RTA100

ADSL Bridge/Router

User Manual

September 2002
Part No. A148Rev05

Contents

1 Introduction

Congratulations on becoming the owner of the ADSL Ethernet bridge/router. Your LAN (local area network) will now be able to access the Internet using your high-speed ADSL connection.

This manual will show you how to install and set up your ADSL Bridge/Router, and how to customize its configuration to get the most out of your new product.

Features

- Internal ADSL modem for high-speed Internet access
- 10/100Base-T Ethernet router to provide Internet connectivity to all computers on your LAN
- USB port for connecting a USB-enabled PC
- Network address translation (NAT) and IP filtering functions to provide firewall protection for your computers
- Network configuration through DHCP
- Configuration program you access via an HTML browser
- CLI session configuration via terminal emulation software

Parts Check

In addition to this document, your ADSL Bridge/Router should arrive with the following:

- One ADSL Bridge/Router
- One power adapter
- One straight-through Ethernet cable
- One standard phone/DSL line cable
- One USB cable (Optional)

System Requirements

In order to use your ADSL Bridge/Router, you must have the following:

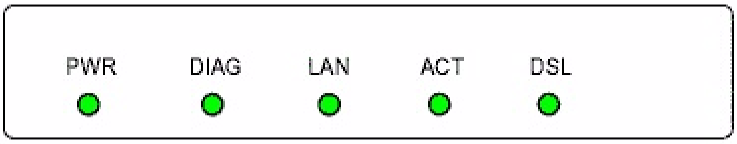
- ADSL service up and running on your telephone line, with at least one public Internet address for your LAN.
- One or more computers each contain an Ethernet 10Base-T/100Base-T network interface card (NIC) and/or a single computer with a USB port.
- An Ethernet hub/switch, if you are connecting the device to more than one computer.

- For system configuration using the supplied web-based program: a web browser such as Internet Explorer v5.0 or later, or Netscape v5.0 or later.

2 Hardware and Connection

Front Panel

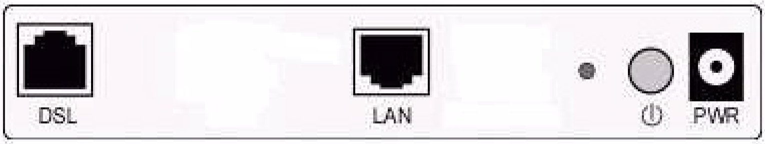
The front panel contains lights called LEDs that indicate the status of the unit.



Label	Color	Function
PWR	green	On: Unit is powered on Off: Unit is powered off
DIAG	green	Flashes on/off at boot-up to indicate that the device software is operational.
LAN	green	On: LAN link established and active Off: No LAN link
ACT	green	Flashes when ADSL data activity occurs. May appear solid when data traffic is heavy.
DSL	green	On: ADSL link established and active Off: No ADSL link

Rear Panel

The rear panel contains the ports for the unit's data and power connections. The functions are described as below (from left to right):



Label	Function
DSL	Connects the device to an ADSL telephone jack using the supplied cable
LAN	Connects the device to your PC's Ethernet port, or to the uplink port on your LAN's hub, using the cable provided
Reset Button	Reset to factory defaults. To reset the device to factory defaults, you don’t need to power off the device. Just push a paper clip into the hole.

Label	Function
	Press down the button for 3 times and then release. Then wait for the device to finish boot-up.
⏻	Switches the unit on and off
PWR	Connects to the supplied power converter cable

Connecting the Hardware

Follow the procedures below to connect related devices. Before you begin, turn the power off for all devices. These include your computer(s), your LAN hub/switch (if applicable), and the ADSL Bridge/Router.

Step 1. Connect to the wall phone jack.

Connect one end of the RJ11 phone cable to the port labeled **DSL** on the rear panel of the device. Connect the other end to your wall phone jack with ADSL service.

Note

Depending on the service type offered by your ISP, an additional splitter may be needed. If this is the case, consult with your ISP for actual connection.

Step 2. Connect to a PC or hub/switch.

- To a single PC - Attach one end of a “straight-through” Ethernet cable to the port labeled **LAN** and the other to your PC’s Ethernet port.
- To a hub/switch - Attach one end of a “cross-over” Ethernet cable to a hub/switch and the other to the LAN port on the ADSL Bridge/Router.
- To a hub/switch’s uplink port: - Use a “straight-through” cable to connect it to the uplink port and the other to the **LAN** port on the ADSL Bridge/Router.

Step 3. Attach the power connector.

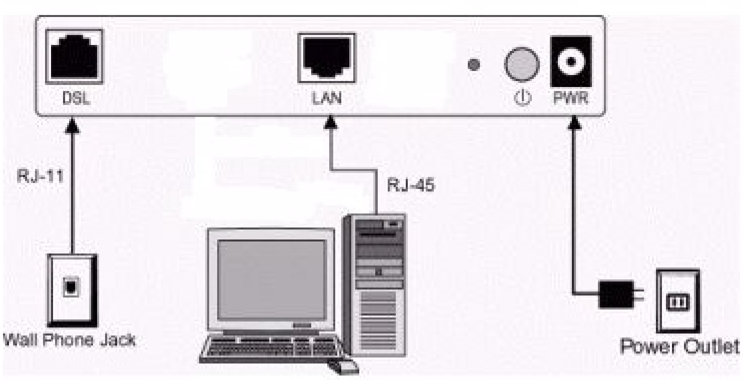
Connect the AC power adapter to the **PWR** connector on the back of the device and plug in the adapter to a wall outlet or power strip.

Step 4. Turn on the ADSL Bridge/Router and power up your systems.

Press the power switch on the back panel of the device to turn on the device.

Turn on and boot up your computer(s) and any LAN devices such as hubs or switches.

The following diagram illustrates a connection example:



3 Local PC Configuration

By default, the ADSL Bridge/Router acts as DHCP server and automatically assigns all required Internet settings to your PCs, i.e., the DHCP clients. The predefined IP address and DHCP pool is as below:

LAN Port IP address	192.168.1.1
Subnet mask	255.255.255.0
DHCP pool	192.168.1.3~34

These instructions assume that your PC meets the following prerequisites:

1. Already connected to the device's LAN port through its network interface card (NIC).

2. Has the appropriate Ethernet adapter software.

3. The TCP/IP protocol is installed. If not, refer to Microsoft documentations to install the TCP/IP.

You need only to configure the PCs to accept the information when it is assigned. Follow the instructions that correspond to the operating system installed on each PC.

Configuring your PCs as DHCP clients

Windows 95, 98, Me PCs:

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

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

3. On **Configuration** tab, select the TCP/IP network associated with your network card and then click **Properties**.

4. In the TCP/IP Properties dialog box, click the **IP Address** tab.

5. Click the radio button labeled **Obtain an IP address automatically**.

6. Click **OK** twice to confirm and save your changes.

7. You will be prompted to restart Windows. Click **Yes**.

Windows NT 4.0 workstations:

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

2. In the Control Panel window, double click the **Network** icon.

3. In the Network dialog box, click the **Protocols** tab.

4. In the Protocols tab, select **TCP/IP**, and then click **Properties**.

5. In the Microsoft TCP/IP Properties dialog box, click the radio button labeled **Obtain an IP address from a DHCP server**.

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

Windows 2000, XP PCs:

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

2. Double-click the **Network and Dial-up Connections** (or **Network Connections** for Windows XP) icon.

3. Right-click the **Local Area Connection** icon, and then select **Properties**.

4. Highlight **Internet Protocol (TCP/IP)**, and then click **Properties**.

5. In the **Internet Protocol (TCP/IP) Properties** dialog box, click the radio button labeled **Obtain an IP address automatically**. Also click the radio button labeled **Obtain DNS server address automatically**.

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

To assign static IP information to your PCs

In some cases, you may want to assign static IP to your PC directly if:

- In **bridge** mode, you have completed initial configuration and you need to use the IP address and default gateway given by your ISP.
- You have obtained one or more public IP addresses that you want to always associate with specific computers (for example, if you are using a computer as a public web server).

- You maintain different subnets on your LAN.

Before you begin, contact your ISP if you do not already have the following information:

- IP address and subnet mask.
- Default gateway.
- DNS server.

On each PC to which you want to assign static information, follow the instructions for displaying each of the TCP/IP properties. Instead of enabling dynamic assignment of the IP addresses for the computer, click the radio buttons that enable you to enter the IP address, DNS and default gateway manually.

4 Configuration via CLI Session

CLI can be accessed through a Telnet client. However, it is strongly recommended that you configure your device through the Web based Configuration Manager. For more information, please see next Chapter 5.

Logging in to CLI

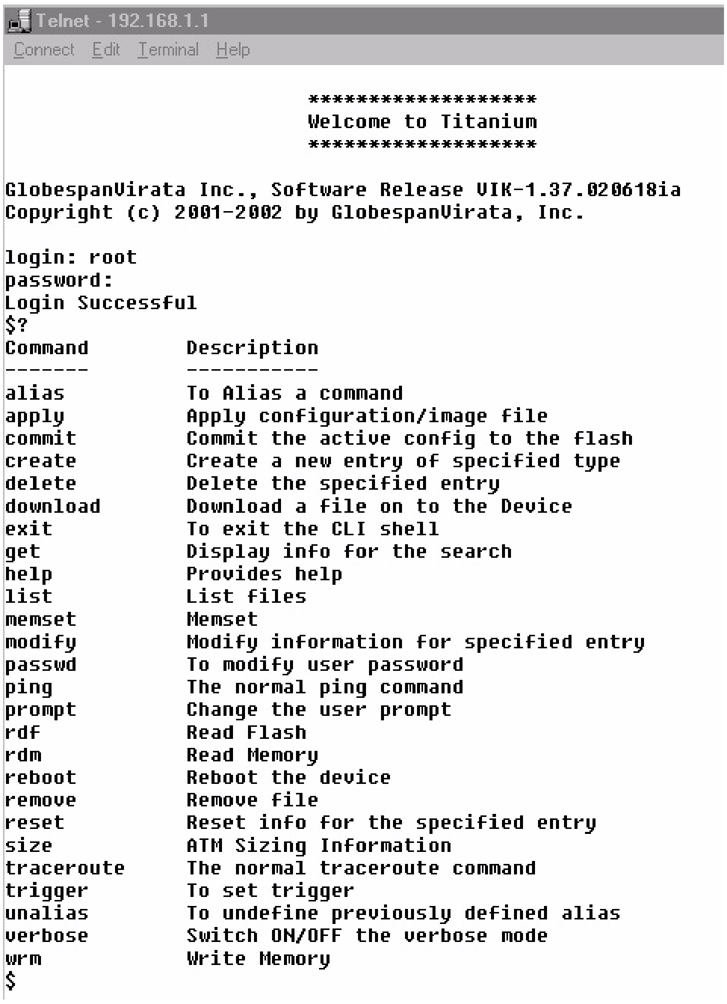
To log in for the first time, use the default user name and password:

Login: root

Password: root

The default user is pre-configured with root privilege level and is allowed to modify the system configuration as needed. From now on, you may start to configure your ADSL Bridge/Router with CLI.

Type '?' to get a list of commands



```
                         ********************
                         Welcome to Titanium
                         ********************

GlobespanVirata Inc., Software Release VIK-1.37.020618ia
Copyright (c) 2001-2002 by GlobespanVirata, Inc.

login: root
password:
Login Successful
$?
Command        Description
-------        -----------
alias          To Alias a command
apply          Apply configuration/image file
commit         Commit the active config to the flash
create         Create a new entry of specified type
delete         Delete the specified entry
download       Download a file on to the Device
exit           To exit the CLI shell
get            Display info for the search
help           Provides help
list           List files
memset         Memset
modify         Modify information for specified entry
passwd         To modify user password
ping           The normal ping command
prompt         Change the user prompt
rdf            Read Flash
rdm            Read Memory
reboot         Reboot the device
remove         Remove file
reset          Reset info for the specified entry
size           ATM Sizing Information
traceroute     The normal traceroute command
trigger        To set trigger
unalias        To undefine previously defined alias
verbose        Switch ON/OFF the verbose mode
wrm            Write Memory
$
```

5 Getting Started with the Configuration Manager

Your ADSL Bridge/Router includes a Web-based *Configuration Manager*, which enables you to configure the device settings to meet the needs of your network.

Accessing the Configuration Manager

You can access the program from any computer connected to the ADSL Bridge/Router via the LAN or USB ports.

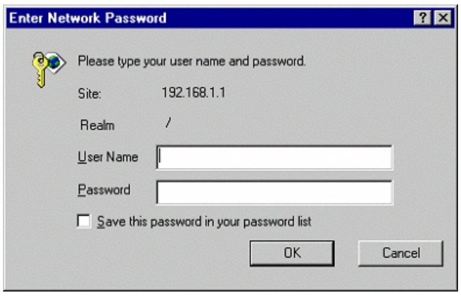
1. At any PC connected to the ADSL Bridge/Router, open your web browser, type the following URL in the web address (or location) box, and press **<Enter>**:

   `http://192.168.1.1`

2. When the login screen displays, enter your user name and password, and then click **OK**.

   The first time you launch the program, use these defaults:

Default User Name:	root
Default Password:	root



Enter Network Password

Please type your user name and password.

Site: 192.168.1.1

Realm /

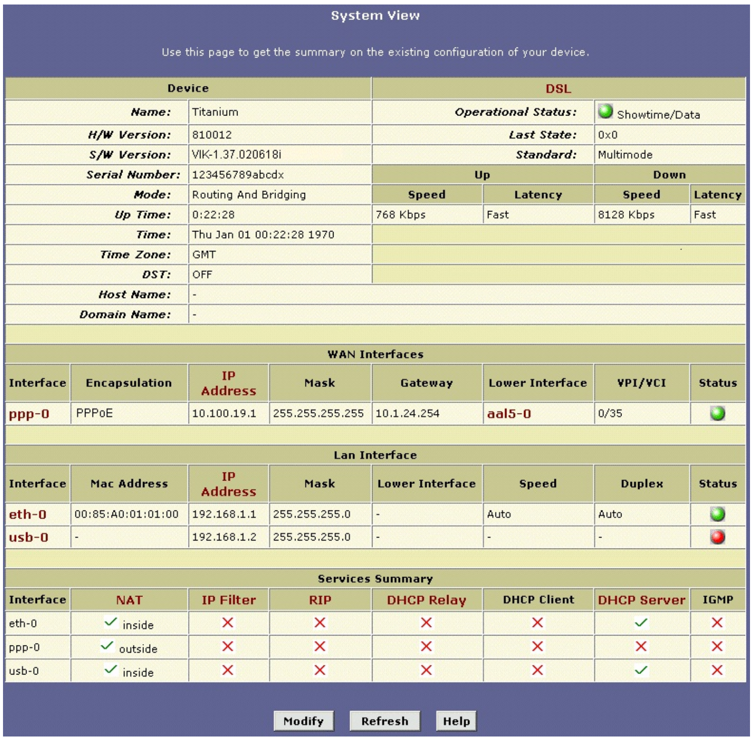
After successful login, the **System View** page displays.

Commonly Used Buttons and Icons

Button	Function
Submit	Stores in temporary system memory any changes you have made on the current page.
Refresh	Redisplays the current page with updated statistics.
Clear	When accumulated statistics are displaying, this button resets the statistics to their initial values.
Help	Launches the online help for the current topic in a separate browser window. Help is available from any main topic page.
🗑	Delete an entry.
✏	Modify an entry.
🔍	View details for an entry.

Viewing Basic System Information

The System View page displays when you first access the program:



System View

Use this page to get the summary on the existing configuration of your device.

Device	
Name:	Titanium
H/W Version:	810012
S/W Version:	VIK-1.37.020618i
Serial Number:	123456789abcdx
Mode:	Routing And Bridging
Up Time:	0:22:28
Time:	Thu Jan 01 00:22:28 1970
Time Zone:	GMT
DST:	OFF
Host Name:	-
Domain Name:	-

DSL			
Operational Status:		🟢 Showtime/Data	
Last State:		0x0	
Standard:		Multimode	
Up		Down	
Speed	Latency	Speed	Latency
768 Kbps	Fast	8128 Kbps	Fast

WAN Interfaces

Interface	Encapsulation	IP Address	Mask	Gateway	Lower Interface	VPI/VCI	Status
ppp-0	PPPoE	10.100.19.1	255.255.255.255	10.1.24.254	aal5-0	0/35	🟢

Lan Interface

Interface	Mac Address	IP Address	Mask	Lower Interface	Speed	Duplex	Status
eth-0	00:85:A0:01:01:00	192.168.1.1	255.255.255.0	-	Auto	Auto	🟢
usb-0	-	192.168.1.2	255.255.255.0	-	-	-	🔴

Services Summary

Interface	NAT	IP Filter	RIP	DHCP Relay	DHCP Client	DHCP Server	IGMP
eth-0	✓ inside	✗	✗	✗	✗	✓	✗
ppp-0	✓ outside	✗	✗	✗	✗	✗	✗
usb-0	✓ inside	✗	✗	✗	✗	✓	✗

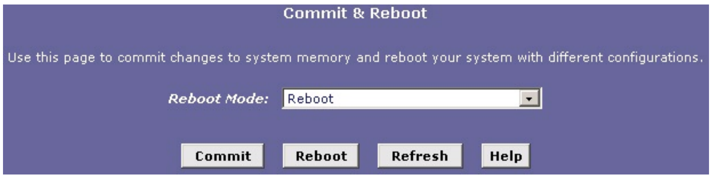
The System View table provides a snapshot of your system configuration. You can click on the provided links that enable you to configure each setting (if available). Refer to the appropriate chapters in this document for more information.

Committing Changes to Permanent Storage

Whenever you change system settings, the changes are initially placed in temporary storage (called random access memory or RAM). Your changes are made effective when you submit them, but will be lost if the device is reset or turned off.

Follow these steps to commit changes to permanent storage.

1. Select **Admin** > **Commit & Reboot**. The Commit & Reboot page displays:



Commit & Reboot

Use this page to commit changes to system memory and reboot your system with different configurations.

Reboot Mode: Reboot

2. Click **Commit**. (Disregard the selection in the Reboot Mode drop-down list; it does not affect the commit process.)

   The changes are saved to permanent storage.

When committing your changes, note that:

- If you change the LAN IP address information, you **must** commit the changes and then reboot the system to activate them.
- All other changes are activated when you commit them (no reboot is needed).

Rebooting the device using Configuration Manager

If, after rebooting the device, you find that it does not operate properly with the new configuration, you can reboot using options that reactivate a previous configuration or the manufacturer's default configuration.

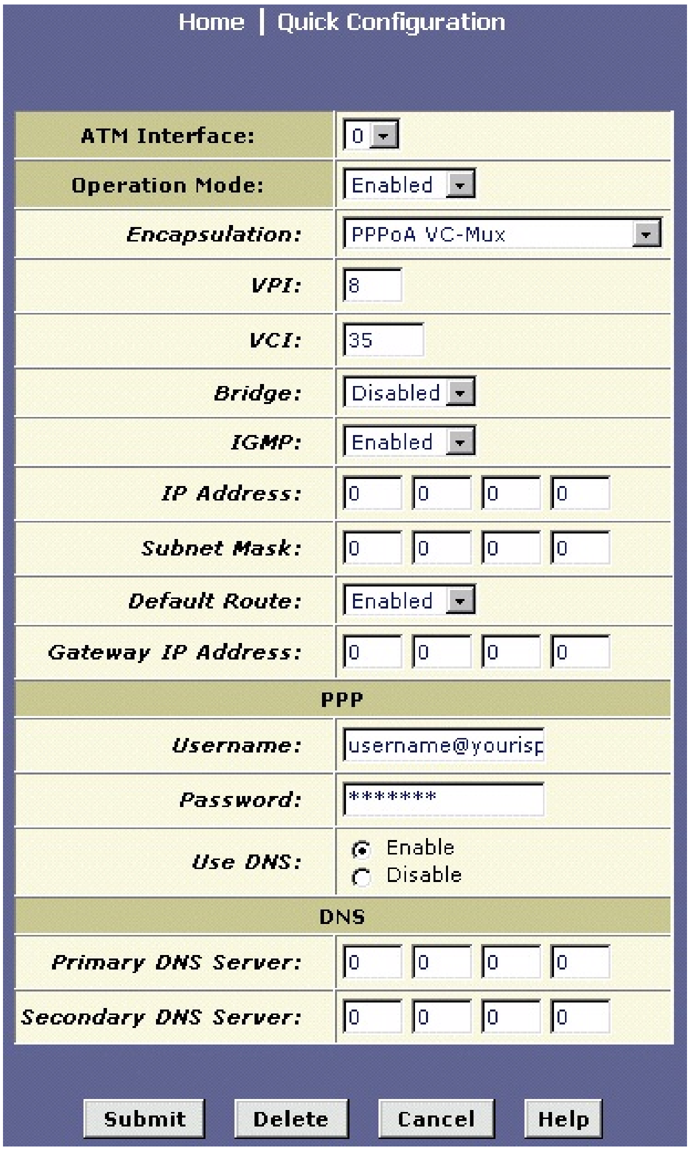
You can select from the following three options when rebooting:

Setting	Description
Reboot	Reboot the device to activate your new settings (if any).
Reboot from Last Configuration	Reboots the device using the current settings in permanent memory, including any changes you just committed.
Reboot from Backup Configuration	Reboots the device using settings stored in backup memory. These are the settings that were in effect before you committed new settings in the current session.
Reboot from Default Configuration	Reboots the device to default settings provided by your ISP or the manufacturer. Choosing this option erases any custom settings.

Quick Configuration

The Quick Configuration page allows you to quickly configure your ADSL Bridge/Router for Internet connection. Your ISP should provide you with the necessary information to complete the quick setup.

To quickly configure the system, go to **Home** > **Quick Configuration**. The Quick Configuration page displays.



ATM Interface:	0
Operation Mode:	Enabled
Encapsulation:	PPPoA VC-Mux
VPI:	8
VCI:	35
Bridge:	Disabled
IGMP:	Enabled
IP Address:	0 0 0 0
Subnet Mask:	0 0 0 0
Default Route:	Enabled
Gateway IP Address:	0 0 0 0
PPP	
Username:	username@yourisp
Password:	*******
Use DNS:	● Enable ○ Disable
DNS	
Primary DNS Server:	0 0 0 0
Secondary DNS Server:	0 0 0 0

Enter the provided fields as below.

Field	Description
ATM Interface	Select the ATM interface you want to use (usually **atm-0**) for this connection.
Operation Mode	Select **Yes**. If set to **No**, the device cannot provide Internet connectivity for your network.

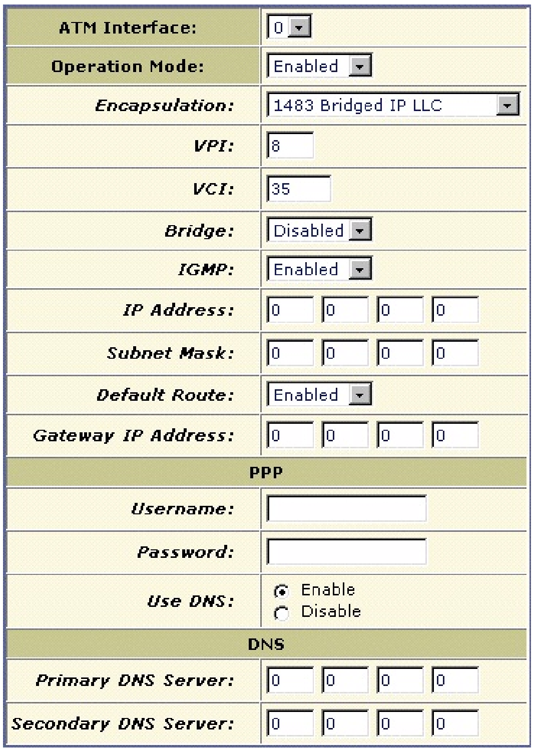
Field	Description
Encapsulation	Select the connection type your ISP uses to communicate with your ADSL Bridge/Router.
VCI and VPI	Enter the VPI/VCI values given by your ISP.
Bridge	This setting enables or disables bridging between the ADSL Bridge/Router and your ISP. Your ISP may also refer to this using “RFC 1483” or “Ethernet over ATM”.
IGMP	This setting enables or disables the Internet Group Management Protocol. Contact your ISP whether to enable this setting.
IP Address and *Subnet Mask*	If your ISP has assigned a public IP address to your LAN, enter the IP address and the associated subnet mask in the boxes provided. Otherwise keep the default 0.0.0.0/0.0.0.0.
Default Route	When enabled, the IP address specified above will be used as the default route for your LAN.
Gateway IP Address	Specify the IP address that identifies the ISP server through which your Internet connection will be routed.
Username and *Password*	If you select PPP as the Encapsulation type, enter the username and password you use to log in to your ISP.
Use DNS	Click Enable to turn on the DNS forwarding service, which forwards to your LAN PCs the DNS server addresses that your PPP connections learns from your ISP. This option can only be used when the ADSL Bridge/Router acts as a DHCP server for your LAN.
Primary/ Secondary DNS Server	You may just keep the default 0.0.0.0. If you enter the Primary and Secondary DNS addressed given by your ISP, these DNS servers will be used in addition to any DNS servers discovered automatically.

After completing the required settings, click **Submit**.

Then go to **Admin** > **Commit & Reboot** and click **Commit** to store your changes to permanent memory.

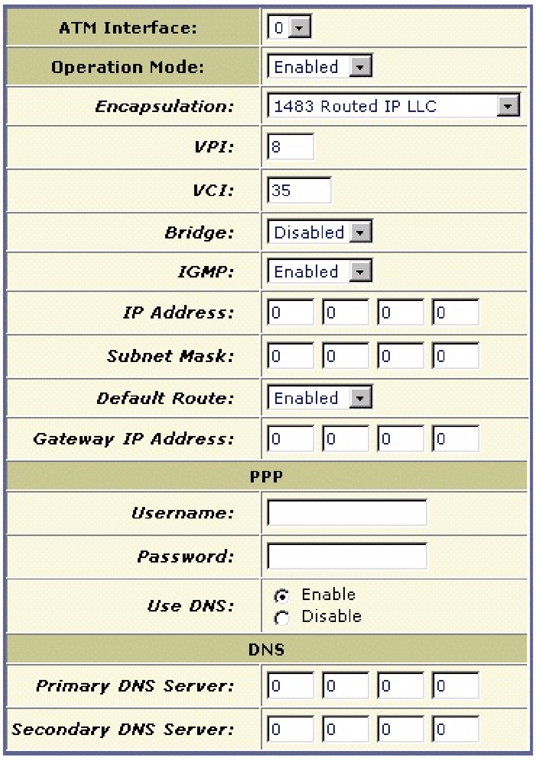
Quick Configuration Examples

RFC 1483 Bridge



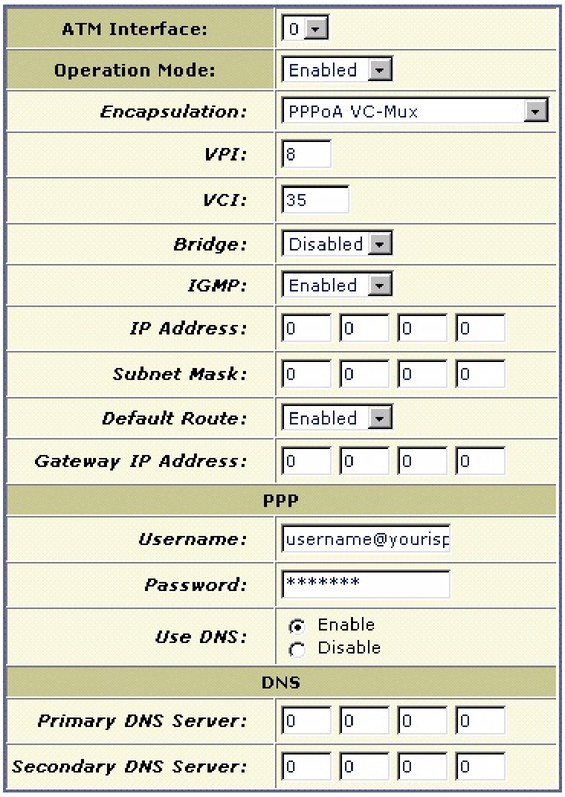
ATM Interface:	0
Operation Mode:	Enabled
Encapsulation:	1483 Bridged IP LLC
VPI:	8
VCI:	35
Bridge:	Disabled
IGMP:	Enabled
IP Address:	0 0 0 0
Subnet Mask:	0 0 0 0
Default Route:	Enabled
Gateway IP Address:	0 0 0 0
PPP	
Username:	
Password:	
Use DNS:	● Enable ○ Disable
DNS	
Primary DNS Server:	0 0 0 0
Secondary DNS Server:	0 0 0 0

RFC 1483 Routed



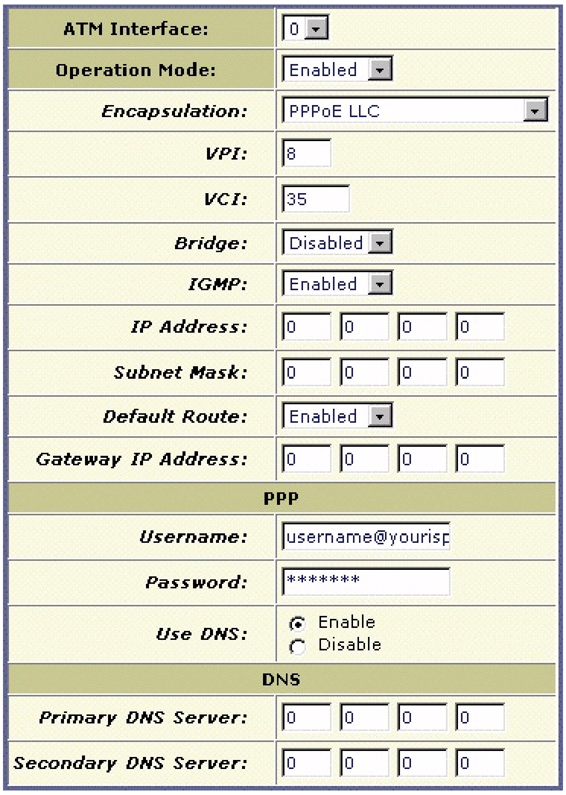
ATM Interface:	0
Operation Mode:	Enabled
Encapsulation:	1483 Routed IP LLC
VPI:	8
VCI:	35
Bridge:	Disabled
IGMP:	Enabled
IP Address:	0 0 0 0
Subnet Mask:	0 0 0 0
Default Route:	Enabled
Gateway IP Address:	0 0 0 0
PPP	
Username:	
Password:	
Use DNS:	● Enable ○ Disable
DNS	
Primary DNS Server:	0 0 0 0
Secondary DNS Server:	0 0 0 0

RFC 2364 PPPoA



ATM Interface:	0 ▾
Operation Mode:	Enabled ▾
Encapsulation:	PPPoA VC-Mux ▾
VPI:	8
VCI:	35
Bridge:	Disabled ▾
IGMP:	Enabled ▾
IP Address:	0 . 0 . 0 . 0
Subnet Mask:	0 . 0 . 0 . 0
Default Route:	Enabled ▾
Gateway IP Address:	0 . 0 . 0 . 0
PPP	
Username:	username@yourisp
Password:	*******
Use DNS:	● Enable ○ Disable
DNS	
Primary DNS Server:	0 . 0 . 0 . 0
Secondary DNS Server:	0 . 0 . 0 . 0

RFC 2516 PPPoE



ATM Interface:	0 ▾
Operation Mode:	Enabled ▾
Encapsulation:	PPPoE LLC ▾
VPI:	8
VCI:	35
Bridge:	Disabled ▾
IGMP:	Enabled ▾
IP Address:	0 . 0 . 0 . 0
Subnet Mask:	0 . 0 . 0 . 0
Default Route:	Enabled ▾
Gateway IP Address:	0 . 0 . 0 . 0
PPP	
Username:	username@yourisp
Password:	*******
Use DNS:	● Enable ○ Disable
DNS	
Primary DNS Server:	0 . 0 . 0 . 0
Secondary DNS Server:	0 . 0 . 0 . 0

6 Basic Configuration

The chapter provides you with the basic configurations to get your device run and have your network connected to the Internet.

The instructions assume that the device is not predefined with any ATM VC, PPP and IPoA settings. For each connection method, example parameters are given for your better understanding. You should consult with your IPS to determine your connection mode and enter the actual values provided by your ISP.

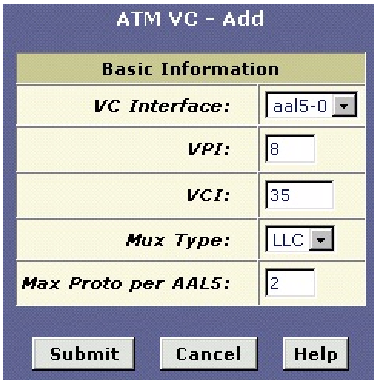
Your device may already be pre-configured with the necessary settings to get your network connected to the Internet. Contact your ISP to determine whether you should change any existing values.

Bridge Mode

Part 1: Configuring the ADSL Bridge/Router

1. Creating an ATM VC interface.

a. Select **Bridging** > **ATM VC** > **Add**. The ATM VC-Add page displays.



ATM VC - Add

Basic Information

VC Interface:	aal5-0
VPI:	8
VCI:	35
Mux Type:	LLC
Max Proto per AAL5:	2

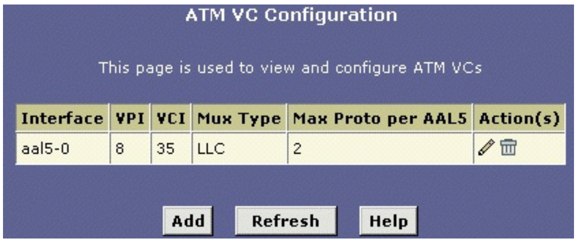
b. Enter the provided fields as below.

Field	Description
VC Interface	Select a VC interface from the available interfaces, e.g., ***aal5-0***.
VPI/VCI	Enter the VPI/VCI values given by your ISP,e.g., ***8/35***.
Mux Type	Select **LLC** or **VC** as required by your ISP.
Max Proto per AAL5	Keep the default **2**.

After entering the fields above, click **Submit**.

c. When confirmation page appears, click **Close**.

d. You will return to the **ATM VC Configuration** table and see the newly added ATM VC entry.



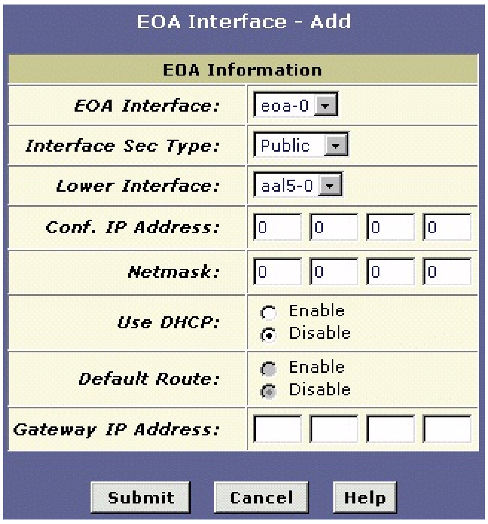
ATM VC Configuration

This page is used to view and configure ATM VCs

Interface	VPI	VCI	Mux Type	Max Proto per AAL5	Action(s)
aal5-0	8	35	LLC	2	✎ 🗑

2. Creating an EoA interface.

a. Select **Bridging** > **RFC1483 Interface (EoA)** > **Add** to add a new EoA interface.



EOA Interface - Add

EOA Information

EOA Interface:	eoa-0 ▾
Interface Sec Type:	Public ▾
Lower Interface:	aal5-0 ▾
Conf. IP Address:	0 . 0 . 0 . 0
Netmask:	0 . 0 . 0 . 0
Use DHCP:	○ Enable ● Disable
Default Route:	○ Enable ● Disable
Gateway IP Address:	

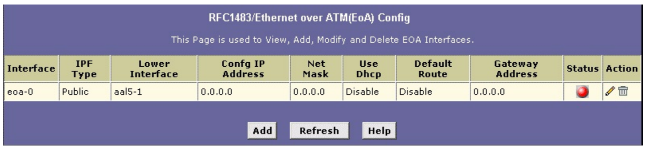
b. Enter the provided fields as below.

Field	Description
EOA Interface	Select an EoA interface from the available interfaces, e.g., ***eoa-0***.
IPF Type	**Public**.
Lower Interface	Select the ATM VC interface you created in Step 1, e.g., ***aal5-0***.
Config. IP Address/Net Mask	**0.0.0.0/0.0.0.0**. To use the device as a bridge, you don't need to set the IP address and subnet mask. Just keep the default.
Use DHCP	**Disable**
Default Route	**Disable**
Gateway IP Address	Leave it empty. You don't need to set the gateway.

After entering the fields above, click **Submit**.

c. When confirmation page appears, click **Close**.

d. You will return to the **EOA** table and see the newly added EOA entry.



RFC1483/Ethernet over ATM(EoA) Config

This Page is used to View, Add, Modify and Delete EOA Interfaces.

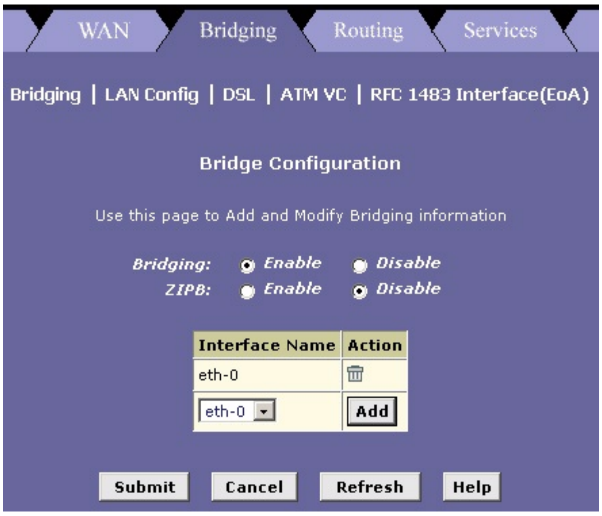
Interface	IPF Type	Lower Interface	Confg IP Address	Net Mask	Use Dhcp	Default Route	Gateway Address	Status	Action
eoa-0	Public	aal5-1	0.0.0.0	0.0.0.0	Disable	Disable	0.0.0.0	●	✎ 🗑

3. Enable Bridging function.

a. Select **Bridging** > **Bridging** page to display the Bridge Configuration page.

b. Select **eth-0** from the list and click **Add**. If the device's USB port is connected to a PC, select **usb-0** and click **Add**.

c. Select the EOA interface to be used (e.g. **eoa-0**) from the drop-down list, and then click **Add**.



WAN
Bridging
Routing
Services
Bridging | LAN Config | DSL | ATM VC | RFC 1483 Interface(EoA)

Bridge Configuration

Use this page to Add and Modify Bridging information

Bridging: ● Enable ○ Disable

ZIPB: ○ Enable ● Disable

Interface Name	Action
eth-0	🗑
eth-0 ▾	Add

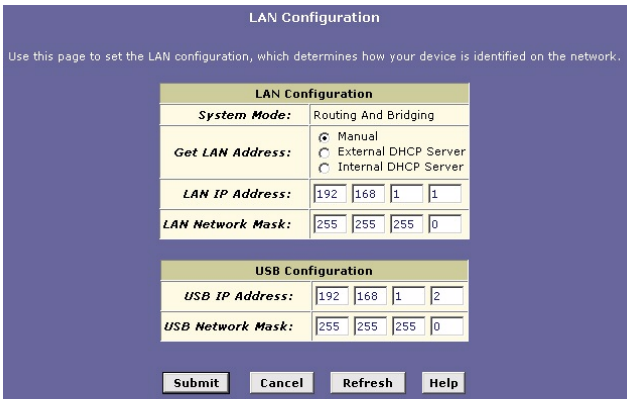
Submit
Cancel
Refresh
Help

d. Set the Bridging item to **Enable** and click **Submit**. A confirmation page display to confirm your changes.

4. LAN configuration.

a. Select **Bridging** > **LAN Config**.

b. Don't modify the settings; just keep the default shown as the figure below:



LAN Configuration

Use this page to set the LAN configuration, which determines how your device is identified on the network.

LAN Configuration	
System Mode:	Routing And Bridging
Get LAN Address:	● Manual ○ External DHCP Server ○ Internal DHCP Server
LAN IP Address:	192 . 168 . 1 . 1
LAN Network Mask:	255 . 255 . 255 . 0

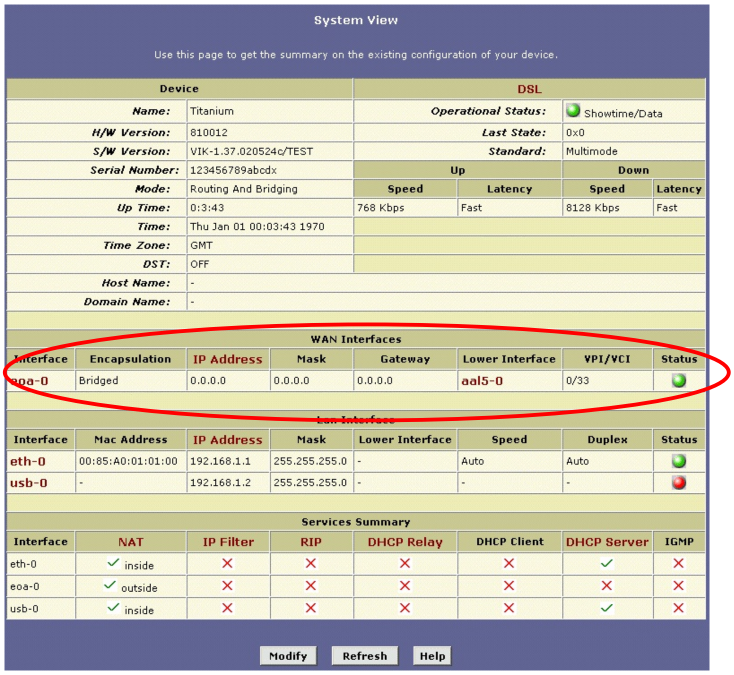
USB Configuration	
USB IP Address:	192 . 168 . 1 . 2
USB Network Mask:	255 . 255 . 255 . 0

5. Commit your changes.

Select **Admin** > **Commit & Reboot** and click **Commit** to store your changes to permanent memory.

Part 2: Check your connection status.

The WAN Interface item should display the interface you created to communicate with your ISP. A green ball in the Status field indicates a successful connection.



System View

Use this page to get the summary on the existing configuration of your device.

Device		DSL			
Name:	Titanium	Operational Status:		● Showtime/Data	
H/W Version:	810012	Last State:		0x0	
S/W Version:	VIK-1.37.020524c/TEST	Standard:		Multimode	
Serial Number:	123456789abcdx	Up		Down	
Mode:	Routing And Bridging	Speed	Latency	Speed	Latency
Up Time:	0:3:43	768 Kbps	Fast	8128 Kbps	Fast
Time:	Thu Jan 01 00:03:43 1970				
Time Zone:	GMT				
DST:	OFF				
Host Name:	-				
Domain Name:	-				

WAN Interfaces

Interface	Encapsulation	IP Address	Mask	Gateway	Lower Interface	VPI/VCI	Status
eoa-0	Bridged	0.0.0.0	0.0.0.0	0.0.0.0	aal5-0	0/33	●

Lan Interface

Interface	Mac Address	IP Address	Mask	Lower Interface	Speed	Duplex	Status
eth-0	00:85:A0:01:01:00	192.168.1.1	255.255.255.0	-	Auto	Auto	●
usb-0	-	192.168.1.2	255.255.255.0	-	-	-	●

Services Summary

Interface	NAT	IP Filter	RIP	DHCP Relay	DHCP Client	DHCP Server	IGMP
eth-0	✓ inside	✗	✗	✗	✗	✓	✗
eoa-0	✓ outside	✗	✗	✗	✗	✗	✗
usb-0	✓ inside	✗	✗	✗	✗	✓	✗

Part 2: Configuring the PC.

Option 1: Your PC uses the IP given by your ISP.

If this is the case, configure your PC to use the static IP given by your ISP, for example:

IP address: 10.100.16.2

Subnet mask: 255.255.255.0

Default gateway: 10.100.16.254

Note

With the configuration above, your PC should be able to access the Internet now but will lose the local connection to the device's LAN port. If you want to configure the ADSL Bridge/Router via the Web browser again, you should re-configure the PC to **192.168.1.x** to be in the same subnet of the device's LAN port.

Option 2: Your client use PPPoE software to connect to your ISP.

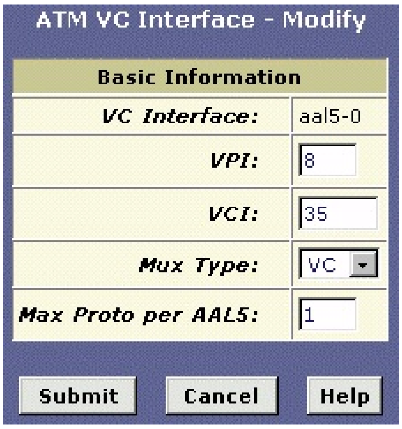
Just keep your PC's setting as a DHCP client and execute the PPPoE software to make the connection.

PPP Connection Mode

Part 1: Configuring the ADSL Bridge/Router

1. Creating an ATM VC interface.

a. Select **Routing**> **ATM VC** > **Add** to display ATM VC-Add page.



ATM VC Interface - Modify

Basic Information

VC Interface:	aal5-0
VPI:	8
VCI:	35
Mux Type:	VC
Max Proto per AAL5:	1

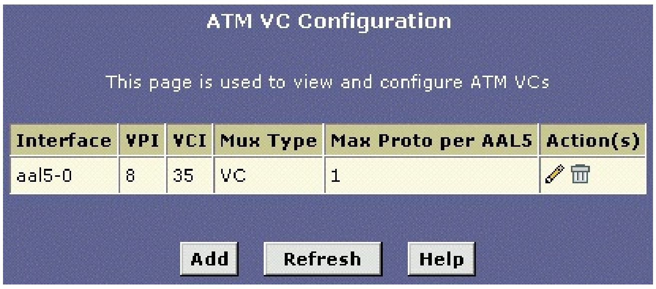
b. Enter the provided fields as below.

Field	Description
VC Interface	Select a VC interface from the available interfaces, e.g., ***aal5-0***.
VPI/VCI	Enter the VPI/VCI values given by your ISP,e.g., **8/35**.
Mux Type	For PPPoE, select **LLC**.
	For PPPoA, select **VC**.
Max Proto per AAL5	Keep the default **1**.

After entering the fields above, click **Submit**.

c. When confirmation page appears, click **Close**.

d. You will return to the **ATM VC Configuration** table and see the newly added ATM VC entry.



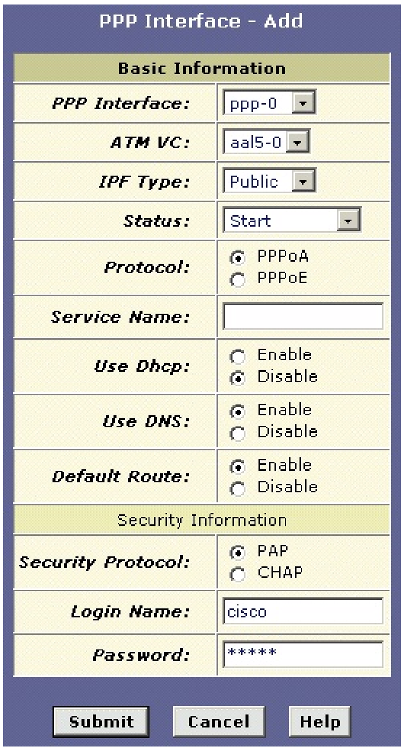
ATM VC Configuration

This page is used to view and configure ATM VCs

Interface	VPI	VCI	Mux Type	Max Proto per AAL5	Action(s)
aal5-0	8	35	VC	1	✎ 🗑

2. Creating a PPP interface.

a. Select **Routing** > **PPP** > **Add** to add a new PPP interface.



PPP Interface - Add

Basic Information

PPP Interface:	ppp-0
ATM VC:	aal5-0
IPF Type:	Public
Status:	Start
Protocol:	● PPPoA ○ PPPoE
Service Name:	
Use Dhcp:	○ Enable ● Disable
Use DNS:	● Enable ○ Disable
Default Route:	● Enable ○ Disable

Security Information

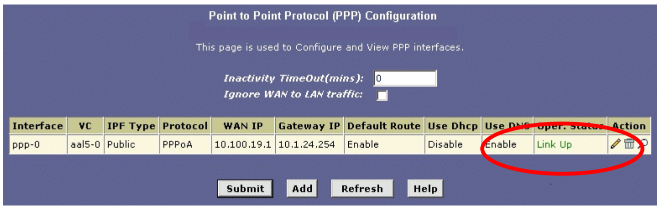
Security Protocol:	● PAP ○ CHAP
Login Name:	cisco
Password:	*****

b. Enter the provided fields as below.

Field	Description
PPP Interface	Select a PPP interface from the available interfaces, e.g., ***ppp-0***.
ATM VC	Select the ATM VC you created in step 1, e.g., ***aal5-0***.
IPF Type	**Public**
Status	Select **Start** or **StartOnData**. **Start** – To establish connection whenever you turn on the ADSL Bridge/Router. **StartOnData** – To establish connection whenever the device gets request to connect to the Internet, such as when you open browser requesting for web pages.
Protocol	**PPPoA** or **PPPoE** as required by your ISP.
Service Name	For **PPPoA**, no need to set up. For **PPPoE**, enter the Service Name if this is required by your ISP. Otherwise leave it blank.
Use DHCP	Select **Disable** unless your ISP instructs you to enable this service.
Use DNS	**Enable**
Default Route	**Enable**

Field	Description
Security Protocol	Select **PAP** or **CHAP** as required by your ISP.
Login Name/ Password	The login name and password given by your ISP. Note that characters of colon (:), semicolon (;) and question mark (?) are not allowed when entering login name and password.

c. You will return to PPP Configuration page and see the new PPP interface. The Oper. Status **Link Up** indicates the link is currently up.



Point to Point Protocol (PPP) Configuration

This page is used to Configure and View PPP interfaces.

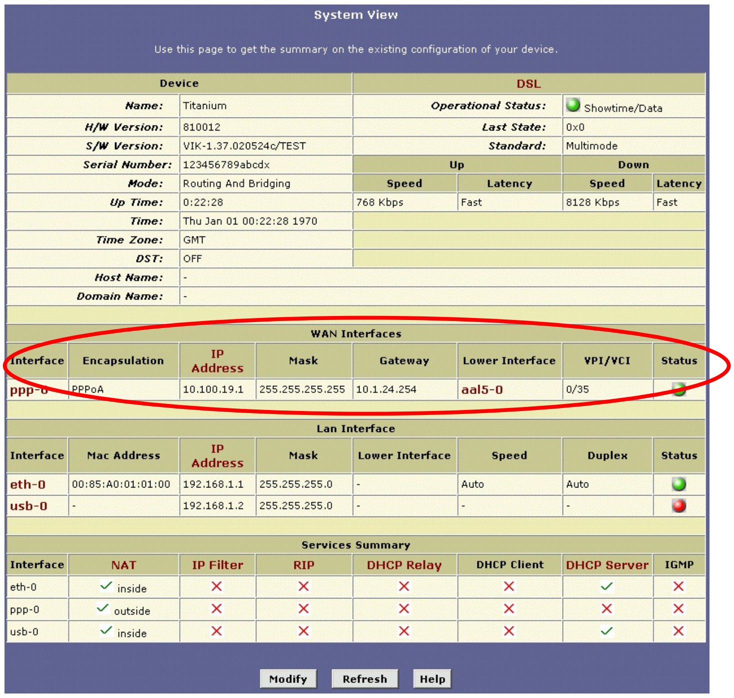
Inactivity TimeOut(mins): 0

Ignore WAN to LAN traffic: □

Interface	VC	IPF Type	Protocol	WAN IP	Gateway IP	Default Route	Use Dhcp	Use DNS	Oper. Status	Action
ppp-0	aal5-0	Public	PPPoA	10.100.19.1	10.1.24.254	Enable	Disable	Enable	Link Up	

Part 2: Check your connection status.

The WAN Interface item should display the interface you created to communicate with your ISP. A green ball in the Status field indicates a successful connection.



System View

Use this page to get the summary on the existing configuration of your device.

Device	
Name:	Titanium
H/W Version:	810012
S/W Version:	VIK-1.37.020524c/TEST
Serial Number:	123456789abcdx
Mode:	Routing And Bridging
Up Time:	0:22:28
Time:	Thu Jan 01 00:22:28 1970
Time Zone:	GMT
DST:	OFF
Host Name:	-
Domain Name:	-

DSL			
Operational Status:	● Showtime/Data		
Last State:	0x0		
Standard:	Multimode		
Up		Down	
Speed	Latency	Speed	Latency
768 Kbps	Fast	8128 Kbps	Fast

WAN Interfaces

Interface	Encapsulation	IP Address	Mask	Gateway	Lower Interface	VPI/VCI	Status
ppp-0	PPPoA	10.100.19.1	255.255.255.255	10.1.24.254	aal5-0	0/35	●

Lan Interface

Interface	Mac Address	IP Address	Mask	Lower Interface	Speed	Duplex	Status
eth-0	00:85:A0:01:01:00	192.168.1.1	255.255.255.0	-	Auto	Auto	●
usb-0	-	192.168.1.2	255.255.255.0	-	-	-	●

Services Summary

Interface	NAT	IP Filter	RIP	DHCP Relay	DHCP Client	DHCP Server	IGMP
eth-0	✓ inside	✗	✗	✗	✗	✓	✗
ppp-0	✓ outside	✗	✗	✗	✗	✗	✗
usb-0	✓ inside	✗	✗	✗	✗	✓	✗

Part 3: Configuring the PC.

Keep your PC’s setting as a DHCP client. No further configuration is required.

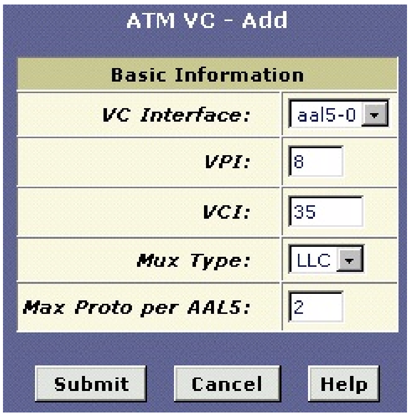
Router Connection Mode

This section describes both **RFC1577** and **RFC1483 Router** connection methods.

Part 1: Configuring the ADSL Bridge/Router

1. **Creating an ATM VC interface.**

a. Select **WAN** > **ATM VC** > **Add** to add a new ATM VC interface.



ATM VC - Add

Basic Information

VC Interface:	aal5-0
VPI:	8
VCI:	35
Mux Type:	LLC
Max Proto per AAL5:	2

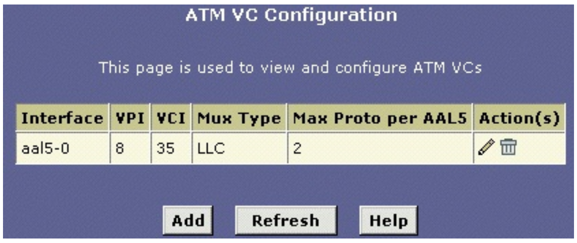
b. Enter the provided fields as below.

Field	Description
VC Interface	Select a VC interface from the available interfaces, e.g., ***aal5-0***.
VPI/VCI	Enter the VPI/VCI values given by your ISP, e.g., **8/35**.
Mux Type	Select **LLC** or **VC** as required by your ISP.
Max Proto per AAL5	Keep the default **2**.

After entering the fields above, click **Submit**.

c. When confirmation page appears, click **Close**.

d. You will return to the **ATM VC Configuration** table and see the newly added ATM VC entry.



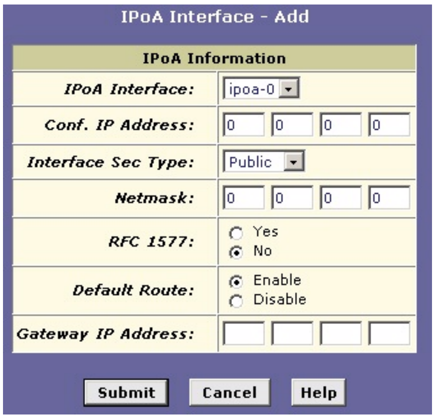
ATM VC Configuration

This page is used to view and configure ATM VCs

Interface	VPI	VCI	Mux Type	Max Proto per AAL5	Action(s)
aal5-0	8	35	LLC	2	✎ 🗑

2. Creating a IPoA interface.

a. Select **WAN** > **IPoA** > **Add** to add a new IPoA interface.



IPoA Interface - Add

IPoA Information

IPoA Interface:	ipoa-0 ▾
Conf. IP Address:	0 . 0 . 0 . 0
Interface Sec Type:	Public ▾
Netmask:	0 . 0 . 0 . 0
RFC 1577:	○ Yes ● No
Default Route:	● Enable ○ Disable
Gateway IP Address:	

b. The ATM VC interface, e.g., aal5-0 should has been added to your lower interface.

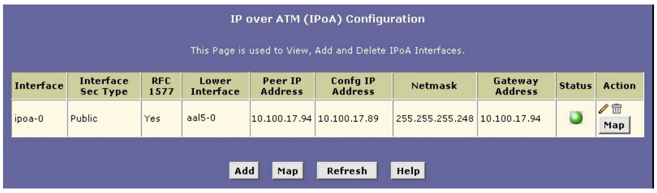
c. Then enter the fields below:

Field	Description
IPoA Interface	Select an IPoA interface from the available interfaces, e.g., ***ipoa-0***.
Conf. IP Address	Enter the IP address given by your ISP, e.g., **10.100.17.89**.
Interface Sec Type	Select the type of firewall protections that are in effect on the interface. e.g., **Public**.
Net Mask	Enter the IP address given by your ISP, e.g., **255.255.255.248**.
IPoA Type	For RFC 1577-Classical IP and ARP over ATM, select **Yes**. For RFC 1483 Router, select **No**.
Default Route	**Enable**
Gateway IP Address	Enter the gateway IP address given by your ISP, e.g., **10.100.17.94**.

After entering the fields above, click **Submit**.

d. When confirmation page appears, click **Close**.

e. You will return to the **IPoA Configuration** table and see the newly added IPoA entry.



IP over ATM (IPoA) Configuration

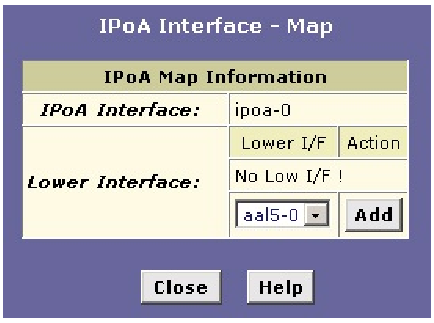
This Page is used to View, Add and Delete IPoA Interfaces.

Interface	Interface Sec Type	RFC 1577	Lower Interface	Peer IP Address	Confg IP Address	Netmask	Gateway Address	Status	Action
ipoa-0	Public	Yes	aal5-0	10.100.17.94	10.100.17.89	255.255.255.248	10.100.17.94	●	Map

3. **Mapping IPoA interface to a lower interface.**

   In the **IPoA Configuration** table, locate the new IPoA entry and click **Map** in the Action column.

   In IPoA Interface-Map page, from the drop-down list select the ATM VC you created in step 1 to be mapped to this IPoA interface and then click **Add**. Then click **Close** to exit the confirmation page.

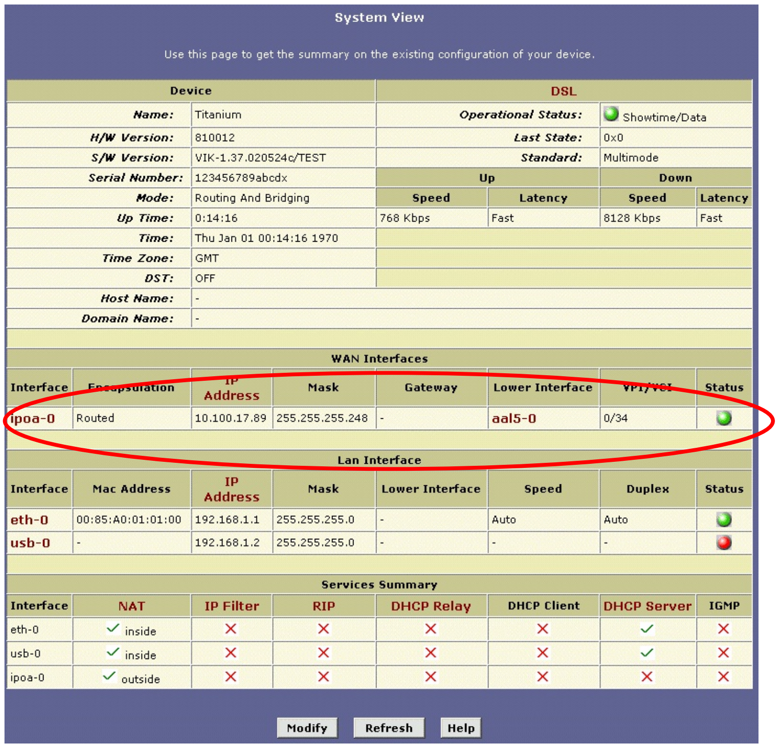


IPoA Interface - Map

IPoA Map Information		
IPoA Interface:	ipoa-0	
Lower Interface:	Lower I/F	Action
	No Low I/F !	
	aal5-0 ▾	Add

Part 2: Check your connection status.

The WAN Interface item should display the interface you created to communicate with your ISP. A green ball in the Status field indicates a successful connection.



System View

Use this page to get the summary on the existing configuration of your device.

Device		DSL			
Name:	Titanium	***Operational Status:***	● Showtime/Data		
H/W Version:	810012	***Last State:***	0x0		
S/W Version:	VIK-1.37.020524c/TEST	***Standard:***	Multimode		
Serial Number:	123456789abcdx	Up		Down	
Mode:	Routing And Bridging	Speed	Latency	Speed	Latency
Up Time:	0:14:16	768 Kbps	Fast	8128 Kbps	Fast
Time:	Thu Jan 01 00:14:16 1970				
Time Zone:	GMT				
DST:	OFF				
Host Name:	-				
Domain Name:	-				

WAN Interfaces

Interface	Encapsulation	IP Address	Mask	Gateway	Lower Interface	VPI/VCI	Status
ipoa-0	Routed	10.100.17.89	255.255.255.248	-	aal5-0	0/34	●

Lan Interface

Interface	Mac Address	IP Address	Mask	Lower Interface	Speed	Duplex	Status
eth-0	00:85:A0:01:01:00	192.168.1.1	255.255.255.0	-	Auto	Auto	●
usb-0	-	192.168.1.2	255.255.255.0	-	-	-	●

Services Summary

Interface	NAT	IP Filter	RIP	DHCP Relay	DHCP Client	DHCP Server	IGMP
eth-0	✓ inside	✗	✗	✗	✗	✓	✗
usb-0	✓ inside	✗	✗	✗	✗	✓	✗
ipoa-0	✓ outside	✗	✗	✗	✗	✗	✗

Part 3: Configuring the PC.

Keep your PC's setting as a DHCP client. No further configuration is required.

7 Configuring IP Routes

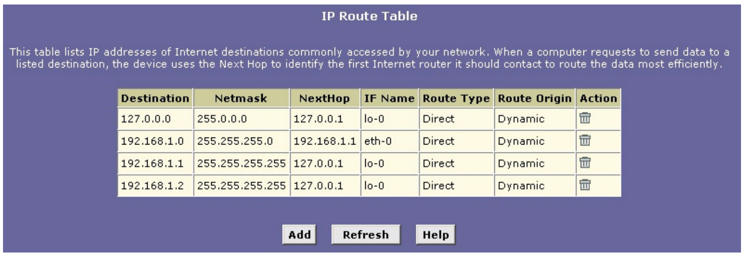
You can use Configuration Manager to define specific routes for your Internet and network data. This chapter provides instructions for creating routes.

Most users do not need to define IP routes. You may need to define routes if:

- Your network setup includes two or more networks or subnets.
- You connect to two or more ISP services.
- You connect to a remote corporate LAN.

Viewing the IP Routing Table

To view the ADSL Bridge/Router’s routing table, select **Routing** > **IP Route**. The following page displays:



This table lists IP addresses of Internet destinations commonly accessed by your network. When a computer requests to send data to a listed destination, the device uses the Next Hop to identify the first Internet router it should contact to route the data most efficiently.

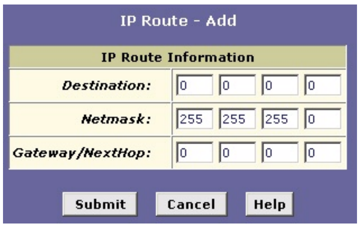
Destination	Netmask	NextHop	IF Name	Route Type	Route Origin	Action
127.0.0.0	255.0.0.0	127.0.0.1	lo-0	Direct	Dynamic	🗑
192.168.1.0	255.255.255.0	192.168.1.1	eth-0	Direct	Dynamic	🗑
192.168.1.1	255.255.255.255	127.0.0.1	lo-0	Direct	Dynamic	🗑
192.168.1.2	255.255.255.255	127.0.0.1	lo-0	Direct	Dynamic	🗑

The IP Route Table includes routes that were predefined on the device, routes you may have added, and routes that the device has identified automatically through communication with other devices.

The routing table should reflect a default gateway, which directs outbound Internet traffic to your ISP. This default gateway is shown in the row containing destination address 0.0.0.0.

Adding IP Routes

1. Select **Routing** > **IP Route** > **Add**. The IP Route – Add page displays:



IP Route Information				
Destination:	0	0	0	0
Netmask:	255	255	255	0
Gateway/NextHop:	0	0	0	0

2. Specify the destination, network mask, and gateway or next hop for this route.

To create a route that defines the default gateway for your LAN, enter **0.0.0.0** in both the **Destination** and **Net Mask** fields. Enter your ISP's IP address in the **Gateway**/**NextHop** field.

You cannot specify the interface name, route type or route origin. These parameters are used only for routes that are identified automatically as the device communicates with other routing devices. For routes you create, the routing table displays system default values in these fields.

3. Click **Submit**.

   The IP Routing Table will now display the new route.

4. Select **Admin** > **Commit & Reboot** and click **Commit** to save your changes to permanent storage.

8 DHCP Configuration

You can configure your network and ADSL Bridge/Router to use the Dynamic Host Configuration Protocol (DHCP). This chapter provides instructions for implementing DHCP on your network.

ADSL Bridge/Router DHCP Modes

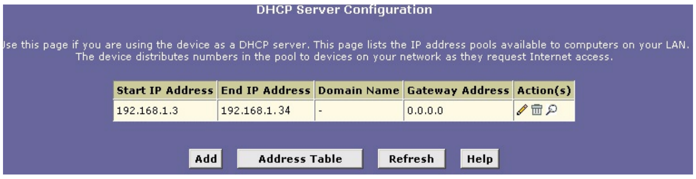
The device can be configured as a DHCP server, DHCP relay agent, or, in some cases, a DHCP client.

- **DHCP server** - It will maintain the pool of addresses and distribute them to your LAN computers. If the pool of addresses includes private IP addresses, you must also configure the Network Address Translation service, so that the private addresses can be translated to your public IP address on the Internet. Both DHCP server and NAT are enabled in the default configuration.
- **DHCP relay agent** - If your ISP performs the DCHP server function for your network, then you can configure the device as a DHCP relay agent. When the ADSL Bridge/Router receives a request for Internet access from a computer on your network, it contacts your ISP for the necessary IP information, and then relays the assigned information back to the computer.
- **DCHP Client** - If you have another PC or device on your network that is already performing the DHCP server function, then you can configure the LAN port on the ADSL Bridge/Router to be a DHCP client of that server.

Configuring DHCP Server

Part 1. Creating IP address pools

1. Select **LAN** > **DHCP Server**. The DHCP Server Configuration page displays:



DHCP Server Configuration

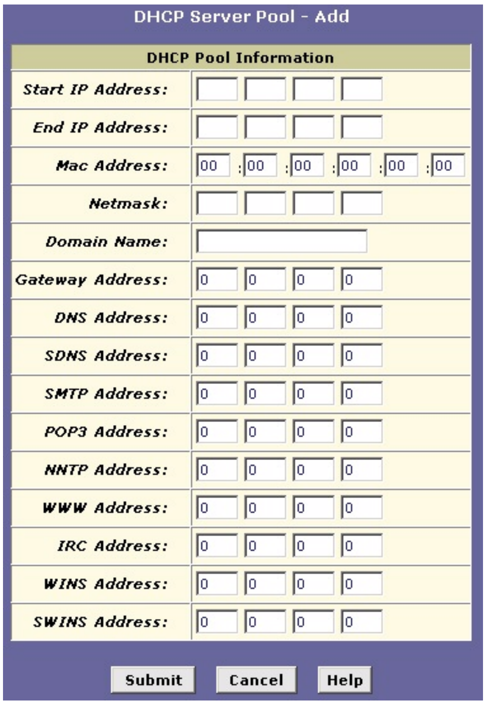
Use this page if you are using the device as a DHCP server. This page lists the IP address pools available to computers on your LAN. The device distributes numbers in the pool to devices on your network as they request Internet access.

Start IP Address	End IP Address	Domain Name	Gateway Address	Action(s)
192.168.1.3	192.168.1.34	-	0.0.0.0	✎ 🗑 🔍

Each pool you create displays in a row on the table on this page. You can create up to eight pools. In this example, one pool has been created for the LAN interface and another for the USB interface. Additional pools may be needed when the device is configured with multiple LAN interfaces.

2. To add an IP address pool, click **Add**.

   The DHCP Server Pool – Add page displays.



DHCP Server Pool - Add

DHCP Pool Information

Start IP Address:	
End IP Address:	
Mac Address:	00 : 00 : 00 : 00 : 00 : 00
Netmask:	
Domain Name:	
Gateway Address:	0 0 0 0
DNS Address:	0 0 0 0
SDNS Address:	0 0 0 0
SMTP Address:	0 0 0 0
POP3 Address:	0 0 0 0
NNTP Address:	0 0 0 0
WWW Address:	0 0 0 0
IRC Address:	0 0 0 0
WINS Address:	0 0 0 0
SWINS Address:	0 0 0 0

The ***Start IP Address***, ***End IP Address***, ***Net Mask***, and ***Gateway Address*** fields are required; the others are optional.

Field	Description
Start/End IP Addresses	Specify the lowest and highest addresses in the pool.
Mac Address	Allows you to assign a specific IP address to a specific computer, identified by this MAC address. If this is the case, you must have specified the same IP address in both the Start/End IP Address fields.
Net Mask	Specifies the associated subnet mask of the IP address in this range.
Domain Name	The domain name to be used by DHCP clients.
Gateway Address	The address of the default gateway. Typically, it is the device's LAN port IP address.
DNS	The IP address of the DNS Server . Its typically located with your ISP.
SDSN...SWINS (optional)	The IP addresses of devices that perform various services for DHCP clients.

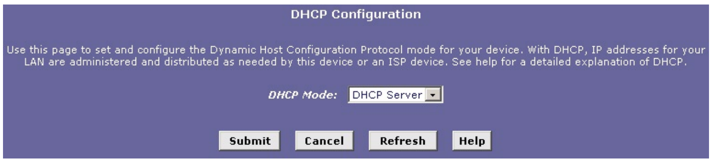
3. Click **Submit**.

   A confirmation page displays to indicate that the pool has been added successfully.

4. Click **Close** to return to the DHCP Configuration page.

Part 2. Enabling DHCP Server Mode

1. Select **LAN** > **DHCP Mode**, from the DHCP Mode drop-down list, select **DHCP Server**, and then click **Submit**.



DHCP Configuration

Use this page to set and configure the Dynamic Host Configuration Protocol mode for your device. With DHCP, IP addresses for your LAN are administered and distributed as needed by this device or an ISP device. See help for a detailed explanation of DHCP.

DHCP Mode: DHCP Server

A page displays to confirm the change.

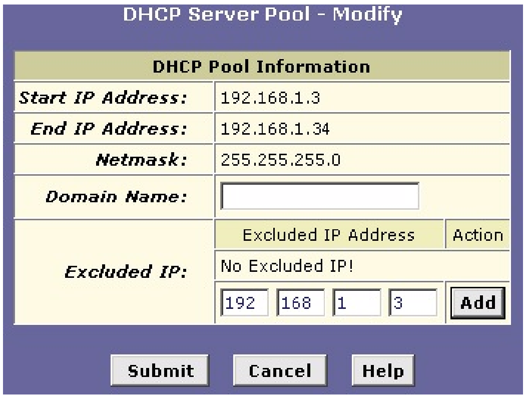
2. Select **Admin** > **Commit & Reboot** and click **Commit** to save your changes to permanent storage.

Part 3. Configuring your PCs as DHCP clients

For each computer that you want to configure to receive IP information automatically, configure the TCP/IP properties to "Obtain an IP address automatically" (the actual text may vary depending on your operating system).

Modifying Address Pools

Select **LAN** > **DHCP Server** and then click the modify icon on the DHCP pool which you want to modify. The DHCP Server Pool – Modify page displays:



DHCP Server Pool - Modify

DHCP Pool Information		
Start IP Address:	192.168.1.3	
End IP Address:	192.168.1.34	
Netmask:	255.255.255.0	
Domain Name:		
Excluded IP:	Excluded IP Address	Action
	No Excluded IP!	
	192 168 1 3	Add

When modifying an address pool, you are ***only*** allowed to:

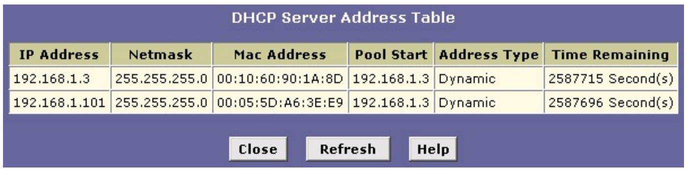
- Change the domain name associated with the pool.
- Exclude IP addresses within its range from distribution. To excluded an IP address, enter it in the fields provided and click **Add**.

If you want to change other attributes, you must delete the pool and create a new one.

After entering your changes, click **Submit** and be sure to use the Commit feature to save your changes to permanent memory.

Viewing Current DHCP Address Assignments

To view a table of all current IP address assignments, select **LAN** > **DHCP Server** > **Address Table**. The DHCP Server Address Table is as below:



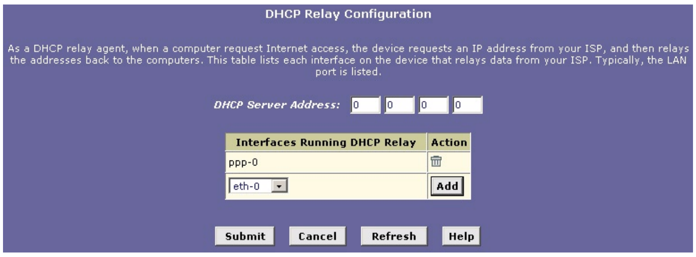
DHCP Server Address Table

IP Address	Netmask	Mac Address	Pool Start	Address Type	Time Remaining
192.168.1.3	255.255.255.0	00:10:60:90:1A:8D	192.168.1.3	Dynamic	2587715 Second(s)
192.168.1.101	255.255.255.0	00:05:5D:A6:3E:E9	192.168.1.3	Dynamic	2587696 Second(s)

Configuring DHCP Relay

Part 1. Defining the DHCP relay interface(s)

1. Select **LAN** > **DHCP Relay**. The DHCP Relay Configuration page displays:



DHCP Relay Configuration

As a DHCP relay agent, when a computer request Internet access, the device requests an IP address from your ISP, and then relays the addresses back to the computers. This table lists each interface on the device that relays data from your ISP. Typically, the LAN port is listed.

DHCP Server Address: 0 0 0 0

Interfaces Running DHCP Relay	Action
ppp-0	🗑
eth-0	Add

This page provides a text box for entering the IP address of your ISP's DHCP server and a table that lists the interfaces on your ADSL Bridge/Router that can relay DHCP information.

2. Type the IP address of your ISP's DHCP server in the fields provided.

   If you do not have this number, it is not essential to enter it here. Requests for IP information from your LAN will be passed to the default gateway, which should route the request appropriately.

3. If the interface named eth-0 is not already displaying, select it from the drop-down list and click **Add.**

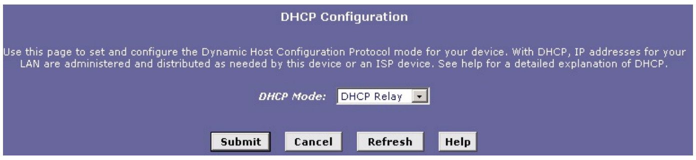
4. Click **Submit**.

   A page displays to confirm your changes.

Part 2. Enabling DHCP relay mode

1. Select **LAN** > **DHCP Mode**, from the DHCP Mode drop-down list, select **DHCP Relay**, and then click **Submit**.

   A page displays to confirm the change.



DHCP Configuration

Use this page to set and configure the Dynamic Host Configuration Protocol mode for your device. With DHCP, IP addresses for your LAN are administered and distributed as needed by this device or an ISP device. See help for a detailed explanation of DHCP.

DHCP Mode: DHCP Relay

2. Select **Admin** > **Commit & Reboot** and click **Commit** to save your changes to permanent storage.

Part 3. Configuring your PCs as DHCP clients

For each computer that you want to configure to receive IP information automatically, configure the TCP/IP properties to "Obtain an IP address automatically" (the actual text may vary depending on your operating system).

9 NAT Configuration

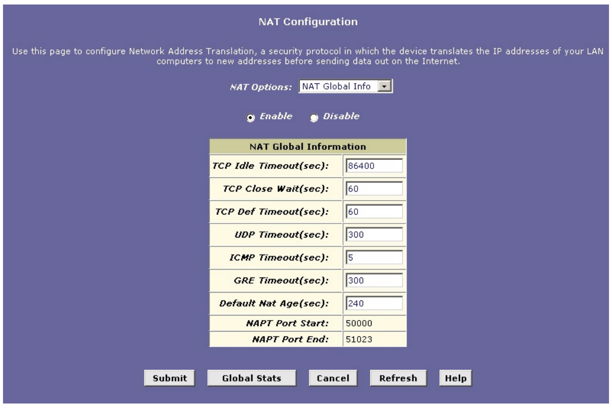
This chapter provides an overview of Network Address Translation (NAT) and instructions for modifying the default configuration on your device.

Your Default NAT Setup

By default, NAT is enabled, with an *network address port translation* (napt) rule configured that translates any private address on the LAN side to your ISP-assigned public IP address on the WAN side.

Viewing Your NAT Configuration

To view your NAT settings, select **Services** > **NAT**. The NAT Configuration page displays:



NAT Configuration

Use this page to configure Network Address Translation, a security protocol in which the device translates the IP addresses of your LAN computers to new addresses before sending data out on the Internet.

NAT Options: NAT Global Info

● *Enable* ○ *Disable*

NAT Global Information	
TCP Idle Timeout(sec):	86400
TCP Close Wait(sec):	60
TCP Def Timeout(sec):	60
UDP Timeout(sec):	300
ICMP Timeout(sec):	5
GRE Timeout(sec):	300
Default Nat Age(sec):	240
NAPT Port Start:	50000
NAPT Port End:	51023

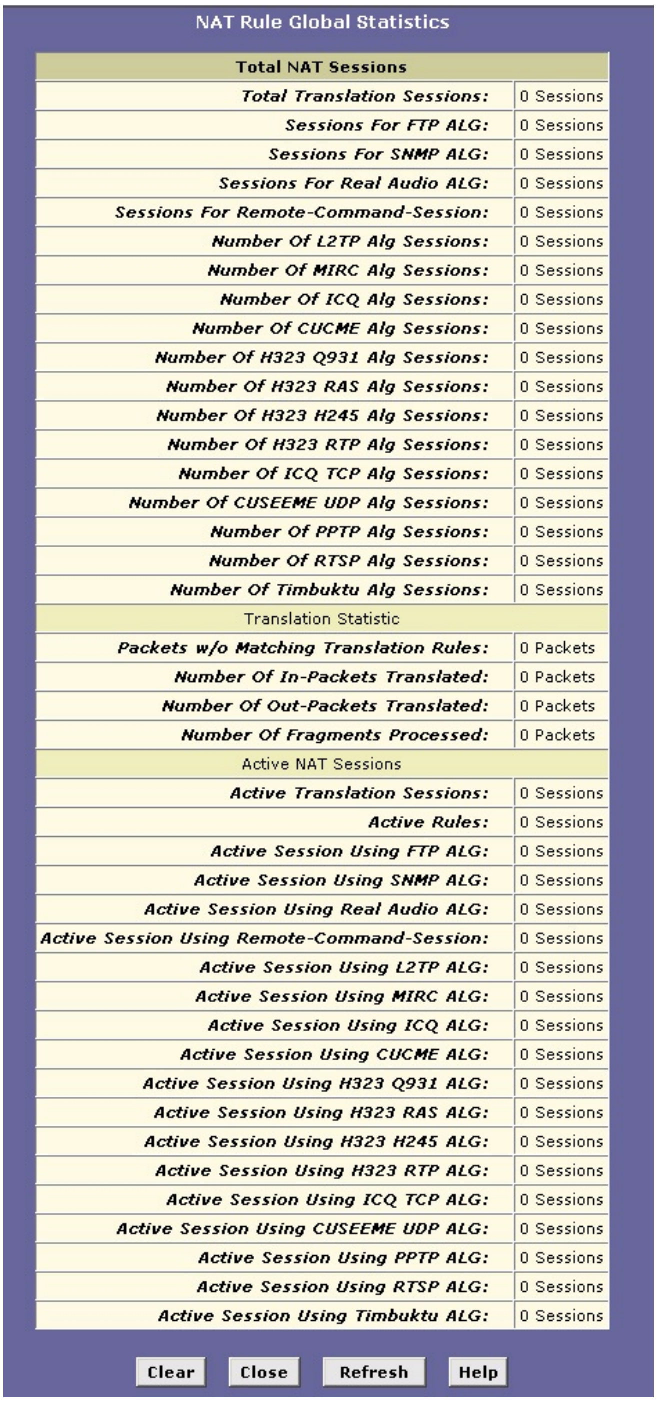
The NAT Global Information table contains the following fields:

Field	Description
TCP Idle Timeout (sec *TCP Close Wait (sec)* *TCP Def Timeout (sec)*	When a NAT rule is in effect on a TCP session in the **active** state, the session will timeout if no packets are received for the time specified in **TCP Idle Timeout**. When in the TCP session's closing sate, the session will timeout if no packets are received for the time specified in **TCP Close Wait**. When in the TCP session's establishing state, the session will timeout if no packets are received for the time specified in **TCP Def Timeout**.
UDP Timeout (sec)	Same as TCP Idle Timeout, but for UDP packets.

Field	Description
ICMP Timeout (sec)	Same as TCP Idle Timeout, but for ICMP packets.
GRE Timeout (sec)	Same as TCP Idle Timeout, but for GRE packets.
Default Nat Age (sec)	For all other NAT translation sessions, the number of seconds after which a translation session will no longer be valid.
NAPT Port Start/End	When an napt rule is defined, the source ports will be translated to sequential numbers in this range.

If you change any values, click **Submit**, and then commit your changes to permanent system memory.

You can click **Global Stats** to view accumulated data on how many NAT rules have been invoked and how much data has been translated. A page similar to the one below displays:

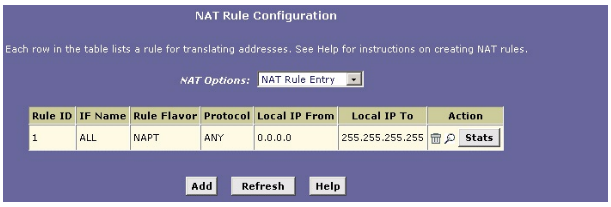


NAT Rule Global Statistics

Total NAT Sessions	
Total Translation Sessions:	0 Sessions
Sessions For FTP ALG:	0 Sessions
Sessions For SNMP ALG:	0 Sessions
Sessions For Real Audio ALG:	0 Sessions
Sessions For Remote-Command-Session:	0 Sessions
Number Of L2TP Alg Sessions:	0 Sessions
Number Of MIRC Alg Sessions:	0 Sessions
Number Of ICQ Alg Sessions:	0 Sessions
Number Of CUCME Alg Sessions:	0 Sessions
Number Of H323 Q931 Alg Sessions:	0 Sessions
Number Of H323 RAS Alg Sessions:	0 Sessions
Number Of H323 H245 Alg Sessions:	0 Sessions
Number Of H323 RTP Alg Sessions:	0 Sessions
Number Of ICQ TCP Alg Sessions:	0 Sessions
Number Of CUSEEME UDP Alg Sessions:	0 Sessions
Number Of PPTP Alg Sessions:	0 Sessions
Number Of RTSP Alg Sessions:	0 Sessions
Number Of Timbuktu Alg Sessions:	0 Sessions
Translation Statistic	
Packets w/o Matching Translation Rules:	0 Packets
Number Of In-Packets Translated:	0 Packets
Number Of Out-Packets Translated:	0 Packets
Number Of Fragments Processed:	0 Packets
Active NAT Sessions	
Active Translation Sessions:	0 Sessions
Active Rules:	0 Sessions
Active Session Using FTP ALG:	0 Sessions
Active Session Using SNMP ALG:	0 Sessions
Active Session Using Real Audio ALG:	0 Sessions
Active Session Using Remote-Command-Session:	0 Sessions
Active Session Using L2TP ALG:	0 Sessions
Active Session Using MIRC ALG:	0 Sessions
Active Session Using ICQ ALG:	0 Sessions
Active Session Using CUCME ALG:	0 Sessions
Active Session Using H323 Q931 ALG:	0 Sessions
Active Session Using H323 RAS ALG:	0 Sessions
Active Session Using H323 H245 ALG:	0 Sessions
Active Session Using H323 RTP ALG:	0 Sessions
Active Session Using ICQ TCP ALG:	0 Sessions
Active Session Using CUSEEME UDP ALG:	0 Sessions
Active Session Using PPTP ALG:	0 Sessions
Active Session Using RTSP ALG:	0 Sessions
Active Session Using Timbuktu ALG:	0 Sessions

Viewing NAT Rules and Rule Statistics

To view the NAT Rules currently defined on your system, select **Services** > **NAT** > **NAT Rule Entry**. The NAT Rule Configuration page displays:



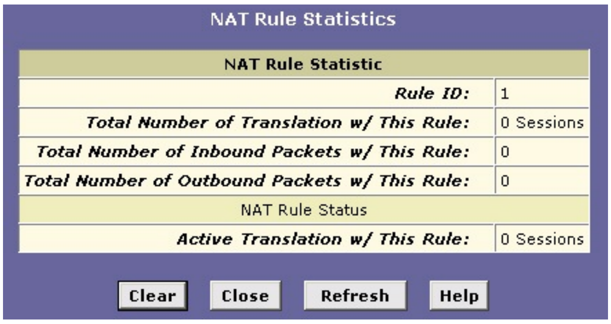
NAT Rule Configuration

Each row in the table lists a rule for translating addresses. See Help for instructions on creating NAT rules.

NAT Options: NAT Rule Entry

Rule ID	IF Name	Rule Flavor	Protocol	Local IP From	Local IP To	Action
1	ALL	NAPT	ANY	0.0.0.0	255.255.255.255	Stats

To view data on how often a specific NAT rule has been used, click **Stats**. A page similar to the one below displays:



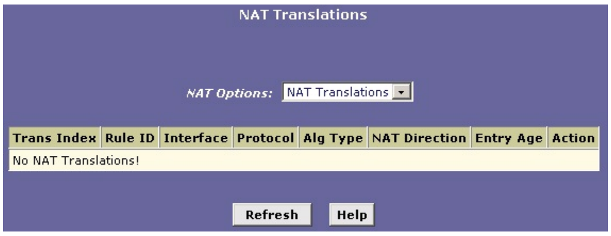
NAT Rule Statistics

NAT Rule Statistic	
Rule ID:	1
Total Number of Translation w/ This Rule:	0 Sessions
Total Number of Inbound Packets w/ This Rule:	0
Total Number of Outbound Packets w/ This Rule:	0
NAT Rule Status	
Active Translation w/ This Rule:	0 Sessions

The statistics show how many times this rule has been invoked and how many currently active sessions are using this rule.

Viewing Current NAT Translations

To view a list of NAT translations that have recently been performed and which remain in effect (for any of the defined rules), select **Services** > **NAT** > **NAT Translations**. The NAT Translations page displays:



NAT Translations

NAT Options: NAT Translations

Trans Index	Rule ID	Interface	Protocol	Alg Type	NAT Direction	Entry Age	Action
No NAT Translations!							

For each current NAT translation session, the table contains the following fields:

Field	Description
Trans Index	The sequential number assigned to the IP session used by this NAT translation session.
Rule ID	The ID of the NAT rule invoked.
Interface	The device interface on which the NAT rule was invoked (from the rule definition).
Protocol	The IP protocol used by the data packets that are undergoing translations (from the rule definition) Example: TCP, UDP, ICMP.
Alg Type	The *Application Level Gateway* (ALG), if any, that was used to enable this NAT translation (ALGs are special settings that certain applications require in order to work while NAT is enabled).
NAT Direction	The direction (incoming or outgoing) of the

Field	Description
	translation (from the port definition).
Entry Age	The elapsed time, in seconds, of the NAT translation session.

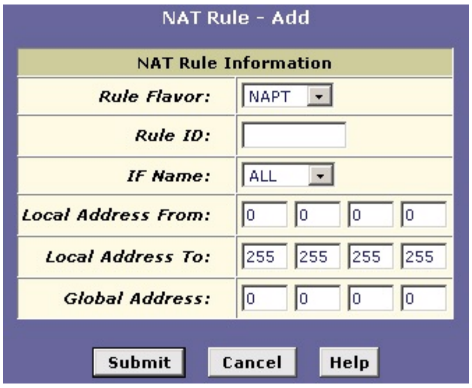
Adding NAT Rules

This section explains how to create rules for the various NAT flavors.

The napt rule: Translating between private and public IP addresses

The NAT flavor napt was used in your default configuration. The napt flavor translates all LAN-side private source IP addresses to a single public IP address. It also translates the source port numbers to port numbers that are defined on the NAT Global Configuration page.

1. Select **Services** > **NAT** > **NAT Rule Entry** > **Add**.



NAT Rule - Add

NAT Rule Information

Rule Flavor:	NAPT
Rule ID:	
IF Name:	ALL
Local Address From:	0 0 0 0
Local Address To:	255 255 255 255
Global Address:	0 0 0 0

2. Click the Rule ID drop-down list to assign a number to the rule.

   The Rule ID determines the order in which rules are invoked (the lowest numbered rule is invoked first, and so on). In some cases, two or more rules may be defined to act on the same set of IP addresses. Once a data packet matches a rule, the data is acted upon according to that rule and is not subjected to higher-numbered rules.

3. In the Rule Flavor drop-down list, select **NAPT**, if necessary.

4. From the IFName drop-down list, select the interface on the ADSL Bridge/Router to which this rule applies.

   Typically, NAT rules apply to communication between your LAN and the Internet. Because the device uses the WAN interface (named *ppp-0* or *eoa-0*) to connect your LAN to your ISP, it is the usual IFName selection.

5. Select a protocol to which this rule applies, or choose **ALL** if the rule applies to all data.

6. In the **Local Address From/To** fields, type the starting and ending IP addresses, respectively, of the range of private address you want to be translated. Or, type the same address in both fields to specify a single value.

   If all LAN addresses should be translated, specify 0.0.0.0 and 255.255.255.255 respectively.

   If you use non-sequential private addresses, you can create an additional napt rule for each separate range of addresses.

7. When you have completed entering all information, click **Submit**.

   A page displays to confirm the change.

8. Click **Close** to return to the NAT Configuration page.

   The new rule should display in the NAT Rule table.

9. On the NAT Configuration page, ensure that the **Enable** radio button is turned on.

10. On the NAT Configuration page, click **Submit**.

    A page displays to confirm your changes.

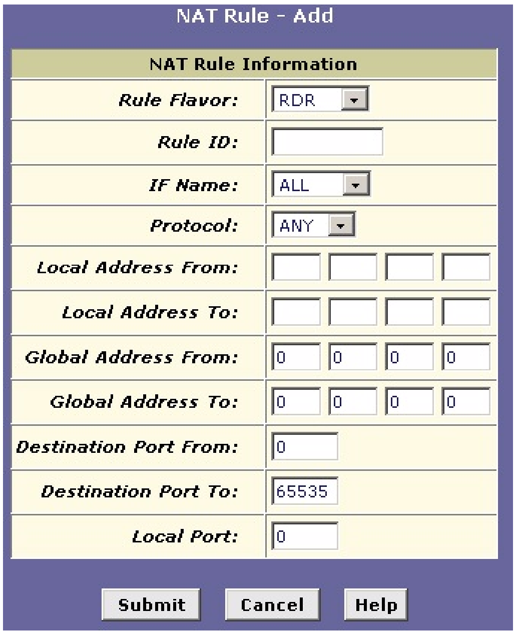
11. Select **Admin** > **Commit & Reboot** and click **Commit** to save your changes to permanent storage.

The rdr rule: Allowing external access to a LAN computer

You can create an rdr rule to make a computer on your LAN, such as a Web or FTP server, available to Internet users without requiring you to obtain a public IP address for that computer. The computer’s private IP address is translated to your public IP address in all incoming and outgoing data packets.

Note

Without an rdr rule (or bimap rule), the ADSL Bridge/Router blocks attempts by external computers to access your LAN computers.



NAT Rule - Add

NAT Rule Information	
Rule Flavor:	RDR
Rule ID:	
IF Name:	ALL
Protocol:	ANY
Local Address From:	
Local Address To:	
Global Address From:	0 0 0 0
Global Address To:	0 0 0 0
Destination Port From:	0
Destination Port To:	65535
Local Port:	0

Follow these instructions to add an rdr rule.

1. Display the NAT Rule – Add Page, choose a Rule ID, and select **RDR** as the Rule Flavor.

2. Select the interface and, if desired, a protocol that this rule applies to.

3. In the **Local Address From**/**To** fields, type the same private IP address, or the lowest and highest addresses in a range:

   - If you type the same IP address in both fields, incoming traffic that matches the criteria of this rule will be redirected to that IP address.

   - If you type a range of addresses, incoming traffic will be redirected to any available computer in that range. This option would typically be used for load balancing, whereby traffic is distributed among several redundant servers.

4. In the **Global Address From**/**To** fields, type the public IP address assigned to you by your ISP.

   If you have multiple WAN interfaces, in both fields type the IP address of the interface to which this rule applies. This rule will not be enforced for data that arrives on WAN interfaces not specified here.

   If you have multiple WAN interfaces and want the rule to be enforced on a range of them, type the starting and ending IP addresses of the range.

5. Enter a destination addresses (or a range) and port ID (or a range) as criteria for incoming traffic.

   Depending on which other fields you define in this step, incoming traffic that meets this criteria will be redirected to the address(es) specified in step 3 (assuming it comes through the interface specified in step 2).

- Enter a starting and ending IP address in the **Destination Address From/To** fields if incoming traffic destined for these addresses should be redirected.

  You can also enter a single address in both fields.

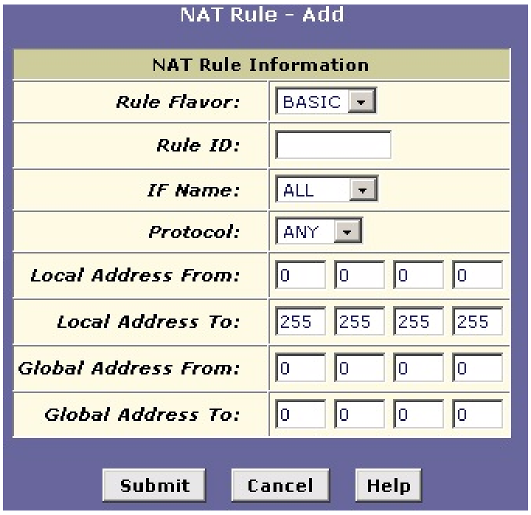
- Enter a starting and ending port number in the **Destination Port From/To** fields if incoming traffic destined for these port types should be redirected to the address(es) specified in step 3. Or, enter the same address in both fields.

6. If the publicly accessible LAN computer uses a non-standard port number for the type of traffic it receives, type the non-standard port number in the **Local Port** field.

The basic rule: Performing 1:1 translations

The basic flavor translates the private (LAN-side) IP address to a public (WAN-side) address, like napt rules. However, unlike napt rules, basic rules do not also translate the port numbers in the packet header; they are passed through untranslated. Therefore, the basic rule does not provide the same level of security as the napt rule.

The figure below shows the fields used for adding a basic rule.



NAT Rule - Add

NAT Rule Information				
Rule Flavor:	BASIC			
Rule ID:				
IF Name:	ALL			
Protocol:	ANY			
Local Address From:	0	0	0	0
Local Address To:	255	255	255	255
Global Address From:	0	0	0	0
Global Address To:	0	0	0	0

1. Display the NAT Rule – Add Page, choose a Rule ID, and select **BASIC** as the Rule Flavor.

2. Select the interface and, if desired, a protocol that this rule applies to.

3. In the **Local Address From/To** fields, type the starting and ending IP addresses that identify the range of private address you want to be translated. Or, type the same address in both fields.

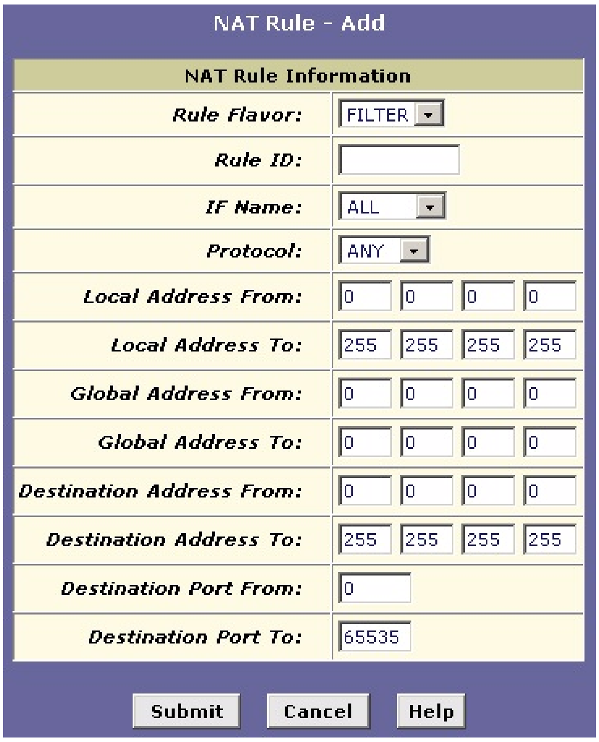
   If you specify a range, each address will be translated in sequence to a corresponding address in a range of global addresses (which you specify in step 4).

4. In the **Global Address From**/**To** fields, type the starting and ending address that identify the pool of public IP addresses to which to translate your private addresses. Or, type the same address in both fields (if you also specified a single address in step 3).

The filter rule: Configuring a basic rule with additional criteria

Like the basic flavor, the filter flavor translates public and private IP addresses on a one-to-one basis. The filter flavor extends the capability of the basic rule.

You can use the filter rule if you want an address translation to occur only when your LAN computers initiate access to specific destinations. The destinations can be identified by their IP addresses, server type (such as FTP or Web server), or both.



NAT Rule - Add

NAT Rule Information

Rule Flavor:	FILTER
Rule ID:	
IF Name:	ALL
Protocol:	ANY
Local Address From:	0 0 0 0
Local Address To:	255 255 255 255
Global Address From:	0 0 0 0
Global Address To:	0 0 0 0
Destination Address From:	0 0 0 0
Destination Address To:	255 255 255 255
Destination Port From:	0
Destination Port To:	65535

1. Display the NAT Rule – Add Page, choose a Rule ID, and select **FILTER** as the Rule Flavor.

2. Select the interface and, if desired, a protocol that this rule applies to.

3. In the **Local Address From**/**To** fields, type the starting and ending IP addresses that identify the range of private address you want to be translated. Or, type the same address in both fields.

   If you specify a range, each address will be translated in sequence to a corresponding address in a range of global addresses (which you specify in step 4).

4. In the **Global Address From**/**To** fields, type the starting and ending address that identify the range of public IP

addresses to translate your private addresses to. Or, type the same address in both fields (if you also specified a single address in step 3).

5. Specify a **Destination Address** (or addresses), **Destination Port** (or ports), or both. You can specify a single value by entering that value in both fields.

- Specify a destination address (or range) if you want this rule to apply only to outbound traffic to the address (or range).

  If you enter only the network ID portion of the destination address, then the rule will apply to outbound traffic to all computers on network.

- Specify a destination ports (or range) if you want this rule to apply to any outbound traffic to the types of servers identified by that port number.
- Specify both a destination address (or range) and a destination port (or range) if you want this translation rule to apply to accesses to the specified server type at the specified location.

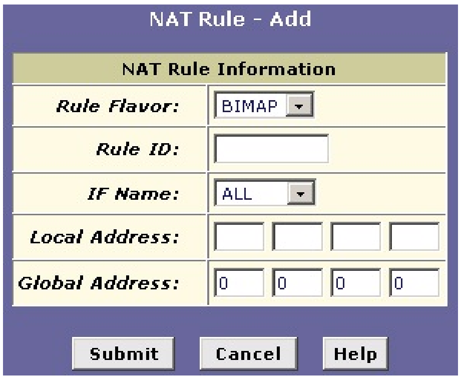
The bimap rule: Performing two-way translations

Unlike the other NAT flavors, the bimap flavor performs address translations in both the outgoing and incoming directions.

In the incoming direction, when the specified interface receives a packet destined to your public IP address, this address is translated to the private IP address of a computer on your LAN.

In the outgoing direction, the private source IP address in a data packet is translated to the LAN's public IP address.

Bimap rules can be used to provide external access to a LAN device. They do not provide the same level of security as rdr rules, because rdr rules also reroute incoming packets based on the port ID. Bimap rules do not account for the port number, and therefore allow external access regardless of the destination port type specified in the incoming packet.



NAT Rule - Add

NAT Rule Information	
Rule Flavor:	BIMAP
Rule ID:	
IF Name:	ALL
Local Address:	
Global Address:	0 . 0 . 0 . 0

1. Display the NAT Rule – Add Page, choose a Rule ID, and select **BIMAP** as the Rule Flavor.

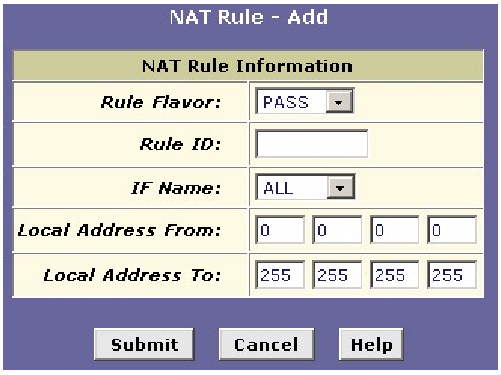
2. Select the interface and, if desired, a protocol that this rule applies to.

3. In the Local Address field, type the private IP address of the computer to which you are granting external access.

4. In the Global Address field, type the address that you want to serve as the publicly known address for the LAN computer.

The pass rule: Allowing specific addresses to pass through untranslated

You can create a pass rule to allow a range of IP addresses to remain untranslated when another rule would otherwise do so.



NAT Rule - Add

NAT Rule Information

Rule Flavor:	PASS
Rule ID:	
IF Name:	ALL
Local Address From:	0 0 0 0
Local Address To:	255 255 255 255

The pass rule must be assigned a rule ID that is a lower number than the ID assigned to the rule it is intended to pass. In you want a specific IP address or range of addresses to not be subject to an existing rule, say rule ID #5, then you can create a pass rule with ID #1 through 4.

1. Display the NAT Rule – Add Page, choose a Rule ID, and select **Pass** as the Rule Flavor.

2. Select the interface and, if desired, a protocol that this rule applies to.

3. In the **Local Address From** and **Local Address To** fields, type the lowest and highest IP addresses that define the range of private address you want to be passed without translation.

   If you want the pass rule to act on only one address, type that address in both fields.

10 Configuring DNS Server Addresses

This chapter describes how to configure DNS relay function on the ADSL Bridge/Router.

DNS Relay Overview

When performing DNS relay, the ADSL Bridge/Router itself is not a DNS server, it forwards DNS requests from LAN PCs to a DNS server at the ISP. It then relays the DNS response to the PCs.

The ADSL Bridge/Router learns DNS address in either or both of the following ways:

- **Learned through PPP**
- **Configured on the ADSL Bridge/Router**

Configuring DNS Relay

Follow these steps to configure DNS relay:

1. Configure the LAN PCs.

   Just set the LAN PCs as DHCP clients of the ADSL Bridge/Router.

2. On the ADSL Bridge/Router, go to **LAN** > **DHCP Server**, enter the LAN IP address (e.g., **192.168.1.1**) or **0.0.0.0** as the DNS address in the DHCP server pool.

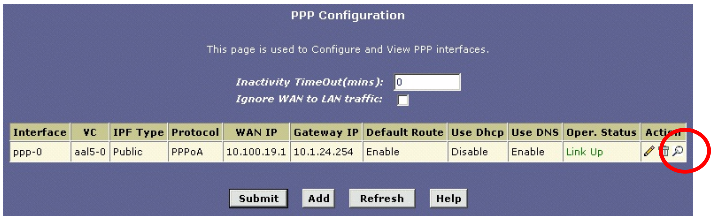
   By default, 0.0.0.0 is already set as the DNS of the DHCP pool.

3. Determines how the router will learn the DNS server address:

   Option 1: Using a PPP connection to learn the DNS

   Use DNS must be enabled in the PPP interface properties.

   Go to **Routing** > **PPP** and check the PPP interface details. If **Use DNS** is disabled, you must delete the interface and recreate it with the new setting.



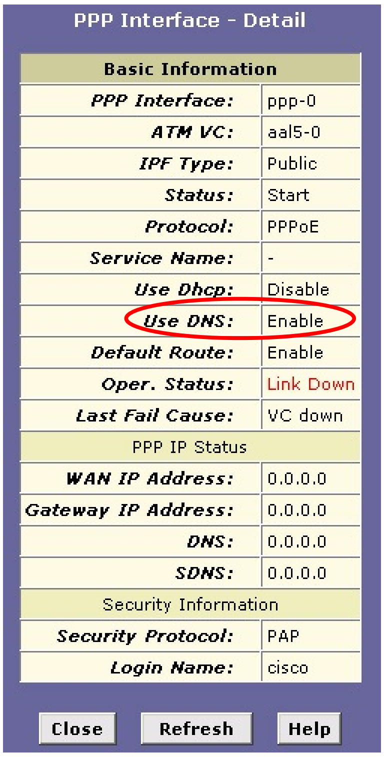
PPP Configuration

This page is used to Configure and View PPP interfaces.

Inactivity TimeOut(mins): 0

Ignore WAN to LAN traffic: □

Interface	VC	IPF Type	Protocol	WAN IP	Gateway IP	Default Route	Use Dhcp	Use DNS	Oper. Status	Action
ppp-0	aal5-0	Public	PPPoA	10.100.19.1	10.1.24.254	Enable	Disable	Enable	Link Up	✎ 🗑 🔍



PPP Interface - Detail

Basic Information	
PPP Interface:	ppp-0
ATM VC:	aal5-0
IPF Type:	Public
Status:	Start
Protocol:	PPPoE
Service Name:	-
Use Dhcp:	Disable
Use DNS:	Enable
Default Route:	Enable
Oper. Status:	Link Down
Last Fail Cause:	VC down
PPP IP Status	
WAN IP Address:	0.0.0.0
Gateway IP Address:	0.0.0.0
DNS:	0.0.0.0
SDNS:	0.0.0.0
Security Information	
Security Protocol:	PAP
Login Name:	cisco

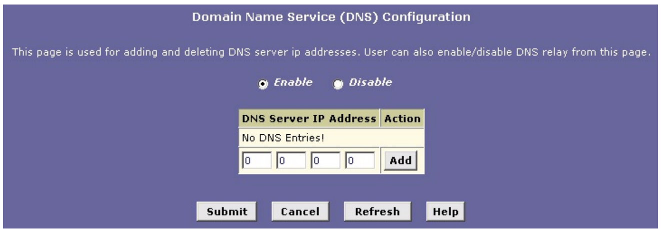
Option 2: Configuring DNS on the ADSL/Ethernet router

You can configure the DNS server address to be relayed on the router if one of the following circumstances applies:

- Not using PPP connection to the ISP (or a protocol other than PPP is used, such as EoA).
- You use PPP connection and **Use DNS** is already **enabled**. Then these configured addresses will be used in addition to those DNS addresses learned through PPP.
- You use PPP connection and **Use DNS** is **disabled**. Then these configured addresses will be used.

Follow these steps to configure DNS relay on the router:

(a) Go to **Service** > **DNS** to display the DNS Configuration page.



Domain Name Service (DNS) Configuration

This page is used for adding and deleting DNS server ip addresses. User can also enable/disable DNS relay from this page.

● *Enable* ○ *Disable*

DNS Server IP Address	Action
No DNS Entries!	
0 0 0 0	Add

(b) Type the IP address of the DNS server in an empty row and click **Add**. Click the **Enable** radio button, and then click **Submit**.

(c) Select **Admin** > **Commit & Reboot** and click **Commit** to save your changes to permanent storage.

11 RIP Configuration

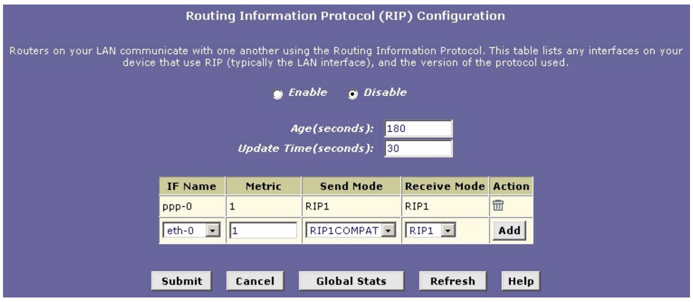
Your ADSL Bridge/Router can be configured to communicate with other routing devices to determine the best path for sending data to its intended destination. This chapter describes how to configure your ADSL Bridge/Router to use one of these, called the Routing Information Protocol (RIP).

Most small home or office networks do not need to use RIP. You may want to configure RIP if any of the following circumstances apply to your network:

- Your network includes an additional router or RIP-enabled PC. The ADSL Bridge/Router and the router will need to communicate via RIP to share their routing tables.
- Your network connects via the ADSL line to a remote network, such as a corporate network. In order for your LAN to learn the routes used within your corporate network, they should *both* be configured with RIP.
- Your ISP requests that you run RIP for communication with devices on their network.

Configuring the RIP

1. Select to **Services** > **RIP**. The RIP Configuration page displays:



Routing Information Protocol (RIP) Configuration

Routers on your LAN communicate with one another using the Routing Information Protocol. This table lists any interfaces on your device that use RIP (typically the LAN interface), and the version of the protocol used.

○ *Enable* ● *Disable*

Age(seconds): 180

Update Time(seconds): 30

IF Name	Metric	Send Mode	Receive Mode	Action
ppp-0	1	RIP1	RIP1	🗑
eth-0	1	RIP1COMPAT	RIP1	Add

2. If necessary, change the **Age** and **Update** Time.

   These are global settings for all interfaces that use RIP.

- *Age* is the amount of time in seconds that the device’s RIP table will retain each route that it learns from adjacent computers.
- *Update Time* specifies how frequently the ADSL Bridge/Router will send out its routing table its neighbors.

3. In the **IFName** column, select the interface on which you want to enable RIP.

   For communication with RIP-enabled devices on your LAN, select eth-0 or the name of the appropriate virtual Ethernet interface.

For communication with your ISP or a remote LAN, select the corresponding ppp, eoa, or other WAN interface.

4. Select a metric value (hop count) for the interface. You can select any integer from 1 to 15.

5. Select a **Send** and **Receive Modes**.

   The Send Mode setting indicates the RIP version this interface will use when it sends its route information to other devices.

   The Receive Mode setting indicates the RIP version(s) in which information must be passed to the ADSL Bridge/Router in order for it to be accepted into its routing table.

   RIP version 1 is the original RIP protocol. Select RIP1 if you have devices that communicate with this interface that understand RIP version 1 only.

   RIP version 2 is the preferred selection because it supports "classless" IP addresses (which are used to create subnets) and other features. Select RIP2 if all other routing devices on the autonomous network support this version of the protocol.

6. Click **Add**.

   The new RIP entry will display in the table.

7. Click the **Enable** radio button to enable the RIP feature.

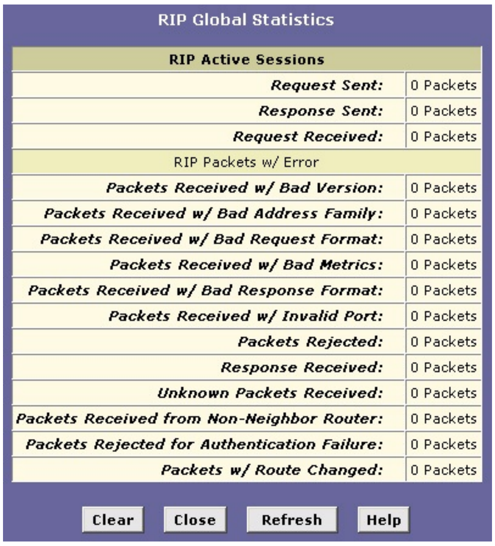
8. When you are finished defining RIP interfaces, click **Submit**.

   A page displays to confirm your changes.

9. Select **Admin** > **Commit & Reboot** and click **Commit** to save your changes to permanent storage.

Viewing RIP Statistics

To view the RIP statistics, select **Services** > **RIP** > **Global Stats**:



RIP Global Statistics

RIP Active Sessions	
Request Sent:	0 Packets
Response Sent:	0 Packets
Request Received:	0 Packets
RIP Packets w/ Error	
Packets Received w/ Bad Version:	0 Packets
Packets Received w/ Bad Address Family:	0 Packets
Packets Received w/ Bad Request Format:	0 Packets
Packets Received w/ Bad Metrics:	0 Packets
Packets Received w/ Bad Response Format:	0 Packets
Packets Received w/ Invalid Port:	0 Packets
Packets Rejected:	0 Packets
Response Received:	0 Packets
Unknown Packets Received:	0 Packets
Packets Received from Non-Neighbor Router:	0 Packets
Packets Rejected for Authentication Failure:	0 Packets
Packets w/ Route Changed:	0 Packets

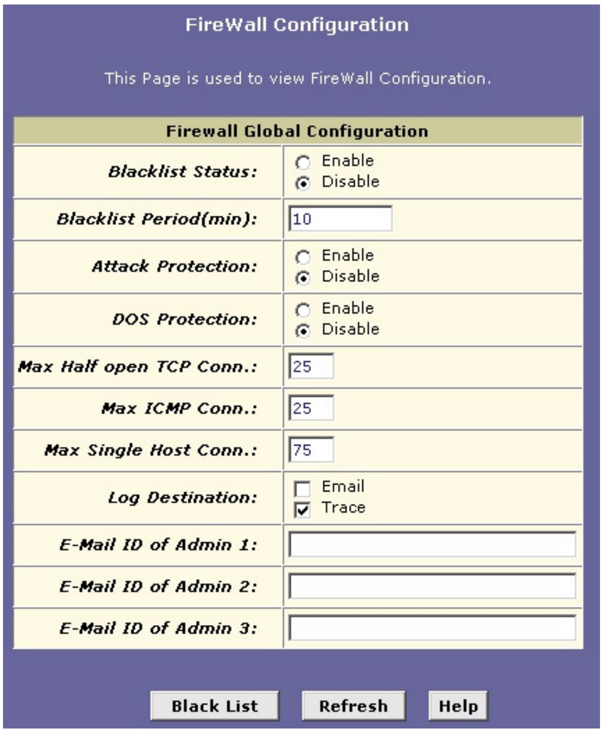
12 Filewall, IP Filters and Blocked Protocols

Configuring Firewall

Configuration Manager provides built-in firewall functions, enabling you to protect the system against denial of service (DoS) attacks and other types of malicious accesses to your LAN. You can also specify how to monitor attempted attacks, and who should be automatically notified.

Configuring Global Firewall Settings

1. Select **Services** > **Firewall**. The Firewall Configuration page displays.



FireWall Configuration

This Page is used to view FireWall Configuration.

Firewall Global Configuration

Blacklist Status:	○ Enable ● Disable
Blacklist Period(min):	10
Attack Protection:	○ Enable ● Disable
DOS Protection:	○ Enable ● Disable
Max Half open TCP Conn.:	25
Max ICMP Conn.:	25
Max Single Host Conn.:	75
Log Destination:	□ Email ☑ Trace
E-Mail ID of Admin 1:	
E-Mail ID of Admin 2:	
E-Mail ID of Admin 3:	

2. Configure any of the following settings:

Field	Description
Black List Status	If you want the device to maintain and use a black list, click *Enable*. Click *Disable* if you do not want to maintain a list.
Black List Period(min)	Specifies the number of minutes that a computer's IP address will remain on the black list.

Field	Description
Attack Protection	Select ***Enable*** to use the built-in firewall protections that prevent the following common types of attacks: o IP Spoofing: Sending packets over the WAN interface using an internal LAN IP address as the source address. o Tear Drop: Sending packets that contain overlapping fragments. o Smurf and Fraggle: Sending packets that use the WAN or LAN IP broadcast address as the source address. o Land Attack: Sending packets that use the same address as the source and destination address. o Ping of Death: Illegal IP packet length.
DoS Protection	Click the Enable radio button to use the following denial of service protections: o SYN DoS o ICMP DoS o Per-host DoS protection
Max Half open TCP Connection	Sets the percentage of concurrent IP sessions that can be in the half-open state. In ordinary TCP communication, packets are in the half-open state only briefly as a connection is being initiated; the state changes to active when packets are being exchanged, or closed when the exchange is complete. TCP connections in the half-open state can use up the available IP sessions. If the percentage is exceeded, then the half-open sessions will be closed and replaced with new sessions as they are initiated.
Max ICMP Connection	Sets the percentage of concurrent IP sessions that can be used for ICMP messages. If the percentage is exceeded, then older ICMP IP sessions will be replaced by new sessions as the are initiated.
Max Single Host Connection	Sets the percentage of concurrent IP session that can originate from a single computer. This percentage should take into account the number of hosts on the LAN.

Field	Description
Log Destination	Specifies how attempted violations of the firewall settings will be tracked. Records of such events can be sent via Ethernet to be handled by a system utility Ethernet to (*Trace*) or can e-mailed to specified administrators.
E-mail ID of Admin 1/2/3	Specifies the e-mail addresses of the administrators who should receive notices of any attempted firewall violations. Type the addresses in standard internet e-mail address format, e.g., *jxsmith@onecompany.com*. The e-mail message will contain the time of the violation, the source address of the computer responsible for the violation, the destination IP address, the protocol being used, the source and destination ports, and the number violations occurring the previous 30 minutes. If the ICMP protocol were being used, then instead of the source and destination ports, the e-mail will report the ICMP code and type.

3. Click **Submit**.

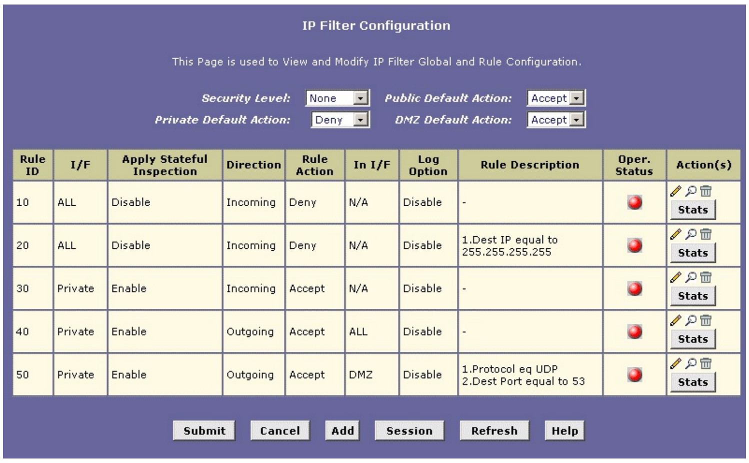
4. Select **Admin** > **Commit & Reboot** and click **Commit** to save your changes to permanent storage.

IP Filter Configuration

The IP filter feature enables you to create rules that control the forwarding of incoming and outgoing data between your LAN and the Internet. This chapter explains how to create IP filter rules.

Viewing Your IP Filter Configuration

Select **Services** > **IP Filter**. The IP Filter page displays:



IP Filter Configuration

This Page is used to View and Modify IP Filter Global and Rule Configuration.

Security Level: None
Public Default Action: Accept
Private Default Action: Deny
DMZ Default Action: Accept

Rule ID	I/F	Apply Stateful Inspection	Direction	Rule Action	In I/F	Log Option	Rule Description	Oper. Status	Action(s)
10	ALL	Disable	Incoming	Deny	N/A	Disable	-	●	Stats
20	ALL	Disable	Incoming	Deny	N/A	Disable	1.Dest IP equal to 255.255.255.255	●	Stats
30	Private	Enable	Incoming	Accept	N/A	Disable	-	●	Stats
40	Private	Enable	Outgoing	Accept	ALL	Disable	-	●	Stats
50	Private	Enable	Outgoing	Accept	DMZ	Disable	1.Protocol eq UDP 2.Dest Port equal to 53	●	Stats

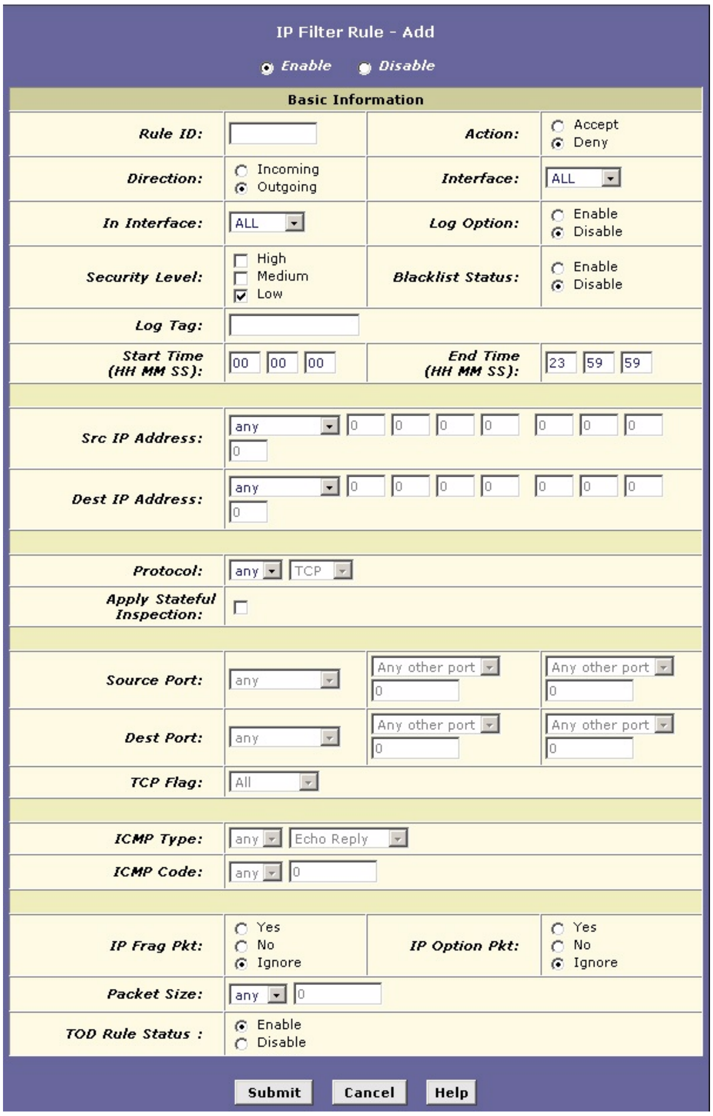
Configuring IP Filter Global Settings

The IP Filter Configuration page enables you to configure several global IP Filter settings, and displays a table showing all existing IP Filter rules. The global settings that you can configure are:

- **Security Level:** When *High* is selected, only those rules that are assigned a security value of *High* will be in effect. The same is true for the *Medium* and *Low* settings. When *None* is selected, IP Filtering is disabled.
- **Private/Public/DMZ Default Action:** This setting specifies a default action to be taken (**Accept** or **Deny**) on private, public, or DMZ-type device interfaces when they receive packets that ***do not*** match any of the filtering rules.
    - Public – The interface connects to the Internet. e.g., PPP, EoA, and IPoA interfaces. Typically, the global setting for public interfaces is *Deny*, so that all accesses to your LAN initiated from external computers are denied (discarded at the public interface), except for those allowed by a specific IP Filter rule.
    - Private – Typically, the global setting for private interfaces is **Accept**, so that LAN computers have access to the ADSL/Ethernet routers' Internet connection.
    - DMZ – Refers to computers that are available for both public and in-network accesses (such as a company's public Web server). Packets received on a DMZ interface—a whether from a LAN or external source—are subject to a set of protections that is in between public and private interfaces. The global setting for DMZ-type interfaces may be set to ***Deny*** so that all attempts to access these servers are denied by default; the administrator may then configure IP Filter rules to allow accesses of certain types.

Creating IP Filter Rules

1. On the main IP Filter page, click **Add**. The IP Filter Rule – Add page displays:



IP Filter Rule - Add

● Enable ○ Disable

Basic Information

Rule ID:		Action:	○ Accept ● Deny
Direction:	○ Incoming ● Outgoing	Interface:	ALL
In Interface:	ALL	Log Option:	○ Enable ● Disable
Security Level:	□ High □ Medium ☑ Low	Blacklist Status:	○ Enable ● Disable
Log Tag:			
Start Time (HH MM SS):	00 00 00	End Time (HH MM SS):	23 59 59
Src IP Address:	any 0 0 0 0 0 0 0 0		
Dest IP Address:	any 0 0 0 0 0 0 0 0		
Protocol:	any TCP		
Apply Stateful Inspection:	□		
Source Port:	any	Any other port 0	Any other port 0
Dest Port:	any	Any other port 0	Any other port 0
TCP Flag:	All		
ICMP Type:	any Echo Reply		
ICMP Code:	any 0		
IP Frag Pkt:	○ Yes ○ No ● Ignore	IP Option Pkt:	○ Yes ○ No ● Ignore
Packet Size:	any 0		
TOD Rule Status :	● Enable ○ Disable		

2. Enter or select data for each field that applies to your rule:

Field	Description
Rule ID	Rules are processed from lowest to highest on each data packet, until a match is found. It is recommended that you assign rule IDs in multiples of 5 or 10 (e.g., *10*, *20*, *30*) so that you leave enough room between them for inserting a new rule if necessary.
Action	The action can be *Accept* (forward to destination) or *Deny* (discard the packet).
Direction	*Incoming* refers to packets coming from the LAN, and *outgoing* refers to packets going to the Internet.
Interface	The interface on which the rule will take effect.

Field	Description
In Interface	The interface from which packets must have been forwarded to the interface specified in the previous selection. This option is valid only for the outgoing direction.
Log Option	When ***Enabled*** is selected, a log entry will be created on the system each time this rule is invoked.
Security Level	The security level that must be enabled globally for this rule to take affect. A rule will be active only if its security level is the same as the globally configured setting (shown on the main IP Filter page). For example, if the rule is set to Medium and the global firewall level is set to Medium, then the rule will be active; but if the global firewall level is set to High or Low, then the rule will be inactive.
Black List Status	Specifies whether or not a violation of this rule will result in the offending computer's IP address being added to the Black List, which blocks the router from forwarding packets from that source for a specified period of time.
Log Tag	A description of up to 16 characters to be recorded in the log in the event that a packet violates this rule. Be sure to set the Log Option to *Enable* if you configure a Log Tag.
Start/End Time	The time range during which this rule is to be in effect, specified in military units.
Src IP Address	IP address criteria for the source computer(s) from which the packet originates. Use the following expression to specify IP: **any**: any source IP address. **lt**: *less than* **lteq**: *less than or equal to*. **gt**: *greater than* **eq**: *equal to* **neq**: *not equal to* **range**: within the specified range, inclusive. **out of range**: outside the specified range. **self**: the IP address of the router interface on which this rule takes effect.

Field	Description
Dest IP Address	IP address rule criteria for the destination computer(s) (i.e., the IP address of the computer to which the packet is being sent). In addition to the options described for the Src IP Address field, the following option is available: **bcast**: Specifies that the rule will be invoked for any packets sent to the broadcast address for the receiving interface. (The broadcast address is used to send packets to all hosts on the LAN or subnet connected to the specified interface.) When you select this option, you do not need to specify the address, so the address fields are dimmed.
Protocol	The basic IP protocol criteria that must be met for rule to be invoked. Using the options in the drop-down list, you can specify that packets must contain the selected protocol (*eq*), that they must not contain the specified protocol (*neq*), or that the rule can be invoked regardless of the protocol (*any*). TCP, UDP, and ICMP are commonly IP protocols; others can be identified by number from 0-255, as defined by IANA.
Store State	If this option is enabled, then *stateful filtering* is performed and the rule is also applied in the other direction on the given interface during an IP session.
Source Port	Port number criteria for the computer(s) from which the packet originates. This field will be dimmed (unavailable for entry) if you have not specified a protocol criteria. See the description of Src IP Address for the selection options.
Dest Port	Port number criteria for the destination computer(s) (i.e., the port number of the type of computer to which the packet is being sent). This field will be dimmed (unavailable for entry) unless you have selected TCP or UDP as the protocol. See the description of Src IP Address for the selection options.

Field	Description
TCP Flag	Specifies whether the rule should apply only to TCP packets that contain the synchronous (*SYN*) flag, only to those that contain the non-synchronous (*NOT-SYN*) flag, or to all TCP packets. This field will be dimmed (unavailable for entry) unless you selected TCP as the protocol.
ICMP Type	Specifies whether the value in the type field in ICMP packet headers will be used as a criteria. The code value can be any decimal value from 0-255. You can specify that the value must equal (*eq*) or not equal (*neq*) the specified value, or you can select *any* to enable the rule to be invoked on all ICMP packets. This field will be dimmed (unavailable for entry) unless you specify ICMP as the protocol.
ICMP Code	Specifies whether the value in the code field in ICMP packet headers will be used as a criteria. The code value can be any decimal value from 0-255. You can specify that the value must equal (*eq*) or not equal (*neq*) the specified value, or you can select *any* to enable the rule to be invoked on all ICMP packets. This field will be dimmed (unavailable for entry) unless you specify ICMP as the protocol.
IP Frag Pkt	Determines how the rule applies to IP packets that contain fragments. You can choose from the following options: ○ **Yes**: The rule will be applied only to packets that contain fragments. ○ **No**: The rule will be applied only to packets that do not contain fragments. ○ **Ignore**: (Default) The rule will be applied to packets whether or not they contain fragments, assuming that they match the other criteria.

Field	Description
IP Option Pkt	Determines whether the rule should apply to IP packets that have options specified in their packet headers. o **Yes:** The rule will be applied only to packets that contain header options. o **No:** The rule will be applied only to packets that do not contain header options. o **Ignore:** (Default) The rule will be applied to packets whether or not they contain header options, assuming that they match the other criteria.
Packet Size	Specifies that the IP Filter rule will take affect only on packets whose size in bytes matches this criteria. (*lt* = less than, *gt* = greater than, *lteq* = less than or equal to, etc.)
TOD Rule Status	The Time of Day Rule Status determines how the Start Time/End Time settings are used. o **Enable:** (Default) The rule is in effect for the specified time period. o **Disable:** The rule is not in effect for the specified time period, but is effective at all other times.

3. When you are done selecting criteria, ensure that the **Enable** is selected and then click **Submit**.

   If the security level of the rule matches the globally configured setting, a green ball in the Status column for that rule, indicating that the rule is now in effect. A red ball will display when the rule is disabled or if its security level is different than the globally configured level.

4. Ensure that the Security Level and Private/Public/DMZ Default Action settings on the IP Filter Configuration page are configured as needed, then click **Submit**.

   A page displays to confirm your changes.

5. Select **Admin** > **Commit & Reboot** and click **Commit** to save your changes to permanent storage.

IP filter rule examples

Example 1. Blocking a specific computer on your LAN from using accessing web servers on the Internet:

1. Add a new rule for outgoing packets on the ppp-0 interface from any incoming interface (this would include the eth-0 and usb-0 interfaces, for example).

2. Specify a source IP address of the computer you want to block.

3. Specify the Protocol = *TCP* and enable the Store State setting.

4. Specify a destination port = *80*, which is the well-known port number for web servers.

5. Enable the rule by clicking the radio button at the top of the page.

6. Click **Submit** to create the rule.

7. On the IP Filter Configuration page, set the Security Level to the same level you chose for the rule, and set both the Private Default Action and the Public Default Action to *Accept*.

8. Click **Submit** and commit your changes.

Example 2. Blocking Telnet accesses to the device:

1. Add a new rule for packets incoming on the ppp-0 interface.

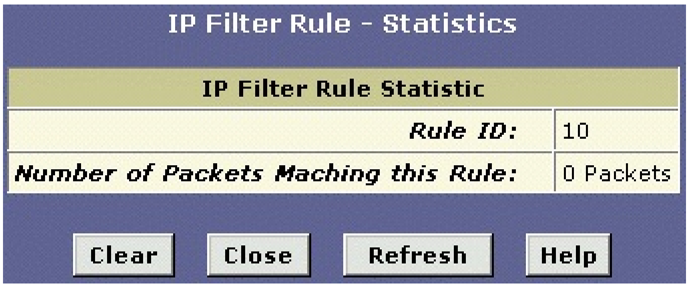
2. Specify that the packet must contain the TCP protocol, and must be destined for port 23, the well-known port number used for the Telnet protocol.

3. Enable the rule by clicking the radio button at the top of the page.

4. Click **Submit**. to create the rule, and commit your changes.

Viewing IP Filter Statistics

To view statistics on how many packets were accepted or denied for a rule, select **Services** > **IP Filter** > **Stats** in the row corresponding to the rule:

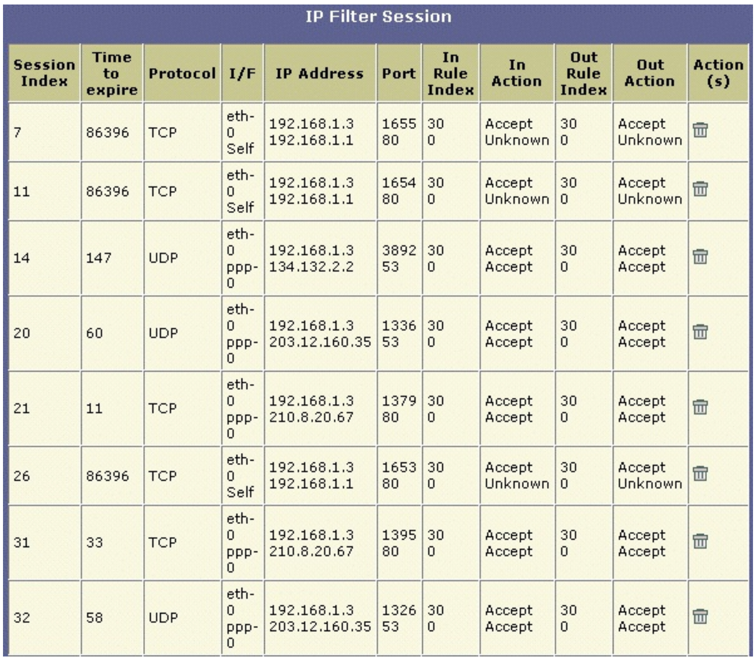


IP Filter Rule - Statistics

IP Filter Rule Statistic	
Rule ID:	10
Number of Packets Maching this Rule:	0 Packets

Managing Current IP Filter Sessions

To view all current IP sessions, select **Services** > **IP Filter** > **Session** to display the IP Filters Session page:



IP Filter Session

Session Index	Time to expire	Protocol	I/F	IP Address	Port	In Rule Index	In Action	Out Rule Index	Out Action	Action (s)
7	86396	TCP	eth-0 Self	192.168.1.3 192.168.1.1	1655 80	30 0	Accept Unknown	30 0	Accept Unknown	🗑
11	86396	TCP	eth-0 Self	192.168.1.3 192.168.1.1	1654 80	30 0	Accept Unknown	30 0	Accept Unknown	🗑
14	147	UDP	eth-0 ppp-0	192.168.1.3 134.132.2.2	3892 53	30 0	Accept Accept	30 0	Accept Accept	🗑
20	60	UDP	eth-0 ppp-0	192.168.1.3 203.12.160.35	1336 53	30 0	Accept Accept	30 0	Accept Accept	🗑
21	11	TCP	eth-0 ppp-0	192.168.1.3 210.8.20.67	1379 80	30 0	Accept Accept	30 0	Accept Accept	🗑
26	86396	TCP	eth-0 Self	192.168.1.3 192.168.1.1	1653 80	30 0	Accept Unknown	30 0	Accept Unknown	🗑
31	33	TCP	eth-0 ppp-0	192.168.1.3 210.8.20.67	1395 80	30 0	Accept Accept	30 0	Accept Accept	🗑
32	58	UDP	eth-0 ppp-0	192.168.1.3 203.12.160.35	1326 53	30 0	Accept Accept	30 0	Accept Accept	🗑

The IP Filter Session table displays the following fields:

Field	Description
Session Index	The ID assigned by the system to the IP session (all sessions, whether or not they are affected by an IP filter rule, are assigned a session index).
Time to expire	The number of seconds in which the connection will automatically expire
Protocol	The underlying IP protocol used on the connection, such as TCP, UDP, IGMP, etc.)
I/F	The interface on which the IP Filter rule is effective
IP Address	The IP addresses involved in the communication. The first one shown is the initiator of the communication.
Port	The hardware addresses of the ports involved in the communication
In/Out Rule Index	The number of the IP Filter rule that is applies to this session (assigned when the rule was created)
In/Out Action	The action (accept, deny, or unknown), being taken on data coming into or going out on the interface. This action is specified in the rule definition.

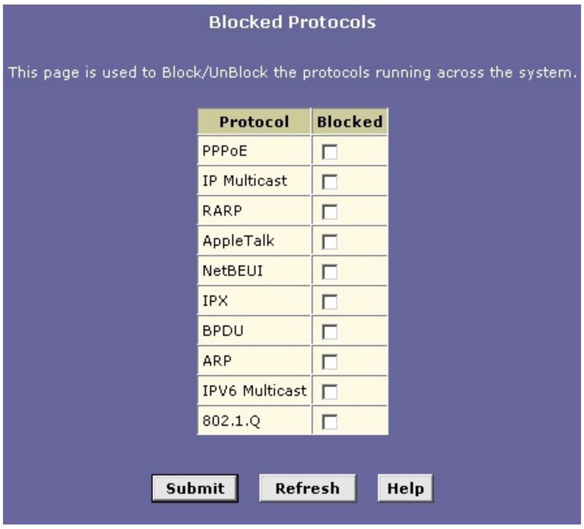
To Block Specific Protocols

The Blocked Protocols feature prevents the ADSL/Ethernet router from passing any data that uses a particular protocol. Unlike the IP Filter feature, you cannot specify additional criteria for blocked protocols, such as particular users or destinations.

Blocking certain protocols may disrupt or disable your network communication or Internet access. Use this feature unless you are certain that a particular protocol is not needed or wanted on your network.

To block specific protocols running across the system, select **Services** > **Blocked Protocols**. Check the protocol type you want to block and click **Submit**. Make sure to use commit feature to save your changes to the permanent memory.

To unblock the specific protocol, uncheck the protocol and repeat the submit and commit task.



Blocked Protocols

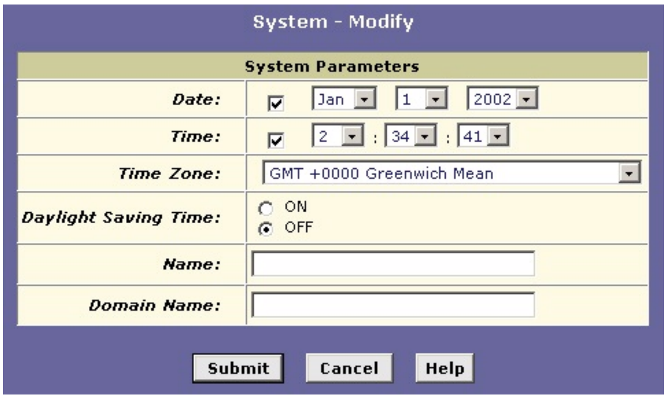
This page is used to Block/UnBlock the protocols running across the system.

Protocol	Blocked
PPPoE	□
IP Multicast	□
RARP	□
AppleTalk	□
NetBEUI	□
IPX	□
BPDU	□
ARP	□
IPV6 Multicast	□
802.1.Q	□

13 Administration Tasks

Changing the System Date and Time

The device keeps a record of the current date and time, which it uses to calculate and report various performance data. You can select **Home** > **Modify** to change the date and time as required. You may also specify the host name and the domain name in the fields provided.



System - Modify

System Parameters

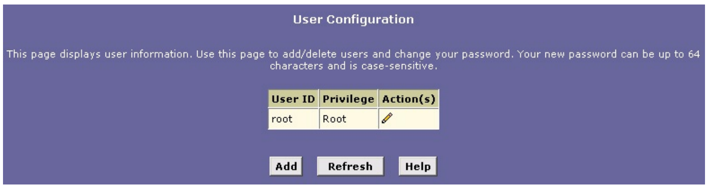
Date:	☑ Jan 1 2002
Time:	☑ 2 : 34 : 41
Time Zone:	GMT +0000 Greenwich Mean
Daylight Saving Time:	○ ON ● OFF
Name:	
Domain Name:	

Adding Login User ID/Changing Login Password

The first time you log into the Configuration Manager, you use the default user ID and password (*root* and *root*). The system allows two levels of privilege: Root and User. Root privilege allows you to change and commit the device’s settings while user privilege is provided with read-only access right.

To add login User ID or change login password:

1. Select **Admin** > **User Config**. The User Configuration page displays.

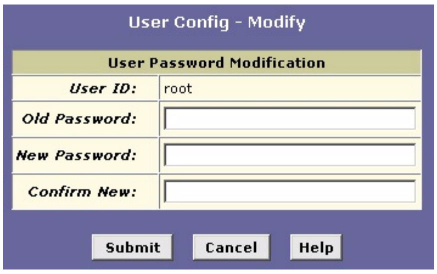


User Configuration

This page displays user information. Use this page to add/delete users and change your password. Your new password can be up to 64 characters and is case-sensitive.

User ID	Privilege	Action(s)
root	Root	✎

To modify the login password, click the modify icon in the Action(s) column and then change the current password.



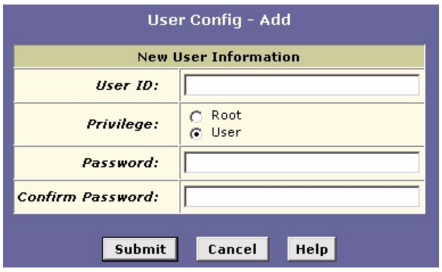
User Config - Modify

User Password Modification

User ID:	root
Old Password:	
New Password:	
Confirm New:	

To add a new login ID, click **Add** to display **User Config-Add** page. Then enter your settings in fields provided.

Note that both the user ID and password are case sensitive.



User Config - Add

New User Information

User ID:

Privilege: ○ Root ● User

Password:

Confirm Password:

2. After making changes, click **Submit**.

3. Select **Admin** > **Commit & Reboot** and click **Commit** to save your changes to permanent storage.

Image Upgrade

This option allows you to upgrade the device to new firmware. After upgrading, your customized configuration will still exist and not reset to the factory defaults. To perform upgrade task, download required firmware file to your host PC and follow the steps below:

1. Click **Browse** to locate the firmware file.

   The name of the upgrade file must be one of the following:

   TEImage.bin
   TEDsl.gsz
   TEAppl.gsz
   Filesys.bin
   TEPatch.bin

2. Click **Upload** to start upgrade. After a few seconds, a message like the following should display (the file name may differ):

   File: TEDsl.gsz successfully saved to the flash. Please reboot for the new image to take effect.

3. Power off the unit, wait a few seconds, and turn it on again to activate the new software.

Note

Do not interrupt the upgrade process otherwise it might cause damage to your router.

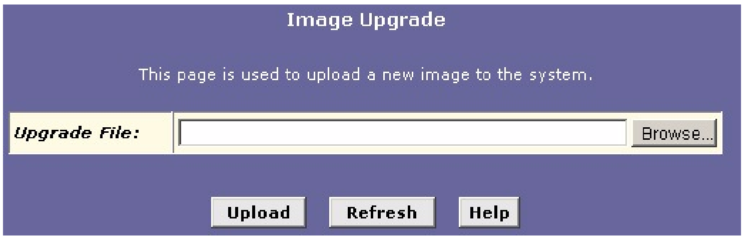


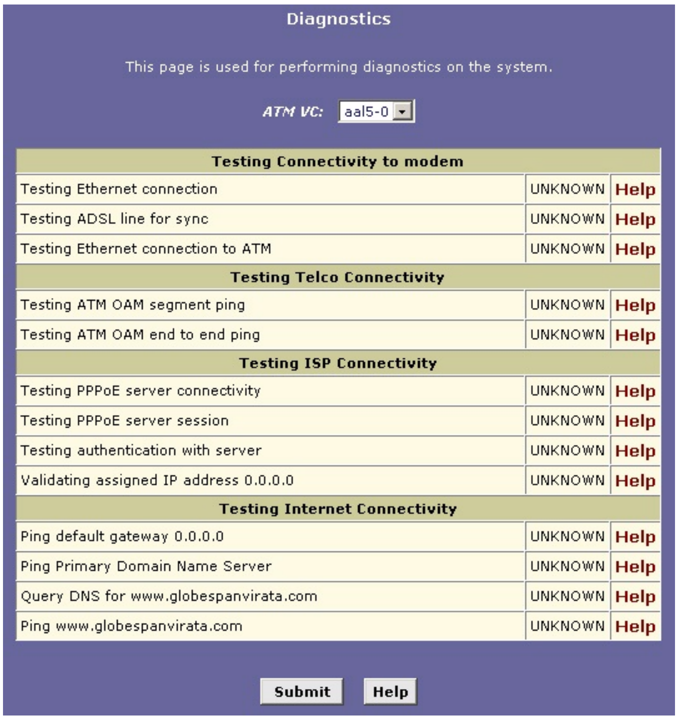
Image Upgrade

This page is used to upload a new image to the system.

Upgrade File:

Diagnostics

To perform diagnostics on specific ATM VC, select **Admin** > **Diagnostics**. Select the VC on which you want to execute diagnostics and then click **Submit**. The diagnostic result will displayed on this page. Note that only the VCs defined in the system will appear on the drop-down list.



Diagnostics

This page is used for performing diagnostics on the system.

ATM VC: aal5-0

Testing Connectivity to modem		
Testing Ethernet connection	UNKNOWN	Help
Testing ADSL line for sync	UNKNOWN	Help
Testing Ethernet connection to ATM	UNKNOWN	Help
Testing Telco Connectivity		
Testing ATM OAM segment ping	UNKNOWN	Help
Testing ATM OAM end to end ping	UNKNOWN	Help
Testing ISP Connectivity		
Testing PPPoE server connectivity	UNKNOWN	Help
Testing PPPoE server session	UNKNOWN	Help
Testing authentication with server	UNKNOWN	Help
Validating assigned IP address 0.0.0.0	UNKNOWN	Help
Testing Internet Connectivity		
Ping default gateway 0.0.0.0	UNKNOWN	Help
Ping Primary Domain Name Server	UNKNOWN	Help
Query DNS for www.globespanvirata.com	UNKNOWN	Help
Ping www.globespanvirata.com	UNKNOWN	Help

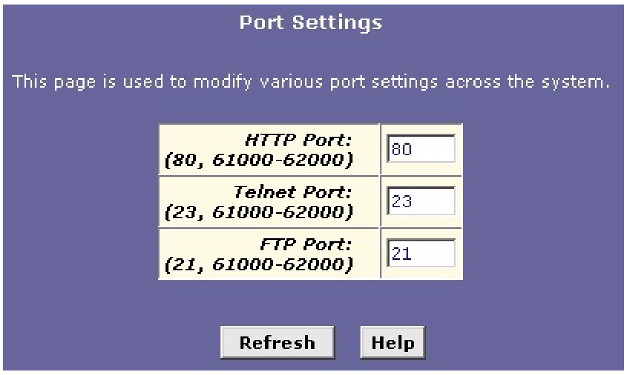
Port Settings

The router's HTTP/Telnet/FTP service are accessible using the standard port number 80, 23 and 21 respectively. It is possible that you want to designate a publicly accessible HTTP, Telnet or FTP server on your LAN side and you want to shift the router's HTTP/Telnet/FTP service to use non-standard port number. If this is the case, select **Admin** > **Port Settings** to modify the port settings and click **Submit**. Then select **Admin** > **Commit & Reboot** and click **Commit** to save your changes to permanent storage.

Note that if you set the router's embedded HTTP/Telnet/FTP server to use non-standard port number, when accessing the embedded HTTP/Telnet/FTP server from the external world, the IP address should be followed by a colon and the non-standard port number, as shown in this following example for a HTTP server (i.e., the Web-based Configuration Manager):

http://10.0.1.16:61000

where **10.0.1.16** is the router's WAN IP address and **61000** is the non-standard port number you specified in Port Settings page.



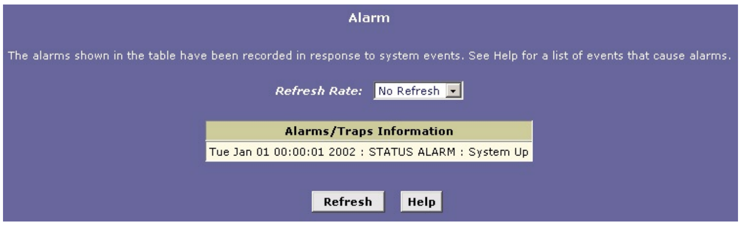
Port Settings

This page is used to modify various port settings across the system.

HTTP Port: *(80, 61000-62000)*	80
Telnet Port: *(23, 61000-62000)*	23
FTP Port: *(21, 61000-62000)*	21

View System Alarms

To display the Alarm page, **Admin** > **Alarm**:



Alarm

The alarms shown in the table have been recorded in response to system events. See Help for a list of events that cause alarms.

Refresh Rate: No Refresh

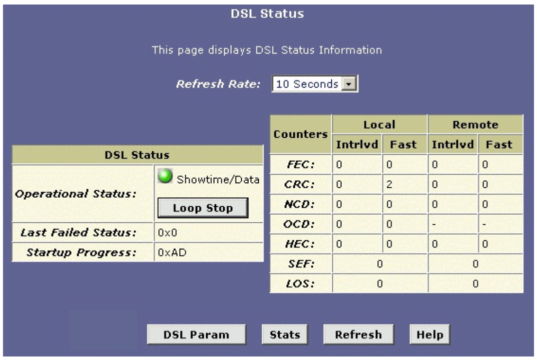
Alarms/Traps Information
Tue Jan 01 00:00:01 2002 : STATUS ALARM : System Up

Each row in the table displays the time and date that an alarm occurred, the type of alarm, and a brief statement indicating its cause.

You can click on the **Refresh Rate** drop-down list to select a recurring time interval after which the page will redisplay with new data.

14 View DSL Parameters

To view configuration parameters and performance statistics for the ADSL Bridge/Router’s DSL line, select **WAN** > **DSL**. The DSL Status page displays:



DSL Status

This page displays DSL Status Information

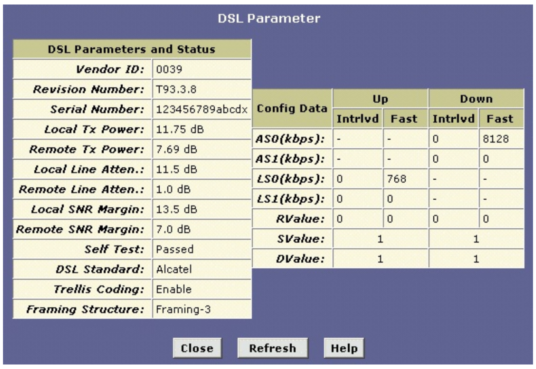
Refresh Rate: 10 Seconds

DSL Status	
Operational Status:	Showtime/Data Loop Stop
Last Failed Status:	0x0
Startup Progress:	0xAD

Counters	Local		Remote	
	Intrlvd	Fast	Intrlvd	Fast
FEC:	0	0	0	0
CRC:	0	2	0	0
NCD:	0	0	0	0
OCD:	0	0	-	-
HEC:	0	0	0	0
SEF:	0		0	
LOS:	0		0	

The DSL Status page displays current information on the DSL line performance. The page refreshes about every 10 seconds.

You can click **DSL Param** to display data about the configuration of the DSL line, as shown below.

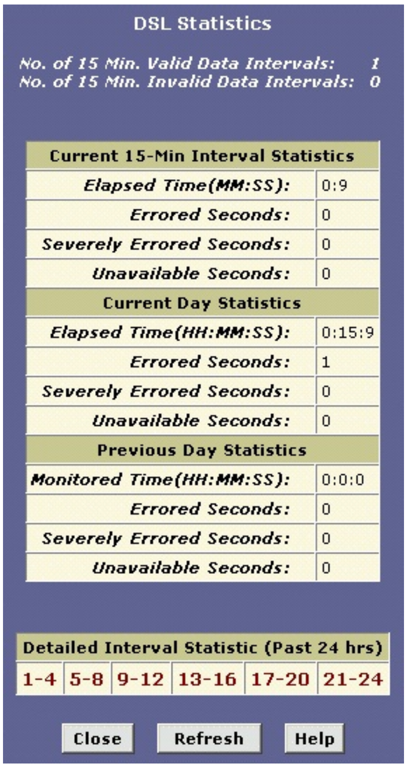


DSL Parameter

DSL Parameters and Status	
Vendor ID:	0039
Revision Number:	T93.3.8
Serial Number:	123456789abcdx
Local Tx Power:	11.75 dB
Remote Tx Power:	7.69 dB
Local Line Atten.:	11.5 dB
Remote Line Atten.:	1.0 dB
Local SNR Margin:	13.5 dB
Remote SNR Margin:	7.0 dB
Self Test:	Passed
DSL Standard:	Alcatel
Trellis Coding:	Enable
Framing Structure:	Framing-3

Config Data	Up		Down	
	Intrlvd	Fast	Intrlvd	Fast
AS0(kbps):	-	-	0	8128
AS1(kbps):	-	-	0	0
LS0(kbps):	0	768	-	-
LS1(kbps):	0	0	-	-
RValue:	0	0	0	0
SValue:	1		1	
DValue:	1		1	

From the DSL Status page, you can click **Stats** to display DSL line performance statistics:



DSL Statistics

No. of 15 Min. Valid Data Intervals: 1
No. of 15 Min. Invalid Data Intervals: 0

Current 15-Min Interval Statistics	
Elapsed Time(MM:SS):	0:9
Errored Seconds:	0
Severely Errored Seconds:	0
Unavailable Seconds:	0
Current Day Statistics	
Elapsed Time(HH:MM:SS):	0:15:9
Errored Seconds:	1
Severely Errored Seconds:	0
Unavailable Seconds:	0
Previous Day Statistics	
Monitored Time(HH:MM:SS):	0:0:0
Errored Seconds:	0
Severely Errored Seconds:	0
Unavailable Seconds:	0

Detailed Interval Statistic (Past 24 hrs)					
1-4	5-8	9-12	13-16	17-20	21-24

The DSL Statistics page reports error data relating to the last 15 minute interval, the current day, and the previous day.

At the bottom of the page, the **Detailed Interval Statistic** table displays links you can click on to display detailed data for each 15 minute interval in the past 24 hours. For example, when you click on 1-4, data displays for the 15-minute such intervals that make up the previous 4 hours (there are 16 of these) shows one such page.

15 Troubleshooting

This appendix suggests solutions for problems you may encounter in installing or using your ADSL Bridge/Router, and provides instructions for using several IP utilities to diagnose problems.

Contact Customer Support if these suggestions do not resolve the problem.

Problem	Troubleshooting Suggestion
LEDs	
Power LED does not illuminate after product is turned on.	Verify that you are using the power cable provided with the device and that it is securely connected to the ADSL Bridge/Router and a wall socket/power strip.
LINK WAN LED does not illuminate after phone cable is attached.	Verify that a standard telephone cable is securely connected to the ADSL port and your wall phone jack. Wait 30 seconds to allow the device to negotiate a connection with your ISP.
LINK LAN LED does not illuminate after Ethernet cable is attached.	Verify that the Ethernet cable is securely connected to your LAN hub or PC and to the ADSL Bridge/Router. Make sure the PC and/or hub is turned on. Verify that you are using correct cable. See “Connecting the Hardware” for more information.
DIAG LED stays illuminated after turning the device on.	The DIAG LED should turn off after about 10-15 seconds. If it does not, turn off the ADSL Bridge/Router, wait 10 seconds, and then turn it back on.
Internet Access	
PC cannot access Internet	Use the ping utility to check whether your PC can communicate with the ADSL Bridge/Router’s LAN IP address (by default 192.168.1.1). If it cannot, check the Ethernet cabling. If you statically assigned a private IP address to the computer, (not a registered public address), verify the following: Check that the gateway IP address on the computer is your public IP address. If it is not, correct the address or configure the PC to receive IP information automatically. Verify with your ISP that the DNS server specified for the PC is valid. Correct the address or configure the PC to receive this information automatically. Verify that a NAT rule has been defined on the ADSL Bridge/Router to translate the private address to your public IP address.
PCs cannot display web pages on the Internet.	Verify that the DNS server specified on the PCs is correct for your ISP. You can use the ping utility to test connectivity with your ISP’s DNS server.

Problem	Troubleshooting Suggestion
Configuration Manager Program	
You forgot/lost your Configuration Manager user ID or password.	You can reset the device to the default configuration by pressing the **Reset** button for 3 times on the back panel of the device (using a pointed object such as a paper clip). Then, type the default User ID and password root/root. **WARNING:** Resetting the device removes any custom settings and returns all settings to their default values.
Cannot access the Configuration Manager program from your browser.	Use the ping utility to check whether your PC can communicate with the ADSL Bridge/Router's LAN IP address (by default 192.168.1.1). If it cannot, check the Ethernet cabling. Verify that you are using Internet Explorer v5.0 or later, or Netscape Navigator v5.0 or later. Support for Javascript® must be enabled in your browser. Support for Java® may also be required. Verify that the PC's IP address is defined as being on the same subnet as the IP address assigned to the LAN port on the ADSL Bridge/Router.
Changes to Configuration Manager are not being retained.	Be sure to use the Commit function after any changes.