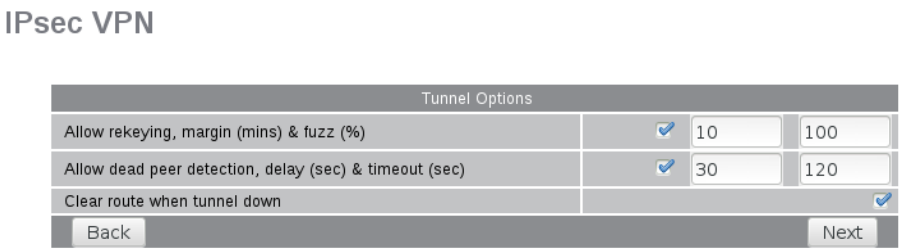


Figure 252: IPsec Tunnel options and Dead Peer Detection configuration.

The options are:

Allow rekeying, margin (mins) & fuzz Re-keying is used to renegotiate the connection encryption keys prior to the previous keys expiring. The options are:

Enable Check the check-box to enable re-keying. Default is On.

Margin The time in minutes prior to the connection expiring at which attempts to negotiate a new connection begin. Default 10 Minutes.

Fuzz defines the maximum percentage by which the Margin can be increased in order to randomise re-keying intervals. Default is 100%.

Allow dead peer detection, delay & timeout Dead Peer Detection (DPD) is a method of detecting a dead Internet Key Exchange (IKE) peer. The method uses IPsec traffic patterns to minimise the number of messages required to confirm the availability of the connection. The configuration options are:

Enable Check the check-box to enable Dead Peer Detection.

Delay Set the delay in seconds between Dead Peer Detection keep-alives that are sent for the connection.

Timeout The time in seconds to declare the peer dead after the delay and not receiving data or a keep-alive.

Clear route when tunnel down Check to clear the routes from the routing table when the tunnel is down.

The clear route when tunnel down option should be used with caution.
It is possible for traffic intended for a secure connection could be sent over an unsecured connection. This would occur if the routes were removed from the routing table and an alternative routing rule for example the default route allowed traffic intended for the secure tunnel to be re-directed over an insecure interface.
It is recommended to leave this setting un-ckecked unless there is a specific requirement for it to be set.

Once configuration is complete on this page click the Next button to move the next page.

11.1.2.7 Tunnel Networks

The tunnel network page is used to configure the way in which the IPsec tunnel is terminated. The IPsec tunnel can be terminated at each end in one of two ways: host and network. In a host connection the tunnel is connected to a single IP address. In a network connection the tunnel is connected to a network subnet. The tunnel network table allows the connections for each end of the tunnel to be defined. Figure 253 is an example of the Tunnel Networks page.

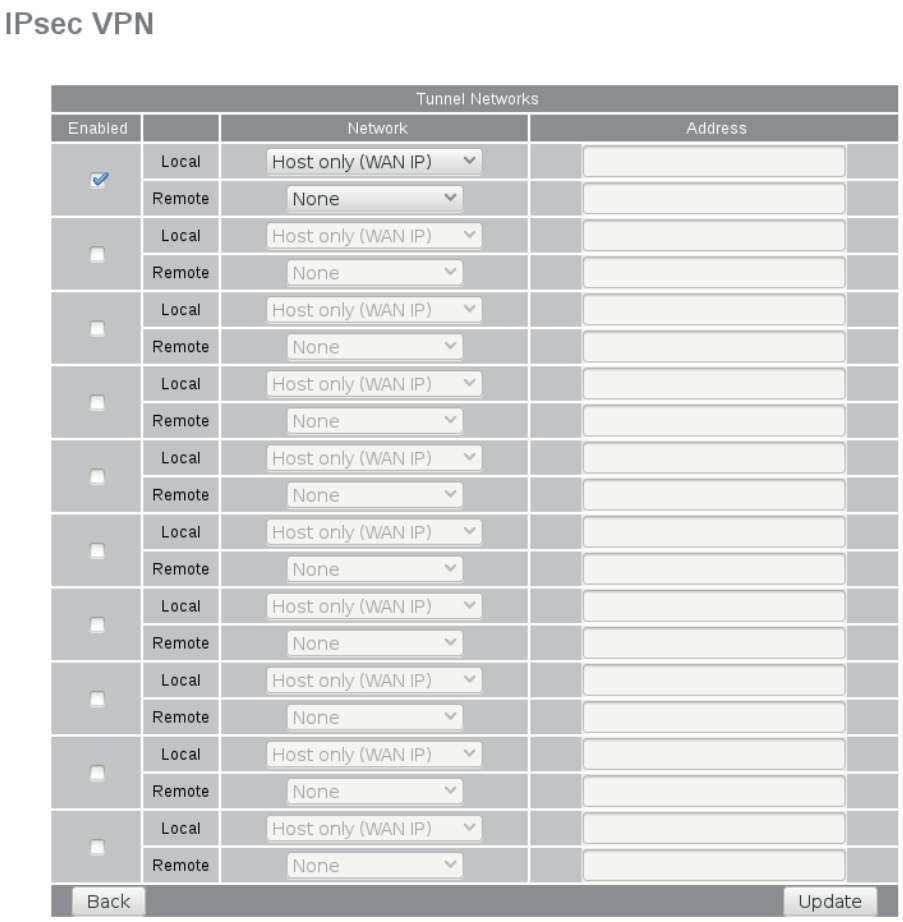


Figure 253: IPsec Tunnel networks.

The options are as follows:

Enabled Check to enable tunnel network definition.

Local Configure the local connection:

Network **Host only (WAN IP)** The tunnel is connected in host mode. The IP address will be that of the wireless interface. This may not be desirable if the wireless interface is assigned a dynamic IP address as the remote end will not know the IP address and so will not be able to route traffic to it.

Host only (LAN IP) The tunnel is connected in host mode. The IP address will be that of the LAN interface.

Host only (Loopbacl) The tunnel is connected in host mode. The IP address will be that of the Loopback interface.

Virtual Host The tunnel is connected in host mode. The IP address will be that set in the address field.

LAN subnet The tunnel is connected in network mode to the LAN subnet.

Specify a subnet The tunnel is connected in network mode to the specified subnet.

All traffic All local traffic is directed to the IPsec interface

Address For host connections enter an IP address. For network connections enter an network IP address including netmask, for example 10.10.10.0/24.

Remote Configure the local connection:

Network **None** The tunnel is connected in host mode.

Specify a subnet The tunnel is connected to the specified subnet.

All traffic All traffic is directed to the IPsec tunnel.

Address For host connections enter an IP address. For network connections enter an network IP address including netmask, for example 10.10.10.0/24.

When the configuration is complete click the Update button to add the tunnel. The main IPsec page will be displayed and the new tunnel will be added to the Tunnels table.

11.1.3 IPsec configuration example

The following example demonstrates how to add an IPsec tunnel which will connect to a remote router. Figure 254 illustrates the connection which will be created in the example. The modem is configured for a standard Internet connection, this means that the IP address assigned to it will be dynamic and private. The example assumes that the router has been configured, has a static IP address and is directly accessible from the Internet. The IPsec tunnel will be terminated as a virtual host on the unit with IP address 11.22.33.44 and will be terminated on a LAN subnet at the router with address 192.168.2.0/24

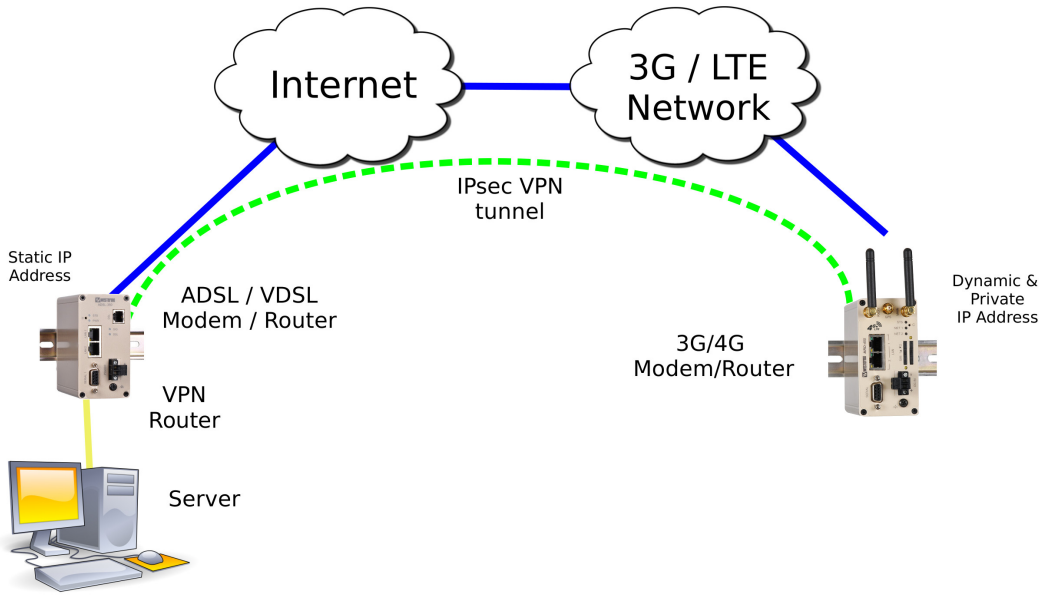


Figure 254: IPsec configuration example network

11.1.3.1 General Configuration

To start, select the IPsec main page by first clicking VPN ▹ IPsecVPN. Click the the Add new tunnel group button. The first page of the IPsec tunnel configuration pages will be displayed, as shown in Figure 255.

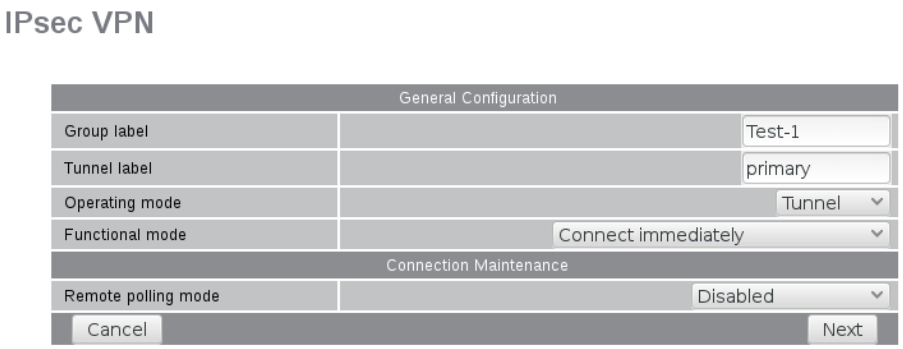


Figure 255: IPsec general configuration example.

The tunnel will be named *Test*. It will operate in **Tunnel** mode and will act as the initiator. The configure settings required are:

General Configuration **Group label:** Test-1
Tunnel label primary
Operating mode: Tunnel
Functional mode Connect immediately

Connection Maintenance **Remote polling mode** Disabled

Once entered click the Next button to continue to the next page.

11.1.3.2 Physical Configuration

The physical configuration page will now be displayed. Figure 256 illustrates this page with the values for the example entered.

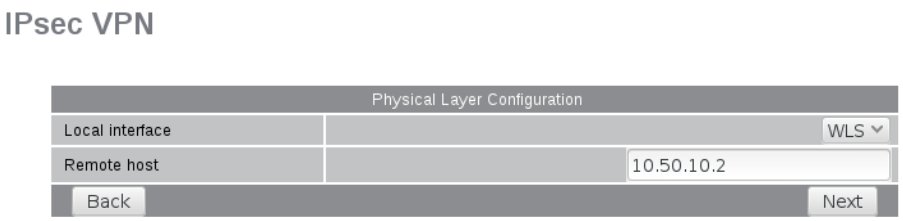


Figure 256: IPsec Physical configuration example.

The tunnel is to be configured to use the wireless port and to connect to the remote host address of 123.123.123.123. The settings required are:

Physical Layer Configuration Local interface WLS

Remote host 123.123.123.123

Once entered click the Next button to continue to the next page.

11.1.3.3 Phase 1 Configuration

The Phase 1 Configuration page with the settings required for this example is shown in Figure 257. In this phase the authentication method is set to pre-shared keys and the key entered. The remote ID is xy.example.com and local ID is ab.example.com. As the wireless IP address is dynamic and private the network provider will use Network Address Translation (NAT) so main mode cannot be used for the negotiation mode requiring the negotiating mode to be set to aggressive mode. The IKE proposal will use AES 128 bit as the encryption algorithm, SHA1 for authentication and Diffie-Hellman group 2. The IKE lifetime will be left at the default value of 60 minutes.

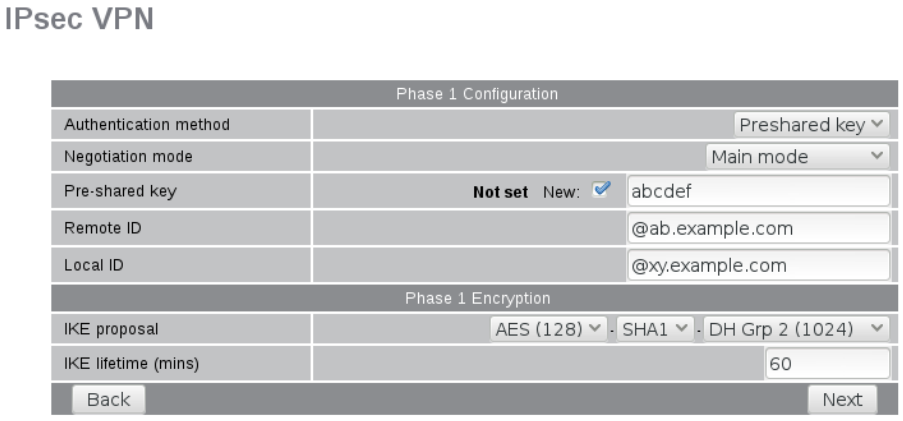


Figure 257: IPsec phase 1 configuration example.

The required parameters are as follows:

Phase 1 Configuration section

Authentication method: Pre-shared key

Negotiation mode: Aggressive mode

Pre-shared key: New: Checked

key: abcdef

Remote ID: @ab.example.com

Local ID: @xy.example.com

Phase 1 Encryption section

IKE proposal: Encryption Algorithm: AES (128)

Authentication Algorithm: SHA1

Diffie-Hellman Group: DH Grp 2 (1024)

IKE lifetime (mins): 60

Once entered click the Next button to continue to the next page.

Phase 2 Configuration

The Phase 2 Configuration page with the settings required for this example is shown in Figure 258. For the Phase 2 configuration enhanced authentication will not be used, the ESP proposal encryption algorithm is set to AES 128 bit and the authentication algorithm set to SHA1. Perfect forward secrecy is enabled and set to Diffie-Hellman group 2, the key lifetime will left at the default value of 480 minutes.

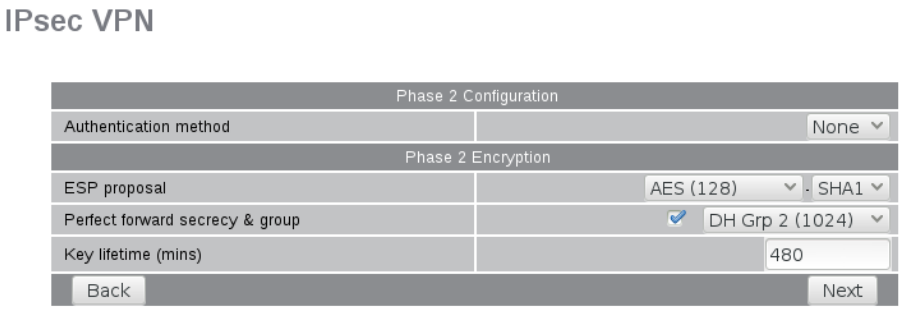


Figure 258: IPsec phase 2 configuration example.

The configuration requires the following parameters to be entered:

Phase 2 Configuration section

Authentication method None

Phase 2 Encryption section

ESP proposal: Encryption Algorithm: AES (128)

Authentication Algorithm: SHA1

Perfect forward secrecy & group: Perfect forward secrecy: Off (un-checked)

Diffie-Hellman Group: DH Grp 2 (1024) (Non-selectable default value)

Key lifetime (mins): 480

Once entered click the Next button to continue to the next page.

11.1.3.4 Tunnel Options & Dead Peer Detection

The Tunnels Options & Dead Peer Detection page with the settings required for this example is shown in Figure 259. The re-keying options are left at the default values. Dead peer detection is enabled with the action set to clear the delay and timeout values are set to 30 and 120 seconds respectively.

The local tunnel will be configured as a virtual host with the IP address 11.22.33.44 and the remote connection will be to the LAN 192.168.2.0/24.

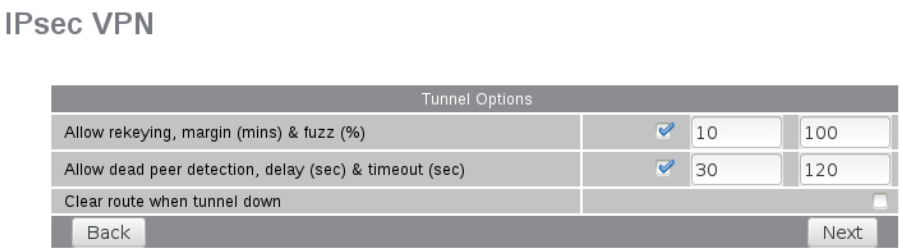


Figure 259: IPsec tunnel options and Dead Peer Detection configuration example.

The configuration requires the following parameters to be entered:

Tunnel Options

Allow rekeying, margin (mins) & fuzz: Enable Checked to enable.

Margin 10 Minutes.

Fuzz 100%.

Allow dead peer detection, delay (sec) & timeout (sec) Enable Check to enable.

Delay 30.

Timeout 120.

Clear route when tunnel down Un-check.

Once entered click the Next button to continue to the next page.

11.1.3.5 Tunnel Networks

The Tunnel Networks page with the settings required for this example is shown in Figure 258. The local tunnel will be configured as a virtual host with the IP address 11.22.33.44 and the remote connection will be to the LAN 192.168.2.0/24.

The for this configuration the following parameters are entered:

Enabled Checked

Local: Network: Virtual Host

Address: 11.22.33.44

Remote: Network: Specify a subnet

Address: 192.168.2.0/24

To complete the process of adding the tunnel click the Update button . The tunnel will be saved and the General IPsec Configuration page will again be displayed, now with the new tunnel added to the Tunnels table, as shown in Figure 261.

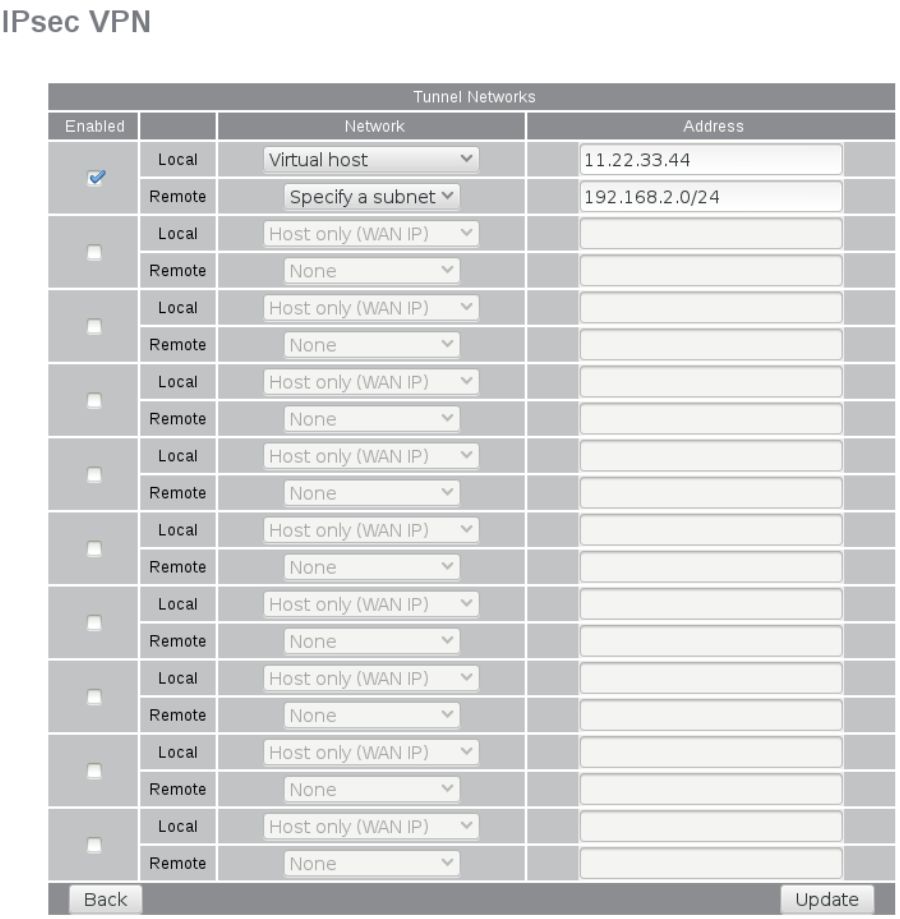


Figure 260: IPsec Tunnel Options configuration example.

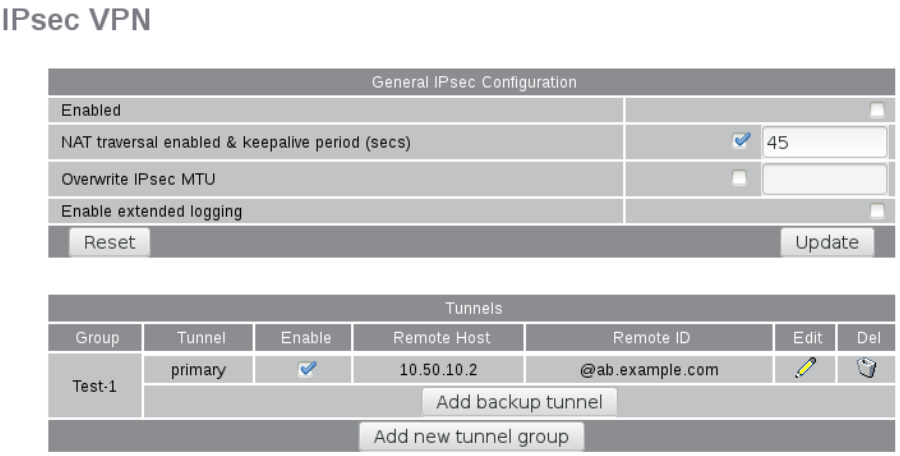


Figure 261: IPsec table with the newly created entry.

11.1.3.6 Enable IPsec

To complete the configuration in the General IPsec Configuration enable IPsec by checking the **Enabled** check-box and enable **NAT traversal**.

Click the Update button to save the settings.

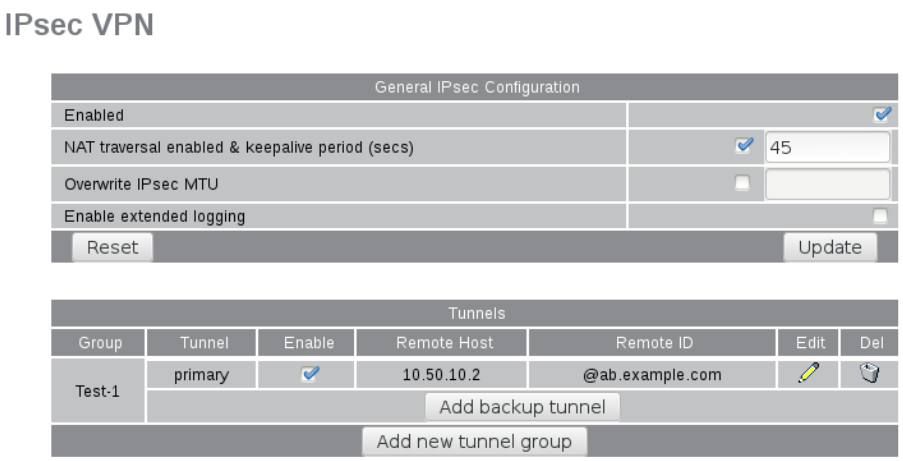


Figure 262: IPsec based VPN main page, with IPsec enabled.

11.1.3.7 IPsec Status

Once the settings have been saved IPsec will start and attempt to establish a tunnel with the remote host. Note that this may take several minutes to complete. To check the status of the tunnel click Status ▷ VPN. A page similar to that shown in Figure 263will be displayed. If the status of the tunnel is **Connected** then the tunnel has been established and data can be passed over it.

To obtain further details on the VPN connection click the link **Detailed IPsec status**. A page similar to that shown in Figure 264 will be displayed. This information is usually only required if the link is not behaving as expected or if the tunnel is not able to be established.

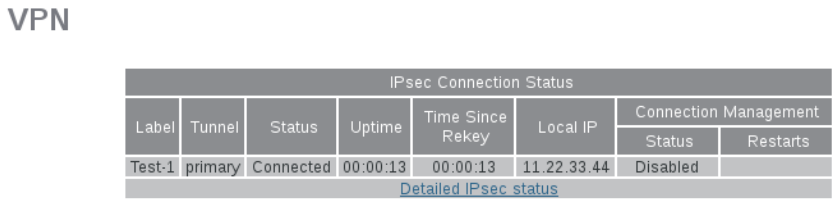


Figure 263: IPsec connection status

The status web pages do not automatically refresh so it may be necessary to refresh the page to obtain the current status.

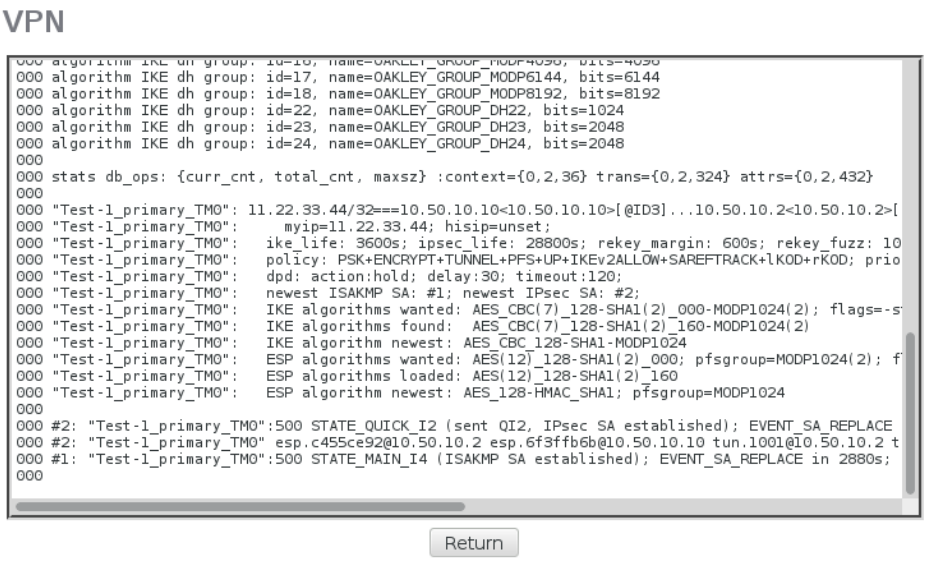


Figure 264: IPsec connection status detail

When the detailed page is selected or refreshed it will automatically scroll to the last entry in the log. To view earlier entries the right hand scroll bar can be used.

11.1.4 Adding a Backup Tunnel

A backup tunnel can be added once a tunnel group and primary tunnel have been defined. The backup tunnel will be used when the primary connection cannot be established.

To add a backup tunnel click the Add backup tunnel button within the tunnel group in which the tunnel is to be added. A page similar to that shown in figure 265 will be displayed.

A Add backup tunnel button will be present in each configured tunnel group. To add a backup tunnel within a group click the button which appears as part of that group in the table.

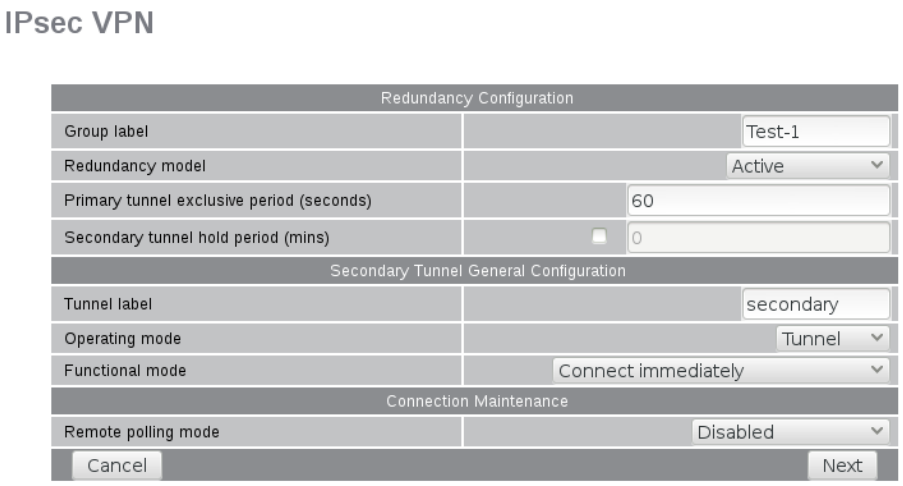


Figure 265: Adding a backup IPsec tunnel.

The options vary between redundancy operating modes, the passive modes are Rotate and Try Primary First and the active mode is Active. The active redundancy options are shown in figure 265 and the passive options are shown in figure 266.

Redundancy Configuration Group label The group label for the tunnel group. This will match the tunnel group for which the Add backup tunnel button was pressed.

Redundancy model Rotate (Passive_redundancy) When either primary or secondary connections fail the other will be tried until a connection is established.

Try primary first (Passive_redundancy) When either primary or secondary tunnels fail try the primary first then the secondary until a connection is established.

Active (Active_redundancy) If the secondary tunnel has a connection established attempt to establish the primary connection in the background. If the connection to the primary is then established switch to the primary and disconnect the secondary.

Reconnect period (Passive_redundancy) Time to wait from a connection failure to attempting to establish a connection on the other tunnel.

Primary tunnel exclusive period (Active redundancy) The time after start-up for which the primary tunnel only will attempt to establish a connection. Once this time has expired if the primary has not connected to secondary will also be tried.

Secondary tunnel hold period Enable Check to enable

Period Passive redundancy the time before disconnecting the backup tunnel and going back to the primary tunnel.

Active redundancy the time before the primary tunnel attempts to reconnect.

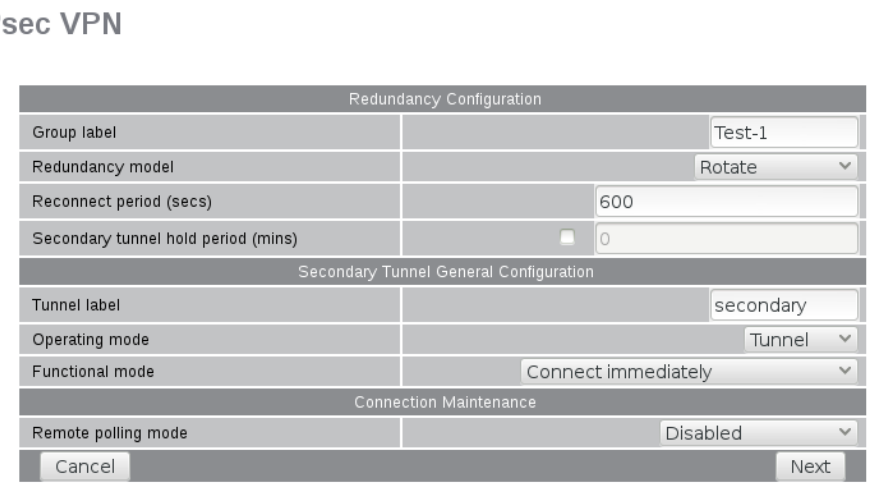


Figure 266: Adding a backup IPsec tunnel.

Secondary Tunnel General Configuration IPsec general configuration for the backup IPsec tunnel. The options are as follows:

Tunnel label Set the label or name for the tunnel within the group. This is used to distinguish between tunnels for example 'primary' and 'secondary'

Operating mode Select the operating mode of the IPsec tunnel from the following options:

Tunnel Tunnel mode encapsulates the entire IP packet to provide a secure connection between two gateways. In tunnel mode the payload, the header and the routing information are all encrypted, and then encapsulated into a new IP packet. This mode is generally used to create a VPN.

Transport Transport mode provides a secure connection between two hosts. Only the payload of the IP packet is encrypted.

Functional mode Select the functional mode of the IPsec tunnel from the following options:

Connect immediately The tunnel will be initiated, that is it will attempt to establish a connection with a remote responder.

Responder or Connect on demand Wait for and respond to incoming connections or if no active connection, establish a connection to a remote server.

Connection Maintenance IPsec connection maintenance options:

Remote polling mode Disabled No remote polling

Poll_at_fixed_interval Enable polling, the following options will appear when selected:

Poll period Specify the time interval in seconds between polls. Minimum value of 15 seconds.

Retry period Check to enable and specify the time in seconds to retry the poll after a failed poll. Minimum value of 15 seconds.

Failed establishment polls before restarting connection Specify the number of failed establishment polls to declare the connection down and to re-start the establishment process.

Failed polls before restarting connection Specify the number of failed polls to declare the connection down and to re-start the establishment process.

Poll type Specify the poll type. The options are:

Ping (ICMP) Ping the specified address.

TCP Socket Establish a TCP socket to the specified address and port number. The connection will be terminated as soon as successfully opened.

Poll address Specify the IP address to poll.

Once configuration is complete on this page click the Next button to move to the next page.

The remaining options are the same as when configuring a primary tunnel. The next page will be the Physical Layer Configuration to continue the configuration go to Section 11.1.2.1 and continue through the configuration pages.

11.1.5 Example of Adding a Backup IPsec Tunnel

The following example demonstrates how to add a backup IPsec tunnel to the configuration described in IPsec configuration example. The backup IPsec tunnel will be terminated as a virtual host on the unit with IP address 11.22.33.44 and will be terminated on a LAN subnet at the router with address 192.168.2.0/24

11.1.5.1 General Configuration

To start, select the IPsec main page by first clicking VPN ▷ IPsecVPN. Click the the Add backup tunnel button within the group Test-1 in the tunnels table. The first page of the IPsec tunnel configuration pages will be displayed, as shown in Figure 267.

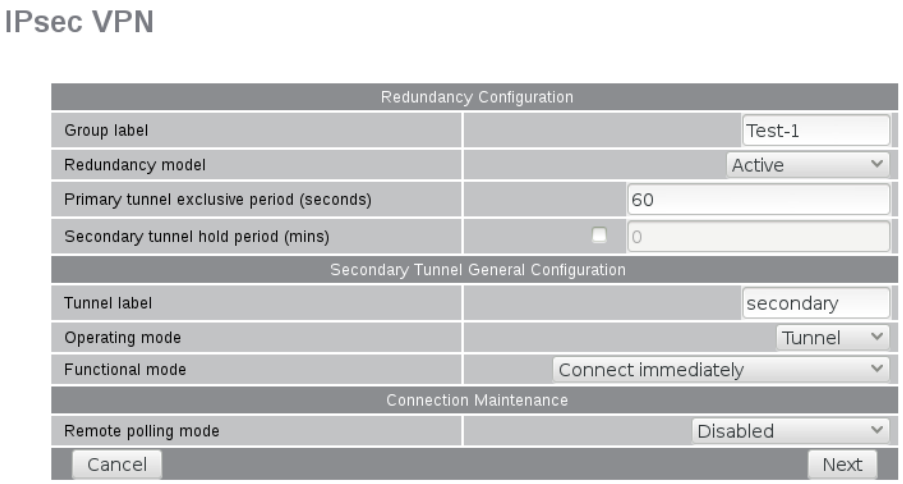


Figure 267: Backup IPsec tunnel configuration example.

The configuration is such that the Primary tunnel should be use whenever possible, so the redundancy model will be active with the secondary hold time disabled. The backup tunnel is to be called secondary, it will operate in **Tunnel** mode and will act as the initiator. The configure settings required are:

Redundancy Configuration Group label: Test-1

Redundancy model Active

Primary tunnel exlusive period 60

Secondary tunnel hold time Disabled

Secondary Tunnel General Configuration Tunnel label secondary

Operating mode: Tunnel

Functional mode Connect immediately

Connection Maintenance Remote polling mode Disabled

Once entered click the Next button to continue to the next page.

11.1.5.2 Physical Configuration

The physical configuration page will now be displayed. Figure 268 illustrates this page with the values for the example entered.

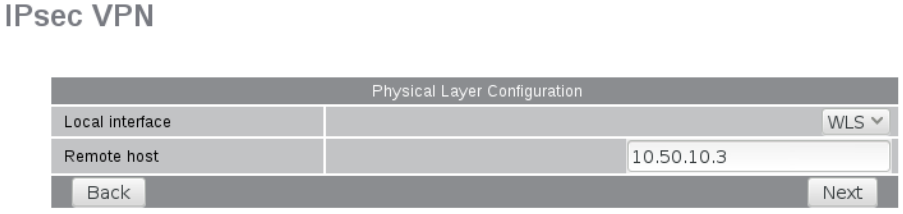


Figure 268: IPsec Physical configuration example.

The tunnel is to be configured to use the wireless port and to connect to the remote host address of 123.123.123.124. The settings required are:

Physical Layer Configuration Local interface WLS

Remote host 123.123.123.124

Once entered click the Next button to continue to the next page.

11.1.5.3 Phase 1 Configuration

The Phase 1 Configuration page with the settings required for this example is shown in Figure 269. In this phase the authentication method is set to pre-shared keys and the key entered. The remote ID is xy.example.com and local ID is ab.example.com. As the wireless IP address is dynamic and private the network provider will use Network Address Translation (NAT) so main mode cannot be used for the negotiation mode requiring the negotiating mode to be set to aggressive mode. The IKE proposal will use AES 128 bit as the encryption algorithm, SHA1 for authentication and Diffie-Hellman group 2. The IKE lifetime will be left at the default value of 60 minutes.

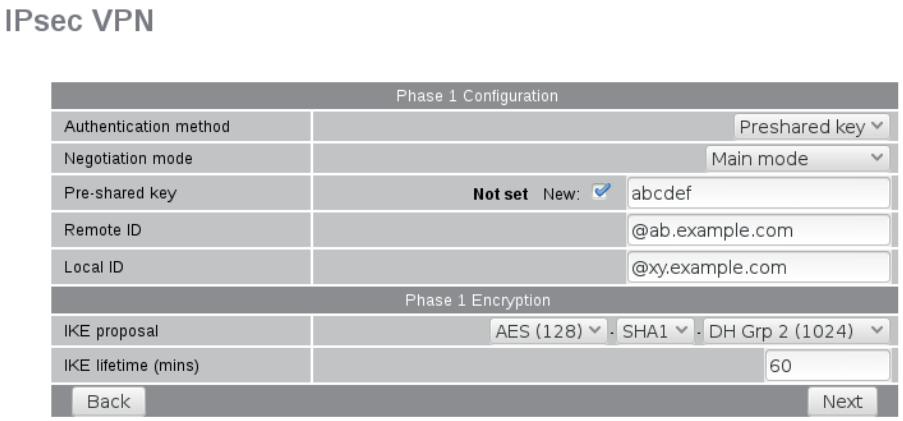


Figure 269: IPsec phase 1 configuration example.

The required parameters are as follows:

Phase 1 Configuration section

Authentication method: Pre-shared key

Negotiation mode: Aggressive mode

Pre-shared key: New: Checked

key: abcdef

Remote ID: @ab.example.com

Local ID: @xy.example.com

Phase 1 Encryption section

IKE proposal: Encryption Algorithm: AES (128)

Authentication Algorithm: SHA1

Diffie-Hellman Group: DH Grp 2 (1024)

IKE lifetime (mins): 60

Once entered click the Next button to continue to the next page.

Phase 2 Configuration

The Phase 2 Configuration page with the settings required for this example is shown in Figure 270. For the Phase 2 configuration enhanced authentication will not be used, the ESP proposal encryption algorithm is set to AES 128 bit and the authentication algorithm set to SHA1. Perfect forward secrecy is enabled and set to Diffie-Hellman group 2, the key lifetime will left at the default value of 480 minutes.

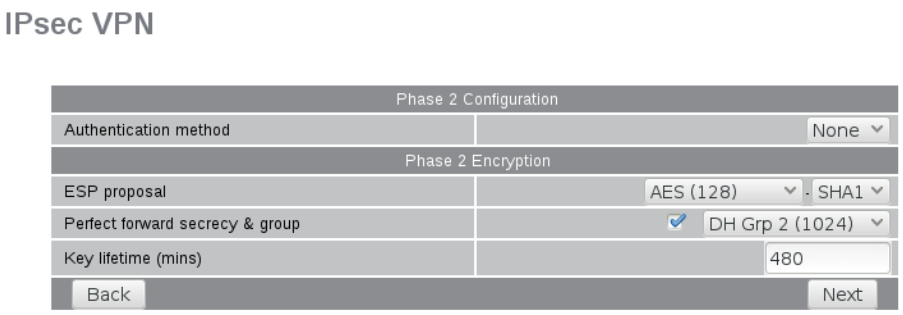


Figure 270: IPsec phase 2 configuration example.

The configuration requires the following parameters to be entered:

Phase 2 Configuration section

Authentication method None

Phase 2 Encryption section

ESP proposal: Encryption Algorithm: AES (128)
Authentication Algorithm: SHA1

Perfect forward secrecy & group: Perfect forward secrecy: Off (un-checked)
Diffie-Hellman Group: DH Grp 2 (1024) (Non-selectable default value)

Key lifetime (mins): 480

Once entered click the Next button to continue to the next page.

11.1.5.4 Tunnel Options & Dead Peer Detection

The Tunnels Options & Dead Peer Detection page with the settings required for this example is shown in Figure 271. The re-keying options are left at the default values. Dead peer detection is enabled with the action set to clear the delay and timeout values are set to 30 and 120 seconds respectively.

The local tunnel will be configured as a virtual host with the IP address 11.22.33.44 and the remote connection will be to the LAN 192.168.2.0/24.

The configuration requires the following parameters to be entered:

Tunnel Options

Allow rekeying, margin (mins) & fuzz: Enable Checked to enable.

Margin 10 Minutes.

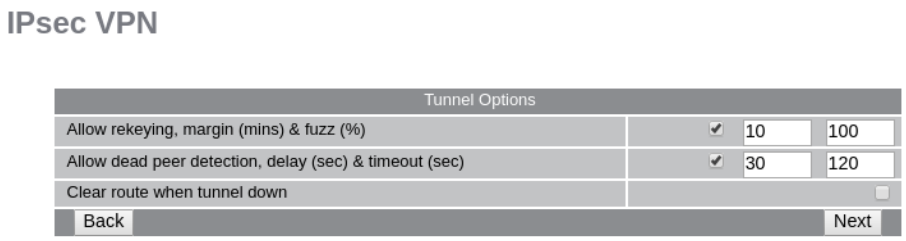


Figure 271: IPsec tunnel options and Dead Peer Detection configuration example.

Fuzz 100%.

Allow dead peer detection, delay (sec) & timeout (sec) Enable Check to enable.

Delay 30.

Timeout 120.

Clear route when tunnel down Un-check.

Once entered click the Next button to continue to the next page.

11.1.5.5 Tunnel Networks

The Tunnel Networks page with the settings required for this example is shown in Figure 270. The local tunnel will be configured as a virtual host with the IP address 11.22.33.44 and the remote connection will be to the LAN 192.168.2.0/24.

The for this configuration the following parameters are entered:

Enabled Checked

Local: Network: Virtual Host

Address: 11.22.33.44

Remote: Network: Specify a subnet

Address: 192.168.2.0/24

To complete the process of adding the tunnel click the Update button . The tunnel will be saved and the General IPsec Configuration page will again be displayed, now with the backup tunnel added to the tunnel group in the Tunnels table, as shown in Figure 273.

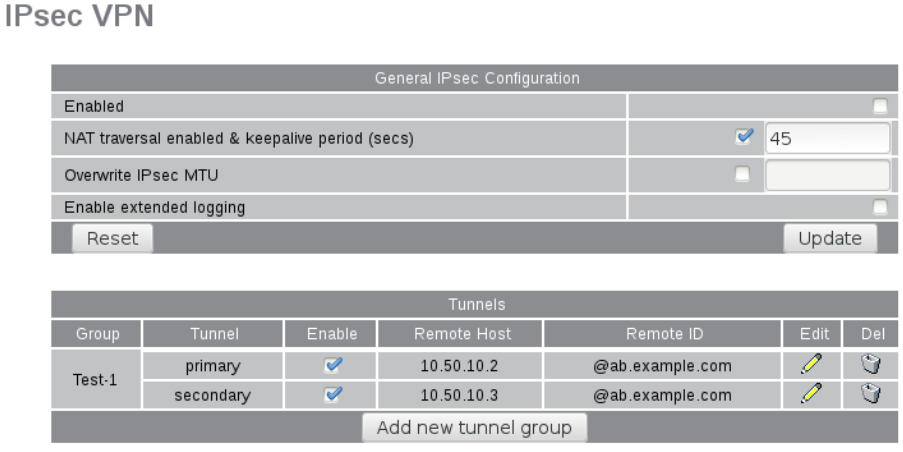


Figure 273: IPsec table with the newly created entry.

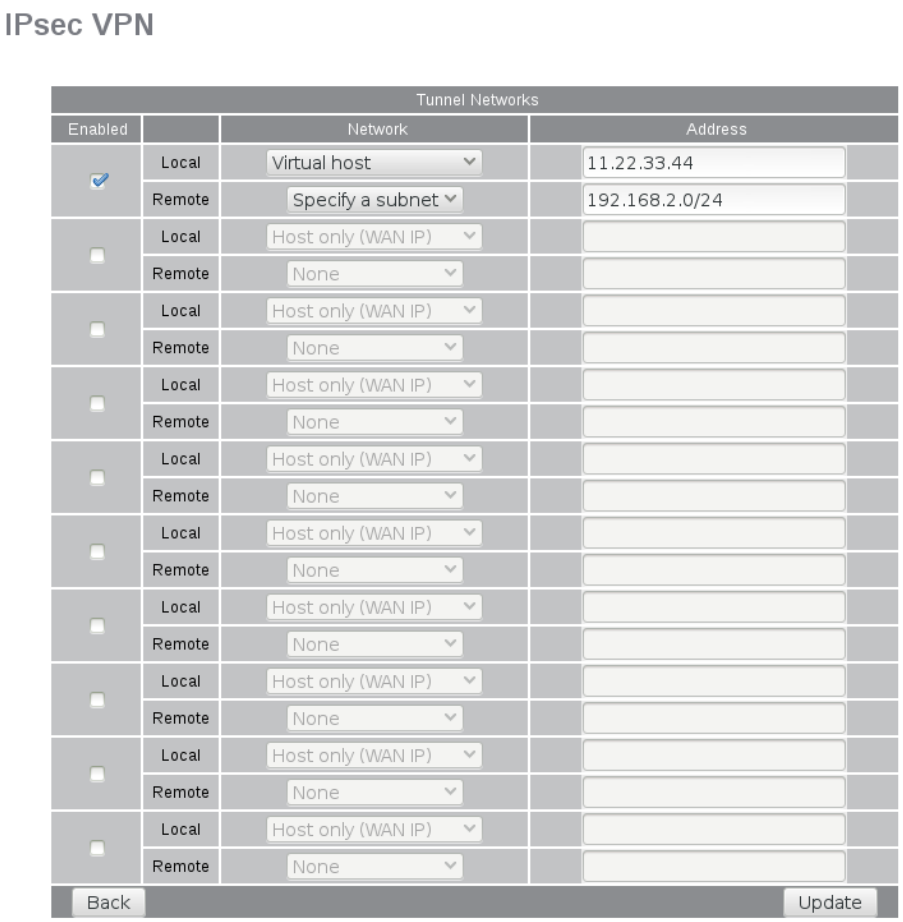


Figure 272: IPsec Tunnel Options configuration example.

11.1.6 Editing an IPsec Tunnel

To edit an IPsec tunnel click the icon in the Edit column in the row of the tunnel to be edited. The process of editing is similar to that of adding a tunnel described in Adding an IPsec tunnel.

11.1.7 Deleting an IPsec Tunnel

To delete an IPsec tunnel click the icon in the Del column in the row of the tunnel to be deleted.

11.1.8 Example of Deleting an IPsec Tunnel

To delete the backup tunnel created in the previous example click the icon in the Del column of the tunnel called secondary in the group Test-1. A pop-up box will be displaye requesting confirmation, as shown in figure 274

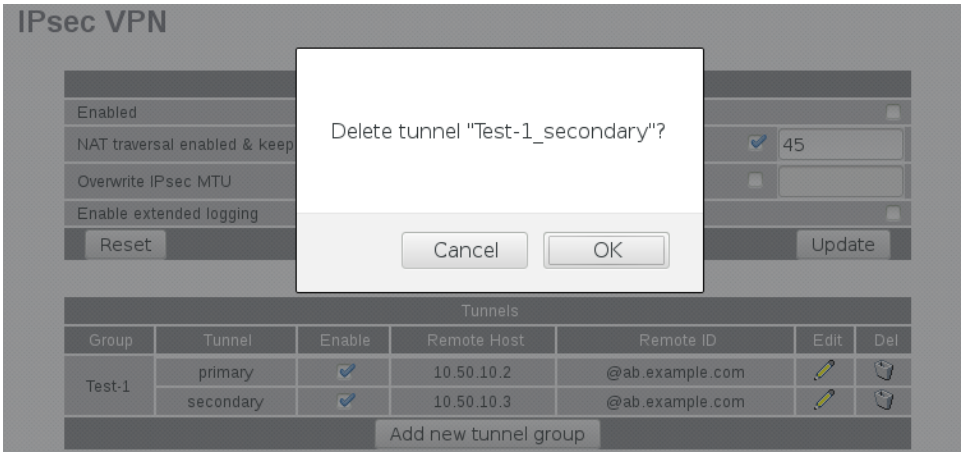


Figure 274: Deleting the backup IPsec tunnel 'secondary'.

Click the OK button to confirm the deletion. The page will update and the secondary tunnel will be removed from the Tunnels table, as shown in figure 275.

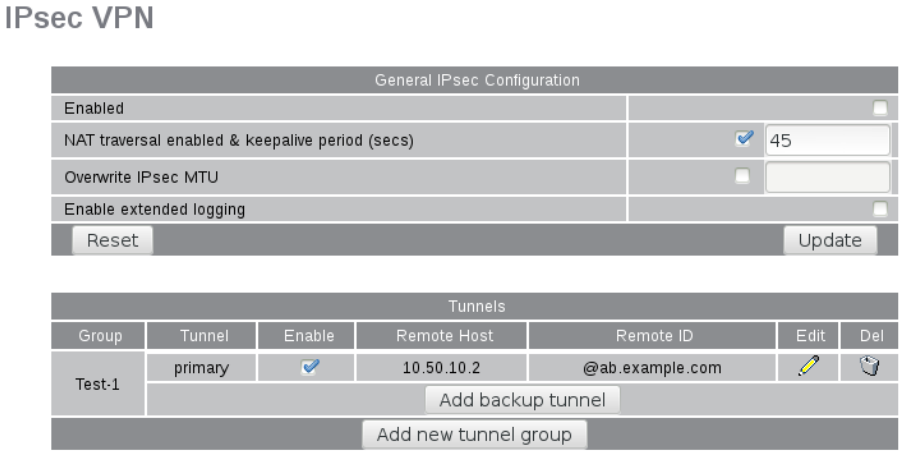


Figure 275: IPsec tunnels table after deleting the 'secondary' tunnel.

11.2 Secure Sockets Layer (SSL) VPN

Secure Sockets Layer (SSL) are cryptographic protocols that provide secure communications over a communications network. SSL operates at the transport layer (layer 4 of the OSI model). This means that it is can be used to create a tunnel through which other layer 4 protocols such as TCP and UDP can pass.

The SSL VPN implementation in the modem is OpenVPN. OpenVPN which is a free and open source virtual private network (VPN) program for creating point-to-point or server-to-multiclient encrypted tunnels. It is capable of establishing direct links between computers that are behind NAT firewalls. For information on installing and configuring OpenVPN refer to the OpenVPN website `http://openvpn.net/`.

11.2.1 SSL VPN configuration

To access the SSL VPN configuration page, select VPN ▸ SSL VPN a page similar to that shown in Figure 276 will be displayed.

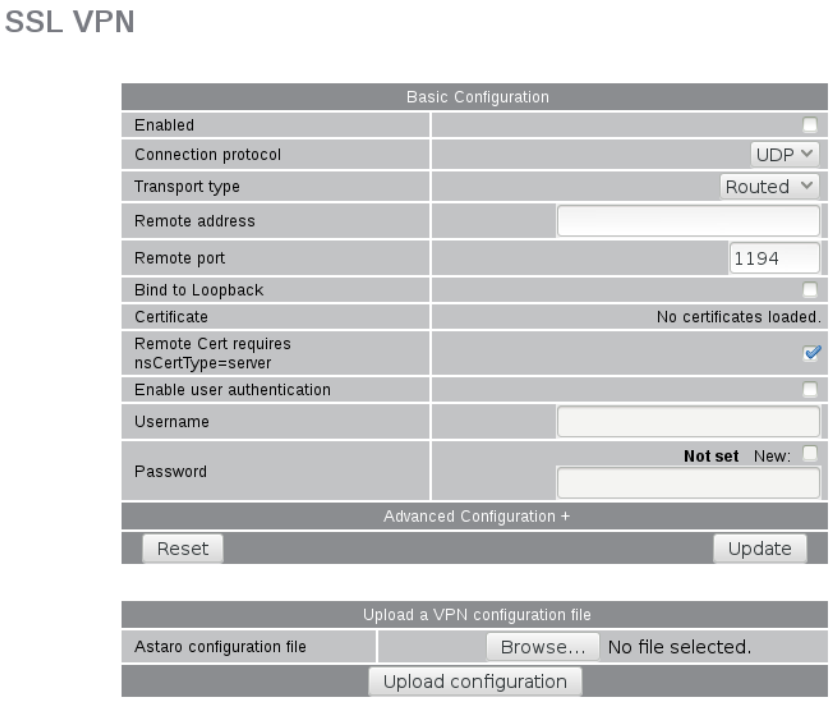


Figure 276: SSL based VPN configuration web page.

The configuration options are divided into **Basic Configuration** in the upper section of the page and optional **Advanced Configuration** in the lower section of the page.

Basic Configuration The Basic Configurations options are as follows:

Enabled Check the box to enable the SSL VPN.

Connection Protocol The protocol used will be must match the configuration of the remote VPN server this tunnel will be established to. Select **UDP** or **TCP** as appropriate. Default is UDP.

Transport Type Select the transport type. The transport used must match the configuration of the remote VPN server.

Bridged Bridging is a technique for creating a virtual, wide-area Ethernet LAN, running on a single subnet. The advantages of bridging are broadcasts will transverse the VPN which in same situations is desirable, and no routing rules are required. The disadvantages are broadcasts can be problematic on a wireless network as the over-the-air traffic is increased and bridging does not scale well as new devices are added to the network.

Routed Routing will create a separate subnet for each VPN connection. To access one subnet from another requires routing rules to be configured at the VPN router. The advantages of routing are efficiency, scalability and no broadcast traffic. This is particularly important with wireless networks to reduce the over-the-air traffic. The disadvantage is that routing rules are required which adds to the configuration.

Remote address Specify the address of the remote VPN server.

Remote port Specify the port number of the remote VPN server. The default OpenVPN port number is 1194.

Bind to Loopback Check to bind the service to the loopback port. Refer to section 8.3 for details on configuring the loopback interface.

Certificate Specify the certificate to use for authentication. For details on how to load certificates refer to Section 11.5 Certificate Management.

Remote Cert requires nsCertType=server The server certificate may have the ns Cert Type set to server. If this is the case this Check to enable this parameter.

Enable user authentication Check to enable user authentication

Username The user name to use for authentication.

Password The password to use for authentication.

Click the Update button to save and commit changes.

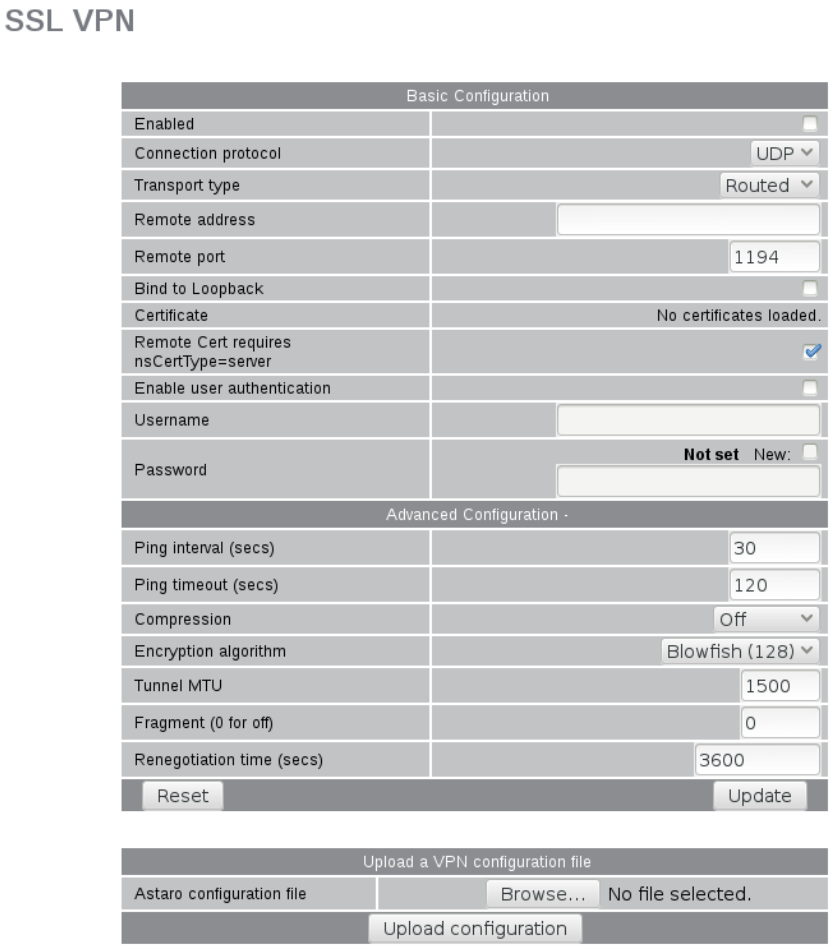


Figure 277: SSL based VPN configuration web page showing advanced options.

Advanced Configuration The advanced options provide more control of the VPN. For most applications the default options do not need to be changed. To access the advanced configuration options click the *Advanced Configuration* + title, the advanced options will then drop down as shown in Figure 277. The Advanced Configurations options are as follows:

Ping interval (secs) Specify the interval in seconds at which to ping the remote server. This is used to determine the status of the connection.

Ping timeout (secs) Specify the ping time-out in seconds. This is used to determine if the VPN connection has terminated. If this time is exceeded without receiving a ping response from the server the connection will be re-established.

Compression Specify if compression is to be used for the data being transmitted through the VPN tunnel. This must match the compression setting at the remote VPN server. Select one of the following options from the drop-down list:

Off Compression is disabled.

Adaptive The performance will be measured with compression on and with compression off, the option with the higher performance will be selected.

On Compression is enabled.

Encryption algorithm Specify the encryption algorithm to use from the drop-down list. The options are:

DES Data Encryption Standard.

3DES (192) 192 bit Triple Data Encryption Standard.

Blowfish (128) 128 bit Blowfish (Default).

AES (128) 128 bit Advanced Encryption Standard (AES).

AES (192) 192 bit Advanced Encryption Standard (AES).

AES (256) 256 bit Advanced Encryption Standard (AES).

Tunnel MTU Specify the MTU of the tunnel.

Fragment (0 for off) Used for UDP only. Meant as a last resort when MTU path discovery does not work.

Renegotiation time (secs) The time at which the data channel key will be renegotiated.

Click the Update button to save and commit changes.

Upload a VPN configuration file VPN Configuration files of the following types may be uploaded to the unit:

Astaro configuration file A configuration file generated by an Astaro Security Gateway Appliance.

Privonet configuration file A configuration file for the Privonet service. `http://www.privonet.com.au`

Click the Choose file button to select the configuration file, then click the Upload configuration button to upload the configuration file to the unit.

11.2.2 Connecting to a VPN server

This section describes an example of connecting to a VPN server. Figure 278 illustrates the network which will be established. For this example a connection will be established from the unit to an OpenVPN server using a routed connection and UDP as the connection protocol. The IP address of the OpenVPN server is 123.123.123.123 and the port number is 1194. The certificate supplied for authentication is called *demoClient*. To ensure the connection remains connected the ping interval will be set to 30 seconds with a time-out of 120 seconds. Compression will be disabled and the Encryption algorithm will 128 bit Blowfish.

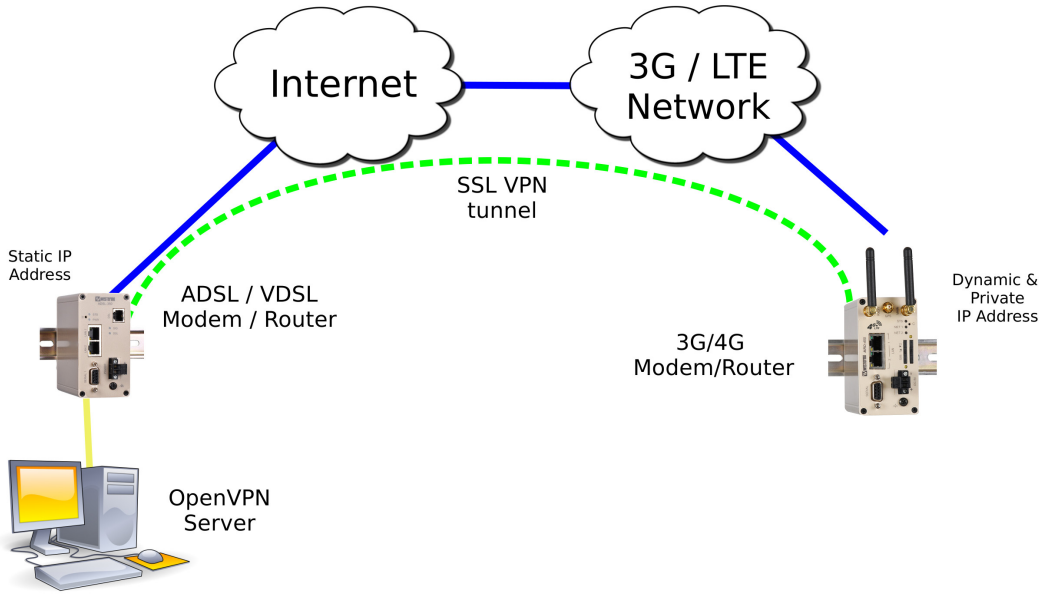


Figure 278: SSL based VPN example network

Select **VPN** on the main menu to display the the *SSL VPN* configuration page. Figure 279 shows the SSL VPN configuration page with the options set for the example.

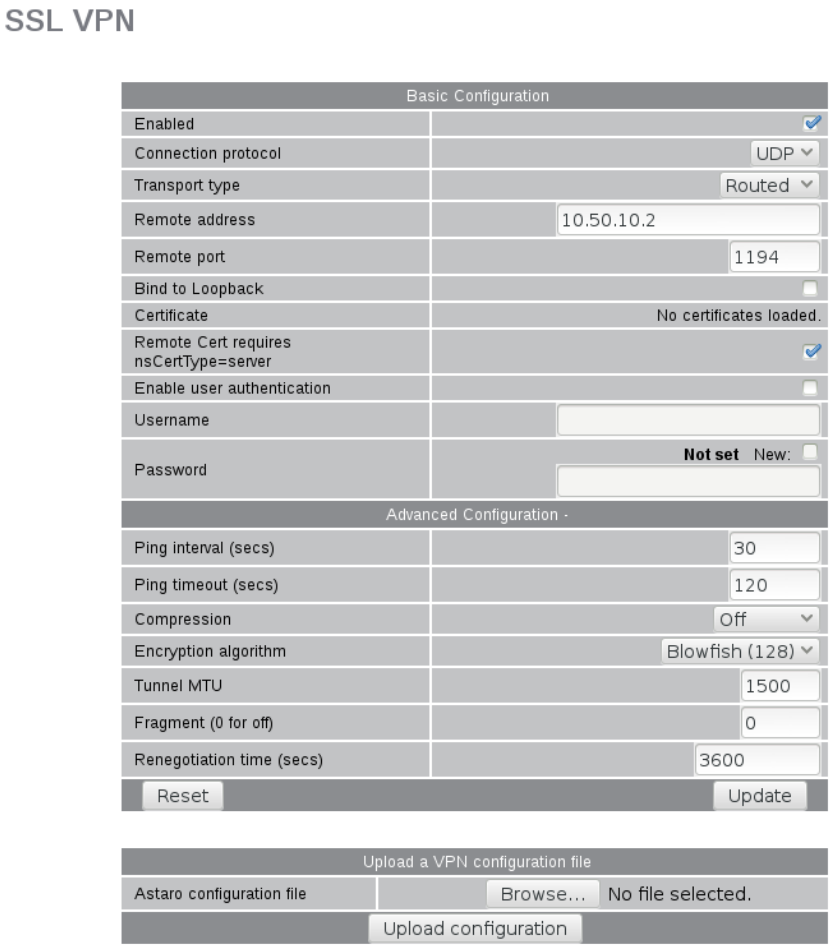


Figure 279: SSL based VPN configuration web page

The following are configuration settings used for the example:

Basic Configuration options Enabled: Checked

Connection Protocol: UDP

Transport Type: Routed

Remote address: 123.123.123.123

Remote port: 1194

Bind to Loopback Un-checked.

Certificate: demoClient

Remote Cert requires nsCertType=server Checked.

Enable user authentication: Un-checked

Username: Not required. Leave blank.

Password: Not required. Leave blank.

Advanced Configuration options Ping interval (secs): 30

Ping timeout (secs): 120

Compression Off

Encryption algorithm Blowfish (128)

Tunnel MTU: 1500

Fragment (0 for off): 0

Renegotiation time (secs): 3600

Once the configuration has been completed click the Update button to save the changes.

The SSL VPN will now be started and it will attempt to establish a connection with the VPN server specified. The status of the VPN can be checked on the VPN status page. To access this page click Status ▷ VPN page similar to that shown in Figure 280 will be shown. This page indicates that the VPN is connected and lists the local IP address.

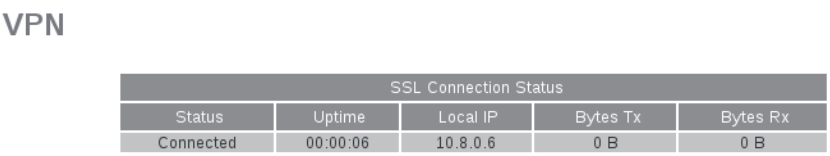


Figure 280: SSL VPN status page

In order to test the VPN a ping command can be run from a machine connected to the VPN server. The following is the result of the ping:

```
$ ping 10.90.91.30
PING 10.90.91.30(10.90.91.30) 56(84) bytes of data.
64 bytes from 10.90.91.30: icmp_seq=1 ttl=62 time=141 ms
64 bytes from 10.90.91.30: icmp_seq=2 ttl=62 time=122 ms
64 bytes from 10.90.91.30: icmp_seq=3 ttl=62 time=120 ms
64 bytes from 10.90.91.30: icmp_seq=4 ttl=62 time=121 ms
64 bytes from 10.90.91.30: icmp_seq=5 ttl=62 time=121 ms
64 bytes from 10.90.91.30: icmp_seq=6 ttl=62 time=122 ms
64 bytes from 10.90.91.30: icmp_seq=7 ttl=62 time=123 ms
--- 10.90.91.30 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 5998ms
rtt min/avg/max/mdev = 120.620/124.725/141.429/6.867 ms
$
```

The unit has responded to the ping and the byte counters on the status page have increased as seen in Figure 281

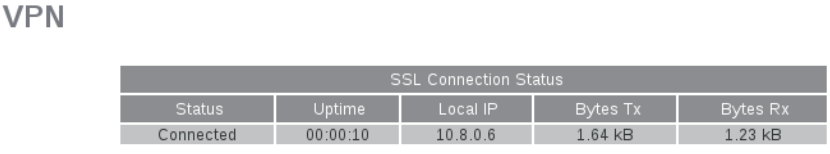


Figure 281: SSL VPN status after running Ping, the byte counts have increased

The VPN is now operational as can be used to pass data.

11.3 PPTP and L2TP

11.3.1 Point-to-Point-Tunneling-Protocol

The Point-to-Point-Tunneling-Protocol (PPTP) is used for establishing Virtual Private Network (VPN) tunnels over an insecure network such as the Internet. PPTP uses a client-server model for establishing the VPN. The unit provides a PPTP client. PPTP was developed by Microsoft and is provided with most versions of the Windows operating system. An advantage of PPTP is it is easy to configure.

11.3.2 Layer 2 Tunnel Protocol

The Layer 2 Tunnel Protocol (L2TP) is an Internet Engineering Task Force (IETF) standard which combines the best features of two existing tunnelling protocols, Layer 2 Forwarding (L2F) developed by Cisco and the Point-to-Point Tunnelling Protocol (PPTP). L2TP can be viewed as an extension to the Point-to-Point Protocol (PPP). One endpoint of an L2TP tunnel is called the L2TP Network Server (LNS), the LNS waits for new tunnels to be established. The other endpoint is called the L2TP Access Concentrator (LAC), the LAC initiates tunnel connections to the LNS, the unit implements an L2TP LAC. Once the L2TP tunnel has been established the traffic over the tunnel is bidirectional.

11.3.3 PPTP and L2TP configuration

To access the PPTP & L2TP configuration page select VPN ▷ PPTP & L2TP a page similar to that shown in Figure 282 will be displayed. The PPTP & L2TP page will list the currently configured tunnels.

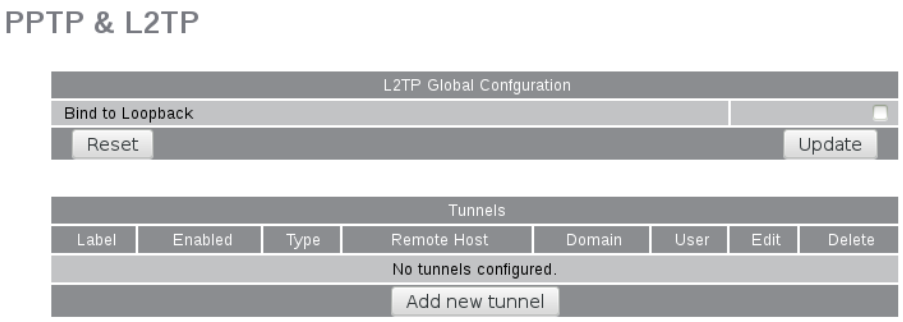


Figure 282: The PPTP & L2TP main page

L2TP Global Confguration Bind to Loopback Check to bind the service to the loopback port. Refer to section 8.3 for details on configuring the loopback interface.

11.3.4 Add a PPTP or L2TP tunnel

To add a new PPTP or L2TP tunnel Click the Add new tunnel button. The Add new tunnel page will be displayed as shown in Figure 283

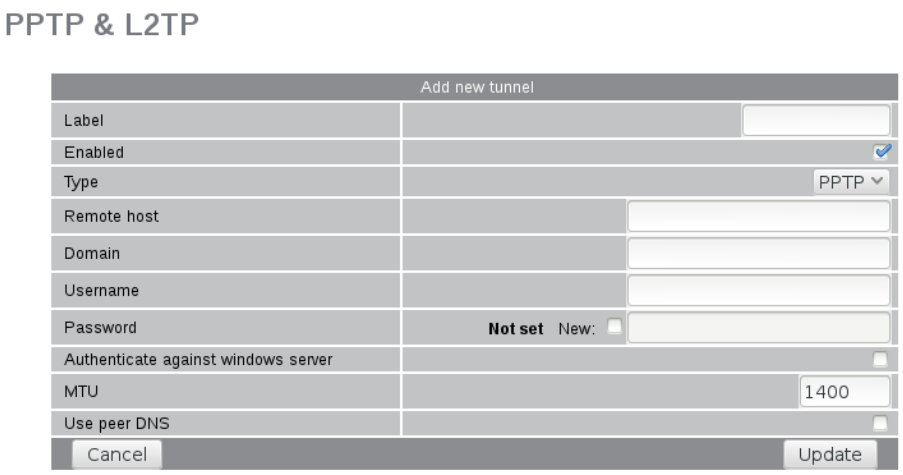


Figure 283: The PPTP & L2TP Add new tunnel page

Add new tunnel Options:

Label A label or name for the tunnel.

Enabled Check the box to enable the tunnel.

Type Select the type of tunnel from the drop-down list, the options are:

PPTP Point-to-Point Tunnelling Protocol

l2TP Layer 2 Tunnelling Protocol

Remote host Specify then IP address or fully qualified domain name of the remote host.

Domain Specify the Windows network domain. (Optional)

Username The user-name for authentication.

Password Specify the password for connection with the remote host. To set a new password click the **New** check-box and then enter the password.

Authenticate against windows server Check to enable authentication with a Windows server.

MTU Specify Maximum Transmission Unit (MTU) is the size (in bytes) of the largest packet which can be sent over the IPsec tunnel. Default value is 1400.

Use peer DNS Check the box to enable peer DNS.

Click the Update button to save and commit changes.

11.3.5 PPTP configuration example

The following is an example of connecting a PPTP tunnel to a PPTP VPN server. Figure 284 illustrates the network which will be established. For this example a connection will be established from the unit to a PPTP server. The tunnel will be called test, it is of type PPTP and the remote host is at IP address 123.123.123.123. The domain is test.com.au, the user-name is *user* and the password *password*. The MTU setting is left at the default of 1400 and peer DNS is enabled.

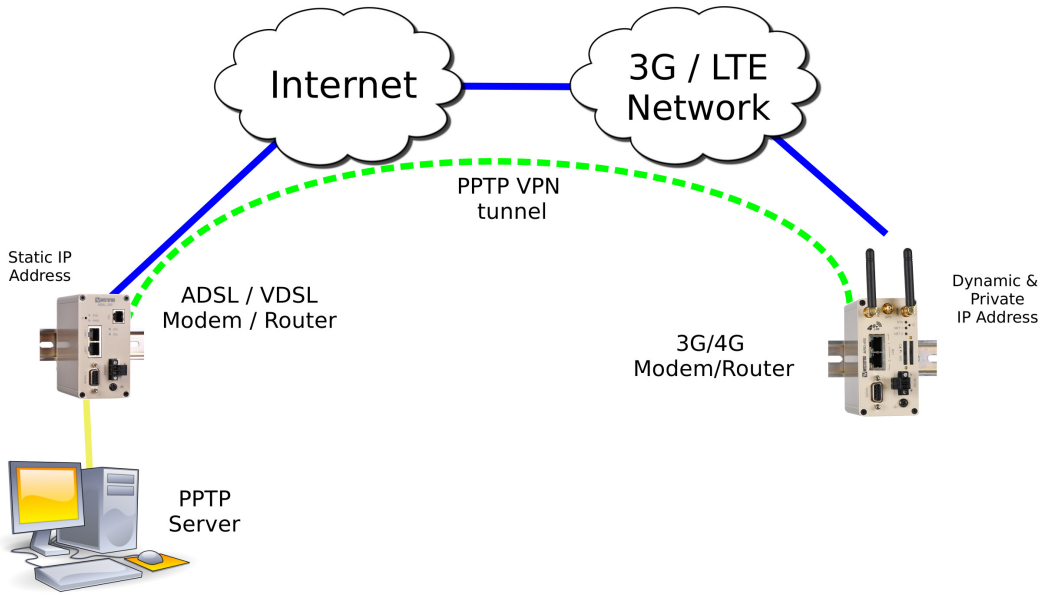


Figure 284: PPTP based VPN example network

To access the PPTP & L2TP configuration page select VPN ▷ PPTP & L2TP from the menu. The PPTP & L2TP page will then be displayed. To add a tunnel Click the Add new tunnel button on the main PPTP & L2TP page. The Add new tunnel page will be displayed. Figure 285 illustrates the PPTP add tunnel page with the parameters entered for the configuration described above.

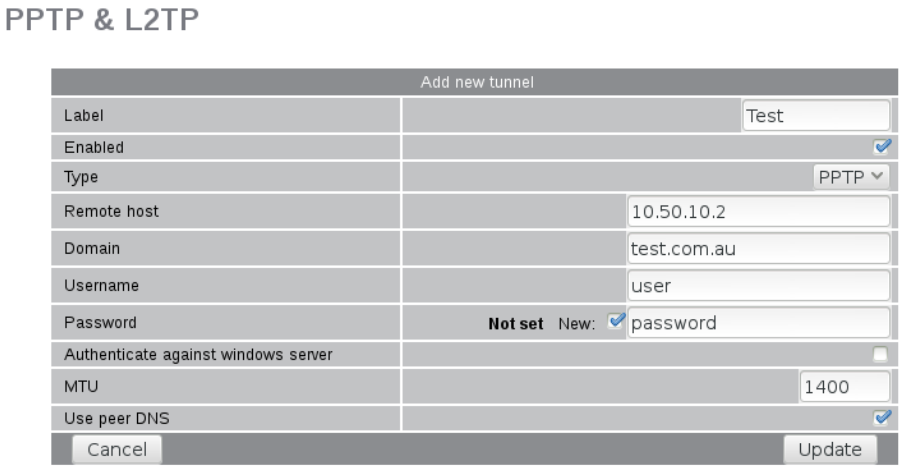


Figure 285: The PPTP & L2TP main page

The following settings are used to configured the tunnel as described:

Label: Test

Enabled: On (Checked)

Type: PPTP

Remote host: 123.123.123.123

Domain: test.com.au

Username: user

Password: password

MTU: 1400

Use peer DNS: On (Checked)

Once the options have been entered click the Update button to save and commit changes.

The settings will be saved and the main PPTP & L2TP page will be displayed with the new tunnel added to the Tunnels table, as shown in Figure 286. The unit will now attempt to establish a connection with the PPTP server.

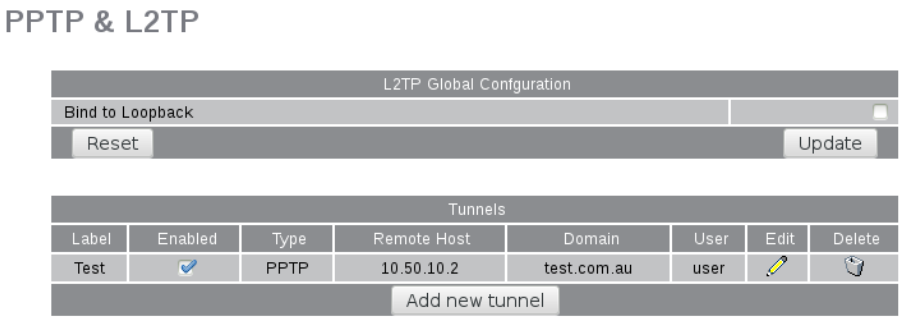


Figure 286: The PPTP & L2TP main page

To check the status of the page click **Status** on the main menu and **VPN** on the sub-menu. The VPN status page will then be displayed. Figure 287 is the status page for the PPTP VPN created in this example.

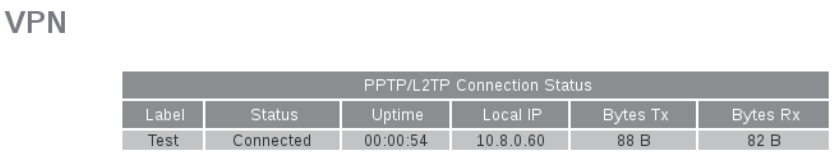


Figure 287: The PPTP & L2TP main page

The status of the tunnel is connected, indicating that the tunnel has been established and traffic can flow. The status page also indicates the local IP address of the tunnels and the number of bytes that have been received and transmitted.

11.4 Multiple VPN Tunnels

The total number of VPN tunnels support is model dependant. On models which support multiple VPN tunnels these can be configured to operate simultaneously. Figure 288 is an example of the VPN Status page with one SSL, one IPsec and one PPTP VPN tunnel operating simultaneously.

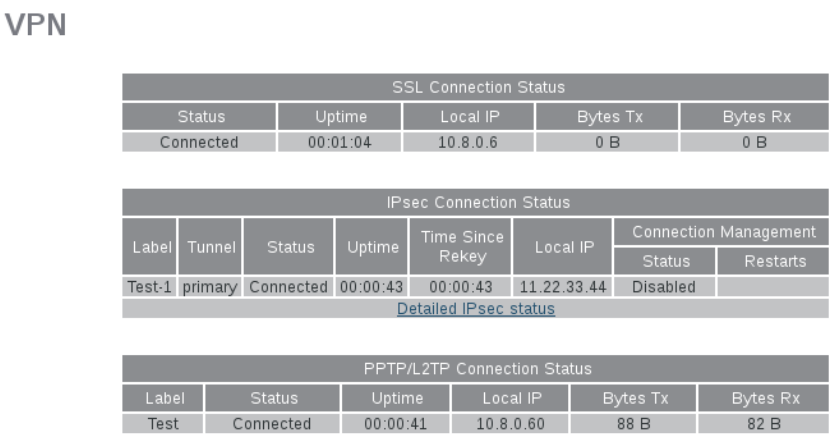


Figure 288: The VPN status page showing 3 active VPN connections

11.5 Certificate Management

Digital certificates are a form of digital identification used for authentication. A digital certificate contains information that identifies a device or user. They are issued in the context of a Public Key Infrastructure (PKI), which uses public-key/private-key encryption to ensure security. Support is provided for X.509 digital certificates (International Telecommunications Union Recommendation X.509), including SSL (Secure Sockets Layer) certificates.

To access the certificate management page select VPN ▷ Certificates a page similar to that shown in Figure 289 will be displayed. The top part of the page lists the currently loaded certificates, the second section is for uploading a new certificate and the last section is for configuring Simple Certificate Enrolment Protocol (SCEP).

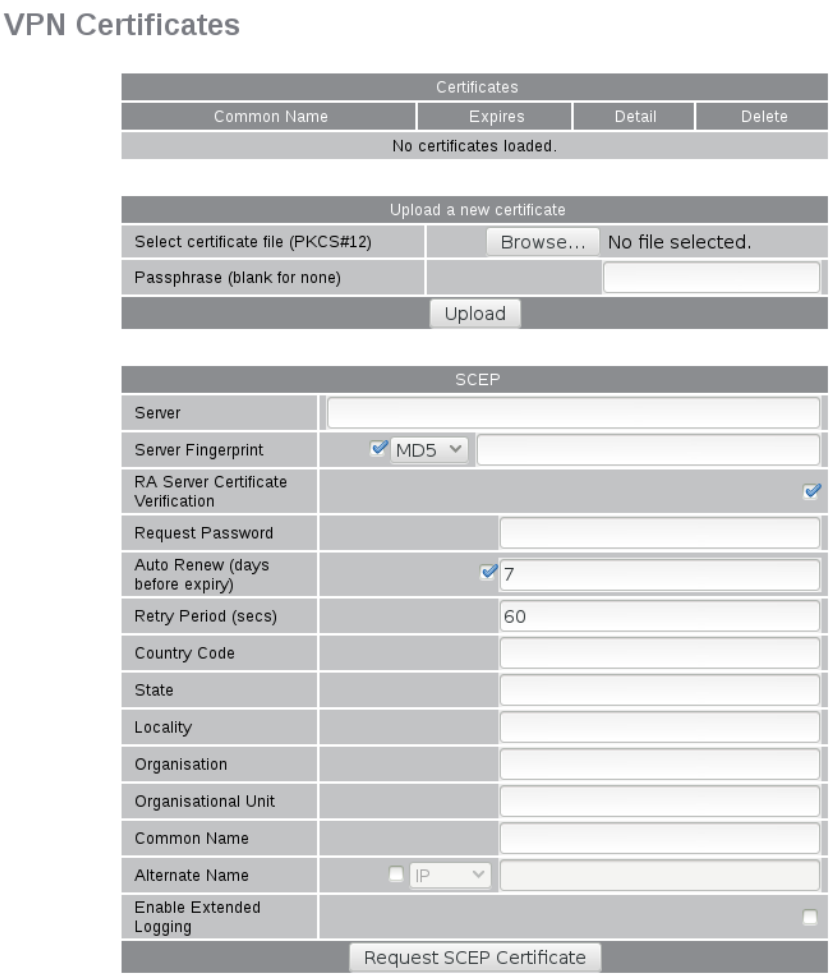


Figure 289: VPN certificate management

11.5.1 Add a certificate

To add a certificate click the Choose file button, then navigate to the certificate and select it. If a passphrase is required to read the certificate then it should be entered in the text box. To upload the certificate click the Upload button.

In the example shown in Figure 290, the file demoClient1.p12 is selected which contains the certificate demoClient. To select the certificate file click the Choose file button, then navigate to and select the certificate file demoClient1.p12, the file name will then be shown next to the Choose file button.

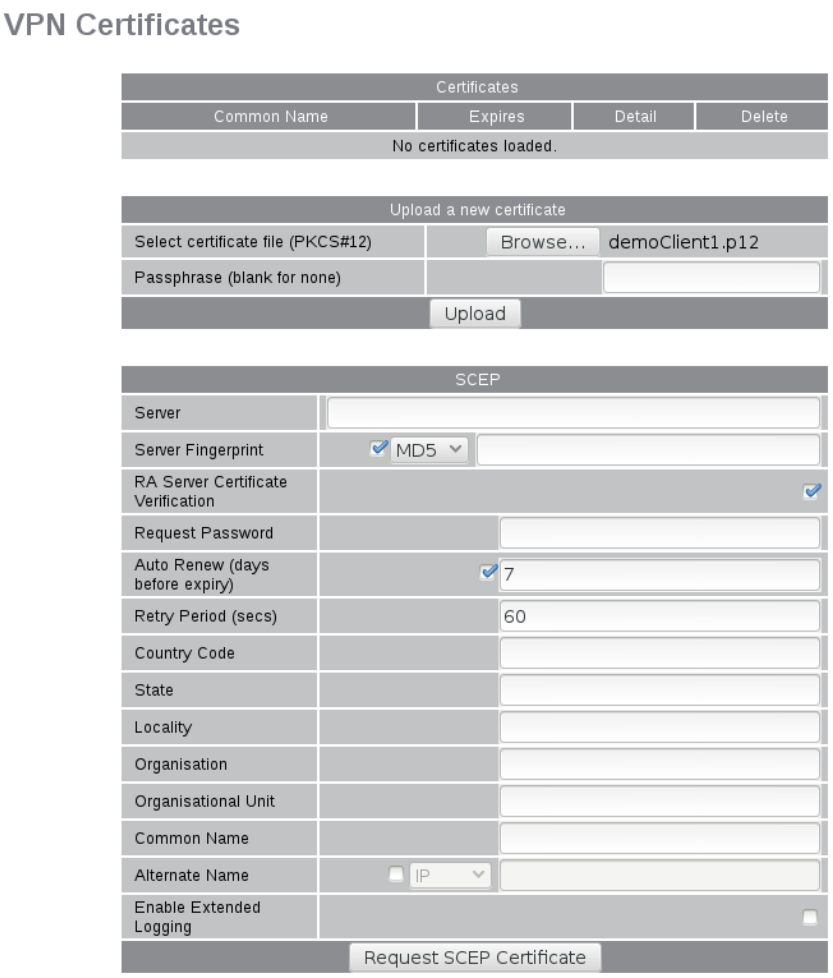


Figure 290: Uploading a VPN certificate

To upload the certificate click the Upload button. The page will be updated and the certificate will be added to the Certificates table as shown in Figure 291.

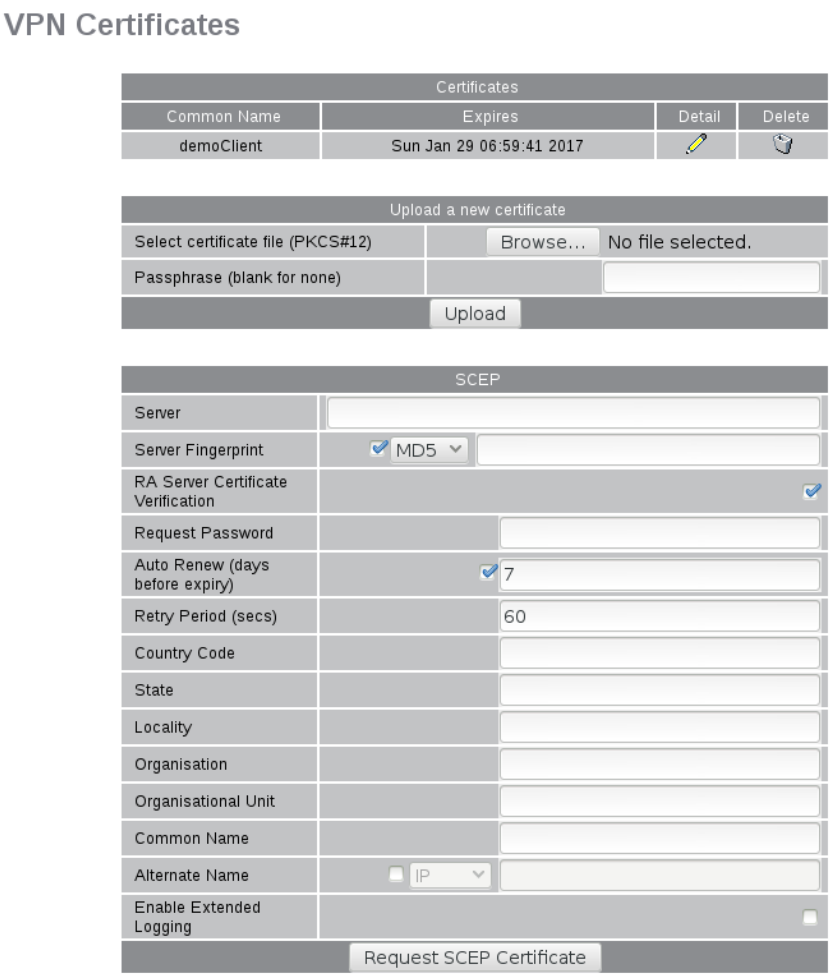


Figure 291: VPN certificate table listing the uploaded certificate

11.5.2 Checking the certificate details

Once uploaded the details of a certificate can be displayed by clicking the icon located in the detail column of the table. Figure 292 is an example of the details of a certificate. Click OK to return to the Certificates page.

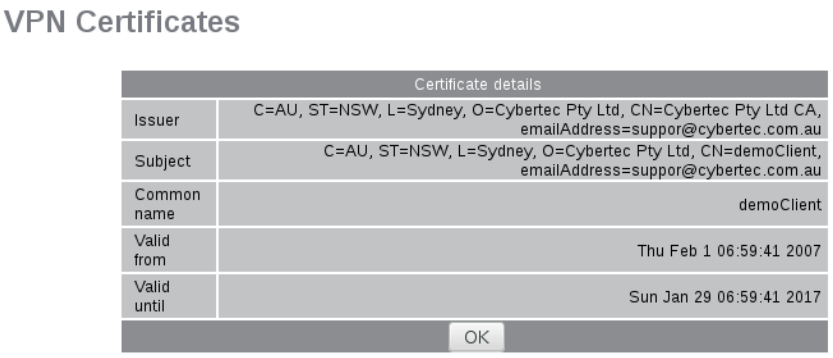


Figure 292: VPN certificate details

Click the OK button to return to the main certificate page.

11.5.3 Adding further certificates

Additional certificates can be uploaded using the same process. For each additional certificate click the Choose file button, navigate to the certificate then click the Upload button.

In the example shown in Figure 293, the file demoClient2.p12 is selected which contains the certificate demoClient2. To select the certificate file click the Choose file button, then navigate to and select the certificate file demoClient2.p12, the file name will then be shown next to the Choose file button.

Figure 293: Adding a second VPN certificate

To upload the certificate click the Upload button. The page will be updated and the certificate will be added to the Certificates table as shown in Figure 294.

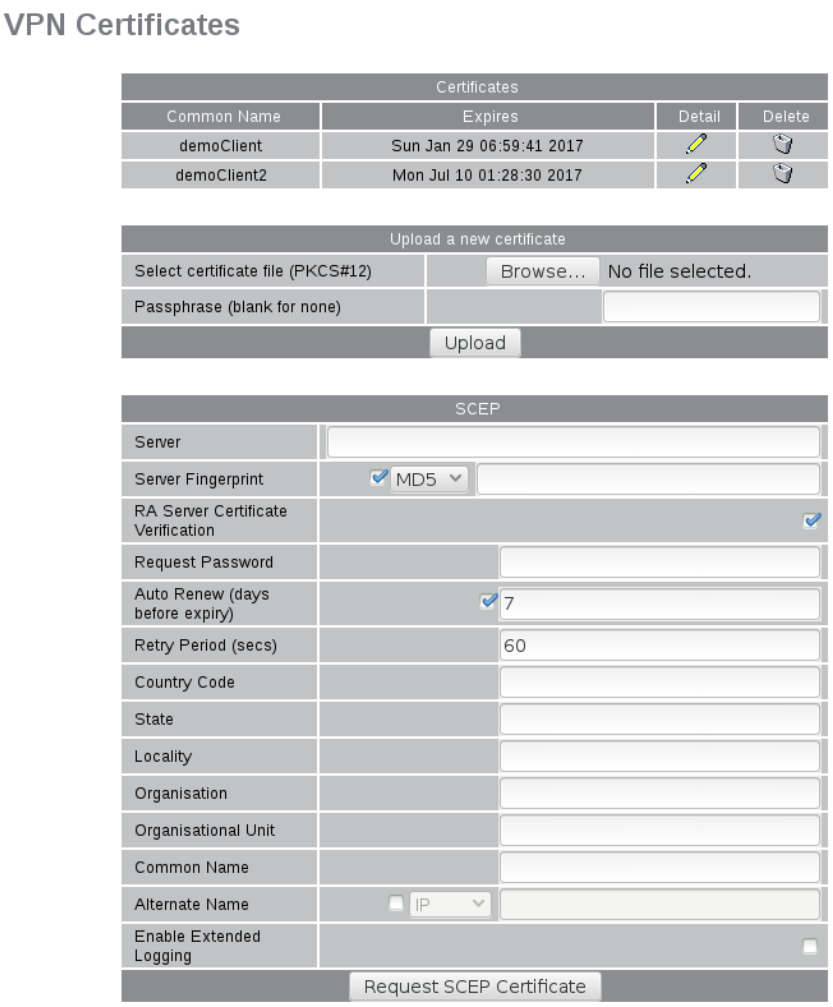


Figure 294: VPN certificate table listing both uploaded certificates

11.5.4 Deleting a certificate

A certificate can be deleted by clicking the icon in the **Delete** column of the certificate to be deleted. When the icon is clicked a warning box will be displayed. Click the OK button to confirm the deletion or click the Cancel button to prevent the certificate from being deleted.

For example, to delete certificate 2 from the table shown in Figure 294, click the icon in row 2 of the table. A warning box will now be displayed as shown if Figure 295, click the OK button and the certificate will be deleted.

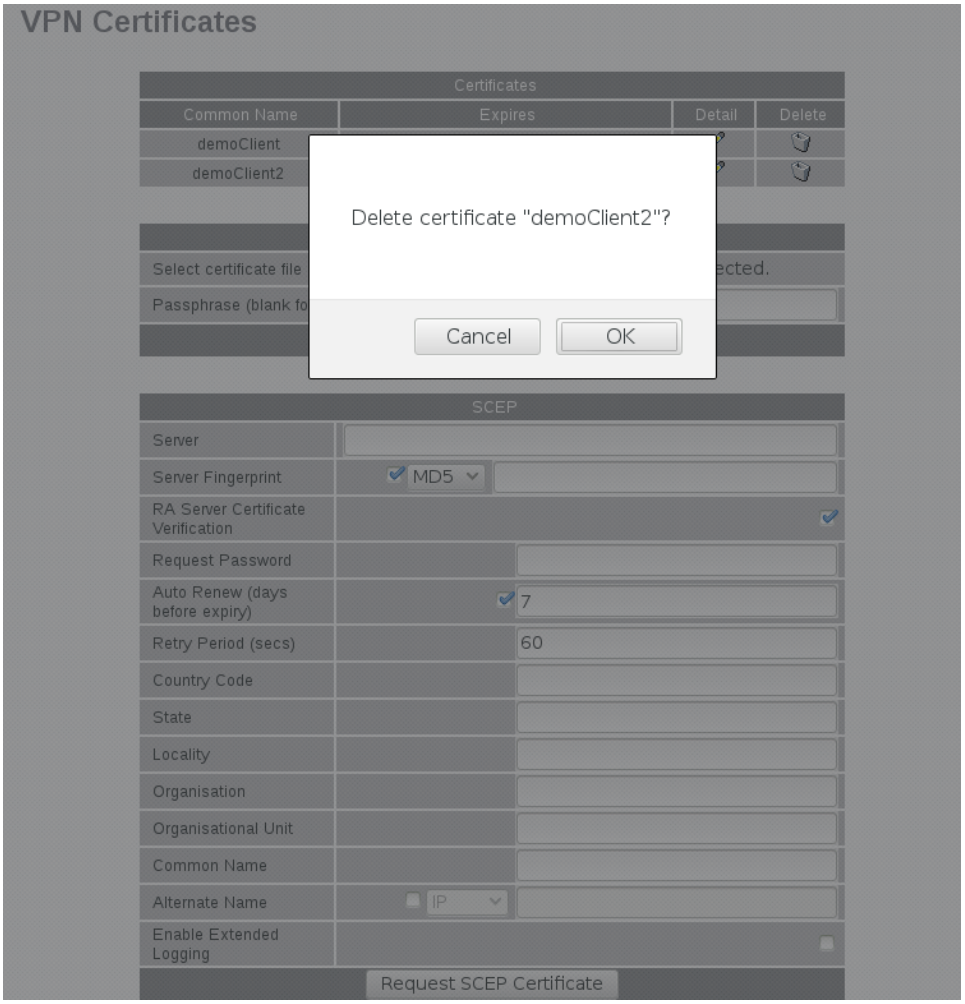


Figure 295: Deleting a VPN certificate

The certificate table will be update and the certificate removed, as shown in Figure 296.

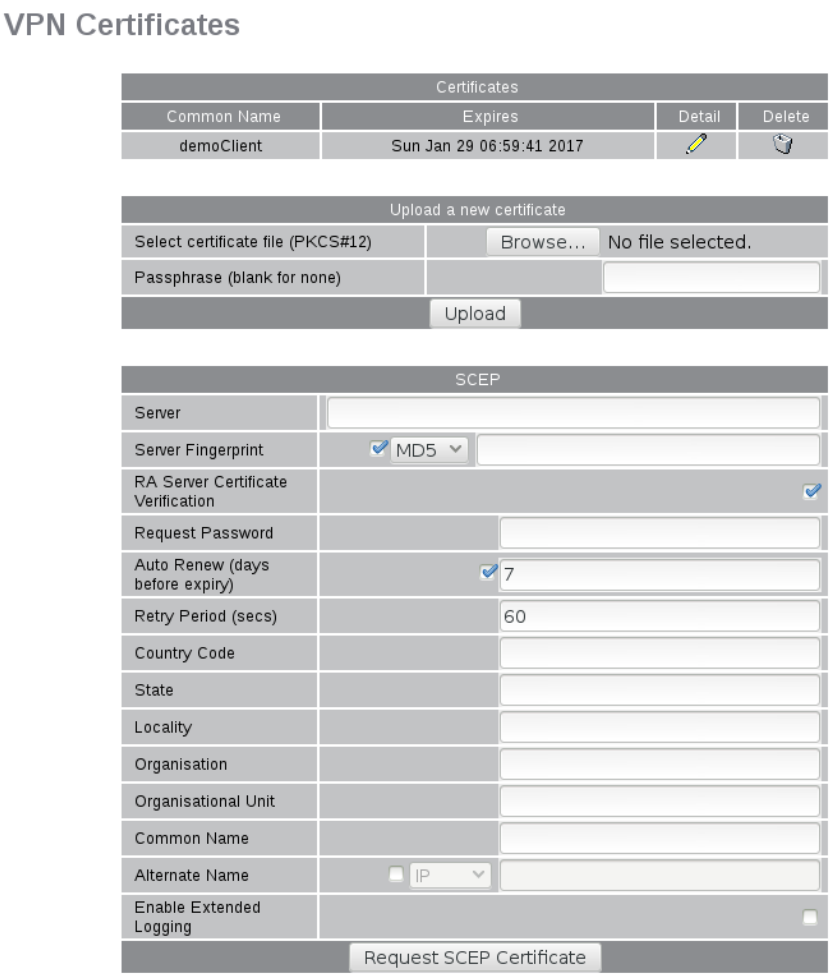


Figure 296: VPN certificate list with the second certificate deleted

11.5.5 Simple Certificate Enrolment Protocol (SCEP)

The Simple Certificate Enrolment Protocol (SCEP), is a protocol which enables a client, which employs Public Key Infrastructure (PKI), to request, renew, update and revoke a certificate from a Certification Authority (CA).

The parameters for SCEP are in a table in the lower section of the main certificate page as shown in Figure 297.

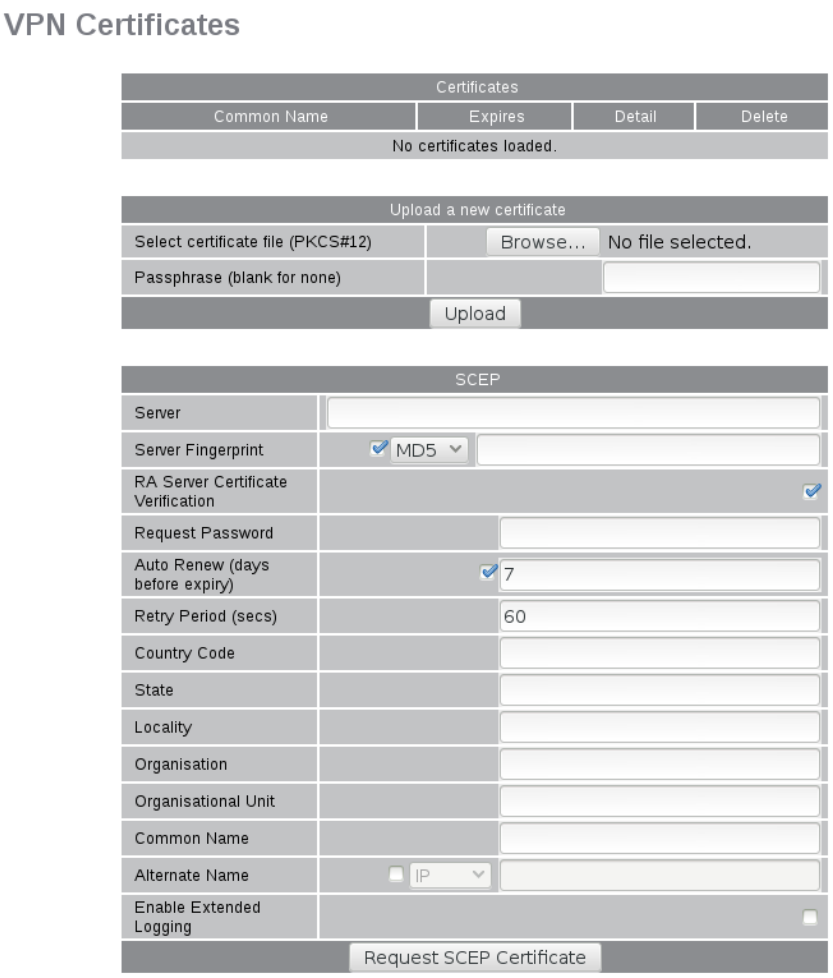


Figure 297: VPN certificate SCEP confguration

Not all parameters are required for SCEP to function. As a minimum the Server address and common name are required.
The number of parameters specified will be determined by the way in which the server has been configured.

SCEP Configuration as follows:

Server The IP address or URL of the Certificate server.

Server Fingerprint The server finger print:

Enable Check to enable

Hash Select the hash algorithm from the drop-down list.

Fingerprint Enter the fingerprint to use.

RA Server Certificate Verification Check to enable.

Request Password

Auto Renew (days before expiry) Enable Check to enable automatic request for certificate renewal.

Days Enter the number of days prior to expiry to request certificate renewal

Retry Period Enter the number of seconds after which to re-try a failed server connection attempt.

Country Code Enter the country code

State Enter the state

Organisation Enter the organisation name.

Organisational Unit Enter the name of the organisational unit.

Common Name Enter the common name of the certificate.

Alternate Name The alternate name:

Enable Check to enable

Type Select from IP address or Fully Qualified Domain Name (FQDN).

Enable Extended Logging Check to enable extending logging.

Click the Request SCEP Certificate button to request a certificate from the certificate server.

12 Serial Server

The serial server is used to transfer data between a physical serial port and an IP connection. The IP connection can be via the Ethernet or the wireless connection of the modem. The remote host that connects to the serial server could be a SCADA master, desktop PC or even another modem.

The Serial Server configuration page is accessed by selecting the **Serial Server** tab from the main menu. When selected a page similar to that shown in Figure 298 will be displayed.

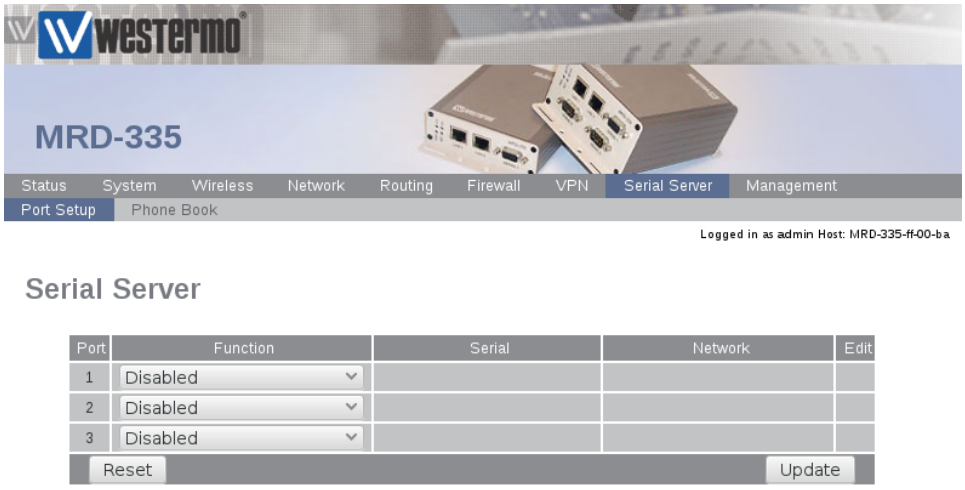


Figure 298: Serial server main page for model with 3 serial ports.

12.1 Selecting a port function

Each port of the serial server can be configured to operate with a different function. The function selected for an application will be determined by the serial equipment attached to the port and the type of IP connection required. To display the Serial Server Port Setup page select Serial Server ▷ Port Setup from the menu. The page shown will differ slightly between models, 299 is an example page from a unit with 1 serial port while figure 300 is an example page from a unit with 3 serial ports.

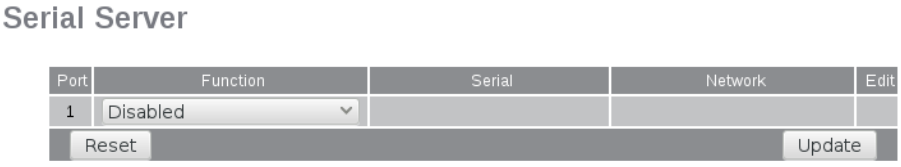


Figure 299: Serial server main page for model with 1 serial port.

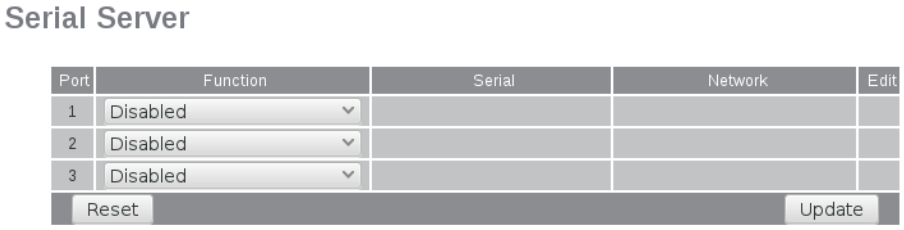


Figure 300: Serial server main page for model with 3 serial ports.

The table provides a summary of the port settings. The columns have the following meanings:

Port The port number this corresponds the physical port number. Refer to hardware manual for the model being configured for details.

Function The port function, the following options are available:

Disabled Serial server functionality is disabled for the port.

Raw TCP Client/Server The serial server will function create a transparent pipe between the serial port and a TCP network connection. Example uses of this mode include connecting to a remote PC running serial port redirector software with virtual COM ports or connecting two modems back-to-back to create a serial bridge.

Raw UDP This function is similar to Raw TCP Client/Server mode, but uses UDP as the network transport. UDP has lower overheads than TCP, but as UDP offers no lost packet detection, this function should only be used with serial protocols than can provide the necessary error correction.

Modem Emulator The serial server provides an AT command interface at the serial port that simulates a traditional dial-up modem. However, instead of dialling out phone calls, the emulator creates TCP network connections. The emulator will also simulate incoming calls if it receives a TCP connection. The function is suited to applications where equipment attached to the serial port expects to see a dial-up modem.

DNP3 IP-Serial Gateway The serial server will act as a DNP3 outstation to be polled by a SCADA master. The outstation mode is configurable as a TCP listen endpoint, TCP dual-function endpoint or UDP endpoint.

Modbus IP-Serial Gateway The serial server will perform conversion from Modbus/TCP to Modbus/RTU or Modbus/ASCII, allowing polling by a Modbus/TCP master.

Telnet (RFC 2217) Server The serial server will function as a Telnet server, including the protocol extensions defined in RFC 2217. In addition to transporting data, this mode also allows a remote PC with appropriate software to change the port configuration (baud rate etc) and read and write the handshaking lines during a session.

PPP Server The port acts as a PPP server. A device is able to connect to the port and establish a PPP session. Once established the connection acts in a similar way to other packet interfaces.

PPP Dialout Client The port establishes a connection to a PPP server. Once established the connection acts in a similar way to other packet interfaces.

Serial The serial port parameters. Listed in the form <baud> <data bits><parity><stop bits>, For example 19200 8N1 this indicates a baud rate of 19200, 8 data bits, Non parity and 1 stop bit. For details on configuring the port parameters refer to section 12.2.1.

Network The network parameters associated with the port. The parameters listed will depend on the mode in which the port is operating.

Click the Update button to save and commit the selected function.

The port options can be edited by clicking the icon for the associated port.

12.2 Common configuration options

12.2.1 Serial port settings

Regardless of the selected port function, each port needs to be configured to match the parameters of the equipment attached to the port. As the configuration of a port function is edited, the options displayed in Figure 301 will be shown.

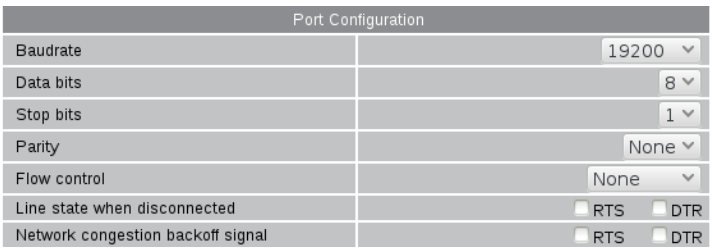


Figure 301: Common port configuration parameters

For each port, the following parameters can be set:

Baudrate The port can be configured for any standard baud-rate from 300 baud to 230400 baud.

Data bits The port can be configured for operation with 5 to 8 data bits.

Stop bits The port can be configured for operation with 1 or 2 stop bits.

Parity The port can be configured for none, odd or even parity.

Flow control The serial server port can be configured for the following modes:

None No flow control is enabled.

Hardware The port will use the RTS and CTS handshake lines to control the flow of data.

Software The port will use XON/XOFF software flow control. The XOFF character is hex 0x11. The XON character is hex 0x13.

Both The port will use both hardware and software flow control.

Line state when disconnected This field determines the state of the port's RTS and DTR handshaking lines while the port is disconnected. To set a signal active while disconnected, check the associated box.

Network congestion backoff signal The serial port line RTS and/or DTR to assert when the network is congested and further data

12.2.2 Packet framer settings

The packet framer is available for all port functions that carry raw data (these settings are not available for the DNP3 IP-Serial Gateway or Modbus IP-Serial Gateway). The packet framer allows data received from the serial port to be packetised in a way consistent with the data being sent and received. This can reduce the overhead incurred in sending and receiving the data and can assist with reducing latency.

Figure 302 shows the configuration options for the packet framer.

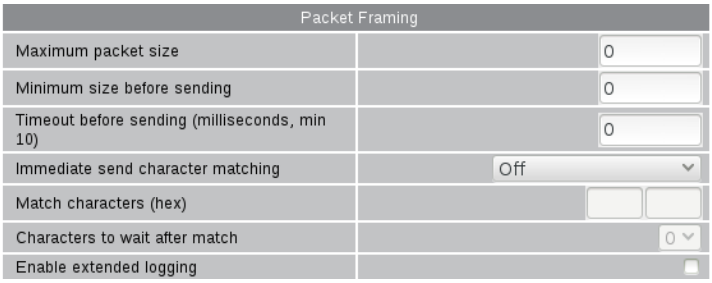


Figure 302: Packet framing configuration options

The following options control the packet framer:

Maximum packet size This value determines the largest packet size to be passed to the network for transmission. If set to 0, the packet framer will be disabled and data will bypass the packet framer. The value chosen will depend on the application, however, the value should not be set higher than 1024, so as to ensure the packet will fit a conventional Ethernet frame.

Minimum size before sending In some applications, it may not be desirable to wait for the exact number of bytes specified in **Maximum packet size** before sending the packet. The value set in this field, which must be less than or equal to the **Maximum packet size**, acts as a send threshold. Once the accumulated byte count reaches this value, the packet will be sent.

Timeout before sending The time-out allows data accumulated by the framer to be sent after a specified period of serial receive inactivity. This prevents data from being held in the framer indefinitely should no more data arrive on the serial port. The time-out value is in milliseconds, with the minimum value being 10 milliseconds.

Immediate send character matching This field allows the framer to be configured so that if certain characters are received the accumulated data is immediately sent. The character matching can function in one of the following modes:

Off No character matching is done.

Match any character If either of the characters set the in **Match characters** field are received, the data will be sent immediately.

Match all characters If both of the characters set in the **Match characters** field are received in the order specified, the data will be sent immediately.

Match characters Used in conjunction with the **Immediate send character matching** field, these characters determine what data will cause an immediate send. The values are entered as a hex value, so, for example, a newline (ASCII 10) would be entered as 0A. To delete a value, clear the text in the field.

Characters to wait after match Used in conjunction with the **Immediate send character matching** field, this count determines how many additional characters will be received after an immediate match character is detected. This is useful if for example trailing characters always follow the match character.

Enable extended logging Check box to enable debugging information to be written to the log file. This can be useful to assist when first configuring the packet framer settings. It is not recommended to have extended logging enabled in a production system as the log buffer is of limited size and the higher number of logging messages could cause other log messages to be lost.

12.3 Raw TCP Client/Server

12.3.1 Description

The serial server will function create a transparent pipe between the serial port and a TCP network connection. Example uses of this mode include connecting to a remote PC running serial port redirector software with virtual COM ports or connecting two modems back-to-back to create a serial bridge.

12.3.2 Selecting the port function

The serial server configuration is accessed by selecting Serial Server ▹ Port Setup. To enable a port for Raw TCP Client/Server function, select **Raw TCP Client/Server** from the **Function** column of the appropriate port. Once selected, click **Update** to confirm the change. Once confirmed, the port will display as shown in Figure 303.

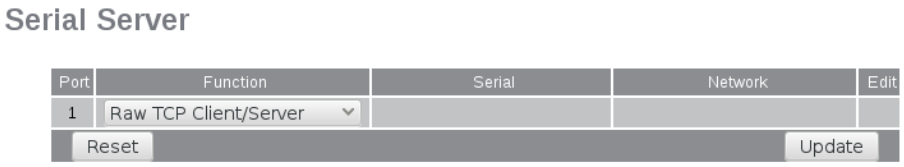


Figure 303: Selecting Raw TCP Client/Server function

12.3.3 Configuring the port function

Once the port function has been selected, click on the icon, in the **Edit** column to edit settings for the associated port. A page similar to that shown in Figure 304 will be displayed.

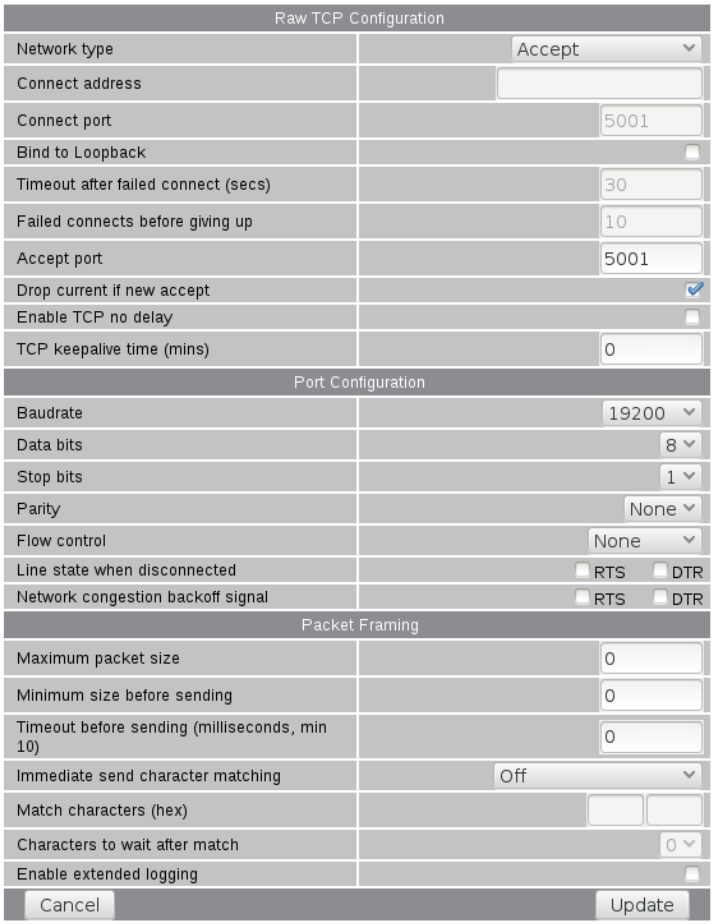


Figure 304: Raw TCP Client/Server configuration

The following options can be set for the Raw TCP Client/Server:

Network type The Raw TCP serial server can be configured for three different network modes:

Accept The serial server will listen for TCP connections on the specified port number.

Connect The serial server will establish a TCP connection to the specified address and port number.

Accept and Connect The serial server will normally listen for TCP connections on the specified port number, however, it data is received at the serial port and no connection exists, it will attempt to establish a connection to the specified address and port number.

Connect address For **Connect** or **Accept and Connect** network modes, this is the address the server will attempt to connect to. The address entered should be in IPv4 decimal dotted notation.

Connect port For **Connect** or **Accept and Connect** network modes, this is the TCP port number the server will attempt to connect to. The value entered should be a valid TCP port number.

Bind to Loopback Check to bind the service to the loopback port. Refer to section 8.3 for details on configuring the loopback interface.

Timeout after failed connect For **Connect** or **Accept and Connect** network modes, if a connection request has failed, the server will wait the amount of time (in seconds) specified in this field before attempting another connection request. While a short time-out may cause the connection to be established more quickly, it may also cause greater network traffic if the remote host is unavailable and repeated attempts fail.

Failed connects before giving up For **Accept and Connect** network modes, the serial server will attempt to establish a connection for the number of times specified in this field be giving up and waiting for a connection to be accepted.

Accept port For **Accept** or **Accept and Connect** network modes, this is the TCP port number on which the server will listen for connections.

Drop current if new accept For **Accept** or **Accept and Connect** network modes, if a TCP connection is currently active on the serial server, and a new connection request is accepted, this field determines the action that will be taken. If set, the new connection will become the active connection and the existing connection will be closed. If not set, the existing connection will remain active and the newly received connection will be closed.

Enable TCP no delay Check to enable TCP no delay. TCP normally uses Nagle's algorithm to combine a number of small outgoing messages, to be sent all at once. Specifically, as long as there is a sent packet for which the sender has not received an acknowledgement, the sender should keep buffering its output until it has a full packet's worth of output, so that output can be sent all at once. For serial communications this can introduce delays which can interfere with the operation of serial protocols. Enabling this option will decrease the efficiency of the TCP communications as the number of packets transmitted will increase. It is for these reason that it is recommended not to enable this option unless the application requires it to be enabled. It could also be that the Raw UDP option may be more suitable.

TCP keepalive time When set to a value greater than 0, TCP keep-alives will be enabled for connections, with probes sent at the frequency specified (minutes). This may assist in detecting failed connections.

For information on setting the Port Configuration, see section 12.2.1. For information on setting the Packet Framing, see section 12.2.2.

Click the Update button to save and commit the changes.

12.4 Raw UDP

12.4.1 Description

This function is similar to Raw TCP Client/Server mode, but uses UDP as the network transport. UDP has lower overheads than TCP, but as UDP offers no lost packet detection, this function should only be used with serial protocols than can provide the necessary error correction.

12.4.2 Selecting the port function

The serial server configuration is accessed by selecting **Serial Server** from the main menu and **Port Setup** from the sub-menu. To enable a port for Raw UDP function, select **Raw UDP** from the **Function** column of the appropriate port. Once selected, click **Update** to confirm the change. Once confirmed, the port will display as shown in Figure 305.

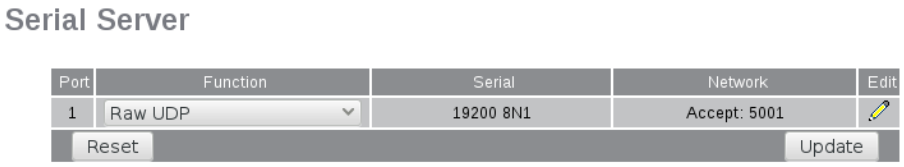


Figure 305: Selecting Raw UDP function

12.4.3 Configuring the port function

Once the port function has been selected, click on the icon, in the **Edit** column to edit settings for the associated port. A page similar to that shown in Figure 306, will be displayed.

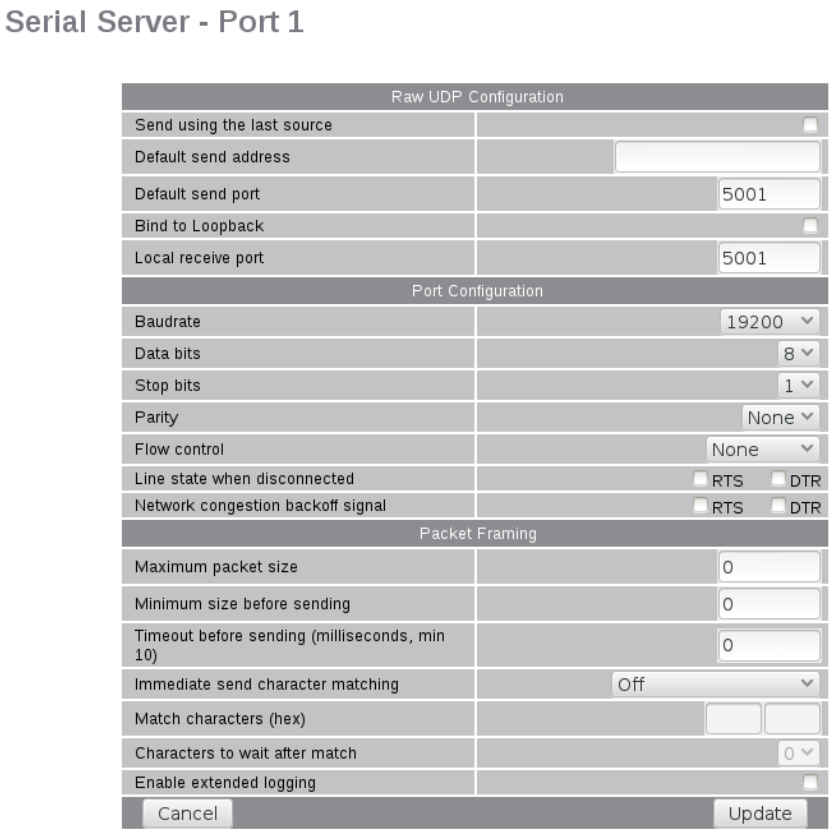


Figure 306: Raw UDP configuration

The following options can be set for Raw UDP mode:

Send using the last source Check to use the last received packet's source address and port number as the send address and port number.

Default send address The default IP address the serial server will send UDP packets to. The address entered should be in IPv4 decimal dotted notation.

Default send port The default UDP port number the server will send UDP packets to. The value entered should a valid UDP port number.

Bind to Loopback Check to bind the service to the loopback interface. Refer to section 8.3 for details on configuring the loopback interface.

Local receive port This is the UDP port number that UDP packets will be received on at the modem. The value entered should a valid UDP port number.

For information on setting the Port Configuration, see section 12.2.1. For information on setting the Packet Framing, see section 12.2.2.

Click the Update button to save and commit the changes.

12.5 Modem Emulator

12.5.1 Description

The serial server provides an AT command interface at the serial port that simulates a traditional dial-up modem. However, instead of dialling out phone calls, the emulator creates TCP network connections. The emulator will also simulate incoming calls if it receives a TCP connection. The function is suited to applications where equipment attached to the serial port expects to see a dial-up modem.

12.5.2 Selecting the port function

The serial server configuration is accessed by selecting **Serial Server** from the main menu and **Port Setup** from the sub-menu. To enable a port for the Modem Emulator function, select **Modem Emulator** from the **Function** column of the appropriate port. Once selected, click **Update** to confirm the change. Once confirmed, the port will display as shown in Figure 307.

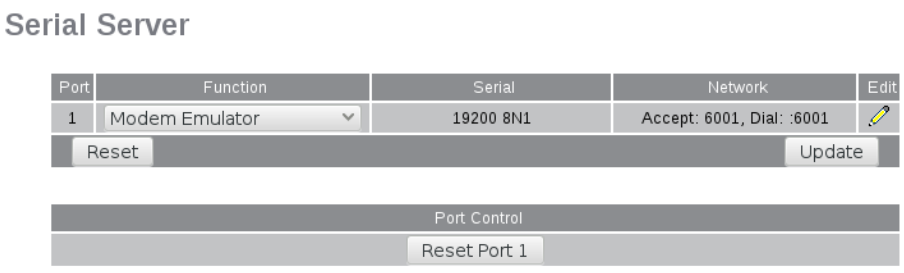


Figure 307: Selecting Modem Emulator function

12.5.3 Modem Emulator Configuration

Once the port function has been selected, click on the icon, in the **Edit** column to edit settings for the associated port. A page similar to that shown in Figure 308, will be displayed.

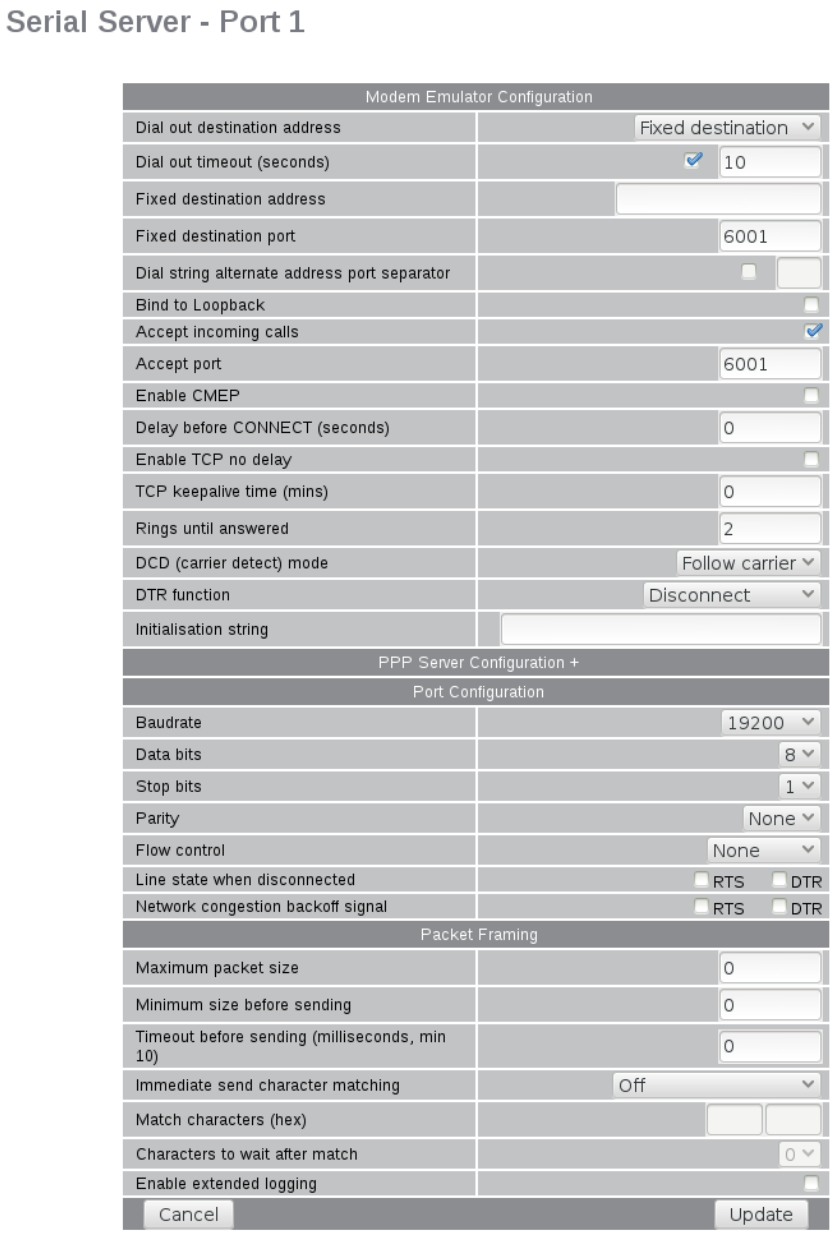


Figure 308: Modem Emulator configuration.

The following options can be set for Modem Emulator mode:

Dial out destination address This field determines how the emulator will handle dial requests from the serial port (ATDxxxx commands). The dial address may be set to:

Fixed destination Regardless of the value entered after the ATD command, the emulator will always connect to the host specified in the **Fixed destination address** and **Fixed destination port** fields.

From dial string The emulator will parse the ATD command to extract the destination address and port number. The examples below show the two different formats that can be used to create a connection to the address 10.10.10.10 and port number 6001.

Dotted Dial string is ATD 10.10.10.10:6001

Padded Dial string is ATD 01001001001006001

From phone book When a dial command is entered, the emulator will look up the modem's phone book and attempt to translate the number to an address and port number. More details on the phone book can be found in section 12.11.

Dial out timeout Check to enable and enter the connection time-out value in seconds.

Fixed destination address The IP address to connect to if Fixed destination is selected.

Fixed destination port The IP port to connect to if Fixed destination is selected.

Dial string alternate address port separator Check to enable and enter a character which separates the IP address from the port number when entered as part of the dial string. The default character is ':'.

Bind to Loopback Check to bind the service to the loopback interface. Refer to section 8.3 for details on configuring the loopback interface.

Accept incoming calls Check to enable. When enabled, the emulator will listen for TCP connections on the port number specified in the **Accept port** field. When a connection is received, the emulator will indicate a ring condition at the serial port. The equipment can then answer the call or wait for the emulator to automatically answer. Once answered, the emulator will indicate the connection is open and data will pass between the remote host and the serial port.

Accept port This is the TCP port number that the server will listen for connections.

Enable Cybertec modem emulation protocol

Delay before CONNECT Enter a delay in seconds from the time of connection to when the CONNECT string is sent. Default value is 0 or no delay.

Enable TCP no delay Check to enable TCP no delay. TCP normally uses Nagle's algorithm to combine a number of small outgoing messages, to be sent all at once. Specifically, as long as there is a sent packet for which the sender has not received an acknowledgement, the sender should keep buffering its output until it has a full packet's worth of output, so that output can be sent all at once. For serial communications this can introduce delays which can interfere with the operation of serial protocols. Enabling this option will decrease the efficiency of the TCP communications as the number of packets transmitted will increase. It is for these reason that it is recommended not to enable this option unless the application requires it to be enabled. It could also be that the Raw UDP option may be more suitable.

TCP keepalive time When set to a value greater than 0, TCP keep-alives will be enabled for connections, with probes sent at the frequency specified (minutes). This may assist in detecting failed connections.

Rings until answered This field determines the default number of rings the emulator will wait before automatically answering a call. This is equivalent to setting the ATS0 S-Register in a conventional modem.

DCD mode This field determines the default state of the Data Carrier Detect (DCD) handshaking line. The following modes are supported:

Always on Regardless of the online state of the emulator, the DCD line will be active (equivalent to AT&C0).

Follow carrier The DCD line will be active when the emulator is in the online state (equivalent to AT&C1).

DTR function This field determines the default response of the modem to changes in the Data Terminal Ready (DTR) handshaking line. The following modes are supported:

Ignore The emulator will ignore changes to the state of DTR (equivalent to AT&D0).

Command mode If the DTR line transitions from the active to inactive state while the emulator is on online data mode, the emulator will drop to AT command mode (equivalent to AT&D1).

Hangup If the DTR line transitions from the active to inactive state while the emulator is on online data mode, the emulator will terminate the current call (equivalent to AT&D2).

Initialising string Enter a string which will be sent as part of the initialisation process. Default is no string will be sent.

Click the Update button to save and commit the changes.

12.5.4 PPP Server Configuration

The modem emulator includes a PPP server which can be enabled if required. To access the PPP Server Configuration click the heading, the display will change to include the options shown in Figure 309.

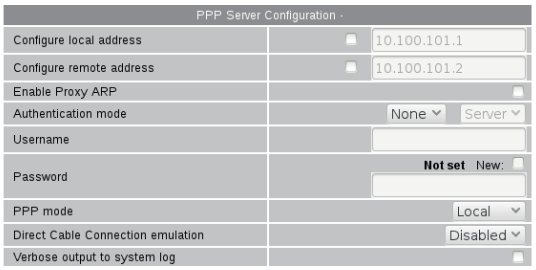


Figure 309: Modem Emulator PPP configuration.

The following options are available for the PPP Server:

Configure local address Check to enable and enter an IP address. This is the IP address the modem will have in the PPP connection. The address entered should be in IPv4 decimal dotted notation (eg. 10.100.100.1).

Configure remote address Check to enable and enter an IP address. This is the IP address the modem will allocate to the connection PPP client. The address entered should be in IPv4 decimal dotted notation (eg. 10.100.100.1) and must be different to the **Local IP address**.

Enable Proxy ARP Check to enable. Proxy ARP is a technique by which a device on a given network, in this case the modem, answers the ARP queries for a network address that is on a different network, in this case the network of the remote IP address.

Authentication mode This fields sets the required level of authentication for remote users connecting to the modem when operating in Server mode or the authentication to use when operating in client mode and connection to a remote server.

Authentication_type: None No authentication will be required.

PAP Authentication will be required using the PAP protocol.

CHAP Authentication will be required using the CHAP protocol.

Mode: Server Set to PPP server. Receive remote connections.

Client Set to PPP client. Connect to remote servers.

Username Where **Authentication** is not set to **None**, this is the user-name a remote user will be required to authenticate with.

Password Where **Authentication** is not set to **None**, this is the password a remote user will be required to authenticate with. To set the password, click the **New** check-box and enter the password in the adjacent field.

PPP mode Select from:

Local Ignores the serial port control lines.

Modem Uses the serial port control lines.

Direct Cable Connection emulation Direct Cable Connection (DCC), is a feature of Microsoft Windows which allows a computer to transfer data with another computer, using either the serial port of each computer. This option is only available if the PPP mode is set to local. Select from:

Disabled Disabled Direct Cable Connection.

Host Act as the host and receive connections from a guest.

Guest Act as the guest and make a connection to a host.

Verbose output to system log Check box to enable extended logging information to be written to the log file. This can be useful to assist when first configuring the PPP settings. It is not recommended to have extended logging enabled in a production system as the log buffer is of limited size and the higher number of logging messages could cause other log messages to be lost.

For information on setting the Port Configuration, see section 12.2.1. For information on setting the Packet Framing, see section 12.2.2.

Click the Update button to save and commit the changes.

12.6 DNP3 IP-Serial Gateway

12.6.1 Description

The DNP3 IP-Serial Gateway carries out translation between DNP3 Serial and DNP3 TCP protocols. This has several advantages:

- DNP3 frames are not fragmented. The translation software identifies and transmits DNP3 link layer frames without fragmentation, ensuring reliable transport of the DNP3 data in a single TCP or UDP packet.
- Sever serial port emulation is not required. The SCADA server can communicate with the DNP3 device directly via TCP rather than through serial port emulation software. This reduces the complexity and number of software layers required on the SCADA servers.
- Dual function endpoint. The remote station can return unsolicited messages DNP3 serial data to the SCADA server.

12.6.2 Selecting the port function

The serial server configuration is accessed by selecting **Serial Server** from the main menu and **Port Setup** from the sub-menu. To enable a port for the DNP3 IP-Serial Gateway function, select **DNP3 IP-Serial Gateway** from the **Function** column of the appropriate port. Once selected, click **Update** to confirm the change. Once confirmed, the port will display as shown in Figure 310.

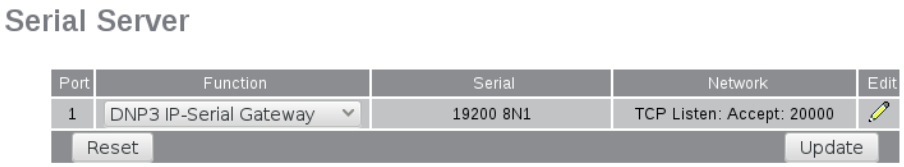


Figure 310: Selecting DNP3 Gateway function

12.6.3 Configuring the port function

Once the port function has been selected, click on the icon, in the **Edit** column to edit settings for the associated port. A page similar to that shown in Figure 311, will be displayed.

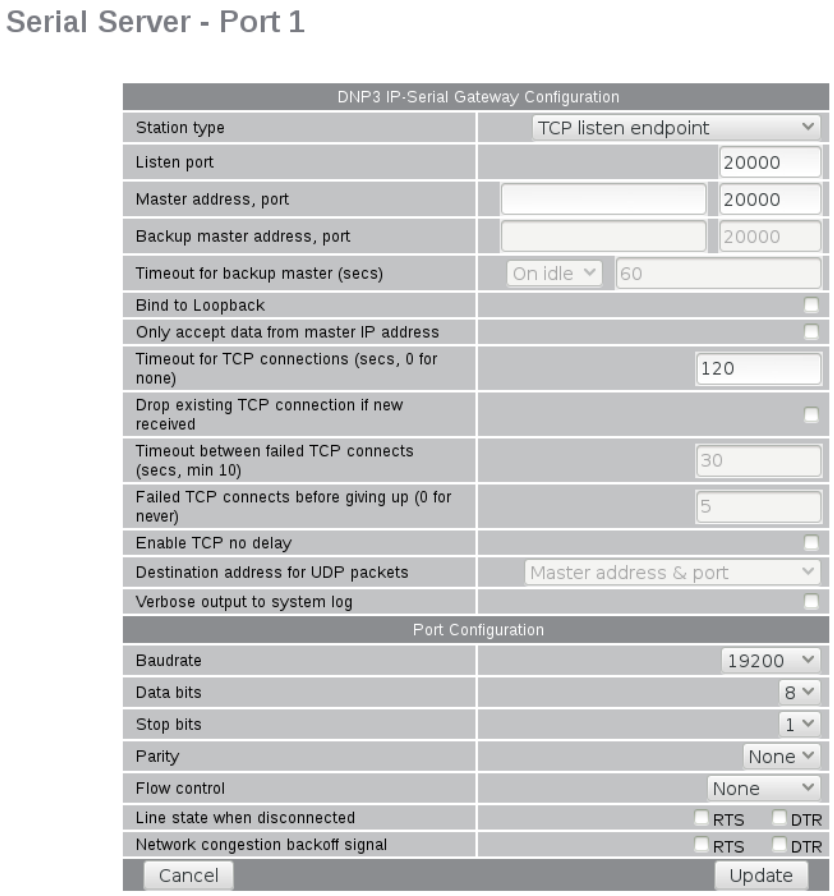


Figure 311: DNP3 Gateway configuration

The following options are available for the DNP3 gateway:

Station type The DNP3 IP-Serial Gateway can be configured to operate in three modes:

TCP listen endpoint The serial server will listen for TCP connections on the specified port number.

TCP dual endpoint The serial server will normally listen for TCP connections on the specified port number, however, if a valid DNP packet is received at the serial port and no connection exists, a connection will be established to the specified master address. This is useful if a SCADA master will poll periodically but facility is required to support unsolicited responses.

TCP redundant dual endpoint Similar to the TCP dual endpoint option but includes to backup DNP master.

UDP (datagram) endpoint The serial server will operate in UDP mode, receiving data on the specified port number and transmitting responses to the specified master.

Listen port For all station types, this determines the TCP/UDP port the serial server will listen for connections (TCP) or data (UDP) on. The value entered should be a valid TCP/UDP port number. The default DNP3 port number is 20000.

Master DNP3 Master address and port number:

address The IP address of the SCADA master. The address entered should be in IPv4 decimal dotted notation.

port The TCP/UDP port the serial server will connect to (TCP) or transmit to (UDP). The value entered should be a valid TCP/UDP port number. The default DNP3 port number is 20000.

Backup master DNP3 Backup Master address and port number:

address The IP address of the SCADA master. The address entered should be in IPv4 decimal dotted notation.

port The TCP/UDP port the serial server will connect to (TCP) or transmit to (UDP). The value entered should be a valid TCP/UDP port number. The default DNP3 port number is 20000.

Timeout for backup master Specify the time for which to stay connected to the back master before attempting to connect to the primary Master. Options:

Disabled Stay connected to the backup Master indefinitely. An attempt to connect with the primary master will only be made if the connection to the backup master is lost.

Fixed The connection the backup master will be maintained for the specified time in seconds.

On idle The connection to the backup master will be maintained until an idle time of the value specified is detected.

Bind to Loopback Check to bind the service to the loopback interface. Refer to section 8.3 for details on configuring the loopback interface.

Only accept data from master IP address When set, this field will cause the serial server to only accept data sourced from the address set in the **Master address** field.

Timeout for TCP connections For TCP connections only, when this field is set to a value greater than 0, the serial server will close connections that have had no receive activity for longer than specified (seconds).

Drop existing TCP connection if new received For TCP connections only, if a connection is currently active on the serial server, and a new connection request is accepted, this field determines the action that will be taken. If set, the new connection will become the active connection and the existing connection will be closed. If not set, the existing connection will remain active and the newly received connection will be closed.

Timeout between failed TCP connects For **TCP dual endpoint** only, if a connection request has failed, the server will wait the amount of time (in seconds) specified in this field before attempting another connection request. While a short time-out may cause the connection to be established more quickly, it may also cause greater network traffic if the remote host is unavailable and repeated attempts fail.

Failed TCP connects before giving up For **TCP dual endpoint** only, the serial server will attempt to establish a connection for the number of times specified in this field be giving up and waiting for a connection to be accepted.

Enable TCP no delay Check to enable TCP no delay. TCP normally uses Nagle's algorithm to combine a number of small outgoing messages, to be sent all at once. Specifically, as long as there is a sent packet for which the sender has not received an acknowledgement, the sender should keep buffering its output until it has a full packet's worth of output, so that output can be sent all at once. For serial communications this can introduce delays which can interfere with the operation of serial protocols. Enabling this option will decrease the efficiency of the TCP communications as the number of packets transmitted will increase. It is for these reason that it is recommended not to enable this option unless the application requires it to be enabled. It could also be that the Raw UDP option may be more suitable.

Destination address for UDP packets For **UDP endpoint** only, the serial server can be configured to behave as follows:

Master address and port Packets transmitted over network will always be sent to the address specified in the **Master address** and **Master port** fields.

Address and port of last request Packets transmitted over network will be sent to the source address of the most recently received packet. If no packets have been received, packets will be transmitted to the address specified in the **Master address** and **Master port** fields.

Verbose output to system log Check box to enable extended logging information to be written to the log file. This can be useful to assist when first configuring the PPP settings. It is not recommended to have extended logging enabled in a production system as the log buffer is of limited size and the higher number of logging messages could cause other log messages to be lost.

For information on setting the Port Configuration, see section 12.2.1.

Click the Update button to save and commit the changes.

12.7 Modbus IP-Serial Gateway

12.7.1 Description

The Modbus IP-Serial Gateway carries out translation between Modbus/TCP and Modbus/RTU or Modbus/ASCII. This means that Modbus serial slaves can be directly attached to the modem's serial ports without any external protocol converters.

12.7.2 Selecting the port function

The serial server configuration is accessed by selecting **Serial Server** from the main menu and **Port Setup** from the sub-menu. To enable a port for the Modbus IP-Serial Gateway function, select **Modbus IP-Serial Gateway** from the **Function** column of the appropriate port. Once selected, click **Update** to confirm the change. Once confirmed, the port will display as shown in Figure 312.

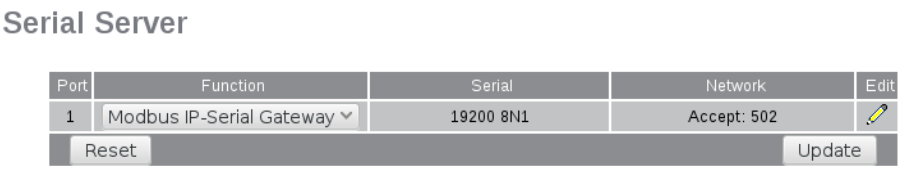


Figure 312: Selecting Modbus Gateway function

12.7.3 Configuring the port function

Once the port function has been selected, click on the icon, in the **Edit** column to edit settings for the associated port. A page similar to that shown in Figure 313, will be displayed.

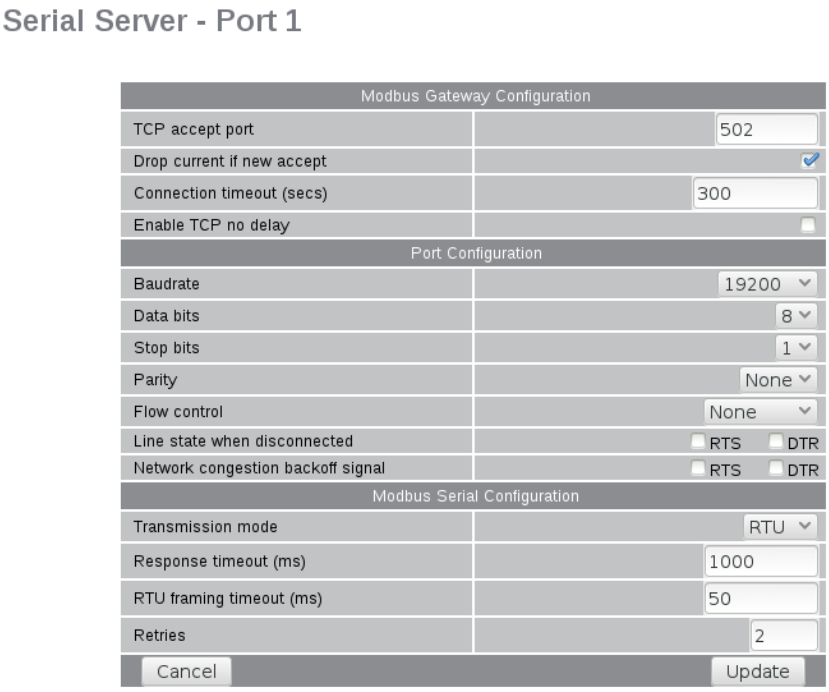


Figure 313: Modbus Gateway configuration

The following options are available for the Modbus Gateway:

Modbus Gateway Configuration TCP accept port This field determines the TCP port number that the serial server will listen for connections on. The value entered should be a valid TCP port number. The default Modbus/TCP port number is 502.

Drop current if new accept If a connection is currently active on the serial server, and a new connection request is accepted, this field determines the action that will be taken. If set, the new connection will become the active connection and the existing connection will be closed. If not set, the existing connection will remain active and the newly received connection will be closed.

Connection time-out When this field is set to a value greater than 0, the serial server will close connections that have had no network receive activity for longer than the specified period.

Enable TCP no delay Check to enable TCP no delay. TCP normally uses Nagle's algorithm to combine a number of small outgoing messages, to be sent all at once. Specifically, as long as there is a sent packet for which the sender has not received an acknowledgement, the sender should keep buffering its output until it has a full packet's worth of output, so that output can be sent all at once. For serial communications this can introduce delays which can interfere with the operation of serial protocols. Enabling this option will decrease the efficiency of the TCP communications as the number of packets transmitted will increase. It is for these reason that it is recommended not to enable this option unless the application requires it to be enabled. It could also be that the Raw UDP option may be more suitable.

Modbus Serial Configuration Transmission mode Select RTU or ASCII, based on the Modbus slave equipment attached to the port.

Response time-out This is the time-out (in milliseconds) to wait for a response from a serial slave device before retrying the request or returning an error to the Modbus master.

RTU framing time-out This is the time-out (in milliseconds) the the serial server will use to determine the boundaries of Modbus/RTU packets received on the serial port.

Retries Should no valid response be received from a Modbus slave, the value in this field determines the number of times the serial server will re-transmit requests before giving up.

For information on setting the Port Configuration, see section 12.2.1.

Click the Update button to save and commit the changes.

12.8 Telnet (RFC 2217) Server

12.8.1 Description

Telnet server mode is ideal for connecting serial terminal equipment, as a standard Telnet client can be used to connect to the server.

The Telnet sever mode also supports the RFC 2217 extensions, which, when used with a remote PC running appropriate serial port redirector software, allow port configuration changes (such as the baud-rate) to be transmitted over the network to the modem. Changes in modem handshaking lines are also transmitted.

12.8.2 Selecting the port function

The serial server configuration is accessed by selecting **Serial Server** from the main menu and **Port Setup** from the sub-menu. To enable a port for the Telnet Server function, select **Telnet (RFC 2217) Server** from the **Function** column of the appropriate port. Once selected, click **Update** to confirm the change. Once confirmed, the port will display as shown in Figure 314.

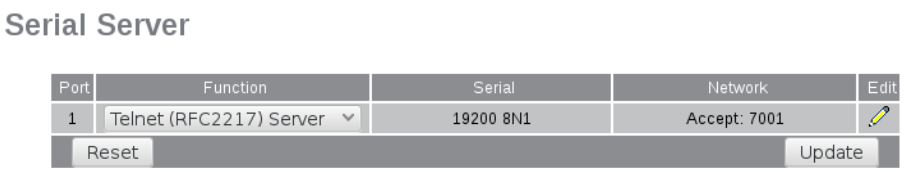


Figure 314: Selecting Telnet Server function

12.8.3 Configuring the port function

Once the port function has been selected, click on the icon, in the **Edit** column to edit settings for the associated port. A page similar to that shown in Figure 315, will be displayed.

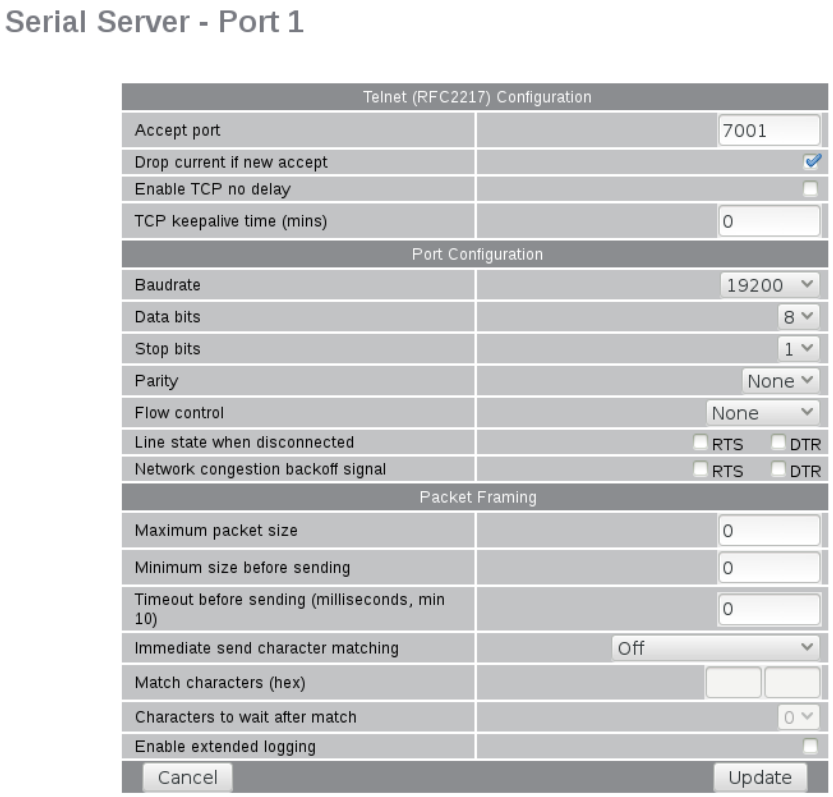


Figure 315: Telnet Server configuration

The following options are available for the Telnet (RFC 2217) Server:

Accept port This field determines the TCP port number that the serial server will listen for connections on. The value entered should be a valid TCP port number.

Drop current if new accept If a connection is currently active on the serial server, and a new connection request is accepted, this field determines the action that will be taken. If set, the new connection will become the active connection and the existing connection will be closed. If not set, the existing connection will remain active and the newly received connection will be closed.

Enable TCP no delay Check to enable TCP no delay. TCP normally uses Nagle's algorithm to combine a number of small outgoing messages, to be sent all at once. Specifically, as long as there is a sent packet for which the sender has not received an acknowledgement, the sender should keep buffering its output until it has a full packet's worth of output, so that output can be sent all at once. For serial communications this can introduce delays which can interfere with the operation of serial protocols. Enabling this option will decrease the efficiency of the TCP communications as the number of packets transmitted will increase. It is for these reason that it is recommended not to enable this option unless the application requires it to be enabled. It could also be that the Raw UDP option may be more suitable.

TCP keepalive time When set to a value greater than 0, TCP keep-alives will be enabled for connections, with probes sent at the frequency specified (minutes). This may assist in detecting failed connections.

For information on setting the Port Configuration, see section 12.2.1. For information on setting the Packet Framing, see section 12.2.2.

Click the Update button to save and commit the changes.

12.9 PPP Server

12.9.1 Description

PPP Server description.

12.9.2 Selecting the port function

The serial server configuration is accessed by selecting **Serial Server** from the main menu and **Port Setup** from the sub-menu. To enable a port for the Telnet Server function, select **PPP Server** from the **Function** column of the appropriate port. Once selected, click **Update** to confirm the change. Once confirmed, the port will display as shown in Figure 316.

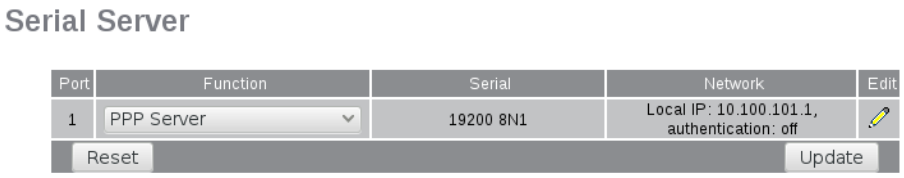


Figure 316: Selecting PPP Server function

12.9.3 Configuring the port function

Once the port function has been selected, click on the icon, in the **Edit** column to edit settings for the associated port. A page similar to that shown in Figure 317, will be displayed.

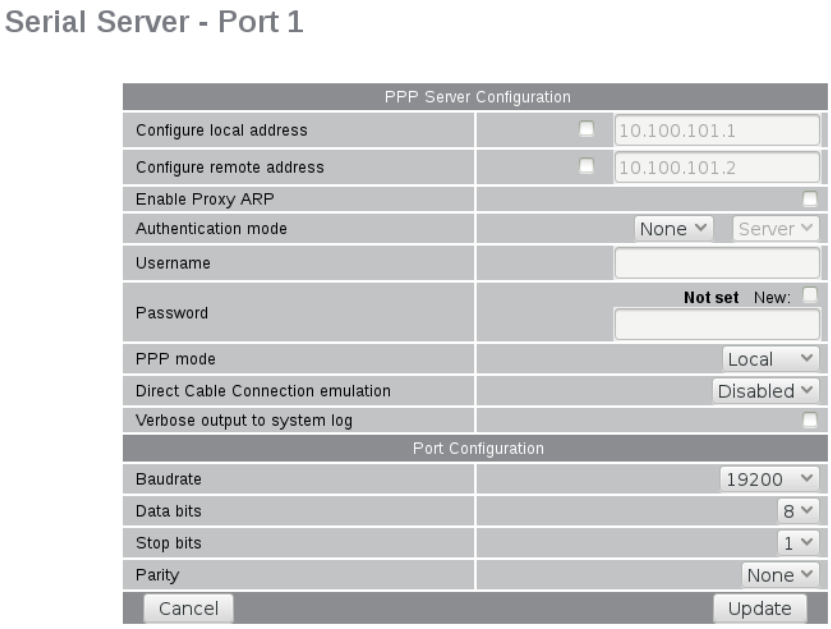


Figure 317: PPP Server configuration

The following options are available for the PPP Server:

Configure local address Check to enable and enter an IP address. This is the IP address the modem will have in the PPP connection. The address entered should be in IPv4 decimal dotted notation (eg. 10.100.100.1).

Configure remote address Check to enable and enter an IP address. This is the IP address the modem will allocate to the connection PPP client. The address entered should be in IPv4 decimal dotted notation (eg. 10.100.100.1) and must be different to the **Local IP address**.

Enable Proxy ARP Check to enable. Proxy ARP is a technique by which a device on a given network, in this case the modem, answers the ARP queries for a network address that is on a different network, in this case the network of the remote IP address.

Authentication mode This fields sets the required level of authentication for remote users connecting to the modem when operating in Server mode or the authentication to use when operating in client mode and connection to a remote server.

Authentication_type: None No authentication will be required.

PAP Authentication will be required using the PAP protocol.

CHAP Authentication will be required using the CHAP protocol.

Mode: Server Set to PPP server. Receive remote connections.

Client Set to PPP client. Connect to remote servers.

Username Where **Authentication** is not set to **None**, this is the user-name a remote user will be required to authenticate with.

Password Where **Authentication** is not set to **None**, this is the password a remote user will be required to authenticate with. To set the password, click the **New** check-box and enter the password in the adjacent field.

PPP mode Select from:

Local Ignores the serial port control lines.

Modem Uses the serial port control lines.

Direct Cable Connection emulation Direct Cable Connection (DCC), is a feature of Microsoft Windows which allows a computer to transfer data with another computer, using either the serial port of each computer. This option is only available if the PPP mode is set to local. Select from:

Disabled Disabled Direct Cable Connection.

Host Act as the host and receive connections from a guest.

Guest Act as the guest and make a connection to a host.

Verbose output to system log Check box to enable extended logging information to be written to the log file. This can be useful to assist when first configuring the PPP settings. It is not recommended to have extended logging enabled in a production system as the log buffer is of limited size and the higher number of logging messages could cause other log messages to be lost.

For information on setting the Port Configuration, see section 12.2.1. For information on setting the Packet Framing, see section 12.2.2.

Click the Update button to save and commit the changes.

12.10 PPP Dial-Out Client

12.10.1 Description

PPP Dial-out Client can be used to establish a PPP connection to a remote PPP server over the serial port. It would typically be used to connect via a dial-up modem connected to the serial port of the unit.

12.10.2 Selecting the port function

The serial server configuration is accessed by selecting **Serial Server** from the main menu and **Port Setup** from the sub-menu. To enable a port for the Telnet Server function, select **PPP Dialout Client** from the **Function** column of the appropriate port. Once selected, click **Update** to confirm the change. Once confirmed, the port will display as shown in Figure 318.

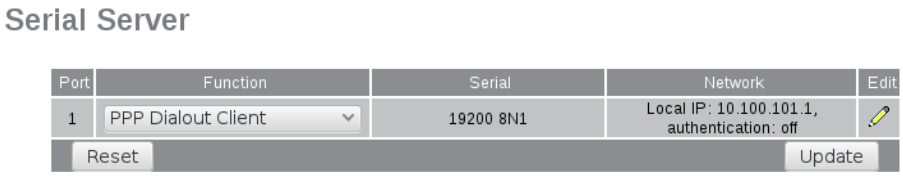


Figure 318: Selecting Telnet Server function

12.10.3 Configuring the port function

Once the port function has been selected, click on the icon, in the **Edit** column to edit settings for the associated port. A page similar to that shown in Figure 319, will be displayed.

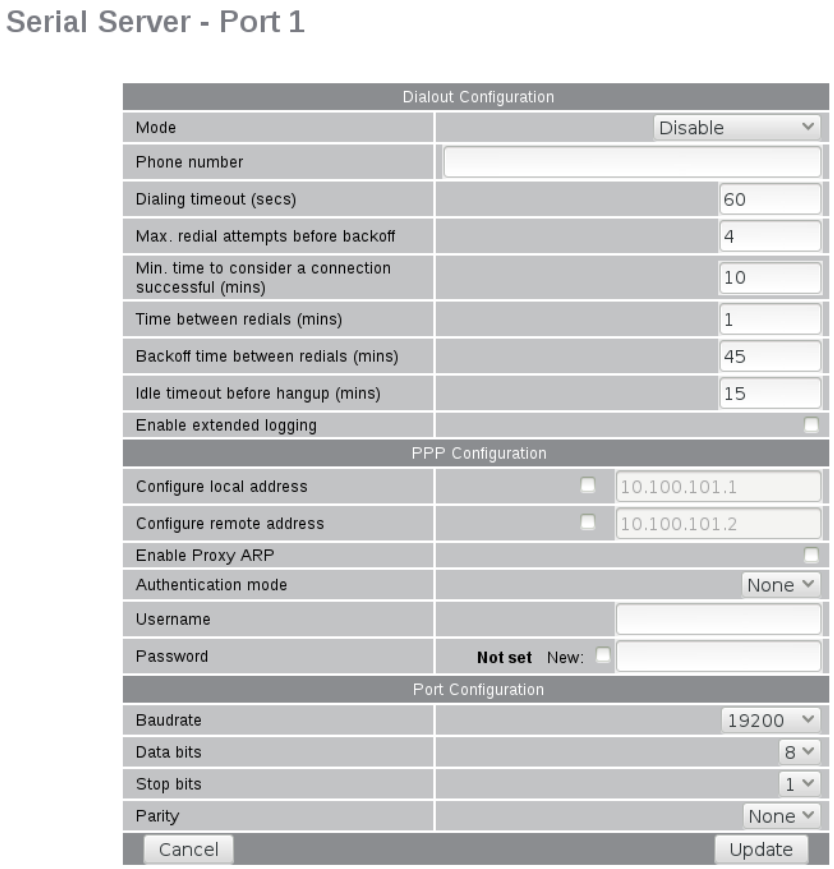


Figure 319: Telnet Server configuration

The following options are available for the PPP Dial-Out Client:

Dialout Configuration Mode This fields sets the operating mode. Available options are:

Disable Disable dial out.

Manual The connection is controlled manually by clicking the Connect and Disconnect buttons which are added to the Serial Server page when this mode is selected.

On demand The connection is made when data is sent to the interface.

Always connect The connection is permanently established.

Phone number The number of the remote server to dial.

Dialing timeout The time in seconds to wait for a connection after dialling.

Max. redial attempts before backoff Set the number of failed dialling attempts after which the time between dialling will be increased. This back-off prevents continuously dialling at a fast rate possibly incurring large call costs.

Min. time to consider a connection successful The minimum connection time in minutes which is considered a successful connection.

Time between redials The time in minutes to wait after a failed dial attempt before redialling.

Backoff time between redials The time in minutes to wait to redial after the back-off count has been reached.

Idle timeout before hangup The connection is considered idle when no data has been transmitted or received for this time in minutes. Once the idle time is reached the connection will be terminated.

Enable debugging information If enabled debugging information is written to the log. This can assist in diagnosing connection problems.

PPP Server Configuration **Local IP address** Check to enable and enter an IP address. This is the IP address the modem will have in the PPP connection. The address entered should be in IPv4 decimal dotted notation (eg. 10.100.100.1).

Remote IP address Check to enable and enter an IP address. This is the IP address the modem will allocate to the connection PPP client. The address entered should be in IPv4 decimal dotted notation (eg. 10.100.100.1) and must be different to the **Local IP address**.

Enable Proxy ARP Check to enable. Proxy ARP is a technique by which a device on a given network, in this case the modem, answers the ARP queries for a network address that is on a different network, in this case the network of the remote IP address.

Authentication required This fields sets the required level of authentication for remote users connecting to the modem. Available options are:

None No authentication will be required.

PAP Authentication will be required using the PAP protocol.

CHAP Authentication will be required using the CHAP protocol.

Username Where **Authentication** is not set to **None**, this is the user-name a remote user will be required to authenticate with.

Password Where **Authentication** is not set to **None**, this is the password a remote user will be required to authenticate with. To set the password, click the **New** check-box and enter the password in the adjacent field.

For information on setting the Port Configuration, see section 12.2.1.

Click the Update button to save and commit the changes.

12.11 Phone Book

12.11.1 Description

The Phone Book works in conjunction with the Modem Emulator to provide a translation table from traditional phone numbers to IP addresses and port numbers. This allows the Modem Emulator to be used as a drop in replacement for a traditional dial-up modem and to create IP connections rather than phone calls.

For more information on the Modem Emulator, see section 12.5.

To access the Phone Book configuration, select Serial Server ▷ Port Setup from the menu. The page will initially have no entries, as shown in Figure 320.

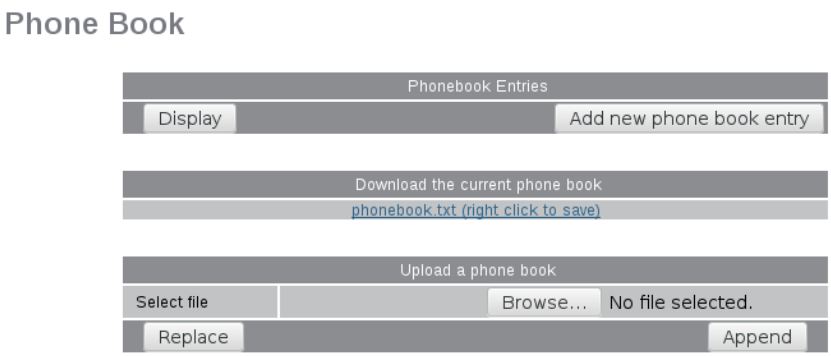


Figure 320: The main Phone Book page

12.11.2 Phone book Entries

This section shows a summary of the current phone book entries, the Display button displays the complete details of the current entry list in tabular format, and new entries can be added by clicking the **Add new phone book entry** button.

A phone book entry consists of a dial string and one or more contact addresses. If more than one connection address is entered for a dial string each address is tried in turn until a connection is made.

To add a new phone book entry click the Add new phone book entry button on the main Phone Book page. The phone book entry page will be displayed as shown in Figure 321.

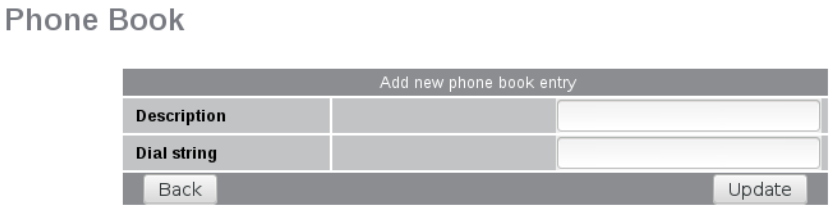


Figure 321: Page for adding Phone Book entry

The following options can be set for each entry:

Description A description for the entry.

Dial string The dial string which will be matched to received dial strings.

Once the details have been entered click the Update button to save and commit the changes. The page will refresh and now include a table for connection entries, as shown in figure 322.

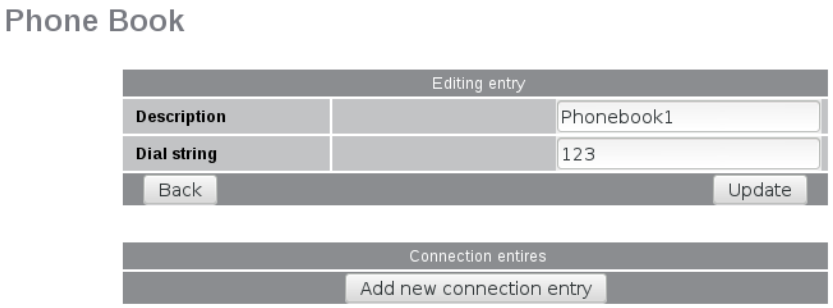


Figure 322: Page for adding Phone Book entry

To add a connection entry click the Add new connection entry button. The connection entry page will be displayed as shown in Figure 321.

Figure 323: Page for adding Phone Book entry

The following options can be set for each entry:

Description A description for the entry.

Connect address This is the IP address the serial server will attempt to connect to.

Connect port This is the IP port number the serial server will attempt to connect to.

Click the Update button to save and commit the entry. Further entries can be added by repeating the process, each new entry will be associated with the dial string entered at the first step.

After completing the phone book entry click the Back button to return to the main phone book page.

12.11.3 Example of Adding a new phone book entry

In this example a new entry is created that translates dial string 123 to connection address 123.123.123.123:123.

From the main phone book page click the Add new phone book entry button. First the details for dial string are added as shown in Figure 324.

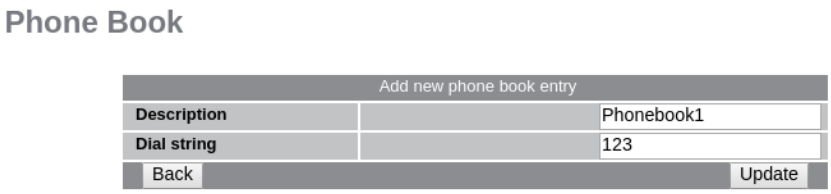


Figure 324: Adding a Phone Book Entry

Click the Update button to save and commit the entry. The page will be updated to include the connection entries table as shown in Figure 325.

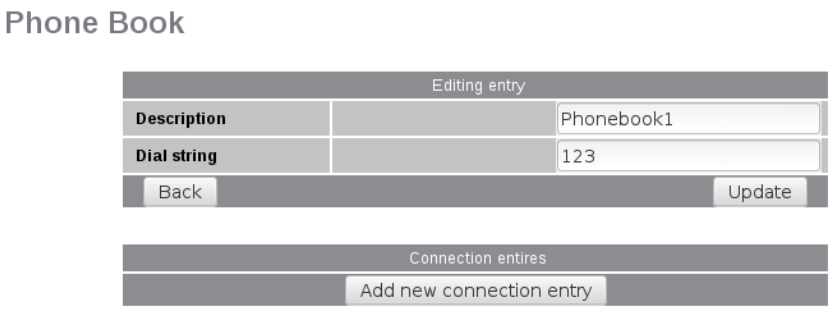


Figure 325: The add phone book entry page with the Connection entries table shown.

Click the Add new connection entry button, now the details for the connection can be added as shown in figure 326.

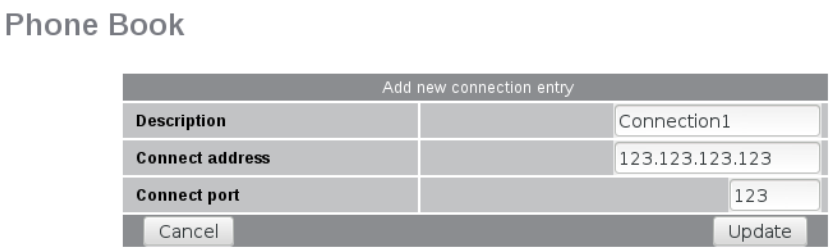


Figure 326: The Phone Book page with a single entry

Click the Update button to save and commit the connection entry.

The page will return to the phone book entry page with the connection now listed in the Connection entries table, as shown in figure 327.

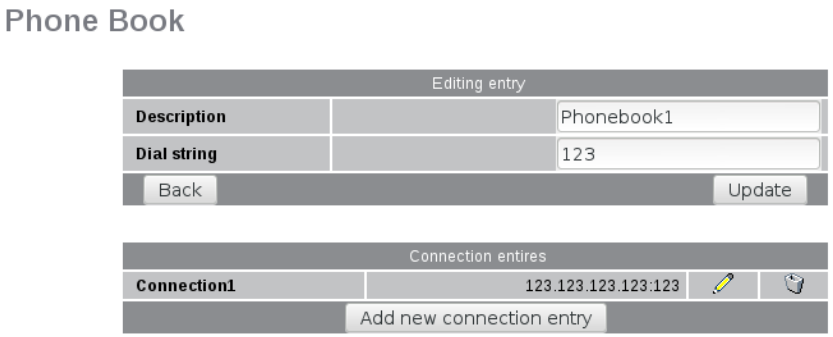


Figure 327: The Phone Book page with a single entry

Click the Back button to return to the main Phone Book page.

The page will return to the phone book entry page with the new phone book entry listed in the main table, as shown in figure 328.

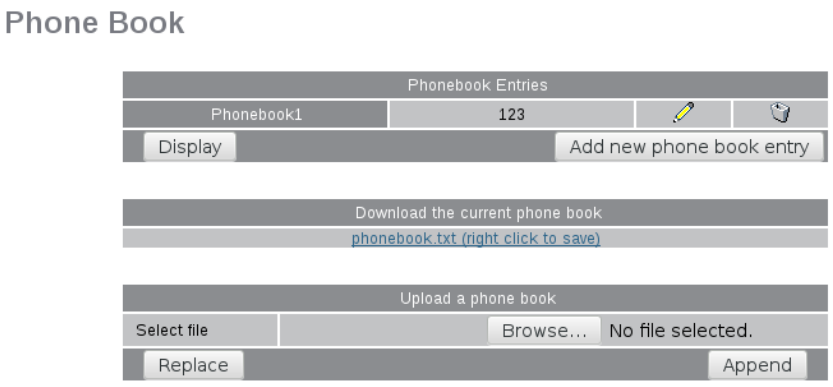


Figure 328: The Phone Book page with a single entry

12.11.4 Example of Adding a Second phone book entry

In this example a second entry will be created created, called Phonebook2, this entry will translate dial string 234 to two connection addresses, 'Connection1' with address is 123.123.123.123:123 and 'Connection2' with address is 234.234.234.234:234.

To add a second entry click the Add new phone book entry button. First the details for the dial string are entered as shown in Figure 329.

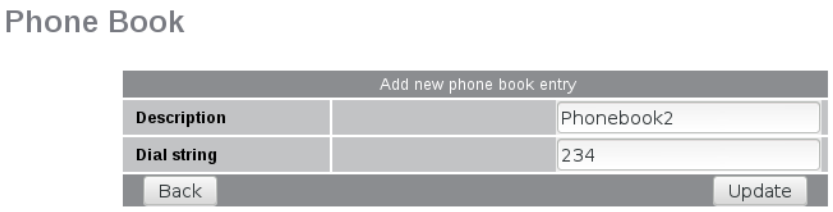


Figure 329: Adding a second phone book entry

To commit the new phone book entry to the table, click the Update button. The add entry page will update to show the connection entries table shown in Figure 330.

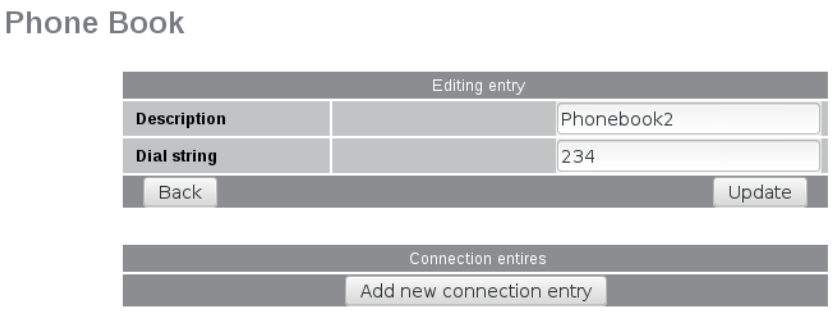


Figure 330: The second phone book entry has been added.

Click the Add new connection entry button, now the details for the connection can be added as shown in figure 331.

Figure 331: The Phone Book page with a single entry

Click the Update button to save and commit the connection entry.

The page will return to the phone book entry page with the connection now listed in the Connection entries table, as shown in figure 332.

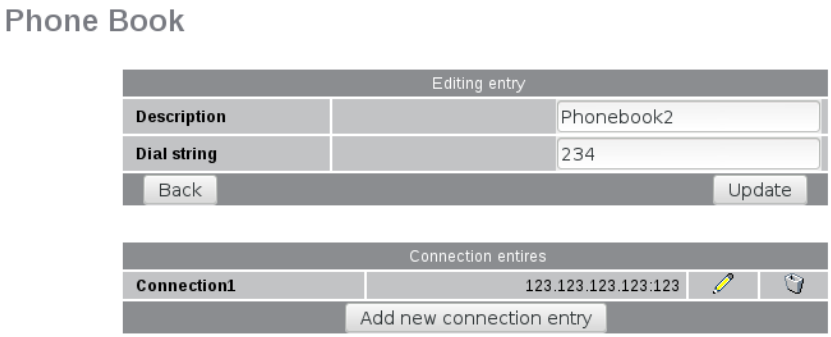


Figure 332: The Phone Book page with a single entry

To add the second connection, again click the Add new connection entry button, the details for the connection can be added as shown in figure 333.

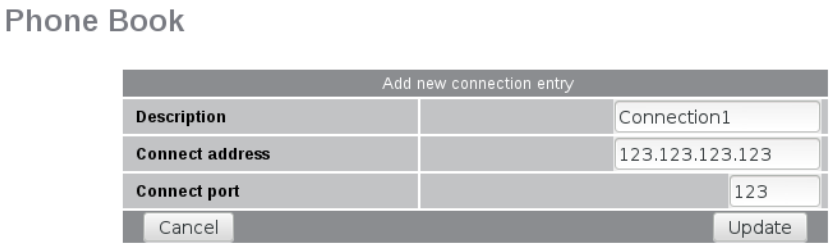


Figure 333: The Phone Book page with a single entry

Click the Update button to save and commit the connection entry.

The page will return to the phone book entry page with both of the connections now listed in the Connection entries table, as shown in figure 334.

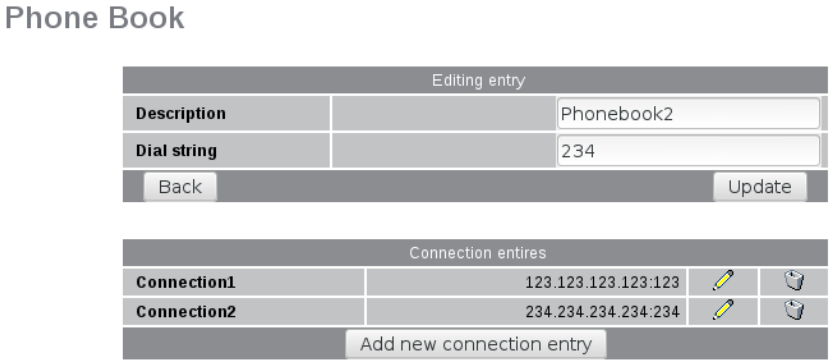


Figure 334: The Phone Book page with a single entry

Click the Back button to return to the main Phone Book page.

The page will return to the phone book entry page with the new phone book entry listed in the main table, as shown in figure 335.

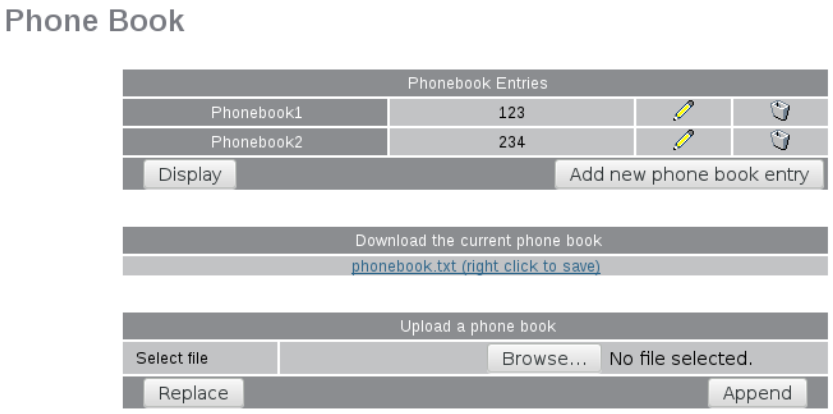


Figure 335: The Phone Book display page with 2 example entries.

12.11.5 Display Phone Book Entry Details

The table show on the main Phone Book page is a summary and does not include the full connection details. The display the list of phone book entries with the connection details for each entry click the Display button. The page shown in figure 336 is the display page after the two entries described in the examples above have been added.

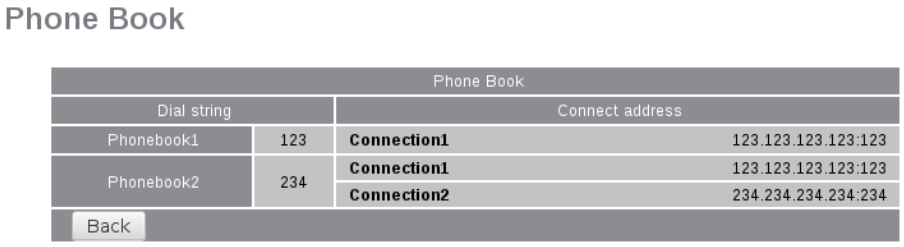


Figure 336: The Phone Book page with a single entry

12.11.6 Editing a phone book entry

A phone book entry can be edited by clicking the icon in the **Edit** column of the entry to be changed. Once clicked, the details of the entry will be displayed in the same table as when creating a new phone book entry.

As an example, to edit the second phone book entry in the table, click the icon in the second row of the table. In this example the dial string will be changed to 235, changes were made as shown in Figure 337.

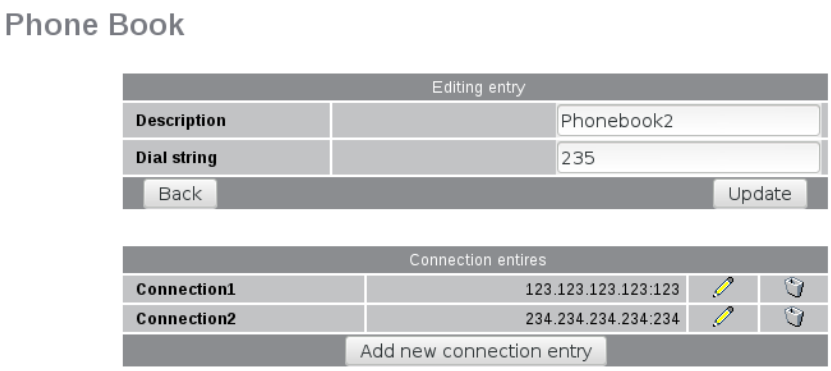


Figure 337: Editing a phone book entry

To save the changes click the Update button or to cancel any changes click the Cancel button. The main page will again be displayed as shown in Figure 338, with the changes for entry 2 added to the table.

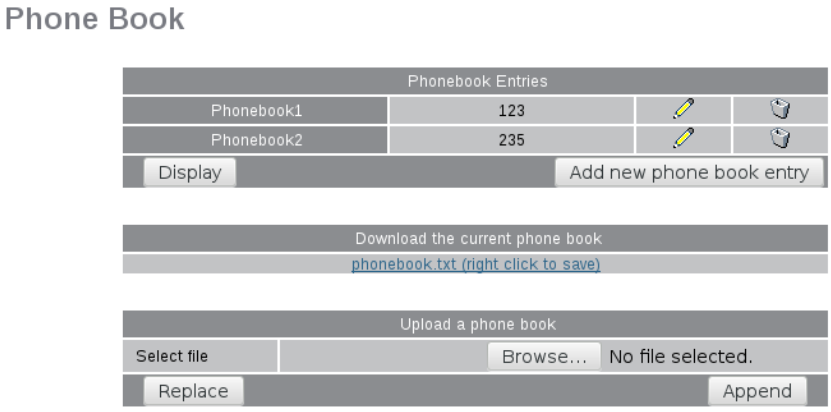


Figure 338: Main phone book page with revised entry

12.11.7 Editing a phone book connection entry

The connection for a phone book entry can be edited by clicking the icon in the **Edit** column of the entry to be changed. Once clicked, the details of the entry will be displayed in the same table as when creating a new phone book entry. To edit a connection entry click the icon in the **Edit** column of the connection entry to be edited.

As an example, the second connection entry 'Connection2' for the 'Phonebook2' entry will be edited to use port 123. To edit the connection entry, first click the icon in the second row of the table for the entry 'Phonebook2'. Once clicked the details for the phone book entry will be displayed as shown in figure 339.

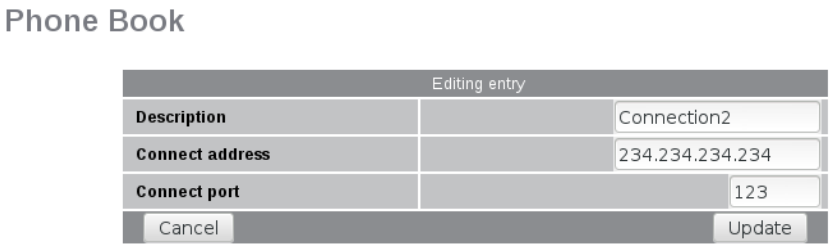


Figure 339: Editing a phone book entry

To select the connection entry for editing click the icon in the second row of the connection entries table Once clicked the details for the phone book entry will be displayed as shown in figure 340.

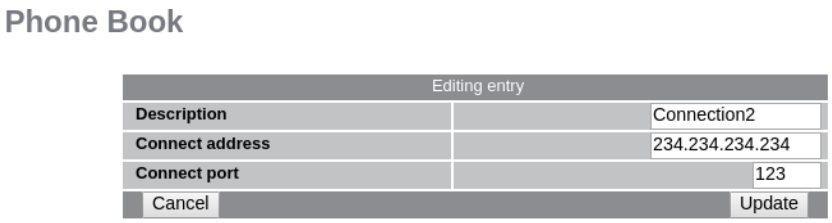


Figure 340: Editing a phone book entry

To save the changes click the Update button or to cancel any changes click the Cancel button.The phone book entry page will again be displayed as shown in Figure 341, with the changes for connection entry 2 updated in the connection entries table.

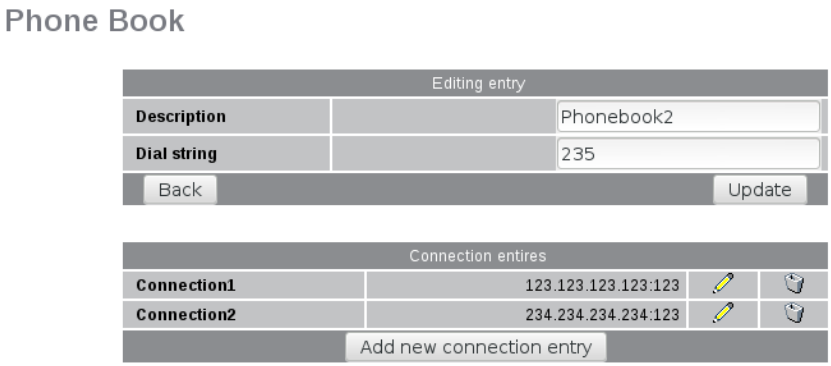


Figure 341: Main phone book page with revised entry

To return to the phone book page click the Back button. The main phone book page will again be displayed as shown in Figure 342.

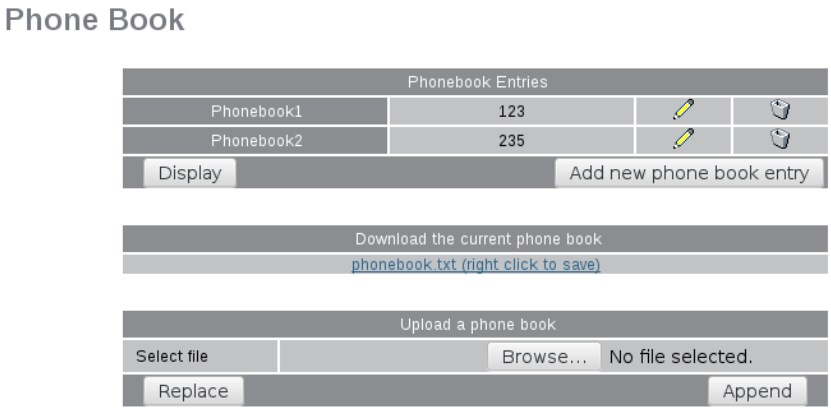


Figure 342: Main phone book page with revised entry

The table shown is a summary of the phone book entries and so the connection details are not shown. To see the full details of the phone book click the Display button, the full details of the phone book will now be displayed as shown in Figure 343.

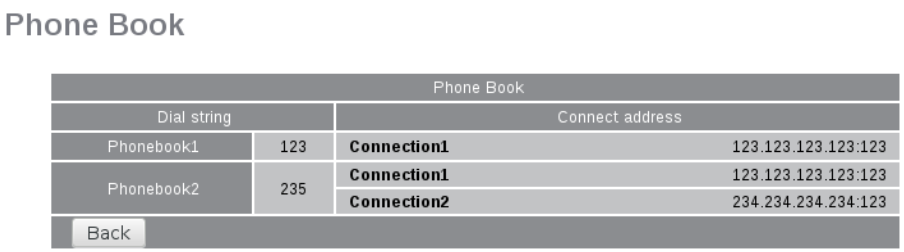


Figure 343: Main phone book page with revised entry

To return to the main phone book page click the Back button.

12.11.8 Deleting a phone book connection entry

A phone book connection entry can be deleted by first clicking the edit icon to edit the phone book entry containing the connection entry and clicking the icon in the **Delete** column of the connection entry to be deleted. A warning box will be displayed. Click the OK button to confirm the deletion.

Deleting of phone book connection details is provided for management of the connection entry details, there is no requirement to delete the connection entries prior to deleting a phone book entry. If the entire phone entry is to be deleted refer to section 12.11.9.

For example, to delete connection entry 'Connection2' for phone book entry 'Phonebook2' first click the edit icon for the 'Phonebook2' entry on the main phone book page. The details for the entry will be displayed as shown in figure 338.

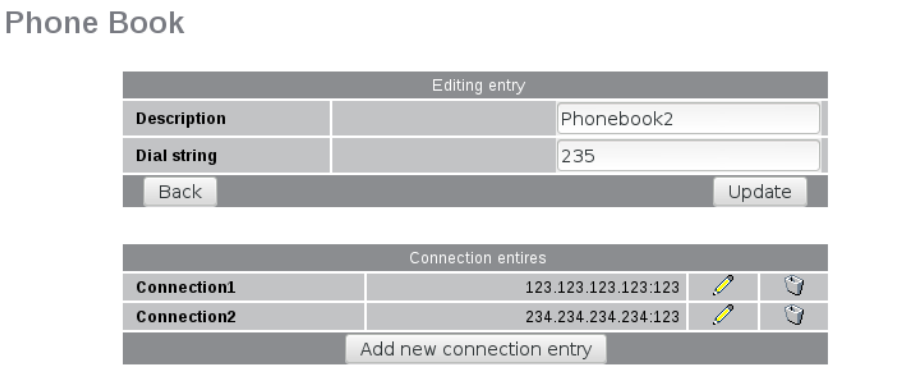


Figure 344: Deleting a phone book entry

To delete the connection entry 'Connection2' click the icon in the **Delete** column of the row labelled 'Connection2'. A warning box will be displayed. Click the OK button to confirm the deletion, as shown in Figure 345.

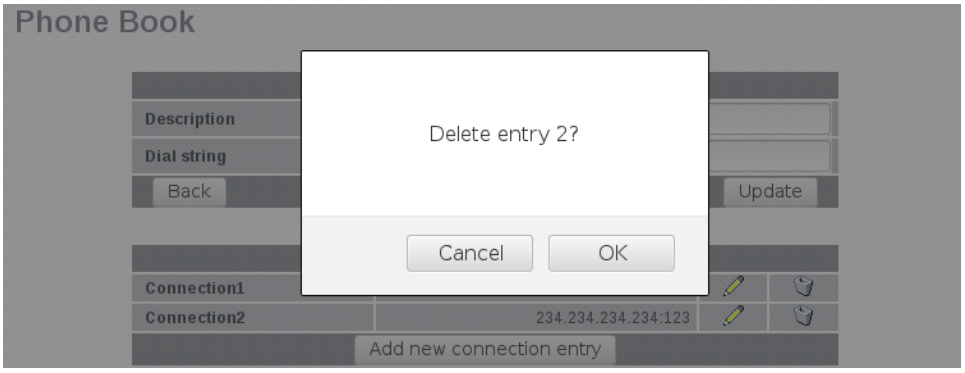


Figure 345: Phone book table after deletion of entry

The connection entry table will be updated with the entry removed, as shown in Figure 346.

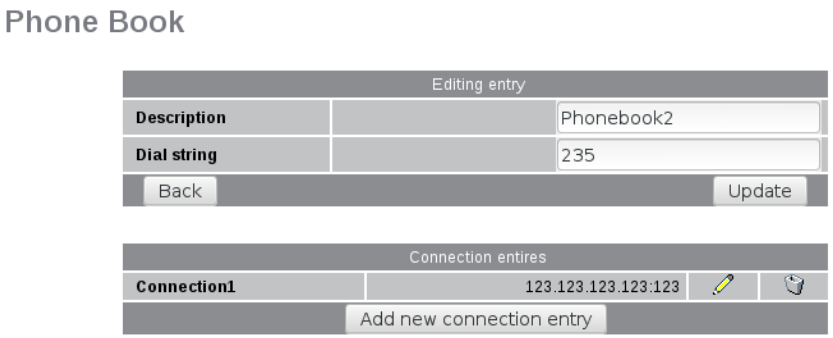


Figure 346: Phone book table after deletion of entry

To return to the main phone book page click the Back button, as shown figure 347 the phone book entries will appear similar to before the deletion because the connection entries are not shown in the summary table.

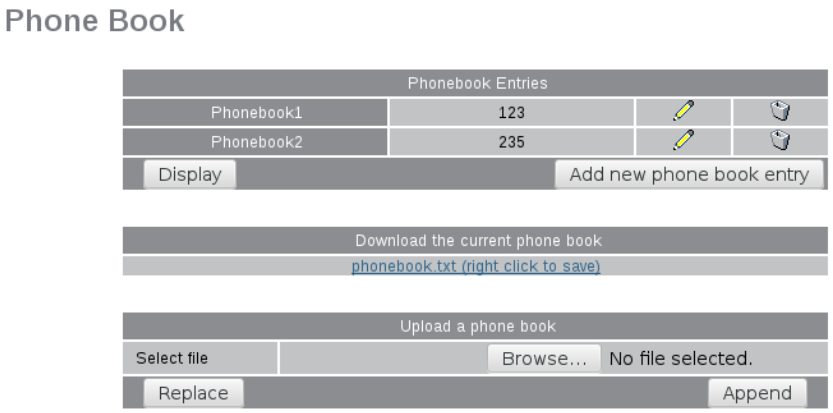


Figure 347: Phone book table after deletion of entry

The display the full update phone book table click the Display button and the full table will be shown as in figure 348.

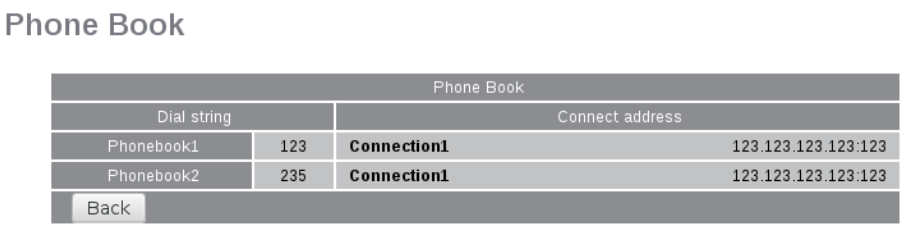


Figure 348: Phone book table after deletion of entry

12.11.9 Deleting a phone book entry

A phone book entry can be deleted by clicking the icon in the **Delete** column of the entry to be deleted. A warning box will be displayed. Click the OK button to confirm the deletion.

Deleting a phone book entry will also delete all associated connection entries. There is no requirement to delete the connection entries prior to deleting a phone book entry.

For example, to delete phone book 'Phonebook2' from the table shown in figure 338, click the icon in row labelled 'Phonebook2'. A warning box will now be displayed as shown if Figure 349. Click the OK button to confirm the detention.

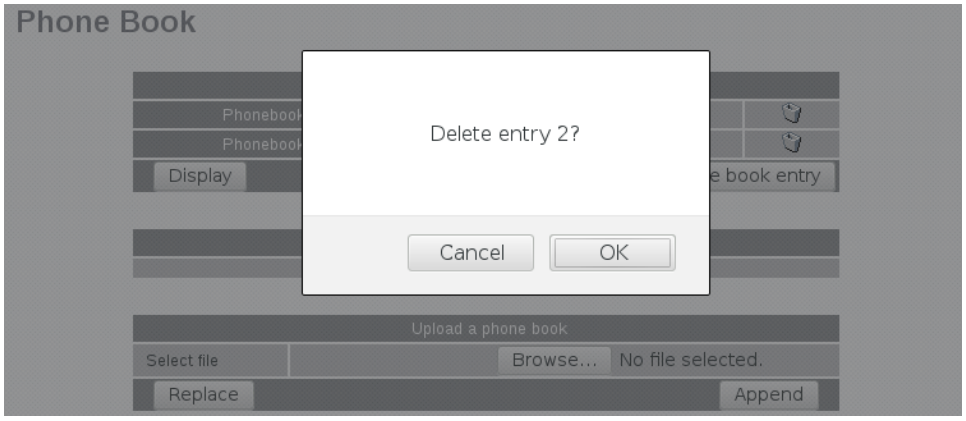


Figure 349: Deleting a phone book entry

The phone book table will be displayed with the entry removed, as shown in Figure 350.

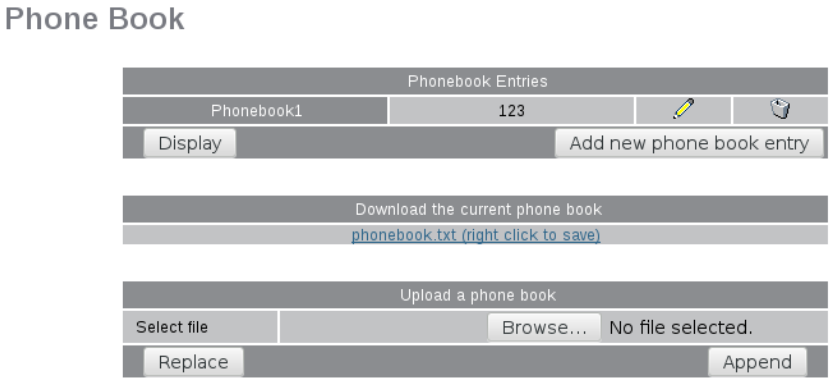


Figure 350: Phone book table after deletion of entry

To display the full updated phone table click the Display button, the table will have been updates to that shown in Figure 351.

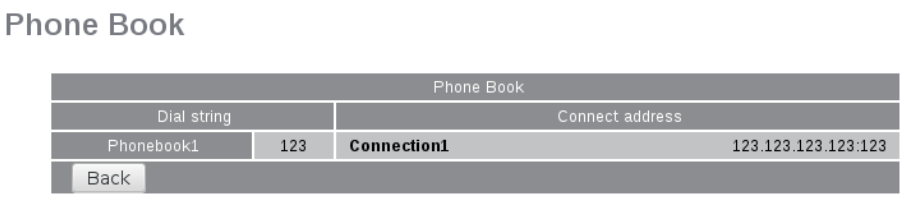


Figure 351: Phone book table after deletion of entry

12.11.10 Exporting the phone book

The current phone book can be exported as a CSV file. The file can be accessed via the link in the section of the page labelled “Download the current phone book”. Clicking the link will display the file as a text file. To save the file right click the link and select ’Save as...’.

Figure 352: The download section of the phone book page.

12.11.11 Importing phone book entries

A CSV file containing phone book entries can be imported. The imported file can either replace to current phone book or be appended to it. To import a file first click the Choose file button in the Select file row of the table under the section titled “Upload a phone book”, then select the file. The file name will now be displayed next to the Choose file button. To load the file click either the Replace button to replace all entries in the current phone book with those contained in the file or the click the Append button to add the entries in the file to the current phone book.

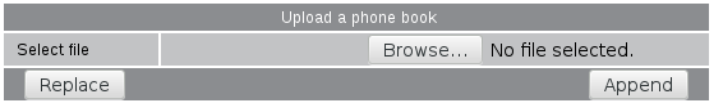


Figure 353: The upload section of the phone book page.

12.11.12 Phone book CSV file format

The first line of the CSV file contains the columns names:

```
"Dial String","Connect Address","Connect Port","Description"
```

The details for the column names are:

Dial String The dial string

Connect Address The connection IP address

Connect Port The connection port number

Description The description or label for the entry.

There are 2 types of entries in the file a dial entry and a connection entry.

The dial entry contains only a dial string and a description the other fields are left blank. An example dial entry is:

```
"123","","","Phonebook1"
```

A connection entry has values for each field. An example connection entry is

```
"123","123.123.123.123","123","Connection1"
```

For this example the complete listing is:

```
"Dial String","Connect Address","Connect Port","Description"
"123","","","Phonebook1"
"123","123.123.123.123","123","Connection1"
```

12.11.13 Example of importing a phone book

In this example a new phone book entry with a number of connection entries will be added to the phone book. The dial string for the new entry will be labelled 'Phonebook2' for number "456" and it will have associated with it 10 connection entries.

The first step is to create CSV file for the entries, as shown:

```
"Dial String","Connect Address","Connect Port","Description"
"456","","","Phonebook2"
"456","123.123.123.120","123","Connection0"
"456","123.123.123.121","123","Connection1"
"456","123.123.123.122","123","Connection2"
"456","123.123.123.123","123","Connection3"
"456","123.123.123.124","123","Connection4"
"456","123.123.123.125","123","Connection5"
"456","123.123.123.126","123","Connection6"
"456","123.123.123.127","123","Connection7"
"456","123.123.123.128","123","Connection8"
"456","123.123.123.123","123","Connection9"
```

The file was saved as 'phonebook-Test1.txt'.

The next step is to upload the file, from the phone book page, as shown in figure 354, click the Choose file button in the 'Upload a phone book' table, and select the file.

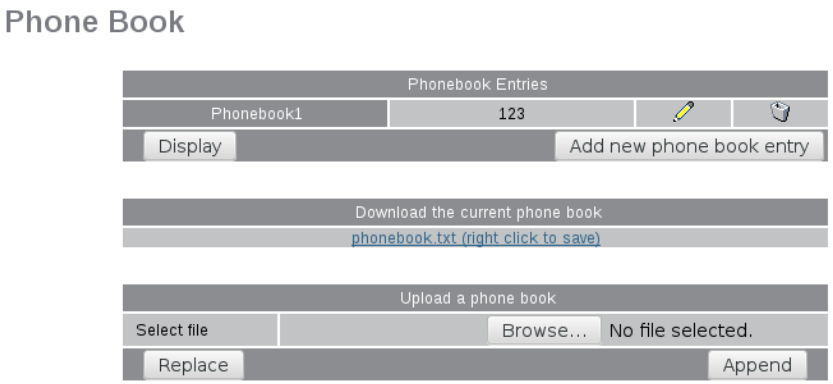


Figure 354: Upload a phone book CSV file.

Once selected the file name of the file to be uploaded will be shown next to the Choose file button, as shown in Figure 355.

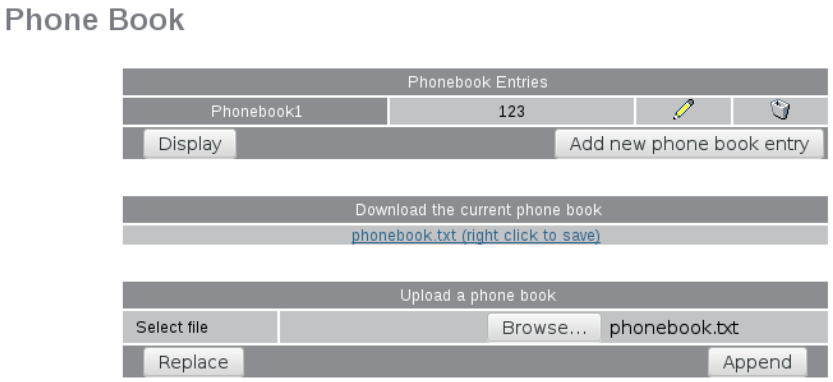


Figure 355: File to be uploaded has been selected.

To upload the file click the Append button, the file will be uploaded and the page will update to shown the new dial entry for 'Phonebook2', as shown in Figure 356.

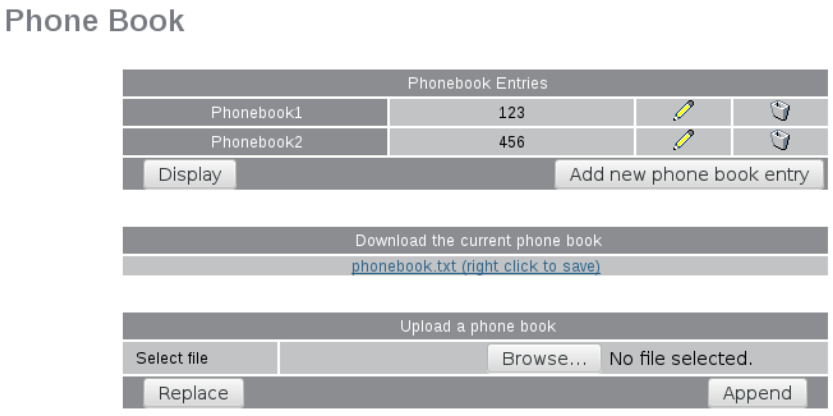


Figure 356: Phone book table with new entry shown.

To display the full details of the updated phone table click the Display button, the table will have been updated to that shown in Figure 357.

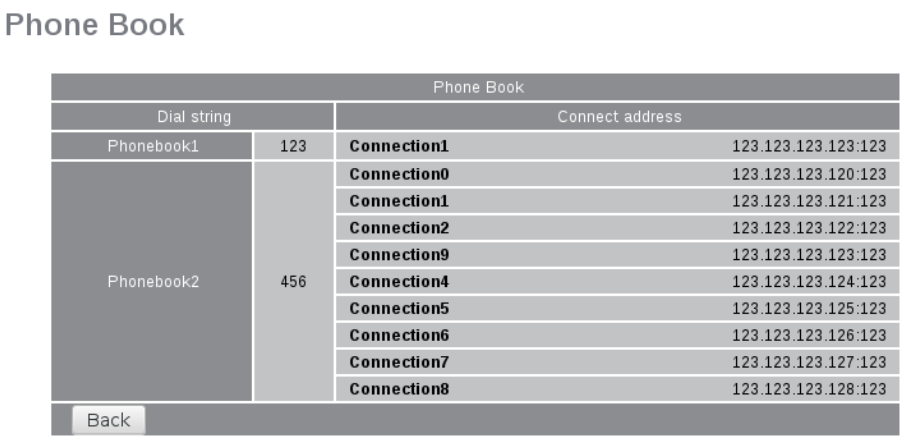


Figure 357: Phone book table with new entries added.

13 Management

The Management section is used to configure the management and system reporting options for services including events, SNMP, DNP3, SMS and email.

The main management page is accessed by clicking the Management tab on the main menu, a page similar to that shown is figure 358 will be displayed. The number and type of events listed will depend on the model.

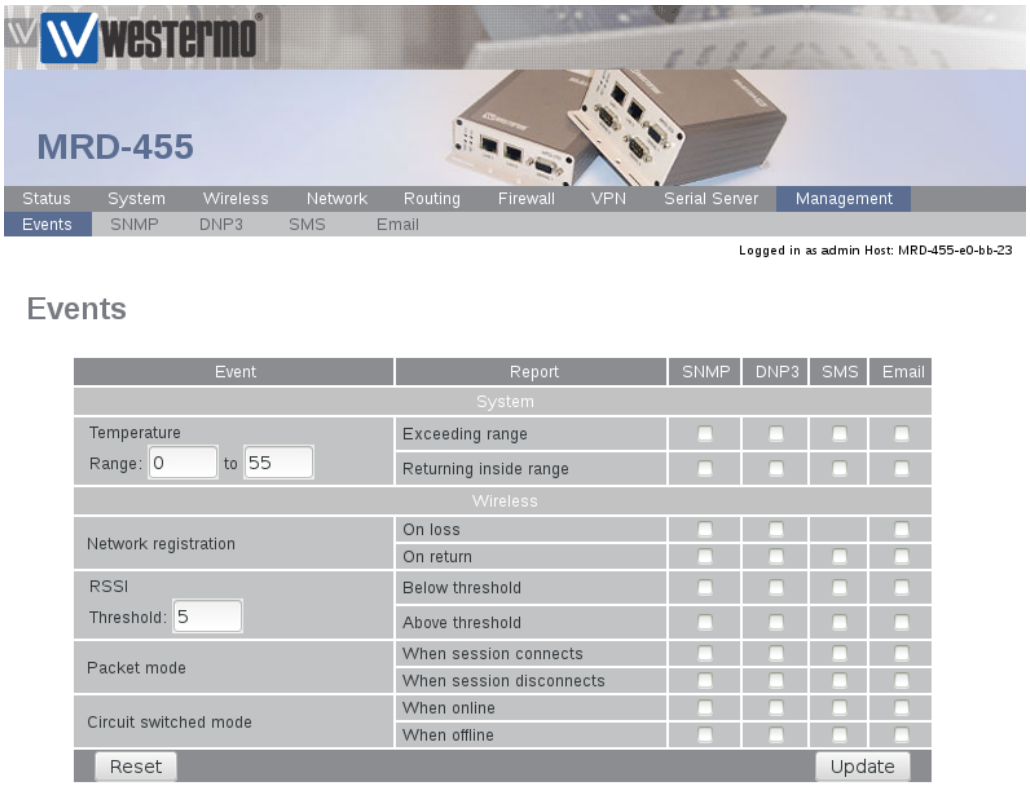


Figure 358: Main management page.

13.1 Events

The Events page is selected by clicking Management ▷ Events. Figure 359 is an example of the Events Management page for models with GPIO and Figure 360 is an example of the Events Management page for a model with GPIO.

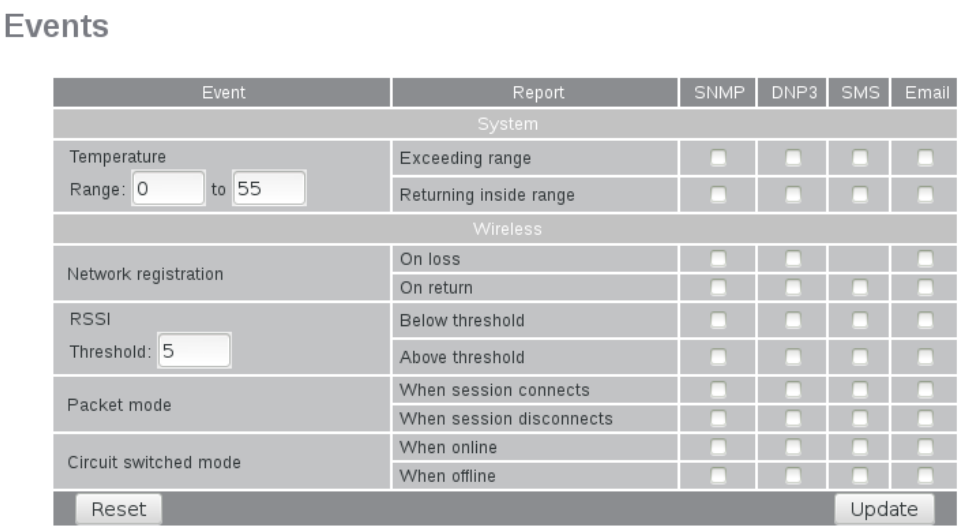


Figure 359: Events Management page .

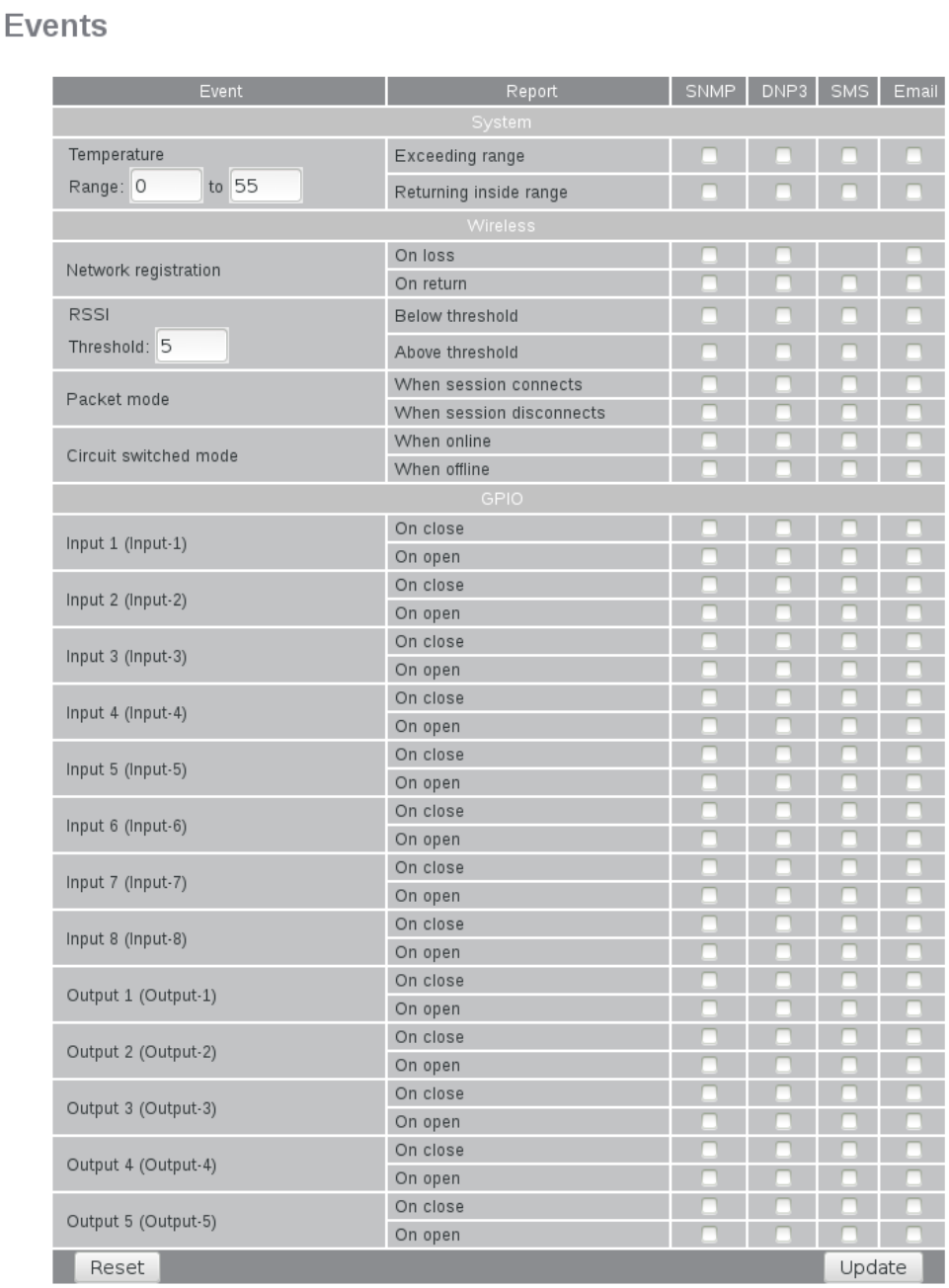


Figure 360: Events Management page with GPIO.

13.1.1 Event Types

The events which may generate triggers are listed in the first column of Events table. The events are as follows:

Temperature The nominal operating range of the may be specified. Events may be generated:

Exceeding range Triggered when the temperature is outside the nominal range. That is lower than the low temperature to higher than the high temperature as set in the range.

Returning inside range Triggered when the temperature returns within the nominal range limits.

The current operating temperature is reported on the Status ▷ Alarms page. Refer to Section 4.1 on page 14 for details.

Network registration The network registration status. Events may be generated:

On loss Triggered when the network registration moves from the connected state to the disconnected state. Note this event cannot trigger an SMS as it will not be possible to send an SMS without network registration.

On return Triggered when network registration is established.

RSSI A threshold may be set for the Receive Signal Strength Indicator (RSSI). Events may be generated:

Threshold Specify the trigger threshold. Minimum 0, maximum 30

Below threshold Triggered when RSSI falls below the threshold.

Above threshold Triggered when RSSI raises above the threshold.

Packet mode The packet mode status. Event may be generated:

When session connects Triggered when a packet mode session connects.

When session disconnects Triggered when a packet mode session disconnects.

Circuit switched mode The Circuit Switched Data (CSD) mode status. Events may be generated:

When online When CSD connects. This will trigger for both incoming and outgoing connections.

When offline When CSD disconnects.

The current state of the wireless connection can be found on the Status ▷ Wireless page. Refer to Section 4.2 on page 16 for details.

GPIO The General Purpose Inputs and Outputs. These events are only available for the models with GPIO. The following events may be generated:

Input n (Input-Name-n) GPIO Input 1, the label associated with the input will be shown enclosed by brackets, for example "(Input 1 label").

On close Triggered when the input transitions from the open to the closed state.

On open Triggered when the input transitions from the closed to the open state.

Output n (Output-Name-n) GPIO Output 1, the label associated with the input will be shown enclosed by brackets, for example "(Output 1 label").

On close Triggered when the output transitions from the open to the closed state.

On open Triggered when the output transitions from the closed to the open state.

Where n represent the number of the input or output.

13.1.2 Trigger Types

When an event condition is met it may generate a trigger which is any of:

None The trigger does not generate any message.

SNMP An SNMP trap is generated.

DNP3 A DNP3 exception is generated.

SMS An SMS is generated.

Email An email is generated.

To select a trigger for an event check the check box for the event row corresponding to the trigger type column. For example to enable SNMP traps for Network Registration loss and return check the two check-boxes in the Network registration row, under the SNMP column. This is illustrated in Figure 361 with the Network Registration selected for SNMP.

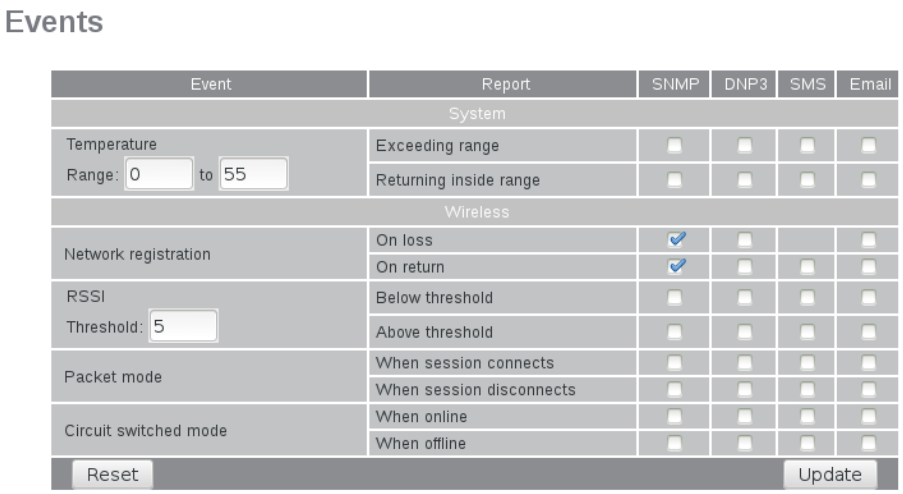


Figure 361: Enabling SNMP traps for the Network Registration events.

Click the Update button to save and commit changes.

13.2 SNMP

The Simple Network Management Protocol (SNMP) can be used for network management of the unit. The current connection status and RF signal level are examples of status variables accessible through SNMP. The custom MIB file for the modem is available for download from the Cybertec website.

The SNMP configuration options are accessed by selecting Management ▷ System. The SNMP configuration page is show in Figure 362.

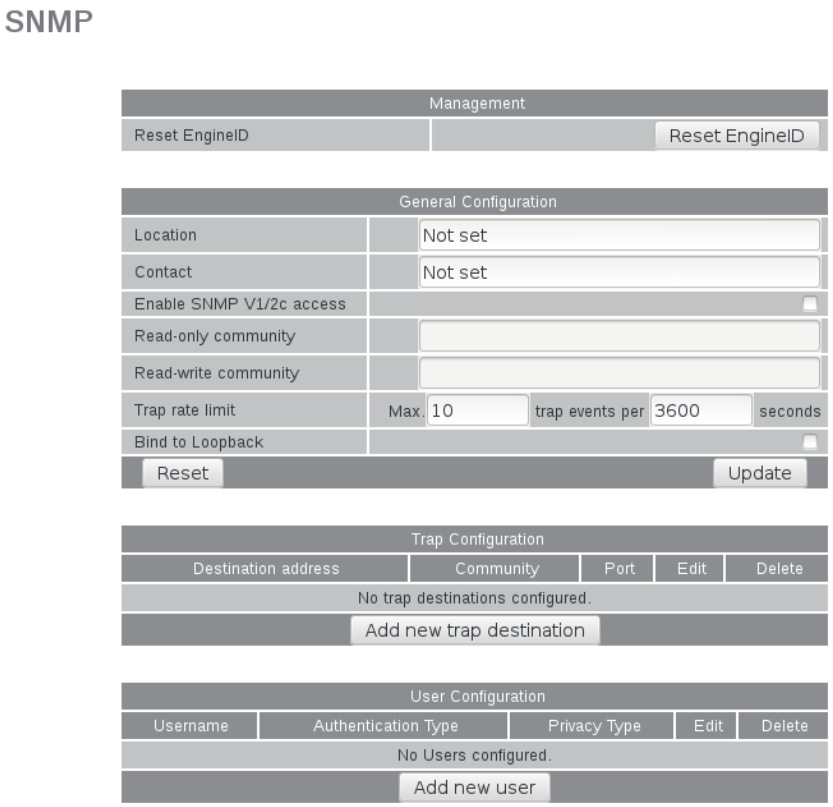


Figure 362: The SNMP configuration page

13.2.1 SNMP Management

This section allows the SNMP Engine ID to be reset. An SNMP Engine ID is assigned to SNMP Agents and SNMP Management applications which communicate using SNMPv3. The Engine ID is required to be unique across the set of communicating SNMPv3 Agents and Managers. To reset the SNMP Engine ID click the Reset EngineID button .

Resetting the SNMP Engine ID will invalidate and delete all user accounts. A warning message to this effect will be shown to proceed click the OK button.

13.2.2 SNMP General Configuration

The general configuration options are described below:

Location The location reported in the standard SNMP Location field.

Contact The contact name reported in the standard SNMP Contact field.

Enable SNMP V1/2c Access Check to enable SNMP V1 and V2c access. The following fields will then be accessible:

Read-only community The community string expected for read-only access.

Read-write community The community string expected for read-write access.

Trap rate limit Specify the maximum traps over a time period. This can be used to prevent an event trigger which changes more frequently than expected from generating a large number of traps. The timer starts at the time the first trap is sent and resets once the number of seconds configured has elapsed. Format Max. <number> trap events per <time> seconds. Where:

<Number> Is the maximum number of trap events for the time period; and

<time> Is the time period in seconds.

Bind to Loopback Check to to bind SNMP to the Loopback address.

Click the Update button to save and commit changes. Click the Reset button to cancel the changes and revert to the saved settings.

13.2.3 SNMP Trap Configuration

SNMP uses messages called traps to report alerts or asynchronous errors to an SNMP master. The modem can generate traps on events such as the RF signal level dropping below a threshold.

The **Trap Configuration** table is used to specify the details of the SNMP master to which SNMP traps will be sent.

To add a new entry click the Add new trap destination button, a page similar to that shown in figure 363 will appear.

Figure 363: The SNMP trap configuration page.

The following fields can be set:

Destination address The IP address of the SNMP master.

Community The community string to send with traps.

Port The IP port of the SNMP master.

Once the details have been entered, click the Update button to save the new trap destination.

13.2.4 Example of Adding an SNMP Trap

To add a new entry click the Add new trap destination button, a page similar to that shown in figure 364 will appear. Add the details for the trap as shown, then click the Update button to save the changes.

Figure 364: Example of adding an SNMP trap.

The main SNMP page will then be shown, now including the trap configuration details as shown in figure 365

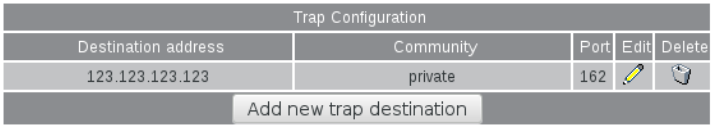


Figure 365: The SNMP trap configuration details.

To add a second entry again click the Add new trap destination button at the bottom of the SNMP Trap configuration table. An example of adding a second entry is shown in Figure 366.

Figure 366: Adding a second entry to the SNMP Trap list.

Click the Update button to add the entry to the table. The SNMP Trap configuration table will now include the new entry as shown in Figure 367.

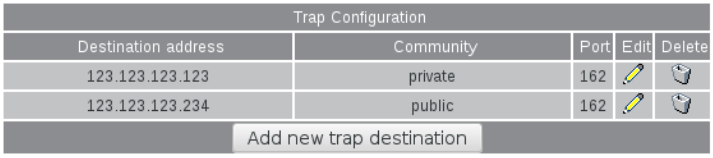


Figure 367: SNMP Trap list showing two entries.

13.2.5 Editing an SNMP Trap Entry

The details for an SNMP Trap can be edited by clicking the icon in the **Edit** column, the details for the SNMP Trap will be shown as above in the Add new SNMP Trap example in figure 364. Changes can be made then click the Update button to save or click the Cancel button to exit and not save any changes.

As an example, to edit the second SMS entry in the table, click the icon in the second row of the table. To change the IP Address to 123.123.234.234, changes were made as shown in Figure 368.

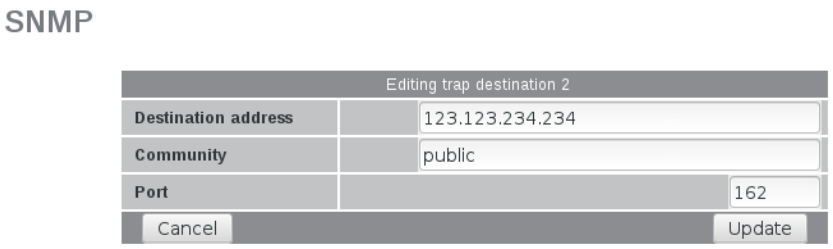


Figure 368: Editing an SNMP Trap entry.

To save the changes click the Update button or to cancel any changes made click the Cancel button. The main page will again be displayed as shown in Figure 369, with the changes for entry 2 added to the table.

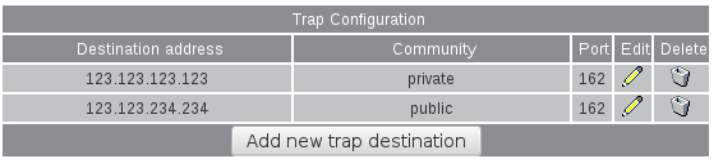


Figure 369: List after editing SNMP Trap entry.

13.2.6 Deleting an SNMP Trap entry

An SNMP Trap entry can be deleted by clicking the icon in the **Delete** column of the SNMP Trap table, a confirmation pop-up box will be displayed asking for confirmation of the delete. After deletion the SNMP Trap table on the main page will be updated.

For example, to delete SNMP Trap entry 2 from the table shown in Figure 398, click the icon in row 2 of the table. A warning box will now be displayed as shown if Figure 370. Click the OK button.

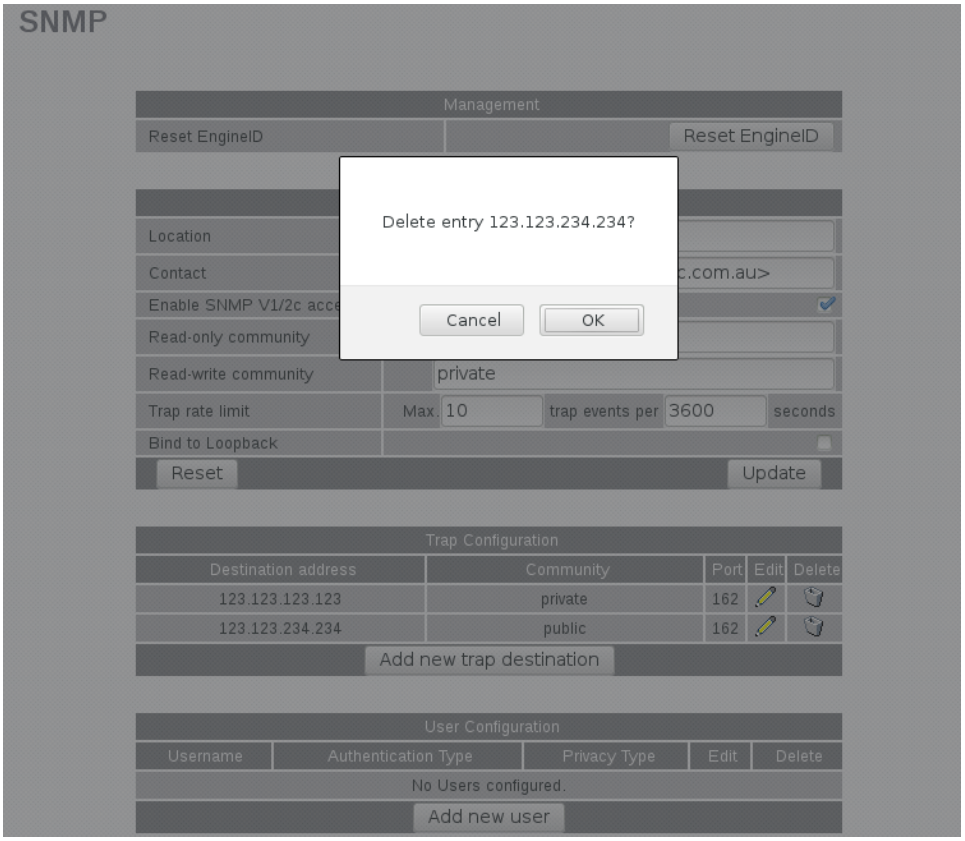


Figure 370: Deleting an SNMP Trap entry.

The main page will again be displayed as shown in Figure 371, with entry 2 no longer included in the table.

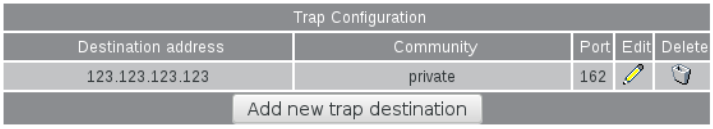


Figure 371: The SNMP Trap table after deleting entry.

13.2.7 SNMP User Configuration

SNMPv3 provides a secure environment for the management of systems, this requires the identification of SNMP entities to facilitate communication only between known SNMP entities. Each SNMP entity has an identifier called the SNMP EngineID, and SNMP communication is possible only if an SNMP entity knows the identity of its peer. Users are defined for read and/or write access. This section describes the SNMP user configuration.

To add a new user click the Add new user button a page similar to that shown in figure 372 will appear.

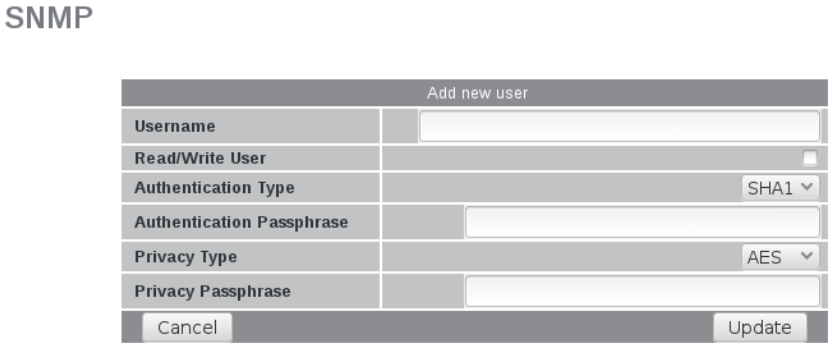


Figure 372: The SNMP add user configuration page.

The following fields can be set:

Username The user-name for the new user.

Ready/Write User Check to enable read / write access for the user. Leave un-ckecked for read only access.

Authentication Type Choose the authentication type. Options are:

None
MD5 Message-Digest algorithm
SHA1 Secure Hash Algorithm 1

Authentication Passphrase Enter a pass-phrase

Privacy Type Choose the privacy type. Options:

None
AES Advanced Encryption Standard
DES Data Encryption Standard

Privacy Passphrase Enter a pass-phrase.

Click the Update button to save the new user configuration.

13.2.8 Example of Adding an SNMP User

To add a new entry click the Add new user button a page similar to that shown in figure 364 will appear. Add the details for the user as shown, then click Update to save the changes.

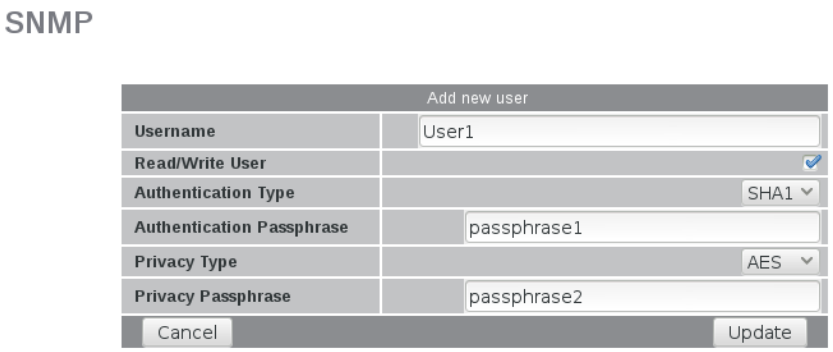


Figure 373: Example of adding a new SNMP user.

The main SNMP page will then be shown, now including the user details as shown in figure 374

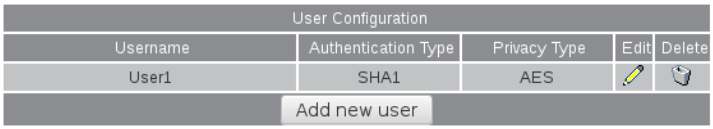


Figure 374: The example SNMP user details on the main SNMP page.

To add a second entry again click the Add new user button at the bottom of the SNMP User configuration table. An example of adding a second entry is shown in Figure 375.

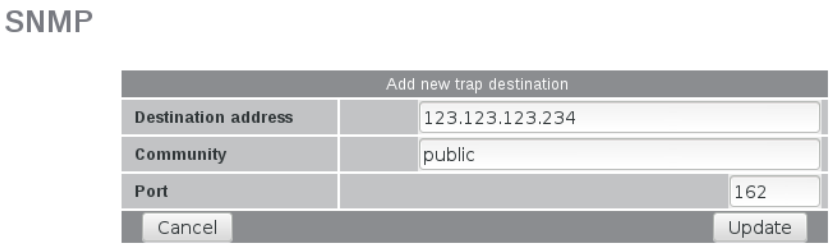


Figure 375: Adding a second entry to the SNMP User list.

Click the Update button to add the entry to the table. The SNMP User configuration table will now include the new entry as shown in Figure 376.

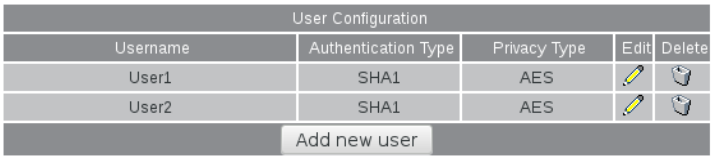


Figure 376: SNMP user list showing two entries.

13.2.9 Editing an SNMP User Entry

The details for an SNMP User can be edited by clicking the icon in the **Edit** column, the details for the SNMP Trap will be shown as above in the Add new SNMP Trap example in figure 364. Changes can be made then click the Update button to save or click the Cancel button to exit and not save any changes.

For security the pass-phrases are not displayed and cannot be edited. To change a passphrase the entire passphrase will need to entered.

As an example, to edit the second SNMP User entry in the table, click the icon in the second row of the table. To change the pass-phrases, changes were made as shown in Figure 377.

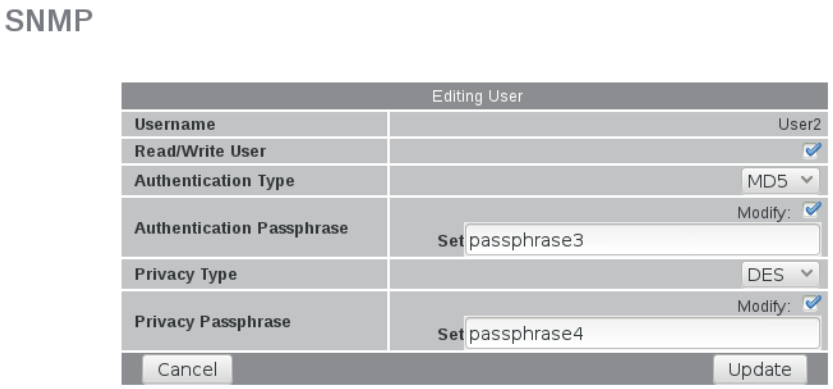


Figure 377: Editing an SNMP User entry.

To save the changes click the Update button or to cancel any changes made click the Cancel button. The main page will again be displayed as shown in Figure 378, with the changes for entry 2 added to the table.

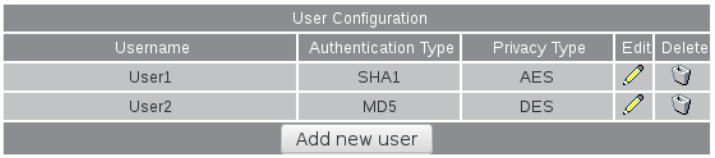


Figure 378: List after editing SNMP User entry.

13.2.10 Deleting an SNMP User entry

An SNMP User entry can be deleted by clicking the icon in the **Delete** column of the SNMP User table, a confirmation pop-up box will be displayed asking for confirmation of the delete. After deletion the SNMP User table on the main page will be updated.

For example, to delete SNMP User entry 2 from the table shown in Figure 398, click the icon in row 2 of the table. A warning box will now be displayed as shown if Figure 379. Click the OK button.

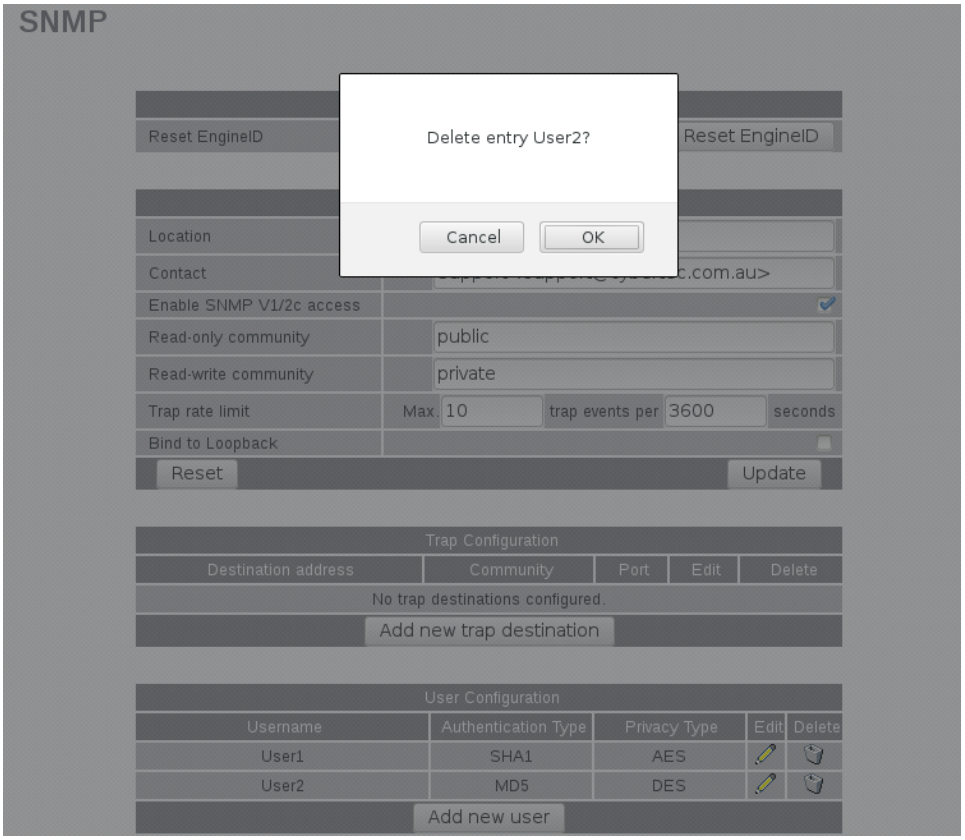


Figure 379: Deleting an SNMP User entry.

The main page will again be displayed as shown in Figure 380, with the entry 2 no longer included in the table.

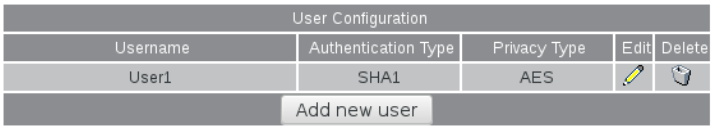


Figure 380: The SNMP User table after deleting entry.

13.3 DNP3

The modem can be configured to operate as a DNP3 outstation for reporting of the modem's state. Information such as the current connection status and RF level are available via DNP3 and, on models with GPIO, the GPIO can also be read and written. The options for these can be found by selecting Management ▷ DNP3.

The DNP3 page is shown in Figure 381.

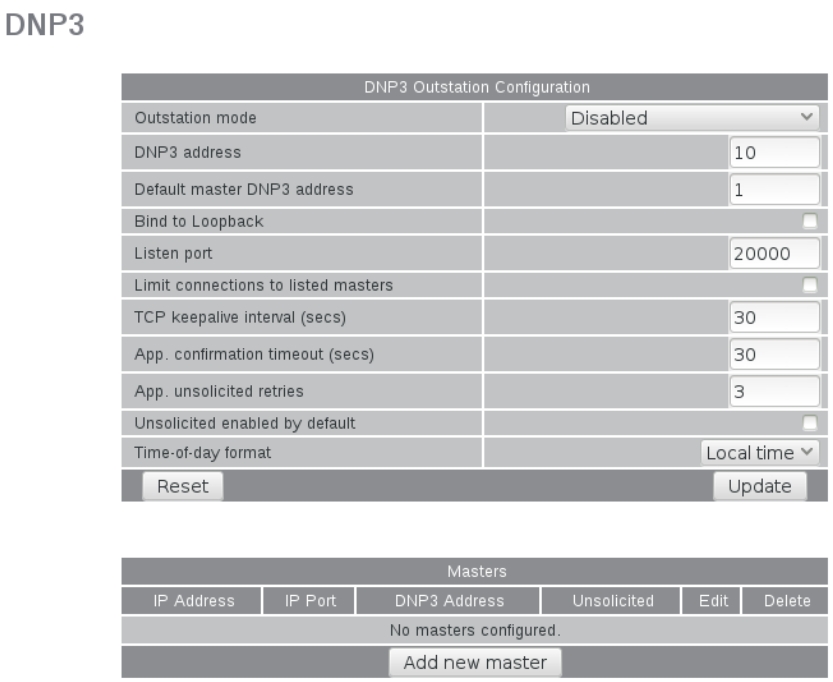


Figure 381: The DNP3 outstation configuration page

13.3.1 Configuring the outstation

The following can be set for the outstation:

Outstation mode The outstation supports the following outstation modes:

Disabled The outstation will not function.

TCP listen endpoint The outstation will accept TCP connections from a DNP3 master.

TCP dual endpoint The outstation will accept TCP connections from a DNP3 master. It will also establish a connection should an event occur while no master is connected.

UDP (datagram) endpoint The outstation can be polled by a DNP3 master using UDP. Events will also be transmitted to the master via UDP.

DNP3 address This is the DNP3 link-layer address for the outstation.

Default master DNP3 address This is the address that will be used for TCP keep-alives if the DNP3 master address for a connection is currently unknown.

Listen port This is the IP port number that the outstation will accept connections. The default DNP3 port number is 20000.

Limit connections to listed masters When set, only masters whose IP addresses are listed in the masters table will be allowed to connect.

TCP keepalive interval (secs) To detect dead TCP connections, the outstation will periodically send DNP3 polls to request the link status. If the master fails to respond, the connection will be closed. This field determines after what idle period (in seconds) that link status messages will be generated.

App. confirmation timeout (secs) This is the time-out (in seconds) that will be used while waiting to receive an application level confirmation from a DNP3 master.

App. unsolicited retries This is the number of times the outstation will retry sending unsolicited responses, should no confirmation be received from a master.

Unsolicited enabled by default When this option is not set, the modem will not send any unsolicited responses until an ENABLE_UNSOLICITED (function code 20) message is received from a master. With this option set, the outstation will default to having unsolicited responses enabled.

Time-of-day format This field determines the time format used in events. When set to UTC, the outstation will adjust all times by the system time zone setting (see section 5.2.4).

Click the Update button to save and commit the changes.

13.3.2 Adding a DNP3 master

Details of the DNP3 masters can be configured to allow limiting of connections or to enable unsolicited responses.

To configure the information about a new DNP3 master, click the Add new master button. A page similar to the shown in figure 382 will be presented.

Figure 382: The DNP3 master configuration page

The following fields can be set for each master:

Master IP address The IP address of the DNP3 master.

Master IP port The IP port number the master receives unsolicited responses on.

DNP3 address The DNP3 link-layer address of the master.

Unsolicited receiver When set, the master will receive unsolicited responses from the outstation.

Click the Update button to save the new master.

13.3.3 Example of Adding a DNP3 Master

To add a new entry click the Add new master button. A page similar to that shown in figure 383 will appear. Add the details for the DNP3 Master as shown, then click the Update button to save the changes.

Figure 383: Example of adding a DNP3 Master.

The main DNP3 page will then be shown, now including the DNP3 Master details as shown in figure.

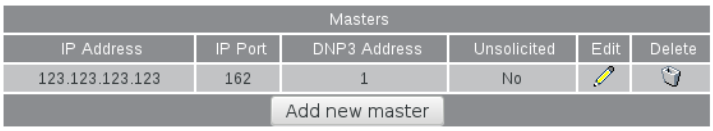


Figure 384: The DNP3 Master list after adding new master.

To add a second entry again click the Add new master button at the bottom of the DNP3 Masters table. An example of adding a second entry is shown in Figure 385.

Figure 385: Adding a second entry to the DNP3 master list.

Click the Update button to add the entry to the table. The DNP3 Master list will now include the new entry as shown in Figure 386.

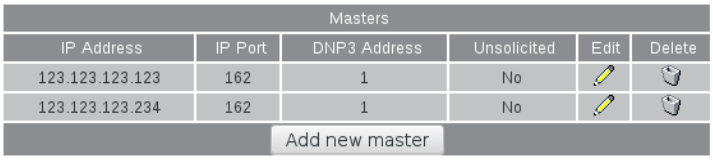


Figure 386: DNP3 Master list showing two entries.

13.3.4 Editing a DNP3 Master Entry

The details for the DNP3 Master can be edited by clicking the icon in the **Edit** column, the details for the DNP3 master will be shown as above in the Add new master example in figure 383. Changes can be made then click the Update button to save or click the Cancel button to exit and not save any changes.

As an example, to edit the second DNP3 Master entry in the table, click the icon in the second row of the table. To change the DNP3 address to 2, changes were made as shown in Figure 387.

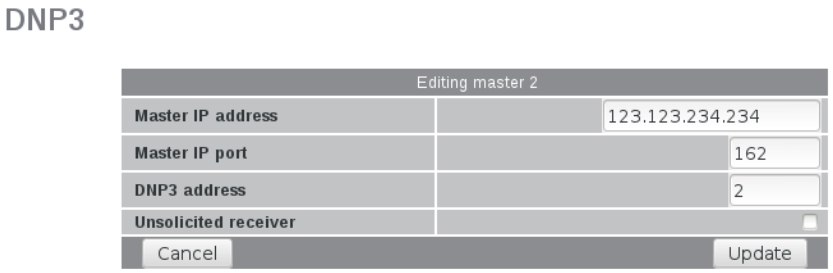


Figure 387: Editing an DNP3 Master entry.

To save the changes click the Update button or to cancel any changes made click the Cancel button . The main page will again be displayed as shown in Figure 388, with the changes for entry 2 added to the table.

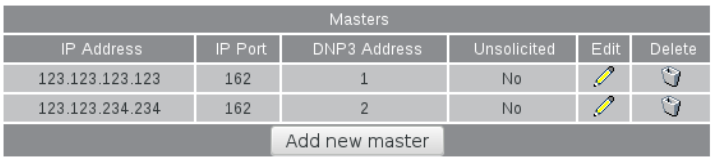


Figure 388: List after editing DNP3 Master entry.

13.3.5 Deleting a DNP3 Master entry

A DNP3 Master entry can be deleted by clicking the icon in the **Delete** column of the DNP3 Masters table, a confirmation pop-up box will be displayed asking for confirmation of the delete. After deletion the DNP3 table on the main page will be updated.

For example, to delete DNP3 Master entry 2 from the table shown in Figure 398, click the icon in row 2 of the table. A warning box will now be displayed as shown if Figure 389. Click the OK button .

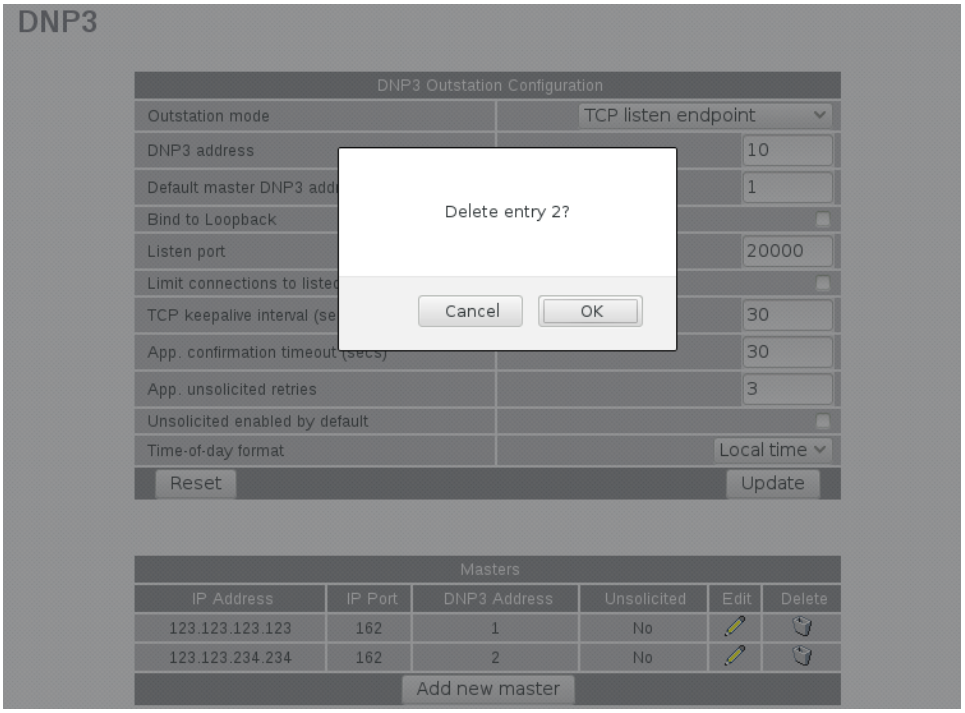


Figure 389: Deleting an DNP3 Master entry.

The main page will again be displayed as shown in Figure 390, with the entry 2 no longer included in the table.

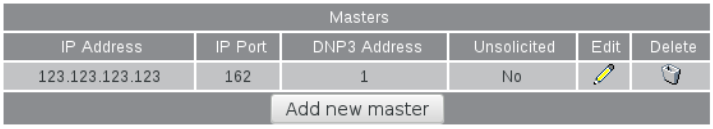


Figure 390: The DNP3 Master list after deleting entry.

13.4 SMS

The SMS page is used to configure the general SMS settings which include the SMS Distribution list and the SMS rate control. The page menu is Management ▷ SMS the page is shown in Figure 391.

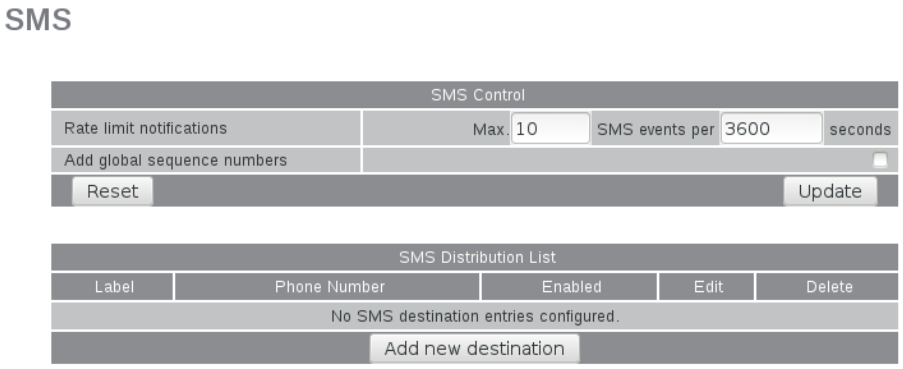


Figure 391: The SMS configuration page

13.4.1 SMS Control

The SMS Control section is used to configure global SMS settings including rate limiting of SMS and global sequence numbers.

The settings are:

Rate limit notifications Used to set the maximum number of SMS which can be sent within a given time. This can be used to prevent an event trigger which changes more frequently than expected from generating a large number of messages. The timer starts at the time the first SMS is sent and resets once the number of seconds configured has elapsed. The Format is: Max. <number> SMS events per <time> seconds. Where:

<Number> Is the maximum number of SMS events which can be sent for the time period; and

<time> Is the time period in seconds.

Add global sequence numbers Check to enable the inclusion of a sequence number in each SMS.

Click Update to save changes.

The global sequence number is set to 1 at boot time and increments by 1 for each message sent. If the unit is powered off or re-booted the global sequence number will be reset to 1.

13.4.2 SMS Distribution List

The SMS distribution list section lists the current numbers to which SMSes will be sent and allows entries to be added, edited and deleted. The fields of the table are:

Label A text label for the entry.

Phone Number The phone to which the SMS will be sent.

Enabled Check to enable this entry.

Edit Click the icon to edit the entry.

Delete Click the icon to delete the entry.

13.4.3 SMS Entry Options

To access the SMS Entry Options click the Add new destination button at the bottom of the SMS distribution list table. The following page will be displayed:

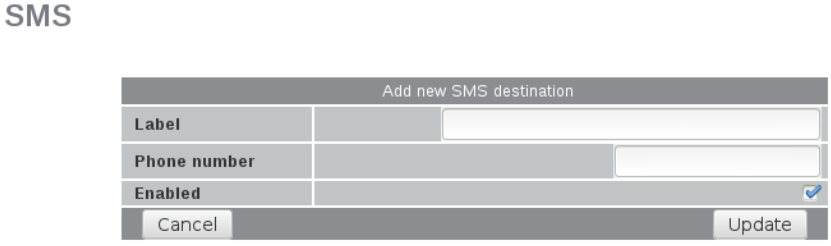


Figure 392: The SMS configuration page

To create a new entry complete the fields which have the following meaning:

Label A text label for the entry.

Phone Number The phone to which the SMS will be sent.

The phone number must be in the form +<country code><phone number>. For example +61432123123 If a number is entered with a 0 as the first digit +61 will automatically be added to the number and the 0 will be removed.

Enabled Check to enable this entry.

When finished click the Update button to save the changes.

13.4.4 Adding a New SMS Entry

To add a new entry click the Add new destination button at the bottom of the SMS distribution list table. The Add new SMS destination page as shown in Figure 392 will be displayed. An example of an entry is shown in Figure 393, in this case the entry will be labelled Test and the phone number is 0411123456.

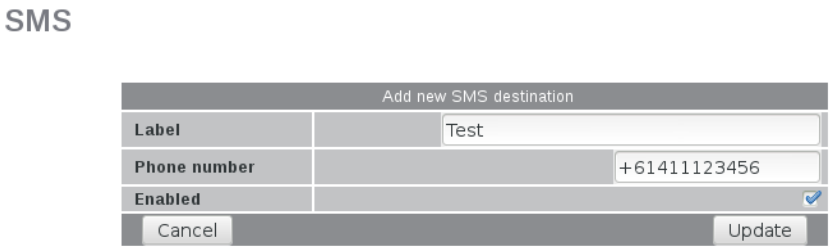


Figure 393: An example of adding an SMS entry.

Once the changes have made click the Update button to save the entry. The SMS distribution list page will be displayed again now with the new entry as shown in Figure 394.

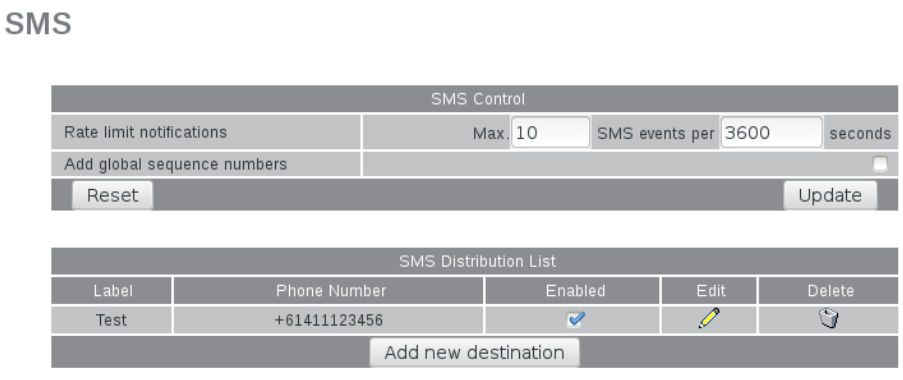


Figure 394: The SMS entry has been added to the list.

To add a second entry againclick the Add new destination button at the bottom of the SMS distribution list table. An example of adding a second entry is shown in Figure 395, in this case the label is called Test2 and the phone number is +61432123456.

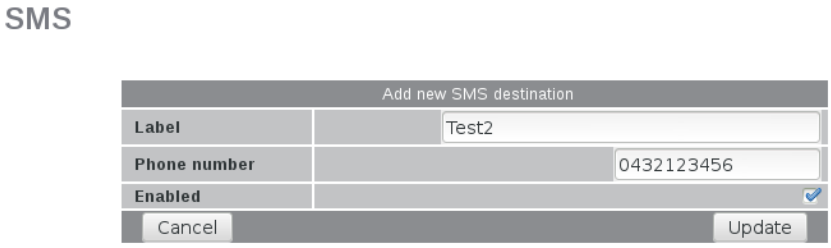


Figure 395: Adding a second SMS entry to the distribution list.

Click the Update button to add the entry to the table. The SMS distribution list will now include the new entry as shown in Figure 396.

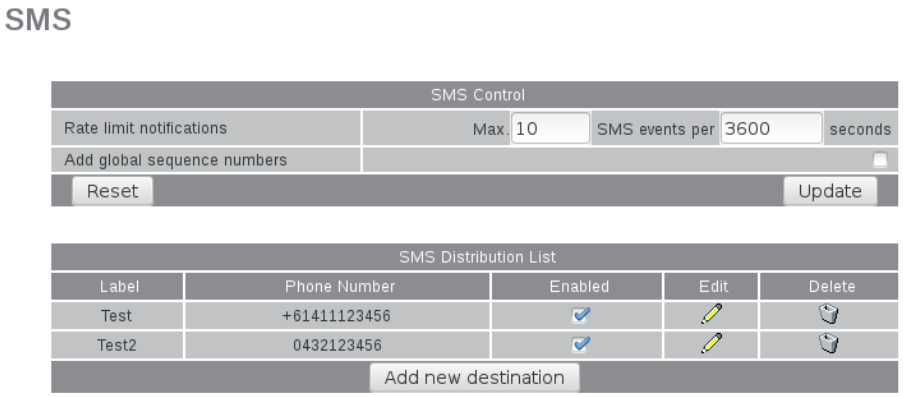


Figure 396: SMS distribution list showing two entries.

13.4.5 Editing an SMS Entry

An SMS entry can be edited by clicking the icon in the **Edit** column of the entry to be changed. Once clicked, the details of the entry will be displayed in the same table as when creating a new SMS entry.

As an example, to edit the second SMS entry in the table, click the icon in the second row of the table. To change the phone number of the entry to +61432123456, changes were made as shown in Figure 397.

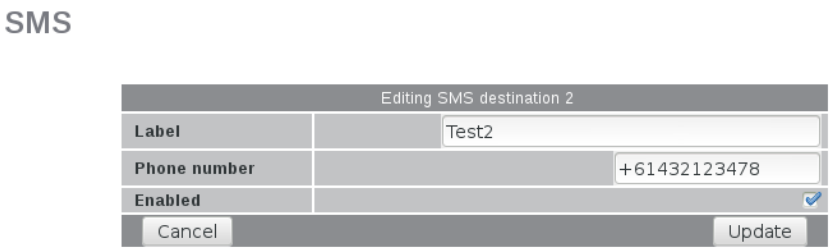


Figure 397: Editing SMS entry.

To save the changes click the Update button or to cancel any changes made click the Cancel button. The main page will again be displayed as shown in Figure 398, with the changes for entry 2 added to the table.

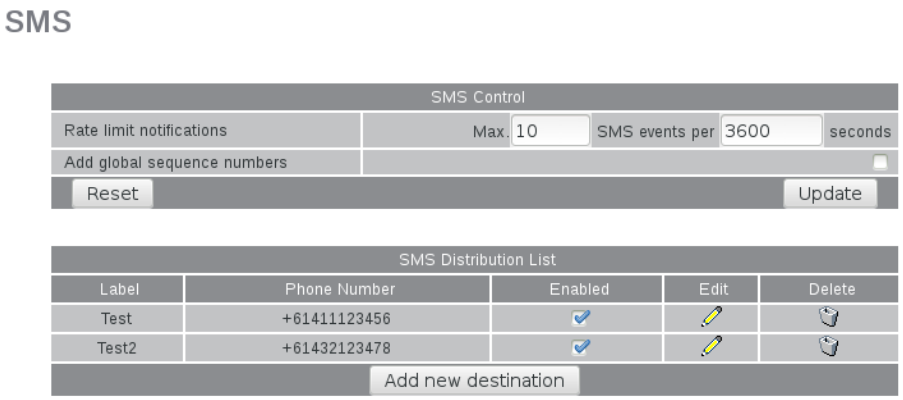


Figure 398: List after editing SMS entry.

13.4.6 Deleting an SMS entry

An SMS entry can be deleted by clicking the icon in the **Delete** column of the entry to be deleted. A warning box will be displayed. Click **OK** to confirm the deletion.

For example, to delete SMS entry 2 from the table shown in Figure 398, click the icon in row 2 of the table. A warning box will now be displayed as shown if Figure 399. Click the OK button.

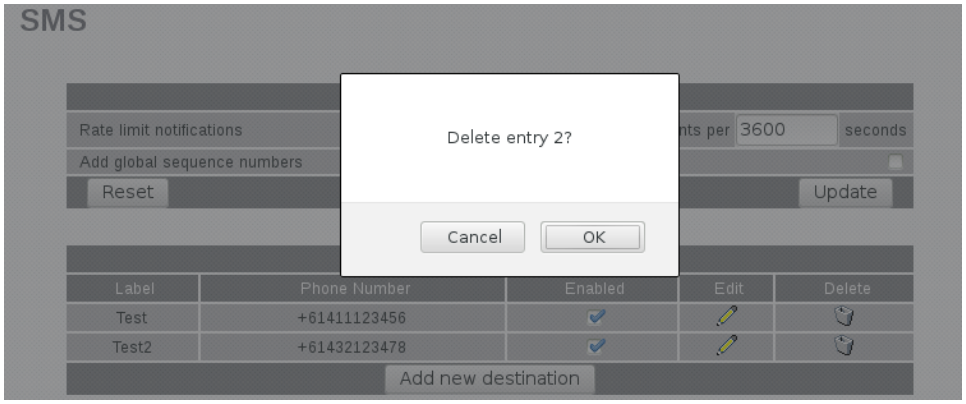


Figure 399: Deleting an SMS entry.

The main page will again be displayed as shown in Figure 400, with the entry 2 no longer included in the table.

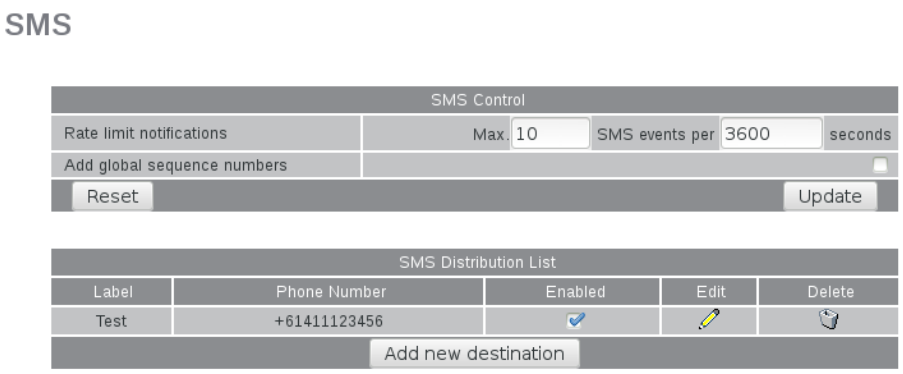


Figure 400: SMS distribution list after deleting SMS entry.

13.5 Email

The Email page is used to configure the general Email settings which include the SMTP Server setting and the message rate control. The page menu is accessed by selecting Management ▷ Email the page is shown in Figure 401.

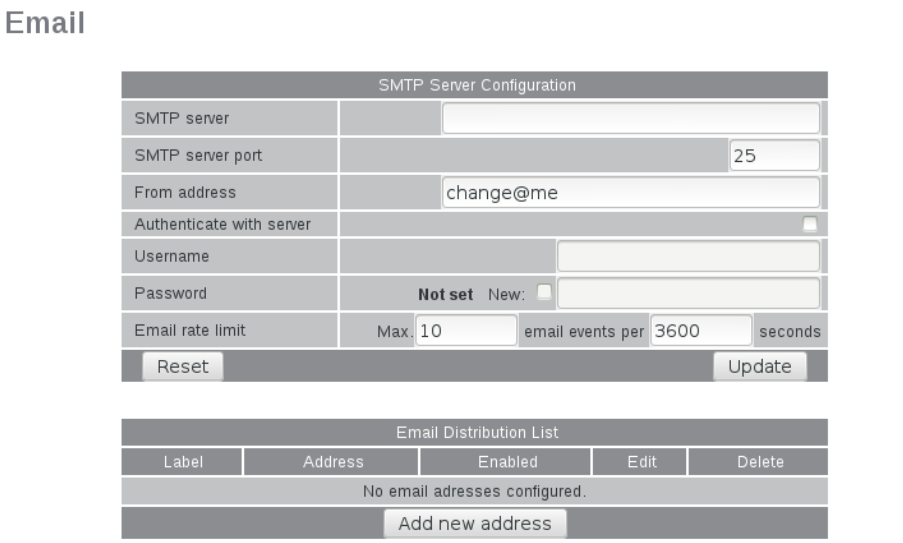


Figure 401: The Email settings page.

13.5.1 SMTP Server Configuration

The first section is used for the SMTP Server configuration. This is the server which will used for outgoing email:

SMTP server The fully qualified host-name or IP address of the server.

SMTP server port The server port number. (Default 25)

From address The email address which will appear in the emails sent.

Authenticate with server Check to enable authentication with the server.

Username The user-name used for authenticating with the server.

Password The password used for authenticating with the server. To set the password first check the New check-box.

Email rate limit Used to set the maximum number of email messages which can be sent within a given time. This can be used to prevent an event trigger which changes more frequently than expected from generating a large number of messages. The timer starts at the time the first email is sent and resets once the number of seconds configured has elapsed. The Format is: Max. <number> email events per <time> seconds. Where:

<Number> Is the maximum number of SMS events which can be sent for the time period; and

<time> Is the time period in seconds.

Click the Update button to save and commit changes.

13.5.2 Email Distribution List

The Email distribution list section lists the current numbers to which emails will be sent and allows entries to be added, edited and deleted. The fields of the table are:

Label A text label for the entry.

Address The email address to which the emails will be sent.

Enabled Check to enable this entry.

Edit Click the icon to edit the entry.

Delete Click the icon to delete the entry.

13.5.3 Email entry options

To access the Email Entry Options click the Add new address button at the bottom of the Email distribution list table. The page shown in figure 402 will be displayed:

Figure 402: Add new email address.

To create a new entry complete the fields which have the following meaning:

Label A text label for the entry.

Address The email address to which the emails will be sent.

Enabled Check to enable this entry.

When finished click the Update button to save the changes.

13.5.4 Adding a New Email Entry

To add a new entry click the Add new address button at the bottom of the Email distribution list table. The Add new email address page as shown in Figure 402 will be displayed. An example of an entry is shown in Figure 403, in this case the entry will be labelled Test and the address is test@example.com.

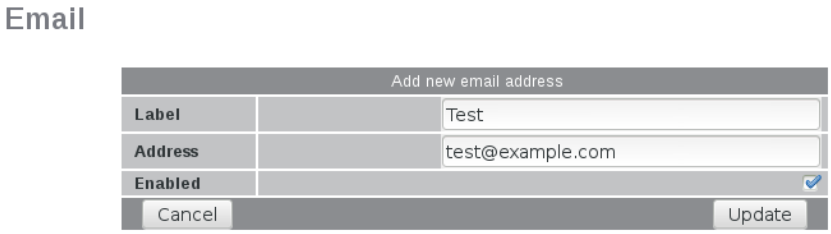


Figure 403: An example of adding an email entry.

Once the changes have made click the Update button to save the entry. The email distribution list page will be displayed again now with the new entry as shown in Figure 404.

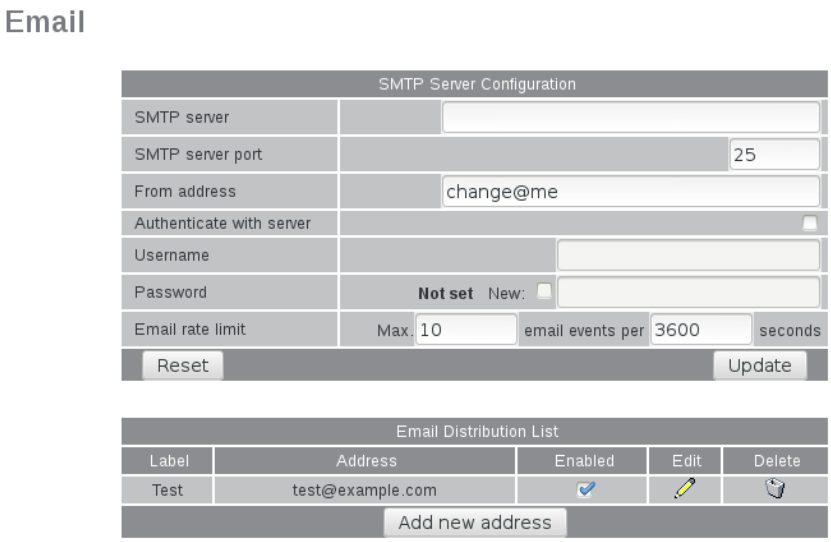


Figure 404: The email entry has been added to the list.

To add a second entry again click the Add new address button at the bottom of the email distribution list table. An example of adding a second entry is shown in Figure 405, in this case the label is called Test2 and the address is test2@example.com.

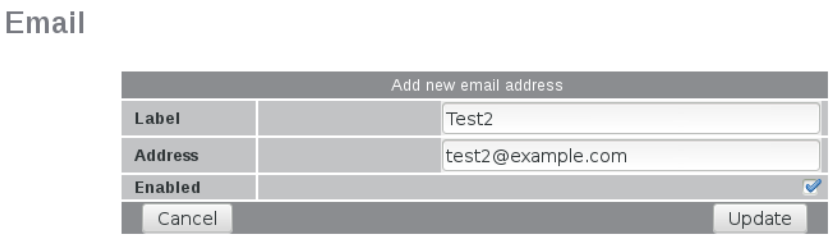


Figure 405: Adding a second email entry to the distribution list.

Click the Update button to add the entry to the table. The email distribution list will now include the new entry as shown in Figure 406.

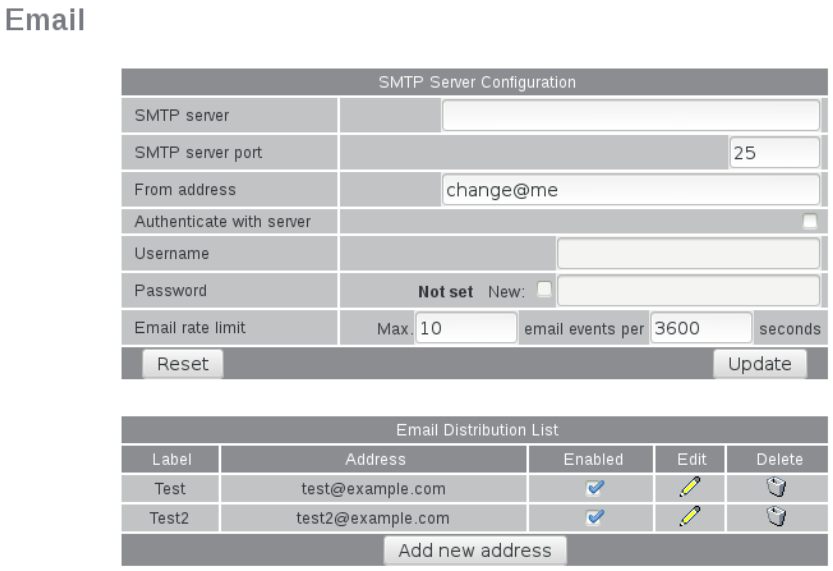


Figure 406: The email distribution list showing two entries.

13.5.5 Editing an Email Entry

An entry can be edited by clicking the icon in the **Edit** column of the entry to be changed. Once clicked, the details of the entry will be displayed in the same table as when creating a new email address.

As an example, to edit the second email entry in the table, click the icon in the second row of the table. The address of the entry is changed to test2@email.com, as shown in Figure 407.

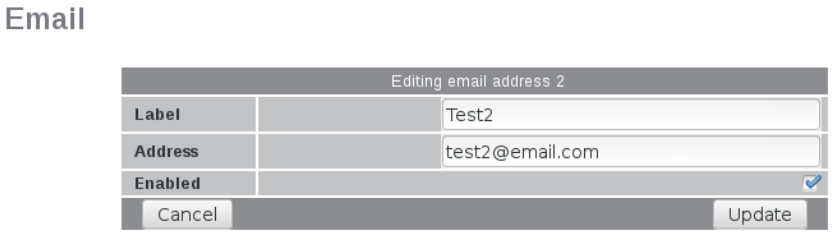


Figure 407: Editing an email entry.

To save the changes click the **Update** button or to cancel any changes made click the **Cancel** button. The main page will again be displayed as shown in Figure 408, with the changes for entry 2 included in the table.

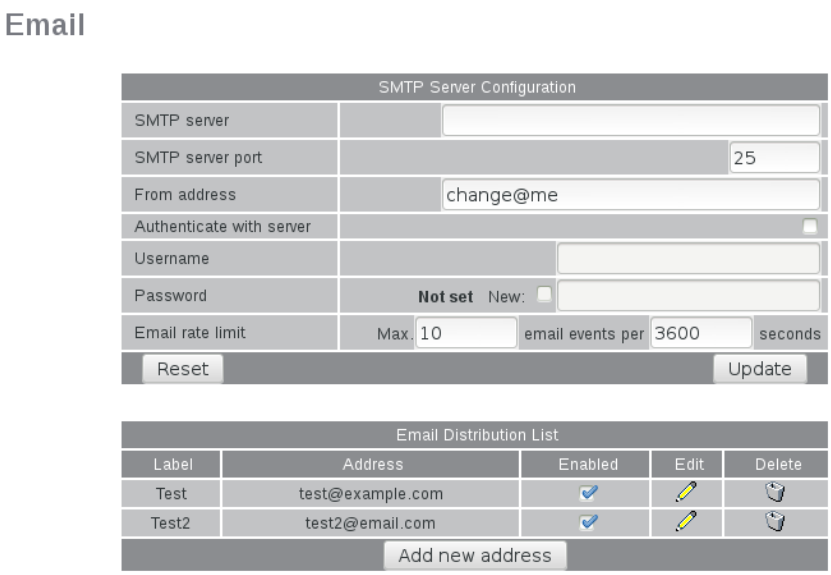


Figure 408: List after editing the email entry.

13.5.6 Deleting an Email entry

An email entry can be deleted by clicking the icon in the **Delete** column of the entry to be deleted. A warning box will be displayed. Click the OK button to confirm the deletion.

For example, to delete SMS entry 2 from the table shown in Figure 408, click the icon in row 2 of the table. A warning box will now be displayed as shown if Figure 409. Click the OK button.

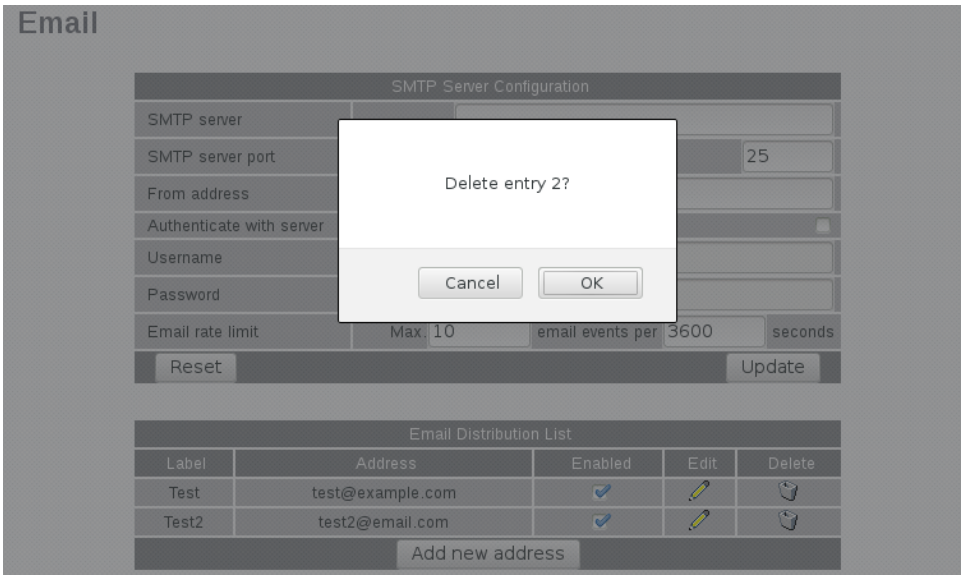


Figure 409: Deleting an email entry.

The main page will again be displayed as shown in Figure 410, with the entry 2 no longer included in the table.

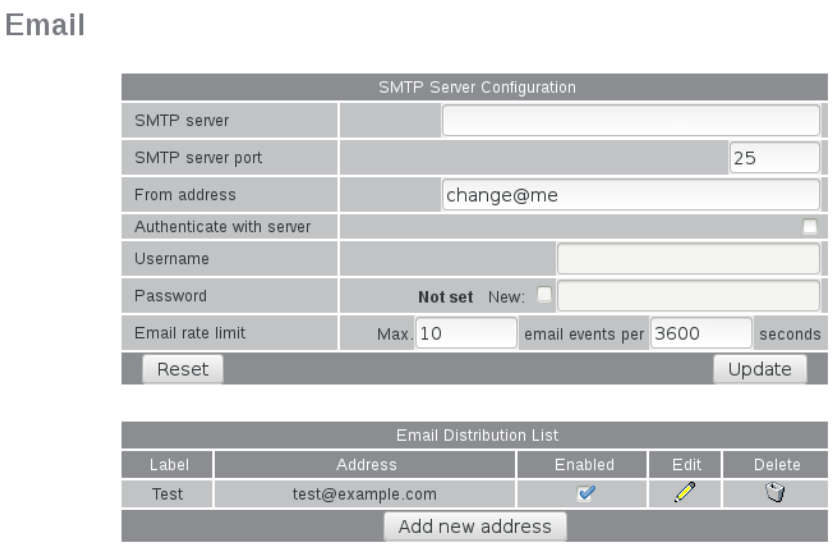


Figure 410: The email distribution list after deleting email entry.

Westermo • SE-640 40 Stora Sundby, Sweden
Tel +46 16 42 80 00 Fax +46 16 42 80 01
E-mail: info@westermo.com
www.westermo.com

Sales Units

Westermo Data Communications

Australia
info@westermo.net.au
www.westermo.net.au

China
sales.cn@westermo.com
www.cn.westermo.com

Finland
tiedot@westermo.fi
www.westermo.fi

France
infos@westermo.fr
www.westermo.fr

Germany
info@westermo.de
www.westermo.de

North America
info@westermo.us
www.westermo.us

Singapore
sales@westermo.com.sg
www.westermo.com

Sweden
info.sverige@westermo.se
www.westermo.se

United Kingdom
sales@westermo.co.uk
www.westermo.co.uk

Other Offices

For complete contact information, please visit our website at www.westermo.com/contact or scan the QR code

6623-3210 Westermo Teleindustri AB, Sweden