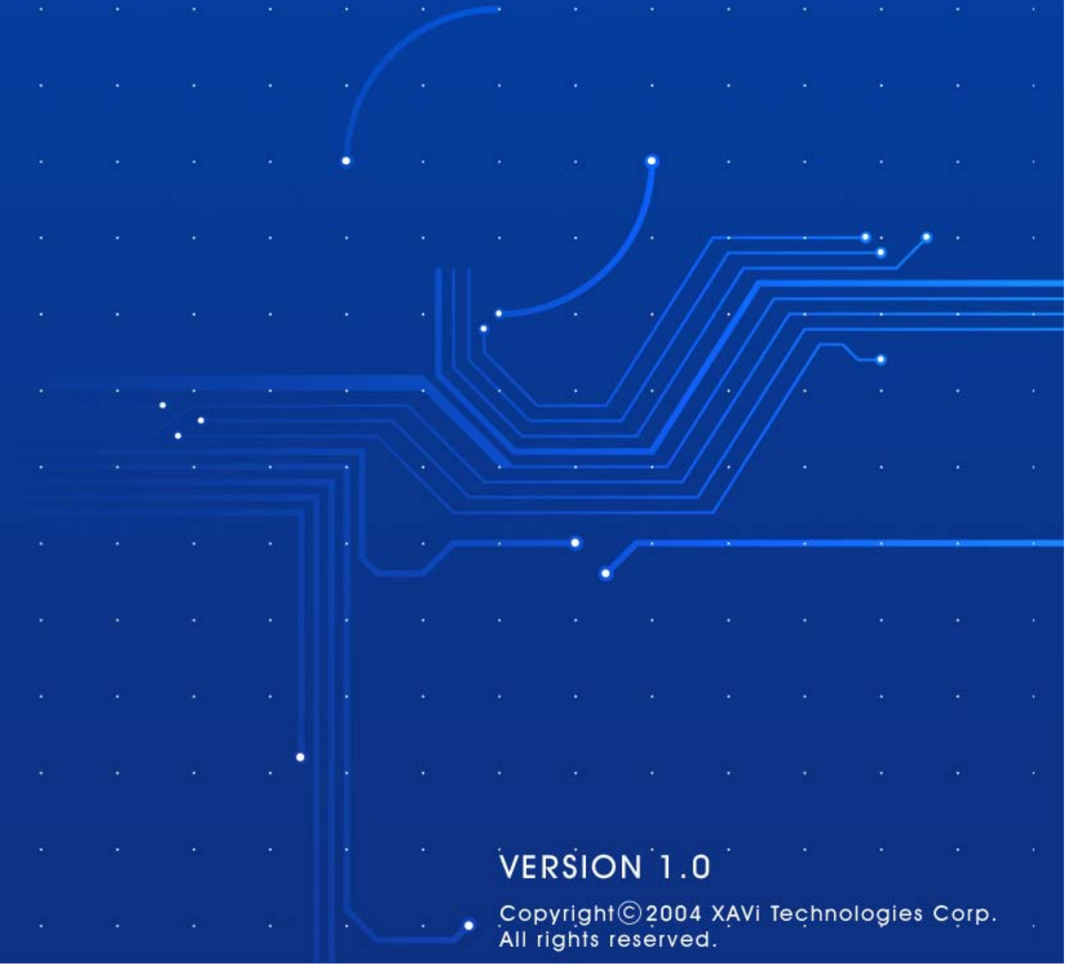
USERMANUAL

X7768r/X7768r$^+$

Wireless ADSL Router
Broadband Wireless Router



VERSION 1.0

XAVi Technologies Corporation
Tel: +886-2-2995-7953
Fax: +886-2-29957954
9F, No. 129, Hsing Te Road, Sanchung City,
Taipei Hsien 241,
Taiwan

XAVi Technologies Corporation provides this documentation without warranty of any kind, implied or expressed, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

Table of Contents

Chapter 1 – Getting Started

Chapter 2 – Web Management Interface

Table of Contents

Appendix A – Specifications

Appendix B – Warranties

Appendix C – Regulations

Chapter 1

Getting Started

I. Overview

The ***X7768r/X7768r+*** is an ADSL and wireless 802.11b/g router.

The ***X7768r/X7768r+*** device belongs to the ADSL/ADSL2/ADSL2+ series of customer premise devices, and ***X7768r+*** supports ADSL2+ as well. The ***X7768r/X7768r+*** provides four 10/100Base-TX Ethernet interfaces and an 802.11b/g WLAN interface on the LAN side. The broadband line interface supports ADSL Annex A & Annex B. The ***X7768r/X7768r+*** delivers broadband Internet access for enterprises, telecommuters, home, and remote office workers with high-speed data transmission requirements. It supports multiple protocols such as PPP (RFC 2364), IP (RFC 2225/RFC 1577), and RFC 1483 over ATM over ADSL, and PPP (RFC 2516) over Ethernet. ***X7768r/X7768r+*** offers convenient configuration and management locally by telnet, SNMP, and a Web-browser through the Ethernet interface, and remotely through the ADSL interface.

II. Features

- High speed asymmetrical data transmission on a single twisted copper pair
- Compliant with G.992.1, G.992.2, G.992.3, G992.4, G.994.5 (X7768r+ only) and T1.413 Issue 2
- Interchangeable between Bridge and Router mode
- RFC2684 (RFC1483) Bridged and Routed over ATM over ADSL
- PPPoE, IPoA and PPPoA Routed over ATM over ADSL
- Build-in four-port 10/100Base-TX Ethernet switch for PC or LAN connection and also automatic MDI/MDIX crossover with each port.
- High quality, simple operation and low power consumption
- Compatible and interoperable with major Central Office side ADSL DSLAM or Multi-service Access System
- Configuration and management with local Telnet through the Ethernet interface and remote Telnet through ADSL interface
- Firmware upgradeable through TFTP, HTTP
- Interoperability complies with TR-48
- 802.11g WLAN supports up to 54Mbps
- Supports Wi-Fi WPA

III. Packaging

This package consists of the following items:

X7768r/X7768r$^+$ ADSL device unit

RJ-45 Cable

RJ-11 Cable

AC Adapter

User's Manual CD

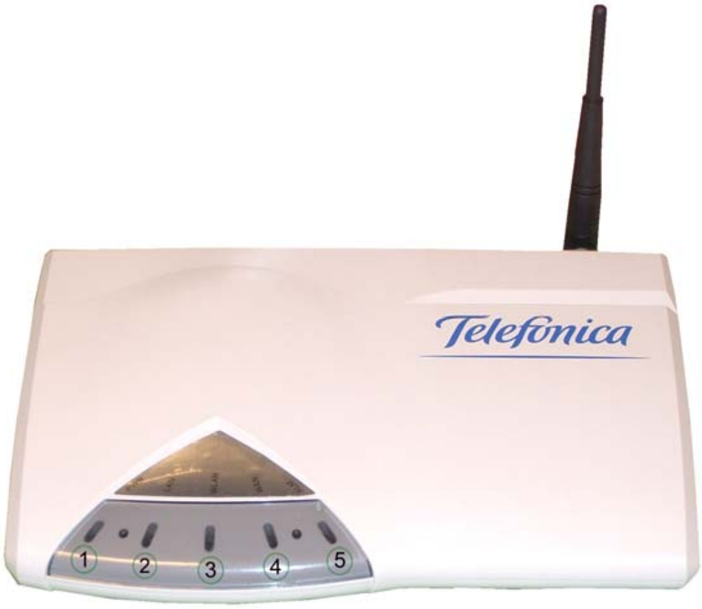
IV. Safety Guidelines

In order to reduce the risk of fire, electric shock and injury, please adhere to the following safety guidelines.

- Carefully follow the instructions in this manual; also follow all instruction labels on this device.
- Except for the power adapter supplied, this device should not be connected to any other adapters.
- Do not spill liquid of any kind on this device.
- Do not place the unit on an unstable stand or table. This unit may drop and become damaged.
- Do not expose this unit to direct sunlight.
- Do not place any hot devices close to this unit, as they may degrade or cause damage to the unit.
- Do not place any heavy objects on top of this unit.
- Do not use liquid cleaners or aerosol cleaners. Use a soft dry cloth for cleaning.

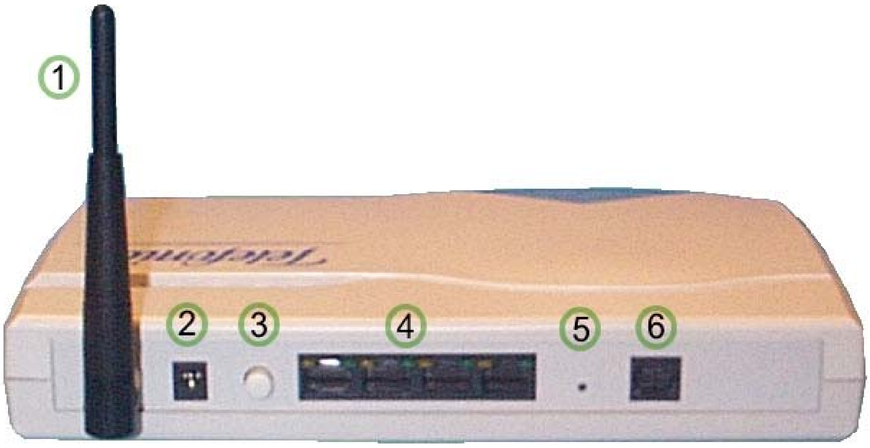
V. Appearance

Front View



	Label	LED Status	Color	Description
①	PWR	ON	Green	Power supply is connected.
②	LAN	ON	Green	Ethernet port is connected.
③	WLAN	Blinking	Green	WLAN transmitting.
		ON	Green	WLAN port is active
④	WAN	Blinking	Green	Training with DSLAM
		ON	Green	ADSL link is ready
⑤	ALM	Blinking	RED	Booting up
		ON	RED	Error

Rear View



	Label	Description
①		Antenna for wireless data reception
②	PWR	Power jack; connect to a power adapter.
③	On/Off	
④	ETHERNET	RJ-45 ports; connect to a PC or LAN.
⑤	RESET	Reset the modem back to factory settings by holding down on this button.
⑥	WAN	RJ-11 port; connect to the ADSL outlet.

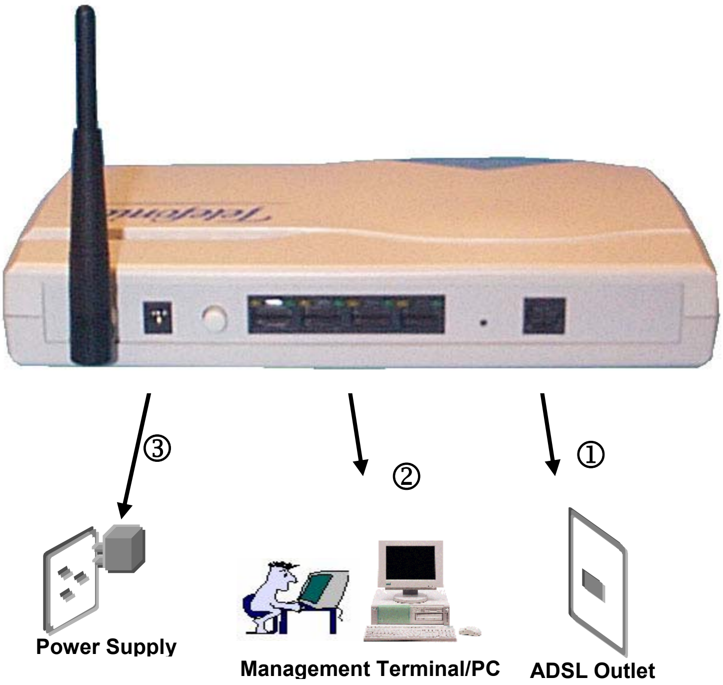
VI. Hardware Installation

Follow the steps below to set up your device:

Step 1: Connect one end of the ADSL cable to the WAN port of ***X7768r/X7768r***$^{+}$ and the other end to the ADSL wall outlet.

Step 2: Use a RJ-45 cable to connect one end to an Ethernet port of ***X7768r/X7768r***$^{+}$ and the other end to the LAN or a PC with an Ethernet adapter installed.

Step 3: Plug in the AC adapter to the AC power socket, and then connect the DC jack to the PWR inlet of ***X7768r/X7768r***$^{+}$. Push the On/Off button to turn it on.



Note: Be sure to use a RJ-45 crossover cable while connecting to a hub.

VII. Management

There are several ways that you can make the configuration:

- **Local Ethernet Port (telnet)** – connect the Ethernet port to your local area network or directly to a PC, "Telnet" ***X7768r/X7768r+*** from any workstation in the LAN. The default local Ethernet IP address is "192.168.1.1". See Chapter 2, Command Line Interface, for more details.
- **Local Ethernet Port (Web browser)** – connect the Ethernet port to your local area network or directly to a PC. Launch your Web browser and enter default local Ethernet IP address "192.168.1.1" into the address bar.
- **ADSL Port from Remote Site** – while the ADSL connection is in service, you may remotely "Telnet" ***X7768r/X7768r+*** from a workstation connected to the CO equipment.

Note: As operating an ADSL device requires technical know-how and experience, it is recommended that only qualified technical staff manage ***X7768r/X7768r+***. Therefore, a password authentication is required when you enter the command line and Web interface. See the *Default Values* section to obtain the password.

VIII. Default Values

X7768r/X7768r$^+$ is pre-configured with the following parameters; you may also re-load the default parameters by pressing the reset button of the modem for about 10 seconds or by using the **System Commands** link in the Web interface.

Username/Password: 1234/1234

Default IP Address

Ethernet (local) IP: 192.168.1.1

Subnet mask: 255.255.255.0

Protocol

PPPoE: VPI/VCI: 8/32

Class (QoS): UBR

WLAN : Disabled

ESSID: default

Default Channel: 1

Web encryption: Disabled

Rf Tx Power: 100 mW

Intranet Relay: Enabled

Rts Threshold: 2347

WAN and ADSL

Local Line Code: t1.413

DHCP Server: Enabled

DHCP start IP: 192.168.1.33

DHCP end IP: 192.168.1.254

DNS Relay: Disabled

Note: The Username and Password are case-sensitive.

IX. Software Upgrade

You may easily upgrade ***X7768r/X7768r$^+$*** embedded software by obtaining the compressed upgrade kit from the service provider and then following the steps for upgrading through either a DOS prompt or a Web-browser:

Software Upgrade through a DOS Prompt

Step 1: Extract the ZIP file for updated firmware.

Step 2: Connect ***X7768r/X7768r$^+$*** via the local Ethernet port or remote ADSL link, making sure that the ***X7768r/X7768r$^+$*** Ethernet IP address and your terminal are properly configured so that you can successfully "*ping*" ***X7768r/X7768r$^+$***. The default local IP address is "192.168.1.1".

Step 3: Under the DOS prompt, execute the command "xupgrade <*IP address of* ***X7768r/X7768r$^+$*** >", for instance, "xupgrade 192.168.1.1".

Step 4: This upgrading process may last as long as 60 seconds.

Step 5: Reboot ***X7768r/X7768r$^+$*** with new software.

Note: Strictly maintain stable power to ***X7768r/X7768r$^+$*** while upgrading its software. If the power fails during the upgrading process, contents in the memory could be destroyed, and the system may hang. In such a case, you must call the dealer or system integrator for repairs.

Software Upgrade through a Web-browser

Step 1: Extract the ZIP file for updated firmware.

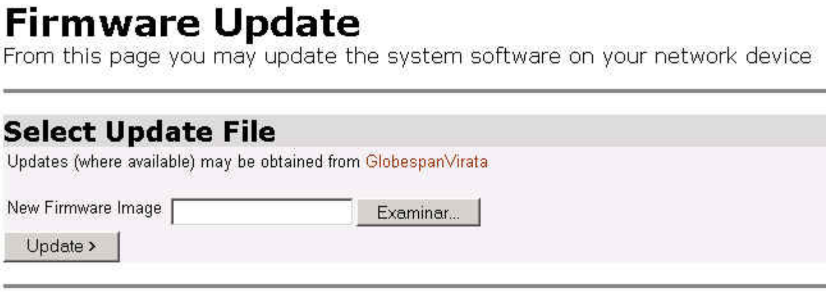
Step 2: Connect ***X7768r/X7768r***$^+$ via the local Ethernet port or remote ADSL link, making sure that the ***X7768r/X7768r***$^+$ Ethernet IP address and your terminal are properly configured so that you can successfully "*ping*" ***X7768r/X7768r***$^+$. The default local IP address is "192.168.1.1".

Step 3: Launch the Web browser (IE or Netscape), and enter the default IP address 192.168.1.1 into the address bar to access the Web management page.

Step 4: Click on the **System** link in the navigation bar and then on the **Firmware Update** link below it.

Step 5: Click on the **Examinar** button to select the upgrade file.

Step 6: Click on the **Update** button when completed.



Firmware Update

From this page you may update the system software on your network device

Select Update File

Updates (where available) may be obtained from GlobespanVirata

New Firmware Image

Note: Strictly maintain stable power to ***X7768r/X7768r***$^+$ while upgrading its software. If the power fails during the upgrading process, contents in the memory could be destroyed, and the system may hang. In such a case, you must call the dealer or system integrator for repairs.

Chapter 2

Web Management Interface

I. Overview

The Web Management Interface is provided to let the configuration of ***X7768r/X7768r***$^+$ as easily as possible. It provides a user-friendly graphical interface through a Web platform. You can configure bridge or router functions to accommodate your needs. In the section below, each configuration item is described in detail.

II. Preparation

Step 1: Please refer to the hardware installation procedure in Chapter 1 to install ***X7768r/X7768r***$^+$.

Step 2: You should configure your PC to the same IP subnet as the ***X7768r/X7768r***$^+$.

Example: ***X7768r/X7768r***$^+$: 192.168.**1.1**
Your PC: 192.168.**1.x**

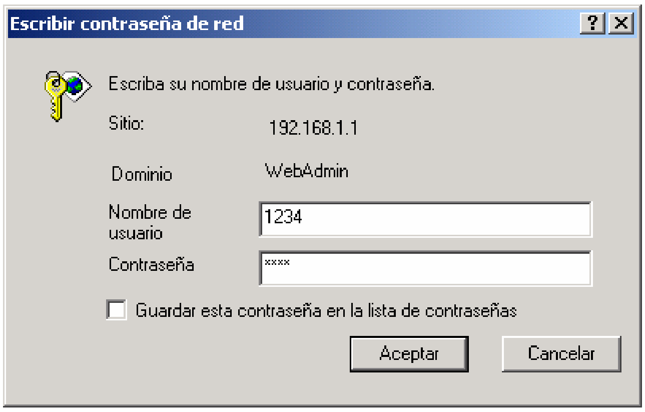
Step 3: Connect your PC to ***X7768r/X7768r***$^+$ and make sure that the PING function is working properly. The default IP address of this device is 192.168.1.1

Step 4: Launch the Web browser (IE or Netscape), and enter the default IP address 192.168.1.1 into the address bar to access the Web management page.

Step 5: The **Login** dialog box will appear first.

1. Login

- The **Enter Network password** window will pop up when starting the configuration. With the window active, type **1234** for both **User name** and **Password**, and then click on the **OK** button. You can also edit the username and password or add a new profile *(see section 4.3 Management for further details).*



Escribir contraseña de red

Escriba su nombre de usuario y contraseña.

Sitio: 192.168.1.1

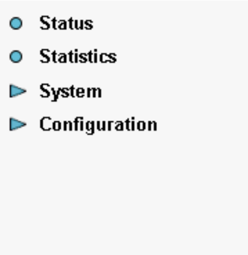
Dominio WebAdmin

Nombre de usuario 1234

Contraseña ****

□ Guardar esta contraseña en la lista de contraseñas

2. Status



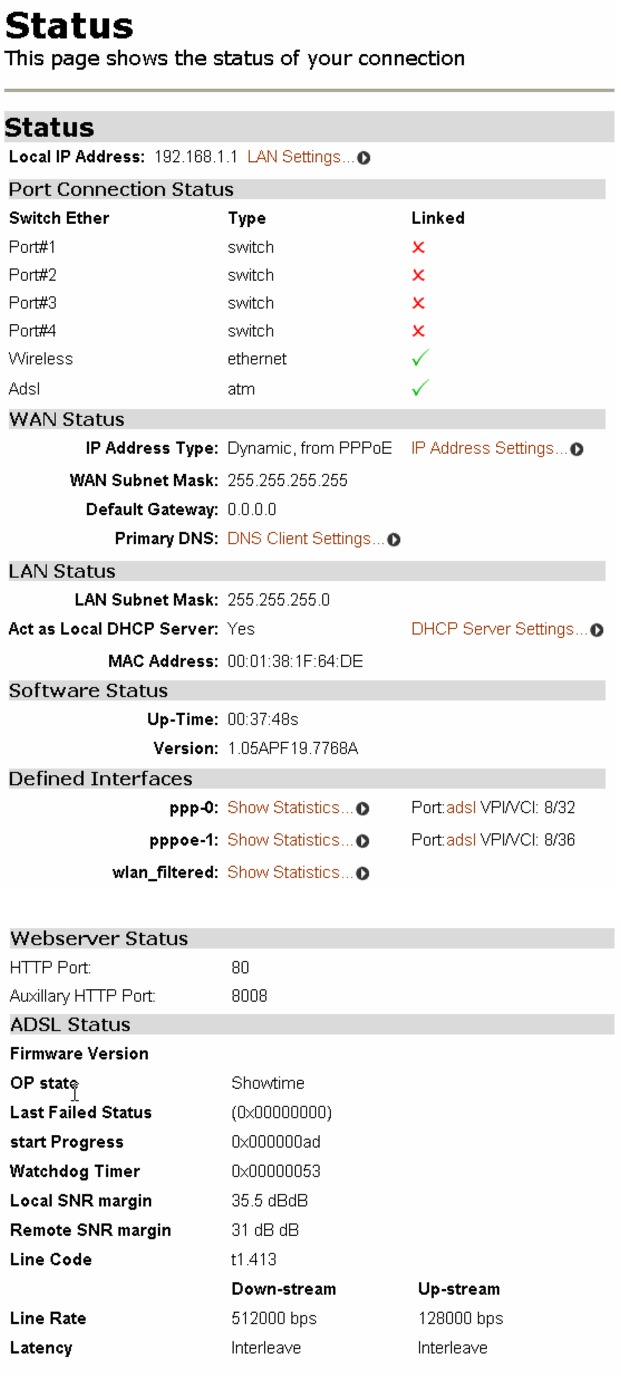
- The **Status** page displays the current configuration of ***X7768r/X7768r$^+$***. You can click on the shortcuts from the **Status** page for quickly editing most frequent configurations.

- Click **WAN Settings…** to edit/add WAN connections refer to *section 5.3 WAN Connections* for further details.

- Click **LAN Settings…** to edit the default LAN IP address refer to *section 5.2 LAN Connection* for further details.

- Click **IP Address Settings…** to edit/add WAN connections refer to *section 5.3 WAN Connections* for further details)

- Click **DHCP Server…** to edit DHCP Server status refer to *section 5.5 DHCP Server* for details.



Status

This page shows the status of your connection

Status

Local IP Address: 192.168.1.1 LAN Settings...

Port Connection Status

Switch Ether	Type	Linked
Port#1	switch	✗
Port#2	switch	✗
Port#3	switch	✗
Port#4	switch	✗
Wireless	ethernet	✓
Adsl	atm	✓

WAN Status

IP Address Type:	Dynamic, from PPPoE	IP Address Settings...
WAN Subnet Mask:	255.255.255.255	
Default Gateway:	0.0.0.0	
Primary DNS:	DNS Client Settings...	

LAN Status

LAN Subnet Mask:	255.255.255.0	
Act as Local DHCP Server:	Yes	DHCP Server Settings...
MAC Address:	00:01:38:1F:64:DE	

Software Status

Up-Time:	00:37:48s
Version:	1.05APF19.7768A

Defined Interfaces

ppp-0:	Show Statistics...	Port:adsl VPI/VCI: 8/32
pppoe-1:	Show Statistics...	Port:adsl VPI/VCI: 8/36
wlan_filtered:	Show Statistics...	

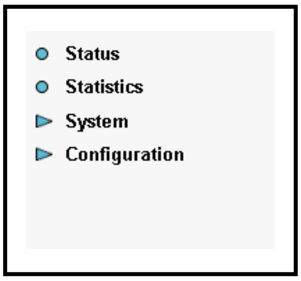
Webserver Status

HTTP Port:	80
Auxillary HTTP Port:	8008

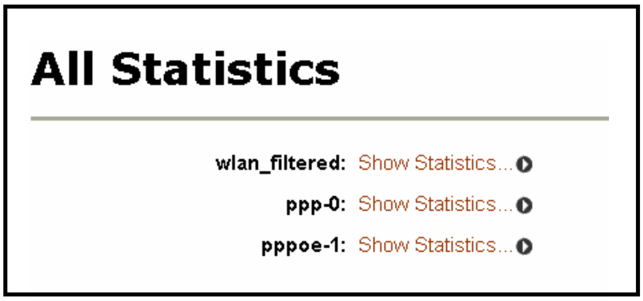
ADSL Status

Firmware Version		
OP state	Showtime	
Last Failed Status	(0x00000000)	
start Progress	0x000000ad	
Watchdog Timer	0x00000053	
Local SNR margin	35.5 dBdB	
Remote SNR margin	31 dB dB	
Line Code	t1.413	
	Down-stream	**Up-stream**
Line Rate	512000 bps	128000 bps
Latency	Interleave	Interleave

3. Statistics



The **Statistics** page displays the current interfaces of ***X7768r/X7768r*****+**. Click on the appropriate **Show Statistics** link to view the statistics of that interface.



All Statistics

wlan_filtered: Show Statistics...

ppp-0: Show Statistics...

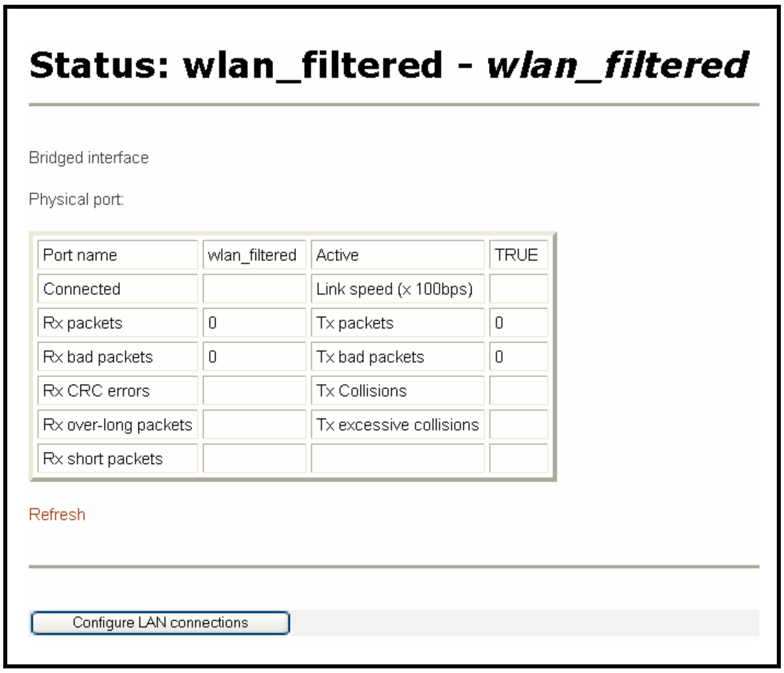
pppoe-1: Show Statistics...

The two examples are listed below.

1. Wlan_filtered Statistics
2. PPPoE Statistics

Example 1: Wlan_filtered Show Statistics

- This page displays the current statistics of the Wireless LAN port. This includes port name, connection status, speed, and transfer/receive packets.
- You may edit the default LAN port by clicking on the **Configure LAN Connections** button. *(For instructions on how to configure LAN connection, refer to section 5.2 LAN Connection)*



Status: wlan_filtered - *wlan_filtered*

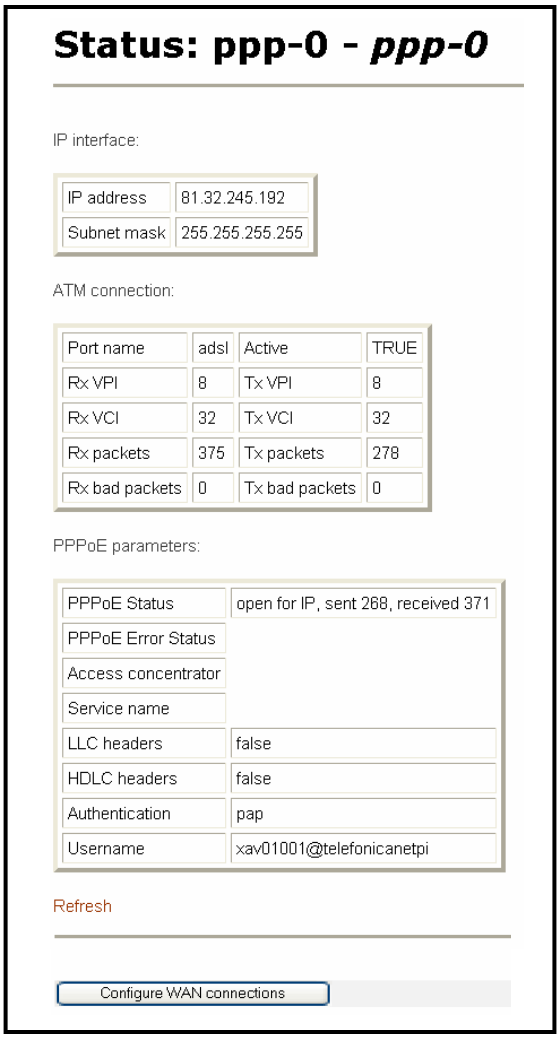
Bridged interface

Physical port:

Port name	wlan_filtered	Active	TRUE
Connected		Link speed (x 100bps)	
Rx packets	0	Tx packets	0
Rx bad packets	0	Tx bad packets	0
Rx CRC errors		Tx Collisions	
Rx over-long packets		Tx excessive collisions	
Rx short packets			

Example 2: PPPoE Show Statistics

- This page displays the current statistics of the PPPoE WAN connection status. This includes IP interface, ATM connections, and PPPoE parameters.
- You may edit/add WAN connections by clicking on the **Configure WAN Connections** button. *(For instructions on how to configure LAN connection, refer to section 5.3 WAN Connections.)*



Status: ppp-0 - *ppp-0*

IP interface:

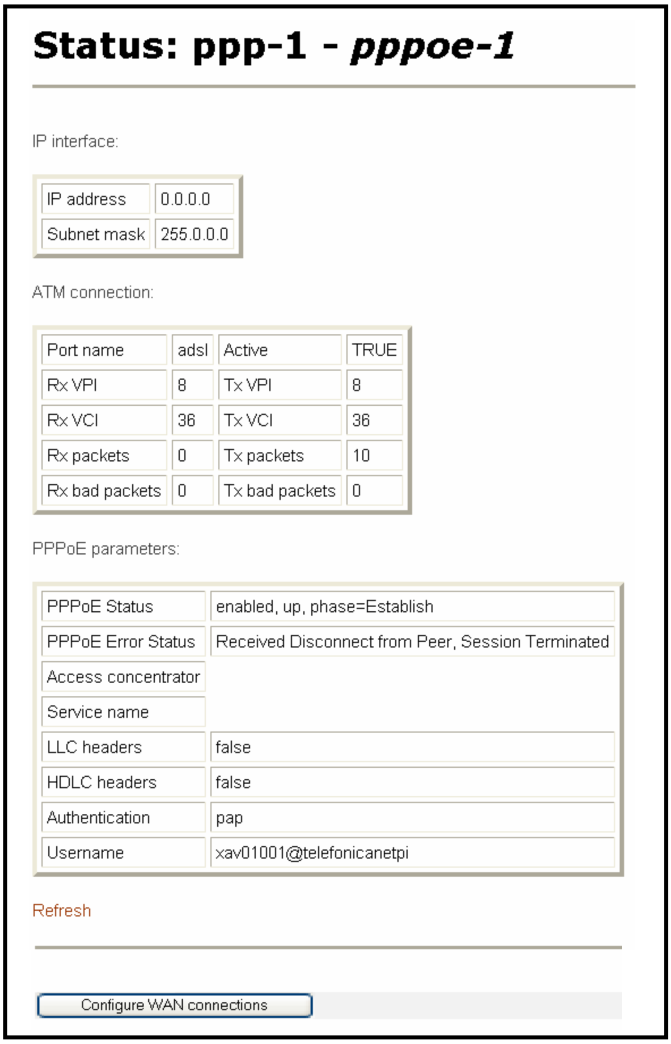
IP address	81.32.245.192
Subnet mask	255.255.255.255

ATM connection:

Port name	adsl	Active	TRUE
Rx VPI	8	Tx VPI	8
Rx VCI	32	Tx VCI	32
Rx packets	375	Tx packets	278
Rx bad packets	0	Tx bad packets	0

PPPoE parameters:

PPPoE Status	open for IP, sent 268, received 371
PPPoE Error Status	
Access concentrator	
Service name	
LLC headers	false
HDLC headers	false
Authentication	pap
Username	xav01001@telefonicanetpi



Status: ppp-1 - *pppoe-1*

IP interface:

IP address	0.0.0.0
Subnet mask	255.0.0.0

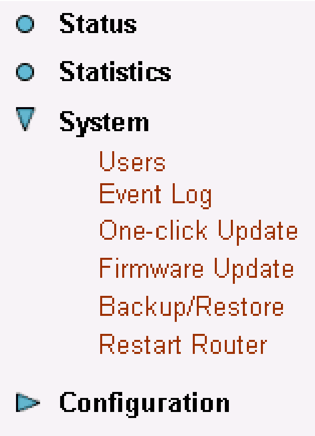
ATM connection:

Port name	adsl	Active	TRUE
Rx VPI	8	Tx VPI	8
Rx VCI	36	Tx VCI	36
Rx packets	0	Tx packets	10
Rx bad packets	0	Tx bad packets	0

PPPoE parameters:

PPPoE Status	enabled, up, phase=Establish
PPPoE Error Status	Received Disconnect from Peer, Session Terminated
Access concentrator	
Service name	
LLC headers	false
HDLC headers	false
Authentication	pap
Username	xav01001@telefonicanetpi

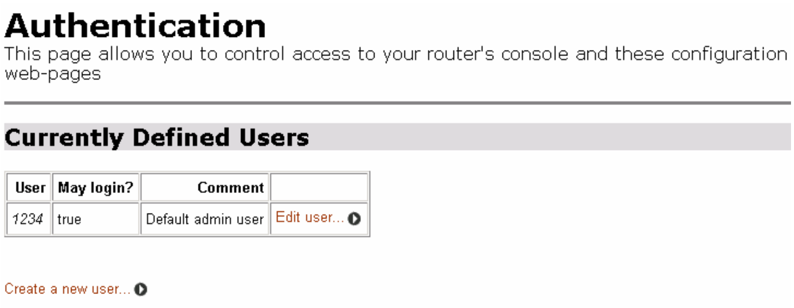
4. System



The **System** section includes **Users, Event Log, One-click Update, Firmware Update, Back/Restore** and **Restart** links. Each link is described in detail below.

4.1 Users

- Click on the **Users** link on the navigation bar to view the list of users. By default, only the **1234** user exists.



Authentication

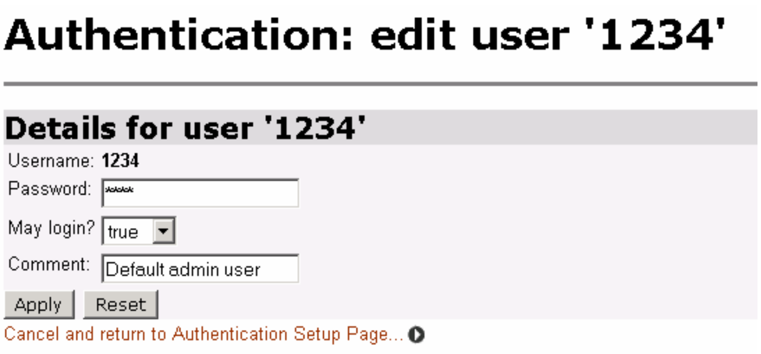
This page allows you to control access to your router's console and these configuration web-pages

Currently Defined Users

User	May login?	Comment	
1234	true	Default admin user	Edit user...

Create a new user...

- Click on the **Edit User…** link to change the settings of the **1234** user. On this page, you can change the password and comment of the **1234** user. Click on the **Apply** button when completed.



Authentication: edit user '1234'

Details for user '1234'

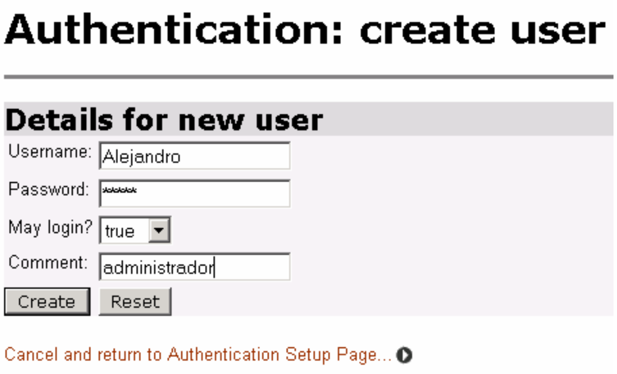
Username: 1234

Password: ****

May login? true

Comment: Default admin user

- Click on the **Create a new user…** link to add a new user. On this page, you need to enter a username, password, and select true or false, if you would like this user to have configuration rights, and add a comment. Click on the **Create** button when completed.



Authentication: create user

Details for new user

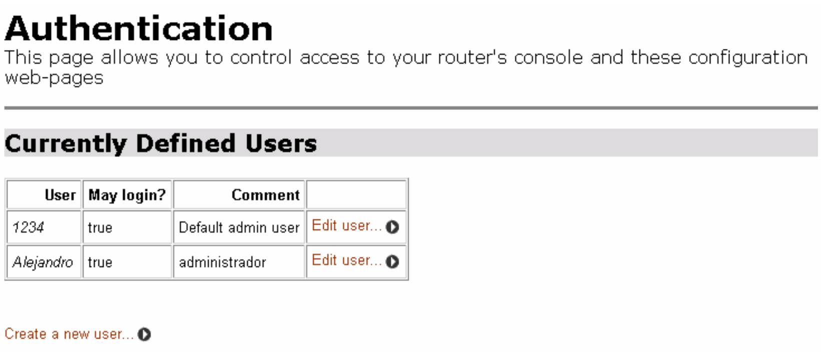
Username: Alejandro

Password: *****

May login? true

Comment: administrador

- You will then notice that the user has been added to the table.



Authentication

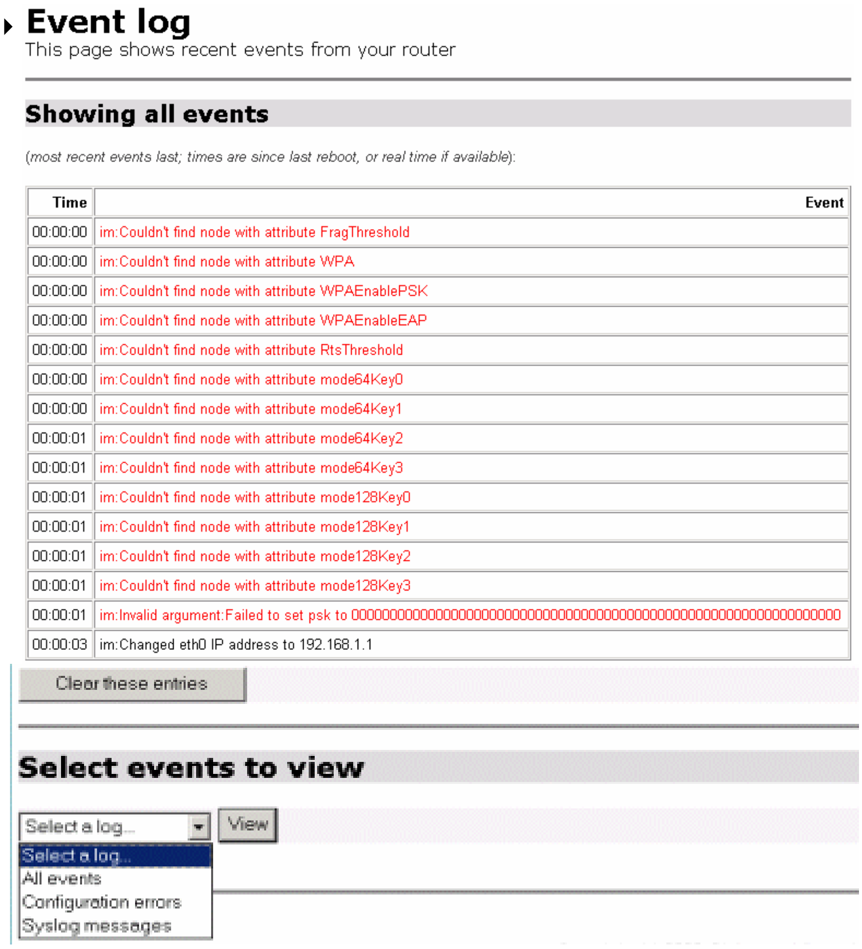
This page allows you to control access to your router's console and these configuration web-pages

Currently Defined Users

User	May login?	Comment	
1234	true	Default admin user	Edit user...
Alejandro	true	administrador	Edit user...

4.2 Event Log

- Click on the **Event Log** link in the navigation bar to view the all the events from this device.



Event log

This page shows recent events from your router

Showing all events

(most recent events last; times are since last reboot, or real time if available):

Time	Event
00:00:00	im:Couldn't find node with attribute FragThreshold
00:00:00	im:Couldn't find node with attribute WPA
00:00:00	im:Couldn't find node with attribute WPAEnablePSK
00:00:00	im:Couldn't find node with attribute WPAEnableEAP
00:00:00	im:Couldn't find node with attribute RtsThreshold
00:00:00	im:Couldn't find node with attribute mode64Key0
00:00:00	im:Couldn't find node with attribute mode64Key1
00:00:01	im:Couldn't find node with attribute mode64Key2
00:00:01	im:Couldn't find node with attribute mode64Key3
00:00:01	im:Couldn't find node with attribute mode128Key0
00:00:01	im:Couldn't find node with attribute mode128Key1
00:00:01	im:Couldn't find node with attribute mode128Key2
00:00:01	im:Couldn't find node with attribute mode128Key3
00:00:01	im:Invalid argument:Failed to set psk to 0000000000000000000000000000000000000000000000000000000000000000
00:00:03	im:Changed eth0 IP address to 192.168.1.1

Select events to view

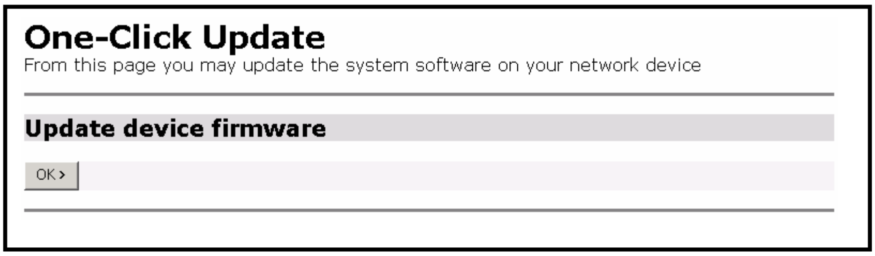
- Click on the **Clear these entries** button to clear all the event records.

- From the drop-down menu, select an event log you want to see, and click **View** then.

4.3 One-Click Update

Click on the **One-Click Updade** link on the navigation bar to update the system software to your device. Click OK button, and system will connect to the equipment manufacture server to check if there is the latest software. The latest software will be automatically installed to your computer.

Note: Be sure that you have got online before you click the "OK" button.



One-Click Update

From this page you may update the system software on your network device

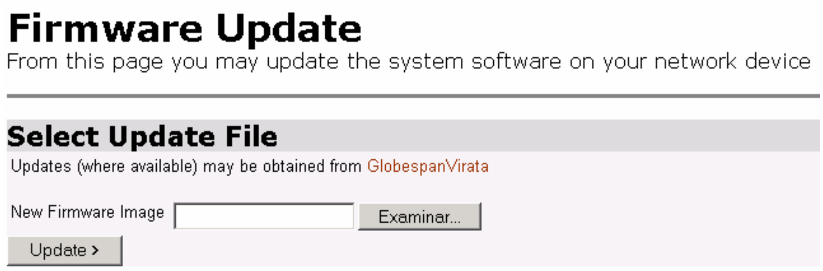
Update device firmware

4.4 Firmware Update

This function provides you to update the firmware manually. Click on the **Firmware Upgrade** link on the navigation bar to view the firmware upgrade page, then follow the steps below:

a) Click on the **Examinar** button to select the upgrade file.

b) Click on the **Upgrade** button when completed.



Firmware Update

From this page you may update the system software on your network device

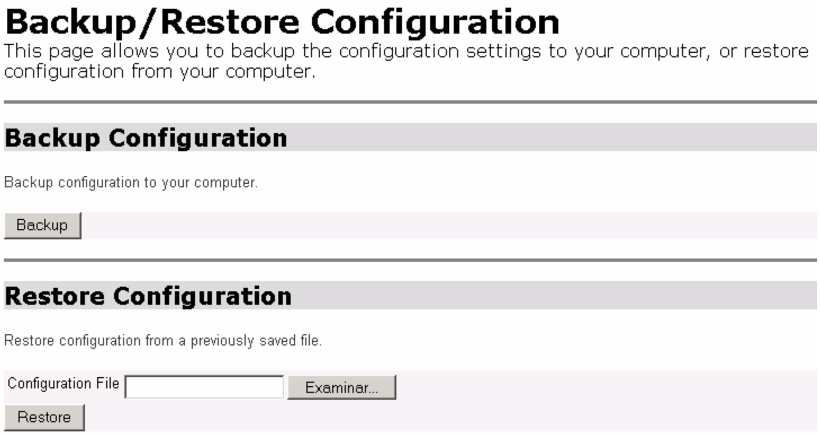
Select Update File

Updates (where available) may be obtained from GlobespanVirata

New Firmware Image

4.5 Backup/Restore Configuration

- Click on the **Backup/Restore** link in the navigation bar to view the Backup/Restore interface.



Backup/Restore Configuration

This page allows you to backup the configuration settings to your computer, or restore configuration from your computer.

Backup Configuration

Backup configuration to your computer.

Restore Configuration

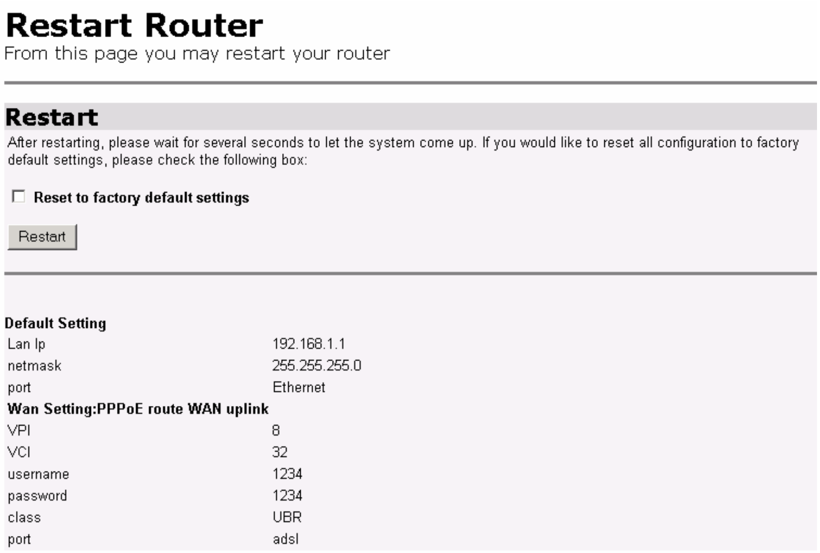
Restore configuration from a previously saved file.

Configuration File

- **Backup Configuration:** To back up a configuration file, click on the **Backup** button, and then select the location where you would like to save the file.
- **Restore Configuration:** To restore a configuration file, click on the **Examinar** button to select the backup file, and then click on the **Restore** button to restore the configuration. Please note that settings can only be permanently saved through the **Configuration → Save** interface.

4.6 Restart Router

To restart the device, click on the **Restart** button. You may also check the box, if you would like to restart the modem with the factory settings. The default settings are displayed at the bottom of this page.



Restart Router

From this page you may restart your router

Restart

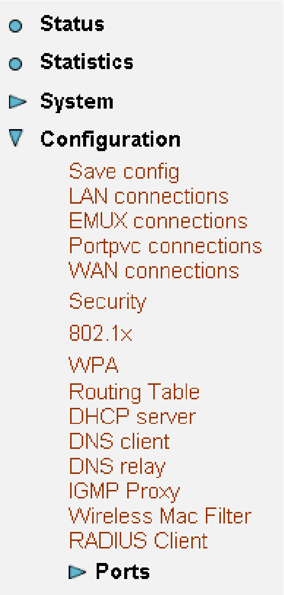
After restarting, please wait for several seconds to let the system come up. If you would like to reset all configuration to factory default settings, please check the following box:

□ **Reset to factory default settings**

Default Setting

Lan Ip	192.168.1.1
netmask	255.255.255.0
port	Ethernet
Wan Setting:PPPoE route WAN uplink	
VPI	8
VCI	32
username	1234
password	1234
class	UBR
port	adsl

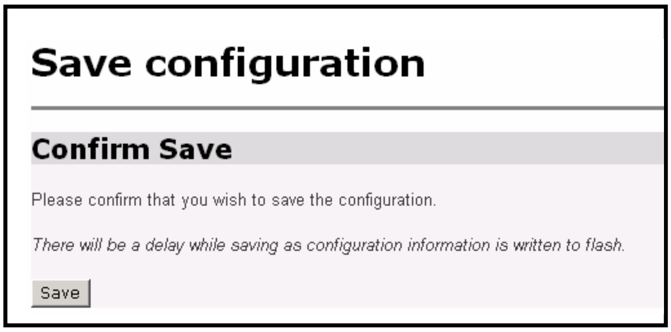
3. Configuration



The **Configuration** section includes **Save config, LAN connections, WAN connections, Security, 802.1x, WPA, Routing Table, DHCP server, DNS relay, SNTP client, IGMP proxy, Wireless Mac Filter,** and **RADIUS Client** links. Each link is described in detail below.

5.1 Save Config

Click on the **Save Config** link in the navigation bar to view the save confirmation page. If you would like to save the current configurations, click on the **Save** button.



Save configuration

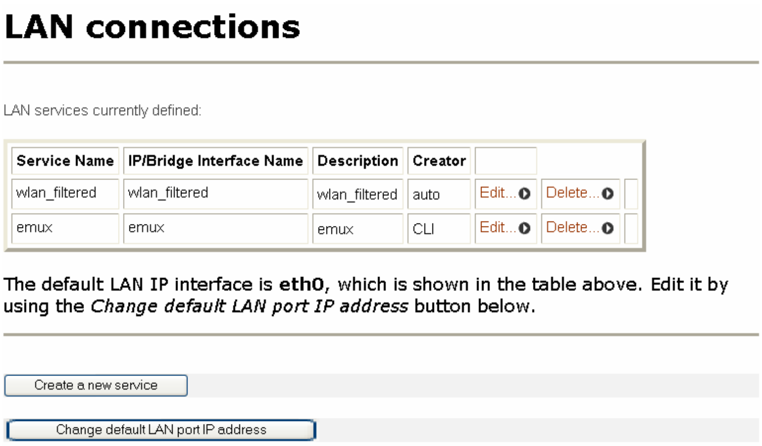
Confirm Save

Please confirm that you wish to save the configuration.

There will be a delay while saving as configuration information is written to flash.

5.2 LAN Connections

Define current LAN services.



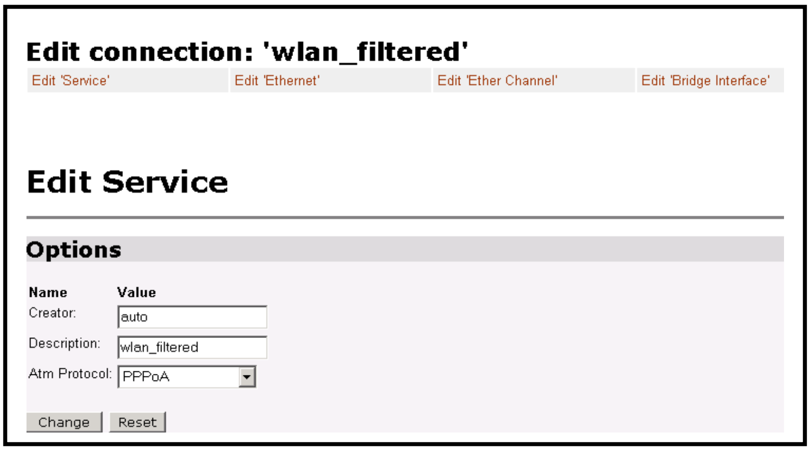
LAN connections

LAN services currently defined:

Service Name	IP/Bridge Interface Name	Description	Creator			
wlan_filtered	wlan_filtered	wlan_filtered	auto	Edit...	Delete...	
emux	emux	emux	CLI	Edit...	Delete...	

The default LAN IP interface is eth0, which is shown in the table above. Edit it by using the *Change default LAN port IP address* button below.

- Click **Edit.** or **Delete…** link to edit/delete service. When you would like to edit a new wlan_filtered/emux service, there are five ATM Protocol you can choose: PPPoA, PPPoE, RFC 1483-Routed, RFC 1483-Bridged and IPoA.



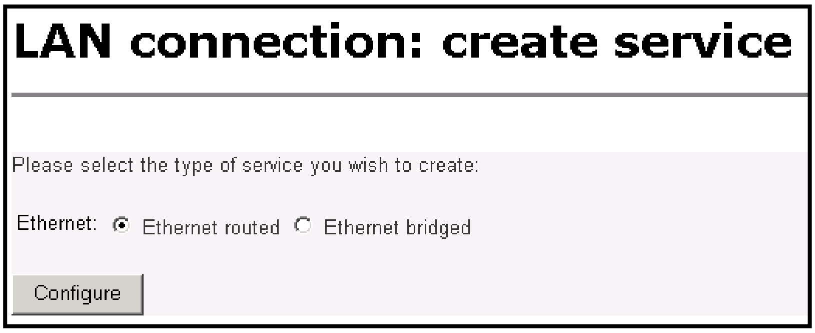
Edit connection: 'wlan_filtered'

Edit Service

Options

Name	Value
Creator:	auto
Description:	wlan_filtered
Atm Protocol:	PPPoA

- **Create a new service:** Click the **Create a new service** button to create Ethernet routed or Ethernet bridged service.



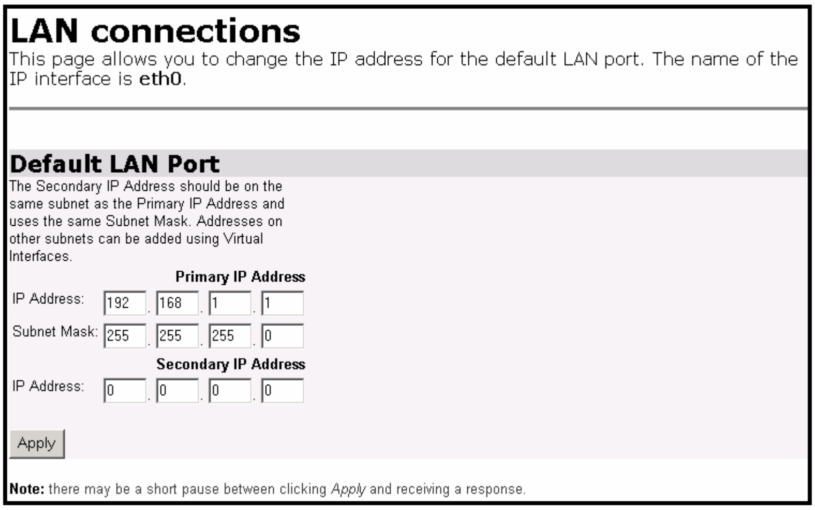
LAN connection: create service

Please select the type of service you wish to create:

Ethernet: ● Ethernet routed ○ Ethernet bridged

- **Change Default LAN port IP Address:** The default LAN IP interface is **eth0**, which is shown in the table above. Edit it by using the **Change default LAN port IP address** button below.

- After reset the Default LAN Port IP Address, click **Apply** button to activate it. ***Note:*** *there may be a short pause between clicking Apply and receiving a response.*



LAN connections

This page allows you to change the IP address for the default LAN port. The name of the IP interface is eth0.

Default LAN Port

The Secondary IP Address should be on the same subnet as the Primary IP Address and uses the same Subnet Mask. Addresses on other subnets can be added using Virtual Interfaces.

Primary IP Address

IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255 . 255 . 255 . 0

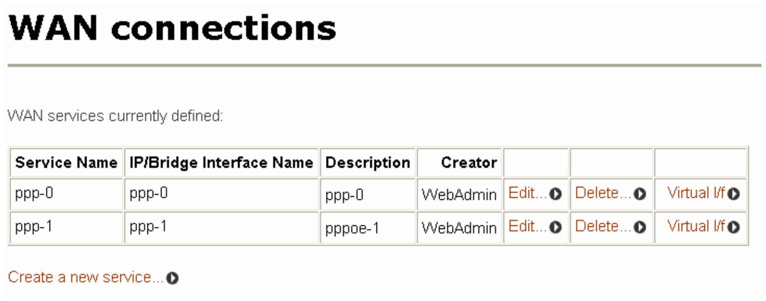
Secondary IP Address

IP Address: 0 . 0 . 0 . 0

Note: there may be a short pause between clicking *Apply* and receiving a response.

5.3 WAN Connections

- The page lists WAN connection protocols that are available on this device. Please see the following instructions on creating each type of the WAN connection.



WAN connections

WAN services currently defined:

Service Name	IP/Bridge Interface Name	Description	Creator			
ppp-0	ppp-0	ppp-0	WebAdmin	Edit...	Delete...	Virtual I/f
ppp-1	ppp-1	pppoe-1	WebAdmin	Edit...	Delete...	Virtual I/f

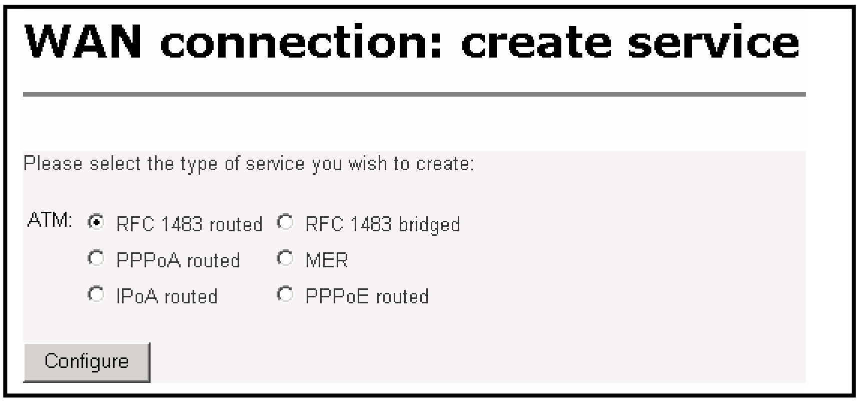
Create a new service...

- You can create multiple WAN connection services from each of following protocols:

5.3.1 RFC 1483 Routed
5.3.2 RFC 1483 Bridged
5.3.3 PPPoA Routed
5.3.4 MER
5.3.5 IPoA Routed
5.3.6 PPPoE Routed

5.3.1 RFC 1483 Routed

- Click **Create a new service** to display the type of service.
- Select **RFC 1483 routed** and then click on the **Configure** button.

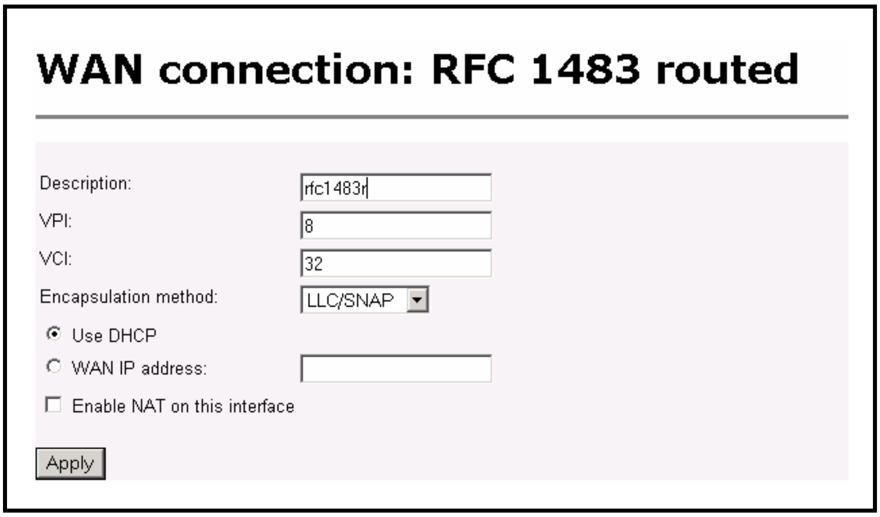


WAN connection: create service

Please select the type of service you wish to create:

ATM: ● RFC 1483 routed ○ RFC 1483 bridged
○ PPPoA routed ○ MER
○ IPoA routed ○ PPPoE routed

- Define the **VPI, VCI, and WAN IP** to match the DSLAM setting. (Provided by the ISP)
- Select **LLC/SNAP** for **Encapsulation**.
- Choose between DHCP and WAN IP, and then click on the **Apply** button to confirm the configuration.

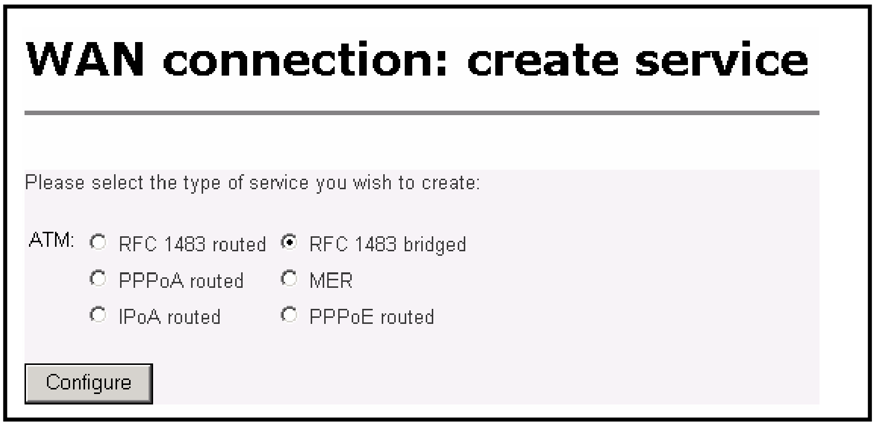


WAN connection: RFC 1483 routed

Description:	rfc1483r
VPI:	8
VCI:	32
Encapsulation method:	LLC/SNAP
● Use DHCP	
○ WAN IP address:	
□ Enable NAT on this interface	

5.3.2 RFC 1483 Bridged

- Click **Create a new service** to display the type of service.
- Select **RFC 1483 bridged** and then click on the **Configure** button.

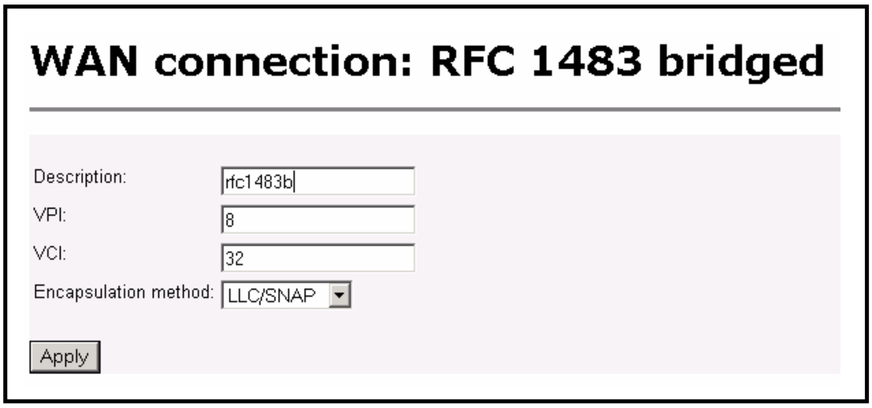


WAN connection: create service

Please select the type of service you wish to create:

ATM: ○ RFC 1483 routed ● RFC 1483 bridged
○ PPPoA routed ○ MER
○ IPoA routed ○ PPPoE routed

- Define the **VPI**, **VCI** to match the DSLAM setting
- Select **LLC/SNAP** for **Encapsulation,** and then click on the **Apply** button to confirm the configuration.

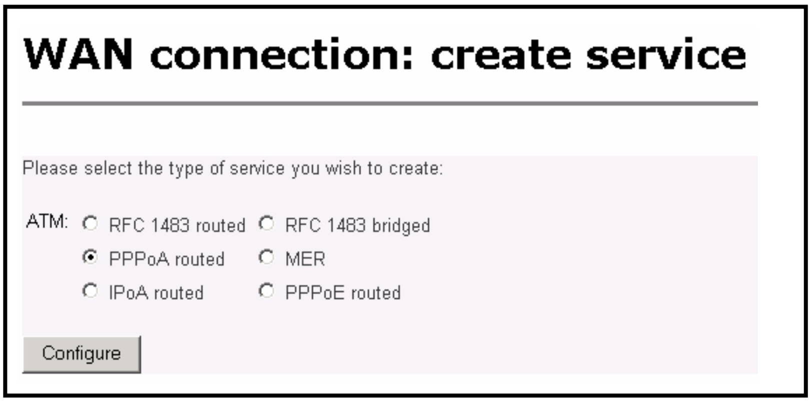


WAN connection: RFC 1483 bridged

Description: rfc1483b
VPI: 8
VCI: 32
Encapsulation method: LLC/SNAP

5.3.3 PPPoA Routed

- Click **Create a new service** to display the type of service.
- Select **PPPoA routed** and then click on the **Configure** button.

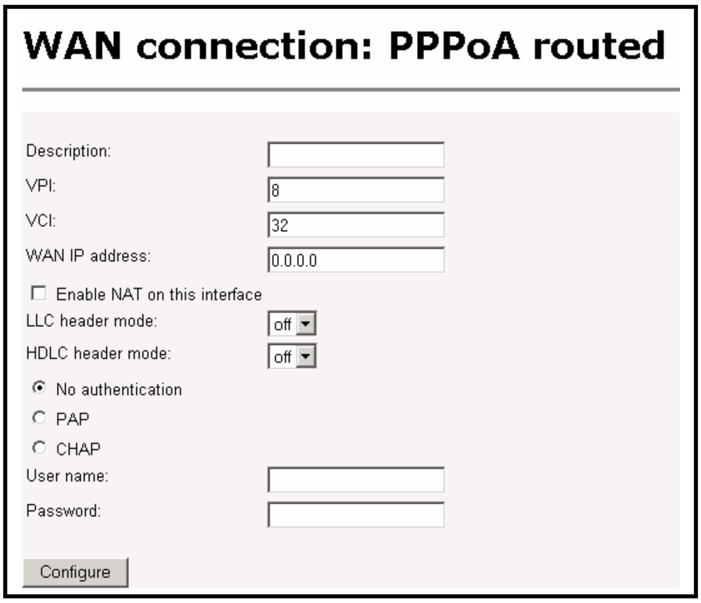


WAN connection: create service

Please select the type of service you wish to create:

ATM: ○ RFC 1483 routed ○ RFC 1483 bridged
● PPPoA routed ○ MER
○ IPoA routed ○ PPPoE routed

- Type **PPPoA router** for the description, then define the **VPI**, **VCI** to match the DSLAM setting
- Keep WAN IP default setting (0.0.0.0.)
- Leave LLC header Mode/HDLC header mode to **off**.
- Select **PAP**
- Type in the **Username** and **Password**.
- Click on the **Configure** button to confirm the configuration.

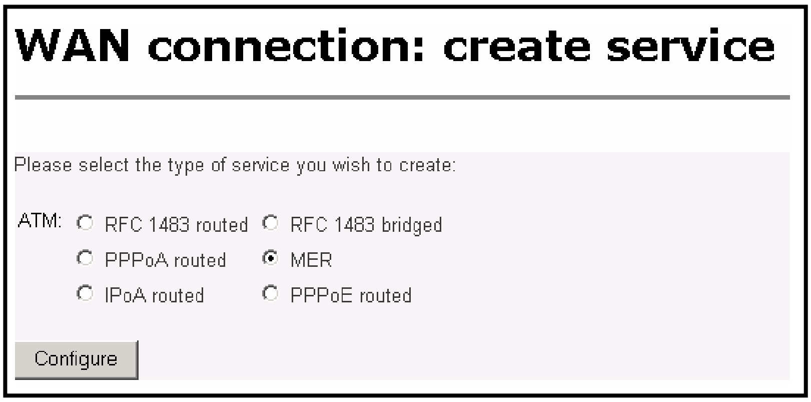


WAN connection: PPPoA routed

Description:
VPI: 8
VCI: 32
WAN IP address: 0.0.0.0
□ Enable NAT on this interface
LLC header mode: off
HDLC header mode: off
● No authentication
○ PAP
○ CHAP
User name:
Password:

5.3.4 MER

- Click **Create a new service** to display the type of service.
- Select **MER** and then click on the **Configure** button.

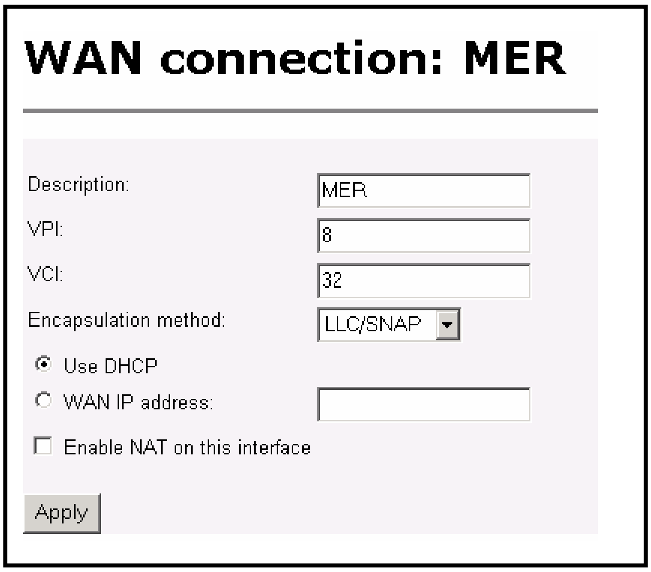


WAN connection: create service

Please select the type of service you wish to create:

ATM: ○ RFC 1483 routed ○ RFC 1483 bridged
○ PPPoA routed ● MER
○ IPoA routed ○ PPPoE routed

- Type **MER** for the description, then define the **VPI**, **VCI** to match the DSLAM setting
- Keep WAN IP default setting (0.0.0.0.)
- Choose LLC/SNAP for the Encapsulation method.
- Click on the **Apply** button to confirm the configuration.

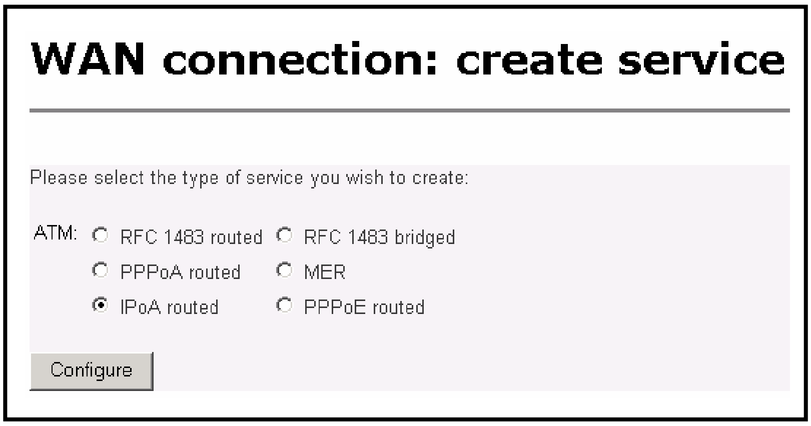


WAN connection: MER

Description:	MER
VPI:	8
VCI:	32
Encapsulation method:	LLC/SNAP
● Use DHCP	
○ WAN IP address:	
□ Enable NAT on this interface	

5.3.5 IPoA Routed

- Click **Create a new service** to display the type of service.
- Select **IPoA routed** and then click on the **Configure** button.

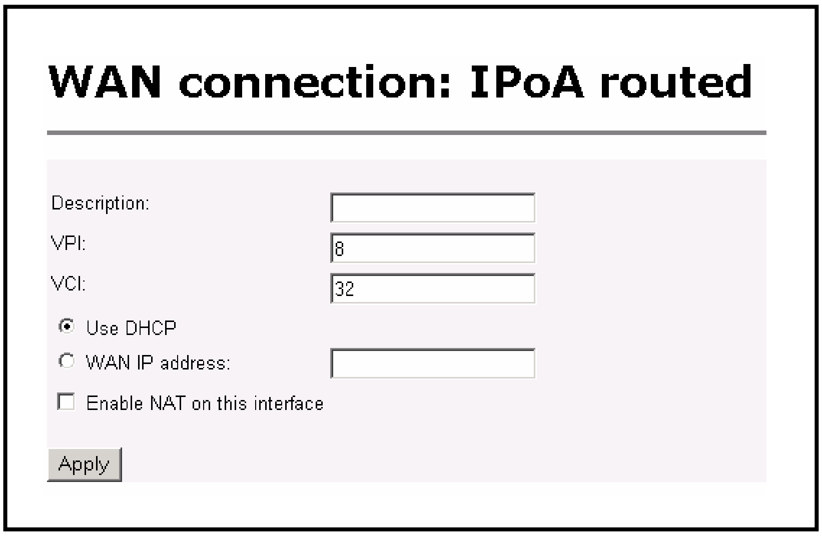


WAN connection: create service

Please select the type of service you wish to create:

ATM: ○ RFC 1483 routed ○ RFC 1483 bridged
○ PPPoA routed ○ MER
● IPoA routed ○ PPPoE routed

- Type **IPoA router** for the description.
- Define the **VPI**, **VCI**, **WAN IP** based on the DSLAM setting.
- Click on the **Apply** button to confirm the configuration.

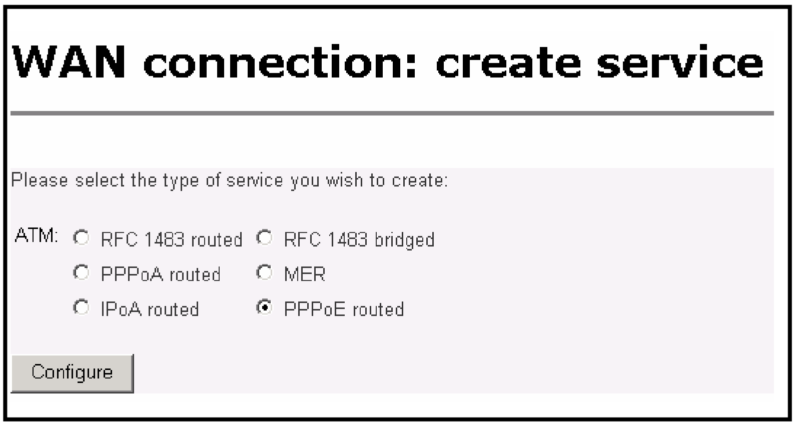


WAN connection: IPoA routed

Description:
VPI: 8
VCI: 32
● Use DHCP
○ WAN IP address:
□ Enable NAT on this interface

5.3.6 PPPoE Routed

- Click **Create a new service** to display the type of service.
- Select **PPPoE routed** and then click on the **Configure** button.

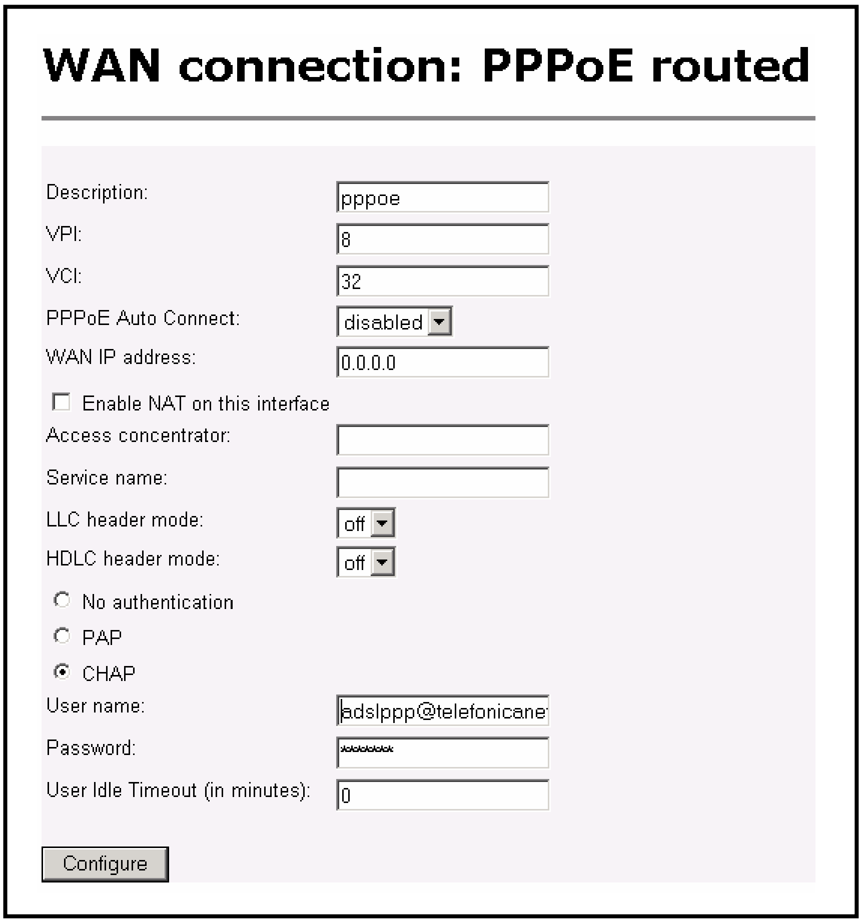


WAN connection: create service

Please select the type of service you wish to create:

ATM: ○ RFC 1483 routed ○ RFC 1483 bridged
○ PPPoA routed ○ MER
○ IPoA routed ● PPPoE routed

- Type **PPPoE router** for the description.
- Define the **VPI**, **VCI** value to match the DSLAM/ISP setting.
- Set **PPPoE Auto Connect** to **Enabled**.
- Use WAN IP default setting (0.0.0.0.)
- Leave **Access concentrator** and **service name** blank
- Leave LLC/HDLC header Mode to **off**.
- Select **PAP** and type the **Username** and **Password** and type **idle time** number.
- Click on the **Configure** button to confirm the configuration.

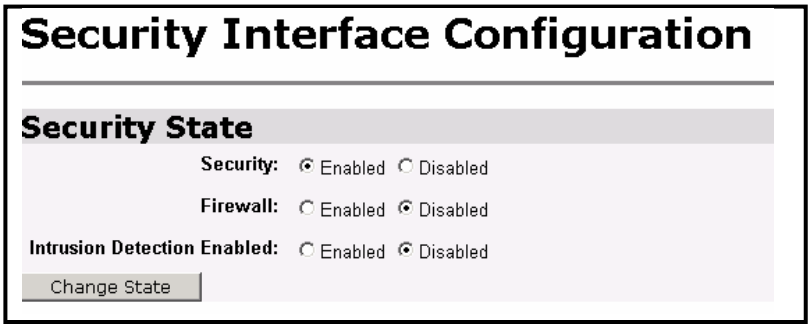


WAN connection: PPPoE routed

Description:	pppoe
VPI:	8
VCI:	32
PPPoE Auto Connect:	disabled ▾
WAN IP address:	0.0.0.0
□ Enable NAT on this interface	
Access concentrator:	
Service name:	
LLC header mode:	off ▾
HDLC header mode:	off ▾
○ No authentication	
○ PAP	
● CHAP	
User name:	adslppp@telefonicane
Password:	*******
User Idle Timeout (in minutes):	0

5.4 Security

- Click on the **Security** link on the navigation bar. In this section, you will be able to configure the Security Interface. This includes the security state, security level, security interfaces, policies, triggers, and intrusion detection.
- Select **Enabled** Security, and then click the **Change State** button



Security Interface Configuration

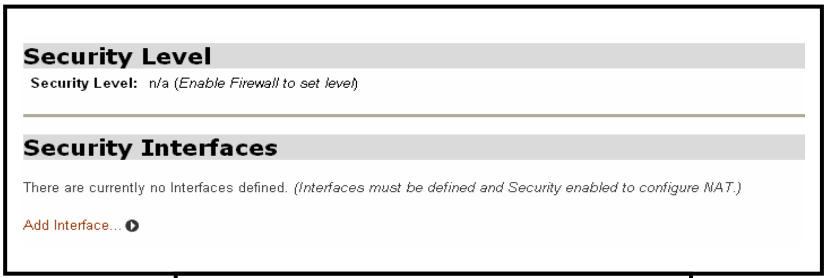
Security State

Security: ● Enabled ○ Disabled

Firewall: ○ Enabled ● Disabled

Intrusion Detection Enabled: ○ Enabled ● Disabled

- Under the Security Interfaces menu, click on the **Add Interface** link to add a security interface. You will then see the following screen. Select an interface name (eth0) and interface type (internal), and then click on the **Apply** button. You will then see the added interface on the main page.

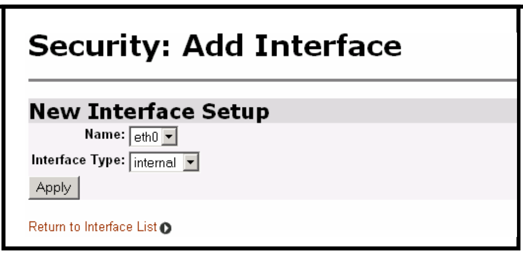


Security Level

Security Level: n/a (*Enable Firewall to set level*)

Security Interfaces

There are currently no Interfaces defined. *(Interfaces must be defined and Security enabled to configure NAT.)*



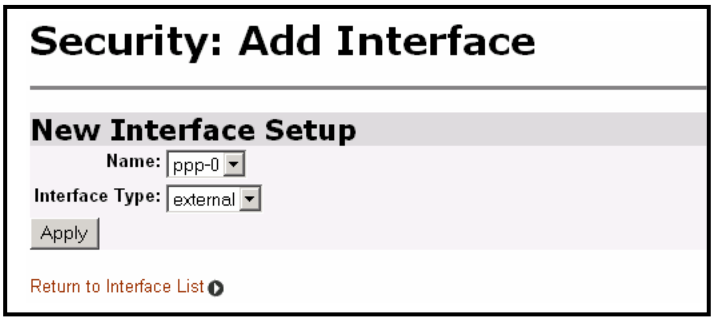
Security: Add Interface

New Interface Setup

Name: eth0

Interface Type: internal

- Once again, click on the **Add Interface** button to add an external interface.
- Select an interface name (ppp-0) and interface type (external), and then click on the **Apply** button.



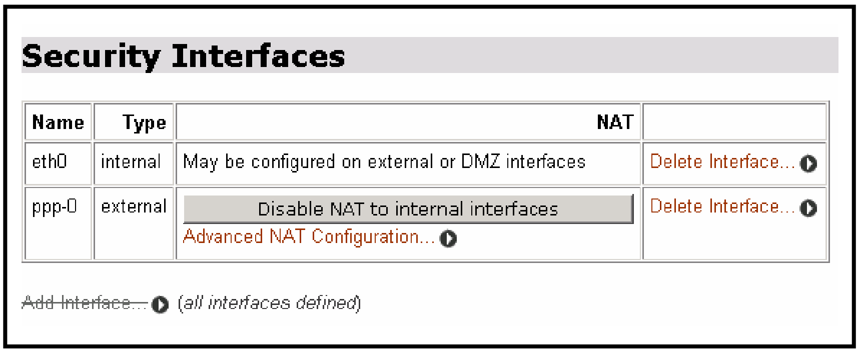
Security: Add Interface

New Interface Setup

Name: ppp-0

Interface Type: external

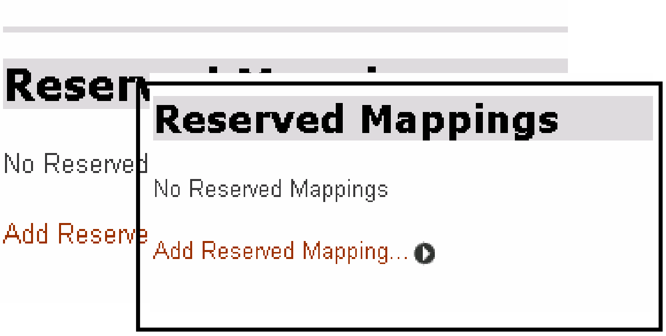
- You will then see the added interface on the main page. Click on the **Enable NAT to internal interfaces** button to enable Network Address Translation (NAT).



Security Interfaces

Name	Type	NAT	
eth0	internal	May be configured on external or DMZ interfaces	Delete Interface...
ppp-0	external	Disable NAT to internal interfaces Advanced NAT Configuration...	Delete Interface...

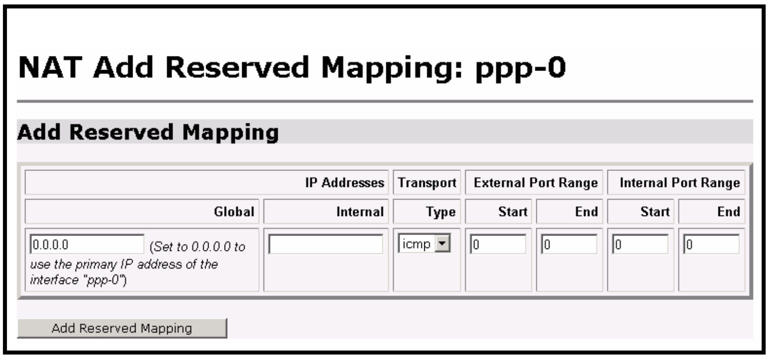
~~Add Interface...~~ *(all interfaces defined)*



Reserved Mappings

No Reserved Mappings

- Click on **Add Reserved Mapping**, to map a global IP address and external port range to an internal IP address and internal port range.

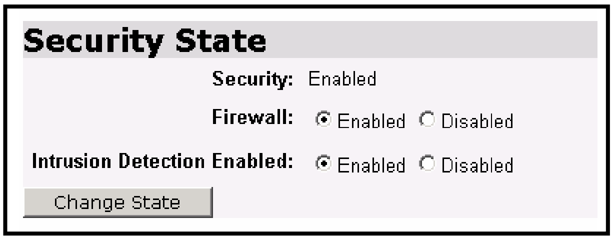


NAT Add Reserved Mapping: ppp-0

Add Reserved Mapping

IP Addresses		Transport	External Port Range		Internal Port Range	
Global	Internal	Type	Start	End	Start	End
0.0.0.0 *(Set to 0.0.0.0 to use the primary IP address of the interface "ppp-0")*		icmp	0	0	0	0

- Scroll back up to the Security State section; select **Enabled** for both **Firewall** and **Intrusion Detection**. Then click on the **Change State** button.



Security State

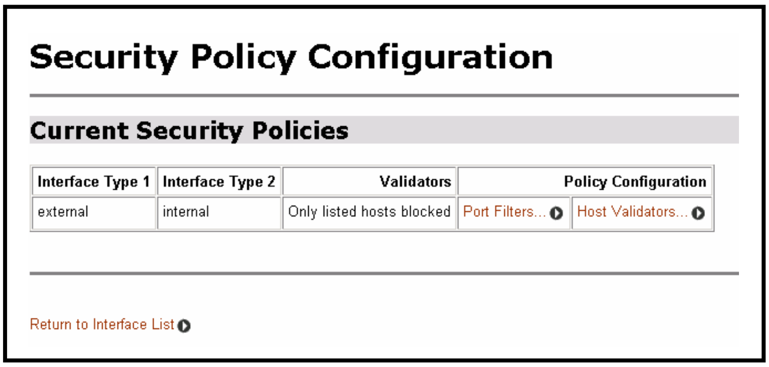
Security: Enabled

Firewall: ● Enabled ○ Disabled

Intrusion Detection Enabled: ● Enabled ○ Disabled

Security Policy Configuration

- Scroll down and click on the **Security Policy Configuration** link under the **Policies, Triggers, Intrusion Detection, Logging** section. You will then see the following screen.



Security Policy Configuration

Current Security Policies

Interface Type 1	Interface Type 2	Validators	Policy Configuration	
external	internal	Only listed hosts blocked	Port Filters...	Host Validators...

Return to Interface List

- To configure port filters, click on the **Port Filters** link for the specified interface. The following port filters may be added:

Field Name	Description
TCP Filter	Requires port range (start/end IP) and direction (inbound/outbound)
UDP Filter	Requires port range (start/end IP) and direction (inbound/outbound)
Raw IP Filter	Requires protocol type (TCP/UDP) and direction (inbound/outbound)

- To configure host validators, click on the **Host Validators** link for the specified interface. The following host validators may be added:

Field Name	Description
Host IP address	IP address of the host, for example 1.1.1.1
Host Subnet mask	Subnet mask of the above host, for example 255.255.255.255
Direction	Select Inbound, Outbound, or Both

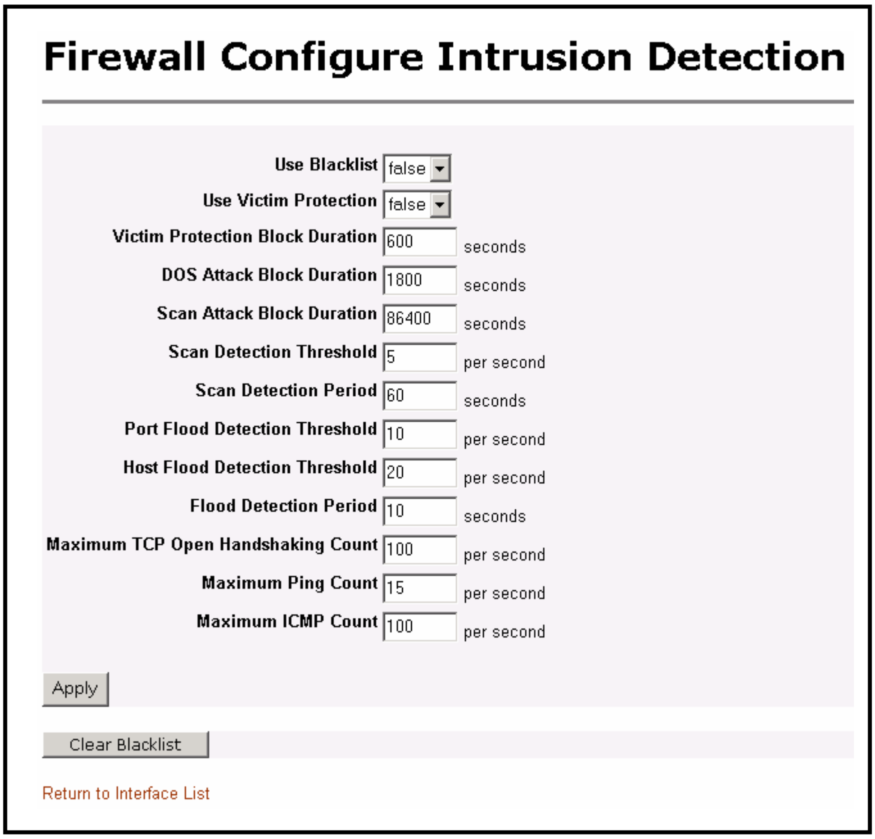
Security Trigger Configuration

- Return to the Interface List and click on the **Security Trigger Configuration** link. A trigger is the term used to describe what happens when a secondary port is opened dynamically to allow protocols such as FTP and NetMeeting to pass data through the Firewall.
- Click on **New Trigger** to add a new security trigger.
- The following fields are required to add a security trigger.

Field Name	Description
Transport type	Choose between TCP or UDP
Port number start	Enter the starting port number, for example 21 for FTP
Port number end	Enter the ending port number, for example 21 for FTP
Allow multiple hosts	Choose between allow or block
Max Activity Interval	Enter the activity interval per second.
Enable Session Chaining	Choose between allow or block
Enable UDP Session Chaining	Choose between allow or block
Binary Address Replacement	Choose between allow or block
Address Translation Type	Choose between TCP, UDP, both, or none.

Configure Intrusion Detection

- Return to the Interface List and click on the **Configure Intrusion Detection** link. On this page you will be able to select whether you would like to use a black list and victim protection. You can also set values for DoS attack block duration, scan attack block duration, Victim protection block duration, maximum TCP open handshaking count, maximum ping count, and maximum ICMP count.



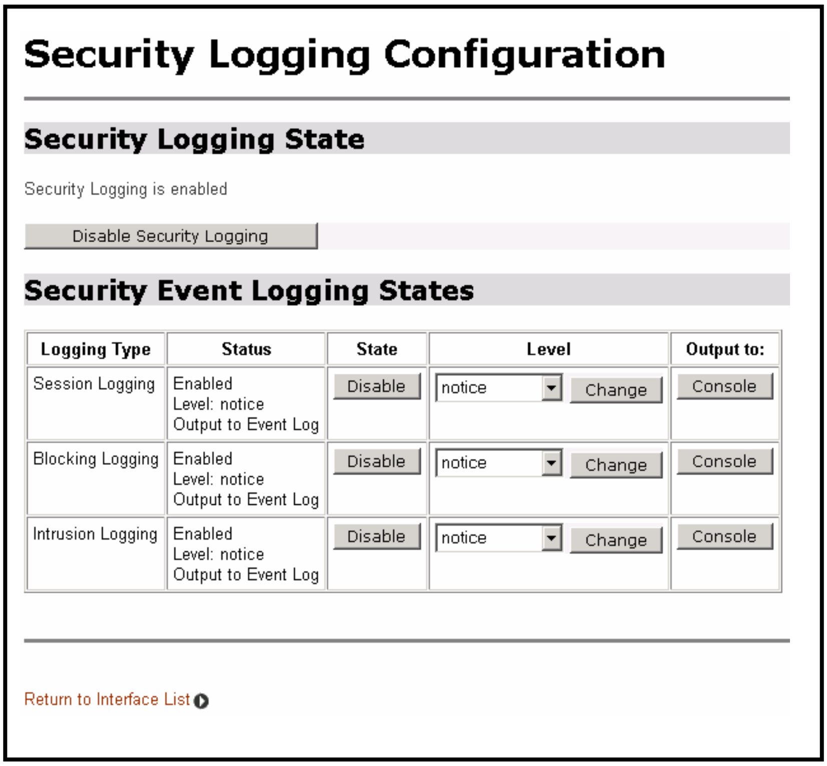
Firewall Configure Intrusion Detection

Use Blacklist	false	
Use Victim Protection	false	
Victim Protection Block Duration	600	seconds
DOS Attack Block Duration	1800	seconds
Scan Attack Block Duration	86400	seconds
Scan Detection Threshold	5	per second
Scan Detection Period	60	seconds
Port Flood Detection Threshold	10	per second
Host Flood Detection Threshold	20	per second
Flood Detection Period	10	seconds
Maximum TCP Open Handshaking Count	100	per second
Maximum Ping Count	15	per second
Maximum ICMP Count	100	per second

- Click on the **Apply** button once you have set/changed these values.

Configure Security Logging

- Return to the Interface List and click on the **Configure Security Logging** link. On this page you may modify security-logging settings. The three types of security logging are **Session Logging**, **Blocking Logging**, and **Intrusion Logging**.



Security Logging Configuration

Security Logging State

Security Logging is enabled

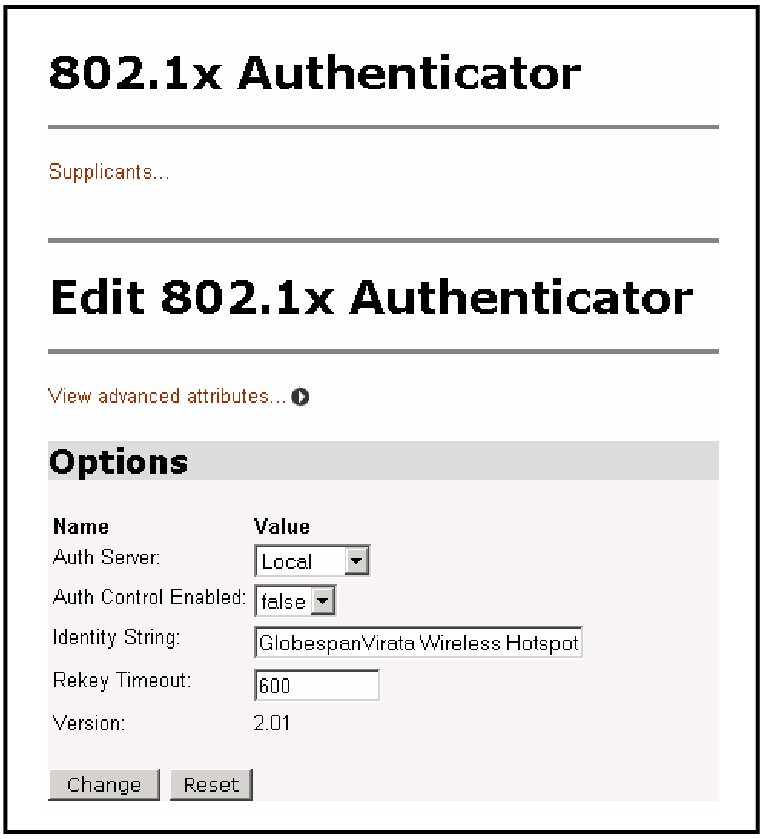
Security Event Logging States

Logging Type	Status	State	Level	Output to:
Session Logging	Enabled Level: notice Output to Event Log	Disable	notice Change	Console
Blocking Logging	Enabled Level: notice Output to Event Log	Disable	notice Change	Console
Intrusion Logging	Enabled Level: notice Output to Event Log	Disable	notice Change	Console

- By default security logging is disabled. Click on the **Enable Security Logging** button to enable the logging feature.
- You may also disable security logging individually by clicking on the **Disable** button of the respected logging type.
- You may change the level of security logging by selecting an option from the drop-down list. Options available are: emergency, alert, critical, error, warning, notice, informational, and debug.

5.5 802.1x

Click on the **802.1x** link on the navigation bar. In this section, you will be able to modify the 802.1x Authenticator.



802.1x Authenticator

Supplicants...

Edit 802.1x Authenticator

View advanced attributes...

Options

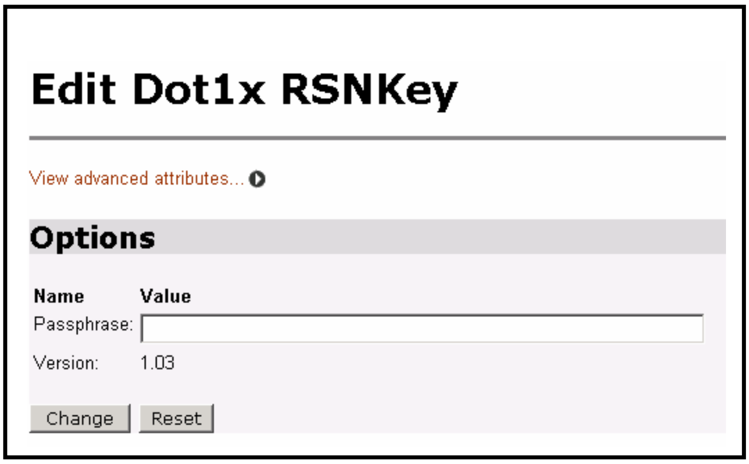
Name	Value
Auth Server:	Local
Auth Control Enabled:	false
Identity String:	GlobespanVirata Wireless Hotspot
Rekey Timeout:	600
Version:	2.01

- Click on the **Supplicants** link to view a list of 802.1x supplicants.
- **Auth Server**: Select an authentication server from the drop-down list. Options available are **None**, **Local**, or **RADIUS**. Settings should be **Local** when no external authentication is used with WPA. In this case, authentication passphrase should be configured in the WPA configuration link.
- **Auth Control Enabled**: Select true or false from the drop-down list in order to enable/disable authentication control.
- **Identity String**: Enter the identity string for the 802.1x authentication server.
- **Rekey Timeout**: Enter a time out period for the key.

- **Key Transmission Enabled**: Select true or false from the drop-down list in order to enable/disable key transmission.
- Click on the **Change** button to confirm the changes.

5.6 WPA

Click on the **WPA** link on the navigation bar. WPA stands for "Wi-Fi Protected Access".



Edit Dot1x RSNKey

View advanced attributes...

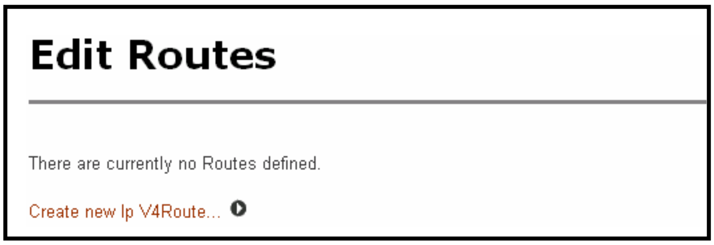
Options

Name	Value
Passphrase:	
Version:	1.03

- Enter the Passphrase and Click on the **Change** button.

5.7 *Routing Table*

- Click on the **Routing Table** link in the navigation bar. This page displays a table of the defined routes. Click on the **Create new IP V4Route**, to add an IP route to the table.

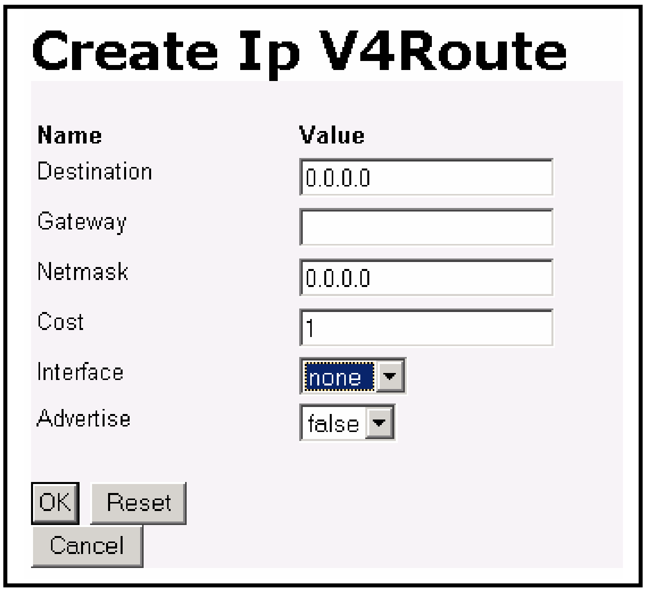


Edit Routes

There are currently no Routes defined.

Create new Ip V4Route...

- In order to create an routing table entry the following fields need to be filled in:
  - **Destination:** Enter the destination of the router.
  - **Gateway:** Enter the IP address of the gateway.
  - **Netmask:** Enter the subnet mask.
  - **Cost:** Enter the cost (number of hops).
  - **Interface:** Enter an interface name.
  - **Advertise:** Select true/false from the drop down list, if you would like the router to display itself.
- Click on the **OK** button.

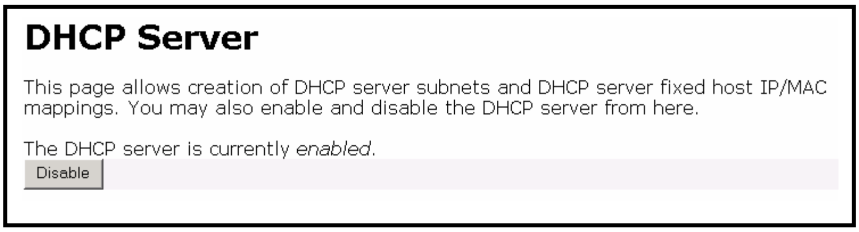


Create Ip V4Route

Name	Value
Destination	0.0.0.0
Gateway	
Netmask	0.0.0.0
Cost	1
Interface	none
Advertise	false

5.8 DHCP Server

- This device can be setup to perform the service of the DHCP Server and enables the data connection between multiple PCs by configuring IP address ranges and lease times.
- Click on the **DHCP Server** link in navigation bar. You will then see the following screen.



DHCP Server

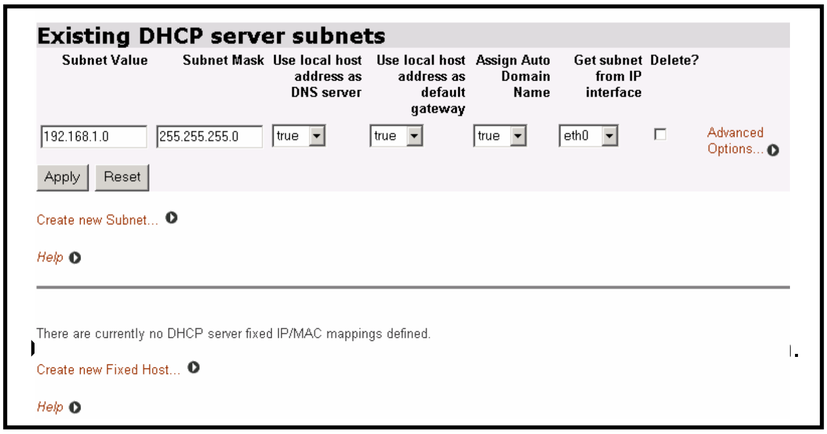
This page allows creation of DHCP server subnets and DHCP server fixed host IP/MAC mappings. You may also enable and disable the DHCP server from here.

The DHCP server is currently *enabled*.

- **Disable:** Click on the **Disable** button to disable the DHCP Server.

Existing DHCP Server Subnets

Scroll down to the Existing DHCP Server Subnets section. You will then see the following information.



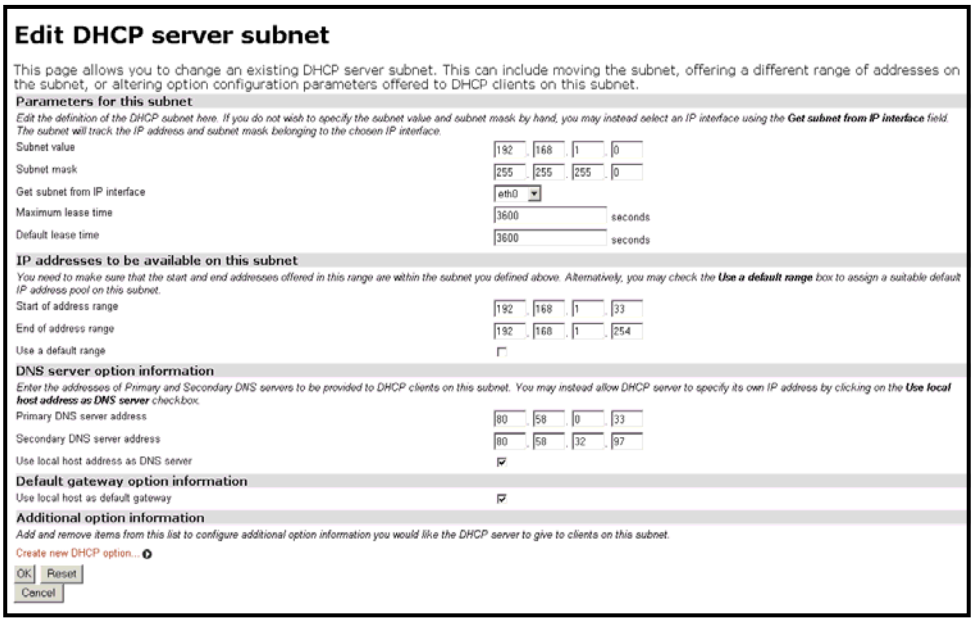
Existing DHCP server subnets

Subnet Value	Subnet Mask	Use local host address as DNS server	Use local host address as default gateway	Assign Auto Domain Name	Get subnet from IP interface	Delete?	
192.168.1.0	255.255.255.0	true	true	true	eth0	□	Advanced Options...

There are currently no DHCP server fixed IP/MAC mappings defined.

- **Subnet Value / Subnet Mask:** These are the base values for your new DHCP server subnet. All addresses offered by the DHCP server have to be located on a particular subnet. Also, if you wish to define some fixed IP/MAC mappings, each fixed IP address must have a corresponding subnet. You do not need to fill in this value if you use the **Get subnet from IP interface** option.

- **Use local host address as DNS server:** Select **true** or **false** from the drop-down list. If enabled, then the local IP address will be passed to DHCP clients who request a DNS server address. For this facility to be useful, you should have the DNS relay configured to be active, which can then forward DNS queries appropriately. In order to configure DNS Relay refer to section **4.5.13 DNS Relay**.
- **Use local host address as default gateway:** Select **true** or **false** from the drop-down list. If enabled, then the local IP address will be passed to DHCP clients who request a default gateway address. Also, any manually configured value for the DHCP default gateway option will be disregarded and overridden by this setting.
- **Get subnet from IP Interface:** Select an interface name from the drop-down list. This binds the appropriate IP address and subnet mask. This is especially useful when combined with the ability to use a default IP address range.
- **Advanced Options:** Click on this link to modify the existing settings.



Edit DHCP server subnet

This page allows you to change an existing DHCP server subnet. This can include moving the subnet, offering a different range of addresses on the subnet, or altering option configuration parameters offered to DHCP clients on this subnet.

Parameters for this subnet

Edit the definition of the DHCP subnet here. If you do not wish to specify the subnet value and subnet mask by hand, you may instead select an IP interface using the ***Get subnet from IP interface*** *field. The subnet will track the IP address and subnet mask belonging to the chosen IP interface.*

Subnet value	192 . 168 . 1 . 0
Subnet mask	255 . 255 . 255 . 0
Get subnet from IP interface	eth0
Maximum lease time	3600 seconds
Default lease time	3600 seconds

IP addresses to be available on this subnet

You need to make sure that the start and end addresses offered in this range are within the subnet you defined above. Alternatively, you may check the ***Use a default range*** *box to assign a suitable default IP address pool on this subnet.*

Start of address range	192 . 168 . 1 . 33
End of address range	192 . 168 . 1 . 254
Use a default range	□

DNS server option information

Enter the addresses of Primary and Secondary DNS servers to be provided to DHCP clients on this subnet. You may instead allow DHCP server to specify its own IP address by clicking on the ***Use local host address as DNS server*** *checkbox.*

Primary DNS server address	80 . 58 . 0 . 33
Secondary DNS server address	80 . 58 . 32 . 97
Use local host address as DNS server	☑

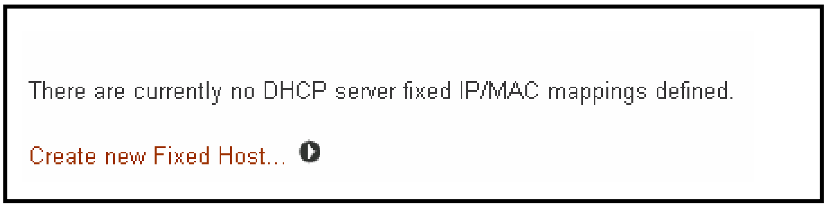
Default gateway option information

Use local host as default gateway	☑

Additional option information

Add and remove items from this list to configure additional option information you would like the DHCP server to give to clients on this subnet.

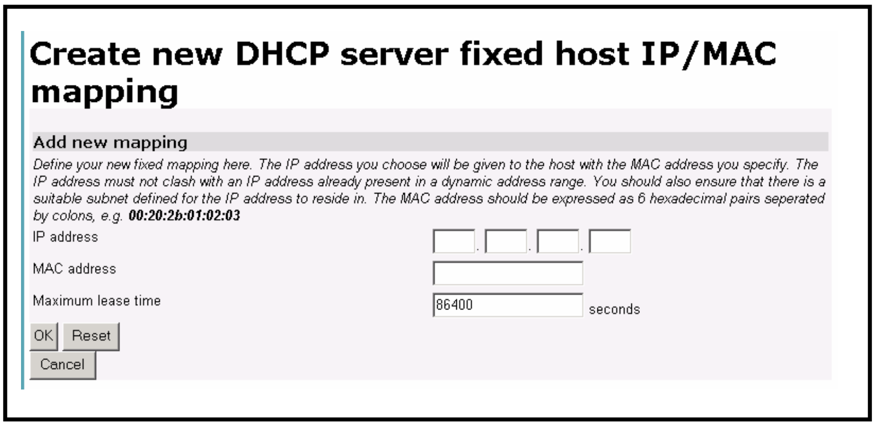
Create New Fixed Host



There are currently no DHCP server fixed IP/MAC mappings defined.

Create new Fixed Host...

- Click on the **Create new Fixed Host** link in order to define fixed IP/MAC pairs mappings so that the Router can assign the IP address corresponding to the MAC address of the DHCP clients.



Create new DHCP server fixed host IP/MAC mapping

Add new mapping

Define your new fixed mapping here. The IP address you choose will be given to the host with the MAC address you specify. The IP address must not clash with an IP address already present in a dynamic address range. You should also ensure that there is a suitable subnet defined for the IP address to reside in. The MAC address should be expressed as 6 hexadecimal pairs seperated by colons, e.g. ***00:20:2b:01:02:03***

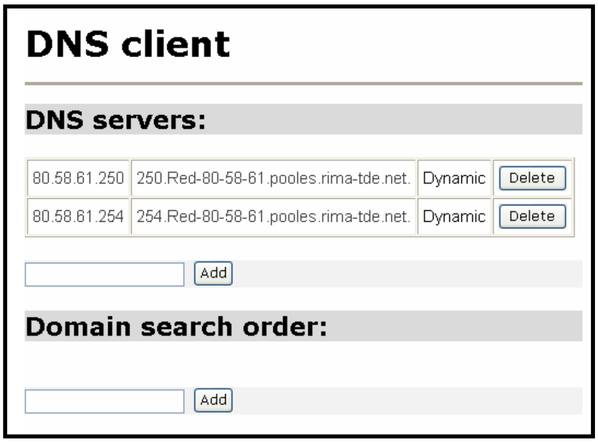
IP address	. . .
MAC address	
Maximum lease time	86400 seconds

Define your new DHCP fixed host here. The IP address you choose will be given to the host with the MAC address you specify. The IP address must not clash with an IP address already present in a dynamic address range. The MAC address should be expressed as 6 hexadecimal pairs separated by colons, e.g. **00:20:2b:01:02:03**. Then, click **OK** with the new setting.

- **Maximum lease time:** Enter a value for a maximum number of seconds a client can lease and IP address.

5.9 *DNS Client*

Click on the **DNS Client** link on the navigation bar. This section displays a list of DNS server addresses, and allows you to add DNS server IP addresses.



DNS client

DNS servers:

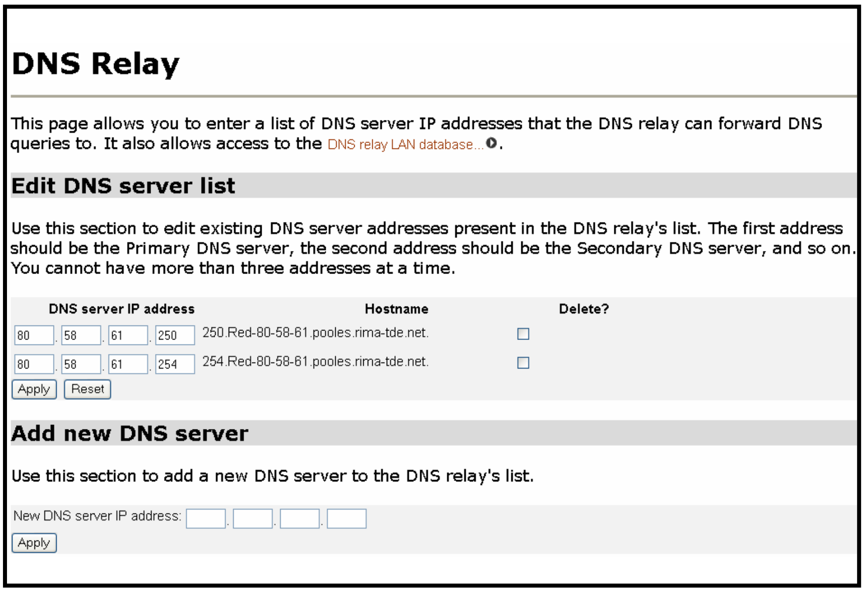
80.58.61.250	250.Red-80-58-61.pooles.rima-tde.net.	Dynamic	Delete
80.58.61.254	254.Red-80-58-61.pooles.rima-tde.net.	Dynamic	Delete

Domain search order:

- **Add:** Enter an IP address of the DNS server, and then click on the **Add** button.

5.10 DNS Relay

- Click on the **DNS Relay** link in the navigation bar. You may enable or disable DNS Relay.



DNS Relay

This page allows you to enter a list of DNS server IP addresses that the DNS relay can forward DNS queries to. It also allows access to the DNS relay LAN database... .

Edit DNS server list

Use this section to edit existing DNS server addresses present in the DNS relay's list. The first address should be the Primary DNS server, the second address should be the Secondary DNS server, and so on. You cannot have more than three addresses at a time.

DNS server IP address	Hostname	Delete?
80 . 58 . 61 . 250	250.Red-80-58-61.pooles.rima-tde.net.	□
80 . 58 . 61 . 254	254.Red-80-58-61.pooles.rima-tde.net.	□

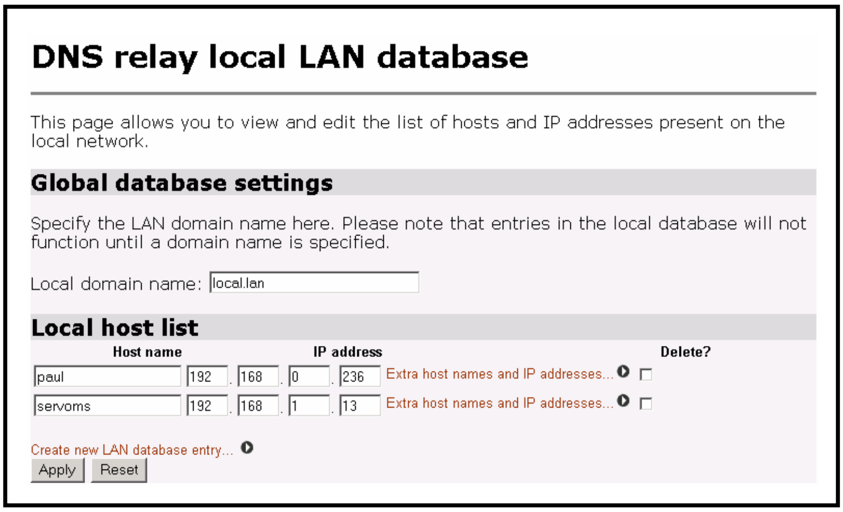
Add new DNS server

Use this section to add a new DNS server to the DNS relay's list.

New DNS server IP address: . . .

- **Edit DNS server list:** displays existing DNS server addresses present in the DNS relay's list. The first address should be the Primary DNS server, the second address should be the Secondary DNS server, and so on. You cannot have more than three addresses at a time.
- **Delete:** Click on the **Delete** button to delete an existing DNS server address.
- **Add new DNS server:** Enter the IP address of the DNS Server and then click on the **Apply** button. The IP address will then be added to the DNS server list.

- Click on the **DNS relay LAN database** to view and edit the list of hosts and IP addresses present on the local network and to specify the LAN domain name.



DNS relay local LAN database

This page allows you to view and edit the list of hosts and IP addresses present on the local network.

Global database settings

Specify the LAN domain name here. Please note that entries in the local database will not function until a domain name is specified.

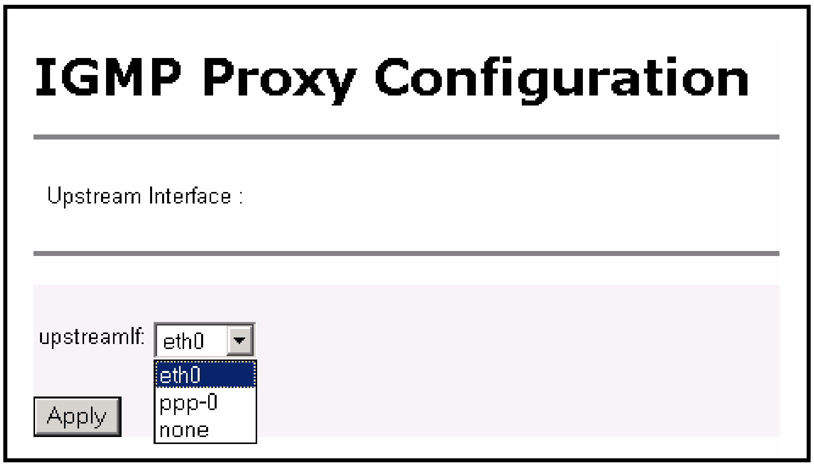
Local domain name: local.lan

Local host list

Host name	IP address					Delete?
paul	192	168	0	236	Extra host names and IP addresses...	□
servoms	192	168	1	13	Extra host names and IP addresses...	□

5.11 IGMP Proxy

Click on the **IGMP Proxy** link on the navigation bar. On this page you will be able to select an Upstream interface for the IGMP proxy. Select and interface from the drop down list, and then click on the **Apply** button.



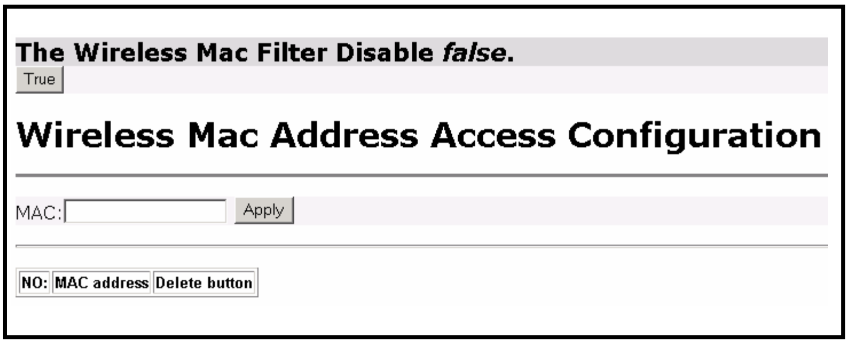
IGMP Proxy Configuration

Upstream Interface :

upstreamIf: eth0

5.12 Wireless Mac Filter

Click the Wireless Mac Filter link to fill in any wireless device Mac address which will have access to the Internet. Click the Apply button when you finish inputting the values.



The Wireless Mac Filter Disable *false*.

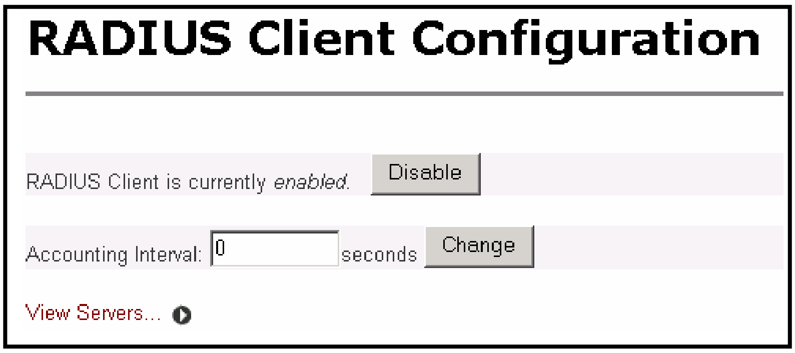
Wireless Mac Address Access Configuration

MAC:

NO:	MAC address	Delete button

5.13 RADIUS Client

Click on the **RADIUS Client** link on the navigation bar. In this section you can view and add the RADIUS servers which are used for client authentication and accounting.



RADIUS Client Configuration

RADIUS Client is currently *enabled*.

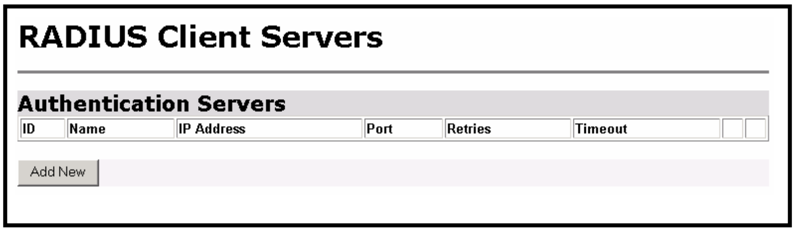
Accounting Interval: 0 seconds

- **RADIUS Client:** By default, the RADIUS Client is disabled. Click on the Enable button to enable the RADIUS server.
- **Accounting Interval:** Enter a value (number of seconds) for the RADIUS accounting server to refresh, and then click on the **Change** button.

Click on the **View Servers** link to configure the Authentication and Accounting server settings. You will then see the following screen.

Authentication Servers

This page displays the list of RADIUS Authentication Servers.

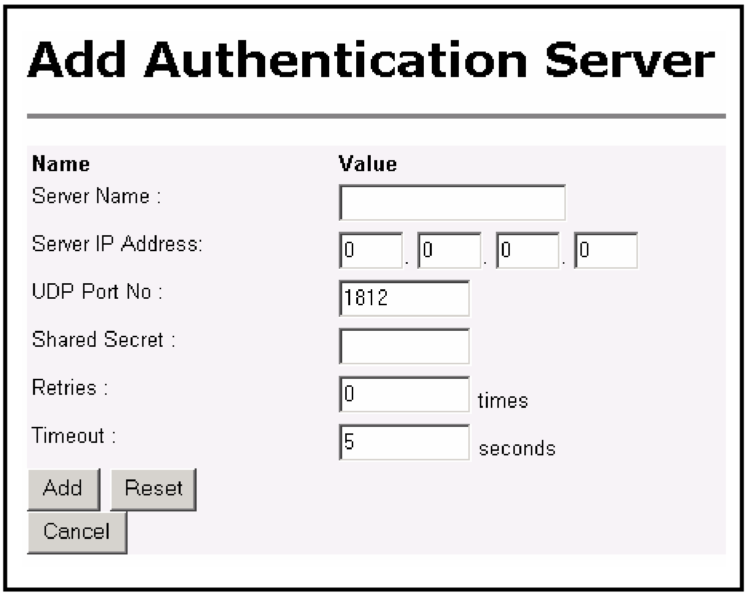


RADIUS Client Servers

Authentication Servers

ID	Name	IP Address	Port	Retries	Timeout		

Click on the **Add New** button to add a new Authentication Server to this Router. You will then see the following screen.

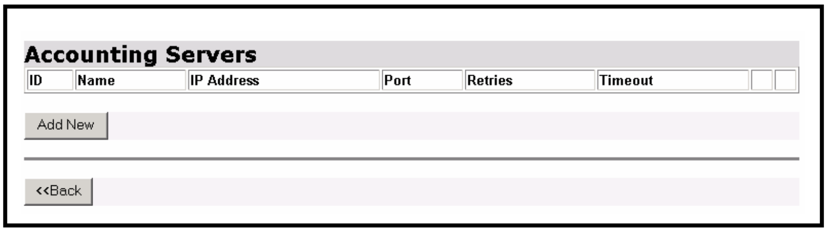


Add Authentication Server

Name	Value
Server Name :	
Server IP Address:	0 . 0 . 0 . 0
UDP Port No :	1812
Shared Secret :	
Retries :	0 times
Timeout :	5 seconds

- **Server Name:** Enter a name for the Authentication Server.
- **Server IP Address:** Enter the IP address of the Authentication Server.
- **UDP Port No:** Enter another UDP port number or leave it as the default.
- **Shared Secret:** Enter the shared secret.
- **Retries:** Enter the number of trials (failed attempts) before the Router stops authenticating.
- **Timeout:** Enter a time out value (seconds) before the Router stops authenticating.
- Click on the **Add** button.

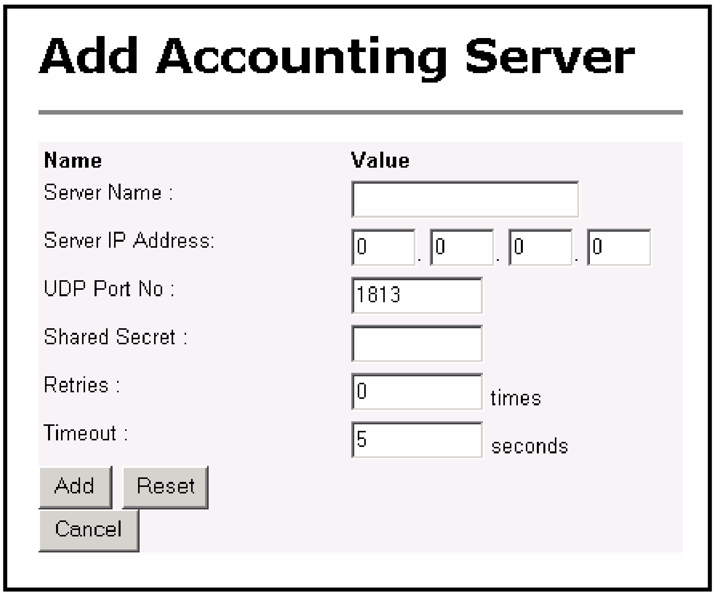
Account Servers



Accounting Servers

ID	Name	IP Address	Port	Retries	Timeout		

Click on the **Add New** button to add a new Accounting Server to this Router. You will then see the following screen.

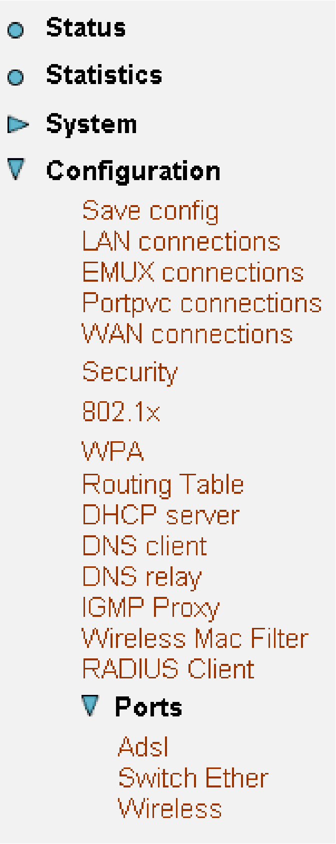


Add Accounting Server

Name	Value
Server Name :	
Server IP Address:	0 . 0 . 0 . 0
UDP Port No :	1813
Shared Secret :	
Retries :	0 times
Timeout :	5 seconds

- **Server Name:** Enter a name for the Accounting Server.
- **Server IP Address:** Enter the IP address of the Accounting Server.
- **UDP Port No:** Enter another UDP port number or leave it as the default.
- **Shared Secret:** Enter the shared secret.
- **Retries:** Enter the number of trials (failed attempts) before the Router stops accounting.
- **Timeout:** Enter a time out value (seconds) before the Router stops accounting.
- Click on the **Add** button.

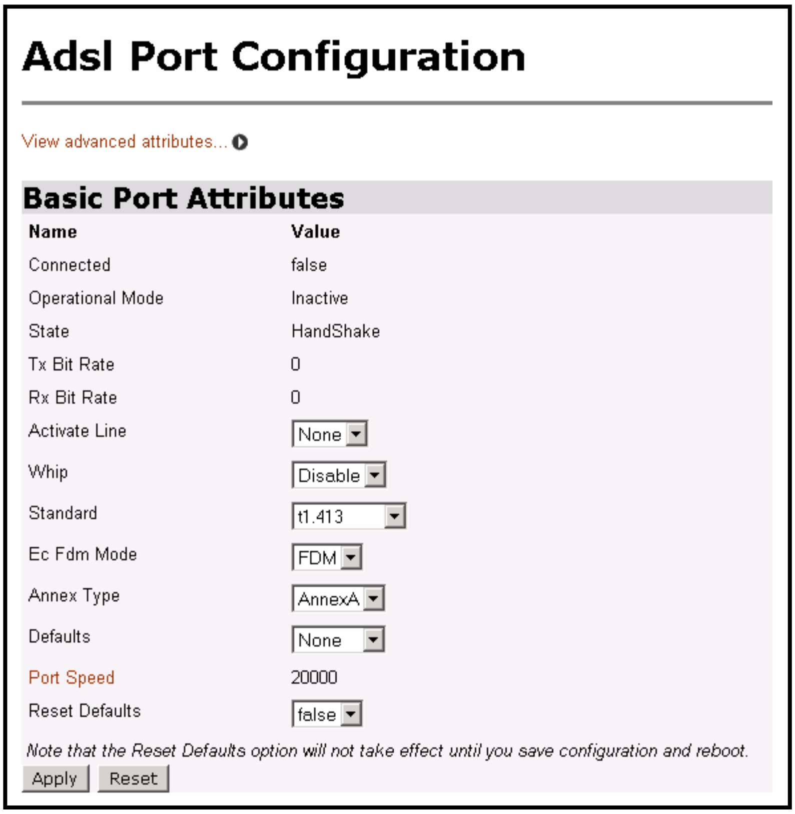
6. Ports



The **Ports** section includes **ADSL**, **Switch Ether**, and **Wireless** links. Each link is described in detail below.

6.1 *ADSL*

Click on the **ADSL** link on the navigation bar. This page displays a table of the default ADSL settings for the basic port attributes. You may change the default settings in order to accommodate your needs, click on the **Apply** button when completed.



Adsl Port Configuration

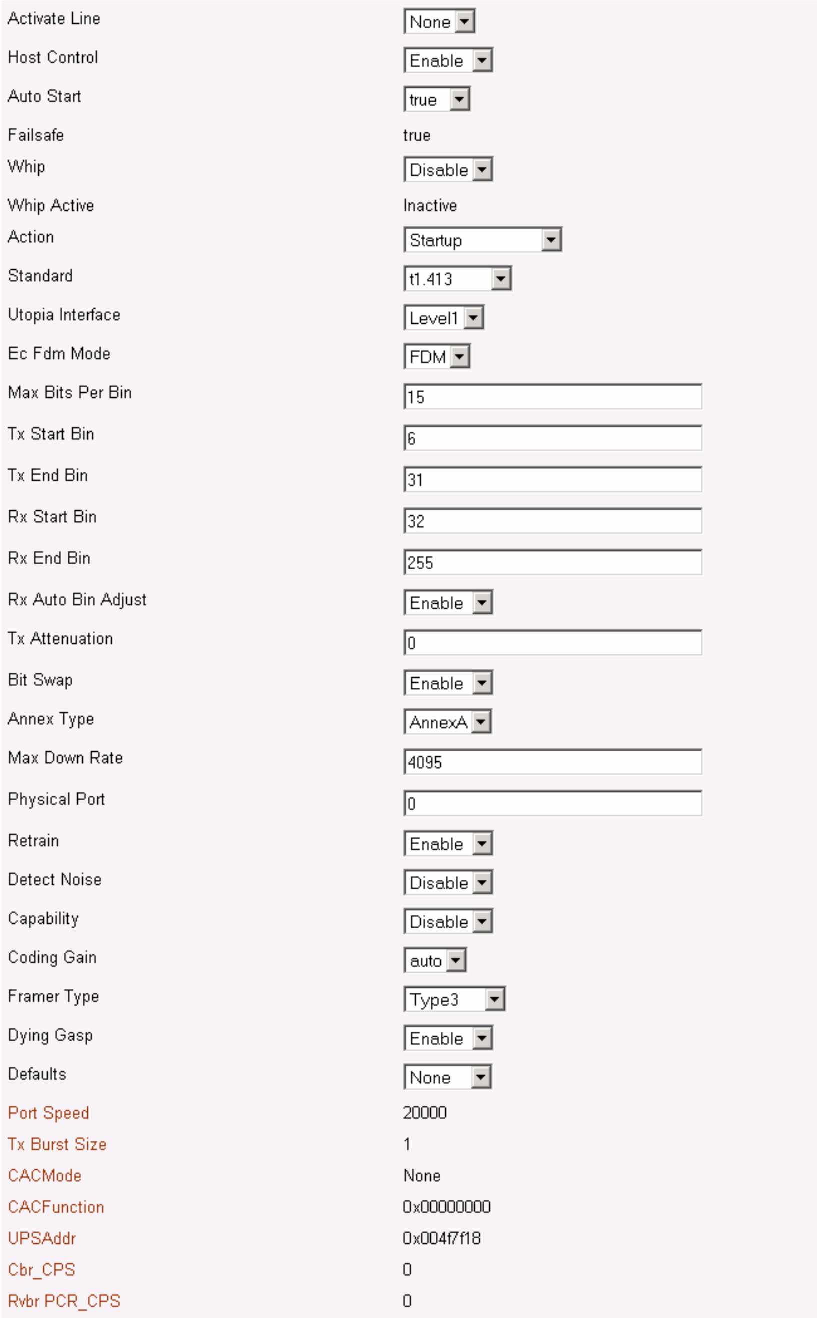
View advanced attributes...

Basic Port Attributes

Name	Value
Connected	false
Operational Mode	Inactive
State	HandShake
Tx Bit Rate	0
Rx Bit Rate	0
Activate Line	None
Whip	Disable
Standard	t1.413
Ec Fdm Mode	FDM
Annex Type	AnnexA
Defaults	None
Port Speed	20000
Reset Defaults	false

Note that the Reset Defaults option will not take effect until you save configuration and reboot.

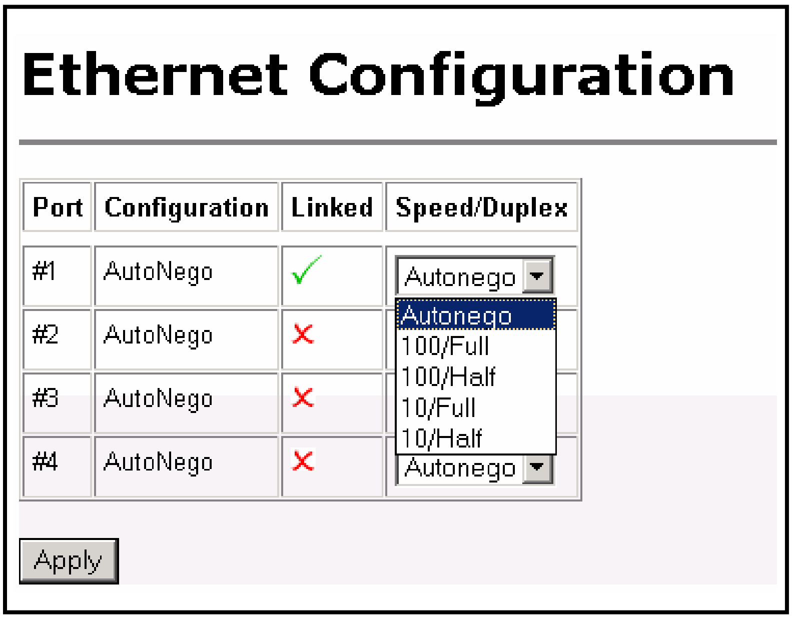
- **Activate Line:** Select **None**, **Abort**, or **Start** from the drop-down list.
- **Whip:** Select **Inactive**, **Serial**, or **TCP** from the drop-down list.
- **Standard:** Select an ADSL standard from the drop-down list. Options available are: **G.dmt, G.Span, t1.413, g.lite, Multimode, ALCTL_14, ALCTL,** and **ADI**. The default setting is **Multimode**.
- **Ec Fdm Mode:** Select EC or FDM from the drop-down list.
- **Annex Type:** Select an Annex A or G.Span from the drop-down list.
- **Defaults:** Select an Annex A or G.Span from the drop-down list.
- **Reset Defaults:** Select **True** or **False** from the drop-down list.
  - **Note:** The **Reset Defaults** option will not take effect until the configuration has been saved and the Router has been restarted.
- Click on the **Apply** button to confirm the changes.
- Click on the **View Advanced Attributes** link at the top of the page to view more detailed settings about the ADSL port.



Activate Line	None
Host Control	Enable
Auto Start	true
Failsafe	true
Whip	Disable
Whip Active	Inactive
Action	Startup
Standard	t1.413
Utopia Interface	Level1
Ec Fdm Mode	FDM
Max Bits Per Bin	15
Tx Start Bin	6
Tx End Bin	31
Rx Start Bin	32
Rx End Bin	255
Rx Auto Bin Adjust	Enable
Tx Attenuation	0
Bit Swap	Enable
Annex Type	AnnexA
Max Down Rate	4095
Physical Port	0
Retrain	Enable
Detect Noise	Disable
Capability	Disable
Coding Gain	auto
Framer Type	Type3
Dying Gasp	Enable
Defaults	None
Port Speed	20000
Tx Burst Size	1
CACMode	None
CACFunction	0x00000000
UPSAddr	0x004f7f18
Cbr_CPS	0
Rvbr PCR_CPS	0

6.2 *Switch Ether*

- Click on the Switch **Ether** link on the navigation bar. This page displays the Ethernet port configuration. Included are the configuration type, link, and speed/duplex.
- You may select a speed/duplex rate from the drop down list. Click on the **Apply** button when completed.

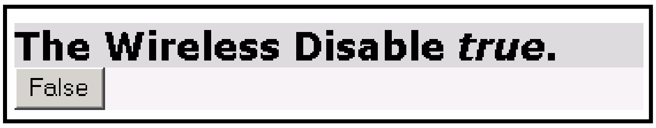


Ethernet Configuration

Port	Configuration	Linked	Speed/Duplex
#1	AutoNego	✓	Autonego
#2	AutoNego	✗	
#3	AutoNego	✗	
#4	AutoNego	✗	Autonego

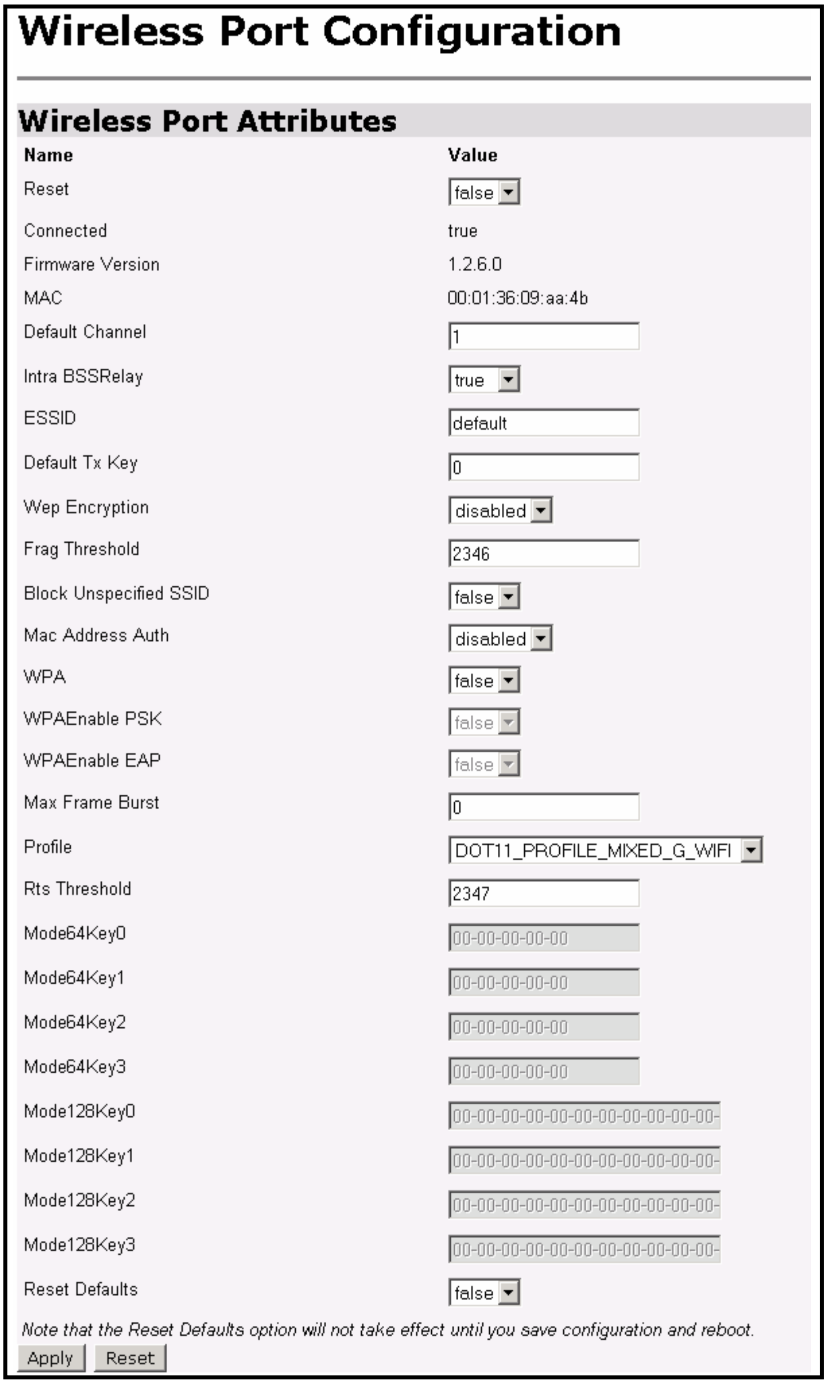
6.3 Wireless

- Click on the **Wireless** link on the navigation bar. This page displays the current Wireless settings and allows you to configure the Wireless card.
- The Wireless Port is disabled by default.
- Click on **False** to enable the Wireless Port.



The Wireless Disable *true*.

- the Wireless Port Configuration windows is displayed.
- **Default Channel:** Enter a default channel or leave this value at 1.
- **ESSID:** Enter the ESSID for the wireless network here. The SSID is a unique name shared among all nodes in your wireless network. The SSID must be identical for all nodes in the network, and is case-sensitive.
- **Wep Encryption:** Select the WEP (Wired Equivalent Privacy) from the drop-down list. Options available are: disabled, 64-bit, and 128-bit.
- **Frag Threshold:** Enter a fragmentation threshold value or leave it as the default.
- **WPA:** Select **true** from the drop-down list to enable WPA (Wi-Fi Protected Access).
- **WPA Enable PSK:** Select **true** from the drop-down list to enable PSK (Pre-shared key) on WPA.
- **WPA Enable EAP:** Select **true** from the drop-down list to enable EAP (Extended Authentication Protocol) on WPA.
- **RTS Threshold:** Enter a RTS threshold value or leave it as the default.
- **Key 0 – 3**: Depending on the encryption method selected above (64-bit or 128-bit) enter the WEP key into the appropriate text box.
- **Reset Defaults:** Select **True** or **False** from the drop-down list.
- **Note:** The **Reset Defaults** option will not take effect until the configuration has been saved and the Router has been restarted.
- Click on the **Apply** button to confirm the changes.



Wireless Port Configuration

Wireless Port Attributes

Name	Value
Reset	false
Connected	true
Firmware Version	1.2.6.0
MAC	00:01:36:09:aa:4b
Default Channel	1
Intra BSSRelay	true
ESSID	default
Default Tx Key	0
Wep Encryption	disabled
Frag Threshold	2346
Block Unspecified SSID	false
Mac Address Auth	disabled
WPA	false
WPAEnable PSK	false
WPAEnable EAP	false
Max Frame Burst	0
Profile	DOT11_PROFILE_MIXED_G_WIFI
Rts Threshold	2347
Mode64Key0	00-00-00-00-00
Mode64Key1	00-00-00-00-00
Mode64Key2	00-00-00-00-00
Mode64Key3	00-00-00-00-00
Mode128Key0	00-00-00-00-00-00-00-00-00-00-00-00-
Mode128Key1	00-00-00-00-00-00-00-00-00-00-00-00-
Mode128Key2	00-00-00-00-00-00-00-00-00-00-00-00-
Mode128Key3	00-00-00-00-00-00-00-00-00-00-00-00-
Reset Defaults	false

Note that the Reset Defaults option will not take effect until you save configuration and reboot.

Appendix A – Specifications

A1. Hardware Specifications

- Local Interface
  - Four 10/100BaseT Ethernet ports, IEEE 802.3u
  - Connector: RJ-45
  - Integrated 802.11g WLAN Access Point
- WAN ADSL Line Interface
  - Compliance: ITU G.992.1, G.992.2, G.992.3, G992.4, G.994.5 (X7768+ only) and ANSI T1.413 Issue 2
  - Line Impedance: 100 Ω
  - Connection Loops: One Pair (2-wire)
  - Connector: RJ-11
- Indicators
  - PWR -- Green LED, "On" while the power supply is properly connected.
  - WLAN -- Green LED, "Blink" while training with DSLAM and "On" when ADSL link is ready.
  - LAN -- Green LED, "On" while indicating either Ethernet port connect.
  - WAN -- Green LED, "Blink" while training with DSLAM and "On" when ADSL link is ready.
  - ALM -- Red LED, "Blink" while booting up and "On" when there is an error. Continuous "On" indicates internal error.
- OAM&P
  - Telnet or Web management via Ethernet
  - Remote: Telnet or Web Management
- Environment
  - Operation Temperature: 0°C ~ 45°C
  - Operation Humidity: 5% ~ 95%
  - Storage Temperature: -20 ~ 85°C
  - Storage Humidity: 5% ~ 95%
- Power
  - AC Adapter: Input 110/220VAC, 50/60Hz; Output 15VAC 1A
  - Power Consumption: Less than 11 Watts
- Certificates
  - CE, CB, Wi-Fi

A2. Software Specifications

- ATM
  - ATM Cells over ADSL, AAL5
  - Bridge mode: Supports 8 PVCs
  - Router mode: Supports 5 PVCs
  - Supports UBR, CBR, nrt-VBR and rt-VBR
  - ATM Forum UNI 3.0, UNI 3.1, UNI 4.0
  - ILMI 4.0
  - PPP over ATM PVC (RFC 2364)
- Bridging
  - Transparent Bridging (IEEE 802.1d)
  - RFC2684 (RFC1483) Bridged
  - Spanning Tree Protocol (IEEE 802.1d)
  - IP and PPPoE packet filtering
  - IP Multicast IGMP Proxy
- Routing
  - IP routing, RIP1, RIP2, OSPF and static routing
  - PPPoE, IP, and PPP over ATM
  - PAP and CHAP
  - RFC2684 (RFC1483) Routed
  - NAT/PAT with extensive ALG support
  - DNS relay
  - Multihoming (IP Aliasing)
- Configuration and Network Management Features
  - DHCP client and server for IP management
  - Telnet for local or remote management
  - TFTP, HTTP for firmware upgrade and configuration
  - Web-based configuration and management
  - SNMP v1, v2, and v3 Agent
  - SNMP MIB II
  - DSL MIB
  - ATM MIB
  - WLAN MIB

Appendix B – Warranties

B1. Product Warranty

XAVi Technologies warrants that the ADSL unit will be free from defects in material and workmanship for a period of twelve (12) months from the date of shipment.

XAVi Technologies shall incur no liability under this warranty if

- The allegedly defective goods are not returned prepaid to XAVi Technologies within thirty (30) days of the discovery of the alleged defect and in accordance with XAVi Technologies' repair procedures; or

- XAVi Technologies' tests disclose that the alleged defect is not due to defects in material or workmanship.

XAVi Technologies' liability shall be limited to either repair or replacement of the defective goods, at XAVi Technologies' option.

XAVi Technologies MARKS NO EXPRESS OR IMPLIED WARRANTIES REGARDING THE QUALITY, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE BEYOND THOSE THAT APPEAR IN THE APPLICABLE USER'S DOCUMETATION. XAVi SHALL NOT BE RESPONSIBLE FOR CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGE, INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS OR DAMAGES TO BUSINESS OR BUSINESS RELATIONS. THIS WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES.

B2. Warranty Repair

1. During the first three (3) months of ownership, XAVi Technologies will repair or replace a defective product covered under warranty within twenty-four (24) hours of receipt of the product. During the fourth (4th) through twelfth (12th) months of ownership, XAVi Technologies will repair or replace a defective product covered under warranty within ten (10) days of receipt of the product. The warranty period for the replaced products shall be ninety (90) days or the remainder of the warranty period of the original unit, whichever is greater. XAVi Technologies will ship surface freight. Expedited freight is at customer's expense.
2. The customer must return the defective product to XAVi Technologies within fourteen (14) days after the request for replacement. If the defective product is not returned within this time period, XAVi Technologies will bill the customer for the product at list price.

B3. Out-of-Warranty Repair

XAVi Technologies will either repair or, at its option, replace a defective product not covered under warranty within ten (10) working days of its receipt. Repair charges are available from the Repair Facility upon request. The warranty on a serviced product is thirty (30) days measured from date of service. Out-of-warranty repair charges are based upon the prices in effect at the time of return.

Appendix C – Regulations

C1. FCC Part 15 Notice

Warning: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 to the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment. This equipment generates, used, and can radiate radio frequency energy, and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is unlikely to cause harmful interference. But if it does, the user will be required to correct the interference at his or her own expense. The authority to operate this equipment is conditioned by the requirement that no modifications will be made to the equipment unless XAVi expressly approves the changes or modifications.

C2. IC CS-03 Notice

The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational, and safety requirements as prescribed in appropriate Terminal Equipment Technical Requirements document(s). The Department does not guarantee that the equipment will operate to the user's satisfaction.

Before installing this equipment, users should make sure that it is permissible to be connected to the facilities of the local telecommunications company. An acceptable method of connection must be used to install the equipment. The customer should be aware that compliance with the above conditions might not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Warning: Users should not attempt to make such connections themselves, but should contact the appropriate electrical inspection authority or an electrician.

C3. UL Safety Regulations

- Disconnect TNV circuit connector or before removing cover or equivalent.
- Disconnect TNV circuit connector(s) before disconnecting power.
- Do not use this product near water for example, near a bathtub, washbowl, and kitchen sink or laundry tub, in a wet basement, or near a swimming pool.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightening.
- Do not use the telephone to report a gas leak in the vicinity of the leak.
- Use only the power cord batteries indicated in this manual. Do not dispose of batteries in a fire, as they may explode. Check with local codes for possible special disposal instructions.

No. 26 AWG Telephone Line Cord shall either be provided with the equipment or shall be described in the safety instruction. If fuse (F1) is not present, see the caution statement listed below:

CAUTION: To reduce the risk of fire, use only No. 26 AWG or larger UL Listed or CSA Certified Telecommunication Line Cord.

Contact Information

You can help us serve you better by sending us your comments and feedback. Listed below are the addresses, telephone and fax numbers of our offices. You can also visit us on the World Wide Web at www.xavi.com.tw for more information. We look forward to hearing from you!

World Headquarter
XAVi Technologies Corporation
9F, No. 129 Hsing Te Road, Sanchung City
Taipei Hsien 241, Taiwan
Tel: +886-2-2995-7953 Fax: +886-2-2995-7954

USA Branch Office
1463 Madera Road, N. Suite 182 Simi Valley
CA 93065, USA
Tel: +805-578-9774

European Branch Office
Papenreye 27, 22453 Hamburg
Germany
Tel: +49-40-589510-0 Fax: +49-40-589510-29

China Agency
Room 401, Floor 4, #608 ZhaoJiaBang Road
Shanghai, 20031
Tel: +86-21-6431-8800 Fax: +86-21-6431-7885

Issued Date: April 11, 2004