PIRELLI
BROADBAND SOLUTIONS

P.RG AV4202N

User Manual

Trademarks:
All terms used in this document that are known to be trademarks or service marks have been noted as such. Pirelli cannot attest to the accuracy of this information. Other product and corporate names used in this document that may be trademarks or service marks of other companies are used only for explanation and to the owner’s benefit, without intent to infringe. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark.
This publication is subject to change without notice. Pirelli reserves the right to make changes to equipment design and system components as well as system documentation and literature as progress in engineering, manufacturing methods, or other circumstances may warrant.
This publication is intended solely for informational and instructional purposes. Refer to the above as to its possible uses. It constitutes neither a contract with the user hereof nor a warranty or guarantee with regard to any of the Pirelli products described herein nor shall it be construed to grant a license or any other rights under any proprietary rights to information or material included herein. Pirelli hereby expressly disclaims any warranty or guarantee, whether express or implied, with regard to items described herein. Any contract, license, or warranty between Pirelli and the user hereof is created solely by separate legal documents.

Manual Code: OGU 930500275-A1

CONTENTS

Welcome 1

About this Guide 1
Naming Convention 1
Conventions 1

Introduction 3

Introduction 3
Package Contents 3
Router Advantages 6
Minimum System and Component Requirements 7
Front Panel 7
Rear Panel 9

Hardware Installation 11

Introduction 11
Positioning the Router 11
Installing Micro Filters 12
Powering up the router 13
Connecting the Router 13

Setting Up Your Computer 19

INSTALL Software 19
Ethernet Connection 20
Ethernet Connection >> TCP/IP Protocol Installation 20
Ethernet Connection >> MS Windows 98SE, ME, 2000 20
Ethernet Connection >> MS Windows XP 22
Ethernet Connection >> MAC OS 10.X 23
USB Connection 24
USB Connection >> MS Windows 25
USB Connection >> MAC OS 10.x 25
Wi-Fi connection 25

Router Configuration 27

Introduction 27

Installation Wizard Section 31

Log In Setup 32
Test Ethernet Link 33
Analyze internet connection Type 33
Setup internet Connection 33
Test service Provider Connection 33
Test Internet Connection 33
Wireless Setup 33
VoIP Setup 34
Installation Completed 34

Quick Setup Section 35

Point-to-point protocol over Ethernet (PPPoE) over ATM 36
Ethernet (PPPoE) over PTM 36
Point-to-point protocol over ATM (PPPoA) 37
Routed Ethernet Connection over ATM (ETHoA) 37
Routed Ethernet Connection over PTM (ETHoP) 37
Bridged Ethernet Connection over ATM (ETHoA) 38
Bridged Ethernet Connection over PTM (ETHoP) 38
No Internet Connection 38
Wireless 38
Administrator 38

Network Connections Section 39

LAN Bridge 40
LAN Bridge >> General 40
LAN Bridge >> Settings 41
LAN Bridge >> Routing 44
LAN Bridge >> Bridging 46
LAN Bridge >> Advanced 47
LAN Ethernet 47
LAN Ethernet >> General 47
LAN Ethernet >> Settings 48
LAN Ethernet >> Advanced 49
LAN Wireless 802.11n Access Point 50
LAN Wireless 802.11nn Access Point >> General 50
LAN Wireless 802.11n Access Point >> Settings 51
LAN Wireless 802.11n Access Point >> Wireless 52
LAN Wireless 802.11n Access Point >> Advanced 57
WAN DSL 57

WAN DSL >> General 58
WAN DSL >> Settings 58

Security Section 61

General 62
Access Control 64
Port Forwarding 65
DMZ Host 68
Port Triggering 69
Web Site Restrictions 69
NAT 70
Connections 71
Advanced Filtering 72
Security Log 73

Voice over IP Section 75

Line Settings 75
Speed Dial 76
Monitoring 77
Advanced 78

Parental Control Section 81

general overview 82
filtering policy 83
advanced options 85
statistics 86

QoS Section 87

General 87
Traffic Priority 89
Traffic Shaping 92
DSCP Settings 93
802.1p Settings 95
Class Statistics 96

Advanced Section 99

About PRG AV4202N 100
Backup and Restore 101
Certificates 103

Configuration File 104
DDNS 105
DNS Server 106
PRG AV4202N Firmware Upgrade 107
Date and Time 109
Diagnostics 110
Disk Management 112
ftp server 113
File Server 113
IP Address Distribution 114
ipsec 116
l2tp server 117
MAC Cloning 118
media sharing 119
Network Objects 120
pptp server 121
PPPoE Relay 122
Print Server 122
Protocols 123
RADIUS 124
Reboot 125
Remote Administration 125
Restore Defaults 128
Routing 128
SSH 130
ssl vpn 131
Scheduler Rules 133
Simple network management protocol 134
system log 136
System Settings 137
umts 140
Universal Plug and Play 140
Users 141
WINS Server 143
Wake Up on LAN 144
Web Server 144

System Monitoring Section 148

Network Connections 148
System Log 149
CPU 150

Troubleshooting 153

Basic Connection Checks 153
Browsing to the Router Configuration Screens 153
Connecting to the Internet 154
Forgotten Password and Reset to Factory Defaults 154
Wireless Networking 155
Frequently Asked Questions 156

Safety Information 157

IP Addressing 159

Technical Specifications 161

Glossary 167

Welcome

ABOUT THIS GUIDE

This guide describes how to install and configure the PRG AV4202N. This guide is intended for use by those responsible for installing and setting up network equipment; consequently, it assumes a basic working knowledge of LANs (Local Area Networks) and Internet Routers.

NAMING CONVENTION

Throughout this guide, the PRG AV4202N is referred to as the “Wireless Router”. Category 5 Ethernet Cables are referred to as Ethernet Cables throughout this guide.

CONVENTIONS

Table 1 and Table 2 list conventions that are used throughout this guide.

TABLE 1. **Notice Icons**

Icon	Notice Type	Description
i	Information note	Information that describes important features or instructions.

TABLE 1. Notice Icons

Icon	Notice Type	Description
⚠	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device.
⚡	Warning	Information that alerts you to potential personal injury.

TABLE 2. Text Conventions

Convention	Description
The words "enter" and "type"	When you see the word "enter" in this guide, you must type something, and then press Return or Enter. Do not press Return or Enter when an instruction simply says "type."
Keyboard key names	If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press Ctrl+Alt+Del
Words in italics	Italics are used to: • Emphasize a point. • Denote a new term at the place where it is defined in the text. • Identify menu names, menu commands, and software button names. Examples: "From the *Help* menu, select *Contents*. Click *OK*."

Introduction

INTRODUCTION

The **PRG AV4202N** is designed to provide a cost-effective means of sharing a single broadband Internet connection between several wired and wireless computers. The Router also provides protection in the form of an electronic “firewall” preventing anyone outside of your network from seeing your files or damaging your computers. The Router offers VoIP functionalities through 2 VoIP channels allowing you to use existing analog phones and a fallback to old telephony at loss of power, WAN, Internet or VoIP.

The **PRG AV4202N** is an VDSL2 router, targeted to residential environments and SOHO customers, that provides routed broadband services from a single and modular access point.

The **PRG AV4202N** is the ideal solution for:

1. Connecting multiple PCs and Video game consoles;
2. Sharing broadband internet connections with all home computers;
3. Sharing printers and peripherals;
4. Performing VoIP connections.

PACKAGE CONTENTS

Your new **PRG AV4202N** VDSL2 Router kit contains the related hardware and software. In it you will find:

1. One **PRG AV4202N** unit
2. One Switching Power Supply adapter
3. One micro filter[*]

[*] This item may be optional and not included in the package: please check with your Service Provider

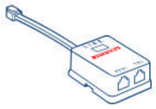
4. One USB cable
5. One phone cable RJ-11 plug (RJ-11)
6. One Ethernet CAT5 cable with RJ-45 plug
7. A CD-ROM containing:
    a. USB Driver
    b. User Manual
    c. Quick Installation Guide
    d. Smart Setup Configuration Utility[†]

TABLE 1. **Kit Material**

	Quantity	**DESCRIPTION**
	1	*PRG AV4202N*
	1	*Switching Power Supplier Adapter*
	1	*Ethernet Cable*
	1	*USB Cable*
	1	*Phone Cable*
	1	*CD-ROM*

[†] This item may be optional and not included in the package: please check with your Service Provider

TABLE 1. **Kit Material**

	Quantity	DESCRIPTION
	*1*	*Micro Filter*[‡]

If any of the items included in the package is damaged, please contact your Service Provider.

It implements an “always-on” very high bitrate Digital Subscriber Line (2/2+) connection to the telephone line on the WAN side, as well as several local connectivity technologies on the LAN side:

- Four switched 10/100 Base-TX Ethernet ports
- One Universal Serial Bus 1.1 (USB) connection to a host PC
- One USB 2.0 Host port for external USB peripherals
- One USB Device port [§]
- One IEEE 802.11b/g/n Wireless LAN access point
- Two FXS ports to analog phones
- One FXO port to wall phone socket [**]

Figure 2 shows a sample network, while in Figure 2 an existing SIP account case is shown: your Router becomes your connection to the Internet. Connections can be made directly to the Router expanding the number of computers you can have in your network.

[‡] This item may be optional and not included in the package: please check with your Service Provider

[§] This port may be optional depending on the product version.

[**] This port may be optional depending on the product version.

FIGURE 1. **Sample Home Network**

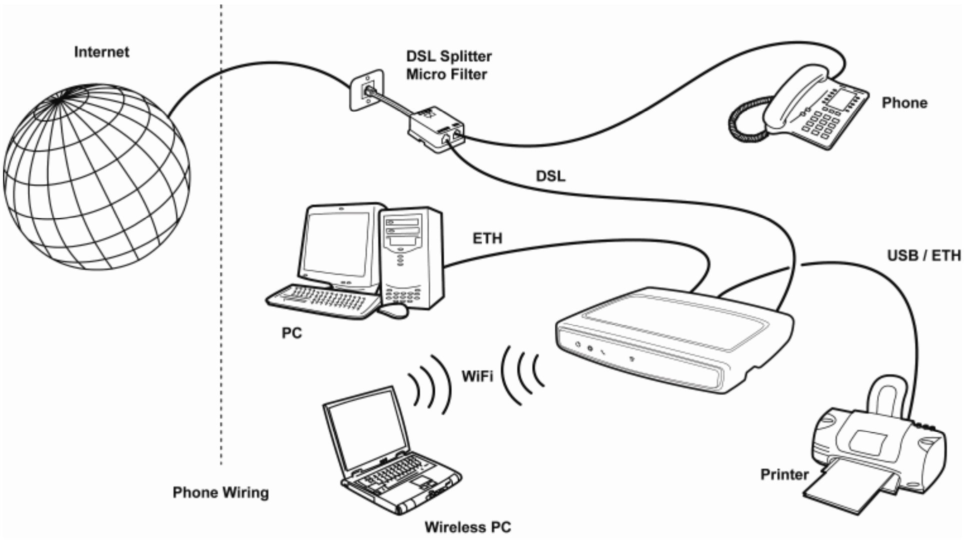
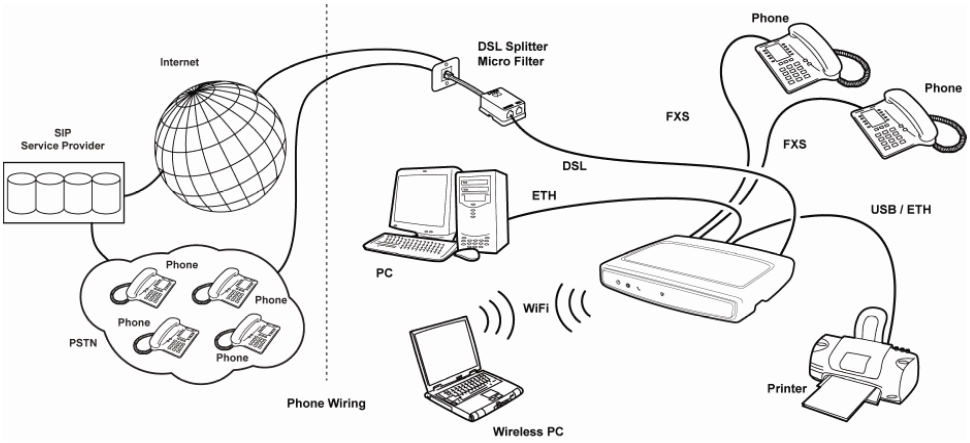


FIGURE 2. **Sample Home Network (existing SIP account case)**



ROUTER ADVANTAGES

The advantages of the Router include:

- Shared Internet connection for both wired and wireless computers
- High speed 802.11b/g/n wireless networking
- No need for a dedicated, “always on” computer serving as your Internet connection
- Cross-platform operation for compatibility with Microsoft® Windows and Apple® MAC computers (see Technical description for supported platforms).

- Easy-to-use, Web-based setup and configuration
- Centralization of all network address settings (DHCP)
- a Virtual server to enable remote access to Web, FTP, and other services on your network
- a Security - Firewall protection - against Internet hacker attacks and encryption to protect wireless network traffic
- VoIP functionalities supporting existing analog phones
- Communication fallback of to analog lines in case of power or hardware faults (if supported by your network operator)
- a multi-language GUI.

MINIMUM SYSTEM AND COMPONENT REQUIREMENTS

Your Router requires the computer(s) and components in your network to be configured with at least the following:

- A computer with the Operating Systems that support TCP/IP networking protocols: Microsoft® Windows 98SE, Windows ME, Windows 2000, Windows XP 32bit or Apple® MAC 10.x
- An Ethernet 10Mbps or 10/100 Mbps NIC for each computer to be connected to one of the four Ethernet ports on the rear of the Router
- An USB 2.0 port
- As optional, an 802.11b/g/n wireless NIC
- At least, 60MB of free hard disk space
- At least, 128 MB of RAM
- Supported Browsers: Internet Explorer 5.5 or higher, Netscape 4.7 or higher

FRONT PANEL

The front panel of the Router contains seven indicator lights (LEDs) that help to describe the state of networking and connection operations.

FIGURE 3. Front Panel LEDs

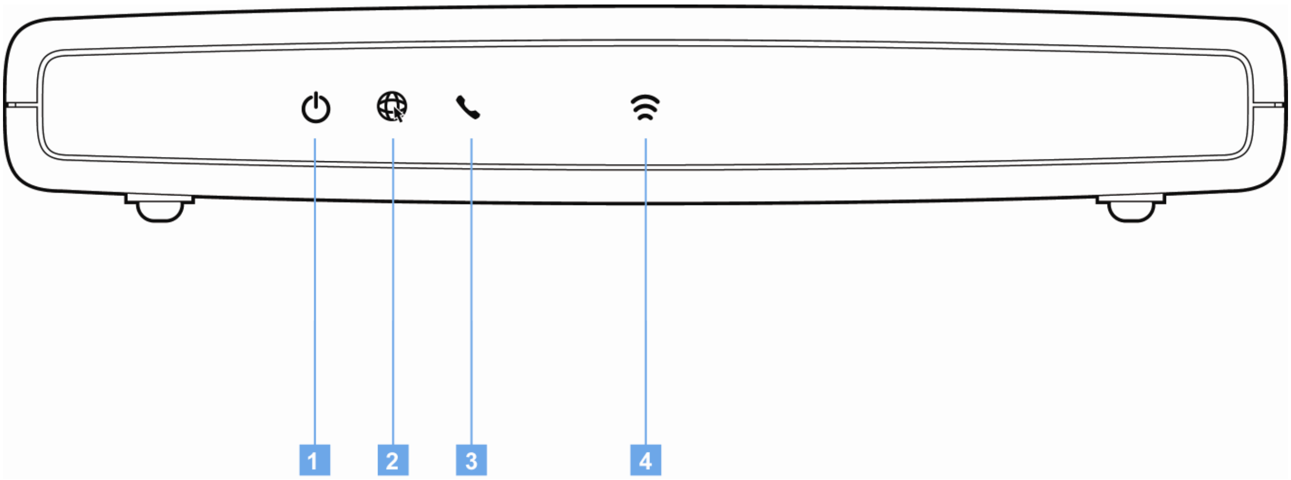


TABLE 2. LED Description

Ref.	LED	LED Color		LED Description
1	***Power***	*White/Red*	*Solid White*	*Power on*
			Solid Red	*Boot Loader Failure*
			Off – white and Red	*Power off*
2	***Internet activity***	*White/Red*	*Solid Green*	*WAN IP address available (e.g. PPP active)*
			Blinking Green	*IP connected and IP traffic is passing through device (either direction)*
			Solid Red	*WAN IP address not available (e.g. PPP failure)*
			Off	*Modem power off or the modem is in bridged mode or connection not present*
3	***Phone***	*White/Red*	*On*	*One of the FXS port has been registered with a SIP proxy server*
			Blinking	*One of the telephones connected to the FXS port is off-hook*
			Off	*Modem power off on phone line 1 or phone line 2 not registered*
4	***Wireless LAN***	*Blue*	*On*	*Wireless functionality enabled*
			Blinking	*Wireless LAN activity present (traffic in either direction)*
			Off	*Wireless functionality disabled*

REAR PANEL

The rear panel of the Router contains a reset button, a power adapter socket, four LAN ports, one port, one USB device port,[††] two USB Host port, one FXO port[‡‡], two FXS ports and one Wi-Fi REG button.

Do not force the antenna beyond its mechanical stops. Rotating the antenna further may cause damage.

FIGURE 4. **Rear Panel Ports**

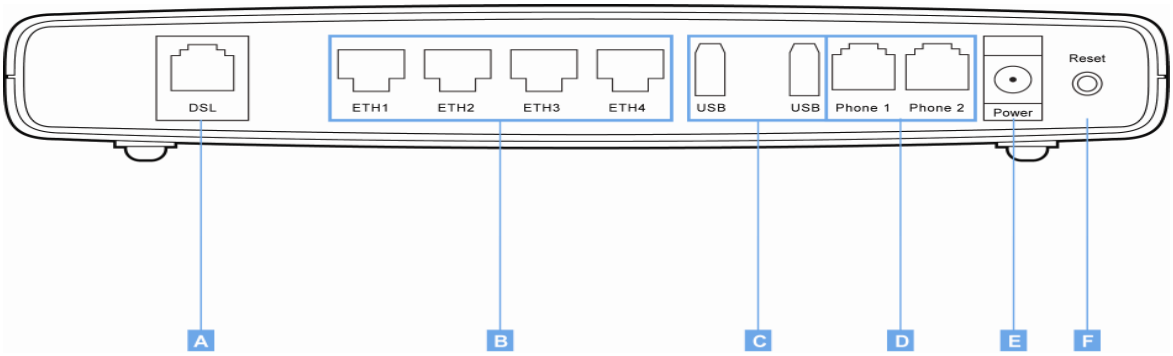


TABLE 3. **Port Description**

PORT	DESCRIPTION
A	*Phone DSL connector (2/2+)*
B	*port Four Ethernet ports 10/100 Mbps*
C	*ports USB 2.0 Host ports*
D	*FXS*
E	*Power connector*
F	*Power button*
-	*Reset to factory default button (located on the side of the device)*
Optional	*FXO*

[††] This port may be optional depending on the product version.
[‡‡] This port may be optional depending on the product version.

Hardware Installation

INTRODUCTION

This chapter will guide you through a basic installation of the Router including:

1. Positioning the **PRG AV4202N**
2. Installing Micro Filters
3. Connecting the Router to your network
4. Setting up your computer for networking with the Router

⚠ *Please read carefully the Safety Information in Appendix "A"*

POSITIONING THE ROUTER

You should place the Router in such a location to ensure that:

- It is located near an electrical outlet and a phone wall socket
- Water or moisture cannot enter the case of the unit
- It is out of direct sunlight and away from sources of heat
- The cabling is away from power lines, fluorescent lighting fixtures, and sources of electrical noise such as radios, transmitters and broadband amplifiers.
- It is centrally located with respect to the wireless devices that will be connected to the Router. A suitable location might be on top of a high shelf to ensure the maximum coverage for all connected devices.

INSTALLING MICRO FILTERS

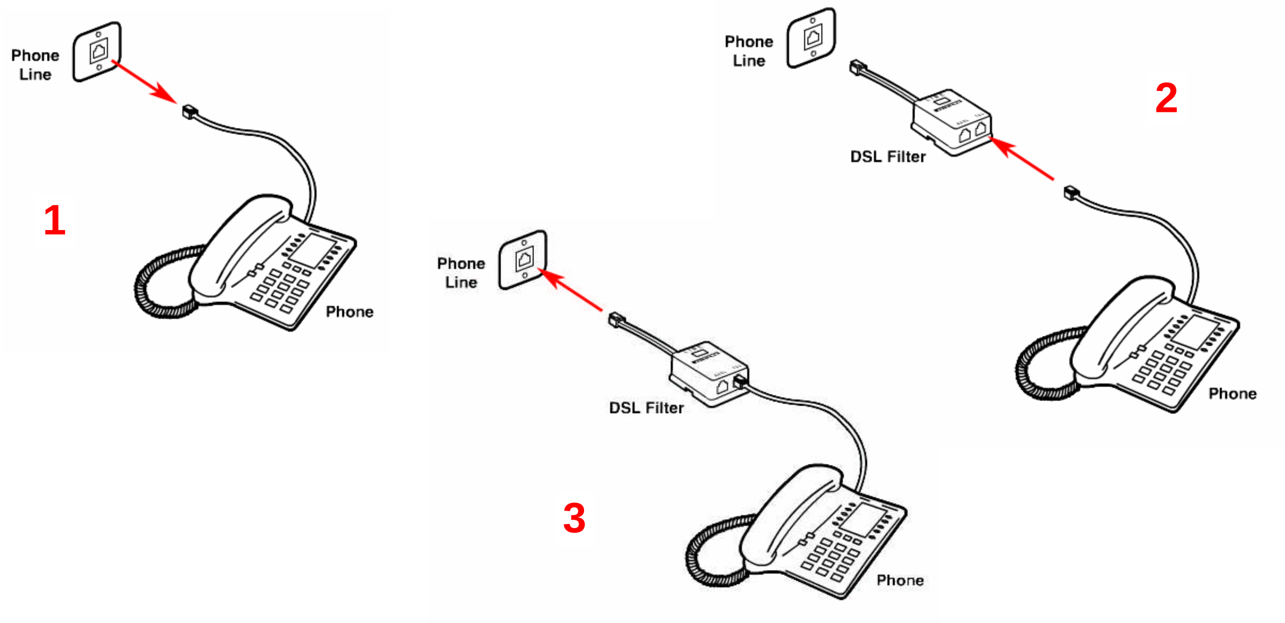
Before beginning installation you must locate devices in your house requiring a DSL filter such as phones, fax machines, answering machines, dial-up modems, Satellite TV dialers or monitored security systems and attach a DSL filter to any one of them sharing the same phone line as your DSL modem.

To install DSL filters please follow these steps:

1. Disconnect the phone cable from the telephone wall socket
2. Insert the phone cable into the DSL filter port identified with a phone symbol
3. Insert the DSL filter cable into the telephone wall socket

⚠ *You do not need to attach a DSL filter to unused wall sockets.*

FIGURE 1. Micro Filter Installation



POWERING UP THE ROUTER

To power up the Router:

1. Plug the power adapter into the power adapter port located on the rear of the Router
2. Plug the power adapter into a standard electrical wall socket
3. Press the Power button located on the rear panel of the Router
4. Wait for the power LED to turn steady green

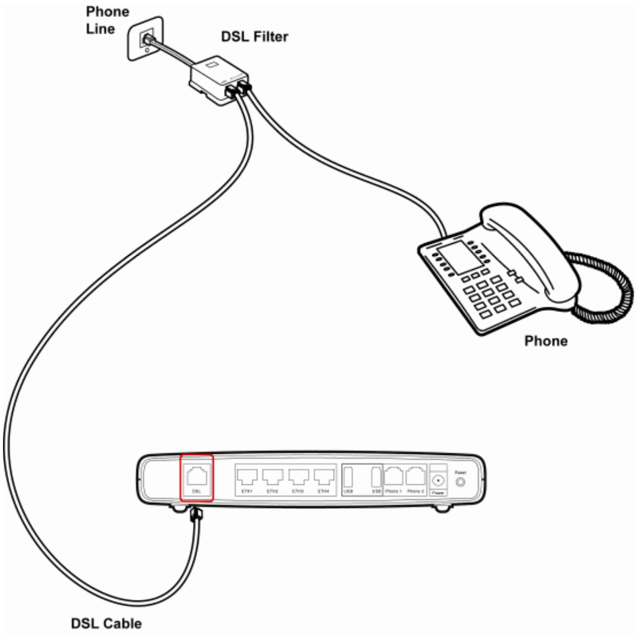
CONNECTING THE ROUTER

The first step to install the router is to physically connect it to the telephone socket and then to connect it to a computer by means of an Ethernet or an USB connection.

To connect the phone cable:

1. Connect one end of the phone cable into the DSL filter port identified with a computer symbol
2. Connect the other end of the phone cable into the DSL port on the rear of the Router

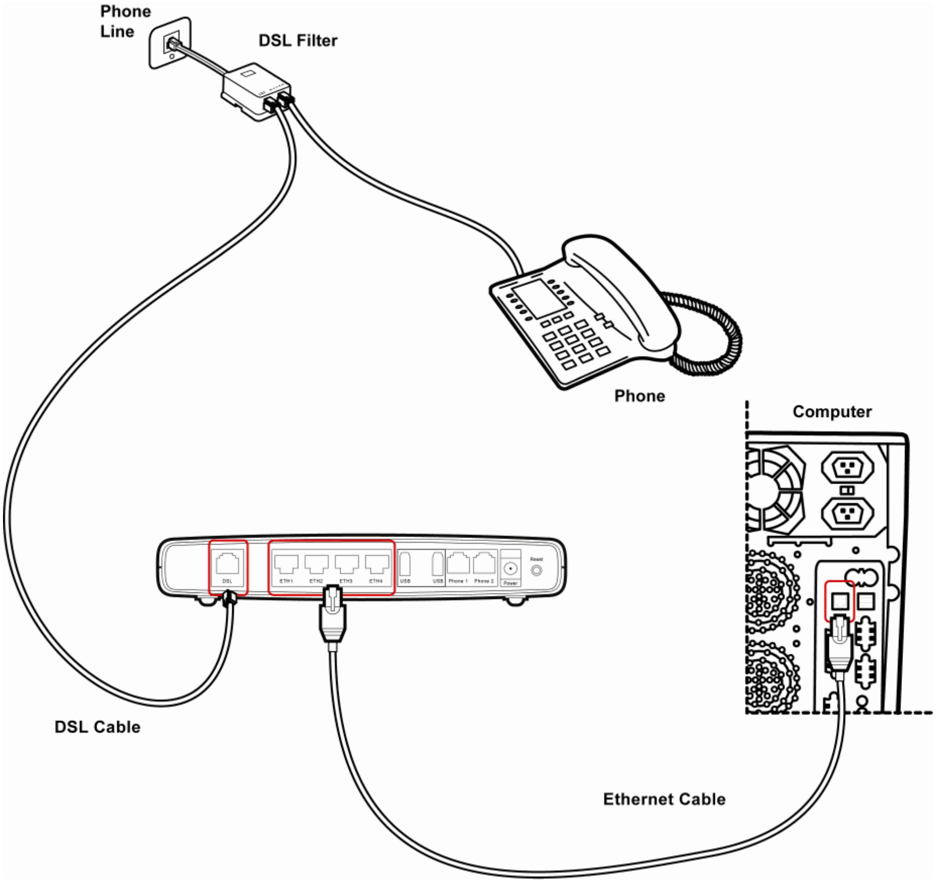
FIGURE 2. Phone Cable Connection



To connect the Ethernet cable:

1. Connect one end of the Ethernet cable into one of the four Ethernet ports on the rear of the Router
2. Connect the other end of the Ethernet cable into the Ethernet Network card of your computer
3. Verify if the Ethernet Network card is configured as DHCP client, otherwise configure it to remain in the same local network of the router interface (see chapter "Setting Up Your Computer")

FIGURE 3. Ethernet Cable Connection



To connect the USB cable, follow the procedure according to your Operating System:

WINDOWS

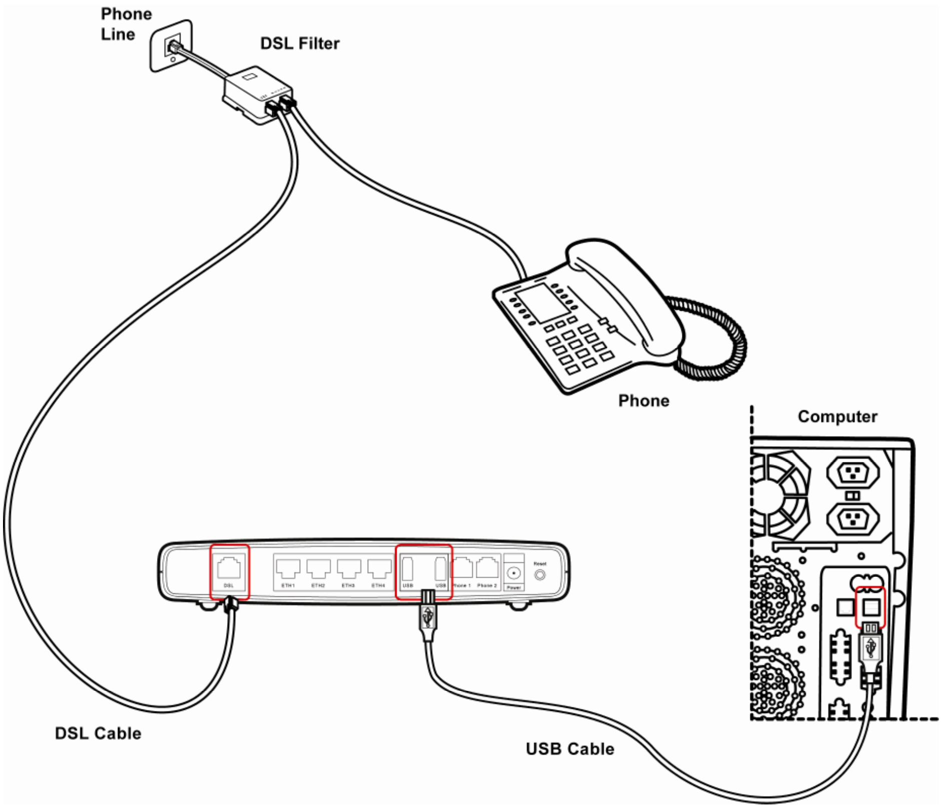
1. Connect one end of the USB cable into the USB port of your PC
2. Browse till *x:\USB driver* folder (where "*x*" is the CD-ROM drive unit letter); launch the "*setup.exe*" executable ("*x:\USB driver\setup.exe*") and follow setup instructions

3. The setup software will invite you to plug the other end of the USB cable into the USB port on the rear of the Router

MAC 10.x

1. Connect one end of the USB cable into the USB port of your PC
2. Connect the other end of the USB cable into the USB port on the rear of the Router. The Operating System will automatically recognize the device

FIGURE 4. USB Cable Connection



Don't plug the other end of the USB cable until setup software will ask you to do it.

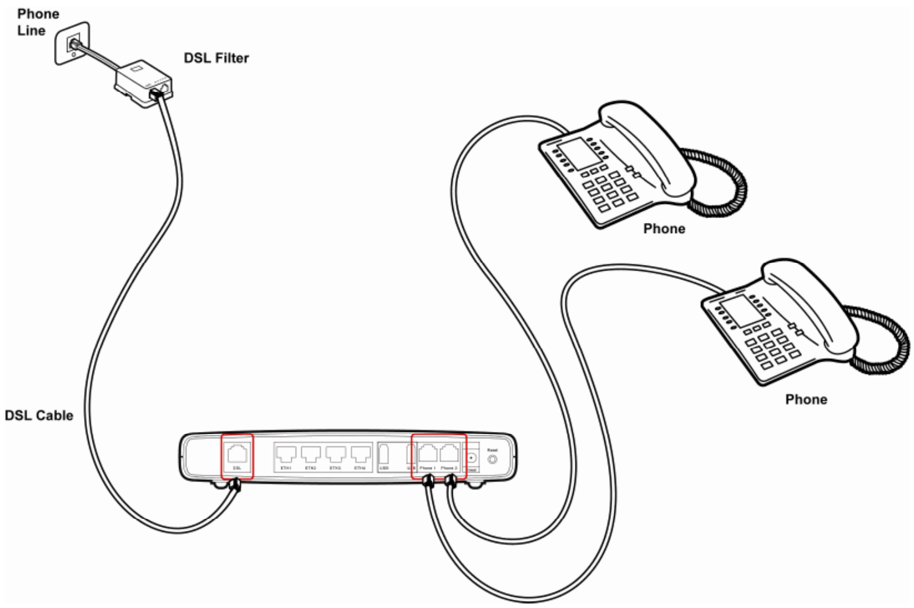
In the case your provider will supply to you a SIP account, it will be needed to properly connect the FXS and FXO ports. In detail you must follow these steps:

1. Connect one end of the first phone cable into the DSL filter port identified with a computer symbol
2. Connect the other end of the first phone cable into the DSL port of the Router

3. Connect one end of the second phone cable into the DSL filter port identified with a phone symbol
4. Connect the other end of the second phone cable into the WALL port of the Router (FXO connection)*
5. Connect a maximum of two analog phones to the Phone 1 or Phone 2 ports of the Router (FXS connection)

* If your product does not include the FXO port, exclude steps 3 and 4

FIGURE 5. **FXS connections**



Connect to your PC with Ethernet or USB cables as described in the previous steps.

Setting Up Your Computer

The Router has the ability to dynamically allocate network addresses to the computers on your network, using DHCP. However, your computers need to be configured correctly for this to take place. To change the configuration of your computers to allow this, follow the instructions in this chapter.

INSTALL SOFTWARE

The very first time you set up your computer, we recommend you to use the Smart Setup Configuration Utility if your ISP has provided you with.

⚠ *Before installing the **PRG AV4202N** software please close all applications to avoid any conflict.*

This utility offers a guided product tour, a step by step hardware installation guide, a software installation guide and setup depending on your connection choice (USB or ETHERNET) and a driven user registration with DSL Internet connection line check.

Smart Setup Configuration Utility allows, for supported Microsoft® Windows Operating Systems, to setup automatically your computer Ethernet settings.

To launch it, insert the CD-ROM in CD-ROM unit: if the auto-play function is enabled it will start automatically, otherwise open it manually from “*x:*”, where *x* is your CD-ROM drive letter.

ETHERNET CONNECTION

In case you already established a connection with your Router a first time and/or you do need to set up manually a connection to your Router, please follow the instructions described in this chapter. You will be guided to set up an Ethernet connection to the Router. To do so, first you have to verify the existence of a TCP/IP protocol stack and, then, according to your Operating System, to establish an Ethernet connection to it. This connection will require you to enable your computer to receive from the Router its own IP Address automatically: in such a case, the Router acts like the DHCP server in your local network.

ETHERNET CONNECTION >> TCP/IP PROTOCOL INSTALLATION

This procedure requires the TCP/IP protocol installed on your computer. Refer to the following chapters and to your Microsoft® Windows or Apple® MacOS 10.x operating systems manuals.

Microsoft® Windows 98SE, ME, 2000

1. Put in the CD-ROM drive your Windows installation CD-ROM
2. Starting from *Start -> Settings -> Control Panel -> Network Control Panel*, make a double click on the *Network* icon
3. Select *Configuration -> TCP/IP* and then click on the *Add* button
4. Select Protocols, click on *Add* button and choose Microsoft TCP/IP. Then click on the *OK* button
5. After the computer reboots, you're ready to configure the TCP/IP settings Configure the Network adapter to obtain automatically an IP address

Microsoft® Windows XP

1. Put in the CD-ROM drive your Windows installation CD-ROM
2. Starting from *Start -> Settings -> Control Panel* make a double click on the *Network* icon.
3. Select *Protocol* and click on the *Add* button. Select *Microsoft* and *TCP/IP*, then click on the *OK* button.
4. Configure the Network adapter to obtain automatically an IP address.

Apple® MacOS 10.x

TCP/IP is installed on a MacOS system as part of Open Transport.

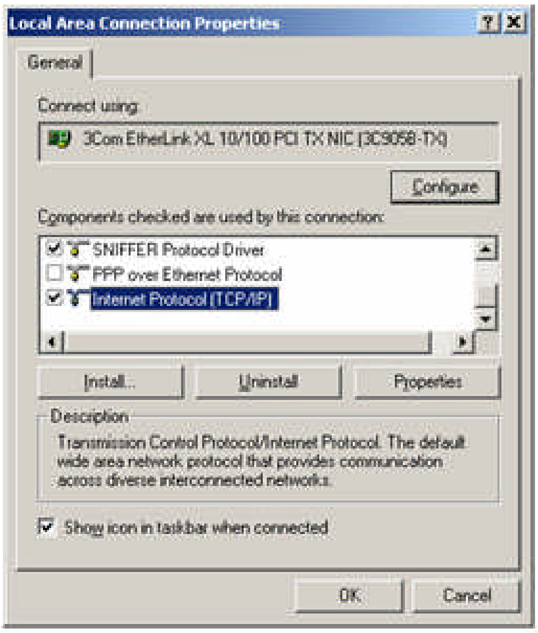
ETHERNET CONNECTION >> MS WINDOWS 98SE, ME, 2000

To configure TCP/IP on these Operating Systems follow these steps:

1. Select *Start -> Settings -> Control Panel* and make a double click on the *Network* icon.

2. Select *Configuration ->TCP/IP* then click on *Properties* button.

FIGURE 1. Local Area Connection Properties



Local Area Connection Properties

General

Connect using:

3Com EtherLink XL 10/100 PCI TX NIC (3C905B-TX)

Components checked are used by this connection:

☑ SNIFFER Protocol Driver
☐ PPP over Ethernet Protocol
☑ Internet Protocol (TCP/IP)

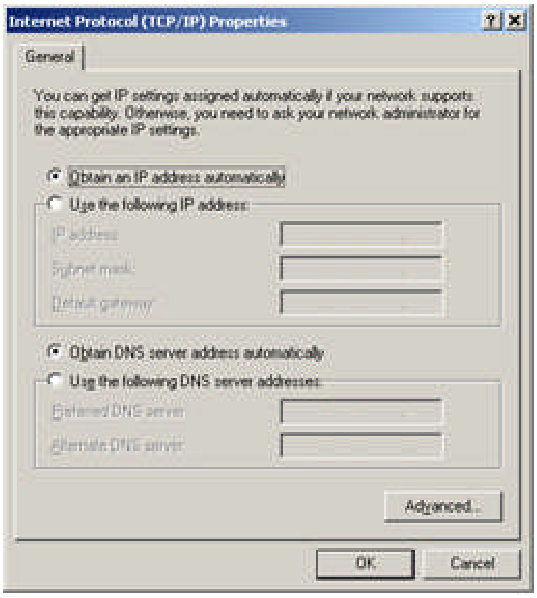
Description

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

☑ Show icon in taskbar when connected

3. Select the *IP Address* Tab, then check to obtain an automatically IP address. Click on *OK* button.

FIGURE 2. Internet Protocol (TCP/IP) Properties



Internet Protocol (TCP/IP) Properties

General

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

● Obtain an IP address automatically
○ Use the following IP address:

IP address:
Subnet mask:
Default gateway:

● Obtain DNS server address automatically
○ Use the following DNS server addresses:

Preferred DNS server:
Alternate DNS server:

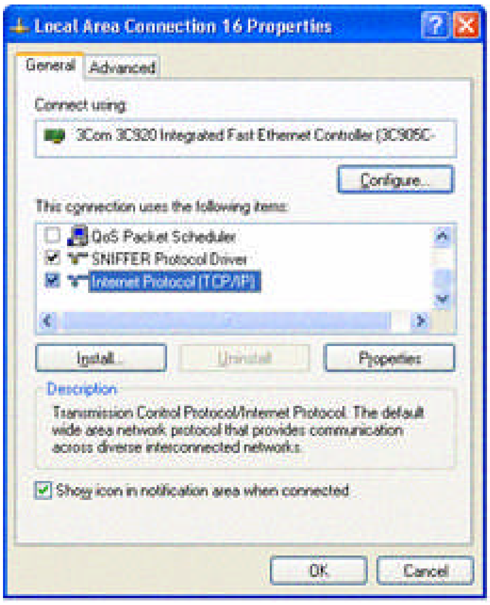
4. A system reboot will be required to make the changes real.
5. Enter http://192.168.1.1/ in the address bar of your browser to open the PRG AV4202N Home Page.

ETHERNET CONNECTION >> MS WINDOWS XP

To configure TCP/IP on MS Windows XP Operating System follow these steps:

1. Select *Start -> Settings -> Control Panel* and make a double click on the *Network* icon.
2. Select *Protocols ->TCP/IP* then click on *Properties* button.

FIGURE 3. Local Area Connection Properties



Local Area Connection 16 Properties

Connect using:

3Com 3C920 Integrated Fast Ethernet Controller (3C905C-

This connection uses the following items:

□ QoS Packet Scheduler
☑ SNIFFER Protocol Driver
☑ Internet Protocol (TCP/IP)

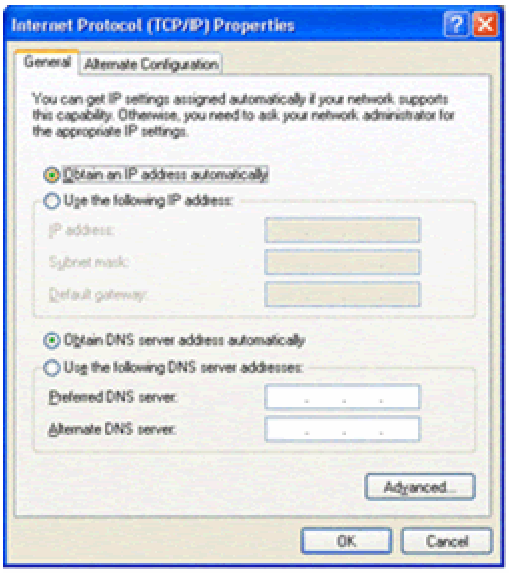
Description

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

☑ Show icon in notification area when connected

3. Select the General Tab, then check to obtain an automatically IP address. Click on *OK* button.

FIGURE 4. **Internet Protocol (TCP/IP) Properties**



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

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

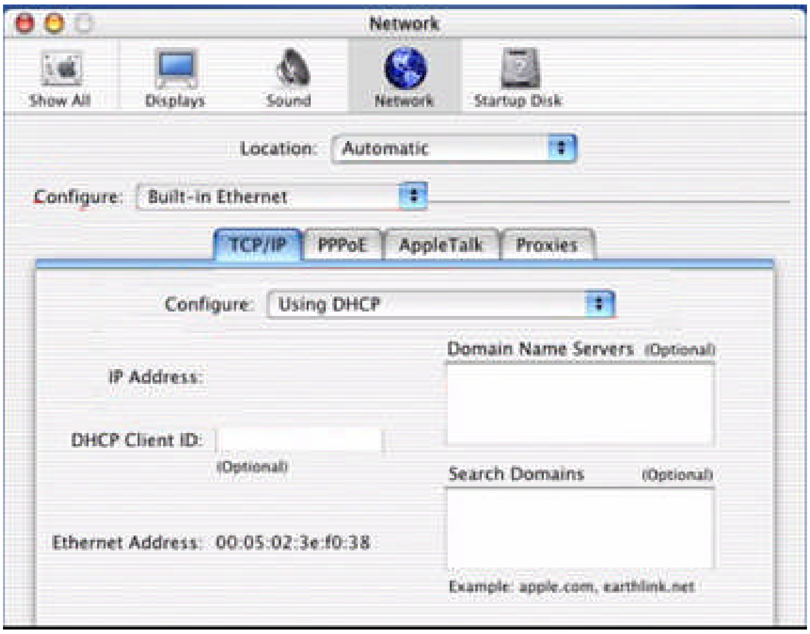
Alternate DNS server:

ETHERNET CONNECTION >> MAC OS 10.X

To configure TCP/IP on MAC OS 10.x follow these steps:

1. Open the Apple Menu -> System Preferences and select Network.
2. From the Show drop down list, according to the type of connection used, select Built-in Ethernet.
3. Select the *TCP/IP* tab.
4. Select *DHCP* from the Configure pop-up menu to have a dynamic IP address.

FIGURE 5. **Network panel on MAC OS 10.x**



Location: Automatic

Configure: Built-in Ethernet

Configure: Using DHCP

Ethernet Address: 00:05:02:3e:f0:38

5. Click Apply Now.
6. Click on the *Register* button to save the changes in the Control Panel.
7. Enter *http://192.168.1.1/* in the address bar of your browser to open the **PRG AV4202N** Home Page.

USB CONNECTION

To connect your first Computer to the **PRG AV4202N** using USB port, you have to install the Router’s USB driver on your computer.

*Before connecting the USB Cable to the USB Port of the **PRG AV4202N** you have to run the setup software and to follow the instructions. Connect the USB Cable only when required from the installation software.*

*Only one Windows or Macintosh computer can be directly connected to the **PRG AV4202N** using the USB connection. Additional computers can be added to your network using the others connection such as Ethernet or Wi-Fi.*

USB CONNECTION >> MS WINDOWS

Using Windows 98SE the system could require the Operating System installation CD-ROM.

1. Browse the Setup CD-ROM and install the USB Windows driver selecting the folder x:\driver (where x is the CD-ROM driver unit).
2. Make a double click on setup.exe file to start driver setup procedure.
3. When the message “NOW CONNECT THE USB CABLE” appears, connect the USB cable from a free USB port of the computer to the **PRG AV4202N** USB port.
4. Enter *http://192.168.1.1/* in the address bar of your browser to open the **PRG AV4202N** Home Page.

USB CONNECTION >> MAC OS 10.X

As MAC OS 10.x will automatically recognize the device, no USB driver installation is required.

1. Enter *http://192.168.1.1/* in the address bar of your browser to open the **PRG AV4202N** Home Page.

WI-FI CONNECTION

It requires a computer with 802.11b/g (Wi-Fi Certified) wireless adapter installed.

1. Install your wireless adapter according to the manufacturer’s instructions and verify that your computer is set to obtain an IP address automatically (DHCP mode).

*You will need to properly configure your adapter to communicate with the **PRG AV4202N** according to the configuration rules.*

2. In the configuration window of your wireless adapter scan the wireless network (marked with the relevant SSID name) present in your physical environment.
3. Select the SSID of the **PRG AV4202N**
4. Complete the configuration of the wireless adapter with the same parameters of the **PRG AV4202N** which are:

- RF channel; automatically detect (default = 6)
- WEP encryption enable or disable (default = Disable)
- WEP key size

- WEP key used

5. To check the connection, connect to the **PRG AV4202N** Home Page, entering http://192.168.1.1/ in the address bar of your browser.

Router Configuration

INTRODUCTION

The Router setup program is web based, which means that it is accessed through your web browser.

To access to Router's web server:

1. Launch your web browser on the computer
2. Enter the following URL in the location or address field of your browser: http://192.168.1.1

The Router comes with a default IP address (192.168.1.1). If you change it, please take note of the new Router's IP address, otherwise a "Reset to Factory Default" operation should be done to be able to access again to the Router.

Access to DSL router configuration pages is controlled through user accounts. The default one is the *admin* user with unrestricted access to change and view configuration of the DSL Router.

The default username and password are both set to "admin". It is recommended to change these default values. Make sure you remember your user name and password, since this is the only way you will be able to manage your Router

You will be asked to choose the Router interface language between *English, French, Russian, Spanish, Korean, Traditional Chinese, Japanese, German, Italian* and *Simplified Chinese* and to insert a *User Name* and a *Password*: insert them to access to Router's configuration panels.

If not already configured, at the first login the *Installation Wizard* panel will be shown to configure the Router connection parameters, otherwise the *Home page* will be opened as shown in Figure 1.

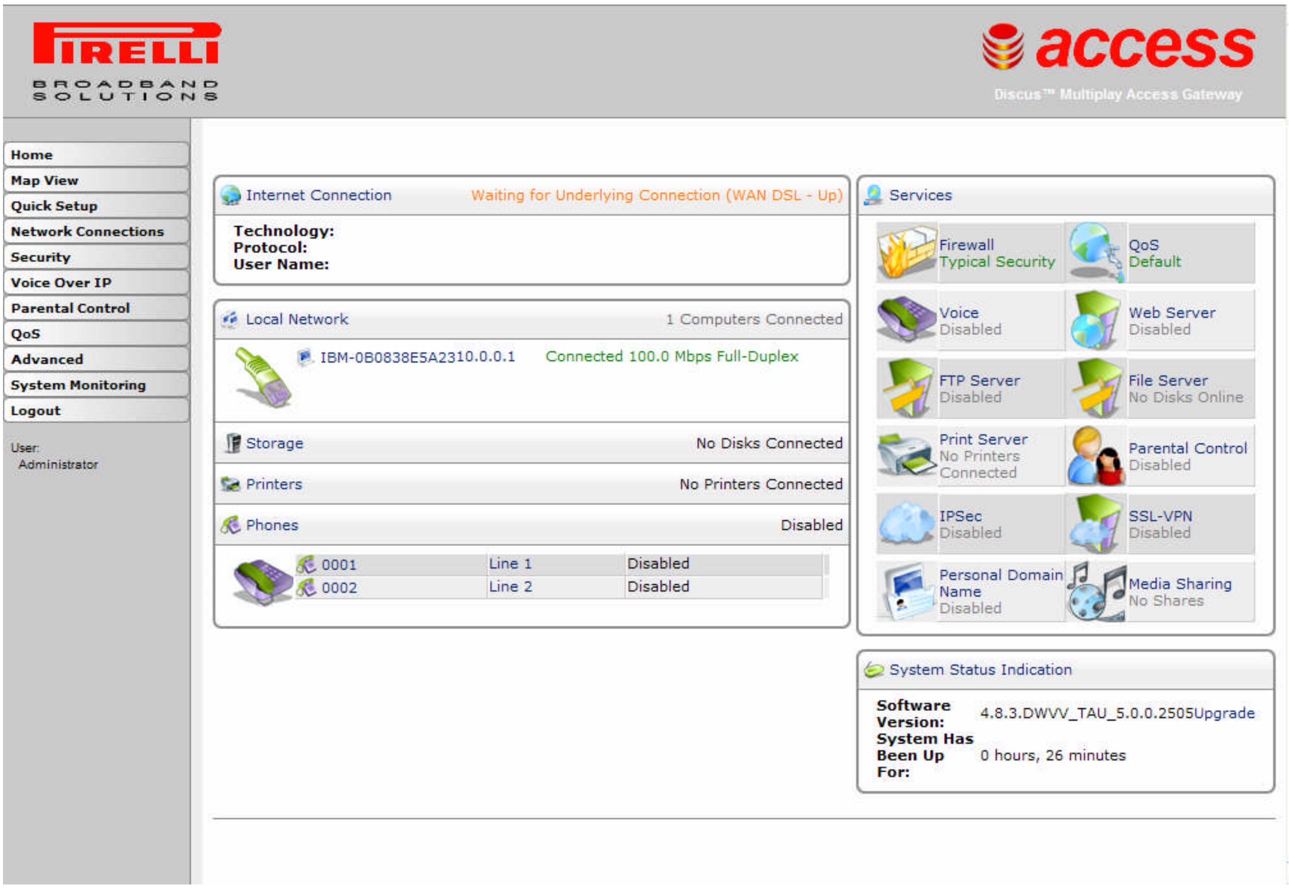
The *Home page* contains a menu on the left - always available in all the web pages which is the starting point for any Router's configuration.

The complete menu has the following main items:

1. **Home**: it shows a graphical representation of your network.
2. **Map View**: it displays the Network Map of attached or configured devices
3. **Quick Setup**: it allows to quickly perform the Router's connection setup
4. **Network Connections**: it shows the status of network connections allowing to modify them or to create new ones
5. **Security**: it allows to set security settings
6. **Voice over IP**: it allows to set VoIP accounts
7. **Parental Control**: it allows to set Parental Control filtering
8. **QoS**: it gathers all QoS parameters and settings
9. **Advanced**: it allows the access to the advanced configuration panels and to define Router parameters devoted to user access, log management, Router's time, Backup Router's configuration, etc.
10. **System Monitoring**: a menu to show and run diagnostic test for trouble-shooting or system behavior analysis and to access to Device Information and Statistics
11. **Logout**: to logout from Router's session.

*In order to submit the changes of most of device parameters you have to click the **Apply** button to save permanently your changes. In some case a Router's reboot is required.*

FIGURE 1. Router’s Home Page



Discus™ Multiplay Access Gateway

- Home
- Map View
- Quick Setup
- Network Connections
- Security
- Voice Over IP
- Parental Control
- QoS
- Advanced
- System Monitoring
- Logout

User:
Administrator

Internet Connection — Waiting for Underlying Connection (WAN DSL - Up)

Technology:
Protocol:
User Name:

Local Network — 1 Computers Connected

IBM-0B0838E5A2310.0.0.1 — Connected 100.0 Mbps Full-Duplex

Storage — No Disks Connected

Printers — No Printers Connected

Phones — Disabled

0001	Line 1	Disabled
0002	Line 2	Disabled

Services

Firewall Typical Security	QoS Default
Voice Disabled	Web Server Disabled
FTP Server Disabled	File Server No Disks Online
Print Server No Printers Connected	Parental Control Disabled
IPSec Disabled	SSL-VPN Disabled
Personal Domain Name Disabled	Media Sharing No Shares

System Status Indication

Software Version: 4.8.3.DWVV_TAU_5.0.0.2505Upgrade

System Has Been Up For: 0 hours, 26 minutes

In the following table a list of all available network objects and related description is shown.

TABLE 1. Available Network Objects

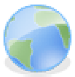
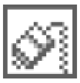
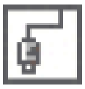
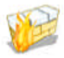
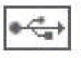
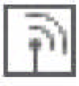
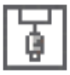
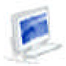
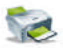
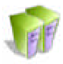
Map Symbol	Description
	*It represents the Internet*
	*It represents your DSL Wide Area Network (WAN) connection. Click this icon to configure the WAN interface*

TABLE 1. **Available Network Objects**

Map Symbol	Description
	*It represents your Ethernet Wide Area Network (WAN) connection or an Ethernet Local Area Network (LAN) connection. Click this icon to configure the WAN interface or the Ethernet LAN device*
	*It represents the gateway's Firewall. The height of the wall corresponds to the security level currently selected: Minimum, Typical or Maximum. Click this icon to configure security settings*
	*It represents a USB LAN connection. Click this icon to configure network parameters for the USB LAN device*
	*It represents a Wireless LAN connection. Click this icon to configure network parameters for the Wireless LAN device*
	*It represents a bridge connected in the home network. Click this icon to view the bridge's underlying devices.*
	*It represents a computer (host) connected in the home network. Each computer connected to the network appears below the network symbol of the network through which it is connected. Click an icon to view network information for the corresponding computer..*
	*It represents a printer that is connected to the Router and is shared by network users. Click the icon to view the printer's settings.*
	*It represents a file server that is connected to the Router and is shared by network users. Click the icon to view the file server configuration.*

Installation Wizard Section

This chapter will describe the **Installation Wizard Section** accessible from the *Home Page* of the **PRG AV4202N** upon user authentication to the Router.

⚠ *Be aware that any configuration changes could compromise your connectivity.*

The *Installation Wizard* enables speedy configuration of your Internet connection.

It is a step-by-step procedure that guides you through your Internet connection and wireless network setup, and helps you to subscribe for different services. The wizard progress box, located at the right hand side of the screen, provides a monitoring tool for the wizard's steps during the installation progress.

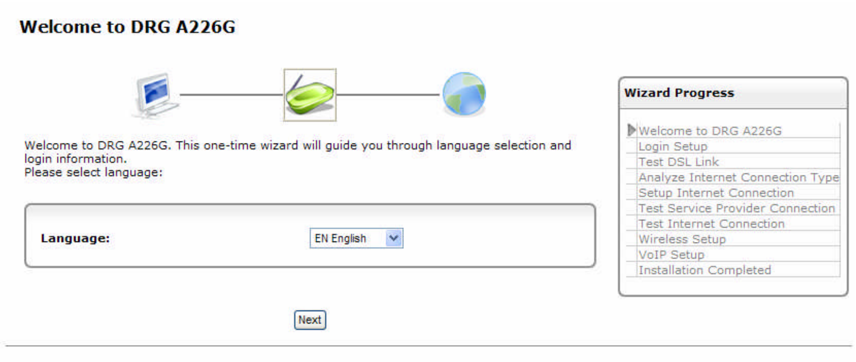
After the setup described in this chapter, you can immediately start using your Router to:

1. Share a broadband connection among multiple users (HTTP, FTP, Telnet, NetMeeting) and between all of the computers connected to your home network.
2. Build a home network by connecting additional PCs and network devices to the gateway.
3. Share resources (file servers, printers, etc.) between computers in the home network using their names; auto-learning DNS enables **PRG AV4202N** to automatically detect the network identification names of the LAN PCs, enabling mutual communication using names, not IP addresses.
4. Control network parameters, including DHCP, DNS and WAN settings.

5. View network status, traffic statistics, system log and more.
6. Allow access from the Internet to games and other services provided by computers in the home network.
7. Prohibit computers in the home network from accessing selected services on the Internet.
8. Block access to specific Internet Web sites from your home network.

To start the installation wizard, click *Next*. The wizard procedure will commence, performing the steps listed in the progress box consecutively, stopping only if a step fails or if input is required. The following sections describe the wizard steps along with their success/failure scenarios. If a step fails, use the *Retry* or *Skip* buttons to continue.

FIGURE 1. Installation Wizard Panel



Welcome to DRG A226G

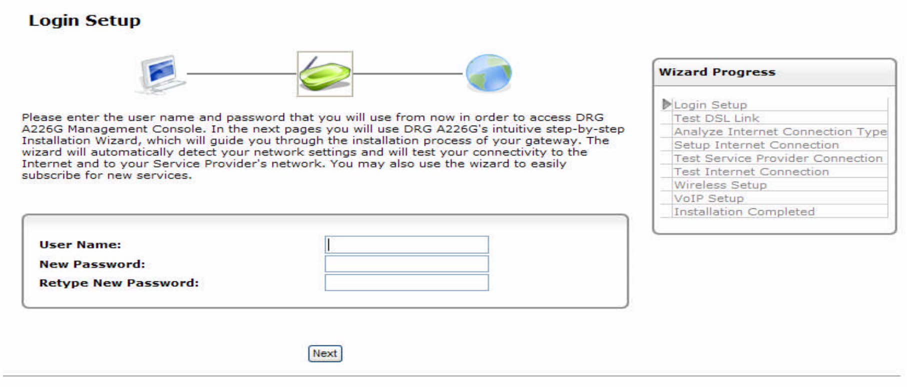
Welcome to DRG A226G. This one-time wizard will guide you through language selection and login information.
Please select language:

Language: EN English

LOG IN SETUP

Insert a user name and password, be sure to remember the log in credentials used. Its advised to write them down in a peace of paper and store it in a safe place.

FIGURE 2. Log In Panel



Login Setup

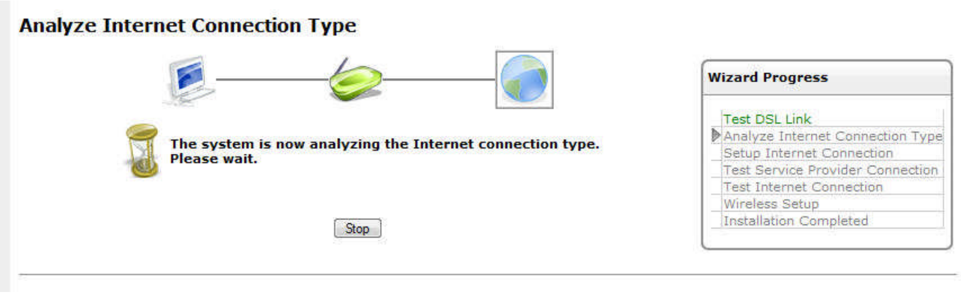
Please enter the user name and password that you will use from now in order to access DRG A226G Management Console. In the next pages you will use DRG A226G's intuitive step-by-step Installation Wizard, which will guide you through the installation process of your gateway. The wizard will automatically detect your network settings and will test your connectivity to the Internet and to your Service Provider's network. You may also use the wizard to easily subscribe for new services.

User Name:
New Password:
Retype New Password:

TEST ETHERNET LINK

The first step is a test of the Ethernet connection. This step may fail if the router cannot detect your Ethernet link (for example, if the cable is unplugged). Verify that your Ethernet cables are connected properly, and click *Retry*.

FIGURE 3. Test Ethernet Link Panel



Analyze Internet Connection Type

The system is now analyzing the Internet connection type. Please wait.

ANALYZE INTERNET CONNECTION TYPE

The next step is an analysis of your Internet connection. This step may fail if the router is unable to detect your Internet connection type.

After three retries, the screen provides a link to manually set the Internet connection type. Click this link. The screen refreshes, displaying a connection type combo box. To learn about manually configuring your Internet connection, please refer to the *Quick Setup Section* of this manual.

SETUP INTERNET CONNECTION

If your Internet connection requires login details provided by your Internet Service Provider (ISP) (e.g when using PPPoE).

Enter your *user name* and *password* and click *Next*.

TEST SERVICE PROVIDER CONNECTION

This step tests the connectivity to your ISP.

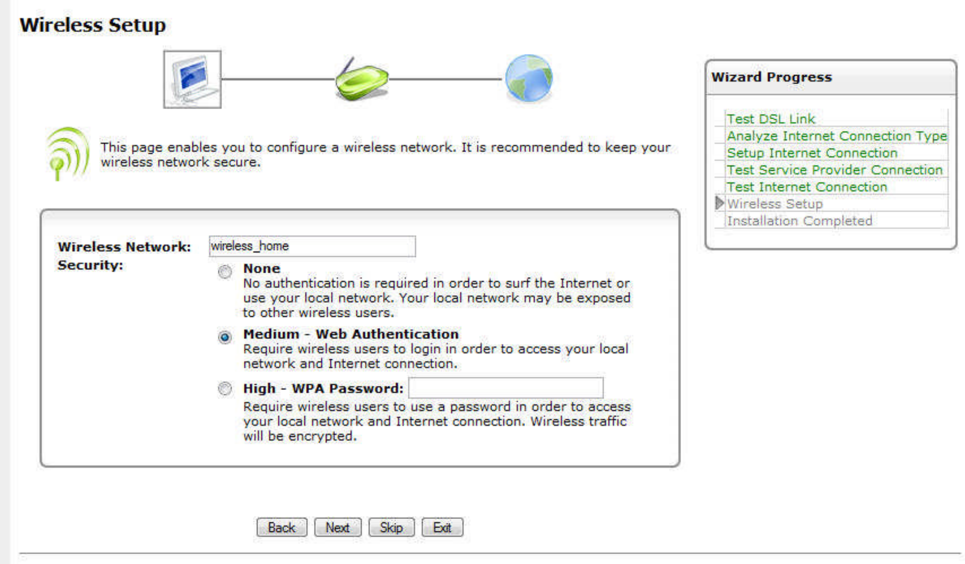
TEST INTERNET CONNECTION

This step tests the connectivity to the Internet.

WIRELESS SETUP

Use this step to configure a wireless network. Enter a name for your wireless network and select its level of security. Click *Next*.

FIGURE 4. **Wireless Setup Panel**



Wireless Setup

This page enables you to configure a wireless network. It is recommended to keep your wireless network secure.

Wireless Network: wireless_home

Security:

○ **None**
No authentication is required in order to surf the Internet or use your local network. Your local network may be exposed to other wireless users.

● **Medium - Web Authentication**
Require wireless users to login in order to access your local network and Internet connection.

○ **High - WPA Password:**
Require wireless users to use a password in order to access your local network and Internet connection. Wireless traffic will be encrypted.

VOIP SETUP

This page enables you to configure a VoIP account.

INSTALLATION COMPLETED

This screen provides a summary of all the above Internet connection configuration steps and their results. Click *Finish* to complete the wizard procedure.

Quick Setup Section

This chapter will describe the **Quick Setup Section** accessible from the *Home Page* of the **PRG AV4202N** upon user authentication to the Router.

⚠ *Be aware that any configuration changes could compromise your connectivity.*

When subscribing to a broadband service, you should be aware of the method by which you are connected to the Internet. Your physical WAN device can be either Ethernet, DSL, or both. Technical information regarding the properties of your Internet connection should be provided by your Internet Service Provider (ISP). For example, your ISP should inform you whether you are connected to the Internet using a static or dynamic IP address, or what protocols, such as PPTP or PPPoE, you will be using to communicate over the Internet.

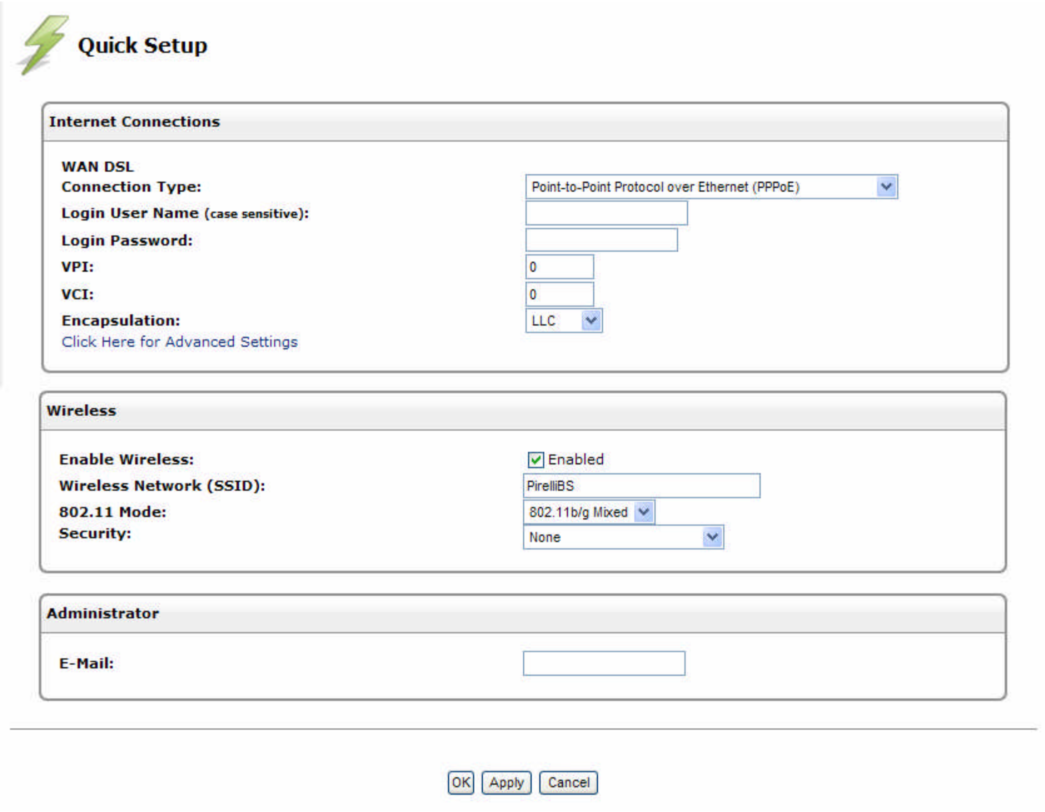
The Router will automatically recognize if you have more than one physical WAN device on your gateway, and will provide a configuration section for each, under the 'Internet Connections' section of the 'Quick Setup' screen.

Your WAN connection(s) can be configured using one of the following methods. Read the configuration instructions relevant to you, by selecting your connection method from the list below:

1. Point-to-point protocol over Ethernet (PPPoE) over ATM
2. Point-to-point protocol over Ethernet (PPPoE) over PTM
3. Point-to-point protocol over ATM (PPPoA)
4. Routed Ethernet Connection over ATM (ETHoA)
5. Bridged Ethernet Connection over ATM (ETHoA)

6. No Internet connection

FIGURE 1. **Quick Setup Panel**



Quick Setup

Internet Connections

WAN DSL
Connection Type: Point-to-Point Protocol over Ethernet (PPPoE)
Login User Name (case sensitive):
Login Password:
VPI: 0
VCI: 0
Encapsulation: LLC
Click Here for Advanced Settings

Wireless

Enable Wireless: ☑ Enabled
Wireless Network (SSID): PirelliBS
802.11 Mode: 802.11b/g Mixed
Security: None

Administrator

E-Mail:

POINT-TO-POINT PROTOCOL OVER ETHERNET (PPPOE) OVER ATM

To configure the Point-to-point protocol over Ethernet, follow these steps:

7. Select 'Point-to-point protocol over Ethernet (PPPoE)' from the 'Connection Type' combo-box.
8. Your Internet Service Provider (ISP) should provide you with the Login user name and Login password.
9. If your board features a DSL connection, you will see an 'Automatic PVC Scan' check box. Select this check box to enable the automatic configuration of the VPI, VCI and encapsulation parameters (relevant to DSL connections).

ETHERNET (PPPOE) OVER PTM

To configure the Point-to-point protocol over Ethernet, follow these steps:

1. Select 'Point-to-point protocol over Ethernet (PPPoE)' from the 'Connection Type' combo-box.
2. Your Internet Service Provider (ISP) should provide you with the Login user name and Login password.

POINT-TO-POINT PROTOCOL OVER ATM (PPPOA)

To configure the Point-to-point protocol over ATM, follow these steps:

1. Select 'Point-to-point protocol over ATM (PPPoA)' from the 'Connection Type' combo-box
2. Your Internet Service Provider (ISP) should provide you with the following information:
   - Login user name
   - Login password
3. By default, the 'Automatic PVC Scan' check box is enabled, which means that the Router configures the VPI, VCI and encapsulation parameters automatically. If you would like to configure these parameters manually, uncheck this check box.
   - Specify the VPI and VCI values.
   - Select the encapsulation method from the combo-box. You can choose among the following methods: LLC, VCMux and VCMux - HDLC

ROUTED ETHERNET CONNECTION OVER ATM (ETHOA)

To configure the Routed Ethernet connection over ATM, follow these steps:

4. Select 'Routed Ethernet Connection over ATM (ETHoA)' from the 'Connection Type' combo-box
5. Your Internet Service Provider (ISP) should provide you with the following information:
   - Specify the value of the VPI and VCI parameters.
   - Select the encapsulation method from the combo-box. You can choose among the following methods: LLC, VCMux.
   - Select the Internet Protocol: Most Internet Service Providers (ISPs) provide dynamic IP addresses, hence the default "Obtain an IP Address Automatically". Should this not be the case, select the "Use the Following IP Address" option. The screen will refresh. Enter the IP Address, Subnet Mask, Default Gateway, and DNS Server details provided to you by your ISP.

ROUTED ETHERNET CONNECTION OVER PTM (ETHOP)

To configure the Routed Ethernet connection over PTM, follow these steps:

1. Select 'Routed Ethernet Connection over PTM (ETHoP)' from the 'Connection Type' combo-box

2. Your Internet Service Provider (ISP) should provide you with the following information:
   - Select the Internet Protocol: Most Internet Service Providers (ISPs) provide dynamic IP addresses, hence the default "Obtain an IP Address Automatically". Should this not be the case, select the "Use the Following IP Address" option. The screen will refresh. Enter the IP Address, Subnet Mask, Default Gateway, and DNS Server details provided to you by your ISP.

BRIDGED ETHERNET CONNECTION OVER ATM (ETHOA)

To configure the Bridged Ethernet Connection over ATM (ETHoA), follow these steps:

1. Select 'Bridged Ethernet Connection over ATM (ETHoA)' from the 'Connection Type' combo-box
2. Your Internet Service Provider (ISP) should provide you with the following information:
   - Specify the value of the VPI and VCI parameters.
   - Select the encapsulation method from the combo-box. You can choose among the following methods: LLC, VCMux

BRIDGED ETHERNET CONNECTION OVER PTM (ETHOP)

To configure the Bridged Ethernet Connection over ATM (ETHoA), follow these steps:

1. Select 'Bridged Ethernet Connection over ATM (ETHoA)' from the 'Connection Type' combo-box

NO INTERNET CONNECTION

Select 'No Internet Connection' from the 'Connection Type' combo-box. Choose this connection type if you do not have an Internet connection, or if you want to disable all existing connections.

WIRELESS

Click the 'Enabled' check box to enable your wireless connection. Specify the wireless network's ID in the 'SSID' field. The default SSID is 'openrg'.

ADMINISTRATOR

In this section it is necessary to specify the administrator's e-mail in the 'E-mail' field. System alerts and notifications are sent to this address.

Network Connections Section

This chapter will describe the **Network Connections Section** accessible from the *Home Page* of the **PRG AV4202N**.

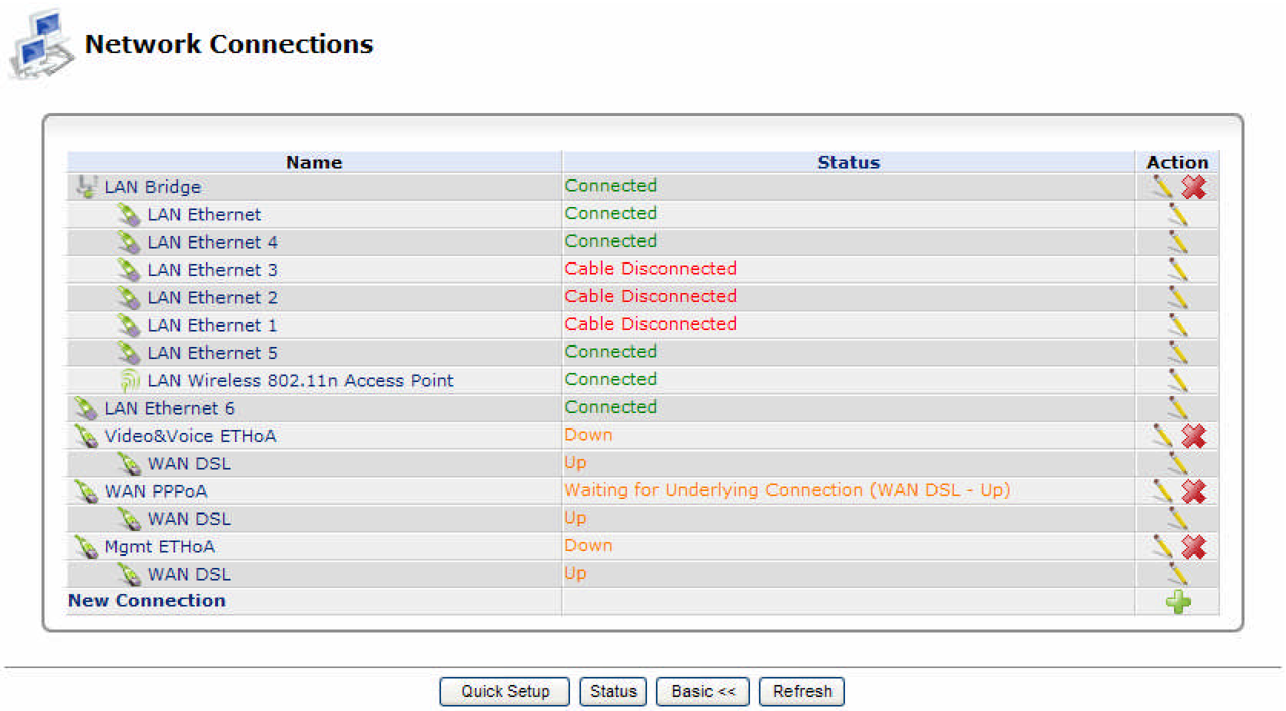
⚠ *Be aware that any configuration changes could compromise your connectivity.*

This section (see Figure 1) is intended to present a summary of the Router's connections, such as WAN and LAN (i.e. Ethernet, USB, Wireless) interfaces.

PRG AV4202N supports various network connections, both physical and logical. The Network Connections screen enables you to configure the various parameters of your physical connections, the LAN and WAN, and create new connections, using tunneling protocols over existing connections, such as PPP and VPN.

Press the *'Advanced'* button to expand the screen and display all connection entries.

FIGURE 1. **Network Connections Panel**



Network Connections

Name	Status	Action
LAN Bridge	Connected	✎ ✖
LAN Ethernet	Connected	✎
LAN Ethernet 4	Connected	✎
LAN Ethernet 3	Cable Disconnected	✎
LAN Ethernet 2	Cable Disconnected	✎
LAN Ethernet 1	Cable Disconnected	✎
LAN Ethernet 5	Connected	✎
LAN Wireless 802.11n Access Point	Connected	✎
LAN Ethernet 6	Connected	✎
Video&Voice ETHoA	Down	✎ ✖
WAN DSL	Up	✎
WAN PPPoA	Waiting for Underlying Connection (WAN DSL - Up)	✎ ✖
WAN DSL	Up	✎
Mgmt ETHoA	Down	✎ ✖
WAN DSL	Up	✎
New Connection		+

LAN BRIDGE

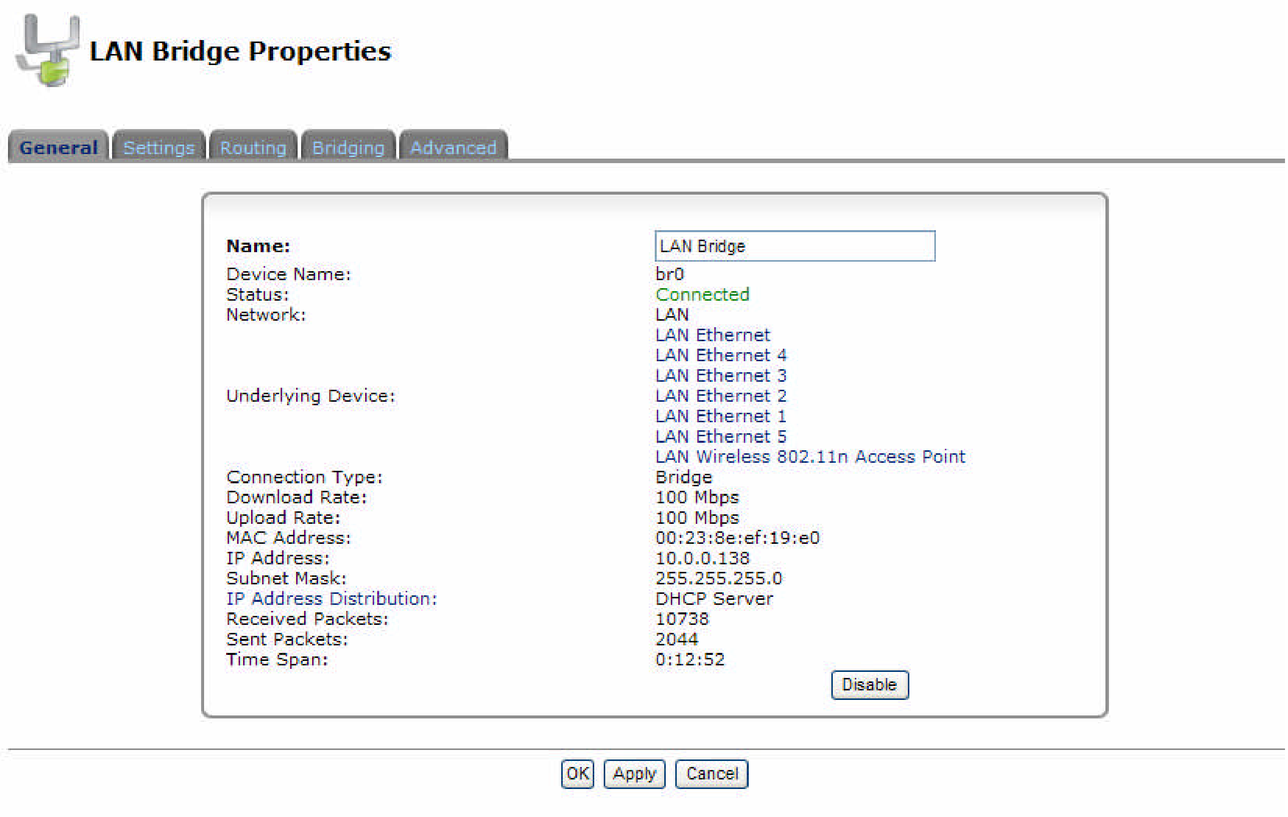
The LAN bridge connection is used to combine several LAN devices under one virtual network. For example, creating one network for LAN Ethernet and LAN wireless devices.

Please note, that when a bridge is removed, its formerly underlying devices inherit the bridge's DHCP settings. For example, the removal of a bridge that is configured as DHCP client, automatically configures the LAN devices formerly constituting the bridge as DHCP clients, with the exact DHCP client configuration.

LAN BRIDGE >> GENERAL

To view and edit the LAN bridge connection settings, click the 'LAN Bridge' link in the 'Network Connections' screen. The 'LAN Bridge Properties' screen will appear, displaying a detailed summary of the connection's parameters, under the 'General' tab. These parameters can be edited in the rest of the screen's tabs, as described in the following sections.

FIGURE 2. LAN Bridge >> General Panel



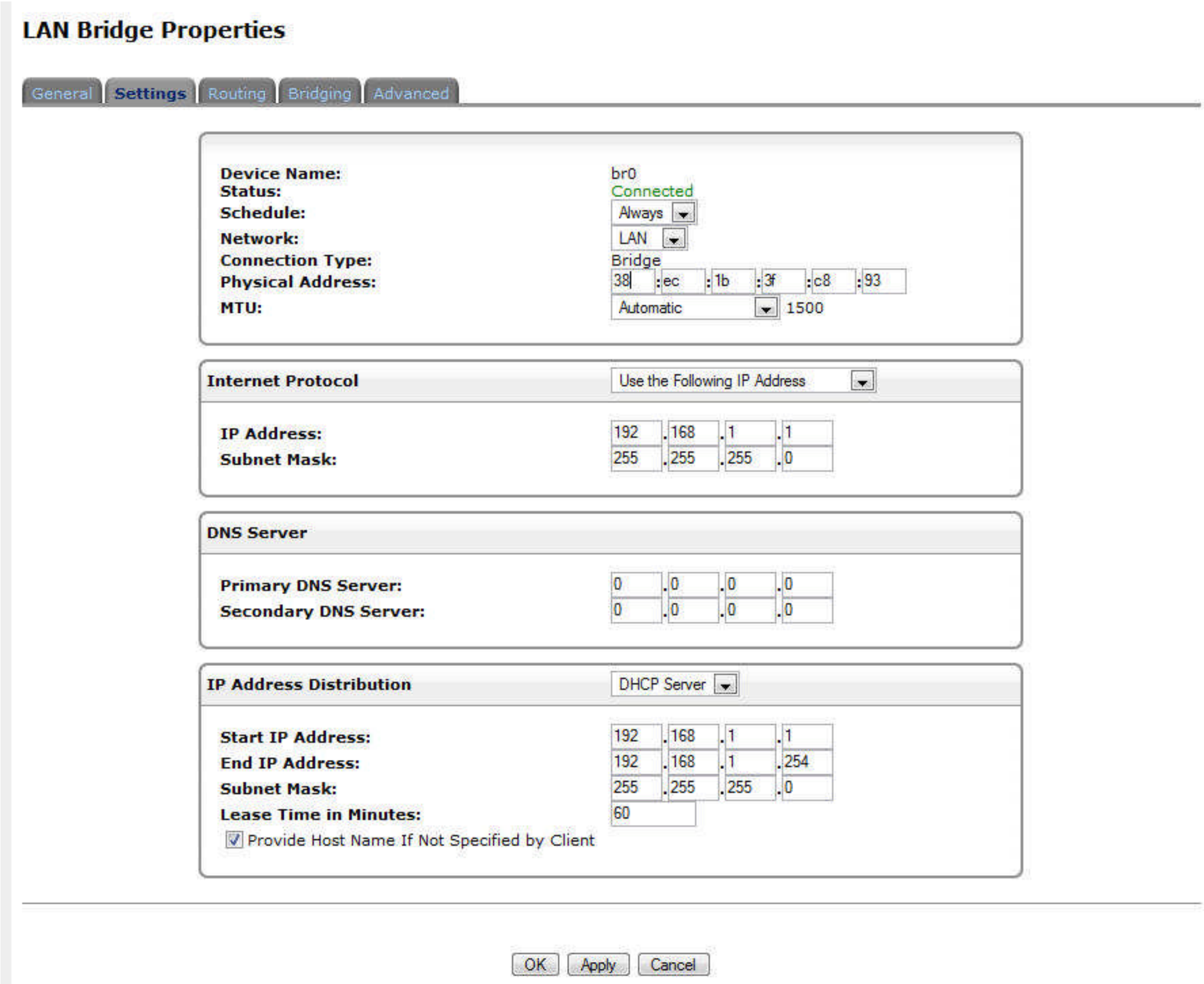
LAN Bridge Properties

Name:	LAN Bridge
Device Name:	br0
Status:	Connected
Network:	LAN
Underlying Device:	LAN Ethernet LAN Ethernet 4 LAN Ethernet 3 LAN Ethernet 2 LAN Ethernet 1 LAN Ethernet 5 LAN Wireless 802.11n Access Point
Connection Type:	Bridge
Download Rate:	100 Mbps
Upload Rate:	100 Mbps
MAC Address:	00:23:8e:ef:19:e0
IP Address:	10.0.0.138
Subnet Mask:	255.255.255.0
IP Address Distribution:	DHCP Server
Received Packets:	10738
Sent Packets:	2044
Time Span:	0:12:52

LAN BRIDGE >> SETTINGS

General. This section displays the connection's general parameters. It is recommended not to change the default values unless familiar with the networking concepts they represent. Since your gateway is configured to operate with the default values, no parameter modification is necessary.

FIGURE 3. **LAN Bridge >> Settings Panel**



LAN Bridge Properties

Device Name:	br0
Status:	Connected
Schedule:	Always
Network:	LAN
Connection Type:	Bridge
Physical Address:	38 : ec : 1b : 3f : c8 : 93
MTU:	Automatic 1500

Internet Protocol	Use the Following IP Address
IP Address:	192 . 168 . 1 . 1
Subnet Mask:	255 . 255 . 255 . 0

DNS Server

Primary DNS Server:	0 . 0 . 0 . 0
Secondary DNS Server:	0 . 0 . 0 . 0

IP Address Distribution	DHCP Server
Start IP Address:	192 . 168 . 1 . 1
End IP Address:	192 . 168 . 1 . 254
Subnet Mask:	255 . 255 . 255 . 0
Lease Time in Minutes:	60

☑ Provide Host Name If Not Specified by Client

Schedule. By default, the connection will always be active. However, you can configure scheduler rules in order to define time segments during which the connection may be active. Once a scheduler rule(s) is defined, this field changes to a combo-box, allowing you to choose between the available rules.

Network. Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the combo-box.

Physical Address. The physical address of the network card used for your network. Some cards allow you to change this address.

MTU. MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. In the default setting, Automatic, the gateway selects the best MTU for your Internet connection. Select "Automatic by DHCP" to have the DHCP determine the MTU. In case you select "Manual", it is recommended to enter a value in the 1200 to 1500 range.

Internet Protocol. Select one of the following Internet protocol options from the 'Internet Protocol' combo-box:

- *No IP Address*: Select 'No IP Address' if you require that your gateway have no IP address. This can be useful if you are working in an environment where you are not connected to other networks, such as the Internet.

- *Obtain an IP Address Automatically*: Your connection is configured by default to act as a DHCP client. You should keep this configuration in case your service provider supports DHCP, or if you are connecting using a dynamic IP address. The server that assigns the gateway with an IP address, also assigns a subnet mask. You can override the dynamically assigned subnet mask by selecting the 'Override Subnet Mask' and specifying your own mask instead. You can press the 'Release' button to release the current leased IP address. Once the address has been released, the button text changes to 'Renew'. Use the 'Renew' button to renew the leased IP address.

- *Use the Following IP Address*: Your connection can be configured using a permanent (static) IP address. Your service provider should provide you with such an IP address and subnet mask.

DNS Server. Domain Name System (DNS) Server is the method by which Web site domain names are translated into IP addresses. You can configure the connection to automatically obtain a DNS server address, or specify such an address manually, according to the information provided by your ISP. If you have previously chosen “Obtain an IP Address Automatically”, a combo-box will appear.
To configure the connection to automatically obtain a DNS server address, select 'Obtain DNS Server Address Automatically' from the 'DNS Server' drop down menu.
To manually configure DNS server addresses, select 'Use the Following DNS Server Addresses' from the 'DNS Server' drop down menu. Specify up to two different DNS server address, one primary, another secondary.

IP Address Distribution. The 'IP Address Distribution' section allows you to configure the gateway's Dynamic Host Configuration Protocol (DHCP) server parameters. The DHCP automatically assigns IP addresses to network PCs. If you enable this feature, make sure that you also configure your network PCs as DHCP clients. Select one of the following options from the 'IP Address Distribution' combo-box:

DHCP Server.

Start IP Address: The first IP address that may be assigned to a LAN host. Since the gateway's default IP address is 192.168.1.1, this address must be 192.168.1.2 or greater.

End IP Address: The last IP address in the range that can be used to automatically assign IP addresses to LAN hosts.

Subnet Mask: A mask used to determine to what subnet an IP address belongs. An example of a subnet mask value is 255.255.255.0.

Lease Time In Minutes: Each device will be assigned an IP address by the DHCP server for this amount of time, when it connects to the network. When the lease expires the server will determine if the computer has disconnected from the network. If it has, the server may reassign this IP address to a newly-connected computer. This feature ensures that IP addresses that are not in use will become available for other computers on the network.

Provide Host Name if Not Specified by Client: If the DHCP client does not have a host name, the gateway will automatically assign one for him.

DHCP Relay. Your gateway can act as a DHCP relay in case you would like to dynamically assign IP addresses from a DHCP server other than your gateway's DHCP server. Note that when selecting this option you must also change Router's WAN to work in routing mode.

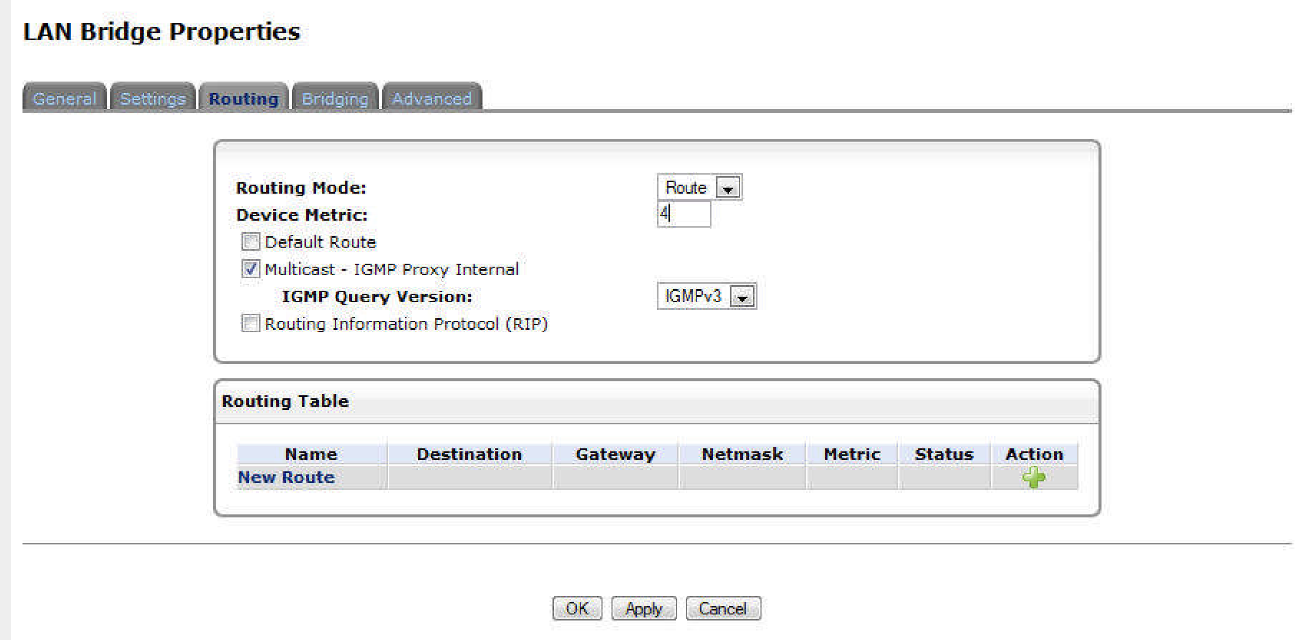
1. After selecting 'DHCP Relay' from the drop down menu, a 'New IP Address' link will appear: Click the 'New IP Address' link. The 'DHCP Relay Server Address' screen will appear.
2. Specify the IP address of the DHCP server.
3. Click 'OK' to save the settings.

Disabled. Select 'Disabled' from the combo-box if you would like to statically assign IP addresses to your network computers.

LAN BRIDGE >> ROUTING

You can choose to setup your gateway to use static or dynamic routing. Dynamic routing automatically adjusts how packets travel on the network, whereas static routing specifies a fixed routing path to neighboring destinations.

FIGURE 4. LAN Bridge >> Routing Panel



LAN Bridge Properties

Routing Mode: Route

Device Metric: 4

□ Default Route

☑ Multicast - IGMP Proxy Internal

IGMP Query Version: IGMPv3

□ Routing Information Protocol (RIP)

Routing Table

Name	Destination	Gateway	Netmask	Metric	Status	Action
New Route						✚

Routing Mode. Select one of the following routing modes:

- Route: Use route mode if you want your gateway to function as a router between two networks.
- NAPT: Network Address and Port Translation (NAPT) refers to network address translation involving the mapping of port numbers, allowing multiple machines to share a single IP address. Use NAPT if your LAN encompasses multiple devices, a topology that necessitates port translation in addition to address translation.

Device Metric. The device metric is a value used by the gateway to determine whether one route is superior to another, considering parameters such as bandwidth, delay, and more.

Default Route. Select this check box to define this device as a the default route.

Multicast - IGMP Proxy Internal. IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. IGMP proxy enables the routing of multicast packets according to the IGMP requests of LAN devices asking to join multicast groups. Select the 'Multicast IGMP Proxy Internal' check-box to enable this feature.

IGMP Query Version. If "*Multicast – IGMP Proxy Internal*" is enabled, this list box allows you to select all three versions of supported IGMP.

Routing Information Protocol (RIP). Select this check box to enable the Routing Information Protocol (RIP). RIP determines a route based on the smallest hop count between source and destination. When RIP is enabled, select the following:

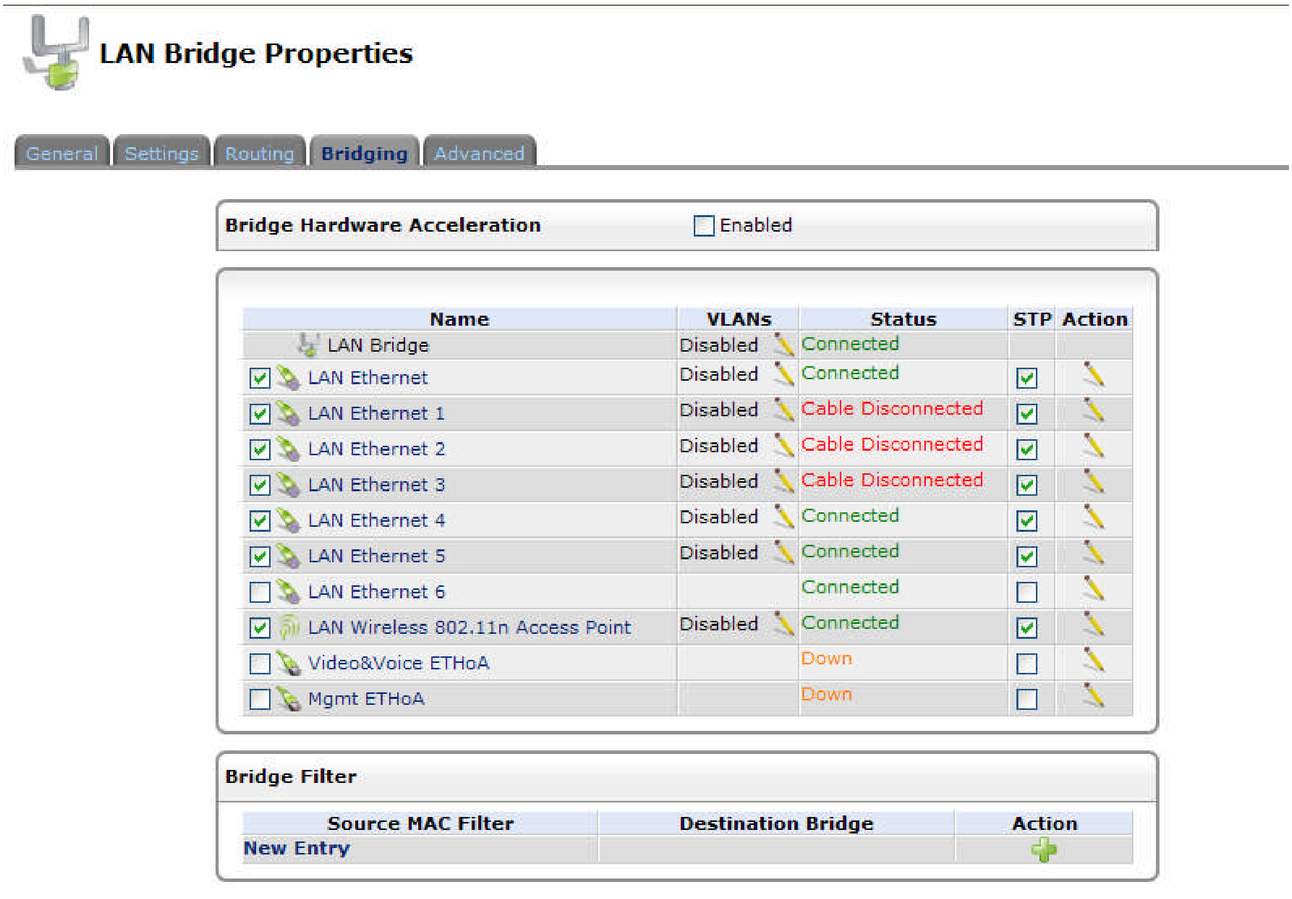
- Listen to RIP messages - select 'None', 'RIPv1', 'RIPv2' or 'RIPv1/2'.
- Send RIP messages - select 'None', 'RIPv1', 'RIPv2-broadcast' or 'RIPv2-multicast'.

Routing Table. Allows you to add or modify routes when this device is active. Use the 'New Route' button to add a route or edit existing routes.

LAN BRIDGE >> BRIDGING

This section allows you to specify the devices that you would like to join under the network bridge. Click the 'Edit' icon on the VLAN column to assign the network connections to specific virtual LANS.

FIGURE 5. LAN Bridge >> Bridging Panel



LAN Bridge Properties

Bridge Hardware Acceleration ☐ Enabled

Name	VLANs	Status	STP	Action
LAN Bridge	Disabled ✎	Connected		
☑ LAN Ethernet	Disabled ✎	Connected	☑	✎
☑ LAN Ethernet 1	Disabled ✎	Cable Disconnected	☑	✎
☑ LAN Ethernet 2	Disabled ✎	Cable Disconnected	☑	✎
☑ LAN Ethernet 3	Disabled ✎	Cable Disconnected	☑	✎
☑ LAN Ethernet 4	Disabled ✎	Connected	☑	✎
☑ LAN Ethernet 5	Disabled ✎	Connected	☑	✎
☐ LAN Ethernet 6		Connected	☐	✎
☑ LAN Wireless 802.11n Access Point	Disabled ✎	Connected	☑	✎
☐ Video&Voice ETHoA		Down	☐	✎
☐ Mgmt ETHoA		Down	☐	✎

Bridge Filter

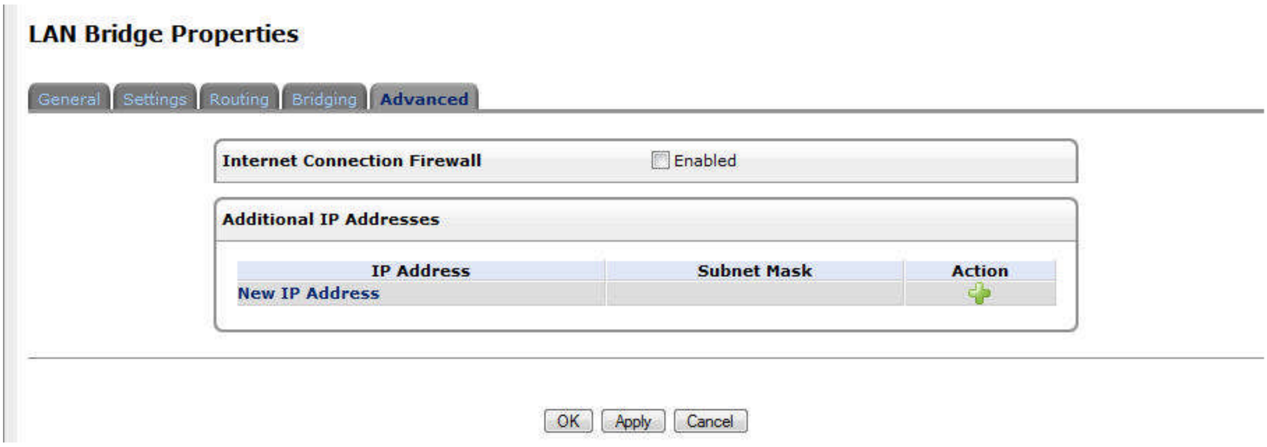
Source MAC Filter	Destination Bridge	Action
New Entry		✚

Select the 'STP' check box to enable the Spanning Tree Protocol on the device. You should use this to ensure that there are no loops in your network configuration, and apply these settings in case your network consists of multiple switches, or other bridges apart from those created by the gateway.

LAN BRIDGE >> ADVANCED

Internet Connection Firewall. Your gateway's firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network such as the Internet. The firewall can be activated per network connection. To enable the firewall on this network connection, select the 'Enabled' check box.

FIGURE 6. **LAN Bridge >> Advanced Panel**



LAN Bridge Properties

Internet Connection Firewall ☐ Enabled

Additional IP Addresses

IP Address	Subnet Mask	Action
New IP Address		✚

Additional IP Addresses. You can add alias names (additional IP addresses) to the gateway by clicking the 'New IP Address' link. This enables you to access the gateway using these aliases in addition to the 192.168.1.1

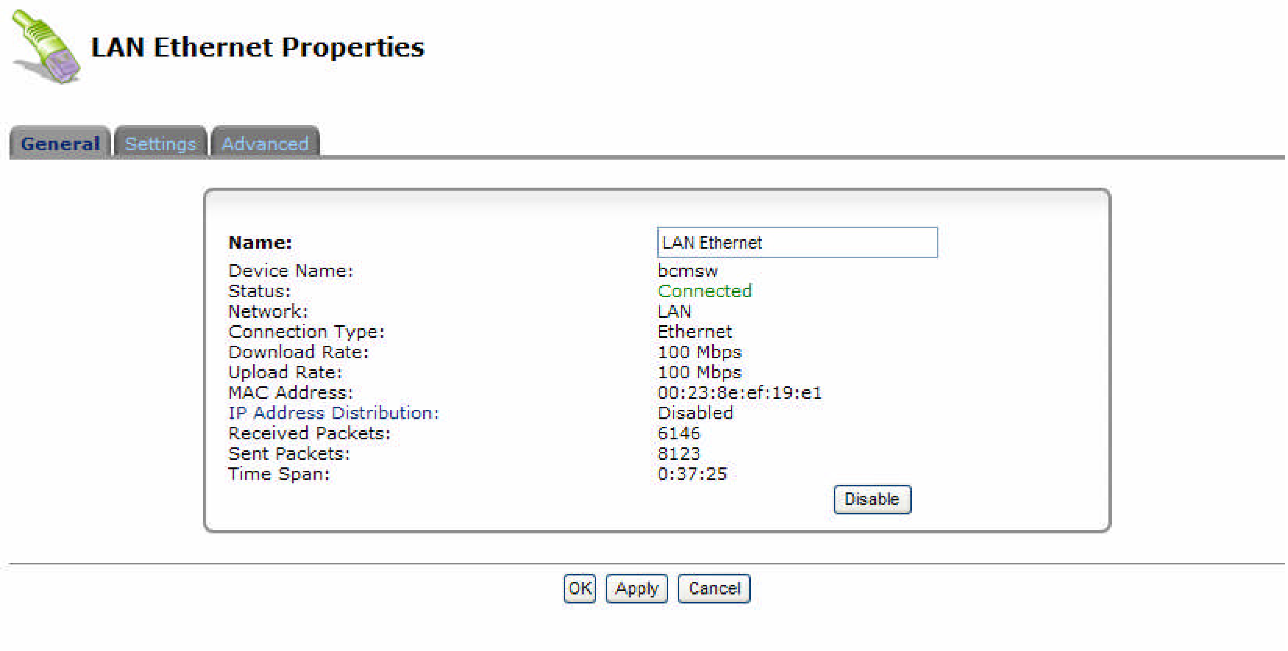
LAN ETHERNET

A LAN Ethernet connection connects computers to the Router using Ethernet cables.

LAN ETHERNET >> GENERAL

To view and edit the LAN Ethernet connection settings, click the 'LAN Ethernet' link in the 'Network Connections' screen. The 'LAN Ethernet Properties' screen will appear, displaying a detailed summary of the connection's parameters, under the 'General' tab. These parameters can be edited in the rest of the screen's tabs, as described in the following sections.

FIGURE 7. LAN Ethernet >> General Panel



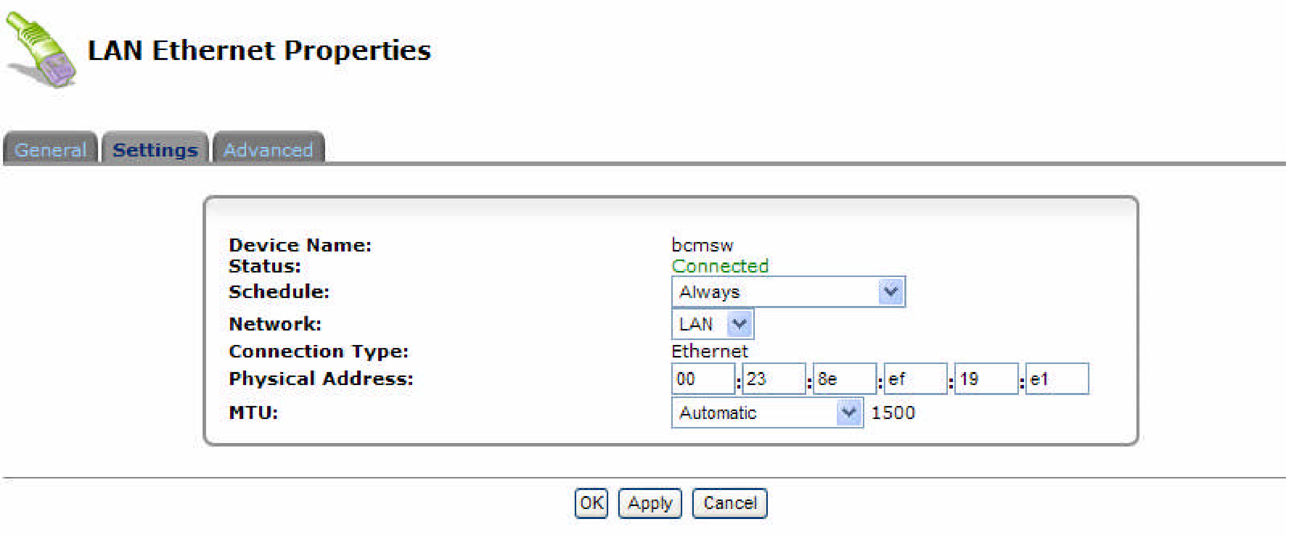
LAN Ethernet Properties

Name:	LAN Ethernet
Device Name:	bcmsw
Status:	Connected
Network:	LAN
Connection Type:	Ethernet
Download Rate:	100 Mbps
Upload Rate:	100 Mbps
MAC Address:	00:23:8e:ef:19:e1
IP Address Distribution:	Disabled
Received Packets:	6146
Sent Packets:	8123
Time Span:	0:37:25

LAN ETHERNET >> SETTINGS

General. This section displays the connection's general parameters. It is recommended not to change the default values unless familiar with the networking concepts they represent. Since your gateway is configured to operate with the default values, no parameter modification is necessary.

FIGURE 8. **LAN Ethernet >> Settings Panel**



LAN Ethernet Properties

Device Name:	bcmsw
Status:	Connected
Schedule:	Always
Network:	LAN
Connection Type:	Ethernet
Physical Address:	00 : 23 : 8e : ef : 19 : e1
MTU:	Automatic 1500

Network. Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the combo-box.

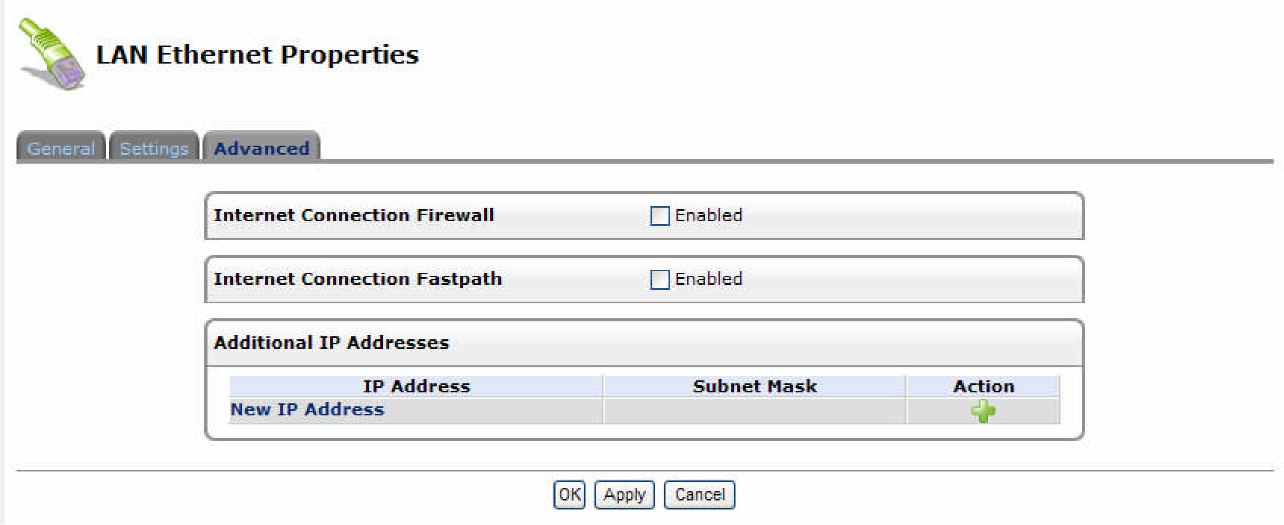
Physical Address. The physical address of the network card used for your network. Some cards allow you to change this address.

MTU. MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for the transmission. In the default setting, Automatic, the gateway selects the best MTU for your Internet connection. Select "Automatic by DHCP" to have the DHCP determine the MTU. In case you select "Manual", it is recommended to enter a value in the 1200 to 1500 range.

LAN ETHERNET >> ADVANCED

Internet Connection Firewall. Your gateway's firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network such as the Internet. The firewall can be activated per network connection. To enable the firewall on this network connection, select the 'Enabled' check box.

FIGURE 9. LAN Ethernet >> Advanced Panel



LAN Ethernet Properties

Internet Connection Firewall	□ Enabled
Internet Connection Fastpath	□ Enabled

Additional IP Addresses

IP Address	Subnet Mask	Action
New IP Address		✚

Additional IP Addresses. You can add alias names (additional IP addresses) to the gateway by clicking the 'New IP Address' link. This enables you to access the gateway using these aliases in addition to the 192.168.1.1

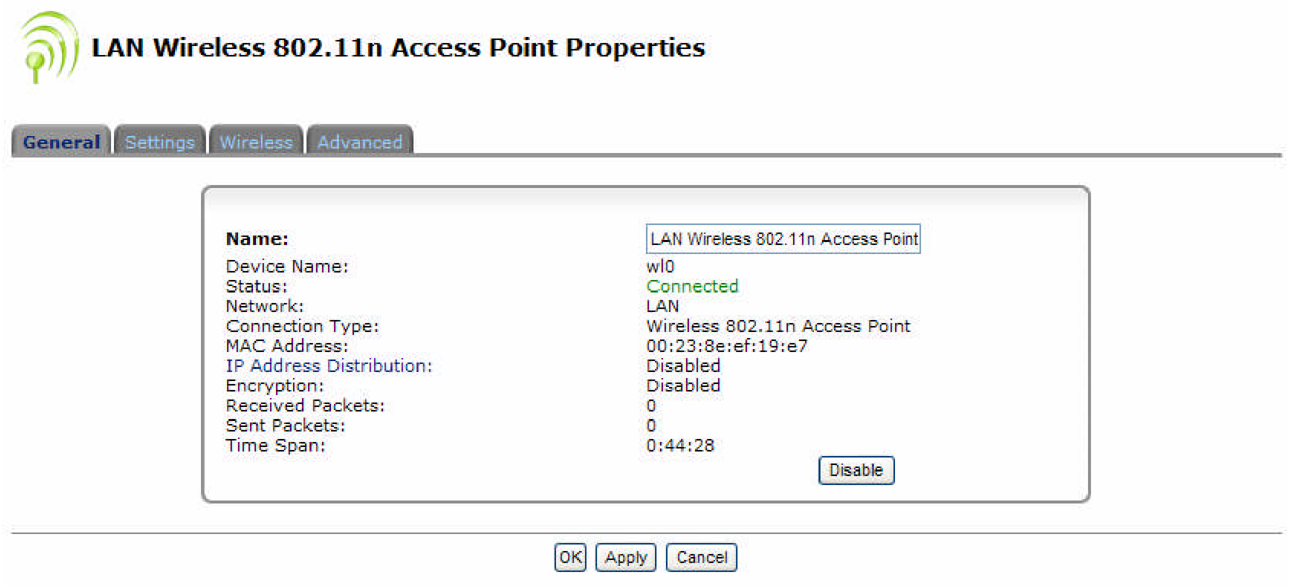
LAN WIRELESS 802.11N ACCESS POINT

PRG AV4202N integrates multiple layers of wireless security. These include the IEEE 802.1x port-based authentication protocol, RADIUS client, EAP-MD5, EAP-TLS, EAP-TTLS, EAP-PEAP, Wi-Fi Protected Access (WPA), WPA2, WPA and WPA2 (mixed mode) and industry leading Discus Firewall and VPN applications. In addition, the Router’s built-in authentication server enables home/SOHO users to define authorized wireless users without the need for an external RADIUS server.

LAN WIRELESS 802.11NN ACCESS POINT >> GENERAL

To view and edit the LAN Wireless connection settings, click the 'LAN Wireless 802.11n Access Point' link in the 'Network Connections' screen. The 'LAN Wireless 802.11n Access Point Properties' screen will appear, displaying a detailed summary of the connection's parameters, under the 'General' tab. These parameters can be edited in the rest of the screen's tabs, as described in the following sections.

FIGURE 10. LAN Wireless 802.11n Access Point >> General Panel



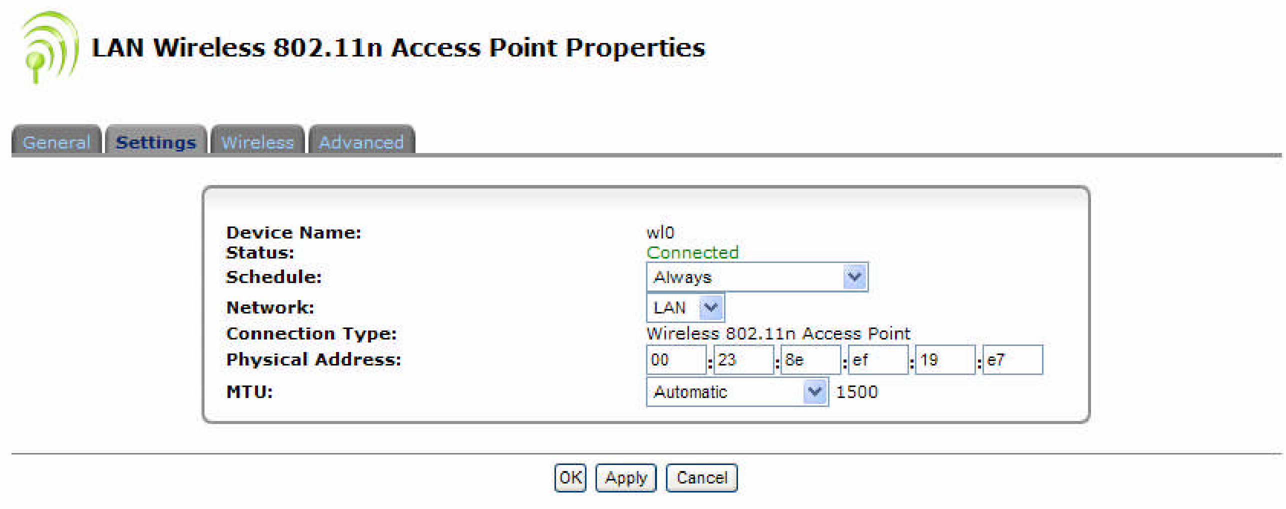
LAN Wireless 802.11n Access Point Properties

Name:	LAN Wireless 802.11n Access Point
Device Name:	wl0
Status:	Connected
Network:	LAN
Connection Type:	Wireless 802.11n Access Point
MAC Address:	00:23:8e:ef:19:e7
IP Address Distribution:	Disabled
Encryption:	Disabled
Received Packets:	0
Sent Packets:	0
Time Span:	0:44:28

LAN WIRELESS 802.11N ACCESS POINT >> SETTINGS

General. This section displays the connection's general parameters. It is recommended not to change the default values unless familiar with the networking concepts they represent. Since your gateway is configured to operate with the default values, no parameter modification is necessary.

FIGURE 11. LAN Wireless 802.11n Access Point >> Settings Panel



LAN Wireless 802.11n Access Point Properties

Device Name:	wl0
Status:	Connected
Schedule:	Always
Network:	LAN
Connection Type:	Wireless 802.11n Access Point
Physical Address:	00 : 23 : 8e : ef : 19 : e7
MTU:	Automatic 1500

Schedule. By default, the connection will always be active. However, you can configure scheduler rules in order to define time segments during which the connection may be active. Once a scheduler rule(s) is defined, this field changes to a combo-box, allowing you to choose between the available rules.

Network. Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the combo-box.

Physical Address. The physical address of the network card used for your network. Some cards allow you to change this address.

MTU. MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. In the default setting, Automatic, the gateway selects the best MTU for your Internet connection. Select "Automatic by DHCP" to have the DHCP determine the MTU. In case you select "Manual", it is recommended to enter a value in the 1200 to 1500 range.

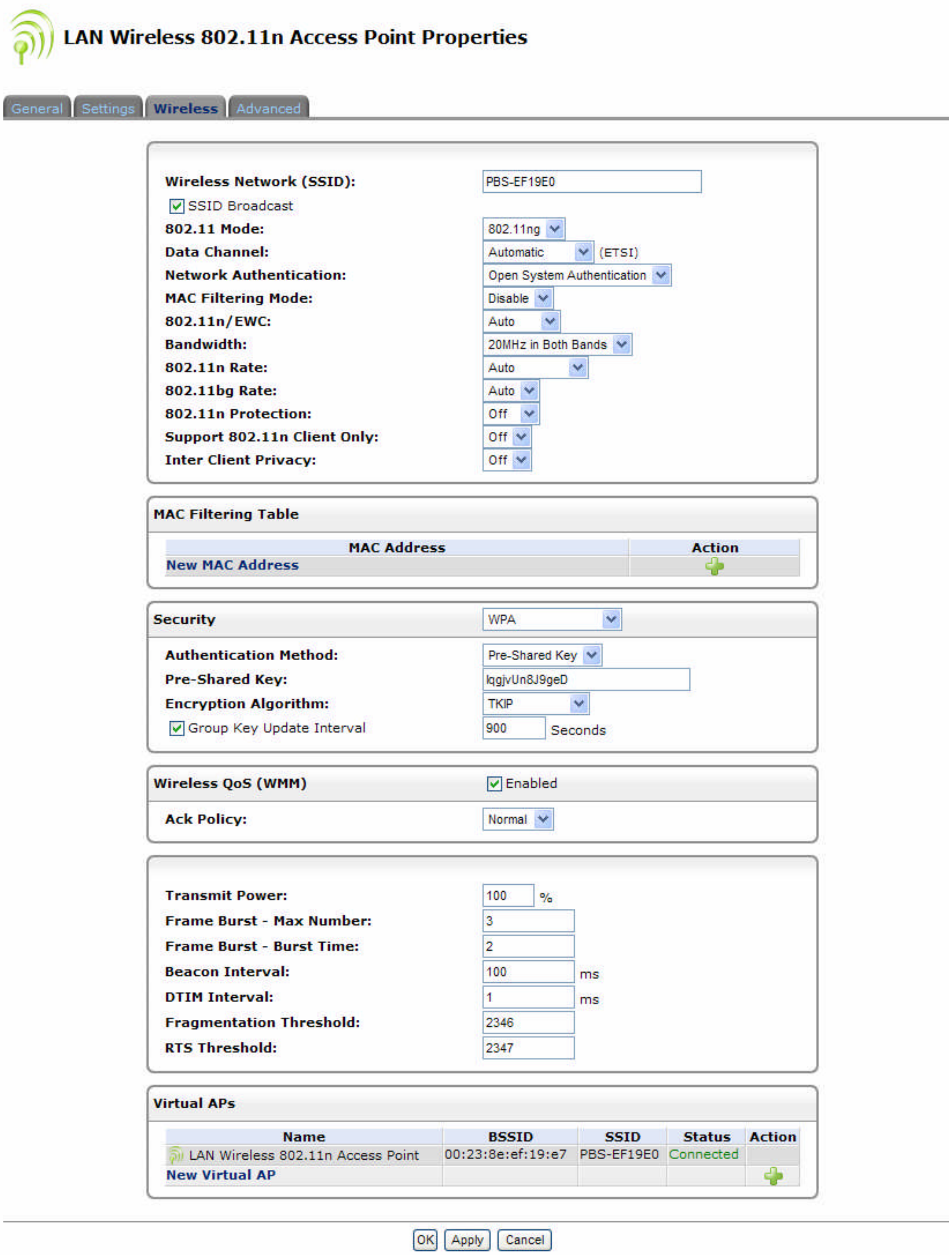
LAN WIRELESS 802.11N ACCESS POINT >> WIRELESS

Wireless Access Point

Use this section to define the basic wireless access point settings.

SSID. The SSID is the network name shared among all points in a wireless network. The SSID must be identical for all points in the wireless network. It is case-sensitive and must not exceed 32 characters (use any of the characters on the keyboard). Make sure this setting is the same for all points in your wireless network. For added security, you should change the default SSID (openrg) to a unique name.

FIGURE 12. LAN Wireless 802.11n Access Point >> Wireless Panel



LAN Wireless 802.11n Access Point Properties

Wireless Network (SSID): PBS-EF19E0

☑ SSID Broadcast

802.11 Mode: 802.11ng

Data Channel: Automatic (ETSI)

Network Authentication: Open System Authentication

MAC Filtering Mode: Disable

802.11n/EWC: Auto

Bandwidth: 20MHz in Both Bands

802.11n Rate: Auto

802.11bg Rate: Auto

802.11n Protection: Off

Support 802.11n Client Only: Off

Inter Client Privacy: Off

MAC Filtering Table

MAC Address	Action
New MAC Address	✚

Security: WPA

Authentication Method: Pre-Shared Key

Pre-Shared Key: lqgjvUn8J9geD

Encryption Algorithm: TKIP

☑ Group Key Update Interval 900 Seconds

Wireless QoS (WMM) ☑ Enabled

Ack Policy: Normal

Transmit Power: 100 %

Frame Burst - Max Number: 3

Frame Burst - Burst Time: 2

Beacon Interval: 100 ms

DTIM Interval: 1 ms

Fragmentation Threshold: 2346

RTS Threshold: 2347

Virtual APs

Name	BSSID	SSID	Status	Action
LAN Wireless 802.11n Access Point	00:23:8e:ef:19:e7	PBS-EF19E0	Connected	
New Virtual AP				✚

SSID Broadcast. Select this check-box to enable the SSID's broadcast. SSID broadcast is used in order to hide the name of the AP (SSID) from clients that should not be aware to its existence.

802.11 Mode. Select the Wireless communication standard that is compatible with you PC's wireless card. You can work in either 802.11n, 802.11g or in mixed mode.

Country. Select the applying Country from the list box.

Channel. Select the appropriate channel from the list provided to correspond with your network settings. All devices in your wireless network must broadcast on different channels in order to function correctly. The channels available depend on the Regulatory Authority (stated in brackets) to which your gateway conforms.

Network Authentication. The WPA network authentication method is 'Open System Authentication', meaning that a network key is not used for authentication. When using the 802.1X WEP or Non-802.1X WEP security protocols, this field changes to a combo-box, offering the 'Shared Key Authentication' method (which uses a network key for authentication), or both methods combined.

MAC Filtering Mode. You can filter wireless users according to their MAC address, either allowing or denying access. Choose the action to be performed by selecting it from the drop down menu.

MAC Filtering Table

Use this section to define advanced wireless access point settings.

New MAC Address. Click this link to define filtering of MAC addresses. Enter the MAC address to be filtered and press the “OK” button. A MAC address list will appear, upon which the selected filtering action (allow/deny) will be performed.

Security

To configure your wireless security, enable this feature by checking its 'Enabled' check-box. The screen will refresh, displaying the wireless security options. Use the 'Stations Security Type' combo-box to select the type of security protocol for securing your wireless network. You may choose between WPA, WPA2, 802.1x WEP, and Non-802.1x WEP. The screen will refresh, presenting each protocol's configuration respectively.

WPA: WPA is a data encryption method for 802.11 wireless LANs.

Authentication Method. Select the authentication method you would like to use. You can choose between Pre-Shared Key and 802.1x.

Pre-Shared Key. This entry appears only if you had selected this authentication method. Enter your encryption key in the 'Pre-Shared Key' field. You can use either an ASCII or a Hex value by selecting the value type in the combo-box provided.

Encryption Algorithm. Select between Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES) for the encryption algorithm.

Group Key Update Interval. It defines the time interval in seconds for updating a group key.

WPA2: WPA2 is an enhanced version of WPA, and defines the 802.11i protocol.

Authentication Method. Select the authentication method you would like to use. You can choose between Pre-Shared Key and 802.1x.

Pre-Shared Key. This entry appears only if you had selected this authentication method. Enter your encryption key in the 'Pre-Shared Key' field. You can use either an ASCII or a Hex value by selecting the value type in the combo-box provided.

Encryption Algorithm. The encryption algorithm used for WPA2 is the Advanced Encryption Standard (AES).

Group Key Update Interval. It defines the time interval in seconds for updating a group key.

WPA and WPA2 Mixed Mode: WPA and WPA2 is a mixed data encryption method.

Authentication Method. Select the authentication method you would like to use. You can choose between Pre-Shared Key and 802.1x.

Pre-Shared Key. This entry appears only if you had selected this authentication method. Enter your encryption key in the 'Pre-Shared Key' field. You can use either an ASCII or a Hex value by selecting the value type in the combo-box provided.

Encryption Algorithm. The encryption algorithm used for WPA and WPA2 is a either the Temporal Key Integrity Protocol (TKIP) or the Advanced Encryption Standard (AES).

Group Key Update Interval. It defines the time interval in seconds for updating a group key.

802.1x WEP: 802.1x WEP is a data encryption method utilizing a statically or automatically defined key for wireless clients that use 802.1x for authentication and WEP for encryption. You may define up to four keys but use only one at a time.

Generate Keys Automatically. Select this option to generate the encryption keys automatically rather than entering them manually. The screen will refresh, hiding the table of keys described below.

Group Key Update Interval. Defines the time interval in seconds for updating a group key. Active Select the encryption key to be activated.

Encryption Key. Type the encryption key until the entire field is filled. The key cannot be shorter than the field's length.

Entry Method. Select the character type for the key: Hex or ASCII. Key Length Select the key length in bits: 40 or 104 bits.

Key Length. Select the key length in bits: 40 or 104 bits.

Non-802.1x WEP: Non-802.1xWEP is a data encryption method utilizing a statically-defined key for wireless clients that do not use 802.1x for authentication and WEP for encryption. This method's configuration is virtually identical to the 802.1x WEP method described above, excluding the automatic key generation and the group key update interval specification. Please refer to the 802.1x WEP section above when configuring this method. Remember that the static key must be defined in the wireless Windows client as well.

Wireless QoS (WMM)

Wi-Fi Multimedia (WMM) provides basic Quality of Service (QoS) features to IEEE 802.11 networks. If your wireless card supports WMM, enable this feature by checking its 'Enabled' check-box.

Upon enabling WMM, the highest priority is given to Voice packets, decreasing towards Background packets which receive the lowest priority.

In addition, you can control the reliability of traffic flow. By default, the 'Ack Policy' for each access category is set to "Normal", meaning that an acknowledge packet is returned for every packet received. This provides a more reliable transmission but increases traffic load, which decreases performance. You may choose to cancel the acknowledgement by selecting "No Ack" in the combo-box of each access category, thus changing the Ack policy. This can be useful for Voice, for example, where speed of transmission is important and packet loss is tolerable to a certain degree.

Virtual APs

You can set up multiple wireless LANs on **PRG AV4202N** , limited only to the number supported by your wireless card. Each wireless LAN is defined as an access point.

The 'Virtual APs' section displays the Router's physical wireless access point, on top of which virtual connections may be created. To create a virtual connection, click the 'New Virtual AP' link.

The new connection will also be added to the network connections list, and will be configurable like any other connection. You can change the connection's default name by clicking its Edit action icon and changing the SSID value in the 'Configure LAN Wireless 802.11n Access Point - Virtual AP' screen.

Wireless WDS

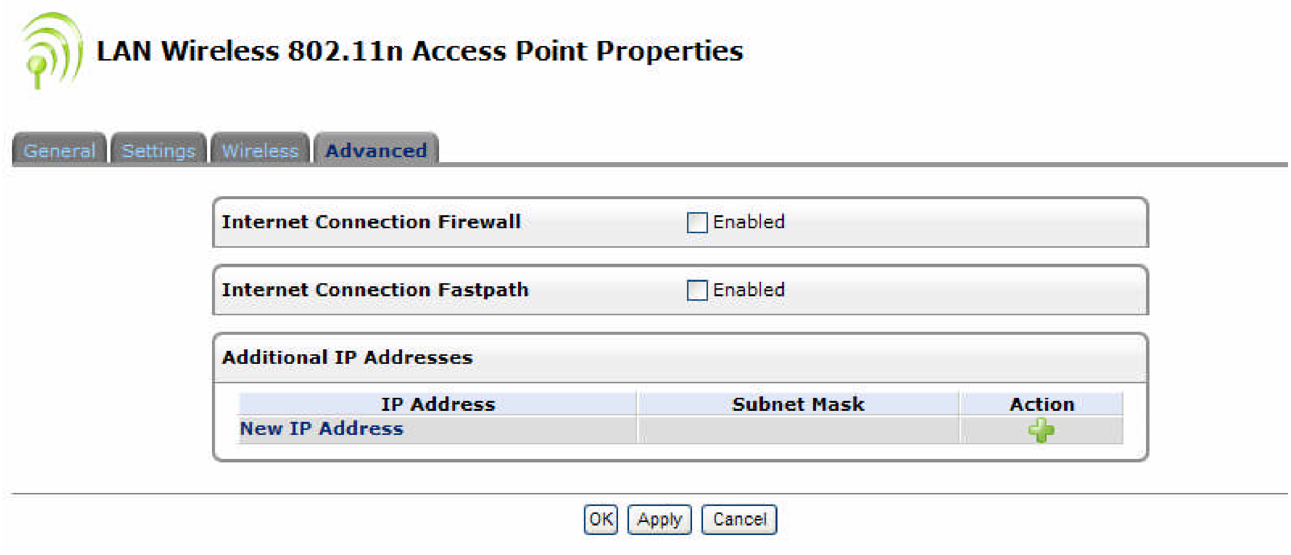
It enables wireless bridging of access points within its range. Virtual access points are used to interact with router's WDS peers, granting LAN users access to remote wireless networks.

When enabled, a WDS List box is shown.

LAN WIRELESS 802.11N ACCESS POINT >> ADVANCED

Internet Connection Firewall. Your gateway's firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network such as the Internet. The firewall can be activated per network connection. To enable the firewall on this network connection, select the 'Enabled' check box.

FIGURE 13. **LAN Wireless 802.11n Access Point >> Advanced Panel**



LAN Wireless 802.11n Access Point Properties

Internet Connection Firewall	☐ Enabled
Internet Connection Fastpath	☐ Enabled

Additional IP Addresses

IP Address	Subnet Mask	Action
New IP Address		✚

Additional IP Addresses. You can add alias names (additional IP addresses) to the gateway by clicking the 'New IP Address' link. This enables you to access the gateway using these aliases in addition to the 192.168.1.1

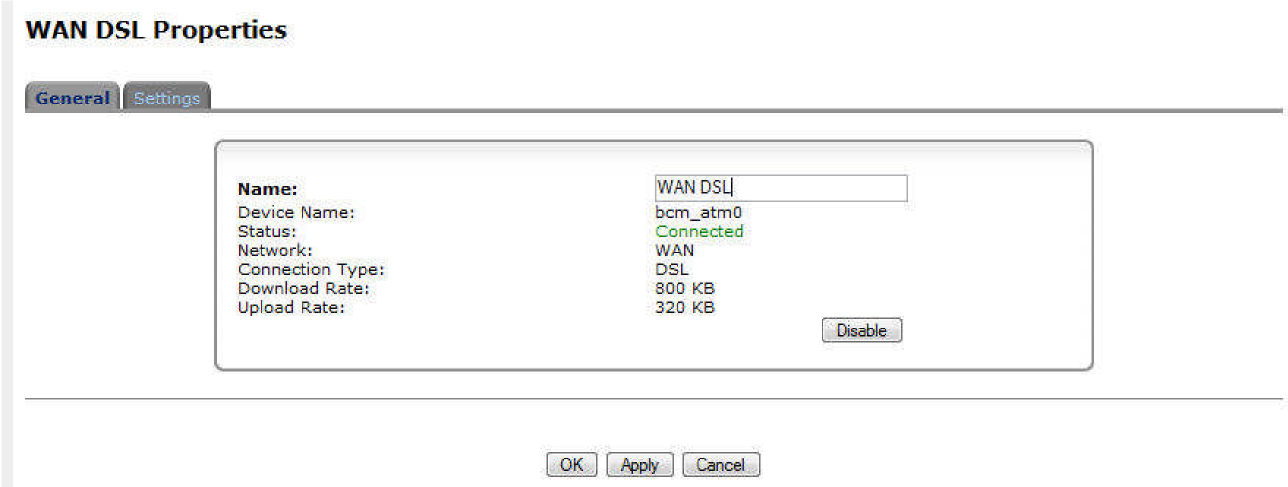
WAN DSL

The WAN DSL panels allows you to check and configure the WAN DSL line interface.

WAN DSL >> GENERAL

From the WAN DSL General panel, it is possible to enable/disable the WAN DSL interface and to set the WAN DSL friendly name.

FIGURE 14. WAN DSL >> General Panel



WAN DSL Properties

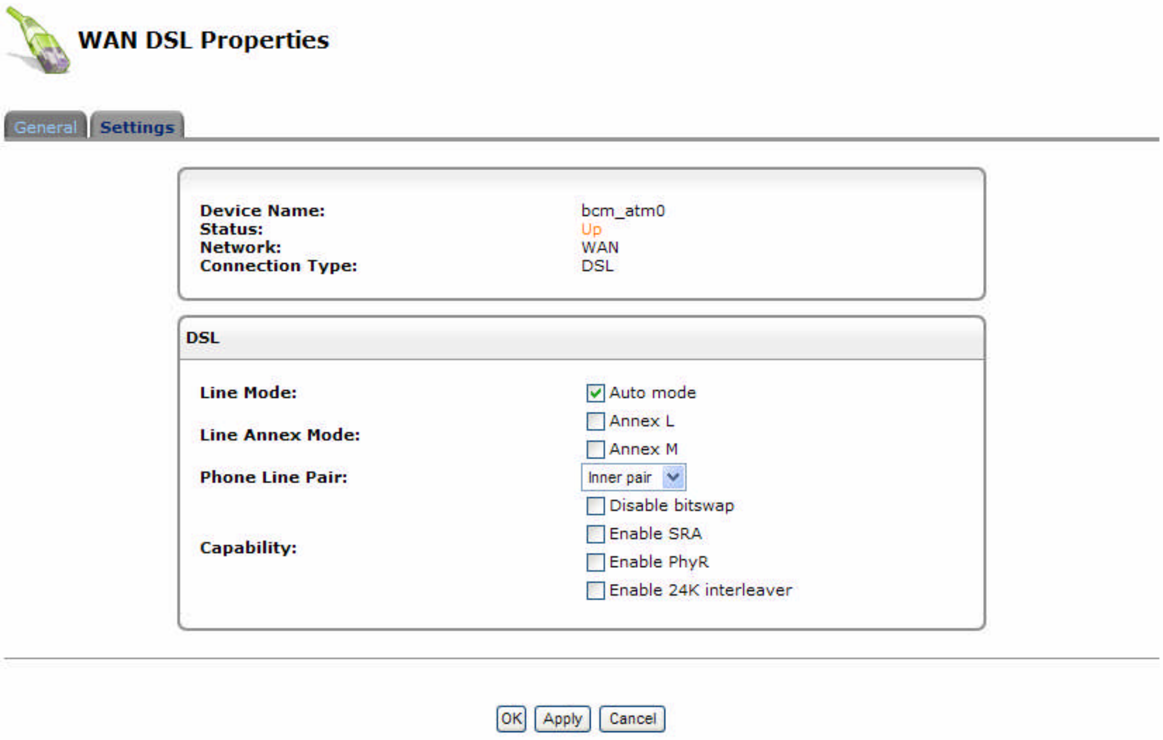
Name: WAN DSL
Device Name: bcm_atm0
Status: Connected
Network: WAN
Connection Type: DSL
Download Rate: 800 KB
Upload Rate: 320 KB

WAN DSL >> SETTINGS

From the WAN DSL Settings panel, it is possible to set the Line Mode.

FIGURE 15. WAN DSL >> Settings Panel

FIGURE 16. WAN DSL >> Settings Panel



WAN DSL Properties

Device Name: bcm_atm0
Status: Up
Network: WAN
Connection Type: DSL

DSL

Line Mode: ☑ Auto mode
Line Annex Mode: □ Annex L □ Annex M
Phone Line Pair: Inner pair
Capability: □ Disable bitswap □ Enable SRA □ Enable PhyR □ Enable 24K interleaver

Security Section

This chapter will describe the **Security Section** accessible from the *Home Page* of the **PRG AV4202N**.

Be aware that any configuration changes could compromise your connectivity.

The Router's gateway security suite includes comprehensive and robust security services: Stateful Packet Inspection Firewall, user authentication protocols and password protection mechanisms. These features together allow users to connect their computers to the Internet and simultaneously be protected from the security threats of the Internet.

The firewall has been exclusively tailored to the needs of the residential/office user and has been pre-configured to provide optimum security.

The Router's firewall provides both the security and flexibility that home and office users seek. It provides a managed, professional level of network security while enabling the safe use of interactive applications, such as Internet gaming and video-conferencing.

Additional features, including surfing restrictions and access control, can also be easily configured locally by the user through a user-friendly Web-based interface, or remotely by a service provider.

The Router firewall supports advanced filtering, designed to allow comprehensive control over the Firewall's behavior. You can define specific input and output rules, control the order of logically similar sets of rules and make a distinction between rules that apply to WAN and LAN network devices.

GENERAL

Use the 'General' screen to configure the gateway's basic security settings.

The firewall regulates the flow of data between the home network and the Internet. Both incoming and outgoing data are inspected and then either accepted (allowed to pass through the Router) or rejected (barred from passing through the Router) according to a flexible and configurable set of rules. These rules are designed to prevent unwanted intrusions from the outside, while allowing home users access to the Internet services that they require.

The firewall rules specify what types of services available on the Internet may be accessed from the home network and what types of services available in the home network may be accessed from the Internet. Each request for a service that the firewall receives, whether originating in the Internet or from a computer in the home network, is checked against the set of firewall rules to determine whether the request should be allowed to pass through the firewall. If the request is permitted to pass, then all subsequent data associated with this request (a “session”) will also be allowed to pass, regardless of its direction.

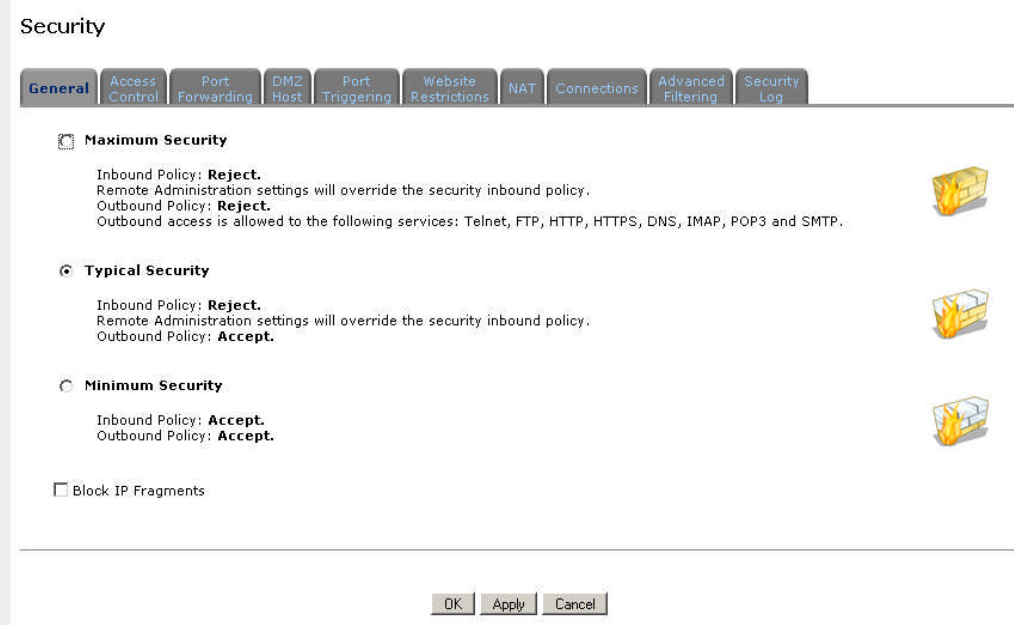
For example, when you point your Web browser to a Web page on the Internet, a request is sent out to the Internet for this page. When the request reaches the Router the firewall will identify the request type and origin - HTTP and a specific PC in your home network, in this case. Unless you have configured access control to block requests of this type from this computer, the firewall will allow this request to pass out onto the Internet. When the Web page is returned from the Web server the firewall will associate it with this session and allow it to pass, regardless of whether HTTP access from the Internet to the home network is blocked or permitted.

The important thing to note here is that it is the origin of the request, not subsequent responses to this request, that determines whether a session can be established or not. You may choose from among three pre-defined security levels for the Router: Minimum, Typical, and Maximum (the default setting). The table below summarizes the behavior of the Router for each of the three security levels.

TABLE 1. Security Levels

Security Level	Requests Originating in the WAN (Incoming Traffic)	Requests Originating in the LAN (Outgoing Traffic)
Maximum Security (Default)	*Blocked: no access to home network from Internet, except as configured in the Port Forwarding, DMZ host and Remote Access screens*	*Limited: by default, only commonly-used services, such as Web browsing and e-mail, are permitted*
Typical Security	*Blocked: no access to home network from Internet, except as configured in the Port Forwarding, DMZ host and Remote Access screens*	*Unrestricted: all services are permitted, except as configured in the Access Control screen*
Minimum Security	*Unrestricted: permits full access from Internet to home network; all connection attempts permitted.*	*Unrestricted: all services are permitted, except as configured in the Access Control screen*

FIGURE 1. Security General panel



○ **Maximum Security**

Inbound Policy: **Reject.**
Remote Administration settings will override the security inbound policy.
Outbound Policy: **Reject.**
Outbound access is allowed to the following services: Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3 and SMTP.

● **Typical Security**

Inbound Policy: **Reject.**
Remote Administration settings will override the security inbound policy.
Outbound Policy: **Accept.**

○ **Minimum Security**

Inbound Policy: **Accept.**
Outbound Policy: **Accept.**

□ Block IP Fragments

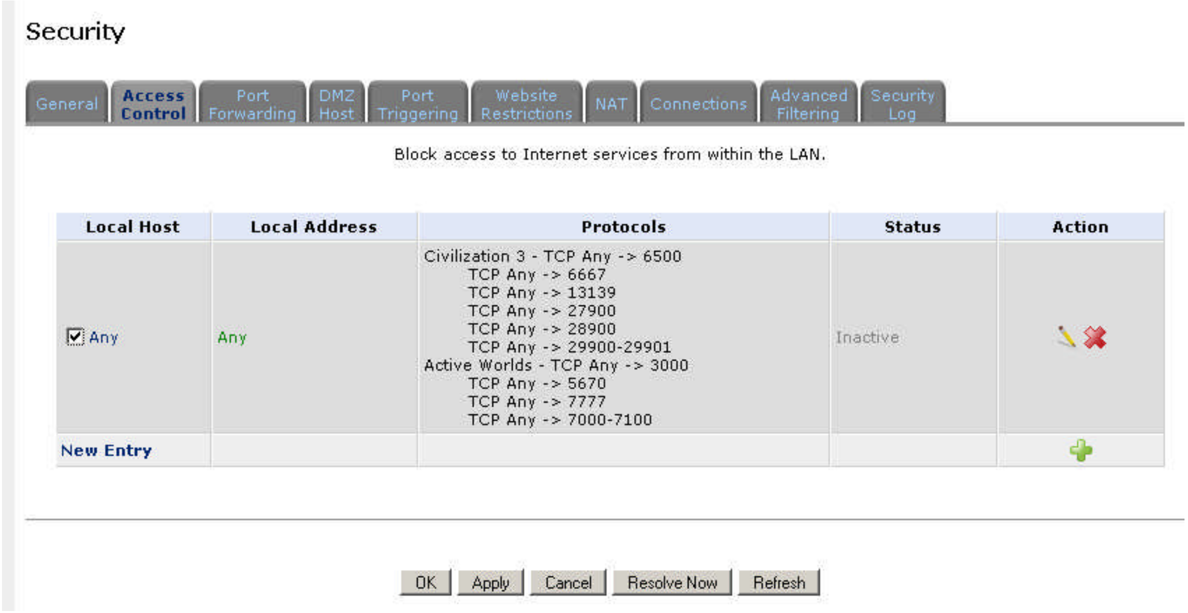
ACCESS CONTROL

You may want to block specific computers within the home network (or even the whole network) from accessing certain services on the Internet. For example, you may want to prohibit one computer from surfing the Web, another computer from transferring files using FTP, and the whole network from receiving incoming e-mail.

Access Control defines restrictions on the types of requests that may pass from the home network out to the Internet, and thus may block traffic flowing in both directions. It can also be used for allowing specific services when maximum security is configured. In the e-mail example given above, you may prevent computers in the home network from receiving e-mail by blocking their outgoing requests to POP3 servers on the Internet.

There are numerous services you should consider blocking, such as popular game and file sharing servers. For example, if you want to make sure that your employees do not put your business at risk from illegally traded copyright files, you may want to block several popular P2P and file sharing applications.

FIGURE 2. Access Control panel



Block access to Internet services from within the LAN.

Local Host	Local Address	Protocols	Status	Action
☑ Any	Any	Civilization 3 - TCP Any -> 6500 TCP Any -> 6667 TCP Any -> 13139 TCP Any -> 27900 TCP Any -> 28900 TCP Any -> 29900-29901 Active Worlds - TCP Any -> 3000 TCP Any -> 5670 TCP Any -> 7777 TCP Any -> 7000-7100	Inactive	✎ ✖
New Entry				✚

To allow or restrict services:

1. *Select the 'Access Control' tab in the 'Security' management screen. The 'Access Control' screen will appear.*
2. *Click the 'New Entry' link. The 'Add Access Control Rule' screen will appear*
3. *The Address combo-box provides you the ability to specify the computer or group of computers for which you would like to apply the access control rule. You can select between any, a specific computer in your LAN, or 'User De-*

fined'. If you choose the 'User Defined' option, the 'Edit Network Object' screen will appear. Specifying an address is done by creating a 'Network Object';

4. *The Protocol combo-box lets you select or specify the type of protocol that will be used. Selecting the 'Show All Services' option will expand the list of available protocols. Select a protocol or add a new one using the 'User Defined' option. This will commence a sequence that will add a new service, representing the protocol.*
5. *Select the 'Reply an HTML page to the blocked client' check-box to display the following message to the client: "Access Denied - this computer is not allowed to surf the WAN. Please contact your admin.". When this check-box is unselected, the client's packets will simply be ignored and he/she will not receive any notification.*
6. *The Schedule combo-box allows you to define the time period during which this rule will take effect. By default, the rule will always be active. However, you can configure scheduled rules by selecting 'User Defined'.*
7. *Click the 'OK' button to save your changes. The 'Access Control' screen will display a summary of the rule that you just added.*

PORT FORWARDING

In its default state, PRG AV4202N blocks all external users from connecting to or communicating with your network.

Therefore the system is safe from hackers who may try to intrude on the network and damage it. However, you may want to expose your network to the Internet in certain limited and controlled ways in order to enable some applications to work from the LAN (game, voice and chat applications, for example) and to enable Internet-access to servers in the home network. The Port Forwarding feature supports both of these functionalities. If you are familiar with networking terminology and concepts, you may have encountered this topic referred to as "Local Servers".

The 'Port Forwarding' screen lets you define the applications that require special handling by the Router.

All you have to do is select the application's protocol and the local IP address of the computer that will be using or providing the service. If required, you may add new protocols in addition to the most common ones provided by the Router.

For example, if you wanted to use a File Transfer Protocol (FTP) application on one of your PCs, you would simply select 'FTP' from the list and enter the local IP address or host name of the designated computer.

All FTP-related data arriving at the Router from the Internet will henceforth be forwarded to the specified computer. Similarly, you can grant Internet users access to servers inside your home network, by identifying each service and the PC that will provide it. This is useful, for example, if you want to host a Web server inside your home network. When an Internet user points his/her browser to the Router's external IP address, the gateway will forward the incoming HTTP request to your Web server.

With one external IP address (Router's main IP address), different applications can be assigned to your LAN computers, however each type of application is limited to use one computer. For example, you can define that FTP will use address X to reach computer A and Telnet will also use address X to reach computer A, but attempting to define FTP to use address X to reach both computer A and B will fail. The Router therefore provides the ability to add additional public IP addresses to port forwarding rules, which you must first obtain from your ISP, and enter into the 'NAT IP Addresses Pool'. You will then be able to define FTP to use address X to reach computer A and address Y to reach computer B. Additionally, port forwarding enables you to redirect traffic to a different port instead of the one to which it was designated.

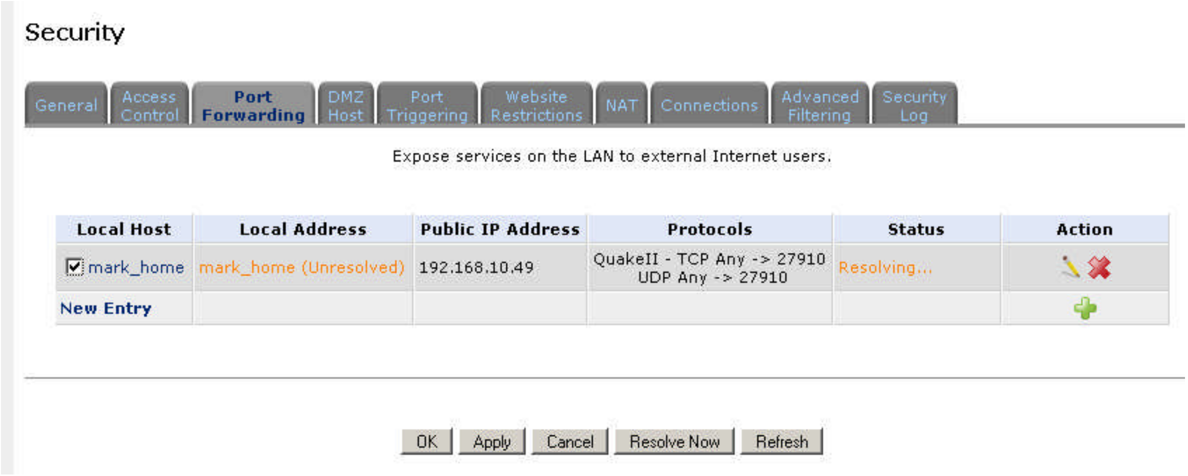
Lets say, that you have a Web server running on your PC on port 8080 and you want to grant access to this server to anyone who accesses the Router via HTTP. To accomplish this, do the following:

- Define a port forwarding rule for the HTTP service, with the PC's IP or host name.
- Specify 8080 in the 'Forward to Port' field.

All incoming HTTP traffic will now be forwarded to the PC running the Web server on port 8080.

When setting a port forwarding service, you must ensure that the port is not already in use by another application, which may stop functioning. A common example is when using SIP signaling in Voice over IP - the port used by the gateway's VoIP application (5060) is the same port on which port forwarding is set for LAN SIP agents.

FIGURE 3. Port Forwarding panel



Expose services on the LAN to external Internet users.

Local Host	Local Address	Public IP Address	Protocols	Status	Action
☑ mark_home	mark_home (Unresolved)	192.168.10.49	QuakeII - TCP Any -> 27910 UDP Any -> 27910	Resolving...	✎ ✖
New Entry					✚

To add a new port forwarding service:

1. *Select the 'Port Forwarding' tab in the 'Security' management screen. The 'Port Forwarding' screen will appear*
2. *Click the 'New Entry' link. The 'Add Port Forwarding Rule' screen will appear*
3. *Select the 'Specify Public IP Address' check-box if you would like to apply this rule on a specific external IP address. The screen will refresh*
4. *Enter the additional external IP address in the 'Public IP Address' field.*
5. *Enter the host name or IP address of the computer that will provide the service (the "server") in the 'Local Host' field. Note that unless an additional external IP address has been added, only one LAN computer can be assigned to provide a specific service or application.*
6. *The Protocol combo-box lets you select or specify the type of protocol that will be used. Selecting the 'Show All Services' option will expand the list of available protocols. Select a protocol or add a new one using the 'User Defined' option. This will commence a sequence that will add a new service, representing the protocol.*
7. *By default, the Router will forward traffic to the same port as the incoming port. If you wish to redirect traffic to a different port, select the 'Specify' option. The screen will refresh, and an additional field will appear enabling you to enter the port number.*
8. *The Schedule combo-box allows you to define the time period during which this rule will take effect. By default, the rule will always be active. However, you can configure scheduled rules by selecting 'User Defined'.*
9. *Click the 'OK' button to save your changes. The 'Port Forwarding' screen will display a summary of the rule that you just added.*

DMZ HOST

The DMZ (Demilitarized) Host feature allows one local computer to be exposed to the Internet.

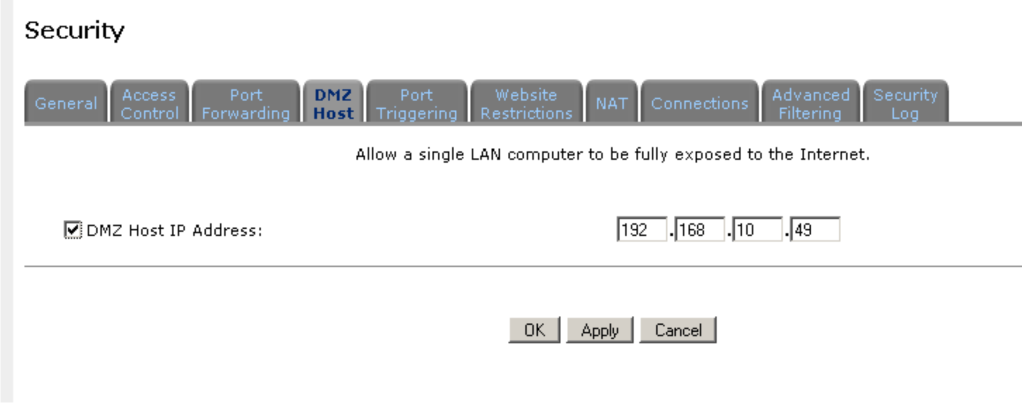
Designate a DMZ host when:

- You wish to use a special-purpose Internet service, such as an on-line game or video-conferencing program, that is not present in the Port Forwarding list and for which no port range information is available.
- You are not concerned with security and wish to expose one computer to all services without restriction.

⚠ *A DMZ host is not protected by the firewall and may be vulnerable to attack. Designating a DMZ host may also put other computers in the home network at risk. When designating a DMZ host, you must consider the security implications and protect it if necessary.*

An incoming request for access to a service in the home network, such as a Web-server, is handled by the Router. PRG AV4202N will forward this request to the DMZ host (if one is designated) unless the service is being provided by another PC in the home network (assigned in Port Forwarding), in which case that PC will receive the request instead.

FIGURE 4. DMZ Host panel



Allow a single LAN computer to be fully exposed to the Internet.

☑ DMZ Host IP Address: 192 . 168 . 10 . 49

To designate a local computer as a DMZ Host:

1. Select the 'DMZ Host' tab in the 'Security' management screen. The 'DMZ Host' screen will appear
2. Enter the local IP address of the computer that you would like to designate as a DMZ host, and select the check-box. Note that only one LAN computer may be a DMZ host at any time.
3. Click 'OK' to save the settings.

PORT TRIGGERING

Port triggering can be used for dynamic port forwarding configuration. By setting port triggering rules, you can allow inbound traffic to arrive at a specific LAN host, using ports different than those used for the outbound traffic. This is called port triggering since the outbound traffic triggers to which ports inbound traffic is directed.

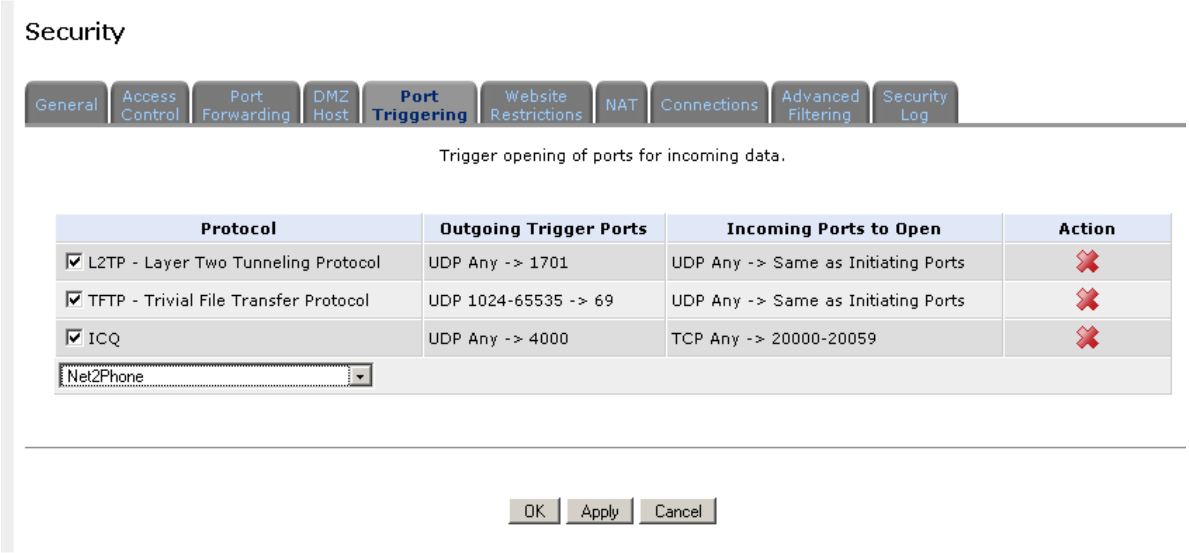
For example, consider a gaming server that is accessed using UDP protocol on port 2222. The gaming server responds by connecting the user using UDP on port 3333 when starting gaming sessions. In such a case you must use port triggering, since this scenario conflicts with the following default firewall settings:

- The firewall blocks inbound traffic by default.
- The server replies to the Router's IP, and the connection is not sent back to your host, since it is not part of a session.

In order to solve this you need to define a Port Triggering entry, which allows inbound traffic on UDP port 3333, only after a LAN host generated traffic to UDP port 2222. This will result in accepting the inbound traffic from the gaming server, and sending it back to the LAN Host which originated the outgoing traffic to UDP port 2222.

Select the 'Port Triggering' tab in the 'Security' management screen. The 'Port Triggering' screen will appear.

FIGURE 5. Port Triggering panel



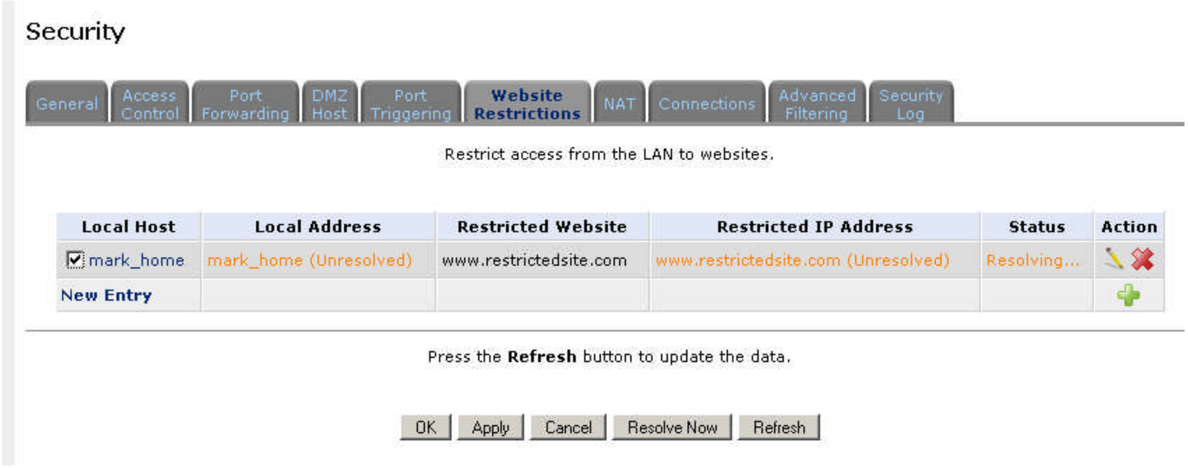
Trigger opening of ports for incoming data.

Protocol	Outgoing Trigger Ports	Incoming Ports to Open	Action
☑ L2TP - Layer Two Tunneling Protocol	UDP Any -> 1701	UDP Any -> Same as Initiating Ports	✖
☑ TFTP - Trivial File Transfer Protocol	UDP 1024-65535 -> 69	UDP Any -> Same as Initiating Ports	✖
☑ ICQ	UDP Any -> 4000	TCP Any -> 20000-20059	✖
Net2Phone			

WEB SITE RESTRICTIONS

You may configure the Router to block specific Internet web sites so that they cannot be accessed from computers in the home network. Moreover, restrictions can be applied to a comprehensive and automatically updated table of sites to which access is not recommended.

FIGURE 6. Web Site Restrictions panel



Restrict access from the LAN to websites.

Local Host	Local Address	Restricted Website	Restricted IP Address	Status	Action
☑ mark_home	mark_home (Unresolved)	www.restrictedsite.com	www.restrictedsite.com (Unresolved)	Resolving...	✎ ✖
New Entry					✚

Press the **Refresh** button to update the data.

To block access to a web site:

1. Click the 'Web Site Restrictions' tab in the 'Security' management screen
2. Click the 'New Entry' link. The 'Restricted Web Site' screen will appear
3. Enter the web site address (IP address or URL) that you would like to make inaccessible from your home network (all Web pages within the site will also be blocked). If the web site address has multiple IP addresses, the Router will resolve all additional addresses and automatically add them to the restrictions table.
4. The Local Host combo-box provides you the ability to specify the computer or group of computers for which you would like to apply the web site restriction. You can select between any, a specific computer in your LAN, or 'User Defined'. If you choose the 'User Defined' option, the 'Edit Network Object' screen will appear. Specifying an address is done by creating a 'Network Object'.
5. The Schedule combo-box allows you to define the time period during which this rule will take effect. By default, the rule will always be active. However, you can configure scheduled rules by selecting 'User Defined'.
6. Click 'OK' to save the settings.You will be returned to the previous screen while the Router attempts to find the site. 'Resolving ...' will appear in the Status column while the site is being located (the URL is 'resolved' into one or more IP addresses).

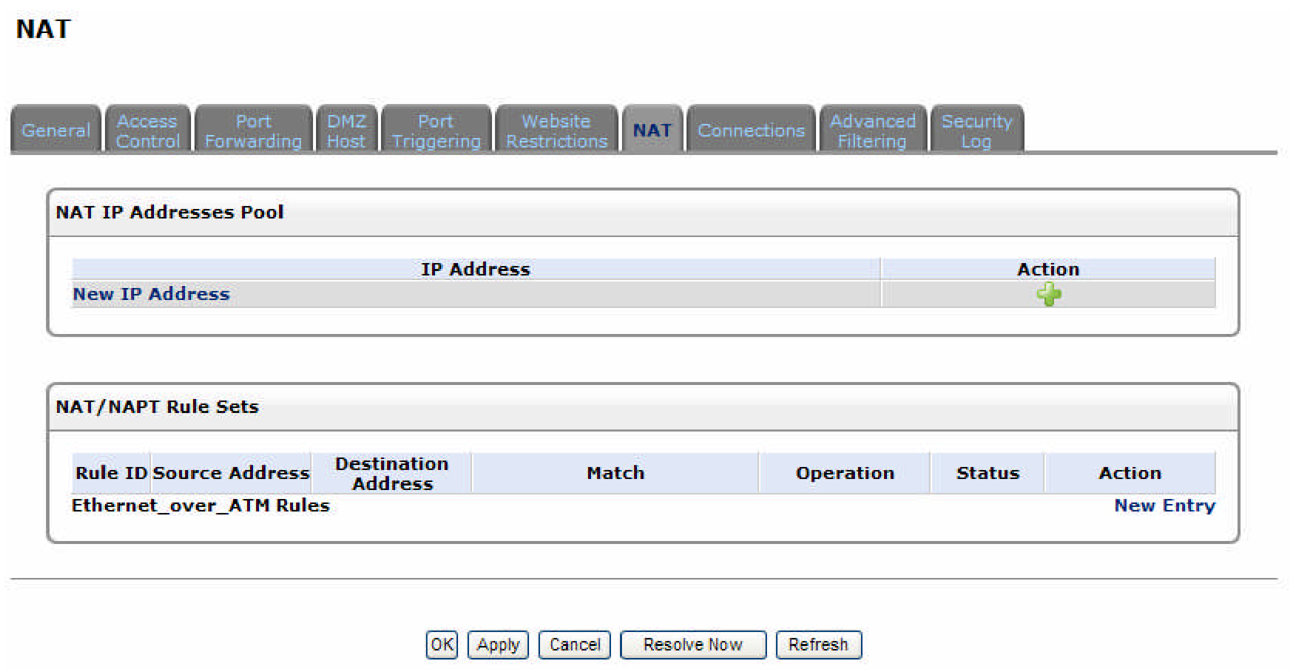
NAT

PRG AV4202N features a configurable Network Address Translation (NAT) and Network Address Port Translation (NAPT) mechanism, allowing you to control the network addresses and ports of packets routed through your gateway. When enabling multiple computers on your network to access the Internet using a fixed number of public IP addresses, you can statically define which LAN IP address will be translated to which NAT IP address and/or ports.

By default, the Router operates in NAPT routing mode. However, you can control your network translation by defining static NAT/NAPT rules. Such rules map LAN computers to NAT IP addresses.

The NAT/NAPT mechanism is useful for managing Internet usage in your LAN, or complying with various application demands. For example, you can assign your primary LAN computer with a single NAT IP address, in order to assure its permanent connection to the Internet. Another example is when an application server with which you wish to connect, such as a security server, requires that packets have a specific IP address - you can define a NAT rule for that address.

FIGURE 7. **NAT panel**



NAT IP Addresses Pool

IP Address	Action
New IP Address	+

NAT/NAPT Rule Sets

Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
Ethernet_over_ATM Rules						New Entry

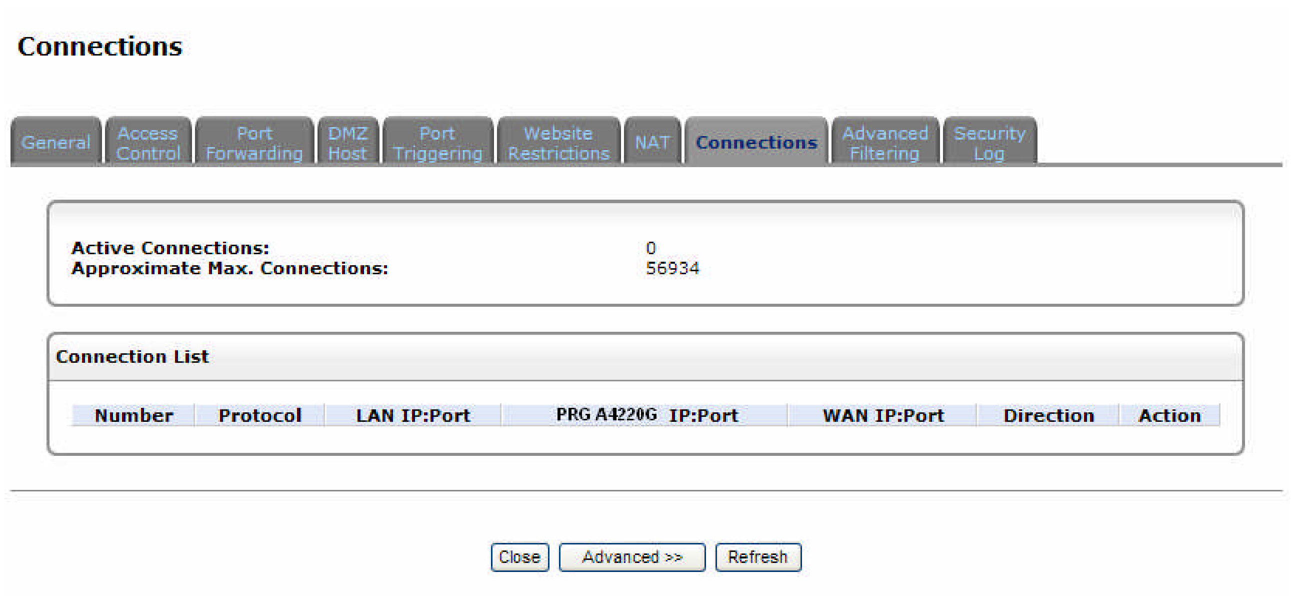
CONNECTIONS

The connection list displays all the connections that are currently open on the firewall, as well as various details and statistics. You can use this list to close undesired connections by clicking their Remove action icons. The basic display includes the name of the protocol, the different ports it uses, and the direction of traffic secured.

Press the 'Advanced' button to display a more detailed connection list, which includes the connection's time-to-live, number of kilo-bytes and packets received and transmitted, the device type and the routing mode.

Use the 'Connections Per Page' combo-box to select the number of connections to display at once. The 'Approximate Max. Connections' value represents the amount of additional concurrent connections possible.

FIGURE 8. Connections panel



Active Connections: 0
Approximate Max. Connections: 56934

Connection List

Number	Protocol	LAN IP:Port	PRG A4220G IP:Port	WAN IP:Port	Direction	Action

ADVANCED FILTERING

Advanced filtering is designed to allow comprehensive control over the Firewall's behavior. You can define specific input and output rules, control the order of logically similar sets of rules and make a distinction between rules that apply to WAN and LAN devices.

To view Router's advanced filtering options, click 'Advanced Filtering' under the 'Firewall' tab in the 'Services' screen. The 'Advanced Filtering' screen will appear.

This screen is divided into two identical sections, one for 'Input Rule Sets' and the other for 'Output Rule Sets', which are for configuring inbound and outbound traffic, respectively. Each section is comprised of subsets, which can be grouped into three main subjects:

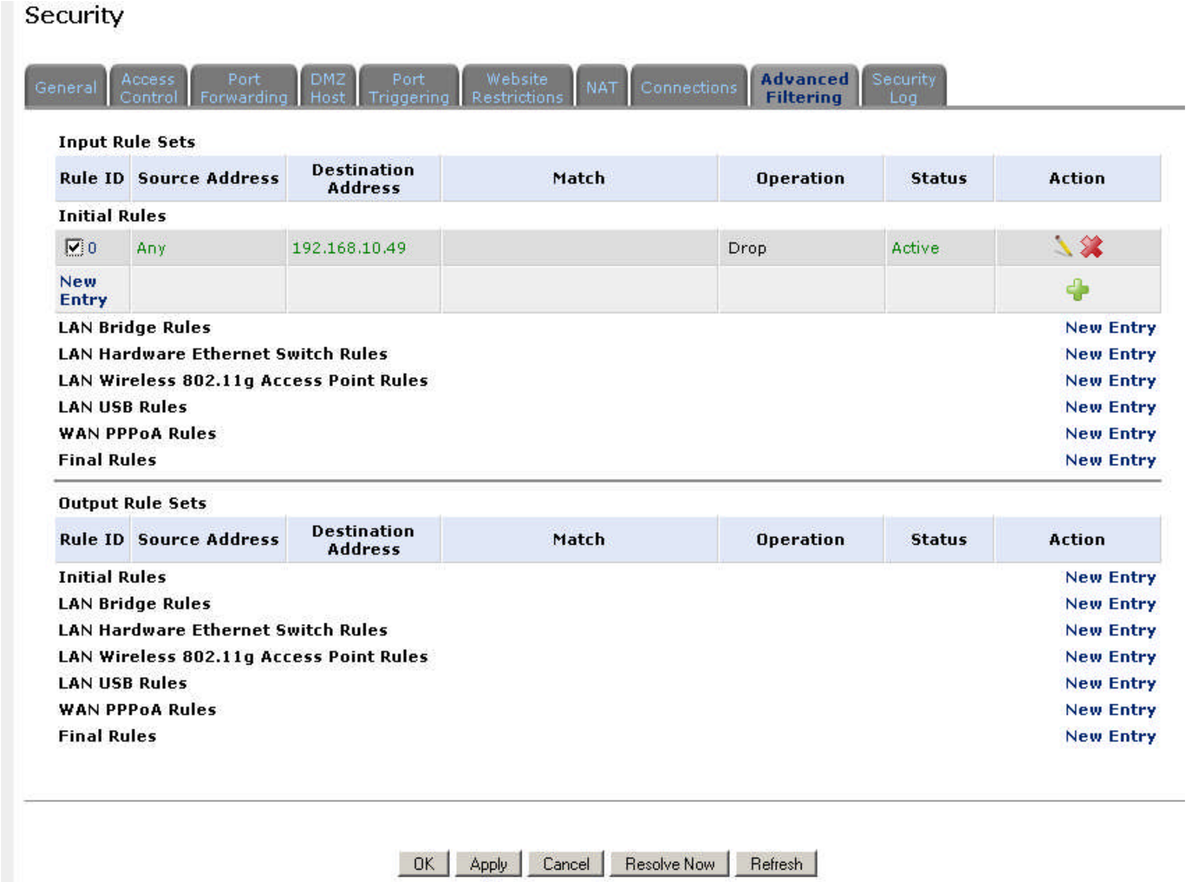
- Initial rules - rules defined here will be applied first, on all gateway devices.
- Network devices rules - rules can be defined per each gateway device.
- Final rules - rules defined here will be applied last, on all gateway devices.

The order of the rules' appearance represents both the order in which they were defined and the sequence by which they will be applied. You may change this order after your rules are already defined (without having to delete and then re-add them), by using the Move Up and Move Down action icons.

There are numerous rules automatically inserted by the firewall in order to provide improved security and block harmful attacks.

To add an advanced filtering rule, first choose the traffic direction and the device on which to set the rule. Then click the appropriate 'New Entry' link. The 'Add Advanced Filter' screen will appear: this screen is divided into two main sections, 'Matching' and 'Operation', which are for defining the operation to be executed when matching conditions apply.

FIGURE 9. Advanced Filtering panel



Security

Input Rule Sets

Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
Initial Rules						
☑ 0	Any	192.168.10.49		Drop	Active	✎ ✖
New Entry						✚
LAN Bridge Rules						New Entry
LAN Hardware Ethernet Switch Rules						New Entry
LAN Wireless 802.11g Access Point Rules						New Entry
LAN USB Rules						New Entry
WAN PPPoA Rules						New Entry
Final Rules						New Entry

Output Rule Sets

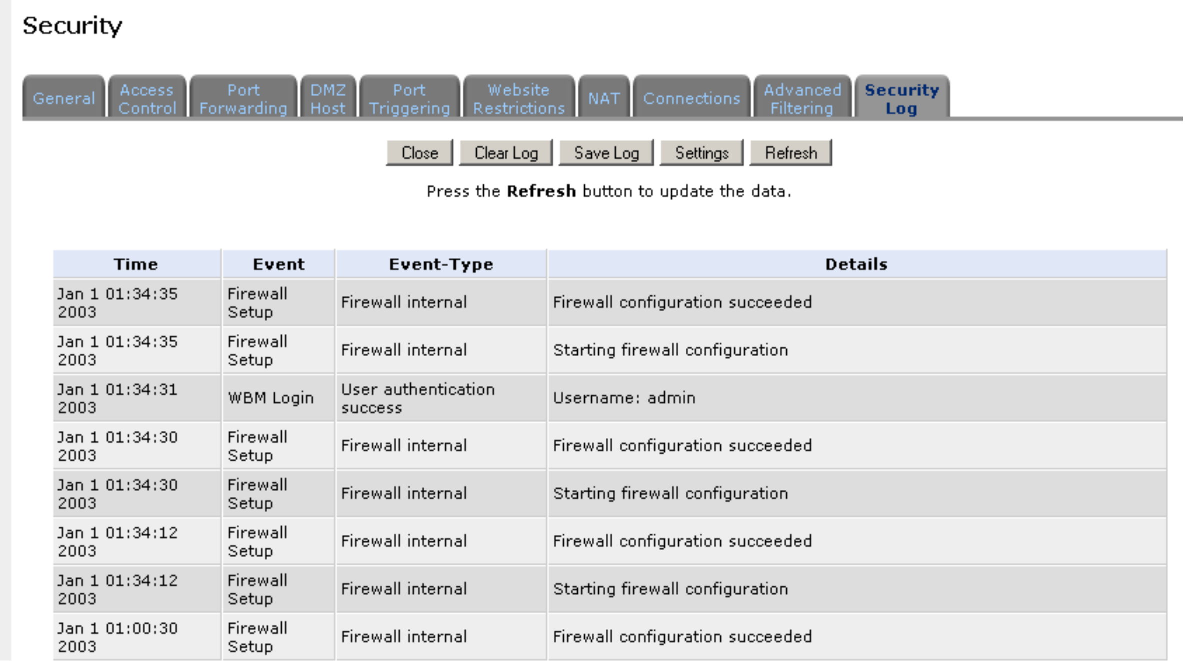
Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
Initial Rules						New Entry
LAN Bridge Rules						New Entry
LAN Hardware Ethernet Switch Rules						New Entry
LAN Wireless 802.11g Access Point Rules						New Entry
LAN USB Rules						New Entry
WAN PPPoA Rules						New Entry
Final Rules						New Entry

SECURITY LOG

The Security Log displays a list of firewall-related events, including attempts to establish inbound and outbound connections, attempts to authenticate through an administrative interface (Web-based management or Telnet terminal), firewall configuration and system start-up.

To view the security log, click the 'Security Log' tab in the 'Security' management screen. The 'Security Log' screen will appear.

FIGURE 10. **Security Log panel**



Press the **Refresh** button to update the data.

Time	Event	Event-Type	Details
Jan 1 01:34:35 2003	Firewall Setup	Firewall internal	Firewall configuration succeeded
Jan 1 01:34:35 2003	Firewall Setup	Firewall internal	Starting firewall configuration
Jan 1 01:34:31 2003	WBM Login	User authentication success	Username: admin
Jan 1 01:34:30 2003	Firewall Setup	Firewall internal	Firewall configuration succeeded
Jan 1 01:34:30 2003	Firewall Setup	Firewall internal	Starting firewall configuration
Jan 1 01:34:12 2003	Firewall Setup	Firewall internal	Firewall configuration succeeded
Jan 1 01:34:12 2003	Firewall Setup	Firewall internal	Starting firewall configuration
Jan 1 01:00:30 2003	Firewall Setup	Firewall internal	Firewall configuration succeeded

Time. The time the event occurred.

Event. There are five kinds of events:

- Inbound Traffic: The event is a result of an incoming packet.
- Outbound Traffic: The event is a result of outgoing packet.
- Firewall Setup: Configuration message.
- WBM Login: Indicates that a user has logged in to WBM.
- CLI Login: Indicates that a user has logged in to CLI (via Telnet).

Event-Type. A textual description of the event:

- Blocked: The packet was blocked. The message is colored red.
- Accepted: The packet was accepted. The message is colored green.

Details. More details about the packet or the event, such as protocol, IP addresses, ports, etc.

To view or change the security log settings, click the 'Settings' button that appears at the top of the 'Firewall Log' screen. The 'Security Log Settings' screen will appear allowing you to set the types of activities for which you would like to have a log message generated.

Voice over IP Section

This chapter will describe the **Voice over IP Section** accessible from the *Home Page* of the **PRG AV4202N**.

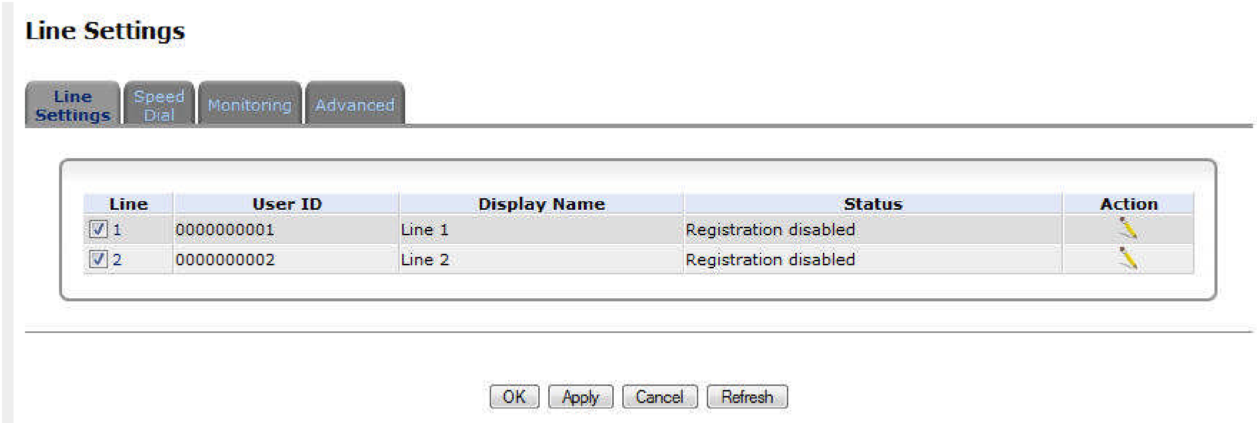
⚠ *Be aware that any configuration changes could compromise your connectivity.*

LINE SETTINGS

The Line Settings tab of the VoIP screen defines the phone ports of the Router and allows you to configure them.

1. Click the 'Voice Over IP' side-bar icon.
2. Click the 'Line Settings' tab, the following screen will appear. Before starting to make phone calls, you need to configure each line's parameters. You can manage which telephone is operational by marking the check-box next to it.

FIGURE 1. **Line Settings Panel**



Line Settings

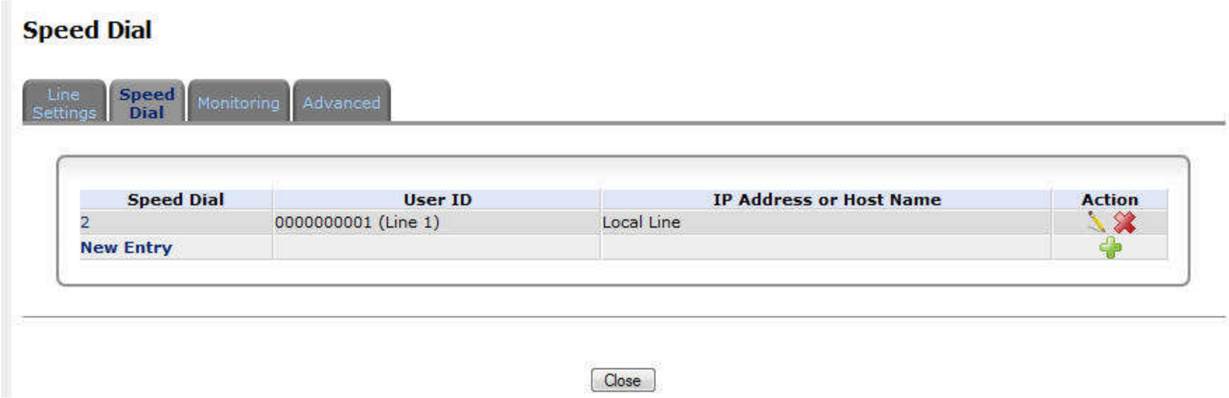
Line	User ID	Display Name	Status	Action
☑ 1	0000000001	Line 1	Registration disabled	✎
☑ 2	0000000002	Line 2	Registration disabled	✎

3. Click the edit action icon of each line to configure its different parameters.

SPEED DIAL

You can assign speed dial numbers to parties you frequently call. A speed dial entry must specify a destination which may be of one of three types: proxy, local line or direct call.

FIGURE 2. **Speed Dial Panel**



Speed Dial

Speed Dial	User ID	IP Address or Host Name	Action
2	0000000001 (Line 1)	Local Line	✎ ✖
New Entry			✚

Speed Dial via Proxy. To add a new proxy speed dial entry:

1. Click the 'Speed Dial' tab.
2. Click the 'New Entry' link to add a new speed dial entry. The 'Speed Dial Settings' screen will appear
3. Enter the following parameters:
   - Speed Dial: A shortcut number which you will dial to call this party.
   - Destination: The entry's destination, in this case a proxy server.
   - User ID: Specify the remote party's user ID.
4. Click 'OK' to save the settings.

Speed Dial via Local Line. To add a new local line speed dial entry:

1. Click the 'New Entry' link on the 'Speed Dial' tab and select the 'Local Line' option from the combo-box.
2. Enter the following parameters:
   - Speed Dial: A shortcut number which you will dial to call this party.
   - Destination: The entry's destination, in this case a local line.
   - Line: A combo-box will display your pre-defined local lines. Select the destination line.
3. Click 'OK' to save the settings.

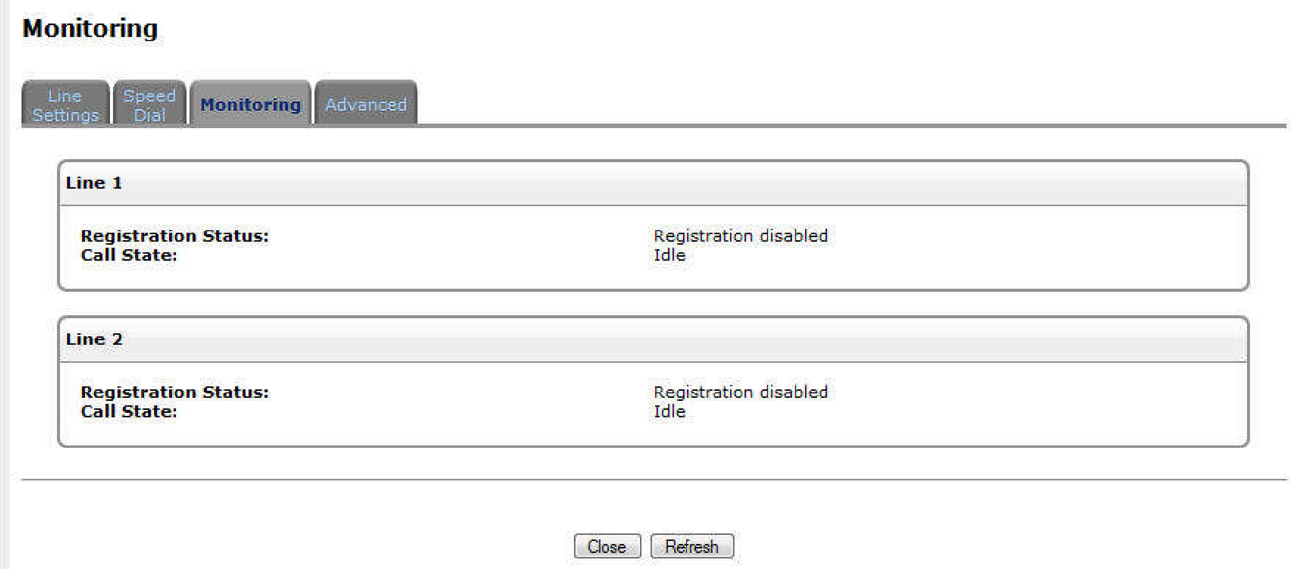
Speed Dial via Direct Call. To add a new direct call speed dial entry:

1. Click the 'New Entry' link on the 'Speed Dial' tab and select the 'Direct Call' option from the combo-box.
2. Enter the following parameters:
   - Speed Dial: A shortcut number which you will dial to call this party.
   - Destination: The entry's destination, in this case a direct call.
   - User ID: Specify the remote party's user ID.
   - IP Address or Host Name: Specify the remote party's IP Address or host name.
3. Click 'OK' to save the settings.

MONITORING

It is possible to access to the line monitoring page by selecting the ‘Monitoring’ Tab panel: the Registration Status and Call State for each line are shown.

FIGURE 3. **Monitoring Panel**



Monitoring

Line 1

Registration Status: Registration disabled
Call State: Idle

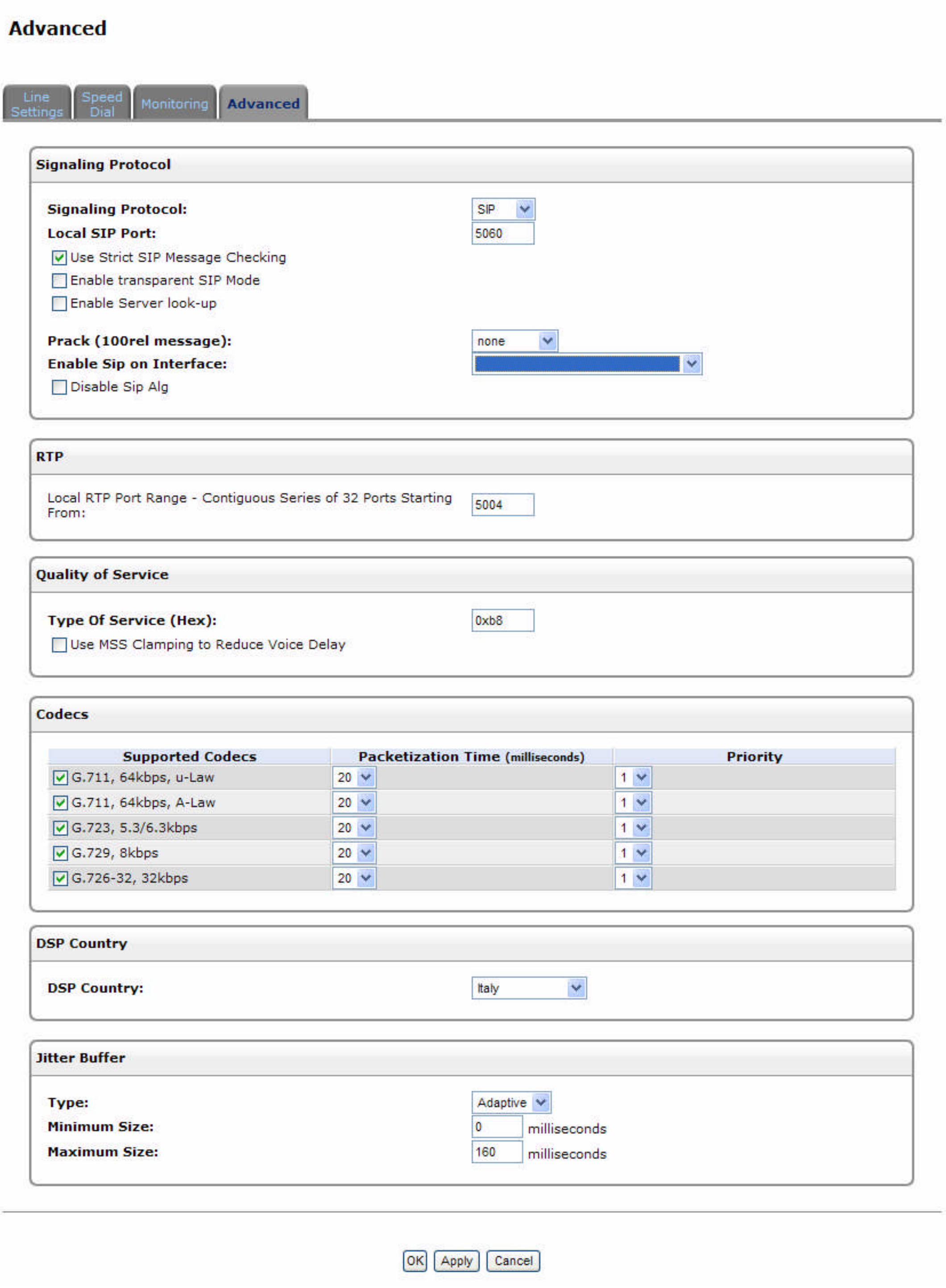
Line 2

Registration Status: Registration disabled
Call State: Idle

ADVANCED

The IP Telephony tab of the Voice over IP screen allows configuration of dialing parameters, VoIP Signaling Protocol, media streaming parameters and codecs. The following sections describe these various parameters.

FIGURE 4. **Advanced Panel**



Advanced

Signaling Protocol

Signaling Protocol: SIP
Local SIP Port: 5060
☑ Use Strict SIP Message Checking
□ Enable transparent SIP Mode
□ Enable Server look-up

Prack (100rel message): none
Enable Sip on Interface:
□ Disable Sip Alg

RTP

Local RTP Port Range - Contiguous Series of 32 Ports Starting From: 5004

Quality of Service

Type Of Service (Hex): 0xb8
□ Use MSS Clamping to Reduce Voice Delay

Codecs

Supported Codecs	Packetization Time (milliseconds)	Priority
☑ G.711, 64kbps, u-Law	20	1
☑ G.711, 64kbps, A-Law	20	1
☑ G.723, 5.3/6.3kbps	20	1
☑ G.729, 8kbps	20	1
☑ G.726-32, 32kbps	20	1

DSP Country

DSP Country: Italy

Jitter Buffer

Type: Adaptive
Minimum Size: 0 milliseconds
Maximum Size: 160 milliseconds

Signaling Protocol. The signaling protocol options available in the combo-box, are determined by the VoIP stack on your gateway.

A different subset of parameters will become visible with each of the combo-box choices. To apply the change of protocol you must press either 'OK' or 'Apply'. If the applied protocol is of another stack, the Router will reboot after you accept the reboot warning.

RTP. Local RTP Port Range defines the port range for Real Time Protocol (RTP) voice transport.

Quality of Service. Type of Service (HEX) This is a part of the IP header that defines the type of routing service to be used to tag outgoing voice packets originated from the Router. It is used to tell routers along the way that this packet should get specific QoS. Leave this value as 0XB8 (default) if you are unfamiliar with the differentiated Services IP protocol parameter.

Codecs. Codecs define the method of relaying voice data. Different codecs have different characteristics, such as data compression and voice quality. For example, G.723 is a codec that uses compression, so it is good for use where bandwidth is limited but its voice quality is not as good compared to other codecs such as the G.711.

Silence Suppression. The Silence Suppression feature allows optimization to be made when no speech is detected. With this feature enabled, the Router is able to detect the absence of audio and conserve bandwidth by preventing the transmission of "silent packets" over the network.

Echo Cancellation. Echo Cancellation is the elimination of reflected signals (echoes) made noticeable by delay in the network. his also improves the bandwidth of the line. When the delay of a voice call exceeds acceptable limits, the router will protect the far end from receiving any echo generated at the local end and sent back through the network.

Parental Control Section

This chapter will describe the **Parental Control** accessible from the *Home Page* of the **PRG AV4202N**.

The abundance of harmful information on the Internet is posing a serious challenge for employers and parents alike - "How can I regulate what my employee/child does on the net?" Discus Web-filtering allows parents and employers to regulate, control and monitor Internet access. By classifying and categorizing online content, it is possible to create numerous Internet access policies, and easily apply them to your home network computers. As a result, you may keep your children from harm's way by limiting access to adult and violent material, or increase employee productivity by regulating access to non work-related Internet content.

To effectively filter Web content one must first have a good idea of the kind of information that is available on the Internet. It is necessary to formulate a landscape of the accessible content, categorize and classify themes and subjects that may be considered inappropriate.

Discus Parental Control categorization methodology provides an easy and straightforward method for fine-grained content filtering. The Parental Control module is constantly updated with URL-based information classified according to the following categories:

- Child protection
- Recreation and Entertainment
- Personal business

- Bandwidth control
- Advertisements
- Chat
- Remote Proxies and Hosting Sites (possibly untrusted sources)
- Other

Each category can be expanded into subcategories for better content control. For instance, the 'Recreation and Entertainment' category is comprised of subcategories such as:

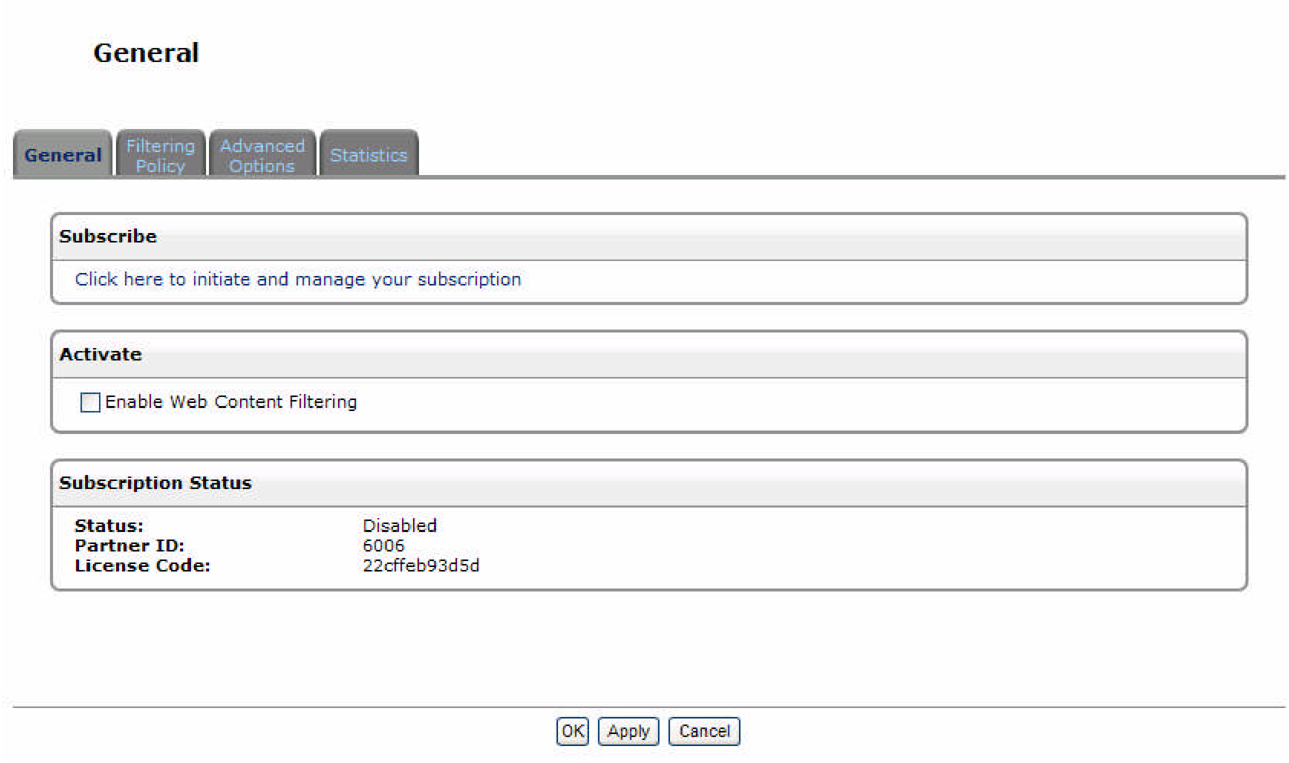
- Arts and Entertainment
- Education
- Games
- Hobbies and Recreation

GENERAL OVERVIEW

Discus Parental Control service is provided by "Surf Control", a company specializing in Internet content filtering. Therefore, you must subscribe to this service in order to use this feature. You can subscribe through Discus WBM, as described in the following section.

1. Under the 'Services; tab, click the 'Parental Control' menu item. The Parental Control's 'General' screen appears.
2. In the 'Activate' section, select the 'Enable Web Content Filtering' check box, and click 'Apply'. A 'Server Status' section is added.
3. If you have not subscribed yet or your subscription has expired, click the 'Click Here to Initiate and Manage your Subscription' link in the 'Subscribe' section. The Web filtering subscription site will then be displayed in a new browser window.
4. Follow the instructions on the site and subscribe for a free trial. You will be sent a verification email. Click the link in the verification email. Your subscription will be activated soon after clicking the verification link.
5. Return to Discus WBM, and click the 'Parental Control' menu item under the 'Services' tab. The 'Filtering Policy' screen should be displayed with subscription expiry date at the top. If this is not the case, click the 'Advanced Options' link and then the 'Refresh Servers'button. Wait a few seconds and repeat this step.

FIGURE 1. **General Panel**



General

Subscribe

Click here to initiate and manage your subscription

Activate

☐ Enable Web Content Filtering

Subscription Status

Status:	Disabled
Partner ID:	6006
License Code:	22cffeb93d5d

FILTERING POLICY

A filtering policy defines which sites will be blocked based on their category. Discus provides four built-in policies:

Home Blocks sites under the 'Child Protection' category.

Employee Blocks sites from non work-related categories.

Block All Blocks all access to the Internet.

Allow All Allows unlimited Internet access.

These policies can be set from the 'Default Filtering Policy' drop-down menu in the 'Filtering Policy' screen. To view or edit the 'Home' and 'Employee' policies, click their respective links in this screen. To create your own filtering policy, perform the following:

1. Click the 'Filtering Policy' link under the 'Parental Control' menu item.

2. Click the 'Add a policy' link.

3. Enter a name and a description for the new policy.

4. Select the content filtering check boxes, which represent content you would like to block. Selecting a category will automatically select all its sub-categories and vice versa. If you would like to make a more refined selection of filtering options, click the plus sign (+) next to each category to display a list of its sub-categories. Note that clicking the minus sign (-) of a category will only be possible if all its sub-categories are either checked or unchecked.

5. You can also manually specify a list of Web sites and a list of URL keywords in the provided text fields, to which you can either block or allow access using the corresponding drop-down menu.

6. Click 'OK' to save the settings.

Once you have created different filtering policies, you can either define a default policy that will be applied to all of your LAN computers, or apply different policies to individual computers separately:

- LAN Filtering Policy – To select a default filtering policy for the LAN, select the policy name from the 'Default Filtering Policy' drop-down menu located in the 'Filtering Policy' screen, and click Apply.

- PC Filtering Policy – To apply separate policies to individual home computers, perform the following:

    1. In the 'Filtering Policy' screen (see Figure 7.318), click the 'Add a LAN Computer' link.

    2. Enter the name or IP address of the LAN computer to which you wish to apply a policy.

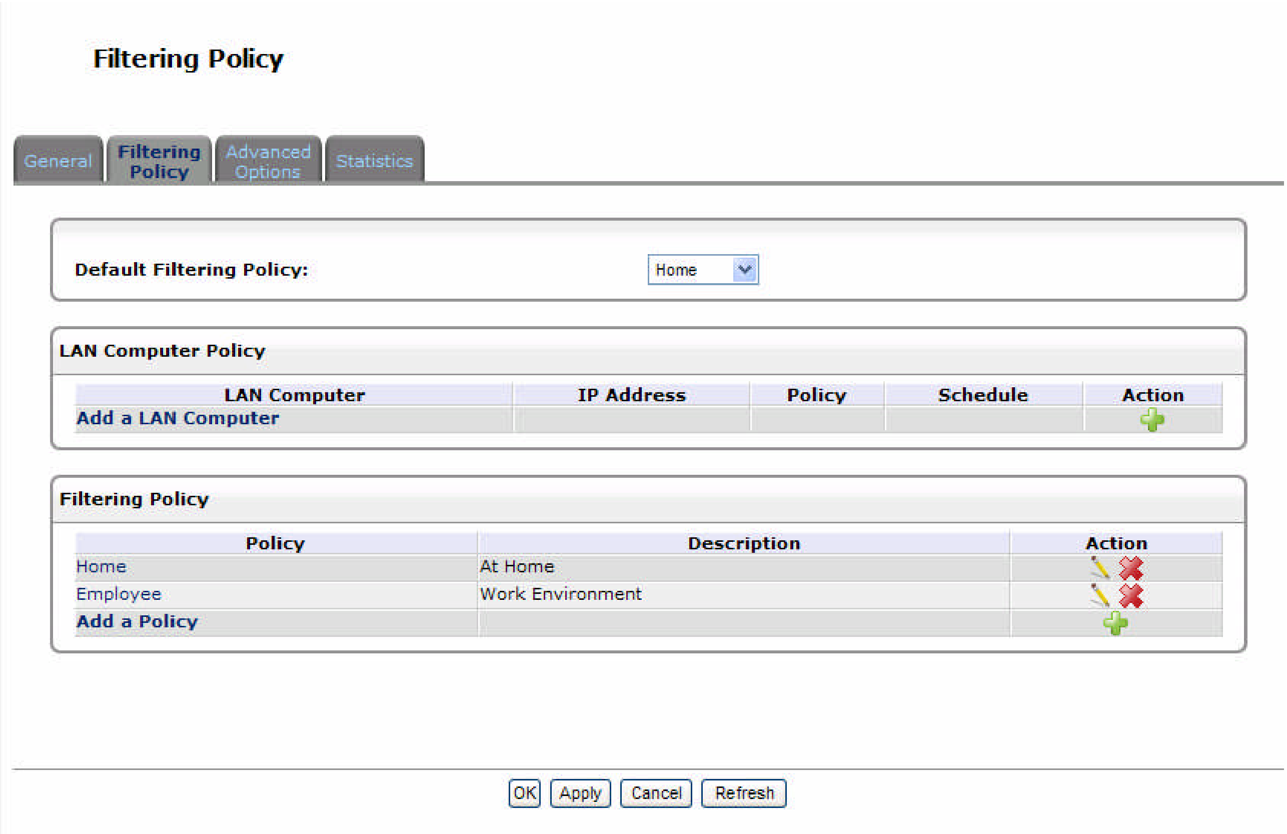
    3. Select the policy you wish to apply in the 'Policy' drop-down menu.

    4. By default, the rule will always be active. However, you can configure scheduler rules by selecting 'User Defined', in order to define time segments during which the rule may be active. After more than one scheduler rule is defined, the 'Schedule' drop-down menu will allow you to choose between the available rules.

    5. Back in the 'Filtering Policy' screen, use the check box next to the computer name in order to enable or disable its policy.

    6. Click 'OK' to save the settings.

FIGURE 2. **Filtering Policy Panel**



Filtering Policy

Default Filtering Policy: Home

LAN Computer Policy

LAN Computer	IP Address	Policy	Schedule	Action
Add a LAN Computer				✚

Filtering Policy

Policy	Description	Action
Home	At Home	✎ ✖
Employee	Work Environment	✎ ✖
Add a Policy		✚

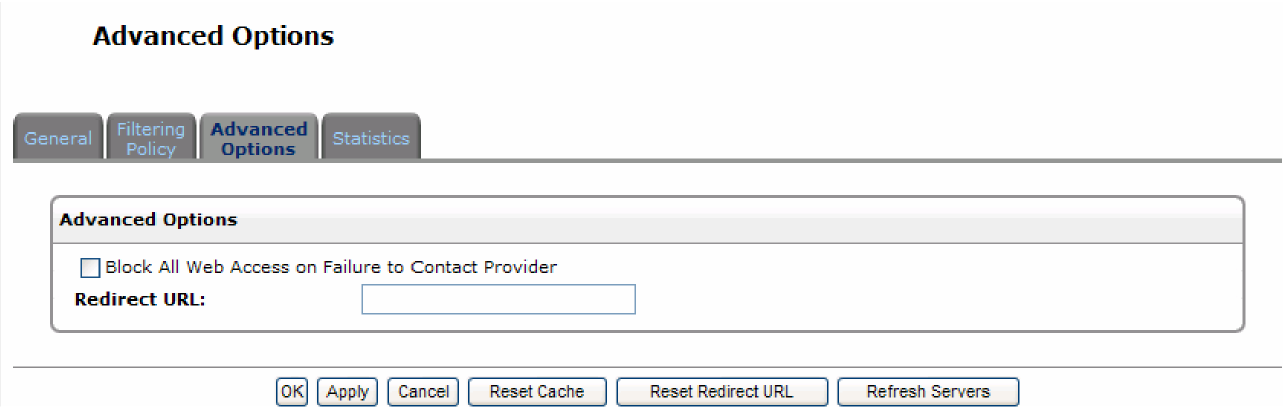
ADVANCED OPTIONS

Click the 'Advanced Options' link of the 'Parental Control' menu item under the 'Services' tab.

Block All Web Access on Failure to Contact Provider The filtering service provider is consulted about every site's category in order to decide whether to allow or block it. If for any reason the provider cannot be consulted, use this check box to determine whether to block or allow access to all sites.

Redirect URL When a site is blocked, an OpenRG 'Blocked Access' page is displayed, specifying the requested URL and the reason it was blocked. Use this field to specify an alternative page to be displayed when a site is blocked.

FIGURE 3. **Advanced Options Panel**



Advanced Options

Advanced Options

□ Block All Web Access on Failure to Contact Provider

Redirect URL:

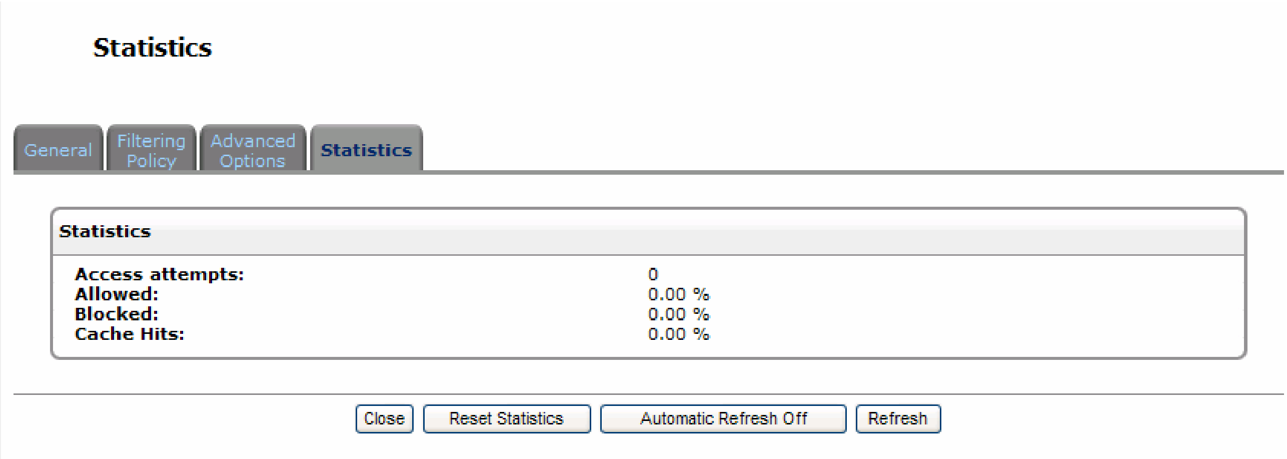
STATISTICS

Click the 'Statistics' link of the 'Parental Control' menu item under the 'Services' tab.

The 'Statistics' screen monitors content filtering statistics. The statistics include a record of:

- Access attempts
- Allowed URLs
- Blocked URLs
- URLs that were accessed from Cache memory

FIGURE 4. **Statistics Panel**



Statistics

Statistics

Access attempts:	0
Allowed:	0.00 %
Blocked:	0.00 %
Cache Hits:	0.00 %

QoS Section

This chapter will describe the **QoS (Quality of Service) Section** accessible from the *Home Page* of the **PRG AV4202N**.

⚠ *Be aware that any configuration changes could compromise your connectivity.*

Quality of Service refers to the capability of a network device to provide better service to selected network traffic. This is achieved by processing higher priority traffic before lower priority traffic.

As Quality of Service is dependent on the "weakest link in the chain", failure of a single component along the data path can easily cause a VoIP call or a Video on Demand (VoD) broadcast to fail miserably.

QoS must therefore obviously be addressed end-to-end.

GENERAL

The 'General' tab provides a Quality of Service "wizard", with which you can configure your QoS parameters according to predefined profiles, with just a few clicks. A chosen QoS profile will automatically define QoS rules, which you can view and edit in the rest of the QoS tab screens.

WAN Devices Bandwidth (Rx/Tx). Before selecting the QoS profile that mostly suits your needs, select your bandwidth from this combo-box. If you do not see an appropriate entry, select 'User Defined', and enter your Tx and Rx bandwidths manually.

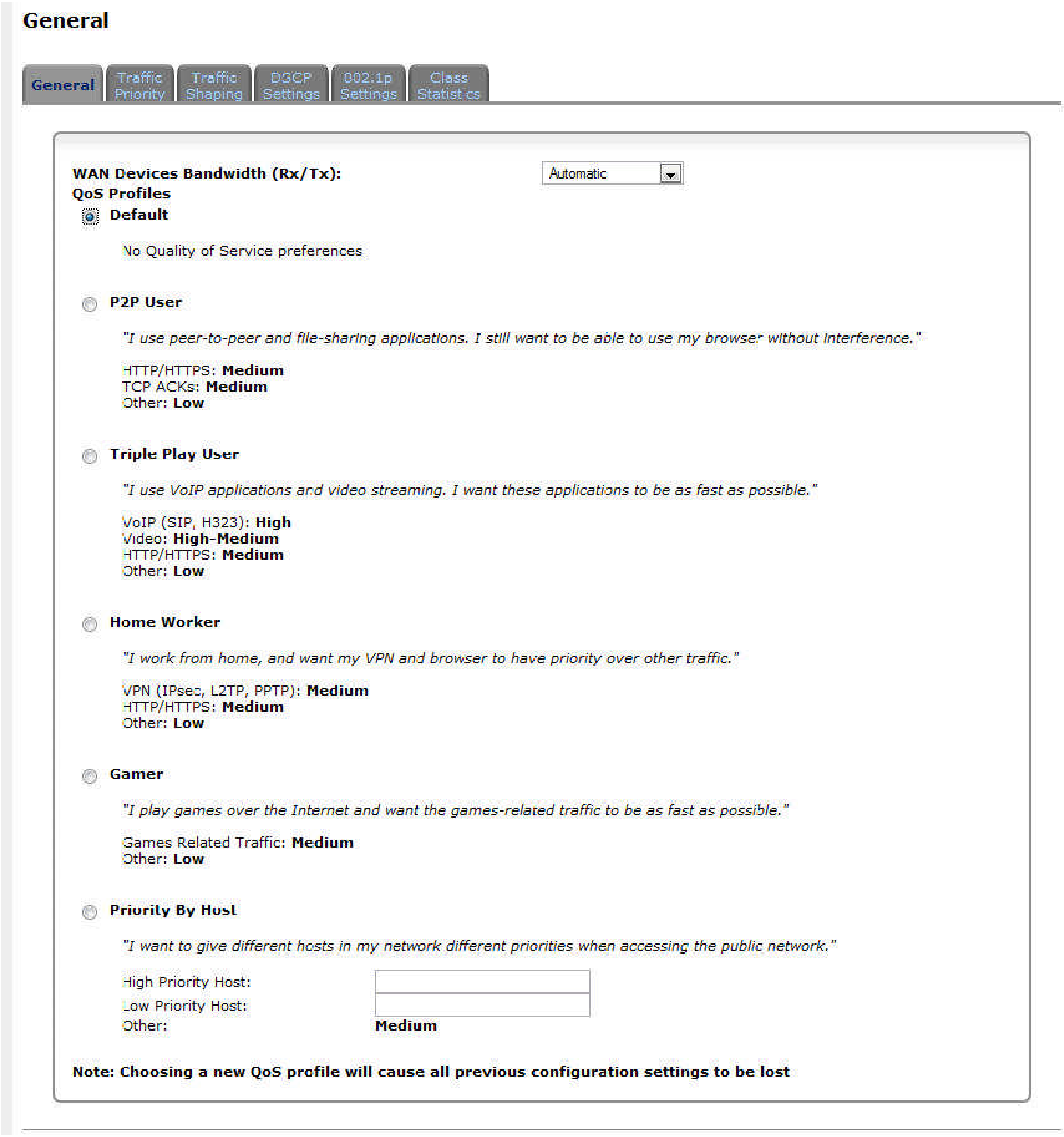
Tx Bandwidth. Enter your Tx bandwidth in Kbits per second.

Rx Bandwidth. Enter your Rx bandwidth in Kbits per second.

QoS Profiles. Select the profile that mostly suits your bandwidth usage. Each profile entry displays a quote describing what the profile is best used for, and the QoS priority levels granted to each bandwidth consumer in this profile.

- **Default**: No QoS preferences
- **P2P User**: Peer-to-peer and file sharing applications will receive priority
- **Triple Play User**: VoIP and video streaming will receive priority
- **Home Worker**: VPN and browsing will receive priority
- **Gamer**: Game-related traffic will receive priority
- **Priority By Host**: This entry provides the option to configure which computer in your LAN will receive the highest priority and which the lowest. If you have additional computers, they will receive medium priority.
  - High Priority Host: enter the host name or IP address of the computer to which you would like to grant the highest bandwidth priority.
  - Low Priority Host: enter the host name or IP address of the computer to which you would like to grant the lowest bandwidth priority.

FIGURE 1. **General Panel**



WAN Devices Bandwidth (Rx/Tx): Automatic

QoS Profiles

● **Default**

No Quality of Service preferences

○ **P2P User**

"I use peer-to-peer and file-sharing applications. I still want to be able to use my browser without interference."

HTTP/HTTPS: **Medium**
TCP ACKs: **Medium**
Other: **Low**

○ **Triple Play User**

"I use VoIP applications and video streaming. I want these applications to be as fast as possible."

VoIP (SIP, H323): **High**
Video: **High-Medium**
HTTP/HTTPS: **Medium**
Other: **Low**

○ **Home Worker**

"I work from home, and want my VPN and browser to have priority over other traffic."

VPN (IPsec, L2TP, PPTP): **Medium**
HTTP/HTTPS: **Medium**
Other: **Low**

○ **Gamer**

"I play games over the Internet and want the games-related traffic to be as fast as possible."

Games Related Traffic: **Medium**
Other: **Low**

○ **Priority By Host**

"I want to give different hosts in my network different priorities when accessing the public network."

High Priority Host:	
Low Priority Host:	
Other:	**Medium**

Note: Choosing a new QoS profile will cause all previous configuration settings to be lost

TRAFFIC PRIORITY

Traffic Priority allows you to manage and avoid traffic congestion by defining inbound and outbound priority rules for each device on your gateway. These rules determine the priority that packets, traveling through the device, will receive. QoS parameters (DSCP marking and packet priority) are set per packet, on an application basis.

You can set QoS parameters using flexible rules, according to the following parameters:

- Source/destination IP address, MAC address or host name
- Device
- Source/destination ports
- Limit the rule for specific days and hours

The Router supports two priority marking methods for packet prioritization:

- DSCP
- 802.1p Priority

The matching of packets by rules is connection-based, known as Stateful Packet Inspection (SPI). Once a packet matches a rule, all subsequent packets with the same attributes receive the same QoS parameters, both inbound and outbound.

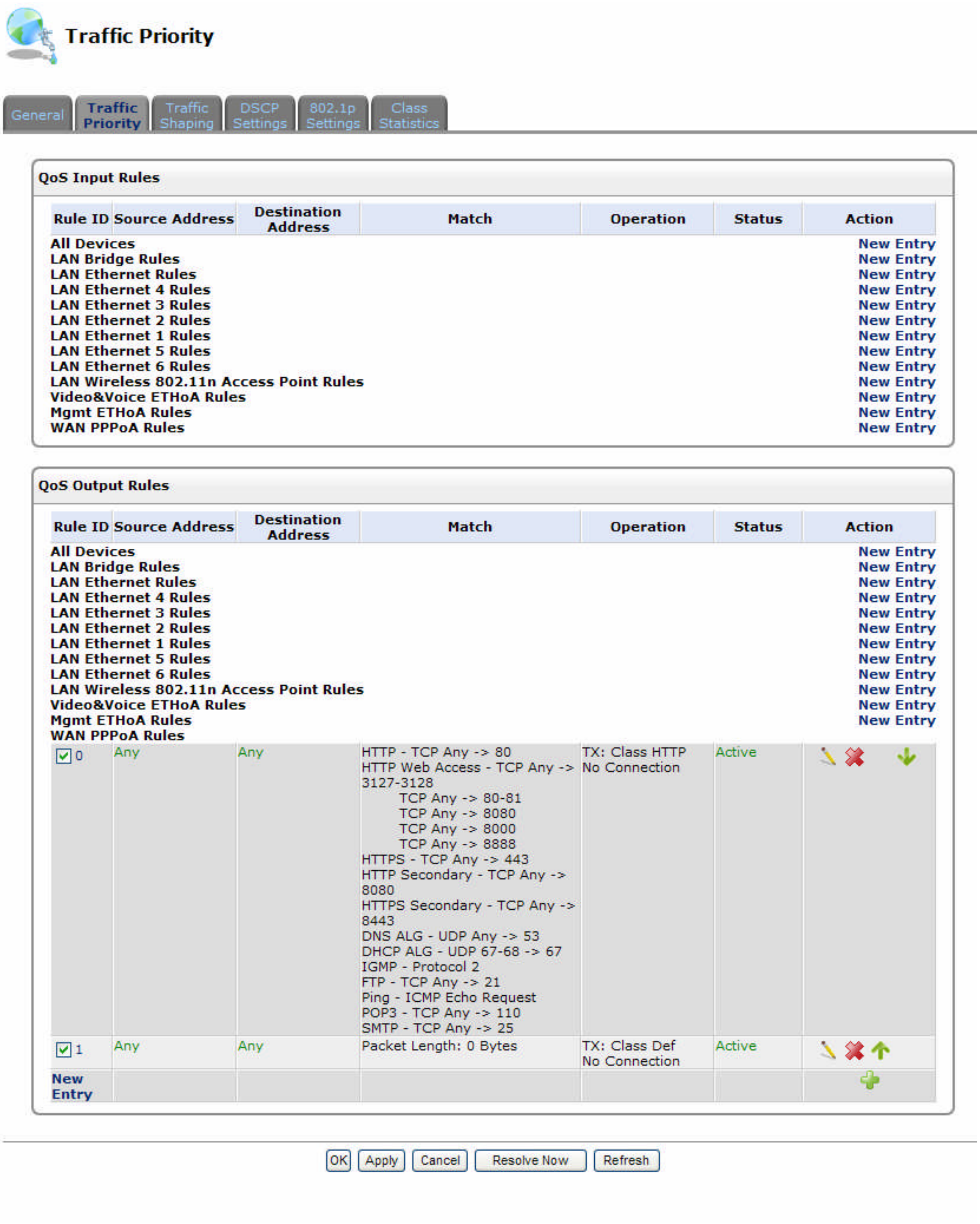
A packet can match more than one rule. Therefore:

- The first class rule has precedence over all other class rules (scanning is stopped once the first rule is reached).
- The first traffic-priority (classless) rule has precedence over all other traffic-priority rules.
- There is no prevention of a traffic-priority rule conflicting with a class rule. In this case, the priority and DSCP setting of the class rule (if given) will take precedence.

Connection-based QoS also allows inheriting QoS parameters by some of the applications that open subsequent connections. For instance, you can define QoS rules on SIP, and the rules will apply to both control and data ports (even if the data ports are unknown):

- SIP
- MSN Messenger/Windows Messenger
- TFTP
- FTP
- MGCP
- H.323
- Port Triggering applications
- PPTP
- IPSec

FIGURE 2. **Traffic Priority Panel**



QoS Input Rules

Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
All Devices						New Entry
LAN Bridge Rules						New Entry
LAN Ethernet Rules						New Entry
LAN Ethernet 4 Rules						New Entry
LAN Ethernet 3 Rules						New Entry
LAN Ethernet 2 Rules						New Entry
LAN Ethernet 1 Rules						New Entry
LAN Ethernet 5 Rules						New Entry
LAN Ethernet 6 Rules						New Entry
LAN Wireless 802.11n Access Point Rules						New Entry
Video&Voice ETHoA Rules						New Entry
Mgmt ETHoA Rules						New Entry
WAN PPPoA Rules						New Entry

QoS Output Rules

Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
All Devices						New Entry
LAN Bridge Rules						New Entry
LAN Ethernet Rules						New Entry
LAN Ethernet 4 Rules						New Entry
LAN Ethernet 3 Rules						New Entry
LAN Ethernet 2 Rules						New Entry
LAN Ethernet 1 Rules						New Entry
LAN Ethernet 5 Rules						New Entry
LAN Ethernet 6 Rules						New Entry
LAN Wireless 802.11n Access Point Rules						New Entry
Video&Voice ETHoA Rules						New Entry
Mgmt ETHoA Rules						New Entry
WAN PPPoA Rules						
☑ 0	Any	Any	HTTP - TCP Any -> 80 HTTP Web Access - TCP Any -> 3127-3128 TCP Any -> 80-81 TCP Any -> 8080 TCP Any -> 8000 TCP Any -> 8888 HTTPS - TCP Any -> 443 HTTP Secondary - TCP Any -> 8080 HTTPS Secondary - TCP Any -> 8443 DNS ALG - UDP Any -> 53 DHCP ALG - UDP 67-68 -> 67 IGMP - Protocol 2 FTP - TCP Any -> 21 Ping - ICMP Echo Request POP3 - TCP Any -> 110 SMTP - TCP Any -> 25	TX: Class HTTP No Connection	Active	✎ ✖ ↓
☑ 1	Any	Any	Packet Length: 0 Bytes	TX: Class Def No Connection	Active	✎ ✖ ↑
New Entry						✚

To set traffic priority rules:

1. Click 'Traffic Priority' under the 'QoS' tab in the 'Services' screen. The 'Traffic Priority' screen will appear. This screen is divided into two identical sections, one for 'QoS input rules' and the other for 'QoS output rules', which are for prioritizing inbound and outbound traffic, respectively. Each section lists all the gateway devices on which rules can be set. You can set rules on all devices at once, using the 'All devices' entry.
2. After choosing the traffic direction and the device on which to set the rule, click the appropriate New Entry link. The 'Add Traffic Priority Rule' screen will appear.

This screen is divided into two main sections, 'Matching' and 'Operation', which are for defining the operation to be executed when matching conditions apply.

- **Matching:** Use this section to define the rule's conditions, which are the LAN computer's parameters to be matched.

- **Operation:** Set rule priority with Quality of Service.

3. Click 'OK' to save the settings.

TRAFFIC SHAPING

Traffic Shaping is the solution for managing and avoiding congestion where a high speed LAN meets limited broadband bandwidth. A user may have, for example, a 100 Mbps Ethernet LAN with a 100 Mbps WAN interface router. The router may communicate with the ISP using a modem with a bandwidth of 2Mbps. This typical configuration makes the modem, having no QoS module, the bottleneck. The router sends traffic as fast as it is received, while its well-designed QoS algorithms are left unused. Traffic shaping limits the bandwidth of the router, artificially forcing the router to be the bottleneck.

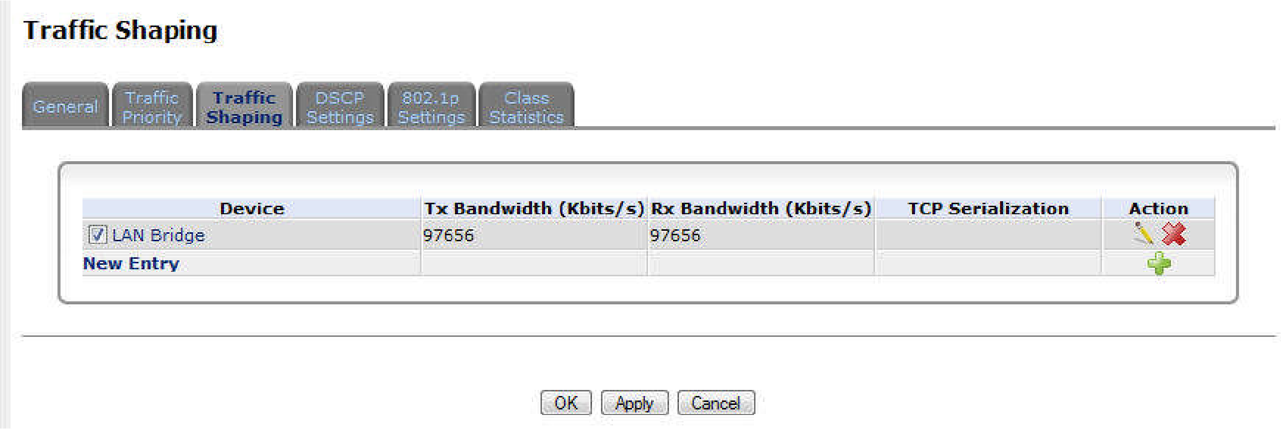
A traffic shaper is essentially a regulated queue that accepts uneven and/or bursty flows of packets and transmits them in a steady, predictable stream so that the network is not overwhelmed with traffic.

While Traffic Priority allows basic prioritization of packets, Traffic Shaping provides more sophisticated definitions. Such are:

- Bandwidth limit for each device
- Bandwidth limit for classes of rules
- Prioritization policy
- TCP serialization on a device

Additionally, you can define QoS traffic shaping rules for a default device. These rules will be used on a device that has no definitions of its own. This enables the definition of QoS rules on Default WAN, for example, and their maintenance even if the PPP or bridge device over the WAN is removed.

FIGURE 3. **Traffic Shaping Panel**



Device	Tx Bandwidth (Kbits/s)	Rx Bandwidth (Kbits/s)	TCP Serialization	Action
☑ LAN Bridge	97656	97656		✎ ✖
New Entry				✚

DSCP SETTINGS

In order to understand what is Differentiated Services Code Point (DSCP), one must first be familiarized with the Differentiated Services model.

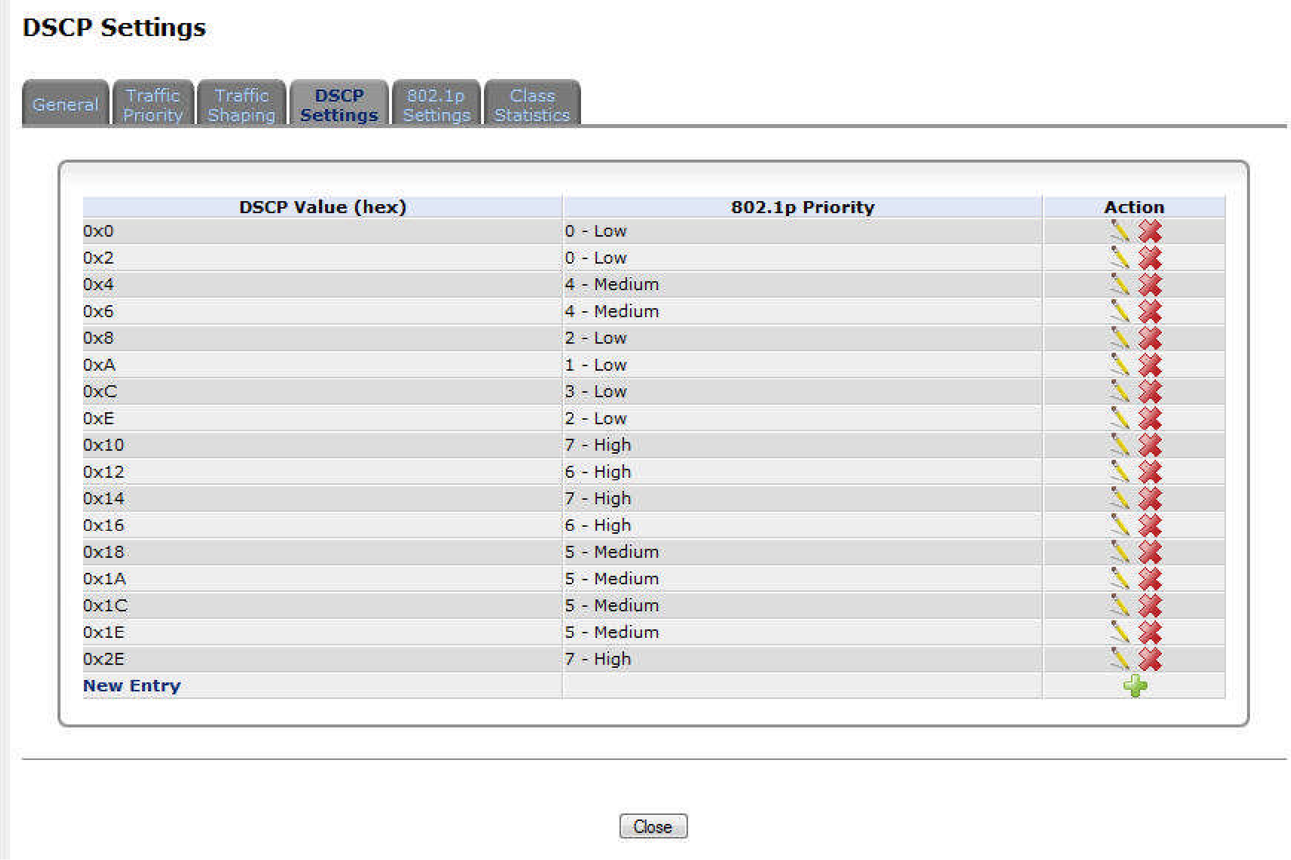
Differentiated Services (Diffserv) is a Class of Service (CoS) model that enhances best-effort Internet services by differentiating traffic by users, service requirements and other criteria. Packets are specifically marked, allowing network nodes to provide different levels of service, as appropriate for voice calls, video playback or other delay-sensitive applications, via priority queuing or bandwidth allocation, or by choosing dedicated routes for specific traffic flows.

Diffserv defines a field in IP packet headers referred to as DSCP. Hosts or routers passing traffic to a Diffserv-enabled network will typically mark each transmitted packet with an appropriate DSCP. The DSCP markings are used by Diffserv network routers to appropriately classify packets and to apply particular queue handling or scheduling behavior.

PRG AV4202N provides a table of predefined DSCP values, which are mapped to 802.1p priority marking method. You can edit or delete any of the existing DSCP setting, as well as add new entries.

1. Click 'DSCP Settings' under the QoS tab in the 'Services' screen. The following screen will appear
2. To edit an existing entry, click its Edit action icon. To add a new entry, click the 'New Entry' link. In both cases, the 'Edit DSCP Settings' screen will appear.
3. Configure the following fields: DSCP Value (hex) Enter a hexadecimal number that will serve as the DSCP value. 802.1p Priority Select a 802.1p priority level from the combo-box (each priority level is mapped to low/medium/high priority).
4. Click 'OK' to save the settings.

FIGURE 4. **DSCP Settings Panel**



DSCP Value (hex)	802.1p Priority	Action
0x0	0 - Low	✎ ✖
0x2	0 - Low	✎ ✖
0x4	4 - Medium	✎ ✖
0x6	4 - Medium	✎ ✖
0x8	2 - Low	✎ ✖
0xA	1 - Low	✎ ✖
0xC	3 - Low	✎ ✖
0xE	2 - Low	✎ ✖
0x10	7 - High	✎ ✖
0x12	6 - High	✎ ✖
0x14	7 - High	✎ ✖
0x16	6 - High	✎ ✖
0x18	5 - Medium	✎ ✖
0x1A	5 - Medium	✎ ✖
0x1C	5 - Medium	✎ ✖
0x1E	5 - Medium	✎ ✖
0x2E	7 - High	✎ ✖
New Entry		✚

802.1P SETTINGS

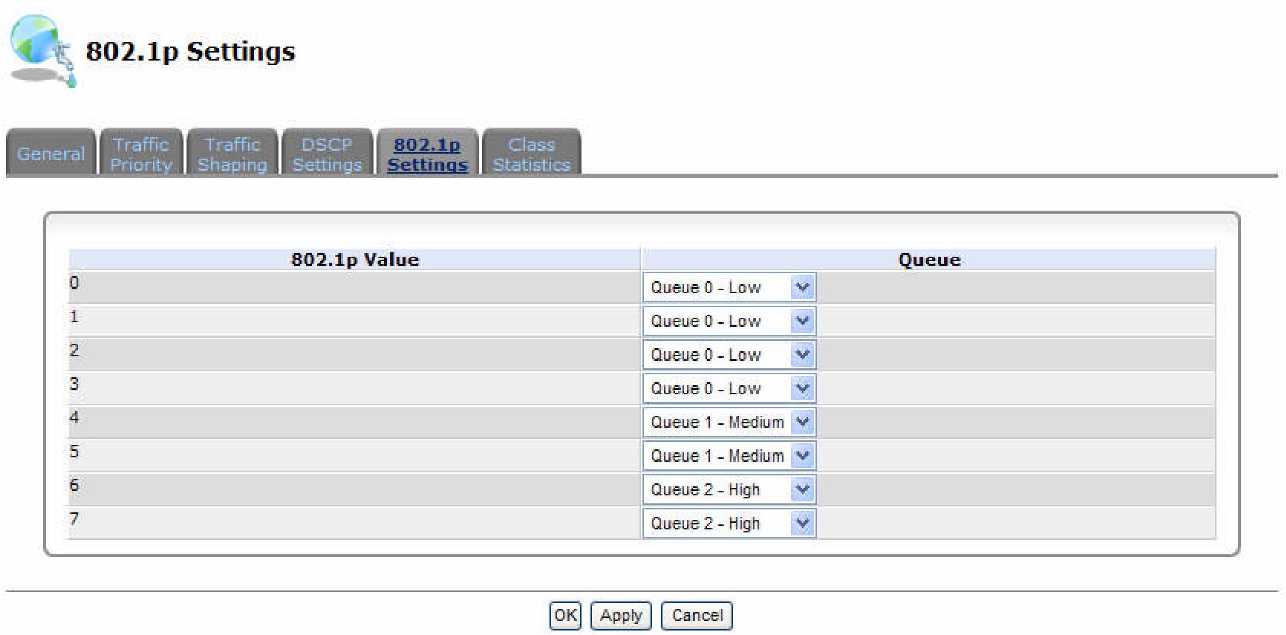
The IEEE 802.1p priority marking method is a standard for prioritizing network traffic at the data link/Mac sub-layer. 802.1p traffic is simply classified and sent to the destination, with no bandwidth reservations established.

The 802.1p header includes a 3-bit prioritization field, which allows packets to be grouped into eight levels of priority. PRG AV4202N maps these eight levels to three main priorities: high, medium and low. By default, values six and seven are mapped to high priority, which may be assigned to network-critical traffic. Values four and five are mapped to medium priority, which may be applied to delay-sensitive applications, such as interactive video and voice. Values three to zero are mapped to low priority, which may range from controlled-load applications down to “loss eligible” traffic. The zero value is normally used for best-effort traffic. It is the default value for traffic with unassigned priority.

1. Click '802.1p Settings' under the QoS tab in the 'Services' screen. The following screen will appear

2. The eight 802.1p values are pre-configured with the three priority levels: high, medium and low. You can change these levels for each of the eight values in their respective combo-box.
3. Click 'OK' to save the settings.

FIGURE 5. 802.1p Settings Panel



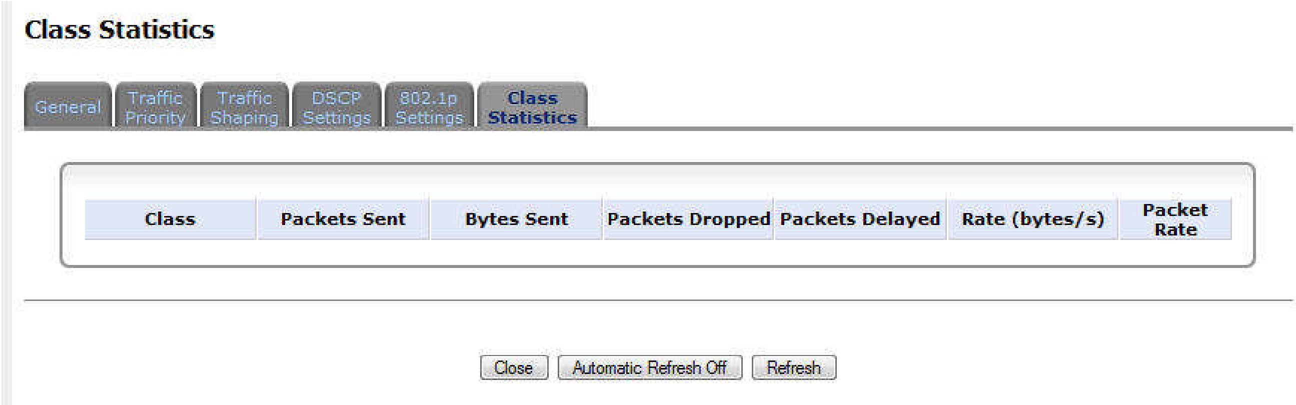
802.1p Value	Queue
0	Queue 0 - Low
1	Queue 0 - Low
2	Queue 0 - Low
3	Queue 0 - Low
4	Queue 1 - Medium
5	Queue 1 - Medium
6	Queue 2 - High
7	Queue 2 - High

CLASS STATISTICS

PRG AV4202N provides you with accurate, real-time information on the traffic moving through your defined device classes. For example, the amount of packets sent, dropped or delayed, are just a few of the parameters that you can monitor per each shaping class.

To view your class statistics, click 'Class Statistics' under the QoS tab in the 'Services' screen. The following screen will appear. Note that class statistics will only be available after defining at least one class (otherwise the screen will not present any information).

FIGURE 6. Class Statistics Panel



Class Statistics

Class	Packets Sent	Bytes Sent	Packets Dropped	Packets Delayed	Rate (bytes/s)	Packet Rate

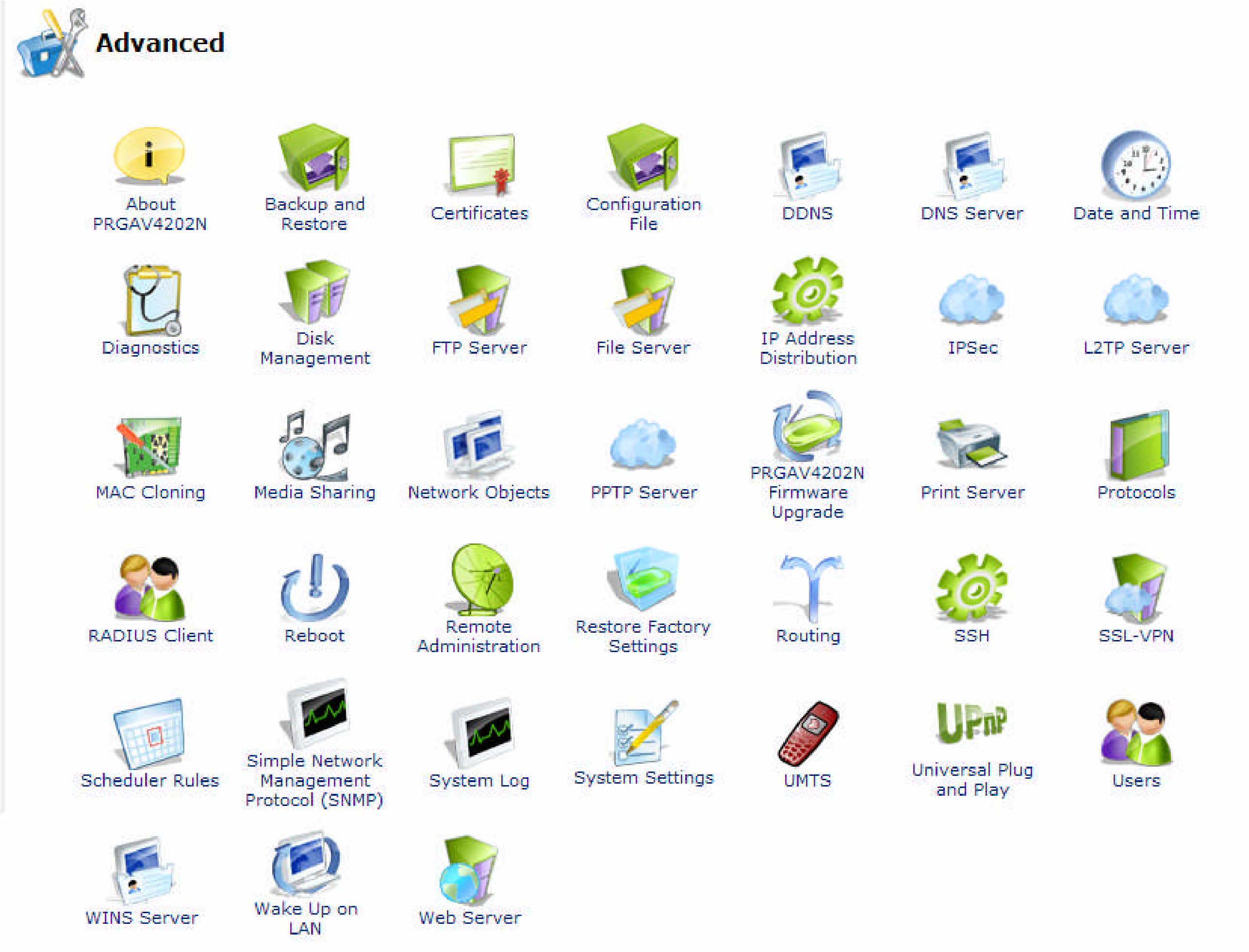
Advanced Section

This chapter will describe the **Advanced Section** accessible from the *Home Page* of the **PRG AV4202N**.

⚠ *Be aware that any configuration changes could compromise your connectivity.*

The Advanced panel collects many functionalities from the operating and configuration point of view. This chapter will describe one by one all icons and related features as shown in the following screen shot.

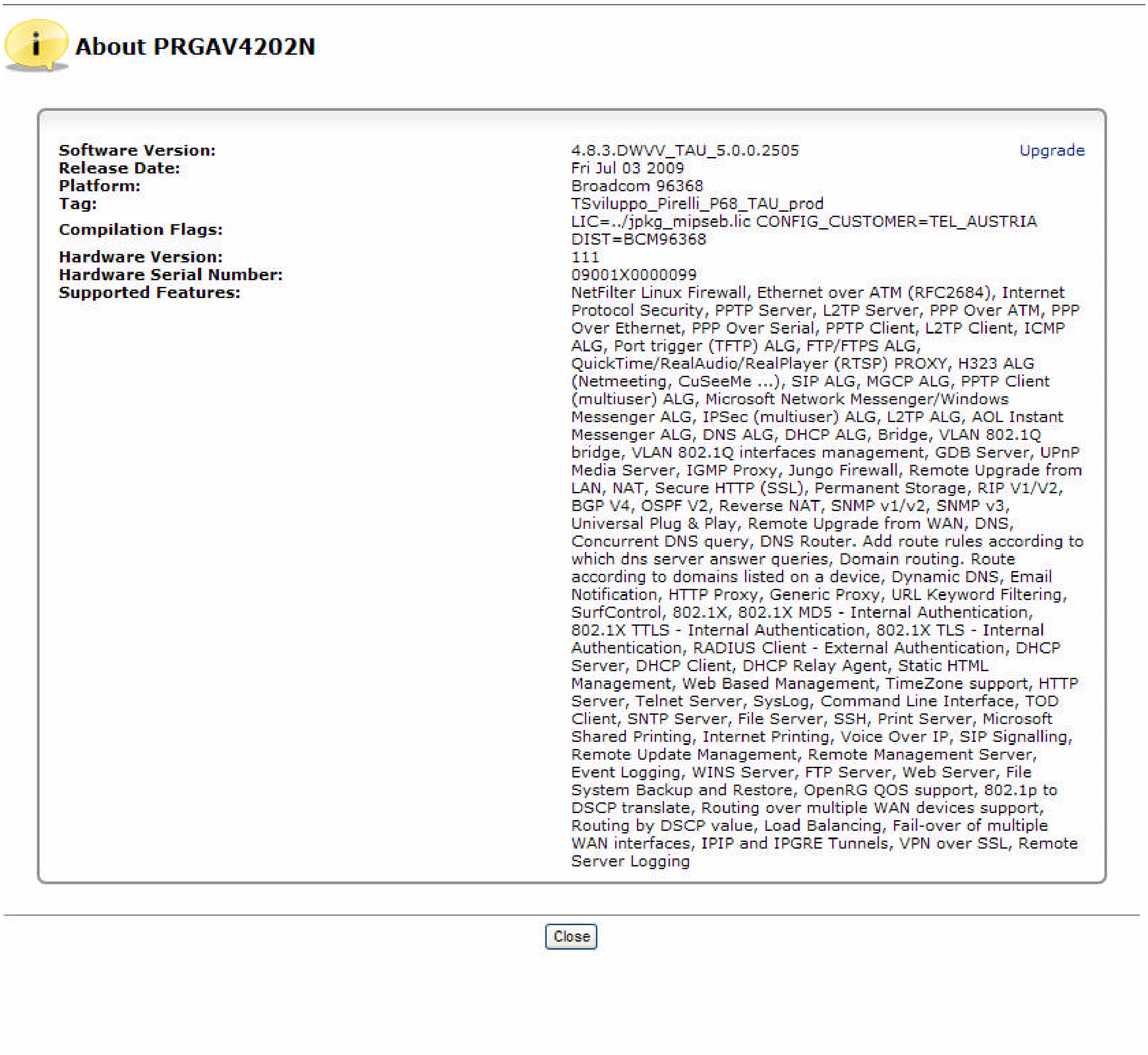
FIGURE 1. Advanced Panel



ABOUT PRG AV4202N

The 'About PRG AV4202N' screen presents various details about Router's software version, such as version number, type of platform and list of features.

FIGURE 2. **About PRG AV4202N Panel**



About PRGAV4202N

Software Version:	4.8.3.DWVV_TAU_5.0.0.2505
Release Date:	Fri Jul 03 2009
Platform:	Broadcom 96368
Tag:	TSviluppo_Pirelli_P68_TAU_prod
Compilation Flags:	LIC=../jpkg_mipseb.lic CONFIG_CUSTOMER=TEL_AUSTRIA DIST=BCM96368
Hardware Version:	111
Hardware Serial Number:	09001X0000099
Supported Features:	NetFilter Linux Firewall, Ethernet over ATM (RFC2684), Internet Protocol Security, PPTP Server, L2TP Server, PPP Over ATM, PPP Over Ethernet, PPP Over Serial, PPTP Client, L2TP Client, ICMP ALG, Port trigger (TFTP) ALG, FTP/FTPS ALG, QuickTime/RealAudio/RealPlayer (RTSP) PROXY, H323 ALG (Netmeeting, CuSeeMe ...), SIP ALG, MGCP ALG, PPTP Client (multiuser) ALG, Microsoft Network Messenger/Windows Messenger ALG, IPSec (multiuser) ALG, L2TP ALG, AOL Instant Messenger ALG, DNS ALG, DHCP ALG, Bridge, VLAN 802.1Q bridge, VLAN 802.1Q interfaces management, GDB Server, UPnP Media Server, IGMP Proxy, Jungo Firewall, Remote Upgrade from LAN, NAT, Secure HTTP (SSL), Permanent Storage, RIP V1/V2, BGP V4, OSPF V2, Reverse NAT, SNMP v1/v2, SNMP v3, Universal Plug & Play, Remote Upgrade from WAN, DNS, Concurrent DNS query, DNS Router. Add route rules according to which dns server answer queries, Domain routing. Route according to domains listed on a device, Dynamic DNS, Email Notification, HTTP Proxy, Generic Proxy, URL Keyword Filtering, SurfControl, 802.1X, 802.1X MD5 - Internal Authentication, 802.1X TTLS - Internal Authentication, 802.1X TLS - Internal Authentication, RADIUS Client - External Authentication, DHCP Server, DHCP Client, DHCP Relay Agent, Static HTML Management, Web Based Management, TimeZone support, HTTP Server, Telnet Server, SysLog, Command Line Interface, TOD Client, SNTP Server, File Server, SSH, Print Server, Microsoft Shared Printing, Internet Printing, Voice Over IP, SIP Signalling, Remote Update Management, Remote Management Server, Event Logging, WINS Server, FTP Server, Web Server, File System Backup and Restore, OpenRG QOS support, 802.1p to DSCP translate, Routing over multiple WAN devices support, Routing by DSCP value, Load Balancing, Fail-over of multiple WAN interfaces, IPIP and IPGRE Tunnels, VPN over SSL, Remote Server Logging

BACKUP AND RESTORE

The PRG AV4202N backup facility allows backing user and system data to external USB disks connected to the router. You may specify backups to run automatically at scheduled times.

Two preliminary conditions must be met before enabling the backup mechanism:

- The file server feature must be activated and configured.

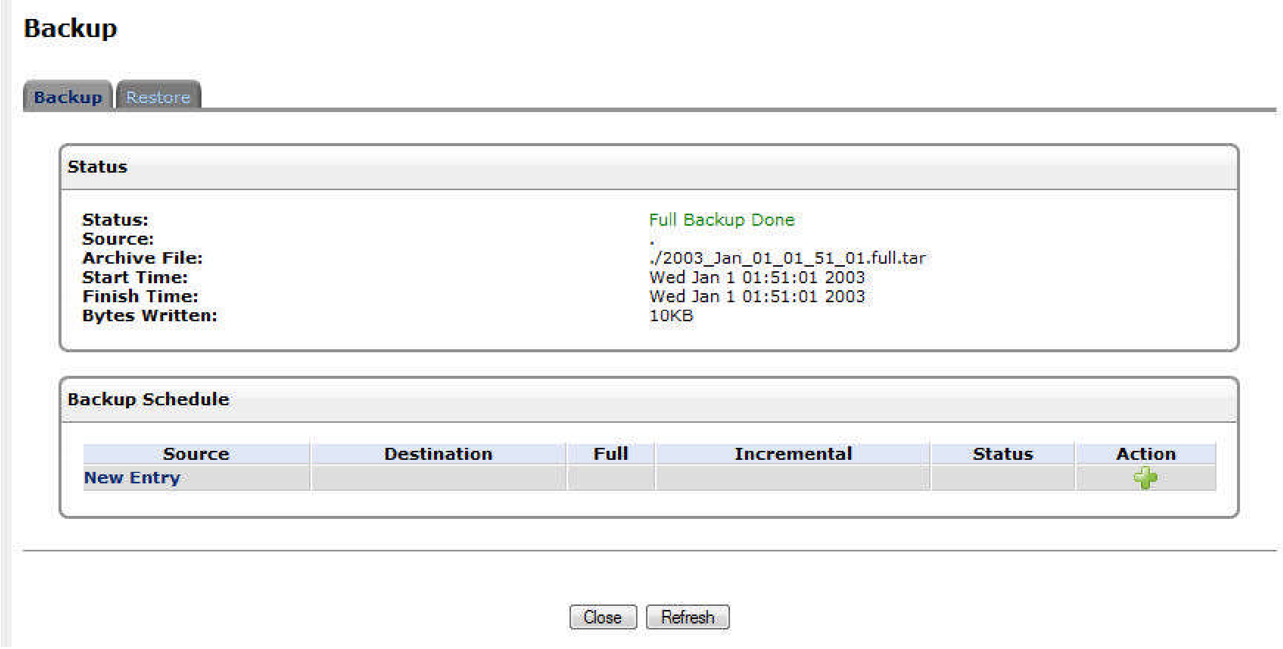
- The file server must be consisted of at least two disks.

Please note that the backup is done at the directory level, meaning that it is not possible to backup a single stand-alone file.

To backup your data:

1. Access the Backup settings either from its link in the 'Advanced' tab under the 'Services' screen, or by clicking the 'Backup and Restore' icon in the 'Advanced' screen. The 'Backup and Restore' screen will appear
2. Click the 'New Entry' link in the 'Backup Schedule' section.
3. In the 'Edit Backup' screen that appears, configure the following parameters: (a) Type the source to backup. For example, A/homes. (b) Type the destination of the backup files. For example, B/backups. It is recommended that the destination be an external storage device. (c) Choose between full backup, incremental backup, or both, by scheduling a time for the backup operation. You can choose between daily, weekly or monthly backups in the 'Schedule' combo-boxes.
4. Press 'OK' to save the schedule settings.
5. Press 'Backup Now' to run the backup operation immediately. When backing up, the screen will display the status and progress of the operation.

FIGURE 3. **Backup Panel**



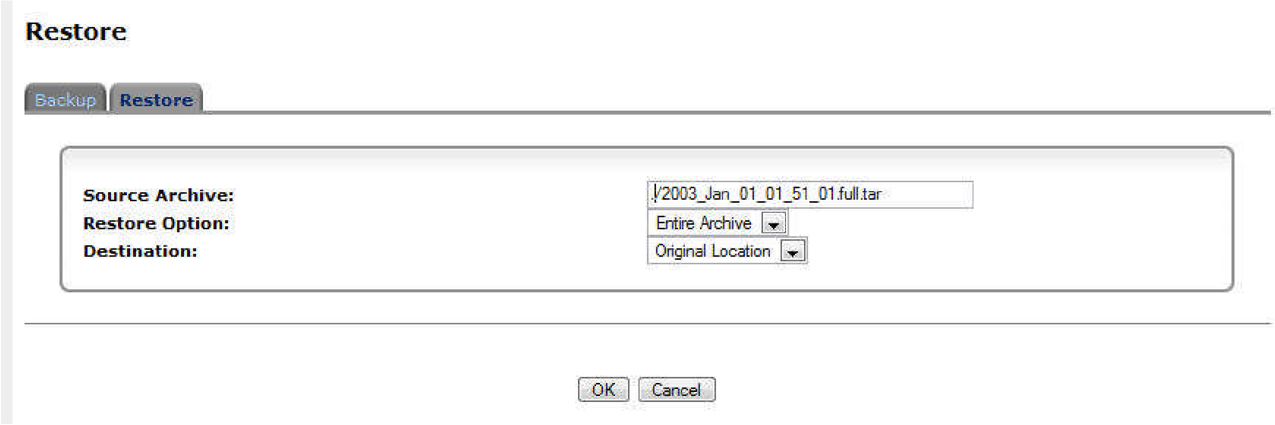
Status:	Full Backup Done
Source:	.
Archive File:	./2003_Jan_01_01_51_01.full.tar
Start Time:	Wed Jan 1 01:51:01 2003
Finish Time:	Wed Jan 1 01:51:01 2003
Bytes Written:	10KB

Source	Destination	Full	Incremental	Status	Action
New Entry					✚

To restore your data:

1. Press the 'Backup and Restore' icon in the 'Advanced' screen of the Management Console. The 'Backup and Restore' screen will appear.
2. Press the 'Restore' tab.
3. In the Restore screen that appears, configure the following parameters:
   (a) Type the source to restore in the 'Source Archive' field. For example, A/homes.
   (b) Choose whether to restore the entire archive or only a sub directory, in the 'Restore Option' combo-box. If you choose sub directory, a second field will appear in which you must enter the name of the sub directory, relative to the source archive. For example, to restore A/homes/john, type john as the sub directory.
   (c) Choose a destination for which to restore the archive. You can choose between the original location or any other directory. If you choose the another directory, a second field will appear in which you must enter the name of the directory. Note that the path of the restored directory will be created under the path of the destination directory. For example, if you specify the directory A/restore dir, the result will be A/restore dir/A/homes/john.

FIGURE 4. **Restore Panel**



Restore

Source Archive: /2003_Jan_01_01_51_01.full.tar
Restore Option: Entire Archive
Destination: Original Location

CERTIFICATES

PRG AV4202N maintains two certificate stores:

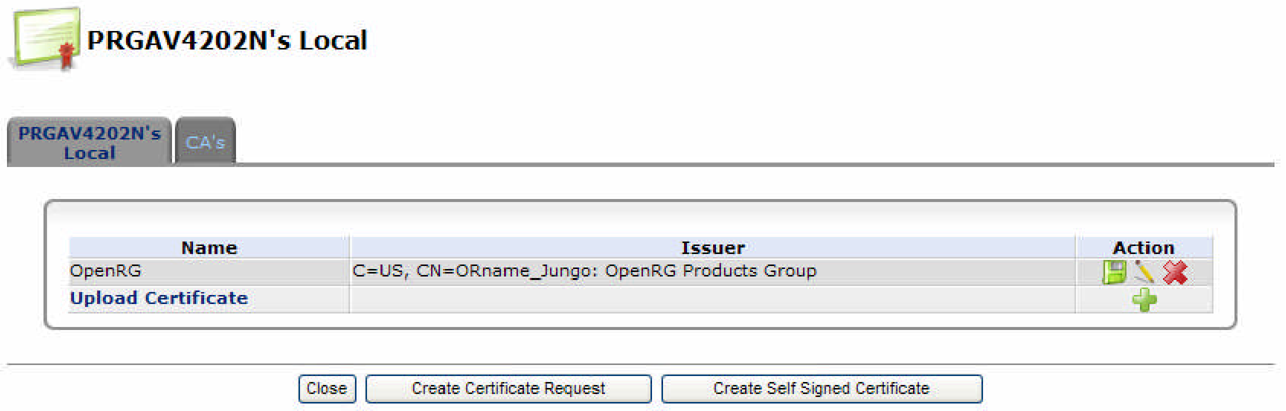
PRG AV4202N's Local. This store contains a list of approved certificates that are used to identify the Router to its clients. The list also includes certificate requests that are pending a CA's endorsement.

You can obtain certificates for the Router using the following methods:

- Requesting an X509 Certificate. This method creates both a private and a matching public key. The public key is then sent to the CA to be certified.

- Creating a Self-Signed Certificate. This method is the same as requesting a certificate, only the authentication of the public key does not require a CA. This is mainly intended for use within small organizations.
- Loading a PKCS#12 Format Certificate. This method loads a certificate using an already available and certified set of private and public keys.

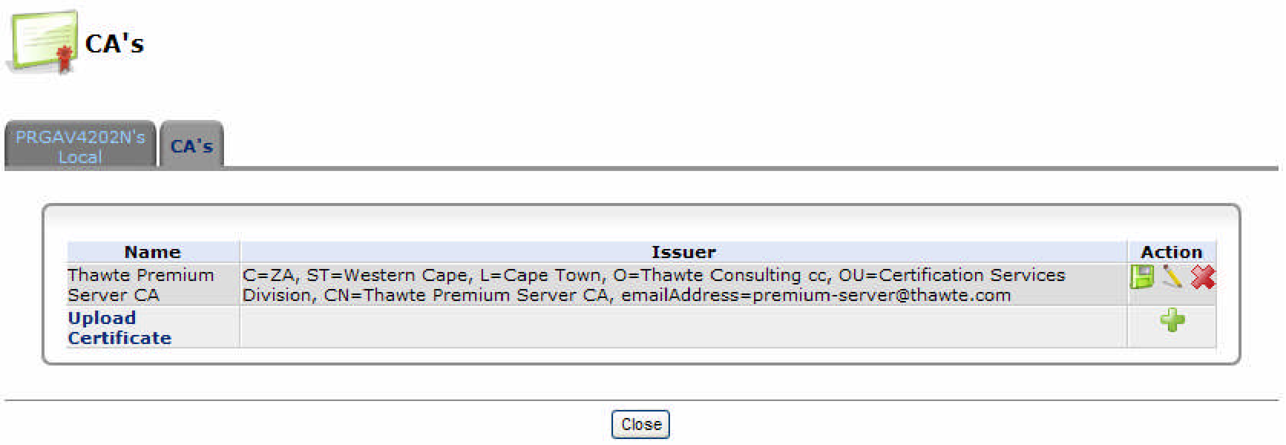
FIGURE 5. Certificates >> Discus's Local Panel



Name	Issuer	Action
OpenRG	C=US, CN=ORname_Jungo: OpenRG Products Group	💾 ✎ ✖
Upload Certificate		+

Certificate Authority (CA) Store. This store contains a list of the trusted certificate authorities, which is used to check certificates presented by the Router clients.

FIGURE 6. Certificates >> CA's Panel

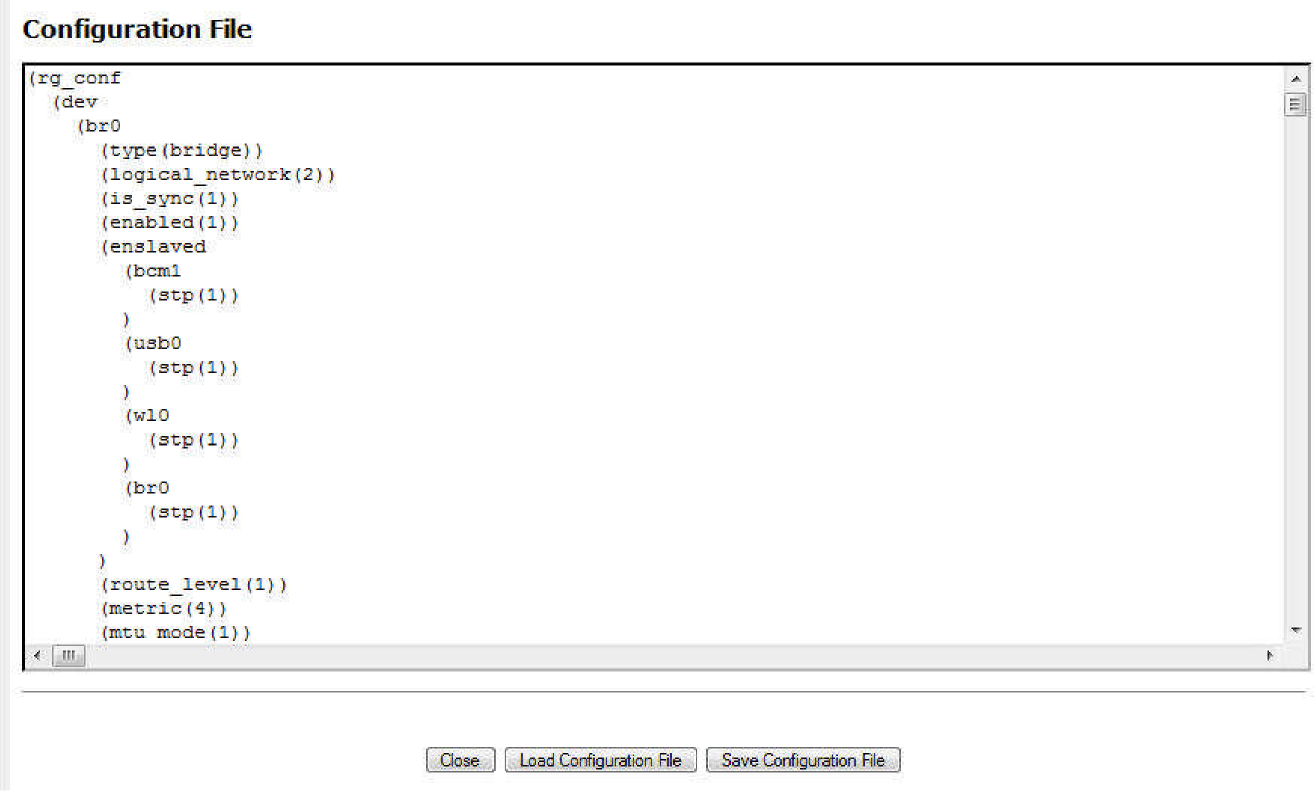


Name	Issuer	Action
Thawte Premium Server CA	C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc, OU=Certification Services Division, CN=Thawte Premium Server CA, emailAddress=premium-server@thawte.com	💾 ✎ ✖
Upload Certificate		+

CONFIGURATION FILE

This feature is intended to provide the whole configuration of the PRG AV4202N in only one step. You are asked only to locate the file and begin the configuration file loading process. The configuration file is a script containing all the parameters you want to change and it is an alternative to the manually step by step change of the same parameters performed by means of the web screenshots.

FIGURE 7. **Configuration File**



Configuration File

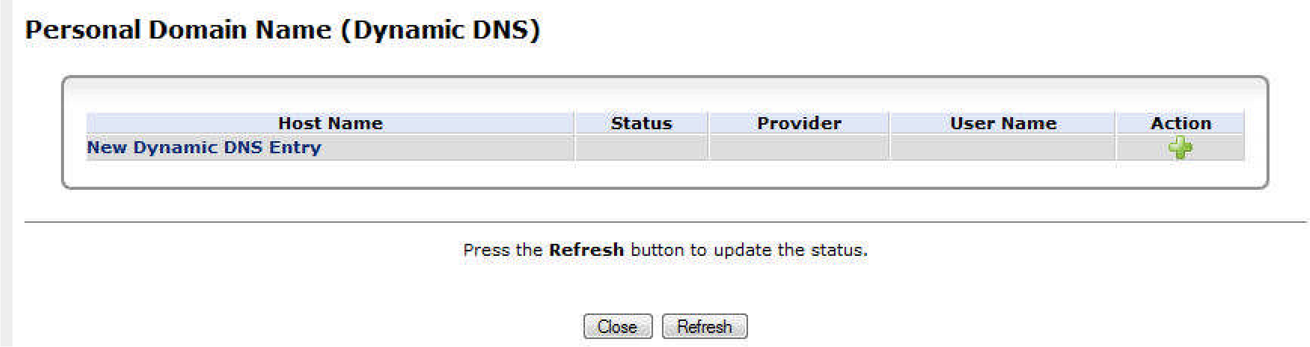
```
(rg_conf
  (dev
    (br0
      (type(bridge))
      (logical_network(2))
      (is_sync(1))
      (enabled(1))
      (enslaved
        (bcm1
          (stp(1))
        )
        (usb0
          (stp(1))
        )
        (wl0
          (stp(1))
        )
        (br0
          (stp(1))
        )
      )
      (route_level(1))
      (metric(4))
      (mtu mode(1))
```

DDNS

The Dynamic DNS (DDNS) service enables you to alias a dynamic IP address to a static hostname, allowing your computer to be more easily accessible from various locations on the Internet. Typically, when you connect to the Internet, your service provider assigns an unused IP address from a pool of IP addresses, and this address is used only for the duration of a specific connection. Dynamically assigning addresses extends the usable pool of available IP addresses, whilst maintaining a constant domain name.

When using the DDNS service, each time the IP address provided by your ISP changes, the DNS database will change accordingly to reflect the change. In this way, even though your IP address will change often, your domain name will remain constant and accessible.

FIGURE 8. **DDNS**



Personal Domain Name (Dynamic DNS)

Host Name	Status	Provider	User Name	Action
New Dynamic DNS Entry				✚

Press the **Refresh** button to update the status.

In order to use the DDNS feature, you must first obtain a DDNS account. For example, you can open a free account at http://www.dyndns.org/account/create.html. When applying for an account, you will need to specify a user name and password.

DNS SERVER

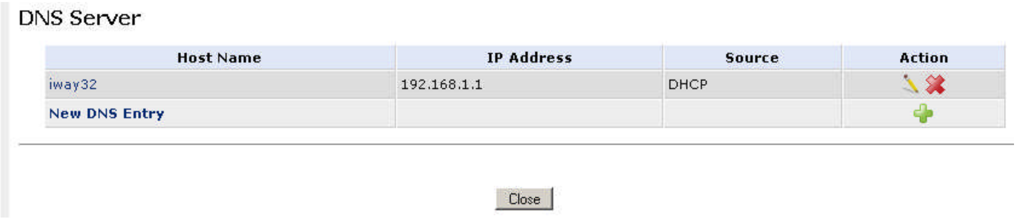
Domain Name System (DNS) provides a service that translates domain names into IP addresses and vice versa. The gateway's DNS server is an auto-learning DNS, which means that when a new computer is connected to the network the DNS server learns its name and automatically adds it to the DNS table. Other network users may immediately communicate with this computer using either its name or its IP address.

In addition your gateway's DNS:

- Shares a common database of domain names and IP addresses with the DHCP server.
- Supports multiple sub-nets within the LAN simultaneously.
- Automatically appends a domain name to unqualified names.
- Allows new domain names to be added to the database using Router's WBM.
- Permits a computer to have multiple host names.
- Permits a host name to have multiple IPs (needed if a host has multiple network cards).

The DNS server does not require configuration. However, you may wish to view the list of computers known by the DNS, edit the host name or IP address of a computer on the list, or manually add a new computer to the list.

FIGURE 9. **DNS Server Panel**



DNS Server

Host Name	IP Address	Source	Action
iway32	192.168.1.1	DHCP	✎ ✖
New DNS Entry			+

To add a new entry to the list:

1. Click the 'New DNS Entry' button. The 'DNS Entry' screen will appear.
2. Enter the computer's host name and IP address.
3. Click 'OK' to save the settings.

PRG AV4202N FIRMWARE UPGRADE

PRG AV4202N offers a built-in mechanism for upgrading its software image, without losing any of your custom configurations and settings. There are two methods for upgrading the software image:

1. Upgrading from a local computer: use a software image file pre-downloaded to your PC's disk drive or located on the accompanying evaluation CD.
2. Upgrading from the Internet: also referred to as Remote Update, use this method to upgrade your Firmware by remotely downloading an updated software image file.

Upgrading From a Local Computer.

To upgrade the router’s software image using a locally available .rmt file: access this feature either from the 'Maintenance' tab under the 'System' screen, or by clicking its icon in the 'Advanced' screen. The ‘Firmware Upgrade' screen will appear

Remote Update.

It helps you keep your software image up-to-date, by performing routine daily checks for newer software versions, as well as letting you perform manual checks.

To view the automatic check utility's settings and last check result, click the 'Firmware Upgrade' icon from the 'Advanced' screen. The 'Firmware Upgrade' screen will appear. In the 'Upgrade From the Internet' section, you can select the utility's checking method and interval. The result of the last performed check is displayed by the line between the 'Check Now' and 'Force Upgrade' buttons, indicating whether a new version is available or not.

If a new version is available:

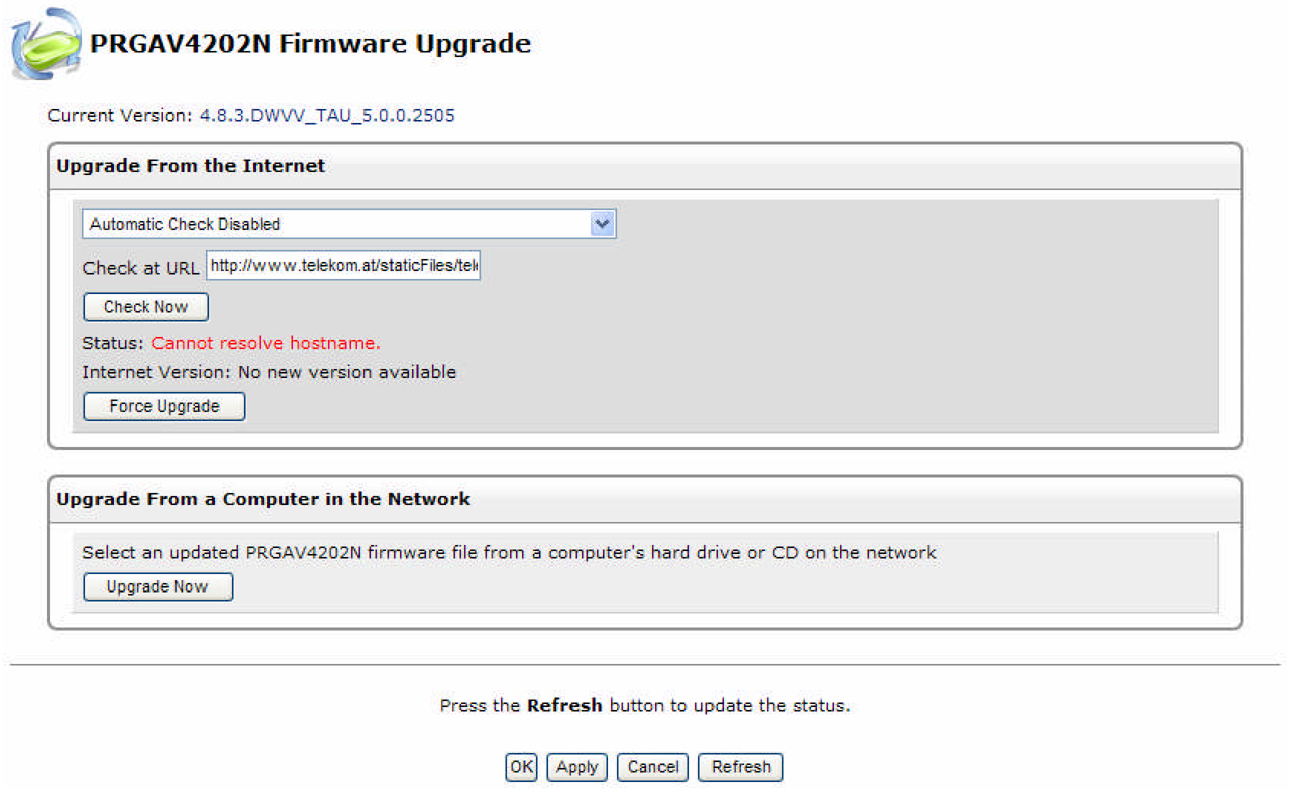
- Press the 'Force Upgrade' button. A download process will begin. When downloading is completed, a confirmation screen will appear, asking you if you want to upgrade to the new version.

- Click 'OK' to confirm. The upgrade process will begin and should take no longer than one minute to complete.

At the conclusion of the upgrade process the Router will automatically reboot. The new software version will run, maintaining your custom configurations and settings.

If a new version is not available press the 'Check Now' button to perform an immediate check (instead of waiting for the next scheduled one). The screen will display a green "*Check in progress...*" message.

FIGURE 10. PRG AV4202N Firmware Upgrade Panel



PRGAV4202N Firmware Upgrade

Current Version: 4.8.3.DWVV_TAU_5.0.0.2505

Upgrade From the Internet

Automatic Check Disabled

Check at URL http://www.telekom.at/staticFiles/tel

Status: Cannot resolve hostname.

Internet Version: No new version available

Upgrade From a Computer in the Network

Select an updated PRGAV4202N firmware file from a computer's hard drive or CD on the network

Press the **Refresh** button to update the status.

DATE AND TIME

To configure date, time and daylight savings time settings perform the following:

1. Click the 'Date and Time' icon in the 'Advanced' screen of the Web-based Management. The 'Date & Time' settings screen will be displayed
2. Select the local time zone from the pull-down menu. The Router can automatically detect daylight saving setting for selected time zones. If the daylight saving settings for your time zone are not automatically detected, the following fields will be displayed:

   - Enabled. Select this check box to enable daylight saving time.

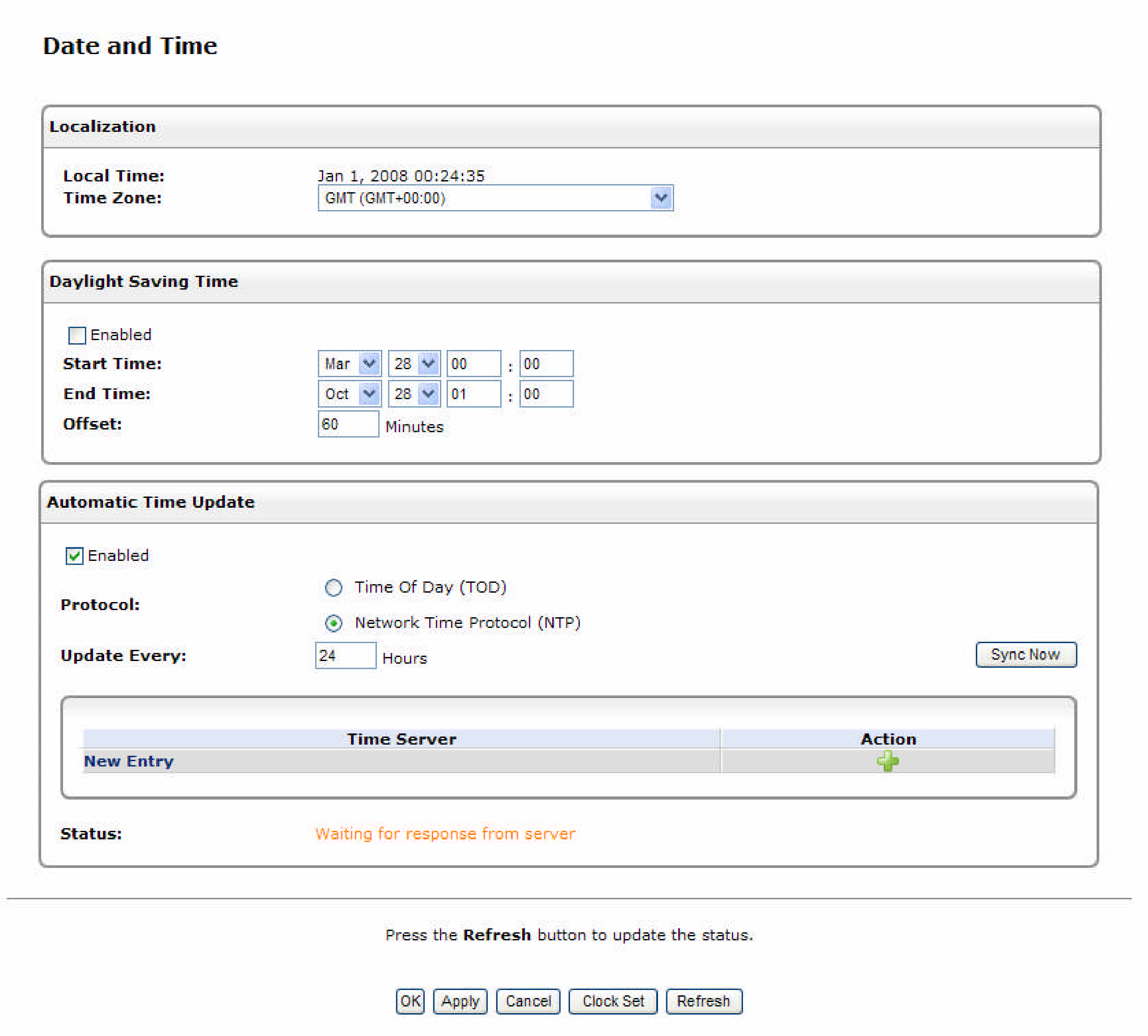
   - Start. Date and time when daylight saving starts.

   - End. Date and time when daylight saving ends.

   - Offset. Daylight saving time offset.
3. If you want the gateway to perform an automatic time update, perform the following:

- Select the 'Enabled' check-box under the 'Automatic Time Update' section.
- Select the protocol to be used to perform the time update by selecting wither the 'Time of Day' or 'Network Time Protocol' radio button.
- Specify how often to perform the update in the 'Update Every' field.
- You can define time server addresses by pressing the 'New Entry' link on the bottom of the 'Automatic Time Update' section.

FIGURE 11. Date and Time Panel



Date and Time

Localization

Local Time: Jan 1, 2008 00:24:35

Time Zone: GMT (GMT+00:00)

Daylight Saving Time

☐ Enabled

Start Time: Mar 28 00 : 00

End Time: Oct 28 01 : 00

Offset: 60 Minutes

Automatic Time Update

☑ Enabled

Protocol: ○ Time Of Day (TOD) ● Network Time Protocol (NTP)

Update Every: 24 Hours

Time Server	Action
New Entry	✚

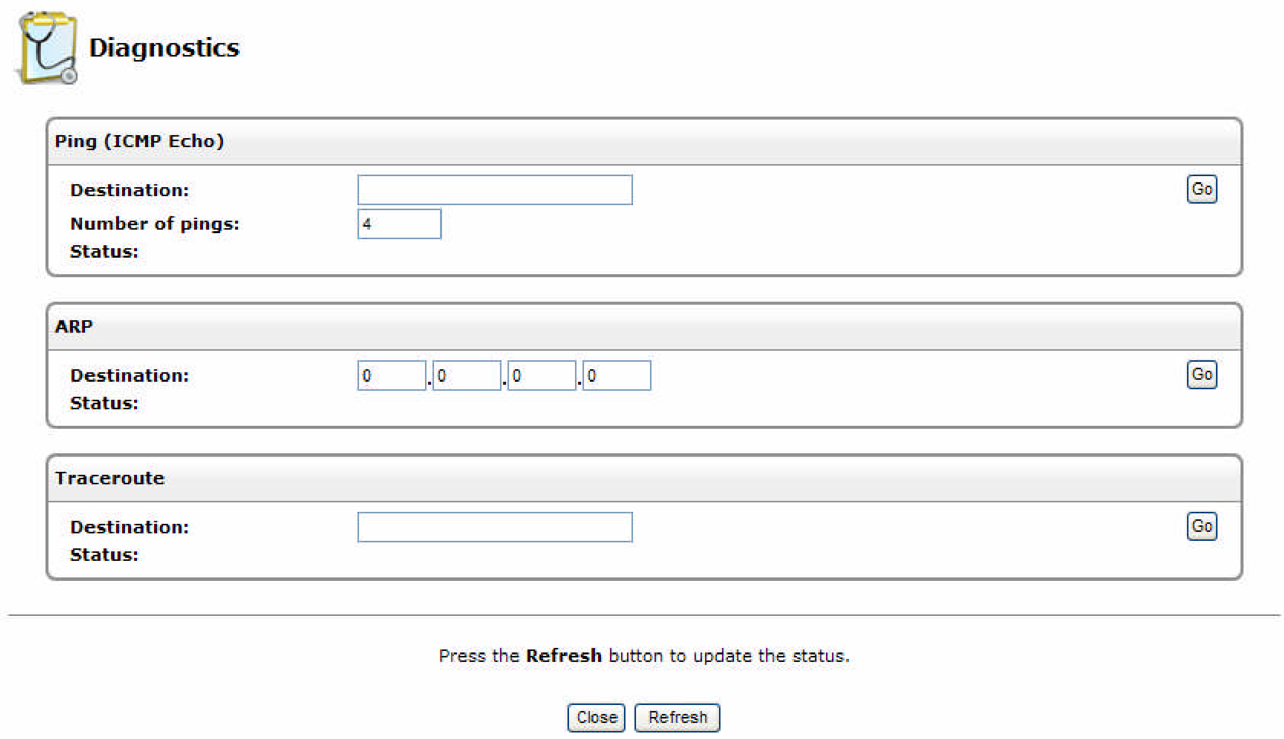
Status: Waiting for response from server

Press the **Refresh** button to update the status.

DIAGNOSTICS

The Diagnostics screen can assist you in testing network connectivity and viewing statistics, such as the number of packets transmitted and received, round-trip time and success status.

FIGURE 12. **Diagnostics Panel**



Diagnostics

Ping (ICMP Echo)

Destination:

Number of pings: 4

Status:

ARP

Destination: 0 . 0 . 0 . 0

Status:

Traceroute

Destination:

Status:

Press the **Refresh** button to update the status.

Ping (ICMP Echo). To diagnose network connectivity, follow these steps:

1. Click the 'Diagnostics' icon from the 'Advanced' screen in the Web-based Management. The 'Diagnostics' screen will appear.
2. Under the Ping (ICMP Echo) section, enter the IP address or URL to be tested in the 'Destination' field.
3. Enter the number of pings you would like to perform.
4. Press the 'Go' button.
5. In a few seconds, diagnostic statistics will be displayed. If no new information is displayed, press the 'Refresh' button.

ARP. To perform an ARP packet test.

Performing a Traceroute. To perform a traceroute, follow these steps:

1. Click the 'Diagnostics' icon from the 'Advanced' screen in the Web-based Management. The 'Diagnostics' screen will appear.
2. Under the Traceroute section, enter the IP address or URL to be tested in the 'Destination' field.
3. Press the 'Go' button. A traceroute will commence, constantly refreshing the screen.

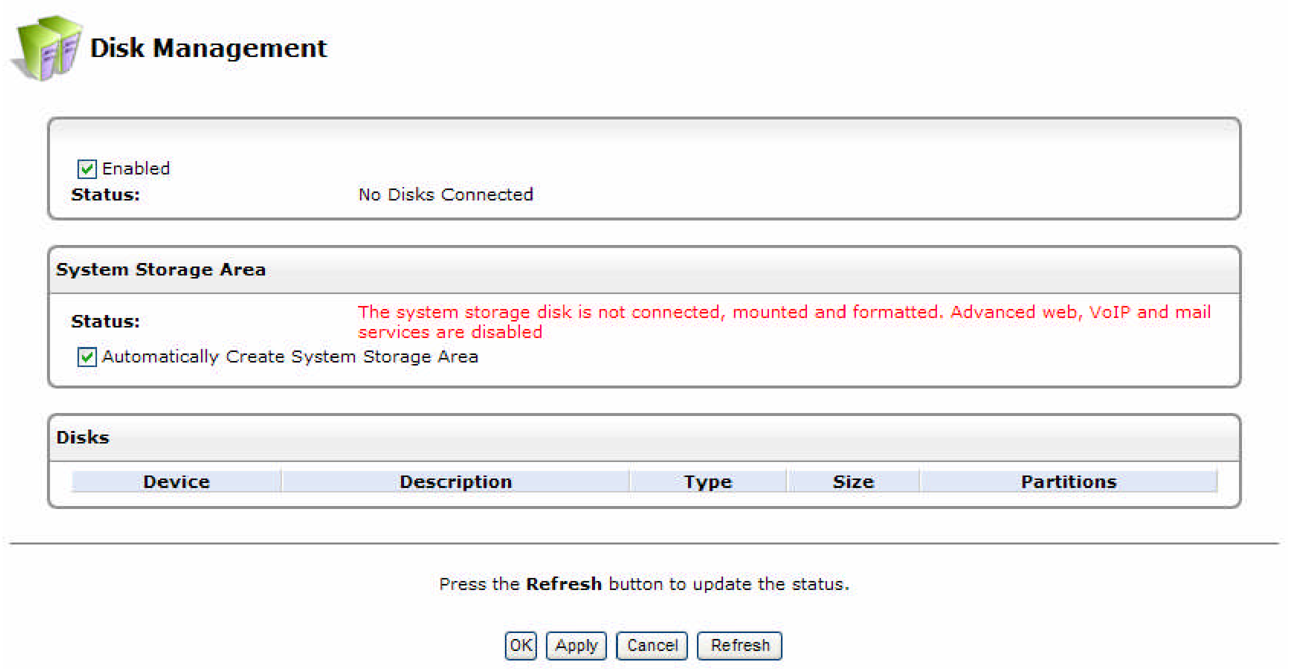
4. To stop the trace and view the results, press 'Cancel'.

DISK MANAGEMENT

PRG AV4202N can operate as a disk manager for external storage devices connected via USB or FireWire. Your home-network's LAN devices can share this storage device as a mapped network drive, and exchange information without directly accessing each other. The Web based management provides disk management utilities such as partitioning and formatting.

An internal disk or a connected storage device will appear on the network map. You can view information about the disk by clicking its icon. The 'Disk Information' screen will appear. For a broader view, click the 'Shared Storage' link from the 'Local Network' tab of the Web-based management. The 'Disk Management' screen will appear.

FIGURE 13. Disk Management Panel



Disk Management

☑ Enabled

Status: No Disks Connected

System Storage Area

Status: The system storage disk is not connected, mounted and formatted. Advanced web, VoIP and mail services are disabled

☑ Automatically Create System Storage Area

Disks

Device	Description	Type	Size	Partitions

Press the **Refresh** button to update the status.

Enabled. Check or un-check this box to enable or disable this feature.

System Data. The the name of the partition intended to hold the system data.

User Data. The the name of the partition intended to hold the user data.

Disks. This section displays a table with your connected storage devices. The 'Device' column displays the names the Router grants connected devices. Click this link to view the device's 'Disk Information' screen. If a device is partitioned, the 'Partitions' column will display its partition names. If the partitions are formatted, their name will include a letter.

RAID Devices. This section displays the RAID devices when configured.

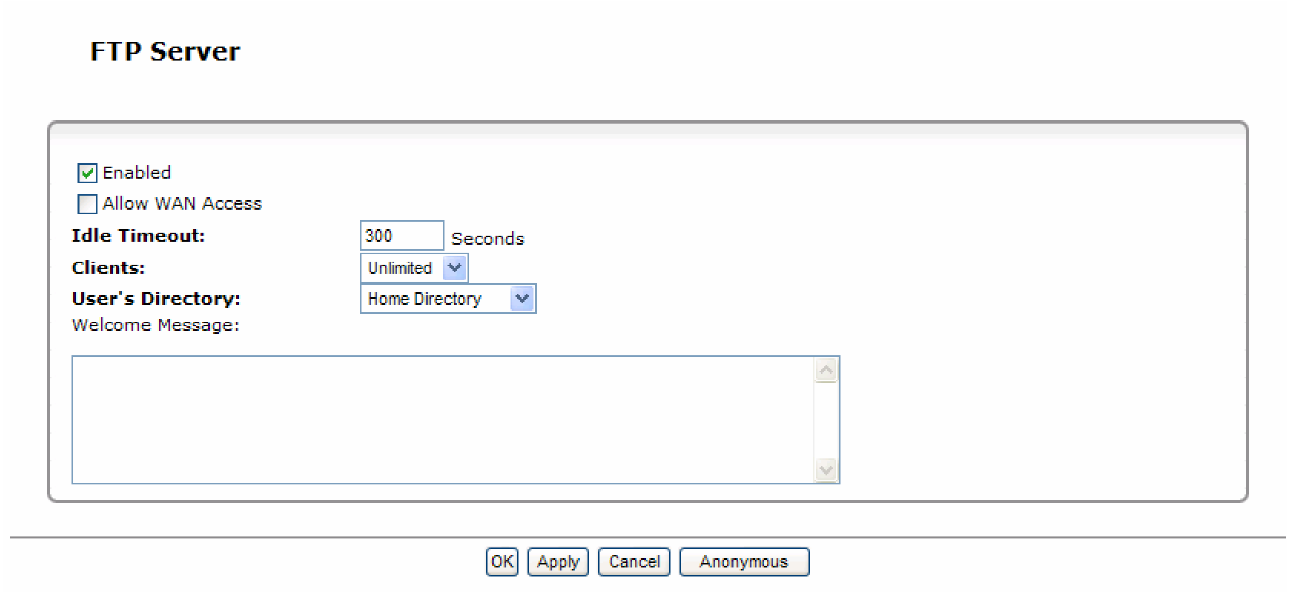
FTP SERVER

Discus can operate as a File Transfer Protocol (FTP) server, allowing users and guests to access its internal disks, to easily (but securely) exchange files. Discus FTP access consists of two levels:

• User Access Registered users can access predefined directories, which are protected by their username and password.

• Anonymous Access Guests can access predefined public directories. This feature allows you,

FIGURE 14. FTP Server Panel



FTP Server

☑ Enabled

□ Allow WAN Access

Idle Timeout: 300 Seconds

Clients: Unlimited

User's Directory: Home Directory

Welcome Message:

FILE SERVER

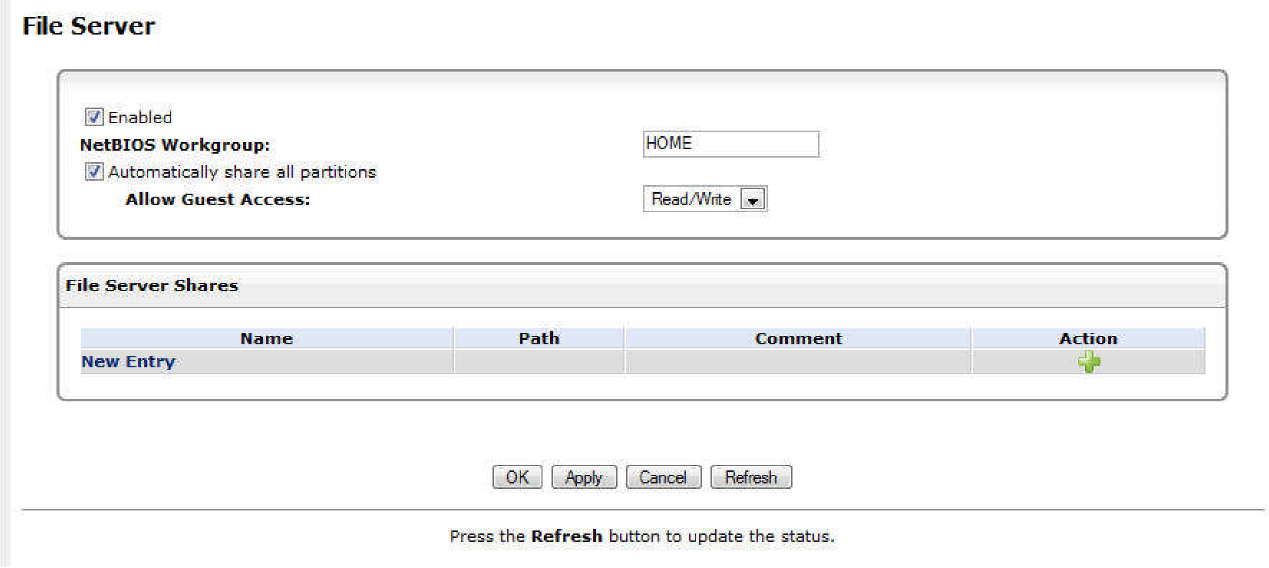
The Router provides a file server utility, allowing you to perform various tasks on your files, such as manage file server shares and define access control lists. The file server utility complements Discus' disk management.

Access the File Server settings either from its link in the 'Storage' tab under the 'Services' screen, or by clicking the 'File Server' icon in the 'Advanced' screen. The 'File Server' screen will appear.

Enabled. Check or un-check this box to enable or disable this feature. NetBIOS Workgroup Discus' workgroup name that will be displayed in the Windows network map of LAN hosts.

File Server Shares. Define file shares on your disk partitions.

FIGURE 15. **File Server Panel**



File Server

☑ Enabled

NetBIOS Workgroup: HOME

☑ Automatically share all partitions

Allow Guest Access: Read/Write

File Server Shares

Name	Path	Comment	Action
New Entry			✚

Press the **Refresh** button to update the status.

IP ADDRESS DISTRIBUTION

Your gateway's Dynamic Host Configuration Protocol (DHCP) server makes it possible to easily add computers that are configured as DHCP clients to the home network. It provides a mechanism for allocating IP addresses and delivering network configuration parameters to such hosts. Router's default DHCP server is the LAN bridge.

A client (host) sends out a broadcast message on the LAN requesting an IP address for itself. The DHCP server then checks its list of available addresses and leases a local IP address to the host for a specific period of time and simultaneously designates this IP address as `taken'. At this point the host is configured with an IP address for the duration of the lease.

The host can choose to renew an expiring lease or let it expire. If it chooses to renew a lease then it will also receive current information about network services, as it did with the original lease, allowing it to update its network configurations to reflect any changes that may have occurred since it first connected to the network. If the host wishes to terminate a lease before its expiration it can send a release message to the DHCP server, which will then make the IP address available for use by others.

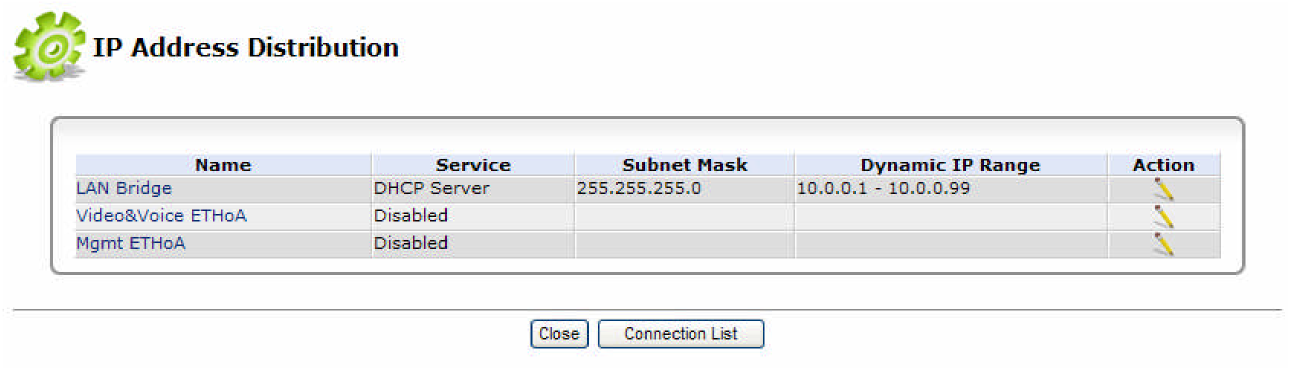
Your gateway's DHCP server:

- Displays a list of all DHCP host devices connected to the Router
- Defines the range of IP addresses that can be allocated in the LAN
- Defines the length of time for which dynamic IP addresses are allocated
- Provides the above configurations for each LAN device and can be configured and enabled/disabled separately for each LAN device
- Can assign a static lease to a LAN PC so that it receives the same IP address each time it connects to the network, even if this IP address is within the range of addresses that the DHCP server may assign to other computers
- Provides the DNS server with the host name and IP address of each PC that is connected to the LAN

Additionally, the Router can act as a DHCP relay, escalating DHCP responsibilities to a WAN DHCP server. In this case, PRG AV4202N will act merely as a router, while its LAN hosts will receive their IP addresses from a DHCP server on the WAN.

With the Router's optional Zero Configuration Technology feature, the IP Auto Detection method detects statically-defined IP addresses in addition to the Router's DHCP clients. It learns all the IP addresses on the LAN, and integrates the collected information with the database of the DHCP server. This allows the DHCP server to issue valid leases, thus avoiding conflicting IP addresses used by other computers in the network.

FIGURE 16. IP Address Distribution Panel



IP Address Distribution

Name	Service	Subnet Mask	Dynamic IP Range	Action
LAN Bridge	DHCP Server	255.255.255.0	10.0.0.1 - 10.0.0.99	✎
Video&Voice ETHoA	Disabled			✎
Mgmt ETHoA	Disabled			✎

IPSEC

Internet Protocol Security (IPSec) is a series of guidelines for the protection of Internet Protocol (IP) communications. It specifies procedures for securing private information transmitted over public networks. The IPSec protocols include: AH (Authentication Header) provides packet-level authentication, ESP (Encapsulating Security Payload) provides encryption and authentication, IKE (Internet Key Exchange) negotiates connection parameters, including keys, for the other two services.

Services supported by the IPSec protocols (AH, ESP) include confidentiality (encryption), authenticity (proof of sender), integrity (detection of data tampering), and replay protection

(defense against unauthorized resending of data). IPSec also specifies methodologies for key management. Internet Key Exchange (IKE), the IPSec key management protocol, defines a series of steps to establish keys for encrypting and decrypting information; it defines a common language on which communications between two parties is based. Developed by the Internet Engineering Task Force (IETF), IPSec and IKE together standardize the way data protection is performed, thus making it possible for security systems developed by different vendors to interoperate.

Access this feature either from the 'VPN' menu item under the 'Services' tab, or by clicking its icon in the 'Advanced' screen. The 'Internet Protocol Security (IPSec)' screen appears.

Block Unauthorized IP Select the 'Enabled' check box to block unauthorized IP packets to Discus. Specify the following parameters:

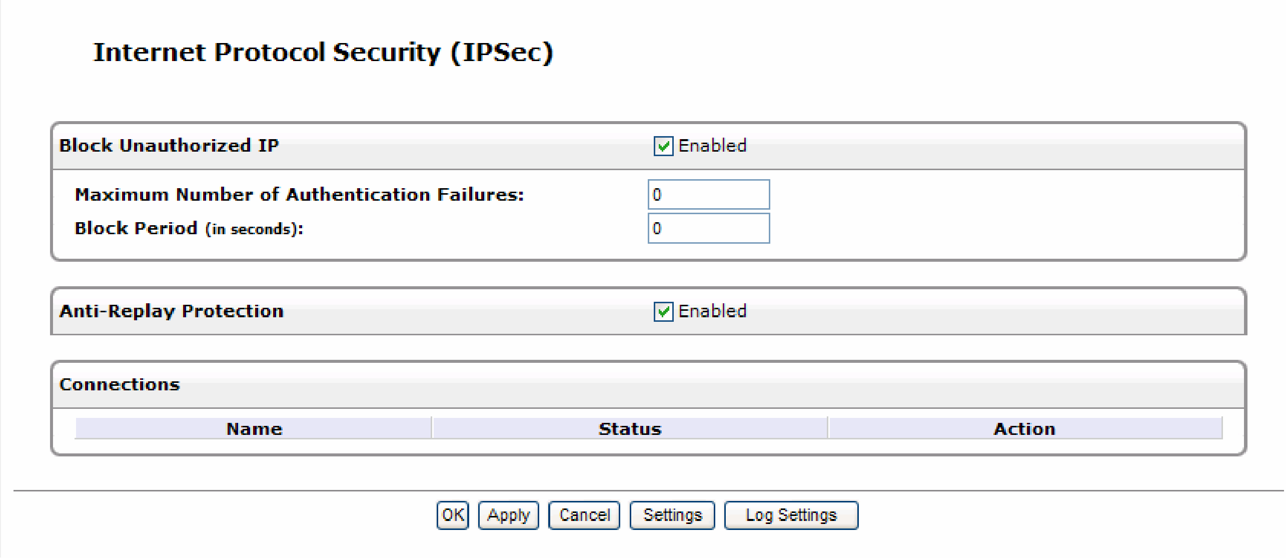
- **Maximum Number of Authentication Failures** The maximum number of packets to authenticate before blocking the origin's IP address.

• **Block Period (in seconds)** The timeframe during which Discus will drop packets from an unauthorized IP address.

Enable Anti-Replay Protection Select this option to enable dropping of packets that are recognized (by their sequence number) as already been received.

Connections This section displays the list of IPSec connections.

FIGURE 17. **IPSec Panel**



Internet Protocol Security (IPSec)

Block Unauthorized IP ☑ Enabled

Maximum Number of Authentication Failures: 0

Block Period (in seconds): 0

Anti-Replay Protection ☑ Enabled

Connections

Name	Status	Action

L2TP SERVER

Access this feature either from its link in the 'VPN' tab under the 'Services' screen, or by clicking the 'L2TP' icon in the 'Advanced' screen. This screen enables you to configure the following:

Enabled Select or deselect this check box to enable or disable this feature. Note that checking this box creates an L2TP server (if not yet created with the wizard), but does not define remote users.

Click Here to Create VPN Users Click this link to define remote users that will be granted access to your home network.

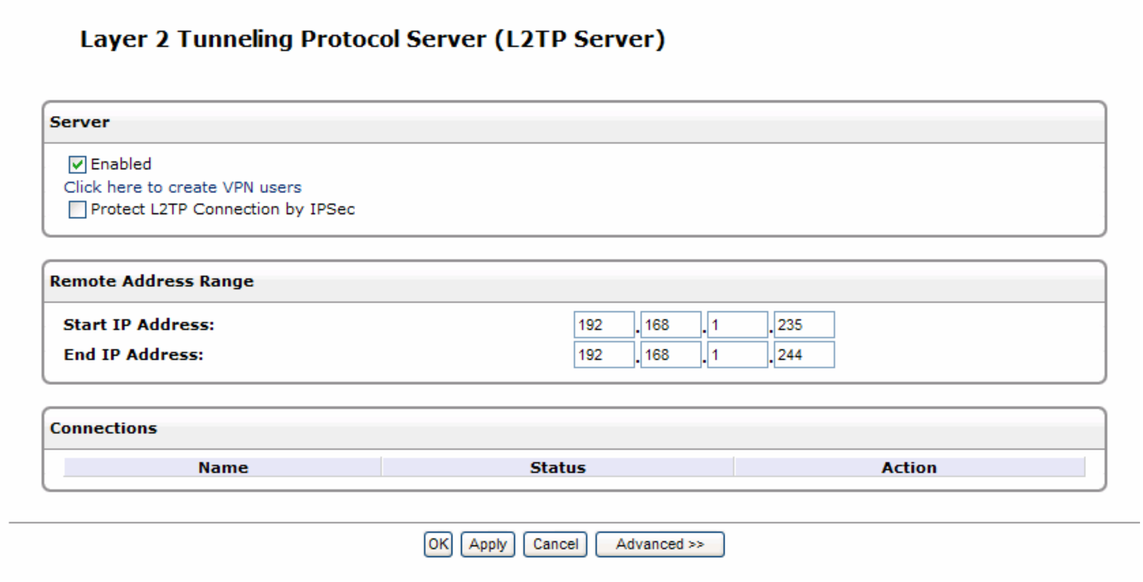
Protect L2TP Connection by IPSec By default, the L2TP connection is not protected by the IP Security (IPSec) protocol. Check this option to enable this feature. When enabled, the following entry appears.

Create Default IPSec Connection When creating an L2TP Server with the connection wizard, a default IPSec connection is created to protect it. If you wish to disable this feature, uncheck this option. However, note that if L2TP protection is enabled by IPSec (see previous entry), you must provide an alternative, active IPSec connection in order for users to be able to connect. When this feature is enabled, the following entry appears.

L2TP Server IPSec Shared Secret You may change the IPSec shared secret, provided when the connection was created, in this field.

Remote Address Range Use the 'Start IP Address' and 'End IP Address' fields to specify the range of IP addresses that will be granted by the L2TP server to the L2TP client.

FIGURE 18. **IPSec Panel**



Layer 2 Tunneling Protocol Server (L2TP Server)

Server

☑ Enabled

Click here to create VPN users

□ Protect L2TP Connection by IPSec

Remote Address Range

Start IP Address:	192 . 168 . 1 . 235
End IP Address:	192 . 168 . 1 . 244

Connections

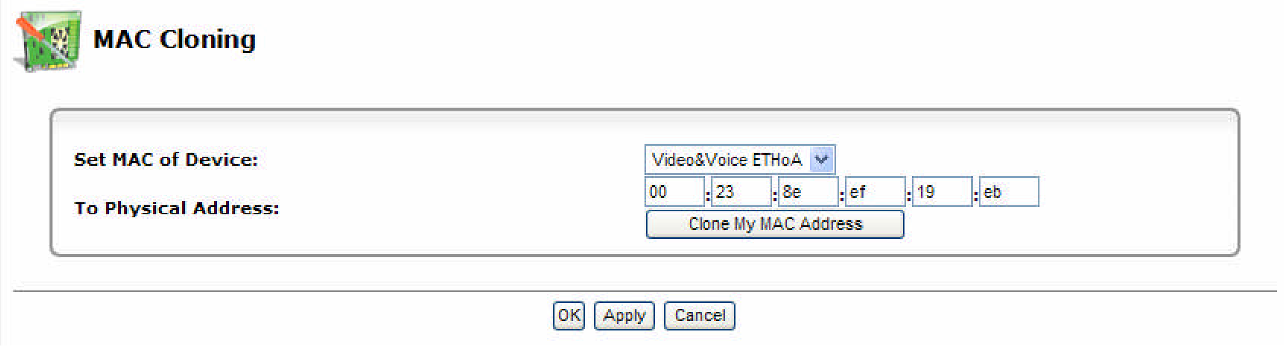
Name	Status	Action

MAC CLONING

A Media Access Control (MAC) address is the numeric code that identifies a device on a network, such as your external cable/DSL modem or a PC network card. Your service provider may ask you to supply the MAC address of your PC, external modem, or both.

When replacing an external modem with the Router, you can simplify the installation process by copying the MAC address of your existing PC to the router. In such a case, you do not need to delay the setup process by informing your service provider of newly installed equipment.

FIGURE 19. MAC Cloning Panel



MAC Cloning

Set MAC of Device: Video&Voice ETHoA

To Physical Address: 00 : 23 : 8e : ef : 19 : eb

MEDIA SHARING

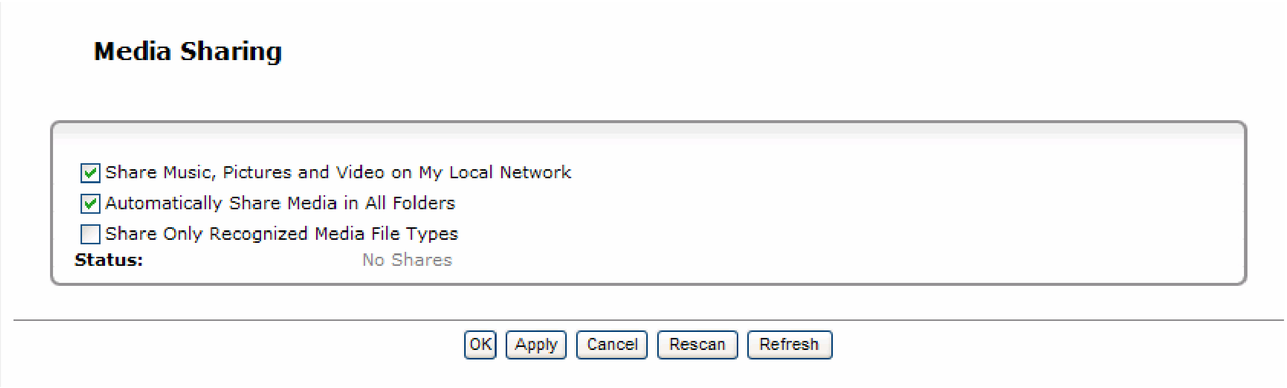
Discus Media Sharing solution enables you to share and stream media files from a storage device connected to Discus. You can access the shared media files with either a networkaware Consumer Electronic (CE) device, or from a LAN PC with an installed media rendering software. Both methods utilize a Universal Plug and Play (UPnP) media renderer. The 'Media Sharing' screen contains the following options:

Share Music, Pictures and Video on My Local Network By default, this option is selected. To disable media sharing, deselect this option.

Automatically Share Media in All Folders By default, this option is selected, causing all partitions and folders on the storage device to become shared automatically.

Share Only Recognized Media File Types When this option is selected, only recognized media files are shared.

FIGURE 20. **Media Sharing Panel**



Media Sharing

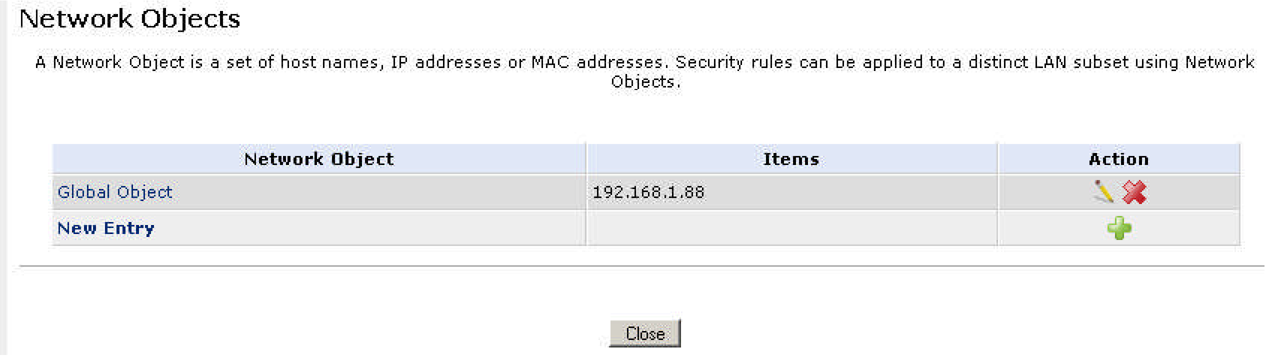
☑ Share Music, Pictures and Video on My Local Network
☑ Automatically Share Media in All Folders
□ Share Only Recognized Media File Types
Status: No Shares

NETWORK OBJECTS

Network Objects is a method used to abstractly define a set of LAN hosts, according to one or more MAC address, IP address, and host name. Defining such a group can assist when configuring system rules. For example, network objects can be used when configuring the Router's security filtering settings such as IP address filtering, host name filtering or MAC address filtering.

You can use network objects in order to apply security rules based on host names instead of IP addresses. This may be useful, since IP addresses change from time to time. Moreover, it is possible to define network objects according to MAC addresses, making rule application more persistent against network configuration settings.

FIGURE 21. **Network Objects Panel**



Network Objects

A Network Object is a set of host names, IP addresses or MAC addresses. Security rules can be applied to a distinct LAN subset using Network Objects.

Network Object	Items	Action
Global Object	192.168.1.88	✎ ✖
New Entry		✚

To define a network object:

1. Click the 'Network Objects' icon in the 'Advanced' screen of the Web-based Management. The 'Network Objects' screen will appear
2. Click the 'New Entry' link, the 'Edit Network Object' screen will appear.
3. Name the network object in the Description field, and click New Entry to actually create it. The 'Edit Item' screen will appear. The source address can be entered in one of the following methods: IP Address, IP Subnet, IP Range, MAC Address and Host Name. When selecting a method from the combo-box, the screen will refresh, presenting the respective fields by which to enter the relevant information.
4. Select a method and enter the source address accordingly.
5. Click 'OK' to save the settings.

PPTP SERVER

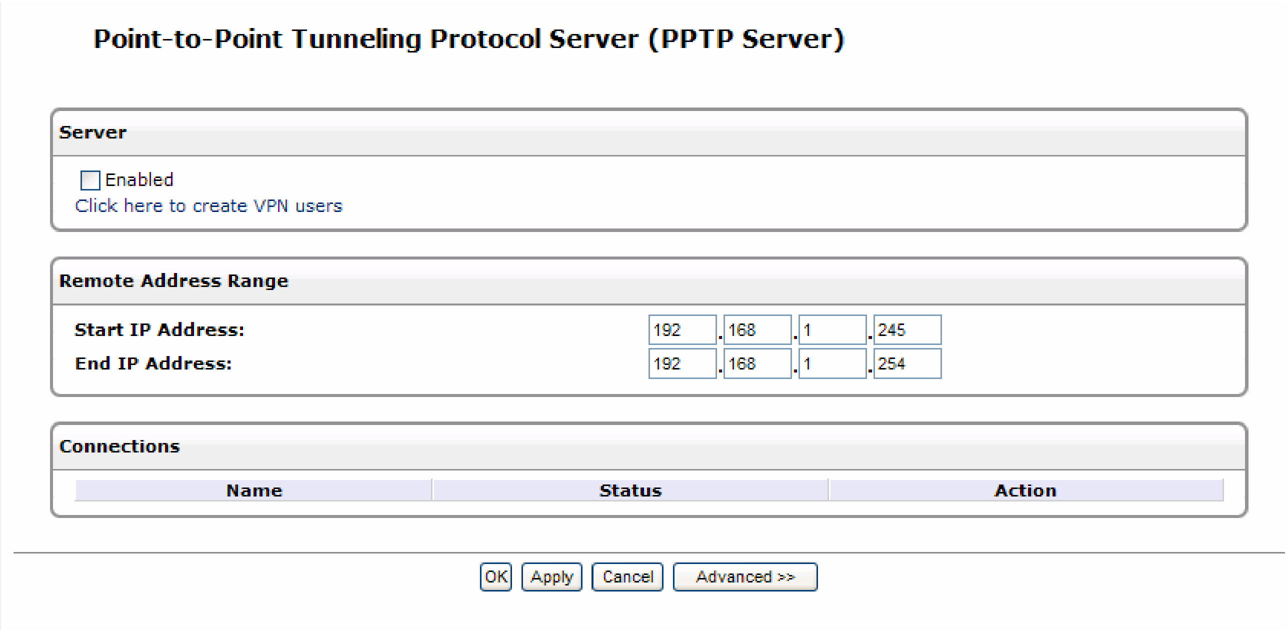
PRG AV4202N can act as a Point-to-Point Tunneling Protocol Server (PPTP Server), accepting PPTP client connection requests. This screen enables you to configure:

Enabled Select or deselect this check box to enable or disable this feature. Note that checking this box creates a PPTP server (if not yet created with the wizard), but does not define remote users.

Click Here to Create VPN Users Click this link to define remote users that will be granted access to your home network.

Remote Address Range Use the 'Start IP Address' and 'End IP Address' fields to specify the range of IP addresses that will be granted by the PPTP server to the PPTP client.

FIGURE 22. **PPTP Server Panel**



Point-to-Point Tunneling Protocol Server (PPTP Server)

Server

□ Enabled

Click here to create VPN users

Remote Address Range

Start IP Address: 192 . 168 . 1 . 245

End IP Address: 192 . 168 . 1 . 254

Connections

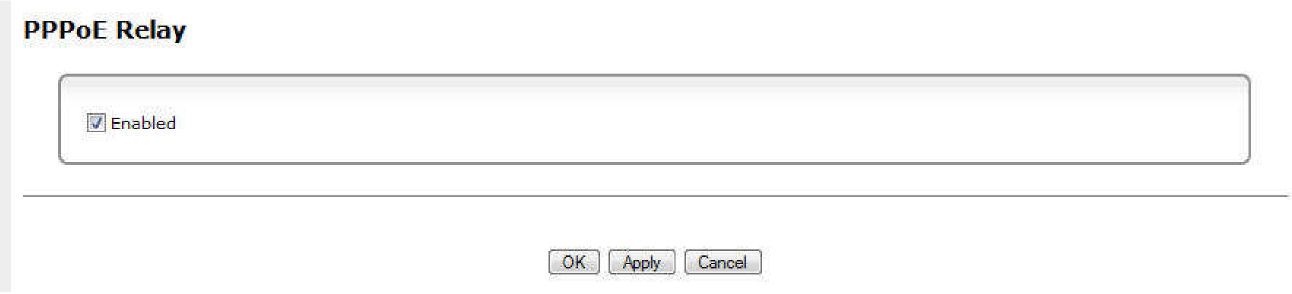
Name	Status	Action

PPPOE RELAY

PPPoE Relay enables PRG AV4202N to relay packets on PPPoE connections, while keeping its designated functionality for any additional connections.

The PPPoE Relay screen displays a check-box that enables PPPoE Relay.

FIGURE 23. **PPPoE Relay Panel**



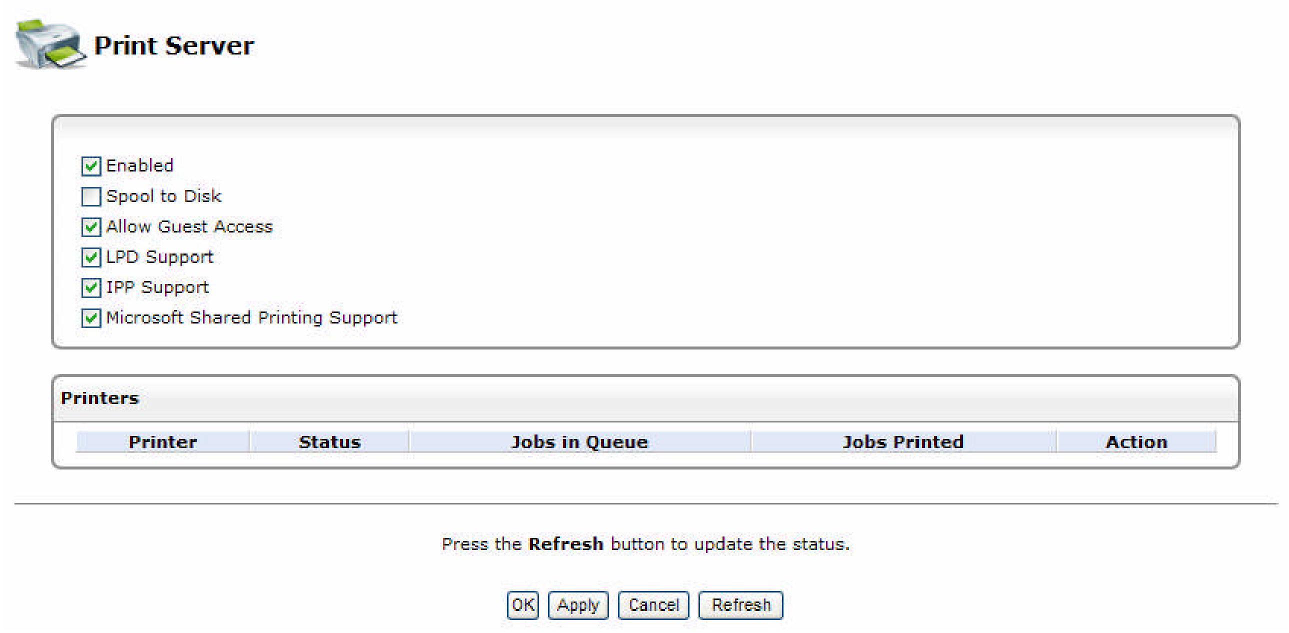
PPPoE Relay

☑ Enabled

PRINT SERVER

The PRG AV4202N can act as a Print Server. Through this panel user can manage and track printer server tasks.

FIGURE 24. **Print Server Panel**



Print Server

☑ Enabled
□ Spool to Disk
☑ Allow Guest Access
☑ LPD Support
☑ IPP Support
☑ Microsoft Shared Printing Support

Printers

Printer	Status	Jobs in Queue	Jobs Printed	Action

Press the **Refresh** button to update the status.

PROTOCOLS

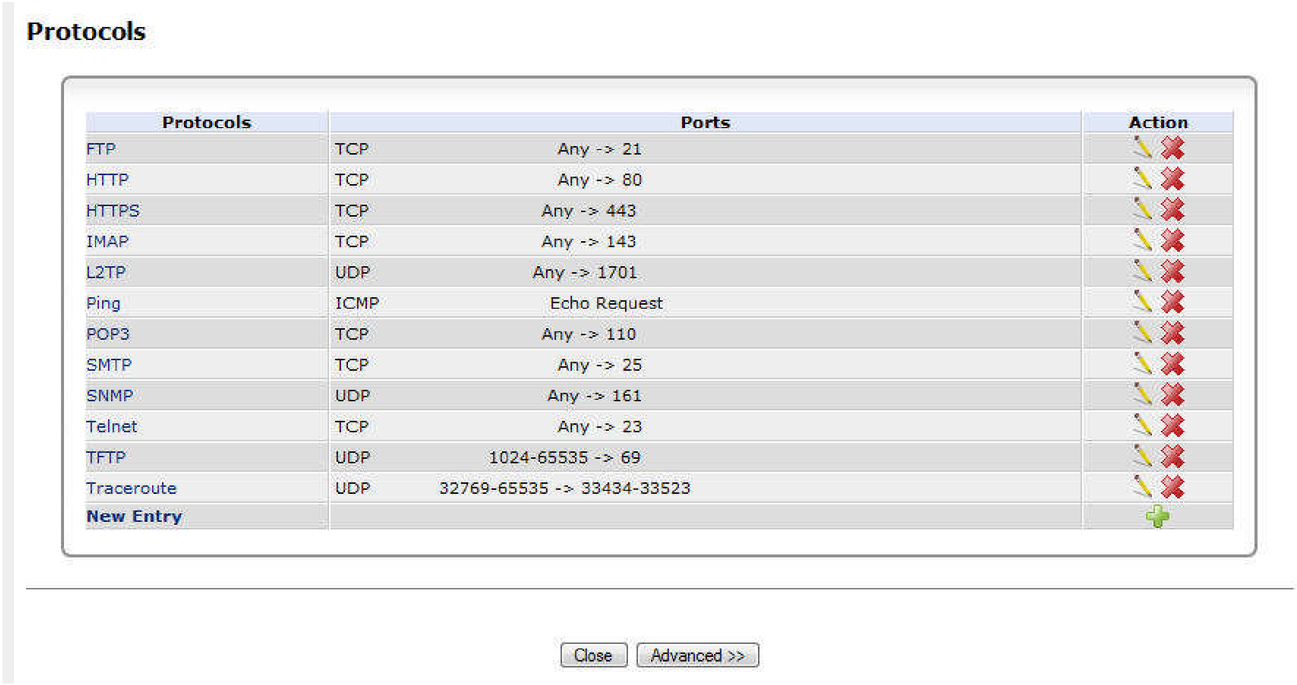
The Protocols feature incorporates a list of preset and user-defined applications and common port settings. You can use protocols in various security features such as Access Control and Port Forwarding. You may add new protocols to support new applications or edit existing ones according to your needs.

To view the basic protocols list, click the 'Protocols' icon in the 'Advanced' screen. Press the 'Advanced' button at the bottom of this screen for the full list of protocols supported by the Router.

To define a protocol:

1. Click the 'Protocols' icon in the 'Advanced' screen. The 'Protocols' screen will appear.
2. Click the 'New Entry' link, the 'Edit Service' screen will appear.
3. Name the service in the 'Service Name' field, and click the 'New Service Ports' link. The 'Edit Service Server Ports' screen will appear. You may choose any of the protocols available in the combo-box, or add a new one by selecting 'Other'. When selecting a protocol from the combo-box, the screen will refresh, presenting the respective fields by which to enter the relevant information.
4. Select a protocol and enter the relevant information.
5. Click 'OK' to save the settings.

FIGURE 25. **Protocols Panel**



Protocols

Protocols	Ports		Action
FTP	TCP	Any -> 21	✎ ✖
HTTP	TCP	Any -> 80	✎ ✖
HTTPS	TCP	Any -> 443	✎ ✖
IMAP	TCP	Any -> 143	✎ ✖
L2TP	UDP	Any -> 1701	✎ ✖
Ping	ICMP	Echo Request	✎ ✖
POP3	TCP	Any -> 110	✎ ✖
SMTP	TCP	Any -> 25	✎ ✖
SNMP	UDP	Any -> 161	✎ ✖
Telnet	TCP	Any -> 23	✎ ✖
TFTP	UDP	1024-65535 -> 69	✎ ✖
Traceroute	UDP	32769-65535 -> 33434-33523	✎ ✖
New Entry			✚

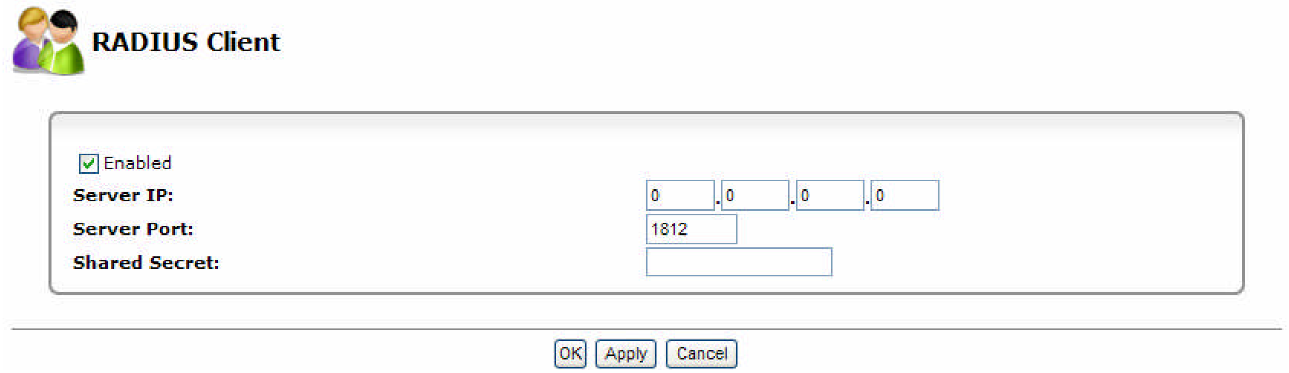
RADIUS

For authentication to work, the client's transmission must go through the Router, and reach the back-end server that performs the actual authentication. The wireless client contacts the access point, which in turn communicates with the Remote Authentication Dial-in User Service (RADIUS) server. The RADIUS server verifies the client's credentials to determine whether the device is authorized to connect to the LAN. If the RADIUS server accepts the client, the server responds by exchanging data with the Router, including security keys for subsequent encrypted sessions.

To configure the RADIUS authentication mechanism, perform the following steps:

1. Click the 'RADIUS' icon in the 'Advanced' screen of the Web based Management. The RADIUS screen will appear.
2. Specify the following parameters:
   - **Enabled**: Select this check-box to enable RADIUS client authentication.
   - **Server IP**: Type in the RADIUS server's IP address.
   - **Server Port**: Type in the RADIUS server's port.
   - **Shared Secret**: Type in your shared secret.

FIGURE 26. **RADIUS Panel**



RADIUS Client

☑ Enabled

Server IP: 0 . 0 . 0 . 0

Server Port: 1812

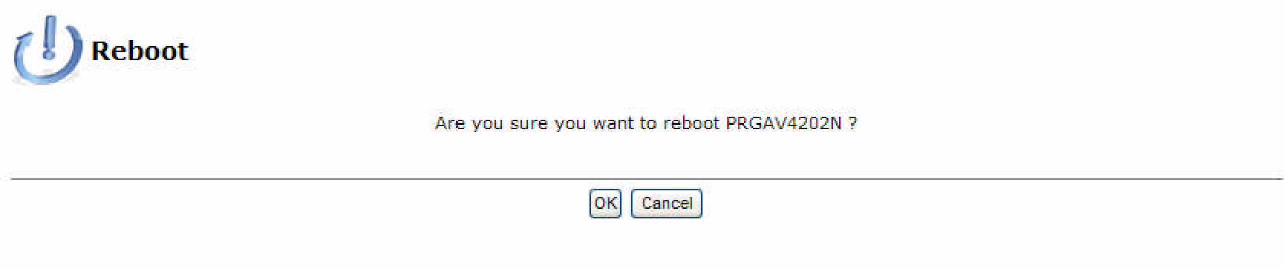
Shared Secret:

REBOOT

To reboot **PRG AV4202N**:

1. Click the 'Reboot' icon in the 'Advanced' screen of the WBM. The 'Reboot' screen will appear.
2. Press 'OK' to reboot the Router. This may take up to one minute. To re-enter the WBM after restarting the gateway, press the browser's 'Refresh' button.

FIGURE 27. **Reboot Panel**



Reboot

Are you sure you want to reboot PRGAV4202N ?

REMOTE ADMINISTRATION

It is possible to access and control **PRG AV4202N** not only from within the home network, but also from the Internet. This allows you to view or change settings while travelling. It also enables you to allow your ISP to change settings or help you troubleshoot functionality or communication issues from a remote location.

Remote access to the Router is blocked by default to ensure the security of your home network. However, remote access is supported by the following services, and you may use the 'Remote Administration' screen to selectively enable these services if they are needed.

To view the Router's remote administration options, click the 'Remote Administration' icon in the 'Advanced' screen of the Web-based management. The 'Remote Administration' screen will appear.

To allow remote access to the Router services:

1. Select the services that you would like to make available to computers on the Internet. The following should be taken into consideration:

- Although Telnet service is password-protected, it is not considered a secured protocol. When allowing incoming access to a Telnet server, if port forwarding is configured to use port 23, select port 8023 to avoid conflicts.
- When allowing incoming access to the Web-based management, if port forwarding is configured to use port 80, select port 8080 to avoid conflicts.

2. Click 'OK' to save the settings.

Allow Incoming WAN Access to the Web-Management. Used to obtain access to the Web-based Management and gain access to all system settings and parameters (using a browser). Both secure (HTTPS) and non-secure (HTTP) access is available.

Allow Incoming WAN Access to the Telnet Server. Used to create a command-line session and gain access to all system settings and parameters (using a text-based terminal).

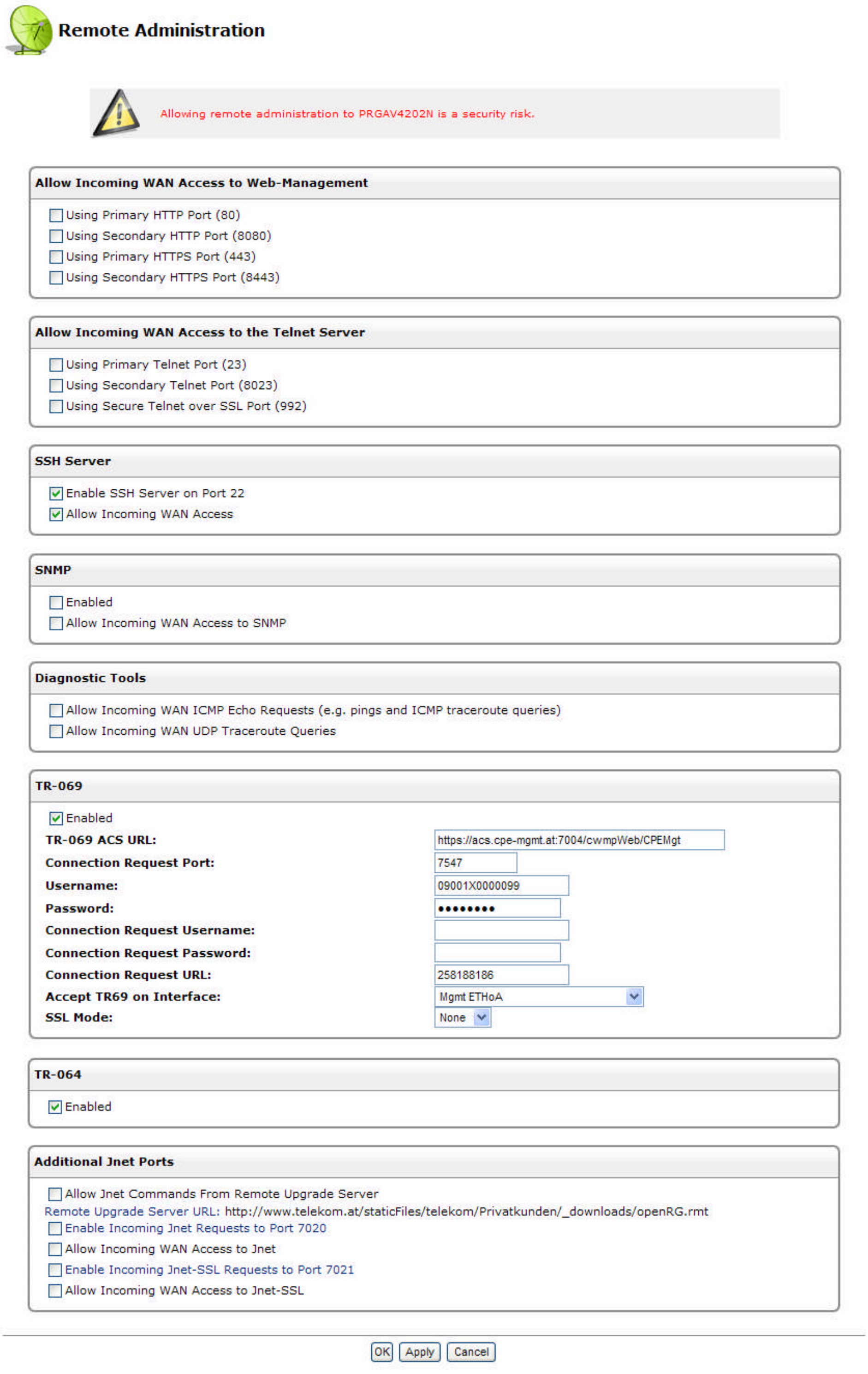
SSH Server. Similar to Telnet, this protocol is used to create a secured command line session and gain access to all system settings and parameters.

Diagnostic Tools. Used for troubleshooting and remote system management by you or your Internet Service Provider. The utilities that can be used are Ping and Traceroute (over UDP).

TR-069. TR-069 is a WAN management protocol intended for communication between Customer Premise Equipment (CPE) and an Auto-Configuration Server (ACS). It defines a mechanism that encompasses secure auto configuration of a CPE, and also incorporates other CPE management functions into a common framework.

TR-064. As residential gateways offer increasingly complex services, customer premise installation and configuration increase the operators' operational costs. DSL Forum's LAN-Side DSL CPE Configuration protocol, known as TR-064, provides a zero-touch solution for automating the installation and configuration of gateways from the LAN side.

FIGURE 28. Remote Administration Panel



Remote Administration

Allowing remote administration to PRGAV4202N is a security risk.

Allow Incoming WAN Access to Web-Management

☐ Using Primary HTTP Port (80)
☐ Using Secondary HTTP Port (8080)
☐ Using Primary HTTPS Port (443)
☐ Using Secondary HTTPS Port (8443)

Allow Incoming WAN Access to the Telnet Server

☐ Using Primary Telnet Port (23)
☐ Using Secondary Telnet Port (8023)
☐ Using Secure Telnet over SSL Port (992)

SSH Server

☑ Enable SSH Server on Port 22
☑ Allow Incoming WAN Access

SNMP

☐ Enabled
☐ Allow Incoming WAN Access to SNMP

Diagnostic Tools

☐ Allow Incoming WAN ICMP Echo Requests (e.g. pings and ICMP traceroute queries)
☐ Allow Incoming WAN UDP Traceroute Queries

TR-069

☑ Enabled

TR-069 ACS URL:	https://acs.cpe-mgmt.at:7004/cwmpWeb/CPEMgt
Connection Request Port:	7547
Username:	09001X0000099
Password:	••••••••
Connection Request Username:	
Connection Request Password:	
Connection Request URL:	258188186
Accept TR69 on Interface:	Mgmt ETHoA
SSL Mode:	None

TR-064

☑ Enabled

Additional Jnet Ports

☐ Allow Jnet Commands From Remote Upgrade Server
Remote Upgrade Server URL: http://www.telekom.at/staticFiles/telekom/Privatkunden/_downloads/openRG.rmt
☐ Enable Incoming Jnet Requests to Port 7020
☐ Allow Incoming WAN Access to Jnet
☐ Enable Incoming Jnet-SSL Requests to Port 7021
☐ Allow Incoming WAN Access to Jnet-SSL

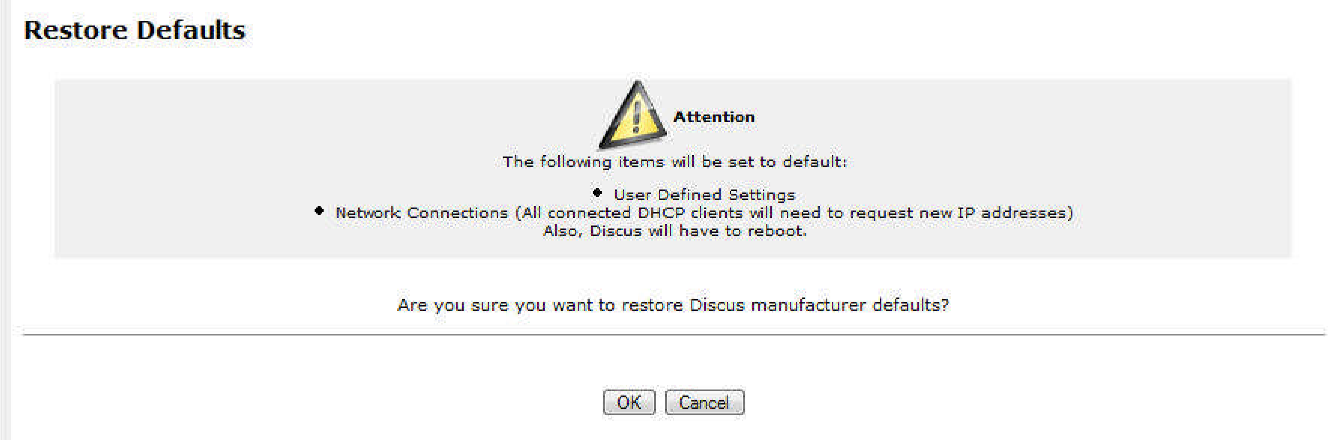
RESTORE DEFAULTS

You may sometimes wish to restore the Router's factory default settings. This may happen, for example, when you wish to build a new network from the beginning, or when you cannot recall changes made to the network and wish to go back to the default configuration.

To restore default settings:

1. Click the 'Restore Defaults' icon in the 'Advanced' screen of the Web-based Management. The 'Restore Defaults' screen will appear
2. Press 'OK' to restore Discus' factory default settings.

FIGURE 29. Restore Defaults Panel



Restore Defaults

Attention

The following items will be set to default:

- User Defined Settings
- Network Connections (All connected DHCP clients will need to request new IP addresses)

Also, Discus will have to reboot.

Are you sure you want to restore Discus manufacturer defaults?

ROUTING

Access the Router's routing settings by clicking the 'Routing' icon from the 'Advanced' screen. The basic 'Routing' screen will appear. Press the 'Advanced' button to view the full routing settings.

Routing Table.

You can add, edit and delete routing rules from the routing table. Click the New Route link. The 'Route Settings' screen will appear. When adding a routing rule, you need to specify the following:

Name: Select the network device.

Destination: The destination is the destination host, subnet address, network address, or default route. The destination for a default route is 0.0.0.0.

Netmask: The network mask is used in conjunction with the destination to determine when a route is used.

Gateway: Enter the gateway's IP address.

Metric: A measurement of the preference of a route. Typically, the lowest metric is the most preferred route. If multiple routes have the same metric value, the default route will be the first in order of appearance.

Routing Protocols

Routing Information Protocol (RIP): Select this check-box in order to enable connections previously defined to use RIP. If this check-box is not selected, RIP will be disabled for all connections, including those defined to use RIP.

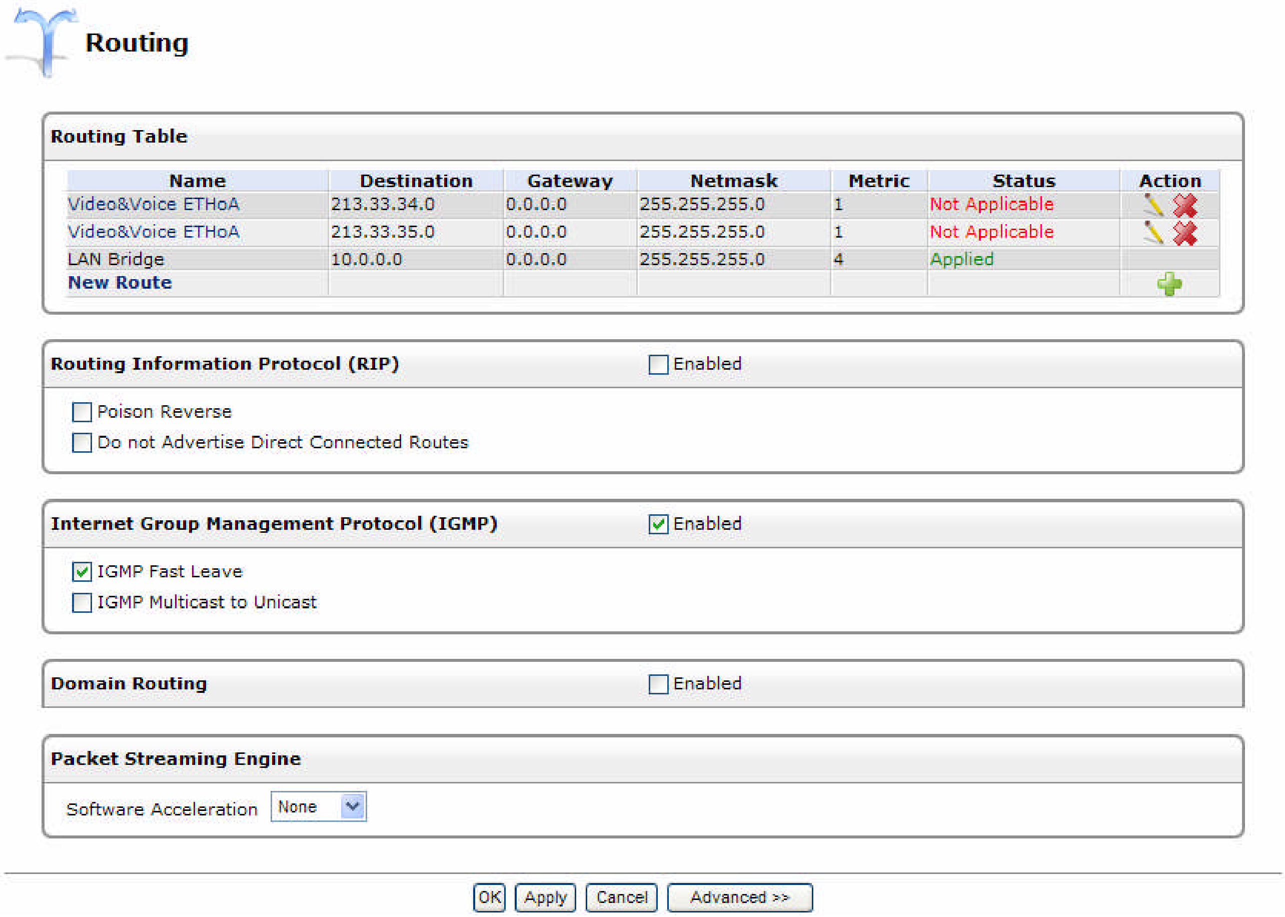
- *Reverse:* Discus will advertise acquired route information with a high metric, in order for other routers to disregard it.

- *Do not Advertise Direct Connected Routes*: the Router will not advertise the route information to the same subnet device from which it was obtained.

Internet Group Management Protocol (IGMP): the Router provides support for IGMP multicasting, which allows hosts connected to a network to be updated whenever an important change occurs in the network. A multicast is simply a message that is sent simultaneously to a pre-defined group of recipients. When you join a multicast group you will receive all messages addressed to the group, much like what happens when an e-mail message is sent to a mailing list. IGMP multicasting may be useful when connected to the Internet through a router. When an application running on a LAN computer sends out a request to join a multicast group, the Router will listen and intercept this group's messages, sending them to the subscribed application.

Domain Routing: When Router's DNS server receives a reply from an external DNS server, it will add a routing entry for the IP address of the reply through the device from which it arrived. This means that future packets from this IP address will be routed through the device from which the reply arrived.

FIGURE 30. Routing Panel



Routing

Routing Table

Name	Destination	Gateway	Netmask	Metric	Status	Action
Video&Voice ETHoA	213.33.34.0	0.0.0.0	255.255.255.0	1	Not Applicable	✎ ✖
Video&Voice ETHoA	213.33.35.0	0.0.0.0	255.255.255.0	1	Not Applicable	✎ ✖
LAN Bridge	10.0.0.0	0.0.0.0	255.255.255.0	4	Applied	
New Route						✚

Routing Information Protocol (RIP) □ Enabled

□ Poison Reverse

□ Do not Advertise Direct Connected Routes

Internet Group Management Protocol (IGMP) ☑ Enabled

☑ IGMP Fast Leave

□ IGMP Multicast to Unicast

Domain Routing □ Enabled

Packet Streaming Engine

Software Acceleration: None

SSH

Secure Shell (SSH) is a protocol that provides encrypted connections to remote hosts or servers. PRG AV4202N supports SSH connection requests from LAN clients with administrative permissions. When connected, a secured command-line session will grant a user access to all system settings and parameters. This service can also be opened to WAN clients.

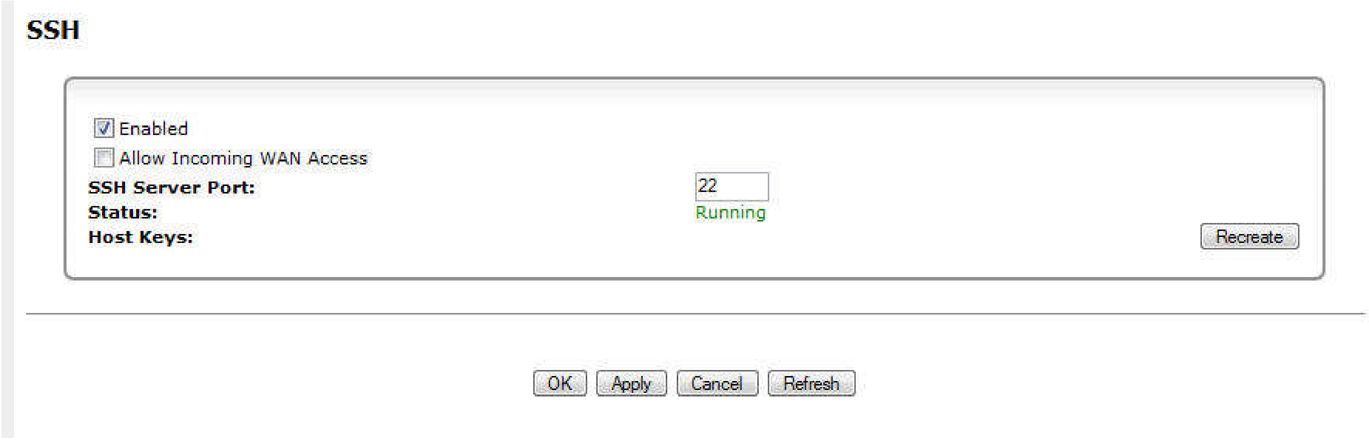
Click the 'SSH' icon in the 'Advanced' screen of the Web-based management. The 'SSH' screen will appear.

Enabled. Check or un-check this box to enable or disable this feature.

Status. This feature is enabled by default, and its status appears as “Running”. This status will change reflecting actions performed.

Host Keys. Host keys are used to identify the Router to incoming SSH connection requests. You may wish to use new keys instead of the old ones. To do so, press the 'Recreate' button. The status will change to “Generating Host Keys” until the keys are created and saved in the Router's configuration file.

FIGURE 31. **SSH Panel**



SSH

☑ Enabled

□ Allow Incoming WAN Access

SSH Server Port: 22

Status: Running

Host Keys: Recreate

SSL VPN

Secure Socket Layer Virtual Private Network (SSL VPN) provides simple and secure remote access to home and office network resources. It provides the security level of IPSec, but with the simplicity of using a standard Web browser. The unparalleled advantage of SSL VPN is its zero-configuration on the client's end. Remote users can simply browse to Discus from any computer in the world and run applications on its LAN computers. However, since SSL VPN is not a tunnel such as PPTP or IPSec, only pre-defined applications may be used. When using this feature, non-administrator remote users browsing to Discus will be routed to the "SSL VPN Portal". This portal will present them each with their list of applications.

Setting up a Remote Desktop (RDP) application over SSL VPN in order to remotely connect and control a computer inside Discus LAN consists of two stages—creating a remote desktop global shortcut, and launching the application from a remote computer via the SSL VPN portal.

To create an RDP shortcut, perform the following:

1. Access the Secure Socket Layer VPN (SSL VPN) settings either from its link under the 'VPN' menu item of the 'Services' screen, or by clicking the 'SSL VPN' icon in the 'Advanced' screen.

2. To enable SSL VPN, select the 'Enabled' check box, and click 'Apply'. The screen refreshes, adding a link to the SSL VPN Portal.

3. Click the 'Click Here to Allow Incoming HTTPS Access' link. The 'Remote Administration' screen appears. In the 'Allow Incoming WAN Access to Web-Management' section, select both HTTPS port 443 and 8443, and click 'OK'.

4. Back in the 'SSL VPN' screen, click the 'Click Here to Create SSL-VPN Users' link. The 'Users' screen appears, where you can define a user with the 'Remote Access by SSL VPN' option enabled.

5. In the 'SSL VPN' screen, click the 'New Shortcut' link. The 'Shortcut Wizard' screen appears.

6. Choose whether to select a host from a given list, comprised of DHCP leases that are known to Discus, or to manually enter the host's IP address, and click 'Next'. If you choose 'From a List', the following screen appears. Select the host to which you would like to add a shortcut, and click 'Next'. The next wizard screen appears, either with the IP address of a selected host, or without an IP address for manual selection.

7. In the 'Application' drop-down menu, select 'Remote Desktop (RDP)'. The screen refreshes, displaying the RDP parameters.

8. In this screen, perform the following:

   - Enter a name for the shortcut.

   - Enter the IP address of the LAN computer on which the RDP will be performed.

   - Select the 'Override Default Port' option if the LAN computer uses a port other than the application's "well known" default port. An additional field appears, in which you must enter the alternative port.

   - If you choose the default setting of requiring the user to specify login information when connecting with RDP, provide the username and password that are used to login to the LAN computer.

   - Select the size of the screen in which the remote desktop application will be displayed.

9. Select the 'Edit the Newly Created Shortcut' check box in order to associate a user or a group with this shortcut, and click 'Finish'. The 'Edit Shortcut' screen appears.

10. Click the 'New User' link (or 'New Group' according to your preference), and select a user with remote SSL VPN access permission from the drop-down menu.

11. Click 'OK'. The new user is added to the 'Users' section in the 'Edit Shortcut' screen. Click 'OK' to save the settings. The new shortcut is added to the

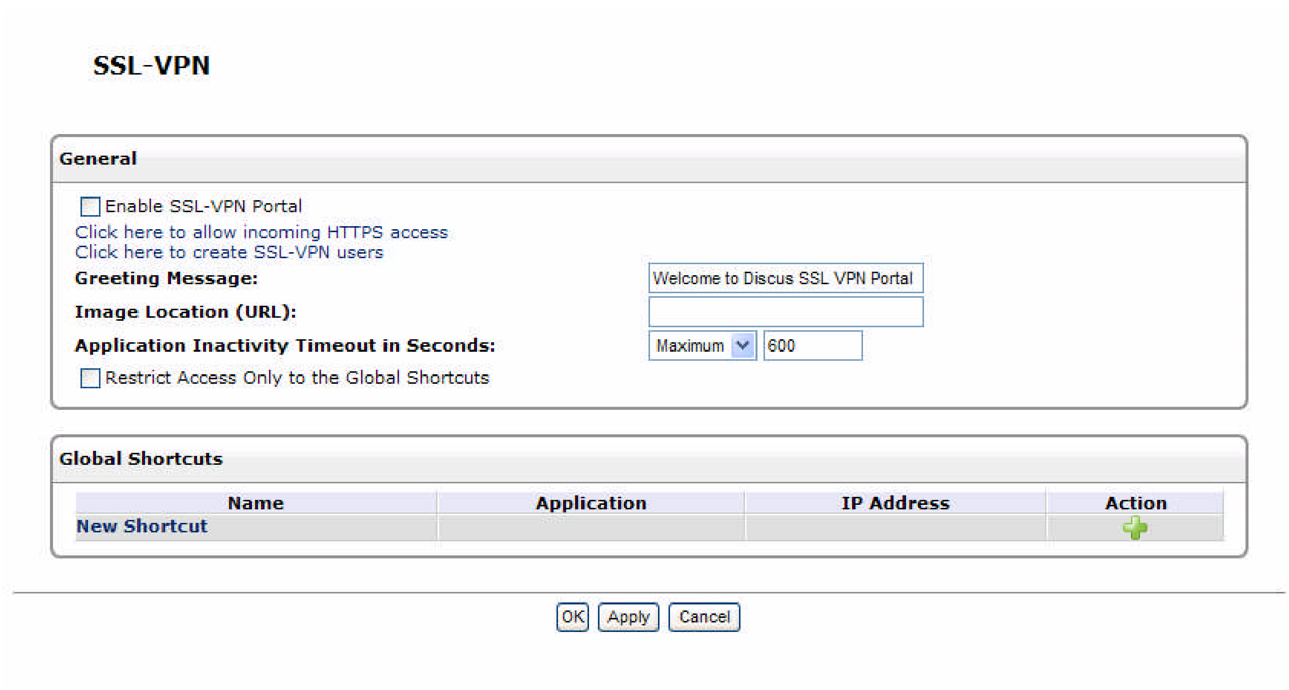
'Shortcuts' screen, and will be available for this user when connecting to the SSL VPN portal.

To launch the remote desktop application from a remote computer, perform the following:

1. Browse to Discus from a remote computer by typing https://<Discus Internet address> (Discus Internet address can be found under the 'Internet Connection' tab). For example, **https://10.71.86.21**.

2. Log in with the newly added user. The portal screen appears. Click the name of the RDP shortcut. A Remote Desktop session screen opens, prompting you for login details. Enter the computer's login username and password to gain RDP control. If an RDP screen fails to load, check that JRE is properly installed on the client computer

FIGURE 32. **SSL VPN Panel**



SSL-VPN

General

☐ Enable SSL-VPN Portal

Click here to allow incoming HTTPS access

Click here to create SSL-VPN users

Greeting Message:	Welcome to Discus SSL VPN Portal
Image Location (URL):	
Application Inactivity Timeout in Seconds:	Maximum 600

☐ Restrict Access Only to the Global Shortcuts

Global Shortcuts

Name	Application	IP Address	Action
New Shortcut			✚

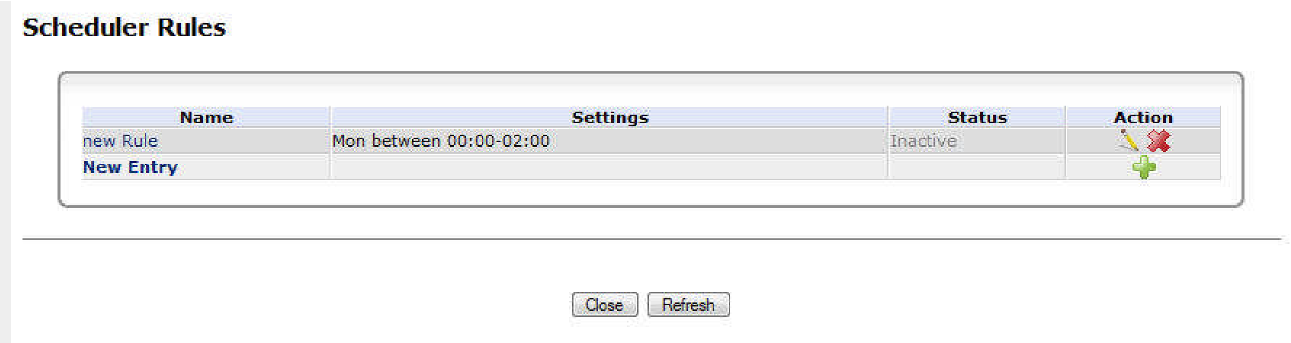
SCHEDULER RULES

Scheduler rules are used for limiting the activation of Firewall rules to specific time periods, specified in days of the week, and hours.

To define a Rule:

1. Click the 'Scheduler Rules' icon in the 'Advanced' screen of the Web-base Management. The 'Scheduler Rules' screen will appear.
2. Click the 'New Scheduler Entry' link. The 'Scheduler Rule Edit' screen will appear
3. Specify a name for the rule in the 'Name' field.
4. Specify if the rule will be active/inactive during the designated time period, by selecting the appropriate 'Rule Activity Settings' check-box.
5. Click the 'New Time Segment Entry' link to define the time segment to which the rule will apply. The 'Time Segment Edit' screen will appear.
   (a) Select active/inactive days of the week.
   (b) Click the 'New Time Segment Entry' to define an active/inactive hourly range.
6. Click 'OK' to save the settings.

FIGURE 33. Scheduler Rules Panel



Scheduler Rules

Name	Settings	Status	Action
new Rule	Mon between 00:00-02:00	Inactive	✎ ✖
New Entry			✚

SIMPLE NETWORK MANAGEMENT PROTOCOL

Simple Network Management Protocol (SNMP) enables network management systems to remotely configure and monitor Discus. Your Internet Service Provider (ISP) may use SNMP in order to identify and resolve technical problems. Technical information regarding the properties of Discus SNMP agent should be provided by your ISP. To configure Discus SNMP agent, perform the following:

1. Access this feature either from the 'Management' menu item under the 'System' tab, or by clicking its icon in the 'Advanced' screen.

2. Specify the SNMP parameters, as provided by your Internet service provider:

   Allow Incoming WAN Access to SNMP Select this check box to allow access to Discus SNMP over the Internet.

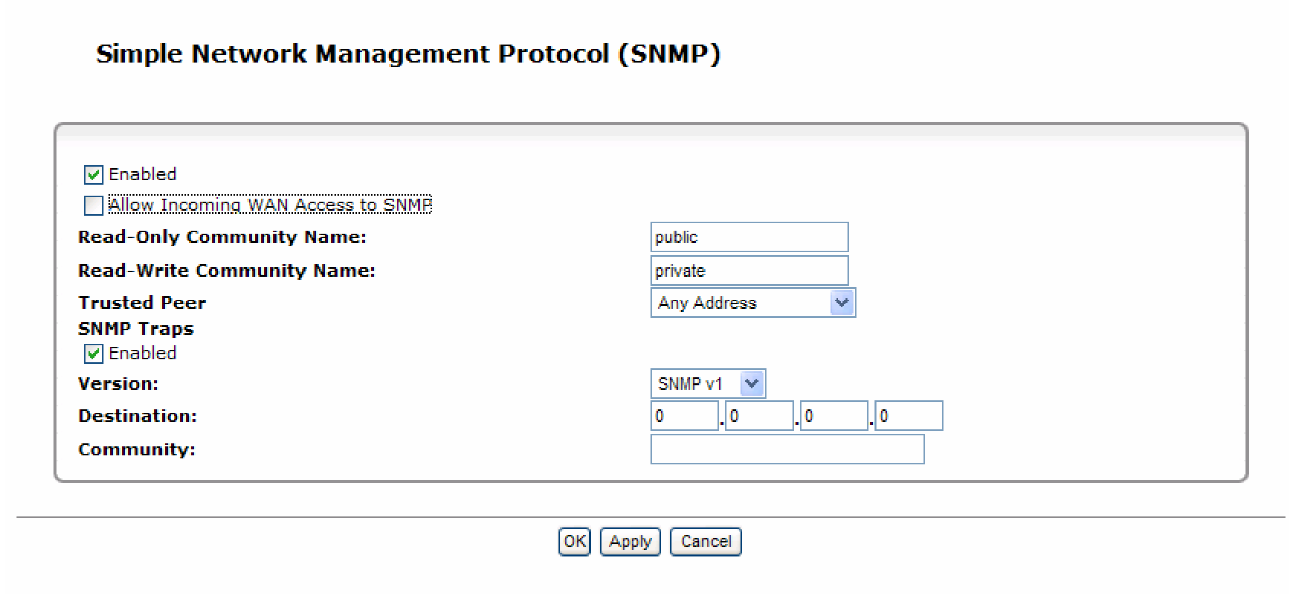
   Read-only/Write Community Names SNMP community strings are passwords used in SNMP messages between the management system and Discus. A read-only community allows the manager to monitor Discus. A read-write community allows the manager to both monitor and configure Discus.

Trusted Peer The IP address, or subnet of addresses, that identify which remote management stations are allowed to perform SNMP operations on Discus.

SNMP Traps Messages sent by OpenRG to a remote management station, in order to notify the manager about the occurrence of important events or serious conditions. Discus supports both SNMP version 1 and SNMP version 2c traps. Check the Enabled check box to enable this feature. The screen refreshes, displaying the following fields.

- **Version** Select between version SNMP v1 and SNMP v2c.
- **Destination** The remote management station's IP address.
- **Community** Enter the community name that will be associated with the trap messages.

FIGURE 34. **Simple Network Management Protocol Panel**



Simple Network Management Protocol (SNMP)

☑ Enabled

□ Allow Incoming WAN Access to SNMP

Read-Only Community Name:	public
Read-Write Community Name:	private
Trusted Peer	Any Address
SNMP Traps	
☑ Enabled	
Version:	SNMP v1
Destination:	0 . 0 . 0 . 0
Community:	

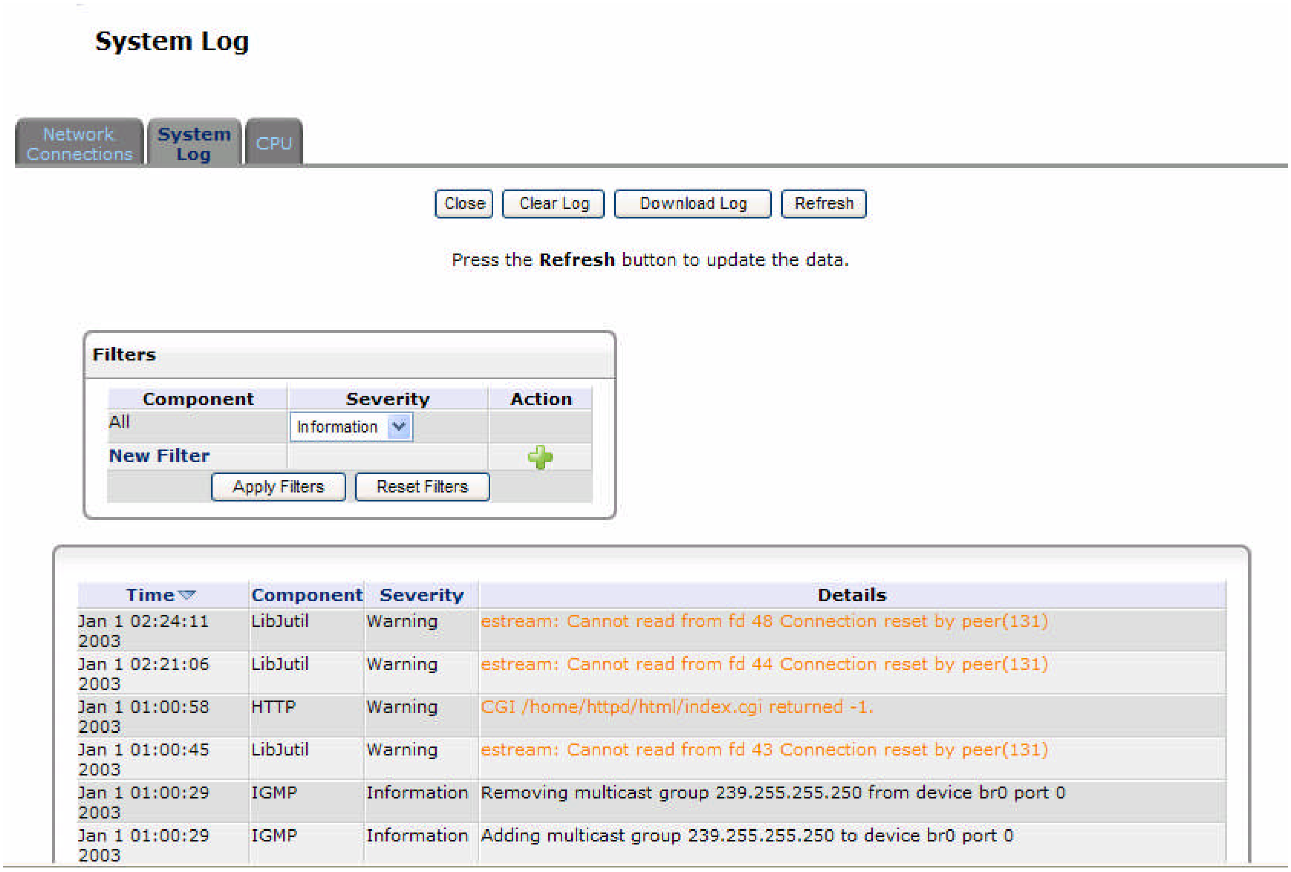
SYSTEM LOG

The 'System Log' screen displays a list of recent activities that has taken place on Discus.

By default, all log messages are displayed one after another, sorted by their order of posting by the system (newest on top). You can sort the messages according to the column titles---Time, Component, or Severity. This screen also enables you to filter the log messages by the component that generated them, or by their severity, providing a more refined list. This ability is useful mainly for software developers debugging Discus. By default, the screen displays log messages with 'debug' severity level and higher, for all components. You may change the severity level for this filter. To add a new filter, click the 'New Filter' link or its corresponding icon . The screen refreshes.

Using the drop-down lists, select the component and severity level by which to sort the log messages. Click 'Apply Filters' to display the messages in your specified criteria. You can add more filters in the same way, or delete filters using their respective action icons. Defined filters override the default filter that displays all messages.

FIGURE 35. **System Log Panel**



Press the **Refresh** button to update the data.

Filters

Component	Severity	Action
All	Information	
New Filter		✚

Time	Component	Severity	Details
Jan 1 02:24:11 2003	LibJutil	Warning	estream: Cannot read from fd 48 Connection reset by peer(131)
Jan 1 02:21:06 2003	LibJutil	Warning	estream: Cannot read from fd 44 Connection reset by peer(131)
Jan 1 01:00:58 2003	HTTP	Warning	CGI /home/httpd/html/index.cgi returned -1.
Jan 1 01:00:45 2003	LibJutil	Warning	estream: Cannot read from fd 43 Connection reset by peer(131)
Jan 1 01:00:29 2003	IGMP	Information	Removing multicast group 239.255.255.250 from device br0 port 0
Jan 1 01:00:29 2003	IGMP	Information	Adding multicast group 239.255.255.250 to device br0 port 0

SYSTEM SETTINGS

The System Settings screen allows you to configure various system and management parameters.

System. Configures general system parameters.

- Discus's Hostname Specify the gateway's host name. The host name is the gateway's URL address.
- Local Domain Specify your network's local domain.

Discus Management Console. Configure Web-based management settings.

- Automatic Refresh of System Monitoring Web Pages. Select this check-box to enable the automatic refresh of system monitoring web pages.
- Warn User Before Network Configuration. Changes Select this check-box to activate user warnings before network configuration changes take effect.

- Session Lifetime. The duration of idle time (in seconds) in which the WBM session will remain active. When this duration times out, the user will have to re-login.
- Language. Select a different language for the WBM interface.

Management Application Ports. Configure the following management application ports:

1. Primary/secondary HTTP ports
2. Primary/secondary HTTPS ports
3. Primary/secondary Telnet ports
4. Secure Telnet over SSL ports

Management Application SSL Authentication Options. It allows to define the Client Authentication options.

System Logging. Configure system logging parameters.

- System Log Buffer Size. Set the size of the system log buffer in Kilobytes.
- Remote System Notify Level The remote system notification level can be one of the following: None, Error, Warning and Information.

Security Logging. Configure security logging parameters.

- Security Log Buffer Size Set the size of the security log buffer in Kilobytes.
- Remote Security Notify Level The remote security notification level can be one of the following: None, Error, Warning and Information.

Outgoing Mail Server. Configure outgoing mail server parameters.

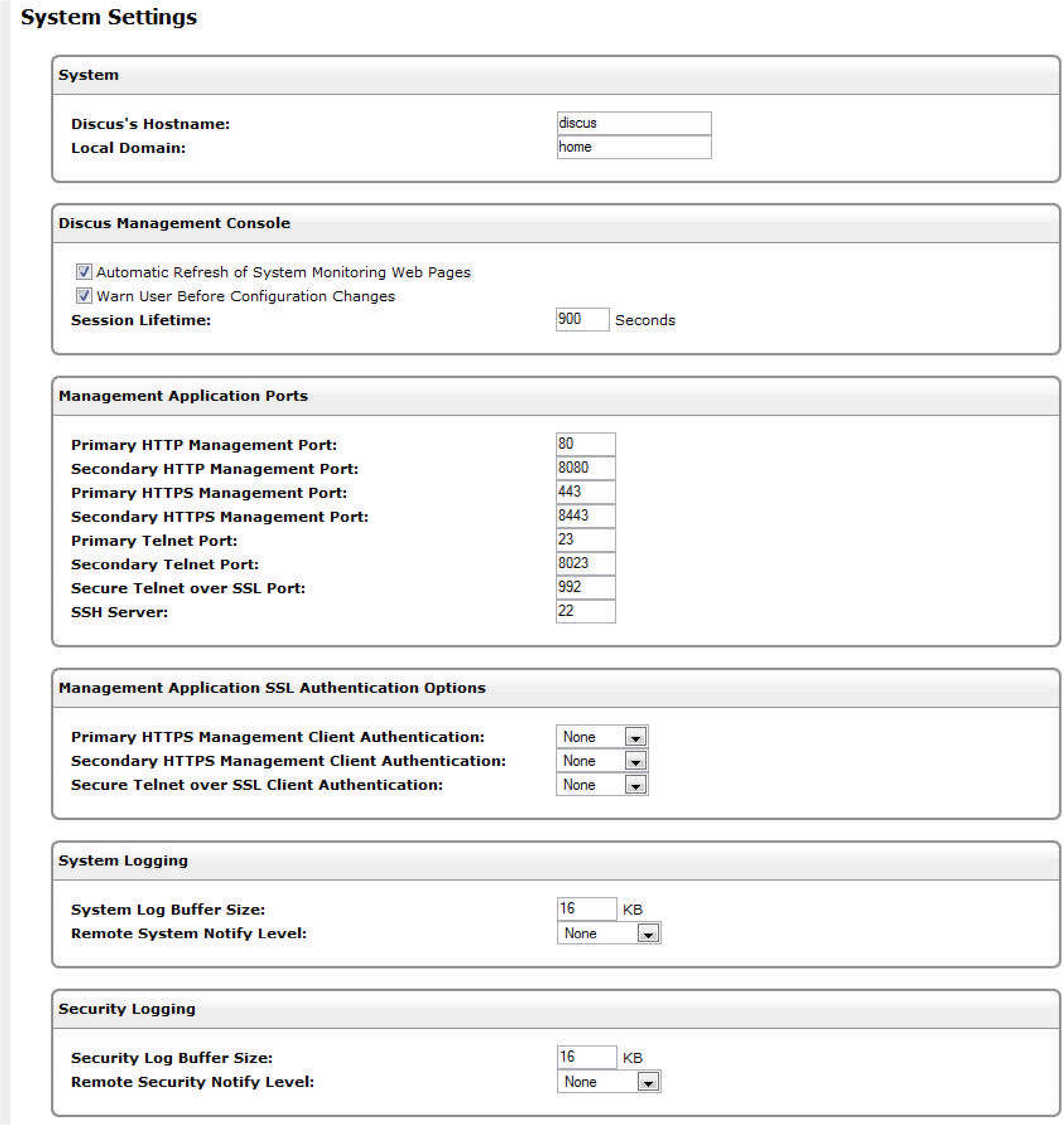
- Server Enter the hostname of your outgoing (SMTP) server in the 'Server' field.
- From Email Address Each email requires a 'from' address and some outgoing servers refuse to forward mail without a valid 'from' address for anti-spam considerations. Enter a 'from' email address in the 'From Email Address' field.
- Port Enter the port that is used by your outgoing mail server.
- Server Requires Authentication If your outgoing mail server requires authentication check the 'Server Requires Authentication' check-box and enter your user name and password in the 'User Name' and 'Password' fields respectively.

SWAP. If enabled, it allows to define the swap size (MB).

HTTP Interception. When no Internet connection is available, the Router will display an attention screen explaining the connection's status instead of the standard “The page cannot be displayed” window.

Host Information. It allows to enable/disable the host services auto-detection feature.

FIGURE 36. System Settings Panel



System Settings

System

Discus's Hostname: discus
Local Domain: home

Discus Management Console

☑ Automatic Refresh of System Monitoring Web Pages
☑ Warn User Before Configuration Changes
Session Lifetime: 900 Seconds

Management Application Ports

Primary HTTP Management Port:	80
Secondary HTTP Management Port:	8080
Primary HTTPS Management Port:	443
Secondary HTTPS Management Port:	8443
Primary Telnet Port:	23
Secondary Telnet Port:	8023
Secure Telnet over SSL Port:	992
SSH Server:	22

Management Application SSL Authentication Options

Primary HTTPS Management Client Authentication:	None
Secondary HTTPS Management Client Authentication:	None
Secure Telnet over SSL Client Authentication:	None

System Logging

System Log Buffer Size: 16 KB
Remote System Notify Level: None

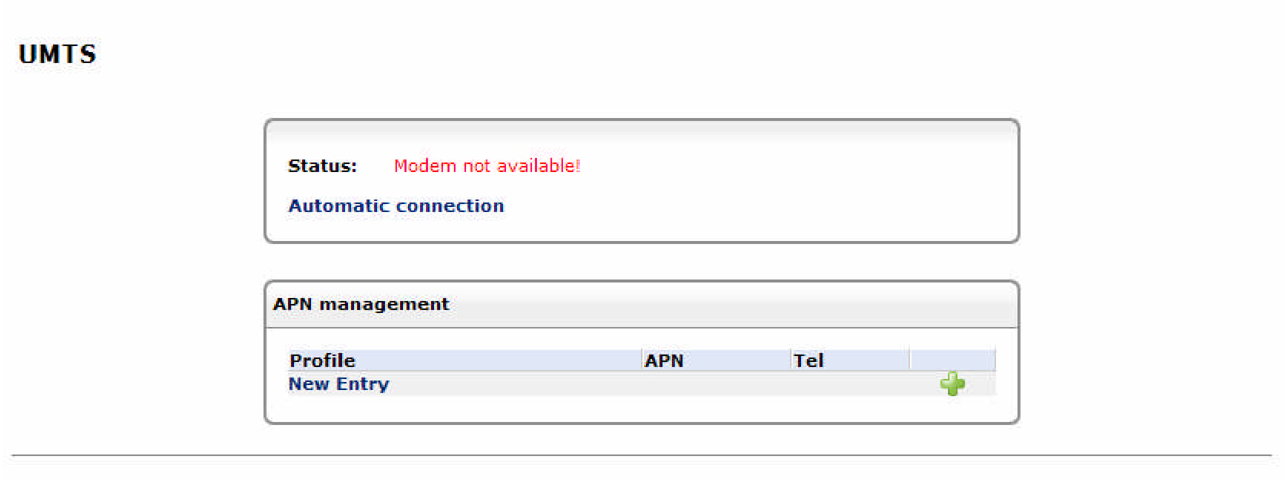
Security Logging

Security Log Buffer Size: 16 KB
Remote Security Notify Level: None

UMTS

PRG AV4202N allows you to navigate using a 3G sim card, you can create a new APN profile where you should fill in the information provided by your service provider (APN, Tel, User Name, Password and Protocol). You can also enable an automatic connection to be able to automatically connect with your UMTS according to pre-defined rules.

FIGURE 37. UMTS Panel



UMTS

Status: Modem not available!

APN management

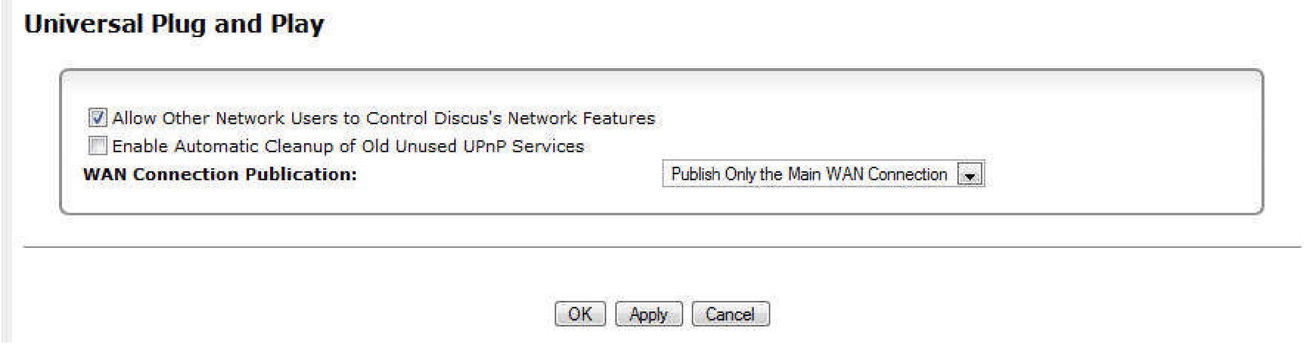
Profile	APN	Tel	
New Entry			✚

UNIVERSAL PLUG AND PLAY

Universal Plug-and-Play is a networking architecture that provides compatibility among networking equipment, software and peripherals. UPnP-enabled products can seamlessly connect and communicate with other Universal Plug-and-Play enabled devices, without the need for user configuration, centralized servers, or product-specific device drivers.

If your computer is running an operating system that supports UPnP, such as Windows XP, you can add the computer to your home network and access the Web-based Management directly from within Windows.

FIGURE 38. **Universal Plug and Play Panel**



Universal Plug and Play

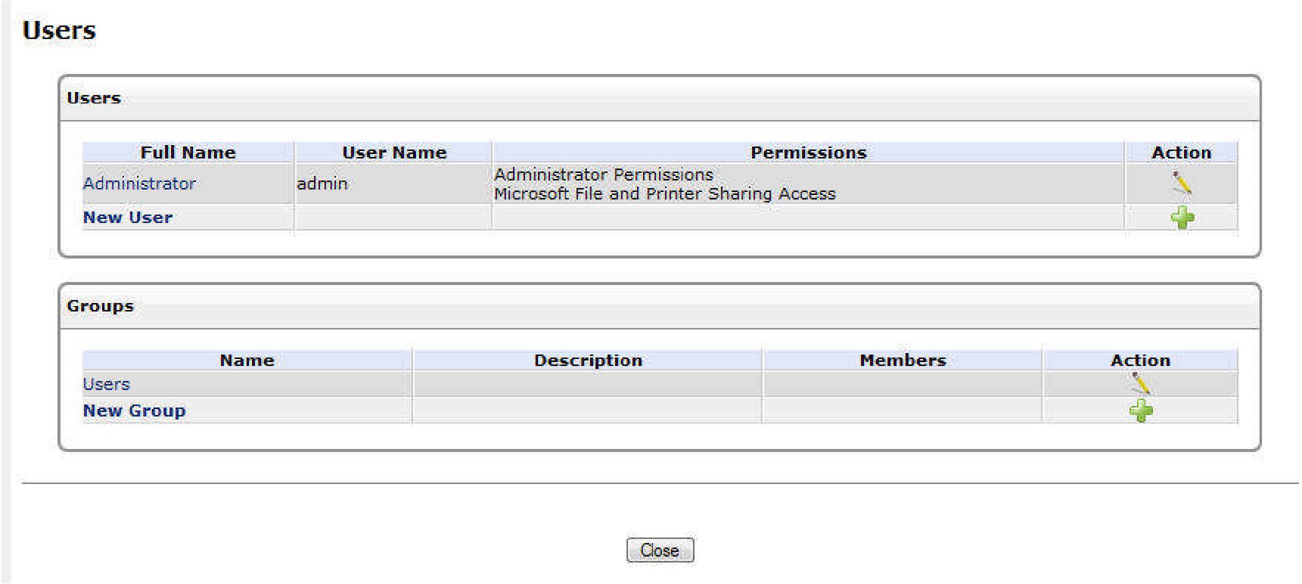
☑ Allow Other Network Users to Control Discus's Network Features
□ Enable Automatic Cleanup of Old Unused UPnP Services
WAN Connection Publication: Publish Only the Main WAN Connection

USERS

You can add, edit and delete users. You may also group users according to your preferences. To access the user settings, click the 'Users' icon in the 'Advanced' screen.

The 'Users' screen will appear. This screen lists the users and groups defined in the Router. The “Administrator” is a default user provided by the system.

FIGURE 39. **Users Panel**



Users

Users

Full Name	User Name	Permissions	Action
Administrator	admin	Administrator Permissions Microsoft File and Printer Sharing Access	✎
New User			+

Groups

Name	Description	Members	Action
Users			✎
New Group			+

To add a new user, click the 'New User' link. The 'User Settings' screen will appear

- Full Name: The remote user's full name.
- User Name: The name that a user will use to access your network.

- New Password: The user's password.
- Retype New Password: If a new password is assigned, type it again to verify its correctness.
- Primary Group: This check-box will only appear after a user is defined, enabling you to select the primary group to which this user will belong.
- Permissions: Select the user's privileges on your home network.
- Administrator Permissions: Grants permissions to remotely modify system setting via Web-based management or Telnet.
- Remote Access by SSL-VPN: Grants remote access to the Router using the SSL-VPN protocol.
- Mail Server Access: Grants permission to use the Router's mail server. When selecting this option, you must also enable the user home directory and mailbox in the following sections.
- Microsoft File and Printer Sharing Access: Grants permission to use shared files and printers.
- FTP Server Access: Grants permission to use the Router's FTP server.
- Internet Printer Access: Grants permission to use an Internet Printing Protocol (IPP) printer.
- Remote Access by VPN: Grants remote access to the Router using the VPN protocol.

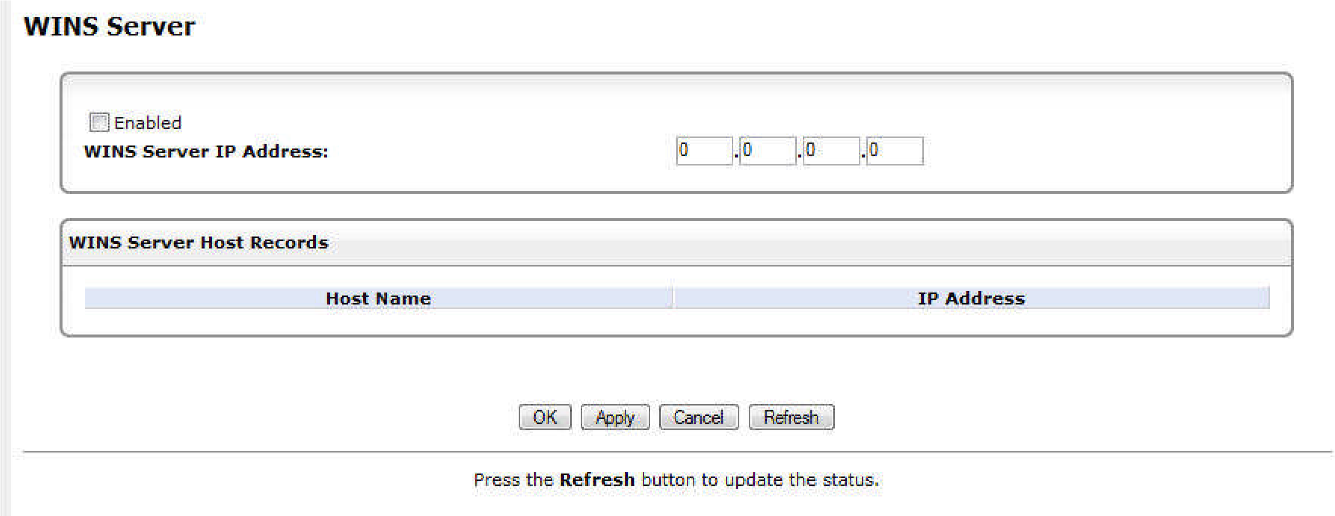
WINS SERVER

The Router can operate as a Windows Internet Naming Service (WINS) server, handling name registration requests from WINS clients and registering their names and IP addresses. WINS is a name resolution software from Microsoft that converts NetBIOS names to IP addresses. Windows machines that are named as PCs in a workgroup rather than in a domain use NetBIOS names, which must be converted to IP addresses if the underlying transport protocol is TCP/IP.

Windows machines identify themselves to the WINS server, so that other Windows machines can query the server to find the IP address. Since the WINS server itself is contacted by IP address, which can be routed across subnets, WINS allows Windows machines on one LAN segment to locate Windows machines on other LAN segments by name.

When a host connects to the LAN, it is assigned an IP address by router's DHCP. The WINS database is automatically updated with its NetBIOS name and the assigned IP address. Router's WINS server also responds to name queries from WINS clients by returning the IP address of the name being queried (assuming the name is registered with the WINS server). The “Internet” in the WINS name refers to the enterprise Internet (LAN), not the public Internet.

FIGURE 40. WINS Server Panel



WINS Server

□ Enabled

WINS Server IP Address: 0 . 0 . 0 . 0

WINS Server Host Records

Host Name	IP Address

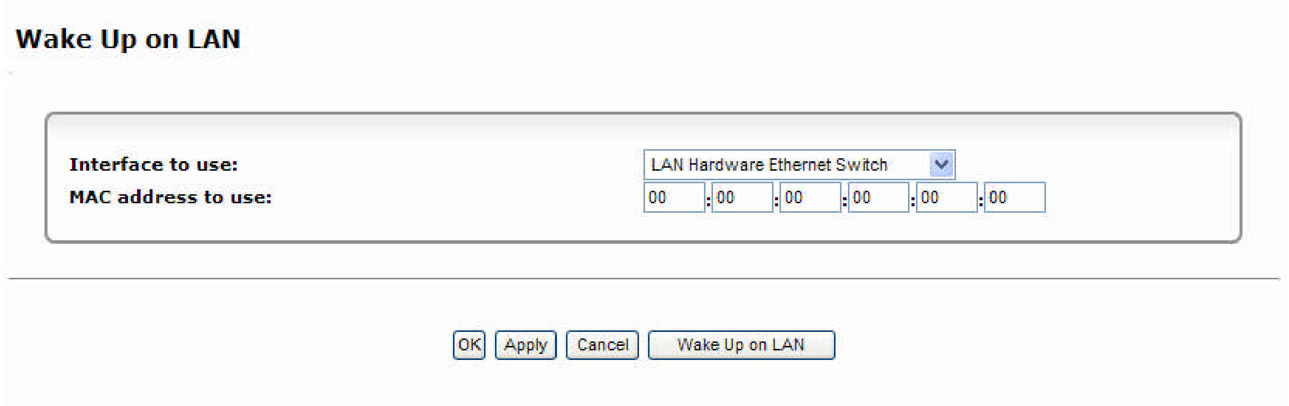
Press the **Refresh** button to update the status.

WAKE UP ON LAN

PRG AV4202N Allows you to wake up your PC remotely from a software shutdown state, Connecting to the Router's Homepage and accessing the Wake Up on LAN section. You should configure the Wake up on LAN option in windows in the network interface configuration window to enable this function.

On the Wake Up on LAN section of your PRG AV4202N have to select the Interface you want to use and the MAC address of the PC to Wake Up.

FIGURE 41. Wake Up on LAN Panel



Wake Up on LAN

Interface to use: LAN Hardware Ethernet Switch

MAC address to use: 00 : 00 : 00 : 00 : 00 : 00

WEB SERVER

PRG AV4202N can operate as a Web server, hosting one or more Web sites which are accessible from the LAN or the WAN. The advantages of this feature are:

- The Web site is hosted on PRG AV4202N , eliminating the need to assign a station on the LAN to act as a Web server, or to outsource expensive hosted services.
- LAN security: users from the Internet can access your Web site without entering your LAN.
- Simple and fast configuration.

To configure the Web Server, fill the following fields:

- **Enabled** Select or deselect this check box to enable or disable this feature.
- **WAN Access** Select this check box to allow access to your Web server over the Internet.

- **Log Requests** Select this check box to log connection requests sent to your Web server.
- **HTTP Port** The port your Web server uses for HTTP traffic.
- **HTTPS Port** The port your Web server uses for HTTPS traffic.
- **Data Allocation** Enter the file system path of the PRG AV4202N folder containing your Web site's content.

Each user on the LAN can configure a private Web page, which can be reached by browsing to http://openrg.home/~<username>. This path will be mapped to a sub directory of the users' home directory on PRG AV4202N.To set a private Web page:

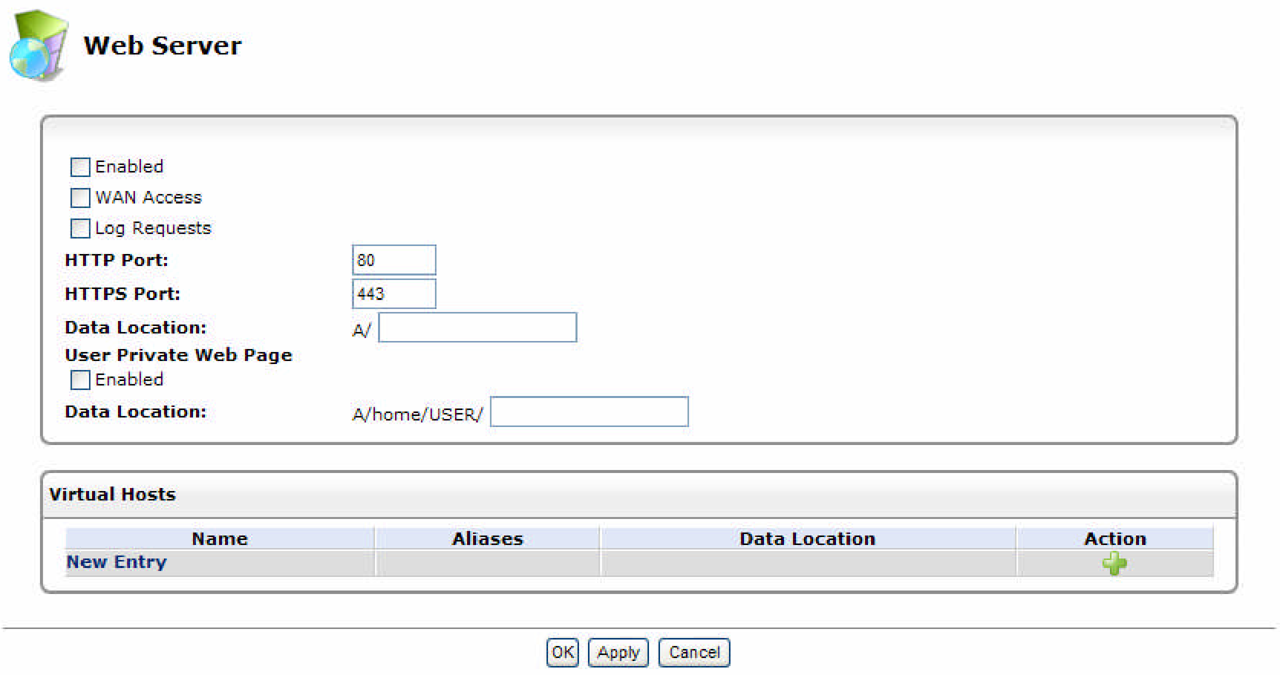
1. Verify that the 'User Home Directory' option is enabled in the user's account settings screen (for more information, refer to **Section 6.3.1**).
2. In the 'User Private Web Page' section of the 'Web Server' screen, select the 'Enabled' check box.
3. In the 'Data Location' field, enter the user's sub directory containing the Web site's content.
4. Click OK to save the settings

You can configure any number of additional Web sites on the PRG AV4202N Web server. Each of these sites will appear to the Internet user as if they are located on separate hosts. This method is referred to as *Virtual Hosts*. In addition, you can add any number of aliases to each virtual host. Browsers from within the LAN will reach your Web sites directly. However, to provide external access to your sites, you will have to register domain names. These domain names must be mapped to PRG AV4202N WAN IP address by the DNS. To configure additional Web sites:

1. In the 'Virtual Hosts' section of the 'Web server' screen, click the 'New Entry' link.
2. In the 'Server Name' field, type the Web site's domain name.
3. In the 'Data Location' field, type the file system path to the PRG AV4202N folder containing the Web site's content.
4. To add an alias to the virtual host, click the 'New Entry' link in the 'Aliases' section.
5. Type an alias URL in the 'Alias' field, and click 'OK'. The new alias appears under the 'Aliases' section

6. Click 'OK' to save the settings. Your site's URL and alias are added to the 'Virtual Hosts' section of the Web server

FIGURE 42. **Web Server Panel**



Web Server

□ Enabled
□ WAN Access
□ Log Requests

HTTP Port:	80
HTTPS Port:	443
Data Location:	A/

User Private Web Page

□ Enabled

Data Location: A/home/USER/

Virtual Hosts

Name	Aliases	Data Location	Action
New Entry			✚

System Monitoring Section

This chapter will describe the **System Monitoring Section** accessible from the *Home Page* of the PRG AV4202N upon user authentication to the Router.

⚠ *Be aware that any configuration changes could compromise your connectivity.*

NETWORK CONNECTIONS

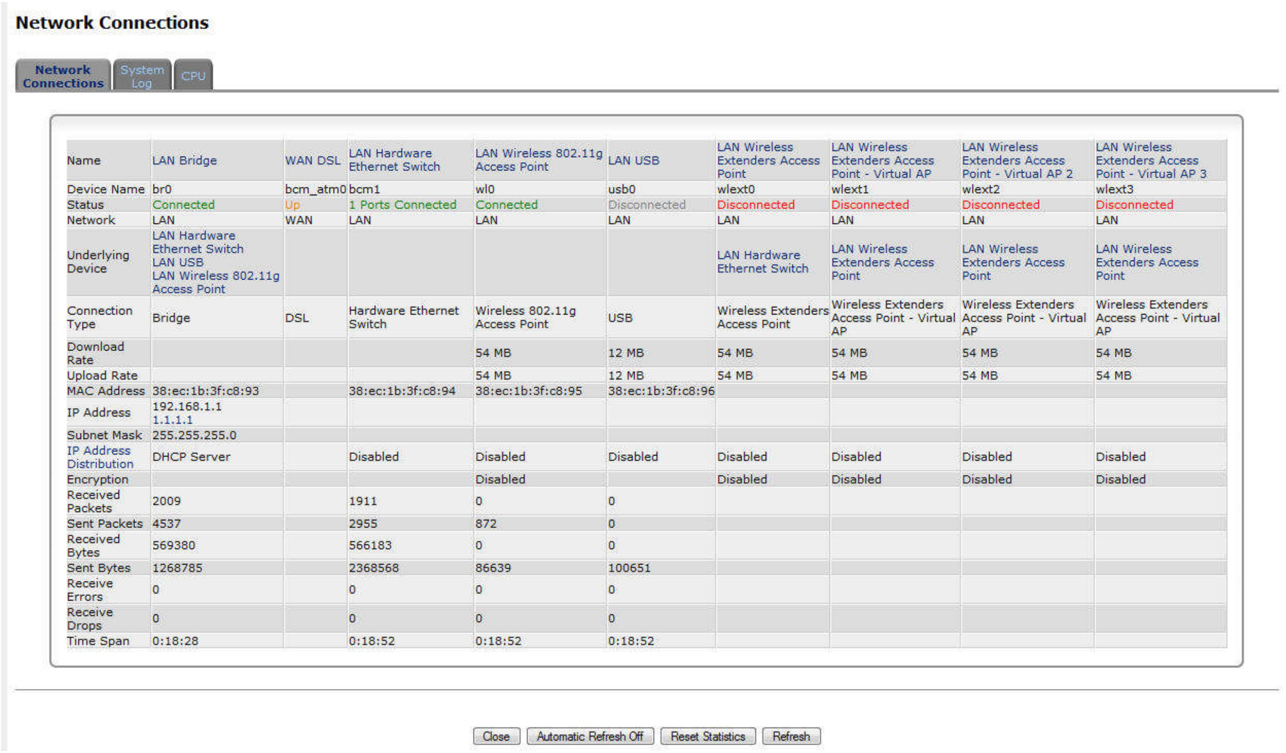
The Monitoring screen displays a table summarizing the monitored connection data.

PRG AV4202N constantly monitors traffic within the local network and between the local network and the Internet.

You can view statistical information about data received from and transmitted to the Internet (WAN) and to computers in the local network (LAN).

Click the 'Refresh' button to update the display, or press the 'Automatic Refresh On' button to constantly update the displayed parameters.

FIGURE 1. Network Connections Panel



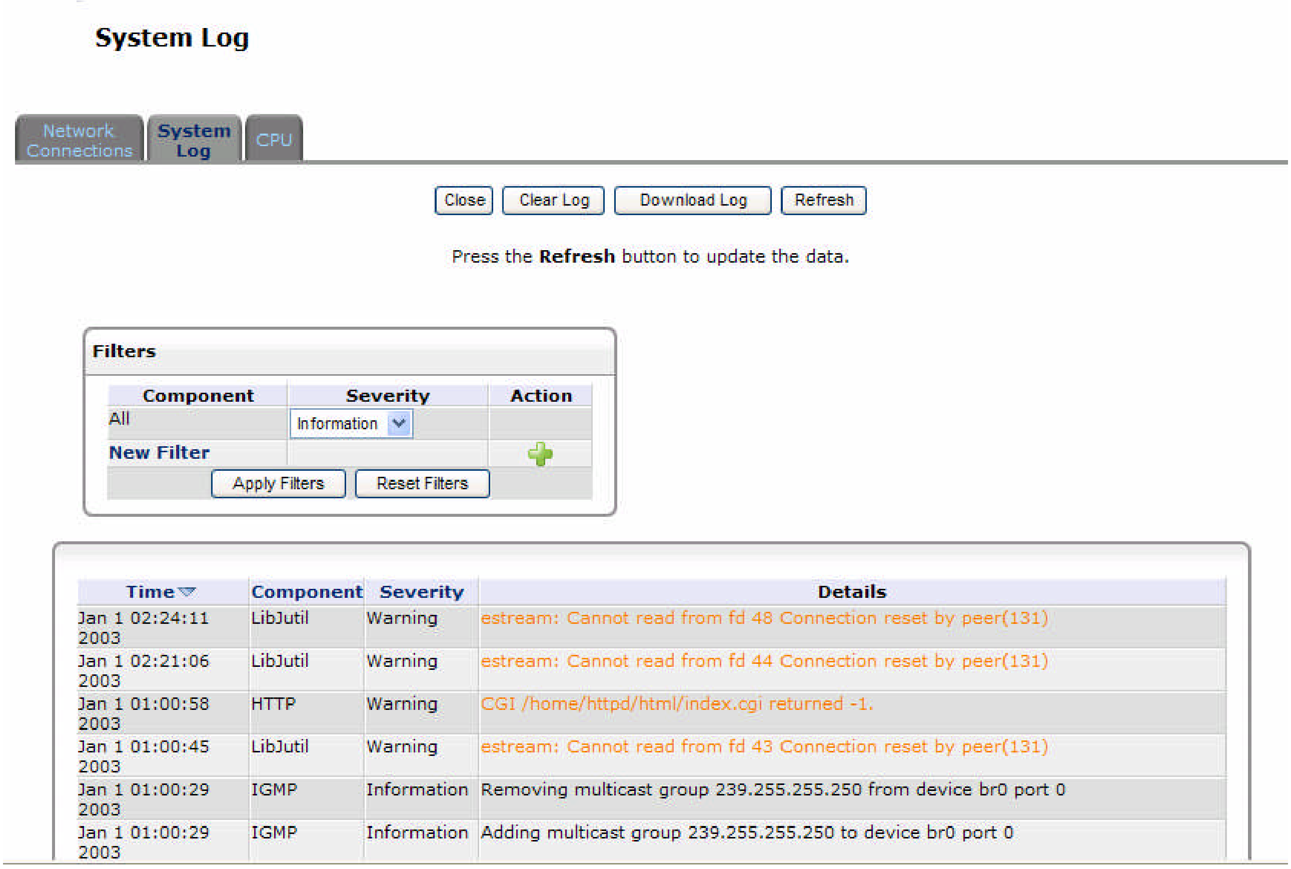
Network Connections

Name	LAN Bridge	WAN DSL	LAN Hardware Ethernet Switch	LAN Wireless 802.11g Access Point	LAN USB	LAN Wireless Extenders Access Point	LAN Wireless Extenders Access Point - Virtual AP	LAN Wireless Extenders Access Point - Virtual AP 2	LAN Wireless Extenders Access Point - Virtual AP 3
Device Name	br0	bcm_atm0	bcm1	wl0	usb0	wlext0	wlext1	wlext2	wlext3
Status	Connected	Up	1 Ports Connected	Connected	Disconnected	Disconnected	Disconnected	Disconnected	Disconnected
Network	LAN	WAN	LAN	LAN	LAN	LAN	LAN	LAN	LAN
Underlying Device	LAN Hardware Ethernet Switch LAN USB LAN Wireless 802.11g Access Point					LAN Hardware Ethernet Switch	LAN Wireless Extenders Access Point	LAN Wireless Extenders Access Point	LAN Wireless Extenders Access Point
Connection Type	Bridge	DSL	Hardware Ethernet Switch	Wireless 802.11g Access Point	USB	Wireless Extenders Access Point	Wireless Extenders Access Point - Virtual AP	Wireless Extenders Access Point - Virtual AP	Wireless Extenders Access Point - Virtual AP
Download Rate				54 MB	12 MB	54 MB	54 MB	54 MB	54 MB
Upload Rate				54 MB	12 MB	54 MB	54 MB	54 MB	54 MB
MAC Address	38:ec:1b:3f:c8:93		38:ec:1b:3f:c8:94	38:ec:1b:3f:c8:95	38:ec:1b:3f:c8:96				
IP Address	192.168.1.1 1.1.1.1								
Subnet Mask	255.255.255.0								
IP Address Distribution	DHCP Server		Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
Encryption				Disabled		Disabled	Disabled	Disabled	Disabled
Received Packets	2009		1911	0	0				
Sent Packets	4537		2955	872	0				
Received Bytes	569380		566183	0	0				
Sent Bytes	1268785		2368568	86639	100651				
Receive Errors	0		0	0	0				
Receive Drops	0		0	0	0				
Time Span	0:18:28		0:18:52	0:18:52	0:18:52				

SYSTEM LOG

The Log screen displays a list of the most recent activity that has taken place on the Router.

FIGURE 2. System Log Panel



Press the **Refresh** button to update the data.

Filters

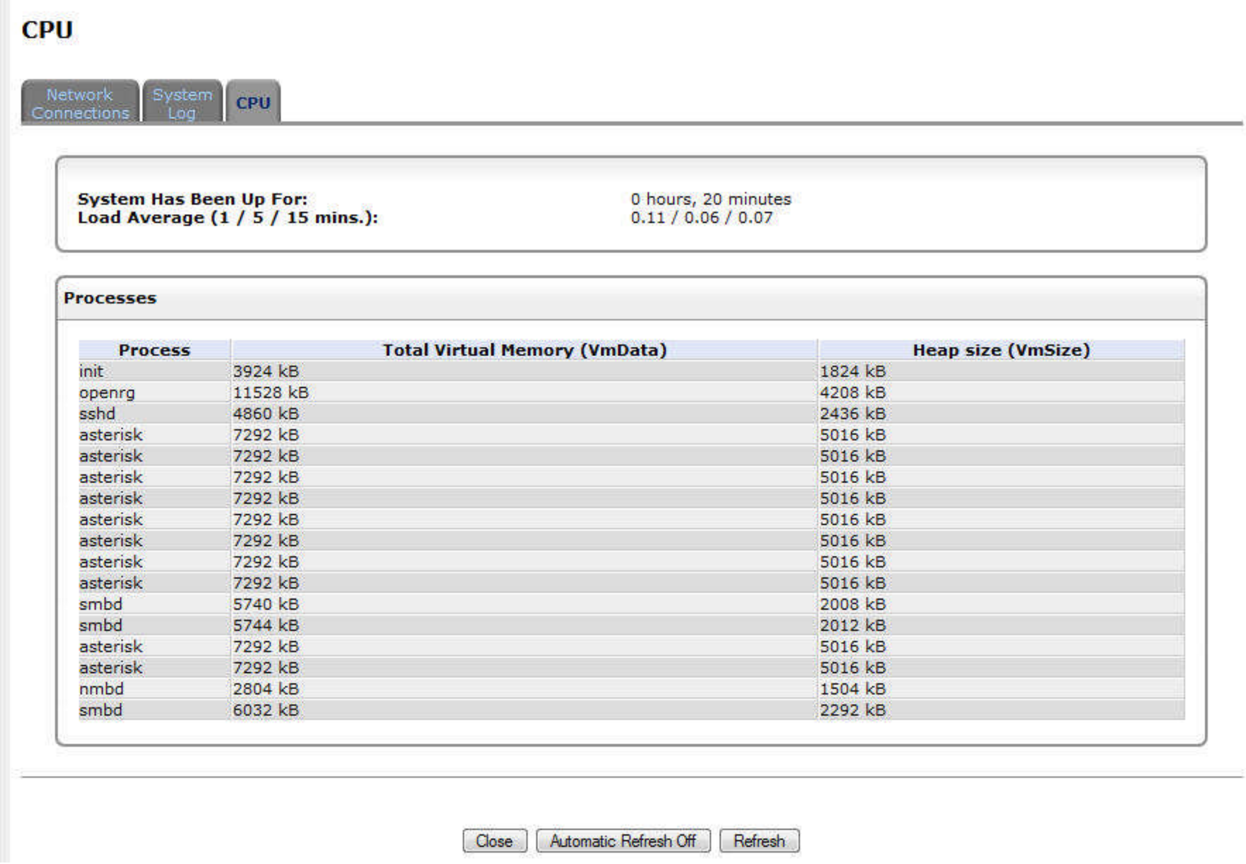
Component	Severity	Action
All	Information	
New Filter		✚

Time	Component	Severity	Details
Jan 1 02:24:11 2003	LibJutil	Warning	estream: Cannot read from fd 48 Connection reset by peer(131)
Jan 1 02:21:06 2003	LibJutil	Warning	estream: Cannot read from fd 44 Connection reset by peer(131)
Jan 1 01:00:58 2003	HTTP	Warning	CGI /home/httpd/html/index.cgi returned -1.
Jan 1 01:00:45 2003	LibJutil	Warning	estream: Cannot read from fd 43 Connection reset by peer(131)
Jan 1 01:00:29 2003	IGMP	Information	Removing multicast group 239.255.255.250 from device br0 port 0
Jan 1 01:00:29 2003	IGMP	Information	Adding multicast group 239.255.255.250 to device br0 port 0

CPU

The 'CPU' screen displays the amount of time that has passed since the system was last started, and the load average. In addition, the screen also displays a list of all the processes currently running on the Router and their virtual memory usage. The screen is automatically refreshed by default, though you may change this by clicking 'Automatic Refresh Off'.

FIGURE 3. **CPU Panel**



CPU

System Has Been Up For: 0 hours, 20 minutes
Load Average (1 / 5 / 15 mins.): 0.11 / 0.06 / 0.07

Processes

Process	Total Virtual Memory (VmData)	Heap size (VmSize)
init	3924 kB	1824 kB
openrg	11528 kB	4208 kB
sshd	4860 kB	2436 kB
asterisk	7292 kB	5016 kB
asterisk	7292 kB	5016 kB
asterisk	7292 kB	5016 kB
asterisk	7292 kB	5016 kB
asterisk	7292 kB	5016 kB
asterisk	7292 kB	5016 kB
asterisk	7292 kB	5016 kB
asterisk	7292 kB	5016 kB
smbd	5740 kB	2008 kB
smbd	5744 kB	2012 kB
asterisk	7292 kB	5016 kB
asterisk	7292 kB	5016 kB
nmbd	2804 kB	1504 kB
smbd	6032 kB	2292 kB

Troubleshooting

BASIC CONNECTION CHECKS

- Check that the Router is connected to your computers and to the telephone line, and that all the equipment is powered on. Check that the LAN or USB Status (according to your connection type) and DSL LEDs on the Router are illuminated, and that any corresponding LEDs on the NIC are also illuminated.
- Ensure that the computers have completed their start-up procedure and are ready for use. Some network interfaces may not be correctly initialized until the start-up procedure has completed.
- If the link status LED does not illuminate for a port that is connected, check that you do not have a faulty cable. Try a different cable.

BROWSING TO THE ROUTER CONFIGURATION SCREENS

If you have connected your Router and computers together but cannot browse to the Router configuration screens, check the following:

- Confirm that the physical connection between your computer and the Router is OK, and that the LAN Status LEDs on the Router and NIC are illuminated. Some NICs do not have status LEDs, in which case a diagnostic program may be available that can give you this information.
- Ensure that you have configured your computer as described in “Setting Up Your Computer” on page 19. Restart your computer while it is connected to the Router to ensure that your computer receives an IP address.
- When entering the address of the Router into your web browser, ensure that you use the full URL including the “*http://*” prefix (e.g. http://192.168.1.1).

- Ensure that you do not have a Web proxy enabled on your computer. Go to the Control Panel and click on Internet Options. Select the Connections tab and click on the LAN Settings button at the bottom. Make sure that the Proxy Server option is unchecked.
- If you cannot browse to the Router, use the *winipcfg* utility in Windows 98/ME to verify that your computer has received the correct address information from the Router. From the Start menu, choose Run and then enter *winipcfg*. Check that the computer has an IP address of the form 192.168.1.xxx (where xxx is in the range 2-254), the subnet mask is 255.255.255.0, and the default Router is 192.168.1.1 (the address of the Router). If these are not correct, use the Release and Renew functions to obtain a new IP address from the Router. Under Windows 2000 and Windows XP, use the *ipconfig* command-line utility to perform the same functions.

CONNECTING TO THE INTERNET

If you can browse to the Router configuration screens but cannot access sites on the Internet, check the following:

- Confirm that the physical connection between the Router and the telephone line is OK, and that the DSL LED on the Router is GREEN on.
- Ensure that you have entered the correct information into the Router configuration screens as required. Use the “Internet Settings” screen to verify this.
- Check that the user name and password are correct.
- Ensure that your computers are not configured to use a Web proxy. On Windows computers, this can be found under Control Panel >Internet Options > Connections.

FORGOTTEN PASSWORD AND RESET TO FACTORY DEFAULTS

If you can browse to the Router configuration screen but cannot log on because you do not know or have forgotten the password, follow the steps below to reset the Router to it’s factory default configuration.

All your configuration changes will be lost, and you will need to configure again your network before you can re-establish your Router connection to the Internet. Also, other computer users will lose their network connections whilst this process is taking place, so choose a time when this would be convenient.

1. Switch off the Router.
2. Disconnect all your computers and the telephone line from the Router.
3. Re-apply power to the Router, and wait for it to finish booting up.
4. Press the Reset button on the rear panel for a while.
5. The Router will restart, and when the start-up sequence has completed, browse to: http://192.168.1.1 and configure your network.
6. Reconnect your network as it was before.

WIRELESS NETWORKING

- Ensure that you have an 802.11b, 802.11g or 802.11n wireless adapter for each wireless computer, and that it is correctly installed and configured. Verify that each Wireless computer has either Windows 98SE or higher or MAC OS 10.x or higher.
- If you have a wired and a wireless NIC in the same computer, ensure that the wired NIC is disabled.
- Check the status of the Router Wireless LED.
- Ensure that the TCP/IP settings for all devices are correct.
- Ensure that the Wireless Clients are using the same SSID or Service Area Name as the Router. The SSID is case-sensitive.
- Ensure that the encryption method and level that you use on your clients are the same as those configured on the Router. The Router cannot simultaneously support WPA and WEP encryption.
- Ensure that you have the Wireless computer enabled in the list of allowed MAC addresses if you are using MAC Address Filtering on the Router.
- If you are having difficulty connecting or are operating at a low speed try changing the antenna positions on the rear of the Router. For more effective coverage you can try reorientating your antenna. Additionally consider moving the wireless computer closer to the Router to confirm that the building structure or fittings are not adversely affecting the connectivity. If this resolves the problem consider relocating the Wireless computer or the Router, or trying a different channel on the Router.
- Sources of interference: The 2.4GHz ISM band is used for 802.11b, 802.11g and 802.11n. This is generally a licence free band for low power applications, and you may have other devices at your location that operate in this frequency band. You should take care to ensure that there are no devices like microwave ovens for example close to the Router or wireless computers as this could affect receiver sensitivity and reduce the performance of your network. If you are unsure try relocating both the wireless computers and the Router to establish whether this problem exists.
- Most wireless computer Adapters will scan the channels for the wireless Router. If a wireless computer has not located the Router then try initiating a search manually if the client software supports this feature or manually set the channel on your wireless computer to correspond to the Router channel number. Please refer to your Wireless computer adapter documentation and vendor to do this.
- Speed of connection: The 802.11b/g and 802.11n standards will automatically choose the best speed depending on the quality of your connection. As the signal quality weakens then the speed falls back to a lower speed. The speeds supported by 802.11g are 54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, and 6 Mbps. The speeds supported by 802.11b are 11 Mbps, 5.5 Mbps, 2 Mbps and 1 Mbps. And the 802.11n supports until 100Mbps.In general the closer you are to the Router the better the speed. If you are not achieving the speed you had anticipated then try moving the antenna on the Router or moving the Wireless computer closer to the Router. In an ideal network the Router should be located in the centre of the network

with Wireless computers distributed around it. Applications are generally available with the computer wireless card to carry out a site survey. Use this application to find the optimal siting for your wireless computer. Consult your Computer Card documentation and vendor for more details.

FREQUENTLY ASKED QUESTIONS

How do I reset the Router to Factory Defaults? See How To "... change the administrator password".

How many computers on the LAN does the Router support? Up to a maximum of 256 computers on the LAN are supported.

⚠ *The Quality of Service (QoS) is related to the guaranteed level of throughput (the amount of data transferred from the Router to the clients). As many clients are connected as lower is the Quality as Service.*

How many wireless clients does the Router support? A maximum of 15 wireless clients are supported.

How are additional computers connected? You can expand the number of connections available on your LAN by using hubs, switches and wireless access points connected to the Router. Wireless access points and hubs and switches provide a simple, reliable means of expanding your network; contact your supplier for more information, or visit: http://www.pirelli.com/

A

Safety Information

Important Safety Information

This appendix contains directions that you must follow for your personal safety.

Follow all directions carefully. You must read the following safety information carefully before you install or remove the unit.

⚠

- Use only the power adapter that is supplied with the unit. The use of an alternative adapter can damage the Router and invalidate the warranty.

- Use an electrical outlet within easy distance and do not damage the power cable.

- To avoid electrical shock, do not open the Router.

- To prevent fire or shock hazard, do not expose your Router to rain or moisture, liquid and toxic substances.

- Particular care must be taken during installation and removal of cables and telephone line.

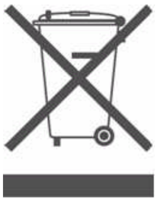
- Never touch uninsulated telephone wire or terminals unless the telephone line has been disconnected at the network interface.

- Ensure the correct ventilation to the Router. Do not obstruct the air conducts and do not lean anything over.

- Verify to place the Router out of direct sunlight and away from sources of heat.

- Avoid using your Router during an electrical storm.

- The Router generates and uses Radio Frequency (RF) energy. In some environments, the use of RF energy is not permitted. The user should seek local advice on whether or not RF energy is permitted within the area of intended use.



The crossed-out wheeled bin symbol on this electric or electronic equipment, or on its packaging, indicates that, at the end of its life, it must not be disposed of as unsorted household waste. Instead it must be separately collected.

As a consumer you must, therefore, use the specific collection schemes and, in particular, the municipal collection schemes provided for waste electrical and electronic equipment.

The separate collection and appropriate treatment of the equipment at the time of disposal helps to conserve natural resources and to ensure that it is recycled in a manner that protects human health and the environment from materials, components and substances that can be dangerous to the environment and harmful to human health.

Furthermore, the separate collection and appropriate treatment of the equipment, at the time of disposal, facilitates its possible reuse or possible materials recovery.

B

IP Addressing

The Internet Protocol Suite

The Internet protocol suite consists of a well-defined set of communications protocols and several standard application protocols. Transmission Control Protocol/Internet Protocol (TCP/IP) is probably the most widely known and is a combination of two of the protocols (IP and TCP) working together. TCP/IP is an internationally adopted and supported networking standard that provides connectivity between equipment from many vendors over a wide variety of networking technologies.

Managing the Router over the NetworK

To manage a device over the network, the Router must be correctly configured with the following IP information:

- An IP address
- A Subnet Mask

IP Addresses and Subnet Masks

Each device on your network must have a unique IP address to operate correctly. An IP address identifies the address of the device to which data is being sent and the address of the destination network. IP addresses have the format n.n.n.x where n is a decimal number between 0 and 255 and x is a number between 1 and 254 inclusive.

However, an IP Address alone is not enough to make your device operate. In addition to the IP address, you need to set a subnet mask. All networks are divided into smaller sub-networks and a subnet mask is a number that enables a device to identify the sub-network to which it is connected.

For your network to work correctly, all devices on the network must have:

- The same sub-network address.
- The same subnet mask.

The only value that will be different is the specific host device number. This value must always be unique.

An example IP address is ‘192.168.10.8’. However, the size of the network determines the structure of this IP Address. In using the Router, you will probably only encounter two types of IP Address and subnet mask structures.

Type One

In a small network, the IP address of ‘192.168.10.8’ is split into two parts:

- Part one (‘192.168.10’) identifies the network on which the device resides.
- Part two (‘.8’) identifies the device within the network.

This type of IP Address operates on a subnet mask of ‘255.255.255.0’.

Type Two

In larger networks, where there are more devices, the IP address of ‘192.168.10.8’ is, again, split into two parts but is structured differently:

- Part one (‘192.168’) identifies the network on which the device resides.
- Part two (‘.10.8’) identifies the device within the network.

This type of IP Address operates on a subnet mask of ‘255.255.0.0’.

How does a Device Obtain an IP Address and Subnet Mask?

There are three different ways to obtain an IP address and the subnet mask. These are:

- Dynamic Host Configuration Protocol (DHCP) Addressing
- Static Addressing
- Automatic Addressing (Auto-IP Addressing)

DHCP Addressing

The Router contains a DHCP server, which allows computers on your network to obtain an IP address and subnet mask automatically. DHCP assigns a temporary IP address and subnet mask which gets reallocated once you disconnect from the network.

DHCP will work on any client Operating System. Also, using DHCP means that the same IP address and subnet mask will never be duplicated for devices on the network. DHCP is particularly useful for networks with large numbers of users on them.

Static Addressing

You must enter an IP Address and the subnet mask manually on every device. Using a static IP and subnet mask means the address is permanently fixed.

Auto-IP Addressing

Network devices use automatic IP addressing if they are configured to acquire an address using DHCP but are unable to contact a DHCP server. Automatic IP addressing is a scheme where devices allocate themselves an IP address at random from the industry standard subnet of 169.254.x.x (with a subnet mask of 255.255.0.0). If two devices allocate themselves the same address, the conflict is detected and one of the devices allocates itself a new address. Automatic IP addressing support was introduced by Microsoft in the Windows 98 operating system and is also supported in Windows 2000 and Windows XP.

C Technical Specifications

This section lists the technical specifications for the **PRG AV4202N**.

Interfaces/Standard

WAN Interface

N°1 Line port (RJ-11plug, inner pair) supporting the following standards:

- VDSL (G.993.2, G.993.2 Amendment 1, 2 and 3)

- ADSL (G.992.1, G992.2, T1.413, G994.1, G.997.1)

- ADSL2 (G.992.3)

- ADSL2+ (G992.5)

Annex A/Annex B are available in different product version

LAN Interface

- N° 4 10/100BASE-T Ethernet ports (RJ-45 plug), compliant IEEE 802.3, with auto MDIX and auto-negotiation

- Ports can be configured in order to be dedicated to video traffic to/from a STB

- N° 2 USB Host v.2.0

Wireless LAN Interface

Wi-Fi access point solution is compliant with the following standards:

- IEEE 802.11b/g/n

- WPA/WPA2 (IEEE 802.11i)

- WMM (IEEE 802.11e)

- N°2 external antennas

Voice Interface

- N°2 FXS Phone port (RJ11 Plug)

DSL (ATM) Features

- AAL5 (ITU-T I.363.5)

- UBR, VBR-nrt, VBR-rt, CBR traffic classes

- Multiple VC/PPP connections

- Classic IP (CLIP) and ARP over ATM, RFCs 1577, 2225

- Multiple PPPoE connections on a single VC

- Multi-protocol encapsulation over AAL5 bridging and routing, RFCs 1483, 268

- PPP over AAL5 (PPPoATM), RFC 2364

- OAM (ITU-T I.610)

– F4, F5

– Loop-back

- Encapsulation modes in ATM stack: LLC and VC-Mux

Routing/Bridging

Routing:

- *Static routing*
- *RIPv1, RIPv2*
- *IP Multicasting – IGMP v2, v3*

Bridge:

- *WAN-LAN transparent bridging*
- *Transparent bridging between LAN devices*
- *Automatic discovery of MAC addresses*
- *Spanning tree protocol*

NAT

- *NAT-NAPT, RFCs 3022*
- *Static NAT*
- *Static NAPT*
- *Application Level Gateway (ALGs) modules*

QoS

- *ATM QoS: UBR, VBR-nrt, VBR-rt, CBR*
- *802.1P/Q prioritization*
- *Diffserv (RFC2474, RFC2475) marking and queuing according to connection type, network interface, MAC, IP, hostname, DSCP/ToS value, port number and application*
- *Port based QoS*

Voice Over IP

Codecs:

G.711 a-law/µ-law, G.729(*) , G.726(*), G.723 (*)

Codecs Control:

- *RTP/RTCP, RFC 1889*
- *SDP, RFC 2327*
- *RTP payload for DTMF digits RFC 2833*

Voip stacks supported:

- *SIP/SIPv2*
- *MGCP*
- *H323*

VoIP QoS:

- *Layer 3 QoS: control ToS and DSCP for VoIP RTP*
- *Prioritization of voice over data at the network stack*

(*) optional to be quoted a part

Remote Management	*DSL Forum TR-069 CPE Management Protocol:* *- Auto- configuration and dynamic service provisioning* *- Software/firmware image management* *- Status and performance monitoring* *- WEB GUI (HTTP-S web server* *- TFTP, RFC 1350* *- Telnet server*
Security	*- Stateful Packet Inspection (SPI) Firewall* *- IP protocol filtering* *- Access Control* *- Parental control*
Environmental Specifications	*Temperature:* *- Operating: +0° to 40° C* *- Non Operating: -20° to 65°C* *Relative Humidity:* *- Operating: 10% to 85% non condensing* *- Non Operating:5% to 95% non condensing*
Power Adapter	*- European Plug* *- Primary: nominal voltage 220V-230V, 50 Hz;* *- Secondary: 15V 1.2A.*

Declaration of Conformity

We, Pirelli BroadBand Solutions SpA, Viale Sarca, 222 - 20126 Milano - www.Pirelli.com - Italy

Declare under our own responsibility that the product **PRG AV4202N** (P/N 151046301) to which this declaration refers conforms with the relevant standards according to the regulation in Article 3.1.a, 3.1.b and 3.2 of the R&TTE Directive 1999/5/EEC of the European Community

Standards Applied:

- EN 55022
- EN 61000-3-2
- EN 61000-3-3
- EN 301 489-1
- EN 301 489-17
- EN 300 328
- EN 60950-1

National Authorities were informed according to Article 6.4 of Frequency Notification. Special Requirements are considered. The product is labeled with CE Marking.

Any unauthorized modification of the product voids this declaration.

This product can be used in the following countries

AT	*BE*	*CY*	*CZ*
DK	*EE*	*FI*	*FR*
DE	*GR*	*HU*	*IE*
IT	*LV*	*LT*	*LU*
MT	*NL*	*PL*	*PT*
SK	*SI*	*ES*	*SE*
GB	*IS*	*LI*	*NO*
CH	*BG*	*RO*	*TR*

WASTE ELECTRICAL AND ELECTRONIC EQUIPMENT (WEEE)

DIRECTIVE 2002/96/EC

This product complies with the WEEE Directive (2002/96/EC) marking requirement. The affixed product label (see above) indicates that you must not discard this electrical/electronic product in domestic household waste.

Product category: With reference to the equipment types in the WEEE directive Annex 1, this product is classified as an “IT and telecommunications equipment” product.

Do not dispose in domestic household waste.

D Glossary

802.11b

The IEEE specification for wireless Ethernet which allows speeds of up to 11 Mbps. The standard provides for 1, 2, 5.5 and 11 Mbps data rates. The rates will switch automatically depending on range and environment.

802.11g

The IEEE specification for wireless Ethernet which allows speeds of up to 54 Mbps. The standard provides for 6, 12, 24, 36, 48 and 54 Mbps data rates. The rates will switch automatically depending on range and environment.

802.11n

The IEEE specification for wireless Ethernet which allows speeds of up to 100 Mbps.

10BASE-T

The IEEE specification for 10 Mbps Ethernet over Category 3, 4 or 5 twisted pair cable.

100BASE-TX

The IEEE specification for 100 Mbps Fast Ethernet over Category 5 twisted-pair cable.

Access Point

An Access Point is a device through which wireless clients connect to other wireless clients and which acts as a bridge between wireless clients and a wired network, such as Ethernet. Wireless clients can be moved anywhere within the coverage area of the access point and still connect with each other. If connected to an Ethernet network, the access point monitors Ethernet traffic and forwards appropriate Ethernet messages to the wireless network, while also monitoring wireless client radio traffic and forwarding wireless client messages to the Ethernet LAN.

Ad Hoc mode

Ad Hoc mode is a configuration supported by most wireless clients. It is used to connect a peer to peer network together without the use of an access point. It offers lower performance than infrastructure mode, which is the mode the router uses. (see also Infrastructure mode.

Auto-negotiation

Some devices in the range support auto-negotiation. Auto-negotiation is where two devices sharing a link, automatically configure to use the best common speed. The order of preference (best first) is: 100BASE-TX full duplex, 100BASE-TX half duplex, 10BASE-T full duplex, and 10BASE-T half duplex. Auto-negotiation is defined in the IEEE 802.3 standard for Ethernet and is an operation that takes place in a few milliseconds.

Bandwidth

The information capacity, measured in bits per second, that a channel can transmit. The bandwidth of Ethernet is 10 Mbps, the bandwidth of Fast Ethernet is 100 Mbps. The bandwidth for 802.11b wireless is 11Mbps.

Category 5 Cables

One of five grades of Twisted Pair (TP) cabling defined by the EIA/TIA-586 standard. Category 5 can be used in Ethernet (10BASE-T) and Fast Ethernet networks (100BASE-TX) and can transmit data up to speeds of 100 Mbps. Category 5 cabling is better to use for network cabling than Category 3, because it supports both Ethernet (10 Mbps) and Fast Ethernet (100 Mbps) speeds.

Channel

Similar to any radio device, the Wireless Cable/DSL router allows you to choose different radio channels in the wireless spectrum. A channel is a particular frequency within the 2.4GHz spectrum within which the Router operates.

Client

The term used to described the desktop PC that is connected to your network.

DHCP

Dynamic Host Configuration Protocol. This protocol automatically assigns an IP address for every computer on your network. Windows 95, Windows 98 and Windows NT 4.0 contain software that assigns IP addresses to workstations on a network. These assignments are made by the DHCP server software that runs on Windows NT Server, and Windows 95 and Windows 98 will call the server to obtain the address. Windows 98 will allocate itself an address if no DHCP server can be found.

DMZ

DMZ (Demilitarized Zone) is an area outside the firewall, to let remote users to have access to items on your network (Web site, FTP download and upload area, etc.).

DNS Server Address

DNS stands for Domain Name System, which allows Internet host computers to have a domain name (such as pirelli.com) and one or more IP addresses (such as 192.168.10.8). A DNS server keeps a database of host computers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing “pirelli.com” into your Internet browser), the user is sent to the proper IP address. The DNS server address used by the computers on your home network is the location of the DNS server your ISP has assigned.

DSL

Short for digital subscriber line, but is commonly used in reference to the asymmetric version of this technology (ADSL) that allows data to be sent over existing copper telephone lines at data rates of from 1.5 to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate). ADSL requires a special ADSL modem. ADSL is growing in popularity as more areas around the world gain access.

DSL modem

DSL stands for digital subscriber line. V DSL modem uses your existing phone lines to send and receive data at high speeds.

Encryption

A method for providing a level of security to wireless data transmissions. The Router uses two levels of encryption; 40/64 bit and 128 bit. 128 bit is a more powerful level of encryption than 40/64 bit.

Ethernet

A LAN specification developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks use CSMA/CD to transmit packets at a rate of 10 Mbps over a variety of cables.

Ethernet Address

See MAC address.

Fast Ethernet

An Ethernet system that is designed to operate at 100 Mbps.

Firewall

Electronic protection that prevents anyone outside of your network from seeing your files or damaging your computers.

Full Duplex

A system that allows packets to be transmitted and received at the same time and, in effect, doubles the potential throughput of a link.

IEEE

Institute of Electrical and Electronics Engineers. This American organization was founded in 1963 and sets standards for computers and communications.

IETF

Internet Engineering Task Force. An organization responsible for providing engineering solutions for TCP/IP networks. In the network management area, this group is responsible for the development of the SNMP protocol.

IGMP

The Internet Group Management Protocol (IGMP) is an Internet protocol that provides a way for an Internet computer to report its multicast group membership to adjacent routers. Multicasting allows one computer on the Internet to send content to multiple other computers that have identified themselves as interested in receiving the originating computer's content. Multicasting can be used for such applications as updating the address books of mobile computer users in the field, sending out company newsletters to a distribution list, and
"broadcasting" high-bandwidth programs of streaming media to an audience that has "tuned in" by setting up a multicast group membership.

Infrastructure mode

Infrastructure mode is the wireless configuration supported by the Router. You will need to ensure all of your clients are set up to use infrastructure mode in order for them to communicate with the Access Point built into your Router. (see also Ad Hoc mode)

IP

Internet Protocol. IP is a layer 3 network protocol that is the standard for sending data through a network. IP is part of the TCP/IP set of protocols that describe the routing of packets to addressed devices. An IP address consists of 32 bits divided into two or three fields: a network number and a host number or a network number, a subnet number, and a host number.

IP Address

Internet Protocol Address. A unique identifier for a device attached to a network using TCP/IP. The address is written as four octets separated with periods (full-stops), and is made up of a network section, an optional subnet section and a host section.

ISP

Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

LAN

Local Area Network. A network of end stations (such as PCs, printers, servers) and network devices (hubs and switches) that cover a relatively small geographic area (usually not larger than a floor or building). LANs are characterized by high transmission speeds over short distances (up to 1000 metres).

MAC

Media Access Control. A protocol specified by the IEEE for determining which devices have access to a network at any one time.

MAC Address

Media Access Control Address. Also called the hardware or physical address. A layer 2 address associated with a particular network device. Most devices that connect to a LAN have a MAC address assigned to them as they are used to identify other devices in a network. MAC addresses are 6 bytes long.

Mbps

Megabits per second.

MDI/MDIX

In cable wiring, the concept of transmit and receive are from the perspective of the PC, which is wired as a Media Dependant Interface (MDI). In MDI wiring, a PC transmits on pins 1 and 2. At the hub, switch, router, or access point, the perspective is reversed, and the hub receives on pins 1 and 2. This wiring is referred to as Media Dependant Interface - Crossover (MDI-X).

NAT

Network Address Translation. NAT enables all the computers on your network to share one IP address. The NAT capability of the Router allows you to access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.

Network

A Network is a collection of computers and other computer equipment that are connected for the purpose of exchanging information or sharing resources. Networks vary in size, some are within a single room, others span continents.

Network Interface Card (NIC)

A circuit board installed into a piece of computing equipment, for example, a computer, that enables you to connect it to the network. A NIC is also known as an adapter or adapter card.

Protocol

A set of rules for communication between devices on a network. The rules dictate format, timing, sequencing and error control.

PSTN

Public Switched Telephone Network.

PPPoA

Point-to-Point Protocol over ATM. PPP over ATM is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

PPPoE

Point-to-Point Protocol over Ethernet. Point-to-Point Protocol is a method of data transmission originally created for dial-up connections; PPPoE is for Ethernet connections.

RJ-45

A standard connector used to connect Ethernet networks. The “RJ” stands for “registered jack”.

Router

A device that acts as a central hub by connecting to each computer's network interface card and managing the data traffic between the local network and the Internet.

Server

A computer in a network that is shared by multiple end stations. Servers provide end stations with access to shared network services such as computer files and printer queues.

SSID

Service Set Identifier. Some vendors of wireless products use SSID interchangeably with ESSID.

Subnet Address

An extension of the IP addressing scheme that allows a site to use a single IP network address for multiple physical networks.

Subnet mask

A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet, which must assigned by InterNIC).

Subnets

A network that is a component of a larger network.

Switch

A device that interconnects several LANs to form a single logical LAN that comprises of several LAN segments. Switches are similar to bridges, in that they connect LANs of a different type; however they connect more LANs than a bridge and are generally more sophisticated.

TCP/IP

Transmission Control Protocol/Internet Protocol. This is the name for two of the most well-known protocols developed for the interconnection of networks. Originally a UNIX standard, TCP/IP is now supported on almost all platforms, and is the protocol of the Internet.

TCP

It relates to the content of the data travelling through a network — ensuring that the information sent arrives in one piece when it reaches its destination. IP relates to the address of the end station to which data is being sent, as well as the address of the destination network.

Traffic

The movement of data packets on a network.

Universal plug and play

Universal plug and play is a system which allows compatible applications to read some of their settings from the Router. This allows them to automatically configure some, or all, of their settings and need less user configuration.

URL Filter

A URL Filter is a feature of a firewall that allows it to stop its clients form browsing inappropriate Web sites.

UTP

Unshielded twisted pair is the cable used by 10BASE-T and 100BASE-Tx Ethernet networks.

VCI

VCI - Virtual Channel Identifier. The identifier in the ATM (Asynchronous Transfer Mode) cell header that identifies to which virtual channel the cell belongs.

VPI

VPI - Virtual Path Identifier. The field in the ATM (Asynchronous Transfer Mode) cell header that identifies to which VP (Virtual Path) the cell belongs.

WAN

Wide Area Network. A network that connects computers located in geographically separate areas (for example, different buildings, cities, or countries). The Internet is an example of a wide area network.

WEP

Wired Equivalent Privacy. A shared key encryption mechanism for wireless networking. Encryption strength is 40/64 bit or 128 bit.

Wi-Fi

Wireless Fidelity. This is the certification granted by WECA to products that meet their inter operability criteria. (see also 802.11b, WECA)

Wi-Fi Alliance

The Wi-Fi Alliance is a trade group, owning the trademark to Wi-Fi, aiming at performing the testing, certifying interoperability of products and promoting the technology.

Wireless Client

The term used to describe a desktop or mobile PC that is wirelessly connected to your wireless network

Wireless LAN Service Area

Another term for ESSID (Extended Service Set Identifier)

Wizard

A Windows application that automates a procedure such as installation or configuration.

WLAN

Wireless Local Area Network. A WLAN is a group of computers and devices connected together by wireless in a relatively small area (such as a house or office).

WPA

Wi-Fi Protected Access. A dynamically changing encryption mechanism for wireless networking. Encryption strength is 256 bit.

PIRELLI Broadband Solutions

Viale Sarca 222
20126 Milano
Italy