1752 and 1754 SHDSL Routers

User’s Guide

Document Number 1752-A2-GB20-00

June 2005

Notice

This publication is protected by federal copyright law. No part of this publication may be copied or distributed, transmitted, transcribed, stored in a retrieval system, or translated into any human or computer language in any form or by any means, electronic, mechanical, magnetic, manual or otherwise, or disclosed to third parties without the express written permission of Paradyne Corporation, 8545 126th Ave. N., Largo, FL 33773.

Paradyne Corporation makes no representation or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for a particular purpose. Further, Paradyne Corporation reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation of Paradyne Corporation to notify any person of such revision or changes.

Changes and enhancements to the product and to the information herein will be documented and issued as a new release to this manual.

Warranty, Sales, Service, and Training Information

Contact your local sales representative, service representative, or distributor directly for any help needed. For additional information concerning warranty, sales, service, repair, installation, documentation, training, distributor locations, or Paradyne worldwide office locations, use one of the following methods:

- **Internet:** Visit the Paradyne World Wide Web site at **www.paradyne.com**. (Be sure to register your warranty at **www.paradyne.com/warranty**.)
- **Telephone:** Call our automated system to receive current information by fax or to speak with a company representative.
  - Within the U.S.A., call 1-800-870-2221
  - Outside the U.S.A., call 1-727-530-2340

Document Feedback

We welcome your comments and suggestions about this document. Please mail them to Technical Publications, Paradyne Corporation, 8545 126th Ave. N., Largo, FL 33773, or send e-mail to **userdoc@paradyne.com**. Include the number and title of this document in your correspondence. Please include your name and phone number if you are willing to provide additional clarification.

Trademarks

Acculink, ADSL/R, Bitstorm, Comsphere, DSL the Easy Way, ETC, Etherloop, FrameSaver, GranDSLAM, GrandVIEW, Hotwire, the Hotwire logo, Jetstream, MVL, NextEDGE, Net to Net Technologies, OpenLane, Paradyne, the Paradyne logo, Paradyne Credit Corp., the Paradyne Credit Corp. logo, Performance Wizard, ReachDSL, StormPort, and TruePut are registered trademarks of Paradyne Corporation. Connect to Success, Hotwire Connected, iMarc, JetFusion, JetVision, MicroBurst, PacketSurfer, Quick Channel, Reverse Gateway, Spectrum Manager, and StormTracker are trademarks of Paradyne Corporation. All other products and services mentioned herein are the trademarks, service marks, registered trademarks, or registered service marks of their respective owners.

⚠ Important Safety Instructions

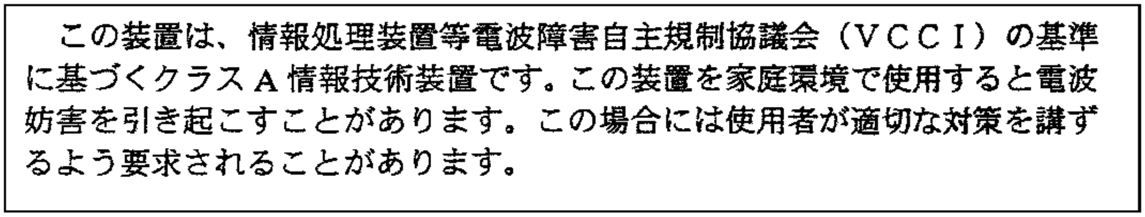
1. Read and follow all warning notices and instructions marked on the product or included in the manual.
2. Slots and openings in the cabinet are provided for ventilation. To ensure reliable operation of the product and to protect it from overheating, these slots and openings must not be blocked or covered.
3. Do not allow anything to rest on the power cord and do not locate the product where persons will walk on the power cord.
4. Do not attempt to service this product yourself, as opening or removing covers may expose you to dangerous high voltage points or other risks. Refer all servicing to qualified service personnel.
5. When installed in the final configuration, the product must comply with the applicable Safety Standards and regulatory requirements of the country in which it is installed. If necessary, consult with the appropriate regulatory agencies and inspection authorities to ensure compliance.
6. A rare phenomenon can create a voltage potential between the earth grounds of two or more buildings. If products installed in separate buildings are **interconnecte**d, the voltage potential may cause a hazardous condition. Consult a qualified electrical consultant to determine whether or not this phenomenon exists and, if necessary, implement corrective action prior to interconnecting the products.
7. Input power to this product must be provided by one of the following: (1) a UL Listed/CSA certified power source with a Class 2 or Limited Power Source (LPS) output for use in North America, or (2) a certified transformer, with a Safety Extra Low Voltage (SELV) output having a maximum of 240 VA available, for use in the country of installation.
8. General purpose cables are used with this product for connection to the network. Special cables, which may be required by the regulatory inspection authority for the installation site, are the responsibility of the customer. Use a UL Listed, CSA certified, minimum No. 26 AWG line cord for connection to the Digital Subscriber Line (DSL) network.
9. In addition, since the equipment is to be used with telecommunications circuits, take the following precautions:
   - Never install telephone wiring during a lightning storm.
   - Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
   - Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
   - Use caution when installing or modifying telephone lines.
   - Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
   - Do not use the telephone to report a gas leak in the vicinity of the leak.

CE Marking

When the product is marked with the CE mark on the equipment label, a supporting Declaration of Conformity may be downloaded from the Paradyne World Wide Web site at **www.paradyne.com**. Select *Library → Technical Manuals → CE Declarations of Conformity*.

Japan

Class A ITE



この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

This is a Class A product based on the standard of the Voluntary Control Council for interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

EMI Notices

United States – EMI Notice

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, 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 likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

The authority to operate this equipment is conditioned by the requirements that no modifications will be made to the equipment unless the changes or modifications are expressly approved by the responsible party.

If the equipment includes a ferrite choke or chokes, they must be installed as described in the installation instructions.

Canada – EMI Notice

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

ACTA Customer Information

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the bottom of the network extender is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXXX. If requested, this number must be provided to the telephone company.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. See installation instructions for details.

If the network extender causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment, please contact your local sales representative, service representative, or distributor directly for any help needed. For additional information concerning warranty, sales, service, repair, installation, documentation, training, distributor locations, or Paradyne worldwide office locations, use one of the following methods:

- Internet: Visit the Paradyne World Wide Web site at www.paradyne.com. (Be sure to register your warranty at www.paradyne.com/warranty.)
- Telephone: Call our automated system to receive current information by fax or to speak with a company representative.

  — Within the U.S.A., call 1-800-870-2221
  — Outside the U.S.A., call 1-727-530-2340

If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

The customer may make no repairs to the equipment.

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

Notice to Users of the Canadian Telephone Network

NOTICE: This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation IC before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

NOTICE: The Ringer Equivalence Number (REN) for this terminal equipment is labeled on the equipment. The REN assigned to each terminal equipment provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed five.

If your equipment is in need of repair, contact your local sales representative, service representative, or distributor directly.

Contents

Chapter 1 – Introduction

Thank you for choosing a 1750 Series SHDSL router as your broadband access solution. This manual is designed to help you with the setup and configuration of your product.

1750 Series Overview

The 1750 Series G.SHDSL.bis standalone routers take advantage of the latest G.SHDSL.bis technology— Extended Rate Bonded SHDSL— to provide unprecedented possibilities for symmetric transmission.

Multi-pair bonding allows symmetric data rates up to 5.69 Mbps, 11.38 Mbps, or 22.76 Mbps over 2-wire, 4-wire, or 8-wire connections respectively.

Features

- **Rate and Reach Improvements**

  Symmetric transmission rate is up to 5704 kbps, 11408 kbps, 17112 kbps, and 22816 kbps over 2-wire, 4-wire, 6-wire, or 8-wire telephone lines respectively, over a distance as great as 12,000 ft.

- **CO and CPE Mode selectable**

  Selectable site mode provides point-to-point connectivity.

- **2-wire / 4-wire/ 8-wire M-Pair Mode selectable**

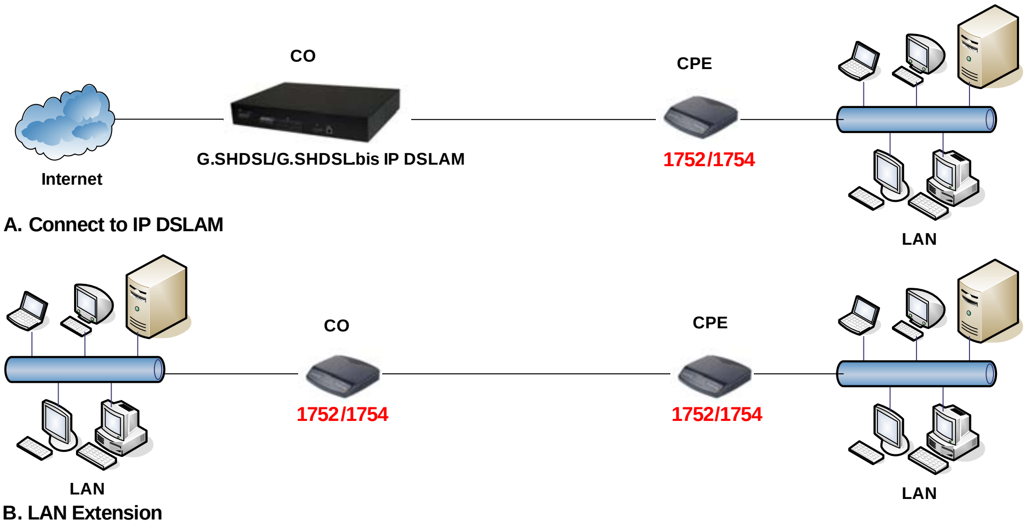
  Selectable wire pair mode offers flexible rate options.

- **Easy Management**

  The routers support both a web-based GUI and CLI-based management.

- **Backward Compatible to G.shdsl (G.991.2)**

Applications



A. Connect to IP DSLAM

B. LAN Extension

Specifications

Standards Compliance

- ✓ Auto load balancing with bonded pairs
- ✓ ITU-T G.991.2
- ✓ Supports Annex A, Annex B, Annex F, and Annex G
- ✓ Supports point-to-point configuration
- ✓ Transmission rate up to 5704 kbps on 2-wire
- ✓ Transmission rate up to 11408 kbps on 4-wire
- ✓ Transmission rate up to 17112 kbps on 6-wire
- ✓ Transmission rate up to 22816 kbps on 8-wire

Maintenance

- ✓ Firmware upgradeable via FTP, TFTP, or web interface
- ✓ Statistics on DSL link and data ports
- ✓ Supports ATM OAM F5 End to End and Segment loopbacks
- ✓ Supports Telnet
- ✓ System log

Management

- ✓ Access Control
- ✓ Attack Alert and log
- ✓ Command Line Interface (CLI)
- ✓ Denial of Service protection
- ✓ Firewall Security
- ✓ MIB-II (RFC 1213, RFC 1573)
- ✓ Packet Filter
- ✓ PAP and CHAP support

- ✓ Password protection
- ✓ Real time log
- ✓ Remote access management via telnet
- ✓ SNMPv1
- ✓ Stateful Packet Inspection (SPI)
- ✓ Web based GUI interface

Protocol

- ✓ DHCP client/server and DHCP relay functionality
- ✓ DMZ support
- ✓ IEEE 802.1Q VLAN
- ✓ IEEE802.1P Priority Output Queuing
- ✓ IEEE802.3u Fast Ethernet 100BaseT
- ✓ IP support: TCP, RIPv1, RIPv2, UDP, ICMP, ARP, RTP
- ✓ IPSec VPN Support
- ✓ MAC bridging(IEEE 802.3 and 802.1D)
- ✓ MAC Filtering
- ✓ NAT/PAT support
- ✓ PPPoE (RFC 2416)
- ✓ QoS support VBR-rt, VBR-nrt, CBR and UBR
- ✓ RFC 1483/2684 Bridged encapsulation (routing mode optional)
- ✓ Supports ATM over G.SHDSL.bis and G.SHDSL
- ✓ Supports 8 PVCs
- ✓ Supports IGMP Snooping
- ✓ Supports Port-based VLAN
- ✓ VPN pass-through IPSec and L2TP

LED

- ✓ LED indicator; power, DSL links, Alarm, Ethernet ports and CO/CPE mode

Hardware Interface

- ✓ 4 - 10/100BaseT auto-sensing RJ45
- ✓ 1 - Serial connector for local console access
- ✓ 1 - RJ11 for 2-pair bonding on the 1752
- ✓ 2 - RJ11 for 4-pair bonding on the 1754
- ✓ 1 - AC power adapter (90–265 VAC, 47–63 Hz)

Dimensions & Weight

- ✓ Dimensions: 35 mm (1.4 in) high × 210 mm (8.3 in) wide × 193 mm (7.6 in) deep
- ✓ Weight: 914 g (2 lb)

Operating Requirements

- ✓ Storage temperature: –40° C to +70° C (–40° to 158° F)
- ✓ Operating temperature: 0° C to +50° C (32° to 122° F)
- ✓ Operating humidity: 5% to 90% Relative Humidity, Non-condensing

Chapter 2 – Hardware Setup and Startup

Front Panel LED and Rear Panel description

Following illustrations show the front panels of the 2-wire and 4-wire routers.

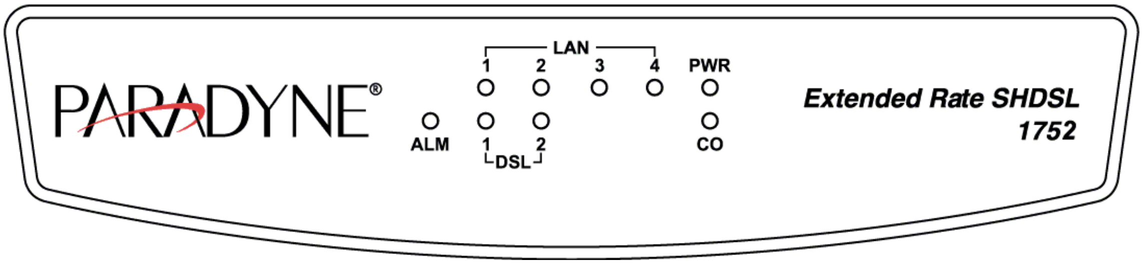


Figure 2-1. 2-Wire 1752 Front Panel LEDs

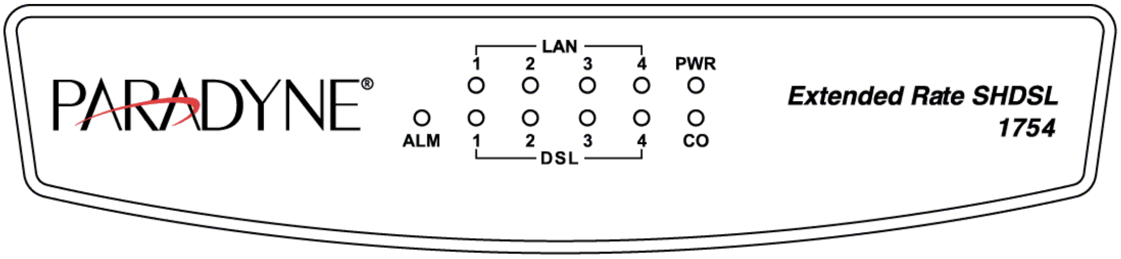


Figure 2-2. 4-wire 1754 Front Panel LED

LED	Usage
PWR	Power Indicator.
DSL	DSL loop activity.
CO	On: unit is in CO mode.
	Off: unit is in CPE mode.
ALM	An error has been detected.
LAN	On: The Ethernet Link is connected.

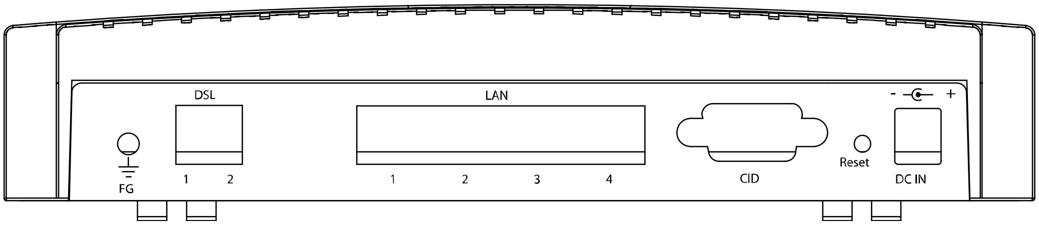


Figure 2-4. 2-wire 1752 rear view

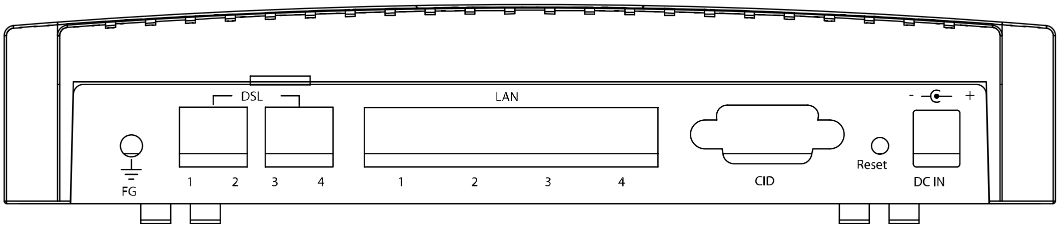


Figure 2-3. 4-wire 1754 rear view

Back Panel Feature	Usage
DC IN	Power Adapter Input
Reset Button	Reset device to factory default setting
CID	Connected to PC serial port for console
LAN	Connected to Ethernet Port
DSL 1–2 (1752) DSL 1–4 (1754)	Connected to loops 1 through 2 Connected to loops 1 through 4
FG	Connected to ground wire

DSL Connectors Description

DSL Connectors on back of the unit are RJ11 sockets. RJ11 uses a 6-position connector and cable. Two wire pairs are used for SHDSL.

Pin	Purpose
Pin 1	Not used.
Pin 2	Tip for DSL pair 2 or 4.
Pin 3	Tip for DSL pair 1 or 3
Pin 4	Ring for DSL pair 1 or 3
Pin 5	Ring for DSL pair 2 or 4
Pin 6	Not used.

Restore Factory Defaults/Reboot Button

Press the reset button to reset the 1750 Series router to its factory default settings. If you forget your password or cannot access the device, reset the device to return it to the default settings. Follow this procedure:

1. Power off the router.

2. Press the Reset button.

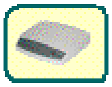
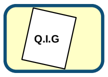
3. With the Reset button still depressed, power on the router, watching the front panel.

4. When the LEDs blink very quickly, release the Reset button. The reset fails if you hold the button in too long.

5. Save the current configuration again to overwrite your previous user configuration. (This is a so-called "one-time recall".)

Parts check

Check the following items in your package. Contact your sales representative if any item is missing or damaged.

	Extended rate SHDSL Router		RJ11 Cable (One with 1752, two with 1754)
	Power Adapter		Support CD
	RJ45 Cable		Quick Installation Instructions

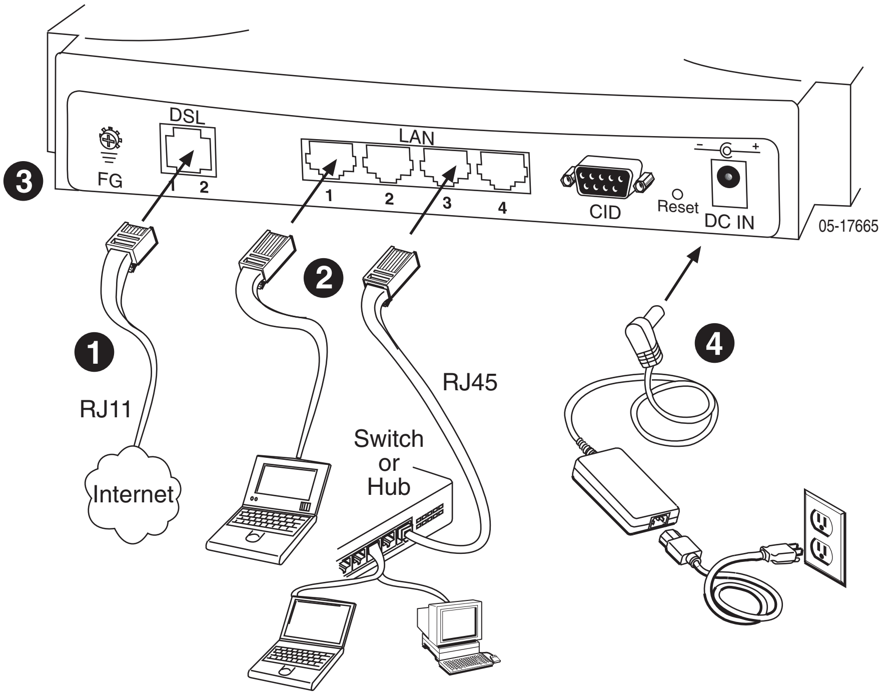
Hardware Connection – Model 1752

1. Connect the supplied RJ11 cable to the port marked DSL at the back of the SHDSL router. Connect the other end of the cable to your SHDSL source.

2. Insert one end of the RJ45 Ethernet cable into one of the LAN ports marked LAN on the back of the SHDSL router. Connect the other end of the cable into the Ethernet Network Interface Card (NIC) in your PC. Connect up to four Ethernet devices to the router. Use a crossover cable for a hub.

3. Connect an earth ground to the grounding terminal (marked FG).

4. Connect the supplied external AC adapter into the DC power outlet on the back of the router. Connect the power supply into your wall outlet or surge protector.



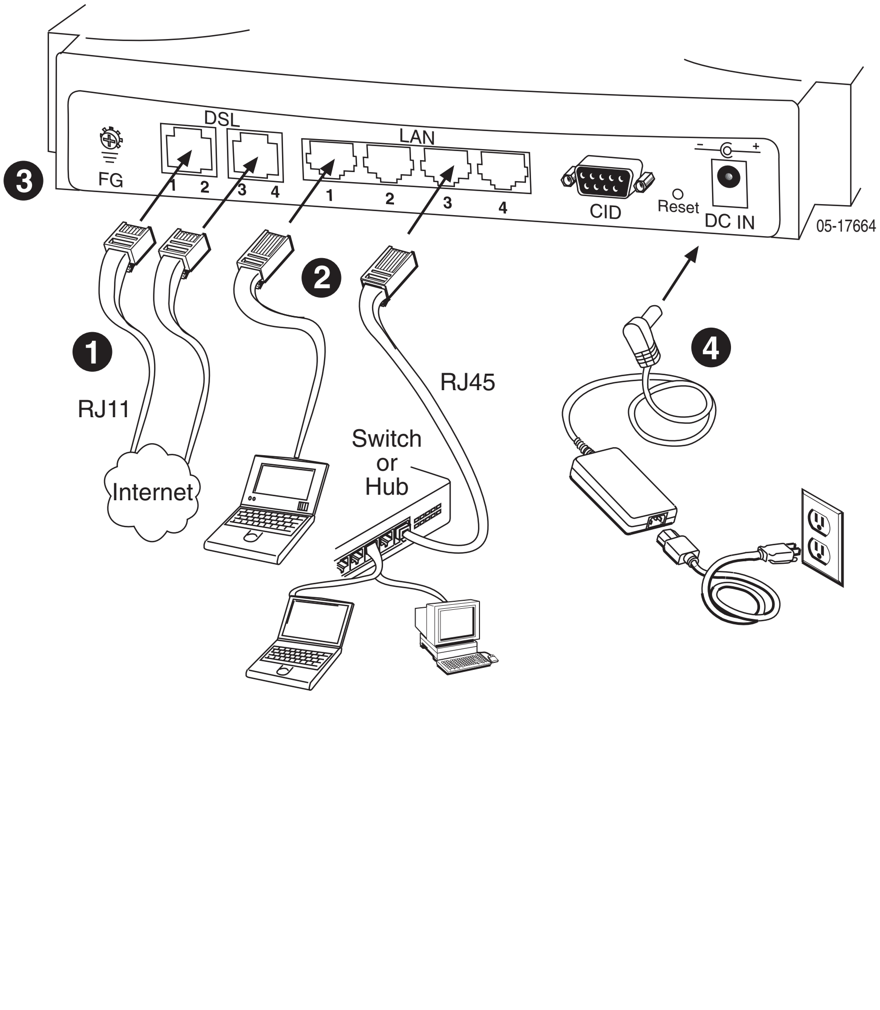
Hardware Connection – Model 1754

1. Connect one of the supplied RJ11 cables to the port marked DSL 1-2 at the back of the SHDSL router. Connect the other end of the cable to the SHDSL source. Connect the other supplied RJ11 cable to the port marked DSL 3-4. Connect the other end of the cable to the SHDSL source.

2. Insert one end of the RJ45 Ethernet cable into one of the LAN ports marked LAN on the back of the SHDSL router. Connect the other end of the cable into the Ethernet Network Interface Card (NIC) in your PC. Connect up to four Ethernet devices to the router. Use a crossover cable for a hub.

3. Connect an earth ground to the grounding terminal (marked FG).

4. Connect the supplied external AC adapter into the DC power outlet on the back of the router. Connect the power supply into your wall outlet or surge protector.



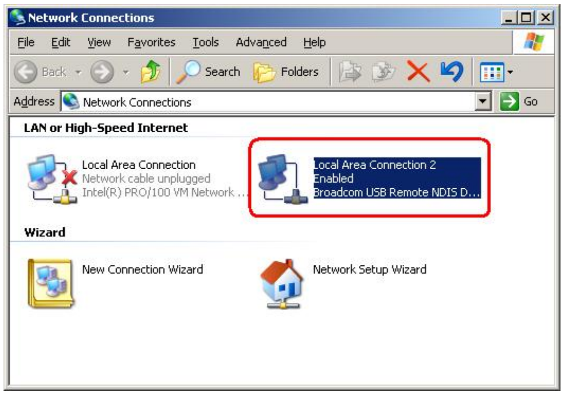
Configuring Windows PCs

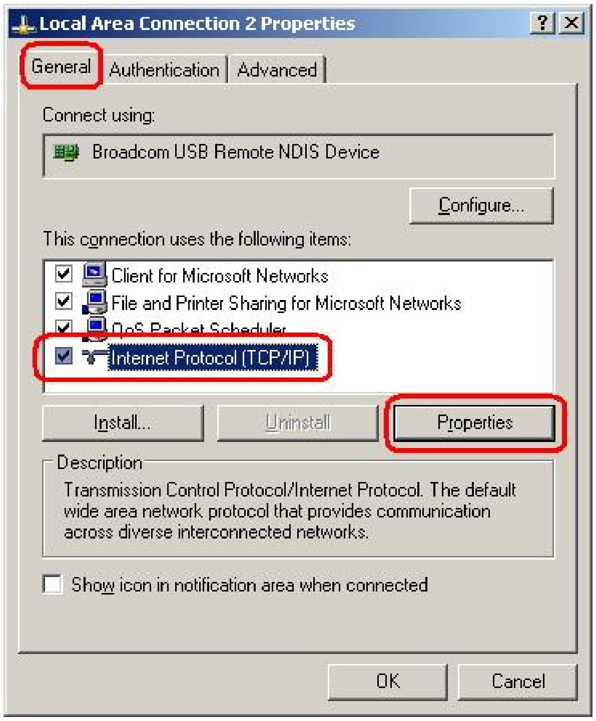
To access the router using the web interface, you must configure your PC's TCP/IP address to be **192.168.1.*x***, where *x* is any number between 3 and 254. The subnet mask is **255.255.255.0**.

Your router's default IP address is **192.168.1.1**.

Windows XP:

1. In the Windows task bar, click on the **Start** button, and then click on **Control Panel**.
2. Double-click on the **Network Connections** icon.
3. In the LAN or High-Speed Internet window, right-click on the icon corresponding to your network interface card (NIC) and select **Properties**. (Often this icon is labeled *Local Area Connection*). The **Local Area Connection** dialog box is displayed with a list of currently installed network items.
4. Ensure that the check box to the left of the item labeled **Internet Protocol (TCP/IP)** is checked, and click on Properties .


Network Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network Connections Go
LAN or High-Speed Internet
Local Area Connection
Network cable unplugged
Intel(R) PRO/100 VM Network ...
Local Area Connection 2
Enabled
Broadcom USB Remote NDIS D...
Wizard
New Connection Wizard
Network Setup Wizard



Connect using:

Broadcom USB Remote NDIS Device

This connection uses the following items:

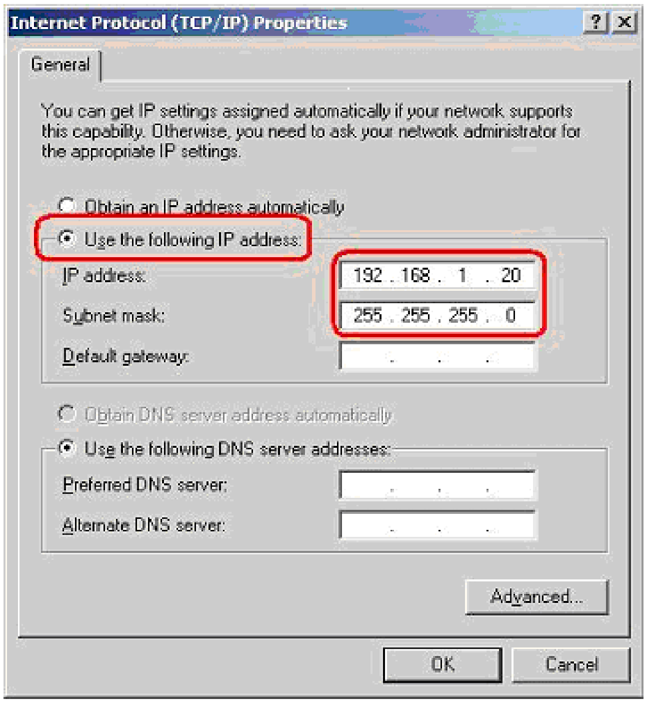
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

□ Show icon in notification area when connected

5. In the **Internet Protocol (TCP/IP) Properties** dialog box, click in the radio button labeled **Use the following IP address** and type **192.168.1.*x*** (where ***x*** is any number between 3 and 254) in the IP Address field. Type **255.255.255.0** in the Subnet Mask field.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 20

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

6. Click on OK twice to confirm your changes, and close the **Control Panel**.

Windows 2000:

1. In the Windows task bar, click on the **Start** button, point to **Settings**, and then select **Control Panel**.
2. Double-click on the **Network and Dial-up Connections** icon.
3. In the **Network and Dial-up Connections** window, right-click on the **Local Area Connection** icon, and then select **Properties**.
4. The **Local Area Connection Properties** dialog box is displayed with a list of currently installed network components. If the list includes **Internet Protocol (TCP/IP)**, the protocol has already been enabled, in which case you can skip to Step 12.
5. If **Internet Protocol (TCP/IP)** does not appear as an installed component, click on Install... .
6. In the **Select Network Component Type** dialog box, select **Protocol**, and then click on Add... .
7. Select **Internet Protocol (TCP/IP)** in the **Network Protocols** list, and then click on OK .
8. You may be prompted to install files from your Windows 2000 installation CD or other media. Follow the instructions to install the files.
9. If prompted, click on OK to restart your computer with the new settings.
10. After restarting your PC, double-click on the **Network and Dial-up Connections** icon in the **Control Panel**.
11. In **Network and Dial-up Connections** window, right-click on the **Local Area Connection** icon, and then select **Properties**.
12. In the **Local Area Connection Properties** dialog box, select **Internet Protocol (TCP/IP)**, and then click on Properties .
13. In the **Internet Protocol (TCP/IP) Properties** dialog box, click in the radio button labeled **Use the following IP address** and type **192.168.1.*x*** (where ***x*** is any number between 3 and 254) in the IP Address field. Type **255.255.255.0** in the Subnet Mask field.
14. Click on OK twice to confirm and save your changes, and then close the **Control Panel**.

Windows Me:

1. In the Windows task bar, click on the **Start** button, point to **Settings**, and then click on **Control Panel**.
2. Double-click on the **Network and Dial-up Connections** icon.
3. In the **Network and Dial-up Connections** window, right-click on the **Network** icon, and then select **Properties**.
4. The **Network Properties** dialog box is displayed with a list of currently installed network components. If the list includes **Internet Protocol (TCP/IP)**, the protocol has already been enabled, in which case you can skip to Step 13.

5. If **Internet Protocol (TCP/IP)** does not appear as an installed component, click on Add....

6. In the **Select Network Component Type** dialog box, select **Protocol**, and then click on Add....

7. Select **Microsoft** in the Manufacturers box.

8. Select **Internet Protocol (TCP/IP)** in the Network Protocols list, and then click on OK.

9. You may be prompted to install files from your Windows Me installation CD or other media. Follow the instructions to install the files.

10. If prompted, click on OK to restart your computer with the new settings.

11. After restarting your PC, double-click on the **Network and Dial-up Connections** icon in the **Control Panel**.

12. In **Network and Dial-up Connections** window, right-click on the **Network** icon, and then select **Properties**.

13. In the **Network Properties** dialog box, select **TCP/IP**, and then click on Properties.

14. In the **TCP/IP Settings** dialog box, click in the radio button labeled **Use the following IP address** and type **192.168.1.*x*** (where ***x*** is any number between 3 and 254) in the IP Address field. Type **255.255.255.0** in the Subnet Mask field.

15. Click on OK twice to confirm and save your changes, and then close the **Control Panel**.

Windows 95, 98:

1. In the Windows task bar, click on the **Start** button, point to **Settings**, and then click on **Control Panel**.

2. Double-click on the **Network** icon.

3. The **Network** dialog box is displayed with a list of currently installed network components. If the list includes **TCP/IP**, the protocol has already been enabled, in which case you can skip to Step 12.

4. If **TCP/IP** does not appear as an installed component, click on Add.... The **Select Network Component Type** dialog box appears.

5. Select **Protocol**, and then click Add....

6. The **Select Network Protocol** dialog box appears.

7. Click on **Microsoft** in the Manufacturers list box, and then click **TCP/IP** in the Network Protocols list box.

8. Click OK to return to the **Network** dialog box, and then click OK again.

9. You may be prompted to install files from your Windows 95/98 installation CD. Follow the instructions to install the files.

10. Click on OK to restart the PC and complete the TCP/IP installation.
11. After restarting your PC, open the **Control Panel** window, and then click on the **Network** icon.
12. Select the network component labeled **TCP/IP**, and then click on Properties.
13. If you have multiple TCP/IP listings, select the listing associated with your network card or adapter.
14. In the **TCP/IP Properties** dialog box, click on the **IP Address** tab.
15. Click in the radio button labeled **Use the following IP address** and type **192.168.1.*x*** (where ***x*** is any number between 3 and 254) in the IP Address field. Type **255.255.255.0** in the Subnet Mask field.
16. Click on OK twice to confirm and save your changes. You will be prompted to restart Windows. Click on Yes and restart your PC again.

Windows NT 4.0:

1. In the Windows NT task bar, click on the **Start** button, point to **Settings**, and then click on **Control Panel**.
2. In the **Control Panel** window, double click on the **Network** icon.
3. In the **Network** dialog box, click on the **Protocols** tab.
4. The Protocols tab displays a list of currently installed network protocols. If the list includes **TCP/IP**, the protocol has already been enabled, in which case you can skip to Step 12.
5. If **TCP/IP** does not appear as an installed component, click on Add....
6. In the **Select Network Protocol** dialog box, select **TCP/IP**, and then click on OK.
7. You may be prompted to install files from your Windows NT installation CD or other media. Follow the instructions to install the files.
8. After all files are installed, a window displays to inform you that a TCP/IP service called DHCP can be set up to dynamically assign IP information.
9. Click on Yes to continue, and then click on OK if prompted to restart your computer.
10. After restarting your PC, open the **Control Panel** window, and then double-click on the **Network** icon.
11. In the **Network** dialog box, click on the **Protocols** tab.
12. In the **Protocols** tab, select **TCP/IP**, and then click on Properties.
13. In the **Microsoft TCP/IP Properties** dialog box, click in the radio button labeled **Use the following IP address** and type **192.168.1.*x*** (where ***x*** is any number between 3 and 254) in the IP Address field. Type **255.255.255.0** in the Subnet Mask field.
14. Click on OK twice to confirm and save your changes, and then close the **Control Panel**.

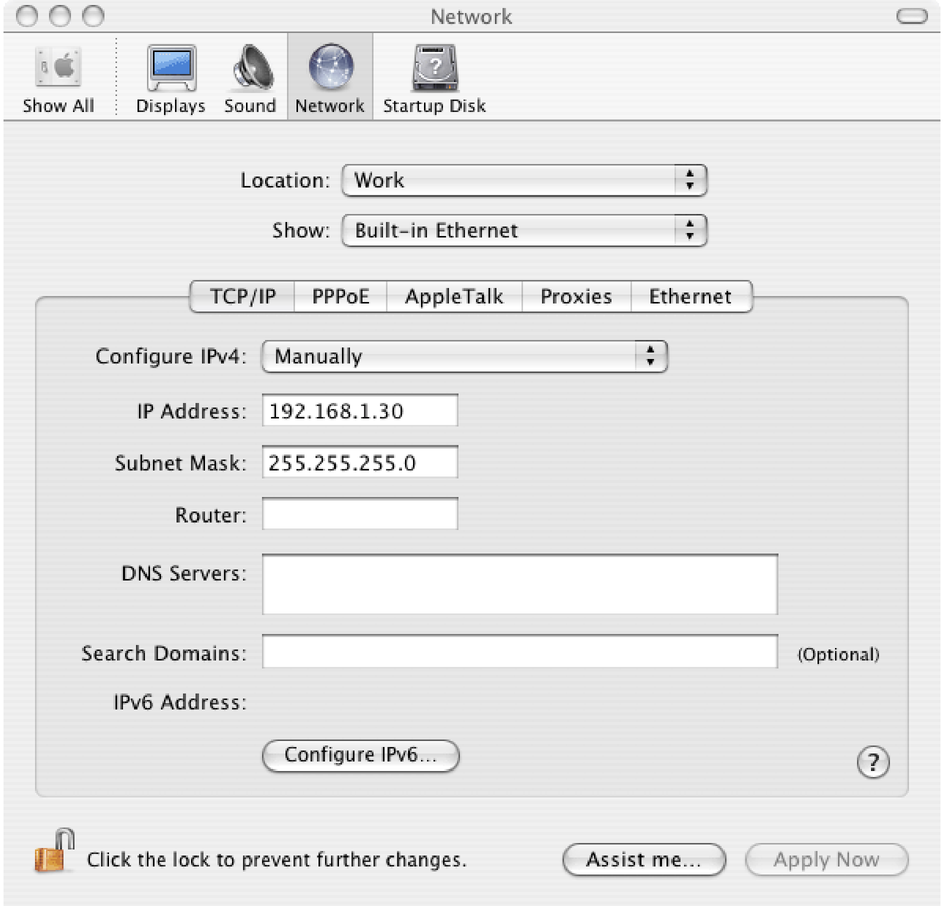
Configuring Apple PCs

To access the router using the web interface, you must configure your PC's TCP/IP address to be **192.168.1.*x***, where *x* is any number between 3 and 254. The subnet mask is **255.255.255.0**.

Your router's default IP address is **192.168.1.1**.

Mac OS X

1. Under the Apple menu, select System Preferences.
2. Click on the Network icon.
3. In the Network window, choose the item that corresponds to your Ethernet interface from the Show: drop-down list.
4. Select Manually from the Configure IPv4: drop-down list.
5. Type an address between 192.168.1.3 and 192.168.1.254 in the IP Address field (192.168.1.30 is shown here as an example) and 255.255.255.0 in the Subnet Mask field.



Location: Work

Show: Built-in Ethernet

Configure IPv4: Manually

IP Address: 192.168.1.30

Subnet Mask: 255.255.255.0

Router:

DNS Servers:

Search Domains: (Optional)

IPv6 Address:

Click the lock to prevent further changes.

6. Click the Apply Now button to apply your changes and quit the System Preferences application.

Mac OS 8.x or 9.0

1. Under the Apple menu, select Control Panels, then TCP/IP.
2. In the TCP/IP control panel, choose the item that corresponds to your Ethernet interface from the Connect via: drop-down list.
3. Select Manually from the Configure: drop-down list.
4. Type an address between 192.168.1.3 and 192.168.1.254 in the IP Address field and 255.255.255.0 in the Subnet Mask field.
5. Close the control panel and save your changes when prompted.

Chapter 3 – Configuring the Router Using EmWeb

Accessing EmWeb

EmWeb is an application for configuring your router. It is accessed using a web browser such as Internet Explorer version 5 or above.

To access EmWeb on a router set to the factory default configuration:

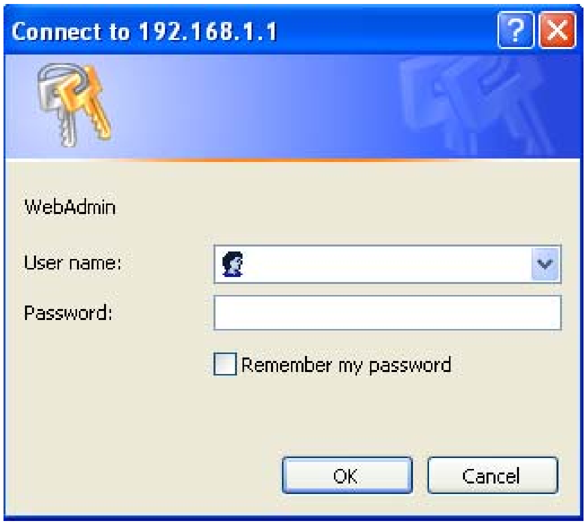
1. Attach a PC to one of the LAN interfaces. On the Address line of your web browser, enter the URL: http://192.168.1.1

2. A login box is displayed. Enter the default User Name and Password:

   User Name: admin

   Password: admin

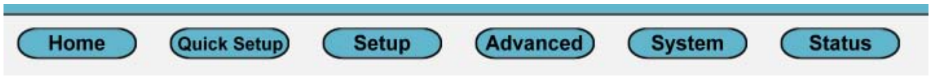
3. Click on OK. You are now ready to configure the router using EmWeb.



About EmWeb pages

EmWeb provides a series of web pages that you can use to set up and configure the router.

These pages are organized into six main topics.



You can select the topics using the buttons at the top of the main window:

- Home: Returns you to the front page.
- Quick Setup: Guides you through the steps to configure your router.
- Setup: Allows you to configure WAN and LAN connections.

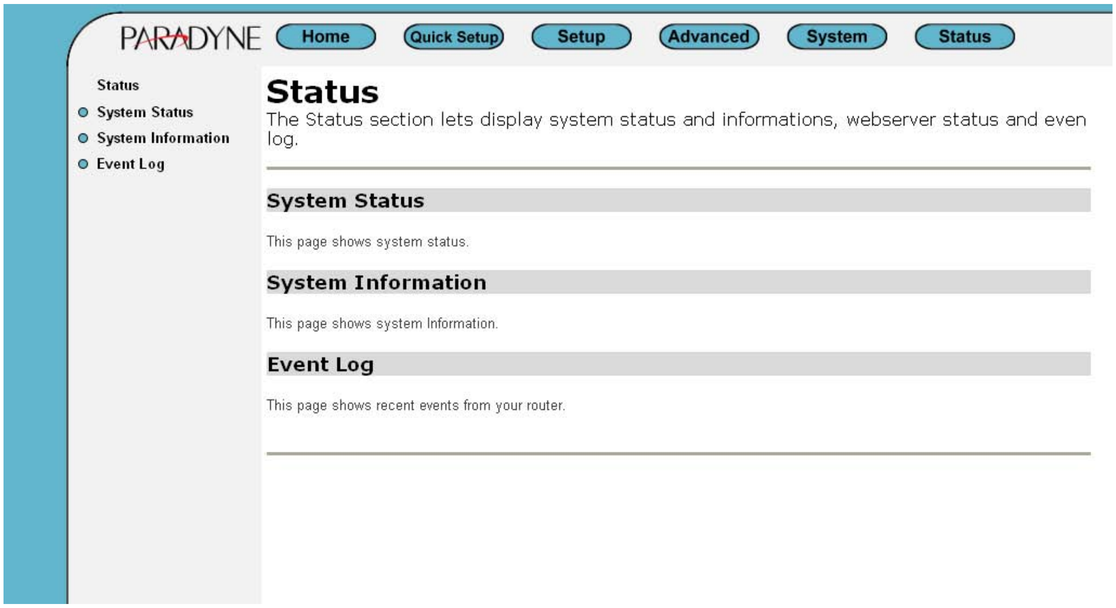
- Advanced: Lets you configure advanced features like Security, IP routes, and Bridge.
- System: Lets you execute system-level commands like Event Log, Firmware Update, Backup/Restore, Save configuration, and Authentication.
- Status: Provides information about the current setup and status of the system.

The exact information displayed on each web page depends on the specific configuration that you are using. The following sections give you a general overview of the setup and configuration details.

Status Pages

The Status home page has links to the following:

- System status
- System information
- Event log



Status

The Status section lets display system status and informations, webserver status and even log.

System Status

This page shows system status.

System Information

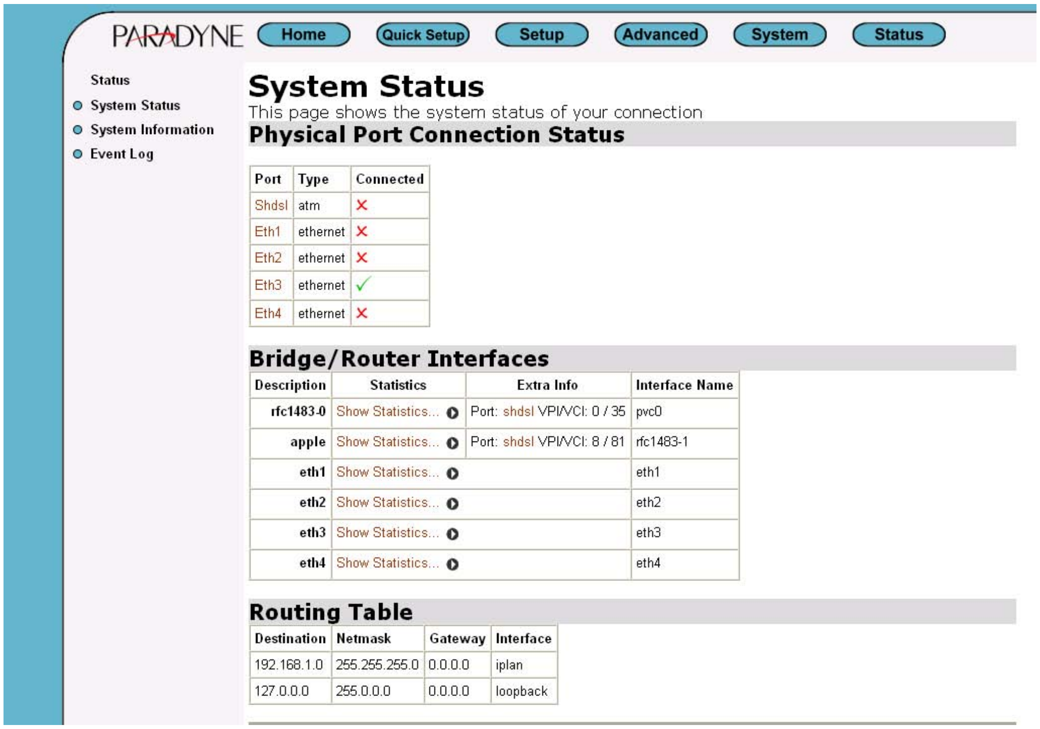
This page shows system Information.

Event Log

This page shows recent events from your router.

System status page

Click on System Status to invoke the system status page from which the status of the bridge/router interfaces or routing table is displayed.



System Status

This page shows the system status of your connection

Physical Port Connection Status

Port	Type	Connected
Shdsl	atm	✗
Eth1	ethernet	✗
Eth2	ethernet	✗
Eth3	ethernet	✓
Eth4	ethernet	✗

Bridge/Router Interfaces

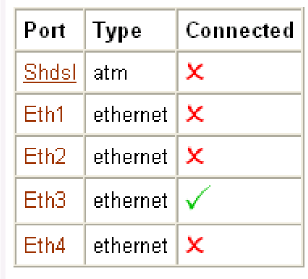
Description	Statistics	Extra Info	Interface Name
rfc1483-0	Show Statistics...	Port: shdsl VPI/VCI: 0 / 35	pvc0
apple	Show Statistics...	Port: shdsl VPI/VCI: 8 / 81	rfc1483-1
eth1	Show Statistics...		eth1
eth2	Show Statistics...		eth2
eth3	Show Statistics...		eth3
eth4	Show Statistics...		eth4

Routing Table

Destination	Netmask	Gateway	Interface
192.168.1.0	255.255.255.0	0.0.0.0	iplan
127.0.0.0	255.0.0.0	0.0.0.0	loopback

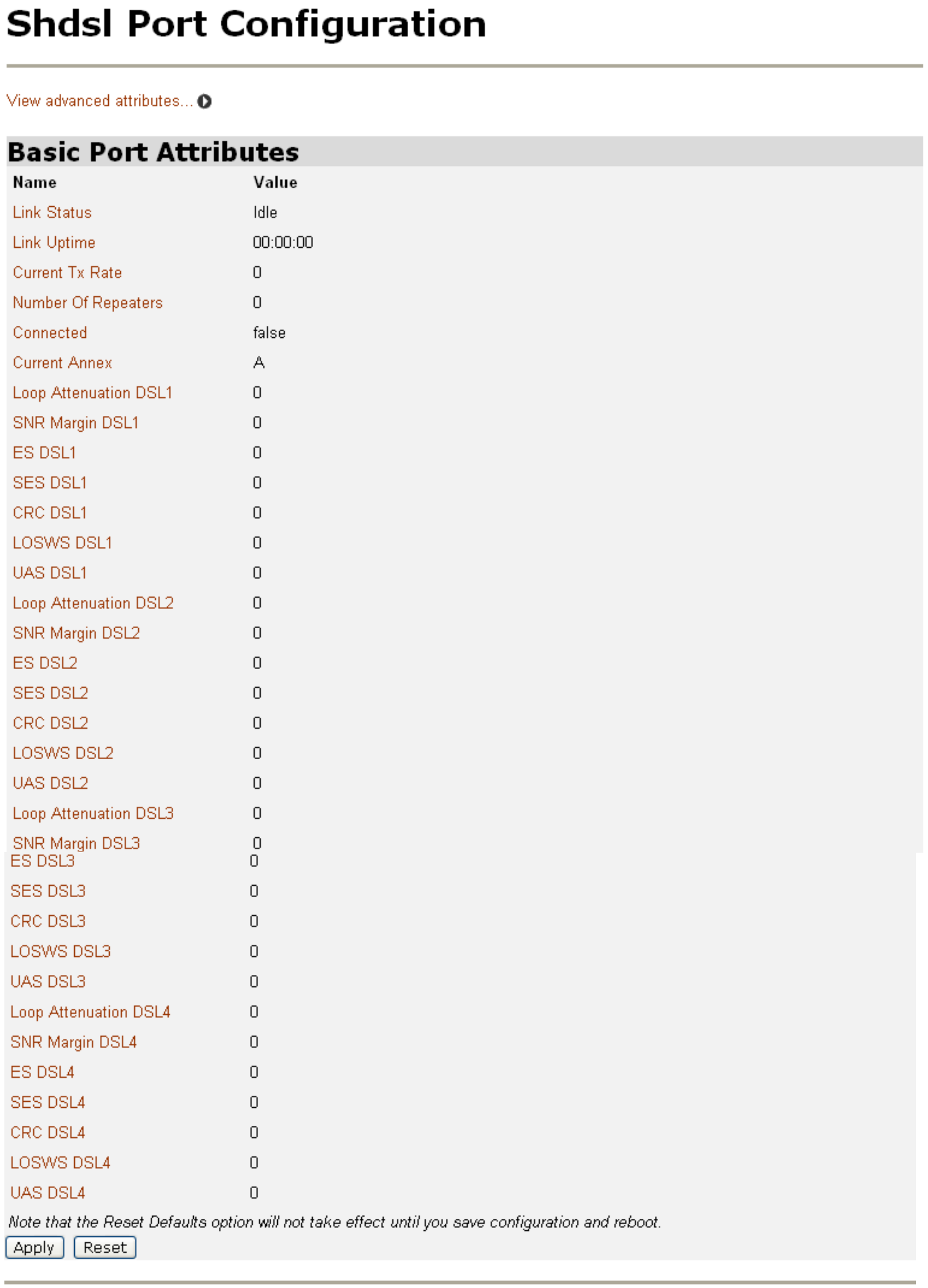
Physical port connection status:

If to view or change a physical port configuration, select a port to see configuration information for that port.



Port	Type	Connected
Shdsl	atm	✗
Eth1	ethernet	✗
Eth2	ethernet	✗
Eth3	ethernet	✓
Eth4	ethernet	✗

The following figure shows basic port attributes under SHDSL port configuration page.



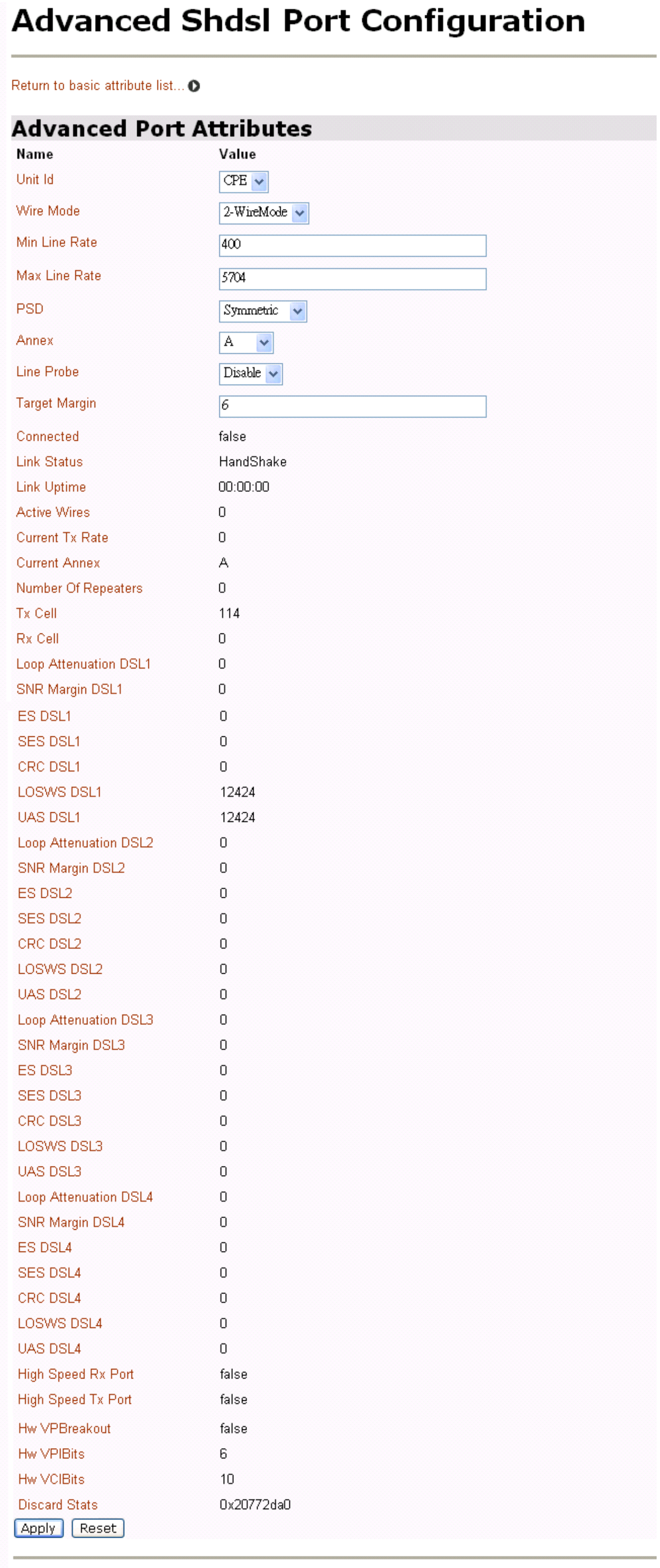
Shdsl Port Configuration

Basic Port Attributes

Name	Value
Link Status	Idle
Link Uptime	00:00:00
Current Tx Rate	0
Number Of Repeaters	0
Connected	false
Current Annex	A
Loop Attenuation DSL1	0
SNR Margin DSL1	0
ES DSL1	0
SES DSL1	0
CRC DSL1	0
LOSWS DSL1	0
UAS DSL1	0
Loop Attenuation DSL2	0
SNR Margin DSL2	0
ES DSL2	0
SES DSL2	0
CRC DSL2	0
LOSWS DSL2	0
UAS DSL2	0
Loop Attenuation DSL3	0
SNR Margin DSL3	0
ES DSL3	0
SES DSL3	0
CRC DSL3	0
LOSWS DSL3	0
UAS DSL3	0
Loop Attenuation DSL4	0
SNR Margin DSL4	0
ES DSL4	0
SES DSL4	0
CRC DSL4	0
LOSWS DSL4	0
UAS DSL4	0

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

To view or change advanced configuration settings for the SHDSL port, click on *View advanced attributes.* The SHDSL Port Configuration page is displayed. “Shdsl” is the default port name. You can configure SHDSL parameters from this page.



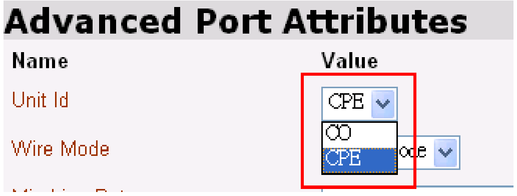
Advanced Shdsl Port Configuration

Return to basic attribute list...

Advanced Port Attributes

Name	Value
Unit Id	CPE
Wire Mode	2-WireMode
Min Line Rate	400
Max Line Rate	5704
PSD	Symmetric
Annex	A
Line Probe	Disable
Target Margin	6
Connected	false
Link Status	HandShake
Link Uptime	00:00:00
Active Wires	0
Current Tx Rate	0
Current Annex	A
Number Of Repeaters	0
Tx Cell	114
Rx Cell	0
Loop Attenuation DSL1	0
SNR Margin DSL1	0
ES DSL1	0
SES DSL1	0
CRC DSL1	0
LOSWS DSL1	12424
UAS DSL1	12424
Loop Attenuation DSL2	0
SNR Margin DSL2	0
ES DSL2	0
SES DSL2	0
CRC DSL2	0
LOSWS DSL2	0
UAS DSL2	0
Loop Attenuation DSL3	0
SNR Margin DSL3	0
ES DSL3	0
SES DSL3	0
CRC DSL3	0
LOSWS DSL3	0
UAS DSL3	0
Loop Attenuation DSL4	0
SNR Margin DSL4	0
ES DSL4	0
SES DSL4	0
CRC DSL4	0
LOSWS DSL4	0
UAS DSL4	0
High Speed Rx Port	false
High Speed Tx Port	false
Hw VPBreakout	false
Hw VPIBits	6
Hw VCIBits	10
Discard Stats	0x20772da0

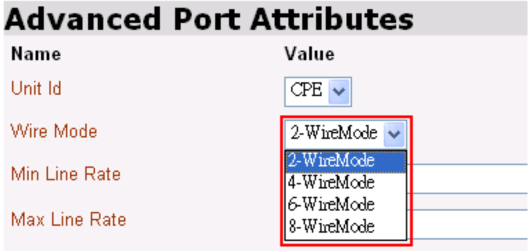
1. In the Unit Id drop-down menu, set the device as CO or CPE, and then click on Apply to submit your setting.



Advanced Port Attributes

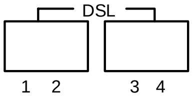
Name	Value
Unit Id	CPE CO CPE
Wire Mode	

2. To set the router's Wire Pair mode, click on the Wire Mode drop-down list to select the Wire Pair number needed. Click on Apply to submit your setting.

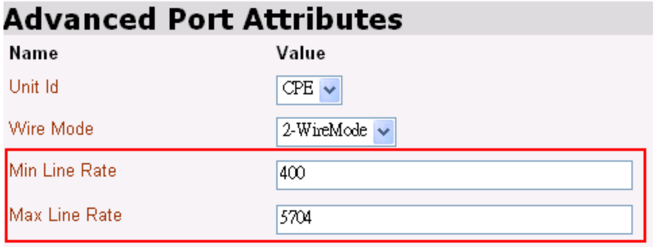


Advanced Port Attributes

Name	Value
Unit Id	CPE
Wire Mode	2-WireMode 2-WireMode 4-WireMode 6-WireMode 8-WireMode
Min Line Rate	
Max Line Rate	

Wire Pair	DSL Pair to Use	Illustration
WirePair1	1	
WirePair2	1,2	
WirePair3	1,2,3	
WirePair4	1,2,3,4	

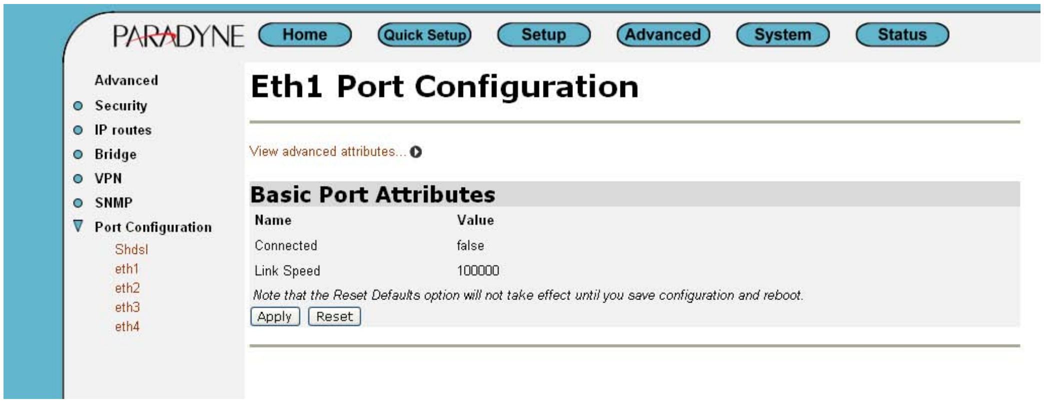
3. To set the maximum and minimum line rate, input the Max Line Rate and Min Line Rate respectively (where values range from 192000 bps to 5696000 bps) and then click on Apply to submit your setting. After the handshaking between STU-R and STU-C devices, the actual transmission rate will be presented in the Current Tx Rate attribute.



Advanced Port Attributes

Name	Value
Unit Id	CPE
Wire Mode	2-WireMode
Min Line Rate	400
Max Line Rate	5704

From the Port Configuration menu, click on eth1. The Eth1 Port Configuration page is displayed:



Eth1 Port Configuration

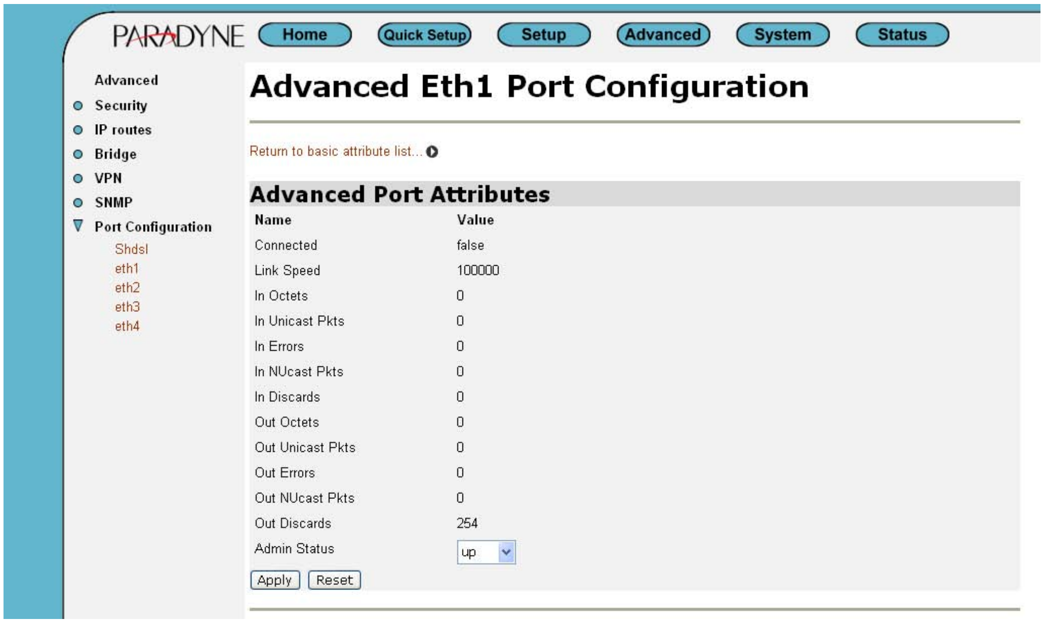
Basic Port Attributes

Name	Value
Connected	false
Link Speed	100000

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

1. The page displays basic port attributes for the Ethernet port on your router.

2. For advanced configuration of Ethernet port attributes, from the *Eth1t Port Configuration* page, click on *View advanced attributes.* The *Advanced Eth1 Port Configuration* page is displayed.



Advanced Eth1 Port Configuration

Advanced Port Attributes

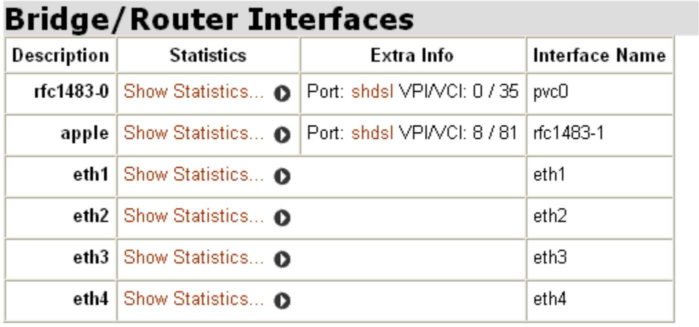
Name	Value
Connected	false
Link Speed	100000
In Octets	0
In Unicast Pkts	0
In Errors	0
In NUcast Pkts	0
In Discards	0
Out Octets	0
Out Unicast Pkts	0
Out Errors	0
Out NUcast Pkts	0
Out Discards	254
Admin Status	up

3. Update the port attributes that are available for editing, then click on Apply to update the advanced configuration, or Reset to revert back to the default advanced configuration settings. Click on the Return to basic attribute list to return to the Eth1 Port Configuration page.

4. For routers with 4 LAN ports, you can configure eth1 to eth4.

Bridge/Router Interfaces:

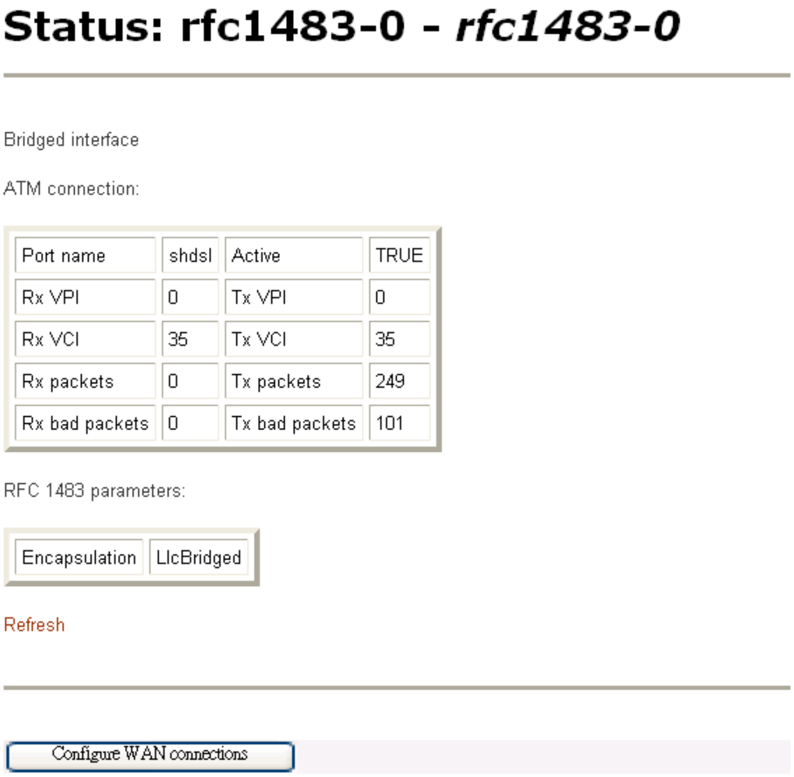
To view the statistics on Bridge/Router Interfaces, select a specified interface to invoke the status page.



Bridge/Router Interfaces

Description	Statistics	Extra Info	Interface Name
rfc1483-0	Show Statistics... ▶	Port: shdsl VPI/VCI: 0 / 35	pvc0
apple	Show Statistics... ▶	Port: shdsl VPI/VCI: 8 / 81	rfc1483-1
eth1	Show Statistics... ▶		eth1
eth2	Show Statistics... ▶		eth2
eth3	Show Statistics... ▶		eth3
eth4	Show Statistics... ▶		eth4

The following figure shows the statistics on the interface, rfc1483-0, under SHDSL port configuration page.



Status: rfc1483-0 - *rfc1483-0*

Bridged interface

ATM connection:

Port name	shdsl	Active	TRUE
Rx VPI	0	Tx VPI	0
Rx VCI	35	Tx VCI	35
Rx packets	0	Tx packets	249
Rx bad packets	0	Tx bad packets	101

RFC 1483 parameters:

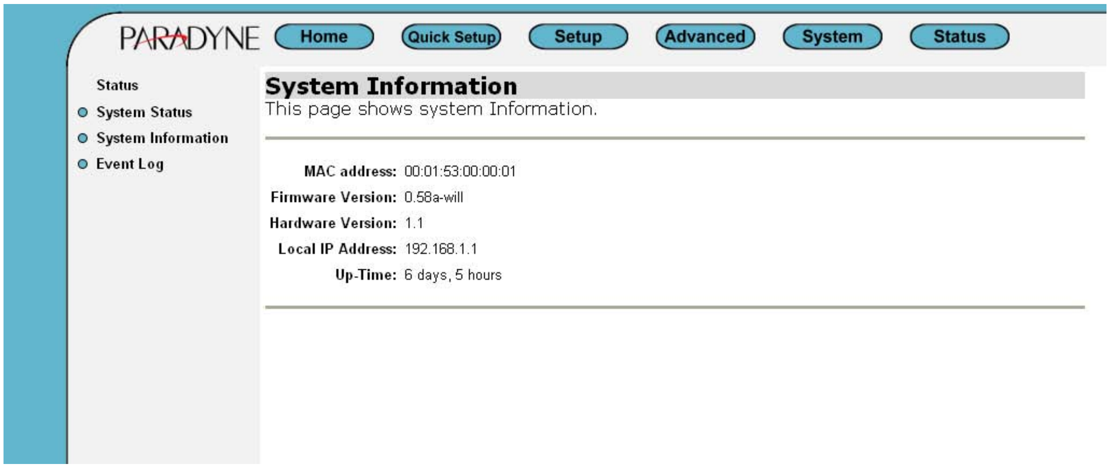
Encapsulation	LlcBridged

Refresh

Click Configure WAN connections to configure WAN connections. The procedure refers to the WAN connections section on Setup pages.

System information

This page shows system information, including MAC address, Firmware version, hardware version, IP address, and the amount of time the system has been up.



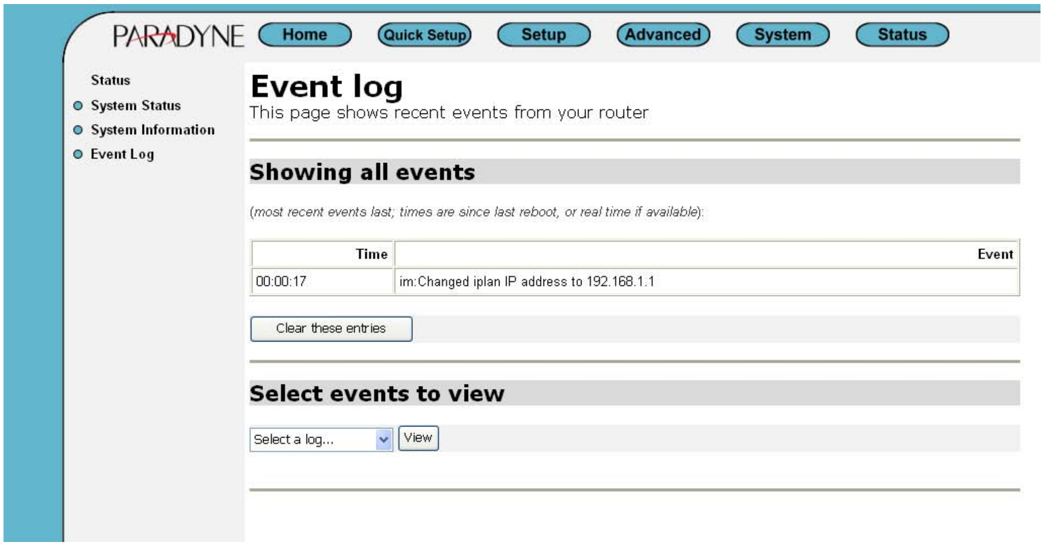
System Information

This page shows system Information.

MAC address: 00:01:53:00:00:01
Firmware Version: 0.58a-will
Hardware Version: 1.1
Local IP Address: 192.168.1.1
Up-Time: 6 days, 5 hours

Event Log

Click on Event Log to display the Event Log screen:



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
00:00:17	im:Changed iplan IP address to 192.168.1.1

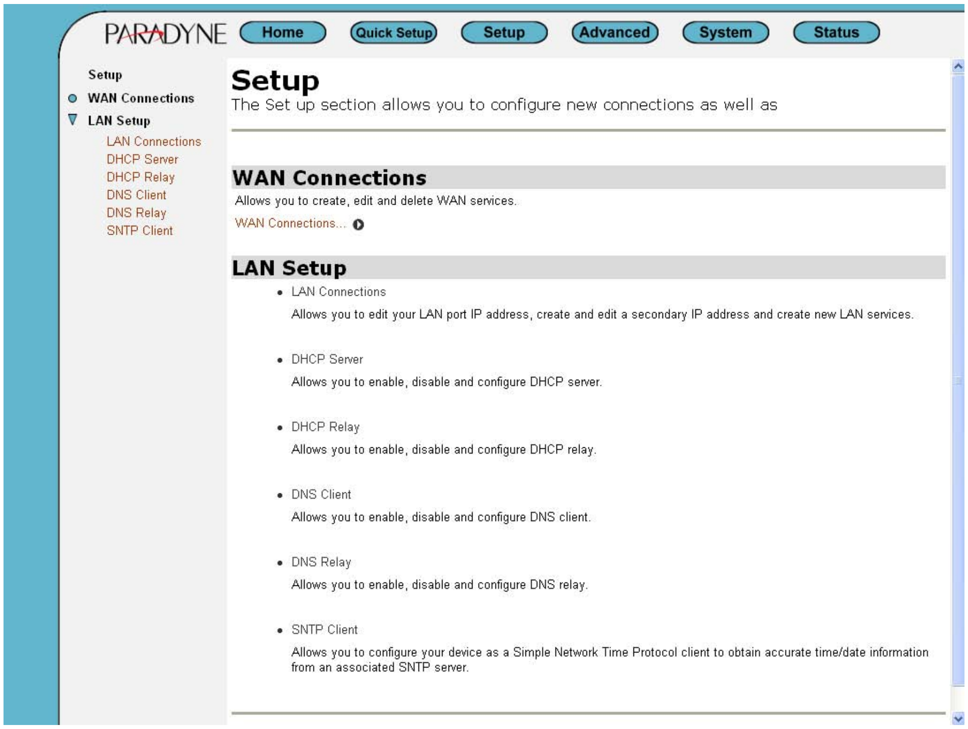
Select events to view

This page displays a table containing all configuration errors experienced by the router during the current session. The table also tells you:

- All Events: Shows all events that have occurred
- Config errors: Shows error messages regarding configuration errors
- Syslog Messages: Shows all messages regarding system actions other then Configuration errors

Setup pages

This page allows you to configure WAN and LAN connections.



Setup

The Set up section allows you to configure new connections as well as

WAN Connections

Allows you to create, edit and delete WAN services.

WAN Connections...

LAN Setup

- LAN Connections

  Allows you to edit your LAN port IP address, create and edit a secondary IP address and create new LAN services.

- DHCP Server

  Allows you to enable, disable and configure DHCP server.

- DHCP Relay

  Allows you to enable, disable and configure DHCP relay.

- DNS Client

  Allows you to enable, disable and configure DNS client.

- DNS Relay

  Allows you to enable, disable and configure DNS relay.

- SNTP Client

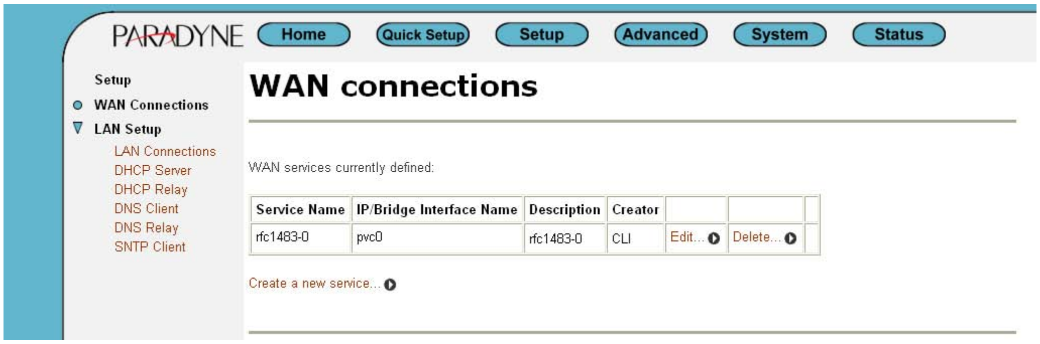
  Allows you to configure your device as a Simple Network Time Protocol client to obtain accurate time/date information from an associated SNTP server.

The Setup page allows users to configure:

1. LAN connections
2. DHCP Server
3. DHCP Relay
4. DNS Client
5. DNS Relay
6. SNTP Client

WAN Connection

This screen allows you to create and configure WAN connections for your router. You can also create virtual interfaces on routed services. Click on WAN connections to display the WAN Connections screen:



WAN connections

WAN services currently defined:

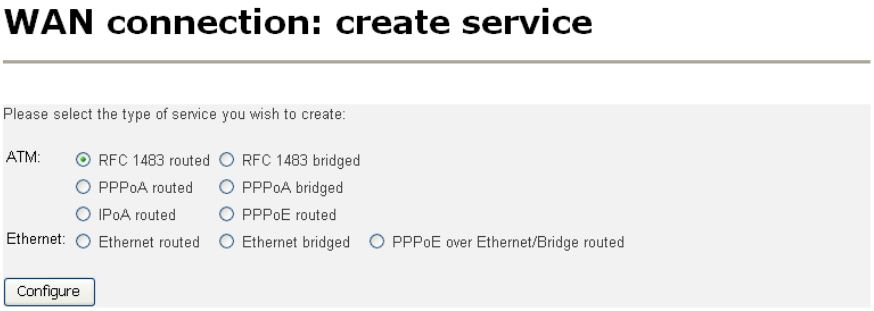
Service Name	IP/Bridge Interface Name	Description	Creator		
rfc1483-0	pvc0	rfc1483-0	CLI	Edit...	Delete...

Create a new service...

Creating a WAN service

1. Click on *Create a new service.* A page is displayed containing a list of WAN service options.

2. Select an option, and then click on *Configure*. You need to add detailed configuration information about the WAN service that you are creating.



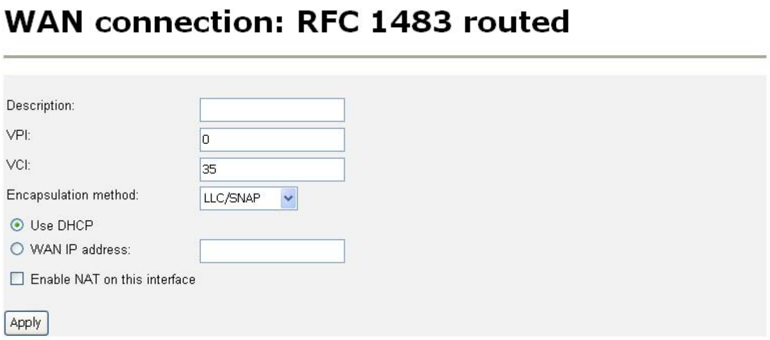
WAN connection: create service

Please select the type of service you wish to create:

ATM: ● RFC 1483 routed ○ RFC 1483 bridged
○ PPPoA routed ○ PPPoA bridged
○ IPoA routed ○ PPPoE routed
Ethernet: ○ Ethernet routed ○ Ethernet bridged ○ PPPoE over Ethernet/Bridge routed

Configure

3. Click on Apply. The WAN connections page is displayed. The table now contains details of the service that you have just created.



WAN connection: RFC 1483 routed

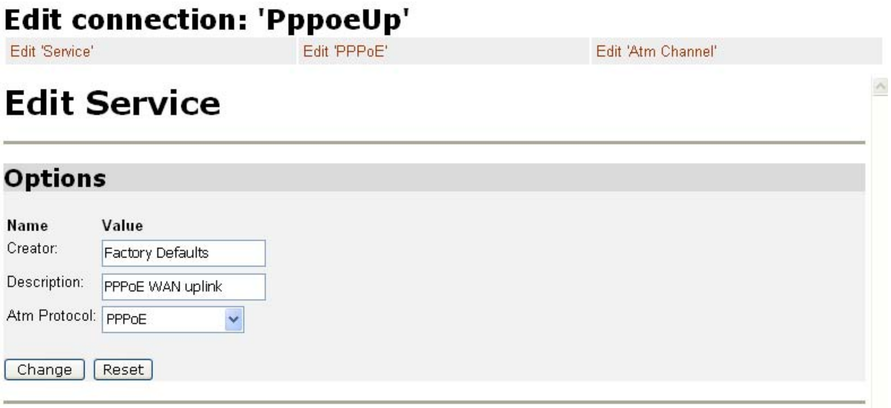
Description:	
VPI:	0
VCI:	35
Encapsulation method:	LLC/SNAP
● Use DHCP	
○ WAN IP address:	
☐ Enable NAT on this interface	

Apply

Editing a WAN service

1. Click on the *Edit* link for a specific service. The *WAN connection:*

edit page is displayed.



Edit connection: 'PppoeUp'

Edit 'Service' | Edit 'PPPoE' | Edit 'Atm Channel'

Edit Service

Options

Name	Value
Creator:	Factory Defaults
Description:	PPPoE WAN uplink
Atm Protocol:	PPPoE

Change Reset

2. Change the values for the existing service. If you want to carry out advanced editing, click on the links at the top of the edit page. The links that appear depend on the type of service that you are configuring. For example, for a PPPoE routed service, you can choose from the following advanced editing links:

Edit 'Service'

Edit 'PPPoE'

Edit 'Atm Channel'

3. Click on *Change*. The edit page is displayed and changes are applied to the service.

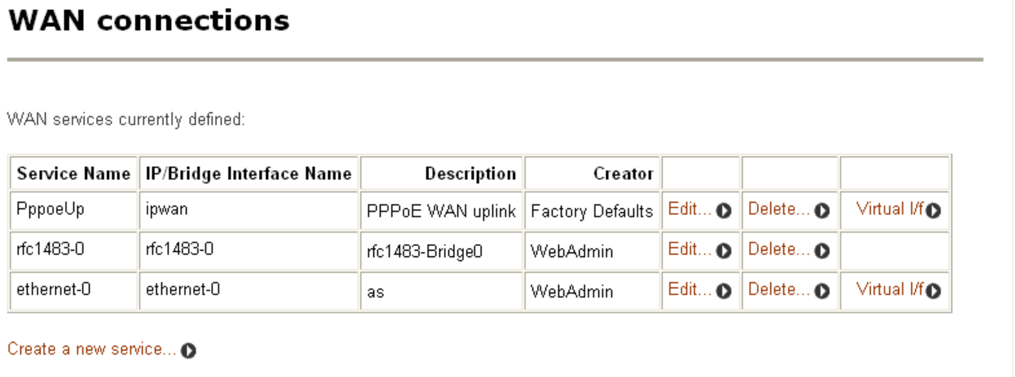
Deleting a WAN service

1. At the *WAN connections* page, click on the *Delete* link for a specific service. The *WAN connection: delete* page is displayed.

2. Check the details displayed, and then click on the *Delete this connection* button.

Creating a virtual interface (routed services only)

1. Click on the *Virtual I/f* link for a specific service. The *Virtual interface* page is displayed.



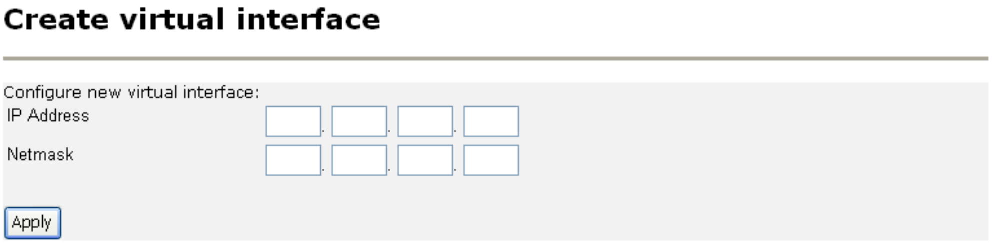
WAN connections

WAN services currently defined:

Service Name	IP/Bridge Interface Name	Description	Creator			
PppoeUp	ipwan	PPPoE WAN uplink	Factory Defaults	Edit...	Delete...	Virtual I/f
rfc1483-0	rfc1483-0	rfc1483-Bridge0	WebAdmin	Edit...	Delete...	
ethernet-0	ethernet-0	as	WebAdmin	Edit...	Delete...	Virtual I/f

Create a new service...

2. Click on the *Create a new virtual interface...* hyperlink. On the *Create virtual interface* page, type the IP address and netmask of the virtual interface, and then click on the Apply button.



Create virtual interface

Configure new virtual interface:

IP Address	. . .
Netmask	. . .

3. The WAN connections page is displayed. If you click on the *Virtual I/f* link, the *Virtual interface* page displays a table listing the names of existing virtual interfaces. Each virtual interface is called *item#* by default.

LAN Setup

LAN Setup provides following options to configure:

- LAN Connections
- DHCP Service
- DHCP Relay

- DNS Client
- DNS Relay
- SNTP client

LAN connections

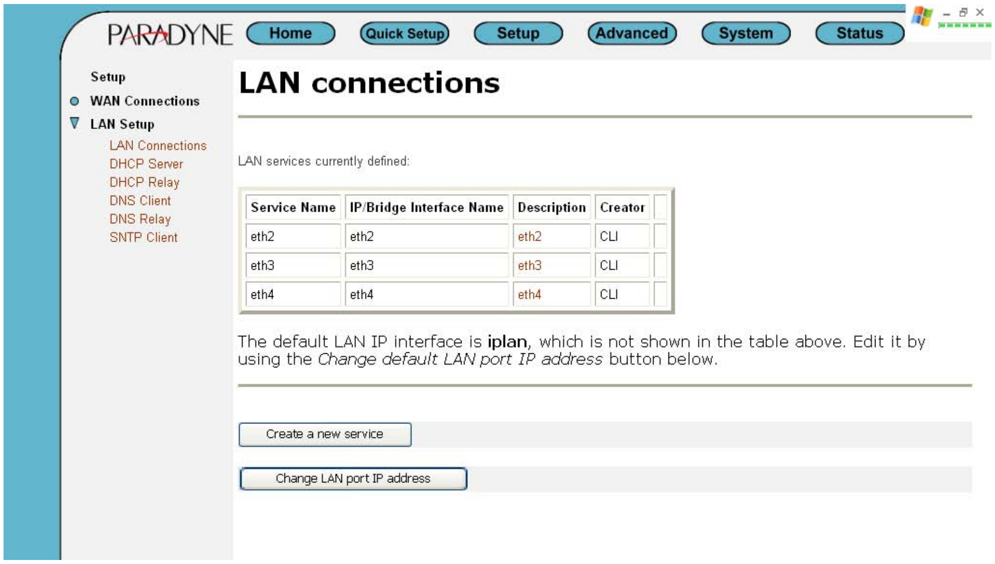
This option allows you to:

• Configure the IP address and subnet of the default LAN connection to the Router.

• Configure a secondary IP address on the same subnet as the primary IP address.

• Create virtual interfaces. Multiple virtual interfaces can be associated with the existing primary LAN interface.

From the Configuration menu, click on LAN connections. The following page is displayed:



LAN connections

LAN services currently defined:

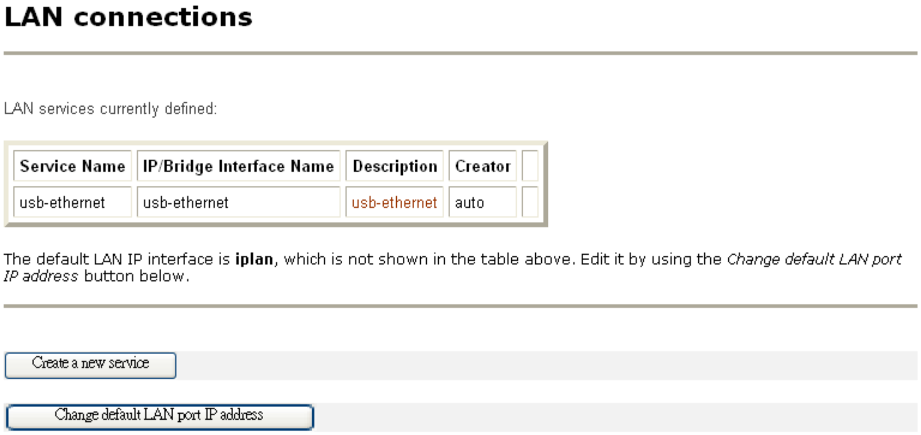
Service Name	IP/Bridge Interface Name	Description	Creator
eth2	eth2	eth2	CLI
eth3	eth3	eth3	CLI
eth4	eth4	eth4	CLI

The default LAN IP interface is **iplan**, which is not shown in the table above. Edit it by using the *Change default LAN port IP address* button below.

Configuring primary and secondary LAN connections

1 The Default LAN Port section contains two subsections:

a. IP address and subnet mask details of your primary LAN connection. To edit these, click on Change default LAN port IP address and type new primary address details.



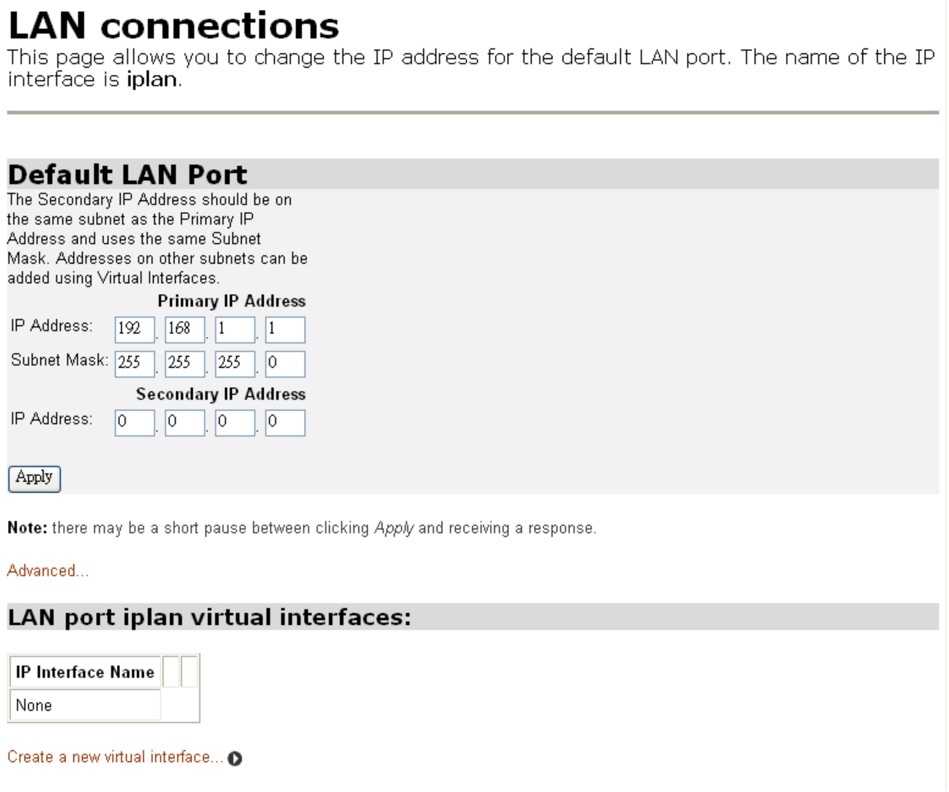
LAN connections

LAN services currently defined:

Service Name	IP/Bridge Interface Name	Description	Creator
usb-ethernet	usb-ethernet	usb-ethernet	auto

The default LAN IP interface is **iplan**, which is not shown in the table above. Edit it by using the *Change default LAN port IP address* button below.

b. Secondary IP address details. To create/configure a secondary IP address, click in the Secondary IP Address text box and type the new address details.



LAN connections

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

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.

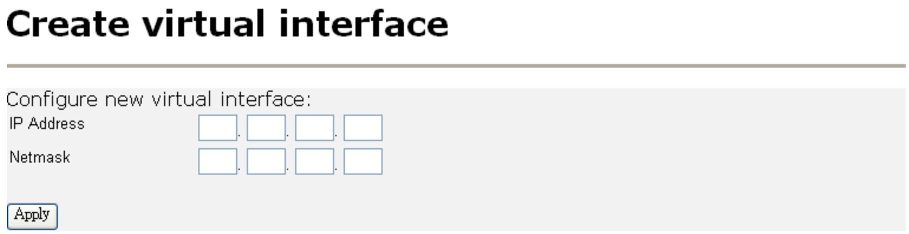
LAN port iplan virtual interfaces:

IP Interface Name		
None		

Once you have configured the IP address(es), click on the Apply button. A message is displayed confirming that your address information is being updated. If you have changed the primary IP address, you may need to enter the new address in your web browser Address box.

Creating virtual interfaces

1. Click on the Create a new virtual interface... hyperlink at the bottom of the LAN connections page. On the Create virtual interface page, type the IP address and netmask of the virtual interface, and then click on the Apply button.



Create virtual interface

Configure new virtual interface:

IP Address	. . .
Netmask	. . .

2. The LAN connections page is displayed. The virtual interfaces section contains a table listing the names of the virtual interface(s). Each virtual interface is called item# by default.

3. Each virtual interface name has an Edit and a Delete link associated with it. To edit a service:

a. Click on the Edit link.

b. Change the options for the existing virtual interface, then click on Change. The page is reset and the new values are displayed.

To delete a service:

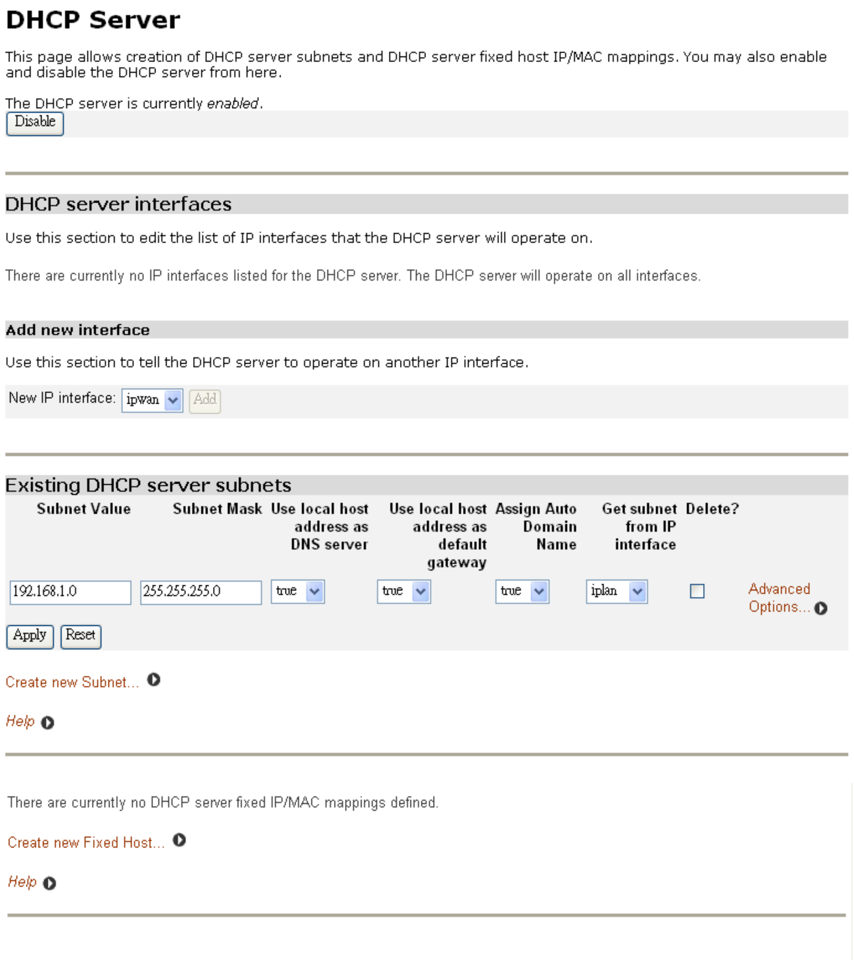
a. Click on the Delete link.

b. Check the details displayed, and then click on the Delete this connection button.

DHCP Server

This option allows you to enable or disable the DHCP server and create, configure, and delete DHCP server subnets and DHCP fixed IP /MAC mappings.

From the *Configuration* menu, click on *DHCP server*. The following page is displayed:



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

DHCP server interfaces

Use this section to edit the list of IP interfaces that the DHCP server will operate on.

There are currently no IP interfaces listed for the DHCP server. The DHCP server will operate on all interfaces.

Add new interface

Use this section to tell the DHCP server to operate on another IP interface.

New IP interface: ipwan Add

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	iplan	□	Advanced Options...

Apply Reset

Create new Subnet...

Help

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

Create new Fixed Host...

Help

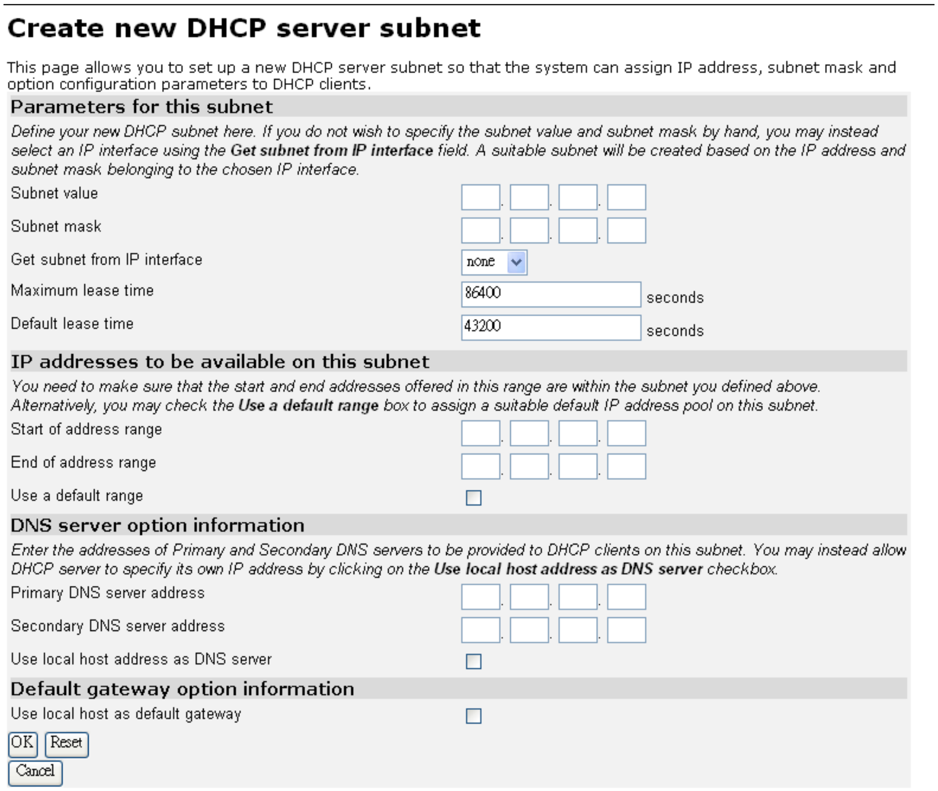
Enabling/disabling the DHCP server

The DHCP server is enabled by default. If to disable the DHCP server, click on Disable.

Note: If DHCP relay is enabled, DHCP server will be disabled by default. You can not enable DHCP server unless you disable DHCP relay.

Creating a DHCP server subnet

Click on the *Create new Subnet* link. The following page is displayed:



Create new DHCP server subnet

This page allows you to set up a new DHCP server subnet so that the system can assign IP address, subnet mask and option configuration parameters to DHCP clients.

Parameters for this subnet

*Define your new 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. A suitable subnet will be created based on the IP address and subnet mask belonging to the chosen IP interface.*

Subnet value	. . .
Subnet mask	. . .
Get subnet from IP interface	none
Maximum lease time	86400 seconds
Default lease time	43200 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	. . .
End of address range	. . .
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	. . .
Secondary DNS server address	. . .
Use local host address as DNS server	□

Default gateway option information

Use local host as default gateway	□

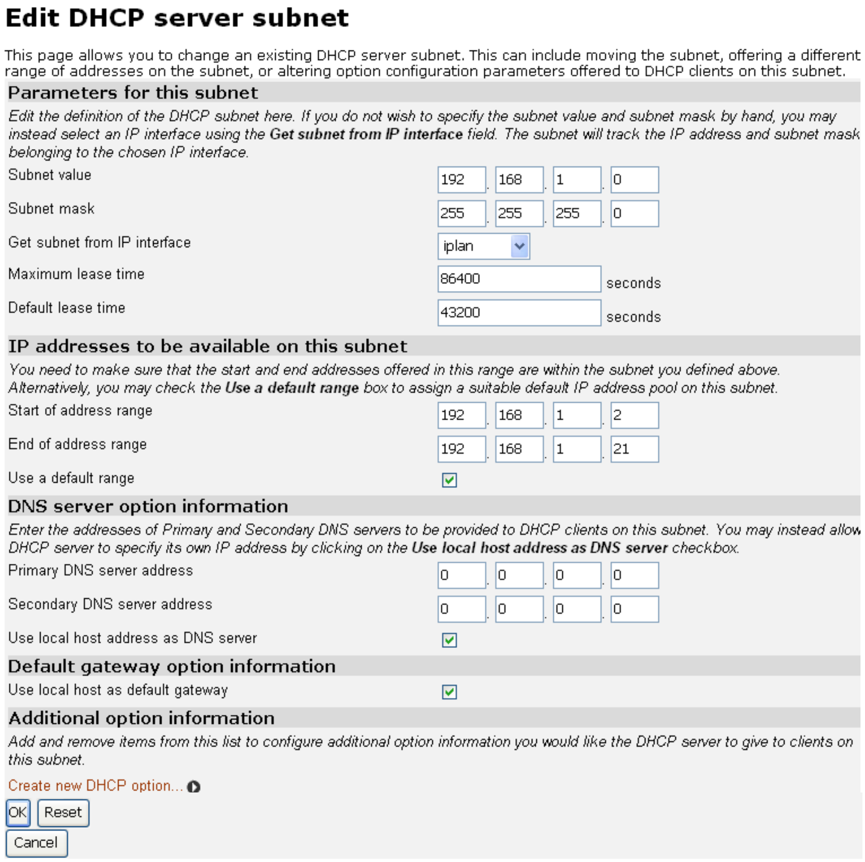
2. This page allows you to:

- Set the value and netmask of the subnet (either manually or by selecting an IP interface whose value and mask is used instead), and set the maximum and default lease times.
- Set the DHCP address range (or use a default range of 20 addresses).
- Set the Primary and Secondary DNS Server addresses or set your System to give out its own IP address as the DNS Server address.
- Set your router to supply its own IP address as the default Gateway address.

3. Once you have entered new configuration details for your DHCP server, click on OK. The *DHCP Server* page is displayed, containing details of your new subnet.

Editing a DHCP Subnet

Click on the *Advanced Options* link for a specific subnet. The *Edit DHCP server subnet* page is displayed. This allows you to edit all of the values that were set when the subnet was created.



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	iplan
Maximum lease time	86400 seconds
Default lease time	43200 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 . 2
End of address range	192 . 168 . 1 . 21
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	0 . 0 . 0 . 0
Secondary DNS server address	0 . 0 . 0 . 0
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 DHCP option...

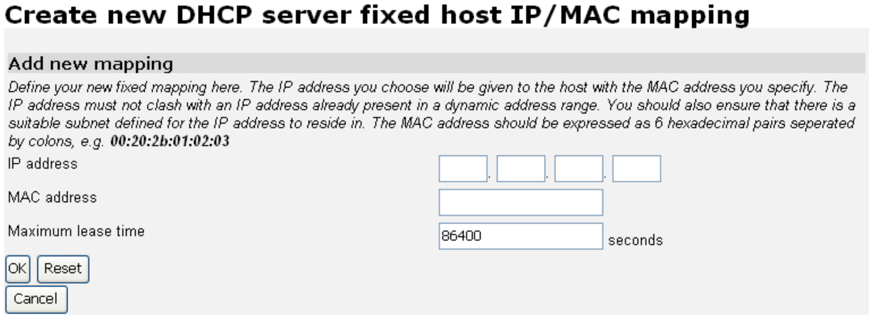
2. This page also allows you to add additional option information. At the bottom of the page, click on the *Create new DHCP option* link.

3. Click on the *Option name* drop-down list and select a name. Type a value that matches the selected option name in the *Option value* text box. Click on OK.

4. The *Edit DHCP server subnet* page is displayed, and details of you new option are displayed under the sub-heading *Additional option information*. To delete an existing option, check the *Delete* box for a specific option and click on OK.

Creating a Fixed Host

1. Click on the *Create new Fixed Host* link. The following page is displayed:



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

2. Complete the following:

a. Type in the IP address that will be given to the host with the specified MAC address.

b. Type in the MAC address and the maximum lease time (default is 86400 seconds).

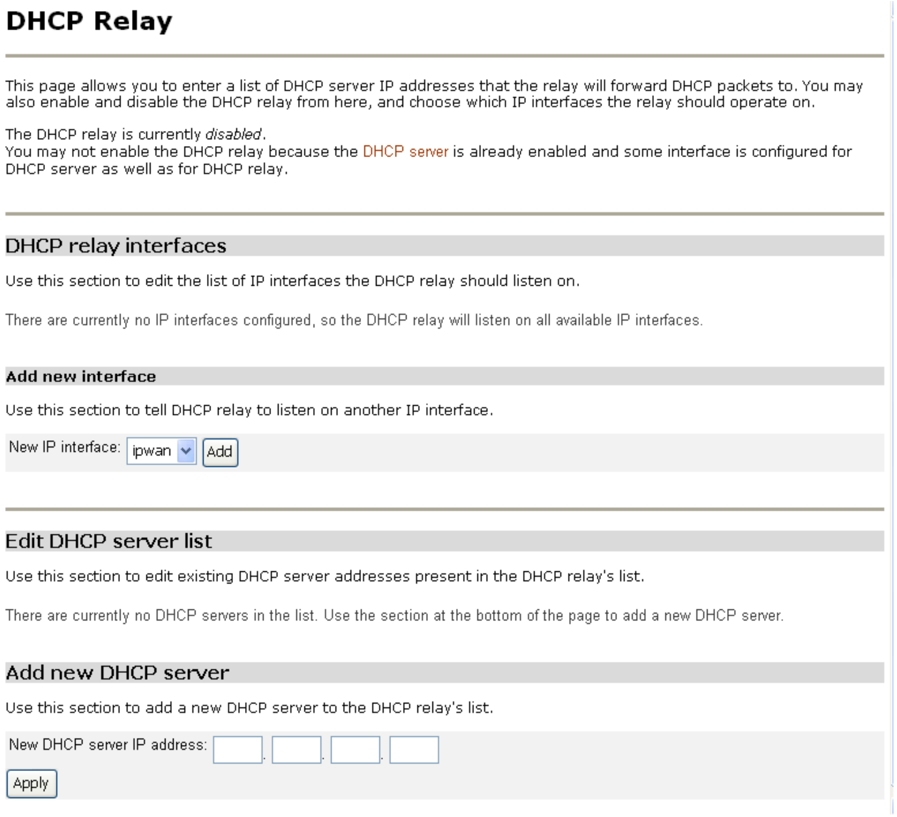
3. Click on OK. The *DHCP Server* page is displayed, and details of your new fixed host are displayed under the sub-heading *Existing DHCP fixed IP/MAC mappings*. To edit a fixed mapping, click on the IP address, MAC address, or max lease time, type a new entry, and click on Apply. To delete a fixed mapping, check the *Delete* box for a specific mapping and click on Apply.

DHCP Relay

This option allows you to:

- Enable and disable DHCP relay.
- Add DHCP servers to the DHCP relay list.
- Configure and delete server entries on the DHCP relay list.

From the Configuration menu, click on DHCP relay. The following page is displayed:



DHCP Relay

This page allows you to enter a list of DHCP server IP addresses that the relay will forward DHCP packets to. You may also enable and disable the DHCP relay from here, and choose which IP interfaces the relay should operate on.

The DHCP relay is currently *disabled*.
You may not enable the DHCP relay because the DHCP server is already enabled and some interface is configured for DHCP server as well as for DHCP relay.

DHCP relay interfaces

Use this section to edit the list of IP interfaces the DHCP relay should listen on.

There are currently no IP interfaces configured, so the DHCP relay will listen on all available IP interfaces.

Add new interface

Use this section to tell DHCP relay to listen on another IP interface.

New IP interface: ipwan Add

Edit DHCP server list

Use this section to edit existing DHCP server addresses present in the DHCP relay's list.

There are currently no DHCP servers in the list. Use the section at the bottom of the page to add a new DHCP server.

Add new DHCP server

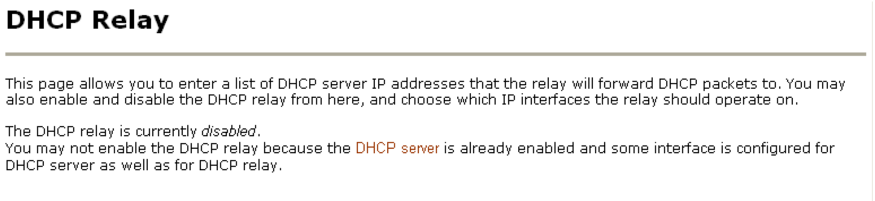
Use this section to add a new DHCP server to the DHCP relay's list.

New DHCP server IP address: ☐.☐.☐.☐

Apply

Enabling/disabling DHCP relay

This screen shows that the DHCP relay is currently disabled. If you click on the *Enable* button, DHCP server is disabled and the button changes to *Enable*.



DHCP Relay

This page allows you to enter a list of DHCP server IP addresses that the relay will forward DHCP packets to. You may also enable and disable the DHCP relay from here, and choose which IP interfaces the relay should operate on.

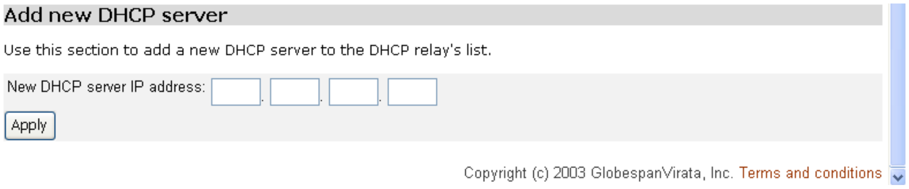
The DHCP relay is currently *disabled*.
You may not enable the DHCP relay because the DHCP server is already enabled and some interface is configured for DHCP server as well as for DHCP relay.

Note: If DHCP server is enabled, DHCP relay will be disabled by default. You can not enable DHCP relay unless you disable DHCP server.

Adding a DHCP server to the DHCP relay list:

1. In the *Add new DHCP server* section, type an address in the *New DHCP server IP address* text box.

2. Click on Apply. The address is displayed in the *Edit DHCP server list* section.



Add new DHCP server

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

New DHCP server IP address: [ ].[ ].[ ].[ ]

Copyright (c) 2003 GlobespanVirata, Inc. Terms and conditions

Editing/deleting entries in the DHCP relay list

1. To edit an entry, click on an IP address and type a new entry, then click on Apply.

2. To delete an entry, check the *Delete* box for a specific IP address, then click on Apply.

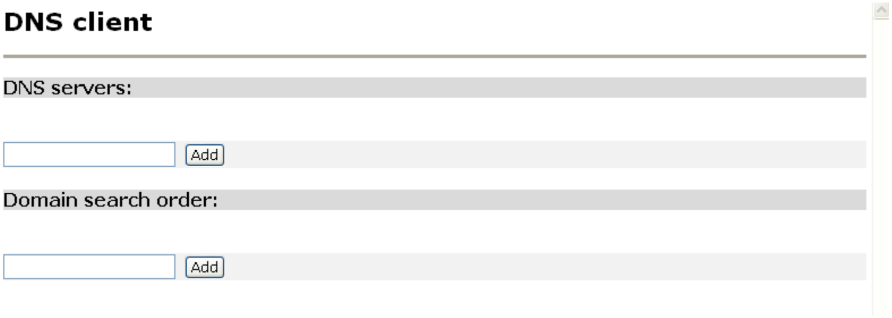
DNS Client

This option allows you to:

- Create a list of *server addresses*. This enables you to retrieve a domain name for a given IP address.

- Create a *domain search list*. DNS client uses this list when a user asks for the IP address list for an incomplete domain name.

From the *Configuration* menu, click on *DNS client*. The following page is displayed:



DNS client

DNS servers:

Domain search order:

Configuring DNS servers

1. Type the IP address of the unknown domain name in the *DNS servers:* text box.

2. Click on Add. The IP address appears in the DNS servers table. You can add a maximum of three server IP addresses. Each IP address entry has a *Delete* button associated with it. Click on Delete to remove an IP address from this list.

Configuring DNS search domains:

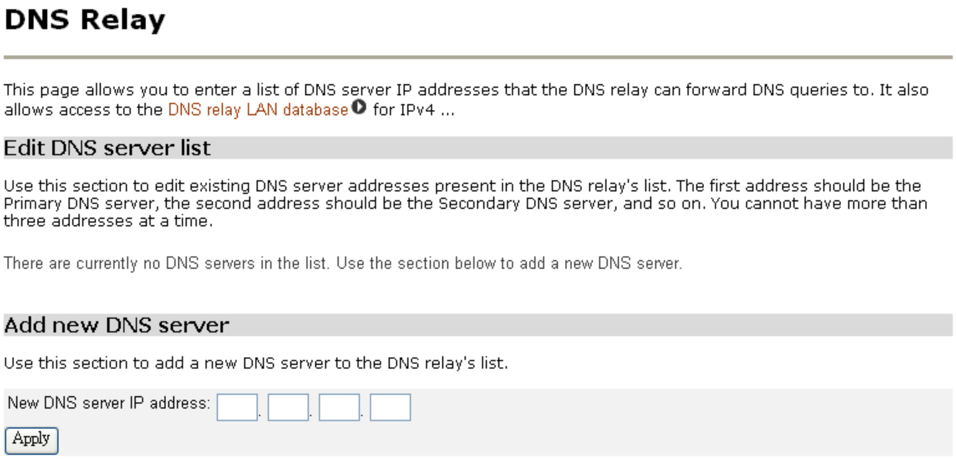
1. Type a search string in the *Domain search order:* text box.

2. Click on Add. The search string is displayed in the *Domain search order* table. You can add a maximum of six search strings. Each search string entry has a *Delete* button associated with it. Click on Delete to remove a string from this list.

DNS Relay

This option allows you to create, configure and delete DNS relay's primary and secondary DNS servers. DNS relay can forward DNS queries to the DNS servers on this list.

From the *Configuration* menu, click on *DNS Relay*. The following page is displayed:



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 for IPv4 ...

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.

There are currently no DNS servers in the list. Use the section below to add a new DNS server.

Add new DNS server

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

New DNS server IP address: □ . □ . □ . □

Apply

Configuring the DNS relay list

1. In the *Add new DNS server* section, type an address in the *New DNS server IP address* text box.

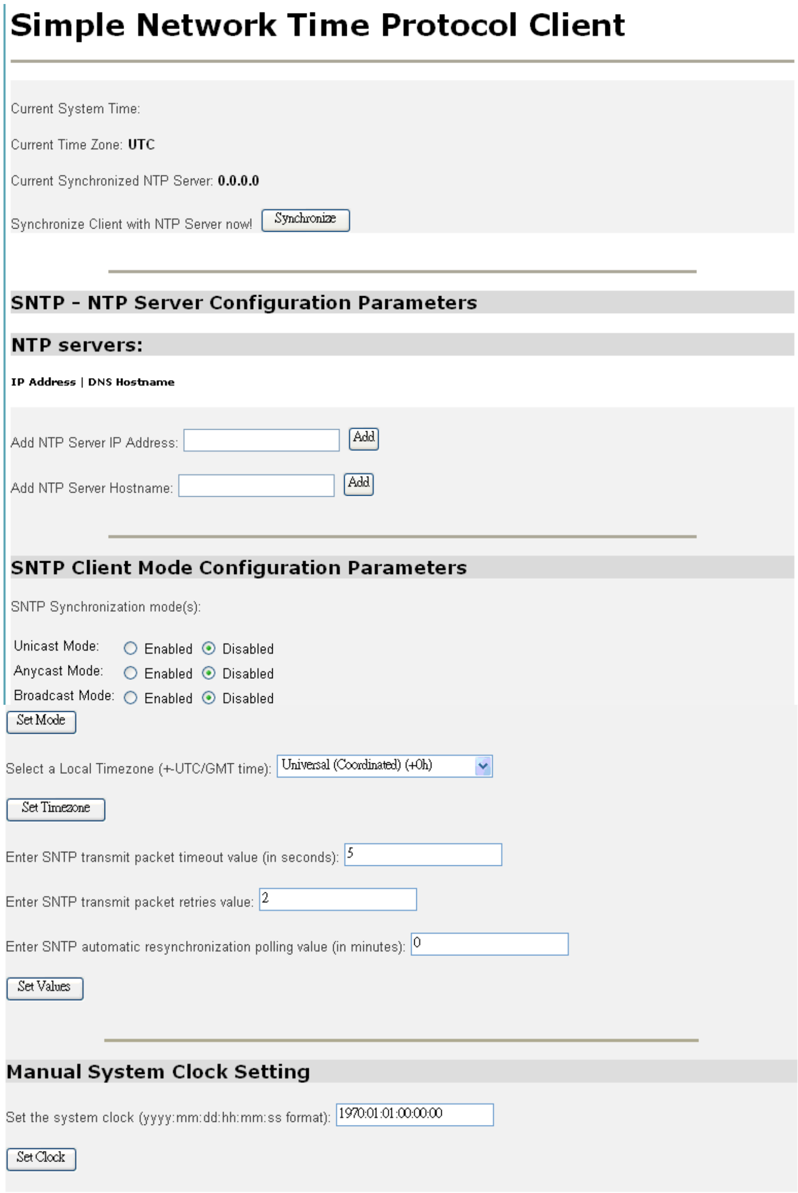
2. Click on Apply. The address is displayed in the *Edit DHCP server list* section. To edit an entry, click on an IP address and type a new entry, then click on Apply. To delete an entry, check the *Delete?* Box for a IP address, then click on Apply.

SNTP Client

The option allows you to:

- Synchronize Client with NTP Server
- Configure SNTP-NTP Server
- Set the system clock

From the *Configuration* menu, click on *SNTP client*. The following page is displayed:



Simple Network Time Protocol Client

Current System Time:

Current Time Zone: **UTC**

Current Synchronized NTP Server: **0.0.0.0**

Synchronize Client with NTP Server now! Synchronize

SNTP - NTP Server Configuration Parameters

NTP servers:

IP Address | DNS Hostname

Add NTP Server IP Address: Add

Add NTP Server Hostname: Add

SNTP Client Mode Configuration Parameters

SNTP Synchronization mode(s):

Unicast Mode: ○ Enabled ● Disabled
Anycast Mode: ○ Enabled ● Disabled
Broadcast Mode: ○ Enabled ● Disabled

Set Mode

Select a Local Timezone (+-UTC/GMT time): Universal (Coordinated) (+0h)

Set Timezone

Enter SNTP transmit packet timeout value (in seconds): 5

Enter SNTP transmit packet retries value: 2

Enter SNTP automatic resynchronization polling value (in minutes): 0

Set Values

Manual System Clock Setting

Set the system clock (yyyy:mm:dd:hh:mm:ss format): 1970:01:01:00:00:00

Set Clock

Synchronize Client with NTP Server

Click on Synchronize to force the SNTP client to immediately synchronize the local time with the server located in the association list (if unicast) or, if anycast is enabled, initiate an anycast sequence to the network.

Note: to Synchronize Client with NTP Server, NTP servers, SNTP client mode, and local time zone should be pre-configured.

Configure SNTP-NTP Server

Type the NTP Server IP address in the text box of Add NTP Server IP Address, and then click on Add.

Type the NTP Server Hostname in the text box of Add NTP Sever Hostname, and then click on Add.

Configure SNTP Client Mode

Select SNTP Synchronization mode(s): This action enables/disables the STNP client in a particular time synchronous access mode. There are three modes to choose from, and each mode has enable and disable options:

Unicast mode:

- *Enable* - The mode uses a unicast server and the IP address or hostname in the SNTP server association list is used to synchronize the client time with the server. The SNTP client attempts to contact the specific server in the association in order to receive a timestamp when the *sntpclient sync* command is issued.
- *Disable* - The unicast server is removed from the association list.

Broadcast mode:

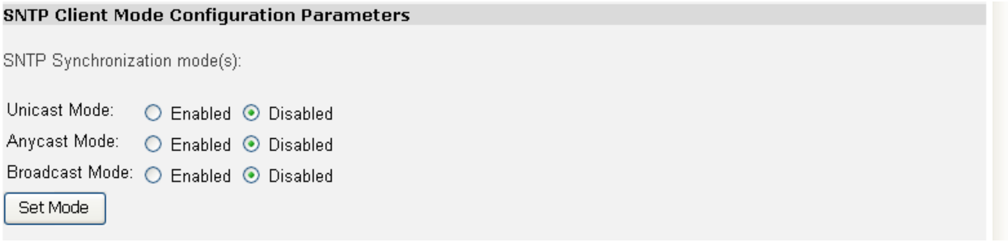
- *Enable* - Allows the SNTP client to accept time synchronization broadcast packets from an SNTP server located on the network, and update the local system time accordingly.
- *Disable* - Stops synchronization via broadcast mode.

Anycast Mode:

- *Enable* - The SNTP client sends time synchronized broadcast packets to the network and subsequently expects a reply from a valid timeserver. The client then uses the first reply it receives to establish a link for future sync operations in unicast mode. This server will then be added to the server association list. The client ignores any later replies from servers after the first one is received.

The enabled anycast mode takes precedence over any entries currently in the associations list when the *sntpclient sync* command is issued. The entry will then be substituted for any existing entry in the unicast association list.

- *Disable* - stops synchronization via anycast mode.



SNTP Client Mode Configuration Parameters

SNTP Synchronization mode(s):

Unicast Mode: ○ Enabled ● Disabled

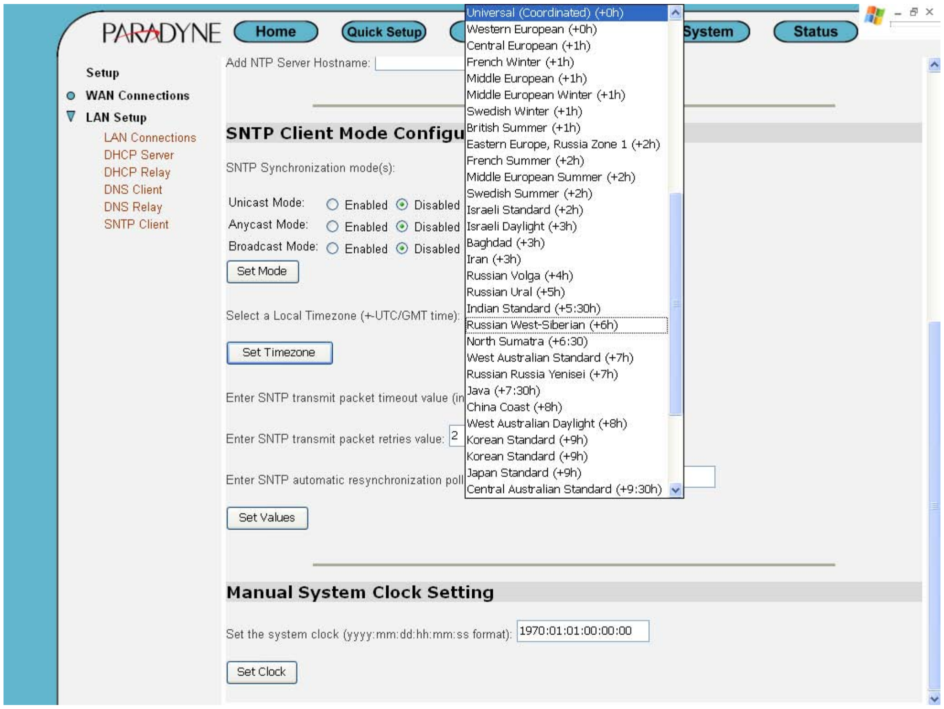
Anycast Mode: ○ Enabled ● Disabled

Broadcast Mode: ○ Enabled ● Disabled

Click on Set Mode to validate your setting after choosing the SNTP Synchronization mode.

Select a time zone:

Click on the local timezone drop down list and select a time zone. And then click on Set Timezone to validate your setting.



Add NTP Server Hostname:

SNTP Client Mode Configu

SNTP Synchronization mode(s):

Unicast Mode: ○ Enabled ● Disabled

Anycast Mode: ○ Enabled ● Disabled

Broadcast Mode: ○ Enabled ● Disabled

Select a Local Timezone (+-UTC/GMT time):

Enter SNTP transmit packet timeout value (in

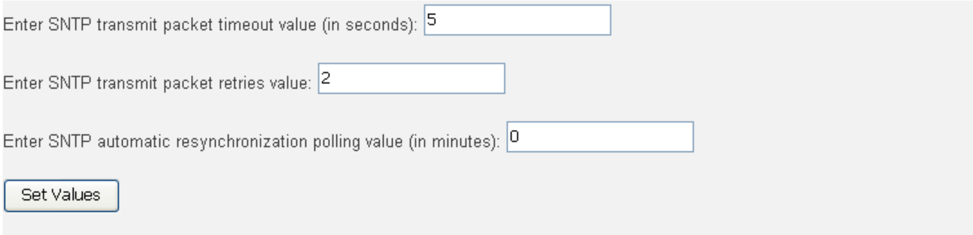
Enter SNTP transmit packet retries value: 2

Enter SNTP automatic resynchronization poll

Manual System Clock Setting

Set the system clock (yyyy:mm:dd:hh:mm:ss format): 1970:01:01:00:00:00

Enter SNTP transmit packet timeout value, SNTP transmit packet retries value, and SNTP automatic resynchronization polling value in their respective text boxes. Click on Set Values to validate your setting.



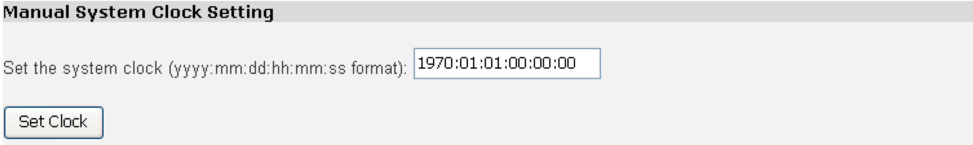
Enter SNTP transmit packet timeout value (in seconds): 5

Enter SNTP transmit packet retries value: 2

Enter SNTP automatic resynchronization polling value (in minutes): 0

Setting the System Clock

Enter the date and time with yyyy:mm:dd:hh:mm:ss format in the text box to set the system clock. Click on Set Clock to validate your setting.



Manual System Clock Setting

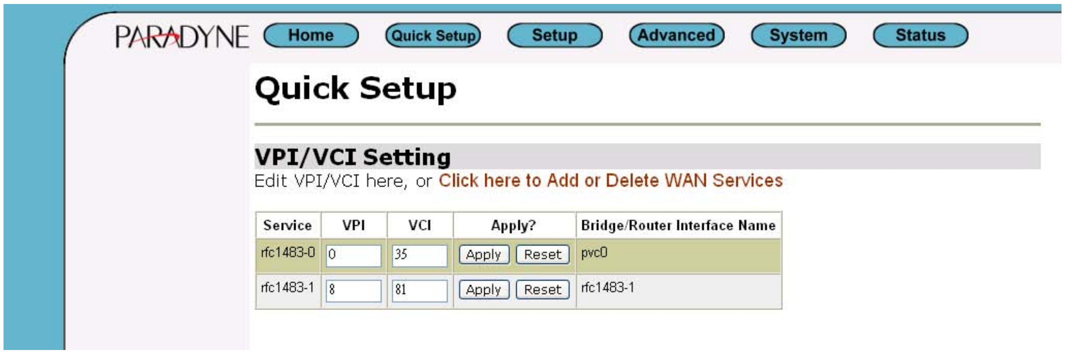
Set the system clock (yyyy:mm:dd:hh:mm:ss format): 1970:01:01:00:00:00

Note: if using manual system clock setting, the local time will follow the internal clock that you set.

Quick Setup page

The Quick Setup will guide you to configure virtual circuits in this device. To set VPI/VCI:

1. Enter the VPI and VCI for each service listed.
2. Click on Apply to submit your settings or Reset to clear your settings.
3. If to create or delete WAN services, click on the *Click here to Add or Delete WAN Services* link.



Quick Setup

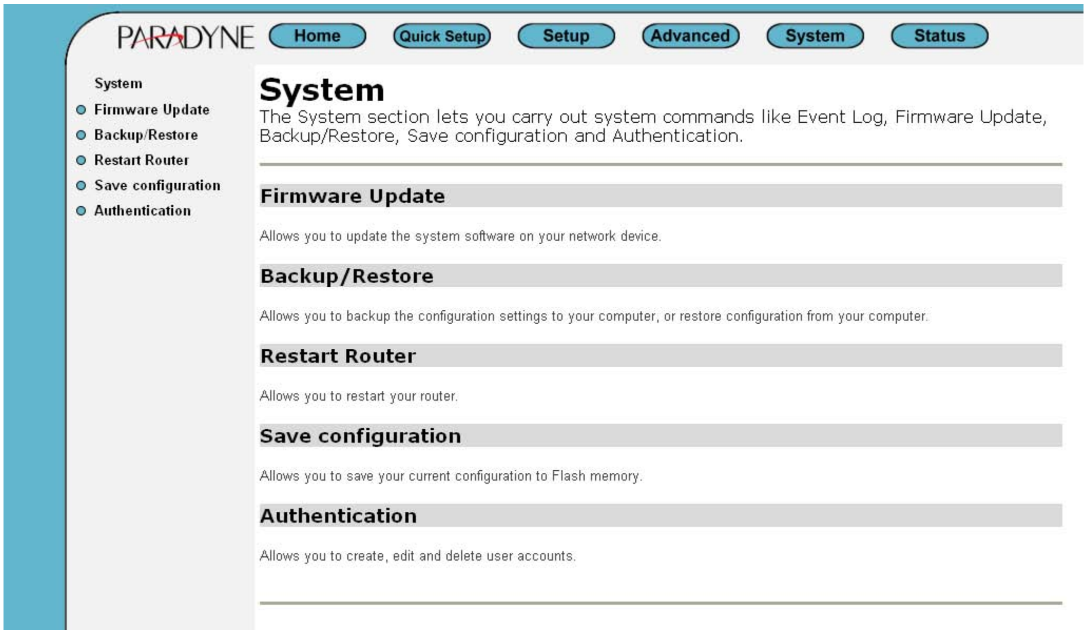
VPI/VCI Setting

Edit VPI/VCI here, or Click here to Add or Delete WAN Services

Service	VPI	VCI	Apply?	Bridge/Router Interface Name
rfc1483-0	0	35	Apply Reset	pvc0
rfc1483-1	8	81	Apply Reset	rfc1483-1

System Pages

Click on *System*, and the following screen appears:



System

The System section lets you carry out system commands like Event Log, Firmware Update, Backup/Restore, Save configuration and Authentication.

Firmware Update

Allows you to update the system software on your network device.

Backup/Restore

Allows you to backup the configuration settings to your computer, or restore configuration from your computer.

Restart Router

Allows you to restart your router.

Save configuration

Allows you to save your current configuration to Flash memory.

Authentication

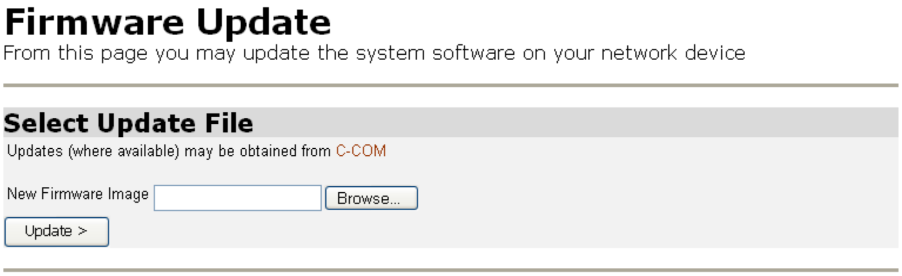
Allows you to create, edit and delete user accounts.

The System menu includes Firmare Update, Backup/Restore, Restart Router, Save configuration, and Authentication.

Firmware Update

This option allows you to upload firmware images to the router using HTTP.

1. From the System menu, click Firmware update. The following page is displayed:



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 C-COM

New Firmware Image [Browse...]

[Update >]

2. Type in the location of the new firmware image that you want to upload, or use [Browse...] to browse and select the file. Click on [Update >].

3. Once the file has been uploaded to the RAM of your device, it is written to Flash ROM. A status page is displayed confirming that the upload is complete and telling you how much of the file (in bytes and as a percentage) has been written to Flash ROM.

4. Once the file has been written to Flash ROM, the Firmware Update page is refreshed. The page confirms completion of the update and asks you to restart your router in order to use the new firmware. Click on Restart Router from the System menu.

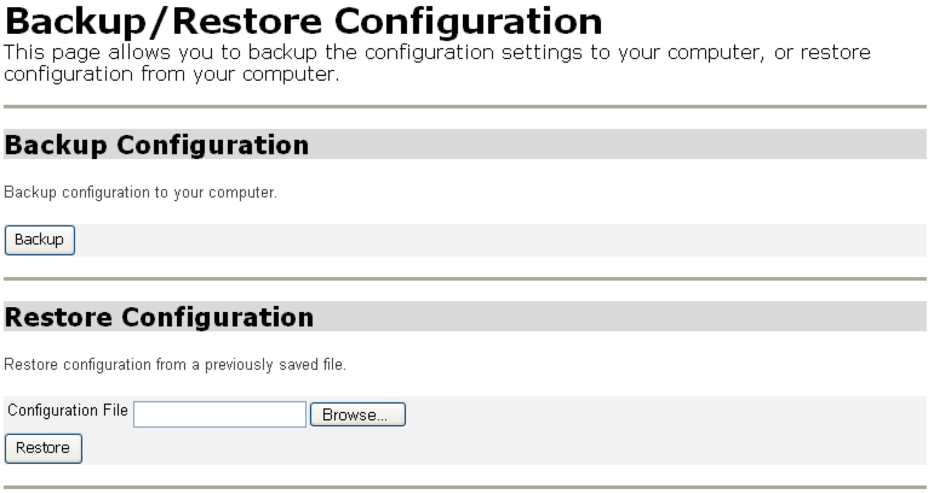
Note: Do not power off the device while updating firmware or saving your configuration. Powering off the router while updating the firmware might disable the router.

Backup/Restore

This page allows you to back up your configuration to, or restore it from, your PC.

Backing up your configuration:

1. From the *System* menu, click on *Backup/restore*. The following page is displayed:



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.

[Backup]

Restore Configuration

Restore configuration from a previously saved file.

Configuration File [Browse...]

[Restore]

2. From the *Backup Configuration* section, click on the [Backup] button. The *File Download* window is displayed. Click on [Save]. In the Save As window, select a file in which to save your backup configuration. Click on [Save].

Restoring your configuration

1. From the *System* menu, click on *Backup/restore*.

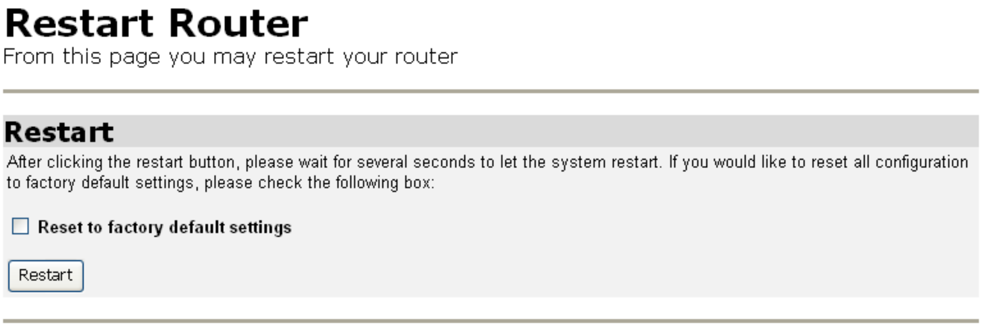
2. In the *Restore Configuration* section, click in the *Configuration File* text box and type the network path of the file that you wish to restore. If you do not know the path details, click on Browse... and locate the file using the *Choose file* box.

3. Click on Restore. The page is refreshed with a *Configuration Restored* message and details of the number of bytes uploaded.

Restart Router

This page allows you to restart your router. With the Reset box selected, it has the same effect as resetting your router by pressing the Reset button on the hardware.

1. From the System menu, click on *Restart Router*. The following page is displayed:



Restart Router

From this page you may restart your router

Restart

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

☐ **Reset to factory default settings**

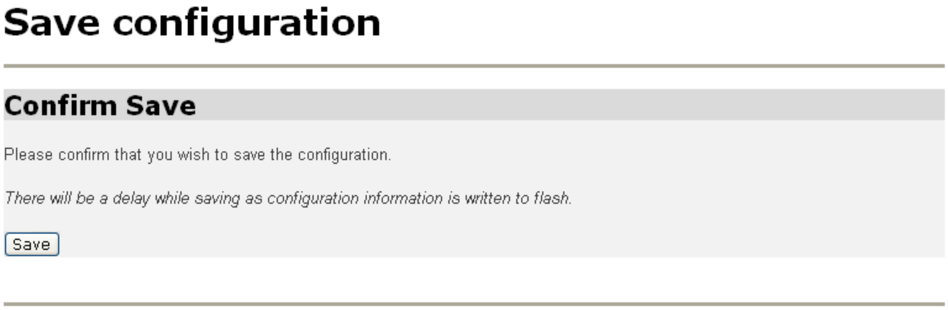
2. Click on Restart to reset your router. The *Restart* page also provides you with the option of restarting and restoring the factory default settings. Click in the *Reset to factory default settings* box to check it, and then click on the Restart. Read the console status output to check how the reset is progressing.

3. Once the login and password prompt is displayed at the console, you can login as usual (with login = *admin*, password = *admin*), then refresh the browser that is running EmWeb. The *Status* page is displayed when your router has been reset.

Save configuration

To save your current configuration to flash ROM:

1. From the System menu, click on *Save configuration*. The following page is displayed:



Save configuration

Confirm Save

Please confirm that you wish to save the configuration.

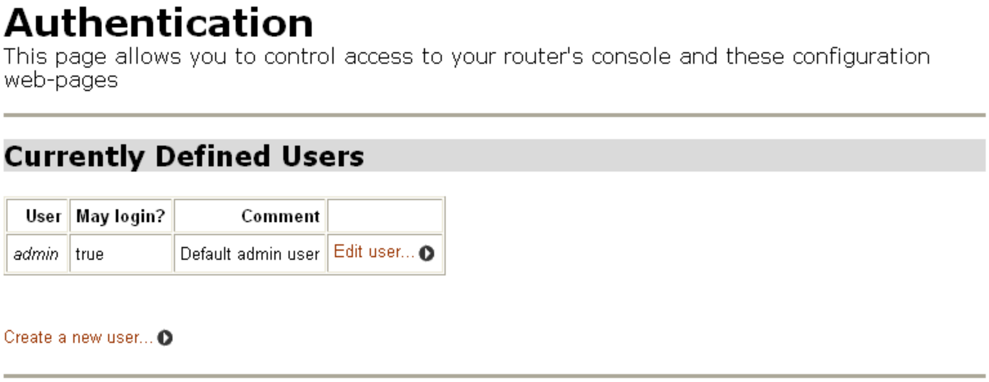
There will be a delay while saving as configuration information is written to flash.

2. Click on Save to save your current configuration in the device.

After a short time the configuration is saved and the following confirmation message is displayed: Saved information model to file //flashfs/im.conf

Authentication

This option allows you to administer accounts for users who access the router. From the Configuration menu, click on *Authentication*. The following page is displayed:



Authentication

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

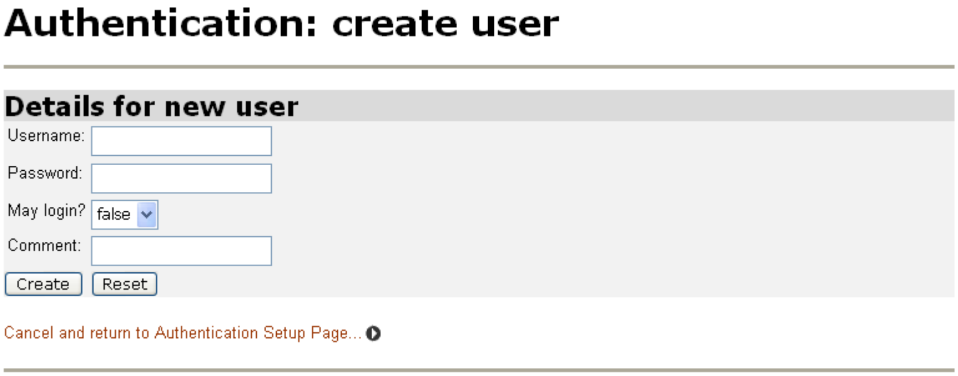
Currently Defined Users

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

Create a new user...

Creating a new login account

1. Click on the *Create a new user*. The following page is displayed:



Authentication: create user

Details for new user

Username:

Password:

May login? false

Comment:

Cancel and return to Authentication Setup Page...

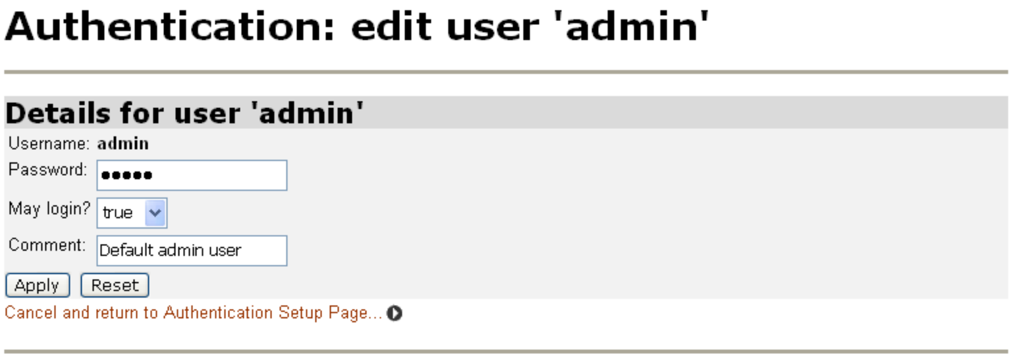
2. Type details for the new user into the username, password and comment text boxes, and select a May login? Option:

- true means that the user can login
- false means that the user can not login

3. Click on the Create button. The Authentication page is displayed. The table now contains details for the user that you have just created.

Editing or Deleting a Login Account

1. The Authentication page table contains an Edit user hyperlink for each user account entry. Click on a link. The following page is displayed:



Authentication: edit user 'admin'

Details for user 'admin'

Username: **admin**

Password: ●●●●●

May login? true

Comment: Default admin user

Apply Reset

Cancel and return to Authentication Setup Page...

This page allows you to:

• Update details for a specific user account. Modify the necessary text boxes then click on the Apply button.

• Delete a user account. Click on the Delete this user button.

2. Once you have edited or deleted a user account, the Authentication page is displayed and the table reflects any changes that you have made on the edit user page.

Advanced Pages

The Advanced pages allow you to configure:

- Security
- IP Routes
- Bridge
- VPN
- SNMP
- Port

These options are introduced in the following pages.

Security

Security allows you to:

- Enable Security
- Configure Security interfaces
- Configure triggers

NAT allows you to:

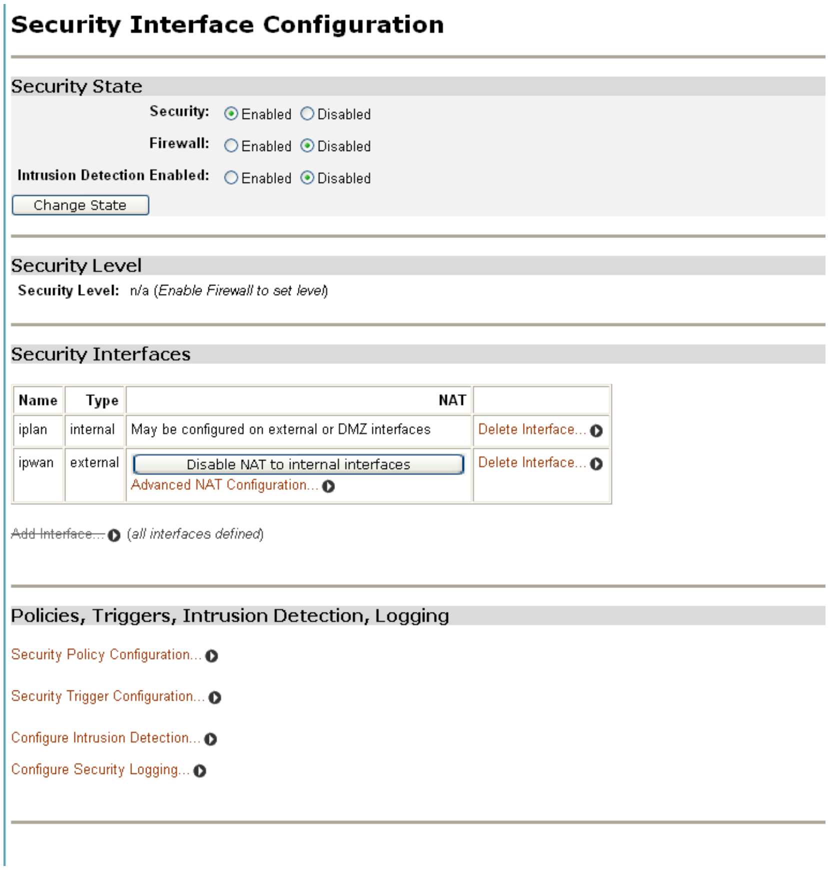
- Enable NAT between interfaces
- Configure global addresses
- Configure reserved mapping

Firewall allows you to:

- Enable Firewall and Firewall Intrusion Detection settings
- Set the Firewall security level
- Configure Firewall policies, portfilters and validators

- Configure Intrusion Detection settings

Via the Advanced menu, click on *Security* and then the following page is displayed:



Security Interface Configuration

Security State

Security: ● Enabled ○ Disabled

Firewall: ○ Enabled ● Disabled

Intrusion Detection Enabled: ○ Enabled ● Disabled

Change State

Security Level

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

Security Interfaces

Name	Type	NAT	
iplan	internal	May be configured on external or DMZ interfaces	Delete Interface... ▶
ipwan	external	Disable NAT to internal interfaces Advanced NAT Configuration... ▶	Delete Interface... ▶

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

Policies, Triggers, Intrusion Detection, Logging

Security Policy Configuration... ▶

Security Trigger Configuration... ▶

Configure Intrusion Detection... ▶

Configure Security Logging... ▶

Enabling Security

You must enable *Security* before you can enable *Firewall* and/or *Intrusion Detection*. In the *Security State* section:

1. Click on the *Security Enabled* radio button.

2. Click on Change State to update the *Security State* section.

Enabling Firewall and/or Intrusion Detection:

You must create a security interface before you can enable Firewall and/or Intrusion Detection.

Once you have created a security interface:

1. Click on the Firewall Enabled and/or Intrusion Detection Enabled radio buttons.

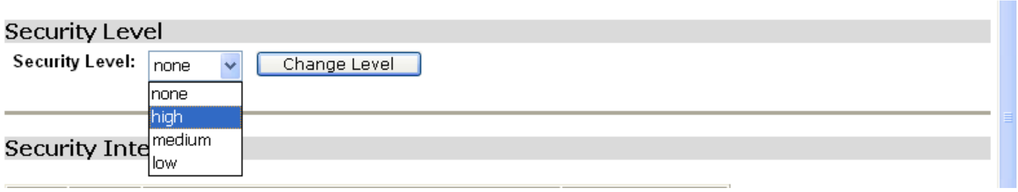
2. Click on Change State to update the *Security State* section.

Setting a default security level:

You must have *Security* and *Firewall* enabled in order to set a default Security level.

1. From the *Security Level* section, click on the *Security Level* drop-down list.

2. Click on the level that you want to set: *none*, *high*, *medium* or *low*.



Security Level

Security Level: none

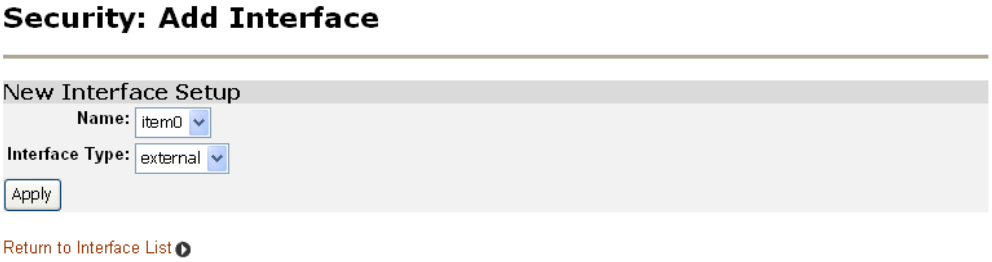
3. Click on the Change Level button.

Configuring security interfaces

Security interfaces are based on existing LAN services. You must create a LAN service for every security interface that you want to configure.

For details on how to create LAN services:

1. From the Security Interfaces section, click on Add Interface. Add Interface page is displayed:



Security: Add Interface

New Interface Setup

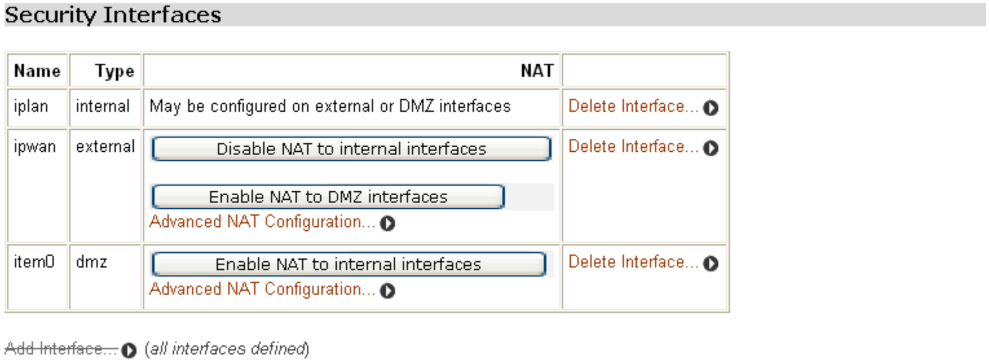
Name: item0

Interface Type: external

2. Click on the *Name* drop-down list and select the LAN service that you want to base your security interface on.

3. Click on the *Interface Type* drop-down list and specify what kind of interface it is, depending on how it connects to the network; *external*, *internal* or *DMZ*.

4. Click on Apply. The Security page is displayed. The *Security Interfaces* section contains a table that displays information about each security interface that you have created:



Security Interfaces

Name	Type	NAT	
iplan	internal	May be configured on external or DMZ interfaces	Delete Interface...
ipwan	external	Disable NAT to internal interfaces Enable NAT to DMZ interfaces Advanced NAT Configuration...	Delete Interface...
item0	dmz	Enable NAT to internal interfaces Advanced NAT Configuration...	Delete Interface...

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

- *Name* - name of LAN service that the security interface is based on
- *Type* of network connection specified
- *NAT* setting. It contains hyperlinks that allow you to configure NAT. See *Configuring NAT*
- *Delete Interface...* hyperlink. Click on this to display the *Security: Delete Interface*

page. Check the interface details, then click on the *Delete* button.

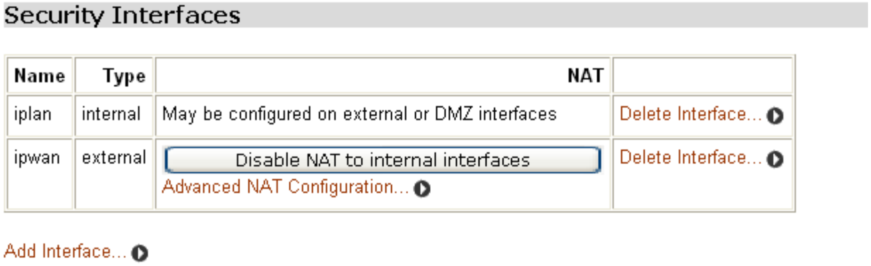
Configuring NAT

To configure NAT, you need to:

1. Enable Security; see the *Enabling Security* section.

2. Create at least two different security interface types based on existing LAN services; see the *Configuring Security Interfaces* section.

Once you have created more than one security interface, the *NAT* column in the *Security Interfaces* table tells you that you can enable NAT between the existing security interface and a network interface type. For example, if you create an external interface and an internal interface, your table will look like this:



Security Interfaces

Name	Type	NAT	
iplan	internal	May be configured on external or DMZ interfaces	Delete Interface...
ipwan	external	Disable NAT to internal interfaces Advanced NAT Configuration...	Delete Interface...

Add Interface...

The NAT column for the external interface tells you that you can enable NAT to internal interfaces. If you also had a DMZ interface configured, this column would also include an *Enable NAT to DMZ interfaces* button.

4. To enable NAT between the external interface and the internal interface type, click on Enable NAT to internal interfaces. The *Security* page is refreshed and NAT is enabled. To disable NAT between these interfaces, click on Disable NAT to internal interfaces.

Once you have enabled NAT between interfaces, you can:

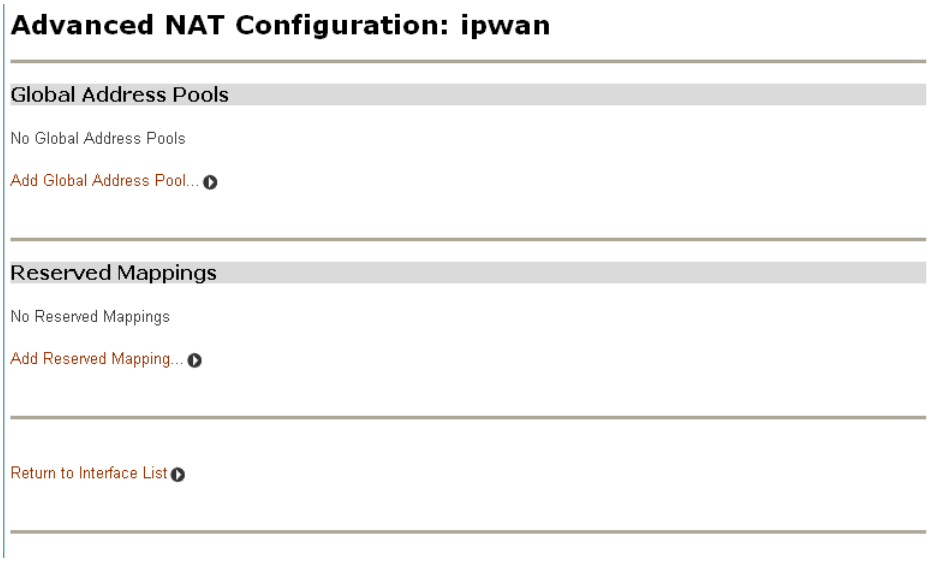
- Configure global addresses; see the Configuring NAT global addresses section.
- Configure reserved mapping; see the Configuring NAT reserved mapping section.

Configuring NAT Global Addresses

Global address pools allow you to create a pool of outside network addresses that is visible outside your network. Before you can configure global addresses, you need to configure NAT. See *Configuring NAT Section*

If you want to set up a global address pool on your existing NAT enabled interfaces:

1. From the *NAT Security Interfaces* table, click on the *Advanced NAT Configuration* hyperlink for the interface that you want to add a global pool to. The following page is displayed:



Advanced NAT Configuration: ipwan

Global Address Pools

No Global Address Pools

Add Global Address Pool...

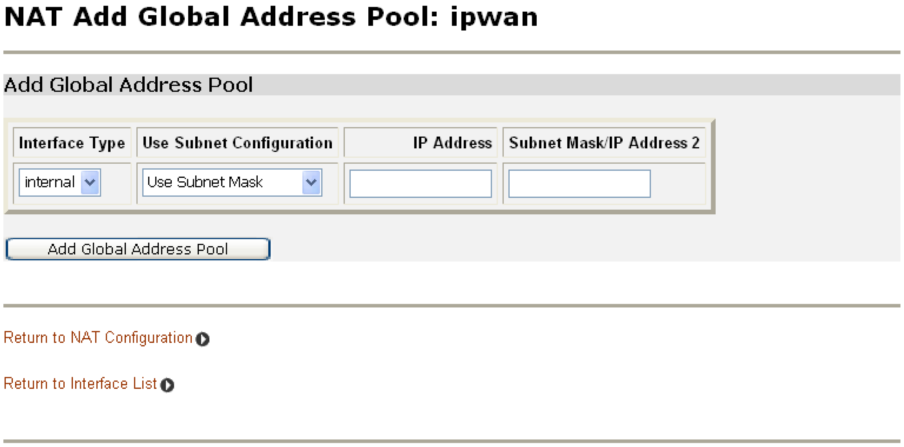
Reserved Mappings

No Reserved Mappings

Add Reserved Mapping...

Return to Interface List

2. Click on *Add Global Address Pool.* The following page is displayed:



NAT Add Global Address Pool: ipwan

Add Global Address Pool

Interface Type	Use Subnet Configuration	IP Address	Subnet Mask/IP Address 2
internal	Use Subnet Mask		

Return to NAT Configuration

Return to Interface List

3. This page allows you to create a pool of network IP addresses that are visible outside your network. Add values for the following table entries:

• *Interface type*. The internal address type that you want to map your external global IP addresses to. Click on the drop-down list and select an interface type.

• *Use Subnet Configuration*. There are two ways to specify a range of IP addresses. You can either *Use Subnet Mask* (specify the subnet mask address of the IP address) or *Use IP Address Range* (specify the first and last IP address in the range). Click on the drop-down list and select a method.

• Type in the *IP Address* that is visible outside the network

• *Subnet Mask/IP Address 2*. The value you specify here depends on the subnet configuration that you are using. If you chose *Use Subnet Mas*k, type in the subnet mask of the IP address. If you chose *Use IP Address Range*, type in the last IP address in the range of addresses that make up the global address pool.

4. Once you have configured the table, click on Add Global Address Pool. The table is refreshed and the global address pool is added to your NAT configuration. To delete a global address pool, click on the *Delete* hyperlink, then click on the *Delete Global Address Pool* button.

Click on Return to Interface List to display the Security Interface Configuration page.

To create a reserved mapping, click on the Add Reserved Mapping hyperlink. See the Configuring NAT Reserved Mapping section.

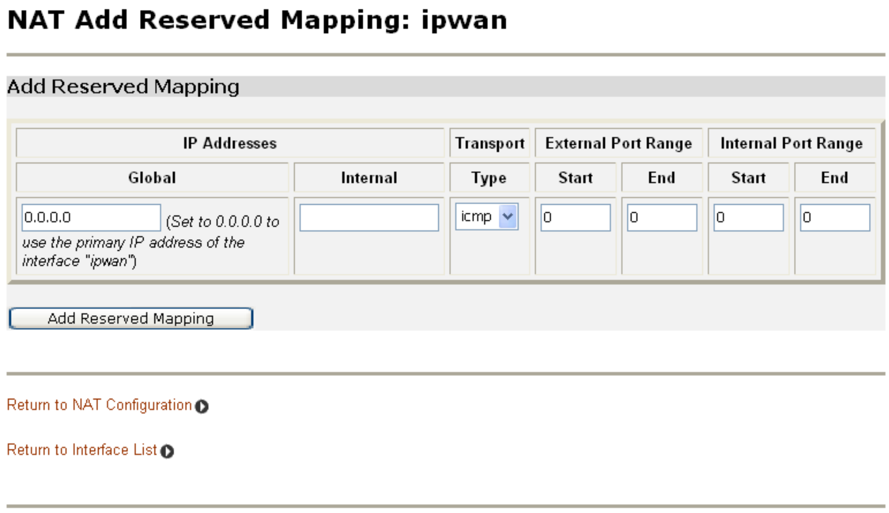
Configuring NAT Reserved Mapping

Reserved mapping allows you to map an outside security interface or an IP address from a global pool to an individual IP address inside the network. Mapping is based on transport type and port number. Before you can configure reserved mapping, you need to configure NAT. See the Configuring NAT section.

If you want to set up a reserved mapping on your existing NAT enabled interfaces:

1. From the NAT Security Interfaces table, click on the Advanced NAT Configuration hyperlink for the interface that you want to add reserved mapping to. The Advanced NAT Configuration page is displayed. (See the Advanced NAT configuration section.)

2. Click on the Add Reserved Mapping hyperlink. The following page is displayed:



NAT Add Reserved Mapping: ipwan

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 "ipwan")*		icmp	0	0	0	0

3. This page allows you to configure your reserved mapping. Add specific values for the following table entries:

• Global IP Address. If you are mapping from a global IP address, type the address here. If you are mapping from a security interface, type 0.0.0.0.

• Internal IP Address. Specify the IP address of an individual host inside your network.

• Transport Type. Specify the transport type that you want to map from the outside interface to the inside.

• Port Number. Specify the port number that your transport uses.

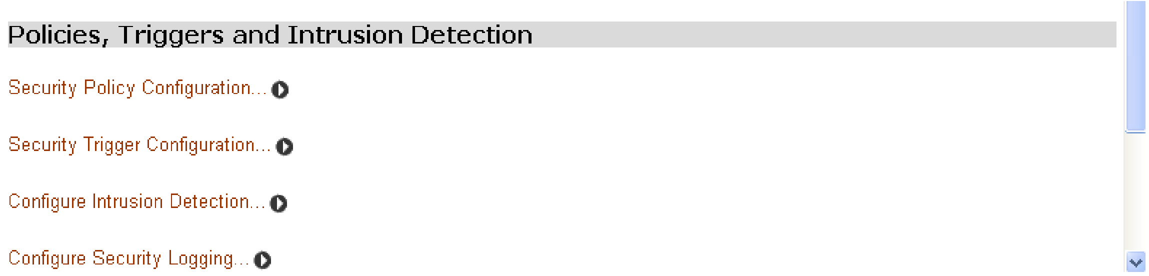
4. Once you have configured the table, click on Add Reserved Mapping. The table is refreshed and the reserved mapping is added to your NAT configuration.

To delete a reserved mapping setup, click on the Delete hyperlink, and then click on Delete Reserved Mapping.

Click on *Return to Interface List* to display the Security Interface Configuration page.

Configuring Firewall Policies

To configure firewall policies, click on the *Security Policy Configuration* link under Policy, Triggers and Intrusion Detection as shown.



Policies, Triggers and Intrusion Detection

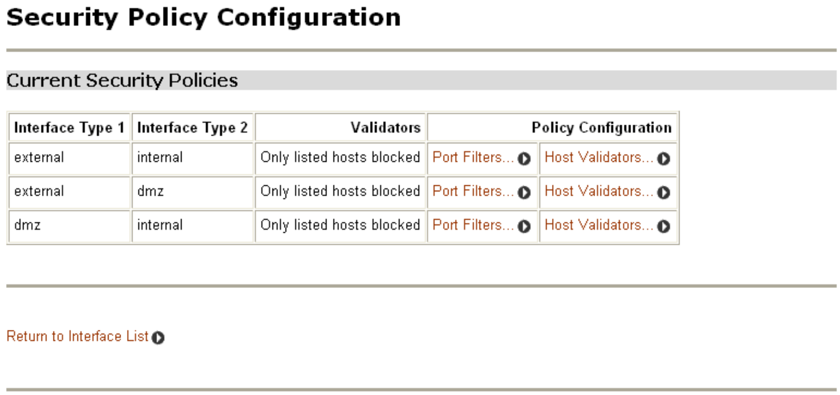
Security Policy Configuration...

Security Trigger Configuration...

Configure Intrusion Detection...

Configure Security Logging...

A table is displayed containing details of each Firewall policy.



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...
external	dmz	Only listed hosts blocked	Port Filters...	Host Validators...
dmz	internal	Only listed hosts blocked	Port Filters...	Host Validators...

Return to Interface List

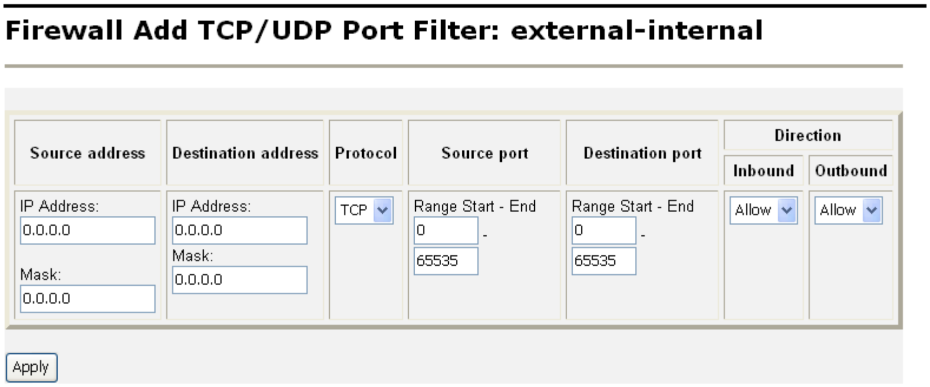
You can now configure the policies to include port filters and validators. See the Configuring portfilters and Configuring Validators sections.

A port filter is an individual rule that determines what kind of traffic can pass between two interfaces specified in an existing policy. This section assumes that you have followed the instructions in Configuring Firewall Policies section.

To configure a port filter:

1. From the *Current Firewall Policies* table, click on the *Port Filters* link for the policy that you want to configure. The page displayed contains three *Add Filter* hyperlinks that allow you to create three different kinds of port filter.

- For a TCP/UDP port filter, click on *Add TCP or UDP Filter*. The following page is displayed:

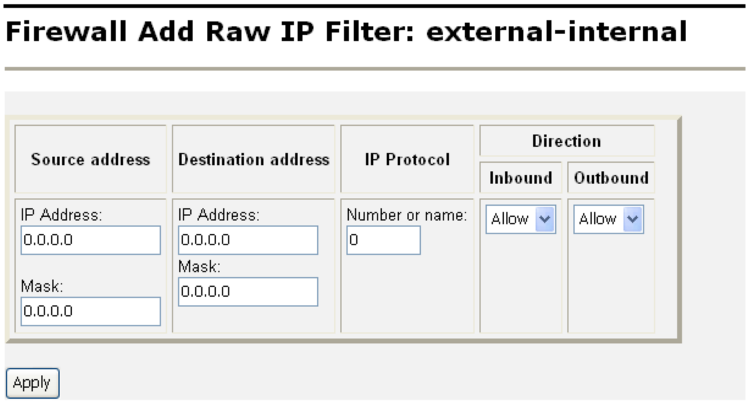


Firewall Add TCP/UDP Port Filter: external-internal

Source address	Destination address	Protocol	Source port	Destination port	Direction	
					Inbound	Outbound
IP Address: 0.0.0.0 Mask: 0.0.0.0	IP Address: 0.0.0.0 Mask: 0.0.0.0	TCP	Range Start - End 0 - 65535	Range Start - End 0 - 65535	Allow	Allow

Specify the start and end of the port range for the TCP/UDP protocol that you want to filter. Then select TCP or UDP protocol from the Protocol drop-down list. After that, use the Direction drop-down lists to specify whether you want to allow or block inbound traffic, and allow or block outbound traffic. Click on Apply. The Firewall Port Filters page is displayed, containing details of the TCP port filter that you have just added.

- For a non-TCP/UDP port filter click on *Add Raw IP Filter*. The following page is displayed:



Firewall Add Raw IP Filter: external-internal

Source address	Destination address	IP Protocol	Direction	
			Inbound	Outbound
IP Address: 0.0.0.0 Mask: 0.0.0.0	IP Address: 0.0.0.0 Mask: 0.0.0.0	Number or name: 0	Allow	Allow

Specify the protocol number in the Transport Type text box. For example, for IGMP, enter protocol number 2. Then use the Direction drop-down lists to specify whether you want to allow or block inbound traffic, and allow or block outbound traffic. Click on Apply. The Firewall Port Filters page is displayed, containing details of the IP port filter that you have just added.

2. Each port filter displayed in the Firewall Port Filters page has a *Delete* hyperlink assigned to it. To delete a port filter, click on this link, then at the confirmation page, click on Delete. The port filter is removed from the Firewall configuration.

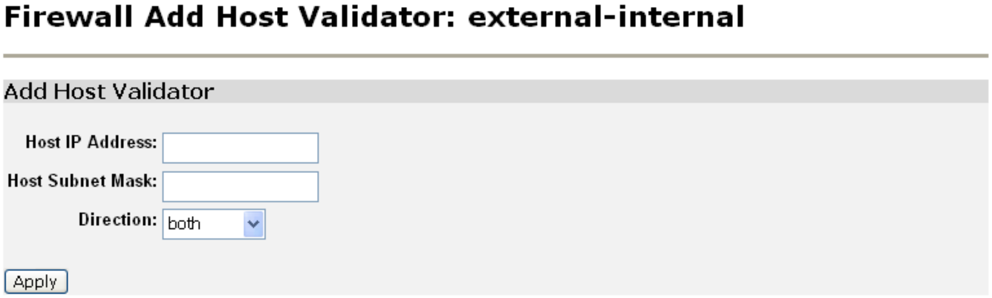
Configuring validators

A validator allows or blocks traffic based on the source and destination IP address and subnet mask. Traffic will be allowed or blocked depending on the validator configuration specified when the policy was created. See the Configuring Firewall Policies section. This section assumes that you have previously followed the instructions in that section.

To configure a validator:

1. From the Current Firewall Policies table, click on the *Host Validators* link for the policy that

you want to configure. The Configure Validators page is displayed. Click on the *Add Host Validator* link. The following page is displayed:



Firewall Add Host Validator: external-internal

Add Host Validator

Host IP Address:

Host Subnet Mask:

Direction: both

Apply

2. In the Host IP Address text box, type the IP address that you want to allow/block.

3. In the Host Subnet Mask text box, type the IP mask address. If you want to filter a range of addresses, you can specify a mask (for example, 255.255.255.0). If you want to filter a single IP address, use the specific IP address mask (255.255.255.255).

4. Click on the Direction drop-down list and select the direction of traffic that you want the validator to filter.

5. Click on Apply. The Configure Validators page is displayed, containing details of the host validator that you have just added.

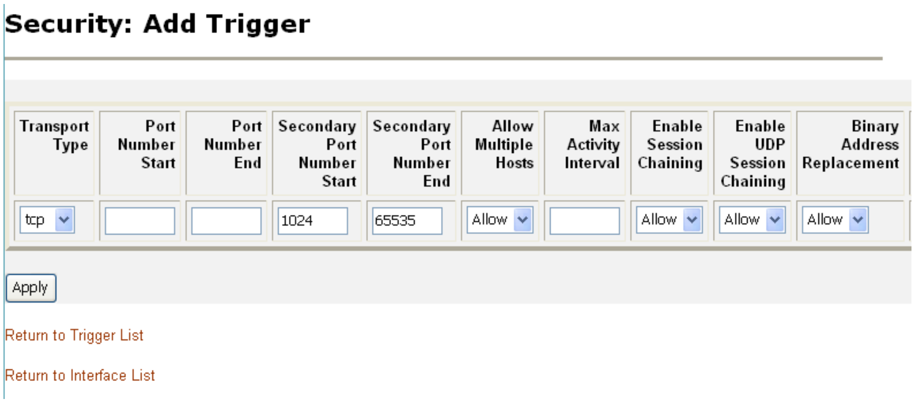
6. Each port filter displayed in the Configure Validators page has a Delete Host Validator hyperlink assigned to it. To delete a validator, click on this link, then at the confirmation page, click on the Delete Host Validator button. The validator is removed from the Firewall configuration.

Configuring Triggers

A trigger allows an application to open a secondary port in order to transport packets. Two common applications that require secondary ports are FTP and NetMeeting. This section assumes that you have followed the instructions in Enabling Security section.

To configure a trigger:

1. Go to the Policies, Triggers and Intrusion Detection section of the Security Interface Configuration. Click on Trigger Configuration. The Firewall Trigger Configuration page is displayed, at first with no triggers defined. Click on the New Trigger link. The following page is displayed:



Security: Add Trigger

Transport Type	Port Number Start	Port Number End	Secondary Port Number Start	Secondary Port Number End	Allow Multiple Hosts	Max Activity Interval	Enable Session Chaining	Enable UDP Session Chaining	Binary Address Replacement
tcp			1024	65535	Allow		Allow	Allow	Allow

Apply

Return to Trigger List

Return to Interface List

2. Configure the trigger as follows:

a. Transport Type. Select a transport type from the drop-down list, depending on whether you are adding a trigger for a TCP or a UDP application.

b. Port Number Start. Type the start of the trigger port range that the primary session uses.

c. Port Number End. Type the end of the trigger port range that the primary session uses.

d. Allow Multiple Hosts. Select allow if you want a secondary session to be initiated to or from different remote hosts. Select block if you want a secondary session to be initiated only to or from the same remote host.

e. Max Activity Interval. Type the maximum interval time (in milliseconds) between the use of secondary port sessions.

f. Enable Session Chaining. Select Allow or Block depending on whether you want to allow multi-level TCP session chaining.

g. Enable UDP Session Chaining. Select Allow or Block depending on whether you want to allow multi-level UDP and TCP session chaining. Set Enable Session Chaining to Allow to enable it.

h. Binary Address Replacement. Select Allow or Block depending on whether you want to use binary address replacement on an existing trigger.

i. Address Translation Type. Specify what type of address replacement is set on a trigger. Set Binary Address Replacement to Allow to enable it.

3. Once you have configured the trigger, click on Apply. The Firewall Trigger Configuration page is displayed, containing details of the trigger that you have just configured.

4. Each trigger displayed in the Firewall Trigger Configuration page has a Delete hyperlink assigned to it. To delete a trigger, click on this link, then at the confirmation page, click on the Delete button. The Firewall Trigger Configuration page is displayed with details of the deleted trigger removed. There are two hyperlinks on the page:

a. To add a new trigger, click on *New Trigger*.

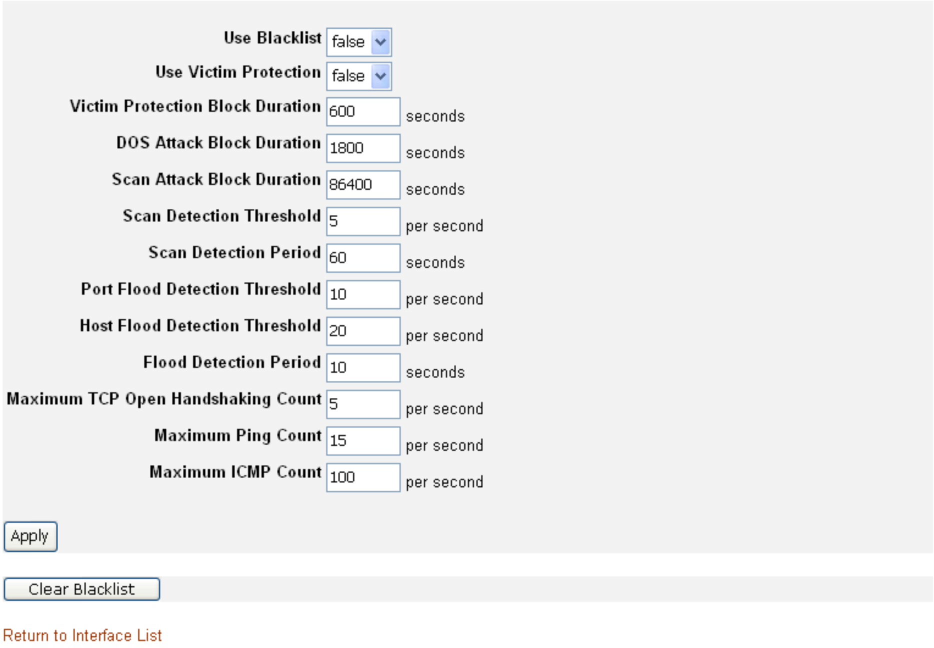
b. To display the Security Interface Configuration page, click on *Return to Interface List*.

Configuring Intrusion Detection Settings

Intrusion Detection settings allow you to protect your network from intrusions such as denial of service (DOS) attacks, port scanning, and web spoofing. This section assumes that you have followed the instructions in the *Enabling Security section* and the *Enabling Firewall and/or Intrusion Detection section*.

To configure Intrusion Detection settings:

1. Go to the Policies, Triggers and Intrusion Detection section of the Security Interface Configuration page. Click on Configure Intrusion Detection. The Firewall Configure Intrusion Detection page is displayed:



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	5	per second
Maximum Ping Count	15	per second
Maximum ICMP Count	100	per second

The values displayed on the Firewall Configure Intrusion Detection page are the default values.

2 . Configure Intrusion Detection as follows:

a. Use Blacklist. Select true or false depending on whether you want external hosts to be blacklisted if the Firewall detects an intrusion from that host. Click on the Clear Blacklist button at the bottom of the page to clear blacklisting of an external host.

The Security Interface Configuration page is displayed.

b. Use Victim Protection. Select true or false depending on whether you want to protect a victim from an attempted web spoofing attack.

c. DOS Attack Block Duration. Type the length of time (in seconds) that the Firewall blocks suspicious hosts for once a DOS attack attempt has been detected.

d. Scan Attack Block Duration. Type the length of time (in seconds) that the Firewall blocks suspicious hosts for after it has detected scan activity.

e. Victim Protection Block Duration. Type the length of time (in seconds) that the Firewall blocks packets destined for the victim of a spoofing style attack.

f. Maximum TCP Open Handshaking Count. Type in the maximum number of unfinished TCP handshaking sessions (per second) that are allowed by Firewall before a SYN Flood is detected.

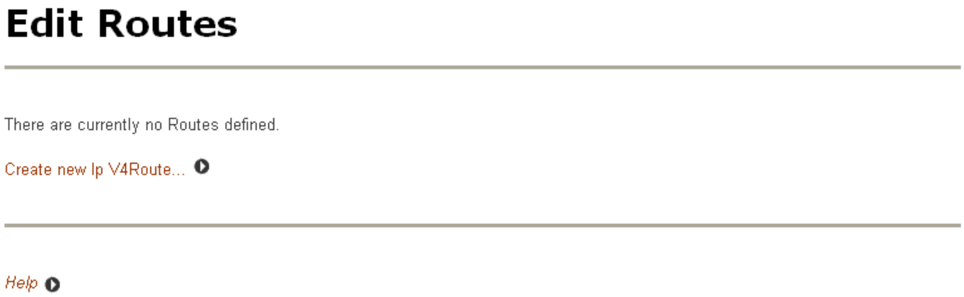
g. Maximum Ping Count. Type in the maximum number of pings (per second) that are allowed before the Firewall detects an Echo Storm DOS attack.

h. Maximum ICMP Count. Type in the maximum number of ICMP packets (per second) that are allowed by the Firewall before an ICMP Flood DOS is detected.

3. Once you have configured Intrusion Detection, click on Apply. The Intrusion Detection settings are applied to the Firewall, and the Security Interface Configuration page is displayed.

IP Routes

This option allows you to create static IP routes to destination addresses via an IP interface name or a Gateway address. From the *Advanced* menu, click on *IP routes*. The *Edit Routes* page is displayed:



Edit Routes

There are currently no Routes defined.

Create new Ip V4Route... ●

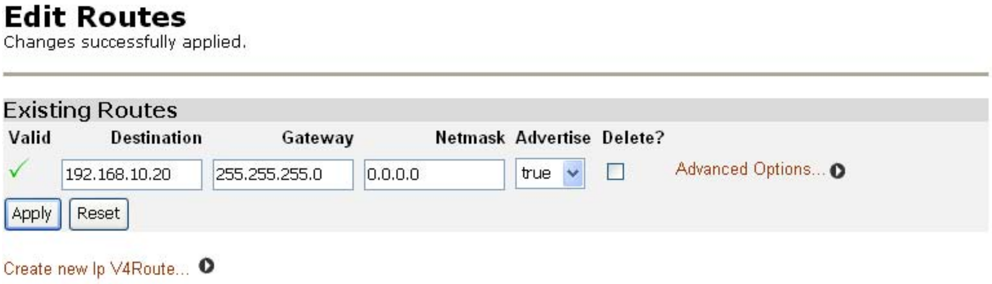
Help ●

This page lists the following information about existing routes:

- Whether the route is valid or invalid
- Destination IP address
- Gateway address
- Netmask address
- Whether the route is advertised via RIP (true or false)

Editing a route

1. To edit the destination, gateway and netmask address of a route, Click in the relevant text box, update the information then click on Apply.



Edit Routes

Changes successfully applied.

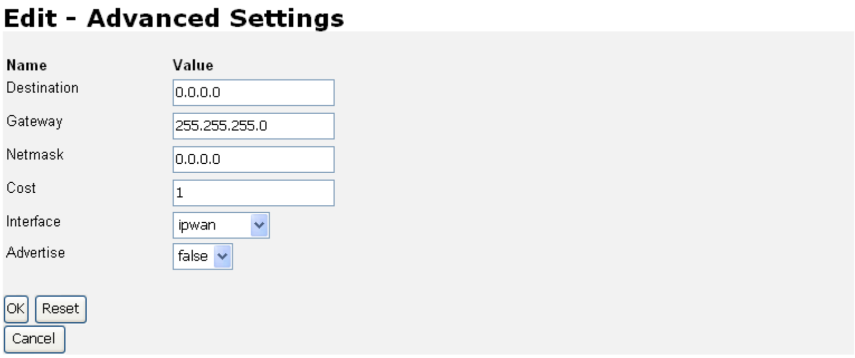
Existing Routes

Valid	Destination	Gateway	Netmask	Advertise	Delete?	
✓	192.168.10.20	255.255.255.0	0.0.0.0	true	□	Advanced Options... ●

Apply Reset

Create new Ip V4Route... ●

2. To edit the cost, interface setting, or advertise status for the route, click on the *Advanced Options* hyperlink for a specific route and update the relevant information. Click on OK.



Edit - Advanced Settings

Name	Value
Destination	0.0.0.0
Gateway	255.255.255.0
Netmask	0.0.0.0
Cost	1
Interface	ipwan
Advertise	false

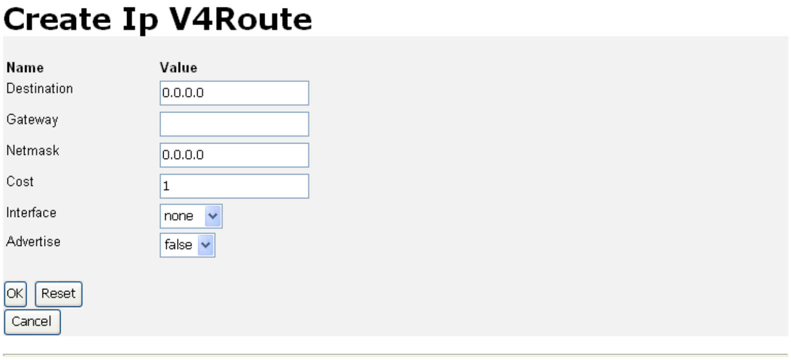
Deleting a route

1. To delete an existing route, check in the *Delete box* for a specific route.

2. Click on Apply.

Creating an IP V4 Route

1. Click on the *Create new Ip V4 Route* hyperlink. The following page is displayed.

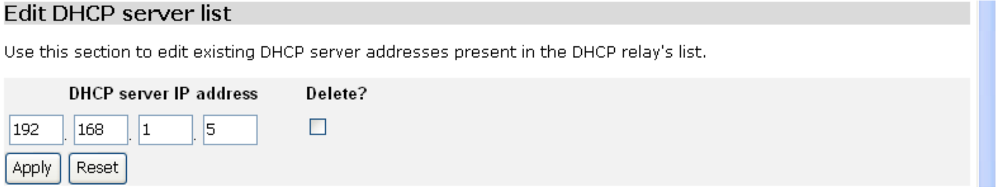


Create Ip V4Route

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

2. Complete the Create IP v4 Route form in order to configure the route.

3. When you have typed the details, click onOK. The *Edit Routes* page is displayed. The table now contains details of the route that you have just created.



Edit DHCP server list

Use this section to edit existing DHCP server addresses present in the DHCP relay's list.

DHCP server IP address	Delete?
192 . 168 . 1 . 5	□

Bridge

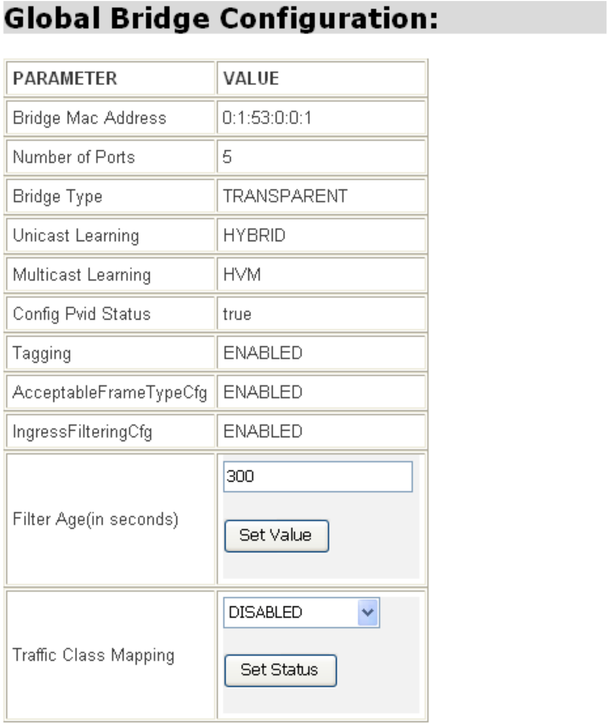
From the Advanced menu, click on Bridge to display the Bridge page.

This page lists the following bridge information:

- Global bridge configuration
- VLAN configuration
- Spanning tree configuration

Global Bridge Configuration

Following figure displays the global configuration settings for the bridge.



Global Bridge Configuration:

PARAMETER	VALUE
Bridge Mac Address	0:1:53:0:0:1
Number of Ports	5
Bridge Type	TRANSPARENT
Unicast Learning	HYBRID
Multicast Learning	HVM
Config Pvid Status	true
Tagging	ENABLED
AcceptableFrameTypeCfg	ENABLED
IngressFilteringCfg	ENABLED
Filter Age(in seconds)	300 Set Value
Traffic Class Mapping	DISABLED Set Status

The following bridge information is displayed:

1. Bridge MAC Address
2. Number of bridge interfaces configured
3. Type of the Bridge
4. Unicast learning which is non-configurable, and always set to Hybrid, i.e. VLAN learning is both “Independent” as well as “Shared” depending on the association of VLANS with filtering databases.
5. Multicast Learning setting which is non-configurable and always set to HVM(Hybrid VLAN Multicast Learning), i.e. if two VLANs are associated with the same FDB, the filtering information for a multicast MAC address in one VLAN would be used in the forwarding decision for the same MAC address in the other VLAN too.
6. Config Pvid Status which is non-configurable and is always true, i.e. the bridge supports the ability to override the default PVID setting and its egress status (VLAN tagged or untagged) on each bridge interface.
7. Tagging which is non-configurable and always enabled, i.e. each bridge interface supports 802.1Q VLAN tagging of frames.
8. AcceptableFrameTypeCfg which is non-configurable and always enabled, i.e. each bridge interface can be configured to accept all frames or only tagged frames.
9. IngressFilteringCfg which is non-configurable and is always enabled, i.e. each bridge interface supports discarding of frames whose VLAN classification does not include that interface in its member set.
10. Filter Age is the time (in seconds) after which MAC addresses are removed from the filter table when there has been no activity. The time may be an integer value between

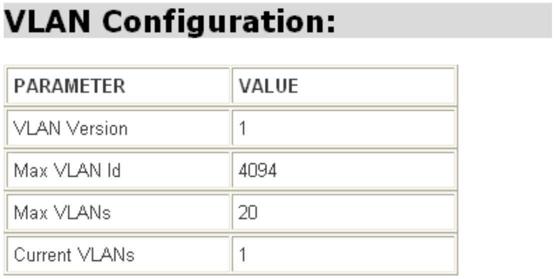
10 and 100,000 seconds. The default value is 300 seconds. If to change the filter age, input the seconds desired in the filter age field, and then clock on Set Value to submit your setting.

11. Traffic Class setting which is the status of traffic class mapping. If to set traffic class, select your option from the drop-down list and click on Set Status to submit your setting. The following table gives the range of values for each option which can be specified with this command and a default value.

Option	Description	Default value
enable	Enable the mapping of regenerated priority to its traffic class.	disable
disable	Disable the mapping of regenerated disable priority to its traffic class.	
prioritybased	Traffic class mapping would happen only if traffic class has not been already set.	

VLAN configuration

Following figure displays the VLAN settings for the bridge.



VLAN Configuration:

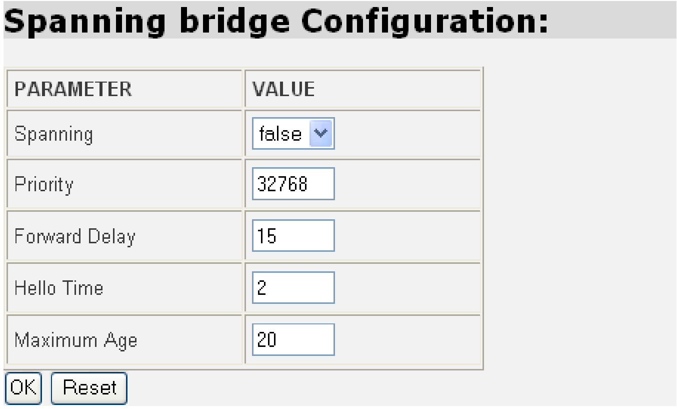
PARAMETER	VALUE
VLAN Version	1
Max VLAN Id	4094
Max VLANs	20
Current VLANs	1

The following VLAN information is displayed:

1. VLAN version: IEEE 802.1q version number that this device supports, which is 1.
2. Max VLAN Id: The maximum VLAN Id for a VLAN in the bridge.
3. Max VLANs: The maximum number of VLANs supported in the bridge.
4. Current VLANs: The number of VLANs that are currently existing in the bridge.

Spanning bridge configuration

Following figure displays the spanning bridge settings for the bridge.



Spanning bridge Configuration:

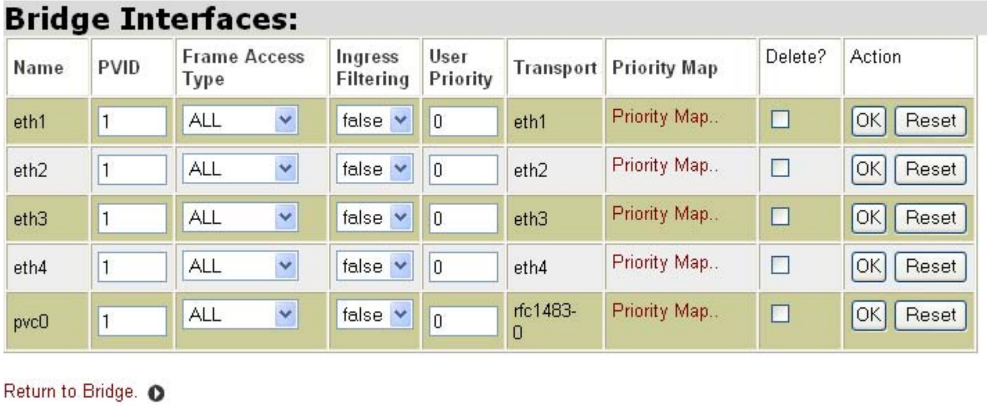
PARAMETER	VALUE
Spanning	false
Priority	32768
Forward Delay	15
Hello Time	2
Maximum Age	20

The following spanning bridge information is displayed and allows users to configure:

1. Spanning: spanning tree setting (true or false)
2. Priority: spanning tree priority value
3. Forward Delay: spanning tree forward delay time (seconds)
4. Hello time: spanning tree hello time (seconds)
5. Maximum Age: spanning tree maximum age (seconds)

Interface Configuration

Click on *Interface configuration* and then bridge interfaces page is displayed as shown in the following figure.



Bridge Interfaces:

Name	PVID	Frame Access Type	Ingress Filtering	User Priority	Transport	Priority Map	Delete?	Action
eth1	1	ALL	false	0	eth1	Priority Map..	□	OK Reset
eth2	1	ALL	false	0	eth2	Priority Map..	□	OK Reset
eth3	1	ALL	false	0	eth3	Priority Map..	□	OK Reset
eth4	1	ALL	false	0	eth4	Priority Map..	□	OK Reset
pvc0	1	ALL	false	0	rfc1483-0	Priority Map..	□	OK Reset

The following table gives the range of values for each option which can be specified with this command and a default value.

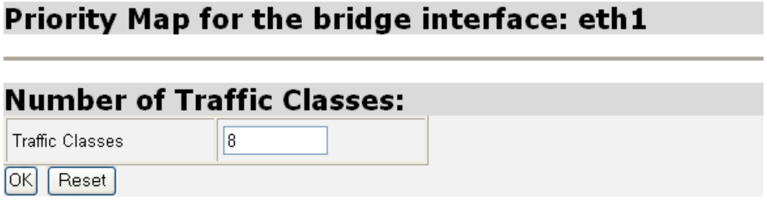
option	Description	Default value
Name	Interface name	
PVID	Port VLAN Id (PVID) associated with the interface.	1
Frame Access type	Acceptable Frame Type setting. Each bridge interface can be configured to accept all frames or only tagged frames.	all
Ingress filtering	Ingress Filtering Setting. Accepts VLAN tagged frames, only if the VLAN Id in the frame has this	false

	interface in its egress interface list.	
User priority	The user priority to regenerated user-priority mapping for a bridge interface.	0
Transport	Name of attached transport.	
Priority map	The mapping of user priority in the incoming frames to the regenerated user priority that would be used for traffic class mapping as well as set in the VLAN tag of the outgoing frame. How to configure is introduced in the following section.	

Priority map configuration

Click on *priority map* for a specified bridge interface, and then the Priority Map for the bridge interface page is displayed. In this page, number of traffic classes, user priority to regenerated priority map and Regenerated Priority to Traffic Class Map are provided to configure. The procedure is shown as follows:

1. Number of traffic classes, as shown in the following figure, specifies the number of traffic classes supported by the bridge interface. It can be any value between 1 and 8.

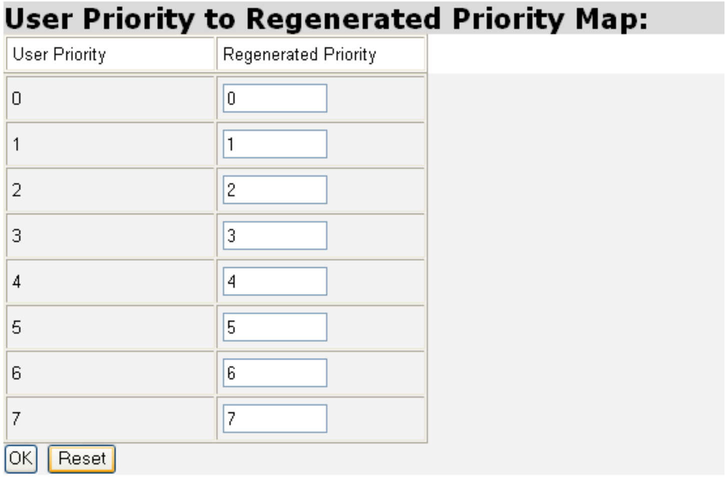


Priority Map for the bridge interface: eth1

Number of Traffic Classes:

Traffic Classes	8

2. User Priority to Regenerated Priority Map, as shown is the following figure, specifies the mapping of user priority in the incoming frames to the regenerated user priority that would be used for traffic class mapping as well as set in the VLAN tag of the outgoing frame.



User Priority to Regenerated Priority Map:

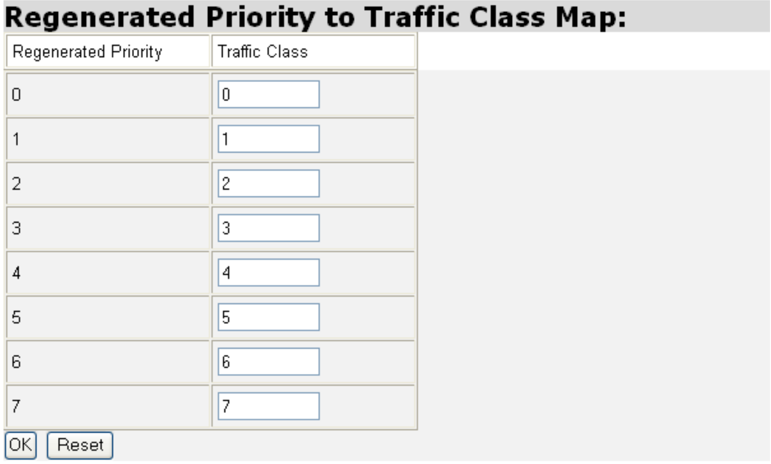
User Priority	Regenerated Priority
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

The following table gives the range of values for each option which can be specified with this command and a default value.

Option	Description	Default value
Priority 0	The regenerated user-priority to which the user priority with value 0 in the incoming frame should be mapped.	0

Option	Description	Default value
Priority 1	The regenerated user-priority to which the user priority with value 1 in the incoming frame should be mapped.	1
Priority 2	The regenerated user-priority to which the user priority with value 2 in the incoming frame should be mapped.	2
Priority 3	The regenerated user-priority to which the user priority with value 3 in the incoming frame should be mapped.	3
Priority 4	The regenerated user-priority to which the user priority with value 4 in the incoming frame should be mapped.	4
Priority 5	The regenerated user-priority to which the user priority with value 5 in the incoming frame should be mapped.	5
Priority 6	The regenerated user-priority to which the user priority with value 6 in the incoming frame should be mapped.	6
Priority 7	The regenerated user-priority to which the user priority with value 7 in the incoming frame should be mapped.	7

3. Regenerated Priority to traffic class map, as shown in the following figure, specifies the mapping of regenerated priority to their traffic class values.



Regenerated Priority to Traffic Class Map:

Regenerated Priority	Traffic Class
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

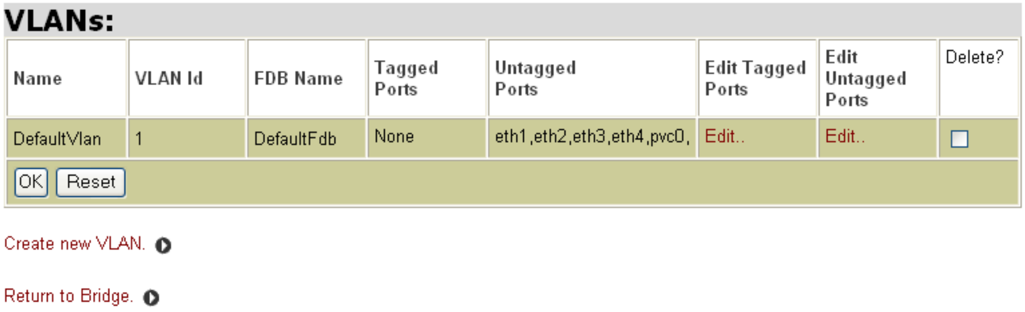
The following table gives the range of values for each option which can be specified with this command and a default value.

Option	Description	Default value
Priority 0	The traffic class to which the regenerated priority of value 0 is mapped.	0
Priority 1	The traffic class to which the regenerated priority of value 1 is mapped.	1
Priority 2	The traffic class to which the regenerated priority of value 2 is mapped.	2
Priority 3	The traffic class to which the regenerated priority of	3

	value 3 is mapped.	
Priority 4	The traffic class to which the regenerated priority of value 4 is mapped.	4
Priority 5	The traffic class to which the regenerated priority of value 5 is mapped.	5
Priority 6	The traffic class to which the regenerated priority of value 6 is mapped.	6
Priority 7	The traffic class to which the regenerated priority of value 7 is mapped.	7

VLAN Configuration

Click on *VLAN configuration* and then VLAN interfaces page is displayed as shown in the following figure. Users can configure the VLAN existing currently or create new VLAN via this page.



VLANs:

Name	VLAN Id	FDB Name	Tagged Ports	Untagged Ports	Edit Tagged Ports	Edit Untagged Ports	Delete?
DefaultVlan	1	DefaultFdb	None	eth1,eth2,eth3,eth4,pvc0,	Edit..	Edit..	□

Create new VLAN.

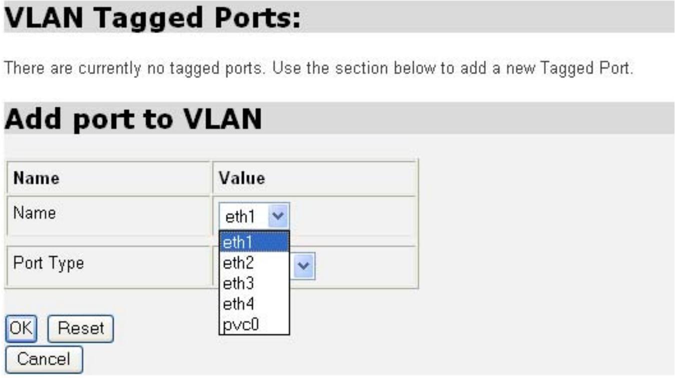
Return to Bridge.

The following table gives the range of values for each option, which can be specified with this command and a default value.

option	Description	Default value
Name	An arbitrary name that identifies the VLAN. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	DefaultVlan
VLAN ID	The VLAN Id that the user wants to assign to the named VLAN. The valid values for the VLAN Id ranges between 1 and 4094.	1
FDB Name	The name of an existing Filtering Database with which the user wants the VLAN to be associated. If the FDB already exists, the VLAN becomes associated with that FDB. If the FDB does not exist, it is created and the VLAN becomes associated with it.	DefaultFdb
Tagged Ports	the tagged port list of the named VLAN	None
User priority	the untagged port list of the named VLAN	eth1,eth2,eth3,eth4,pvc0
Edit Tagged Ports	Allow users to edit tagged ports while clicking on *Edit.*	
Edit untagged Ports	Allow users to edit untagged ports while clicking on *Edit*	

Edit Tagged Ports

As shown in the following figure, user can add a specified port to VLAN through name drop-down list. Click on OK to submit your setting, Reset to clear your setting and Cancel to return to previous page.



VLAN Tagged Ports:

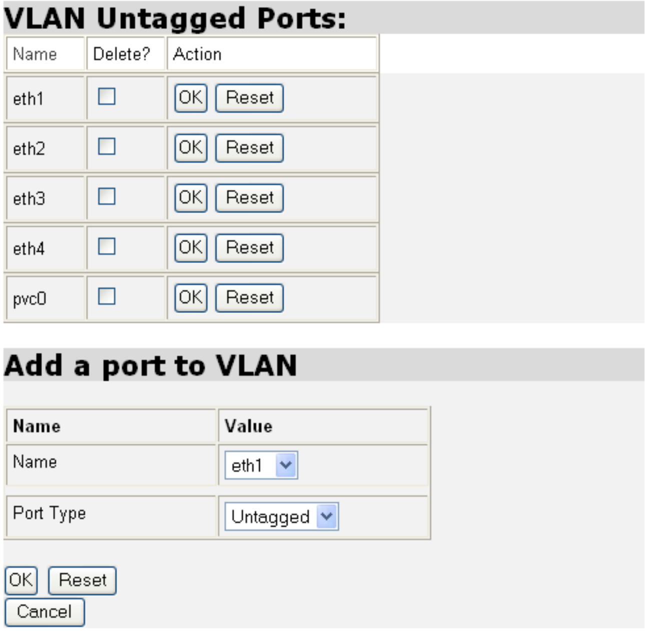
There are currently no tagged ports. Use the section below to add a new Tagged Port.

Add port to VLAN

Name	Value
Name	eth1
Port Type	

Edit untagged Ports

As shown in the following figure, user can add or delete a specified untagged port. Click on OK to submit your setting, Reset to clear your setting and Cancel to return to previous page.



VLAN Untagged Ports:

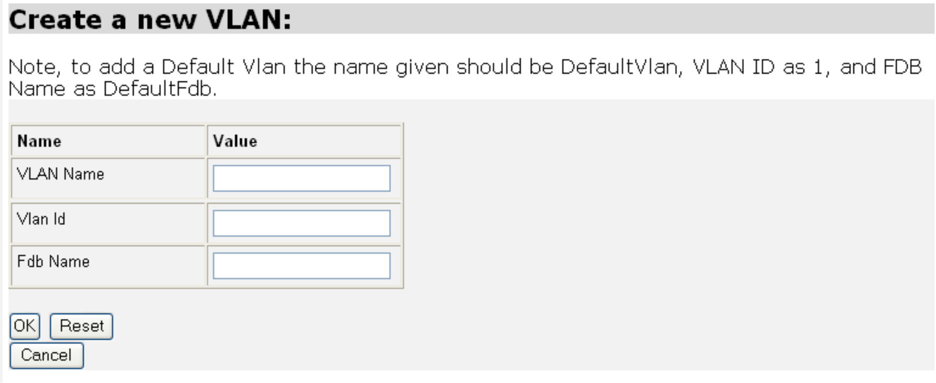
Name	Delete?	Action
eth1	□	OK Reset
eth2	□	OK Reset
eth3	□	OK Reset
eth4	□	OK Reset
pvc0	□	OK Reset

Add a port to VLAN

Name	Value
Name	eth1
Port Type	Untagged

Create a new VLAN

Click on *Create a new VLAN*, the Create a new VLAN page is displayed, as shown in the following figure. In this page, user can create a new VLAN after configuring VLAN name, Vlan Id and Fdb Name respectively. Click on OK to submit your setting, Reset to clear your setting and Cancel to return to previous page.



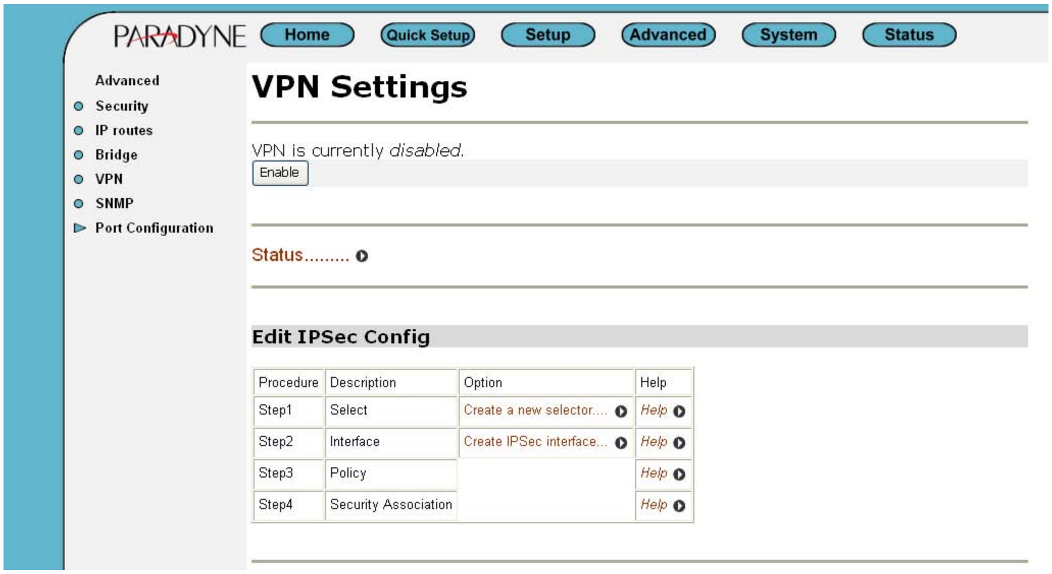
Create a new VLAN:

Note, to add a Default Vlan the name given should be DefaultVlan, VLAN ID as 1, and FDB Name as DefaultFdb.

Name	Value
VLAN Name	
Vlan Id	
Fdb Name	

VPN

VPN (Virtual private network) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. To configure VPN, click on VPN via the Advanced menu to invoke the VPN Settings screen.



VPN Settings

VPN is currently *disabled.*

Edit IPSec Config

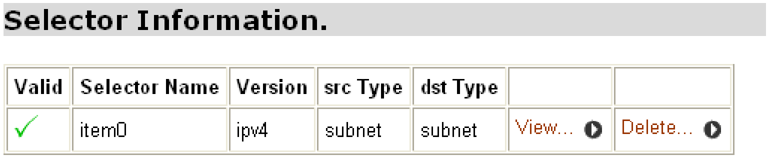
Procedure	Description	Option	Help
Step1	Select	Create a new selector....	Help
Step2	Interface	Create IPSec interface...	Help
Step3	Policy		Help
Step4	Security Association		Help

To activate the VPN configuration, click on Enable. The VPN page then shows the VPN is currently enabled.

VPN Status

Click on *Status* to view current VPN status, including selector information, WAN service information, policy information, and security association information:

1. Selector information allows users to view and delete a specified selector.



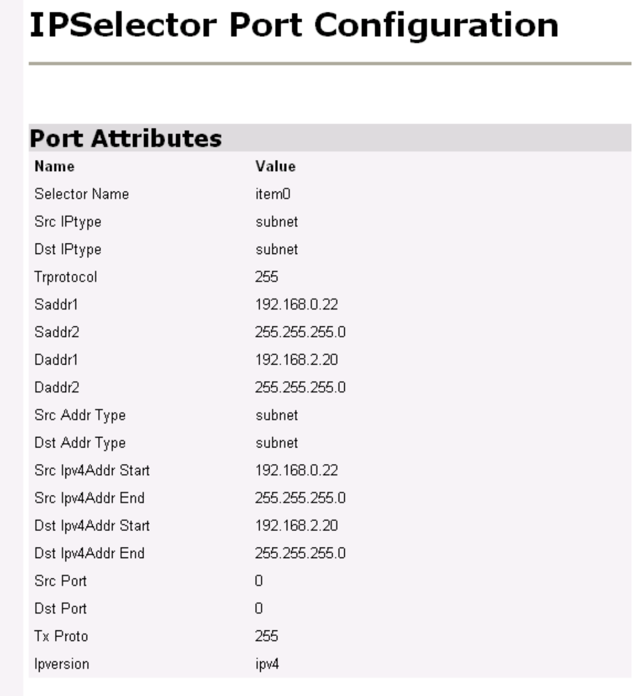
Selector Information.

Valid	Selector Name	Version	src Type	dst Type		
✓	item0	ipv4	subnet	subnet	View...	Delete...

Following table shows the definition of each field.

Field	Description
Valid	Created successfully
Selector name	Name of the selector
Version	IP version
src Type	Source address type
dst Type	Destination address type

Click on *View* to show advanced selector information or *Delete* the selector.

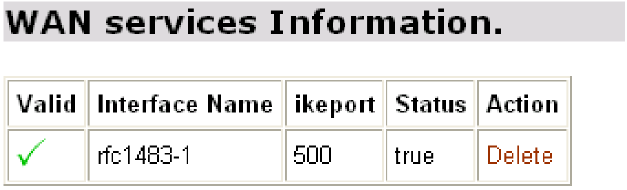


IPSelector Port Configuration

Port Attributes

Name	Value
Selector Name	item0
Src IPtype	subnet
Dst IPtype	subnet
Trprotocol	255
Saddr1	192.168.0.22
Saddr2	255.255.255.0
Daddr1	192.168.2.20
Daddr2	255.255.255.0
Src Addr Type	subnet
Dst Addr Type	subnet
Src Ipv4Addr Start	192.168.0.22
Src Ipv4Addr End	255.255.255.0
Dst Ipv4Addr Start	192.168.2.20
Dst Ipv4Addr End	255.255.255.0
Src Port	0
Dst Port	0
Tx Proto	255
Ipversion	ipv4

2. WAN services information allows users to view and delete a specified service.



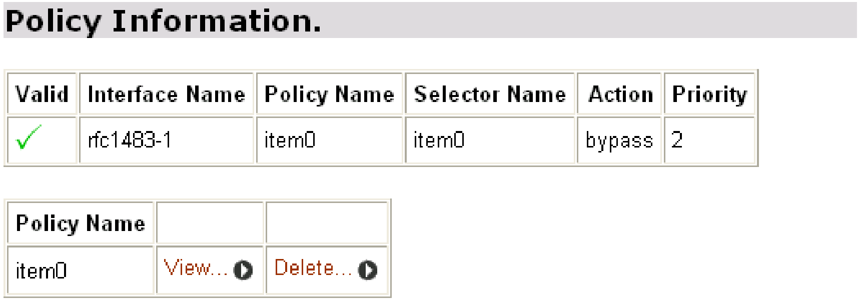
WAN services Information.

Valid	Interface Name	ikeport	Status	Action
✓	rfc1483-1	500	true	Delete

Following table shows the definition of each field.

Field	Description
Valid	Created successfully
interface name	Name of the interface
ikeport	The IKE port value; the UDP port number on which IKE daemon listens on all valid unicast IPv4 and IPv6 addresses of this interface. The default value is 500.
Status	The status of IPsec on this interface. The default value is true.
Action	To delete the interface

3. Policy Information allows users to view and delete a specified IPSec policy.



Policy Information.

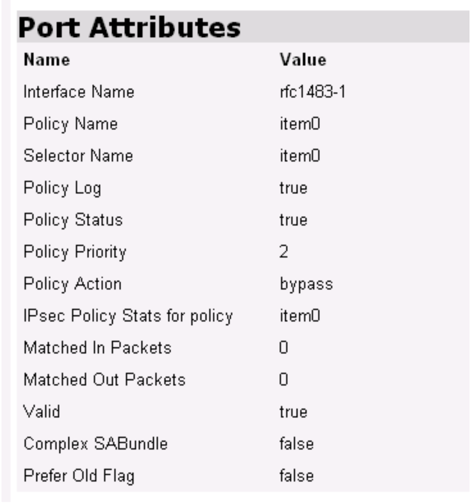
Valid	Interface Name	Policy Name	Selector Name	Action	Priority
✓	rfc1483-1	item0	item0	bypass	2

Policy Name		
item0	View... ●	Delete... ●

Following table shows the definition of each field.

Field	Description
Valid	Created successfully
interface name	Name of the interface
policy name	Name of the policy
Selector name	Name of the selector
Action	The action specified by the policy (deny, bypass or applyipsec)

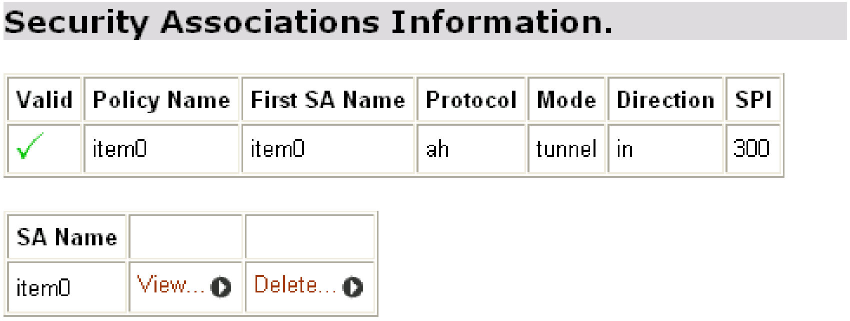
Click on *View,* and then IPSec Policy Port Configuration page is invoked as follows.



Port Attributes

Name	Value
Interface Name	rfc1483-1
Policy Name	item0
Selector Name	item0
Policy Log	true
Policy Status	true
Policy Priority	2
Policy Action	bypass
IPsec Policy Stats for policy	item0
Matched In Packets	0
Matched Out Packets	0
Valid	true
Complex SABundle	false
Prefer Old Flag	false

4. Security Associations Information: a security association (SA) provides security services between IPsec peers for certain IP packets. SAs operate in a single direction; you would usually create a pair of SAs for two-way traffic (inbound and outbound).



Security Associations Information.

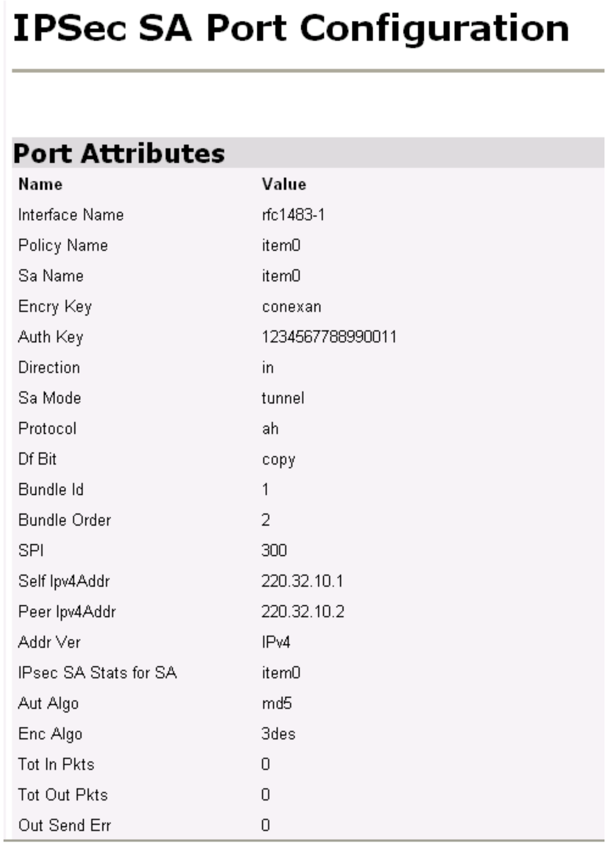
Valid	Policy Name	First SA Name	Protocol	Mode	Direction	SPI
✓	item0	item0	ah	tunnel	in	300

SA Name		
item0	View... ●	Delete... ●

Following table shows the definition of each field.

Field	Description
Valid	Created successfully
Policy Name	Name of the policy
First SA Name	Name of 1st security association
Protocol	Each SA supports a single security protocol - AH or ESP. If you want to use both protocols simultaneously, you need to create a bundle of one or more SA pairs.
Mode	The SA mode - tunnel or transport: • in tunnel mode you must also specify the source and destination addresses (either IPv4 or IPv6) of the security gateways that form the IPsec peers. You can also optionally configure how IPsec deals with fragmentation and reassembly of packets. • in transport mode, the IPsec policy referenced in the command provides the necessary source and destination address information.
Direction	the direction of traffic that the SA will apply to
SPI	a unique identifier called the Security Parameter Index
SA Name	Name of security association

Click on *View,* and the IPSec SA Port Configuration page is invoked as follows.



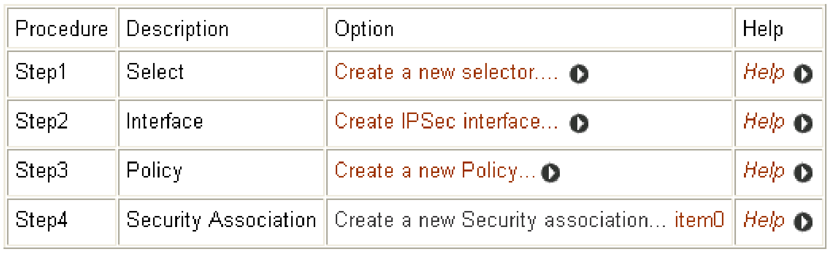
IPSec SA Port Configuration

Port Attributes

Name	Value
Interface Name	rfc1483-1
Policy Name	item0
Sa Name	item0
Encry Key	conexan
Auth Key	1234567788990011
Direction	in
Sa Mode	tunnel
Protocol	ah
Df Bit	copy
Bundle Id	1
Bundle Order	2
SPI	300
Self Ipv4Addr	220.32.10.1
Peer Ipv4Addr	220.32.10.2
Addr Ver	IPv4
IPsec SA Stats for SA	item0
Aut Algo	md5
Enc Algo	3des
Tot In Pkts	0
Tot Out Pkts	0
Out Send Err	0

Edit IPSec Config

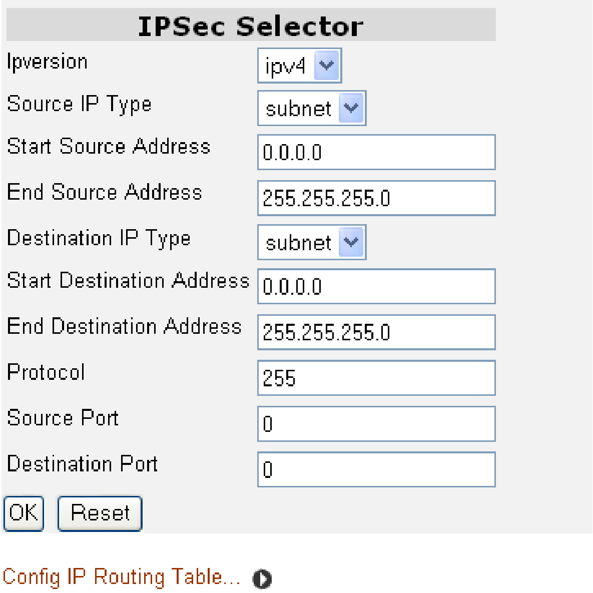
If to create a IPSec, the procedure is shown as follows:



Procedure	Description	Option	Help
Step1	Select	Create a new selector....	Help
Step2	Interface	Create IPSec interface...	Help
Step3	Policy	Create a new Policy...	Help
Step4	Security Association	Create a new Security association... item0	Help

Step 1: Create a new IPSec selector

Click on the *Create a new selector* link. The IPSec Selector page is displayed as follows:



IPSec Selector

Ipversion: ipv4

Source IP Type: subnet

Start Source Address: 0.0.0.0

End Source Address: 255.255.255.0

Destination IP Type: subnet

Start Destination Address: 0.0.0.0

End Destination Address: 255.255.255.0

Protocol: 255

Source Port: 0

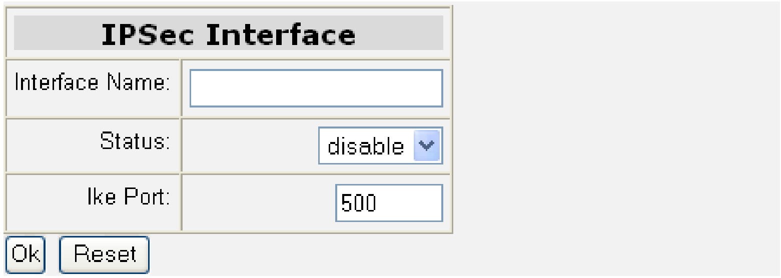
Destination Port: 0

Input the values on the fields respectively. The following table gives the range of values for each option, which can be specified with this command and a default value.

Option	Description
Ipversion	IPv4 only currently
Source IP Type	Name of the selector
Start Source Address	Start source address
End Source Address	End source address type
Destination IP Type	Destination address type
Start Destination Address	Start Destination Address
Protocol	This option allows you to specify a protocol number (protnum) value. The value 255 is interpreted as a wild card entry.
Source Port	Source TCP/UDP port
Destination Port	Destination TCP/UDP port

Step 2: Create IPSec Interface

Click on the *Create IPSec Interface* link, the IPSec Interface page is displayed as follows:



IPSec Interface

Interface Name:	
Status:	disable
Ike Port:	500

Note: This has to be the Name of IP interface, example: ***ipwan***

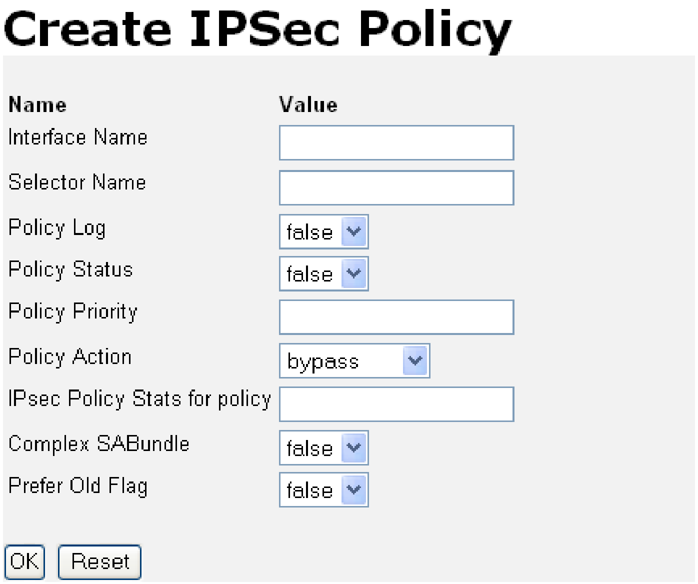
Input the values on the fields respectively. The following table gives the range of values for each option, which can be specified with this command and a default value.

field	Description
interface name	Name of the interface
ikeport	The IKE port value; the UDP port number on which IKE daemon listens on all valid unicast IPv4 and IPv6 addresses of this interface. The default value is 500.
Status	The status of IPsec on this interface. The default value is disabled.

Note: if to create a IPSec Interface successfully, a new WAN service should be created in advance via WAN connection page.

Step 3: Create IPSec Policy

If step1 and step 2 are successfully created, the *Create IPSec Interface* link will appear. Click on the link, and then the IPSec Interface page is displayed as follows:



Create IPSec Policy

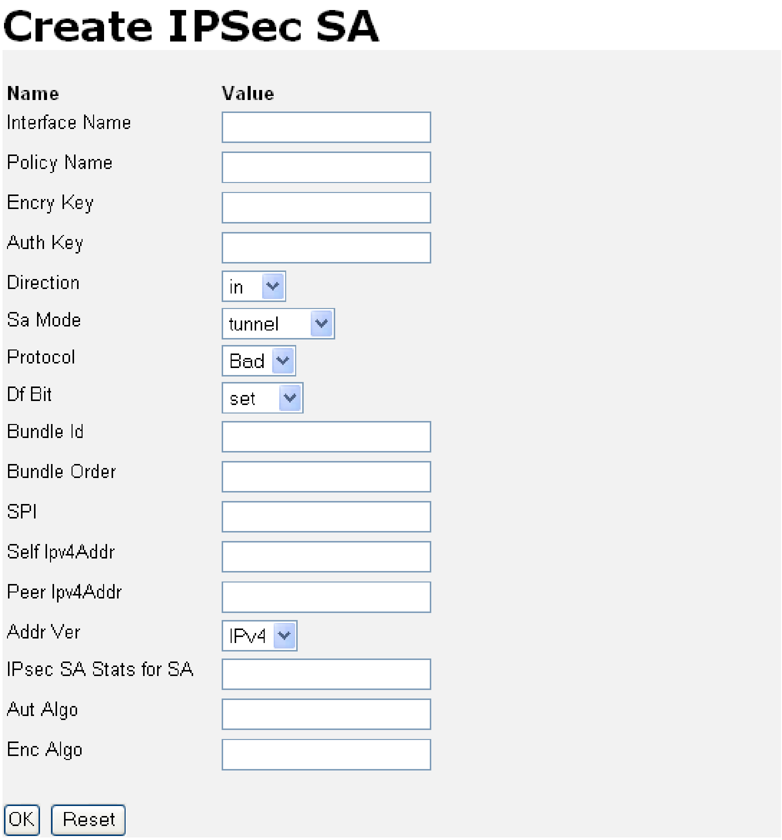
Name	Value
Interface Name	
Selector Name	
Policy Log	false
Policy Status	false
Policy Priority	
Policy Action	bypass
IPsec Policy Stats for policy	
Complex SABundle	false
Prefer Old Flag	false

Input the values on the fields respectively. The following table gives the range of values for each option, which can be specified with this command and a default value.

Option	Description	Default value
interface name	Name of the interface	n/a
Selector name	Name of the selector	n/a
Policy log	Enables or disables the status of the IPsec policy log.	false
Policy status	Enables or disables the status of the IPsec policy.	false
Policy priority	The priority for the policy lookup. A lower priority value means that this policy will be searched before a policy with a higher priority value. The priority value should be between 1 and 65565 inclusive, but it cannot be set to 255 or 256. These values are reserved for dynamic policies. e.g. 1.	n/a
Policy action	The action specified by the policy (deny, bypass or applyipsec)	bypass
IPsec Policy Stats for policy	statistics about the number of inbound and outbound packets that match a specific IPsec policy.	n/a
Complex SABundle	This option is only relevant if *applyipsec* has been selected. It is used to control the interpretation of two tunnel mode SAs in an SA bundle as follows: When two tunnel-mode SAs (SA1 and SA2) in a bundle have the same local and peer end points and *complexsabundle* is set to *disable*, then apart from IPsec headers, only one new IP header is added on to the original packet. For example, for an AH tunnel - ESP tunnel SA bundle, the packet formed would be as follows: IP-AH-ESP-[IP_internal+Upper layer] If *complexsabundle* is set to enable, the packet formed would be as follows: IP-AH-IP-ESP-[IP_internal+Upper layer]	false
Prefer Old Flag	When set to *enable*, this option specifies whether to prefer the DYING SAs over MATURE SAs. When set to disable, MATURE SAs are preferred instead. This option is only applicable if your image supports IKE.	false

Step 4: Create IPSec SA

After successfully creating a new IPSec Policy, click on the *Create IPSec SA link* in step 4, and then Create IPSec SA page is shown as follows:



Create IPSec SA

Name	Value
Interface Name	
Policy Name	
Encry Key	
Auth Key	
Direction	in
Sa Mode	tunnel
Protocol	Bad
Df Bit	set
Bundle Id	
Bundle Order	
SPI	
Self Ipv4Addr	
Peer Ipv4Addr	
Addr Ver	IPv4
IPsec SA Stats for SA	
Aut Algo	
Enc Algo	

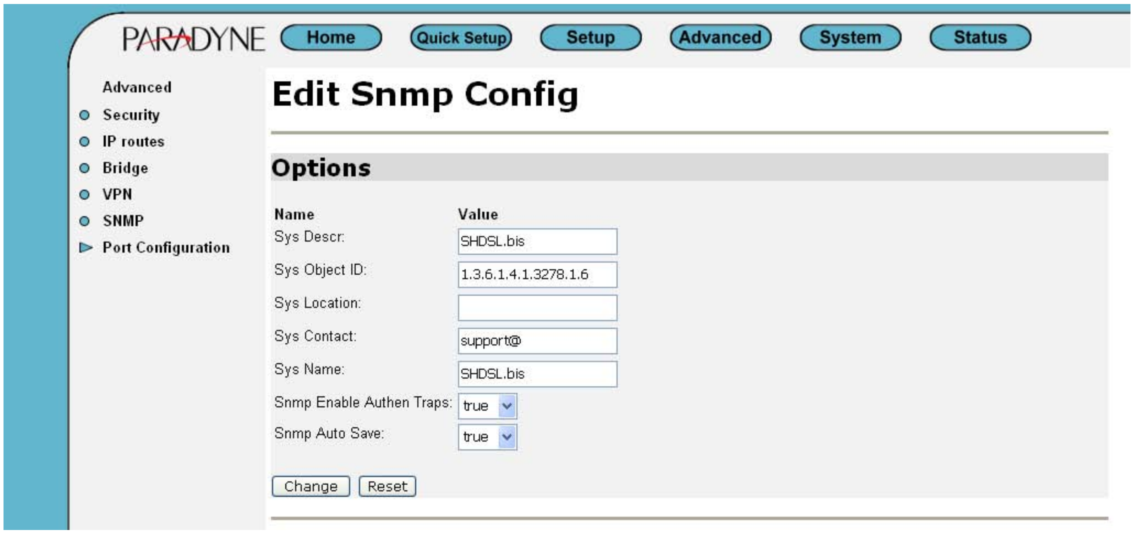
Input the values on the fields respectively. The following table gives the range of values for each option, which can be specified with this command.

Option	Description
Interface name	Name of the interface
Policy name	Name of the IPsec policy previously created.
Encry Key	Encry Key is a cryptographic key for an encryption. algorithm.The key requirements for specific algorithms are as follows: DES - 64 bit(8 characters) e.g. *conexant*. 3DES - 192 bit(24 characters) e.g. *conexantconexantconexant*
Auth Key	Auth Key is a cryptographic key for an authentication. algorithm.algorithm.The key requirements for specific algorithms are as follows: SHA1 - 160 bit(20 characters) e.g. *conexantconexantconexantcone*. MD5 - 128 bit(16 characters) e.g. *conexantconexant*
Direction	Specifies the direction in which the SA is applicable.
Sa Mode	Tunnel or transparent mode selectable
Protocol	Specifies that this SA is being created for the authentication header protocol. esp Specifies that this SA is being created for the encapsulation security payload protocol.

Option	Description
Df Bit	Df Bit indicates how the Don't Fragment (DF) bit in the IP header should be be handled in tunnel mode. You can choose from the following dfbitcfg values: If copy is set, the DF bit in the outer IP (tunnel) header is copied from the inner IP header. If set is set, the DF bit is always set to 1 in the tunnel IP header. This should only be specified if the SA is a tunnel mode SA. If clear is set, the DF bit in the tunnel header will always be reset.
Bundle Id	A unique identifier for each SA that forms part of a bundle. All SA bundles associated with a policy should have different bundleids. By default, the bundleid is 0, signifying that the SA is not part of any bundle or is a single SA. e.g. 0.
Bundle Order	The Bundle Order specifies the location of a particular SA in a bundle. This is a mandatory parameter if bundleid is specified. It can take positive integer values. The SA with the lowest bundleorder value is applied first, followed by the higher bundleorder value, irrespective of the direction of the SA. e.g. 0.
SPI	SPI specifies a unique value. If the SA is applicable to inbound traffic (in), the SPI is assigned by the sender. If the SA is applicable to outbound traffic (out), the SPI is assigned by the receiver. This value must be greater than 255 and less than 65536. e.g. 300.
Self Ipv4Addr	The source gateway addresses for IPv4 packets. These are only specified in tunnel mode.
Peer Ipv4Addr	The destination gateway addresses for IPv4 packets. These are only specified in tunnel mode.
Addr Ver	IPv4 or IPv6. Only IPv4 is currently supported.
IPsec SA Stats for SA	statistics about the number of inbound and outbound packets that match a specific IPsec policy.
Aut Algo	Indicates the authentication algorithm used for IPsec processing. Supported values are md5 and sha1. e.g. md5
Enc Algo	Indicates the encryption algorithm used for IPsec processing. It can only be specified if the IPsec protocol used is ESP. Supported values are des and 3des. e.g. 3des.

SNMP

Click on SNMP to invoke the Edit SNMP Config screen where you can edit SNMP (Simple Network Management Protocol) configuration.



Edit Snmp Config

Options

Name	Value
Sys Descr:	SHDSL.bis
Sys Object ID:	1.3.6.1.4.1.3278.1.6
Sys Location:	
Sys Contact:	support@
Sys Name:	SHDSL.bis
Snmp Enable Authen Traps:	true
Snmp Auto Save:	true

Change Reset

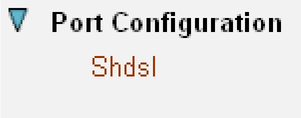
Enter or select the appropriate values. Click on Change to submit your setting or Reset to clear your setting. The following table gives the range of values for each option.

Option	Description	Default value
Sys Descr	A description of the SNMP agent system. The description is represented by a string of up to 255 characters (no spaces).	N/A
Sys Object ID	A series of non-negative integers that identifies individual variables contained in the SNMP agent's database. You can refine OIDs by adding more components at the end of the integer.	N/A
Sys Location	A name that identifies the location of the SNMP agent system. The location is represented by a string of up to 255 characters (no spaces).	N/A
Sys Contact	Contact details (e.g., telephone number, email address) for the person responsible for maintaining the SNMP agent system. The details are represented by a string of up to 255 characters (no spaces).	N/A
Sys Name	A name that identifies the system that the SNMP agent is running on. The name is a string of up to 255 characters (no spaces).	N/A
Snmp Enable Authen Traps	Allows you to configure whether or not a trap is sent if a request arrives from the SNMP manager with an invalid community name. True: A trap is generated when an SNMP request with an unrecognized community name is received. False: A trap is not generated when an SNMP request with an unrecognized community name is received.	true
Snmp Auto Save	Save SNMP configuration in the device automatically	true

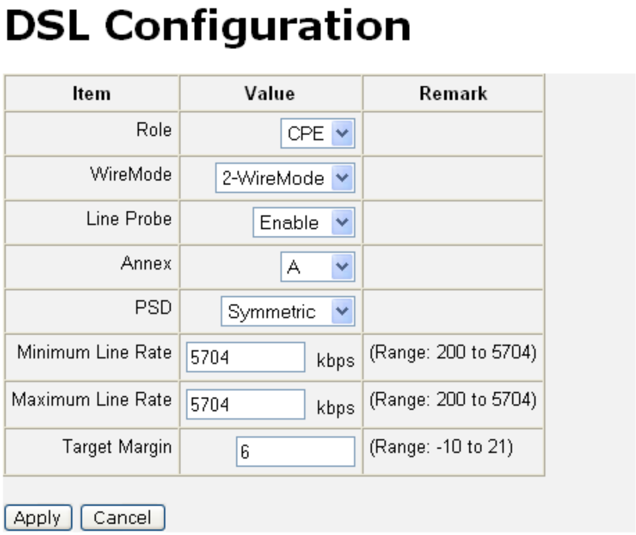
Ports

This option allows you to configure the SHDSL port on your router.

1. From the *Advanced* menu, click on *Port Configuration*. The SHDSL port available on your router is displayed.



From the Ports Configuration menu, click on SHDSL. The SHDSL Port Configuration page is displayed:

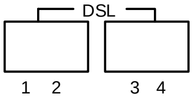


DSL Configuration

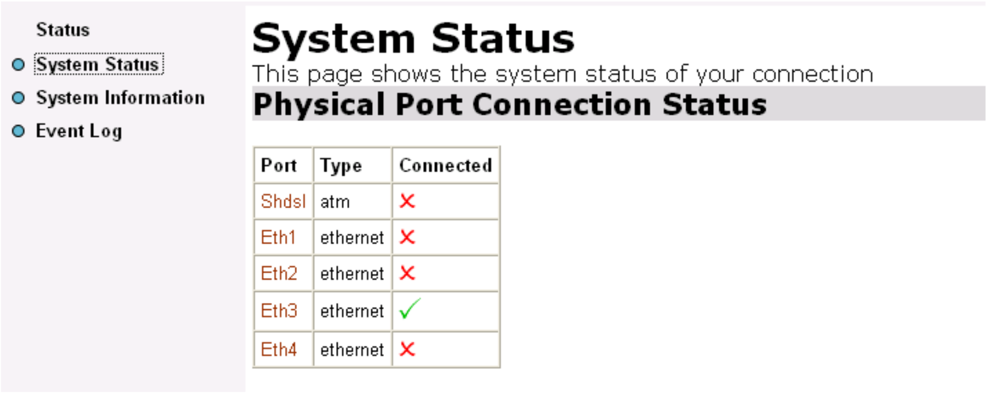
Item	Value	Remark
Role	CPE	
WireMode	2-WireMode	
Line Probe	Enable	
Annex	A	
PSD	Symmetric	
Minimum Line Rate	5704 kbps	(Range: 200 to 5704)
Maximum Line Rate	5704 kbps	(Range: 200 to 5704)
Target Margin	6	(Range: -10 to 21)

"Shdsl" is the default port name. You can configure basic SHDSL parameters in this page.

1. In the Role drop-down list, select CPE or CO.
2. To set the router's Wire mode, Click on the Wire Pair drop-down list to select the Wire Pair number needed.

Wire Mode	DSL Pair to Use	Illustration
2-Wire Mode	1	
4-Wire Mode	1,2	
6-Wire Mode	1,2,3	
8-Wire Mode	1,2,3,4	

3. Click on the Line Probe drop-down list to set line probe as enable or disable.
4. Click on the Annex drop-down list to select the desired annex mode: A, B, A&B, F, G, or F&G.
5. Click on the PSD drop-down list to set PSD as symmetric or asymmetric.
6. To set the maximum and minimum line rate, click on the Max Line Rate and Min Line Rate drop-down list respectively (200 kbps to 5704 kbps).
7. To set the target margin, input the desired number in the target margin field (range: –6 to 21 dB).
8. Click on Apply to submit your setting or Cancel to clear your setting.
9. To view the advanced status of SHDSL and Ethernet ports, refer to the system status screen:



System Status

This page shows the system status of your connection

Physical Port Connection Status

Port	Type	Connected
Shdsl	atm	✗
Eth1	ethernet	✗
Eth2	ethernet	✗
Eth3	ethernet	✓
Eth4	ethernet	✗

Chapter 4 – Diagnostic and Troubleshooting

Use the LEDs to determine the status of connections.

Description	Suggestion
Power LED, Ethernet LED, or DSL LED is not lit.	Check the appropriate connection.
Ethernet LED blinks green when the line is first plugged in. It should turn solid green when the connection is established.	If your Ethernet LED does not light, make sure the RJ45 cable you are using is connected properly. Use a straight-through or crossover cable, as appropriate, for devices without autosensing.
DSL LED blinks green when the line is first plugged in. It should turn solid green when the connection is established.	If the DSL LED does not stop blinking, the router is training and the connection is not established. Verify that your ISP user name and password are correct, and the DSL link is connected properly.