1740 SHDSL
2/4-Wire Router
User's Guide

Document Number 1740-A2-GB20-00

July 2004

PARADYNE®

Copyright © 2004 Paradyne Corporation.
All rights reserved.
Printed in U.S.A.

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, Comsphere, ETC, Etherloop, FrameSaver, GranDSLAM, Hotwire, the Hotwire logo, Jetstream, MVL, NextEDGE, OpenLane, Paradyne, the Paradyne logo, Paradyne Credit Corp., the Paradyne Credit Corp. logo, Performance Wizard, StormPort, TruPut are all registered trademarks of Paradyne Corporation. ADSL/R, BitStorm, Connect to Success, GrandVIEW, Hotwire Connected, iMarc, JetFusion, JetVision, MicroBurst, PacketSurfer, ReachDSL, Spectrum Manager, StormTracker and TriplePlay 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.

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*.

Preface

This manual is designed to provide information to network administrators. It covers the installation, operation and applications of the 1740 SHDSL router.

Warning

- Before servicing or disassembling this equipment, always disconnect all power and telephone lines from the wall outlet.
- Use an appropriate power supply and a UL Listed telephone line cord. Specification of the power supply is clearly stated in Appendix A - Specifications.

TABLE OF CONTENTS

CHAPTER 1 OVERVIEW 7

1.1 Application 7

1.2 LED Indicators 8

CHAPTER 2 INSTALLATION 9

2.1 Preparing for Hardware Installation 9

2.2 Rear-panel Connections 10

CHAPTER 3 QUICK INSTALLATION 11

3.1.1 Login 11

3.1.2 Web Page Layout 13

3.1.3 Monitoring the SHDSL Line 14

3.2 WAN Interface Configurtion 15

3.2.1 Bridge mode: Service for one fixed IP address 16

3.2.2 Router Mode: Service for Five Static IP Addresses 18

3.2.3 PPPoE 22

3.2.4 PPPoA 24

3.2.5 Password Setup 26

3.2.6 Setting the Bridge 27

3.3 Spanning Tree Protocol 27

3.4 Static Bridging 28

3.4.1 Write System Configurations 29

3.4.2 Load Factory Default Values 30

CHAPTER 4 SETTING UP WAN AND LAN INTERFACES 31

4.1 LAN Interface 31

4.2 Configuring the WAN Interface 32

4.2.1 VC Data Flow Control 33

4.2.2 Setting up an ISP 34

CHAPTER 5 SNMP 35

5.1 Enable SNMP 35

5.2 Disable SNMP 36
CHAPTER 6 PACKET FILTER 37
6.1.1 Add a Packet Filter entry 37
6.1.2 Delete a Packet Filter entry 38
6.1.3 Enable/Disable Packet Filter 38
CHAPTER 7 ROUTING 39
7.1 Static Route 39
7.2 Set Up the RIP function 40
7.3 Displaying the Routing Table 42
CHAPTER 8 NAT 43
8.1 Multiple to One 44
8.2 One to One NAT 45
8.3 Multi-NAT 46
8.4 Virtual Server 48
CHAPTER 9 DHCP 49
9.1 DHCP Server 49
9.2 DHCP Relay 50
CHAPTER 10 DNS PROXY 51
CHAPTER 11 IGMP 52
CHAPTER 12 VLAN 54
CHAPTER 13 MAINTENANCE AND DIAGNOSTICS 55
13.1 Software Upgrade and Configuration Backup /Restoration 55
13.2 OAM Loopback 58
13.3 Ping 59
13.4 Performance Monitoring 60
CHAPTER 14 APPLICATION EXAMPLE 63
14.1 Adding the Static Route (Web) 63
CHAPTER 15 PIN ASSIGNMENTS 65
CHAPTER 16 CONSOLE ACCESS 66
16.1.1 Login 66
16.1.2 Keyboard Operations 67
16.1.3 Motoring the SHDSL Line Status 69

16.1.4 Password Setup 70
16.1.5 Retrieve the Factory Default Settings 70
16.1.6 Disable the Web Browser 70
16.1.7 Save the Configurations 71
16.1.8 Login 71
APPENDIX A: SPECIFICATIONS 73

CHAPTER 1 Overview

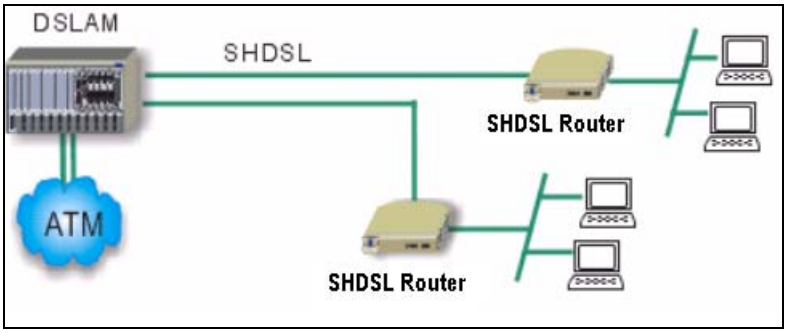
The 1740 SHDSL router satisfies the needs of multiple users in small/home offices and remote/branch offices. It provides symmetrical transmission speeds of up to 4.6 Mbps through a SHDSL connection, over a two-wire or four-wire line. In addition, it supports up to 16 virtual concurrent connections to multiple destinations. The integrated four-port switch enables up to four devices to be connected to the LAN.

The SHDSL router can be used for variety of applications, including video conferencing, remote training, e-commerce, and other multimedia applications. Easy configuration and monitoring can be accomplished using the Web browser.

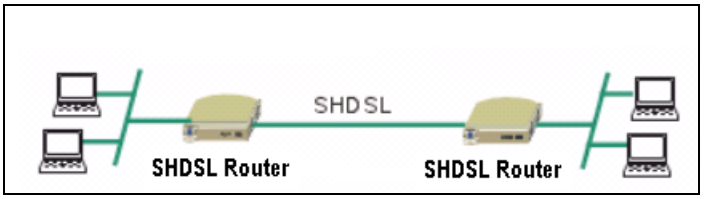
The SHDSL router has full routing capabilities to segment/route IP protocol and is capable of bridging other protocols. It can be also configured in either server or client mode enabling point-to-point connectivity between two sites.

1.1 Application

The router can be used for DSLAM and point-to-point applications.



DSLAM Application



Point-to-Point Application

1.2 LED Indicators

There are eight LEDs on the front panel of the router; the functions of the LEDs are described in the table below.

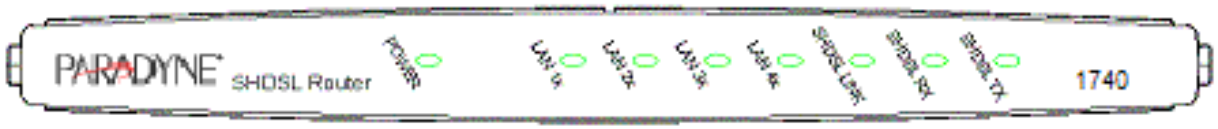


Figure 1-1 Faceplate LED Indicators

LED	Color	Mode	Function
POWER	Green	On	Power is supplied
		Off	Power is not supplied
LAN 1–4	Green	Off	No data transmitted or received over the Ethernet link
		On	The Ethernet link is established
		Flash	Transmitting or receiving data over Ethernet link
SHDSL LINK	Green	On	The physical link through the RJ45 connection cable is established
		Flash	The SHDSL line is training
		Off	A SHDSL connection is not established
SHDSL RX	Green	On	Receiving data over the SHDSL link
		Off	No data receiving over the SHDSL link
SHDSL TX	Green	On	Transmitting data over the SHDSL link
		Off	No data transmitting over the SHDSL link

CHAPTER 2 Installation

2.1 Preparing for Hardware Installation

The following equipment may be necessary to install the router:

- **AC power adapter**

A power adapter is shipped with the router.

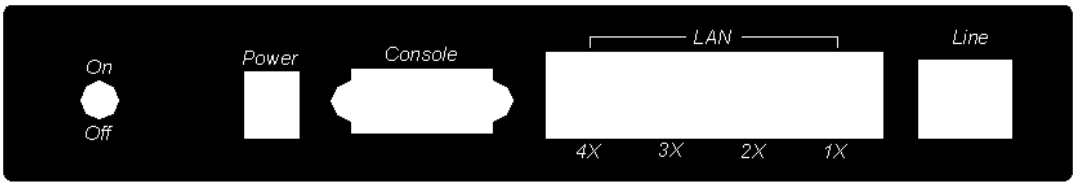
- **LAN connection cable**

To connect to the hub, use a straight-through RJ45 cable. To connect to a PC, use a crossover RJ45 cable.

- **Four-wire (8P8C) straight-through RJ45 cable**

A four-wire (8P8C) straight through RJ45 cable is needed to connect to the LINE port to the wall outlet.

2.2 Rear-panel Connections



DSL connection

Connect the supplied RJ45 cable to the port marked LINE at the back of the SHDSL router. Connect the other end of the cable to your telephone-line wall outlet. Ensure your computer is turned on before you connect the DSL line to the router. A green LED on the front of the device labeled LINK will illuminate steadily. If the SHDSL LINK LED does not illuminate steadily within one minute of it being connected, check your cable connections to ensure they are correct and securely installed.

Ethernet connection

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 your Ethernet Network Interface Card (NIC) installed in your computer. When the Ethernet connection is established, the correspondent green LED on the front panel labeled LAN will illuminate steadily. You can connect up to four PCs to the router.

Power connection

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. Turn on the power switch. After powering on, the router performs a self-test. Wait for a few seconds until the test is finished, then the router will be ready to operate. The POWER indicator on the front of the router will illuminate green to indicate that power is being supplied to the router.

Caution 1: If the router fails to power up, or it malfunctions, first verify that the power supply is connected correctly. Then power it on again. If the problem persists, contact your technical support representative.

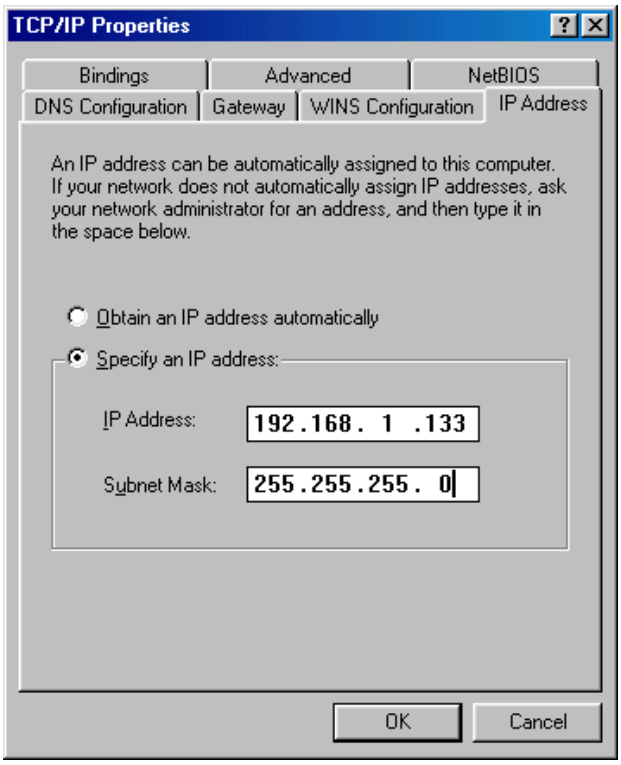
Caution 2: Before servicing or disassembling this equipment always disconnect all power cords and telephone lines from the wall outlet.

CHAPTER 3 Quick Installation

This section describes how to manage the router via the Web browser from the remote end. The Web page is best read with a display resolution of 1024 x 768. To change the resolution, go to the Microsoft Windows Control Panel and click on the **Display** icon. You will find the display settings there.

3.1.1 Login

STEP 1: Configure your workstation to the same network segment as the router, if for example the router is set to its default address of 192.168.1.1, we could set the PC to 192.168.1.133 and subnet mask 255.255.255.0.



STEP 2: Start your Internet browser.

STEP 3: Enter the IP address of the router in the Web address field. For example, if the IP address is 192.168.1.1, enter http:// 192.168.1.1

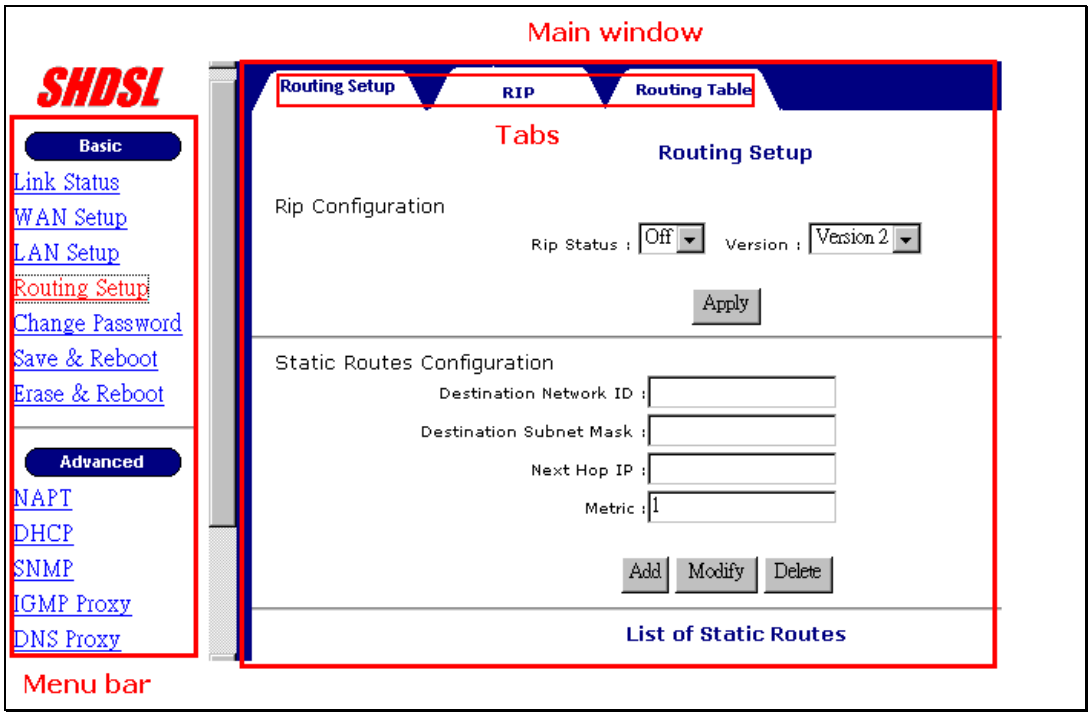
STEP 4: You will be prompted to enter your user name and password. Type your password, or if the password was not changed, type the default passwords. The default ADMINISTRATOR user name and password are **root**.

STEP 5: After successfully logging in, you will reach the main configuration page. The left hand side has a menu and the right side is blank.

3.1.2 Web Page Layout

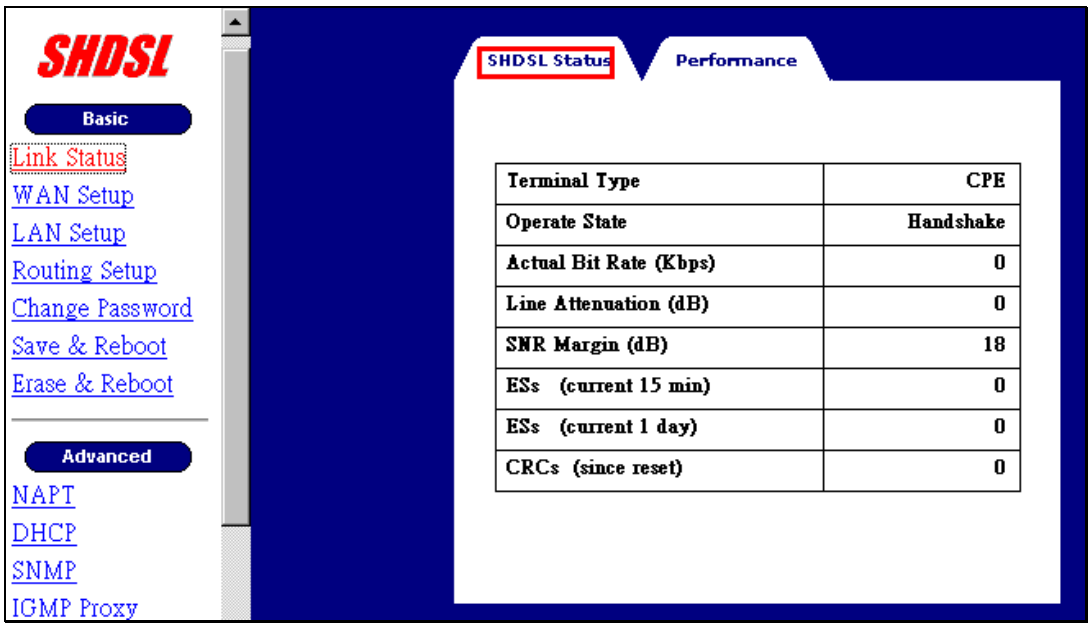
On each Web page, there are two areas.

- **Menu Bar:** On the left side of the Web page is the menu bar. It is divided into two parts: Basic and Advanced. The **Basic** menu bar sets up the device for quick setup. The **Advanced** menu bar configures advance functions such as SNMP, DHCP server, and DNS proxy. The menu also covers the maintenance function.
- **Main Window:** The main window in middle of the page displays after clicking a button on the menu bar. It includes the tabs on the top of the window. The tabs lead to other sub-screens.

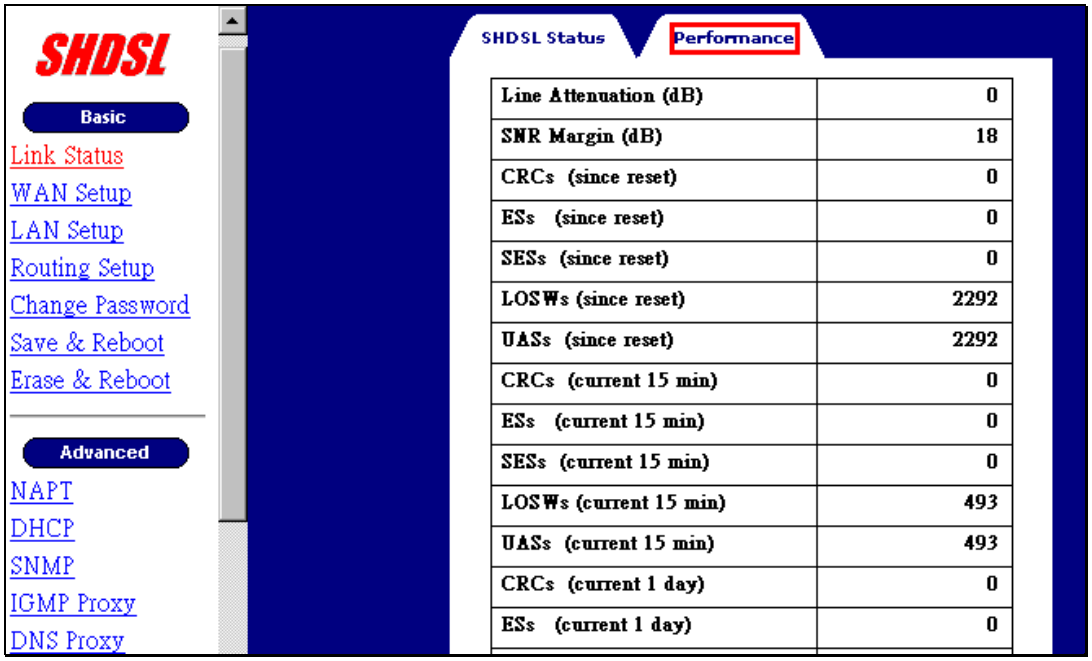


3.1.3 Monitoring the SHDSL Line

Click **Link Status** on the Basic menu bar. The Link Status screen has two tabs: SHDSL Status and Performance. **SHDSL Status** is used to monitor the SHDSL link and the **Performance** is used to monitor the SHDSL performance.



The following is the screen after clicking the **[Performance]** button.



3.2 WAN Interface Configuration

The router supports 16 ATM interfaces. A virtual channel (VC) can be configured for each ATM interface such as ATM1 to VC1, ATM 2 to VC2, and so on. Each VC can be specified with a protocol, which can be RFC 1483 bridged, RFC 1483 Routed, PPPoE, or PPPoA.

By default, VC1 is enabled with the parameters VPI/VCI 0/33 and protocol RFC 1483 Bridged. VC1 can work without any modifications. VCs 2 to 16 are disabled.

If the VC is added on the Basic> Wan Setup, it will be added from VC2 to VC16. (VC1 is already enabled for 0/33).

If a PPPoE-based VC is created on Basic>WAN Setup, the DHCP server will be automatically enabled. If a PPPoE based VC is created on Advanced>Interface, the DHCP server function must be enabled manually.

The WAN interface can be configured to operate in the following modes: bridge, router, PPPoE, or PPPoA. Configuration for each mode is explained in the sections that follow.

3.2.1 Bridge Mode: Service for One Fixed IP Address

To configure one static IP address, you need to set up the VC in RFC 1483 bridged mode. The router has a default Virtual Channel (VC) of 0/33. It can function without other modifications.

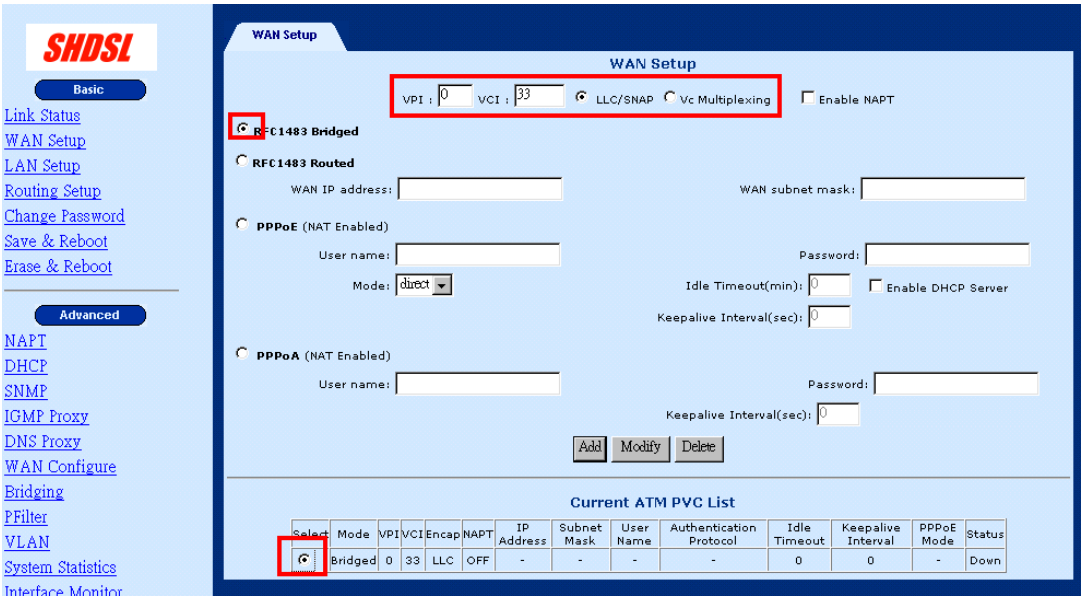
STEP 1: Click **WAN Setup** on the Basic menu bar, and enter values for: VPI, VCI, Encapsulation (LLC or VC MUX).

VPI	Enter a value for the vitual path identifier
VCI	Enter a value for the virtual channel identifier
LLCEncapsulation:	With LLC encapsulation, a link control header is added to the Ethernet packet that identifies the protocol type (Ethernet). This allows multiple protocols to be transmitted over the ATM Virtual Circuit.
VC Multiplexing:	With VC Multiplexing, no link control header is needed as the ATM Virtual Circuit is assumed to be carrying a single protocol.
Enable NAPT	This function cannot be set for bridge mode.

STEP 2: Click on RFC 1483 Bridged.

STEP 3: Click on the **Add** button. The new VC is added in the Current ATM PVC List on the bottom screen.

To modify the VC, click a VC from the Current ATM PVC List to display the parameters of the VC. Change its parameters and click on the **Modify** button.



3.2.2 Router Mode: Service for Five Static IP Addresses

To set up the service for five static IP addresses, you need to set up the VC in RFC 1483 Routed mode.

STEP 1: Click **WAN Setup** on the Basic menu bar.

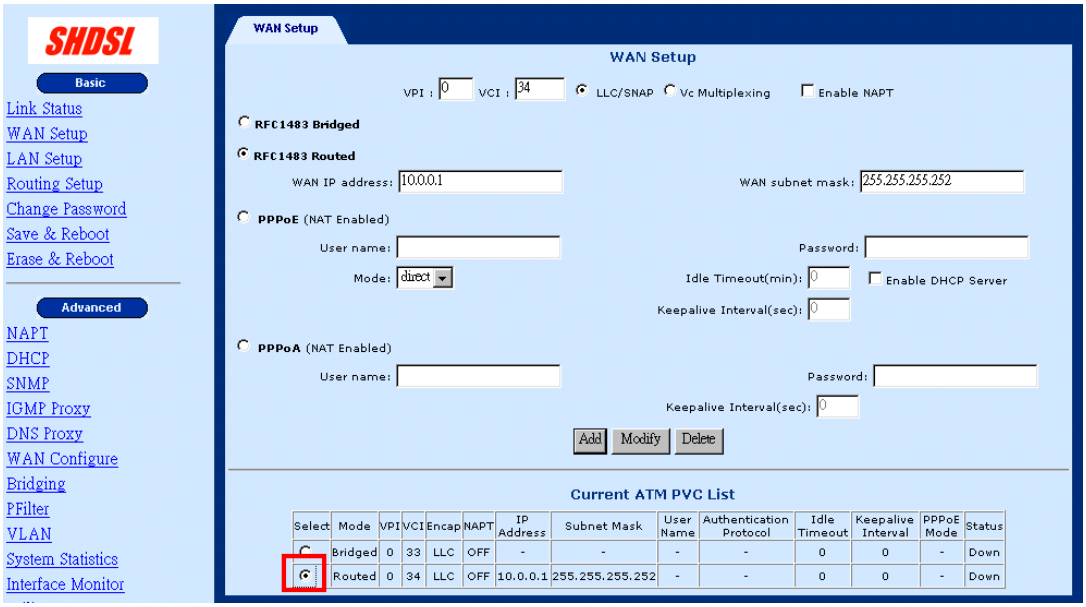
STEP 2: Enter values for: VPI, VCI, Encapsulation (LLC or VC MUX), Enable NAPT.

VPI	Enter a value for the vitual path identifier
VCI	Enter a value for the virtual channel identifier
LLCEncapsulation:	With LLC encapsulation, a link control header is added to the Ethernet packet that identifies the protocol type (Ethernet). This allows multiple protocols to be transmitted over the ATM Virtual Circuit.
VC Multiplexing:	With VC Multiplexing, no link control header is needed as the ATM Virtual Circuit is assumed to be carrying a single protocol.
Enable NAPT	Selecting **Enabling NAPT** will enable Network Port Address Translation on the WAN interface.

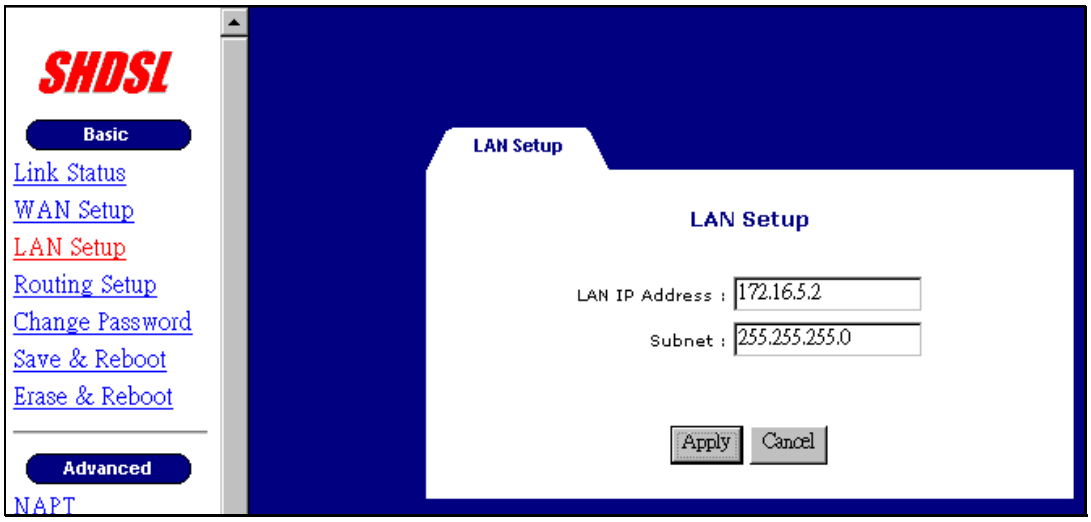
STEP 3: Click on the **RFC 1483 Routed** option.

STEP 4: Click on the **Add** button. The new VC is added in the Current ATM PVC List on the bottom screen.

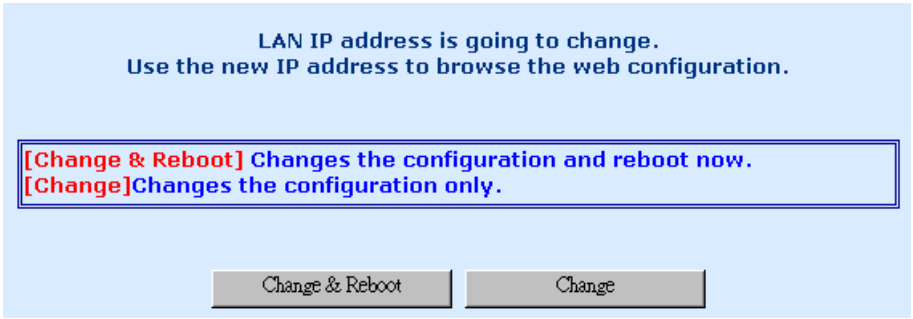
To modify the VC, click a VC from the Current ATM PVC List to display the parameters of the VC. Change its parameters and click on the **Modify** button.



After creating an RFC 1483 Routed VC, click **LAN Setup** to set up the router's Ethernet IP address.



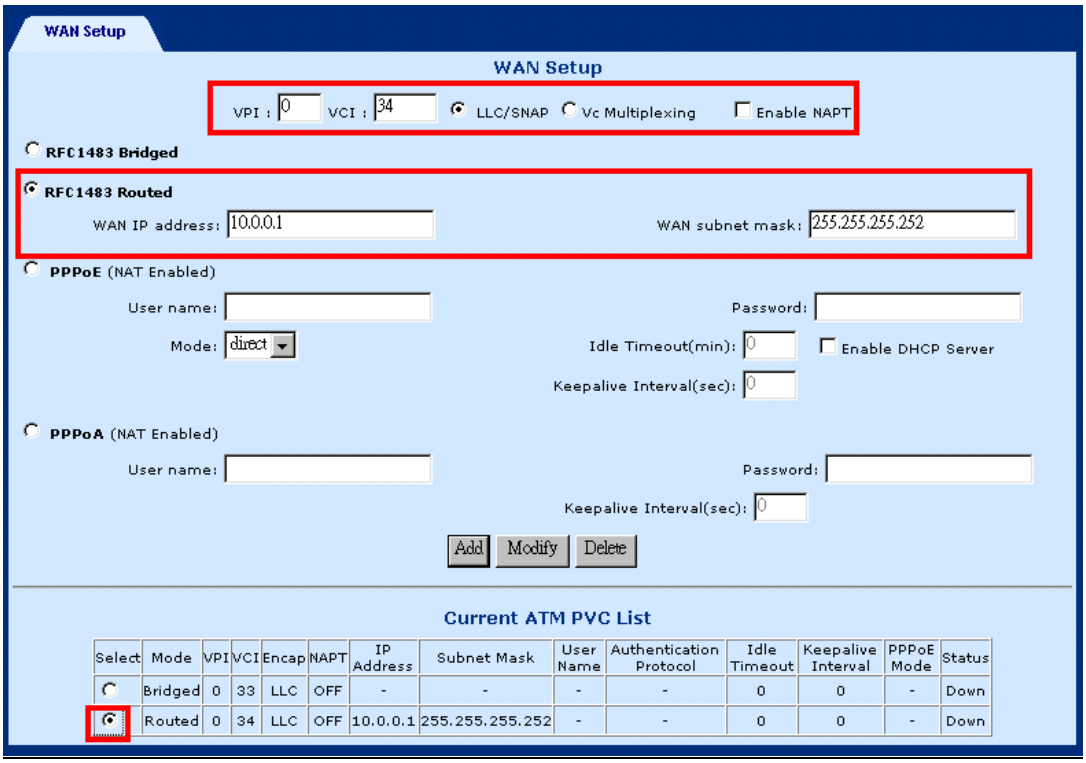
- After changing the IP address, click **Apply** to display the following screen. The Change & Reboot button allows you to use the new IP address and reboot the router immediately. The Change button allows using the IP address immediately but you need to save the setting by clicking **Save & Reboot** on the Basic menu bar. To use the Web Browser, make sure you change the PC's IP address.



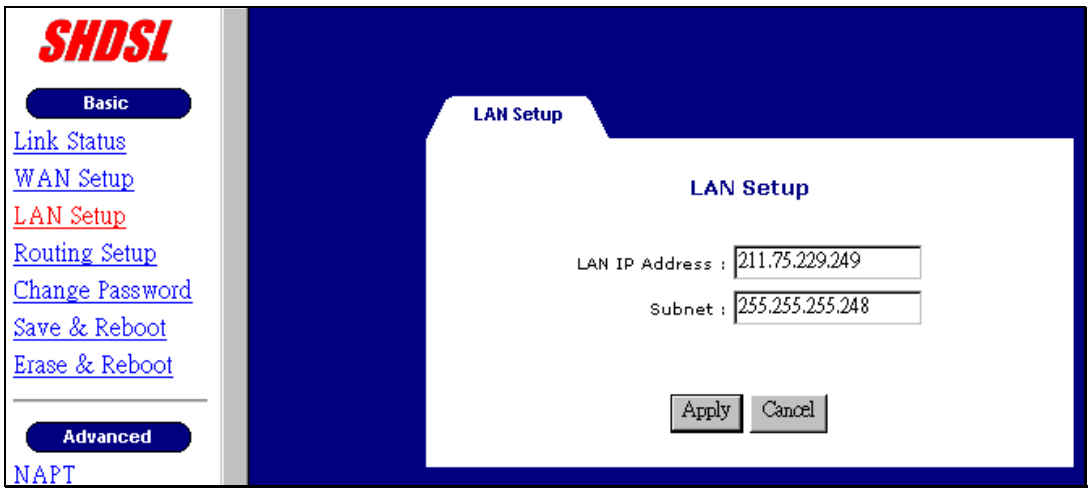
For example, to change the VC 0/34 from Mode RFC 1483 Bridged to Mode RFC 1483 Routed, follow the steps below.

STEP1: Click **WAN Setup** on the Basic menu bar.

STEP2: select 0/34 from the Current ATM PVC List to display the parameters and click **RFC 1483 Routed** and then click on the **Modify** button.

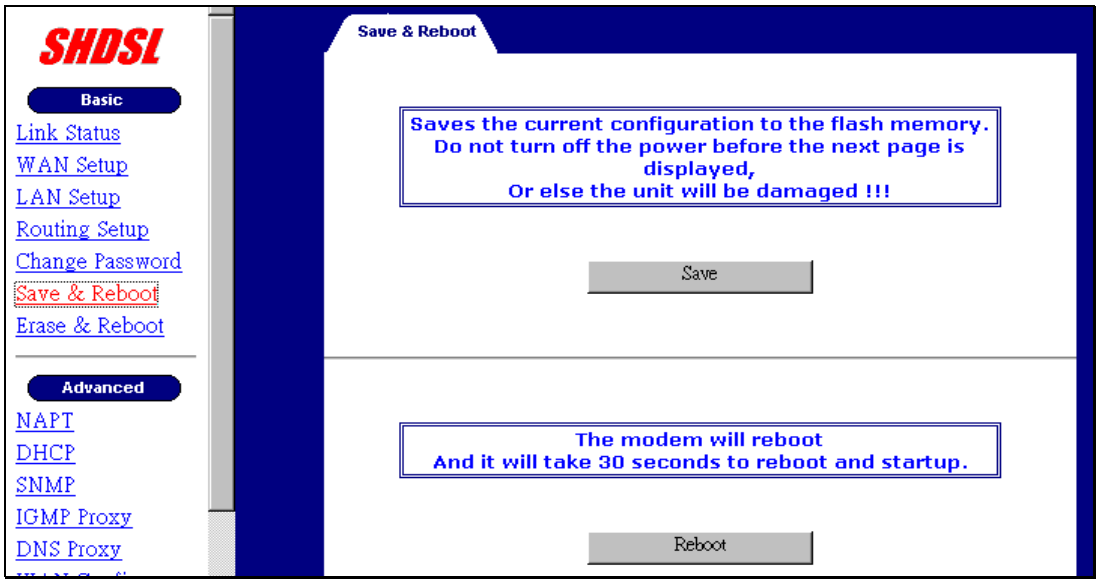


STEP 3: Click **LAN Setup** on the menu bar to type the IP address for the LAN port. Click **LAN Setup** on the menu bar and type the IP address and Subnet (should be 255.255.255.248 for static five IP address service) and then click **Apply**.



Note: After the IP address is changed, your PC and the router are on different network segments. Therefore, you cannot use the web browser to configure the router. You must change your PC's IP address.

STEP 4: Click **Save & Reboot** on the Basic menu bar to save your settings.



3.2.3 PPPoE

When a VC is set in the PPPoA, the router will auto-detect the Authentication code (PAP or CHAP). The NAPT and DHCP server functions will be enabled automatically.

STEP 1: Click **WAN Setup** on the Basic menu bar and enter the following parameters to set up the PPPoE.

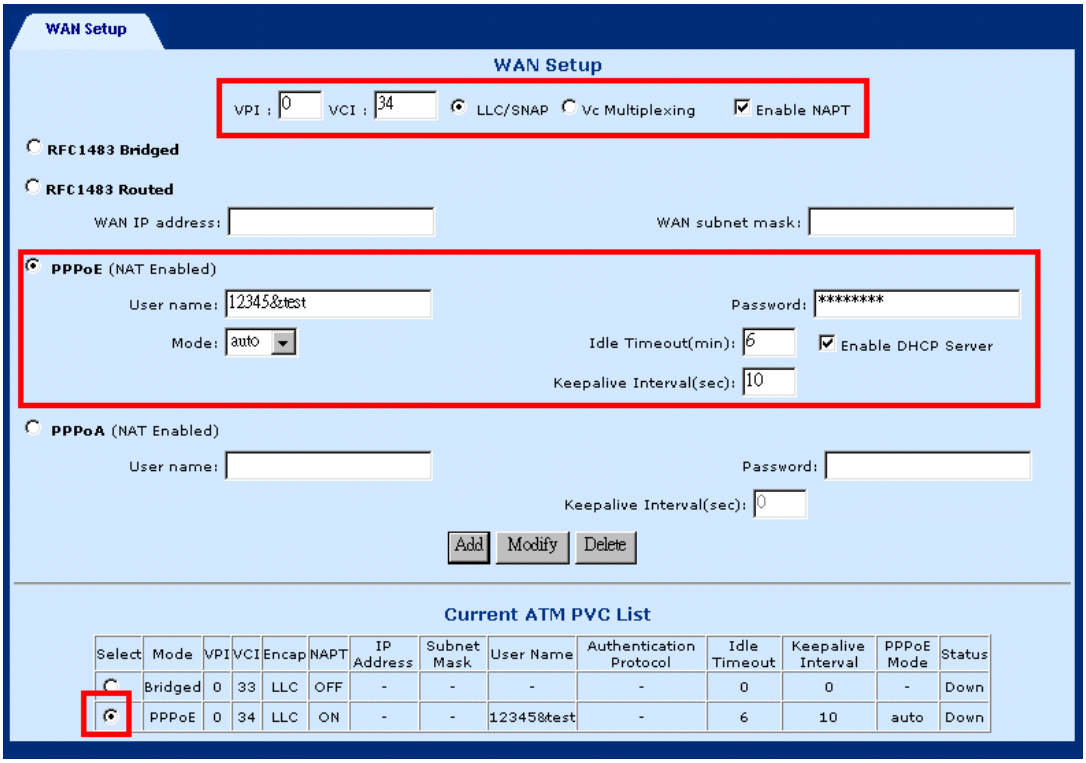
VPI	Enter a value for the vitual path identifier
VCI	Enter a value for the virtual channel identifier
LLCEncapsulation:	With LLC encapsulation, a link control header is added to the Ethernet packet that identifies the protocol type (Ethernet). This allows multiple protocols to be transmitted over the ATM Virtual Circuit.
VC Multiplexing:	With VC Multiplexing, no link control header is needed as the ATM Virtual Circuit is assumed to be carrying a single protocol.
Enable NAPT	Selecting **Enabling NAPT** will enable Network Port Address Translation on the WAN interface.
User Name/Password	These two fields are used for remote subscriber to log on for Internet access.
Mode	Direct and Auto. If the mode is set to Auto, the PPPoE negotiation automatically starts when the system identifies any traffic required to be transferred on the link. When DIRECT is selected the PPPoE negotiation is started manually.

Idle Timeout	The Idle Time field defines the period of idle time after which the PPPoE link will be terminated. It is functional in the auto mode. The default setting is 5 minutes. In Direct mode, this function is not used and the field displays zero.
Enable DHCP server	Check the item to enable the DHCP server or uncheck it to disable it.
Keepalive Interval(sec):	Keep-alive is a networking operation that periodically (default-every 10 seconds) checks the availability of a PPPoE/PPPoA connection between the CO and CPE. If the keep-alive message is not acknowledged, the connection will be interrupted.

STEP 3: Click **PPPoE**, and type the user name and password that the remote subscriber needs for Internet access.

STEP 4: Click on the **Add** button. The new VC is added in the Current ATM PVC List on the bottom screen.

To modify the VC, click a VC from the Current ATM PVC List to display the parameters of the VC. Change its parameters and click on the **Modify** button.



3.2.4 PPPoA

When a VC is configured for PPPoA, the router will auto-detect the Authentication code (PAP or CHAP), and the NAPT function will be enabled automatically.

STEP 1: Click **WAN Setup** on the Basic menu bar.

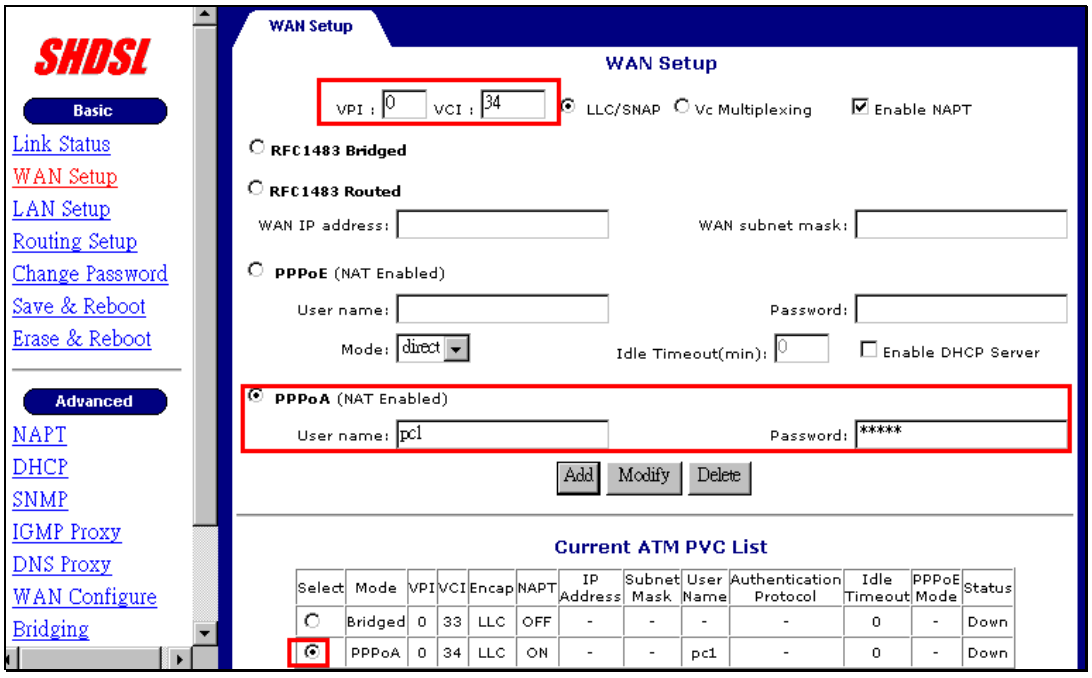
STEP 2: Enter values for the following fields: VPI, VCI, Encapsulation (LLC or VC MUX), Enable NAPT.

VPI	Enter a value for the vitual path identifier
VCI	Enter a value for the virtual channel identifier
LLC Encapsulation:	With LLC encapsulation, a link control header is added to the Ethernet packet that identifies the protocol type (Ethernet). This allows multiple protocols to be transmitted over the ATM Virtual Circuit.
VC Multiplexing:	With VC Multiplexing, no link control header is needed as the ATM Virtual Circuit is assumed to be carrying a single protocol.
Enable NAPT	Selecting **Enabling NAPT** will enable Network Port Address Translation on the WAN interface.
Keepalive Interval(sec):	Keep-alive is a networking operation that periodically checks the availability of a PPPoE/PPPoA connection between the CO and CPE. If the keep-alive message is not acknowledged, the connection will be interrupted.

STEP 3: Click **PPPoA**, and type the user name and password that the remote subscriber needs for Internet access.

STEP 4: Click on the **Add** button. The new VC is added in the Current ATM PVC List on the bottom screen.

To modify the VC, click a VC from the Current ATM PVC List to display the parameters of the VC. Change its parameters and click on the **Modify** button.



3.2.5 Password Setup

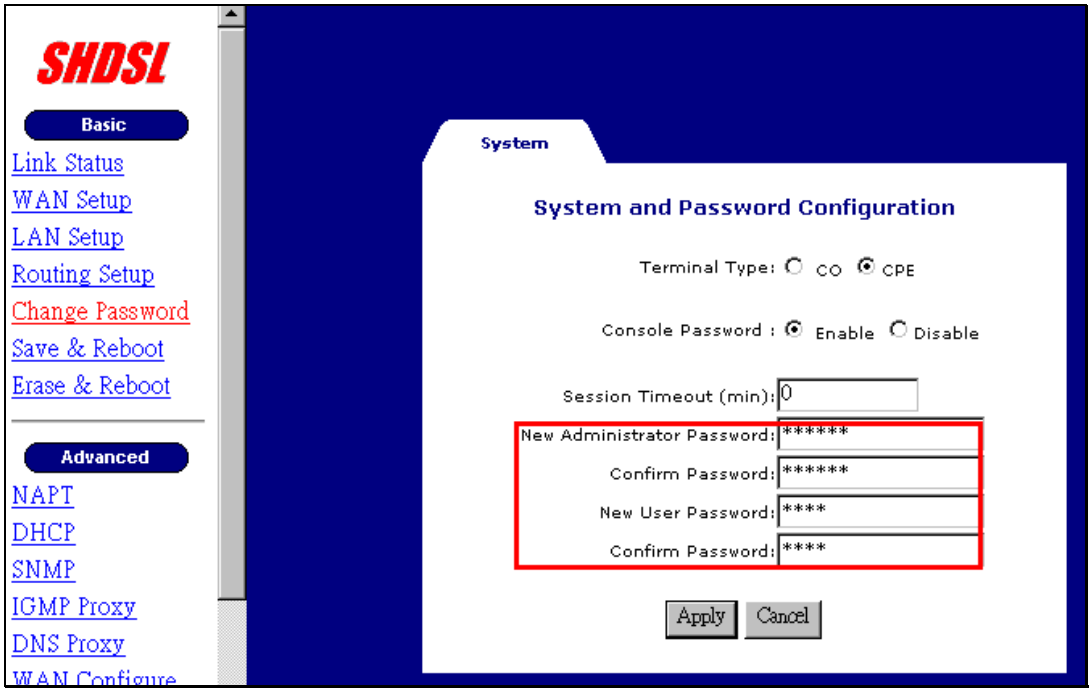
There are two types of access privileges. A system ADMINISTRATOR is the only person that can configure, change parameters, monitor, and read the performance and status of the system. A USER can only monitor and read the status of the system. The password for access through the Web is the same as for Telnet access.

To set up a password, complete the following steps:

STEP 1 Click **Change Password** on the Basic menu bar.

STEP 2 Enter the passwords for Administrator and User, and confirm the new password by re-typing the password again.

STEP 3 Click **Apply** to complete the settings and save the setting by entering the **Save & Reboot** screen on the basic menu bar.



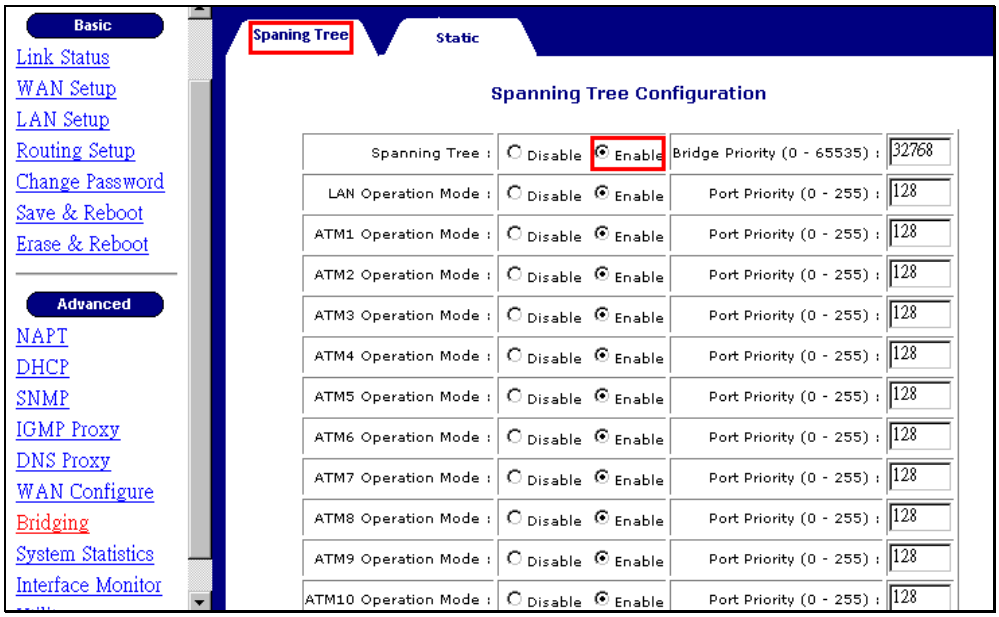
- Terminal Type: When the router is connected to the DSLAM, select CPE. When the router is connect to a router for point to point application, one of the devices should be set to CO with the other set to CPE. The default setting is CPE.
- Console Password: **Disabled**, a local user does not have to enter a password to enter the console mode. **Enabled**, users who attempt to access the device from the console will be prompted for the password.
- Session Timeout: The console or telnet session will be terminated after this idle time. It is calculated in minutes. Users need to re-log on to the device when the session times out. The default setting is zero, which means the function is disabled.

3.2.6 Setting the Bridge

Click on **Bridging** on the Advanced menu bar to set up the static bridging and Spanning Tree Protocol (STP) functions.

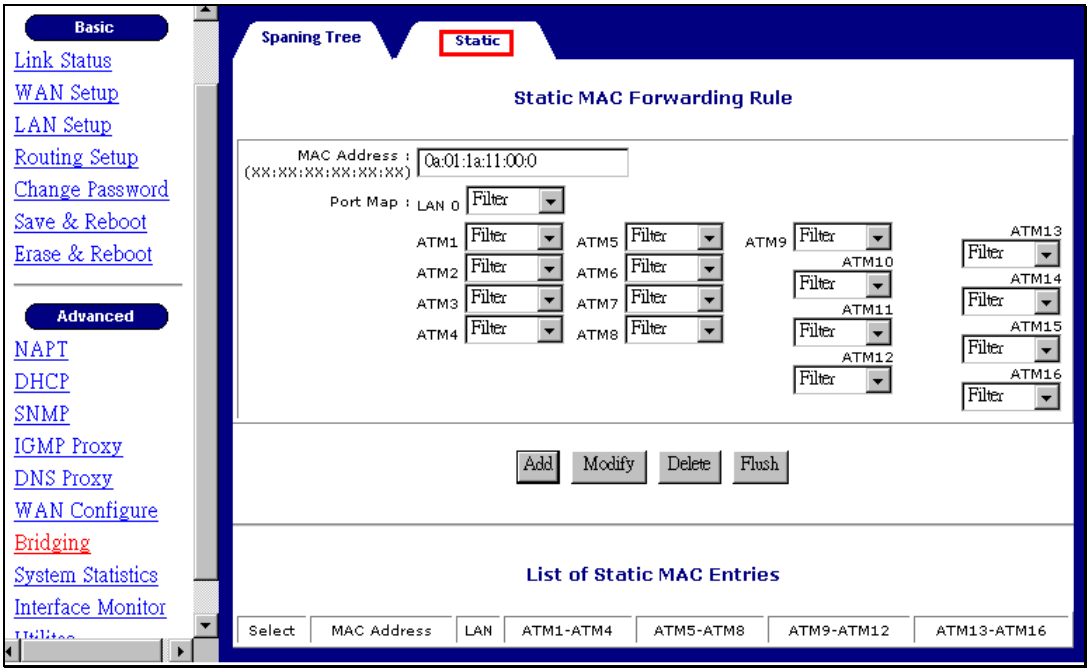
3.3 Spanning Tree Protocol

The STP function is disabled by factory default. To enable it, click **Enable** in the Spanning Tree field and configure the interfaces on the screen. When the parameters are set up, click **Apply** to submit the settings.



3.4 Static Bridging

Click on the **Static** tab to configure, modify, and delete the static bridging functions.



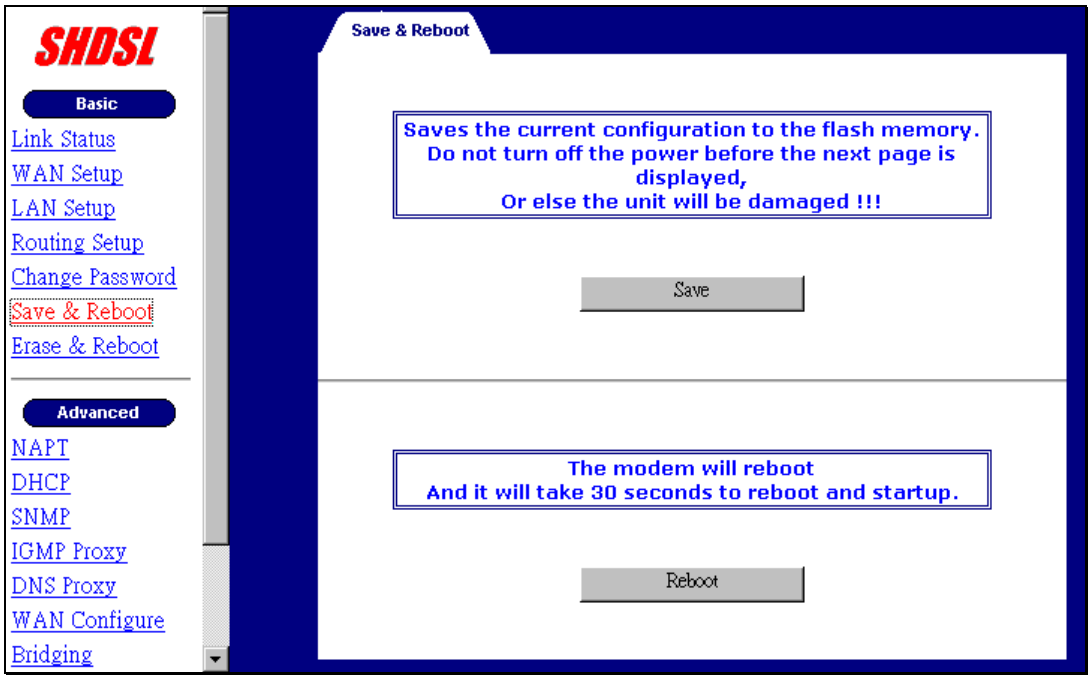
Add	Add a static bridging entry
Delete	Delete a static bridging static entry
List	Displays all the static bridging entries
Flush	Delete all the static bridging entries

- MAC Address: This is the MAC address of the PC. Each PC has a unique MAC address, such as 0a:01:1a:11:00:0b.
- Port Map: There are three modes to set up the data processing method for the LAN and ATM interfaces: **filter**, **forward**, and **dynamic**. For example, if the Port Map is set to: LAN – Forward, and others- Filter, it means the packets will be forwarded to the LAN interface and will not reach the ATM interfaces. In dynamic mode, the operating mode of the MAC address in the interface follows the learning result of the bridging function.

3.4.1 Write System Configurations

The new parameters can function immediately without being saved to the flash memory. To use these parameters after you restart the router, you must save them to the flash memory.

To write the configurations, click on the **Save & Reboot** button. Click on the **Save** button on the main screen. If you need to reboot the device after writing the configurations, also click on the **Reboot** button.



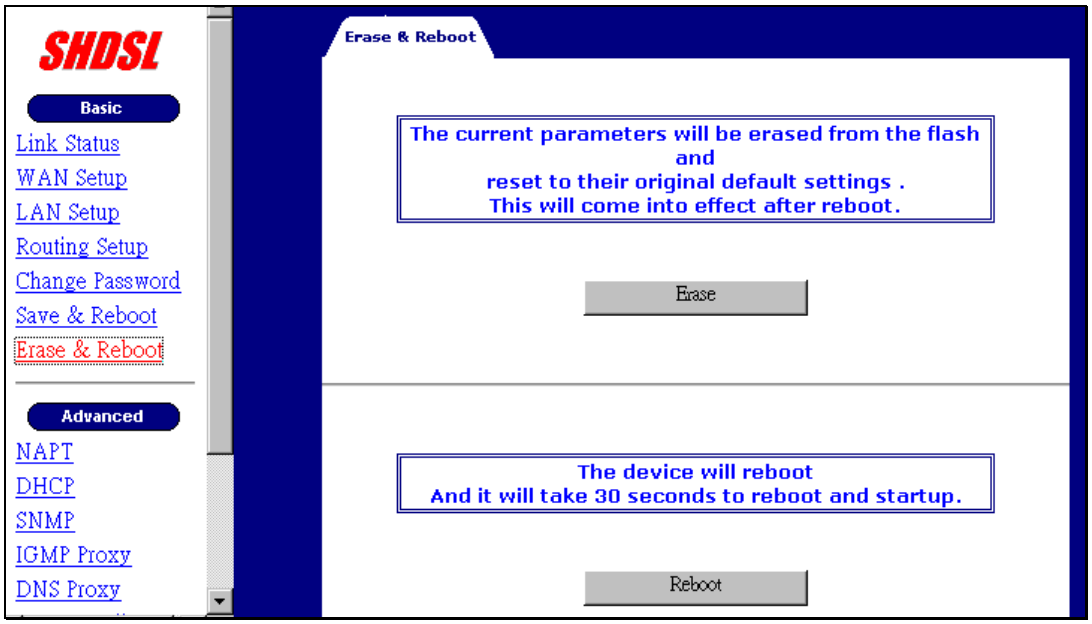
3.4.2 Load Factory Default Values

Caution! If you reset your device to the factory defaults, any changes to parameters will be lost and all parameters will revert to their default values.

To retrieve the factory default settings:

STEP 1: Click **Erase & Reboot** on the Basic menu bar.

STEP 2: Click **Erase** and **Reboot** respectively.

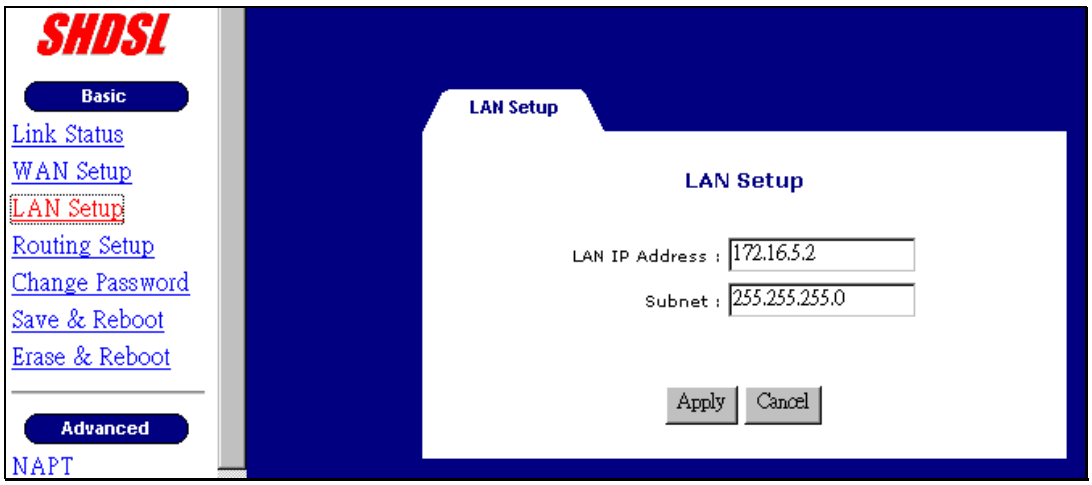


CHAPTER 4 Setting up WAN and LAN Interfaces

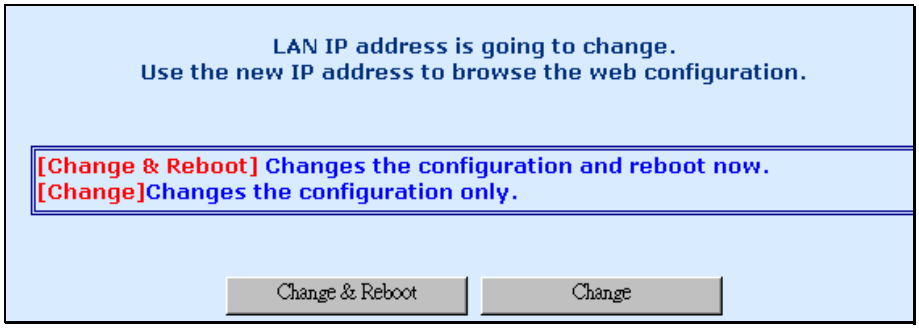
4.1 LAN Interface

To set up the Ethernet Interface:

STEP 1: Click **LAN Setup** on the Basic Menu bar.



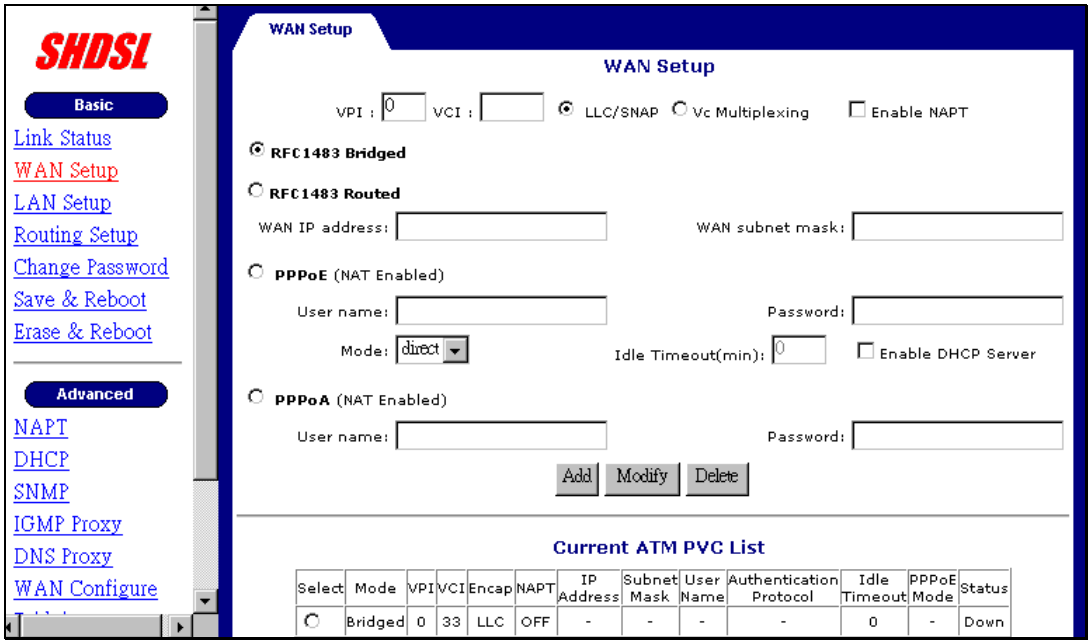
STEP 2: Enter the new IP address and Subnet, and click on **Apply** to display the following screen.



STEP 3: You can click on the **Change & Reboot** button to use the new IP address and reset the device immediately. This does not require the Save action. Alternatively, you can click on the **Change** button to use the new IP address, but you need to save the new setting before you reset the router. After the IP address is changed, to be able to use the Web browser or Telnet, make sure your PC's IP address is set to the same network segment.

4.2 Configuring the WAN Interface

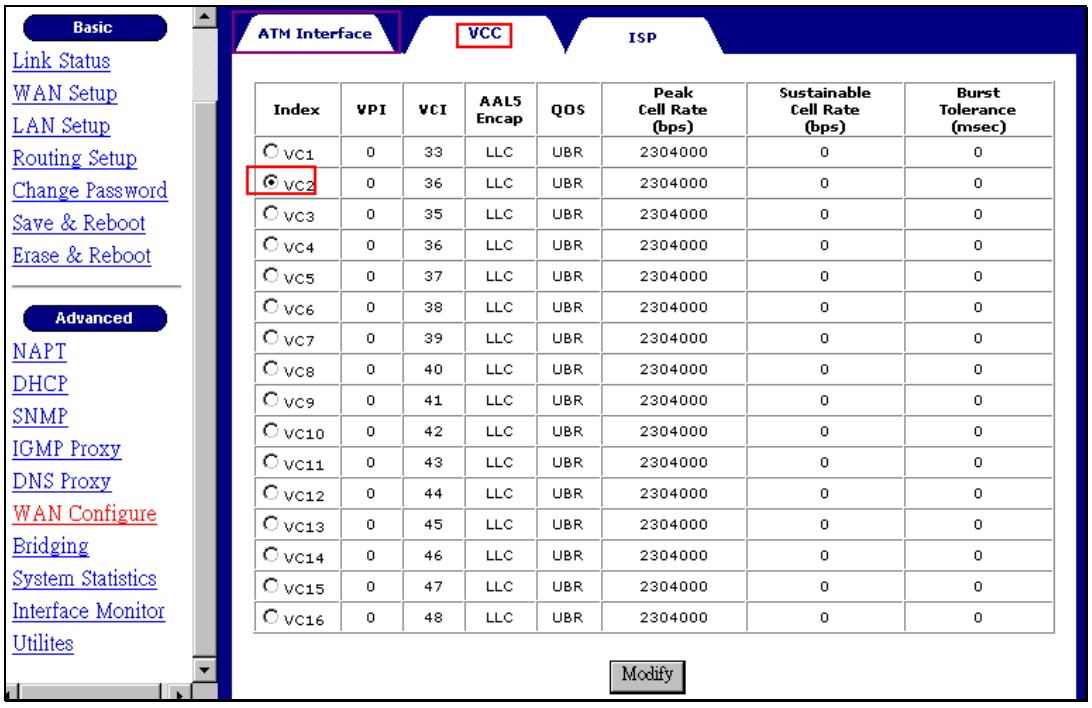
Click **WAN Setup** on the Basic menu bar and configure the VC to RFC 1483 Bridged, RFC 1483 Routed, PPPoE, or PPPoA. To set up these services, refer to Section 3.2.



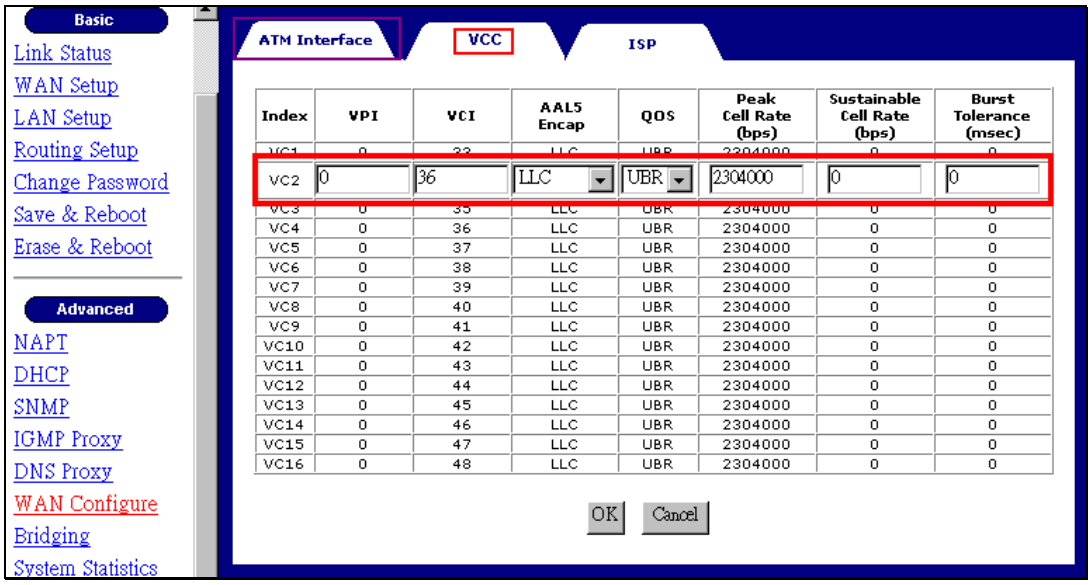
4.2.1 VC Data Flow Control

To set up the flow control parameters, such as AAL5 encapsulation, QOS, Peak Cell Rate, Sustainable Cell Rate, and Burst Tolerance, follow the steps below.

Click **WAN Configure** on the Advanced menu bar, and click on the **VCC** tab on the main menu.

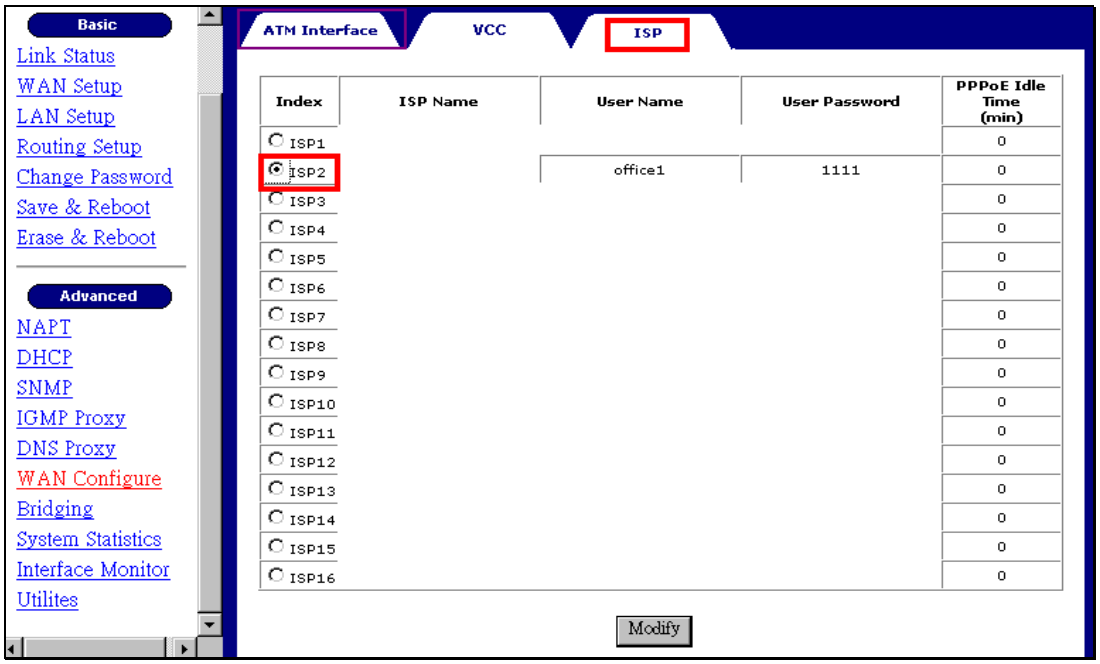


Select a VC in the Index field and click on the **Modify** button to configure the VC's flow control parameters. Click on **OK** to complete the settings.

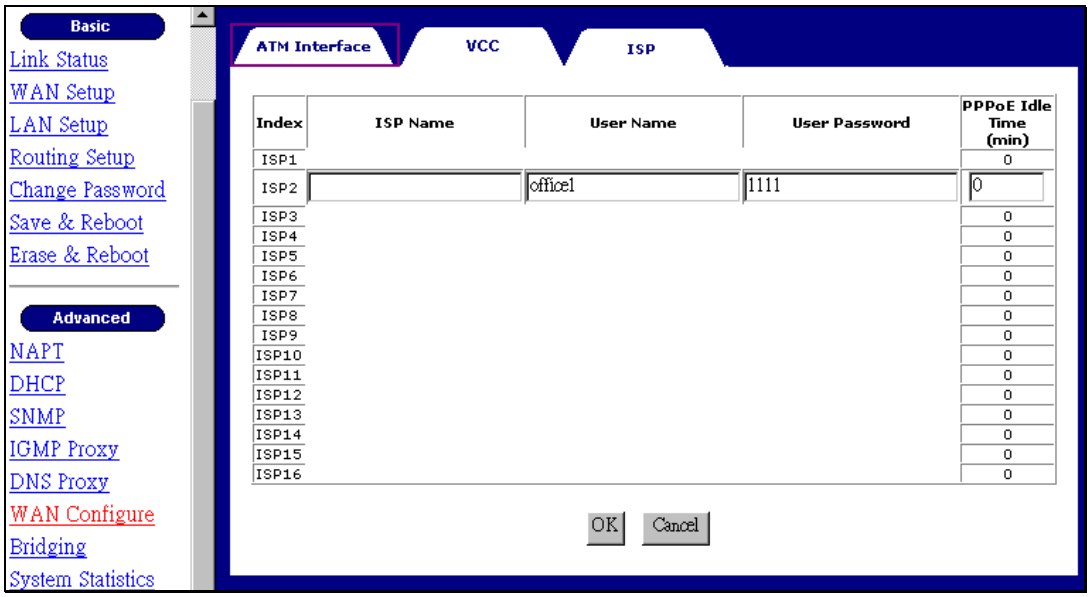


4.2.2 Setting up an ISP

The router supports connection to up to 16 ISPs. Each ATM Interface can connect to an ISP.To set up or configure the connection parameters to ISP, click on **WAN Configure** on the Advanced menu bar. Click on the **ISP** tab on the main screen.



Select an ISP and click on the **Modify** button on the bottom screen. After modifying the parameters, click on **OK** to complete the settings.

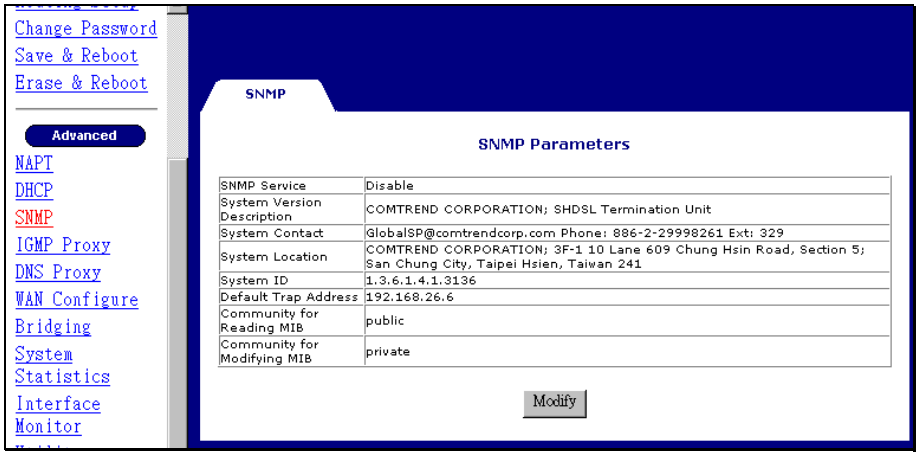


CHAPTER 5 SNMP

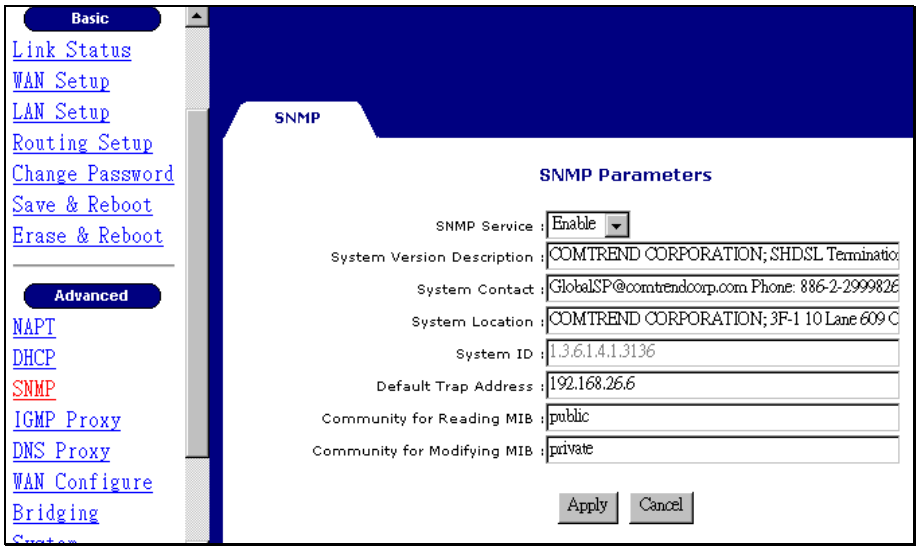
The default setting of the SNMP function is enabled. SNMP is a software entity that responds to information and action request messages sent by a network management station. The messages exchanged enable you to access and manage objects in an active or inactive (stored) MIB on a particular router.

5.1 Enable SNMP

To configure the SNMP parameters, click on the **SNMP** button on the Advanced menu bar. The window displays the SNMP parameters.

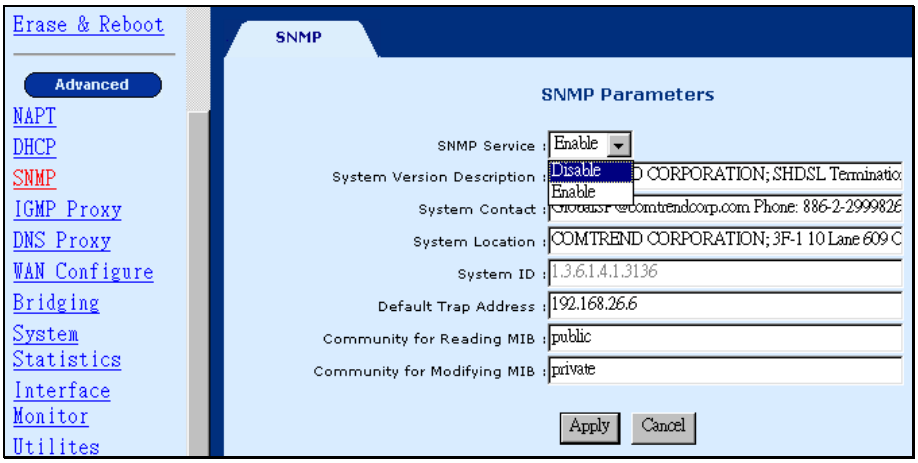


To modify the SNMP parameters, click on the **Modify** button at the bottom of the screen. Click **Apply** to submit the settings.



5.2 Disable SNMP

Click **SNMP** on the **Advanced** menu bar and click on the **Modify** button at the bottom of the screen. Choose Disable in the SNMP Service field and click on **Apply** to submit the setting.

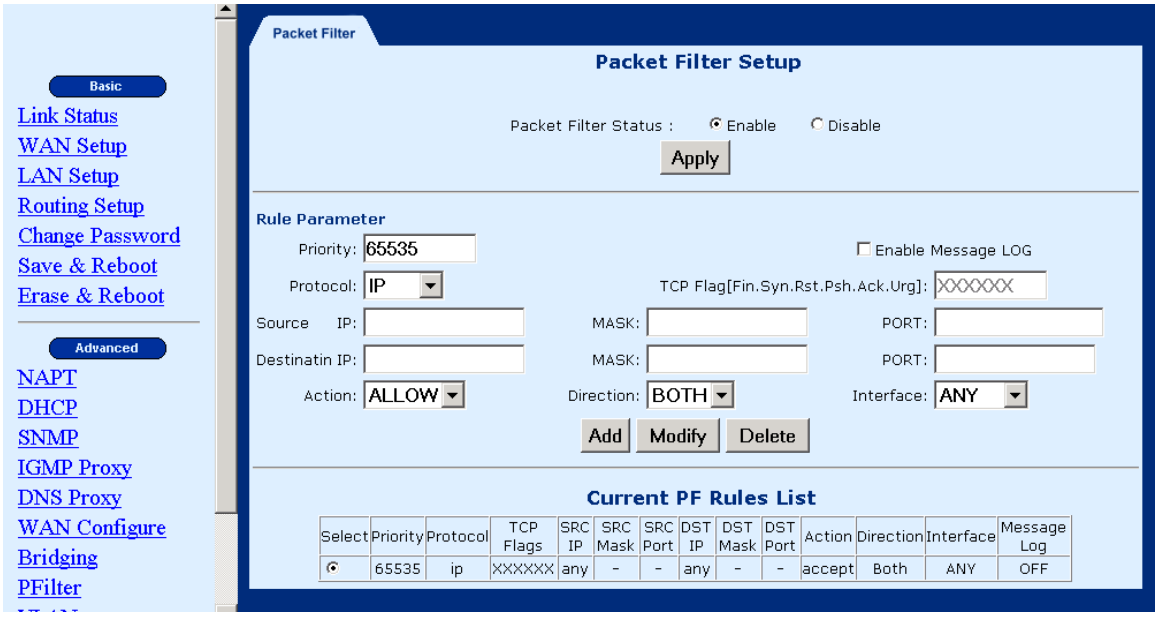


CHAPTER 6 Packet Filter

Packet filter, a firewall security measure, examines incoming and outgoing packet headers (IP address, port number, and so on) on the network and determines whether to forward the packets based on user-defined rules (deny, accept, and count).

The SHDSL router provides packet filter and stateful packet inspection. It has denial of service protection against attacks such as ICMP Flood, Ping of Death, IP spoofing, Port Scans, Land Attacks, Tear Drop Attacks, IP Source Route and WinNuke Attacks.

To access the packet filter functions, select **Packet Filter** from the advanced menu. The screen will display as below, showing a list of the currently configured filter entries.



6.1.1 Add a Packet Filter entry

To add a Packet Filter, complete the following steps:

STEP 1: Click on the **Add** button, the Packet Filter Add screen will appear.

STEP 2: Enter values for the parameters (explained below).

STEP 3: Click on the **Apply** button at the bottom of the page.

Priority	You can enter a number here to assign the priority of a filter, in case there are overlapping rules. The lower the number the higher its priority.
Protocol	Select from TCP/UDP/ICMP/IP.
Source IP	Source IP of a packet you wish to filter.
Source Mask	Source Mask of a packet.
Source Port	Source Port of a packet you wish to filter.

Destination IP	Destination IP of a packet you wish to filter.
Destination Mask	Destination Mask of a packet.
Destination Port	Destination Port of a packet you wish to filter.
TCP Flag ([F.S.R.P.A.U]	This field allows you to filter according to a TCP flag.
Action	This field determines the action the router will take when it receives a packet that corresponds to a filtering rule. It can be set to: **allow**, to let the packet pass through the filter. **deny,** to drop the packet. **count**, which has no effect on whether the packet will be allowed through the filter, causes the packet to be included in the accounting statistics kept by the filter.
Interface	You can choose to apply this setting to a specific LAN or ATM interface. This function is called **Packet Binding.** **Packet Binding** is a function that can be used when we have multiple Virtual Channels (VC) and we are utilizing IP Packet Filtering. In some cases, we may not wish to apply the packet filtering to all VCs. In this case, we can bind IP packet filtering to a VC. This means that filtering will only be applied to the bound VC, and thus the remaining VCs will not filter packets.
Direction	This field determines whether the rule applies to **In**bound, **out**bound or **both** directions

6.1.2 Delete a Packet Filter entry

To delete an entry, select an entry from the list, and click on **Delete**.

6.1.3 Enable/Disable Packet Filter

If you wish to Enable or Disable the Packet Filter, click **Enable** or **Disable** and click on the **Apply** button.

CHAPTER 7 Routing

This chapter describes how to set up the static routes and RIP. Click **Routing Setup** from the Basic menu bar to configure the routing functions.

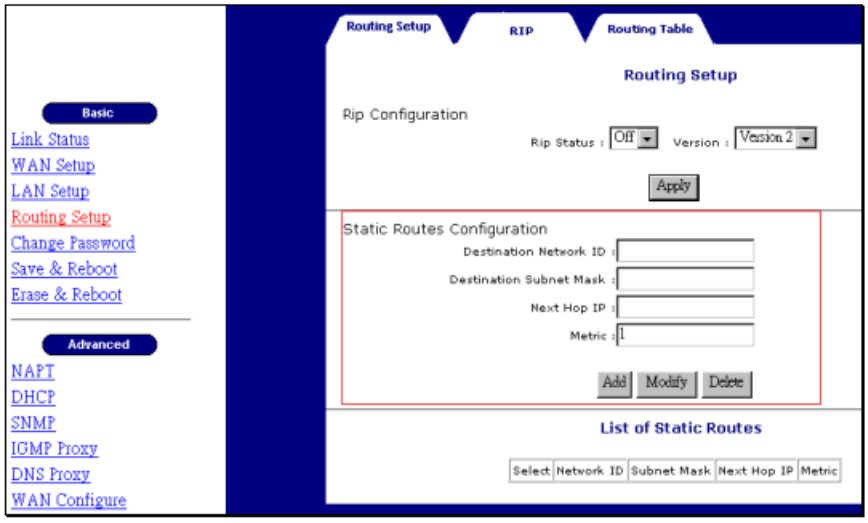
7.1 Static Route

The Static Route Configuration field allows you to add, modify, and delete a static route. Type the Destination Network ID, subnet mask, and next hop IP and click a button below to perform the requested function.

The router has no default static route. After an RFC 1483-routed VC is created, a static route as follows will be created.

Network ID	Subnet Mask	Next Hop IP
0.0.0.0	0.0.0.0	10.0.0.2

Click **Routing Setup** on the Basic menu bar to access the Routing Setup window. It allows adding, modifying, and deleting the static routes.



Add:

To add a static route complete the following steps:

STEP 1: Enter the parameters for Destination Network ID, Subnet Mask, Next Hop IP

STEP 2: Click on the **ADD** button

Modify:

To modify a static route complete the following steps:

STEP 1: Select the entry you wish to modify from the List of Static Routes

STEP 2: Change the parameters

STEP 3: Click on the **Modify** button

Delete:

STEP 1: Select the entry you wish to **delete** from the List of Static Routes

STEP 2: Change the parameters

STEP 3: Click on the **Delete** button

7.2 Set Up the RIP function

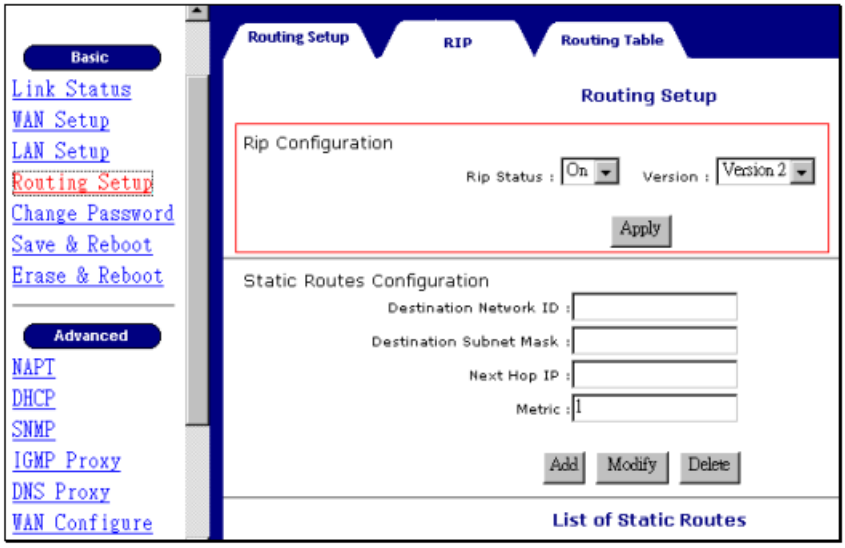
To enable the RIP, complete the following steps:

STEP 1: Click **Routing Setup** from the Basic menu bar

STEP 2: Select **On** in the Rip Status field.

STEP 3: Select a RIP Version (Version 1 or Version 2) from the Version field.

STEP 4: Click **Apply** to submit the settings.



To configure the advance functions of the RIP, click on the **RIP** tab on the main screen, and configure the requested parameters.

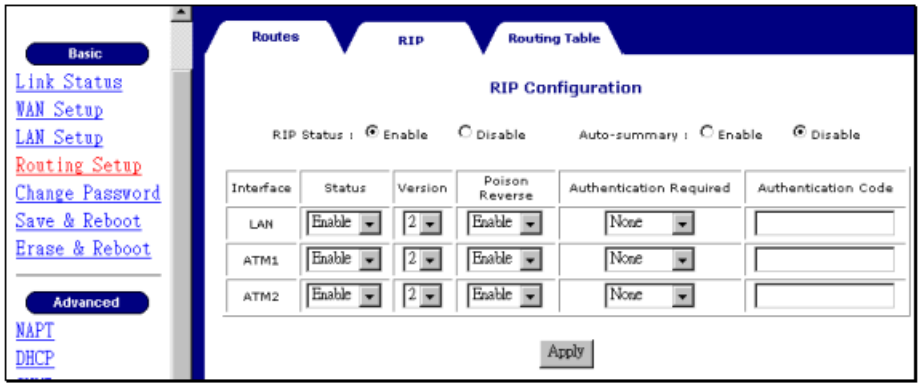
Mode:	Select **Enabled**
Version:	RIP version 2 or version 1
Authentication:	**none:** no authentication code is required. **PlainText:** an authentication code is required. You should also fill in the Authentication Code field to assign a password. **MD5:** an authentication code is required. You should also fill in the Authentication Code field to assign a password.

Poison Reverse:	**Enabled:** to enable the Poison Reverse **Disabled:** to enable the Splitting Horizon The default setting of poison reverse parameter is **Enabled**. It means the router adopts the split horizon with poison reverse scheme to avoid routing loop problems. If the parameter is **disabled**, the router will use the simple split horizon scheme to solve the problem.
Authentication Code:	Enter the password for authentication.

- Mode: Enabled
- Auto Summary: Enabled, Disabled

The RIP function is now enabled. The default RIP parameter for each interface is RIPv2. In this default mode, this router can operate normally without other adjustments. If you want to configure advanced RIP functions, perform the procedures that follow.

Enter BASIC/ROUTING/RIP/INTERFACE/LAN to configure the parameters.

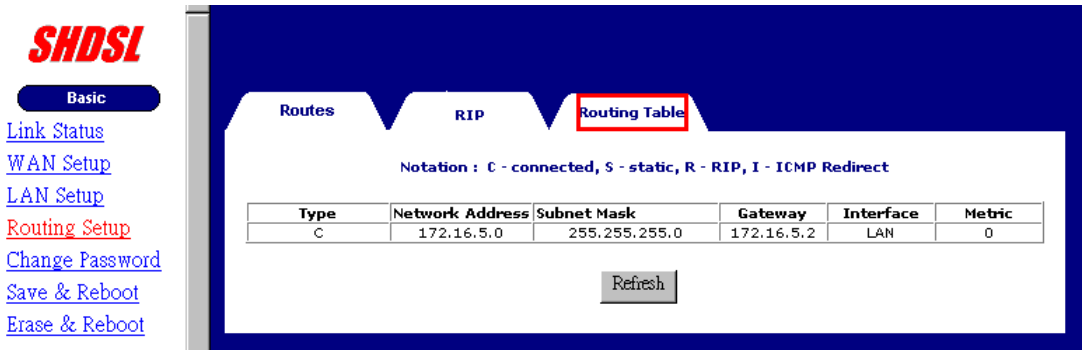


7.3 Displaying the Routing Table

To display the routing table, you can enter either of the following screens:

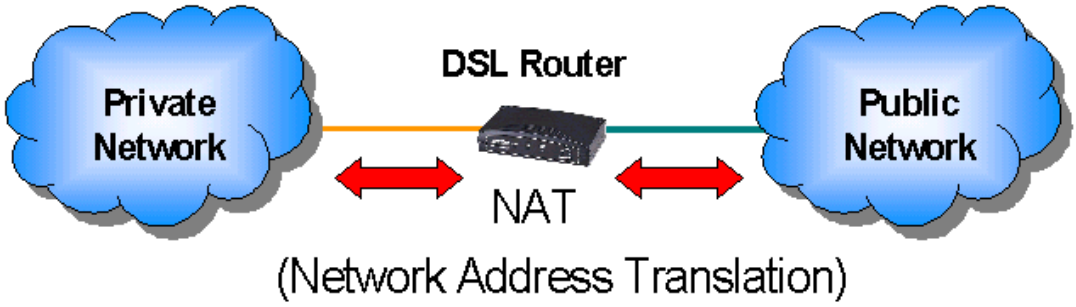
- BASIC/ROUTING SETUP/ROUTING TABLE screen
- Advance/Utilities/Routing Table

The following routing table appears after clicking Basic>Routing Setup>Routing Table.



CHAPTER 8 NAT

Network Address Translation (NAT or NAPT) is a transparent routing function that translates a private IP address on a LAN into a public address that can be used in a public network. Port Address Translation (PAT) is a form of NAT that maps multiple private IP addresses to a single public IP address. Port numbers (TCP or UDP) ensure that packets are delivered properly. Both Network Address Translation (NAT) and Port Address Translation (PAT) are supported by this router. NAT and PAT are common solutions for: overcoming the shortage of public IP addresses, security (private IP addresses are not transparent), and assisting network administration.



The router supports many types of NAT functions, including:

- Fixed-NAT: this maps a private IP address to a public IP address.
- Multi-NAT: this maps multiple private IP addresses to multiple public IP address.
- PAT: When private IP addresses are more than public IP addresses, port address translation is supported to translate the public IP addresses.

Note the usage of synonyms below:

Local: private, illegal, unregistered

Public: legal, registered

In PPPoE or PPPoA mode, the NAT function is automatically enabled. In RFC 1483 Routed mode, to enable NAT, you must select the Enable NAPT item on the WAN Setup screen.

The following pages describe how to set up a virtual server (Redirect port) and different types of NAT.

8.1 Multiple to One

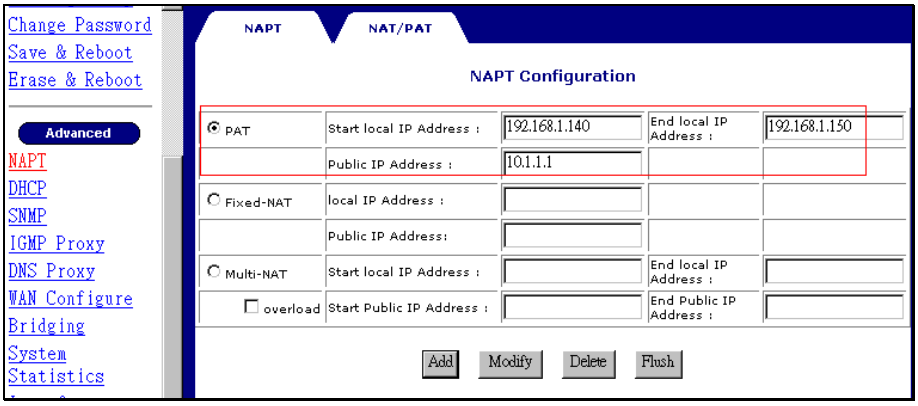
This application requires a series of private IP addresses (such as 192.168.1.140- 192.168.1.150). These private IP address share a public IP address, such as 10.1.1.1.

STEP 1: Click on **NAPT** on the Advanced menu bar.

STEP 2: Click on **PAT** and enter the following parameters:

- **Start Private IP Address:** Type the first IP address. For example, 192.168.1.140
- **End Private IP Address:** Type the last IP address. For example, 192.168.1.150
- **Global IP Address:** Type the public IP address. For example, 10.1.1.1.

STEP 2: Click on the **Add** button to submit the settings.



8.2 One to One NAT

One-to-one NAT maps a private IP address to a public IP address, such as 192.168.1.10 to 10.1.1.34.

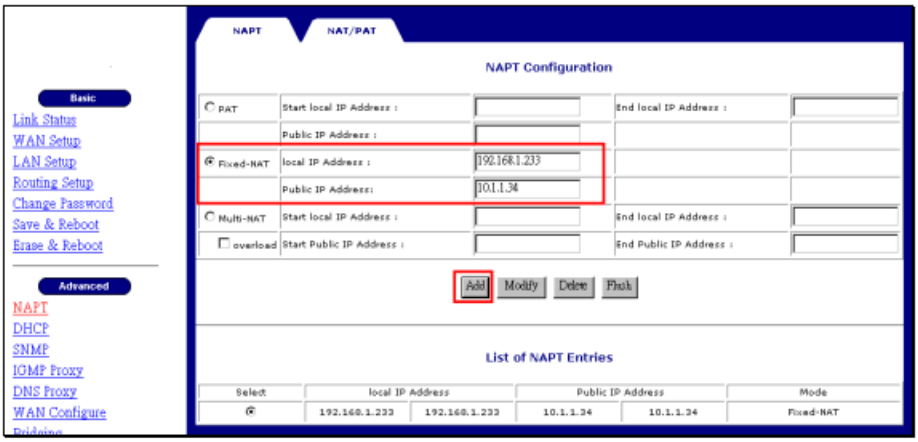
Click **NAPT** on the **Advanced** menu bar and click on the **NAT/PAT** tab to access the NAT/PAT Configuration screen.

Follow the steps below:

STEP 1: Select Fixed-NAT.

STEP 2: Type the private IP address in the **Private IP Address** field (for example, 192.168.1.233), and type the public IP address in the **Public IP Address** field.

STEP 3: Click on the **Add** button

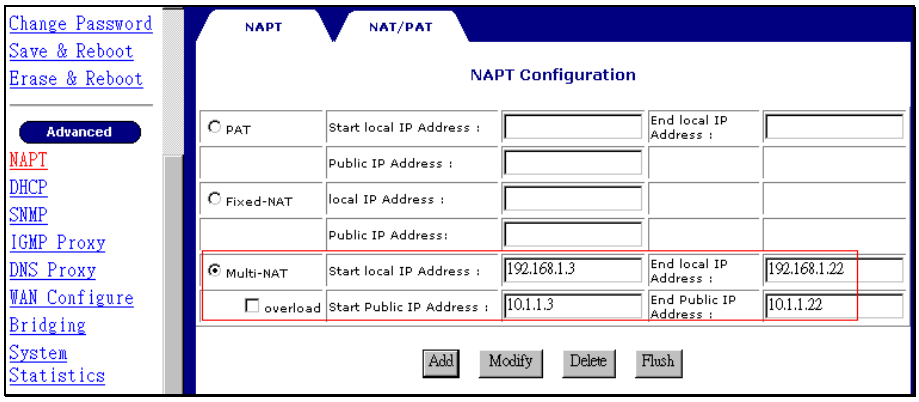


8.3 Multi-NAT

Multi-NAT maps a set of continuous private IP addresses to a set of continuous public IP addresses. There are two ways Multi-NAT can be used to translate the private IP addresses to public IP addresses. One way is to have each public IP address map to an individual private IP address. The other way is to have some of the private IP addresses share the same public IP address. This is required when there are fewer public IP addresses than private IP addresses.

One-to-one mapping. When the number of private IP addresses is less than or equal to the number of public IP addresses, each private IP address can be mapped to a public IP address. The following parameters are used:

- Start Private IP address- End Private IP Address: For example, 192.168.1.3- 192.168.1.22
- Start Global IP Address- End Global IP Address: For example, 10.1.1.3-10.1.1.22



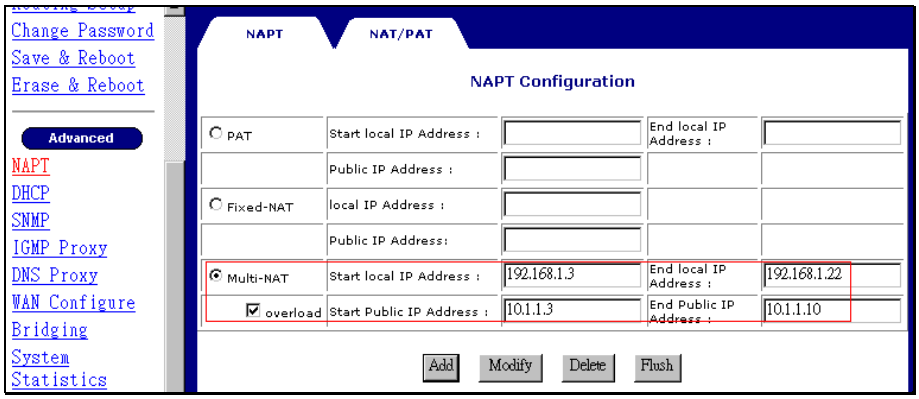
STEP 1: Enter the above parameters

- Start Private IP address: For example, 192.168.1.3
- End Private IP Address: For example, 192.168.1.22
- Start Global IP Address: For example, 10.1.1.3
- End Global IP Address: For example, 10.1.1.22

STEP 2: Click on the **Add** button.

Overload. When the number of private IP addresses is greater than the number of public IP addresses, private IP addresses must share public IP addresses. The following parameters are used:

- Start Private IP address- End Private IP Address: For example, 192.168.1.3- 192.168.1.22
- Start Global IP Address- End Global IP Address: For example, 10.1.1.3-10.1.1.10



STEP 1: Fill out the above parameters in the relevant fields.

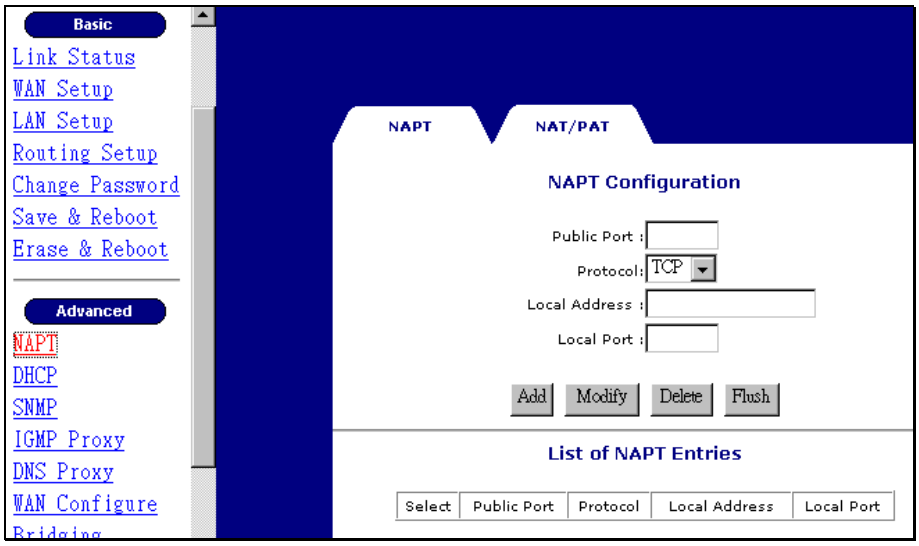
- Start Private IP address: For example, 192.168.1.3
- End Private IP Address: For example, 192.168.1.22
- Start Global IP Address: For example, 10.1.1.3
- End Global IP Address: For example, 10.1.1.10

STEP 2: Select Overload and click on the **Add** button.

8.4 Virtual Server

If you want to set up Internet servers (such as an e-mail server, web server, or FTP server) on the virtual LAN when PAT is enabled, you should register the servers with the router first to allow Internet users to access the service via the WAN interface of router. This section describes how to configure a virtual server.

Click on **NAPT** on the Advanced menu bar to access the NAPT Configuration screen.



- Global Port: The virtual server provides service for the Internet users via this port.
- Protocol: **TCP** or **UDP** (default: TCP).
- Private Address: This is the IP address of the Virtual Server
- Private port: This is the port that the virtual server is connected to the Ethernet.

After configuring the parameters, click **Add** to add an entry.

To modify the parameters, select an item from the List of NAPT Entries. Modify the parameters, and click on the **Modify** button.

To delete the parameters, select an item from the List of NAPT Entries. Click on the **Delete** button.

CHAPTER 9 DHCP

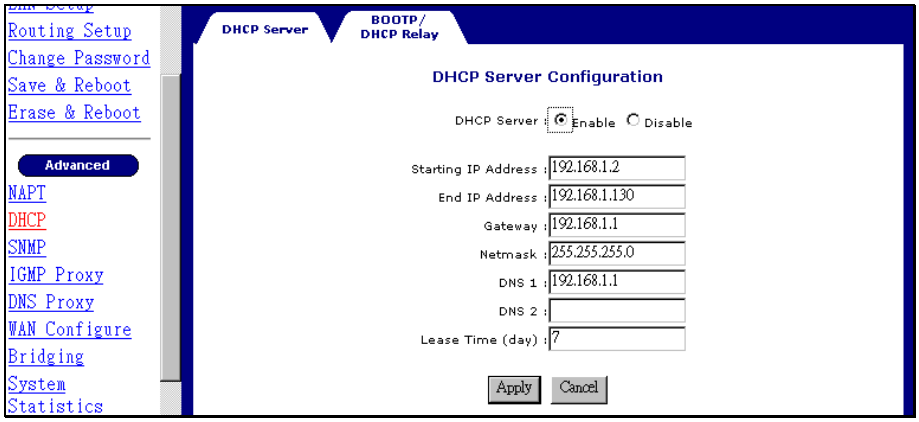
The router can be set as a Dynamic Host Configuration Protocol (DHCP) server or a DHCP relay. The former acts like an IP address pool. Upon power on, the PCs on the same domain will request an available IP address from the IP address pool of DHCP server. DHCP provides a centralized approach to allocating IP addresses. It allows IP addresses to be dynamically assigned on an as needed basis, from a pool of addresses. DHCP relay acts as an intermediate station. The DHCP server is at a remote location. PCs are directed to the remote location by the DHCP relay to obtain an available IP address.

9.1 DHCP Server

When a workstation is configured for automatic IP address assignment, it broadcasts a request to the LAN.

- When the router is configured as a DHCP server, the IP addresses in the DHCP pool should be at the same network segment as the DHCP server.
- DNS IP must be a valid parameter to activate the DHCP server to forward the DNS IP address to the workstations. The router supports DNS Proxy function. It can forward the name of the website to the correct DNS server to obtain the correct IP address.

To configure the router as a DHCP server, click on **DHCP** on the Advanced menu bar. Click **Enable** in the DHCP Server field, and fill out the parameters. Click **Apply** to submit the settings.

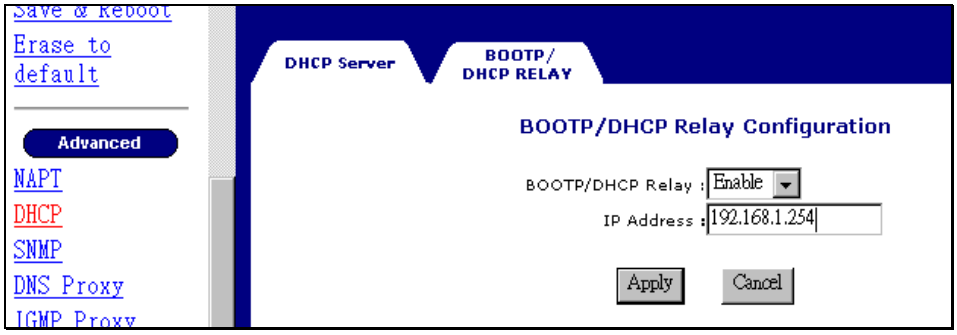


9.2 DHCP Relay

Click on **DHCP** on the Advanced menu bar. On the main screen, click on the **BOOTP/DHCP Relay** tab and configure the following parameters:

- BOOTP/DHCP Relay: Enable
- IP Address: This defines the IP address of the remote DHCP server.

After completing the settings, click **Apply**] to submit the settings. Also, change the router's LAN IP address.

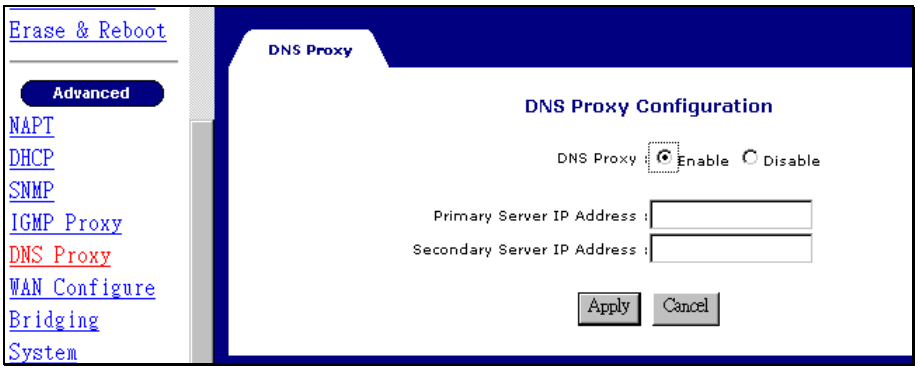


CHAPTER 10 DNS Proxy

A Domain Name Server (DNS) provides an IP address to a host computer for an applied Domain Name. The router supports the DNS proxy feature, which receives and attempts to find an entry in its local tables, and when one is not found, it forwards the request to a remote server.

Click **DNS Proxy** on the Advance men bar and configure the following parameters:

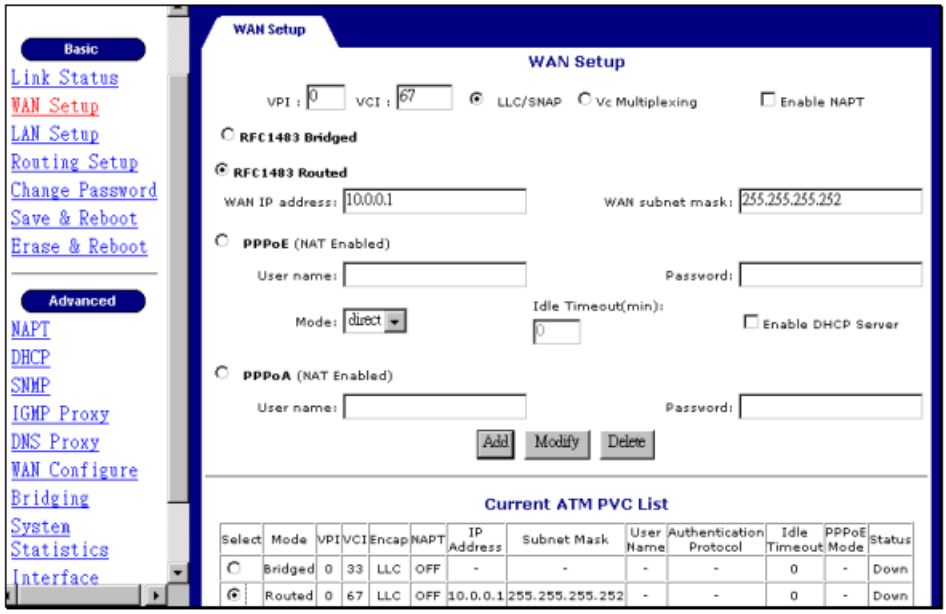
DNS proxy:	Enabled/ Disabled (factory default: disabled)
Primary Server IP address:	Enter the primary server IP address
Secondary Server IP address:	Enter the secondary server IP address that will be used immediately when the primary server IP address fails or is not available



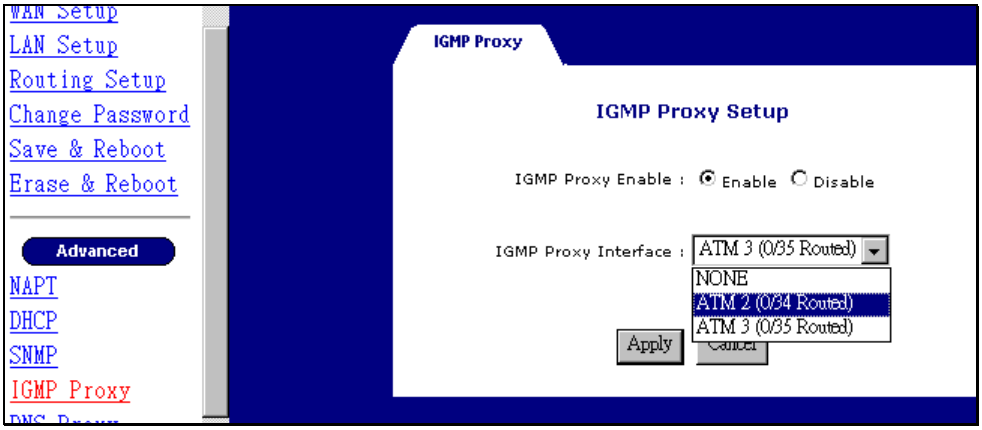
CHAPTER 11 IGMP

IGMP (Internet Group Membership Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers.

STEP 1: Add a VC and set it to RFC 1483 Routed mode.

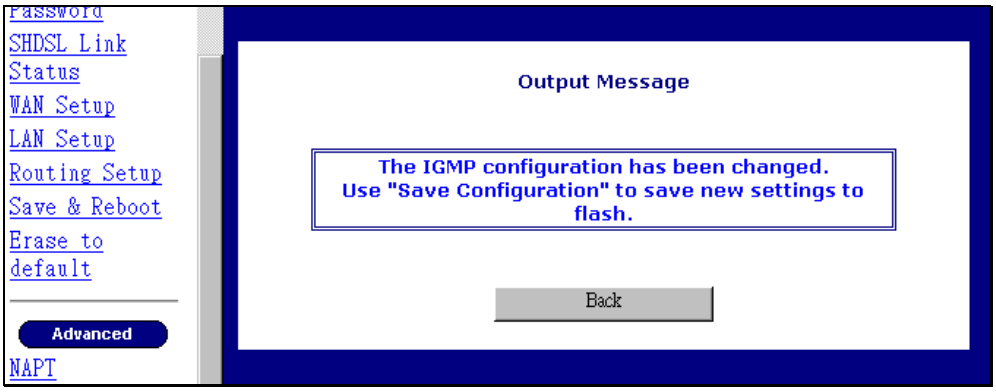


STEP 2: Click **IGMP Proxy** on the Advanced menu bar.



STEP 3: Click **Enable** and choose the interface ATM1-ATM16 that the router is used to connect to the server. This depends on VC to which interface it is assigned.

STEP 4: Click **Apply** to submit the settings.



CHAPTER 12 VLAN

To configure the VLAN function, click on **VLAN** in the Advanced menu bar. VLAN is disabled by factory default. To enable it, select **Enable** and click on the **Set** button. Then you can proceed to create the VLAN groups. The router supports four VLAN groups, 1 to 4. You can choose and join different Ethernet ports to the PVC running in RFC 1483 bridged mode. Packets will be transmitted or received from these ports to the appointed PVC. The packets of the VLAN groups are not routable. Packets that do not belong to the VLAN group are routable.

Parameters and buttons

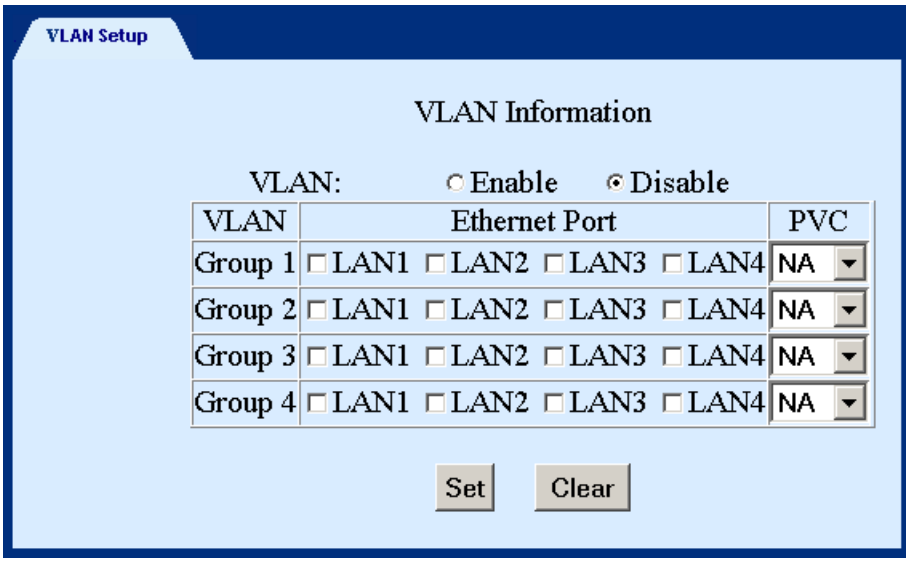
The PVC field displays the values of the PVCs that have been set up (refer to the WAN Setup section). Click on the Set button to apply the settings, or click on the Clear button to delete a VLAN group.

Notes:

1. You must save the parameters and reboot your router before the VLAN will be active.

2. Each LAN can be assigned to only one group.

3. Each PVC can be assigned to only one group.

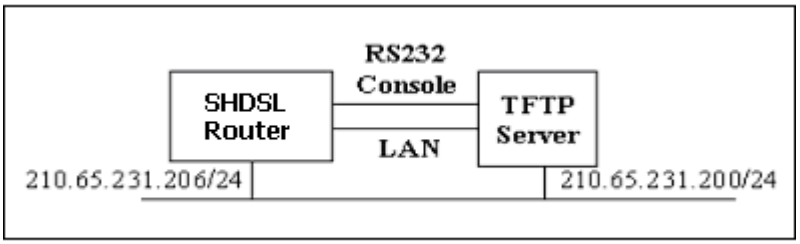


CHAPTER 13 Maintenance and Diagnostics

This chapter describes how to perform a software upgrade, configuration backup, or configuration restoration, and how to use the diagnostic functions of the router.

13.1 Software Upgrade and Configuration Backup /Restoration

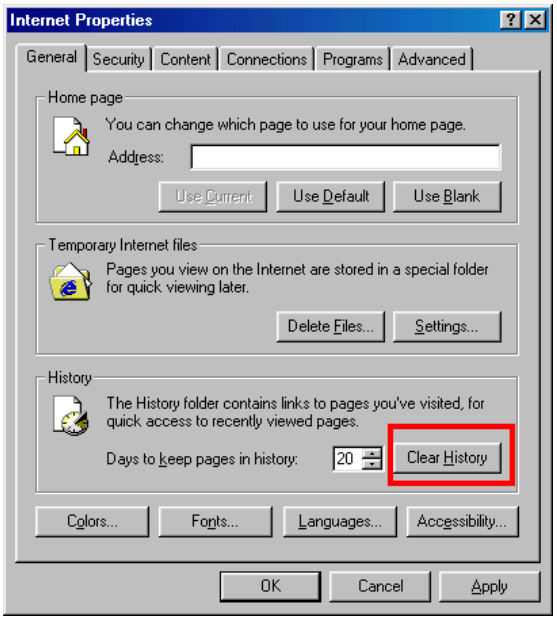
The router supports TFTP upgrade via the console, Telnet, and Web browser. Using a TFTP server, you can upgrade the software, back up the configuration, and retrieve past configurations. This section describes how to achieve these tasks using the console port or LAN port.



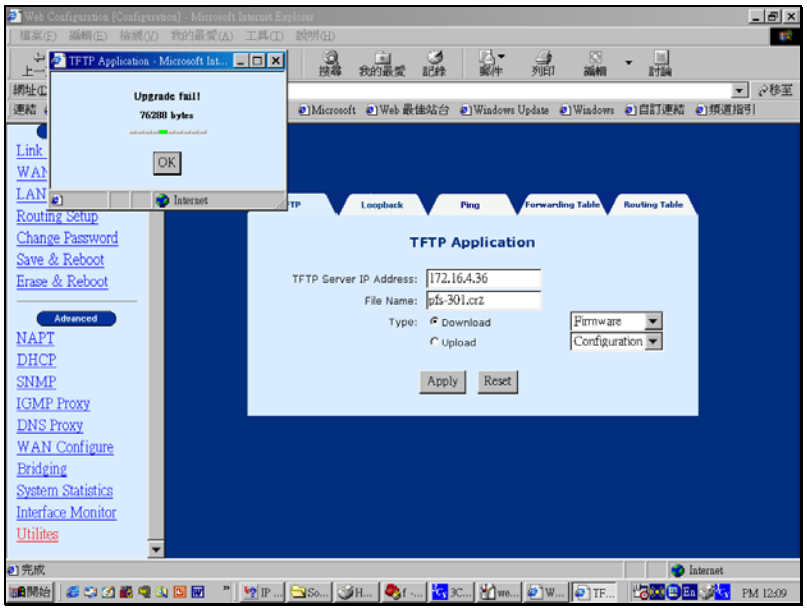
In the above diagram, the TFTP server is a PC with TFTP software installed. If you will use the console port to perform the TFTP upgrade, connect the console port of the router to your PC. If you will use Telnet or Web browser, connect the LAN port of the router to your Ethernet LAN.

Notes:

After the home page is upgraded, right-click your Internet Explorer shortcut icon on your desktop and choose Properties on the popup menu. On the Internet Properties window, click on the **Clear History** button and click **OK**. Then you can use the Web browser to log on to the router.



If a wrong format of the file us uploaded, a failure message will display during the upgrade. The following is an example of upgrade failure resulting from an incorrect file format.



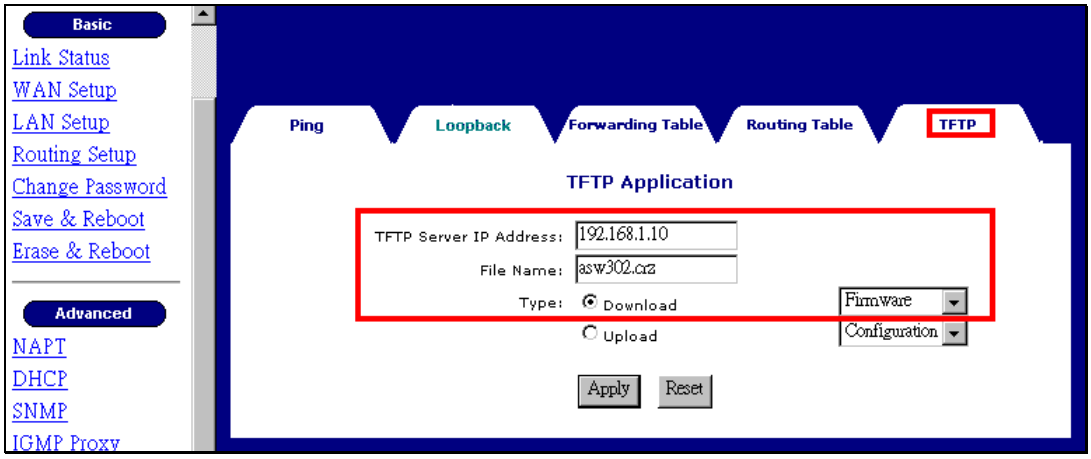
Before performing the TFTP upgrade, run the TFTP software. Click on **Utilities** on the Advanced menu bar. Fill out the TFTP Server IP address, file name, and upgrade type.

- Software upgrade: Check Download and choose Firmware in the column to the right.
- Homepage upgrade: Check Download and choose Homepage in the column to the right.
- Configuration backup: Check Upload and choose Configuration in the column to the right
- Retrieving Configurations: Check Download and choose Configuration in the column to the right

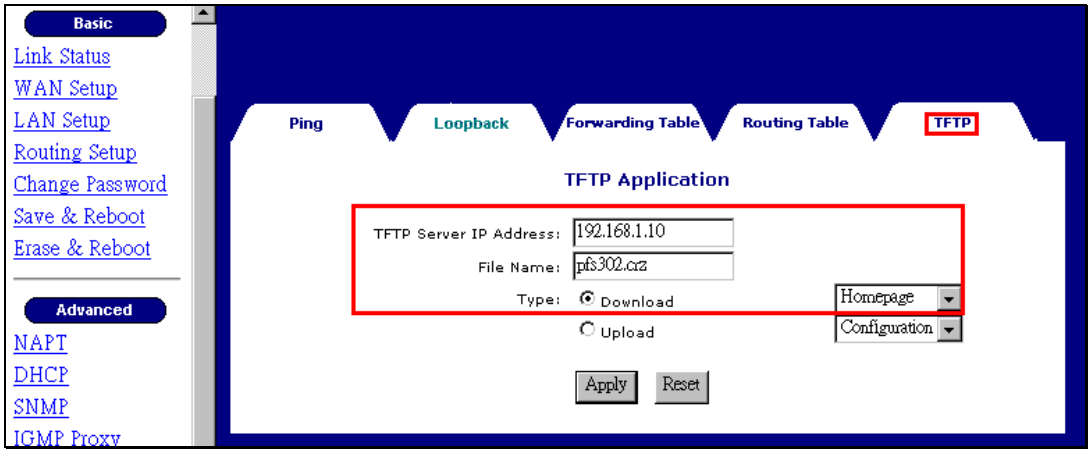
After completing the settings, click **Apply** to perform the function and note the following.

- After software or homepage upgrades are complete, reboot the device to run the new file.
- After the configurations are retrieved, also write the configurations to the Flash memory.

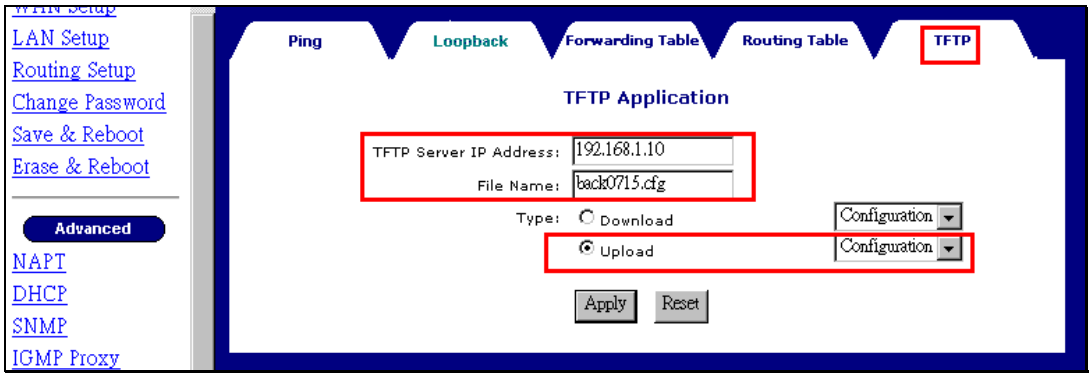
The following is an example of how to set up the parameters for software upgrade.



The following is an example of how to set up the parameters for homepage upgrade.

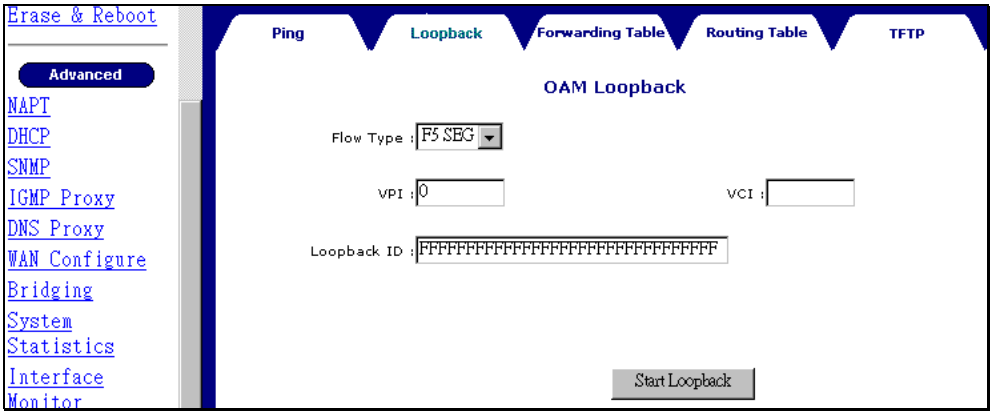


To upload the configurations, check **Upload**, select **Configuration,** and click on the **Apply** button to submit the settings.



13.2 OAM Loopback

Click on **Utilities** on the Advanced menu bar, and click on the **Loopback** tab on the main screen.



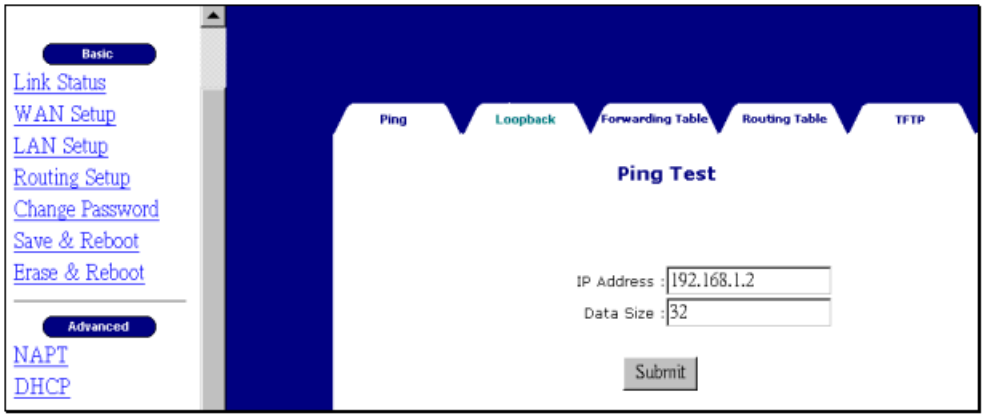
After filling out the following parameters, click **Start Loopback** to perform the loopback.

Flow Type	Choose the F5 loopback type. Seg is the segment loopback. It verifies the connection between the router and DSLAM. Ete is the end-to-end loopback, verifying the connection between the router and the ISP Broadband RAS.
VPI	Specify the VPI that will perform the loopback.
VCI	Specify the VCI that will perform the loopback.
Loopback ID	Specify the ID number on the ATM network that will loop back the signals.

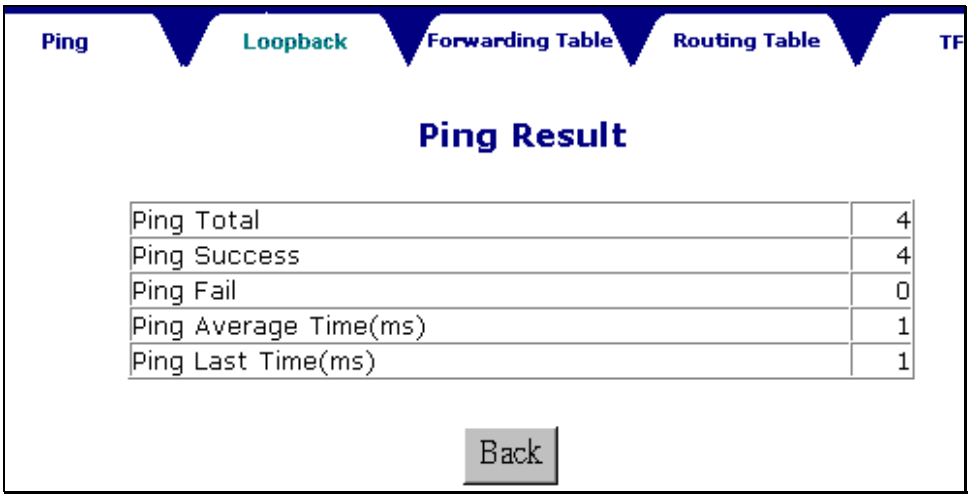
13.3 Ping

A Ping test is used to verify the status of a network connection after the RIP or static route function is enabled. Ping sends a request message to the host and waits for a return message. This diagnostic function can verify if the remote host is reachable. Ping can also measure the round-trip time to the remote host.

Click **Utilities** on the Advanced menu bar, and click on the **Ping** tab on the main screen. After typing the IP address and the ping data size, click **Submit** to perform the test. The ping result will display later.



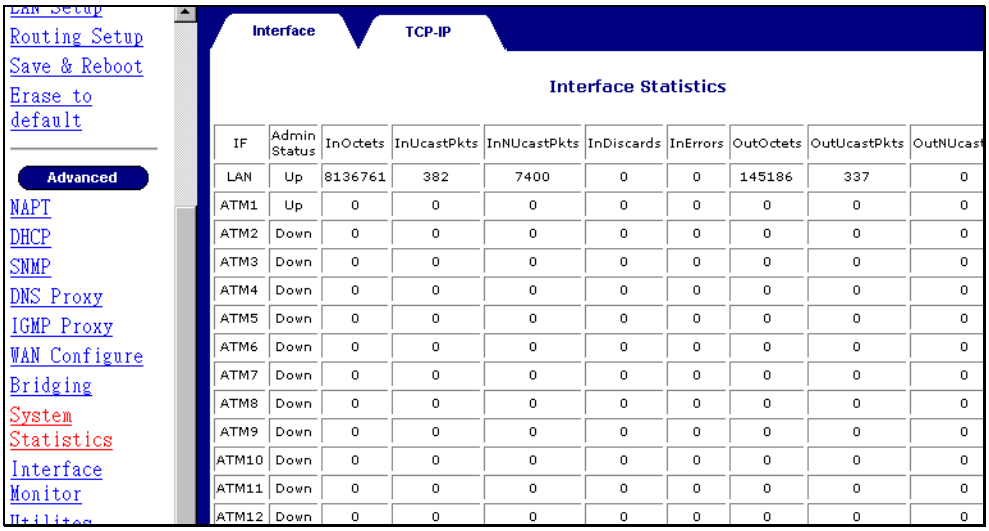
The following is an example of the ping result.



13.4 Performance Monitoring

- System statistics

Click **System Statistics** on the Advanced menu bar to monitor the interface status and collect the statistics of the TCP/IP.

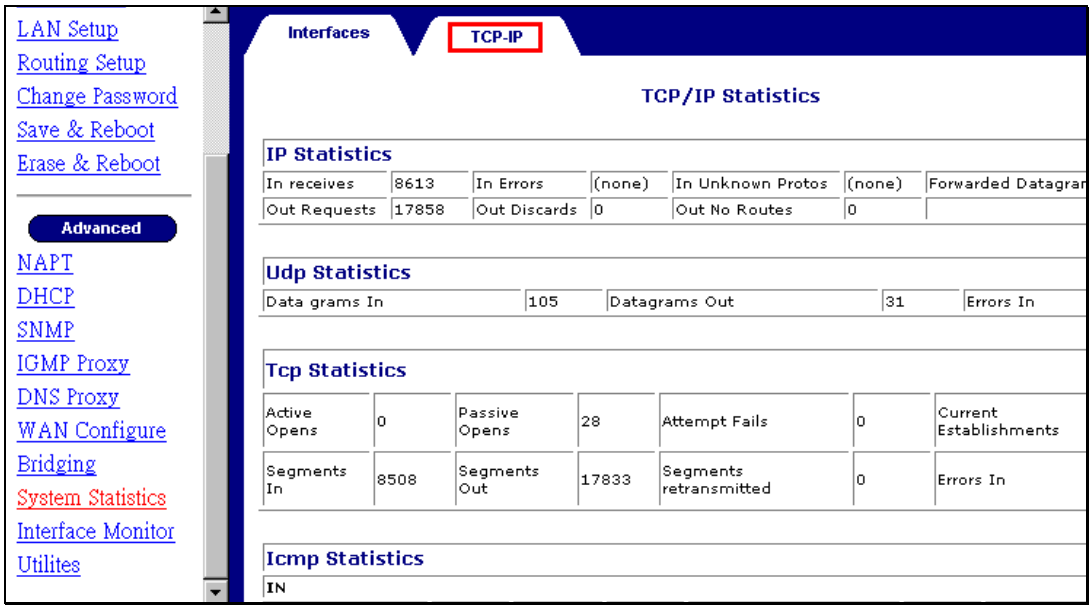


IF	Admin Status	InOctets	InUcastPkts	InNUcastPkts	InDiscards	InErrors	OutOctets	OutUcastPkts	OutNUcast
LAN	Up	8136761	382	7400	0	0	145186	337	0
ATM1	Up	0	0	0	0	0	0	0	0
ATM2	Down	0	0	0	0	0	0	0	0
ATM3	Down	0	0	0	0	0	0	0	0
ATM4	Down	0	0	0	0	0	0	0	0
ATM5	Down	0	0	0	0	0	0	0	0
ATM6	Down	0	0	0	0	0	0	0	0
ATM7	Down	0	0	0	0	0	0	0	0
ATM8	Down	0	0	0	0	0	0	0	0
ATM9	Down	0	0	0	0	0	0	0	0
ATM10	Down	0	0	0	0	0	0	0	0
ATM11	Down	0	0	0	0	0	0	0	0
ATM12	Down	0	0	0	0	0	0	0	0

To display the interface statistics, click on the **Interface** tab, located at the top-left of the System Statistics screen. The Interface Statistics page displays statistics for all interfaces. The following information is displayed:

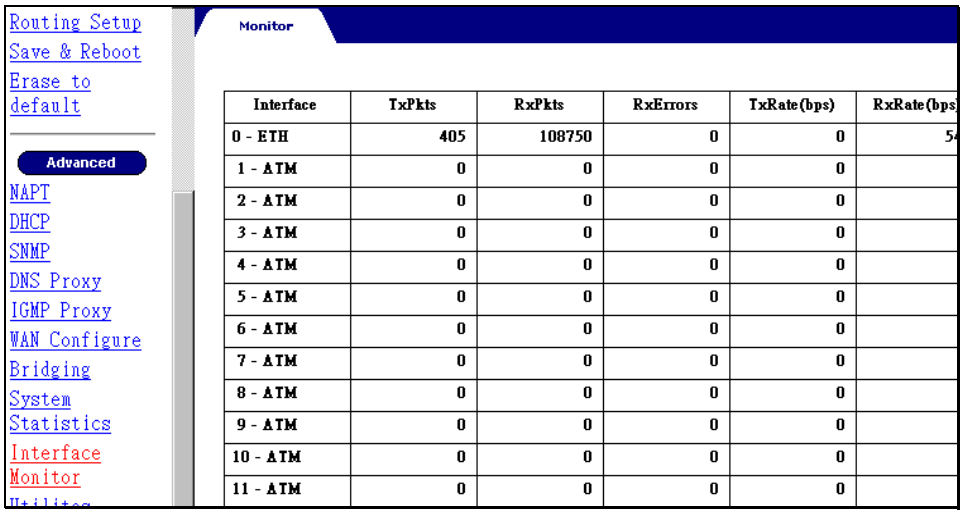
IF	The name of the interface
Admin Status	Indicates whether the interface is Up or Down
In Octets	The number of Octets (bytes) received
InUncastPkts	The number of unicast packets received
InUncastPkts	The number of broadcast packets received
InDiscards	The number of packets received that were discarded
InErrors	The number of inward errors
OutOctets	The number of Octets (bytes) transmitted
OutUcastPkts	The number of unicast packets transmitted
Broadcast PktsOut	The number of broadcast packets transmitted
OutDiscards	The number of packets transmitted that were discarded
OutErrors	The number of outward errors

To view TCP-IP statistics click on the **TCP-IP** tab at the top of the System Statistics page. The TCP-IP page displays the IP statistics, UDP statistics, TCP statistics, and ICMP statistics.



Interface

Click **Interface Monitor** on the Advanced menu bar to monitor the transmission status.

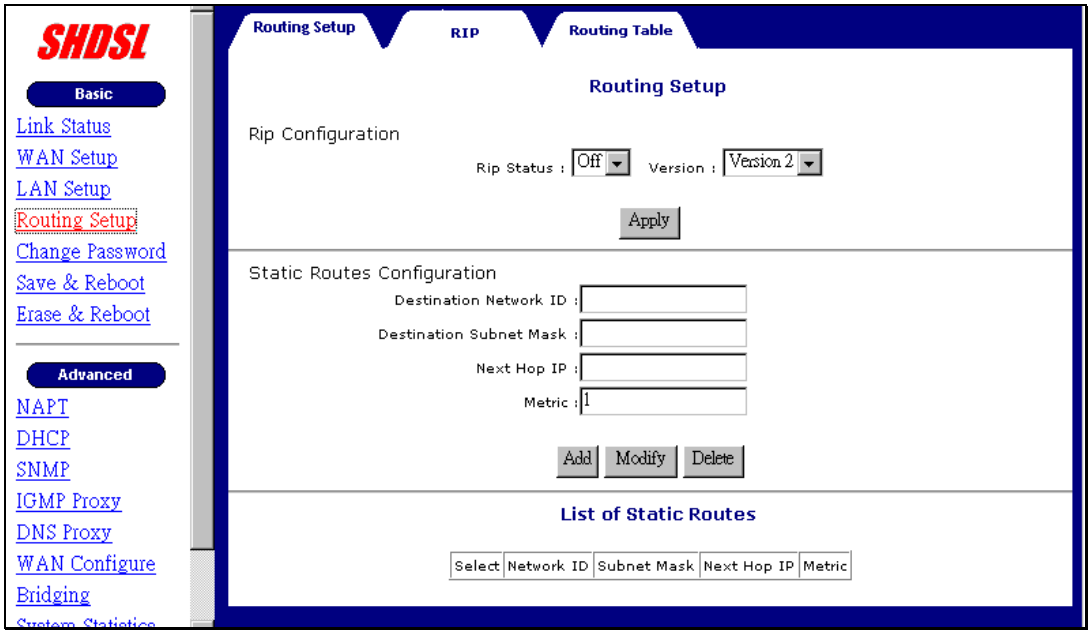


Interface	TxPkts	RxPkts	RxErrors	TxRate(bps)	RxRate(bps)
0 - ETH	405	108750	0	0	5
1 - ATM	0	0	0	0	
2 - ATM	0	0	0	0	
3 - ATM	0	0	0	0	
4 - ATM	0	0	0	0	
5 - ATM	0	0	0	0	
6 - ATM	0	0	0	0	
7 - ATM	0	0	0	0	
8 - ATM	0	0	0	0	
9 - ATM	0	0	0	0	
10 - ATM	0	0	0	0	
11 - ATM	0	0	0	0	

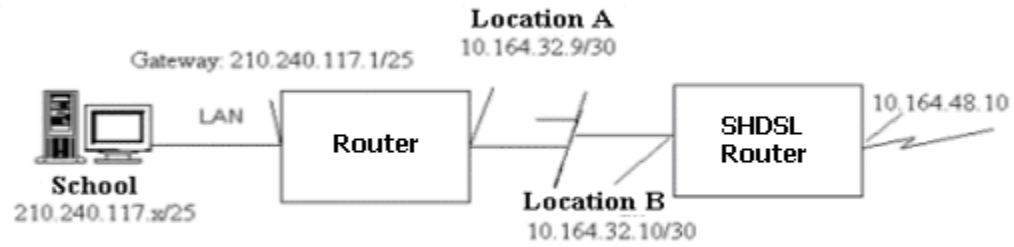
CHAPTER 14 Application Example

14.1 Adding the Static Route (Web)

Click **Routing Setup** on the Advanced menu bar.



The following demonstrates a school application as an example.

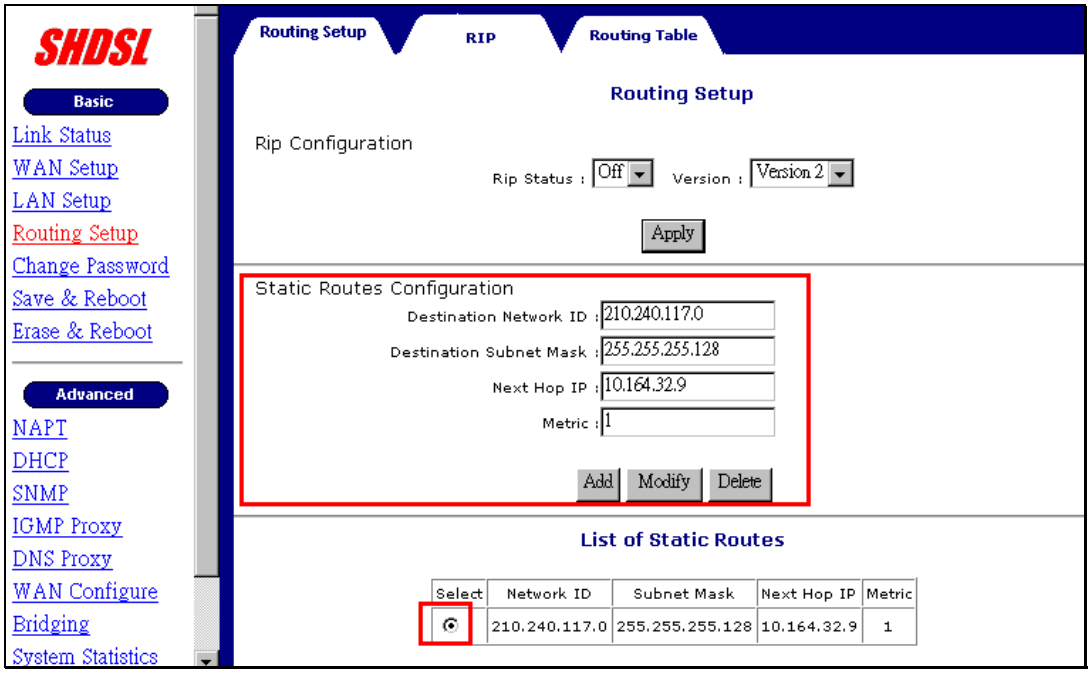


- Location A: 10.164.32.9; Netmask: 255.255.255.252
- Location B: 10.164.32.10; Netmask: 255.255.255.252
- Network of the School: 210.240.117.0; Netmask: 255.255.255.128

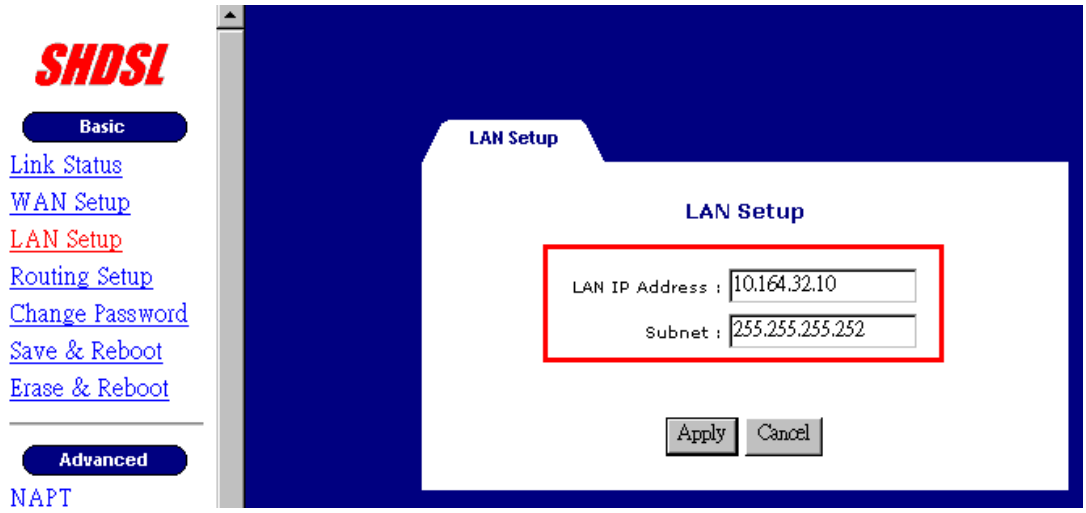
In the above example, you would add the following static route to the router.

210.240.117.0; Netmask: 255.255.255.128; Next hop: 10.164.32.9

Enter the parameters of the static route and click on the **Add** button.



Click **LAN Setup** on the Basic men bar. After typing LAN IP 10.164.32.10 and Netmask 255.255.255.252, click on **Apply** to submit the settings.



CHAPTER 15 Pin Assignments

Console Port (RS232 DB9)

Pin number	Definition	Pin number	Definition
1	NC	6	NC
2	TD	7	NC
3	RD	8	NC
4	NC	9	NC
5	GND		

LAN Port (RJ45)

Pin number	Definition	Pin number	Definition
1	RD+	5	NC
2	RD-	6	TD-
3	TD+	7	NC
4	NC	8	NC

LINE Port (RJ45)

Pin number	Definition	Pin number	Definition
1	Loop2-1	5	Loop1-2
2	Loop2-2	6	Short with 2
3	Short with 1	7	NC
4	Loop1-1	8	NC

CHAPTER 16 Console Access

To access the device via the console port the following are required:

- **VT100 Compatible Terminal**

This terminal is essential to perform the initial configuration of the router. This is normally a terminal with a VT100 emulation program, such as Telix or HyperTerminal Edition 5.

- **Console Port Cable**

An RS-232, DB9-to-DB9 straight-through cable is only required if you need to connect the device to a VT100 terminal or equivalent. The cable is not supplied with the SHDSL router.

16.1.1 Login

For access by console, the console PC should be installed with a standard VT100 emulation program, such as HyperTerminal 5 or Telix. You must connect the router to a PC using a serial cable. The following steps describe how to establish the console session.

STEP1: Run a standard VT100 program such as HyperTerminal (Ver. 5 is recommended), or Telix in the local terminal and select an open com port.

STEP2: Enter the following port settings:

- Baud rate: 9600
- Data bits: 8
- Parity: none
- Stop bit: 1
- Flow control: none

STEP3: After the session parameters are set up, press the Enter Key. You will be requested to enter the user name and password.

STEP4: After successfully logging in, the main menu will appear.

```
    SHDSL Router                    Main Menu                          V
-----------------------------------------------------------------------

              >>1.[BASIC]   -  Basic Configuration
                2.[ADVANCE] -  Advance Configuration
                3.[MON]     -  Status/Statistics Monitor
                4.[UTIL]    -  Utilities
                5.[SYS]     -  System Information
                6.[WRITE]   -  Write Configuration
                7.[REBOOT]  -  Reboot
                8.[QUIT]    -  Disconnect

-----------------------------------------------------------------------
[Up(^W)]  [Down(^Z)]  [Left(^A) - Prev Menu]  [Right(^D) - Next Menu]

PATH> MAIN
```

16.1.2 Keyboard Operations

In this table, the caret (^) denotes the Ctrl key.

↑	The upward arrow key moves the cursor upward in the menu
↓	The downward arrow key moves the cursor downward in the menu.
←	Returns to the previous menu. If you are in a leaf menu you may need to push ^S first (to save the information)
→	Skips to the next menu.
^S	Hold down the Ctrl-S keys simultaneously to perform different actions such as Save, Add, Delete and Go.
^X	In the leaf menu, hold down the Ctrl-X keys simultaneously to return to the previous menu.
^L	Hold down the Ctrl-L keys simultaneously to return to the Home Menu.
^T	Hold down the Ctrl-T keys simultaneously to reset the value or statistics counted.
^R	Hold down the Ctrl-R keys simultaneously to refresh or restore the menu.
Q	Press the Q key to stop certain actions, such as software downloading.
Tab	In the leaf menu, some configuration fields are marked TAB. It means you need to press the TAB key to scroll through and select the pre-defined options.

The following backup keys can be used if your software doesn't support arrow keys:

^W	Moves the cursor upward [equal to the up arrow key]
^Z	Moves the cursor downward [equal to the down arrow key]
^A	Return to the previous screen [equal to the left arrow key]
^D	Enter the selected item [equal to the right arrow key]

The backup keys displayed at the bottom of the screen.

```
   SHDSL Router              Basic Configuration
------------------------------------------------------------------------

             >>1.[SYSTEM]   -  System and Password Parameters
               2.[SHDSL]    -  SHDSL Link Status
               3.[WAN]      -  WAN Setup
               4.[LAN]      -  LAN Setup
               5.[ROUTING]  -  Static Route and RIP Parameters
               6.[SAVE]     -  Save and Reboot
               7.[DEFAULT]  -  Erase to Default

------------------------------------------------------------------------
[Up(^W)]  [Down(^Z)]  [Left(^A) - Prev Menu]  [Right(^D) - Next Menu]

PATH> MAIN/BASIC
```

In addition to the arrow keys to move the cursor in the menu, you can enter the requested screen by entering the number. For example, to enter MAIN/ADVANCE/DHCP/RELAY, follow the steps below:

STEP 1: Press the **2** key, to enter the **Advance** menu, and then press the **Enter** key。

```
   SHDSL Router                  Main Menu
------------------------------------------------------------------------

               1.[BASIC]    -  Basic Configuration
          [ 2]>2.[ADVANCE]  -  Advance Configuration
               3.[MON]      -  Status/Statistics Monitor
               4.[UTIL]     -  Utilities
               5.[SYS]      -  System Information
               6.[WRITE]    -  Write Configuration
               7.[REBOOT]   -  Reboot
               8.[QUIT]     -  Disconnect

------------------------------------------------------------------------
[Up(^W)]  [Down(^Z)]  [Left(^A) - Prev Menu]  [Right(^D) - Next Menu]

PATH> MAIN
```

STEP 2: From the **MAIN/ADVANCE** menu, press the **2** key and then press the **Enter** key

```
   SHDSL Router            Advance Configuration
------------------------------------------------------------------------

               1.[NAT]         -  NAT Parameters
          [ 2]>2.[DHCP]        -  DHCP Parameters
               3.[SNMP]        -  SNMP Parameters
               4.[IGMP]        -  IGMP Proxy Parameters
               5.[DNS]         -  DNS Proxy Parameters
               6.[INTERFACE]   -  Interface Parameters
               7.[ROUTING]     -  Routing Parameters
               8.[BRIDGING]    -  Transparent Bridging Parameters
               9.[HTTPD]       -  Web Server Parameters
              10.[TFTP]        -  TFTP Parameters
              11.[SHDSL]       -  SHDSL Characteristics Parameters

------------------------------------------------------------------------
[Up(^W)]  [Down(^Z)]  [Left(^A) - Prev Menu]  [Right(^D) - Next Menu]

PATH> MAIN/ADVANCE
```

STEP 3: Press the **2** key, and then press the **Enter** key in MAIN/ADVANCE/DHCP.

```
    SHDSL Router                DHCP Parameters                      V3.
-----------------------------------------------------------------------

                1.[Server]  -  DHCP Server Parameters
           [ 2]>2.[Relay]   -  BOOTP/DHCP Relay Parameters
                3.[Fixed]   -  Fixed Host IP Address List

-----------------------------------------------------------------------
[Up(^W)]  [Down(^Z)]  [Left(^A) - Prev Menu]  [Right(^D) - Next Menu]

PATH> MAIN/ADVANCE/DHCP
```

STEP 4: Now you have reached MAIN/ADVANCE/DHCP/RELAY.

```
    SHDSL Router          BOOTP/DHCP Relay Parameters
-----------------------------------------------------------------------

                BOOTP/DHCP Relay(TAB)          : Disabled
                Server IP                      :

-----------------------------------------------------------------------
              ^S - Save       ^L - Home Menu      ^X - Prev Menu

PATH> MAIN/ADVANCE/DHCP/RELAY

MESSAGE>
```

16.1.3 Motoring the SHDSL Line Status

Enter MAIN/BASIC/SHDSL to monitor the SHDSL Line status.

```
    SHDSL Router                SHDSL Link Status
-----------------------------------------------------------------------
                Termianl Type/Operate State     :   CPE/Handshake
                Actual Bit Rate(Kbps)           :         0
                Line Attenuation(dB)            :         0
                SNR Margin(dB)                  :        18
                CRC    (since reset)            :         0
                ES     (since reset)            :         0
                SES    (since reset)            :         0
                LOSWS  (since reset)            :     15028
                UAS    (since reset)            :     15028
                CRC    (current 15 min)         :         0
                ES     (current 15 min)         :         0
                SES    (current 15 min)         :         0
                LOSWS  (current 15 min)         :       629
                UAS    (current 15 min)         :       629
                CRC    (current  1 day)         :         0
                ES     (current  1 day)         :         0
                SES    (current  1 day)         :         0
                LOSWS  (current  1 day)         :     15028
                UAS    (current  1 day)         :     15028
-----------------------------------------------------------------------
Any Key - Prev Page    ^T - Reset Counters   ^L - Home Menu

PATH> MAIN/BASIC/SHDSL
```

16.1.4 Password Setup

Enter MAIN/BASIC/SYSTEM to change the passwords.

```
    SHDSL Router        System and Password Parameters
-------------------------------------------------------------------

                Terminal Type(TAB)             : CPE
                Console Password Check(TAB)    : Enabled
                Session Timeout(min)           : 0
                New Administrator Password     : *****
                Retype Password                : *****
                New User Password              : ***
                Retype Password                : ***

-------------------------------------------------------------------
              ^S - Save       ^L - Home Menu      ^X - Prev Menu

PATH> MAIN/BASIC/SYSTEM

MESSAGE>
```

- New Administrator Password and Retype Password: Enter the administrator password in the New Administrator Password and confirm the password by retyping the password in the Retype Password field.
- New User Password and Retype Password: Enter the user password in the New User Password and confirm the password by retyping the password in the Retype Password field.

16.1.5 Retrieve the Factory Default Settings

Enter BASIC/DEFAULT and press the **Y** key. After the default settings are set to the factory default, return to the main menu and enter MAIN>WRITE to save the configurations.

```
This will set system parameters to factory default !(Y/N)
         Set system parameters to factory default!
        Press any key to return to previous menu ...
```

16.1.6 Disable the Web Browser

The router allows access via a Web browser by factory default. To disable this function, enter ADVANCE/HTTPD, choose Disabled, and submit the setting.

```
    SHDSL Router            Web Server Parameters
-------------------------------------------------------------------

                Web Server(TAB)                : Disabled

-------------------------------------------------------------------
              ^S - Save       ^L - Home Menu      ^X - Prev Menu
PATH> MAIN/ADVANCE/HTTPD
MESSAGE>
```

16.1.7 Save the Configurations

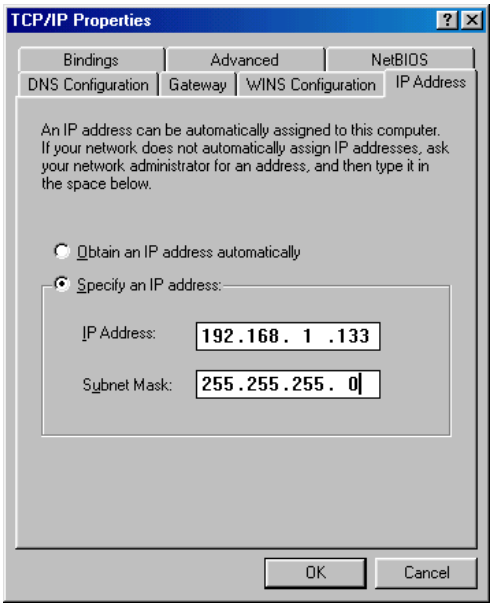
The new parameters can function immediately without being saved to the flash memory. However, to use these parameters after you restart the router, you must save them to the flash memory.

To write the configurations, enter MAIN/WRITE and press the Y key. After saving the configurations, you will be prompted if you need to reboot the device. Press the Y key to reboot the device or press the N key to keep operating the device.

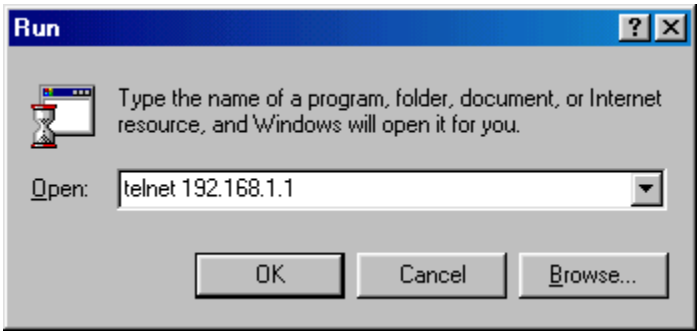
```
This will write configuration to flash!(Y/N)

   Write configuration to flash complete!

         Reboot the system?(Y/N)

           Wait, rebooting ...
```

16.1.8 Login

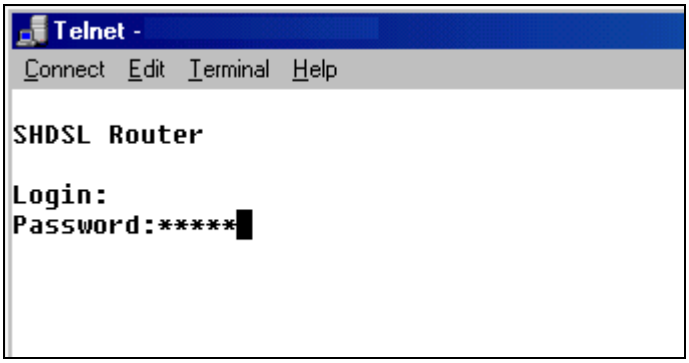
STEP 1: Configure your workstation to the same network segment as the router, such as IP address 192.168.1.133 and subnet mask 255.255.255.0.



STEP 2: Click [Start]> [run], type **telnet 192.168.1.1** and click **OK**. (192.168.1.1 is the default IP address. If it was changed, use the new IP address to login.)



STEP 3: Enter the user name and password and press Enter to login (The default password and user name are root)



STEP 4: The following displays the main menu after login.

```
    SHDSL Router                    Main Menu                              V
--------------------------------------------------------------------------------

              >>1.[BASIC]    -  Basic Configuration
                2.[ADVANCE] -  Advance Configuration
                3.[MON]     -  Status/Statistics Monitor
                4.[UTIL]    -  Utilities
                5.[SYS]     -  System Information
                6.[WRITE]   -  Write Configuration
                7.[REBOOT]  -  Reboot
                8.[QUIT]    -  Disconnect

--------------------------------------------------------------------------------
[Up(^W)]  [Down(^Z)]  [Left(^A) - Prev Menu]  [Right(^D) - Next Menu]

PATH> MAIN
```

Appendix A: Specifications

WAN Interface (One SHDSL port)

SHDSL standard	ITU-T G991.2
SHDSL Line Interface	RJ45
Encoding scheme	TC-PAM
Line rate	Per ITU-T G991.2 (SHDSL)
Data rate	N x 64 Kbps, N=1~36, per Channel (2 channels)

Encapsulation

Multi-protocol over AAL5 Bridged	RFC 2684 (1483)
Multi-protocol over AAL5 Route	RFC 2684 (1483)
PPP over Ethernet	RFC 2516
PPP over AAL5	RFC 2364

ATM Attributes

VCs	16
AAL type	AAL5
ATM service class	UBR/CBR/VBR
ATM UNI support	UNI3.1/4.0
OAM	F4/F5

Management

Console port	RS232/DB9
SNMP	Yes
TR-006 ADS Line MIB	Yes
Telnet	Yes
Web-based management	Yes
LED Indicators	Power, LAN status, ADSL status

Local Interface (Four Ethernet ports)

Standard	IEEE 802.3 10/100 Base-T
Transparent bridge and learning	Yes

Routing functions

IP static route	Yes
RIP and RIPv2	Yes
IGMP Proxy	Yes

Network functions

ARP	Yes
DNS, NAT/PAT, DHCP/BOOTP	Yes
PAP, CHAP	Yes
Automatic IP and DNS Assignment	RFC 1877

Power Supply

External power adapter	110 VAC or 230 VAC
Frequency	50/60 Hz

Environmental Conditions

Operating temperature	0–50 degrees Celsius
Relative humidity	5–95%(non-condensing)

Note: Specifications are subject to change without notice