



User Manual

Version 4.8

Jungo Software Technologies Ltd.

User Manual: Version 4.8

Jungo Software Technologies Ltd.

Copyright © 1998-2008 Jungo Software Technologies Ltd. All Rights Reserved.

Product names mentioned in this document are trademarks of their respective manufacturers and are used here only for identification purposes.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement. The software may be used, copied or distributed only in accordance with that agreement. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means, electronically or mechanically, including photocopying and recording for any purpose without the written permission of Jungo Ltd.

This document is available for download at: <http://www.jungo.com/openrg/documentation.html>, version 4.8

Table of Contents

I. Getting Started	1
1. Introduction to OpenRG	3
2. Installing Your Gateway	5
2.1. Connecting Your Gateway	5
2.1.1. Power Connection	6
2.1.2. Wide Area Network (WAN) Connection	7
2.2. Connecting Your PC	8
2.2.1. Local Area Network (LAN) Connection	8
2.2.2. Wireless LAN Connection	11
2.2.3. USB LAN Connection	13
2.3. Connecting to the Internet	13
2.3.1. Web Interception	14
2.3.2. Installation Wizard	14
2.3.3. Connection Problem Interception Page	27
2.3.4. Saved Login Details	28
2.4. Connecting Peripheral Equipment	28
2.4.1. Connecting a Telephone	28
2.4.2. Connecting a Printer	33
2.4.3. Connecting a Mass Storage Device	36
2.4.4. Connecting a Media Client	41
II. Managing Your Gateway	46
3. Using the Management Console	51
3.1. First Time Login	52
3.2. Accessing the WBM	53
3.3. Navigational Aids	54
3.4. Managing Tables	55
4. Home	56
4.1. Overview	56
4.2. Map View	58
4.3. Installation Wizard	60
4.4. Quick Setup	60
4.4.1. Configuring Your Internet Connection	61
4.4.2. Wireless	70
4.4.3. Jungo.net	71
4.4.4. Quick Setup Completed	72
5. Internet Connection	73
5.1. Overview	73
5.2. Settings	74
5.3. Diagnostics	75
6. Local Network	77
6.1. Overview	77
6.2. Device View	79
6.3. Wireless	80
6.3.1. Overview	80
6.3.2. Settings	81
6.3.3. Advanced	81

6.4. Shared Storage	82
6.4.1. Managing Disk Partitions	83
6.4.2. Defining a Location for System Files	89
6.4.3. Optimizing Data Storage and Backup with RAID	90
6.5. Shared Printers	97
6.5.1. Configuring the Print Server	98
6.5.2. Selecting a Print Protocol	99
6.5.3. Sharing a Samba Printer Driver	121
6.5.4. Controlling Access to Print Jobs	123
6.6. IP-PBX	126
7. Services	128
7.1. Overview	128
7.2. Jungo.net	128
7.2.1. Creating a Jungo.net Account	129
7.2.2. Accessing Jungo.net	134
7.2.3. Reconnecting Your Gateway to Jungo.net	136
7.2.4. Registering and Using the Jungo.net Services	136
7.2.5. Restoring OpenRG's Configuration from Jungo.net	177
7.3. Firewall	180
7.3.1. Configuring Basic Security Settings	181
7.3.2. Controlling Access to Internet Services	183
7.3.3. Using Port Forwarding	186
7.3.4. Designating a DMZ Host	191
7.3.5. Using Port Triggering	192
7.3.6. Restricting Web Access	195
7.3.7. Using OpenRG's Network Address and Port Translation	198
7.3.8. Viewing Open Connections	207
7.3.9. Configuring the Advanced Filtering Mechanism	208
7.3.10. Viewing the Firewall Log	211
7.3.11. Applying Corporate-Grade Security	217
7.4. Quality of Service	226
7.4.1. Overview	227
7.4.2. Internet Connection Utilization	229
7.4.3. Traffic Priority	231
7.4.4. Traffic Shaping	236
7.4.5. Differentiated Services Code Point Settings	241
7.4.6. 802.1p Settings	243
7.4.7. Class Statistics	243
7.4.8. Voice QoS Scenario	244
7.4.9. IPTV QoS Scenario	254
7.5. Media Sharing	265
7.5.1. Configuring the Media Sharing Service	265
7.5.2. Accessing the Shared Media from a LAN Computer	267
7.6. Voice	271
7.6.1. Configuring Your Telephone Line Services	272
7.6.2. Operating Your Telephone	273
7.6.3. Configuring and Using Speed Dial	274
7.6.4. Sending a Fax	276

7.6.5. Customizing Your Phone Service with a Numbering Plan	277
7.6.6. Using Distinctive Ring	279
7.6.7. Ensuring Constant Connectivity with Failover	280
7.6.8. Advanced Telephony Options	280
7.7. IP-PBX	290
7.7.1. Configuring Your Analog Extensions	291
7.7.2. Operating Your Telephone	293
7.7.3. Connecting VoIP Telephones	294
7.7.4. Opening Telephony Service Accounts	298
7.7.5. Defining VoIP Lines	298
7.7.6. Creating Auto Attendants	303
7.7.7. Handling Incoming Calls	306
7.7.8. Handling Outgoing Calls	309
7.7.9. Using the Voice Mail	312
7.7.10. Adding On-Hold Music Files	314
7.7.11. Automating Call Distribution with Hunt Groups	314
7.7.12. Advanced Telephony Options	317
7.8. Parental Control	327
7.8.1. Overview	328
7.8.2. Filtering Policy	329
7.8.3. Advanced Options	332
7.8.4. Statistics	333
7.9. Email Filtering	334
7.9.1. Overview	334
7.9.2. Advanced Options	337
7.10. Virtual Private Network	338
7.10.1. Internet Protocol Security	338
7.10.2. Secure Socket Layer VPN	375
7.10.3. Point-to-Point Tunneling Protocol Server	392
7.10.4. Layer 2 Tunneling Protocol Server	394
7.11. Storage	398
7.11.1. FTP Server	398
7.11.2. File Server	401
7.11.3. WINS Server	417
7.11.4. Web Server	418
7.11.5. Mail Server	422
7.11.6. Backup and Restore	427
7.12. Personal Domain Name (Dynamic DNS)	430
7.12.1. Opening a Dynamic DNS Account	430
7.12.2. Using Dynamic DNS	430
7.13. Advanced	432
7.13.1. DNS Server	432
7.13.2. IP Address Distribution	434
7.13.3. Bluetooth Settings	439
7.13.4. RADIUS Server	441
8. System	454
8.1. Overview	454
8.2. Settings	454

8.2.1. Overview	454
8.2.2. Date and Time	459
8.3. Users	462
8.3.1. User Settings	463
8.3.2. Group Settings	465
8.4. Network Connections	465
8.4.1. The Connection Wizard	468
8.4.2. Network Types	478
8.4.3. LAN Bridge	479
8.4.4. LAN Ethernet	488
8.4.5. LAN Hardware Ethernet Switch	490
8.4.6. LAN USB	493
8.4.7. LAN Wireless	495
8.4.8. WAN Ethernet	526
8.4.9. Point-to-Point Protocol over Ethernet (PPPoE)	533
8.4.10. Ethernet Connection	541
8.4.11. Layer 2 Tunneling Protocol (L2TP)	542
8.4.12. Layer 2 Tunneling Protocol Server (L2TP Server)	552
8.4.13. Point-to-Point Tunneling Protocol (PPTP)	555
8.4.14. Point-to-Point Tunneling Protocol Server (PPTP Server)	565
8.4.15. Internet Protocol Security (IPSec)	568
8.4.16. Internet Protocol Security Server (IPSec Server)	570
8.4.17. Dynamic Host Configuration Protocol (DHCP)	572
8.4.18. Manual IP Address Configuration	574
8.4.19. Determine Protocol Type Automatically	575
8.4.20. Point-to-Point Protocol over ATM (PPPoA)	577
8.4.21. Ethernet over ATM (EThoA)	586
8.4.22. Classical IP over ATM (CLIP)	591
8.4.23. WAN-LAN Bridge	596
8.4.24. Virtual LAN Interface (VLAN)	608
8.4.25. Routed IP over ATM (IPoA)	627
8.4.26. Internet Protocol over Internet Protocol (IPIP)	633
8.4.27. General Routing Encapsulation (GRE)	637
8.5. Monitor	644
8.5.1. Network	644
8.5.2. CPU	645
8.5.3. Log	646
8.6. Routing	648
8.6.1. Overview	648
8.6.2. IPv6	660
8.6.3. BGP and OSPF	668
8.6.4. PPPoE Relay	671
8.7. Management	671
8.7.1. Universal Plug and Play	671
8.7.2. Simple Network Management Protocol	676
8.7.3. Remote Administration	680
8.7.4. Secure Shell	684
8.8. Maintenance	685

8.8.1. About OpenRG	685
8.8.2. Configuration File	686
8.8.3. Reboot	686
8.8.4. Restore Defaults	687
8.8.5. OpenRG Firmware Upgrade	688
8.8.6. MAC Cloning	690
8.8.7. Diagnostics	691
8.9. Objects and Rules	694
8.9.1. Protocols	694
8.9.2. Network Objects	696
8.9.3. Scheduler Rules	698
8.9.4. Certificates	701
9. Advanced	713
III. Additional Features	717
10. Zero Configuration Technology	719
10.1. IP Auto-detection	719
10.2. Automatic Configuration for Non-Plug-and-Play Networks	720
10.3. Network Map Builder	720
IV. Appendix	721
11. List of Acronyms	723
12. Glossary	725
13. Licensing Acknowledgement and Source Code Offering	735
14. Contact Jungo	736

Part I. Getting Started

Table of Contents

1. Introduction to OpenRG	3
2. Installing Your Gateway	5
2.1. Connecting Your Gateway	5
2.1.1. Power Connection	6
2.1.2. Wide Area Network (WAN) Connection	7
2.2. Connecting Your PC	8
2.2.1. Local Area Network (LAN) Connection	8
2.2.2. Wireless LAN Connection	11
2.2.3. USB LAN Connection	13
2.3. Connecting to the Internet	13
2.3.1. Web Interception	14
2.3.2. Installation Wizard	14
2.3.3. Connection Problem Interception Page	27
2.3.4. Saved Login Details	28
2.4. Connecting Peripheral Equipment	28
2.4.1. Connecting a Telephone	28
2.4.2. Connecting a Printer	33
2.4.3. Connecting a Mass Storage Device	36
2.4.4. Connecting a Media Client	41

1

Introduction to OpenRG

OpenRG™ is a leading software solution for broadband service delivery. Its unique hardware-independent design enables service providers to concentrate on enhancing service to their subscribers, offering full flexibility to select the best suited CPE, and eliminating the complexity and costs that are typically associated with using multiple CPE models and deploying new ones.

OpenRG is a best-of-breed middleware product for residential gateways, which resides in the CPE. The middleware includes drivers, OS, protocols and advanced applications to enable all of the broadband applications and services.

OpenRG empowers various network devices in the digital home, including triple play residential gateways, home/SOHO routers, home gateways, wireless access points, cable/DSL routers, voice gateways and more.



Broadband operators worldwide have selected and deployed OpenRG-based home gateways to drive revenue generating business models and services.

Jungo also offers OpenSMB—gateway middleware for the small and medium-sized business market. References to OpenRG in this document also apply to OpenSMB.

You can view OpenRG's specification as well as additional documentation at <http://www.jungo.com/openrg/documentation.html>, version 4.8.

2

Installing Your Gateway

Connecting your computer or home network to the gateway is a simple procedure, varying slightly according to your different hosts' operating systems. By the end of this chapter you will have your gateway installed and be able to surf the Internet from a computer connected to the gateway. You will also have peripheral equipment installed, such as a telephone, printer, mass storage device, or a media client.



Figure 2.1. Your Home Network

This chapter consists of the following steps:

1. Connecting your gateway [[Section 2.1](#)]
2. Connecting your PC [[Section 2.2](#)]
3. Connecting to the Internet [[Section 2.3](#)]
4. Connecting peripheral equipment [[Section 2.4](#)]

2.1. Connecting Your Gateway

Your supplied kit includes a gateway and a power cable. The following illustrations represent a DSL gateway, viewed from both the front and the rear.

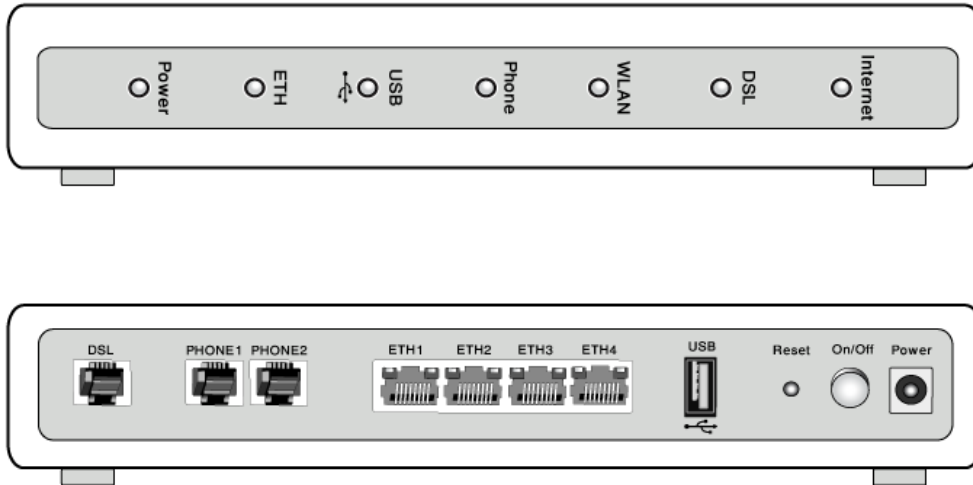


Figure 2.2. Front and Rear Panels

The front panel features LEDs that light up and/or blink when the features they represent are active, providing you feedback of your gateway's activity. The rear panel contains various input sockets, as well as an on/off switch and a reset button.

2.1.1. Power Connection

Connect the supplied power cable to its matching socket on the rear panel of the gateway, and to a wall power outlet. Then, switch the gateway on by pressing the on/off button.

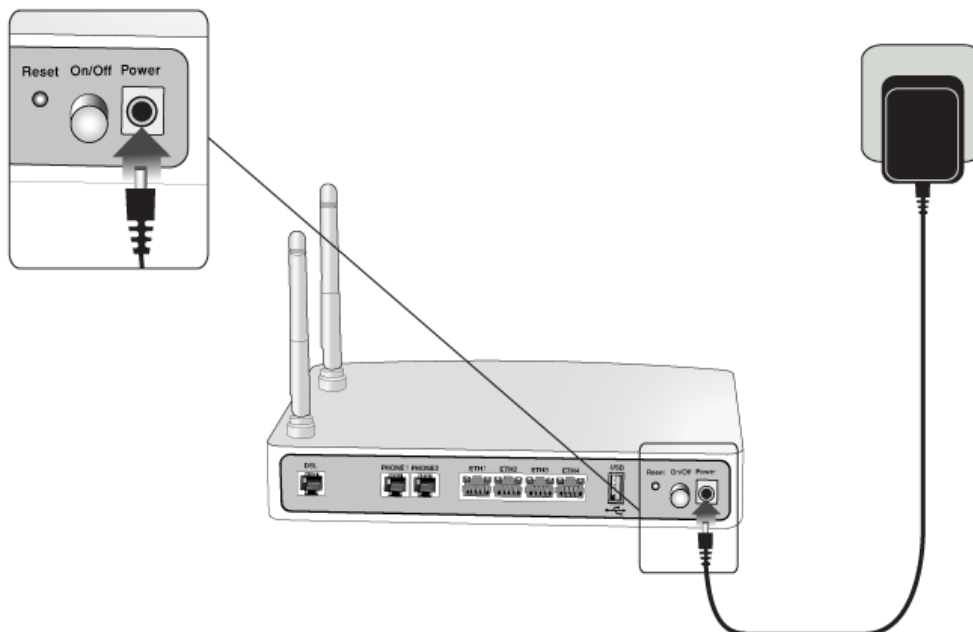


Figure 2.3. Power Connection

2.1.2. Wide Area Network (WAN) Connection

Your connection to the Internet is determined by the type of gateway that you have. If your gateway has a built-in DSL modem, connect its DSL socket to the wall socket using a telephone cable.

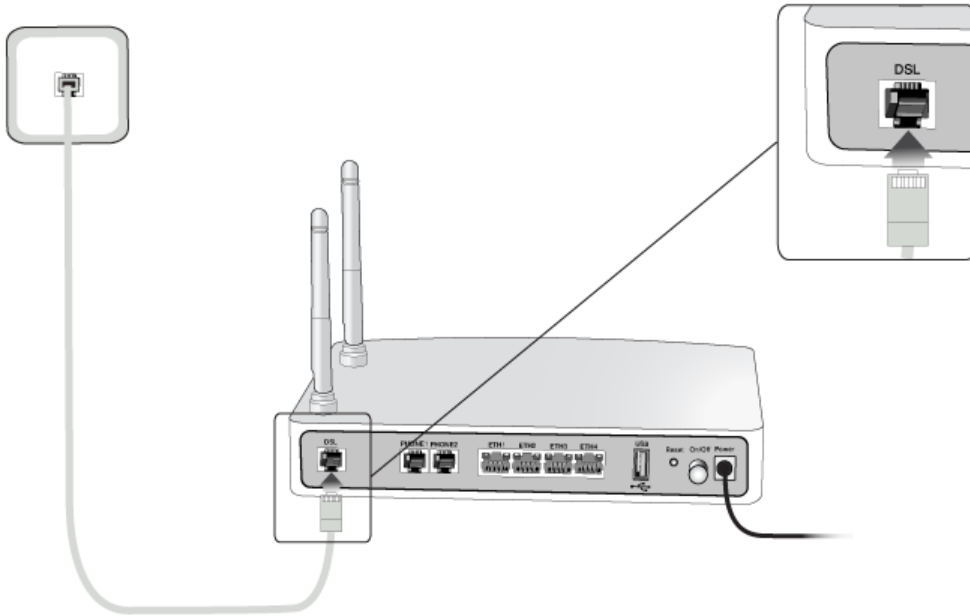


Figure 2.4. DSL Connection

If your gateway has an Ethernet socket for the WAN, connect it to the external modem you have (or any other Ethernet socket you might have), using an Ethernet cable. Your modem should be connected to the wall socket. Refer to your modem's documentation if necessary.

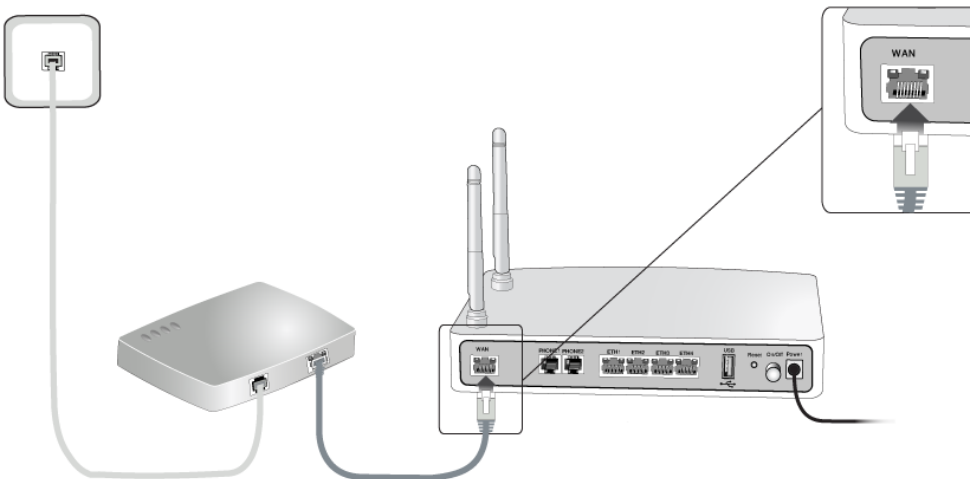


Figure 2.5. WAN Connection

2.2. Connecting Your PC

2.2.1. Local Area Network (LAN) Connection

Your computer can connect to the gateway in various forms (Ethernet, USB, Wireless etc.), each requiring a different physical connection (except for wireless). The most common type of connection is Ethernet. Use an Ethernet cable to connect the computer's network card to any one of the Ethernet ports on your gateway.

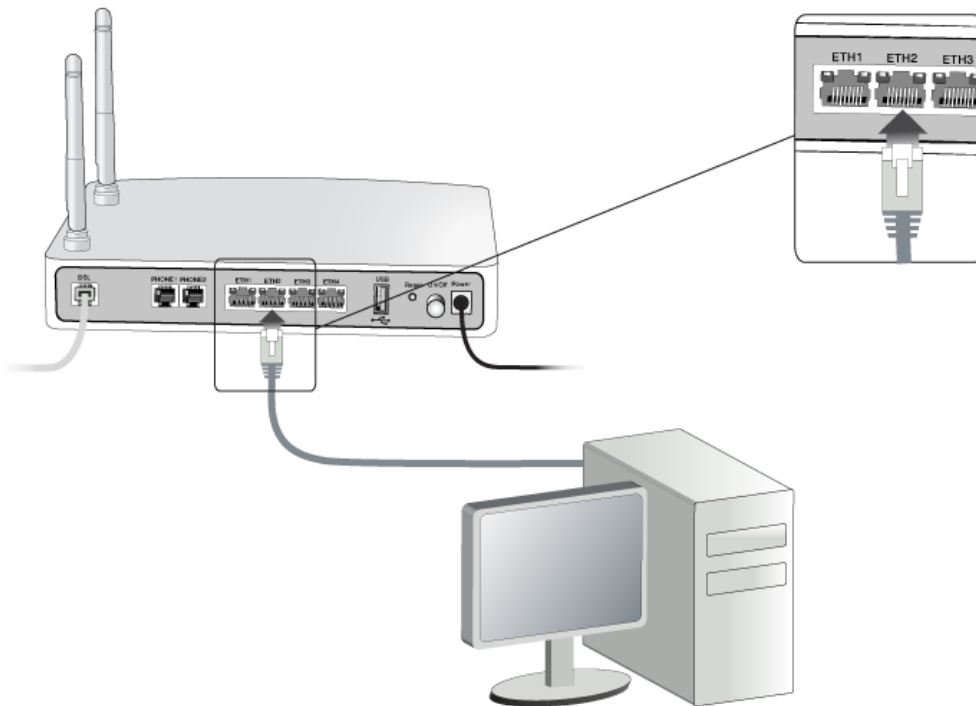


Figure 2.6. LAN Connection

Each network interface on the PC should either be configured with a statically defined IP address and DNS address, or should be instructed to automatically obtain an IP address using the Network DHCP server. OpenRG provides a DHCP server on its LAN and it is recommended to configure your LAN to obtain its IP and DNS server IP settings automatically. This configuration principle is identical but performed differently on each operating system.

Figure 2.7 displays the 'TCP/IP Properties' dialog box as it appears in Windows XP. Following are TCP/IP configuration instructions for all supported operating systems.

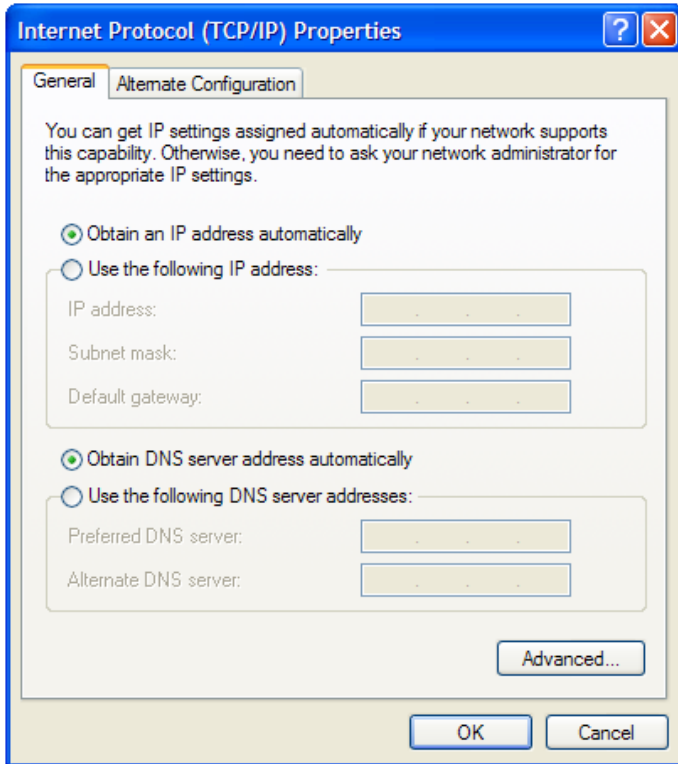


Figure 2.7. IP and DNS Configuration

- **Windows XP**

1. Access 'Network Connections' from the Control Panel.
2. Right-click the Ethernet connection icon, and select 'Properties'.
3. Under the 'General' tab, select the 'Internet Protocol (TCP/IP)' component, and press the 'Properties' button.
4. The 'Internet Protocol (TCP/IP)' properties window appears (see [Figure 2.7](#)).
 - a. Select the 'Obtain an IP address automatically' radio button.
 - b. Select the 'Obtain DNS server address automatically' radio button.
 - c. Click 'OK' to save the settings.

- **Windows 2000/98/Me**

1. Access 'Network and Dialing Connections' from the Control Panel.
2. Right-click the Ethernet connection icon, and select 'Properties' to display the connection's properties.
3. Select the 'Internet Protocol (TCP/IP)' component, and press the 'Properties' button.
4. The 'Internet Protocol (TCP/IP)' properties will be displayed.

- a. Select the 'Obtain an IP address automatically' radio button.
- b. Select the 'Obtain DNS server address automatically' radio button.
- c. Click 'OK' to save the settings.

- **Windows NT**

1. Access 'Network' from the Control Panel.
2. From the 'Protocol' tab, select the 'Internet Protocol (TCP/IP)' component, and press the 'Properties' button.
3. From the 'IP Address' tab select the 'Obtain an IP address automatically' radio button.
4. From the 'DNS' tab, verify that no DNS server is defined in the 'DNS Service Search Order' box and no suffix is defined in the 'Domain Suffix Search Order' box.

- **Linux**

1. Login into the system as a super-user, by entering "su" at the prompt.
2. Type "ifconfig" to display the network devices and allocated IP addresses.
3. Type "pump -i <dev>", where <dev> is the network device name.
4. Type "ifconfig" again to view the new allocated IP address.
5. Make sure no firewall is active on device <dev>.

2.2.2. Wireless LAN Connection

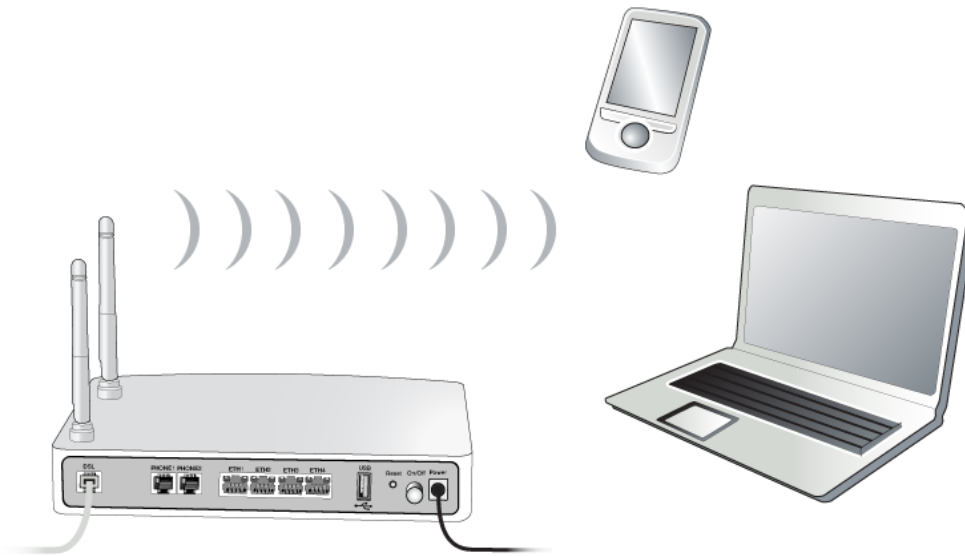


Figure 2.8. Wireless Network

If your PC has wireless capabilities, Windows will automatically recognize this and create a wireless connection for you. You can view this connection in the 'Network Connections' window.



Note: The following description and images are in accordance with Microsoft Windows XP, Version 2002, running Service Pack 2.

1. From the Windows Control Panel, open the 'Network Connections' window.



Figure 2.9. Network Connections

2. Double-click the wireless connection icon. The 'Wireless Network Connection' screen appears, displaying all available wireless networks in your vicinity. If your gateway is connected and active, you will see OpenRG's wireless connection. Note that the connection's status is 'Not connected' and defined as "Unsecured wireless network".

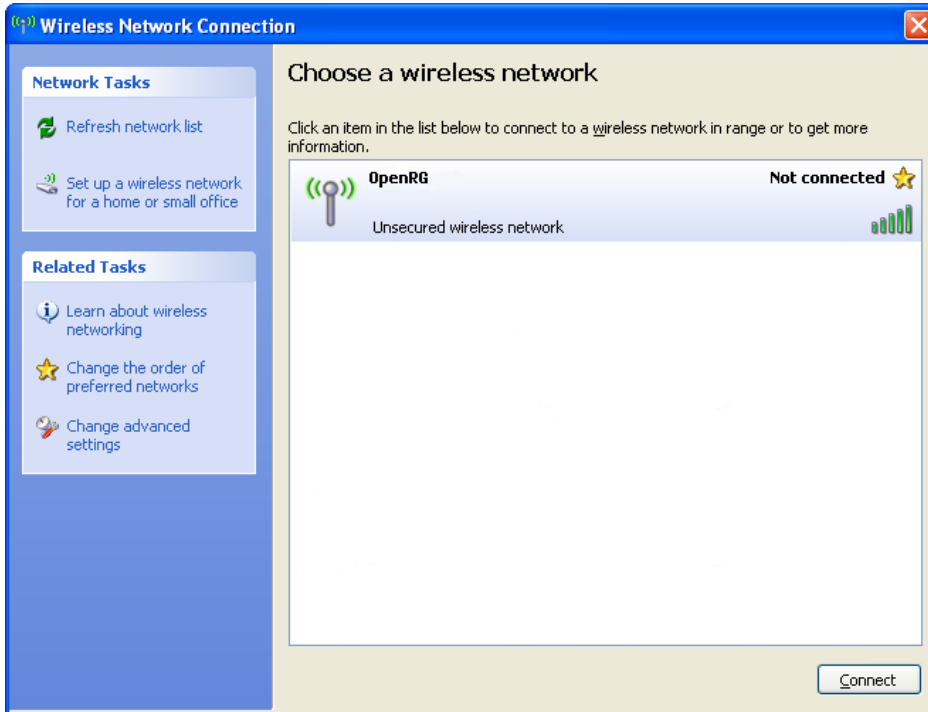


Figure 2.10. Available Wireless Connections

3. Click the connection once to mark it, and then click the 'Connect' button at the bottom of the screen. After the connection is established, its status will change to 'Connected':

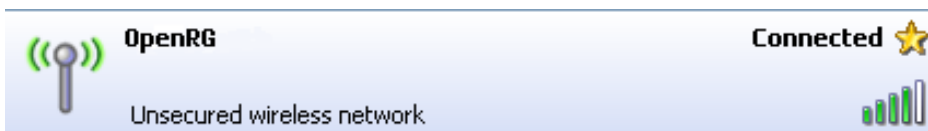


Figure 2.11. Connected Wireless Network

A balloon will appear in the notification area, announcing the successful initiation of the wireless connection.

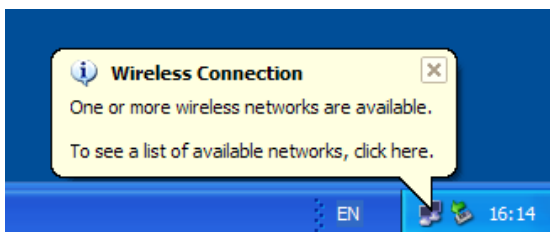


Figure 2.12. Wireless Connection Information

4. Test the connection by disabling all other connections in the Windows 'Network Connections' screen above and browsing the Internet.

2.2.3. USB LAN Connection

Windows computers can be connected to the gateway via a USB port. This requires a download and installation of a USB driver.

1. Connect the Master end of the USB cable to the PC.
2. Connect the Slave end of the USB cable to the gateway. The 'Found New Hardware' dialog box will appear.

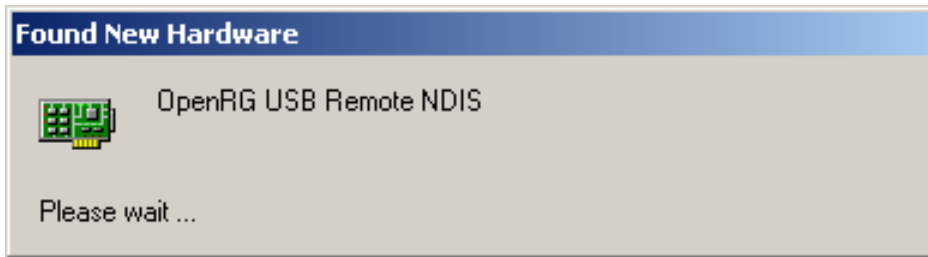


Figure 2.13. Found New Hardware

3. After the device detection process, you will be prompted to specify the location of the USB driver. Download the driver from http://www.jungo.com/openrg/download/openrg_usb_rndis.tgz, and specify its location.

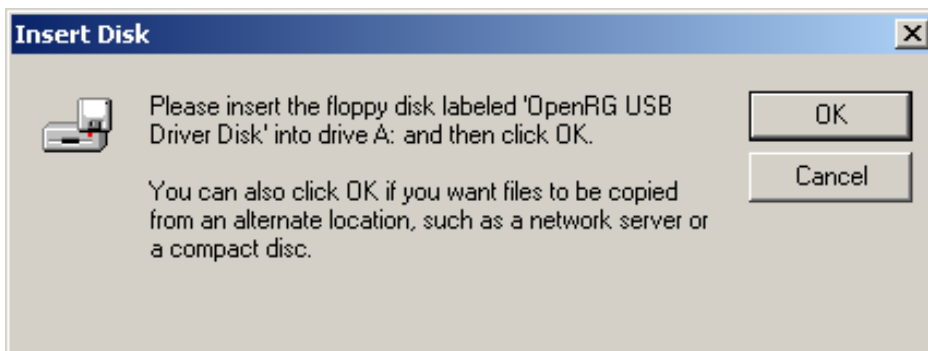


Figure 2.14. Insert Disk

4. Windows will automatically copy all of the files needed for networking and create a new USB network connection.

2.3. Connecting to the Internet

Now that your equipment is connected, open a browser window on your PC and browse to <http://www.cnn.com>.

2.3.1. Web Interception

Any initial attempt to surf the Internet from a computer connected to your gateway will be intercepted by OpenRG, which will display the installation wizard's 'Welcome to OpenRG' screen, along with an attention message:

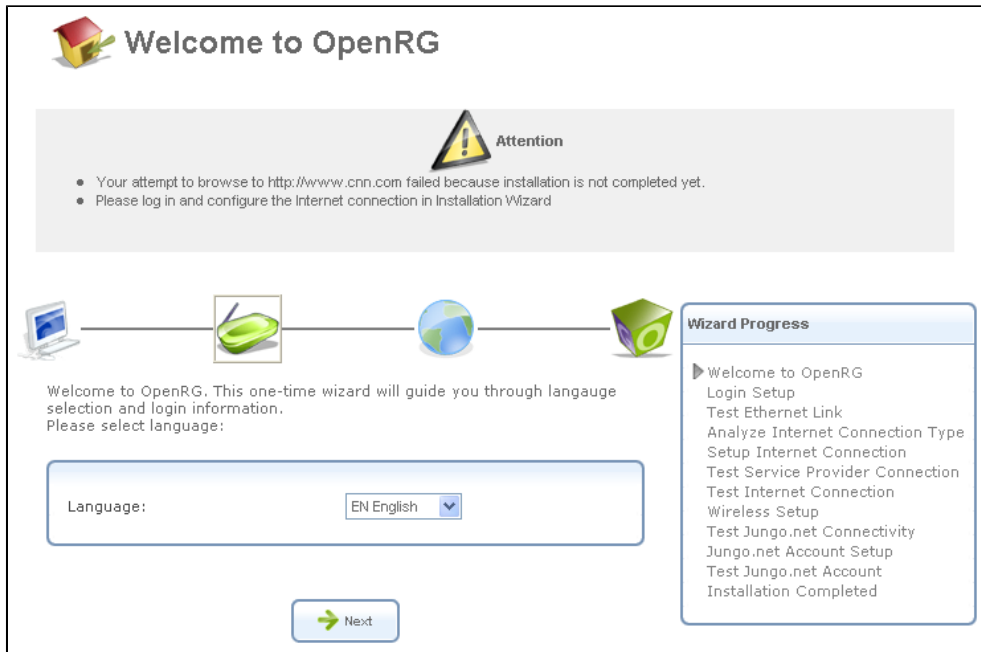


Figure 2.15. Web Interception Message

To gain Internet access and setup your gateway, follow the steps of the wizard procedure. Once an Internet connection is established, the interception attention message will re-appear with a 'here' link that you can click in order to browse to your originally requested Internet address.

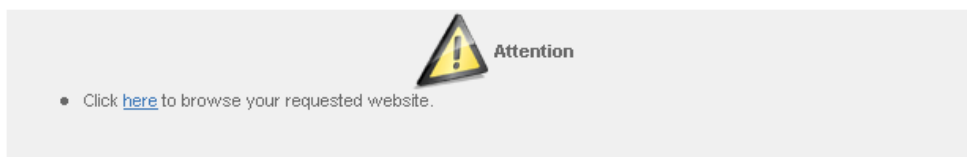


Figure 2.16. Attention

2.3.2. Installation Wizard

Once your gateway is physically connected, OpenRG provides an Installation Wizard that automatically diagnoses your network environment and configures its components. As explained in its first screen, the installation wizard is a step-by-step procedure that guides you through establishing an Internet connection, a wireless network, and helps you to subscribe for different services by creating a Jungo.net account. 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.



Figure 2.17. Installation Wizard



Warning: The installation wizard overrides all Internet connection settings, which you may have previously defined.

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.

2.3.2.1. Step 1: Test Ethernet Link

The first step is a test of the Ethernet connection. This step may fail if OpenRG cannot detect your Ethernet link (for example, if the cable is unplugged).

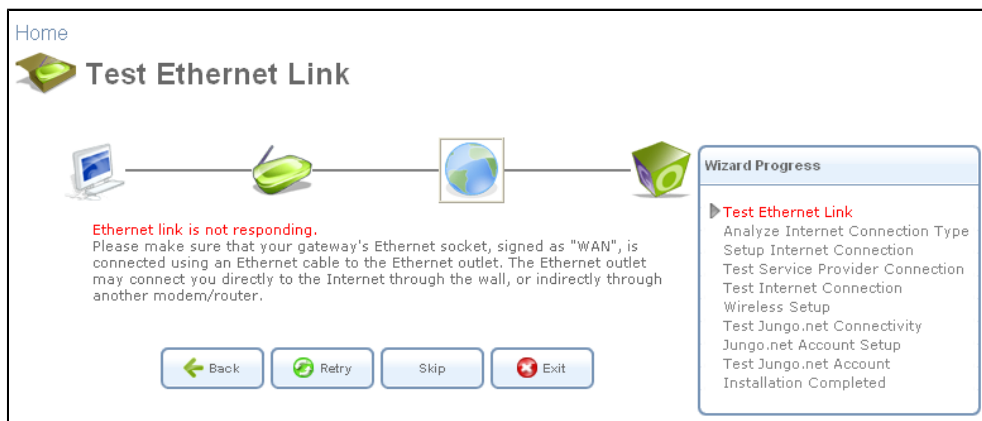


Figure 2.18. Test Ethernet Link

Verify that your Ethernet/DSL cable is connected properly, and click 'Retry'.

2.3.2.2. Step 2: Analyze Internet Connection Type

The next step is an analysis of your Internet connection.

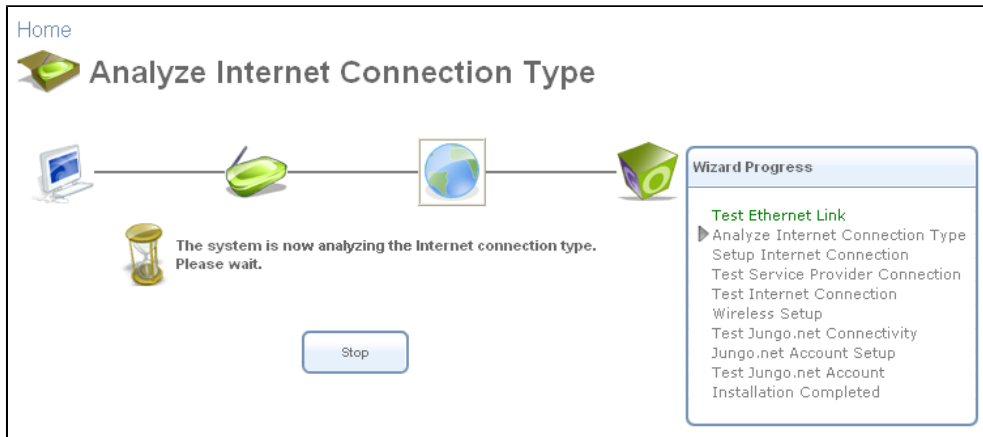


Figure 2.19. Analyze Internet Connection Type

This step may fail if OpenRG is unable to detect your Internet connection type.

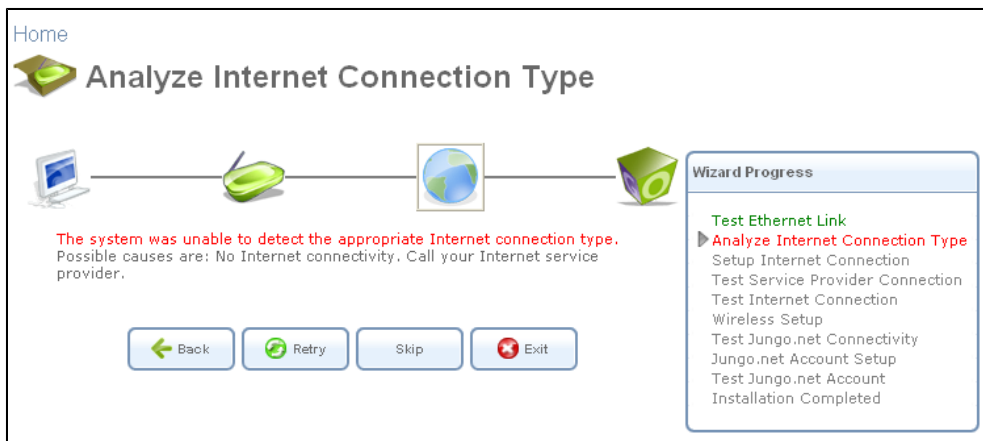


Figure 2.20. Analyze Internet Connection Type – Failure

After three retries, the screen provides a link to manually set the Internet connection type.

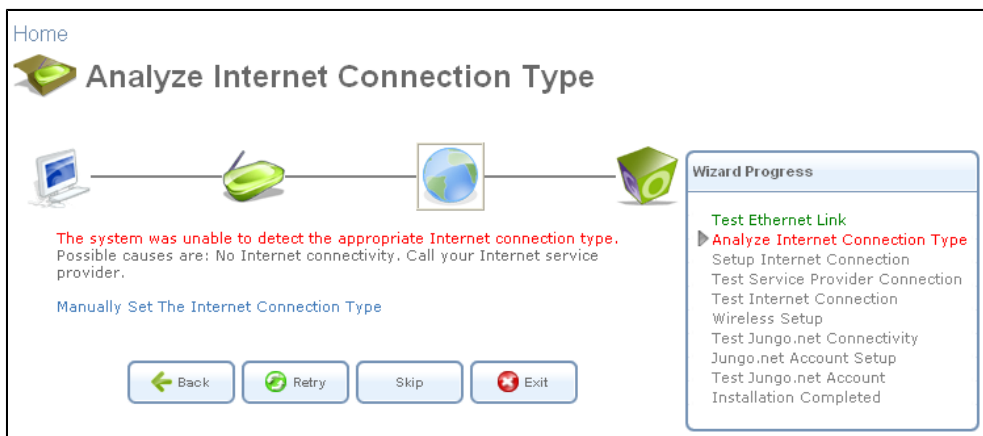


Figure 2.21. Analyze Internet Connection Type – Manual Set

Click this link. The screen refreshes, displaying a connection type combo box.

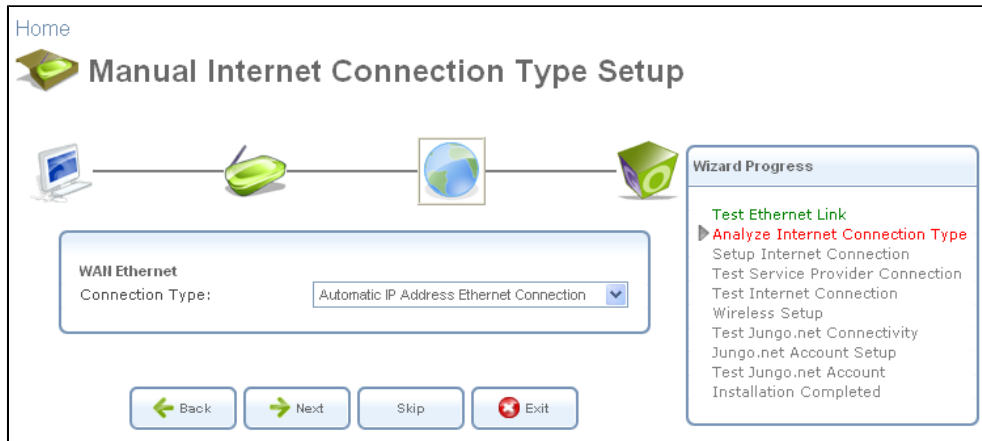


Figure 2.22. Manual Internet Connection Type Setup

To learn about manually configuring your Internet connection, refer to [Section 4.4.1](#).

2.3.2.3. Step 3: Setup Internet Connection

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

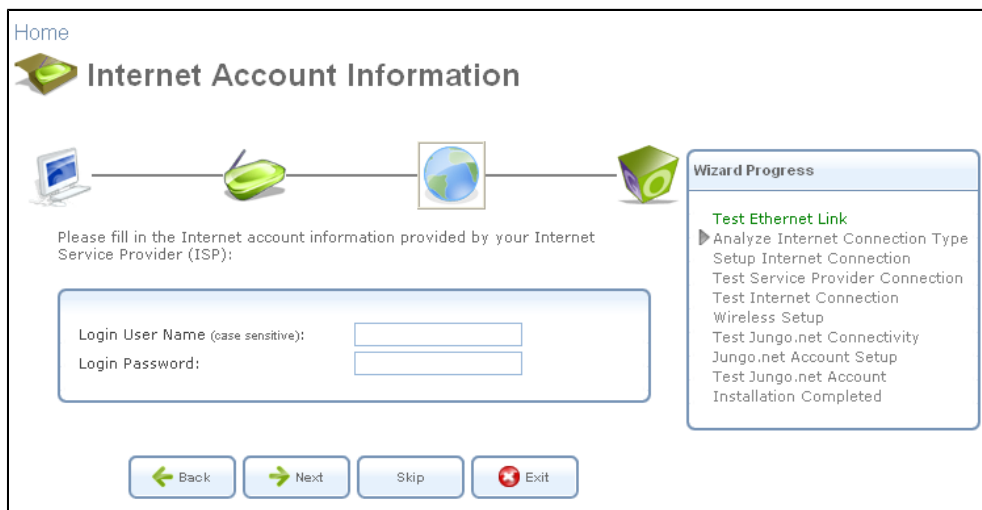


Figure 2.23. Internet Account Information

Enter your user name and password and click 'Next'. Failure to enter the correct details yields the following message. Click 'Back' and try again.

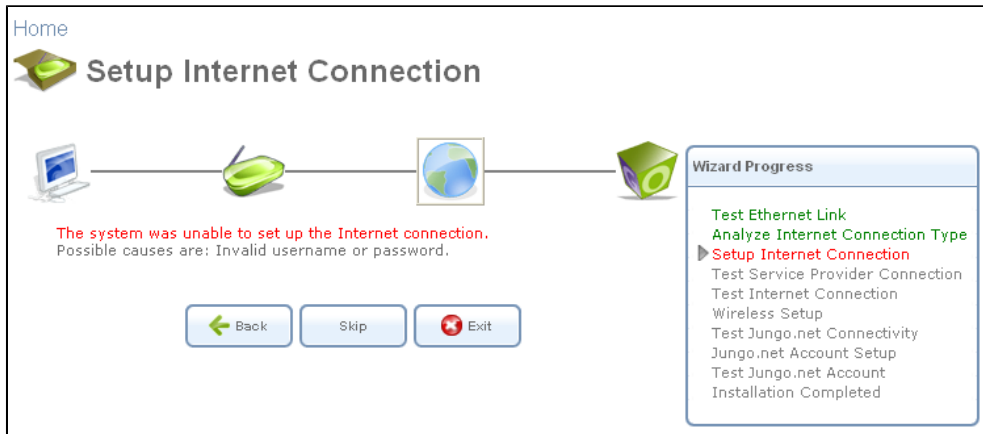


Figure 2.24. Setup Internet Connection

If you had entered a user name and password in the past, the following screen appears, enabling you to either enter new login details, or use your old ones.

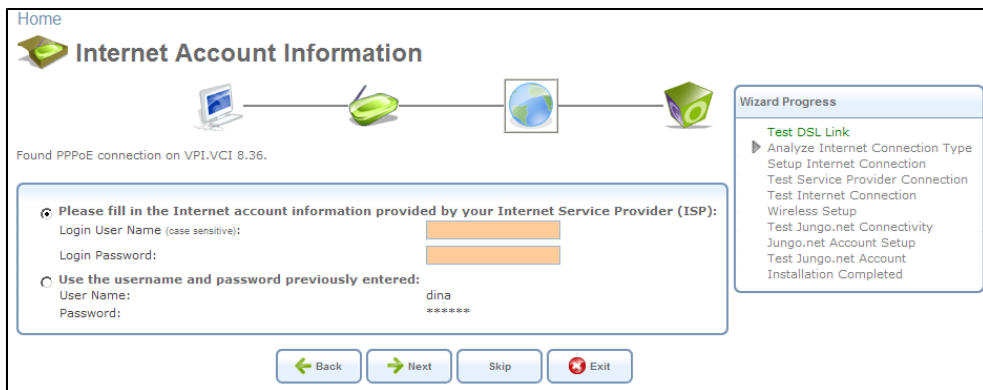


Figure 2.25. Internet Account Information

2.3.2.4. Step 4: Test Service Provider Connection

This step tests the connectivity to your ISP.

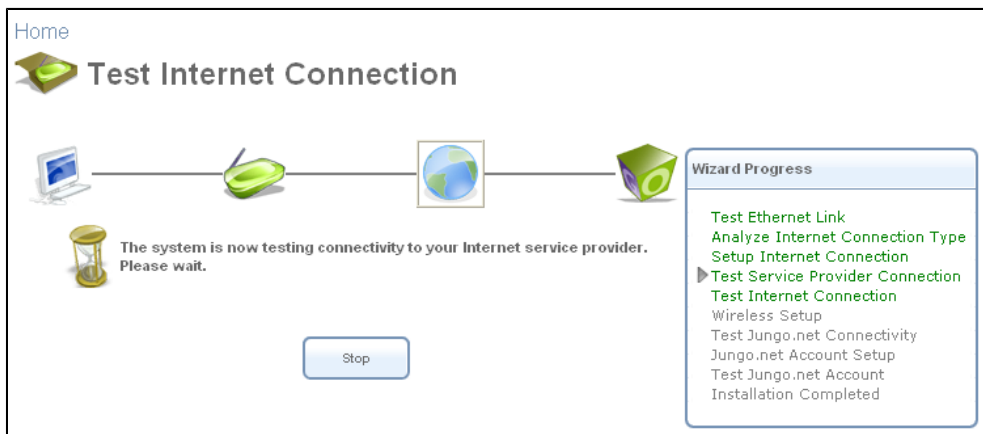


Figure 2.26. Test Internet Connection

2.3.2.5. Step 5: Test Internet Connection

This step tests the connectivity to the Internet.

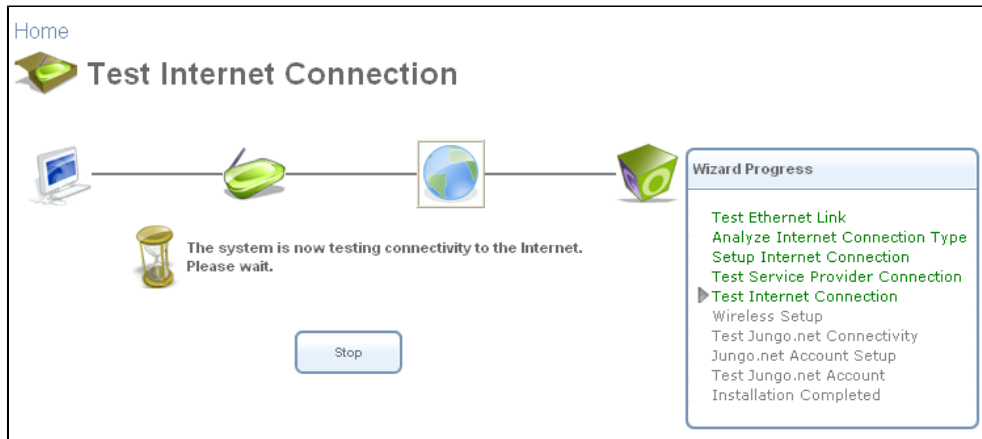


Figure 2.27. Test Internet Connection

2.3.2.6. Step 6: Wireless Setup

This step configures your wireless network. OpenRG personalizes the default "OpenRG" SSID with your username (e.g. "OpenRG_admin"). You may of course change this name according to your preference. Select the wireless security level and click 'Next'.

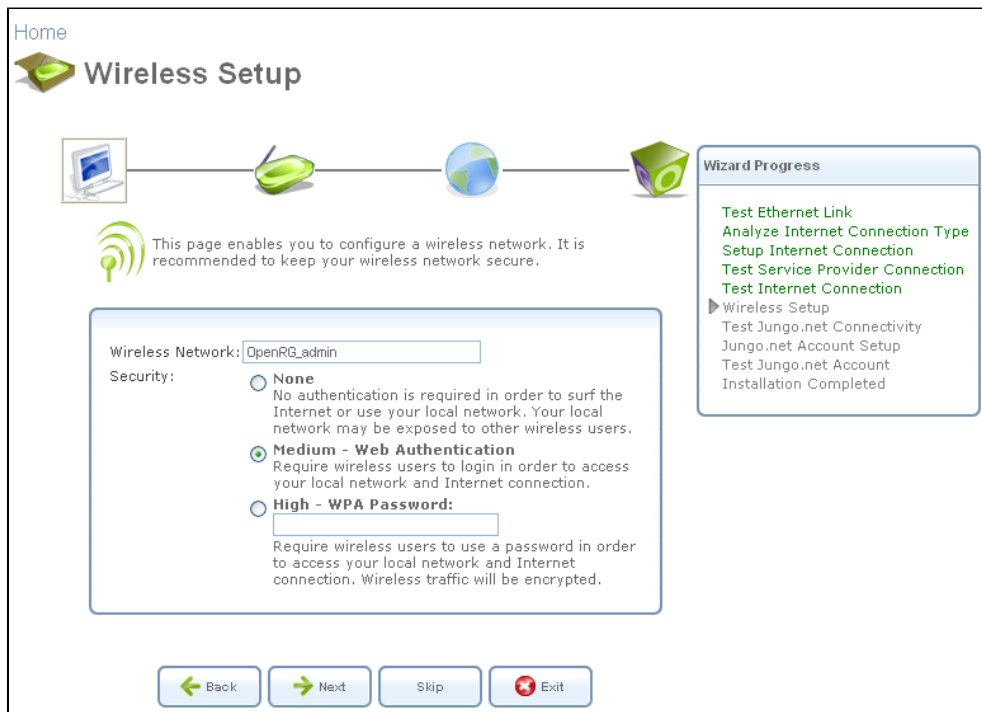


Figure 2.28. Wireless Setup

2.3.2.6.1. Setup via Wireless Connection

If you are running the installation wizard while connected to OpenRG via a wireless connection, the wizard does not change the default SSID (to prevent you from disconnecting). If you choose to change it manually, the following screen appears, requesting that you re-establish your wireless connection (from your computer) before proceeding with the wizard.

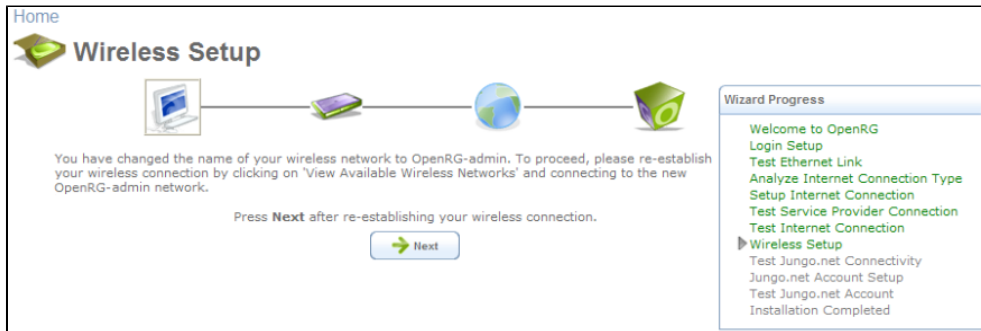


Figure 2.29. Wireless Setup

2.3.2.7. Step 7: Test Jungo.net Connectivity

This step tests connectivity to the Jungo.net server.

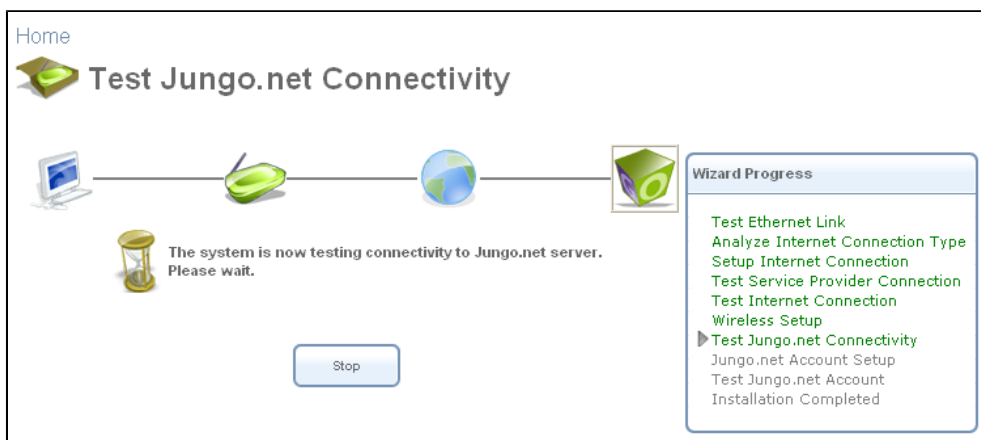


Figure 2.30. Test Jungo.net Connectivity

2.3.2.8. Step 8: Jungo.net Account Setup

This step tests the Jungo.net account supplied by your service provider, or enables you to create one.

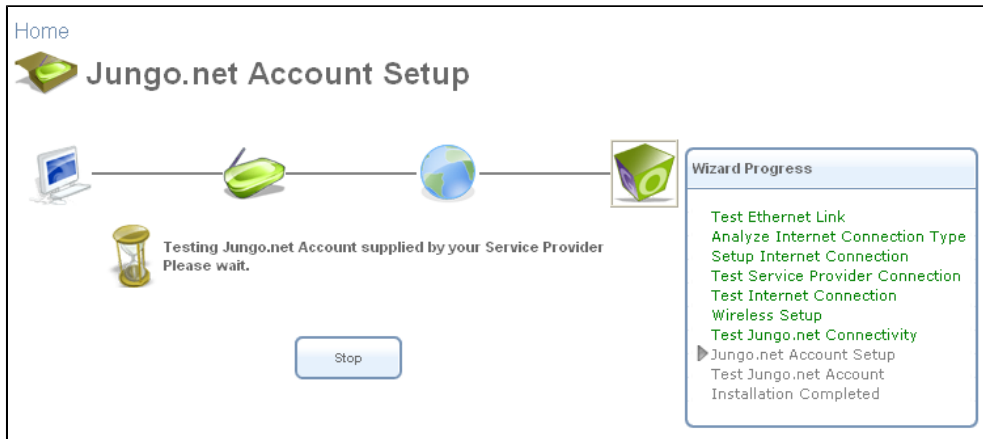


Figure 2.31. Jungo.net Account Setup

During this test, the following screen appears, enabling you to obtain a personal domain name.

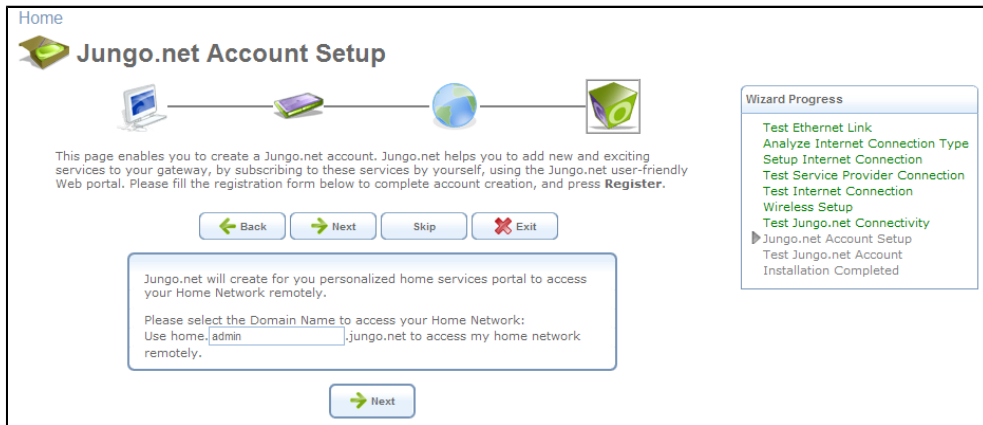


Figure 2.32. Domain Name Registration

Change the default **admin** part of the domain name to a personal username. This username will be also used as part of your Jungo.net account. If the username you entered had been already occupied by another person, the following screen appears.

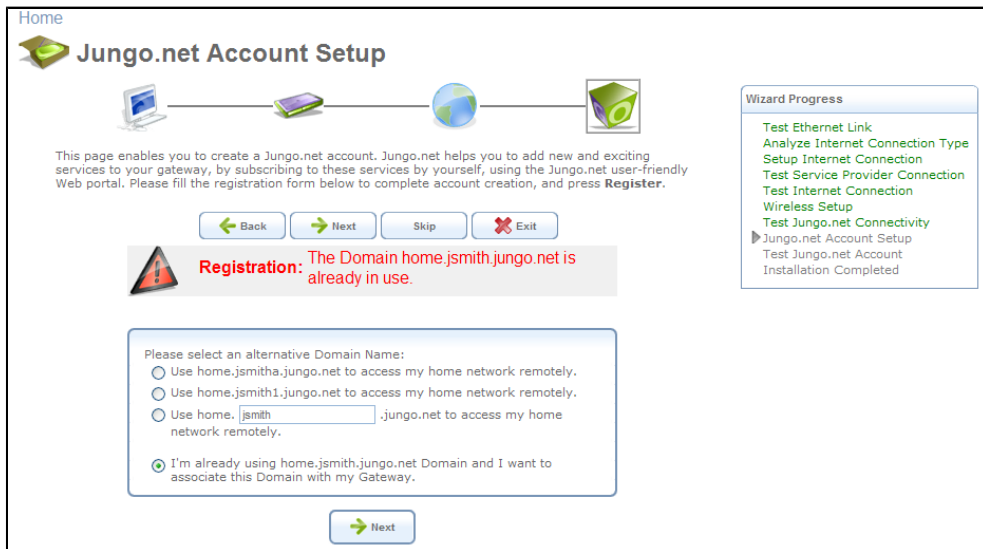


Figure 2.33. Domain Name in Use

This screen enables you to select another username by clicking its respective radio button. If you obtained the originally specified username from your service provider or registered it in the Jungo.net portal, select the last radio button and click 'Next' to proceed. The domain ownership confirmation screen appears.

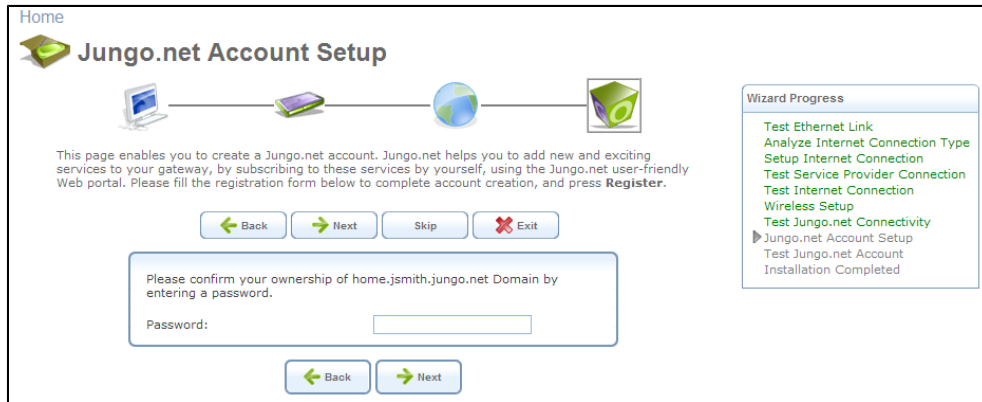


Figure 2.34. Domain Ownership Confirmation Request

Enter your Jungo.net password, and click 'Next'. If the password is correct, your gateway is configured with the specified domain name, and the domain settings screen appears.

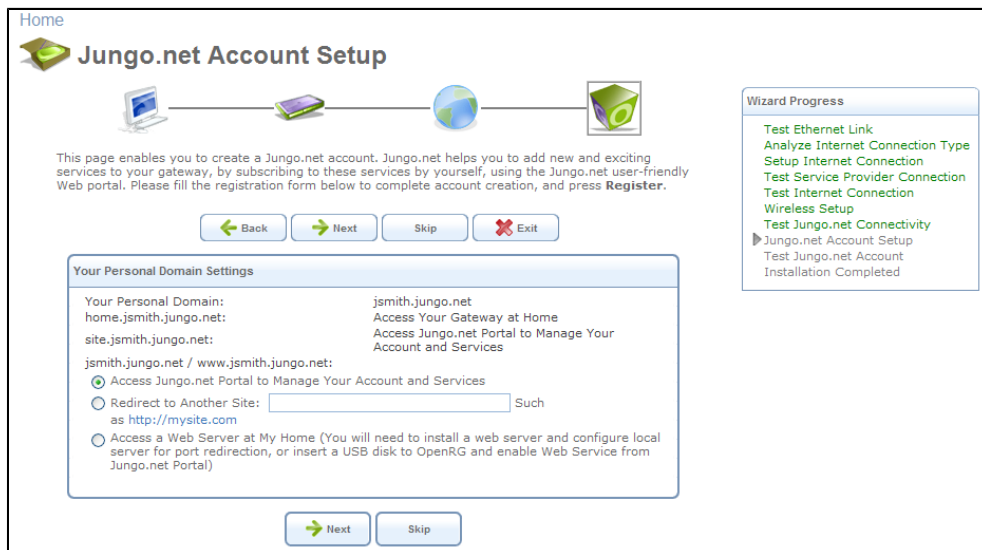


Figure 2.35. Personal Domain Settings

This screen displays the following three URLs that you will obtain for personal use after registration:

home.your_username.jungo.net Leads to your gateway's WBM.

site.your_username.jungo.net Leads to the Jungo.net portal.

your_username.jungo.net Your personal domain name that can be used for the following purposes:

- Access your personal account in the Jungo.net portal to add and manage the broadband services on your gateway. To enable this option, select the first radio button located in the 'Service Settings' section.

- Redirect to another Web site. To enable this option, select the second radio button and specify the Web site's URL in the designated text field.
- Access your Web site. To enable this option, select the third radio button and perform **either** of the following:
 - Set up a Web server, and configure your local server for port redirection. This option is recommended for advanced users.
 - Connect a USB disk with your Web site content to the gateway, and enable the Web service in the Jungo.net portal. For more information, refer to [Section 7.2.4.3](#).

Click 'Next' to enable the 'Personal Domain Name' service on the gateway. Alternatively, click 'Skip' if you would like to enable and configure this service later. In both cases, the wizard proceeds to detect the rest of the Jungo.net services supported by the gateway. When all supported services are detected, the gateway is automatically configured with the obtained service settings and the following screen appears.

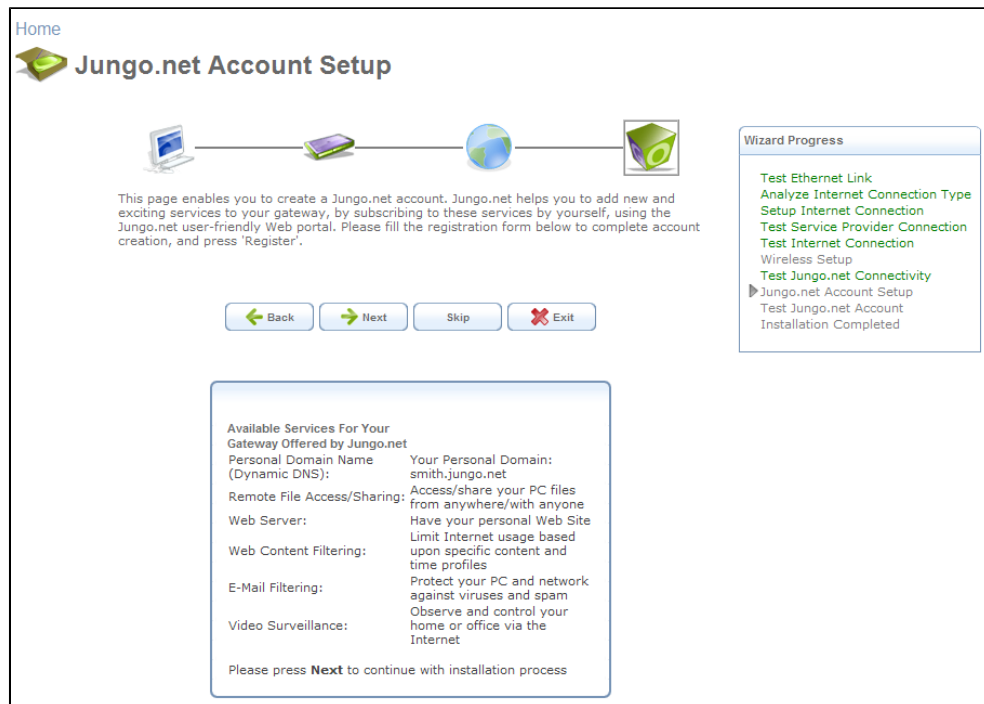


Figure 2.36. Available Jungo.net Services



Note: The detection of services may fail, if the Internet traffic is overloaded. In this case, return to the installation wizard later.

In case you do not have a Jungo.net account yet, the domain name registration step enables you to create a personal Jungo.net username. Complete the rest of your account details in the following screen that appears after clicking 'Next'.

Figure 2.37. Jungo.net Account Setup – Creating an Account

Enter the following information:

Password The password you will use for entering Jungo.net.

Confirm Password Retype the password for confirmation.

E-Mail Your email address.

Security Question A question asked to verify your identity.

Security Answer An answer you create for the security question.

To create the account, click 'Register'. The gateway is configured with your Jungo.net account settings.

Figure 2.38. Configuring OpenRG with the Jungo.net Account

If the gateway is configured successfully, the following screen appears.

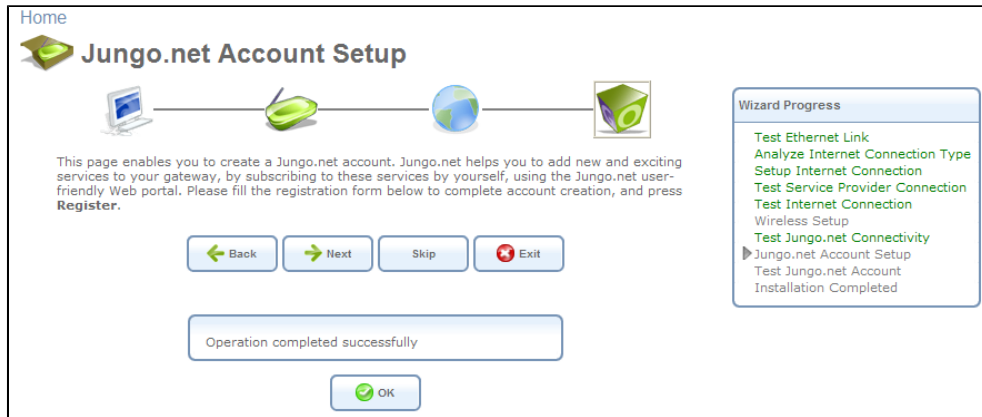


Figure 2.39. Successful Gateway Configuration

Click 'OK'. The wizard proceeds to detect Jungo.net services supported by the gateway, and displays the following screen.

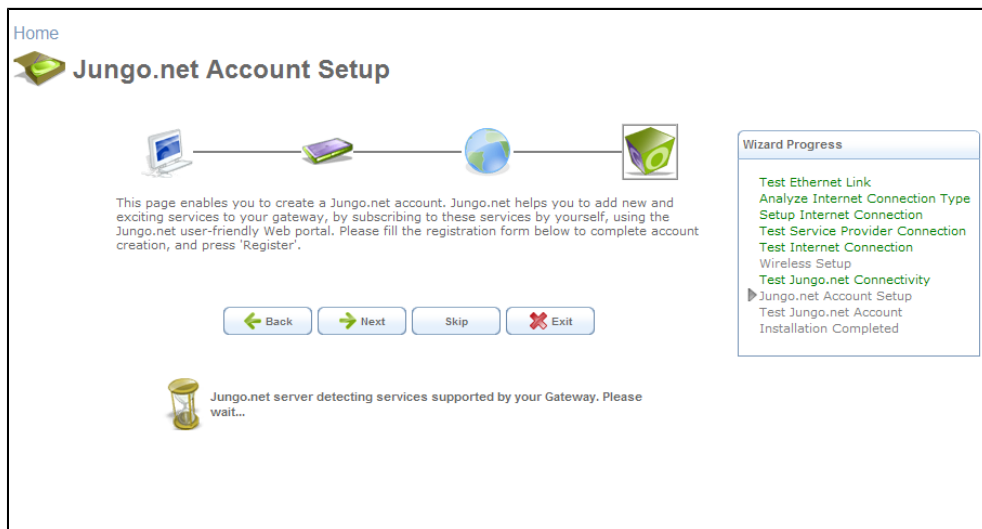


Figure 2.40. Detecting Jungo.net Services

While detecting the Jungo.net services and configuring the gateway, the wizard displays the domain name settings screen (see [Figure 2.35](#)), enabling you to configure this service as described earlier. If your gateway supports the NationZone service (refer to [Section 7.2.4.7](#)), the following screen appears, offering you to enable the service on your gateway.

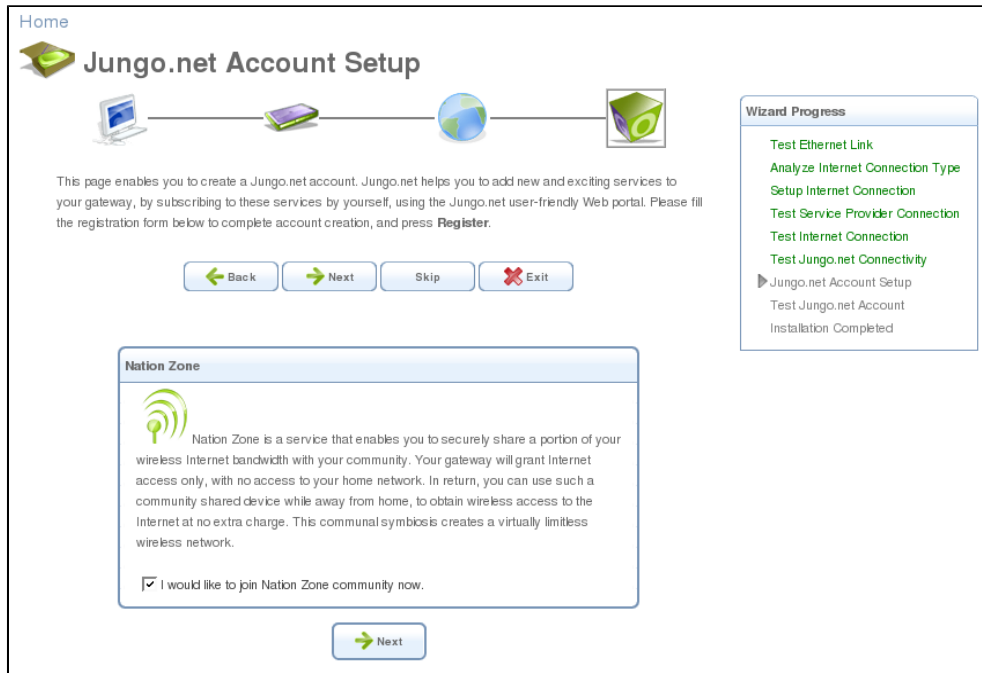


Figure 2.41. Enable NationZone

If you would like to enable this service, select the corresponding check box and click 'Next'. A list of available Jungo.net services appears (see [Figure 2.36](#)). Click 'Next' to proceed to the Jungo.net account validation step.

2.3.2.9. Step 9: Test Jungo.net Account

This step validates your account on the Jungo.net server.

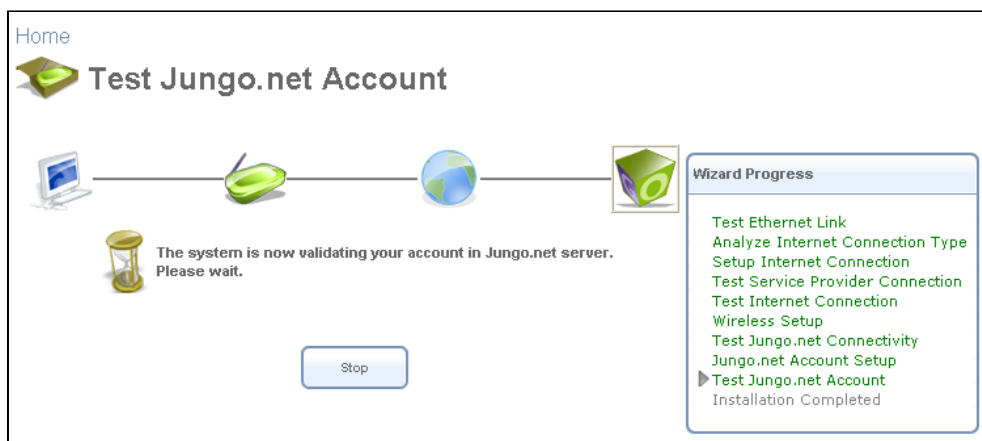


Figure 2.42. Test Jungo.net Account

2.3.2.10. Step 10: 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.



Figure 2.43. Installation Completed

2.3.3. Connection Problem Interception Page

There may be cases where Internet connection problems will prevent you from surfing. In such cases, OpenRG will intercept the browsing attempt and display the following screen, instead of the browser's standard 'Error 404: The page cannot be displayed' page.

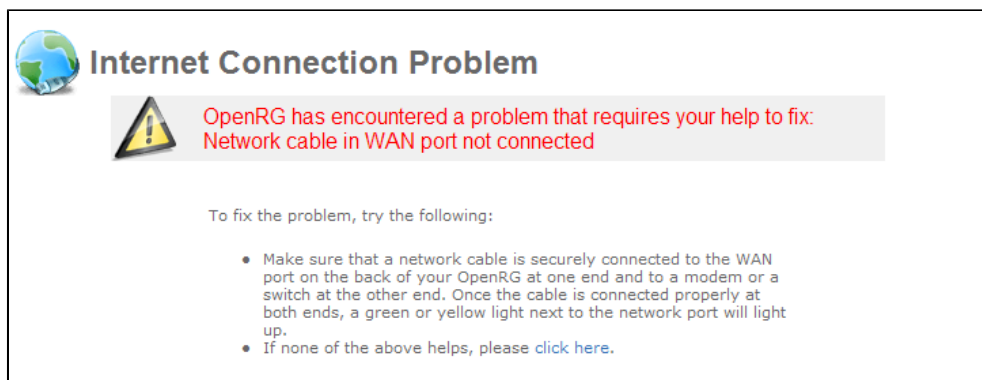


Figure 2.44. Internet Connection Problem

This page informs not only of the problem, but also of its possible reasons, and even provides troubleshooting options. In this example, the cause for the problem is that the WAN port network cable is not connected. If reconnecting the cable does not resolve the problem, this screen provides an additional link for further advice. Click the 'click here' link. The following screen appears.

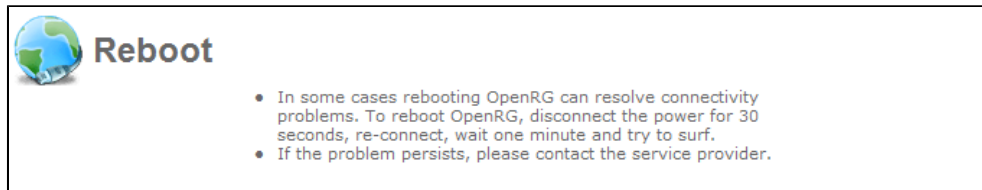


Figure 2.45. Reboot OpenRG

Rebooting OpenRG is another measure you can take in attempt to restore your Internet connection. As evident, this feature is more interactive and informative than the browser's standard 'Error 404' page.

2.3.4. Saved Login Details

You may have forgotten your login details, issued by your ISP. OpenRG saves the user name and password of the PPPoE or PPPoA connection to the ISP, even if it is restored to company defaults. When restoring the connection with the installation wizard, OpenRG will offer your old login details.

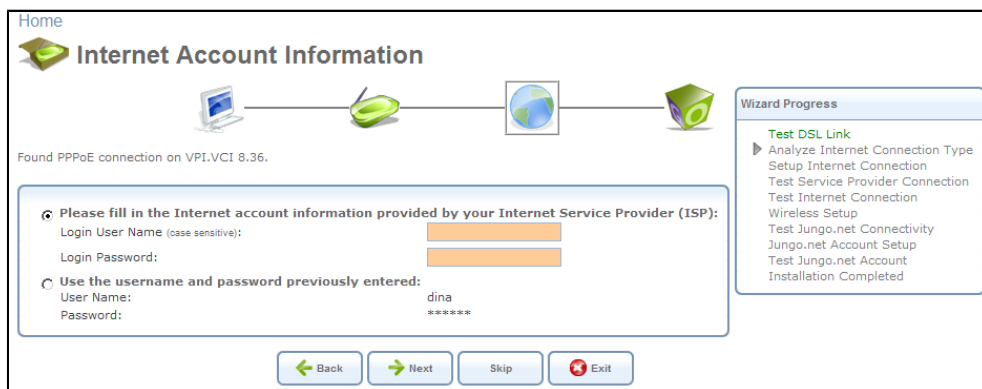


Figure 2.46. Internet Account Information

2.4. Connecting Peripheral Equipment

At this stage, you are ready to connect peripheral equipment to your gateway, such as a telephone, printer, mass storage device, or a media client, according to your needs.

2.4.1. Connecting a Telephone

Connect a standard Plain Old Telephone Service (POTS) telephone to one of the available FXS telephone ports on your gateway.

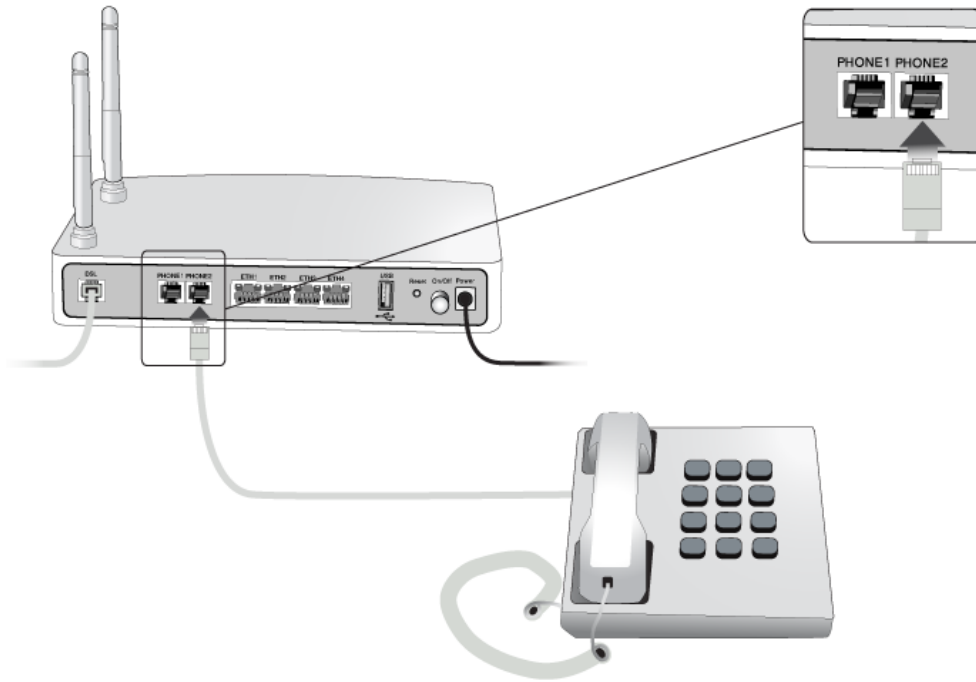


Figure 2.47. Telephone Connection

OpenRG's Analog Telephone Adapter (ATA) telephony system can connect to a remote Session Initiation Protocol (SIP) server in order to conduct world-wide phone calls. The following sections describe the configurations of both a SIP server and OpenRG, required for conducting such calls. Note that these instructions are valid when OpenRG is at its default settings.

In addition to SIP, OpenRG also supports the H.323 and MGCP signaling protocols. For more information, refer to [Section 7.6.8.3](#).

If you are already using a different ATA device with your POTS telephone, or if you are using an IP telephone, you may connect them directly to a LAN port on your gateway. In this case, you will not need to configure OpenRG, which will act merely as a router to the SIP server.

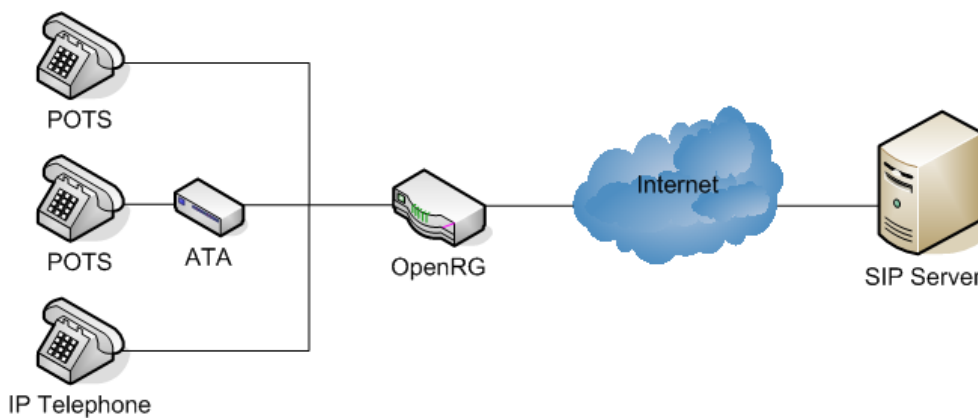


Figure 2.48. Telephony Infrastructure

2.4.1.1. Opening a SIP Account

Before you can connect to a SIP server, it is necessary that you obtain a SIP account. This section describes how to open a free world-wide dialing SIP account. You can also obtain a paid SIP account.



Note: Free accounts limit placing calls to 1-800 numbers and other free account holders only, while paid services offer access to any number.

To open a "Free World Dialup" ("FWD") SIP account:

1. Browse to <http://www.pulver.com/fwd>
2. Click the 'my.FWD' tab.
3. Click the 'Sign Up for Fwd' link, and open an account.

You should get instructions by e-mail containing your ID and password, and a SIP IP address.

2.4.1.2. Configuring a Telephone Line

After creating a SIP account and obtaining the necessary details, configure OpenRG as follows:

1. Click the 'Voice' tab under the 'Services' screen. The 'Line Settings' screen appears.

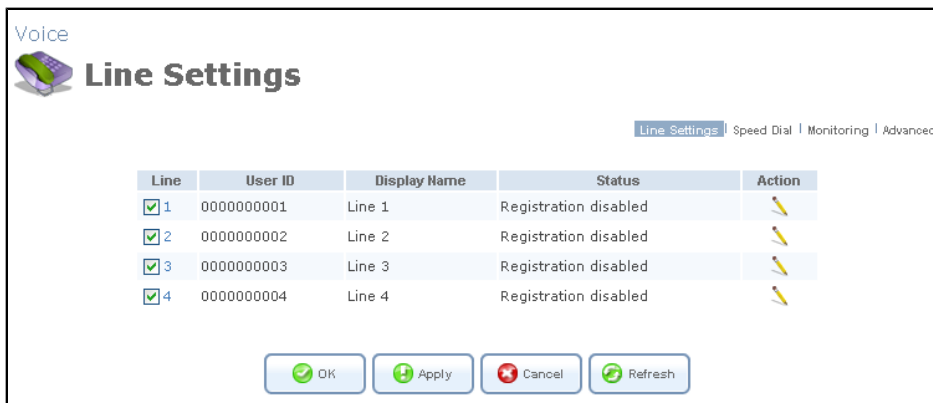


Figure 2.49. Line Settings

2. Click the action icon of an enabled line (whose check box is checked) to configure its parameters. The line's 'Line Settings' screen appears.

Voice
Line Settings

Line Settings |
 [Speed Dial](#) |
 [Monitoring](#) |
 [Advanced](#)

Line Number:

User ID:

Block Caller ID

Display Name:

Services

Enable Call Waiting

Enable 3-Way Calling

Enable Message Waiting Indication

Enable Do Not Disturb

Enable Call Forwarding Always

Enable Call Forwarding on Busy

Enable Call Forwarding on No Answer

SIP Account

Authentication User Name:

Authentication Password:

SIP Proxy

Use SIP Proxy

Outbound Proxy

Use Outbound Proxy

Numbering Plan

Minimum Number of Digits:

Maximum Number of Digits:

Inter-Digit Timer: milliseconds

Prefixes

Prefix Range	Maximum Number of Digits	Facility Action	Action
*72	40	Activate Call Forwarding Always	
*73	3	Deactivate Call Forwarding Always	
*78	40	Activate Do Not Disturb	
*79	3	Deactivate Do Not Disturb	
*90	40	Activate Call Forwarding on Busy	
*91	3	Deactivate Call Forwarding on Busy	
*92	40	Activate Call Forwarding on No Answer	
*93	3	Deactivate Call Forwarding on No Answer	

[New Entry](#)

Failover

Failover if SIP "OPTIONS" Keep-Alive Check Failed

Failover if WAN Connectivity Check Failed

Failover if Registration Failed

Dial Tone to Play on Registration Failure:

Advanced SIP Settings

DTMF Transmission Method:

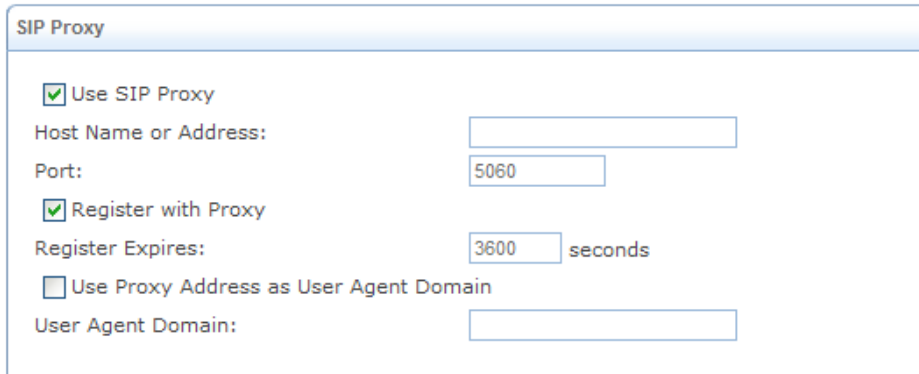
Compatibility Mode:

Disconnect Supervision

Forward Disconnect Enabled

Figure 2.50. SIP Line Settings

3. Enter your newly obtained ID in the 'User ID' field, enter a display name, and select whether to block the caller ID from the remote party for this line.
4. Enter your newly obtained username and password in their respective fields of the 'SIP Account' section.
5. Check the 'Use SIP Proxy' check box. The following fields become visible.



The screenshot shows a configuration window titled "SIP Proxy". It contains the following elements:

- Use SIP Proxy
- Host Name or Address: [Empty text box]
- Port: [Text box containing 5060]
- Register with Proxy
- Register Expires: [Text box containing 3600] seconds
- Use Proxy Address as User Agent Domain
- User Agent Domain: [Empty text box]

Figure 2.51. SIP Proxy

- a. Enter the IP address or host name you received when registering your SIP account in the 'Host Name or Address' field. Your free account's host name should be fwd.pulver.com (this may vary; you should check your registration e-mail).
 - b. Verify that the SIP Proxy's 'Port' field is set to 5060. This is the port on which the proxy is listening.
 - c. Verify that the 'Register with Proxy' check box is checked.
 - d. Verify that the 'Register Expires' field is set to 3600. This is the number of seconds between registration renewals.
 - e. Verify that the 'Use Proxy Address as User Agent Domain' check box is selected. The set proxy or its IP address will be used as the domain name specified in outgoing SIP messages. When this option is unchecked, the 'User Agent Domain' field appears. Use this field for setting another proxy address as a user agent domain.
6. Check the 'Use Outbound Proxy' check box. The free world-wide dialing service is an example of a service provider that requires the use of an outbound proxy. This is an additional proxy, through which all outgoing calls are directed. In some cases, the outbound proxy is placed alongside the firewall and is the only way to let SIP traffic pass from the internal network to the Internet. Once checked, the following fields become visible.



Outbound Proxy

Use Outbound Proxy

Host Name or Address:

Port:

Figure 2.52. Outbound Proxy

- a. Enter the outbound proxy's IP address or host name that you received when registering your SIP account in the 'Host Name or Address' field. Your free account's outbound proxy's name should be fwdnat.pulver.com (this may vary; you should check your registration e-mail).
 - b. Set the outbound proxy's 'Port' field to 5082 (this may also vary).
7. Click 'OK' to save the settings.

Back in the 'Line Settings' screen (see [Figure 2.49](#)), verify that the status of the line has changed to "Registered". After a few seconds you will get a ring tone on the telephone connected to this line on your gateway. You can now dial to any number that your SIP account allows.

For more on the voice functionality of your gateway, refer to [Section 7.6](#).

2.4.2. Connecting a Printer

To set up a network printer that will be shared by all LAN computers, connect a printer to the USB port on your gateway.

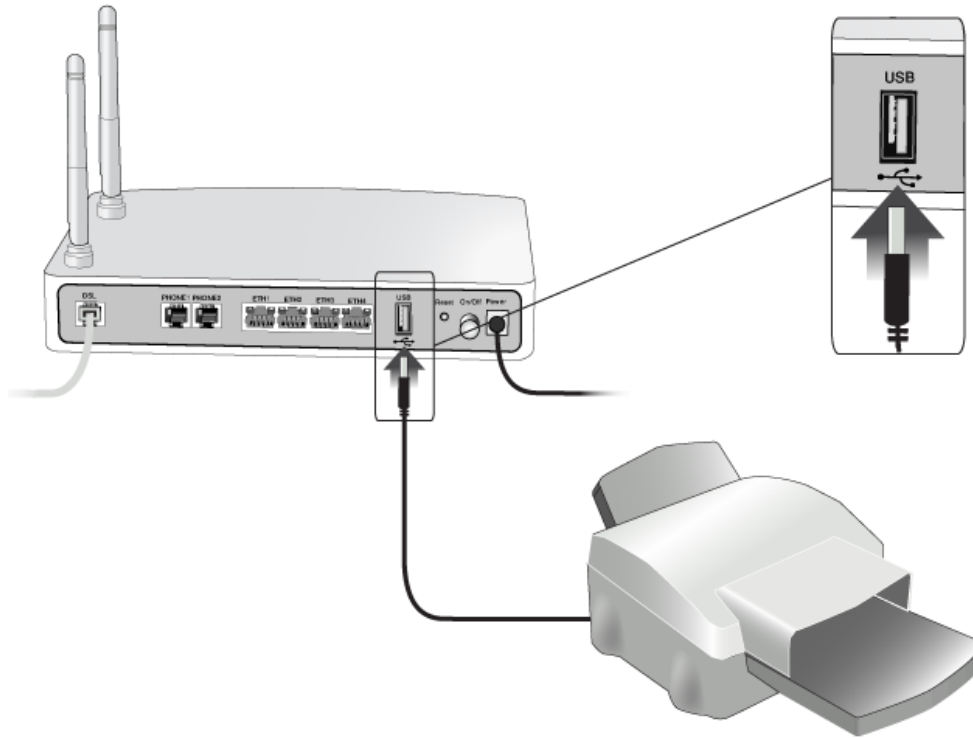


Figure 2.53. Printer Connection

The connected printer is managed by OpenRG's print server (for more information, refer to [Section 6.5](#)).

2.4.2.1. Setting Up a Samba Printer on Windows

This section describes how to establish a network printer connection on a Windows host using the Microsoft File and Printer Sharing (Samba) protocol.

1. Once logged into OpenRG, browse to `\\openrg` (use a Windows Explorer window if you are using a browser other than Internet Explorer). Should a Windows login dialog box appear, enter your WBM username and password. The following window appears.

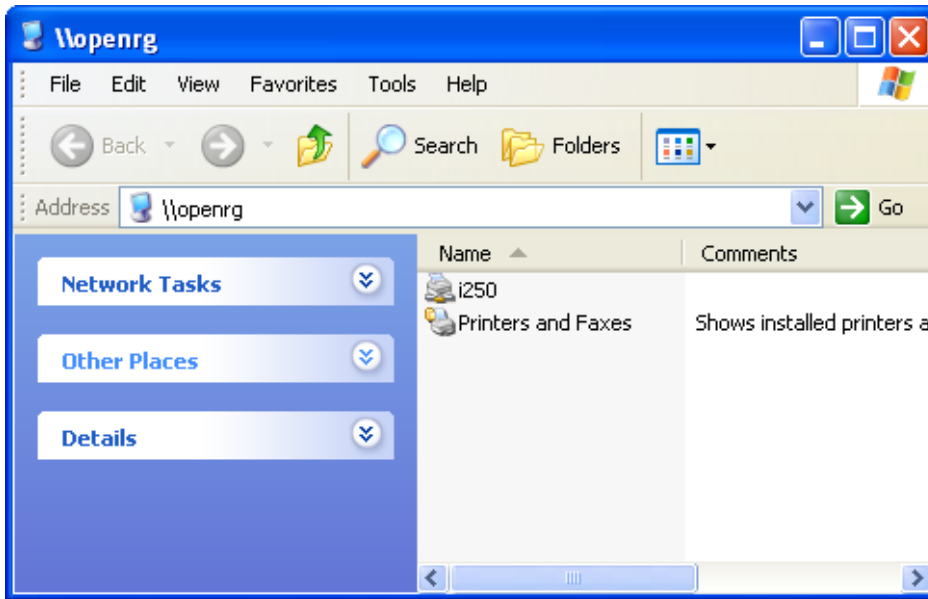


Figure 2.54. OpenRG Shares

2. Click the icon of the printer you would like to designate as a LAN printer. The following warning appears.

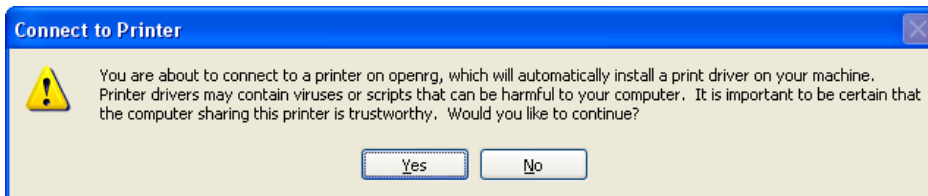


Figure 2.55. Connect to Printer Warning

3. Click 'Yes'. You will be prompted to select a printer driver from a list. If unavailable, you can either browse to a location on your computer where you have stored the driver, or click 'Have Disk' and insert the CD containing the driver (supplied with your printer). After a short upload and installation of the driver, the printer's print queue window appears, determining that the printer is ready for use.

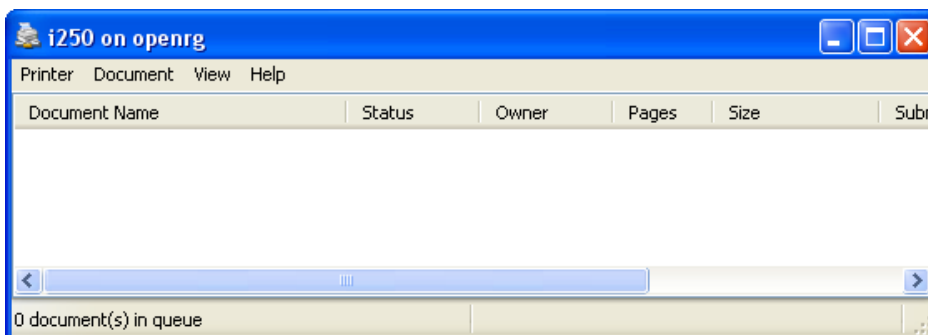


Figure 2.56. Printer Queue

The new printer is added to your "Printers and Faxes" list as a network printer (to view this list press "Start", then "Settings" and then "Printers and Faxes"). As any printer, you can choose to make it your default printer, or specify its use when printing.

4. Print a test page by right-clicking the printer icon in the disk and printer shares window (Figure 2.54) and selecting 'Properties'. The 'Print Test Page' button is located at the bottom of the 'General' tab.



Note: The above configuration must be applied to each LAN PC individually in order to use the network printer.

To learn how to establish a network printer connection via other print protocols supported by OpenRG, refer to [Section 6.5.2](#).

2.4.3. Connecting a Mass Storage Device

To set up a file server that will be shared by all LAN computers, connect a mass storage device (e.g. disk-on-key, hard drive) to the USB port on your gateway.

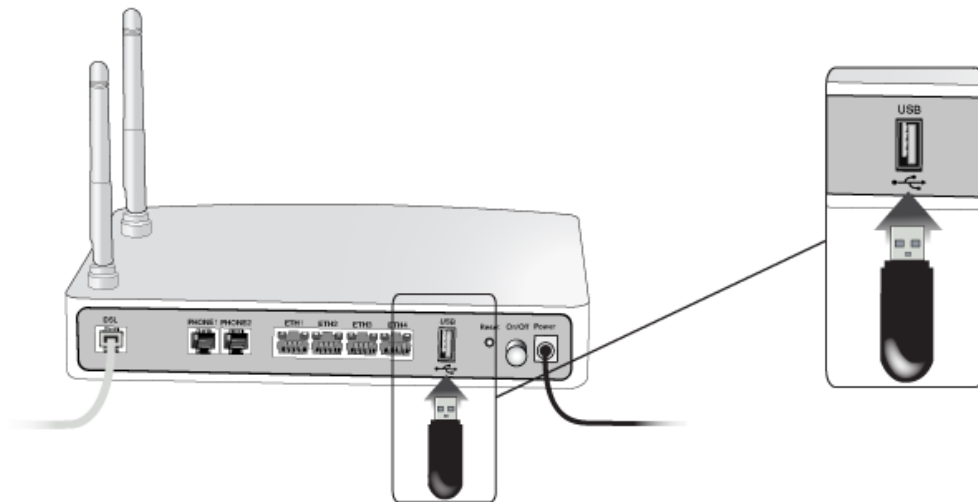


Figure 2.57. Disk-on-key Connection

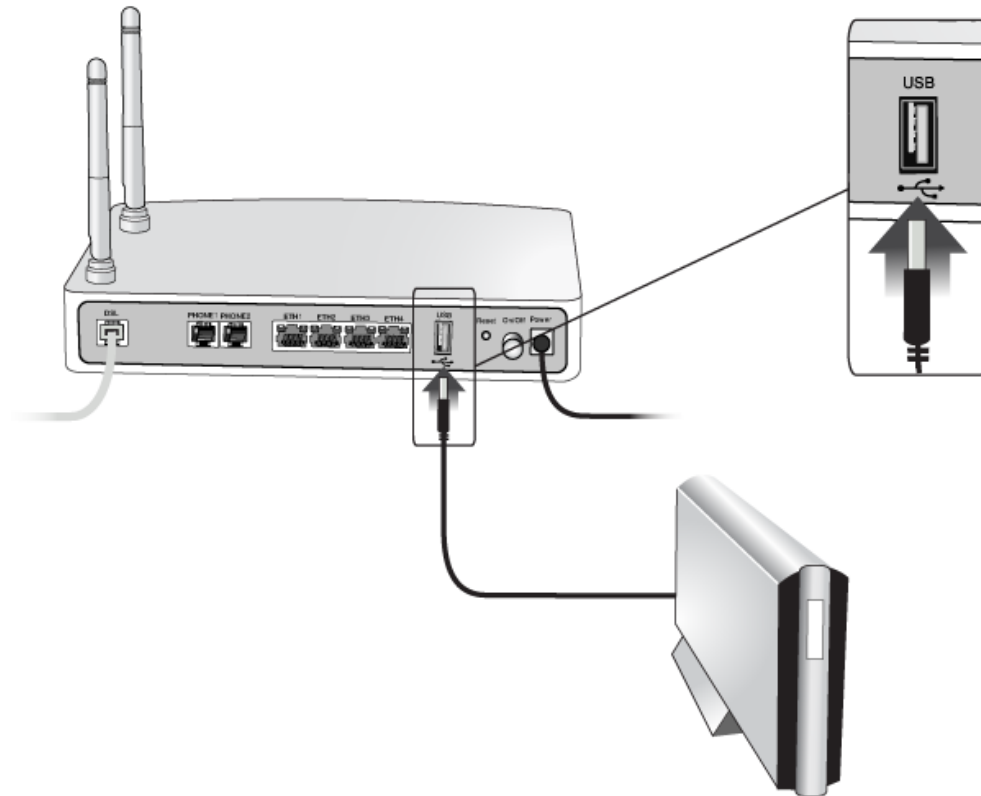


Figure 2.58. Hard Drive Connection

2.4.3.1. Adding and Formatting a Partition

In order to be used, a mass storage device must first be partitioned and formatted. However, partitioning can only be performed on unallocated disk space. If your device is already partitioned, you may not be able to add a partition, unless unallocated space is available.

To add a Windows formatted partition, perform the following:

1. Click the 'Shared Storage' menu item under the 'Local Network' tab. The 'Disk Management' screen appears.

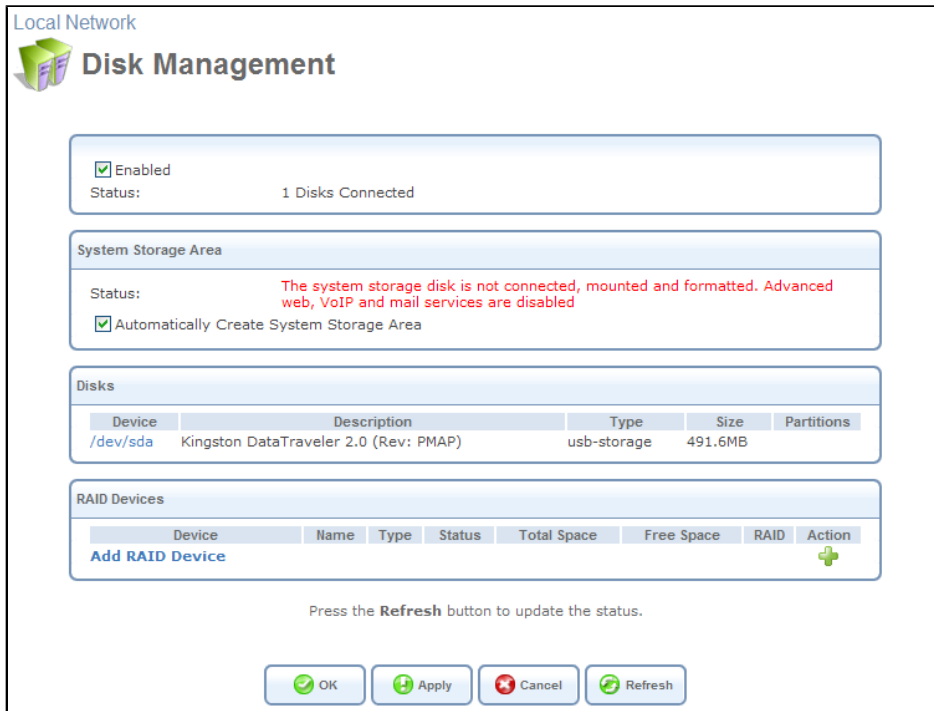


Figure 2.59. Disk Management

2. In the 'Disks' section, displaying your connected storage devices, click the disk's link. The 'Disk Information' screen appears.

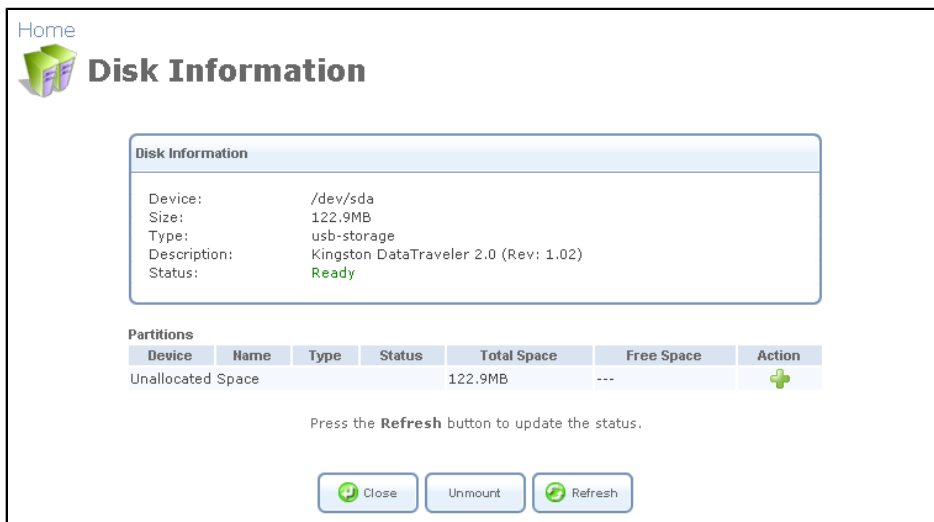


Figure 2.60. Disk Information

3. In the 'Partitions' section, click the action icon . The 'Partition Type' screen appears.

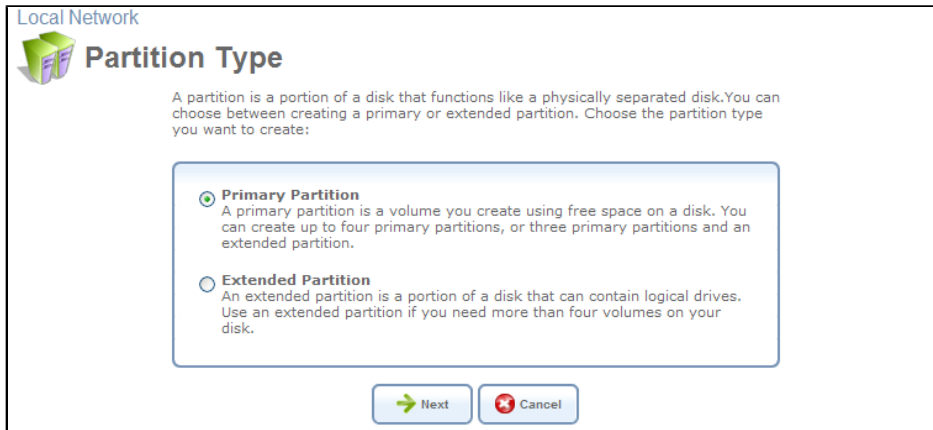


Figure 2.61. Partition Type

4. Select 'Primary Partition', and click 'Next'. The 'Partition Size' screen appears.

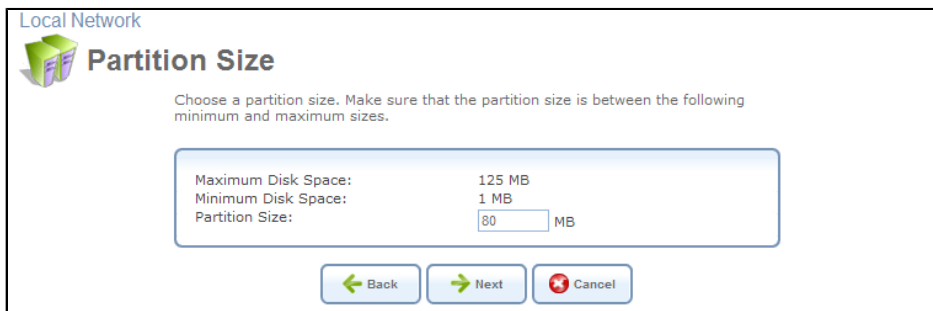


Figure 2.62. Partition Size

5. Enter a volume for the new partition (in mega bytes) and click 'Next'. The 'Partition Format' screen appears.

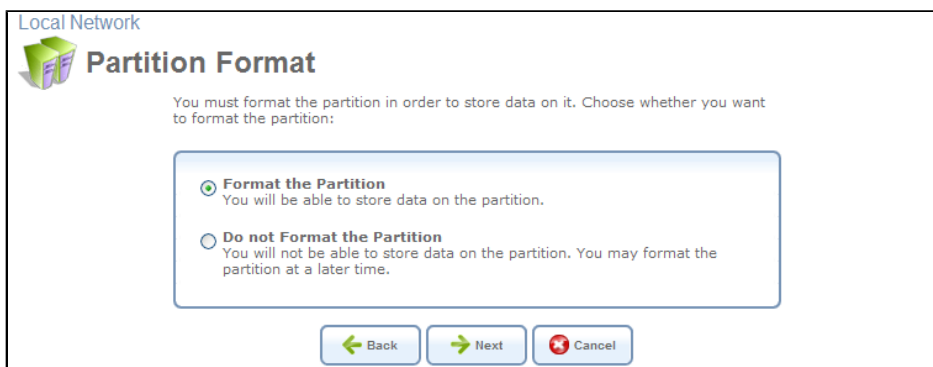


Figure 2.63. Partition Format

6. Select 'Format the Partition', and click 'Next'. The 'Partition File System' screen appears.

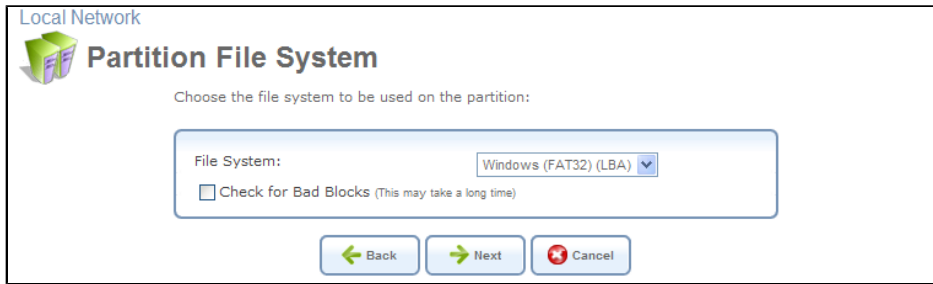


Figure 2.64. Partition File System

7. Select 'Windows (FAT32) (LBA)' as the file system for the partition and click 'Next'. The 'Partition Summary' screen appears.

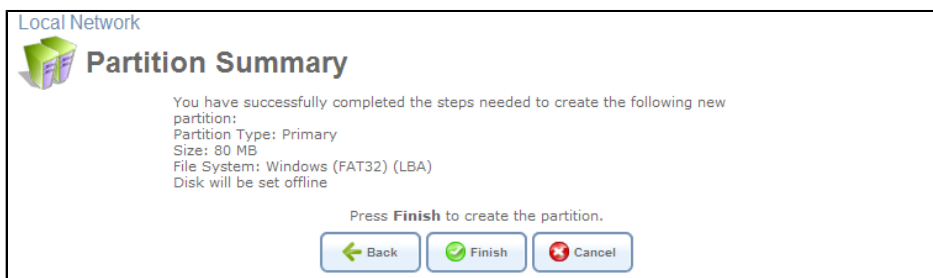


Figure 2.65. Partition Summary

8. Click 'Finish' to create the new partition. The 'Disk Information' screen reappears, refreshing as the partition formatting progresses, until the status changes to 'Ready'.

Device	Name	Type	Status	Total Space	Free Space	RAID	Action
/dev/sda1	Partition operation in progress...	Windows FAT32 (LBA)	Formatting...	79.93MB	---		
	Unallocated Space				45.04MB	---	

Figure 2.66. Partition Formatting in Progress

The new partition path names are designated as "A", "B", etc.




Device	Name	Type	Status	Total Space	Free Space	RAID	Action
/dev/sda1	B	Windows FAT32 (LBA)	Ready	78.69MB	78.57MB		 
	Unallocated Space				45.04MB	---	

Figure 2.67. Formatting Complete – Partition Ready

To learn about additional operations you can perform on your storage device, refer to [Section 6.4](#).

2.4.3.2. Using a Disk Share

By default, all partitions are automatically shared and displayed. Any LAN computer can access the disk share to upload or download files. To do so, perform the following:

1. Browse to \\openrg (use a Windows Explorer window if you are using a browser other than Internet Explorer). Should a Windows login dialog box appear, enter your WBM username and password.
2. Open the 'Share' directory. The following window appears, displaying the folders available on the disk.

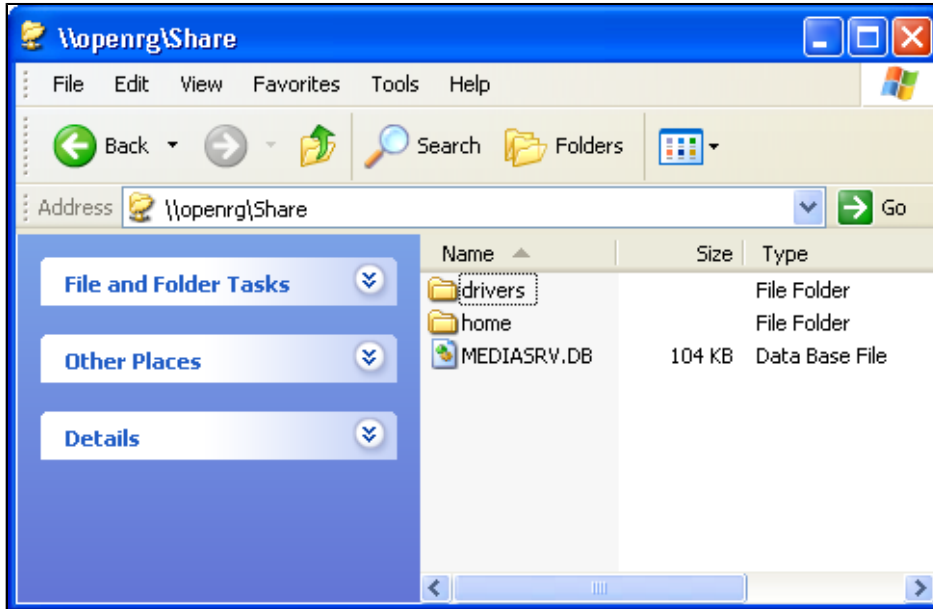


Figure 2.68. Disk Share

3. Copy a file to this location. You can create a new folder for it, or use an existing one.

The disk share contains default system content. In addition, services such as File Server, FTP Server, Mail Server, and Web Server will utilize the disk share when activated (for more information, refer to [Section 7.11](#)). Nevertheless, you can create folders and organize your own content in the disk share according to your needs.

2.4.4. Connecting a Media Client

OpenRG enables you to share and stream media files (music, pictures, and video) from a storage device connected to OpenRG, to a media client. For example, you can view your media files on a television set. In this case, a media client device is required to connect the TV set to your home network. A media client device is a network-aware Consumer Electronic (CE) device with a Universal Plug and Play (UPnP) media renderer. This device will typically have an RCA or a coaxial connection to the TV set, and a LAN socket and/or wireless LAN to connect to the gateway.

1. Connect a mass storage device to the gateway, as described in the previous section. This device should contain your media content (at least one folder with a media file for testing at this point).
2. Connect your TV set to the media client device according to the instructions provided with the device. Make sure you select the correct AV input on the TV set.

3. Connect the media client device to an available Ethernet port on your gateway.

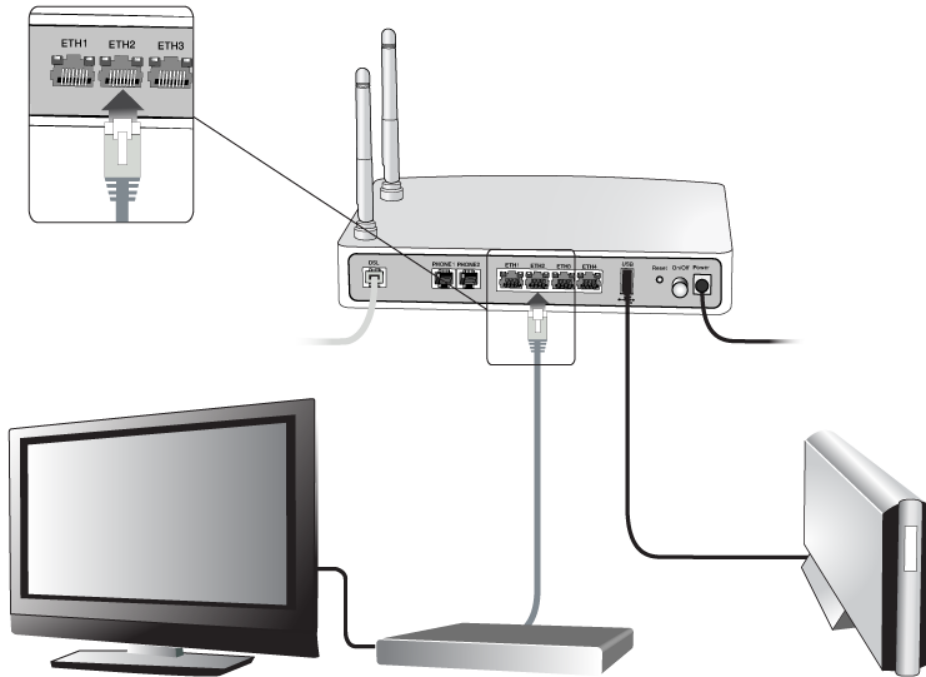


Figure 2.69. Media Client Device and Television Connection

If your media client device has a wireless capability, it can connect to OpenRG without cables. However, since media usage requires streaming high volumes of traffic, wireless use is recommended only if both OpenRG and the media client device support the 802.11n protocol.

2.4.4.1. Viewing and Streaming Media Files

Reception of OpenRG's media server broadcast by the media client device is automatic, requiring no further configuration.

1. Turn on the media client device. The following images represent D-Link's **MediaLounge™** media client device software, displayed on the TV set (connected to the device).



Figure 2.70. MediaLounge Main Screen

2. Use the device's remote control to select 'My Media'. The path letter of the OpenRG share containing your disk content appears.




Figure 2.71. Your Share on OpenRG

3. Select the share. The share's content is displayed.



Figure 2.72. Media Folders on a Share

 Note: MediaLounge displays the same directory hierarchies as on the storage device.

4. Select a folder, for example "photos". The folder's content is displayed.

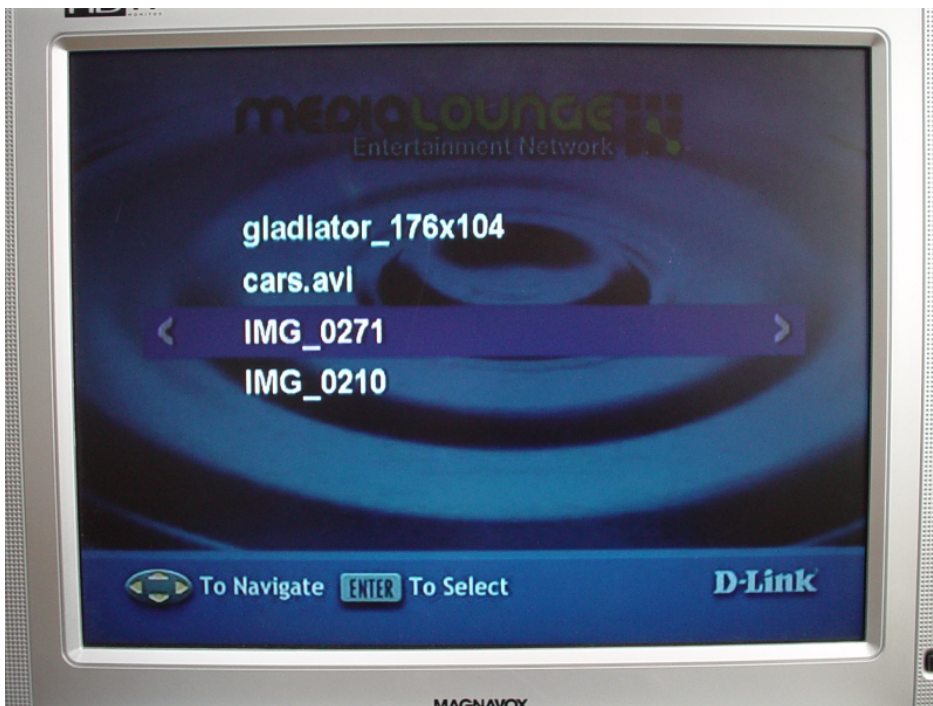


Figure 2.73. Media Files in the Shared Folder

5. Select a photo to display.



Figure 2.74. Displaying a Photograph

In the same method, you can stream music and video files from your disk to your television. Additionally, you can access your shared media files from a LAN PC with an installed media rendering software (for more information, refer to [Section 7.5.2](#)).

Part II. Managing Your Gateway

Table of Contents

3. Using the Management Console	51
3.1. First Time Login	52
3.2. Accessing the WBM	53
3.3. Navigational Aids	54
3.4. Managing Tables	55
4. Home	56
4.1. Overview	56
4.2. Map View	58
4.3. Installation Wizard	60
4.4. Quick Setup	60
4.4.1. Configuring Your Internet Connection	61
4.4.2. Wireless	70
4.4.3. Jungo.net	71
4.4.4. Quick Setup Completed	72
5. Internet Connection	73
5.1. Overview	73
5.2. Settings	74
5.3. Diagnostics	75
6. Local Network	77
6.1. Overview	77
6.2. Device View	79
6.3. Wireless	80
6.3.1. Overview	80
6.3.2. Settings	81
6.3.3. Advanced	81
6.4. Shared Storage	82
6.4.1. Managing Disk Partitions	83
6.4.2. Defining a Location for System Files	89
6.4.3. Optimizing Data Storage and Backup with RAID	90
6.5. Shared Printers	97
6.5.1. Configuring the Print Server	98
6.5.2. Selecting a Print Protocol	99
6.5.3. Sharing a Samba Printer Driver	121
6.5.4. Controlling Access to Print Jobs	123
6.6. IP-PBX	126
7. Services	128
7.1. Overview	128
7.2. Jungo.net	128
7.2.1. Creating a Jungo.net Account	129
7.2.2. Accessing Jungo.net	134
7.2.3. Reconnecting Your Gateway to Jungo.net	136
7.2.4. Registering and Using the Jungo.net Services	136
7.2.5. Restoring OpenRG's Configuration from Jungo.net	177
7.3. Firewall	180
7.3.1. Configuring Basic Security Settings	181
7.3.2. Controlling Access to Internet Services	183

7.3.3. Using Port Forwarding	186
7.3.4. Designating a DMZ Host	191
7.3.5. Using Port Triggering	192
7.3.6. Restricting Web Access	195
7.3.7. Using OpenRG's Network Address and Port Translation	198
7.3.8. Viewing Open Connections	207
7.3.9. Configuring the Advanced Filtering Mechanism	208
7.3.10. Viewing the Firewall Log	211
7.3.11. Applying Corporate-Grade Security	217
7.4. Quality of Service	226
7.4.1. Overview	227
7.4.2. Internet Connection Utilization	229
7.4.3. Traffic Priority	231
7.4.4. Traffic Shaping	236
7.4.5. Differentiated Services Code Point Settings	241
7.4.6. 802.1p Settings	243
7.4.7. Class Statistics	243
7.4.8. Voice QoS Scenario	244
7.4.9. IPTV QoS Scenario	254
7.5. Media Sharing	265
7.5.1. Configuring the Media Sharing Service	265
7.5.2. Accessing the Shared Media from a LAN Computer	267
7.6. Voice	271
7.6.1. Configuring Your Telephone Line Services	272
7.6.2. Operating Your Telephone	273
7.6.3. Configuring and Using Speed Dial	274
7.6.4. Sending a Fax	276
7.6.5. Customizing Your Phone Service with a Numbering Plan	277
7.6.6. Using Distinctive Ring	279
7.6.7. Ensuring Constant Connectivity with Failover	280
7.6.8. Advanced Telephony Options	280
7.7. IP-PBX	290
7.7.1. Configuring Your Analog Extensions	291
7.7.2. Operating Your Telephone	293
7.7.3. Connecting VoIP Telephones	294
7.7.4. Opening Telephony Service Accounts	298
7.7.5. Defining VoIP Lines	298
7.7.6. Creating Auto Attendants	303
7.7.7. Handling Incoming Calls	306
7.7.8. Handling Outgoing Calls	309
7.7.9. Using the Voice Mail	312
7.7.10. Adding On-Hold Music Files	314
7.7.11. Automating Call Distribution with Hunt Groups	314
7.7.12. Advanced Telephony Options	317
7.8. Parental Control	327
7.8.1. Overview	328
7.8.2. Filtering Policy	329
7.8.3. Advanced Options	332

7.8.4. Statistics	333
7.9. Email Filtering	334
7.9.1. Overview	334
7.9.2. Advanced Options	337
7.10. Virtual Private Network	338
7.10.1. Internet Protocol Security	338
7.10.2. Secure Socket Layer VPN	375
7.10.3. Point-to-Point Tunneling Protocol Server	392
7.10.4. Layer 2 Tunneling Protocol Server	394
7.11. Storage	398
7.11.1. FTP Server	398
7.11.2. File Server	401
7.11.3. WINS Server	417
7.11.4. Web Server	418
7.11.5. Mail Server	422
7.11.6. Backup and Restore	427
7.12. Personal Domain Name (Dynamic DNS)	430
7.12.1. Opening a Dynamic DNS Account	430
7.12.2. Using Dynamic DNS	430
7.13. Advanced	432
7.13.1. DNS Server	432
7.13.2. IP Address Distribution	434
7.13.3. Bluetooth Settings	439
7.13.4. RADIUS Server	441
8. System	454
8.1. Overview	454
8.2. Settings	454
8.2.1. Overview	454
8.2.2. Date and Time	459
8.3. Users	462
8.3.1. User Settings	463
8.3.2. Group Settings	465
8.4. Network Connections	465
8.4.1. The Connection Wizard	468
8.4.2. Network Types	478
8.4.3. LAN Bridge	479
8.4.4. LAN Ethernet	488
8.4.5. LAN Hardware Ethernet Switch	490
8.4.6. LAN USB	493
8.4.7. LAN Wireless	495
8.4.8. WAN Ethernet	526
8.4.9. Point-to-Point Protocol over Ethernet (PPPoE)	533
8.4.10. Ethernet Connection	541
8.4.11. Layer 2 Tunneling Protocol (L2TP)	542
8.4.12. Layer 2 Tunneling Protocol Server (L2TP Server)	552
8.4.13. Point-to-Point Tunneling Protocol (PPTP)	555
8.4.14. Point-to-Point Tunneling Protocol Server (PPTP Server)	565
8.4.15. Internet Protocol Security (IPSec)	568

8.4.16. Internet Protocol Security Server (IPSec Server)	570
8.4.17. Dynamic Host Configuration Protocol (DHCP)	572
8.4.18. Manual IP Address Configuration	574
8.4.19. Determine Protocol Type Automatically	575
8.4.20. Point-to-Point Protocol over ATM (PPPoA)	577
8.4.21. Ethernet over ATM (ETHoA)	586
8.4.22. Classical IP over ATM (CLIP)	591
8.4.23. WAN-LAN Bridge	596
8.4.24. Virtual LAN Interface (VLAN)	608
8.4.25. Routed IP over ATM (IPoA)	627
8.4.26. Internet Protocol over Internet Protocol (IPIP)	633
8.4.27. General Routing Encapsulation (GRE)	637
8.5. Monitor	644
8.5.1. Network	644
8.5.2. CPU	645
8.5.3. Log	646
8.6. Routing	648
8.6.1. Overview	648
8.6.2. IPv6	660
8.6.3. BGP and OSPF	668
8.6.4. PPPoE Relay	671
8.7. Management	671
8.7.1. Universal Plug and Play	671
8.7.2. Simple Network Management Protocol	676
8.7.3. Remote Administration	680
8.7.4. Secure Shell	684
8.8. Maintenance	685
8.8.1. About OpenRG	685
8.8.2. Configuration File	686
8.8.3. Reboot	686
8.8.4. Restore Defaults	687
8.8.5. OpenRG Firmware Upgrade	688
8.8.6. MAC Cloning	690
8.8.7. Diagnostics	691
8.9. Objects and Rules	694
8.9.1. Protocols	694
8.9.2. Network Objects	696
8.9.3. Scheduler Rules	698
8.9.4. Certificates	701
9. Advanced	713

3

Using the Management Console

This chapter describes how to use OpenRG's management console, referred to as the **Web-based Management (WBM)**, which allows you to configure and control all of OpenRG's features and system parameters, using a user-friendly graphical interface. This user-friendly approach is also implemented in the WBM's documentation structure, which is based directly on the WBM's structure. You will find it easy to correspondingly navigate through both the WBM and its documentation.

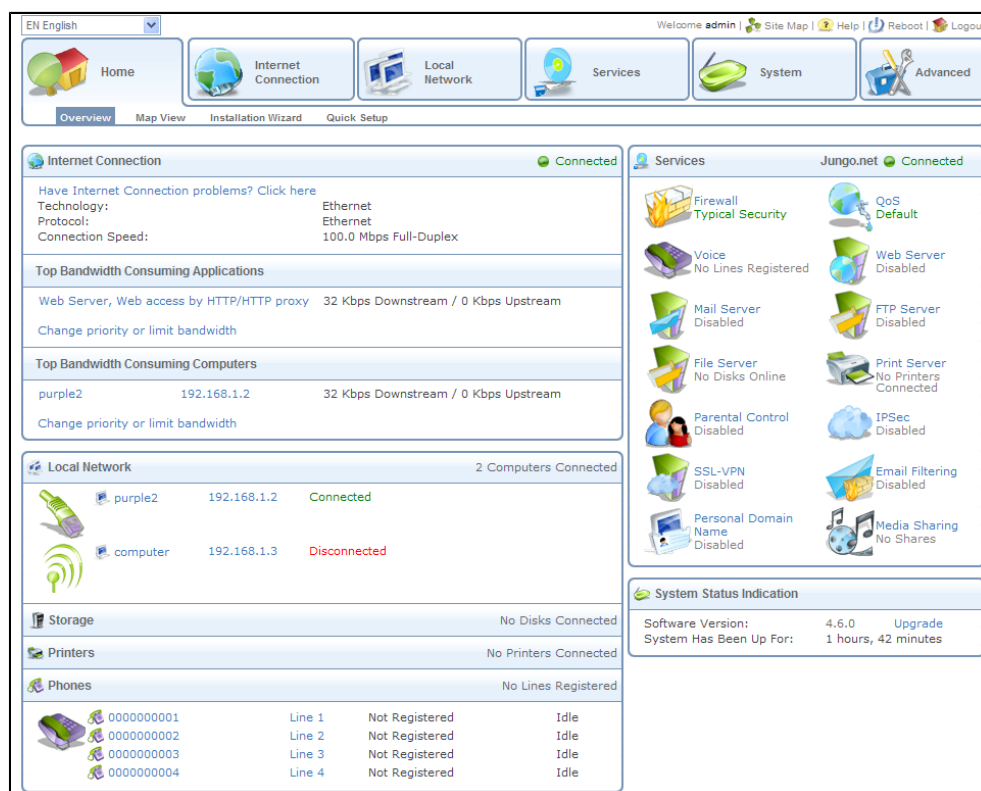


Figure 3.1. Web-based Management Home Page



Note: Some of the documented WBM features may appear slightly different or may not be available on certain platforms.

3.1. First Time Login

When logging into OpenRG for the first time, the installation wizard is the first screen to appear. This wizard is the first and foremost WBM configuration procedure.

1. Launch a Web browser on a computer in the LAN.
2. In the address bar, type the gateway's IP address or name as provided with your gateway. The default IP address is 192.168.1.1, and default name is 'http://openrg.home'. The 'Welcome to OpenRG' screen appears (see [Figure 3.2](#)), enabling you to select the language for the management console.

Figure 3.2. Welcome to OpenRG

3. Select the desired language and click 'Next' to continue. The 'Login Setup' screen appears.

Figure 3.3. WBM First Time Login

4. Enter a user name and password. Retype the password to verify its correctness. The default user name and password are both set to 'admin'. For security reasons, you should change these settings after the initial login.
5. Click 'Next' to login. At this point you can either continue the wizard to completion (refer to [Section 2.3.2](#)), or access the 'Quick Setup' screen in order to configure your Internet connection (refer to [Section 4.4](#)).

3.2. Accessing the WBM

To access the Web-based management:

1. Launch a Web browser on a computer in the LAN.
2. In the address bar, type the gateway's IP address or name as provided with your gateway. The default IP address is 192.168.1.1, and default name is 'http://openrg.home'. The 'Login' screen appears.

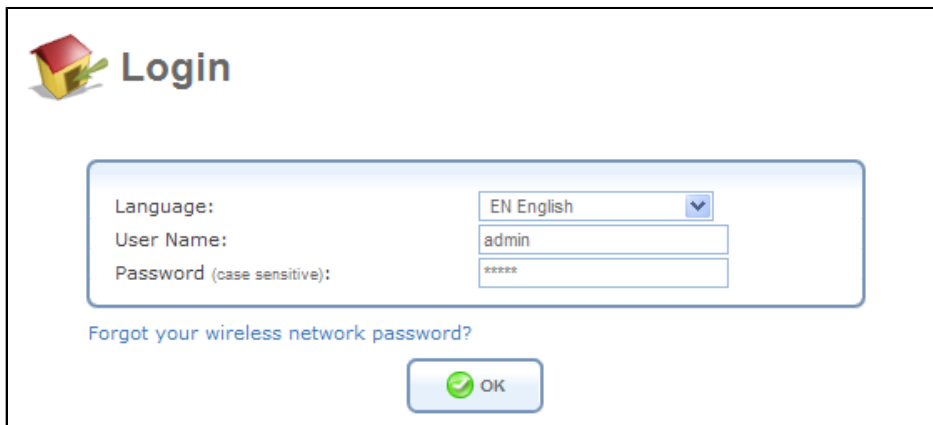


Figure 3.4. WBM Login

3. Enter your username and password to log in to the WBM.

Your session will automatically time-out after a few minutes of inactivity. If you try to operate the WBM after the session has expired, the 'Login' screen will appear and you will have to re-enter your user name and password before proceeding. This feature helps to prevent unauthorized users from accessing the WBM and changing the gateway's settings.



Note: If your computer is running an operating system that supports UPnP, such as Windows XP, you can easily add the computer to your home network and access the WBM directly from within Windows as explained in [Section 8.7.1](#).

3.3. Navigational Aids

The Web-based management is a user-friendly interface, designed as an Internet Web site that can be explored with any Web browser. This section illustrates the WBM's page structure and describes its navigational components and their hierarchial manner.

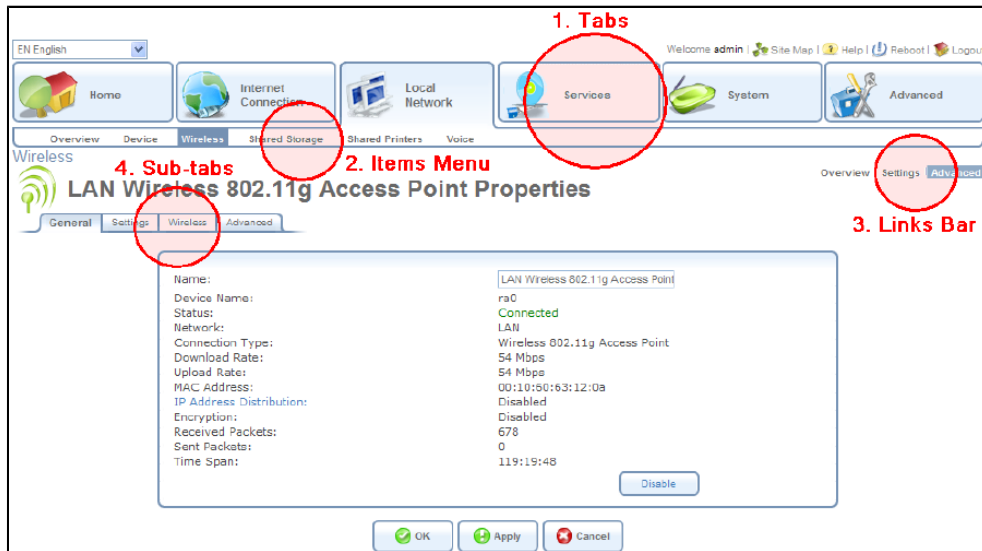


Figure 3.5. Navigation Components

1. The top level navigational aids are the **Tabs**, grouping the WBM screens into several main subject areas.
2. Each tab has an **Items Menu**, listing the different menu items relevant for the subject.
3. A menu item may have a **Links Bar**, located at the top-right of the screen. These links further divide the menu item into different subjects.
4. Lastly, a page content, usually a feature's properties page, may have a set of **Sub-tabs**, providing a division of settings in the form of yet another set of tabs.



Note: For convenience purposes, the entire WBM part of this User Manual has been constructed in accordance with the structure of the WBM—the chapter structure is identical to the tab structure, sections are written after item menus, etc.

In addition, a constant link bar appears at the top of every WBM page, providing shortcuts to information and control actions. These links include the site map, help, reboot and logout.

Welcome admin | Site Map | Help | Reboot | Logout

Figure 3.6. Constant Link Bar

3.4. Managing Tables

Tables are structures used throughout the Web-based management. They handle user-defined entries relating to elements such as network connections, local servers, restrictions and configurable parameters. The principles outlined in this section apply to all tables in the WBM.

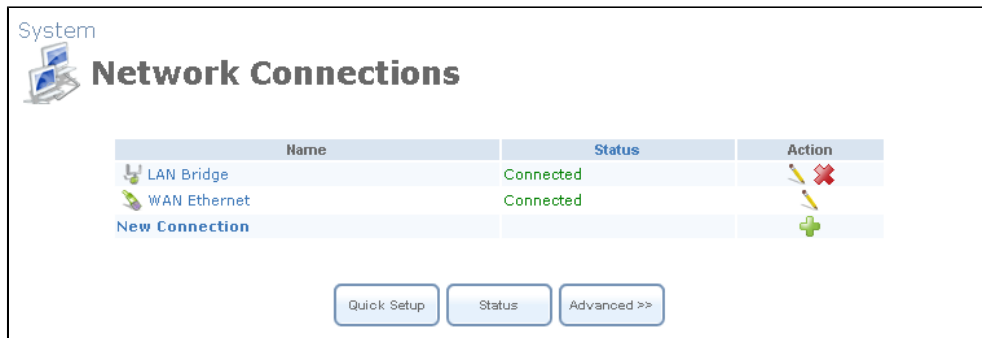


Figure 3.7. Typical Table Structure

Figure 3.7 illustrates a typical table. Each row defines an entry in the table. The following buttons, located in the 'Action' column, enable performing various actions on the table entries.



Use the **Add** action icon to add a row to the table.



Use the **Edit** action icon to edit a row in the table.



Use the **Remove** action icon to remove a row from the table.



Use the **Download** action icon to download a file from the table.



Use the **Copy** action icon to copy an item to the clipboard.



Use the **Move Up** action icon to move a row one step up in the table.



Use the **Move Down** action icon to move a row one step down in the table.

4

Home

4.1. Overview

The 'Overview' screen presents OpenRG's status summary in one convenient location. You can quickly and efficiently view important details of your connection status and hardware peripherals, as well as the statuses of OpenRG's different services. The following is the default 'Overview' screen.

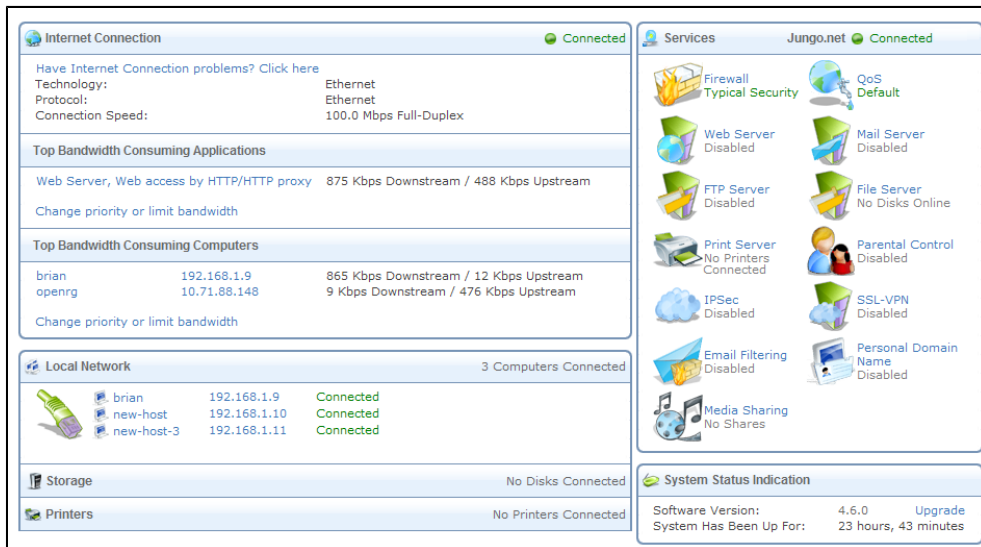


Figure 4.1. OpenRG Overview

Amongst its diverse information, OpenRG's homepage displays your Internet connection status, and specifically the top bandwidth consuming applications and computers.

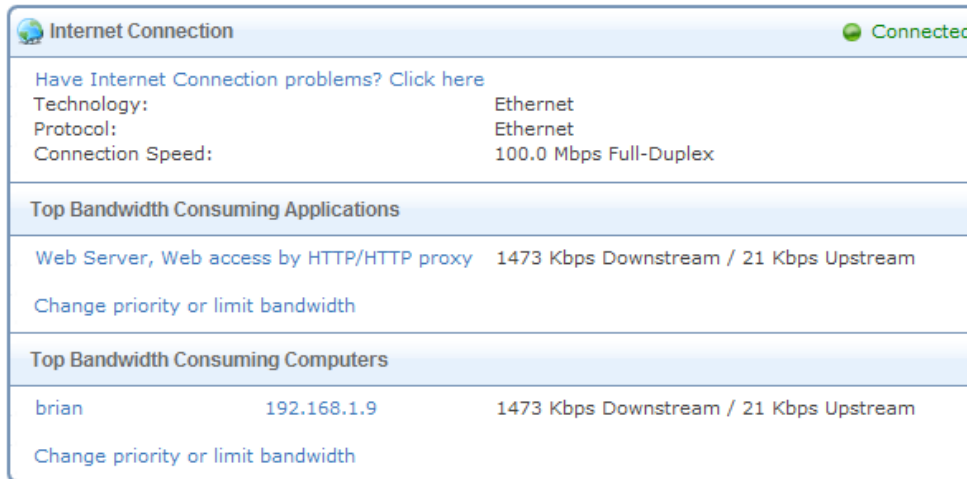


Figure 4.2. Internet Connection and Top Bandwidth Consumers

The top five bandwidth consuming applications and computers are displayed in their respective sections in descending order. The current downstream and upstream volumes are also displayed for every application and computer. The following links are available:

- **Have Internet Connection problems? Click here** This link routes to the 'Diagnostics' screen under the 'Internet Connection' tab, where you can run tests in order to diagnose and resolve Internet connectivity problems (for more information, refer to [Section 5.3](#)).
- **Top Bandwidth Consuming Applications** This headline link is identical to the 'Change priority or limit bandwidth' link inside this section. It routes to the 'Internet Connection Utilization' screen under 'QoS' in the 'Services' tab, and provides 'By Application' view. This section also displays the specific bandwidth consuming applications (for more information, refer to [Section 7.4.2.1](#)). If you would like to view more details about a specific bandwidth-consuming application, click its respective link.
- **Top Bandwidth Consuming Computers** This headline link is identical to the 'Change priority or limit bandwidth' link inside this section. It routes to the 'Internet Connection Utilization' screen under 'QoS' in the 'Services' tab, and provides 'By Computer' view. This section also displays the specific bandwidth consuming computers (for more information, refer to [Section 7.4.2.2](#)). If you would like to view more details about a specific bandwidth-consuming computer, click its respective link.

OpenRG's homepage is not only informative but also functional, conveniently providing shortcuts to different features and their configurations. For example, if you connect an unformatted storage device to OpenRG, the screen's 'Storage' section changes to the following.

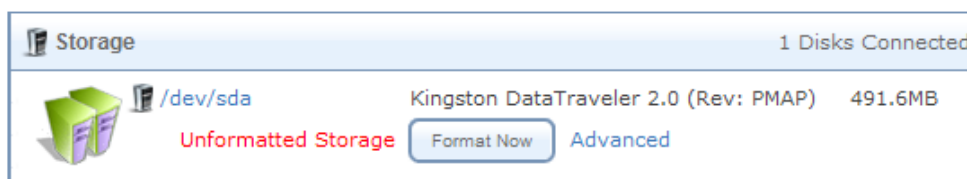


Figure 4.3. Unformatted Storage Device Message

By clicking the 'Format' button, OpenRG will format the disk in the default file system, which is FAT32. To format the disk in another file system, click the 'Advanced' link. This link leads to the 'Disk Information' screen located under 'Local Network'.

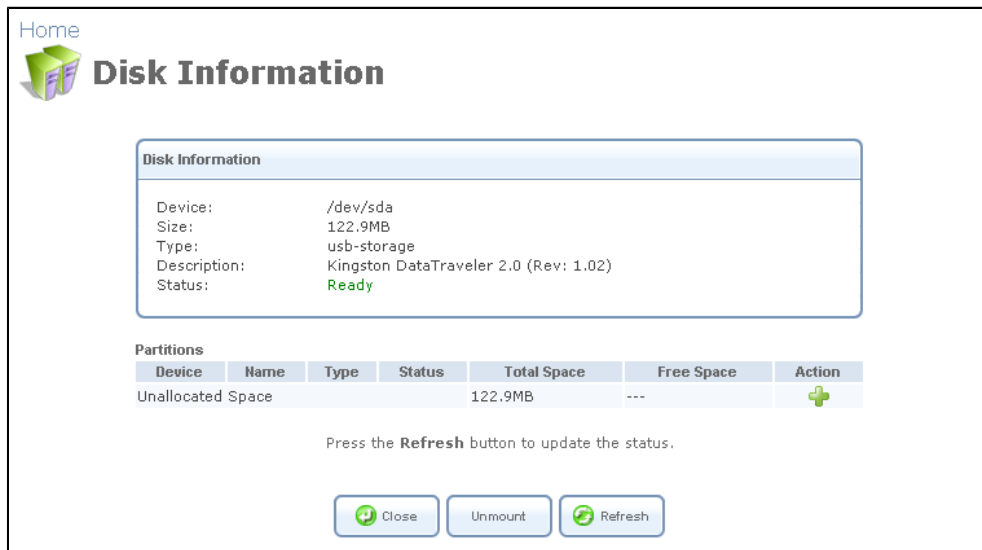


Figure 4.4. Disk Information

Click the + action icon to start the disk configuration wizard. The next steps are described in detail in [Section 6.4](#).

4.2. Map View

The network map depicts the various network elements, such as the Internet connection, firewall, gateway, internal network interface (Ethernet, USB, Wireless, etc.) and local network computers and peripherals.

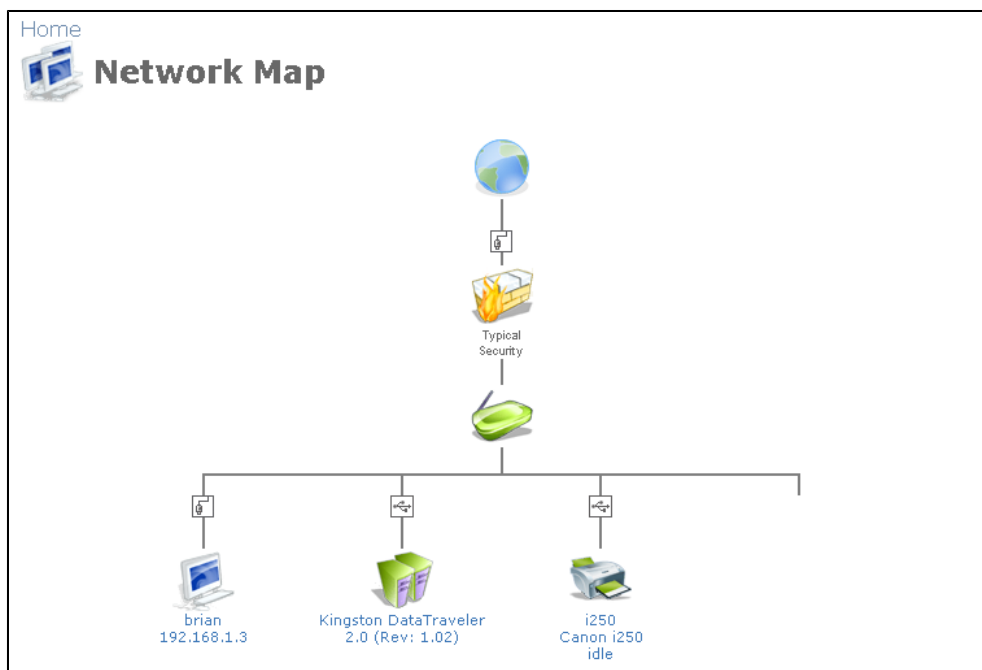


Figure 4.5. The Network Map

The following table explains the meaning of different network map symbols:



Represents the Internet



Represents your DSL Wide Area Network (WAN) connection. Click this icon to configure the WAN interface (refer to [Section 8.4](#)).



Represents your Ethernet Wide Area Network (WAN) connection. Click this icon to configure the WAN interface (refer to [Section 8.4](#)).



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 (refer to [Section 7.3](#)).

If OpenRG is equipped with multiple LAN devices (other than bridges), the network map will display the following icons to indicate the interfaces used for connecting these devices.



Represents an Ethernet Local Area Network (LAN) connection. Click this icon to configure network parameters for the Ethernet LAN device (refer to [Section 8.4](#)).



Represents a USB LAN connection. Click this icon to configure network parameters for the USB LAN device (refer to [Section 8.4](#)).



Represents a Wireless LAN connection. Click this icon to configure network parameters for the Wireless LAN device (refer to [Section 8.4](#)).



Represents a bridge connected in the home network. Click this icon to view the bridge's underlying devices.



Represents a computer (host) connected to the home network. This host is either a DHCP client that has received an IP lease from OpenRG, or a host with a static IP address, auto-detected by OpenRG. Note that OpenRG will recognize a physically connected host and display it in the Network Map only after network activity from that host has been detected (e.g. trying to browse to the WBM or to surf the Internet). Click this icon to view network information for the corresponding host.



Represents a host whose DHCP lease has expired and not renewed. The DHCP lease is renewed automatically, unless the host is no longer physically connected to OpenRG. The disconnected host's icon will disappear from the network map during the next scheduled IP lease query, performed by OpenRG's DHCP server.



Note: This icon also represents a static IP host that has no network activity.



Represents a printer that is connected to OpenRG and is shared by network users. Click this icon to view the printer's settings.



Represents a file server that is connected to OpenRG and is shared by network users. Click this icon to view the file server configuration.

OpenRG's standard network map displays devices that OpenRG recognized and granted a DHCP lease. However, with OpenRG's optional Zero Configuration Technology feature, devices with statically-defined IP addresses will also be recognized and displayed. For more information regarding this option, refer to [Chapter 10](#).

4.3. Installation Wizard

OpenRG provides an Installation Wizard that automatically diagnoses your network environment and configures its components. For a step-by-step description of the wizard procedure, refer to [Section 2.3.2](#).

4.4. Quick Setup

'Quick Setup' enables speedy and accurate configuration of your Internet connection and other important parameters. The following sections describe these various configuration parameters. Whether you configure these parameters or use the default ones, click 'OK' to enable your Internet connection.

Home

Quick Setup

Internet Connections

WAN Ethernet

Connection Type: Automatic IP Address Ethernet Connection

Name: WAN Ethernet

Status: Connected

MAC Address: 2a:b3:0e:32:3f:4f

IP Address: 10.71.85.103

Subnet Mask: 255.255.0.0

Default Gateway: 10.71.1.1

DNS Server: 192.168.71.1

[Click Here for Advanced Settings](#)

WAN DSL

Connection Type: No Internet Connection

[Click Here for Advanced Settings](#)

Wireless

Enable Wireless: Enabled

Jungo.net www.jungo.net

Enabled

Jungo.net User Name:

Don't have Jungo.net account? [Register](#)

Password:

Forgot your password?

State: Not Connected

Server Response: Registration Error

Jungo.net Services [Manage My Account](#)

Web Server:	Disabled
Parental Control:	Disabled
SSL-VPN:	Disabled
DDNS:	Disabled
Email Filtering:	Disabled

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

OK
Apply
Cancel
Refresh

Figure 4.6. Quick Setup

4.4.1. Configuring Your Internet Connection

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.

OpenRG 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.

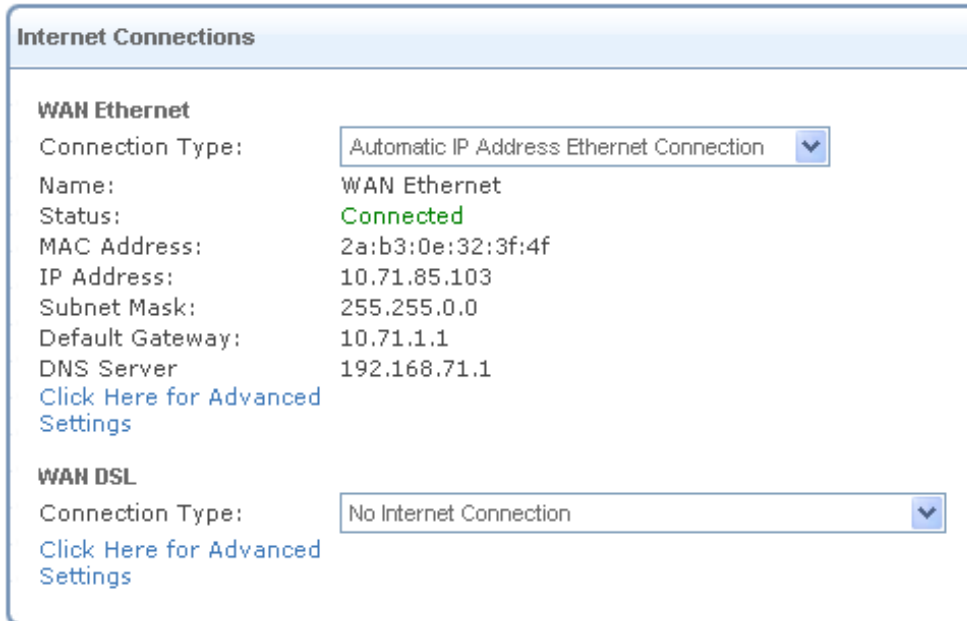


Figure 4.7. Quick Setup - Multiple WAN Devices

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 following list:

- Ethernet device:
 - Manual IP Address Ethernet Connection ([Section 4.4.1.1](#))
 - Automatic IP Address Ethernet Connection ([Section 4.4.1.2](#))
 - Point-to-Point Tunneling Protocol (PPTP) ([Section 4.4.1.3](#))
 - Layer 2 Tunneling Protocol (L2TP) ([Section 4.4.1.4](#))
- DSL device:
 - Point-to-point protocol over ATM (PPPoA) ([Section 4.4.1.5](#))
 - Routed Ethernet Connection over ATM (ETHoA) ([Section 4.4.1.6](#))
 - Bridged Ethernet Connection over ATM (ETHoA) ([Section 4.4.1.7](#))
 - Classical IP over ATM (CLIP) ([Section 4.4.1.8](#))
- Common to both:
 - Point-to-point protocol over Ethernet (PPPoE) ([Section 4.4.1.9](#))
 - No Internet connection ([Section 4.4.1.10](#))

Click the 'Click here for Advanced Settings' link at anytime to navigate to your WAN connection's properties page. The 'WAN Ethernet Properties' screen appears.

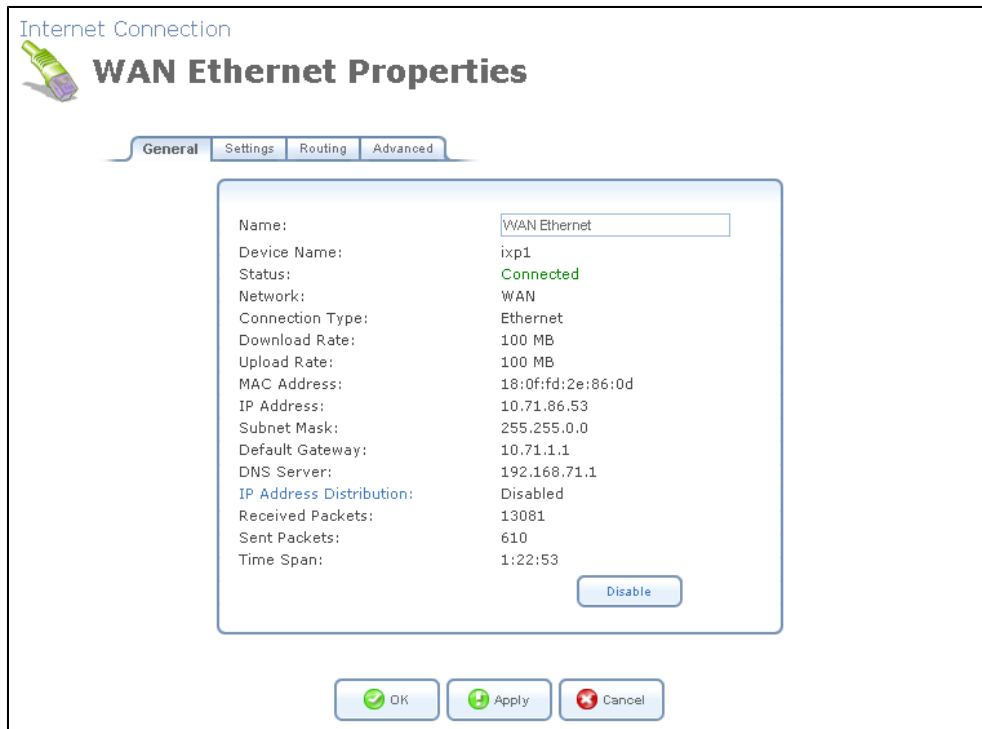


Figure 4.8. WAN Ethernet Properties

This screen provides all the configuration options for your WAN connection. For more information, refer to [Section 8.4.8](#).

4.4.1.1. Manual IP Address Ethernet Connection

1. Select 'Manual IP Address Ethernet Connection' from the 'Connection Type' drop-down menu.

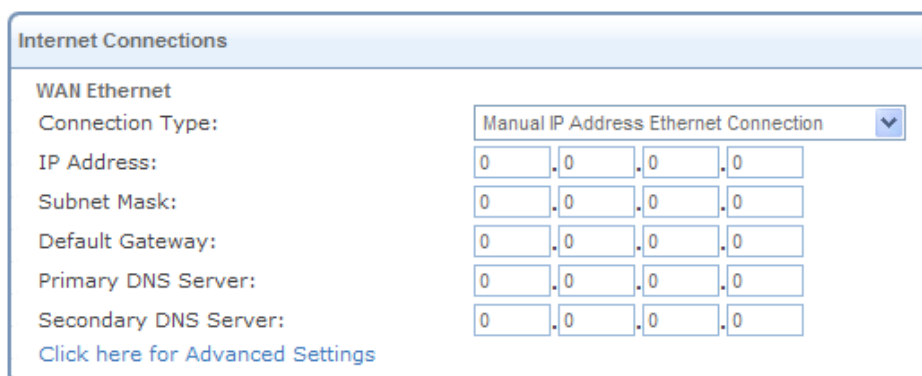


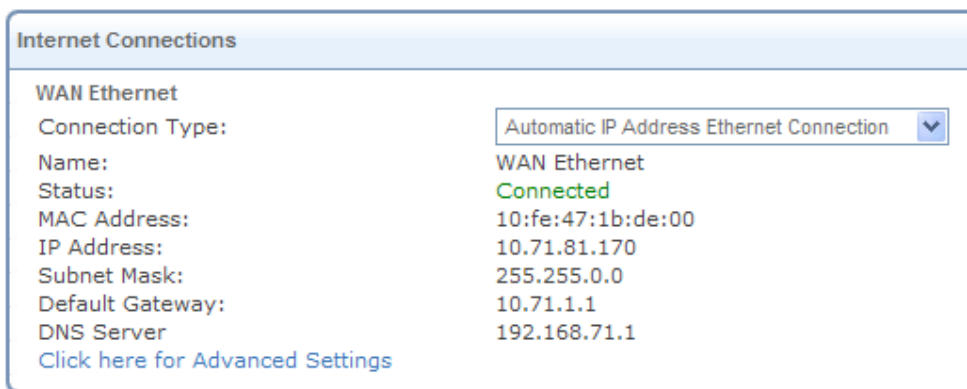
Figure 4.9. Internet Connection – Manual IP Address Ethernet Connection

2. According to your service provider's instructions, specify the following parameters:
 - IP address

- Subnet mask
- Default gateway
- Primary DNS server
- Secondary DNS server

4.4.1.2. Automatic IP Address Ethernet Connection

Select 'Automatic IP Address Ethernet Connection' from the 'Connection Type' drop-down menu (see [Figure 4.10](#)). OpenRG will obtain the WAN IP and DNS IP addresses from a DHCP server on the WAN.



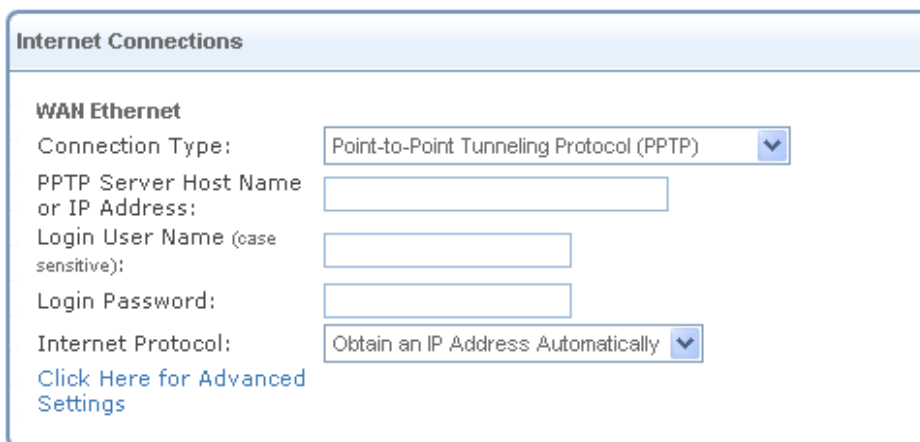
The screenshot shows a window titled "Internet Connections" with a tab for "WAN Ethernet". The "Connection Type" is set to "Automatic IP Address Ethernet Connection". The status is "Connected". The IP address is 10.71.81.170, subnet mask is 255.255.0.0, default gateway is 10.71.1.1, and the DNS server is 192.168.71.1. A link for "Advanced Settings" is provided at the bottom.

WAN Ethernet	
Connection Type:	Automatic IP Address Ethernet Connection
Name:	WAN Ethernet
Status:	Connected
MAC Address:	10:fe:47:1b:de:00
IP Address:	10.71.81.170
Subnet Mask:	255.255.0.0
Default Gateway:	10.71.1.1
DNS Server:	192.168.71.1
Click here for Advanced Settings	

Figure 4.10. Internet Connection – Automatic IP Address Ethernet Connection

4.4.1.3. Point-to-Point Tunneling Protocol (PPTP)

1. Select 'Point-to-Point Tunneling Protocol (PPTP)' from the 'Connection Type' drop-down menu.



The screenshot shows a window titled "Internet Connections" with a tab for "WAN Ethernet". The "Connection Type" is set to "Point-to-Point Tunneling Protocol (PPTP)". The "PPTP Server Host Name or IP Address", "Login User Name (case sensitive)", and "Login Password" fields are empty. The "Internet Protocol" is set to "Obtain an IP Address Automatically". A link for "Advanced Settings" is provided at the bottom.

WAN Ethernet	
Connection Type:	Point-to-Point Tunneling Protocol (PPTP)
PPTP Server Host Name or IP Address:	
Login User Name (case sensitive):	
Login Password:	
Internet Protocol:	Obtain an IP Address Automatically
Click Here for Advanced Settings	

Figure 4.11. Internet Connection – PPTP

2. Configure the following parameters according to your ISP information:

- PPTP Server Host Name or IP Address
- Login User Name
- Login Password
- 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 refreshes. Enter the IP Address, Subnet Mask, and Default Gateway provided to you by your ISP.

Internet Protocol:	<input type="text" value="Use the Following IP Address"/>
IP Address:	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
Subnet Mask:	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
Default Gateway:	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>

Figure 4.12. PPTP – Static IP Address

4.4.1.4. Layer 2 Tunneling Protocol (L2TP)

1. Select 'Layer 2 Tunneling Protocol (L2TP)' from the 'Connection Type' drop-down menu.

The screenshot shows the 'Internet Connections' dialog box. Under the 'WAN Ethernet' section, the 'Connection Type' is set to 'Layer 2 Tunneling Protocol (L2TP)'. Below this, there are three text input fields for 'L2TP Server Host Name or IP Address', 'Login User Name (case sensitive)', and 'Login Password'. The 'Internet Protocol' is set to 'Obtain an IP Address Automatically'. A blue link labeled 'Click Here for Advanced Settings' is located at the bottom left of the dialog box.

Figure 4.13. Internet Connection – L2TP

2. Configure the following parameters according to your ISP information:
 - L2TP Server Host Name or IP Address
 - Login User Name
 - Login Password
 - 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 refreshes. Enter the IP Address, Subnet Mask, and Default Gateway provided to you by your ISP.


Internet Protocol:	Use the Following IP Address 
IP Address:	0 . 0 . 0 . 0
Subnet Mask:	0 . 0 . 0 . 0
Default Gateway:	0 . 0 . 0 . 0


Figure 4.14. L2TP – Static IP Address

4.4.1.5. Point-to-Point Protocol over ATM (PPPoA)

1. Select 'Point-to-point protocol over ATM (PPPoA)' from the 'Connection Type' drop-down menu.

Internet Connections

WAN DSL

Connection Type: Point-to-Point Protocol over ATM (PPPoA) 

Login User Name (case sensitive):

Login Password:

Automatic PVC Scan

[Click Here for Advanced Settings](#)

Figure 4.15. Internet Connection – PPPoA

2. Your Internet Service Provider (ISP) should provide you with the following information:
 - Login user name
 - Login password
 - By default, the 'Automatic PVC Scan' check box is enabled, which means that OpenRG configures the VPI, VCI and encapsulation parameters automatically. If you would like to configure these parameters manually, deselect this check box. The screen refreshes.

Automatic PVC Scan

VPI:

VCI:



Encapsulation: LLC 

Figure 4.16. Manual PVC Scan Parameters



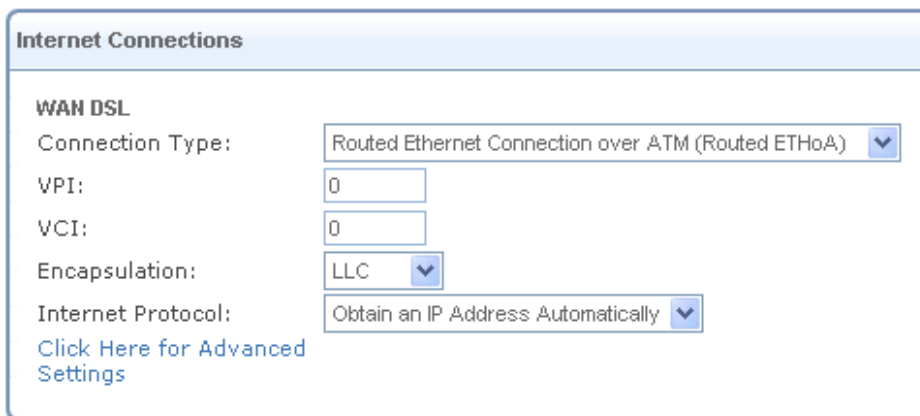
Note: The default VPI and VCI values, queried during the automatic PVC scan, can be viewed in OpenRG's configuration file (for more information, refer to [Section 8.8.2](#)).

- Specify the VPI and VCI values.

- Select the encapsulation method from the drop-down menu. You can choose among the following methods:
 - LLC
 - VCMux
 - VCMux - HDLC

4.4.1.6. Routed Ethernet Connection over ATM (ETHoA)

1. Select 'Routed Ethernet Connection over ATM (ETHoA)' from the 'Connection Type' drop-down menu.



The screenshot shows a configuration window titled "Internet Connections" with a sub-section "WAN DSL". The "Connection Type" dropdown is set to "Routed Ethernet Connection over ATM (Routed ETHoA)". The "VPI" and "VCI" text boxes both contain the value "0". The "Encapsulation" dropdown is set to "LLC". The "Internet Protocol" dropdown is set to "Obtain an IP Address Automatically". A blue link "Click Here for Advanced Settings" is located below the "Internet Protocol" dropdown.

Figure 4.17. Internet Connection – Routed ETHoA

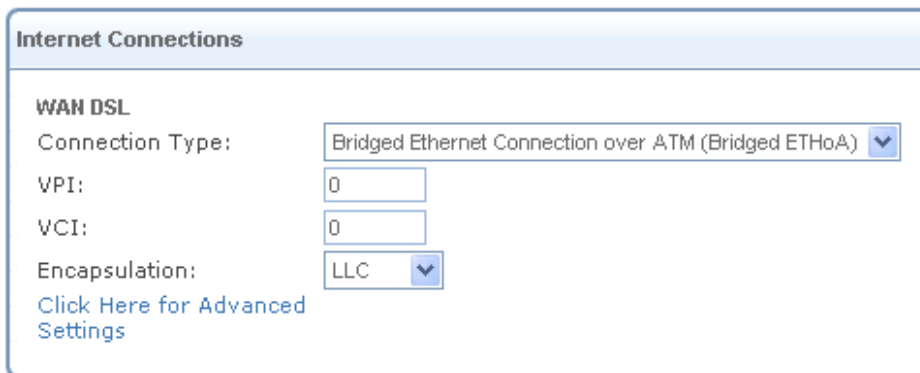
2. Your Internet Service Provider (ISP) should provide you with the following information:
 - Specify the value of the VPI and VCI parameters.
 - Select the encapsulation method from the drop-down menu. You can choose among the following methods:
 - LLC
 - VCMux
 - Select the Internet Protocol: Most 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 refreshes. Enter the IP Address, Subnet Mask, Default Gateway, and DNS Server details provided to you by your ISP.

Internet Protocol:	Use the Following IP Address ▾
IP Address:	0 . 0 . 0 . 0
Subnet Mask:	0 . 0 . 0 . 0
Default Gateway:	0 . 0 . 0 . 0
Primary DNS Server:	0 . 0 . 0 . 0
Secondary DNS Server:	0 . 0 . 0 . 0

Figure 4.18. ETHoA - Static IP Address

4.4.1.7. Bridged Ethernet Connection over ATM (ETHoA)

1. Select 'Bridged Ethernet Connection over ATM (ETHoA)' from the 'Connection Type' drop-down menu.



Internet Connections

WAN DSL

Connection Type: Bridged Ethernet Connection over ATM (Bridged ETHoA) ▾

VPI: 0

VCI: 0

Encapsulation: LLC ▾

[Click Here for Advanced Settings](#)

Figure 4.19. Internet Connection – Bridged ETHoA

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 drop-down menu. You can choose among the following methods:
 - LLC
 - VCMux

4.4.1.8. Classical IP over ATM (CLIP)

1. Select 'Classical IP over ATM (CLIP)' from the 'Connection Type' drop-down menu

The screenshot shows the 'Internet Connections' dialog box with the 'WAN DSL' section selected. The 'Connection Type' is set to 'Classical IP over ATM (CLIP)'. Below this, there are input fields for IP Address, Subnet Mask, Default Gateway, Primary DNS Server, and Secondary DNS Server, each with four individual boxes for the octets. There are also input boxes for VPI and VCI, both containing the value '0'. A link 'Click Here for Advanced Settings' is visible at the bottom left.

Figure 4.20. Internet Connection – CLIP

2. According to your Internet service provider's instructions, configure the following network connection parameters:

- IP Address
- Subnet Mask
- Default Gateway IP address
- Primary DNS Server IP address
- Secondary DNS Server IP address
- VPI
- VCI

4.4.1.9. Point-to-Point Protocol over Ethernet (PPPoE)

1. Select 'Point-to-point protocol over Ethernet (PPPoE)' from the 'Connection Type' drop-down menu.

The screenshot shows the 'Internet Connections' dialog box with the 'WAN Ethernet' section selected. The 'Connection Type' is set to 'Point-to-Point Protocol over Ethernet (PPPoE)'. Below this, there are input boxes for 'Login User Name (case sensitive)' and 'Login Password'. A link 'Click here for Advanced Settings' is visible at the bottom left.

Figure 4.21. Internet Connection – PPPoE

2. Your Internet Service Provider (ISP) should provide you with the following information:
 - Login user name
 - Login password
3. 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).



Note: The default VPI and VCI values, queried during the automatic PVC scan, can be viewed in OpenRG's configuration file (for more information, refer to [Section 8.8.2](#)).

4.4.1.10. No Internet Connection

Select 'No Internet Connection' from the 'Connection Type' drop-down menu (see [Figure 4.22](#)). Choose this connection type if you do not have an Internet connection, or if you want to disable all existing connections.

A screenshot of a web interface titled "Internet Connections". Under the heading "WAN Ethernet", there is a "Connection Type:" label followed by a dropdown menu showing "No Internet Connection". Below this, there is a link that says "Click here for Advanced Settings".

Figure 4.22. Internet Connection – No Internet Connection

4.4.2. Wireless

Click the 'Enabled' check box to enable your wireless connection.

A screenshot of a web interface titled "Wireless". It contains several settings: "Enable Wireless:" with a checked checkbox and the text "Enabled"; "Wireless Network (SSID):" with a text input field containing "OpenRG admin"; "802.11 Mode:" with a dropdown menu showing "802.11b/g Mixed"; and "Security:" with a dropdown menu showing "Web Authentication".

Figure 4.23. Internet Connection - Wireless

Specify the wireless network's ID in the 'Wireless Network (SSID)' field. The default SSID is 'OpenRG admin'. For a full description of the LAN Wireless connection, refer to [Section 8.4.7](#).

4.4.3. Jungo.net

This screen section enables you to connect to the Jungo.net portal, through which you can upgrade OpenRG with advanced broadband services. An additional benefit of using Jungo.net is that it configures the services automatically, thereby saving you time and effort. To start activating the Jungo.net services on your gateway, you need to first obtain a personal Jungo.net account. The account details must then be entered in the respective login fields (see [Figure 4.24](#)), in order to associate the gateway with the account and connect it to the Jungo.net portal.

The screenshot displays two main sections of the Jungo.net configuration interface. The top section, titled 'Jungo.net' with the URL 'www.jungo.net', contains a checked 'Enabled' checkbox. Below it are input fields for 'Jungo.net User Name:' and 'Password:'. To the right of these fields are links for 'Don't have Jungo.net account? Register' and 'Forgot your password?'. The 'State:' field shows 'Not Connected' in red text, and the 'Server Response:' field shows 'Registration Error'. The bottom section, titled 'Jungo.net Services' with a 'Manage My Account' link, lists five services: 'Web Server', 'Parental Control', 'SSL-VPN', 'Dynamic DNS', and 'Email Filtering', all of which are currently 'Disabled'.

Jungo.net		www.jungo.net
<input checked="" type="checkbox"/> Enabled		
Jungo.net User Name:	<input type="text"/>	Don't have Jungo.net account? Register
Password:	<input type="text"/>	Forgot your password?
State:		Not Connected
Server Response:		Registration Error

Jungo.net Services		Manage My Account
Web Server:	Disabled	
Parental Control:	Disabled	
SSL-VPN:	Disabled	
Dynamic DNS:	Disabled	
Email Filtering:	Disabled	

Figure 4.24. Jungo.net

The 'Jungo.net Services' section displays the Jungo.net services that are pre-embedded in OpenRG. You can either configure them manually, or let the Jungo.net portal configure them automatically. These services are:

- Web Server (for more information, refer to [Section 7.11.4](#))
- Parental Control (for more information, refer to [Section 7.8](#))
- SSL-VPN (for more information, refer to [Section 7.10.2](#))
- Dynamic DNS (for more information, refer to [Section 7.12](#))
- Email Filtering (for more information, refer to [Section 7.9](#))

For more information about the Jungo.net portal and its operation, refer to [Section 7.2](#).

4.4.4. Quick Setup Completed

OpenRG does not require further configuration in order to start working. After the setup described in this chapter, you can immediately start using your gateway to:

- Share a broadband connection among multiple users (HTTP, FTP, Telnet, NetMeeting) and between all of the computers connected to your home network.
- Build a home network by connecting additional PCs and network devices to the gateway.
- Share resources (file servers, printers, etc.) between computers in the home network using their names; auto-learning DNS enables OpenRG to automatically detect the network identification names of the LAN PCs, enabling mutual communication using names, not IP addresses.
- Control network parameters, including DHCP, DNS and WAN settings.
- View network status, traffic statistics, system log and more.
- Allow access from the Internet to games and other services provided by computers in the home network.
- Prohibit computers in the home network from accessing selected services on the Internet.
- Block access to specific Internet Web sites from your home network.

To learn about how to configure your Firewall security parameters, refer to [Section 7.3](#). If you wish to apply corporate-grade security to your network, refer to [Section 7.3.11](#). If your gateway is equipped with multiple LAN ports, you can connect additional devices directly to the gateway. Otherwise, connect a hub or switch to the LAN port, to which you can connect additional devices. In both cases, configure newly connected devices to automatically obtain IP address as described above.

5

Internet Connection

5.1. Overview

The 'Overview' screen (see [Figure 5.1](#)) provides general information regarding your WAN Internet connection, such as the connection's status, protocol, speed, duration, and Internet address. Refer to this screen for a quick status reference.

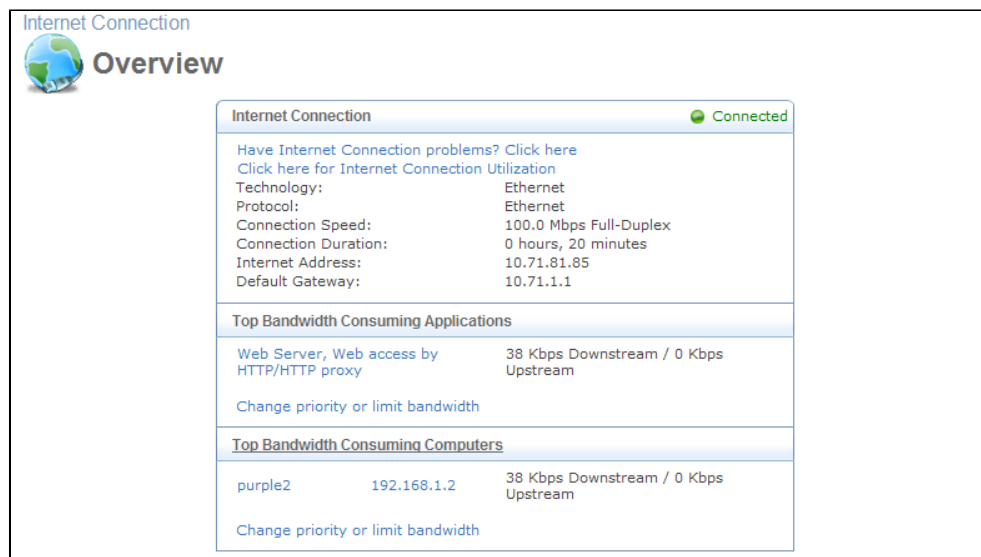


Figure 5.1. Internet Connection – Overview

The following links are available:

- **Have Internet Connection problems? Click here** This link routes you to the 'Diagnostics' screen under the 'Internet Connection' tab, where you can run tests in order to diagnose and resolve Internet connectivity problems (for more information, refer to [Section 5.3](#)).

- **Click Here For Internet Connection Utilization** Click this link to analyze the traffic usage of your WAN connection (for more information, refer to [Section 7.4.2](#)).

In addition, this screen displays OpenRG's top bandwidth consuming applications and computers, described in [Section 4.1](#).

5.2. Settings

The 'Settings' screen provides basic configuration options for the different types of Internet connections supported by OpenRG.

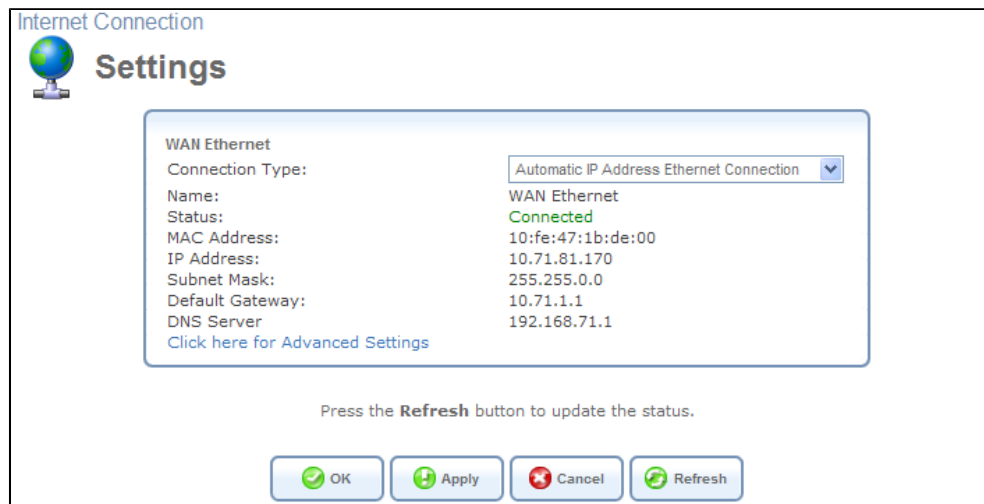


Figure 5.2. Internet Connection – Settings

Select your WAN connection type according to the method by which you are connected to the Internet. Each option in this drop-down menu is described thoroughly in [Section 4.4.1](#).

Click the 'Click here for Advanced Settings' link at anytime to navigate to your WAN connection's properties page. The 'WAN Ethernet Properties' screen appears.

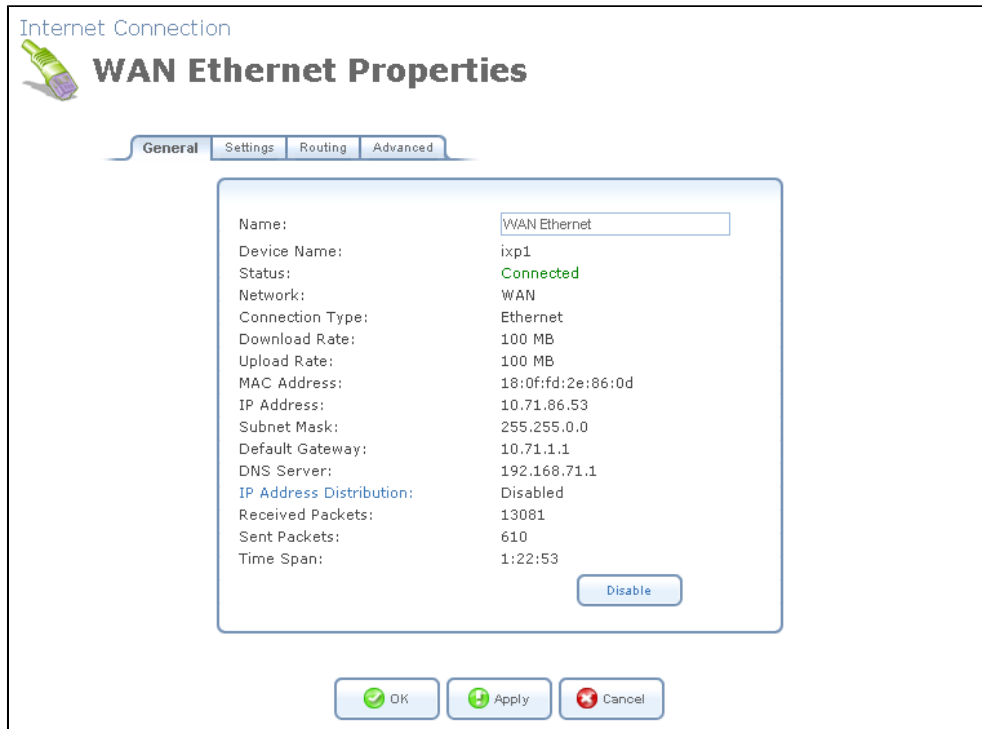


Figure 5.3. WAN Ethernet Properties

This screen provides all the configuration options for your WAN connection. For more information, refer to [Section 8.4.8](#).

5.3. Diagnostics

The 'Diagnostics' screen (see [Figure 5.4](#)) provides a series of tests aimed at validating your gateway's Internet connection.

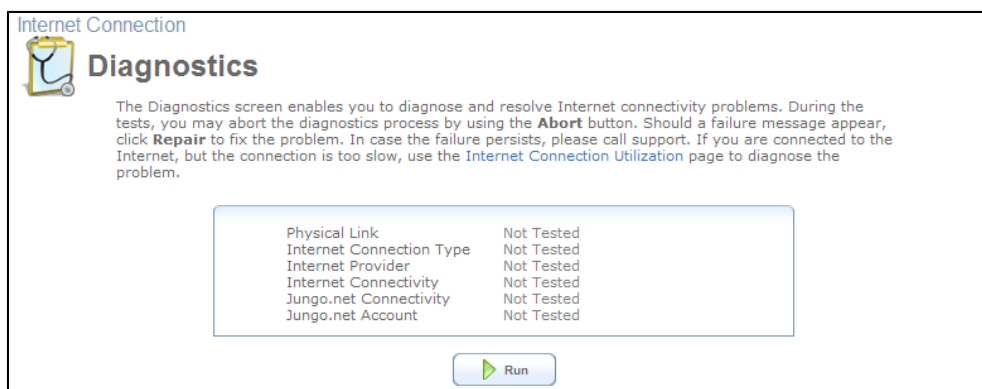


Figure 5.4. Internet Connection -- Diagnostics

Click 'Run' to begin the test routine. While testing is in progress, you may abort the diagnostics process by using the 'Abort' button. Should a failure message appear, click 'Repair' to initiate the Installation Wizard procedure (refer to [Section 2.3.2](#)).

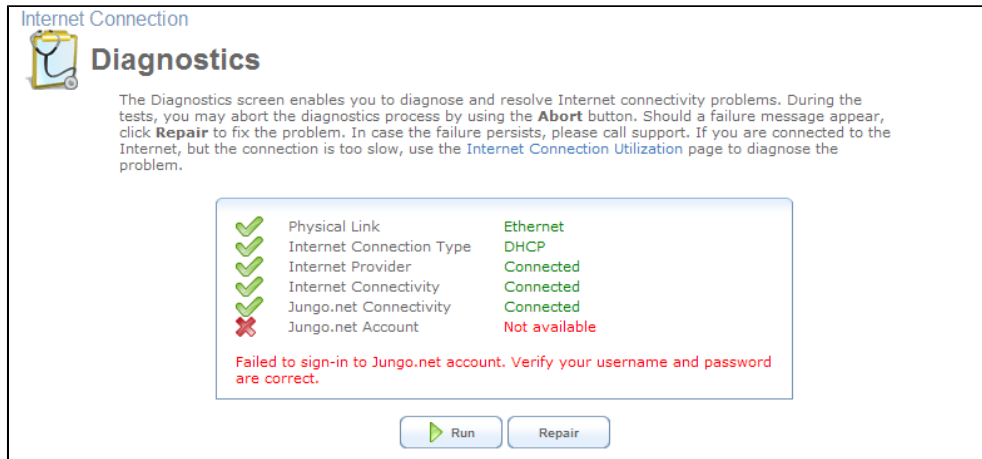


Figure 5.5. Diagnostics Process

6

Local Network

6.1. Overview

The 'Overview' screen presents OpenRG's network summary. This includes all connected devices: computers, disks, printers and phones. When this screen is loaded, OpenRG begins the process of automatically detecting the network services available on connected computers (hosts).

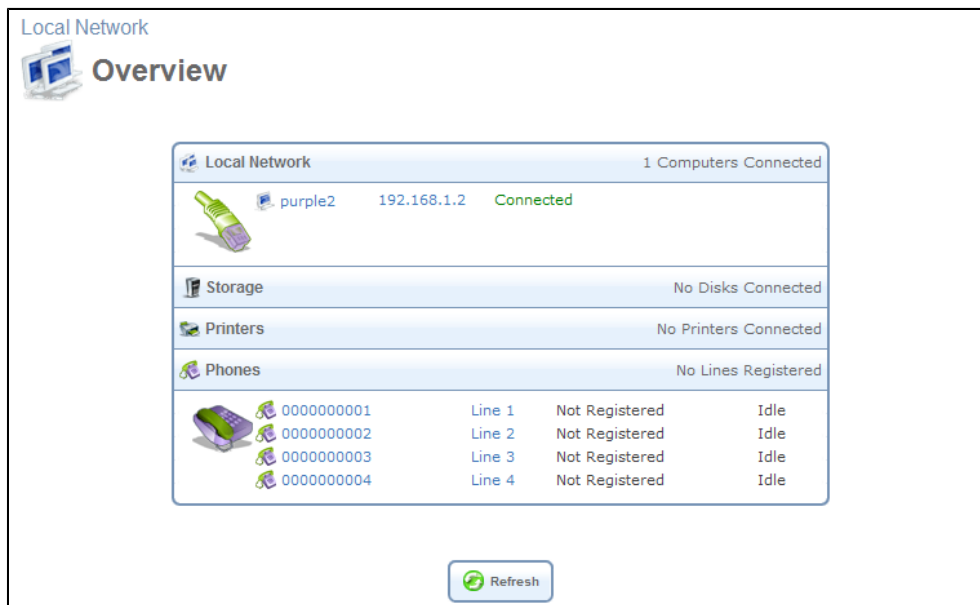


Figure 6.1. Network Services Detection

The screen then refreshes, displaying each computer's network services.

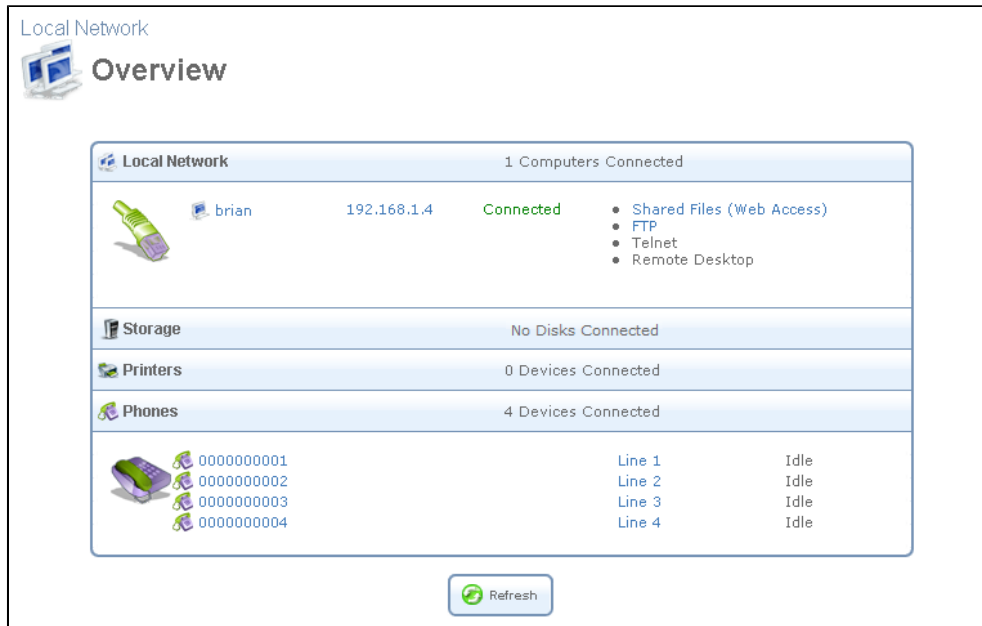


Figure 6.2. Local Network Overview

To view more information on a specific computer, click its respective link. The 'Host Information' screen appears.

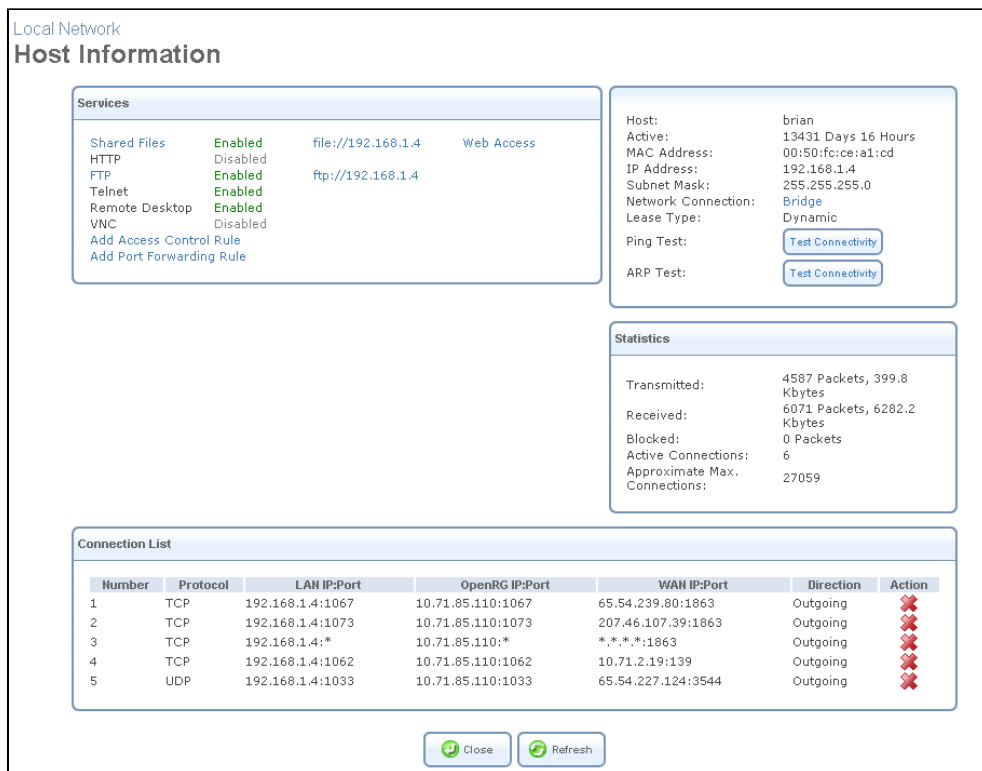


Figure 6.3. Host Information

This screen presents all of the information relevant to the connected computer, such as connection information, available services, traffic statistics, and connection list. It also enables you to perform connectivity tests with the computer.

Services This section lists the services on the computer that are available to other computers either from the LAN, via Web access (SSL-VPN), or from both. Services are accessible only

when enabled on the computer. Services available via SSL-VPN require a secure (HTTPS) connection (for more information, refer to [Section 7.10.2](#)). When a service is accessible from the LAN, you can activate it by either clicking its name or the URL that appears (see [Figure 6.3](#)). When a service is accessible via Web access, you can activate it by clicking the 'Web Access' link that appears. Available services are:

- **Shared Files** Access the computer's shared files directory.
- **HTTP** Access the computer's HTTP server (if available).
- **FTP** Open an FTP session with the computer.
- **Telnet** Open a Telnet session with the computer.
- **Remote Desktop** Remotely control a Windows computer with the Remote Desktop utility.
- **VNC** Remotely control the computer with the Virtual Network Computing desktop protocol.
- **Add Access Control Rule** Block access to Internet services from the computer, or allow access if the firewall is set to a "High" security level (for more information, refer to [Section 7.3.2](#)).
- **Add Port Forwarding Rule** Expose services on the computer to external Internet users (for more information, refer to [Section 7.3.3](#)).

Connection Information This section displays various details regarding the computer's connection settings. To view the connection's properties, click the network connection type ('Bridge' in the above example). The relevant properties screen appears (for more information, refer to [Section 8.4](#)). In addition, you can run a Ping or ARP test by clicking the respective 'Test Connectivity' button. The tests are performed in the 'Diagnostics' screen (refer to [Section 8.8.7](#)).

Statistics This section displays the computer's traffic statistics, such as the number and size of transmitted and received packets.

Connection List This section displays the list of connections opened by the computer on OpenRG's firewall. The table displays the computer's source LAN IP address and port, the gateway's IP address and port to which it is translated, and the destination WAN IP address and port.

6.2. Device View

The 'Device View' screen (see [Figure 6.4](#)) presents a summary of OpenRG's LAN devices, including a bridge (if one exists), Ethernet, USB and wireless, and the status of each one (connected/disconnected).

Name	Status	Action
LAN Bridge	Connected	[Refresh] [Delete]
LAN Hardware Ethernet Switch 1 Computers Connected	2 Ports Connected	[Refresh] [Delete]
LAN USB	Disconnected	[Refresh] [Delete]
LAN Wireless 802.11g Access Point	Device Missing	[Refresh] [Delete]

Figure 6.4. Local Network Device View

6.3. Wireless

The 'Wireless' menu item concentrates the wireless LAN settings of your gateway, which are configurable from the main 'Network Connections' menu item under the 'System' tab (refer to [Section 8.4.7](#)). The 'Wireless' menu item consists of the following screens (according to the links bar).

6.3.1. Overview

The 'Overview' screen presents OpenRG's wireless connection summary, enabling you to edit the following parameters.

Wireless Overview

Overview | Settings | Advanced

Wireless

Enable Wireless: Enabled

Wireless Network (SSID):

802.11 Mode:

Security:

Figure 6.5. Wireless Overview

Enable Wireless Check or uncheck this box to enable or disable the wireless connection.

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.

802.11 Mode Specifies the type of the connection.

Security Select the security type for the connection: None, Web authentication, or Password Protected (WPA).

Pre-Shared Key This field appears when selecting WPA, enabling you to enter a value that will serve as the encryption key for the connection.

6.3.2. Settings

The 'Settings' screen provides basic configuration options for OpenRG's wireless connection.



Figure 6.6. Wireless Settings

To learn more about these configuration options, refer to [Section 8.4.7.7](#).

6.3.3. Advanced

Clicking the 'Advanced' link displays the 'LAN Wireless 802.11g Access Point Properties' screen, providing all wireless configuration options.



Figure 6.7. LAN Wireless 802.11g Access Point Properties

To learn more about this screen and its tabs, refer to [Section 8.4.7](#).

6.4. Shared Storage

OpenRG can operate as a disk manager for storage devices connected via USB. 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 'Shared Storage' menu item provides access to the 'Disk Management' screen, which enables you to manage your storage devices as described in this section.

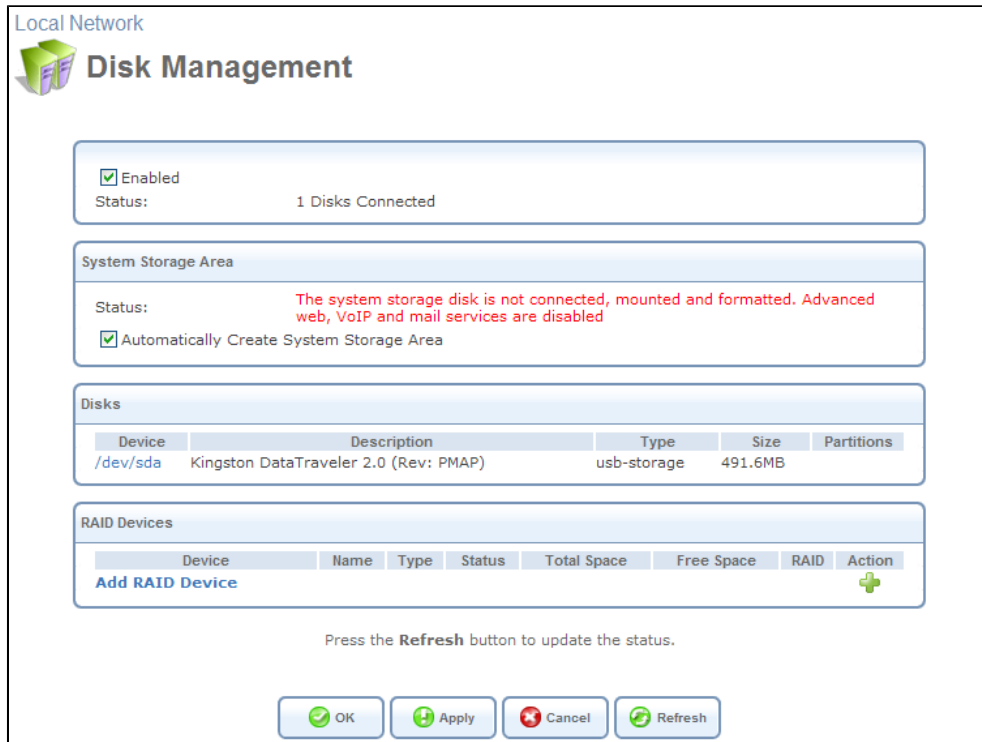



Figure 6.8. Disk Management

6.4.1. Managing Disk Partitions

In [Section 2.4.3](#) you learned how to connect a mass storage device and add a partition to it. A partition can also be checked, reformatted, or deleted. The following sections describe each of these operations.

 **Note:** When applying administrative changes to storage devices, services using these devices are stopped (for more information about such services, refer to [Section 7.11](#)).

6.4.1.1. Checking a Partition

Periodically, you should check the disk's partitions for the presence of bad sectors, to maintain the disk's health and prevent data loss.

To check a partition:

1. In the 'Disks' section of the 'Disk Management' screen (see [Figure 6.8](#)), click the disk's link. The 'Disk Information' screen appears.

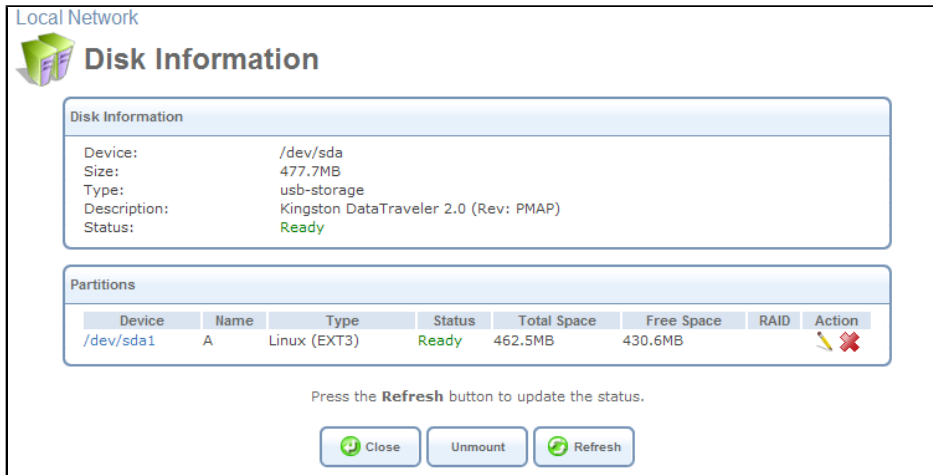


Figure 6.9. Disk Information

2. In the 'Partitions' section, click the action icon of the partition you would like to check. The 'Partition Properties' screen appears.

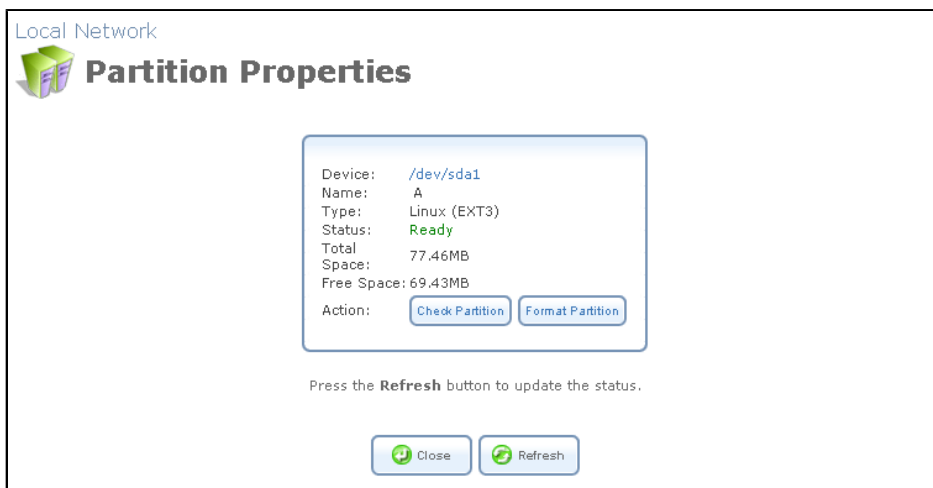


Figure 6.10. Partition Properties

3. Click the 'Check Partition' button. The 'Partition Check' screen appears.

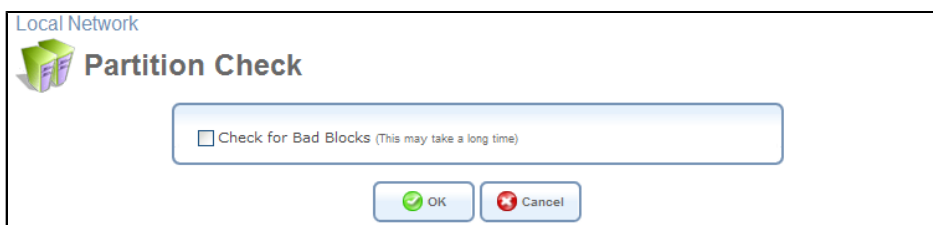


Figure 6.11. Partition Check

This screen enables you to check a partition for presence of bad blocks prior to the regular file system checkup. To do so, select the 'Check for Bad Blocks' check box.

4. Click 'Next'. A warning screen appears, alerting you that the partition will be set to offline.

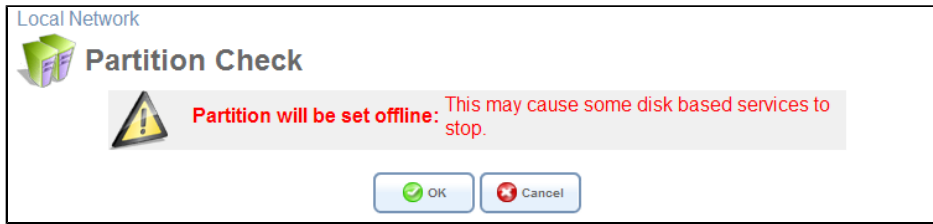


Figure 6.12. Offline Partition Warning

5. Click 'OK' to check the partition. The screen refreshes as the partition checking progresses.

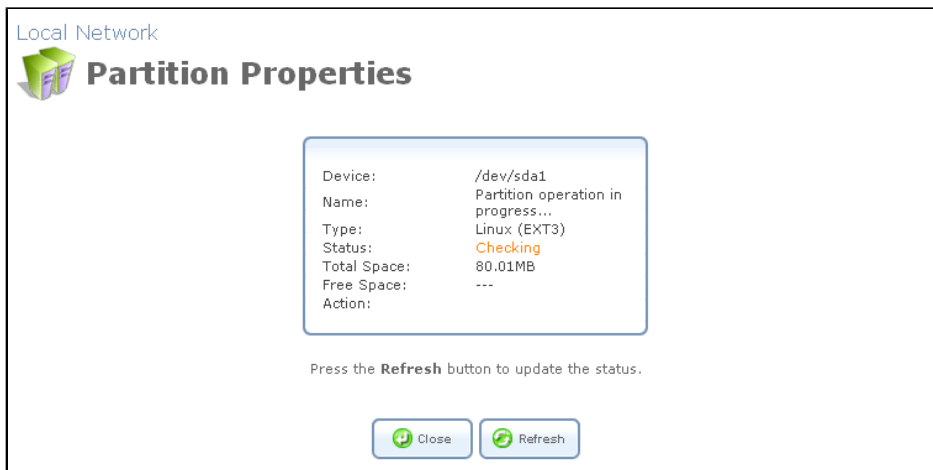


Figure 6.13. Partition Checking in Progress

When the check is complete, the status changes to 'Ready'.

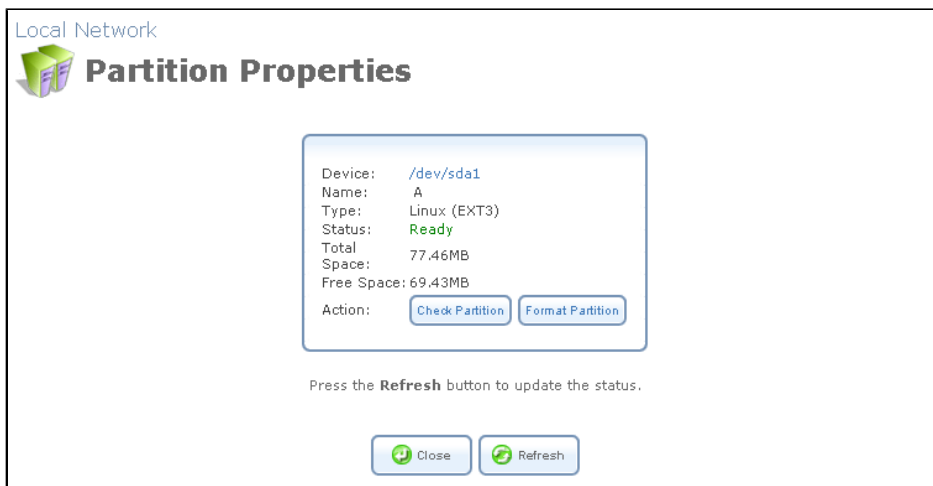


Figure 6.14. Checking Complete – Partition Ready

6.4.1.2. Reformatting a Partition

In addition to formatting a newly created partition, as described in [Section 2.4.3.1](#), you can reformat an existing partition with either EXT2, EXT3, or FAT32 file systems. Unless your gateway is based on the Intel IXP425 or Infineon platform, a partition can also be formatted with NTFS, allowing both *Read* and *Write* access. OpenRG running on the Intel IXP425 or

Infinion platforms identifies a storage device formatted with NTFS, but only allows *Read* access to it.



Note: For security reasons, it is recommended to format disk partitions with the EXT2 or EXT3 file system.

To reformat a partition:

1. In the 'Disks' section of the 'Disk Management' screen (see [Figure 6.8](#)), click the disk's link. The 'Disk Information' screen appears.

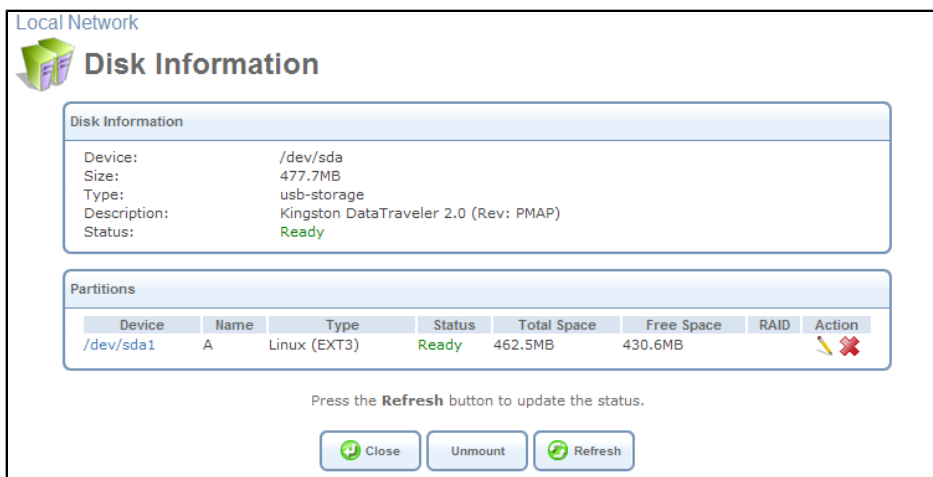



Figure 6.15. Disk Information

2. In the 'Partitions' section, click the  action icon of the partition you would like to edit. The 'Partition Properties' screen appears.

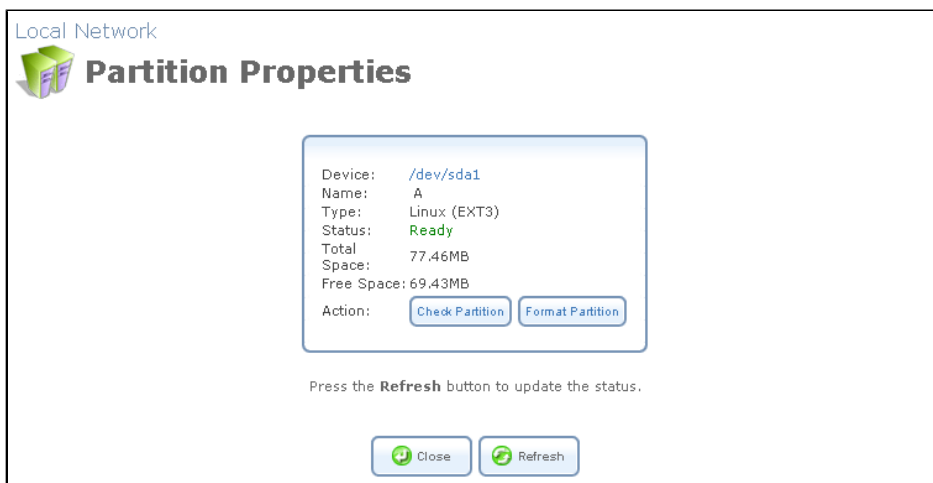


Figure 6.16. Partition Properties

3. Click the 'Format Partition' button. The 'Partition Format' screen appears.

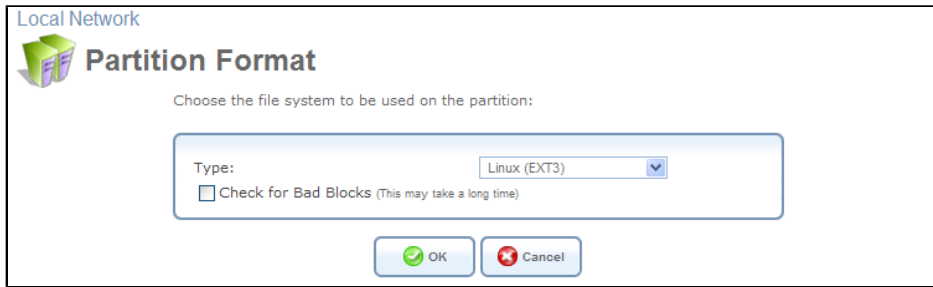



Figure 6.17. Partition Format

 Note: You can also instruct OpenRG to check the disk for bad blocks prior to formatting it, by selecting the corresponding check box. Only the disk space consisting of healthy blocks will be formatted. Bad blocks will be ignored.

4. Select a file system for the partition and click 'Next'. A warning screen appears, alerting you that all the data on the partition will be lost.

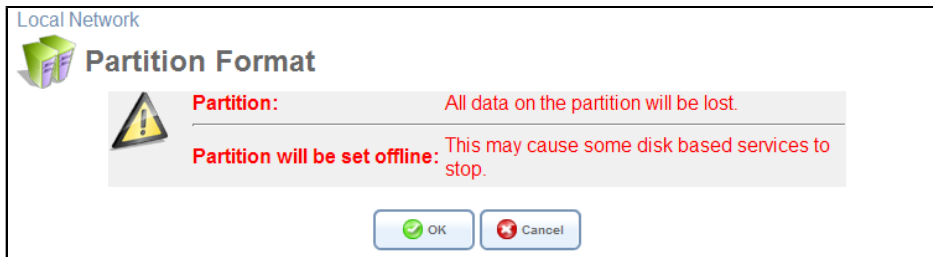


Figure 6.18. Lost Data Warning

5. Click 'OK' to format the partition. The screen refreshes as the partition formatting progresses.

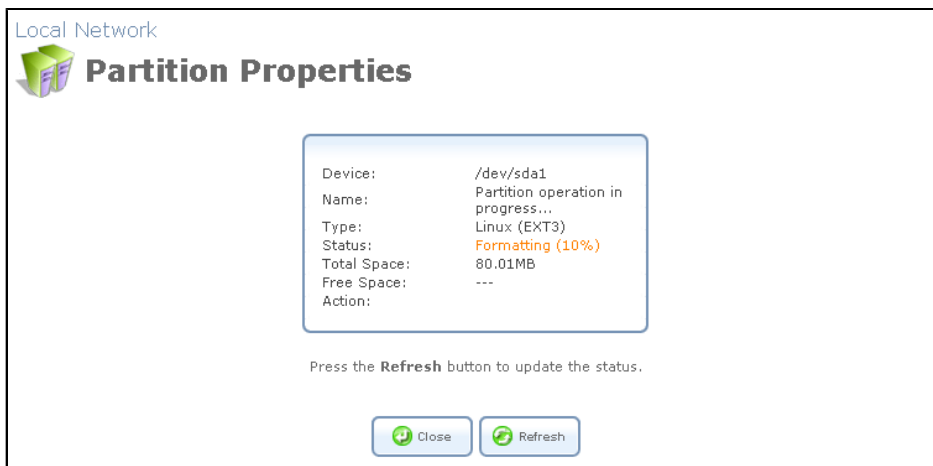


Figure 6.19. Partition Formatting in Progress

When the format is complete, the status changes to 'Ready'.

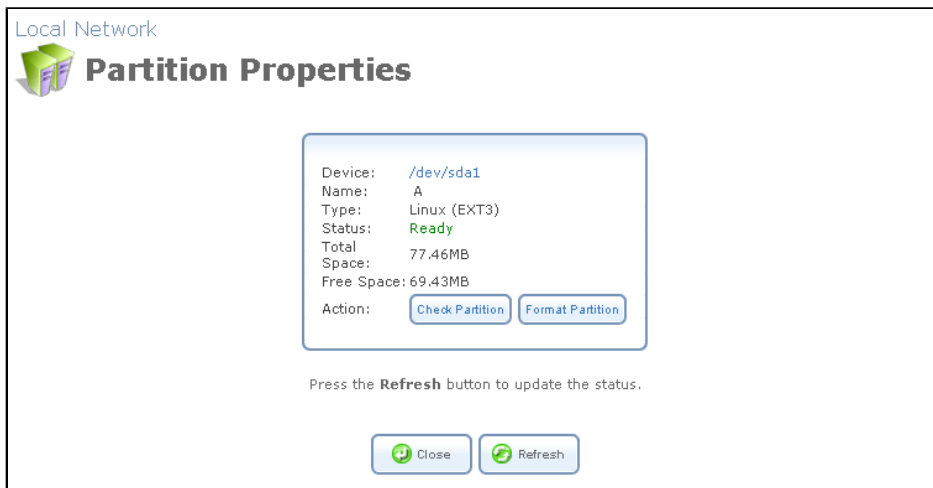


Figure 6.20. Formatting Complete – Partition Ready

6.4.1.3. Deleting a Partition

If you would like to delete a partition on your storage device, perform the following:

1. In the 'Disks' section of the 'Disk Management' screen (see [Figure 6.8](#)), click the disk's link. The 'Disk Information' screen appears.

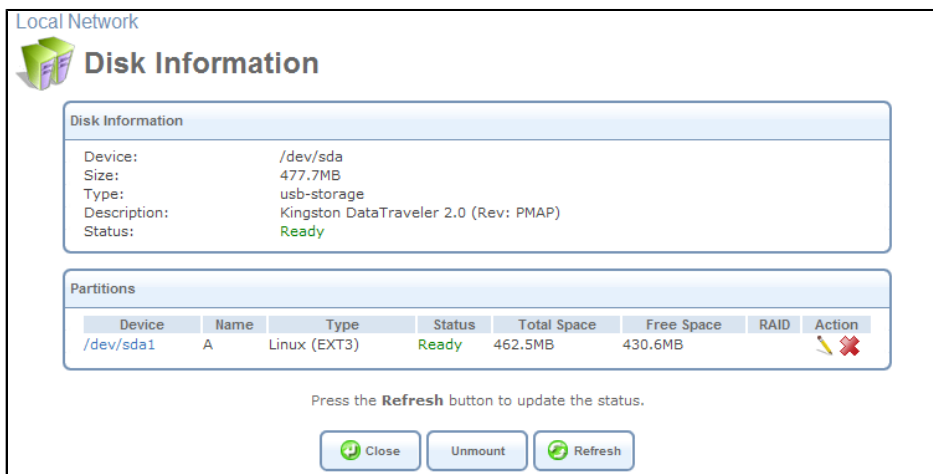


Figure 6.21. Disk Information

2. In the 'Partitions' section, click the action icon of the partition you would like to delete. A warning screen appears, alerting you that all the data on the partition will be lost.

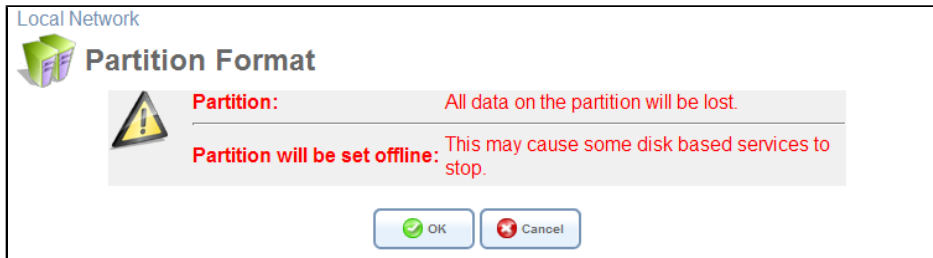


Figure 6.22. Lost Data Warning

3. Click 'OK' to delete the partition.

6.4.2. Defining a Location for System Files

OpenRG uses a specific location on the storage device for storing data used by its various services. This location, referred to as "system storage area", is used by the following services:

- Printer spool and drivers
- Mail server spool
- Mail boxes information
- Backup of OpenRG's configuration file (rg_conf)
- PBX-related audio files for voice mail, auto attendants and music on-hold
- FTP server
- Users' home directories
- Web server content

By default, OpenRG automatically defines one of the disk partitions as the system storage area. This setting is valid until the storage device is disconnected. When reconnected, OpenRG may select another partition for this purpose.

If you would like to permanently set a specific partition as the location for the system storage area, perform the following:

1. In the 'Disk Management' screen (see [Figure 6.8](#)), deselect the **Automatically Create System Storage Area When Not Available** check box. The screen refreshes displaying the 'System Storage Area' field.

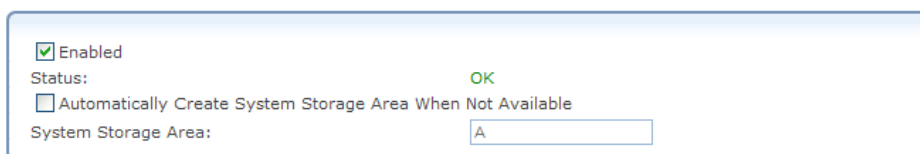


Figure 6.23. Manually Defined System Storage Area

2. Enter the letter of the partition on which you would like to set the system storage area.



Note: If your gateway is based on the Intel IXP425 or Infineon platform, data cannot be written to partitions formatted with NTFS. In this case, if you define an NTFS partition as the system storage area, the services mentioned earlier will not operate on OpenRG, displaying a warning message.

3. Click 'OK' to save the settings.

If you wish to view the system directories, perform the following:

1. Verify that the system storage area is shared (refer to [Section 7.11.2.1](#)).
2. Browse to `\\openrg` (use a Windows Explorer window if you are using a browser other than Internet Explorer). Should a Windows login dialog box appear, enter your WBM username and password.
3. If more than one partition exists, explore the 'Shared' directories to find out in which of them the system storage area is set. You can easily identify its location by the presence of such system folders as **drivers** and **home**.

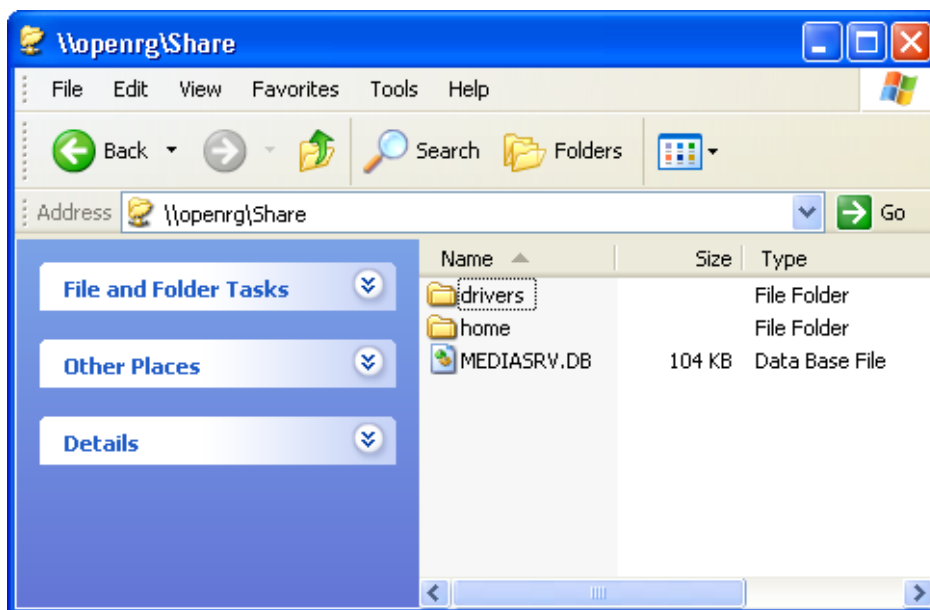


Figure 6.24. Disk Share

6.4.3. Optimizing Data Storage and Backup with RAID

OpenRG supports Redundant Array of Independent Disks (RAID) on storage devices connected to the gateway by USB. A RAID device is a logical device that has physical devices underlying it. These physical devices are disk partitions, each of them belonging to a different disk connected to OpenRG.

The supported RAID levels are:

- Level 0 – Provides data striping, or spreading out blocks of each file across multiple disk drives, but no redundancy. This improves performance but does not deliver fault tolerance. If one drive fails, all data in the array is lost.
- Level 1 – Provides disk mirroring. This is a technique in which data is written to two duplicate disks simultaneously, providing data redundancy. This method improves performance and delivers fault tolerance.
- Level 5 – With a minimum of three disks, this level provides data striping and utilizes one disk for backup information, which enables it to restore any other disk in the array.

When using RAID1, it is recommended that the underlying partitions be of the same size, to avoid loss of disk space due to mirroring.



Note: A disk partition configured with RAID can no longer be managed as a regular partition, but only be controlled by the RAID device. From the moment RAID is configured, it is the RAID device that can be shared, scanned, formatted and mounted as a regular partition.

6.4.3.1. Creating a RAID Device

To create a RAID device:

1. In the 'Disk Management' screen (see [Figure 6.8](#)), click the 'Add RAID Device' link. The 'RAID Properties' screen appears.

Figure 6.25. RAID Properties

2. From the RAID Level drop-down menu, select the RAID level that suits your needs.
3. In the 'Mount Point' field, enter a name for the mount point of the RAID device. The mount point name has the same function as a drive letter assigned to a newly created partition.

4. Select the underlying devices (your pre-configured partitions) from the drop-down menu. For RAID1 you may choose only one device and later add another one.
5. Click 'Next'. The 'Partition Format' screen appears.

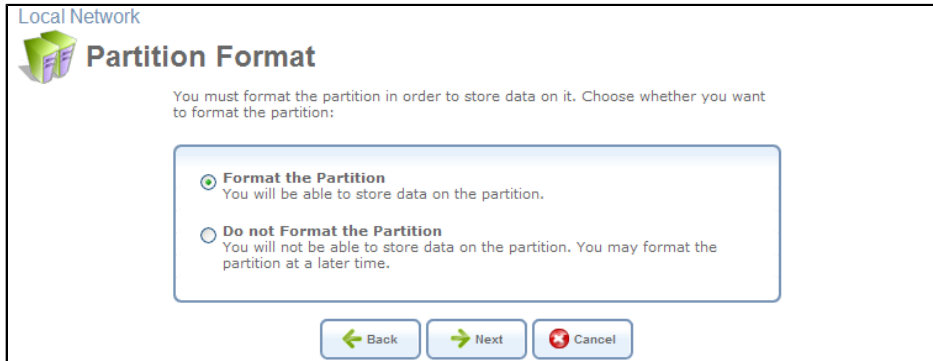


Figure 6.26. Partition Format

6. Select if you would like to format the partition(s), and click 'Next'.
7. If you have chosen to format the partition(s), the 'Partition File System' screen appears.

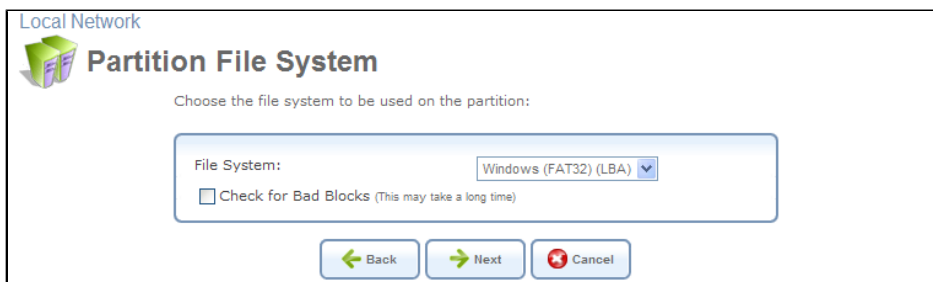


Figure 6.27. Partition File System

Select the file system type and click 'Next'.

8. In both cases, the 'Partition Summary' screen appears, displaying a summary of the chosen device properties. Click the 'Finish' button to execute the RAID device creation, and to format the partition(s) if you have chosen to do so.

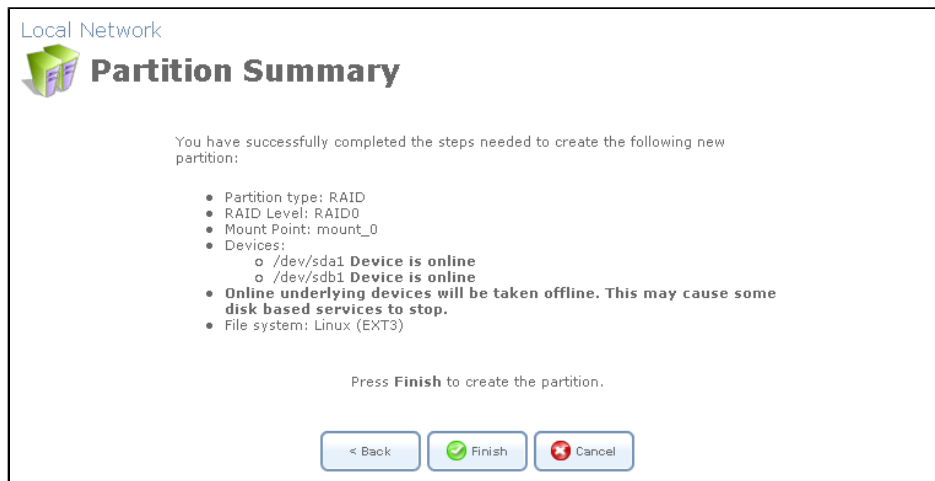


Figure 6.28. Partition Summary

If the device is RAID1 and has two underlying devices, its re-synchronization process (partition mirroring) will begin simultaneously. During re-synchronization, the RAID device is fully usable, and can be mounted and used.

Figure 6.29 depicts a successful configuration of two RAID devices, as they appear in the 'Raid Devices' section of the 'Disk Management' screen. The first is RAID0, consisting of two underlying partitions (one on each disk), and the second is RAID1, consisting of another set of underlying partitions.






RAID Devices							
Device	Name	Type	Status	Total Space	Free Space	RAID	Action
/dev/md0	mount_0	Linux (EXT3)	Ready	154.8MB	142.8MB	RAID0: /dev/sda1, /dev/sdb1	 
/dev/md1	mount_1	Linux (EXT3)	Ready	41.39MB	35.23MB	RAID1: /dev/sda2, /dev/sdb2	 
Add RAID Device							

Figure 6.29. RAID Devices

Note that the RAID0 total space is the sum of the two partitions, while the RAID1 total space is the size of one partition (due to mirroring).

When RAID is configured over the existing partitions, they are no longer independent. It is therefore necessary that you update the location of the system storage area, as services using it will not be available. To update the system storage area location, perform the steps described in [Section 6.4.2](#), with the only difference that you must specify the RAID device's mount point name instead of a partition letter.

6.4.3.2. Using a RAID Device

You can store files and create folders on the shared RAID devices by performing the following:

1. Browse to `\\openrg` (use a Windows Explorer window if you are using a browser other than Internet Explorer). Should a Windows login dialog box appear, enter your WBM

username and password. The following window appears, displaying the RAID and printer/fax shares.

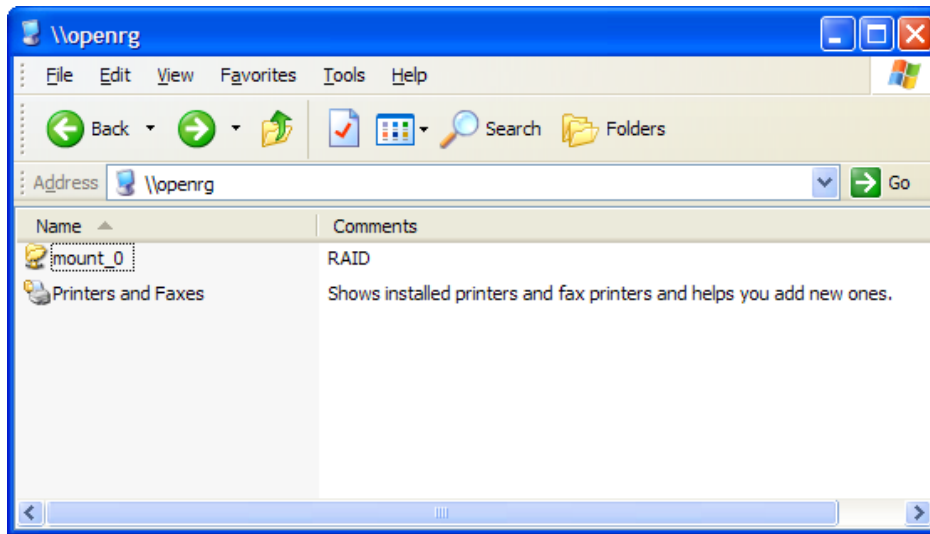


Figure 6.30. RAID and Printer/Fax Shares

2. Access the RAID device's shared folder (in this example, **mount_0**).
3. Copy a file to this directory, or create a new folder for it.

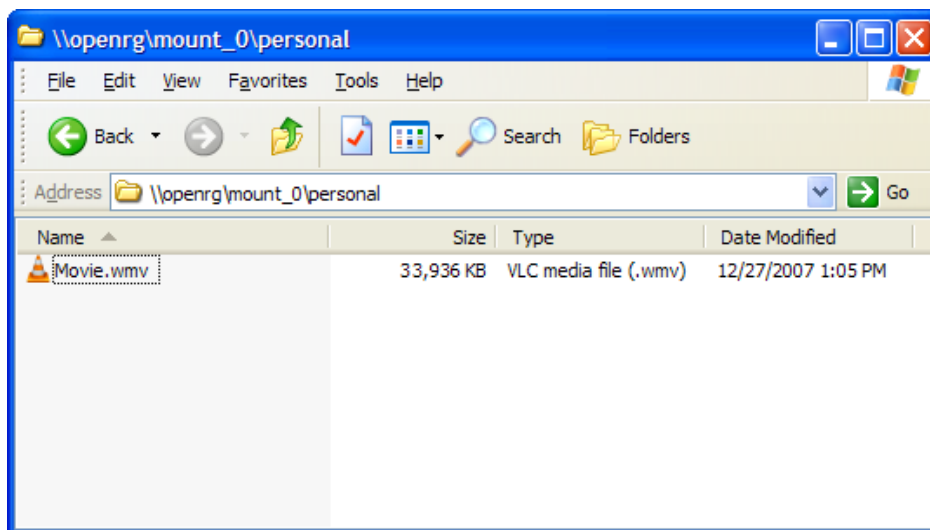



Figure 6.31. Shared Files on RAID

Depending on the type of the RAID device you have set up (either RAID0, RAID1, or RAID5), the file you stored on it will either be fragmented and distributed across the disks (providing faster data storage/retrieval), or it will be simultaneously backed up on the underlying physical disks (providing mirroring), or both of these operations will be executed.

6.4.3.3. Maintaining a RAID Device

A RAID device differs from a regular partition by not being part of a single physical disk. Therefore it can be maintained only in OpenRG. RAID maintenance is divided into two aspects:

- Maintaining the RAID device itself:
 1. Click the  action icon of the RAID device in the 'Disk Management' screen (see [Figure 6.29](#)).
 2. The 'RAID Properties' screen appears (see [Figure 6.32](#)), in which you can:
 - a. Enable or disable the RAID device using the 'Enabled' check box.
 - b. Change the mount point assigned to the device.
 - c. Add or remove the underlying devices (can be done for RAID1 and RAID5 only).

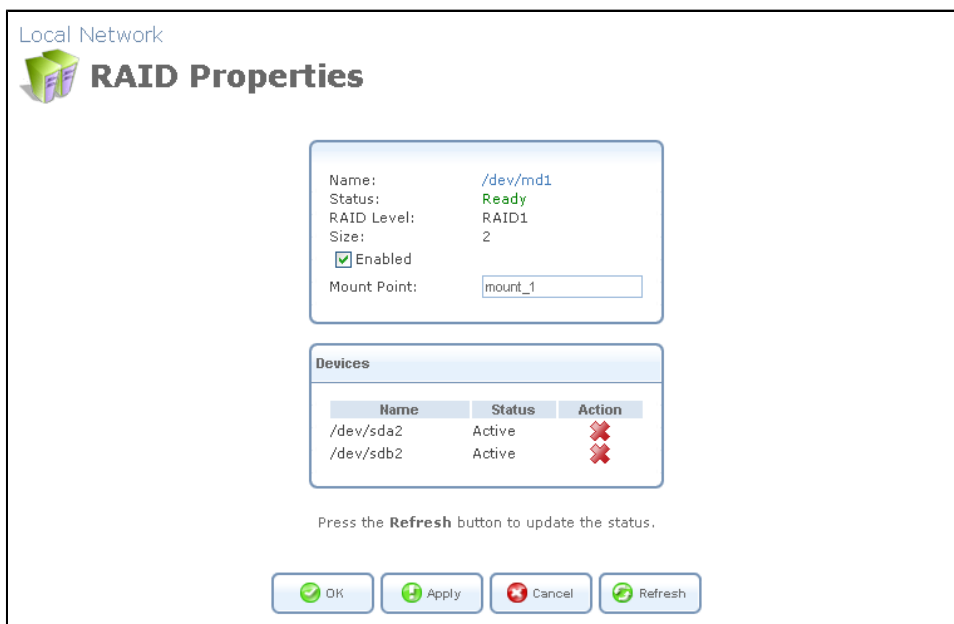


Figure 6.32. RAID Properties

- Maintaining the partition:
 1. Click the device name in the 'RAID Properties' screen (see [Figure 6.32](#)).
 2. The 'Partition Properties' screen appears (see [Figure 6.33](#)), in which you can check and format the RAID partition (refer to [Section 6.4.1.1](#) and [Section 6.4.1.2](#) respectively).




Figure 6.33. Partition Properties

6.4.3.4. Replacing RAID Underlying Devices


Adding or removing a RAID underlying device can only be performed on RAID1 and RAID5 configurations. RAID1 can operate with just one device (although mirroring will not be available), and RAID5 can operate with one device less than its original amount of devices. The names of the RAID underlying devices appear on the 'RAID Properties' screen (see [Figure 6.32](#)). Each device is followed by a status:

- Active: The device is controlled by RAID.
- Inactive: The device failed to join the RAID array or does not exist.
- Faulty: The device joined the RAID array but was marked as faulty due to an error. It is inactive and should be replaced.

Replacing a device on RAID1 or RAID5 is done by first removing the faulty device and then adding a new one. The new device's size must be at least the size of the existing one. To remove a faulty device from RAID1:

1. Click the faulty device's  action icon in the 'RAID Properties' screen (see [Figure 6.32](#)).
2. Click 'OK' to execute the deletion.

To add a new device instead of the one removed:

1. Click the  action icon of the RAID device in the 'Disk Management' screen (see [Figure 6.29](#)).
2. The 'RAID Properties' screen appears, this time with a drop-down menu allowing you to choose the new partition to be added.

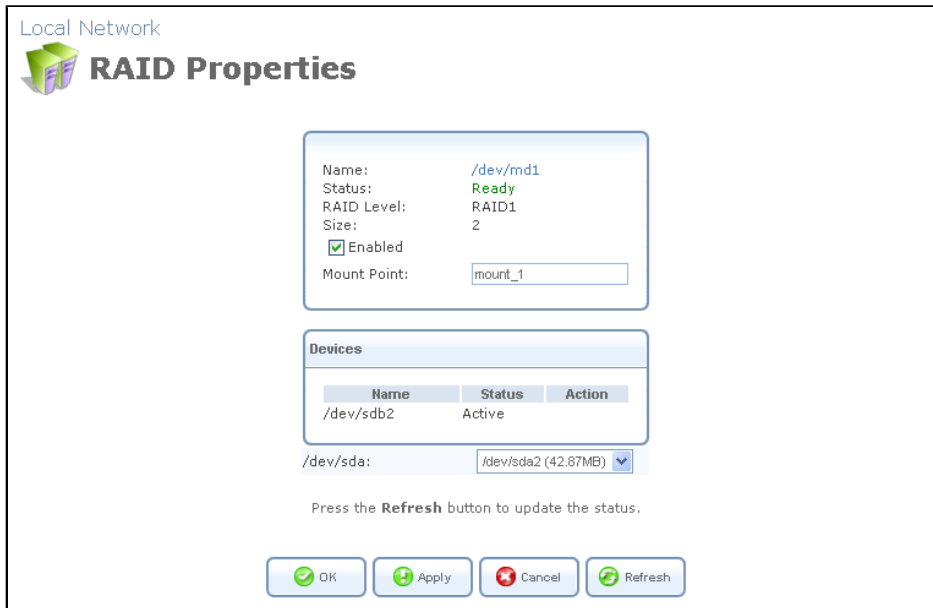


Figure 6.34. RAID Properties

3. Choose the partition and click 'OK' for the changes to take effect.

After adding a new device, RAID1 starts a recovery process in which the content of the existing partition is mirrored to the new device. If the addition or recovery fails, the device status is set to inactive (this status appears in the 'RAID Properties' screen, see [Figure 6.32](#)). In such cases, the device should be removed and another may be added.

You can manipulate your disk partitions using OpenRG's Web-based management. However, it is recommended to configure your disks before setting up RAID. Once RAID is configured, you will not be able to delete an underlying partition, or create a new partition on a disk that one of its partitions is underlying RAID, unless you disable or delete the RAID device. Changing a disk's partition table when its partitions are under RAID (even if RAID is disabled) may result in the need to reconstruct the RAID device.

6.5. Shared Printers

OpenRG includes a print server that enables your LAN users to share printers attached to the gateway via the USB connection. This eliminates the need to physically connect your printer to a dedicated host, which should be shared and always left on. In addition, the print server offers you such advantages as:

- Support for several print protocols, which enable you to connect Windows, Unix and Mac hosts to the network printer.
- Ability to define printer access permissions for specific LAN users.

6.5.1. Configuring the Print Server

Access the printer server settings by clicking the 'Shared Printers' menu item under the 'Local Network' tab. The 'Print Server' screen appears.

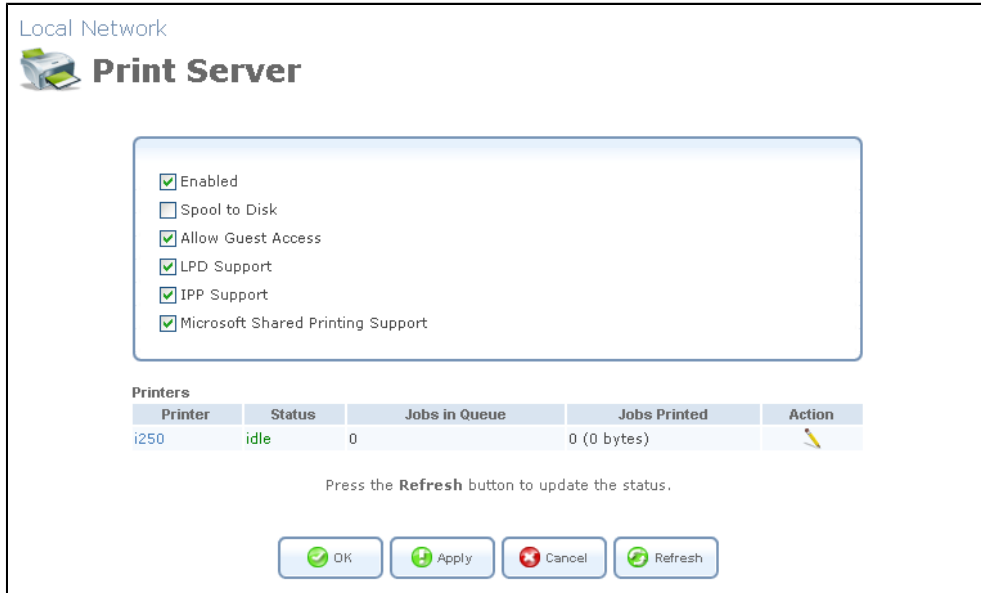


Figure 6.35. Print Server

This screen enables you to configure your print server with the following options:

Enabled Select or deselect this check box to enable or disable this feature.

Spool to Disk Select this check box to temporarily store your print jobs on the disk share, until they are finished. This is especially useful if you would like the printer to process the print job even after you turn the computer off.

Allow Guest Access Select this check box to enable sharing of the printer between all LAN users. You can also share the printer only between specific users, as described in [Section 6.5.4](#).

The next check boxes enable you to define which protocol(s) will be used for connecting the LAN hosts to the printer. OpenRG supports such print protocols as Samba, IPP, and LPD. Prior to selecting a protocol, it is recommended that you read more information about the supported protocols, provided in the next section.

The 'Printers' section of this screen displays the printer(s) connected to OpenRG, their status and print job information. Click a printer's name link to view its details.

When using the Samba protocol, a printer's device mode (responsible for the printing properties) is generated by the printer driver by default. In some cases, this may cause erroneous printer behavior. If you would like the print server to generate a default device mode instead, in the printer's screen, mark the 'Create Default Device Mode' check box and click 'Apply'. Note that if the printer is working properly, it is recommended to leave this check box unchecked. For more information, refer to [Section 6.5.2.2.2](#).

6.5.2. Selecting a Print Protocol

The Samba protocol, with which you can connect a computer to the network printer as described in [Section 2.4.2](#), allows you to upload Windows printer drivers to OpenRG, enabling all Windows-based LAN hosts to connect to the network printer. OpenRG provides two additional protocols for computers to connect to its printers:

1. Internet Printing Protocol (IPP) – A network printing protocol, offering fast installation and ease of use (refer to [Section 6.5.2.1](#)).
2. Line Printer Daemon (LPD) – A legacy network printing protocol, which should only be used for printing from computers that do not support IPP (refer to [Section 6.5.2.3](#)).

The following table compares the specifications of the three protocols:

Specification	IPP	Samba	LPD
Installation	Easy	Easy	Difficult
Driver upload	None	Supported	None
Supported clients	Windows, Unix, Mac	Windows, Mac	Windows, Unix, Mac
Job feedback and control	Print queue monitor and management console	Print queue monitor and management console	Management console only
Printer control	Print queue monitor	None	None
Access controls	Print and administrator	Print and administrator	None

Table 6.1. IPP, Samba, and LPD Specifications



Important Note For Mac Users: When connecting a print server to a Mac computer, you must verify that the printer connected to the gateway is supported by Mac OS as a network printer. Supported printers are marked with an "X" in the following URL: <http://docs.info.apple.com/article.html?artnum=301175#hpdrivers>. The scenarios in this chapter have been tested with Mac OS version 10.4.4.

6.5.2.1. Internet Printing Protocol (IPP)

The IPP protocol enables you to connect any Windows, Linux or Mac-based LAN host to the network printer. The following sections provide the relevant guidelines for each of these operating systems.

6.5.2.1.1. Setting Up an IPP Printer on Windows

1. In the 'Network Map' screen under 'Home', click the printer icon to view the 'Printer' screen.
2. Copy the IPP URL to the clipboard.

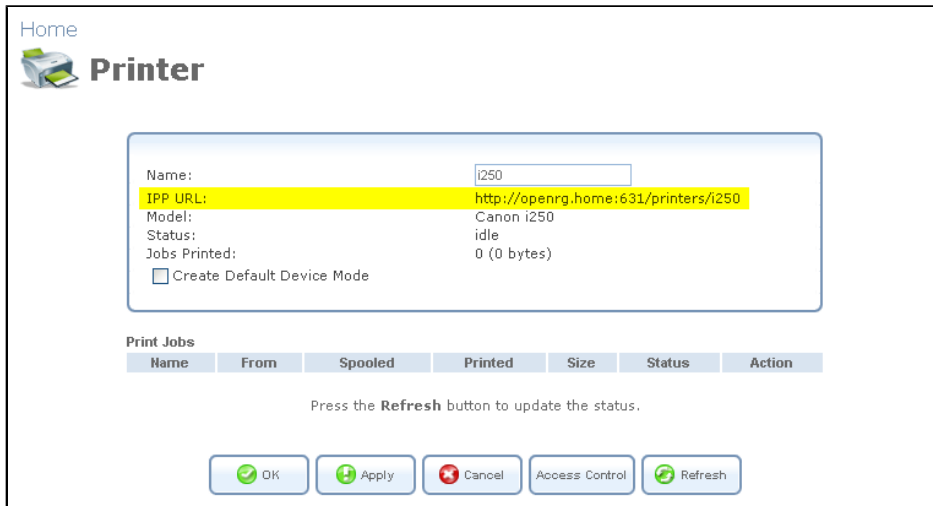


Figure 6.36. Printer

3. On your Windows computer connected to OpenRG, open the 'Printers and Faxes' utility from the 'Settings' menu under 'Start'.
4. Click the 'Add a printer' link to activate the 'Add Printer Wizard'.
5. Click 'Next' to proceed with the wizard sequence.
6. Select 'Network Printer' and click 'Next'.

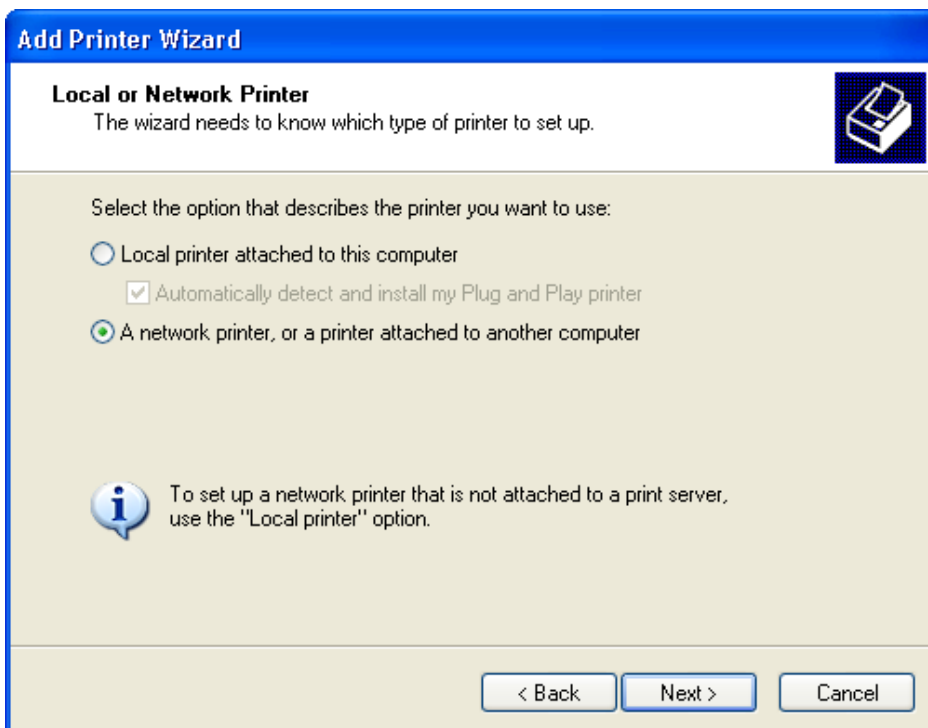


Figure 6.37. Local or Network Printer

7. Select 'Connect to a printer on the Internet'.

8. Paste the printer's IPP URL in the 'URL' field, and click 'Next'.

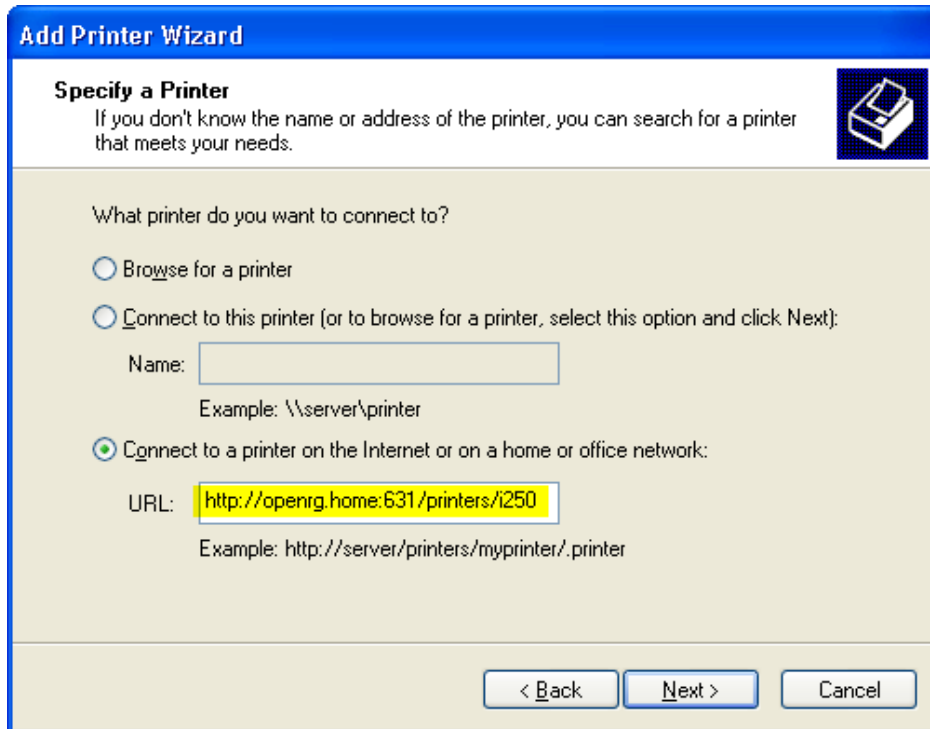


Figure 6.38. Specify a Printer

9. You may be asked to select the driver's make and model or its location. If so, provide the driver location, and click 'Next'.
10. Click 'Finish' to exit the wizard.

6.5.2.1.2. Setting Up an IPP Printer on Linux

You should use CUPS Daemon (CUPSD) when working with Linux operating systems.

1. In the 'Network Map' screen under 'Home', click the printer icon to view the 'Printer' screen.
2. Copy the IPP URL to the clipboard.

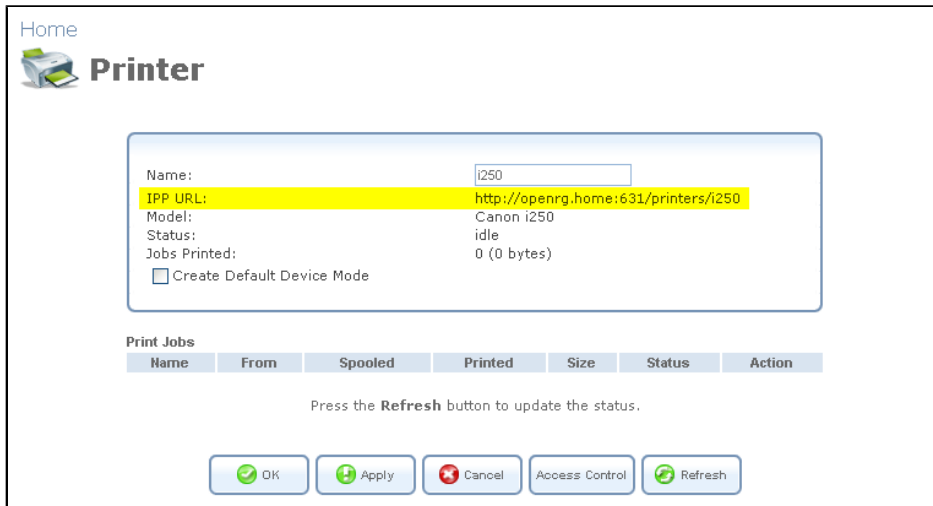


Figure 6.39. Printer

3. On your Linux computer connected to OpenRG, browse to: `http://localhost:631` and choose the 'Manage Printers' link.

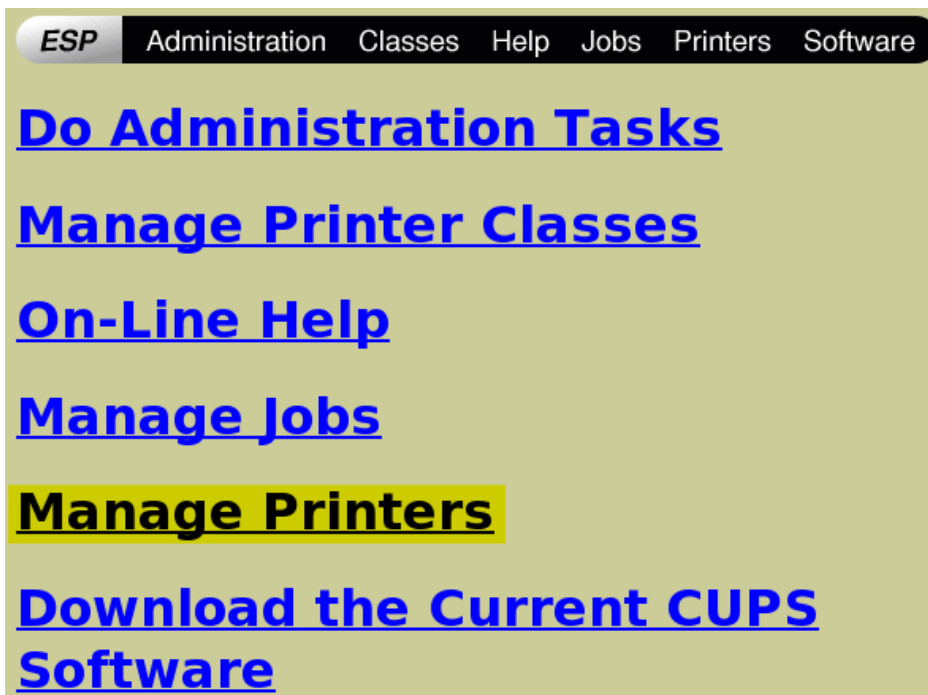


Figure 6.40. Linux CUPS Management

4. Scroll to the bottom of the page and click the 'Add Printer' link.



Figure 6.41. Add Printer

5. Type the printer's name in the 'Name' field and click 'Continue'.

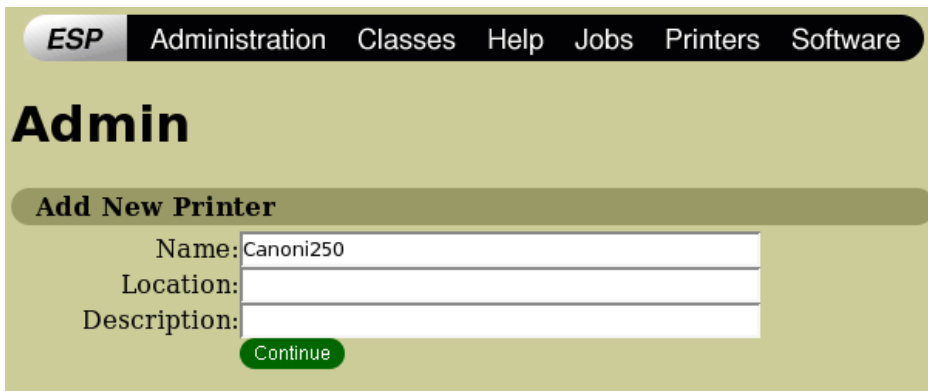


Figure 6.42. Printer Name

6. From the 'Device' drop-down menu, select 'Internet Printing Protocol (http)' and click 'Continue'.

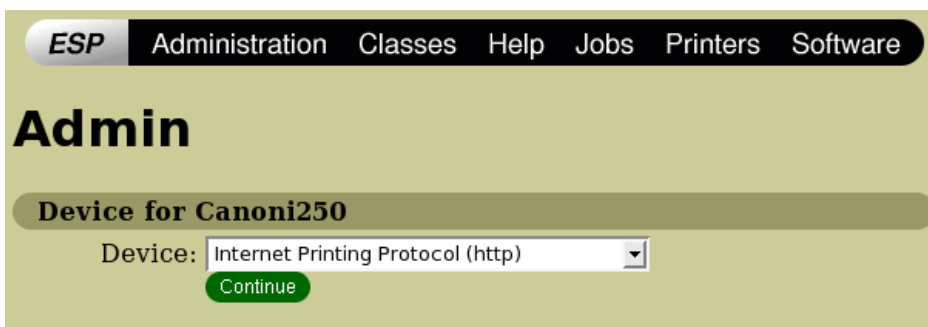


Figure 6.43. Printing Protocol

7. Paste the printer's IPP URL in the 'Device URL' field, and click 'Continue'.

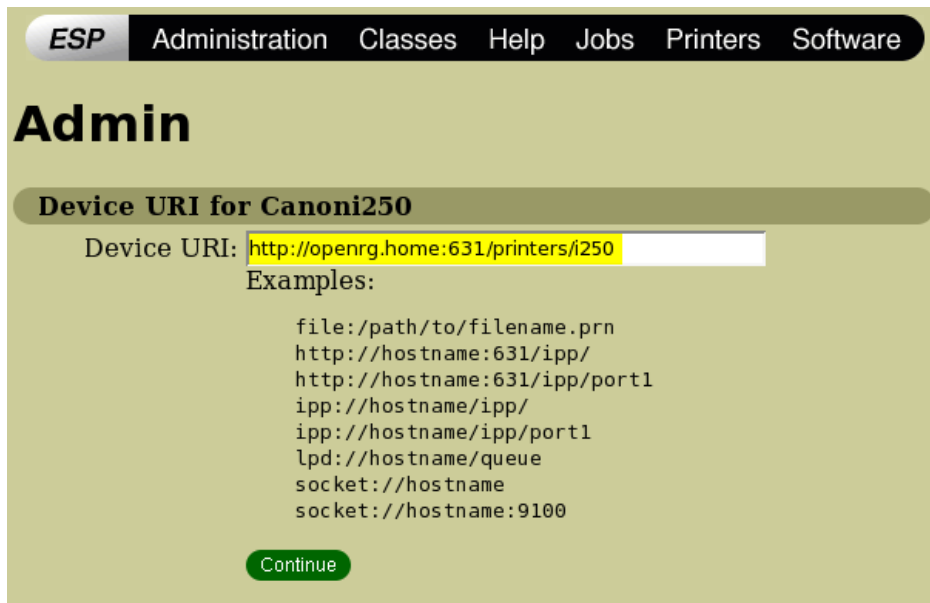


Figure 6.44. IPP URL

8. The next window displays a manufacturer drop-down menu. Select your printer's manufacturer and click 'Continue'.
9. The next window displays a printer model drop-down menu. Select your printer's model and click 'Continue'.
10. The last window displays the following confirmation message: 'Printer has been added successfully'.
11. To test your printer's connection from a Linux PC, open a shell and enter the following command:

```
$ echo hello | lpr -P<Printer Name>
```

6.5.2.1.3. Setting Up an IPP Printer on Mac

1. On your Mac computer connected to OpenRG, open the 'Print & Fax' utility from 'System Preferences'. The 'Print & Fax' screen appears.

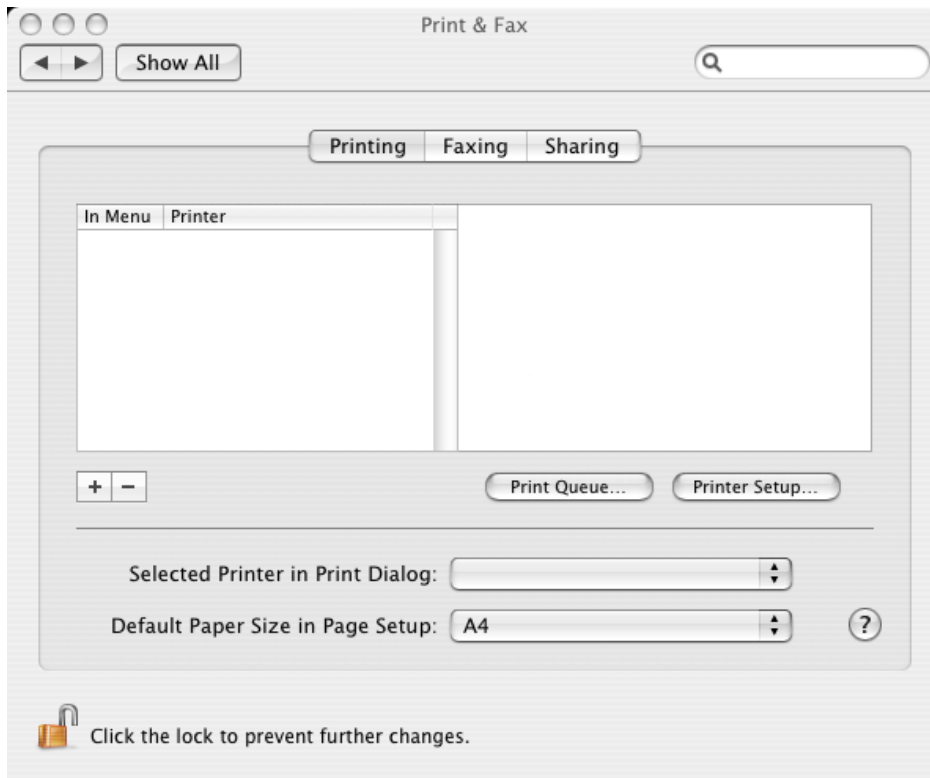


Figure 6.45. Print & Fax

2. Click the '+' (add) button. The 'Printer Browser' screen appears. Select its 'IP Printer' tab.
3. In this screen, configure the following:
 - a. From the 'Protocol' drop-down menu, select IPP.
 - b. In the 'Address' field, enter OpenRG's IP address (192.168.1.1).
 - c. In the 'Queue' field, enter the section of the path containing the folder and printer names, as it appears in the 'Printer' screen of the WBM (see [Figure 6.69](#)). For example, **/printers/MFC9750**.
 - d. The 'Name' and 'Location' fields are optional; the default name is the gateway's IP address.
 - e. From the 'Print Using' drop-down menu, select your printer's make and model.

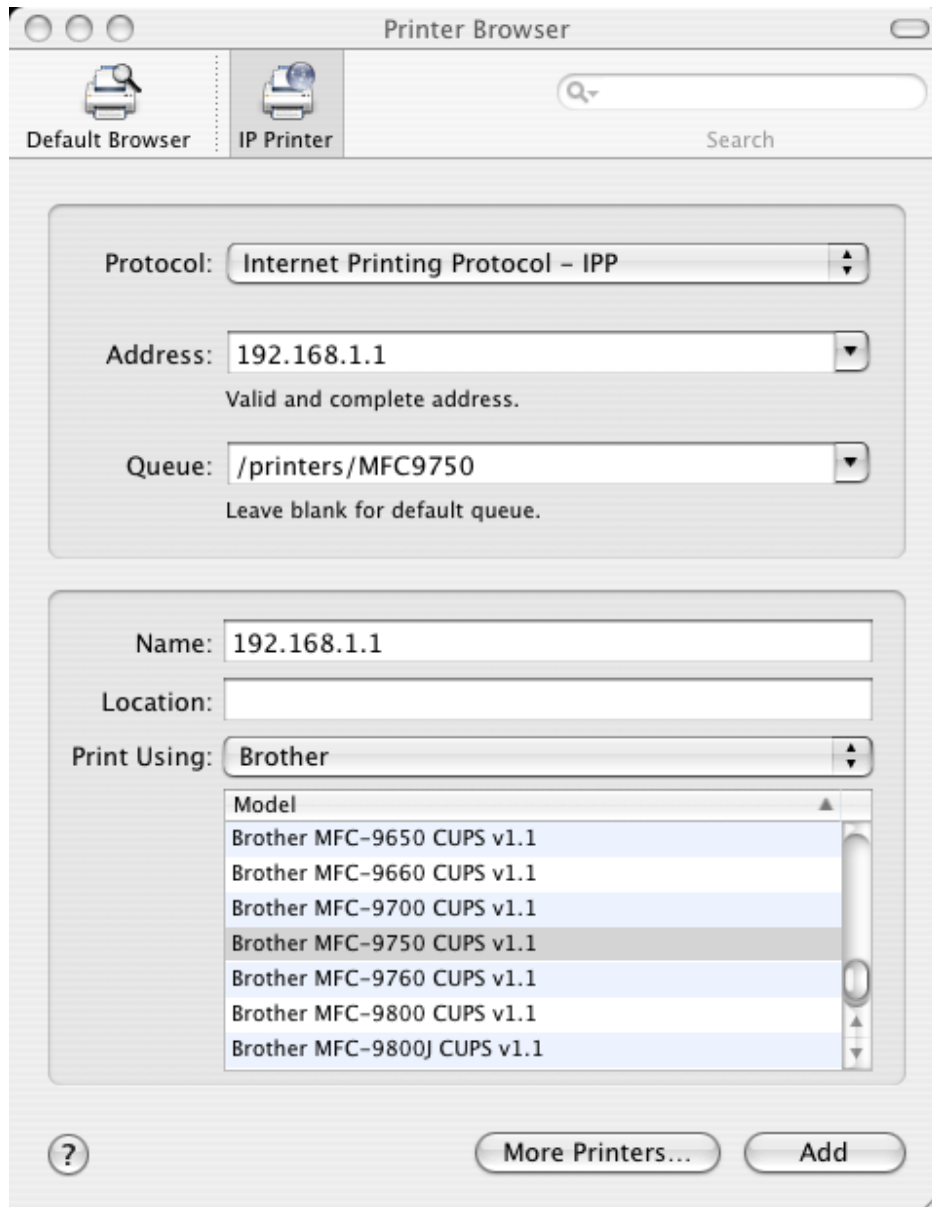


Figure 6.46. Printer Browser – IP Printer

4. Click the 'Add' button. The new printer appears in the 'Print & Fax' screen.

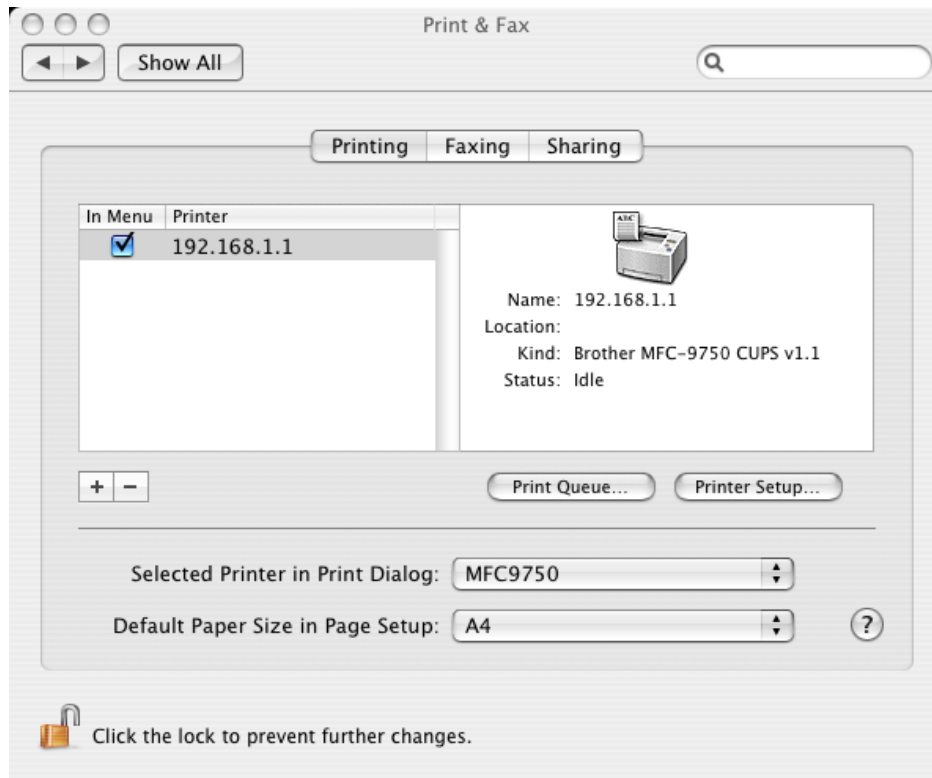


Figure 6.47. Print & Fax – New IPP Printer

6.5.2.1.4. Troubleshooting

- The printer does not respond to printing requests.
 1. Ensure that the print server is enabled: click the "Print Server" icon under "Advanced" in the management console. The first option, "Enabled" should be checked.
 2. The management console screen should show diagnostic information for printer and jobs.
 3. Restart the printer.

6.5.2.2. Microsoft Shared Printing (Samba)

The Samba protocol enables you to connect Windows and Mac hosts to the network printer. To learn how to connect the Samba printer to a Windows host, refer to [Section 2.4.2.1](#). If you are a Mac user, refer to [Section 6.5.2.2.1](#).

6.5.2.2.1. Setting Up a Samba Printer on Mac

1. On your Mac computer connected to OpenRG, open the 'Print & Fax' utility from 'System Preferences'. The 'Print & Fax' screen appears.

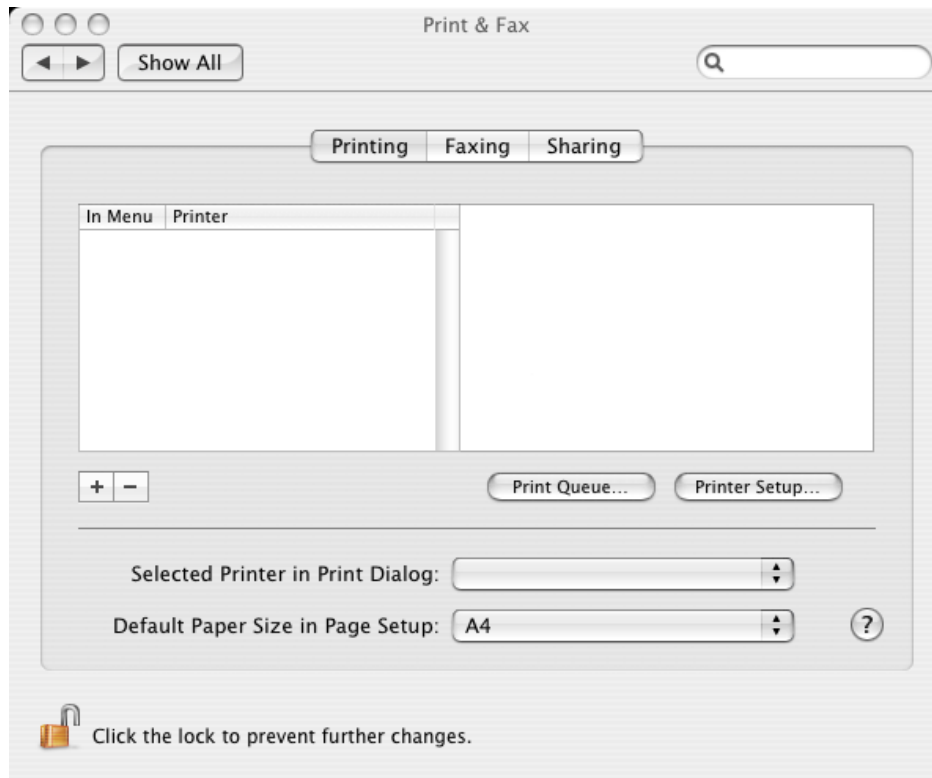


Figure 6.48. Print & Fax

2. Click the '+' (add) button. The 'Printer Browser' screen appears.

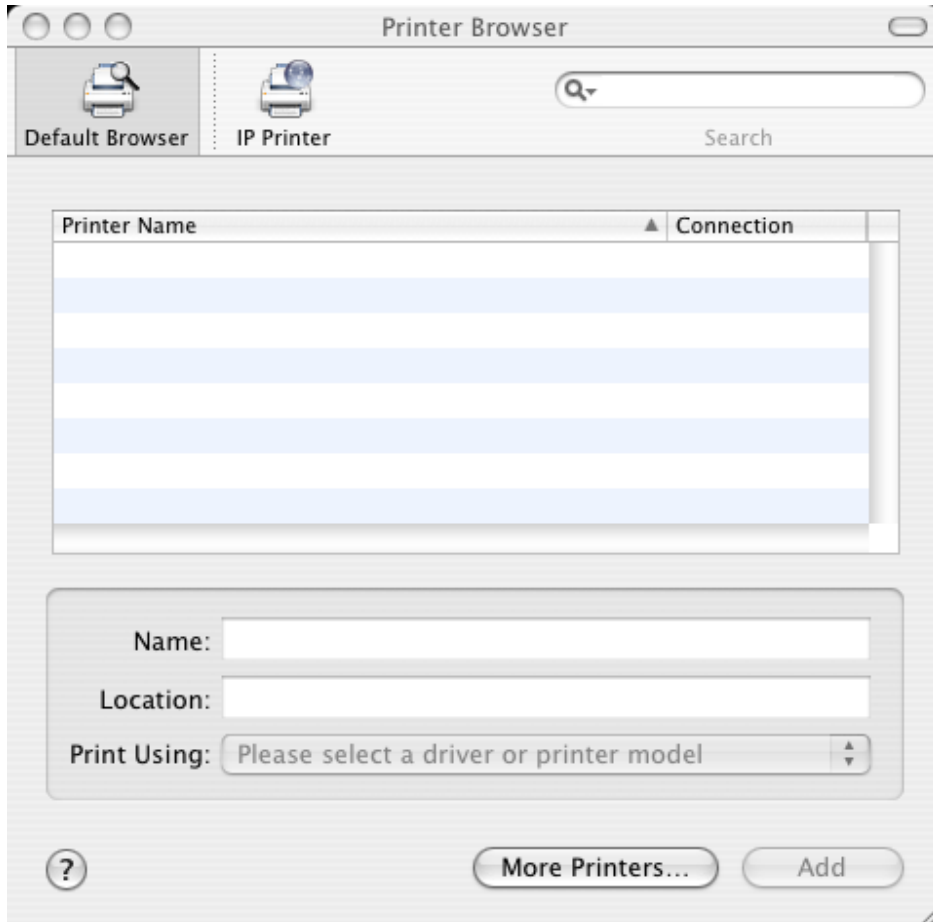


Figure 6.49. Printer Browser – Default Browser

3. Click the 'More Printers...' button. The following screen appears.

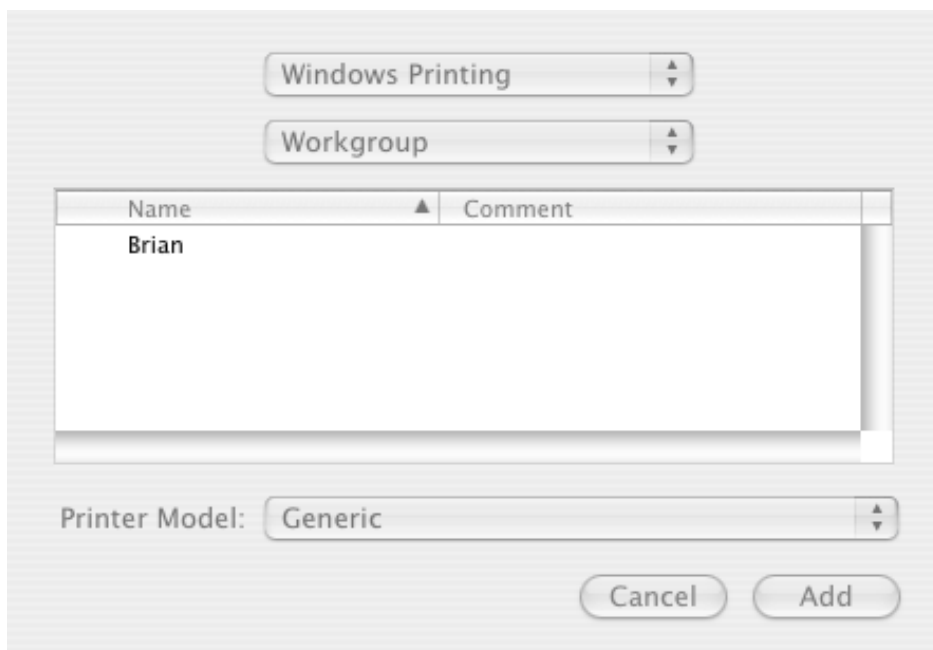


Figure 6.50. Printer Browser – More Printers

4. In the second drop-down menu, select 'Network Neighborhood'.

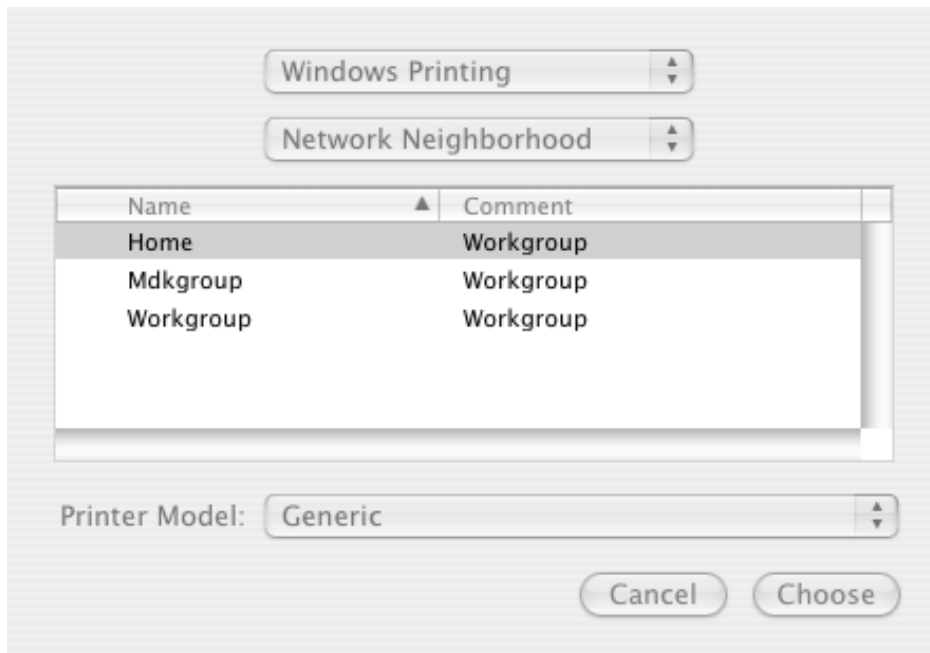


Figure 6.51. Printer Browser – Network Neighborhood

5. Select the 'Home' workgroup and click 'Choose'.

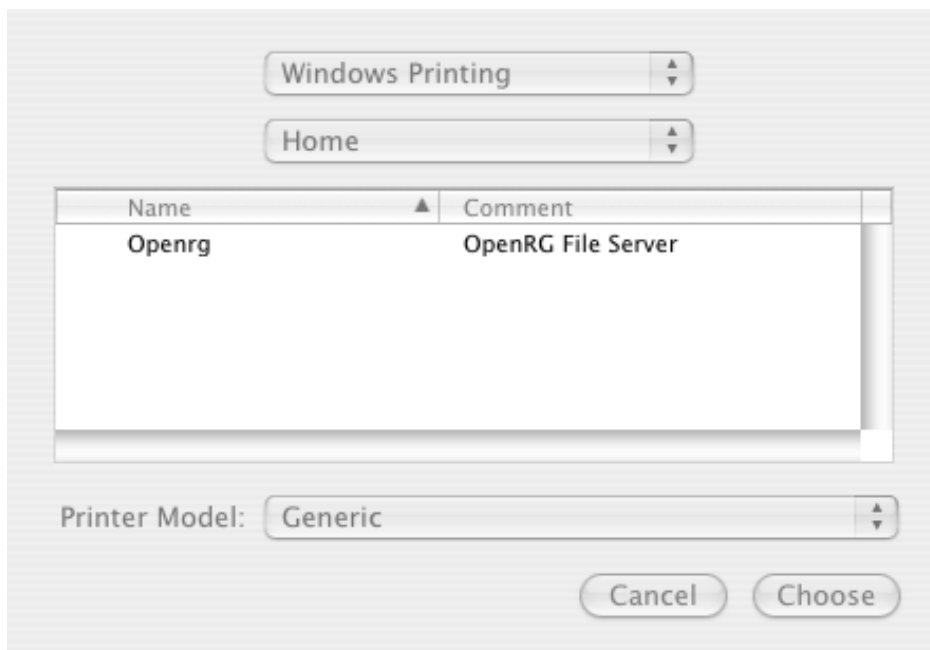


Figure 6.52. Printer Browser – Home

6. Select OpenRG and click 'Choose'.

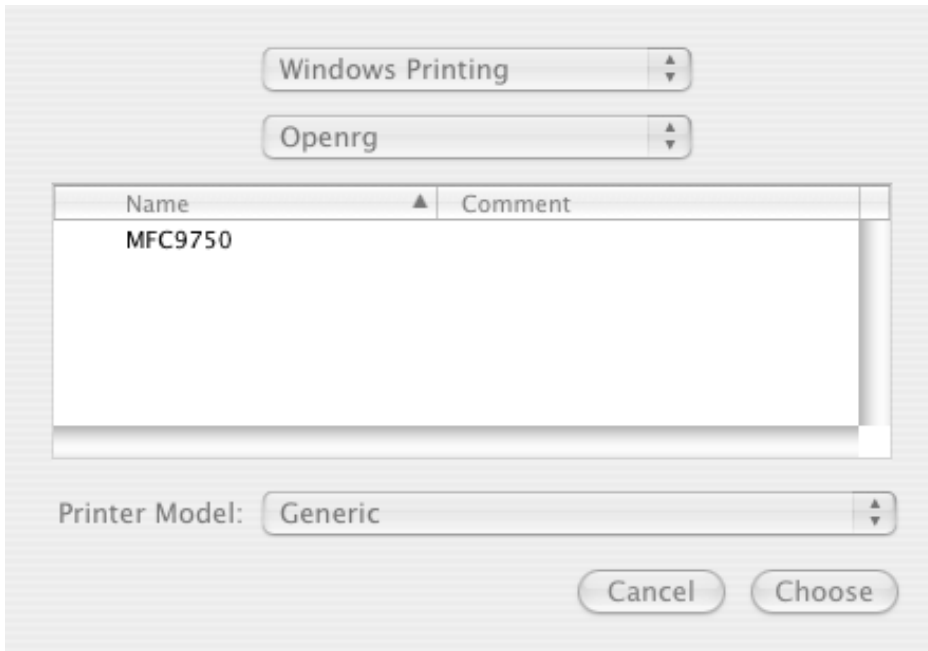


Figure 6.53. Printer Browser – OpenRG

7. Select the printer, and in the 'Printer Model' drop-down menu, select your printer's make and model.

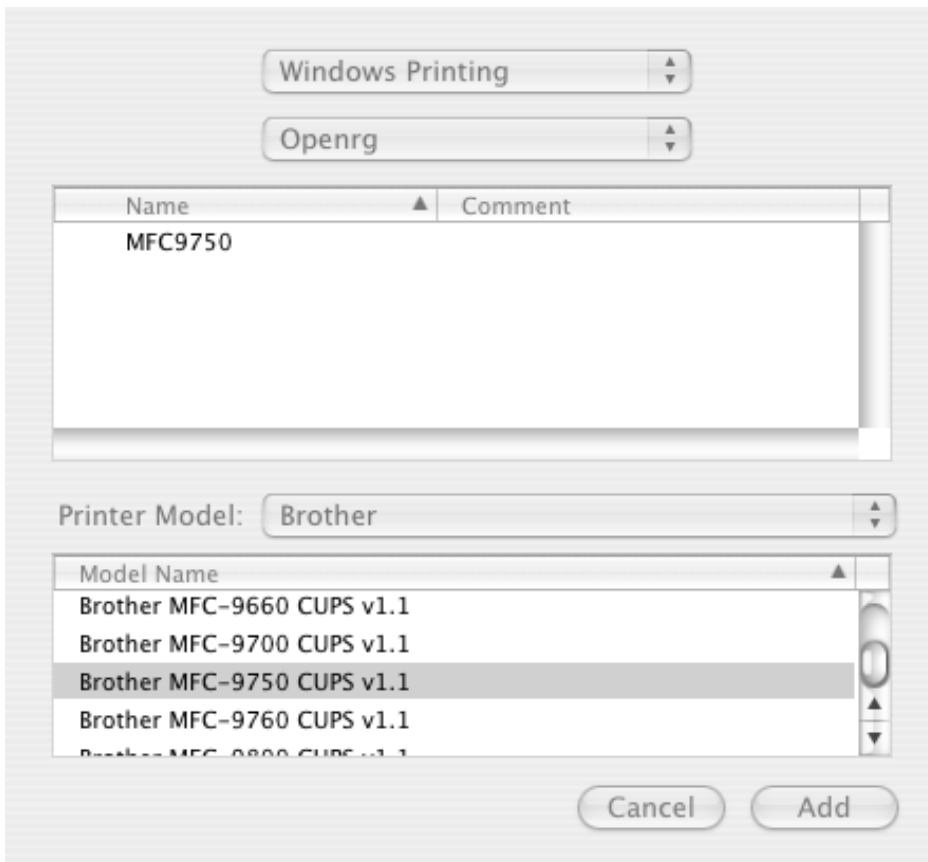


Figure 6.54. Printer Browser – Printer Model

8. Click the 'Add' button. The new printer appears in the 'Print & Fax' screen.

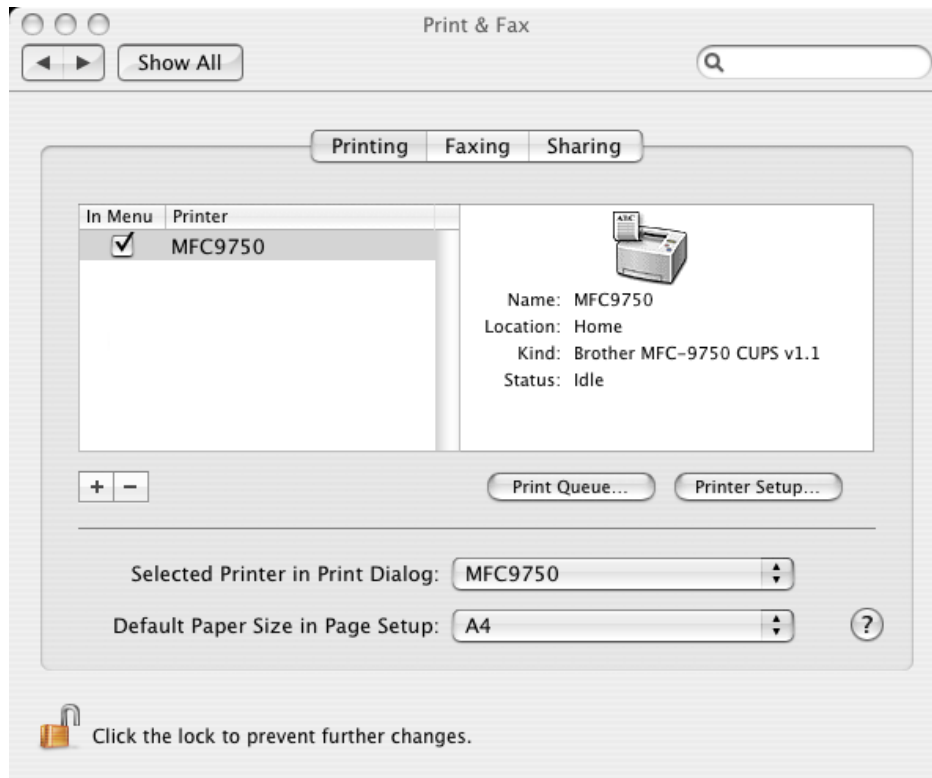


Figure 6.55. Print & Fax – New Samba Printer

6.5.2.2.2. Troubleshooting

- The printer does not respond to printing requests.
 1. Ensure that the print server is enabled: click the "Print Server" icon under "Advanced" in the management console. The first option, "Enabled" should be checked.
 2. The management console screen should show diagnostic information for printer and jobs.
 3. Restart the printer.
- When trying to access the properties page of the printer from Windows, the following error message appears: "Function address 0xXXXXXXXX caused a protection fault (exception code 0xc0000005). Some or all property page(s) may not be displayed."
 1. This message appears in some cases, for example when using the HP DeskJet 3550 printer. It indicates that the printer driver does not have a default device mode, and that the print server should create one for it. To solve the problem, take the following steps:
 - a. Delete the printer drivers from Windows.
 - b. In OpenRG's WBM, browse to the printer screen and select the 'Create Default Device Mode' option.

- c. Log off or reboot Windows.
 - d. Try to reinstall the shared printer. It will obtain the default properties from the print server.
- Windows/Internet Explorer crashes since the printer driver was installed.
 1. Most problems with serving printer drivers for Windows NT/2000/XP clients are associated with the generated device mode. Certain drivers may cause **Explorer.exe** to crash with a NULL devmode. However, other printer drivers can cause the client's spooler service (**spoolsv.exe**) not to operate if the devmode was not created by the driver itself (i.e. OpenRG generates a default devmode).
 2. The default devmode parameter should be used with care and tested with the printer driver in question. It is better to leave the device mode to NULL and let Windows set the correct values. Since drivers seldom do this, setting default devmode=yes will instruct OpenRG to generate a default one.
 3. When OpenRG is serving printer drivers for Windows NT/2000/XP clients, each printer on the Samba server has a device mode defining settings such as paper size, orientation and duplex settings. The device mode can only be generated correctly by the printer driver itself (which can only be executed on a Win32 platform). Because OpenRG is unable to execute the driver code to generate the device mode, the default behavior is not to enable the creation of a default device mode.
 - When trying to print from a Windows computer, an error message informs you that the printer is not properly configured. This problem may happen with some printers, such as Lexmark Z55, Lexmark Z645, and some Epson models. To fix this problem, perform the following:
 1. In the 'Start' menu, click 'Settings' and select 'Printers and Faxes'.
 2. Right-click on the printer's name and select 'Properties'.
 3. Select the 'Advanced' tab and click the 'Print Processor' button.
 4. In the 'Default Data Type' list, select 'RAW'. If this setting does not appear in the list, select the 'WinPrint' print processor and then its 'RAW' setting.
 5. Click 'OK' to save the settings.

6.5.2.3. Line Printer Daemon (LPD)

The following sections describe how to connect an LPD printer to a Windows and Mac host.

6.5.2.3.1. Setting Up an LPD Printer on Windows

Before configuring the LPD protocol on a LAN PC, ensure that a print driver for the specific printer is installed.



Note: The following configuration must be applied to each LAN PC individually in order to use the network printer.

1. Open the 'Printers and Faxes' utility from the 'Settings' menu under 'Start'.
2. Click the 'Add a printer' link to activate the 'Add Printer Wizard'.
3. Click 'Next' to proceed with the wizard sequence.
4. Select 'Local printer attached to this computer'.
5. Deselect 'Automatically detect and install my Plug and Play printer', and click the 'Next' button.

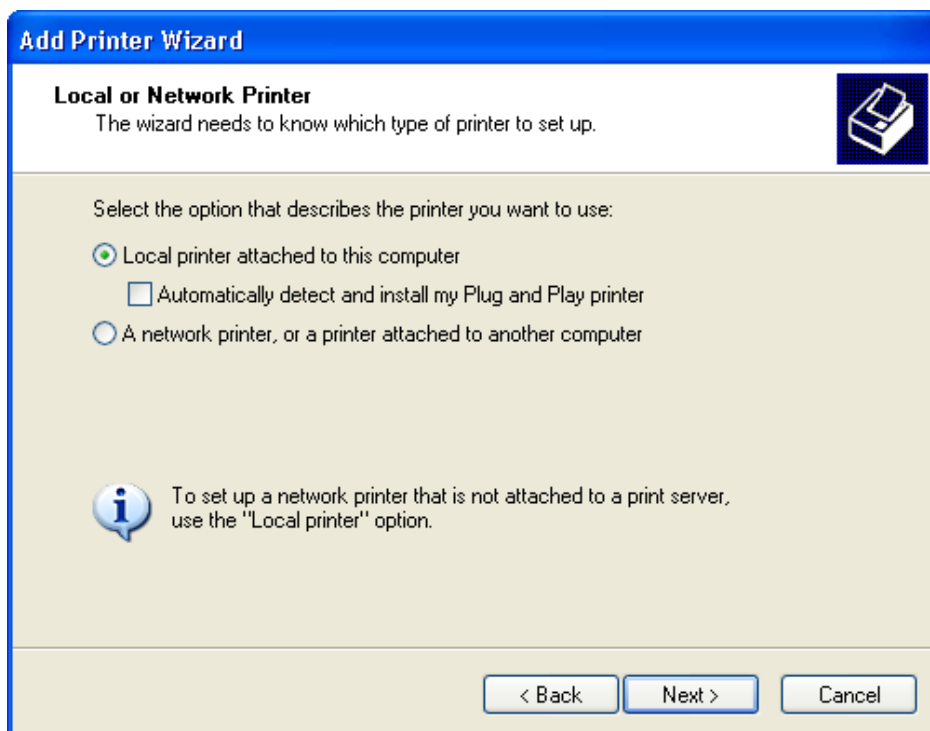


Figure 6.56. Local or Network Printer

6. In the 'Select a Printer Port' screen, select the 'Create a new port' radio button.

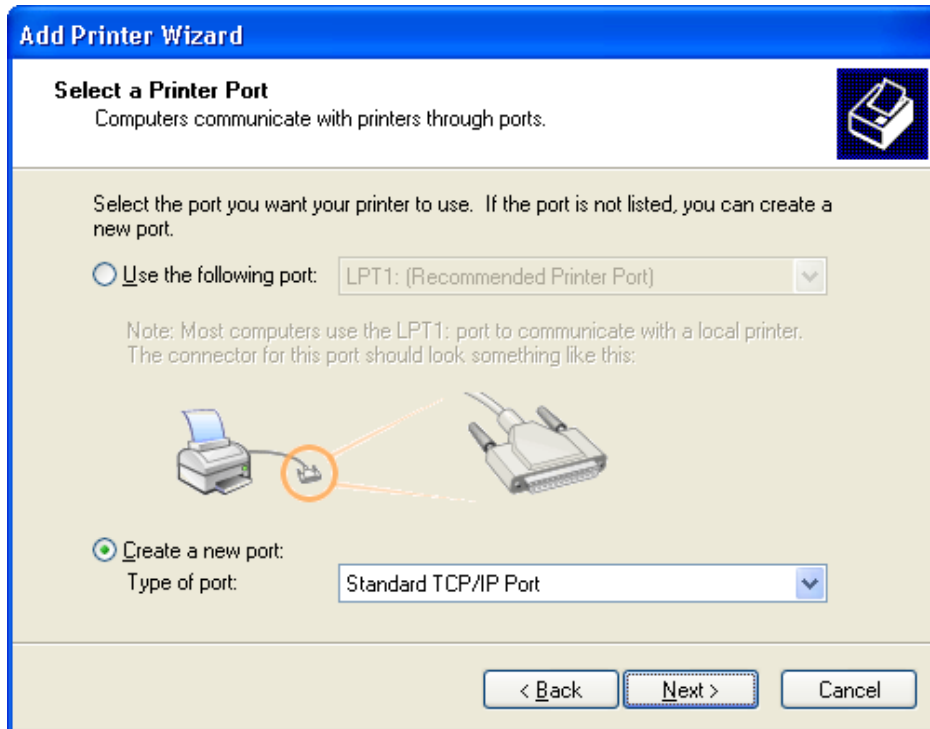


Figure 6.57. Select a Printer Port

7. From the 'Type of port' drop-down menu, select 'Standard TCP/IP Port'.
8. Click 'Next' to activate the 'Add Standard TCP/IP Printer Port Wizard'.
9. Click 'Next' to proceed with the new wizard.
10. Specify 192.168.1.1 in the 'Printer Name or IP Address' field, and click the 'Next' button.

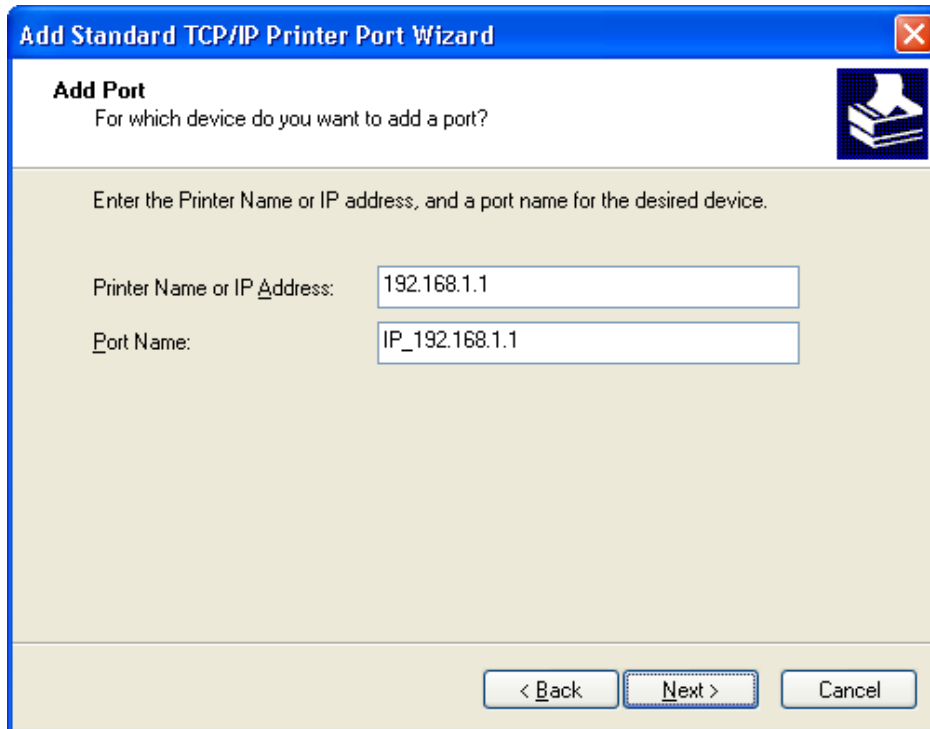


Figure 6.58. Add Port

11. Select the 'Custom' radio button, and click the 'Settings' button.

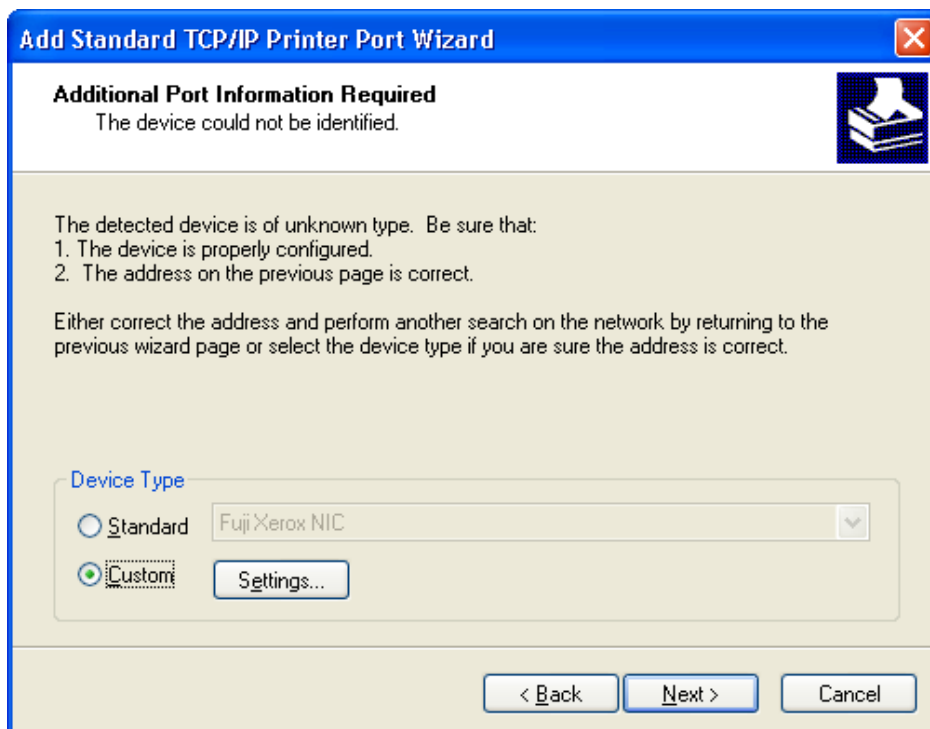


Figure 6.59. Additional Port Information

12. In the 'Configure Standard TCP/IP Port Monitor' window that appears (see [Figure 6.60](#)), configure the following parameters:

- a. Select the 'LPR' radio button.
- b. In OpenRG's management console, click the printer icon on the network map screen to view the 'Printer' screen (see [Figure 6.69](#)).
- c. Copy the printer's name (for example, "i250") and paste it in the 'Queue Name' field of the port monitor configuration window.

Configure Standard TCP/IP Port Monitor

Port Settings

Port Name: IP_192.168.1.1

Printer Name or IP Address: 192.168.1.1

Protocol

Raw LPR

Raw Settings

Port Number: 9100

LPR Settings

Queue Name: i250

LPR Byte Counting Enabled

SNMP Status Enabled

Community Name: public

SNMP Device Index: 1

OK Cancel

Figure 6.60. Printer Port Monitor Configuration

13. Click 'OK' to proceed.
14. Click the 'Finish' button. The 'Add Printer Software' wizard reappears.

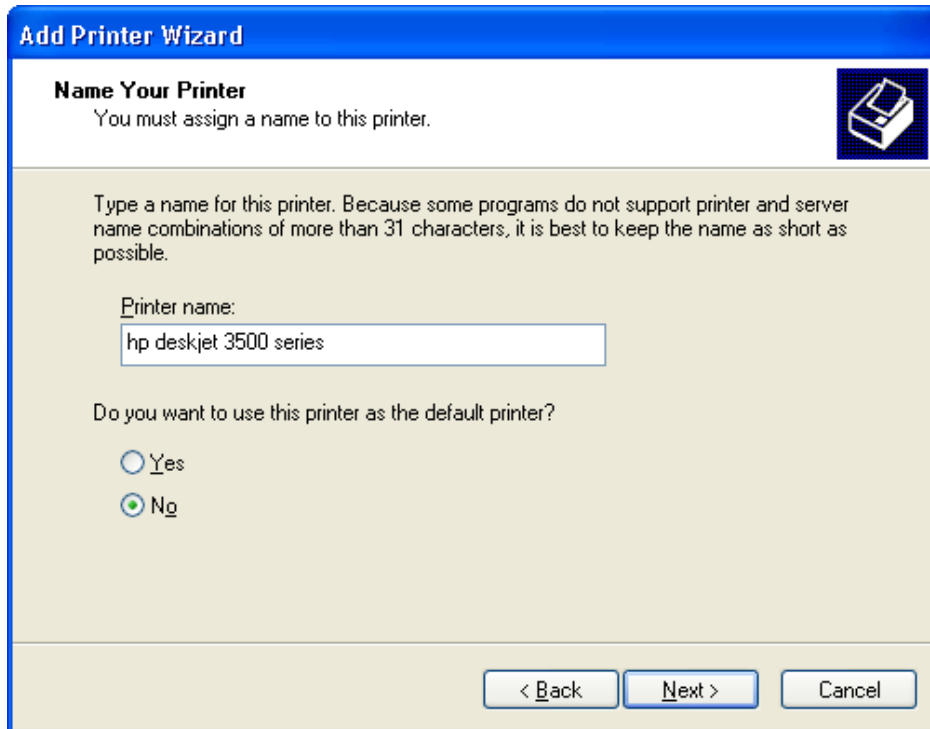


Figure 6.61. Add Printer Wizard

15. Select your printer manufacturer and model from the lists. If it does not appear in the lists, click 'Have disk' to specify the driver location.
16. Specify the name you want to give the printer, and whether you want it to be the default printer. Click 'Next'.

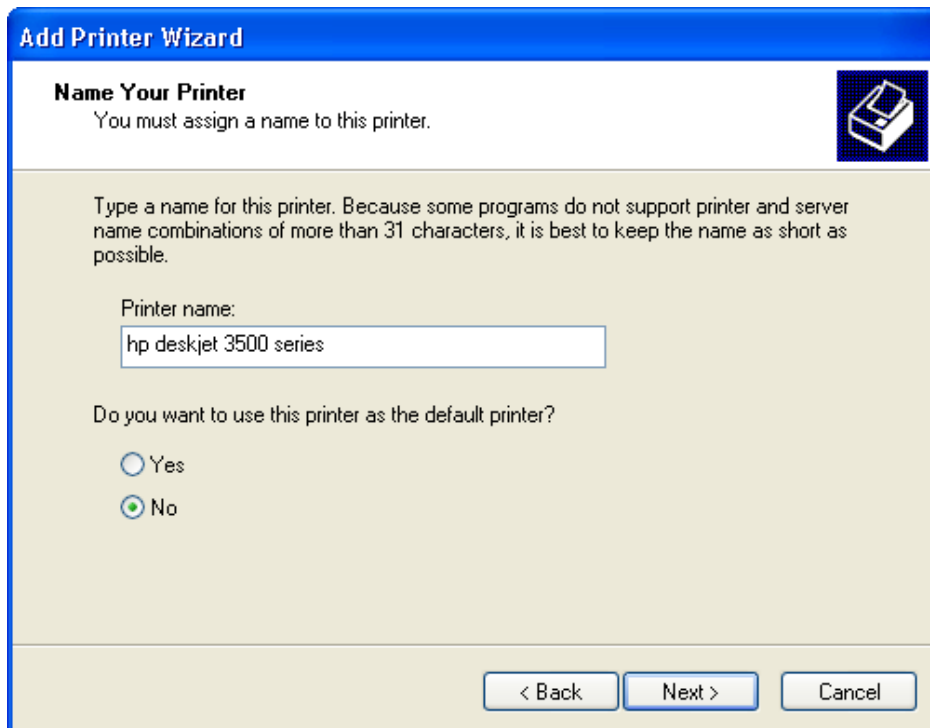


Figure 6.62. Add Printer Wizard

17. Click the 'Next' button to proceed to the final wizard screen.
18. Select 'Yes' to print a test page.
19. Click the 'Finish' button to complete the setup procedure.

6.5.2.3.2. Setting Up an LPD Printer on Mac

1. On your Mac computer connected to OpenRG, open the 'Print & Fax' utility from 'System Preferences'. The 'Print & Fax' screen appears.

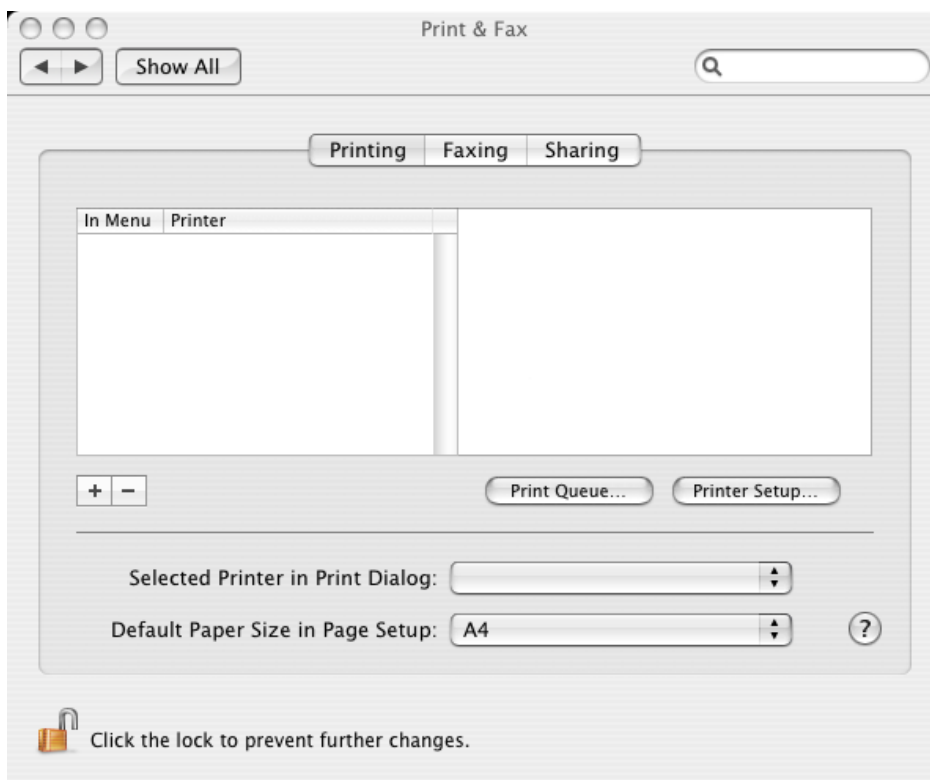


Figure 6.63. Print & Fax

2. Click the '+' (add) button. The 'Printer Browser' screen appears. Select its 'IP Printer' tab.
3. In this screen, configure the following:
 - a. From the 'Protocol' drop-down menu, select LPD.
 - b. In the 'Address' field, enter OpenRG's IP address (192.168.1.1).
 - c. In the 'Queue' field, enter the printer's name as it appears in the 'Printer' screen of the WBM (see [Figure 6.69](#)). For example, **MFC9750**.
 - d. The 'Name' and 'Location' fields are optional; the default name is the gateway's IP address.
 - e. From the 'Print Using' drop-down menu, select your printer's make and model.

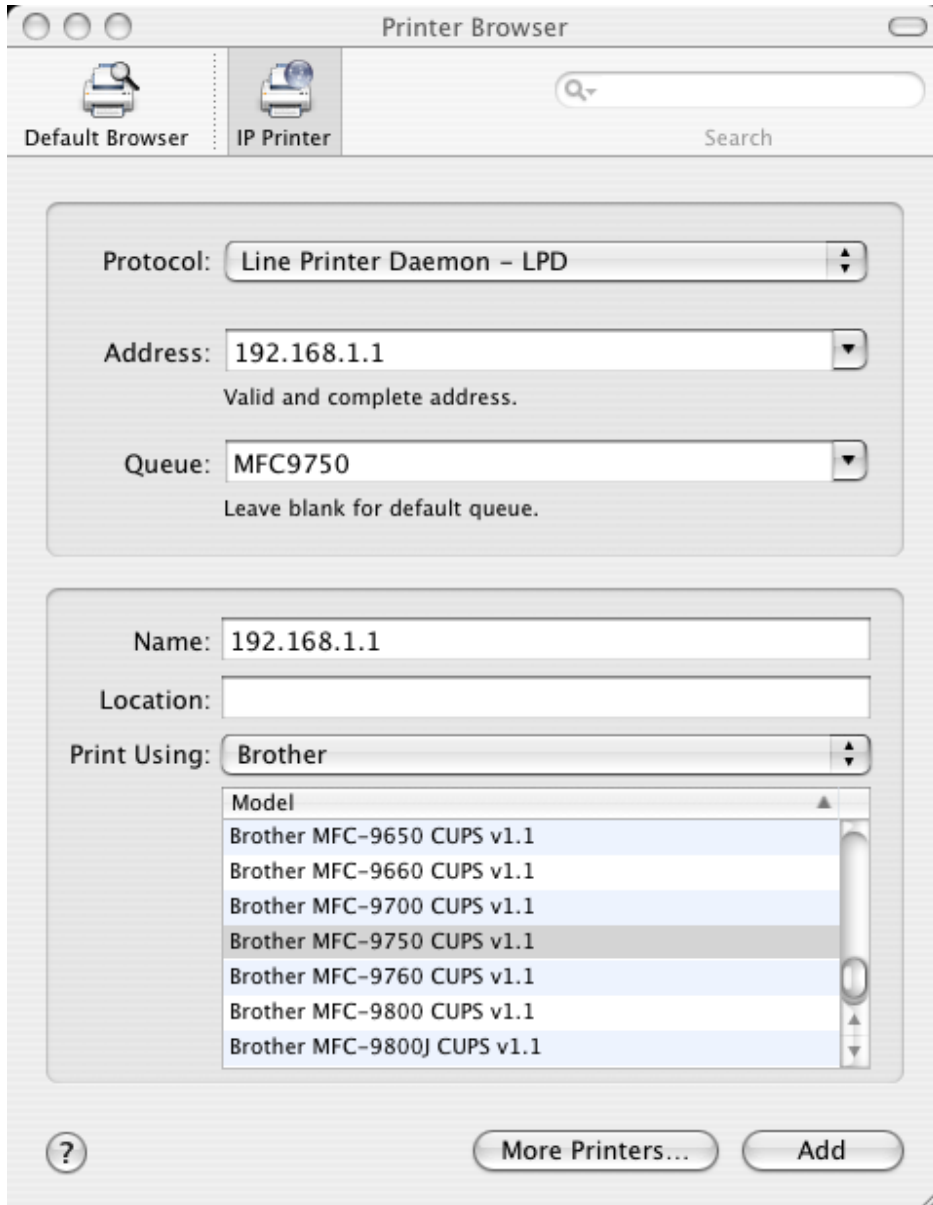


Figure 6.64. Printer Browser – LPD Printer

4. Click the 'Add' button. The new printer appears in the 'Print & Fax' screen.

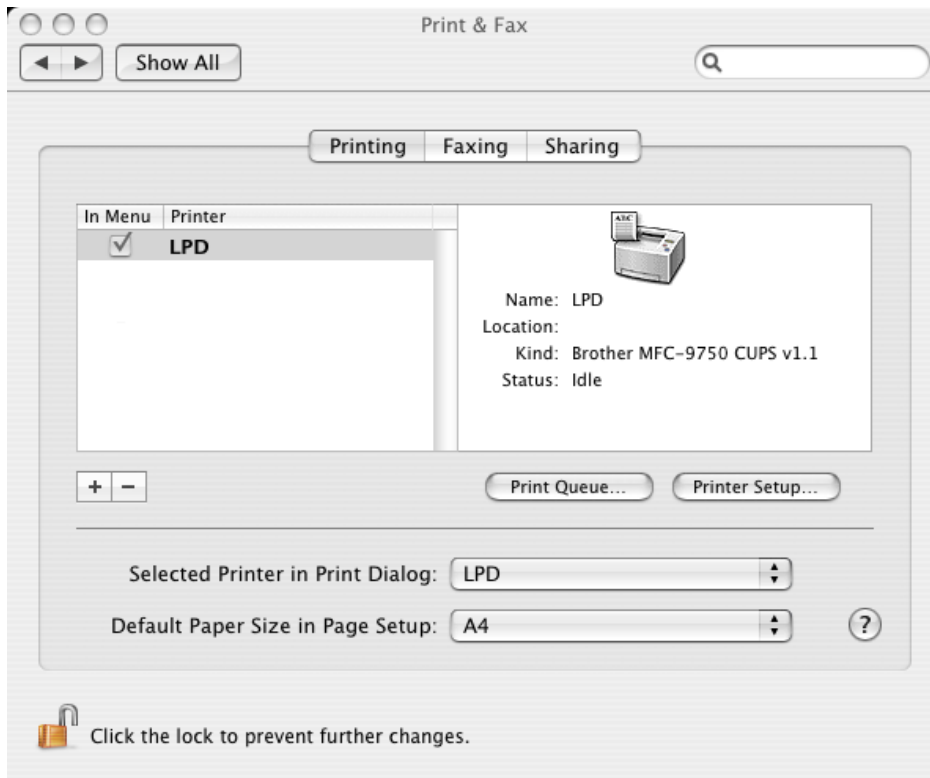


Figure 6.65. Print & Fax – New LPD Printer

6.5.2.3.3. Troubleshooting

- The printer does not respond to printing requests.
 1. Ensure that the print server is enabled: click the "Print Server" icon under "Advanced" in the management console. The first option, "Enabled" should be checked.
 2. The management console screen should show diagnostic information for printer and jobs.
 3. Restart the printer.

6.5.3. Sharing a Samba Printer Driver

As explained earlier in this chapter, in order to use a shared printer connected to OpenRG, a driver for the printer must be installed on the LAN computer from which the print job is to be sent. If your gateway contains a permanent storage device, you can use OpenRG's file server to store printer drivers.

The drivers should be uploaded from a Windows computer and stored in the system storage area that you have created on one of the disk partitions (refer to [Section 6.4.2](#)). The printer can then be installed on other LAN computers using the driver stored on OpenRG. To upload the driver files:

1. Under the Windows 'Start' menu, click 'Run' and type "cmd" to open a command shell.
2. Type "net use" to see the list of shares and their status. The output may be similar to the following.

```

Status      Local      Remote      Network
-----
OK          \\openrg\share-B      Microsoft Windows Network
The command completed successfully.

```

3. Type "net use /del \\openrg\share-B" to delete the specific network mapping entry.



Note: Alternatively, you can use "net use /del *" to delete all network mapping entries. Caution: This command presents no warning.

4. Type "net use * \\openrg\print\$ [Admin's password] [/user:admin]". This ensures that you are logged into the print server using the Admin user and have the permissions to upload files. The output should be similar to the following.

```

Drive Z: is now connected to \\openrg\print$.
The command completed successfully.

```

5. Browse to \\openrg (use a Windows Explorer window if you are using a browser other than Internet Explorer). Should a Windows login dialog box appear, enter your WBM username and password. The following window appears.

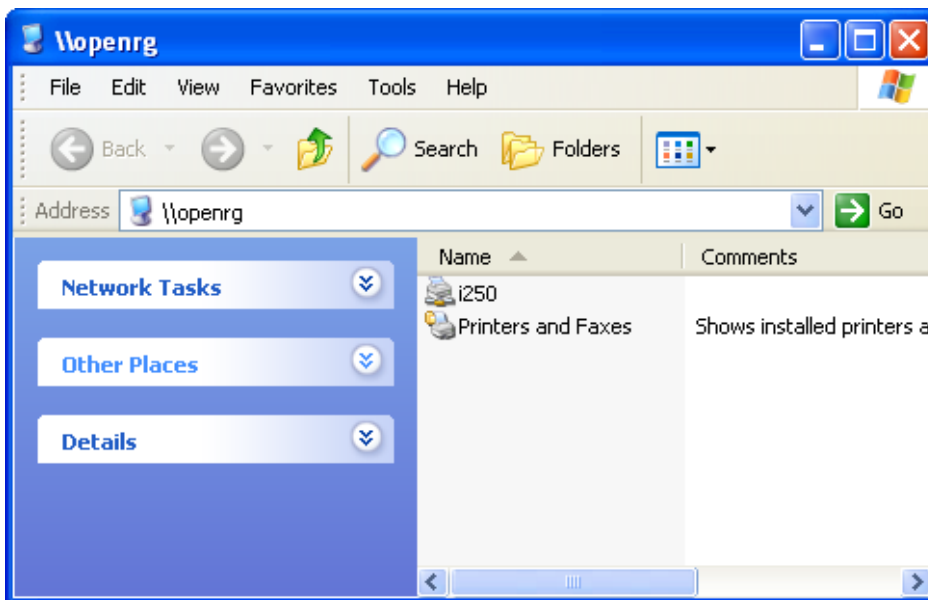


Figure 6.66. OpenRG Shares

6. Click 'Printers and Faxes'.
7. Right-click the printer icon and select 'Properties'.
8. If your operating system does not already have the driver, you will be asked if you want to install it now. Click 'No'.

9. Select the 'Advanced' tab, and click 'New driver'. The 'Add Printer Driver Wizard on openrg' will commence. You will be prompted to select a printer driver from a list. If unavailable, you can either browse to a location on your computer where you have stored the driver, or click 'Have Disk' and insert the CD containing the driver (supplied with your printer).
10. Click 'OK'. The driver is uploaded to OpenRG's system storage directory (e.g. \\openrg\A).

6.5.4. Controlling Access to Print Jobs

If you have established the printer connection on your LAN computers using the Samba or IPP protocol, you can manage the users' permissions for accessing the printer.



Note: With IPP printers, access control is currently supported only by Windows XP.

IPP and Samba printers can work in two modes:

1. **Guest Access** All users on the LAN can print, delete, pause and resume all printer jobs.
2. **Non-Guest Access** The OpenRG administrator can configure each printer with two types of users:
 - a. Users with print access can print, delete, pause and resume their print jobs only.
 - b. Users with administrator permissions can also perform these tasks on other users' jobs, as well as pause and resume the printer.

To define access permissions for specific users:

1. In the 'Print Server' screen (see [Figure 6.35](#)), deselect the 'Allow Guest Access' option.
2. Click 'Apply' to save the change.
3. Click the 'System' tab and select 'Users'. The 'Users' screen appears.

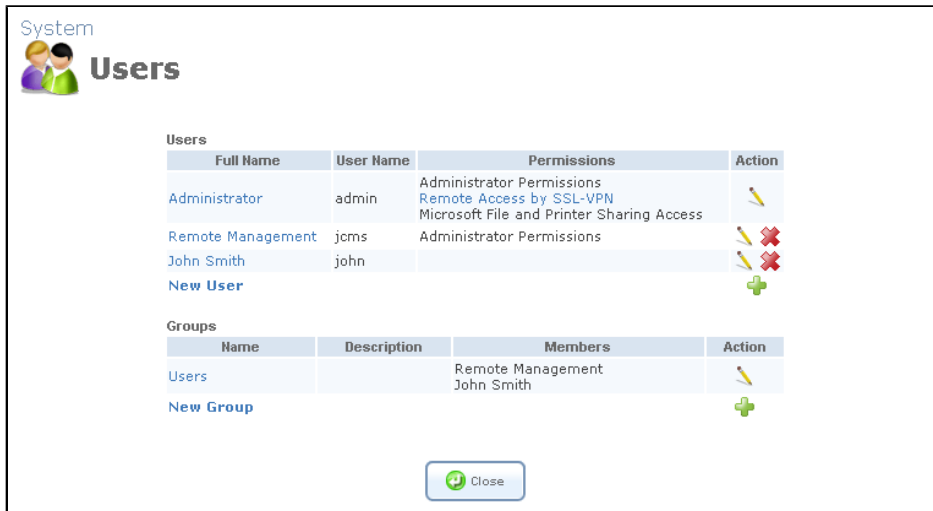


Figure 6.67. Users

- Click the name of the user whom you wish to grant the access. The 'User Settings' screen appears.

General

Full Name:

User Name (case sensitive):

New Password:

Retype New Password:

Primary Group: ▼

Permissions:

- Administrator Permissions
- Remote Access by SSL-VPN
- Mail Server Access
- Microsoft File and Printer Sharing Access
- FTP Server Access
- Internet Printer Access
- Remote Access by VPN

Figure 6.68. User Settings

- In the 'Permissions' section, select the permission level, according to the print protocol the user will utilize— either 'Internet Printer Access' (for IPP) or Microsoft File and Printer Sharing Access' (for Samba).
- Click 'OK' to save the settings.
- Add the user to the 'Printer Access Control' screen:
 - Click the 'Map View' menu item under 'Home' to display the Network Map.
 - Click the printer icon to view the 'Printer' screen, which enables you to manage the print jobs, and define printer access permissions for your LAN users.

Home

Printer

Name: i250
 IPP URL: http://openrg.home:631/printers/i250
 Model: Canon i250
 Status: idle
 Jobs Printed: 0 (0 bytes)
 Create Default Device Mode

Print Jobs

Name	From	Spooled	Printed	Size	Status	Action
Press the Refresh button to update the status.						

OK Apply Cancel Access Control Refresh

Figure 6.69. Printer Settings

- c. Click the 'Access Control' button to open the 'Printer Access Control' screen.

Local Network

Printer Access Control

Users

Name	Access Level	Action
New User		+

Groups

Name	Access Level	Action
New Group		+

OK Cancel

Figure 6.70. Printer Access Control

- d. Click the 'New User' link to select the user and the access level (Print/Admin).

Local Network

User

Name: John Smith
 Access Level: Print

OK Cancel

Figure 6.71. User Access Level

8. Click 'OK' to return to the 'Printer Access Control' screen.
9. Click 'OK' to save the settings.

When installing an IPP or Samba printer, the user is prompted for a username and a password, which will be used for all printing operations.



Note: If you disable 'Allow Guest Printing' on OpenRG after the printer was installed on Windows, it will no longer be available and will have to be re-installed.

After connecting to the network printer from a Windows host, access the print queue monitor by double-clicking the printer's icon in the task bar.

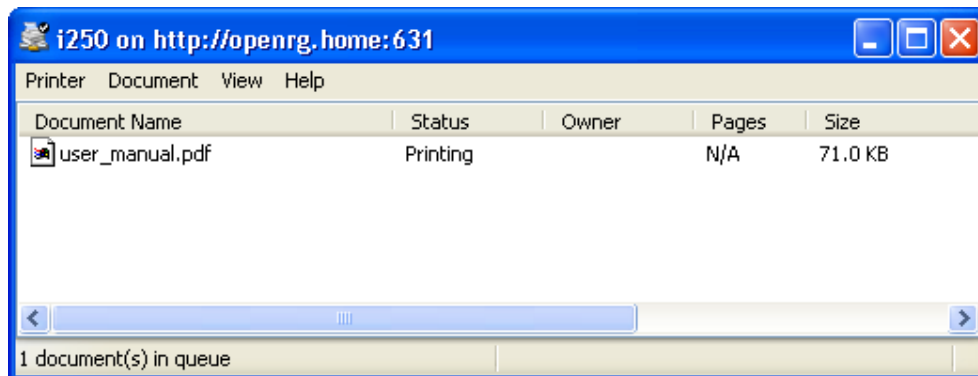


Figure 6.72. Print Queue Monitor

The print queue monitor displays all print jobs in a print queue, including jobs submitted by other users through any printing protocol. By default, the print queue monitor allows users to delete print jobs, or pause and resume the print queue. However, if guest access is disabled, only users with administrator permissions may perform these actions.



Note: Low-end printer models may malfunction if a partially printed job is deleted. Should this happen, reset the printer manually by switching it off and then on again.

6.6. IP-PBX

This tab presents the main screen of the Private Branch Exchange (PBX), displaying both the analog and VoIP telephone extensions available on OpenRG (see [Figure 6.73](#)).

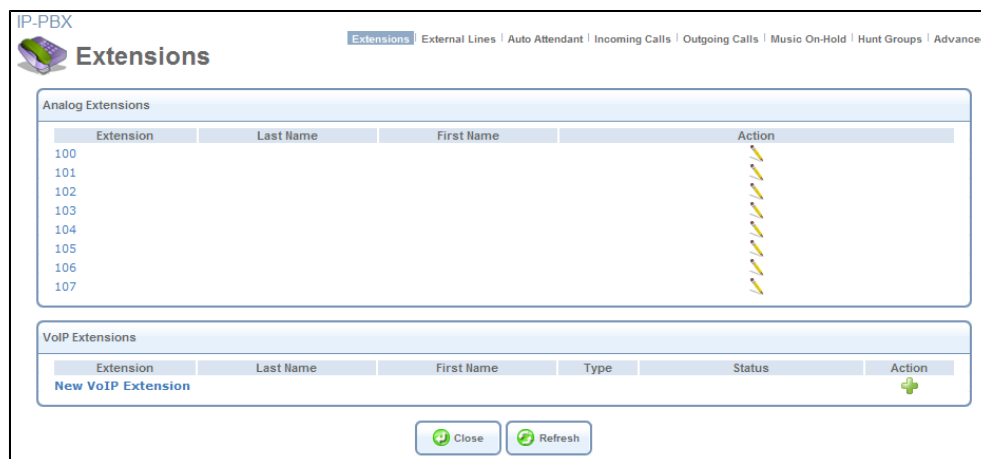


Figure 6.73. PBX Main Screen

For more information about the PBX feature, refer to [Section 7.7](#).

7

Services

7.1. Overview

The 'Overview' screen (see [Figure 7.1](#)) presents a summary of OpenRG's services and their current status (enabled/disabled). These services are configurable via their respective tabs under the 'Services' main tab.

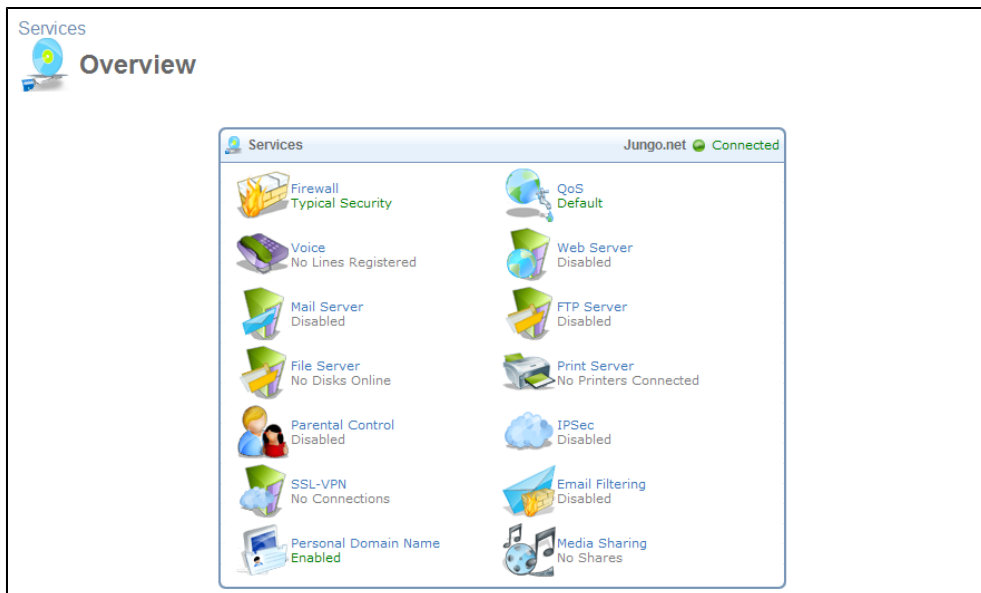


Figure 7.1. Services Overview

7.2. Jungo.net

Jungo.net is a portal that enables you to upgrade your OpenRG gateway with advanced broadband services offered by the service provider, in addition to the standard OpenRG

services package. You can easily enable the Jungo.net services on your gateway, using the intuitive GUI of the Jungo.net portal. An additional benefit of using Jungo.net is that it configures the services automatically, thereby saving you time and effort. To access the portal, you need to obtain a personal Jungo.net account.

For your convenience, OpenRG's Web-based Management (WBM) includes links from which you can access the Jungo.net portal, in the following screens:

- The 'Quick Setup' screen under the 'Home' tab ('Jungo.net' section)
- The 'Jungo.net' screen under the 'Services' tab

Alternatively, you can browse to the Jungo.net portal using the following URL:
<http://www.jungo.net>.

7.2.1. Creating a Jungo.net Account

A Jungo.net account can be created in one of the following methods:

- The service provider can create a Jungo.net account for you, which you can activate using OpenRG's Installation Wizard.
- You can create a Jungo.net account either by using OpenRG's Installation Wizard, or from the Jungo.net portal.

7.2.1.1. Using the Installation Wizard

In case your service provider creates the Jungo.net account for you when subscribing you to the Internet service, you should receive an email that contains a personal Jungo.net username and password. You can use OpenRG's Installation Wizard to setup your account. The wizard appears when logging into the WBM for the first time, but can be launched by clicking its link under the 'Home' tab. The wizard's 'Jungo.net Account Setup' step tests the account supplied by your service provider (or enables you to create one). For more information, refer to [Section 2.3.2.8 \[21\]](#).

7.2.1.2. Using the Jungo.net Portal

An alternative method of creating a Jungo.net account from OpenRG's WBM, is clicking the '**Don't have Jungo.net account? Register**' link located in the 'Jungo.net' screen. The link opens the 'Registration' screen of the Jungo.net portal in a new browser window. It contains the text of the Jungo.net License Agreement.

JUNGO **JUNGO.net**

Registration

JUNGO.net LICENSE AGREEMENT

IMPORTANT - READ CAREFULLY: THIS LICENSE AGREEMENT ("AGREEMENT") IS A LEGAL AGREEMENT BETWEEN YOU AND JUNGO LTD. ("JUNGO"), FOR THE OPENRG / OPENSMB SOFTWARE PRODUCT ACCOMPANYING THIS LICENSE (THE "SOFTWARE"). JUNGO IS WILLING TO SUPPLY YOU THE ACCOMPANYING SERVICES ONLY IF YOU ACCEPT ALL OF THE TERMS IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE YOU START WORKING WITH THE SOFTWARE, BECAUSE BY STARTING TO WORK WITH THE SOFTWARE YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS, LICENSOR WILL NOT APPLY THE OFFERED SERVICES TO YOUR OPENRG/OPENSMB GATEWAY.

Jungo offers to license a personal, exclusive services to maintain his OpenRG/OpenSMB based home/SOHO Router. The services can be applied to routers with Jungo software only. Attempt to apply these services on routers of other vendors doesn't grant services availability, and router's proper functionality after wards. **IF YOU WISH TO OBTAIN A LICENSE TO USE THE SOFTWARE FOR INTERNAL DEVELOPMENT AND FOR COMMERCIAL PURPOSES PLEASE CONTACT JUNGO LTD.**

The Jungo.net software ('Software') and the accompanying written materials are owned by Jungo and are protected by United States of America copyright laws, by laws of other nations, and by international treaties.

Jungo grants to licensee a personal, non-exclusive, non-distributable, non-assignable license to use Jungo.net software solely for internal development, internal testing and internal evaluation purposes. Licensee may not use this software for any other purpose, including

Figure 7.2. Jungo.net License Agreement

To create an account, perform the following:

1. Read the license carefully and click 'I Agree' to proceed. The domain name registration screen appears.

Registration

Jungo.net will create for you personalized home services portal to access your Home Network remotely.

Please select the Domain Name to access your Home Network:
Use home.[]jungo.net to access my home network remotely.

Figure 7.3. Domain Name Registration

2. In the open text field, enter a word (that will also serve as your Jungo.net username) and click 'Next'. The 'Registration' screen appears.

Registration

Domain:	Jungo.net
Gateway ID:	060a6f8083f1
User Name:	jsmith
Password:	<input type="text"/>
Retype Password:	<input type="text"/>
E-Mail:	<input type="text"/>
Security Question:	What is your pet's name? <input type="button" value="v"/>
Security Answer:	<input type="text"/>

Figure 7.4. Registration Form

3. Fill in the registration form, as described earlier.
4. Click 'Next'. Your gateway is configured accordingly, and the 'Confirm Your Registration' screen appears, displaying your account details.

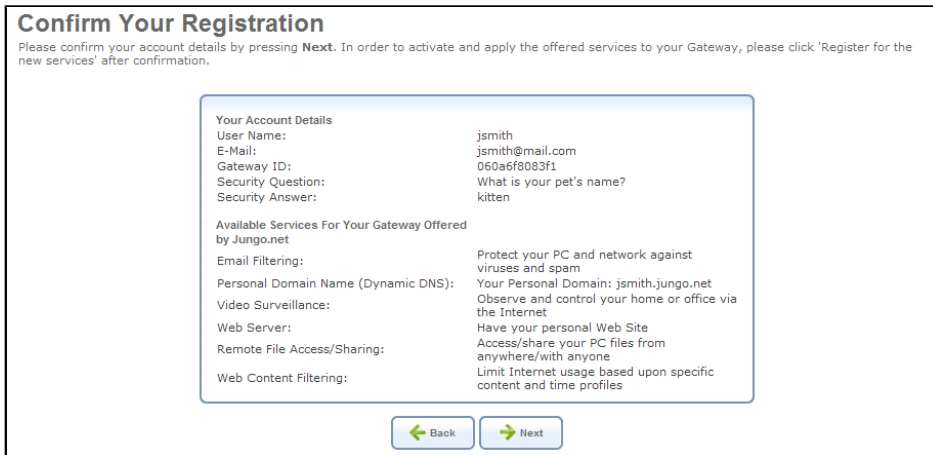


Figure 7.5. Confirm Your Registration

5. Click 'Next'. Jungo.net detects the services that your gateway supports.

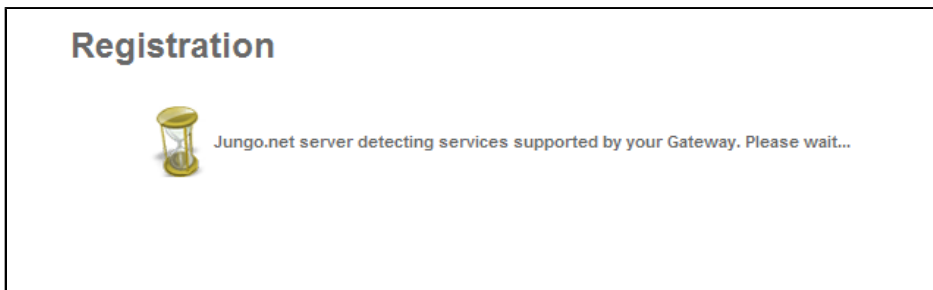


Figure 7.6. Detecting Supported Services

Once the services supported by the gateway are detected, the following screen appears.

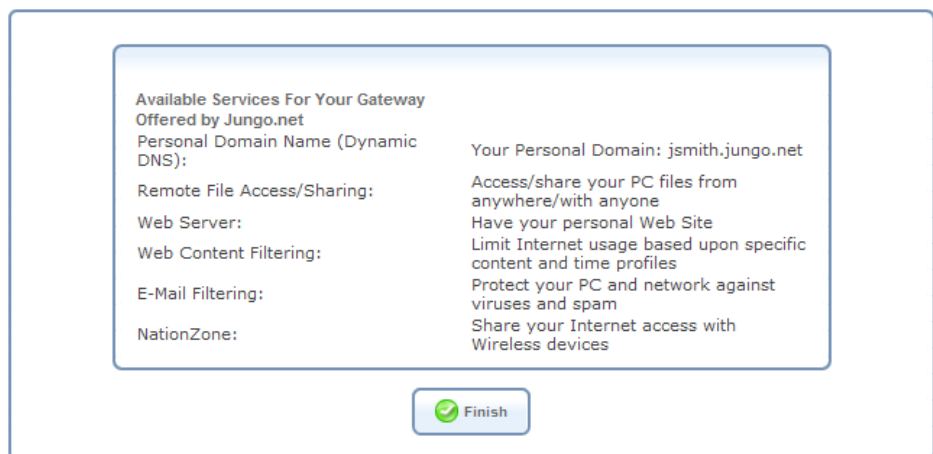


Figure 7.7. Supported Jungo.net Services

6. Click 'Finish'. The portal's homepage appears.

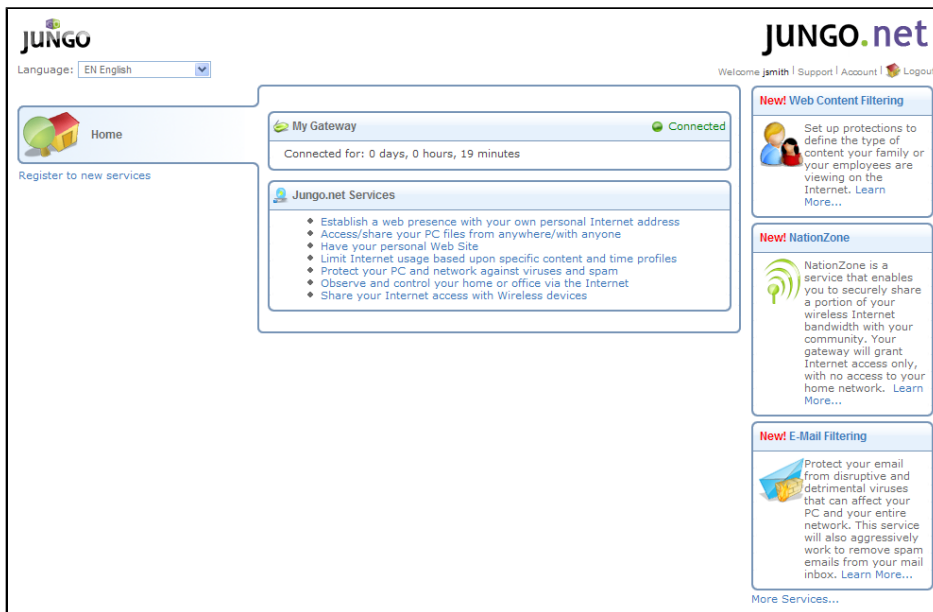


Figure 7.8. Jungo.net Homepage

When you go back to the 'Jungo.net' screen of OpenRG's WBM, you will see that your Jungo.net username and password are already present in their respective fields, and the 'Status' field has changed to 'Connected'.

If you are not at your gateway's location or have not obtained one yet, you can open a Jungo.net account by browsing directly to the Jungo.net portal. As you are not signed in yet, the login page opens.

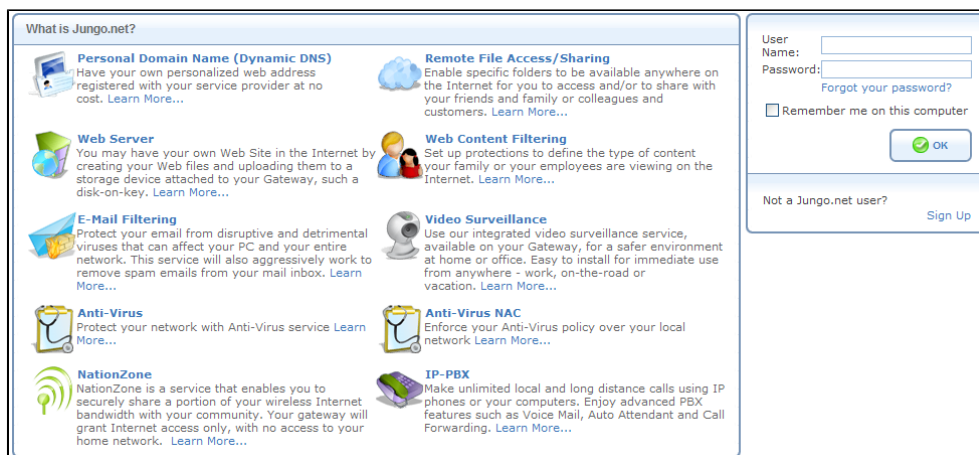


Figure 7.9. Jungo.net's Login Page

To create a Jungo.net account, perform the following:

1. In the lower right corner of the login section, click the 'Sign Up' link. The 'Jungo.net License Agreement' screen appears (see [Figure 7.2](#)).
2. Read the license carefully and click 'I Agree' to proceed. The domain registration screen appears (see [Figure 7.3](#)).

3. Fill the required field as described earlier, and click 'Next'. The 'Registration' screen appears.

Registration

Domain:	Universe
User Name:	jsmith
Password:	<input type="text"/>
Retype Password:	<input type="text"/>
E-Mail:	<input type="text"/>
Security Question:	What is your pet's name? ▾
Security Answer:	<input type="text"/>

← Back → Next

Figure 7.10. Registration Form



Note: In this case, your Jungo.net account is created in the 'Universe' domain. After it is associated with your gateway, the account will move to the domain in which the gateway is registered.

4. Fill in the registration form as described earlier.
5. Click 'Next'. The 'Confirm Your Registration' screen appears.

Confirm Your Registration

Please confirm your account details by pressing **Finish**. In order to activate and apply the offered services to your Gateway, please click 'Register for the new services' after confirmation.

Your Account Details	
User Name:	jsmith
E-Mail:	jsmith@mail.com
Gateway ID:	Not Registered
Security Question:	What is your pet's name?
Security Answer:	kitten

← Back → Finish

Figure 7.11. Confirm Your Registration

6. Click 'Finish' to confirm your registration. The Jungo.net homepage appears (see [Figure 7.8](#)).

After connecting the gateway, you need to associate the account with the gateway's information. You can either contact the service provider or associate the account with the gateway by yourself, as follows:

1. Under the 'Services' tab of the WBM, click 'Jungo.net'. The 'Jungo.net' screen appears.

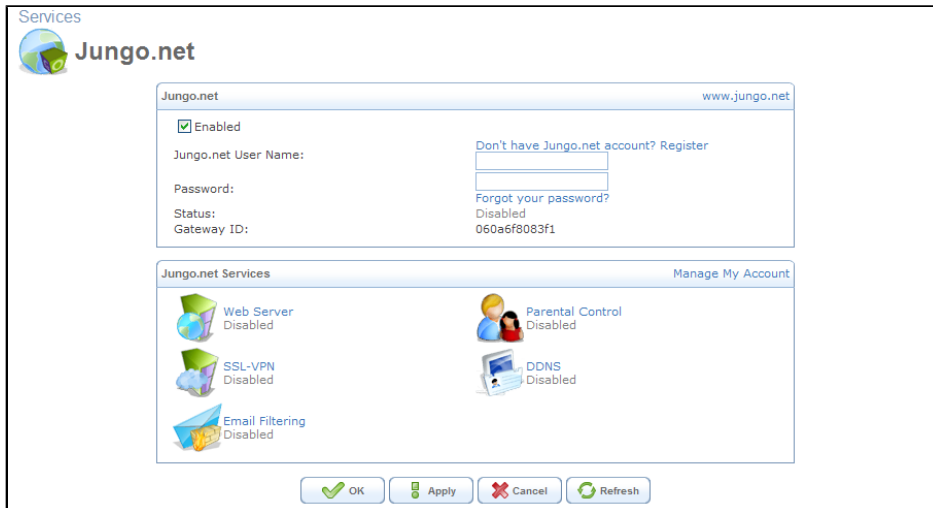


Figure 7.12. Jungo.net

As no account is associated with the gateway yet, the 'Status' field displays 'Disabled'.

2. Enter the account details and click 'Apply'. The 'Status' field displays 'Connecting'. This means that the account is being validated and associated with the gateway.
3. Click 'Refresh' until the 'Status' field changes to 'Connected'.

After the gateway is associated with your user, access the Jungo.net portal to start activating the services. If you click the 'Manage My Account' link in the WBM's 'Jungo.net' screen, you enter the portal, being automatically logged in. However, when browsing to the portal's Web page by clicking the <http://www.jungo.net> link or from outside the WBM, you will have to log in first.

7.2.2. Accessing Jungo.net

7.2.2.1. Logging into Jungo.net

You can log in to the Jungo.net portal by performing the following:

1. Browse to Jungo.net. The login screen appears (see [Figure 7.9](#)).
2. In the login section, enter your username and password, and click 'OK'.

7.2.2.2. Restoring a Lost Password

If you forgot your password, perform the following:

1. In the login section, click the 'Forgot your password?' link. The 'Change Password' screen appears.

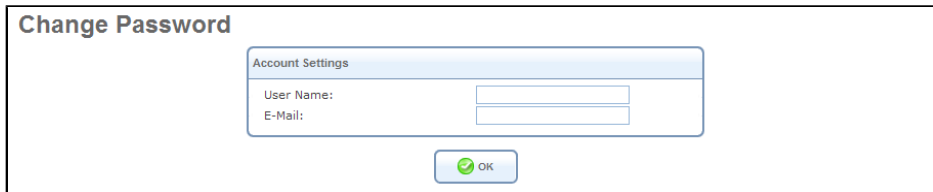


Figure 7.13. Change Password

2. Enter your username and email, and click 'OK'. The following message appears.

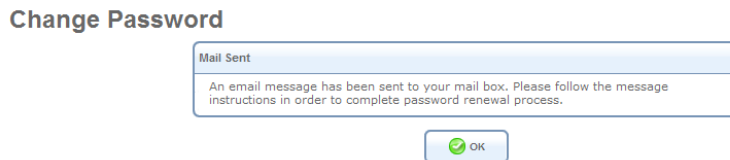


Figure 7.14. Password Reminder Mail

3. Log in to your email account and open the message. You should receive a link to the following password renewal screen.

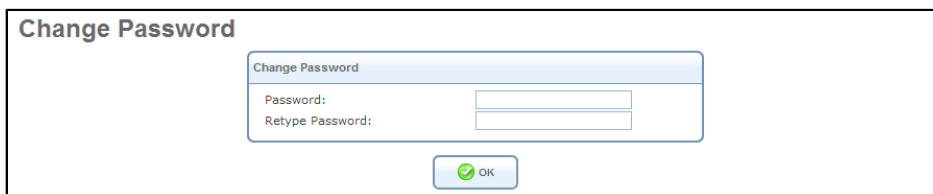


Figure 7.15. Change Password

4. Enter your new password and click 'OK'. The following password change confirmation screen appears.

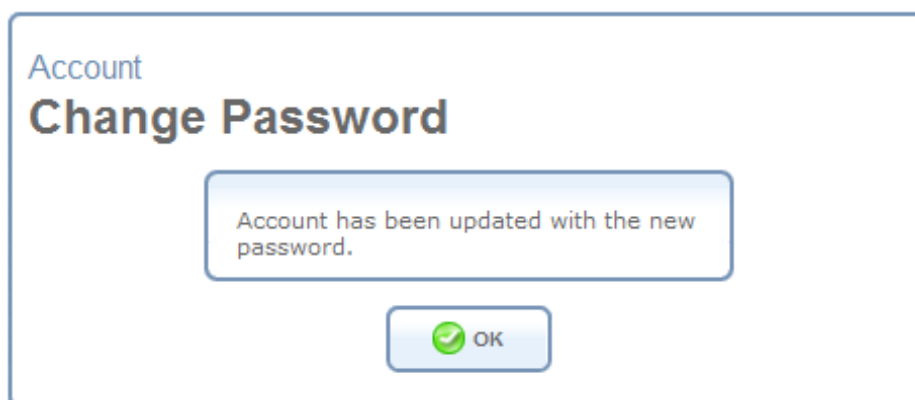


Figure 7.16. Password Change Confirmation

5. Click 'OK' to access the portal's 'Home' screen.

7.2.3. Reconnecting Your Gateway to Jungo.net

Your gateway disconnects from the Jungo.net portal when disabling the Jungo.net feature in OpenRG's WBM. The 'Jungo.net' screen refreshes accordingly.

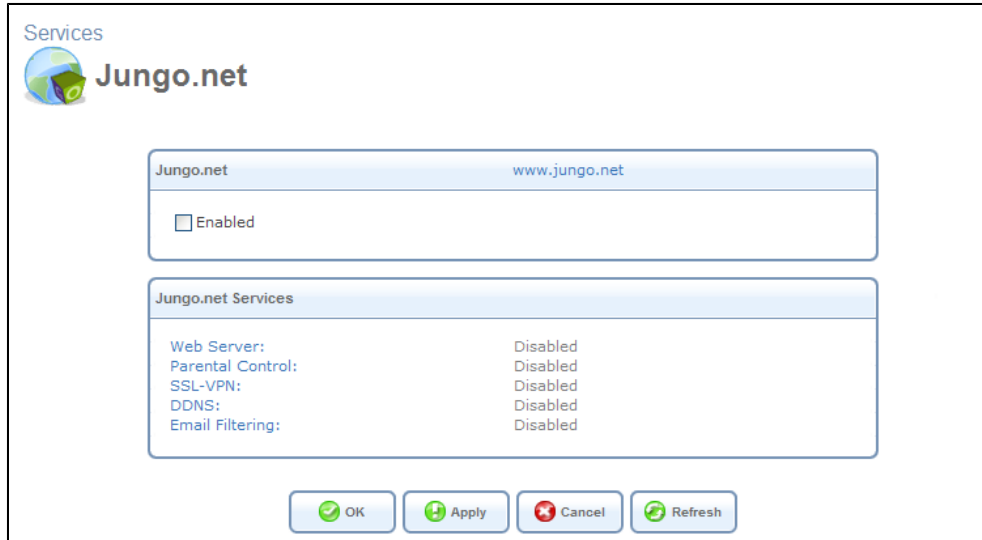


Figure 7.17. Disabled Jungo.net

To reconnect your gateway, you will need your login information. Perform the following:

1. In the WBM's 'Jungo.net' screen, select the 'Enabled' check box. The login information fields become visible.
2. Fill in these fields and click 'Apply'. The 'Status' field changes to "Connecting". Refresh the screen until the status changes to "Connected".
3. In the 'Jungo.net Services' section of the screen, click the 'Manage My Account' link. The Jungo.net portal opens in a new window (see [Figure 7.8](#)).


7.2.4. Registering and Using the Jungo.net Services

Click the 'Jungo.net Services' link or the 'Register for the new services' link in the homepage. The 'Services' screen appears. This screen enables you to view the Jungo.net services and activate them on OpenRG.

Figure 7.18. Junglo.net Services

By default, all Junglo.net services are disabled on the gateway. When you register for a service, Junglo.net enables and configures it automatically. The 'Services' screen contains the following information:

- Services and their short description
- A 'Learn More...' link to the registration page near each service.

 Note: If your gateway's firmware does not support a service, the following message appears instead of the subscription status field: "Service is not supported by your Gateway". To enable the service, contact the service provider to upgrade your gateway's firmware.

Available Junglo.net services are:

- Personal Domain Name (Dynamic DNS)
- Remote File Access/Sharing
- Web Server
- Web Content Filtering
- E-mail Filtering
- Video Surveillance

- NationZone
- IP-PBX

The following sections explain how to activate each of these services on the gateway via the Jungo.net portal.

7.2.4.1. Personal Domain Name

Personal Domain Name or Dynamic DNS is a service that provides you with a personal Internet address. Using this service, you can develop your own Web site, as well as enable OpenRG's remote file sharing feature. To activate the Dynamic DNS service, perform the following:

1. Click the 'Personal Domain Name' link. The service's 'Overview' screen appears.

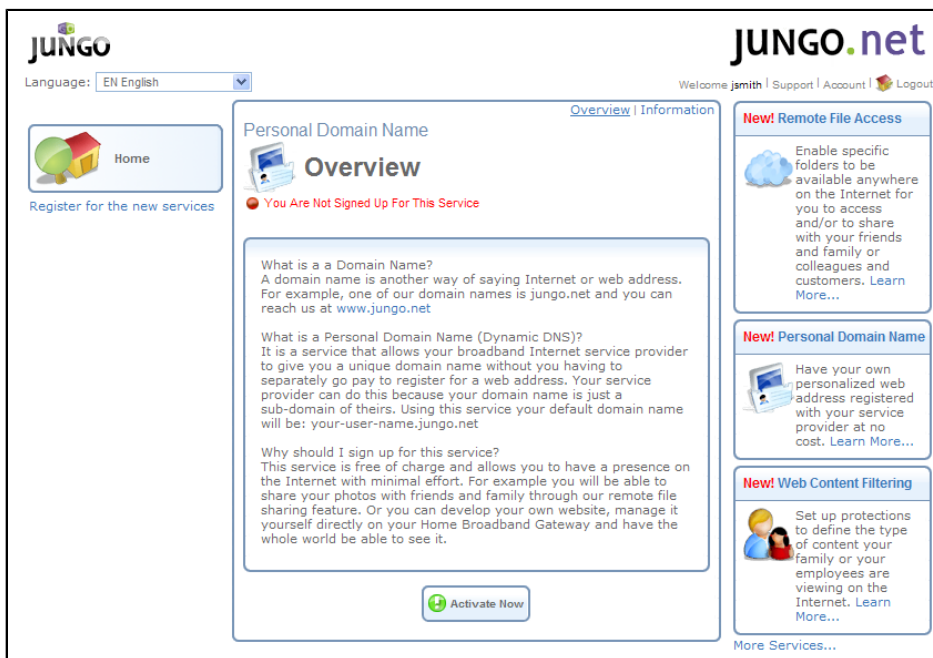



Figure 7.19. Dynamic DNS Service Overview

 Note: Clicking the 'Information' link at the right side of the screen leads you to the 'Information' screen, where additional service information, such as its price, is displayed.

2. Read the service-related information and click 'Activate Now'. The 'Order New Service' screen appears.

The screenshot shows the 'Order New Service' page for a Personal Domain Name on the Jungo.net website. The page is titled 'Personal Domain Name' and 'Order New Service'. It includes a 'Service Settings' section with the following information:

- Your Personal Domain: `jsmith.jungo.net`
- Access Your Gateway at Home: `home.jsmith.jungo.net`
- Access Jungo.net Portal to Manage Your Account and Services: `site.jsmith.jungo.net`
- Access Jungo.net Portal to Manage Your Account and Services: `jsmith.jungo.net / www.jsmith.jungo.net`

There are three radio button options for accessing the gateway, portal, or web server:

- Access Jungo.net Portal to Manage Your Account and Services
- Redirect to Another Site: Such as `http://mysite.com`
- Access a Web Server at My Home (You will need to install a web server and configure local server for port redirection, or insert a USB disk to OpenRG and enable Web Service from Jungo.net Portal)

At the bottom, there are two buttons: 'Confirm Your Order' and 'Cancel'. The page also features promotional boxes for 'New! Web Content Filtering', 'New! Email Filtering', and 'New! Web Server'.

Figure 7.20. Order Dynamic DNS Service

The 'Service Settings' section of this screen displays the following three URLs that you will obtain for personal use after registration:

home.your_username.jungo.net Leads to your gateway's WBM.

site.your_username.jungo.net Leads to the Jungo.net portal.

your_username.jungo.net Your personal domain name that can be used for the following purposes:

- Access your personal account in the Jungo.net portal to add and manage the broadband services on your gateway. To enable this option, select the first radio button located in the 'Service Settings' section.
- Redirect to another Web site. To enable this option, select the second radio button and specify the Web site's URL in the designated text field.
- Access your Web site. To enable this option, select the third radio button and perform **either** of the following:
 - Set up a Web server, and configure your local server for port redirection. This option is recommended for advanced users.
 - Connect a USB disk with your Web site content to the gateway, and enable the Web service in the Jungo.net portal. For more information, refer to [Section 7.2.4.3](#).

3. Click 'Confirm Your Order'. After configuring your gateway, the following screen appears.

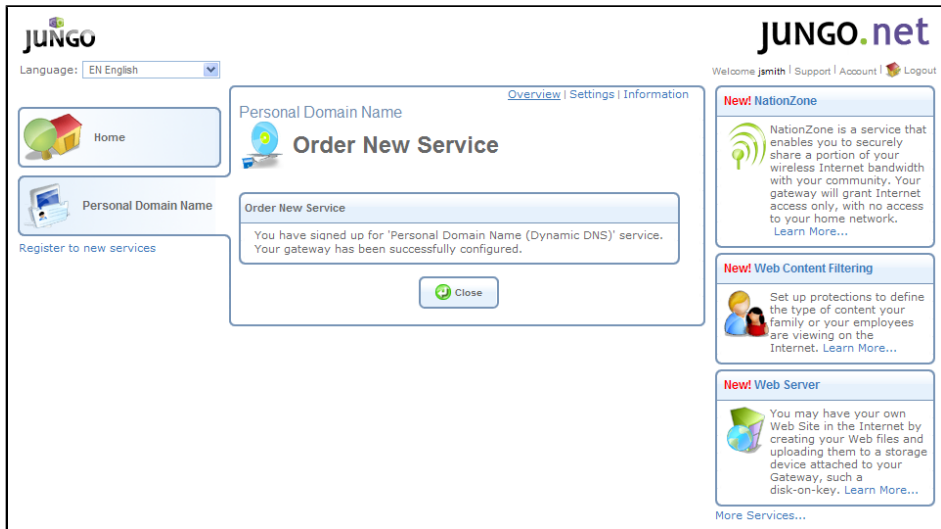


Figure 7.21. Successful Dynamic DNS Activation

4. Click 'Close'. The homepage appears, with the 'Personal Domain Name' tab being added to it.

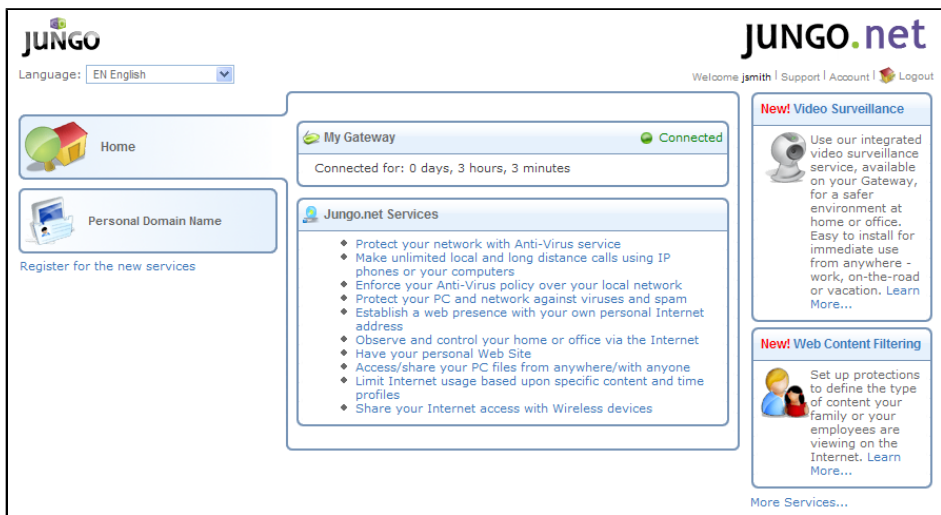


Figure 7.22. Homepage — Personal Domain Name Tab

5. Click the 'Personal Domain Name' tab. The service's 'Overview' screen appears.

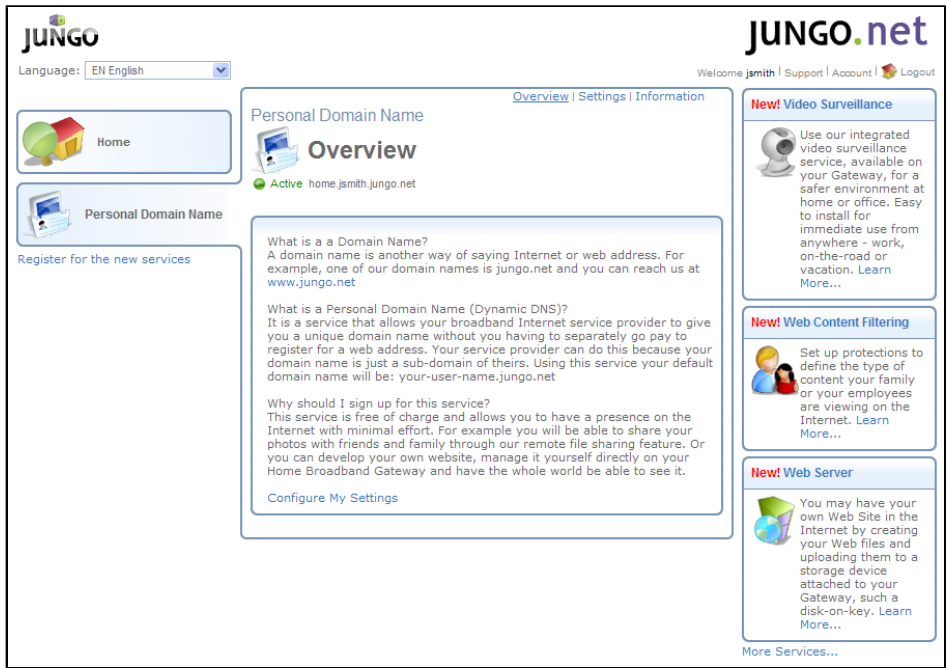


Figure 7.23. Personal Domain Name Overview

The status of the service is now 'Active'. In the example shown in **Figure 7.20**, the user's auto-generated domain name is **jsmith.jungo.net**, according to the username.

6. Click the 'Settings' link. The 'Settings' screen appears.

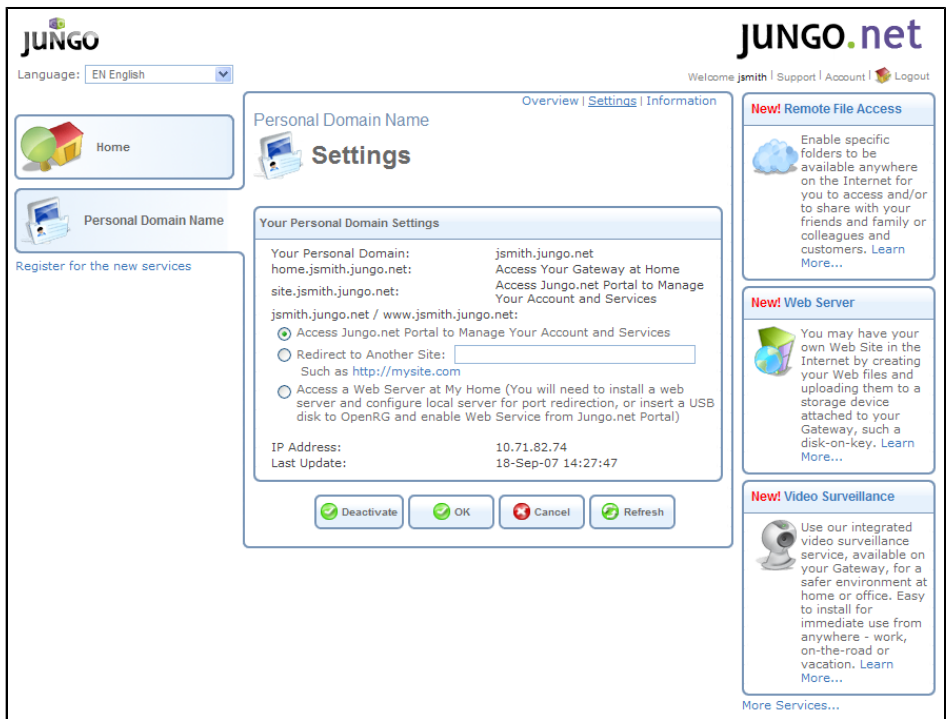


Figure 7.24. Personal Domain Name Settings

This screen enables you to select another function for your domain's URL, by clicking one of the three radio buttons described earlier. In addition, you can deactivate this service and reactivate it at any time, by clicking the 'Deactivate' or 'Activate' button respectively. This

screen also displays the IP address with which your domain name is associated, and the last time this service has been reconfigured on your gateway.

To view the effect on your gateway settings, click the 'DDNS' link in OpenRG's 'Jungo.net' screen. The 'Personal Domain Name' screen appears, configured with **home.your_username.jungo.net** as a Dynamic DNS entry.

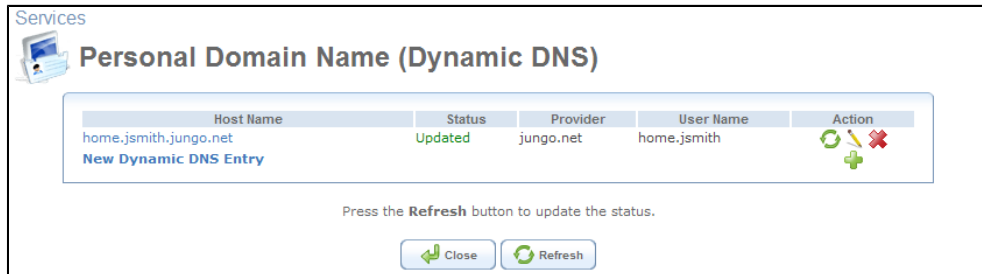
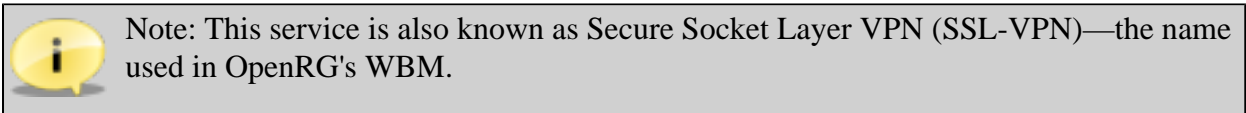


Figure 7.25. Active Dynamic DNS

In addition, to verify that the name is resolved, browse to **home.yourname.jungo.net**. If the name is resolved, the WBM's login page opens.

7.2.4.2. Remote File Access and Sharing

The Remote File Access/Sharing service enables you to access your PC's shared folders from anywhere and at any time. In addition, you can set up a 'Guest' profile to allow the people you trust to use your shared files.



To activate the service, perform the following:

1. Click the 'Remote File Access/Sharing' link. The service's 'Overview' screen appears.




Figure 7.26. Remote File Access/Sharing Service Overview

2. Read the service-related information and click 'Order Now'. The 'Order New Service' screen appears.



Figure 7.27. Order Remote File Access/Sharing Service

In the example shown in **Figure 7.27**, the user's remote access URL is `https://jsmith.junglo.net`.

 Note: If you don't activate the Dynamic DNS service, you can still access your file shares remotely by entering your IP address after the `https://` part of the remote access URL.

3. If you wish, change the default username ("guest"), and enter a password. A remote user will need this information to access the SSL-VPN portal.
4. Click 'Confirm Your Order'. After configuring your gateway, the following screen appears.

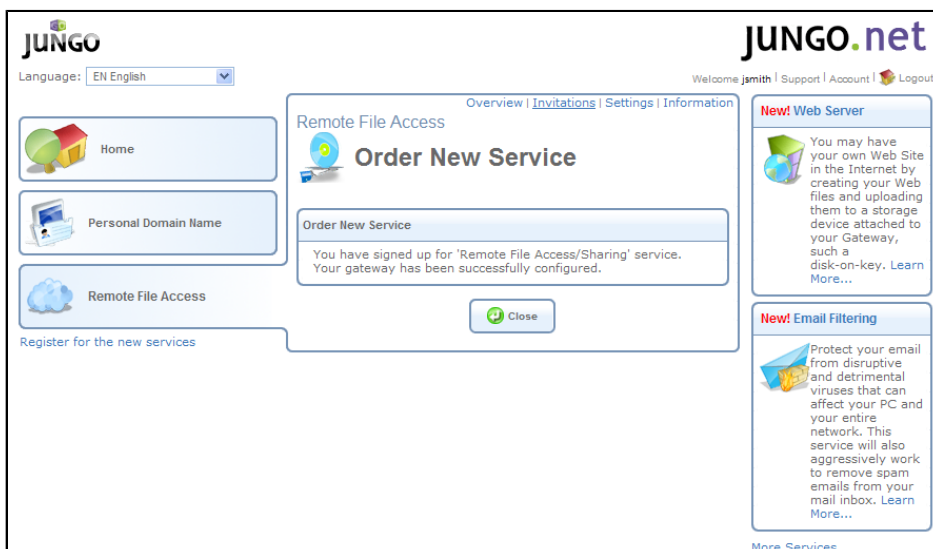


Figure 7.28. Successful Remote File Access/Sharing Activation

- Click 'Close'. The homepage appears, with the 'Remote File Access' tab being added to it.

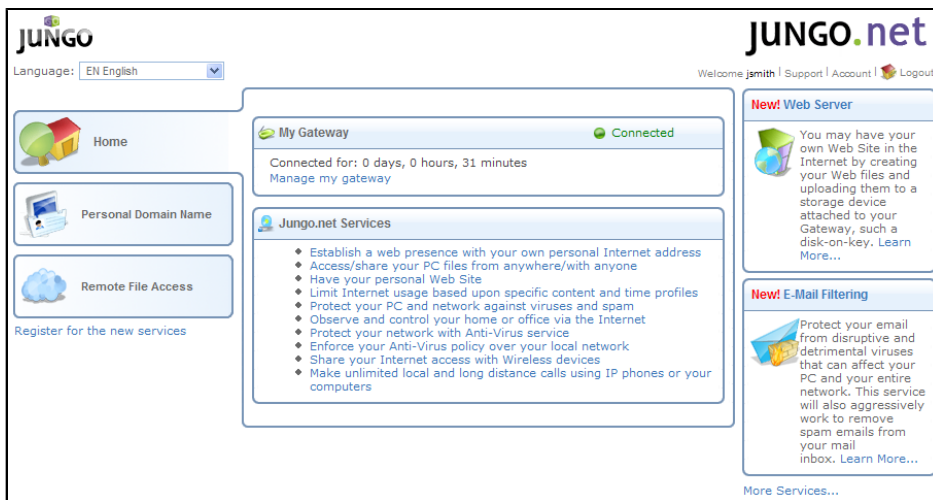


Figure 7.29. Homepage — Remote File Access Tab

In addition, the 'Manage My Gateway' link appears in the 'My Gateway' section. This link enables you to access and manage your gateway remotely.

To test the service, perform the following:

- Click the 'Remote File Access' tab. The service's 'Overview' screen appears.

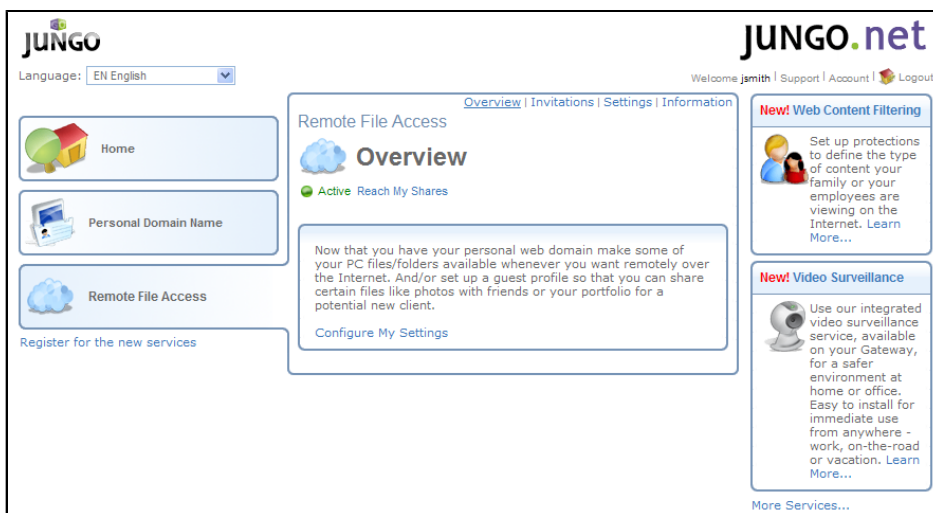
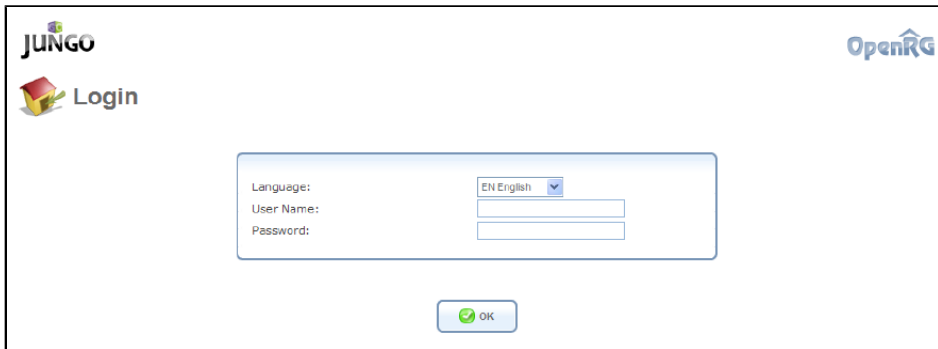


Figure 7.30. Remote File Access Overview

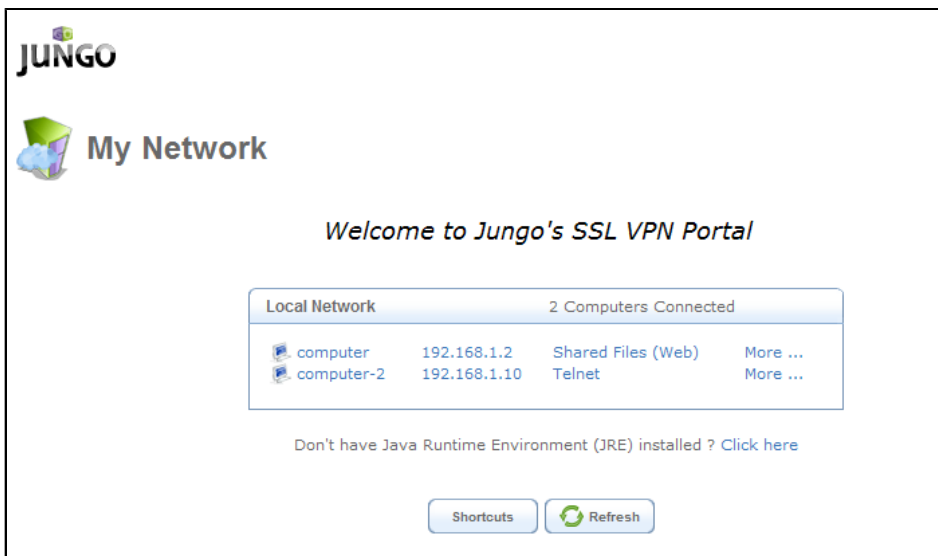
- Click the 'Reach My Shares' link. The 'Login' page of OpenRG's SSL-VPN portal appears.



The screenshot shows the Jungo Login Page. At the top left is the Jungo logo, and at the top right is the OpenRG logo. Below the logos is a 'Login' button. Underneath is a form with three input fields: 'Language' (a dropdown menu showing 'EN English'), 'User Name', and 'Password'. At the bottom of the form is an 'OK' button with a green checkmark icon.


Figure 7.31. SSL-VPN Portal's Login Page

3. Log in with the created account to view your shares. The 'My Network' screen appears.



The screenshot shows the 'My Network' page. At the top left is the Jungo logo, and below it is a 'My Network' icon. The main heading is 'My Network'. Below this is a welcome message: 'Welcome to Jungo's SSL VPN Portal'. Underneath is a table titled 'Local Network' with the subtitle '2 Computers Connected'. The table lists two computers: 'computer' (IP: 192.168.1.2) and 'computer-2' (IP: 192.168.1.10). For 'computer', the shared files are 'Shared Files (Web)' and 'Telnet'. For 'computer-2', the shared files are 'Telnet'. Below the table is a link: 'Don't have Java Runtime Environment (JRE) installed? [Click here](#)'. At the bottom are two buttons: 'Shortcuts' and 'Refresh'.

Figure 7.32. My Network

 Note: If you log in with your OpenRG administrator account, OpenRG's WBM page opens instead of the SSL-VPN portal.

4. Click the relevant PC link to access the shared directories.

To view the effect on your gateway settings, click the 'SSL-VPN' link in OpenRG's 'Jungo.net' screen. The 'SSL-VPN' screen appears.

General

Enabled

SSL-VPN Portal
[Click Here to Allow Incoming HTTPS Access](#)
[Click Here to Create SSL-VPN Users](#)

Greeting Message:

Image Location (URL):

Application Inactivity Timeout in Seconds:

Restrict Access Only to the Global Shortcuts

Figure 7.33. Enabled SSL-VPN

Once the service is activated, the 'Enabled' check box is selected and the 'SSL-VPN Portal' link appears. For more information, refer to [Section 7.10.2](#).

If you wish to inform a remote user about the shared files and how to access them, use the 'Invite a Friend to Share This Folder' link, located in OpenRG's 'File Server' screen. This link appears after connecting the gateway to the Jungo.net portal (for more information, refer to [Section 7.11.2.3](#)).



Note: A file sharing invitation message contains a direct link to a share. When clicked, it automatically authenticates the remote user and opens the share's page. Therefore, there is no need to add the login information to the invitation message.

After sending file sharing invitations to remote users, you can view a list of sent messages by clicking the 'Invitations' link in the 'Remote File Access Overview' screen. The following screen appears.

Remote File Access

Invitations

Overview **Invitations** Settings | Info

Results 1 - 3

ID	Invite Date	Share Name	To Email Address	Subject	Expiry Date	Number Of Visits	Action
1	2007-03-13 17:25:43	share2	becky@hotmail.com	Please share my data: share2	2007-04-13 00:00:00	Unlimited	
2	2007-03-13 17:24:58	share1	benjamin@yahoo.com	Please share my data: share1	2007-04-13 00:00:00	Unlimited	
3	2007-03-13 17:17:38	share5	jack@gmail.com	Please share my data: share5	2007-04-13 00:00:00	Unlimited	

Figure 7.34. Remote File Access Invitations

At any time, you can cancel an invitation by clicking its action icon. The Jungo.net portal configures OpenRG's file server accordingly. From this moment, the invited remote user will not be able to access your SSL-VPN portal and use the shares. If you wish to change the SSL-VPN portal's login settings, perform the following:

1. In the service's 'Overview' screen, click the 'Settings' link. The following screen appears.

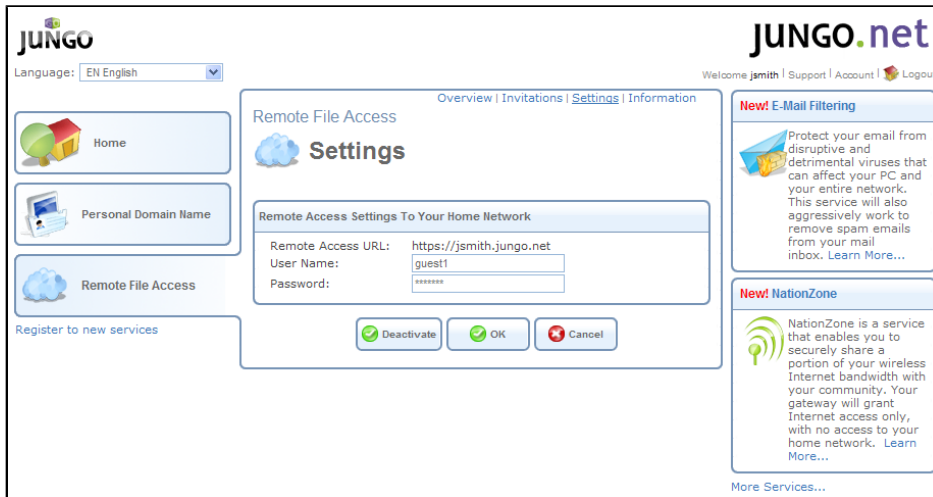


Figure 7.35. Remote File Access Settings

2. Update the login information, and click 'OK'.

7.2.4.3. Web Server

The Web Server service enables you to create your own Web site that is hosted on your gateway. Other Internet users will be able to access your Web site without entering your home or office network. This feature requires that you connect a storage device with Web site content to OpenRG. Your Web site content must be placed in the **website** directory located at the root of the file system.

When the storage device with the Web content is connected to OpenRG, the 'Enabled' message is displayed in WBM's 'Web Server' screen. However, if the storage device is not connected, or improperly formatted, this screen appears as follows.

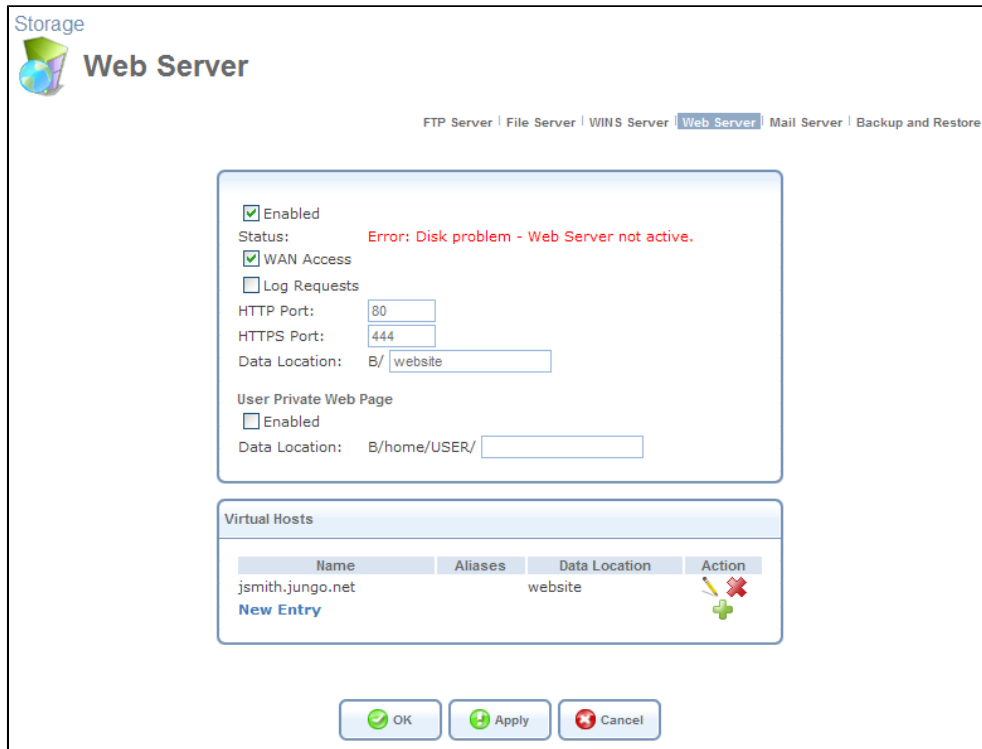


Figure 7.36. Web Server's Disk Problem

It is important that the storage device is formatted in either Linux EXT2 or EXT3 file systems. For more information, refer to [Section 6.4.1.2](#).

To activate the service, perform the following:

1. Click the 'Web Server' link. The service's 'Overview' screen appears.

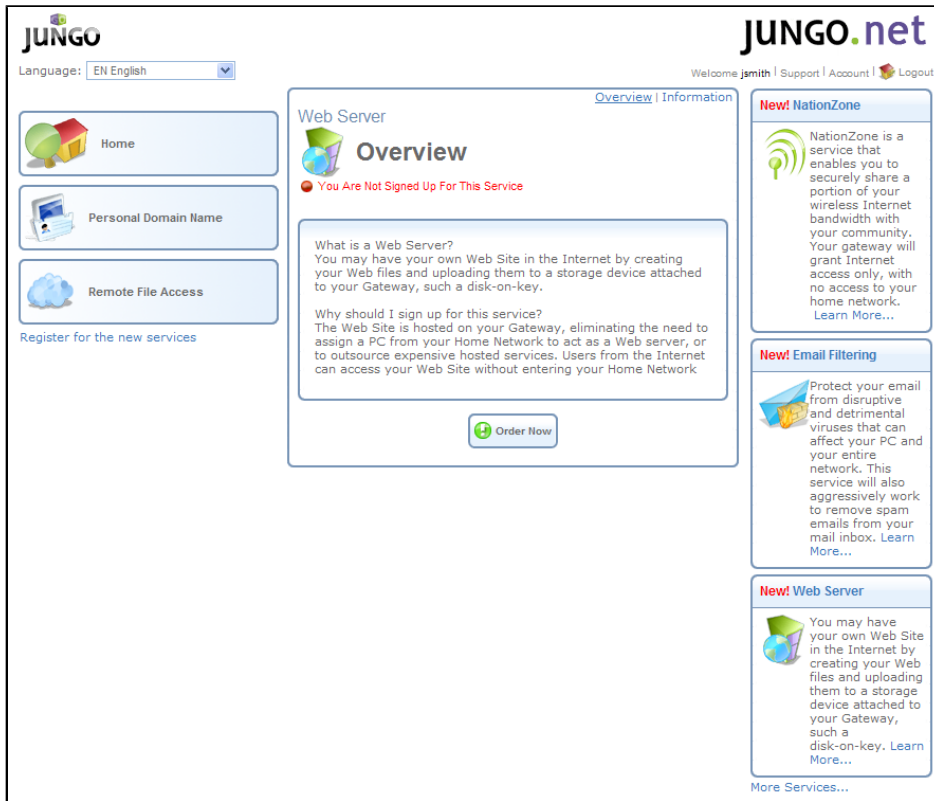


Figure 7.37. Web Server Overview

2. Read the service-related information and click 'Order Now'. The 'Order New Service' screen appears.



Figure 7.38. Order Web Server Service

In the example shown in **Figure 7.38**, the user's Web site URL is `http://jsmith.jungo.net`.

3. Click 'Confirm Your Order'. After configuring your gateway, the following screen appears.

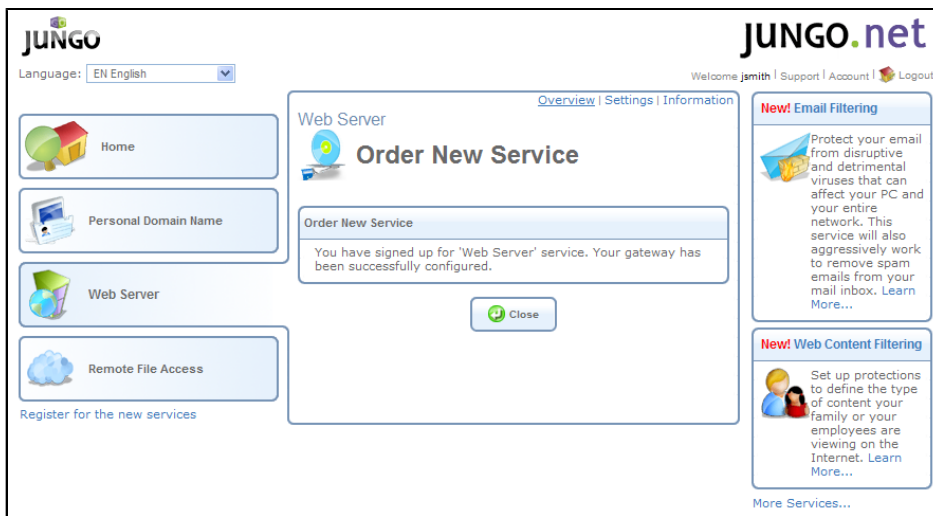


Figure 7.39. Successful Web Server Activation

4. Click 'Close'. The homepage appears, with the 'Web Server' tab being added to it.

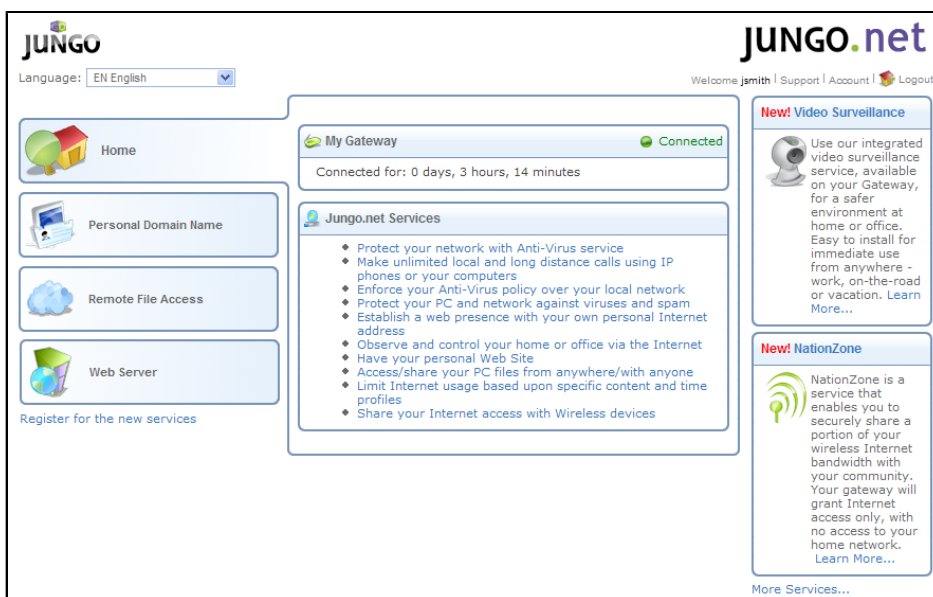


Figure 7.40. Homepage — Web Server Tab


To test the service, perform the following:

1. Click the 'Web Server' tab. The service 'Overview' screen appears.



Figure 7.41. Web Server Overview

2. Click the 'Visit My Web Site' link. If a storage device with the Web site content is connected to OpenRG, your Web site's homepage opens in a new browser window. Alternatively, open a new browser window and enter `http://yourname.junglo.net`.

 Note: After the service is activated, HTTP port 80 is utilized by the Web Server. If OpenRG's WBM uses the same port, it will disconnect. To access it again, enter the following IP address: `192.168.1.1:8080` or `192.168.1.1:8082`. The `:8080` or `:8082` suffix means that the WBM uses an alternative HTTP port (8080 or 8082), as the default port (80) is used by the Web Server.

To view the effect on your gateway settings, click the 'Web Server' link in OpenRG's 'Junglo.net' screen. The 'Web Server' screen appears.

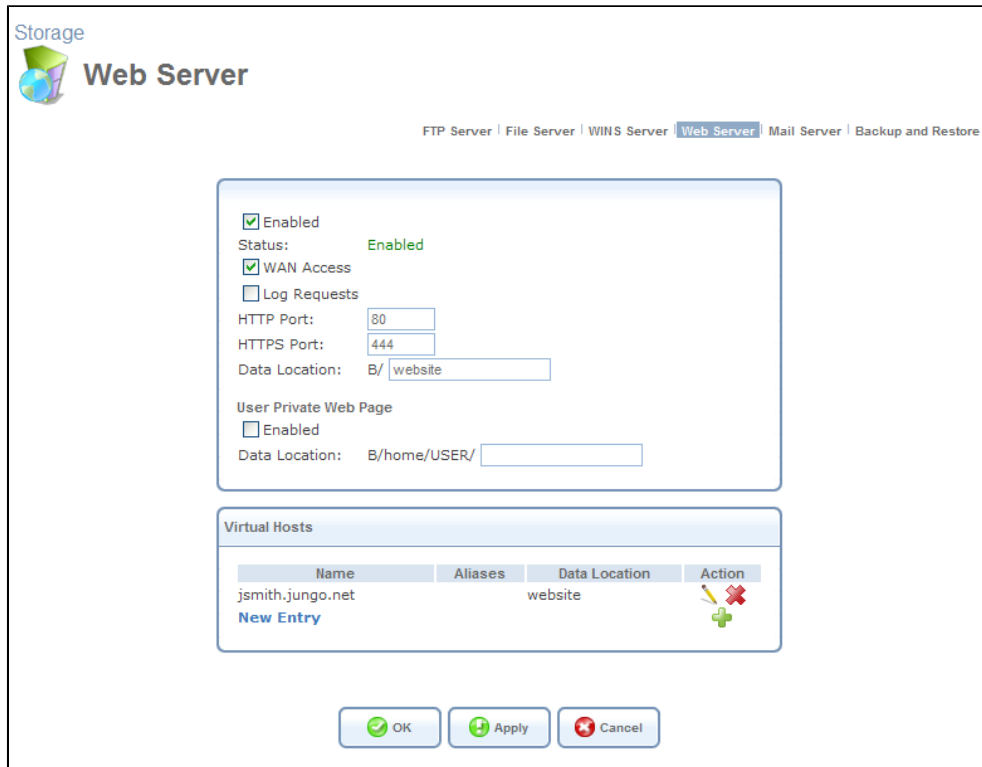


Figure 7.42. Activated Web Server

For more information, refer to [Section 7.11.4](#).

7.2.4.4. Web Content Filtering

The 'Web Content Filtering' service enables you to automatically configure your gateway's 'Parental Control' module, which is responsible for the Web content filtering operations. This module is powered by "[Surf Control](#)", a provider of the Internet content filtering. For more information about the 'Parental Control' module, refer to [Section 7.8](#). When you activate the service, Jungo.net automatically creates for you a personal account on the Surf Control server and configures your gateway's settings accordingly.



Note: The current version of the Jungo.net portal contains a demo version of the 'Web Content Filtering' service, which is used for demonstration purposes only.

To enable the service, perform the following:

1. Click the 'Web Content Filtering' link. The service's 'Overview' screen appears.



Figure 7.43. Web Content Filtering Overview

2. Click 'Order Now'. The 'Order New Service' screen appears.

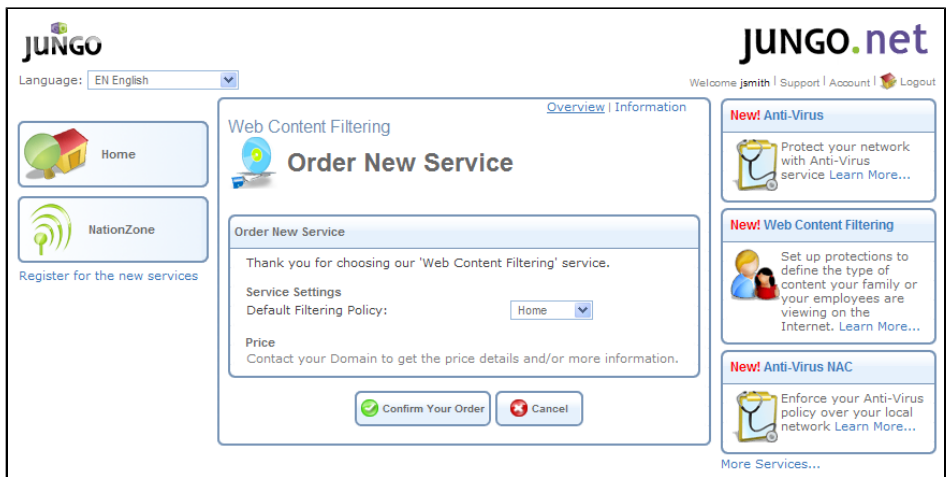


Figure 7.44. Web Content Filtering Order

3. Under 'Service Settings', select a default filtering policy from its drop-down menu. A filtering policy defines what sites will be blocked based on their category. Jungo.net provides two built-in policies:

Home Blocks sites under the 'Child Protection' category.

Employee Blocks sites from non work-related categories.

4. Click 'Confirm Your Order'. The following screen appears.

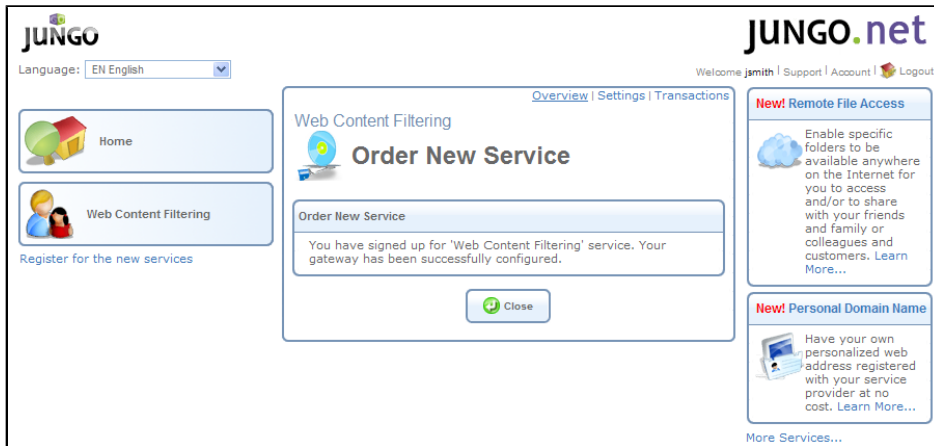


Figure 7.45. Web Content Filtering Order Confirmation

5. Click 'Close'. The homepage appears, with the 'Web Content Filtering' tab being added to it.

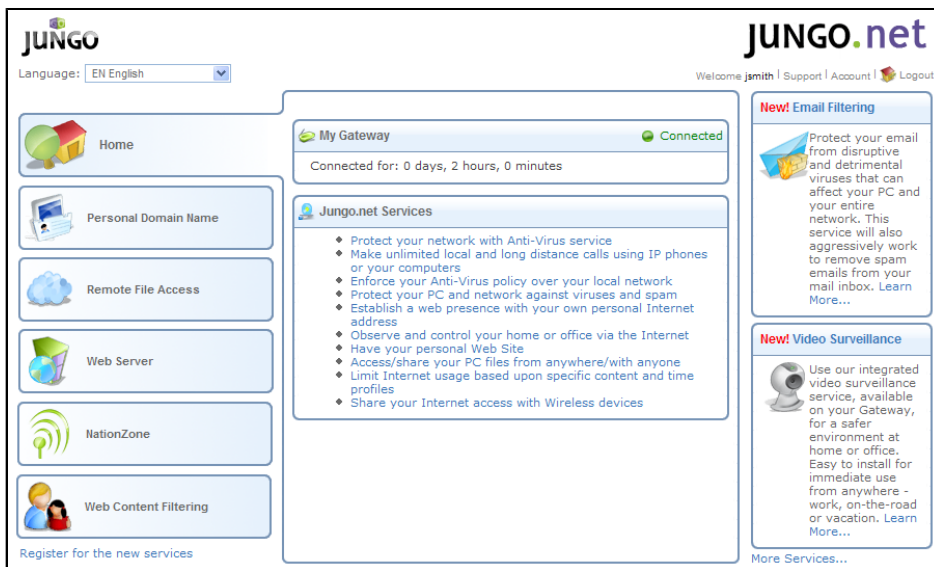


Figure 7.46. Homepage — Web Content Filtering Tab

You can always change the default filtering policy and configure your gateway with it. To change the policy, perform the following:

1. Click the 'Web Content Filtering' tab. The service's 'Overview' screen appears.

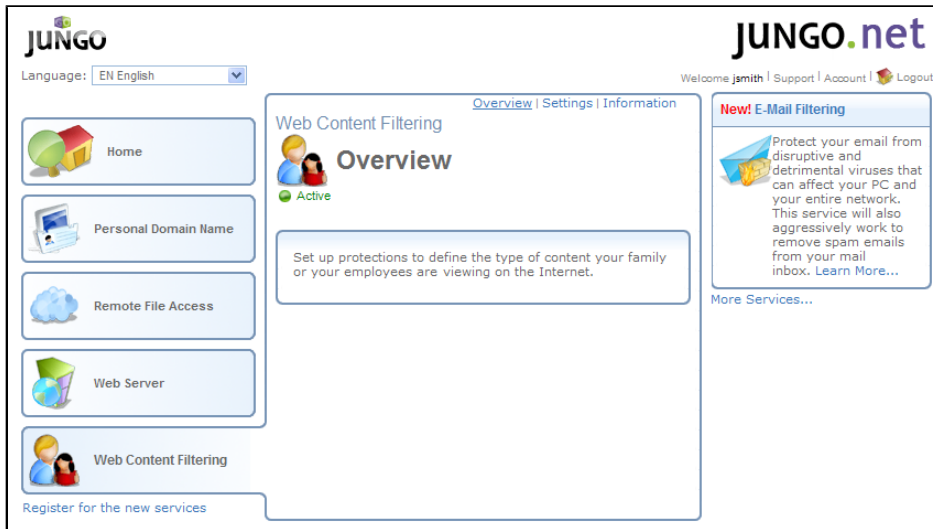


Figure 7.47. Web Content Filtering Overview

2. Click the 'Settings' link. The service's 'Settings' screen appears.

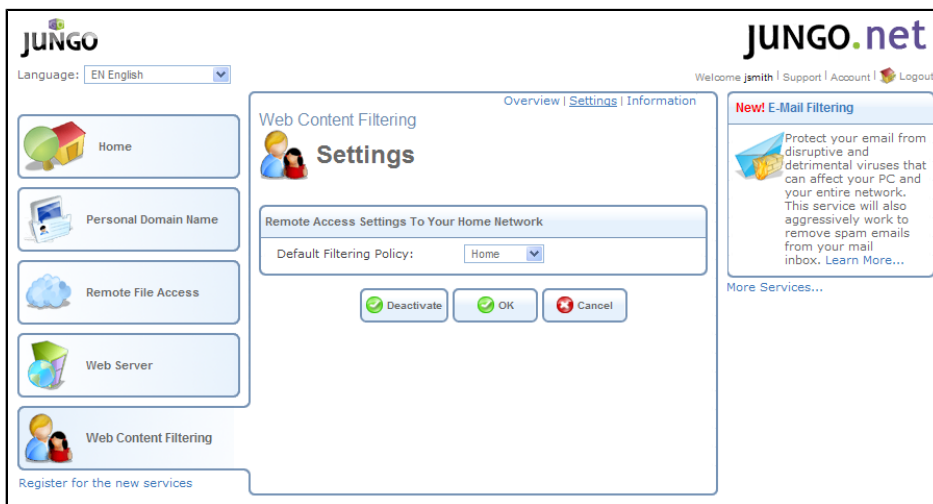


Figure 7.48. Web Content Filtering Overview

3. From the 'Default Filtering Policy' drop-down menu, select the desired filtering policy, and click 'OK'. Your gateway is configured accordingly.

After the gateway is configured, it will block access to Web sites, which are categorized as prohibited according to the filtering policy you have selected. To view the effect on your gateway settings, click the WBM's 'Services' tab and then 'Parental Control'. The following screen appears.

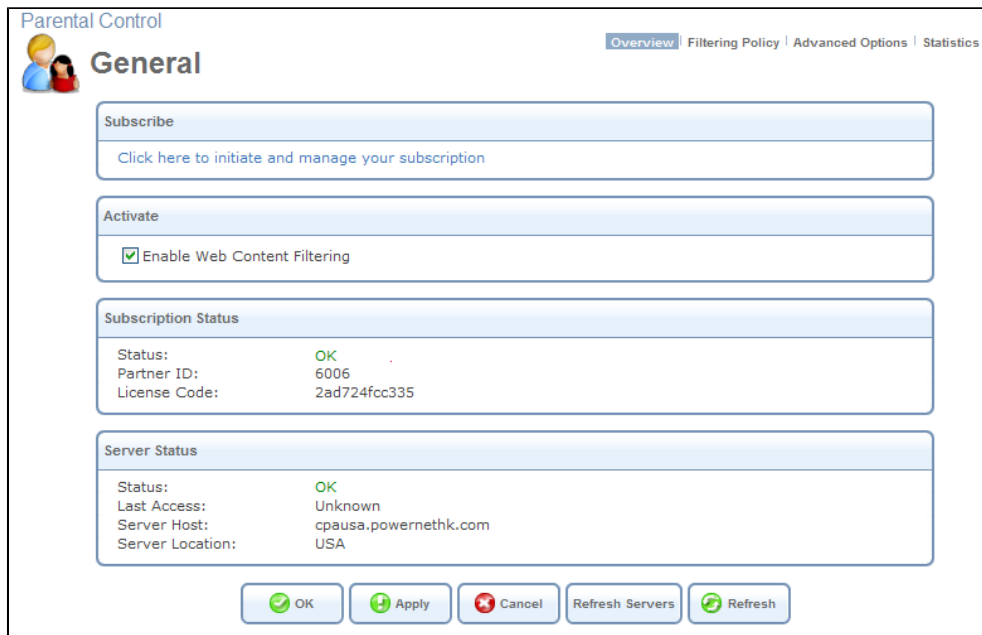


Figure 7.49. Parental Control General Settings

The 'Enable Web Content Filtering' check box is selected, and both the subscription's and the server's status is 'OK'. From now on, any person who tries to surf to a prohibited web site, will fail to do so. The following message is displayed instead.

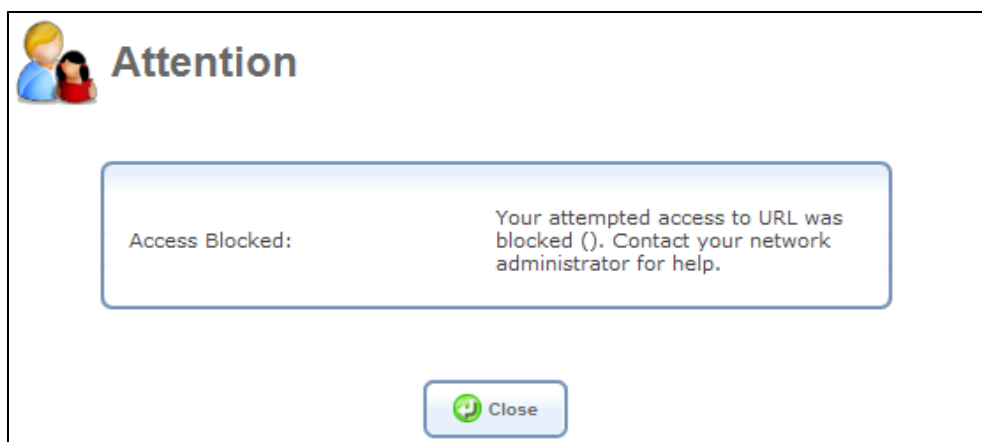


Figure 7.50. Blocked Access

7.2.4.5. E-mail Filtering

The 'E-mail Filtering' service enables you to automatically configure your gateway's 'E-mail Filtering' module, so it will profoundly inspect both your incoming and outgoing mail, or only either of them. While performing the inspection, this module will filter out all the spam and malicious messages, and prevent them from arriving at your mail account. For more information about OpenRG's 'E-mail Filtering' module refer to [Section 7.9](#). To activate the service, perform the following:

1. Click the 'E-mail Filtering' link. The service's 'Overview' screen appears.

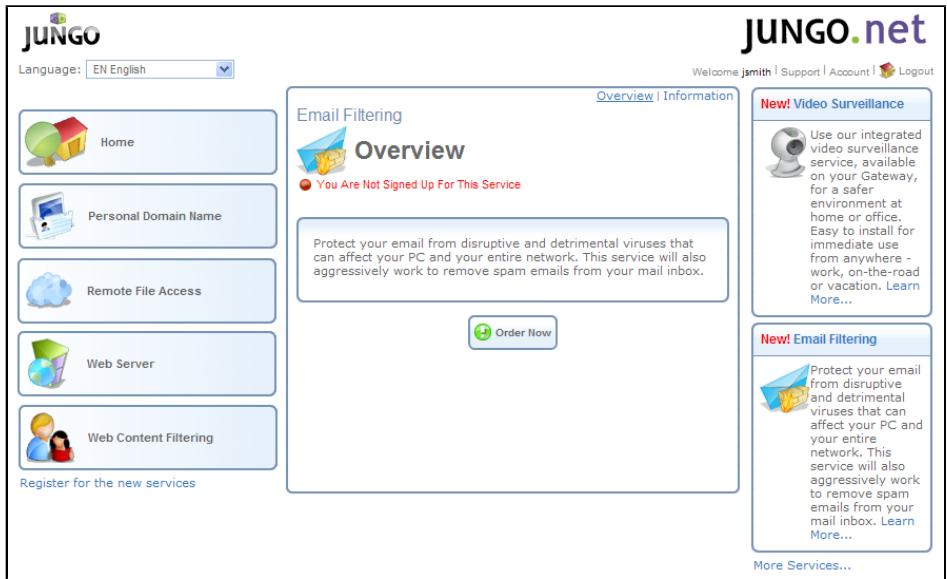


Figure 7.51. E-mail Filtering Overview

2. Click 'Order Now'. The following screen appears.

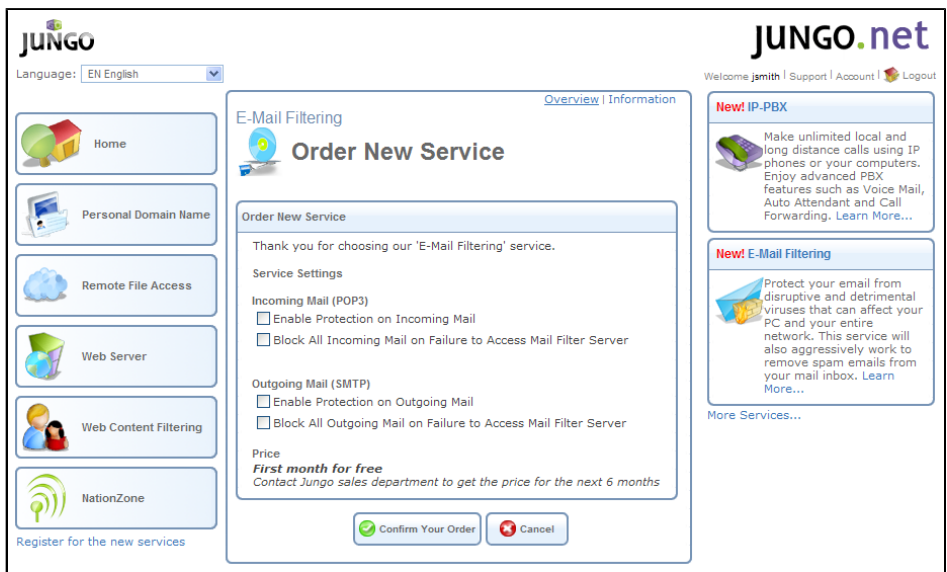


Figure 7.52. E-mail Filtering Order

This screen enables you to select from the following service settings that will be applied on your gateway:

- Incoming Mail (POP3)

Enable Protection on Incoming Mail Email filtering rules will be applied on incoming mail.

Block All Incoming Mail on Failure to Access Mail Filter Server Select this option if you would like to block all incoming mail messages in case email filtering cannot be performed.

- Outgoing Mail (SMTP)

Enable Protection on Outgoing Mail Email filtering rules will be applied on outgoing mail. This option is enabled by default.

Block All Outgoing Mail on Failure to Access Mail Filter Server Select this option if you would like to block all outgoing mail messages in case email filtering cannot be performed.

3. Click 'Confirm Your Order'. After configuring the gateway, the following screen appears.



Figure 7.53. E-mail Filtering Order Confirmation

4. Click 'Close'. The homepage appears, with the 'Email Filtering' tab being added to it.



Figure 7.54. Homepage — E-mail Filtering Tab

At any time, you can change the email filtering settings and reconfigure the gateway accordingly. To change the settings, perform the following:

1. Click the 'Email Filtering' tab. The service's 'Overview' screen appears.



Figure 7.55. E-mail Filtering Overview

2. Click the 'Settings' link. The service's 'Settings' screen appears.

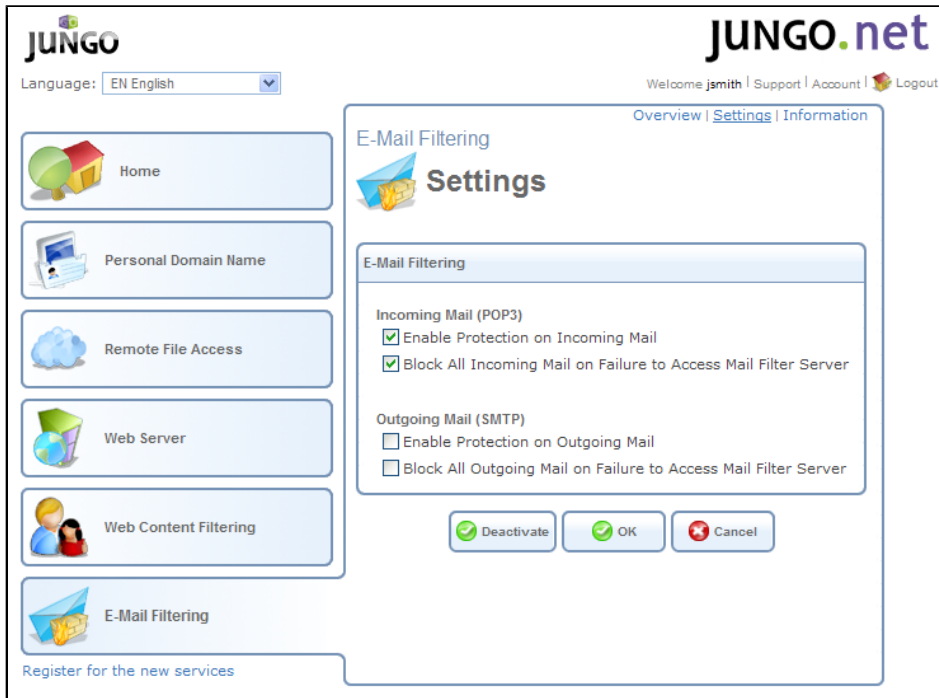


Figure 7.56. E-mail Filtering Settings

3. Change the settings as you wish, and click 'OK'. Your gateway is configured with the new email filtering settings.

To view the effect on your gateway's settings, click the WBM's 'Services' tab, and then 'Email Filtering'. The following screen appears.

Email Filtering

General Overview Advanced Options

Subscribe
Click here to initiate and manage your subscription

User Name
User Name for Service (from service provider):

Activate
 Enable Email Filtering

Subscription Status

Status:	OK
Expiration Date:	26 March 2008
Partner ID:	7000
License Code:	2ad724fcc335
Incoming Mail (POP3):	Enabled
Outgoing Mail (SMTP):	Enabled

POP3 Server Status

Status:	OK
Last Access:	27 June 2007
Server Host:	194.90.113.119
Server Location:	Unknown

SMTP Server Status

Status:	OK
Last Access:	27 June 2007
Server Host:	194.90.113.119
Server Location:	israel

Figure 7.57. Email Filtering — Activated

This screen demonstrates the case in which you have configured Jungo.net to enable e-mail filtering on both the POP3 and SMTP servers. Perform the following email filtering test:

1. Send an email from a WAN computer to a computer in OpenRG's LAN running a PC-based mail client such as Outlook™ or Eudora™. Write the word "sexx" in the subject line of the message.
2. Check for the received message on the LAN computer. The message should arrive with the following subject: "*** Detected as Spam by POP3 spam keywords*** sexx".

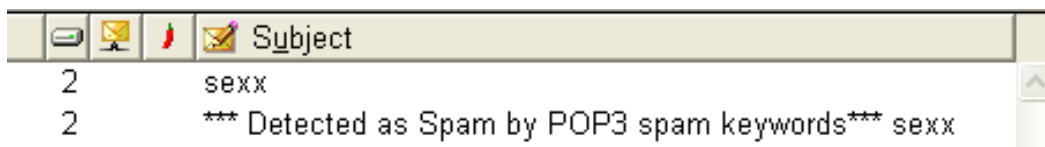


Figure 7.58. LAN Computer Inbox

This is how the email filtering service is configured to handle spam of this sort. However, you may choose how to handle spam and other types of email messages by configuring your email filtering account.

3. Repeat the steps above, only this time deactivate email filtering by deselecting the 'Enable Email Filtering' check-box (see [Figure 7.57](#)). The message should arrive exactly as sent, as no filtering had been performed.

7.2.4.6. Video Surveillance

The Video Surveillance service enables you to monitor your home or office via IP cameras. If you don't have the required surveillance equipment, you can purchase it via the Jungo.net portal, while registering for the service.

To activate the service, perform the following:

1. Click the 'Video Surveillance' link. The 'Overview' screen appears.

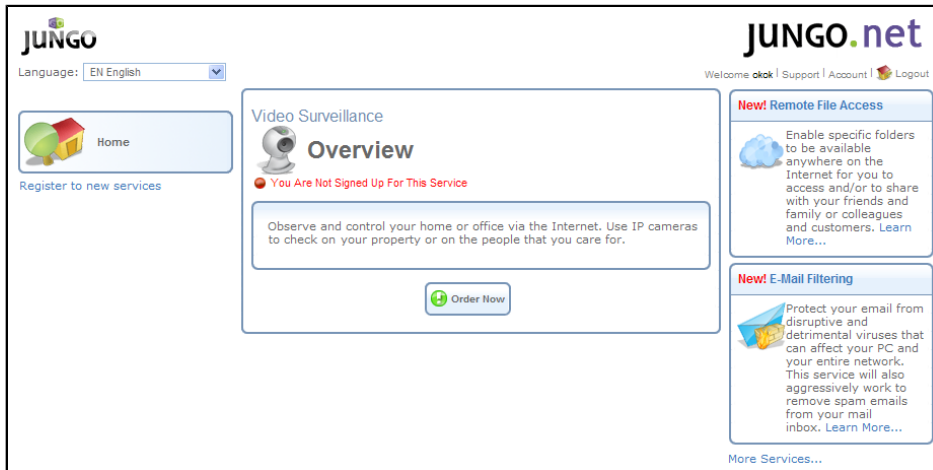


Figure 7.59. Service Overview

2. Click 'Order Now'. The 'Order New Service' screen appears.



Figure 7.60. Order New Service

3. You can view the required Jungo.net-certified equipment by clicking the 'Jungo.net Certified Cameras' link. The following screen appears.

JUNGO Language: EN English

Welcome [j.smith](#) | [Support](#) | [Account](#) | [Logout](#)

JUNGO.net

Home

Personal Domain Name

Remote File Access

Web Content Filtering

Register for the new services

Video Surveillance

Order New Service

Jungo.net Certified Cameras

Name	Description
BL-C10A Panasonic	Wired Pan/Tilt Network Camera
950G D-Link	Wireless 802.11b/g Network Camera
DCS-5300W D-Link	Enhanced 2.4GHz Wireless Internet Camera with Pan/Tilt
CS-5A4457 InfoSmart	Internet Camera with Pan/Tilt
BL-C111 Panasonic	Wired Pan/Tilt Network Camera
DCS-5300 D-Link	Enhanced 2.4GHz Internet Camera with Pan/Tilt

Close

New! Web Server

You may have your own Web Site in the Internet by creating your Web files and uploading them to a storage device attached to your Gateway, such a disk-on-key. [Learn More...](#)

New! Video Surveillance

Use our integrated video surveillance service, available on your Gateway, for a safer environment at home or office. Easy to install for immediate use from anywhere - work, on-the-road or vacation. [Learn More...](#)

New! Email Filtering

Protect your email from disruptive and detrimental viruses that can affect your PC and your entire network. This service will also aggressively work to remove spam emails from your mail inbox. [Learn More...](#)

More Services...

Figure 7.61. Jungo.net-certified IP Cameras

4. Click 'Close' to return to the previous screen.
5. Select whether you want to purchase one or more cameras by clicking the corresponding radio button, and click 'Next'. If you chose to purchase the cameras, the following screen appears.



Figure 7.62. IP Cameras Order Form

- Specify the quantity for the cameras you wish to purchase.
- Click 'Next'. The following screen appears.

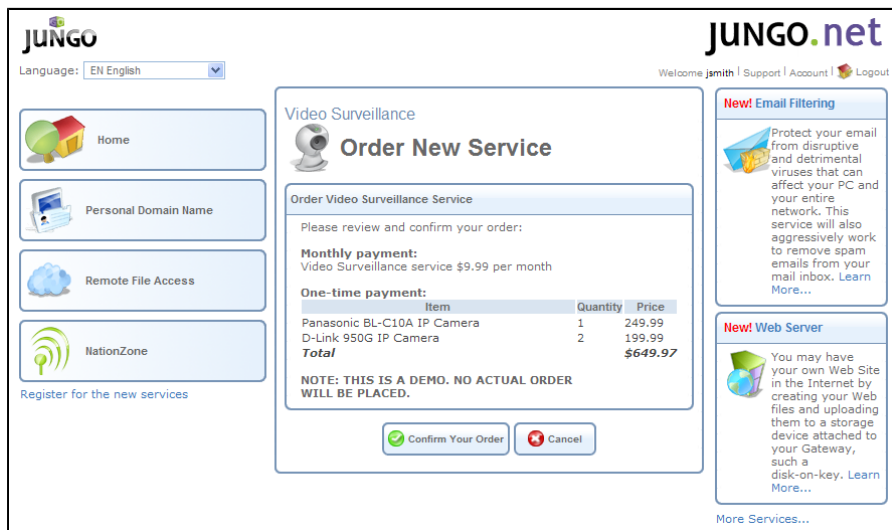


Figure 7.63. IP Cameras Order Summary

- Click 'Confirm Your Order' to submit the equipment order and to activate the service. The order confirmation screen appears.

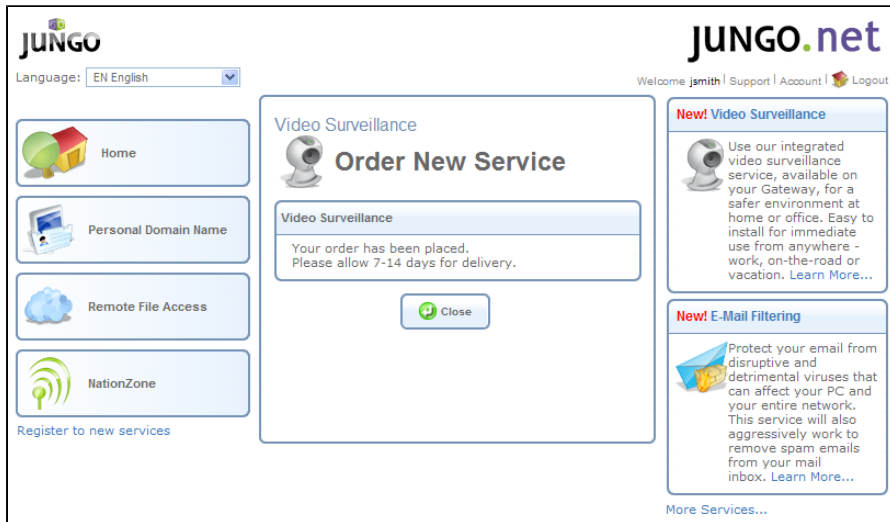


Figure 7.64. IP Cameras Order Confirmation

If you chose not to purchase the cameras (see [Figure 7.60](#)), perform the following:

- a. Click 'Next'. The following screen appears.

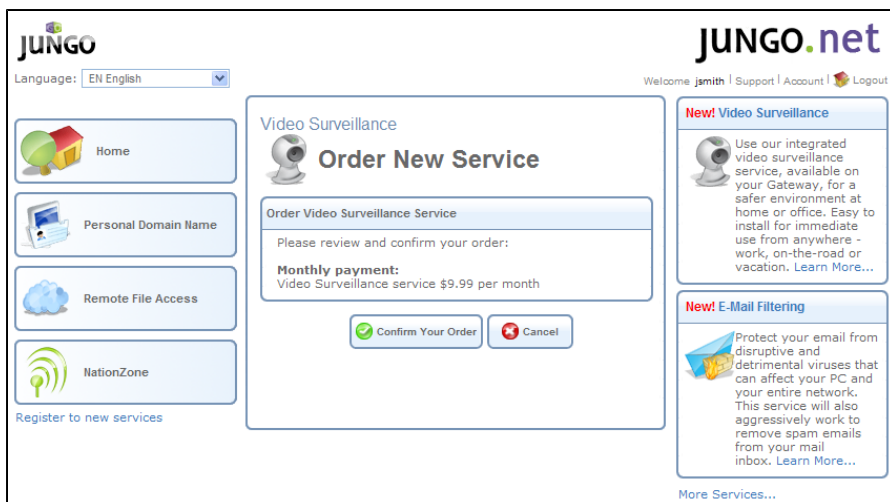


Figure 7.65. Service Order Summary – Without Cameras

- b. Click 'Confirm Your Order' to activate the service. The order confirmation screen appears.



Figure 7.66. Surveillance Order Confirmation

6. In either of the cases, click 'Close'. The homepage appears, with the 'Video Surveillance' tab being added to it.

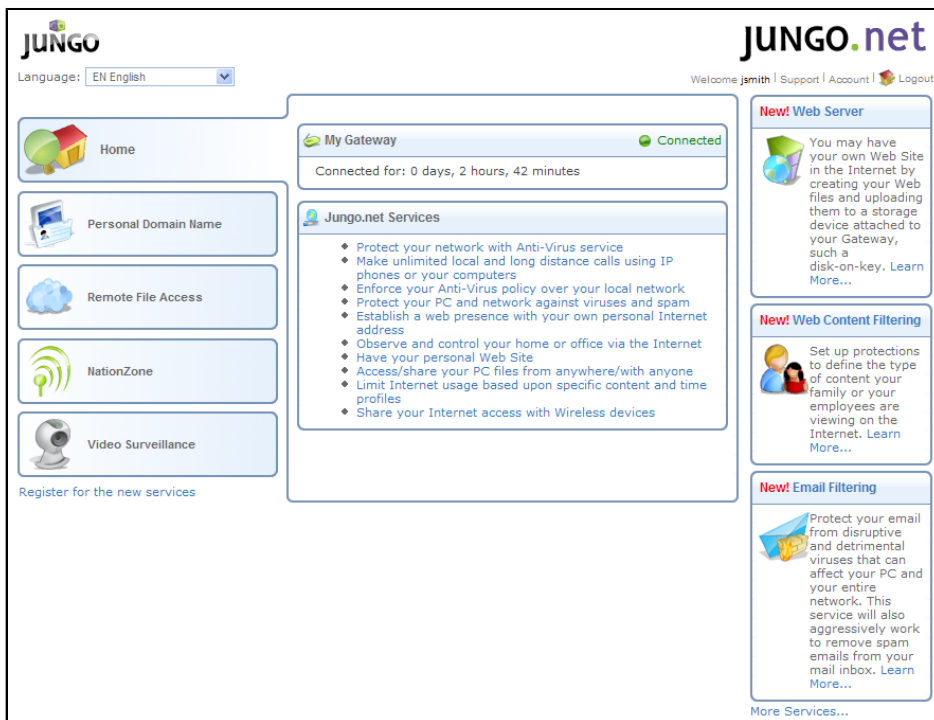


Figure 7.67. Homepage — Video Surveillance Tab

Once a camera is installed, test the service as follows:

1. Click the 'Video Surveillance' tab. Junglo.net searches for the camera connected to the gateway. Once it is found, the following screen appears.

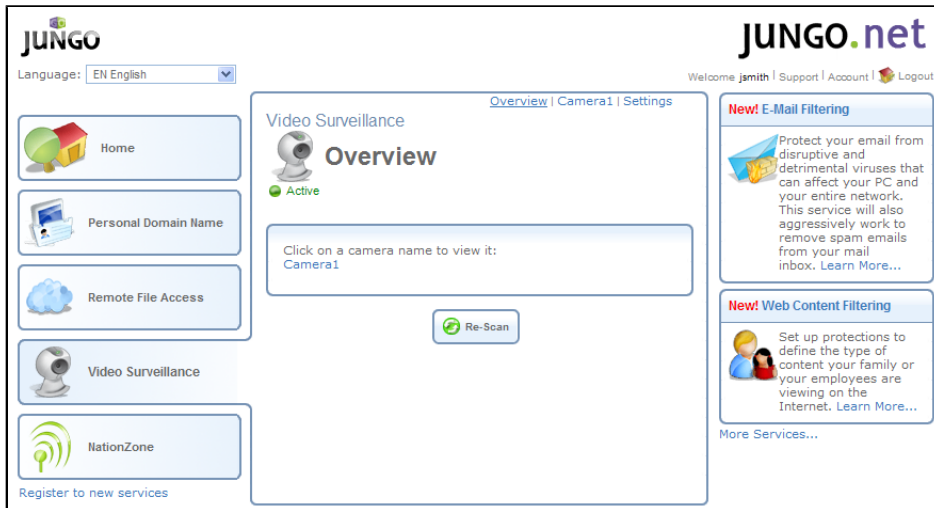


Figure 7.68. Video Surveillance Overview

2. Click the camera link displayed in the 'Video Surveillance Overview' screen. You will see the area on which the camera is focused.

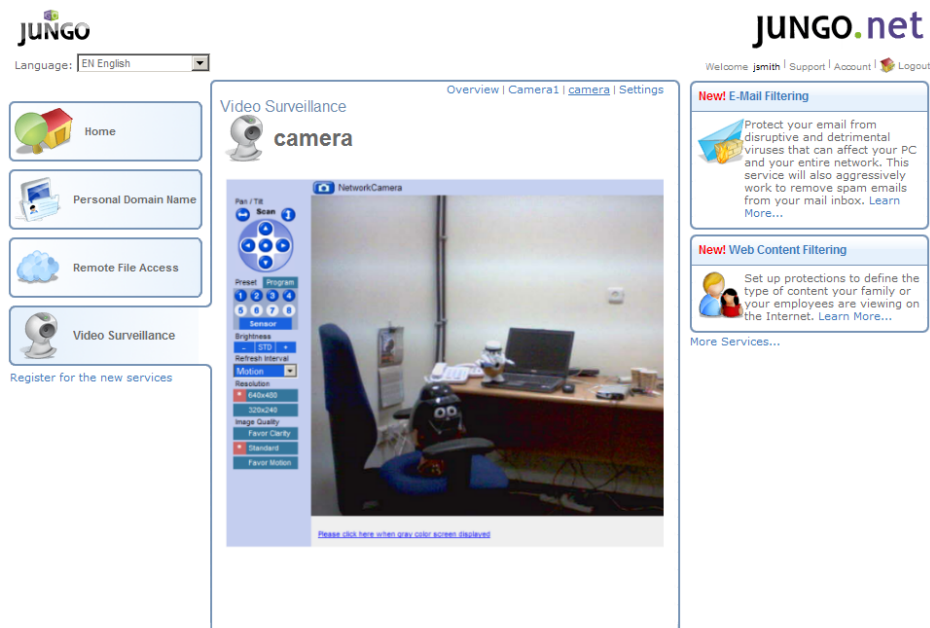


Figure 7.69. Surveilled Area

You can view the settings of your cameras by clicking the 'Settings' link. The 'Settings' screen appears.

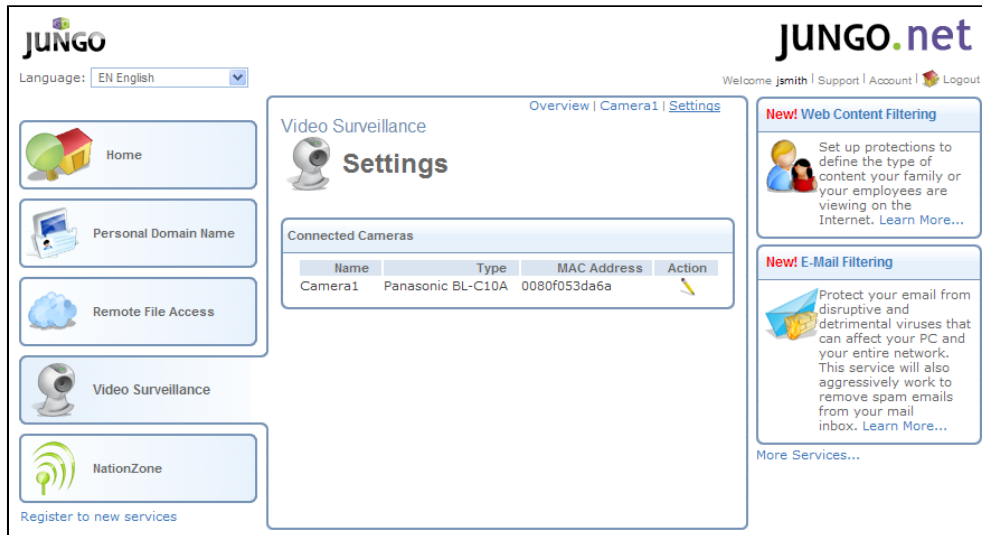


Figure 7.70. Video Surveillance Settings

You can rename a camera by clicking its  action icon . The following screen appears.

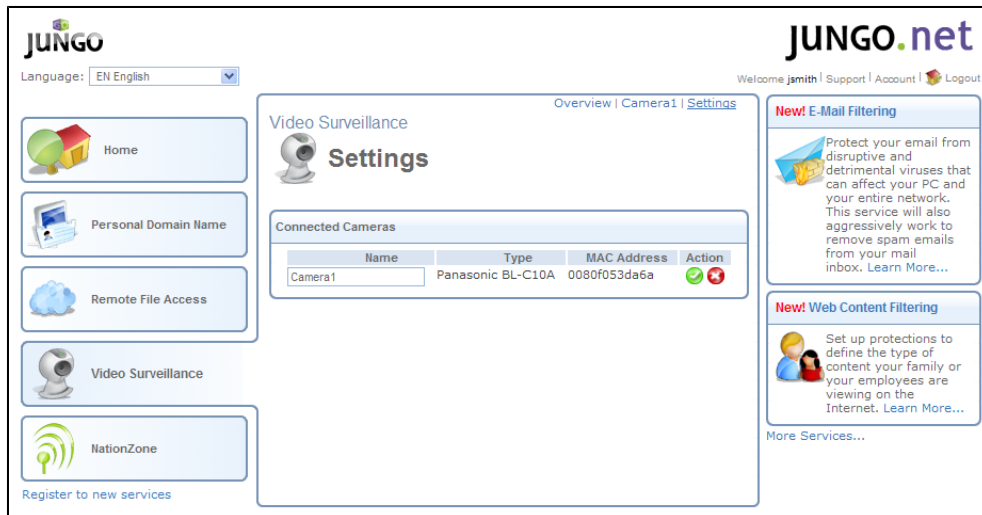




Figure 7.71. Rename Camera

Enter a new name for the camera and click the  action icon . Otherwise, click the  action icon to return to the 'Settings' screen.

7.2.4.7. NationZone

NationZone is a service that enables you to share your wireless Internet connection in a secure and effective way. Only authorized wireless clients will be able to use your Internet connection. Moreover, the wireless clients will not be able to view or access your local network. When this service is activated, the Jungo.net portal automatically configures OpenRG's firewall to secure your LAN, and adds a virtual access point to OpenRG's network devices. This virtual access point is assigned a unique wireless network name, or a Service Set Identifier (SSID), called "NationZone". In addition, Jungo.net configures OpenRG's QoS so that the authorized wireless clients will be granted a total bandwidth of 1000 Kbps for downloading, and 100 Kbps for uploading. To activate the service, perform the following:

1. Click the 'NationZone' link. The 'Overview' screen appears.



Figure 7.72. NationZone Overview

2. Read the service description. For additional information, click the 'Information' link.
3. Click 'Activate Now'. The 'Order New Service' screen appears.

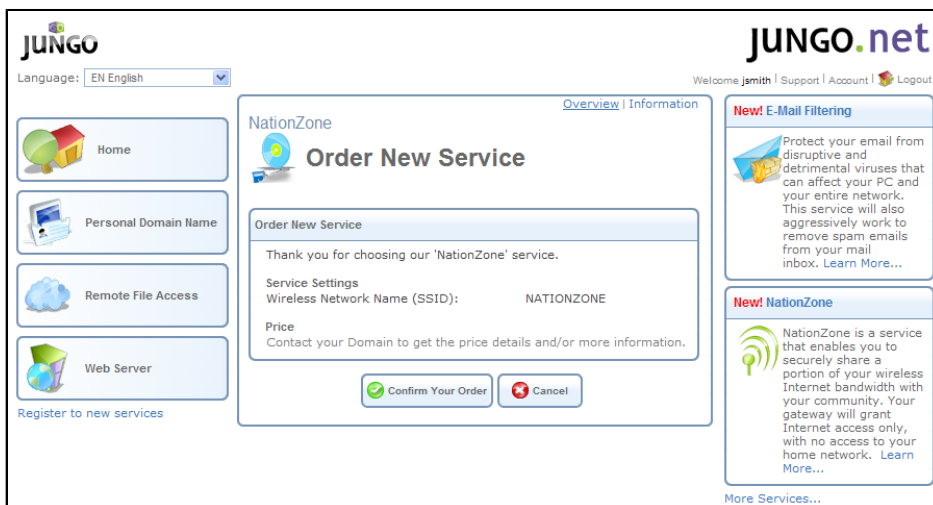


Figure 7.73. Order New Service

4. Click 'Confirm your Order'. After configuring your gateway, the order confirmation screen appears.

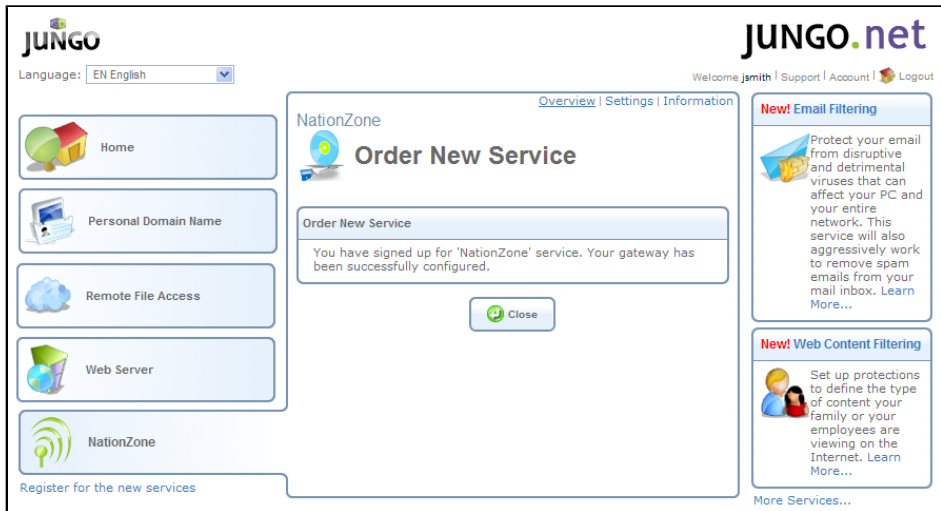


Figure 7.74. Service Order Confirmation

5. Click 'Close'. The homepage appears, with the 'NationZone' tab being added to it.

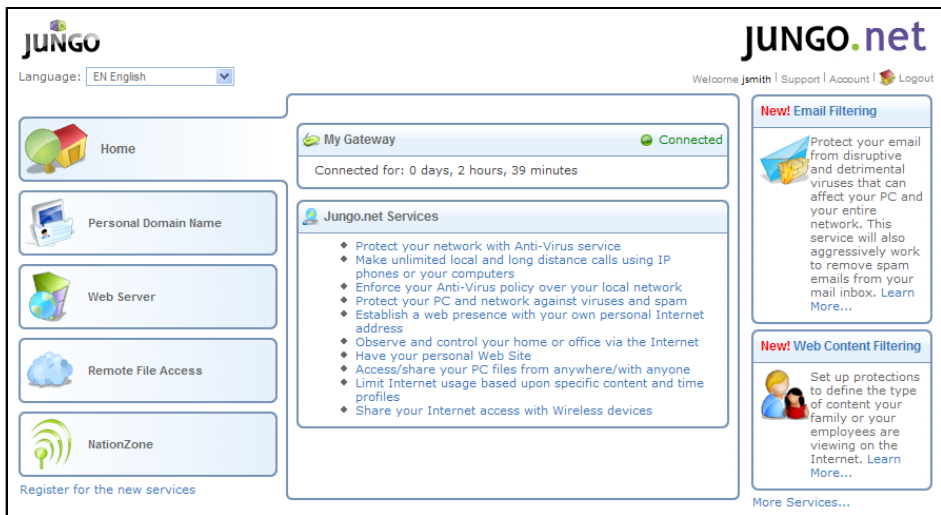


Figure 7.75. Homepage — NationZone Tab

6. Click the 'NationZone' tab. The 'Overview' screen appears, with the service state changed to 'Active'.

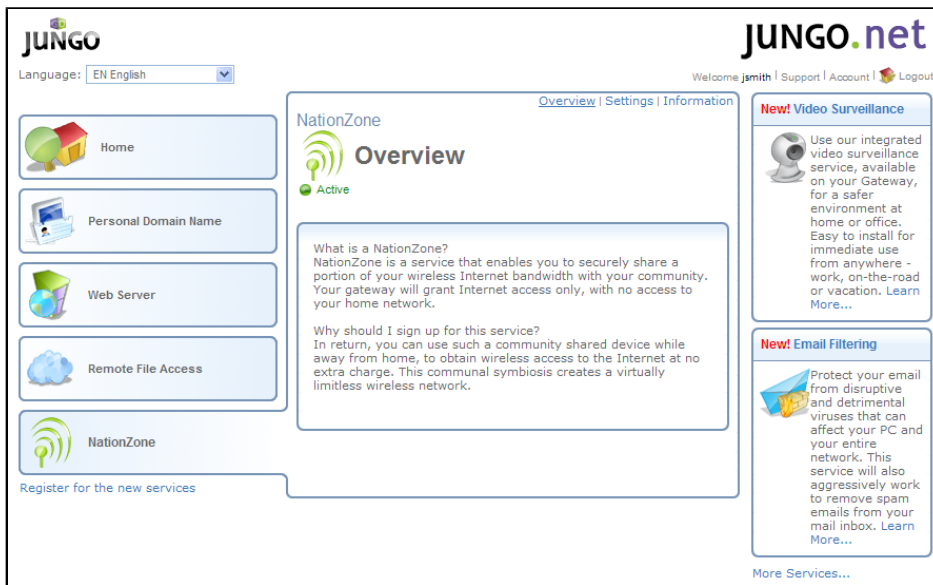


Figure 7.76. NationZone Overview

To access the service's settings, click the 'Settings' link. The 'Settings' screen appears.

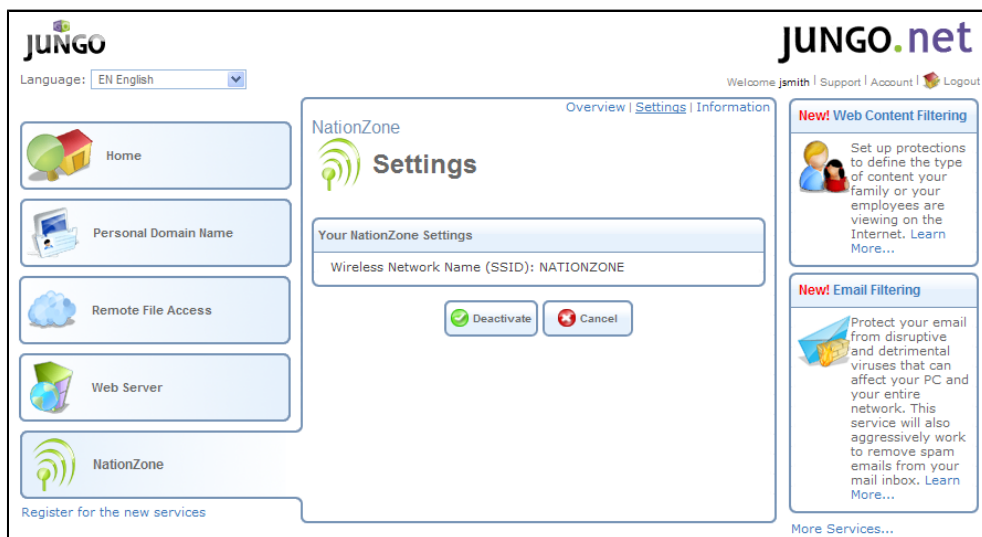


Figure 7.77. NationZone Settings

The 'Settings' screen enables you to deactivate or reactivate the service by clicking the 'Deactivate' or 'Activate' button respectively. In case of restoring OpenRG's default settings or changing some of your wireless connection settings, the 'NationZone' service will stop functioning. To reconfigure OpenRG with the service's settings, perform the following:

1. In the service's 'Overview' screen (see [Figure 7.76](#)), click the 'Configure My Settings' link. The 'Your Jungo.net Account' screen appears.

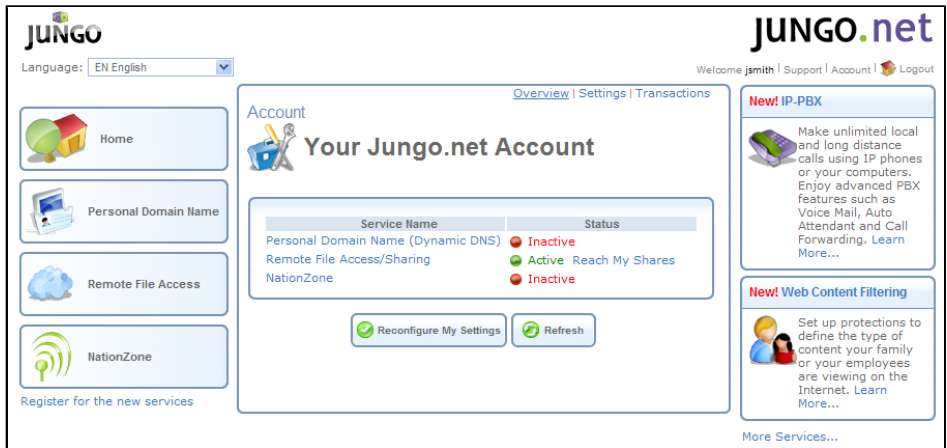


Figure 7.78. Your Jungo.net Account

2. Click the 'Reconfigure My Settings' button. The Jungo.net portal reconfigures OpenRG with the service settings.

To view the effect on your gateway settings, click the WBM's 'Local Network' tab, and then 'Devices'. The 'Device' screen appears, displaying all network devices located under OpenRG's LAN bridge, and the virtual access point that is connected separately.

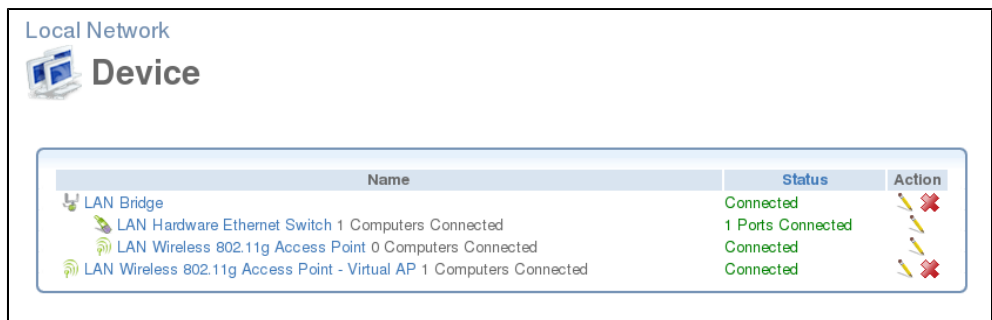



Figure 7.79. Network Devices

To view the virtual access point's properties, click its link or the  action icon . The following screen appears.

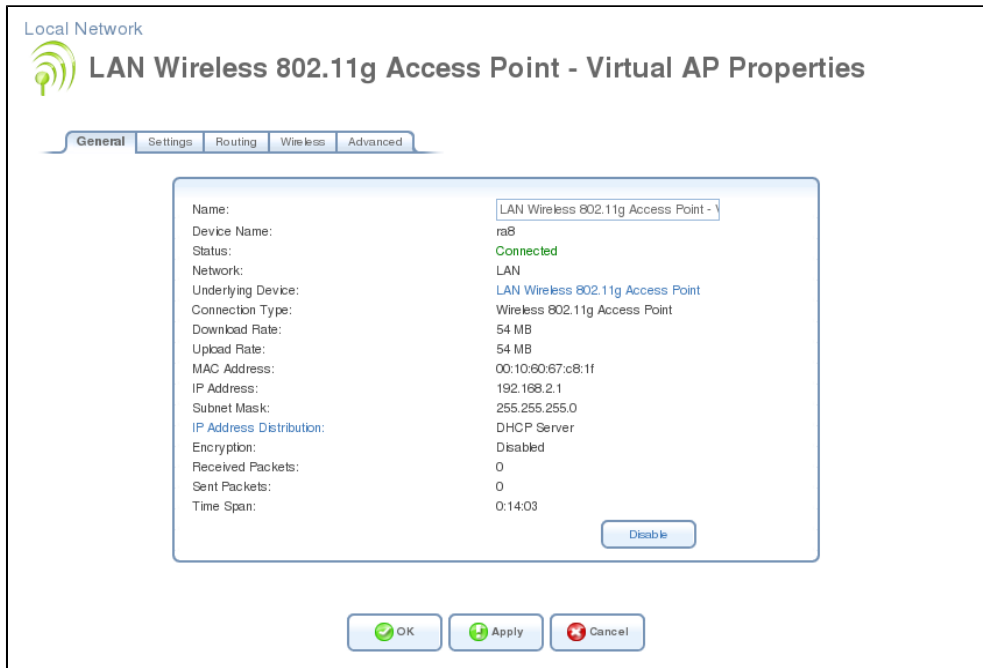


Figure 7.80. Virtual Access Point's Properties

To view its settings, click the screen's 'Settings' tab. The following screen appears.

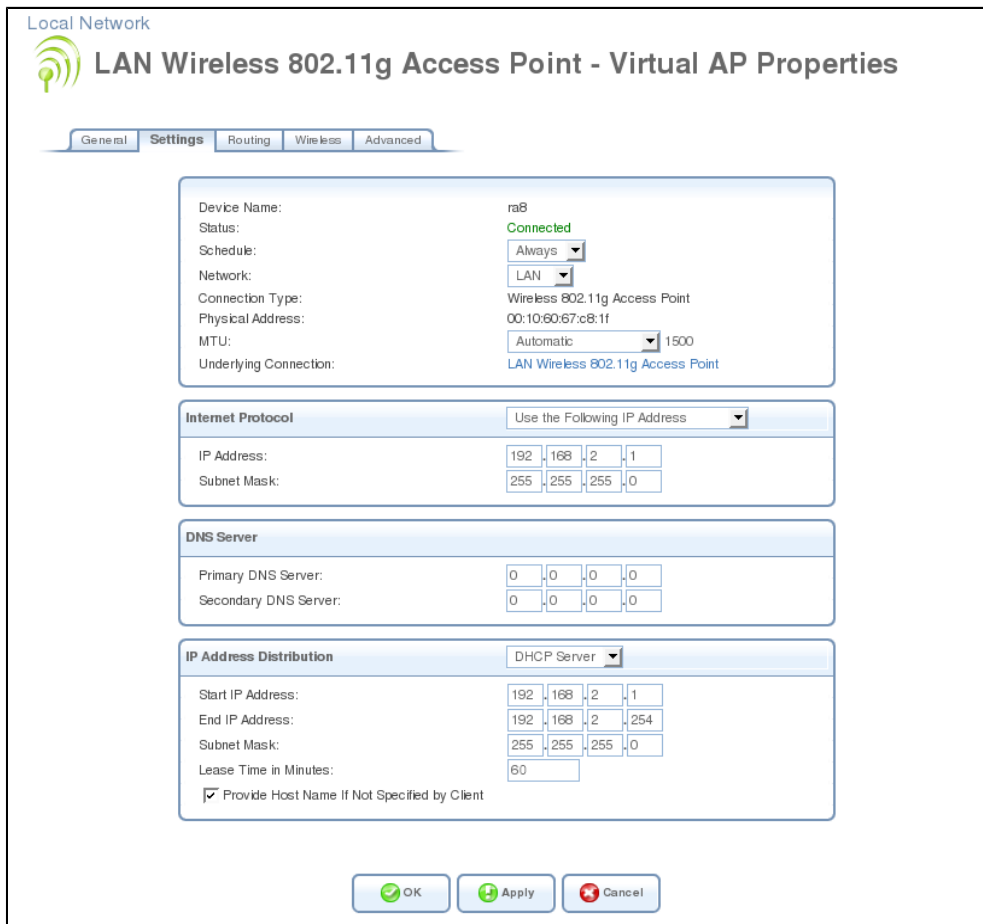


Figure 7.81. Virtual Access Point's Settings

To view the changes in OpenRG's QoS, perform the following:

1. In OpenRG's WBM, click the 'Services' tab, and then 'QoS'. The 'General' screen appears.

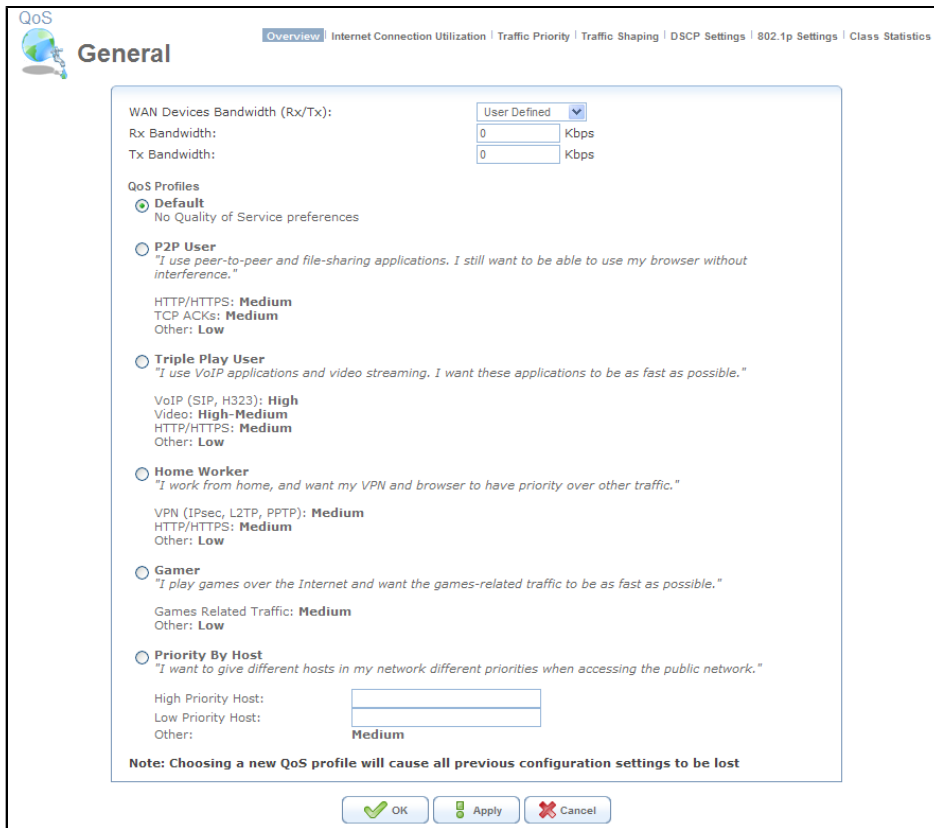


Figure 7.82. General

2. Click the 'Traffic Shaping' link. The 'Traffic Shaping' screen appears.

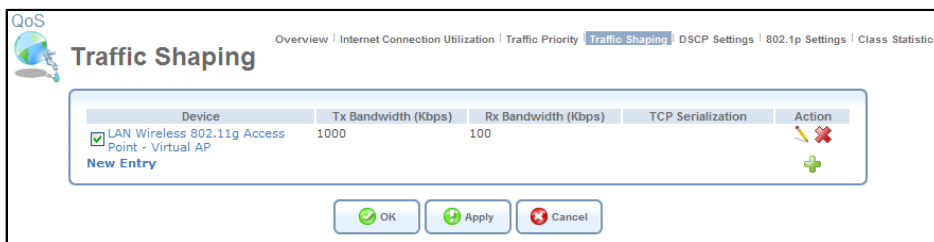


Figure 7.83. Traffic Shaping for the Virtual Access Point

OpenRG's virtual LAN wireless access point is configured with the following parameters:

Tx Bandwidth (Downstream): 1000 Kbps

Rx Bandwidth (Upstream): 100Kbps

This bandwidth will be distributed between all authorized wireless clients located in your area. A wireless client can see the "NationZone" SSID of OpenRG's virtual access point. When trying to connect to the Internet, this client is redirected to the NationZone authentication page.

Figure 7.84. Login Page


To access this page and surf the Internet for free, the wireless client must have a Jungo.net account and a gateway on which the NationZone service is enabled. If the client's gateway supports NationZone, but this service has not been enabled yet, the following screen appears.

Figure 7.85. Welcome Screen — Selecting AccessType

In this case, the client can either activate this service on the gateway and surf for free, or access the NationZone portal as a guest, after paying with a credit card. If the per-access payment option is selected, the following screen appears.

Figure 7.86. Welcome Screen — Payment Form

After entering the required contact information and the credit card details, the client must click 'OK' to confirm the service request.

 **Note:** A password can be stored in the portal's database for automatic identification and payment in case of a future use of the service.

If the entered information is valid, the following page appears, and the client can surf the Internet through your OpenRG's WAN connection.

Figure 7.87. Login Successful

If a client's gateway is connected to the Jungo.net portal, but it does not support the NationZone service (the gateway does not have a wireless network device, or the firmware is not updated), the client can still obtain this service as follows:

1. When accessing the NationZone portal, the following screen appears.

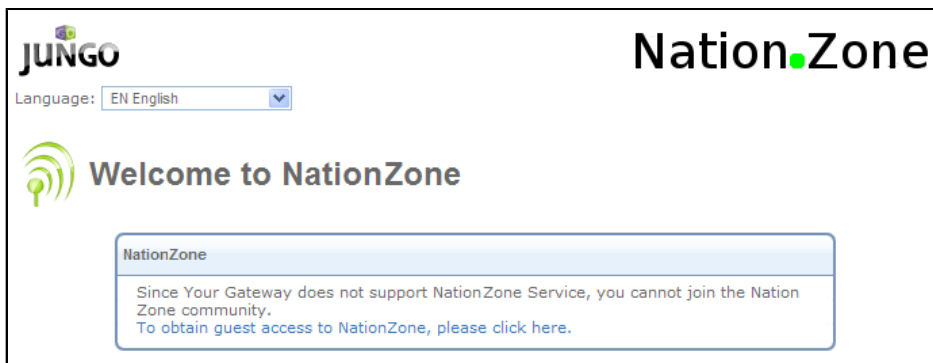


Figure 7.88. Welcome Screen — NationZone is Unsupported

2. To continue with the Internet access request, the client must click the following link: 'To obtain guest access to NationZone, please click here.' The payment form appears (see [Figure 7.86](#)).
3. After entering the required contact information and the credit card details, the client clicks 'OK' to confirm the service request and to start surfing the Internet.

Finally, if the wireless client does not have a Jungo.net account, the NationZone's guest access can be purchased by clicking its link in the **Not a Jungo.net Customer?** section of the NationZone authentication page. The payment form appears (see [Figure 7.86](#)). After having paid, the client obtains Internet access.

7.2.5. Restoring OpenRG's Configuration from Jungo.net

OpenRG's configuration file (**rg_conf**) contains all the entries that determine how OpenRG is configured. This file is updated with every configuration change made to OpenRG. If, for any reason, OpenRG must be restored to a previous state, other than the factory default settings, it is possible to do so with a saved configuration file. For this purpose, when OpenRG connects to Jungo.net, its configuration file is saved on the server. The file is saved again every 24 hours thereafter. You can restore OpenRG to a previous configuration using such a saved configuration file.

To restore a configuration file saved on the Jungo.net server, perform the following:

1. Browse to Jungo.net. The login page appears.



Figure 7.89. Jungo.net Login Page

2. Enter your username and password, and click 'OK'.
3. Under the 'Account' tab, click the 'Settings' link, and then click the 'System Restore' sub-link. The 'System Restore' screen appears.



Figure 7.90. System Restore

This screen displays the configuration files time of saving. Each entry can be used as restoration point.

4. Select a restoration point and click one of the following buttons:
 - **Restore to Gateway** Use this option to restore OpenRG's settings with this configuration file. The following warning appears.

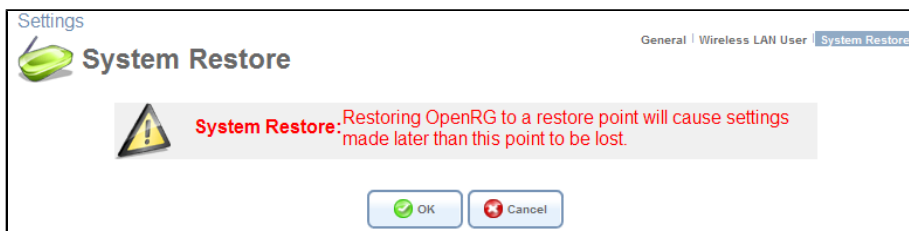


Figure 7.91. System Restore Warning

Click 'OK' to proceed. The screen refreshes as the file is loaded, until the 'A new configuration file was successfully uploaded to gateway' message appears.

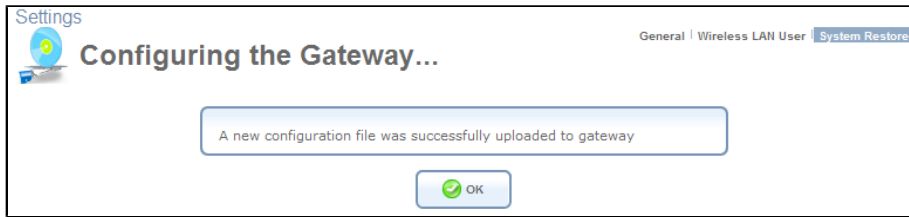


Figure 7.92. Configuration File Uploaded Successfully

- **Download Configuration File** Use this option to download the configuration file to disk. A standard file download dialogue window appears. Select 'Save' and choose a location for saving the **OpenRG.conf** file.

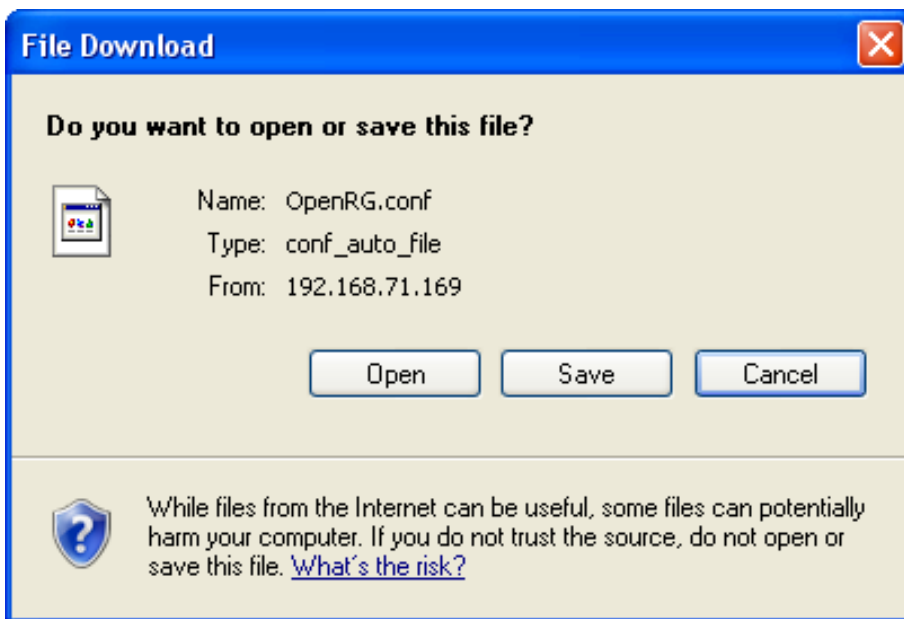


Figure 7.93. Windows Download Dialogue

- **View Configuration File** Use this option to view the configuration file's contents. The 'Configuration File' screen appears.

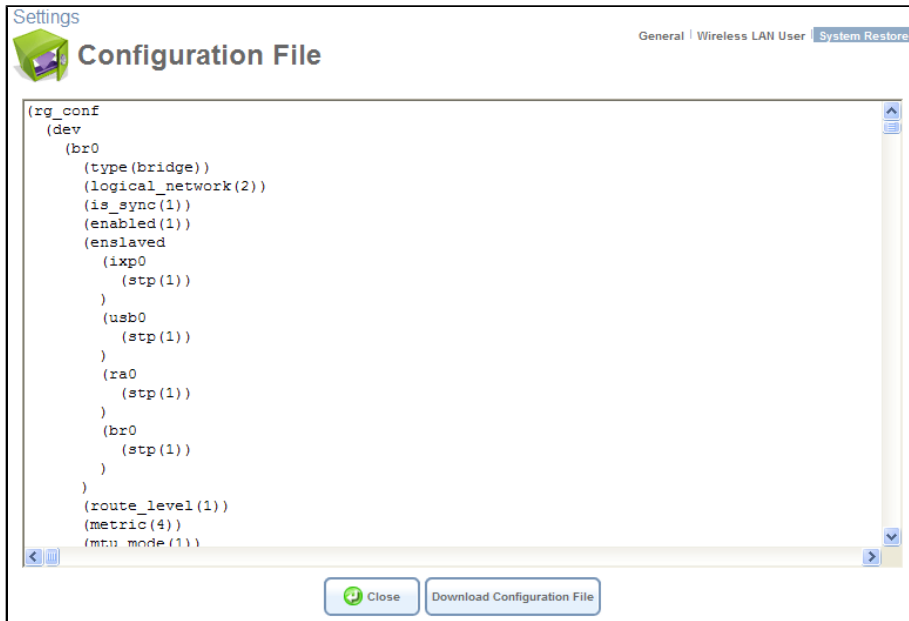


Figure 7.94. Configuration File

7.3. Firewall

OpenRG'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, RG-FW OpenRG™, the cornerstone of your gateway's security suite, has been exclusively tailored to the needs of the residential/office user and has been pre-configured to provide optimum security (see [Figure 7.95](#)).

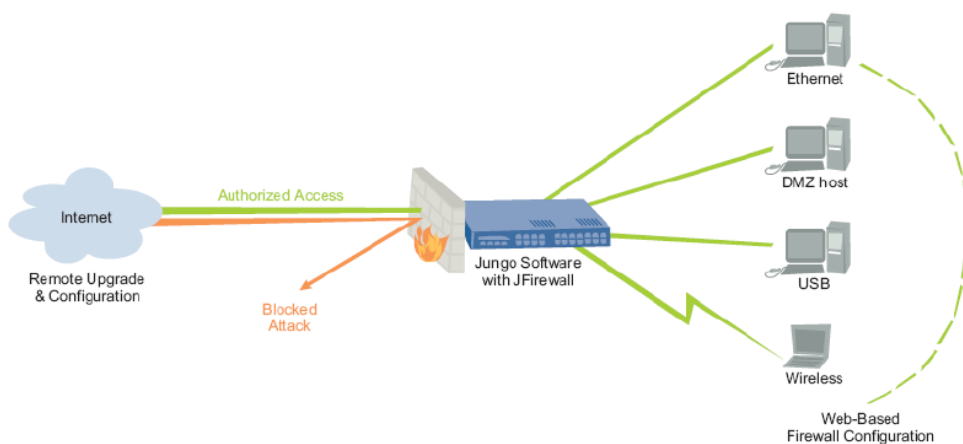


Figure 7.95. OpenRG's Firewall in Action

OpenRG'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 OpenRG 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.

7.3.1. Configuring Basic Security Settings

The 'General' screen enables you to configure the gateway's basic security settings.

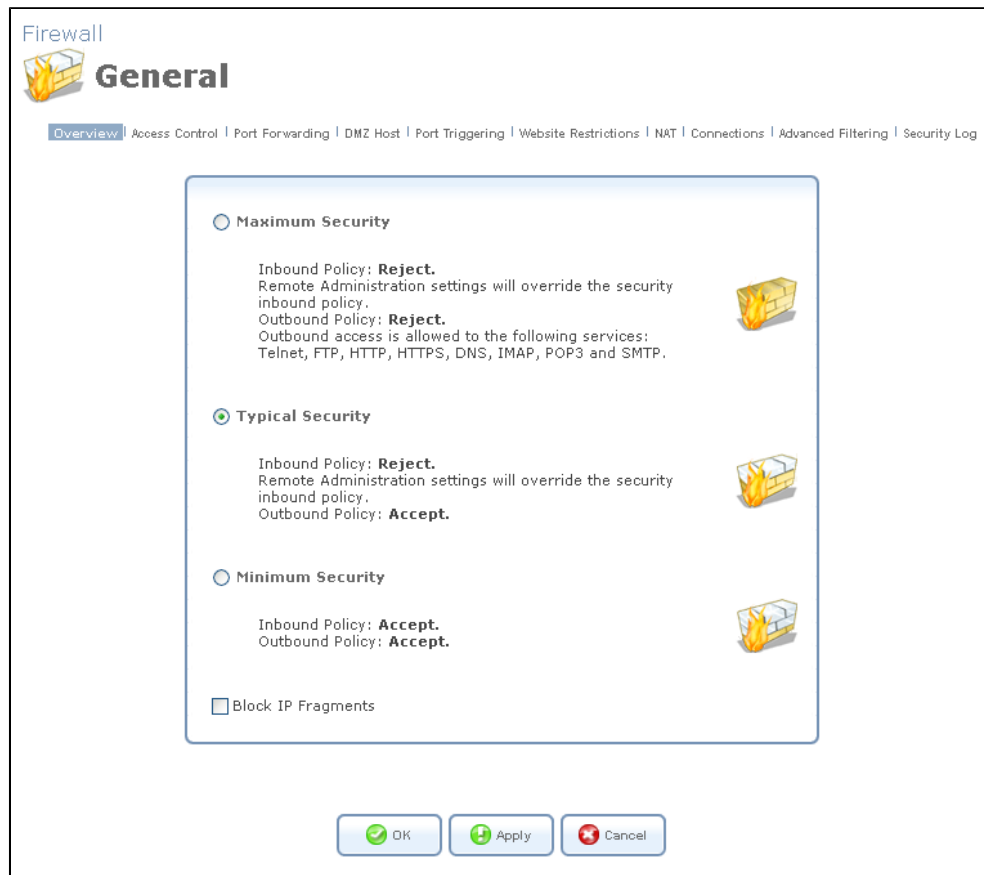


Figure 7.96. General

You may choose between three pre-defined security levels for OpenRG: Minimum, Typical, and Maximum. The following table summarizes OpenRG's behavior for each of the three security levels.

Security Level	Requests Originating in the WAN (Incoming Traffic)	Requests Originating in the LAN (Outgoing Traffic)
Maximum Security (Default)	<i>Blocked:</i> No access to home network from Internet, except as configured in the Port Forwarding, DMZ host and Remote Access screens	<i>Limited:</i> By default, only commonly-used services, such as Web-browsing and e-mail, are permitted. The list of allowed services can be edited

Security Level	Requests Originating in the WAN (Incoming Traffic)	Requests Originating in the LAN (Outgoing Traffic)
		in the Access Control screen (refer to Section 7.3.2)
Typical Security	<i>Blocked:</i> No access to home network from Internet, except as configured in the Port Forwarding, DMZ host and Remote Access screens	<i>Unrestricted:</i> All services are permitted, except as configured in the Access Control screen
Minimum Security	<i>Unrestricted:</i> Permits full access from Internet to home network; all connection attempts permitted	<i>Unrestricted:</i> All services are permitted, except as configured in the Access Control screen

Table 7.1. OpenRG's Firewall Security Levels

To configure OpenRG's basic security settings, perform the following:

1. Choose between the three predefined security levels described in the table above.



Note: Using the *Minimum Security* setting may expose the home network to significant security risks, and thus should only be used, when necessary, for short periods of time.

2. Check the 'Block IP Fragments' box in order to protect your home network from a common type of hacker attack that could make use of fragmented data packets to sabotage your home network. Note that VPN over IPSec and some UDP-based services make legitimate use of IP fragments. In case of enabling these services, you will need to allow IP fragments to pass into the home network.
3. Click 'OK' to save the settings.

By default, the selected security level is applied on such services as Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3 and SMTP. Note that some applications (such as some Internet messengers and Peer-To-Peer client applications) tend to use ports of the above-mentioned services, if these applications cannot connect using their own default ports. When allowing this behavior, the applications' outbound connection requests will not be blocked, even at the Maximum Security level.

After the security level is set, 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 OpenRG) or rejected (barred from passing through OpenRG), 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 from 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 browser to a Web page, a request is sent out to the Internet for retrieving and loading this page. When the request reaches OpenRG, the firewall identifies the request's 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 (refer to [Section 7.3.2](#) for more on setting OpenRG's access control).

When the Web page is returned from the Web server, the firewall associates it with this session and allows it to pass, regardless of whether HTTP access from the Internet to the home network is blocked or permitted. It is the *origin of the request*, not the subsequent responses to this request, that determines whether a session can be established or not.

7.3.2. Controlling Access to Internet Services

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 e-mail (by blocking the *outgoing* requests to POP3 servers on the Internet). The 'Access Control' screen enables you to define 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.

- To allow or restrict services:
 1. Click 'Access Control' under the Firewall menu item. The 'Access Control' screen appears.

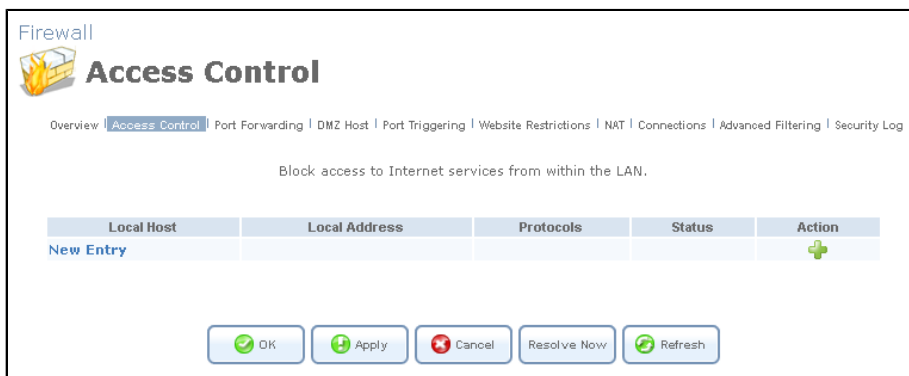


Figure 7.97. Access Control

2. Click the 'New Entry' link. The 'Add Access Control Rule' screen appears.



Figure 7.98. Add Access Control Rule

3. The 'Address' drop-down menu enables you to specify the computer or group of computers on which you would like to apply the access control rule. Select an address or a name from the list to apply the rule on the corresponding host, or 'Any' to apply the rule on all OpenRG's LAN hosts. If you would like to add a new address, select the 'User Defined' option in the drop-down menu. This will commence a sequence that will add a new **Network Object**, representing the new host. Refer to [Section 8.9.2](#) in order to learn how to do so.
4. The 'Protocol' drop-down menu enables you to select or specify the type of protocol that will be used. Selecting the 'Show All Services' option expands 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. Refer to [Section 8.9.2](#) in order to learn how to do so.
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 deselected, the client's packets are simply ignored and no notification is issued.
6. 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. To learn how to configure scheduler rules, refer to [Section 8.9.3](#).
7. Click 'OK' to save your changes. The 'Access Control' screen displays a summary of the rule that you have just added.

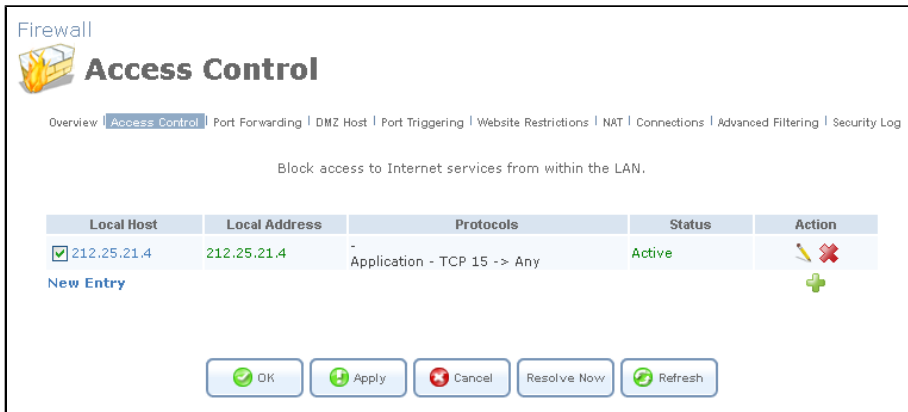



Figure 7.99. Access Control Rule

You may edit the access control rule by modifying its entry displayed under the 'Local Host' column.

- To modify a rule's entry:

1. Click the rule's  action icon . The 'Edit Access Control Rule' screen appears. This screen allows you to edit all the parameters that you configured when creating the access control rule.

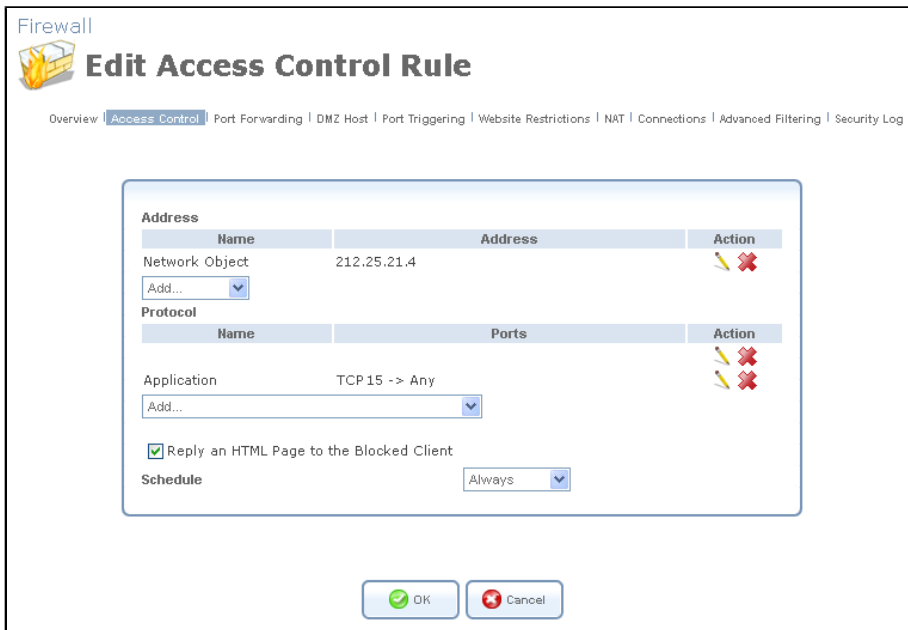



Figure 7.100. Edit Access Control Rule

2. Click 'OK' to save your changes and return to the 'Access Control' screen.

You can disable an access control rule in order to make a service available without having to remove the rule from the 'Access Control' screen. This may be useful if you wish to make the service available only temporarily, intending to reinstate the restriction in the future.

- To temporarily disable a rule, clear the check box next to the service name.

- To reinstate it at a later time, simply reselect the check box.
- To remove a rule, click the service's  action icon . The service will be permanently removed.



Note: When the Parental Control service is enabled (refer to [Section 7.8](#)), HTTP services cannot be blocked by Access Control.

7.3.3. Using Port Forwarding

In its default state, OpenRG blocks all external users from connecting to or communicating with your network. Therefore, the system is safe from hackers who may try to intrude into the network and damage it. However, you may wish to expose your network to the Internet in certain limited and controlled ways. The Port Forwarding feature enables you to do so. If you are familiar with networking terminology and concepts, you may have encountered the port forwarding capability referred to as "Local Servers".

The 'Port Forwarding' screen enables you to define applications (such as Peer-to-Peer, game, voice, chat programs, etc.) that will be allowed a controlled Internet activity. For example, if you wish to use a File Transfer Protocol (FTP) application on one of your PCs, you would simply create a port forwarding rule, which specifies that all FTP-related data arriving at OpenRG 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 would like to host a Web server inside your home network. When an Internet user points a browser to OpenRG's external IP address, the gateway will forward the incoming HTTP request to your Web server, if the corresponding port forwarding rule had been set.

However, there is a limitation that must be considered. With one external IP address (OpenRG'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. OpenRG 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' (refer to [Section 7.3.7](#)). 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 for which it was designated. For example, 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 OpenRG via HTTP (by default, on port 80). To accomplish this, you will have to define a port forwarding rule for the HTTP service, with the PC's IP or host name, as well as specify 8080 in the 'Forward to Port' field. All incoming HTTP traffic will be forwarded to the PC running the Web server on port 8080.

When creating a port forwarding rule, you must first ensure that the port number you enter 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. For more details, refer to [Section 7.6.8.3](#).



Note: Some applications, such as FTP, TFTP, PPTP and H323, require the support of special specific Application Level Gateway (ALG) modules in order to work inside the home network. Data packets associated with these applications contain information that allows them to be routed correctly. An ALG is needed to handle these packets and ensure that they reach their intended destinations. OpenRG is equipped with a robust list of ALG modules in order to enable maximum functionality in the home network. The ALG is automatically assigned based on the destination port.

7.3.3.1. Adding a Port Forwarding Rule

To add a new port forwarding rule, perform the following:

1. Click 'Port Forwarding' under the 'Firewall' menu item. The 'Port Forwarding' screen appears.



Figure 7.101. Port Forwarding

2. Click the 'New Entry' link. The 'Add Port Forwarding Rule' screen appears.

Figure 7.102. Add Port Forwarding Rule

If you would like to apply this rule on OpenRG's non-default IP address (which you can define in the 'NAT' screen, as described in [Section 7.3.7](#)), perform the following:

- a. Select the 'Specify Public IP Address' check box. The screen refreshes.

Figure 7.103. Specify Public IP Address

- b. Enter the additional external IP address in the 'Public IP Address' field.
3. In the 'Local Host' field, enter the host name or IP address of the computer that will provide the service (the "server"). 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.
 4. The 'Protocol' drop-down menu enables you to select or specify the type of protocol that will be used. Selecting the 'Show All Services' option expands 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. Refer to [Section 8.9.2](#) in order to learn how to do so.
 5. By default, OpenRG will forward traffic to the same port as its incoming port. If you wish to redirect traffic to a different port, select the 'Specify' option. The screen refreshes, and an additional field appears, enabling you to enter the port number.

Forward to Port:

Figure 7.104. Forward to a Specific Port

6. 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. To learn how to configure scheduler rules, refer to [Section 8.9.3](#).
7. Click 'OK' to save your changes. The 'Port Forwarding' screen displays a summary of the rule that you have just added.

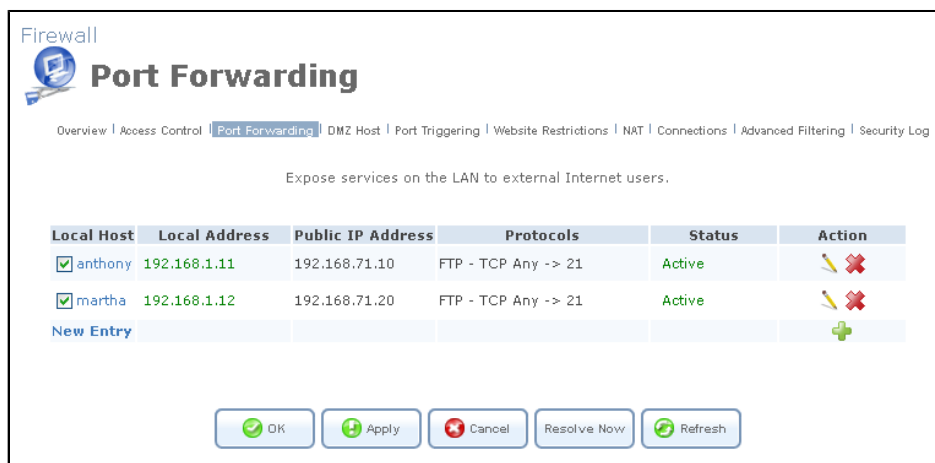


Figure 7.105. Port Forwarding Rule

You may edit the port forwarding rule by clicking its entry under the 'Local Host' column in the 'Port Forwarding' screen. You can also disable the rule in order to make a service unavailable without having to remove the rule from the 'Port Forwarding' screen. This may be useful if you wish to make the service unavailable only temporarily, intending to reinstate it in the future.

- To temporarily disable a rule, clear the check box next to the service name.
- To reinstate it at a later time, simply reselect the check box.
- To remove a rule, click the service's action icon. The service will be permanently removed.

All the computers in the local network can simultaneously use a specific service as clients. Being a client means that the computer within the network initiates the connection—for example, opens an FTP connection with an FTP server on the Internet. However, only one computer can serve as a server, responding to requests from computers on the Internet.

7.3.3.2. A Port Forwarding Example

In order to allow external access (from the WAN) to a server inside your LAN, you must configure OpenRG's firewall, by adding a port forwarding rule. The following example demonstrates how to allow such access to an HTTP server located inside OpenRG's LAN.

When remote administration is enabled on OpenRG, an attempt to browse to OpenRG's WBM from a WAN PC will yield the WBM's 'Home' page. However, when the following port forwarding rule is defined on OpenRG, an attempt to browse to OpenRG's WBM from a WAN PC will yield the HTTP server located on the LAN.

To enable remote administration, perform the following:

1. From a LAN PC, browse to OpenRG's WBM and click 'Advanced'.
2. Click the 'Remote Administration' icon, and select the 'Using Primary HTTP Port (80)' check box in the screen that appears.

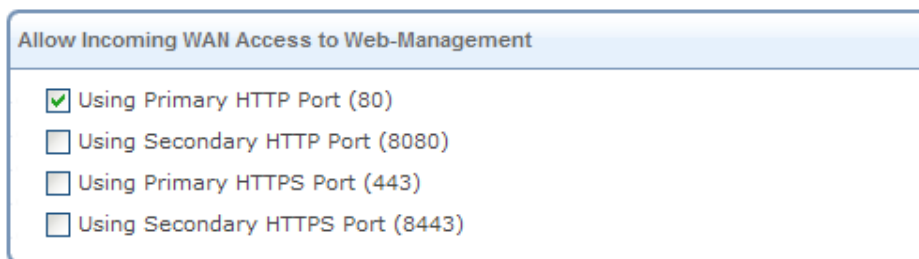


Figure 7.106. Allow Incoming WAN Access to Web-Management

3. Click 'OK' to save the settings.
4. Verify that remote administration is enabled, by accessing OpenRG's WBM from a WAN PC.

To define a port forwarding rule, perform the following:

1. In OpenRG's WBM, select the 'Firewall' menu item under the 'Services' tab.
2. Select 'Port Forwarding', and click 'New Entry'.
3. In the 'Local Host' field, enter the LAN server's PC name or IP address. In the 'Protocol' drop-down menu, select the 'HTTP' protocol.

Figure 7.107. Add Port Forwarding Rule

4. Click 'OK' to save the settings.
5. To verify that port forwarding takes place, access OpenRG's WBM from a WAN PC. You should be redirected to the LAN HTTP server.

You may disable the port forwarding rule by deselecting its check box in the 'Port Forwarding' screen. If you try to access the local server from the WAN, the HTTP server will not be accessible, and OpenRG's WBM 'Home' page will appear instead.

7.3.4. Designating a DMZ Host

The DMZ (Demilitarized) Host feature enables you to expose one local computer 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.



Warning: 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 accessing a service in the home network, such as a Web server, is fielded by OpenRG. OpenRG will forward this request to the DMZ host if one is designated, unless the service is being provided by another LAN PC (defined in a Port Forwarding rule), in which case that PC will receive the request instead.

- To designate a local computer as a DMZ Host:
 1. Click 'DMZ Host' under the 'Firewall' menu. The 'DMZ Host' screen appears.

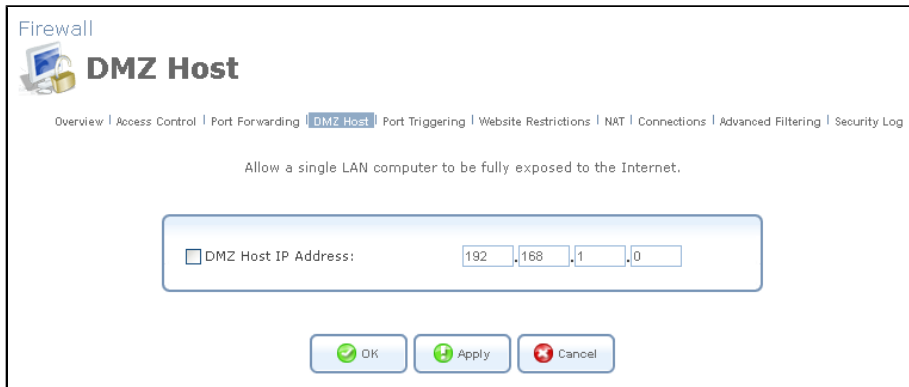


Figure 7.108. DMZ Host

2. Select the check box, and enter the local IP address of the computer that you would like to designate as a DMZ host. Note that only one LAN computer may be a DMZ host at any time.
 3. Click 'OK' to save the settings.
- You can disable the DMZ host so that it will not be fully exposed to the Internet, but will keep its IP address recorded in the 'DMZ Host' screen. To do so, clear the check box next to the DMZ IP field, and click 'OK'. This may be useful if you wish to temporarily disable the DMZ host, intending to enable it again in the future.
 - To reinstate it at a later time, reselect the check box.

7.3.5. Using Port Triggering

Port triggering is used for setting a 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 the 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 OpenRG'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. To do so, perform the following:

1. Click the 'Port Triggering' link under the 'Firewall' menu item. The 'Port Triggering' screen appears. This screen will list all of the port triggering entries.

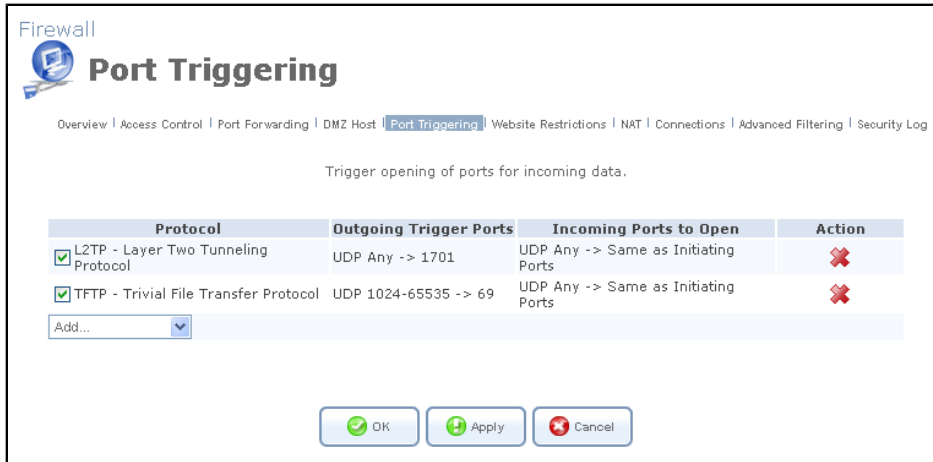


Figure 7.109. Port Triggering

2. Select the 'User Defined' option to add an entry. The 'Edit Port Triggering Rule' screen appears.

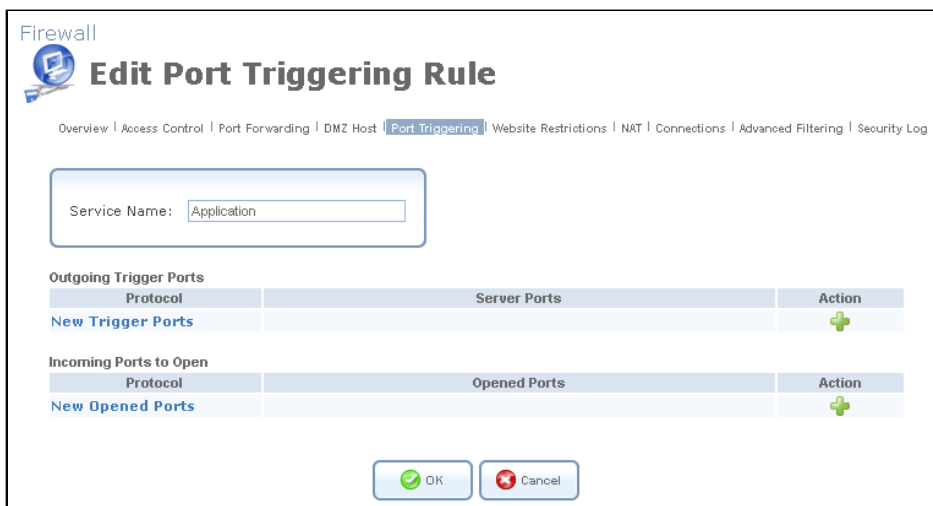
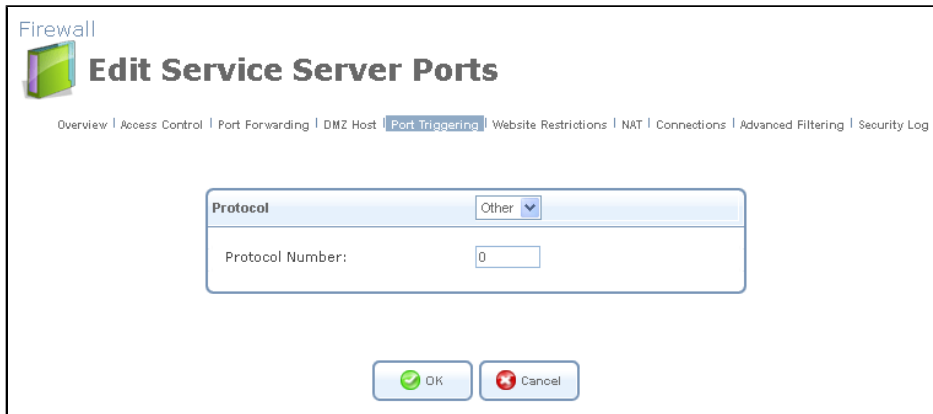


Figure 7.110. Edit Port Triggering Rule

3. Enter a name for the service (e.g. "game_server"), and click the 'New Trigger Ports' link. The 'Edit Service Server Ports' screen appears.



Firewall

Edit Service Server Ports

Overview | Access Control | Port Forwarding | DMZ Host | **Port Triggering** | Website Restrictions | NAT | Connections | Advanced Filtering | Security Log

Protocol: Other

Protocol Number: 0

OK Cancel

Figure 7.111. Edit Service Server Ports

- From the 'Protocol' drop-down menu, select 'UDP'. The screen will refresh, providing source and destination port options (see [Figure 7.112](#)).
- Leave the 'Source Ports' drop-down menu at its default "Any". From the 'Destination Ports' drop-down menu, select "Single". The screen will refresh again, providing an additional field in which you should enter "2222" as the destination port.



Protocol: UDP

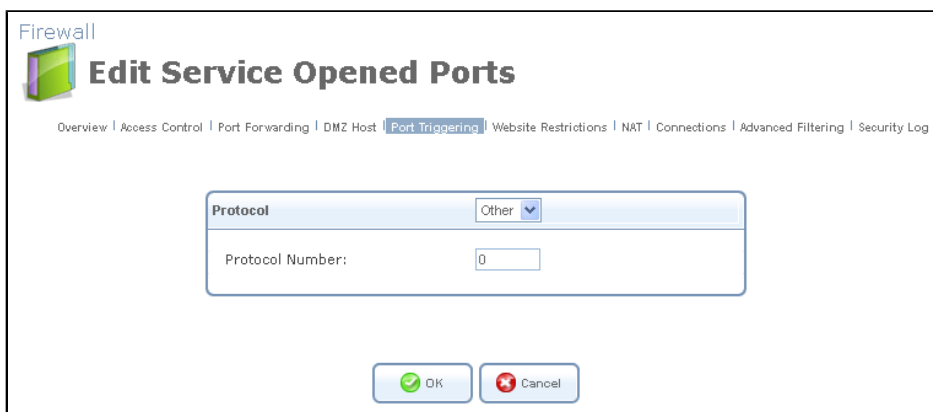
Source Ports: Any

Destination Ports: Single 2222

OK Cancel

Figure 7.112. Edit Service Server Ports

- Click 'OK' to save the settings.
- Back in the 'Edit Port Triggering Rule' screen (see [Figure 7.110](#)), click the 'New Opened Ports' link. The 'Edit Service Opened Ports' screen appears.



Firewall

Edit Service Opened Ports

Overview | Access Control | Port Forwarding | DMZ Host | **Port Triggering** | Website Restrictions | NAT | Connections | Advanced Filtering | Security Log

Protocol: Other

Protocol Number: 0

OK Cancel

Figure 7.113. Edit Service Opened Ports

8. Select UDP as the protocol, leave the source port at "Any", and enter a 3333 as the single destination port.

Figure 7.114. Edit Service Opened Ports


9. Click 'OK' to save the settings. The 'Edit Service' screen will present your entered information. Click 'OK' again to save the port triggering rule. The 'Port Triggering' screen will now include the new port triggering entry.

Protocol	Outgoing Trigger Ports	Incoming Ports to Open	Action
<input checked="" type="checkbox"/> L2TP - Layer Two Tunneling Protocol	UDP Any -> 1701	UDP Any -> Same as Initiating Ports	✘
<input checked="" type="checkbox"/> TFTP - Trivial File Transfer Protocol	UDP 1024-65535 -> 69	UDP Any -> Same as Initiating Ports	✘
<input checked="" type="checkbox"/> game_server	UDP Any -> 2222	UDP Any -> 3333	✎ ✘
Add... <input type="button" value="v"/>			

Figure 7.115. New Port Triggering Rule

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.

- To temporarily disable a rule, clear the check box next to the service name.
- To reinstate it at a later time, simply reselect the check box.
- To remove a rule, click the service's ✘ action icon . The service will be permanently removed.

 Note: There may be a few default port triggering rules listed when you first access the port triggering screen. Disabling these rules may result in impaired gateway functionality.

7.3.6. Restricting Web Access

You can configure OpenRG to block specific websites so that they cannot be accessed from computers in the home network. Moreover, restrictions can be applied according to a comprehensive and automatically updated list of sites to which access is not recommended.

- To block access to a website:
 1. Click the 'Website Restrictions' link under the 'Firewall' menu item.

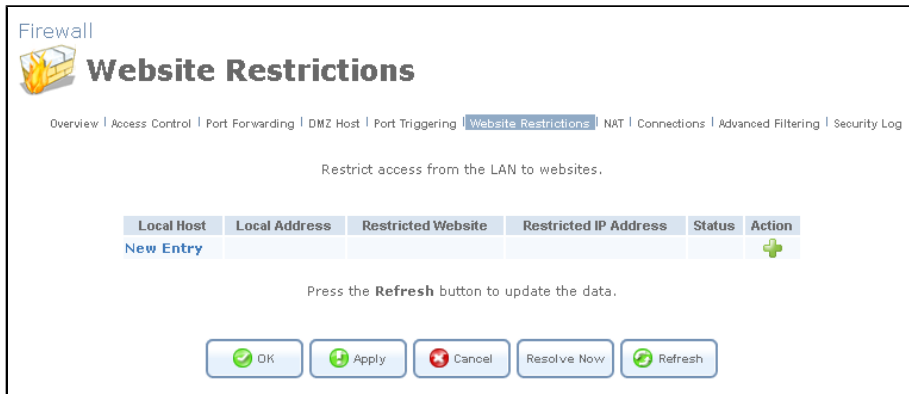


Figure 7.116. Website Restrictions

2. Click the 'New Entry' link. The 'Restricted Website' screen appears.




Figure 7.117. Restricted Website


3. Enter the URL (or part of the URL) that you would like to make inaccessible from your home network (all web pages within this URL will also be blocked). If the URL has multiple IP addresses, OpenRG will resolve all additional addresses and automatically add them to the restrictions table.
4. The 'Local Host' drop-down menu provides you with the ability to specify the computer or group of computers on which you would like to apply the website restriction. Select an address or a name from the list to apply the rule on the corresponding host, or 'Any' to apply the rule on all OpenRG's LAN hosts. If you would like to add a new address, select the 'User Defined' option in the drop-down menu. This will commence a sequence that will add a new **Network Object**, representing the new host. Refer to [Section 8.9.2](#) in order to learn how to do so.
5. 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. To learn how to configure scheduler rules, refer to [Section 8.9.3](#).

6. Click 'OK' to save the settings. You will be returned to the previous screen, while OpenRG 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).
7. Click the 'Refresh' button to update the status if necessary. If the site is successfully located, then 'Resolved' will appear in the status bar. Otherwise, 'Hostname Resolution Failed' will appear. In case OpenRG fails to locate the website, perform the following:
 - a. Use a web browser to verify that the website is available. If it is, then you probably entered the website address incorrectly.
 - b. If the website is not available, return to the 'Website Restrictions' screen at a later time and click the 'Resolve Now' button to verify that the website can be found and blocked by OpenRG.

You may edit the website restriction by modifying its entry under the 'Local Host' column in the 'Website Restrictions' screen.

- To modify an entry:
 1. Click the  action icon for the restriction. The 'Restricted Website' screen appears (see [Figure 7.117](#)). Modify the website address, group or schedule as necessary.
 2. Click the 'OK' button to save your changes and return to the 'Website Restrictions' screen.
- To ensure that all current IP addresses corresponding to the restricted websites are blocked, click the 'Resolve Now' button. OpenRG will check each of the restricted website addresses and ensure that all IP addresses at which this website can be found are included in the IP addresses column.

You can disable a restriction in order to make a website available again without having to remove it from the 'Website Restrictions' screen. This may be useful if you wish to make the website available only temporarily, intending to block it again in the future.

- To temporarily disable a rule, clear the check box next to the service name.
- To reinstate it at a later time, simply reselect the check box.
- To remove a rule, click the service's  action icon . The service will be permanently removed.

7.3.7. Using OpenRG's Network Address and Port Translation

OpenRG features a configurable Network Address Translation (NAT) and Network Address Port Translation (NAPT) mechanism, allowing you to control the network addresses and ports set in 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, OpenRG operates in NAPT routing mode (refer to [Section 8.4.8.3](#)). 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 a single NAT IP address, in order to assure its permanent connection to the Internet. Another example is when an application server to which you would like to connect, such as a security server, requires that packets have a specific IP address—you can define a NAT rule for that address.


7.3.7.1. Configuring the NAT

Click the 'NAT' link under the 'Firewall' menu item. The 'NAT' screen appears.



Figure 7.118. Network Address Translation

Before configuring NAT/NAPT rules, you must first enter the additional public IP addresses obtained from your ISP as your NAT IP addresses, in the 'NAT IP Addresses Pool' section.

 **Note:** The primary IP address used by the WAN device for dynamic NAPT should not be added to this table.

To add a NAT IP address, perform the following:

1. Click the 'New IP Address' link. The 'Edit Item' screen appears.

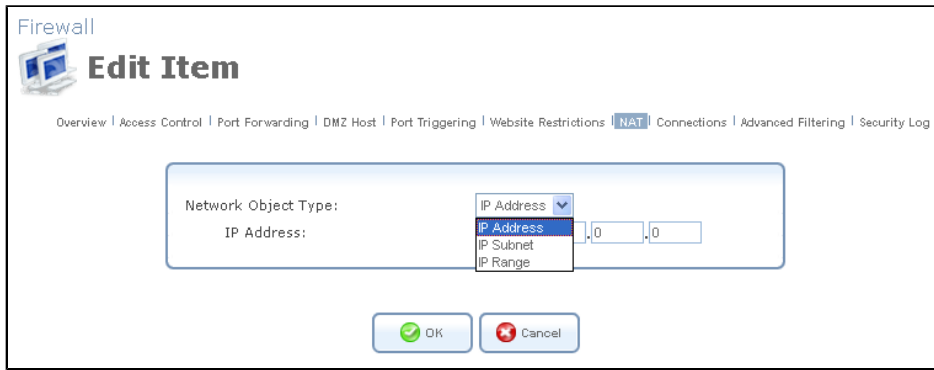


Figure 7.119. Edit Item

2. To add a single public address, select the 'IP Address' option from the 'Network Object Type' drop-down menu, and enter the IP in the fields that appear.



Figure 7.120. Edit Item

To add a range of public IP addresses, select the 'IP Range' option and enter the available IP range.

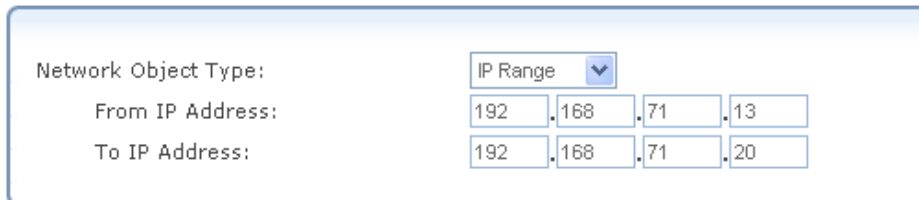


Figure 7.121. Edit Item

3. Click 'OK' to save the settings. The new IP addresses are displayed in the 'NAT IP Addresses Pool' section.

NAT IP Addresses Pool	
IP Address	Action
192.168.71.12	 
192.168.71.13 - 192.168.71.20	 
New IP Address	

Figure 7.122. NAT IP Addresses

To add a new NAT/NAPT rule, click the 'New Entry' link in the 'NAT/NAPT Rule Sets' section of the 'NAT' screen. The 'Add NAT/NAPT Rule' screen appears.

Firewall

Add NAT/NAPT Rule

Overview | Access Control | Port Forwarding | DM2 Host | Port Triggering | Website Restrictions | **NAT** | Connections | Advanced Filtering | Security Log

Matching

Source Address: Any

Destination Address: Any

Protocol: Any

Operation

NAT Source IP translation rule.

NAT Addresses

Add...

Logging

Log Packets Matched by This Rule

Schedule

Always

OK Cancel

Figure 7.123. Add NAT/NAPT Rule

Matching Use this section to define characteristics of the packets matching the rule.

- Source Address** The source address of packets sent or received by OpenRG. Use this drop-down menu to specify a LAN computer or a group of LAN computers on which you would like to apply the rule. Select an address or a name from the list to apply the rule on the corresponding host, or 'Any' to apply the rule on all OpenRG's LAN hosts. If you would like to add a new address, select the 'User Defined' option in the drop-down menu. This will commence a sequence that will add a new **Network Object**, representing the new host. Refer to [Section 8.9.2](#) in order to learn how to do so.
- Destination Address** The destination address of packets sent or received by OpenRG. This address can be configured in the same manner as the source address. For example, use this drop-down menu to specify an IP address of a remote application server (such as a security server), which requires that the incoming packets have a specific IP address (e.g., one of those defined in your NAT IP address pool).
- Protocol** You may also specify a traffic protocol. Selecting the 'Show All Services' option from the drop-down menu expands 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. Refer to [Section 8.9.2](#) in order to learn how to do so.

Operation Use this section to define the operation that will be applied on the IP addresses matching the criteria defined above. The operations available are NAT or NAPT. Selecting each from the drop-down menu refreshes the screen accordingly.

- **NAT Addresses**

The screenshot shows a configuration window for NAT. The top section, titled 'Operation', contains a dropdown menu with 'NAT' selected and the text 'Source IP translation rule.'. The bottom section, titled 'NAT Addresses', contains a dropdown menu labeled 'Add...'.

Figure 7.124. Add NAT Rule

This drop-down menu displays all of your available NAT addresses/ranges, from which you can select an entry. If you would like to add a single address or a sub-range from the given pool/range, select the 'User Defined' option in the drop-down menu. This will commence a sequence that will add a new **Network Object**, representing the new host. Refer to [Section 8.9.2](#) in order to learn how to do so.

- **NAPT Address**

The screenshot shows a configuration window for NAPT. The top section, titled 'Operation', contains a dropdown menu with 'NAPT' selected and the text 'Source IP and port translation rule.'. The bottom section, titled 'NAPT Address', contains a dropdown menu labeled 'Add...'. Below that, the 'NAPT Ports' section has a dropdown menu set to 'Range' and two input fields containing '1024' and '65535'.

Figure 7.125. Add NAPT Rule

This drop-down menu displays all of your available NAPT addresses/ranges, from which you can select an entry. If you would like to add a single address or a sub-range from the given pool/range, select the 'User Defined' option from the drop-down menu. This will commence a sequence that will add a new **Network Object**, representing the new host. Refer to [Section 8.9.2](#) in order to learn how to do so. Note, however, that in this case the network object may only be an IP address, as NAPT is port-specific.

- **NAPT Ports** Specify the port(s) for the IP address into which the original IP address will be translated. Enter a single port or select 'Range' in the drop-down menu. The screen refreshes, enabling you to enter a range of ports.

The close-up shows the 'NAPT Ports' section with a dropdown menu set to 'Range' and two input fields containing '1024' and '65535'.

Figure 7.126. Add NAPT Rule

Logging Monitor the rule.

- **Log Packets Matched by This Rule** Select this check box to log the first packet from a connection that was matched by this rule.

Schedule 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. To learn how to configure scheduler rules, refer to [Section 8.9.3](#).

7.3.7.2. NAT/NAPT Configuration Examples

This section demonstrates the NAT/NAPT usage and capabilities, by creating several rules and observing their implementation. In the following examples, the LAN IP address range is 192.168.1.5 through 192.168.1.25. The NAT addresses are 192.168.71.12 through 192.168.71.20, and they have been entered to the NAT address pool as described earlier.

In the 'NAT' screen, click the 'New Entry' link in the 'NAT/NAPT Rule Sets' section. The 'Add NAT/NAPT Rule' screen appears.

Firewall

Add NAT/NAPT Rule

Overview | Access Control | Port Forwarding | DMZ Host | Port Triggering | Website Restrictions | **NAT** | Connections | Advanced Filtering | Security Log

Matching

Source Address: Any

Destination Address: Any

Protocol: Any

Operation

NAT: Source IP translation rule.

NAT Addresses: Add...

Logging

Log Packets Matched by This Rule

Schedule

Schedule: Always

OK Cancel

Figure 7.127. Add NAT/NAPT Rule

Create the following NAT/NAPT rules:

1. Translate the address 192.168.1.10 to 192.168.71.12. In this example, LAN addresses (192.168.1.X) are not defined yet, therefore do not appear as drop-down menu options, and network objects must be created in order to represent them.
 - a. Select 'User Defined' in the 'Source Address' drop-down menu. The 'Edit Network Object' screen appears.

Firewall

Edit Network Object

Overview | Access Control | Port Forwarding | DMZ Host | Port Triggering | Website Restrictions | **NAT** | Connections | Advanced Filtering | Security Log

Network Object

Description:

Item	Action
New Entry	

Figure 7.128. Edit Network Object

- b. Click 'New Entry'. The 'Edit Item' screen appears.

Firewall

Edit Item

Overview | Access Control | Port Forwarding | DMZ Host | Port Triggering | Website Restrictions | **NAT** | Connections | Advanced Filtering | Security Log

Network Object Type:

IP Address:

Figure 7.129. Edit Item

- c. Select 'IP Address' in the 'Network Object Type' drop-down menu, and enter 192.168.1.10.
 - d. Click 'OK' to save the settings.
 - e. Click 'OK' in the 'Edit Network Object' screen.
 - f. Back in the 'Add NAT/NAPT Rule' screen, select 192.168.1.10 from the 'Source' drop-down menu.
 - g. From the 'NAT Addresses' drop-down menu, select the '192.168.71.12' option. The screen refreshes, adding this address as a NAT IP address.
 - h. Click 'OK' to save the settings.

The NAT rule is displayed in the 'NAT' screen.

NAT/NAPT Rule Sets						
Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
WAN Ethernet Rules						
<input checked="" type="checkbox"/> 0	192.168.1.10	Any		NAT -> 192.168.71.12	Active	
New Entry						

Figure 7.130. NAT/NAPT Rule Sets

This rule translates one LAN IP address to one NAT IP address, meaning that this LAN computer will have WAN access at any time. The status is therefore set to "Active".

- Translate the range 192.168.1.11-192.168.1.15 to 192.168.71.12-192.168.71.15. Define this NAT rule in the same manner depicted above, with the exception of selecting 'IP Range' (instead of 'IP Address') as the network object type. Since both ranges are not predefined (no such drop-down menu options), network objects must be created in order to represent them, using the 'User Defined' option in the 'Source' and 'NAT' drop-down menus respectively. The created rule is displayed in the 'NAT' screen.

NAT/NAPT Rule Sets						
Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
WAN Ethernet Rules						
<input checked="" type="checkbox"/> 0	192.168.1.10	Any		NAT -> 192.168.71.12	Active	
<input checked="" type="checkbox"/> 1	192.168.1.11 - 192.168.1.15	Any		NAT -> 192.168.71.12 - 192.168.71.15	Active	
New Entry						

Figure 7.131. NAT/NAPT Rule Sets

This rule translates five new LAN IP addresses to four NAT IP addresses, which would normally mean that only four of the five LAN computers may have WAN access at the same time. However, note that the NAT address 192.168.71.12 is already in use by the first rule. OpenRG will therefore allow these five LAN computers to use only the three remaining IP addresses ending with 71.13, 71.14 and 71.15. The status is therefore set to "Active".

- Translate the range 192.168.1.21-192.168.1.25 to 192.168.71.13-192.168.71.14. Define this NAT rule in the same manner depicted above. The following attention message is displayed.



Figure 7.132. Attention

Click 'OK'. The rule is displayed in the 'NAT' screen.

NAT/NAPT Rule Sets						
Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
WAN Ethernet Rules						
<input checked="" type="checkbox"/> 0	192.168.1.10	Any		NAT -> 192.168.71.12	Active	
<input checked="" type="checkbox"/> 1	192.168.1.11 - 192.168.1.15	Any		NAT -> 192.168.71.12 - 192.168.71.15	Active	
<input checked="" type="checkbox"/> 2	192.168.1.21 - 192.168.1.25	Any		NAT -> 192.168.71.13 - 192.168.71.14	Error	
New Entry						

Figure 7.133. NAT/NAPT Rule Sets

This rule translates five new LAN IP addresses to two NAT IP addresses, both of which are already in use by the second rule. OpenRG is therefore unable to resolve this situation and the rule's status is set to "Error". Notice that had this rule been defined as the second rule, all three rules would be valid. This is because the NAT address 192.168.71.15 would still be available for rule number 1. This can easily be amended: you can use the green arrow icons to move a rule entry up or down, changing its priority respectively. Click this rule's action icon once. All rules will now be set to "Active".

NAT/NAPT Rule Sets						
Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
WAN Ethernet Rules						
<input checked="" type="checkbox"/> 0	192.168.1.10	Any		NAT -> 192.168.71.12	Active	
<input checked="" type="checkbox"/> 2	192.168.1.21 - 192.168.1.25	Any		NAT -> 192.168.71.13 - 192.168.71.14	Active	
<input checked="" type="checkbox"/> 1	192.168.1.11 - 192.168.1.15	Any		NAT -> 192.168.71.12 - 192.168.71.15	Active	
New Entry						

Figure 7.134. NAT/NAPT Rule Sets

Note: The first rule now maps five LAN addresses to one NAT address. OpenRG subtracts all previously used NAT addresses, requested by previous rules, from the requested NAT addresses of the current rule. The requested range of addresses does not determine how many will be available; the number of available addresses is determined by previous rules configuration and order. Rules will appear as "Active" even if they only have one usable NAT address.

4. Translate the address 192.168.1.5 to 192.168.71.16 **ports** 1024-1050. Define this NAPT rule in the same manner depicted above, with the following exception:
 - a. Select the 'NAPT' option in the 'Operation' section drop-down menu. The screen refreshes.

Operation

NAPT Source IP and port translation rule.

NAPT Address Add...

NAPT Ports: Range -

Figure 7.135. Add NAPT Rule

- b. Add a NAPT address by selecting the 'User Defined' option.
- c. Enter 1024-1050 as the range of ports in the 'NAPT Ports' section.
- d. Click 'OK' to save the settings.

The rule is displayed in the 'NAT' screen.

NAT/NAPT Rule Sets						
Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
WAN Ethernet Rules						
<input checked="" type="checkbox"/> 0	192.168.1.10	Any		NAT -> 192.168.71.12	Active	
<input checked="" type="checkbox"/> 2	192.168.1.21 - 192.168.1.25	Any		NAT -> 192.168.71.13 - 192.168.71.14	Active	
<input checked="" type="checkbox"/> 1	192.168.1.11 - 192.168.1.15	Any		NAT -> 192.168.71.12 - 192.168.71.15	Active	
<input checked="" type="checkbox"/> 3	192.168.1.5	Any		NAPT -> 192.168.71.16 ports 1024-1050	Active	
New Entry						

Figure 7.136. NAT/NAPT Rule Sets

This rule translates a LAN IP address to a NAT IP address with specific ports. Its status is set to "Active".

5. Translate the address 192.168.1.6 to 192.168.71.16 ports 1024-1100. Define this NAPT rule in the same manner depicted above. The rule is displayed in the 'NAT' screen.

NAT/NAPT Rule Sets						
Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
WAN Ethernet Rules						
<input checked="" type="checkbox"/> 0	192.168.1.10	Any		NAT -> 192.168.71.12	Active	
<input checked="" type="checkbox"/> 2	192.168.1.21 - 192.168.1.25	Any		NAT -> 192.168.71.13 - 192.168.71.14	Active	
<input checked="" type="checkbox"/> 1	192.168.1.11 - 192.168.1.15	Any		NAT -> 192.168.71.12 - 192.168.71.15	Active	
<input checked="" type="checkbox"/> 3	192.168.1.5	Any		NAPT -> 192.168.71.16 ports 1024- 1050	Active	
<input checked="" type="checkbox"/> 4	192.168.1.6	Any		NAPT -> 192.168.71.16 ports 1024- 1100	Active	
New Entry						

Figure 7.137. NAT/NAPT Rule Sets

This rule translates a LAN IP address to a NAT IP address with ports 1024-1100. However, only ports 1051-1100 will be used for this LAN computer, as ports 1024-1050 are already in use by the preceding rule. The status is set to "Active".

Every new NAT/NAPT rule is verified in relation to preceding rules. Rules are prioritized according to the order in which they are defined. As long as at least one unused IP address (or port) is available, the rule will be accepted. However, as seen in the examples above, not all addresses in the range defined may be available for computers in that rule; some may already be in use by other rules. OpenRG automatically calculates the relationships between rules, narrowing down the address ranges if needed, and thus provides great flexibility for user input.

The verification performed by OpenRG is as follows:

- NAT rule – Verifies whether the IP address is already in use by another NAT/NAPT rule.
- NAPT rule
 1. Verifies whether the port is already in use by another NAPT rule activated on the same IP address.
 2. Verifies whether the IP address is already in use by another NAT rule.

7.3.8. Viewing Open Connections

The connection list displays all the connections that are currently open, as well as various details and statistics. The summary at the top of the table indicates the number of active connections, and the 'Approximate Max. Connections' value that represents the amount of additional concurrent connections possible. When numerous connections are available, a 'Connections Per Page' drop-down menu appears at the table's heading, enabling you to select the number of connections to be displayed at once.

The basic display includes the name of the protocol, the different ports it uses, and the direction in which the connection was initiated.

Firewall Connections

Overview | Access Control | Port Forwarding | DMZ Host | Port Triggering | Website Restrictions | NAT | **Connections** | Advanced Filtering | Log

Active Connections: 5
Approximate Max. Connections: 50599

Number	Protocol	LAN IP:Port	OpenRG IP:Port	WAN IP:Port	Direction	Action
1	UDP	192.168.66.190:47413	192.168.66.190:47413	192.168.65.1:53	Outgoing	✖
2	UDP	192.168.66.190:123	192.168.66.190:123	207.153.221.89:123	Outgoing	✖
3	TCP	192.168.66.190:4301	192.168.66.190:4301	10.71.3.104:80	Outgoing	✖
4	UDP	0.0.0.0:68	0.0.0.0:68	255.255.255.255:67	Outgoing	✖
5	UDP	*.*.*.*:68	*.*.*.*:68	*.*.*.*:67	Outgoing	✖

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

Close Refresh Advanced >>

Figure 7.138. Connection List

To delete an undesired connection, click its ✖ action icon . Clicking the 'Advanced' button at the bottom of the table adds the following details:

- The connection's time-to-live
- The number of kilo-bytes and packets received and transmitted
- The device type
- The routing mode

Note that the port fields of a protocol may contain "wild connections", that appear with a series of asterisk marks (*) (see [Figure 7.138](#)). Wild connections are created when the IP address or source port of an incoming packet are unknown. When a packet is matched on the connection, the missing details are discovered, resulting in a standard connection.

7.3.9. Configuring the Advanced Filtering Mechanism

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 OpenRG's advanced filtering options, click the 'Advanced Filtering' link of the 'Firewall' menu item. The 'Advanced Filtering' screen appears.

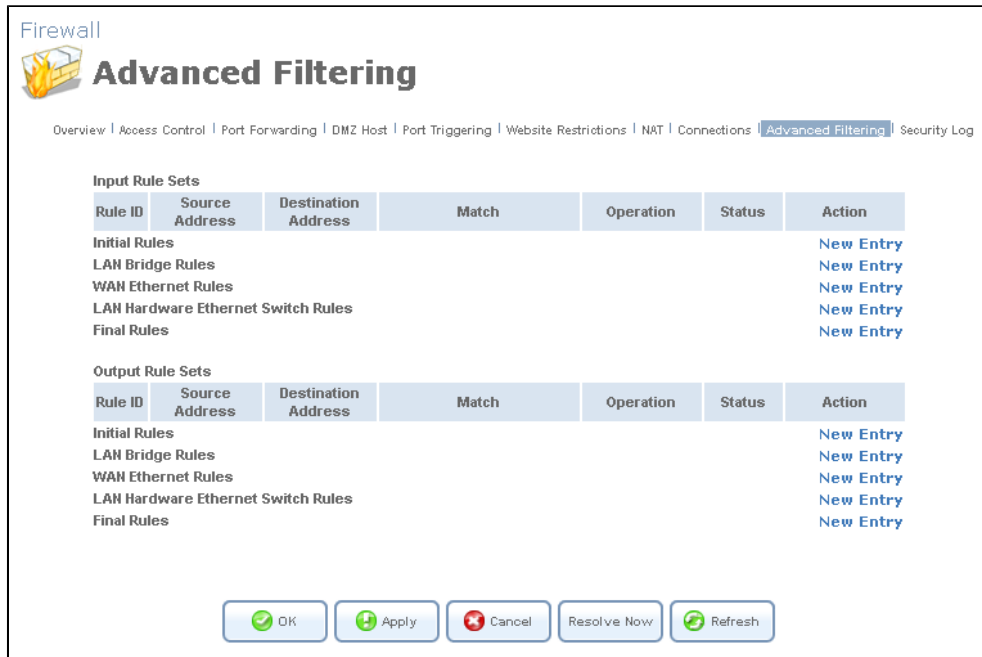




Figure 7.139. Advanced Filtering

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  action icon and  action icon .








Input Rule Sets						
Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
Initial Rules						
<input checked="" type="checkbox"/> 0	192.168.71.20	Any		Drop	Active	  
<input checked="" type="checkbox"/> 1	192.168.71.25	Any		Drop	Active	  
New Entry						

Figure 7.140. Move Up and Move Down Action Icons

There are numerous rules that are 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 appears.

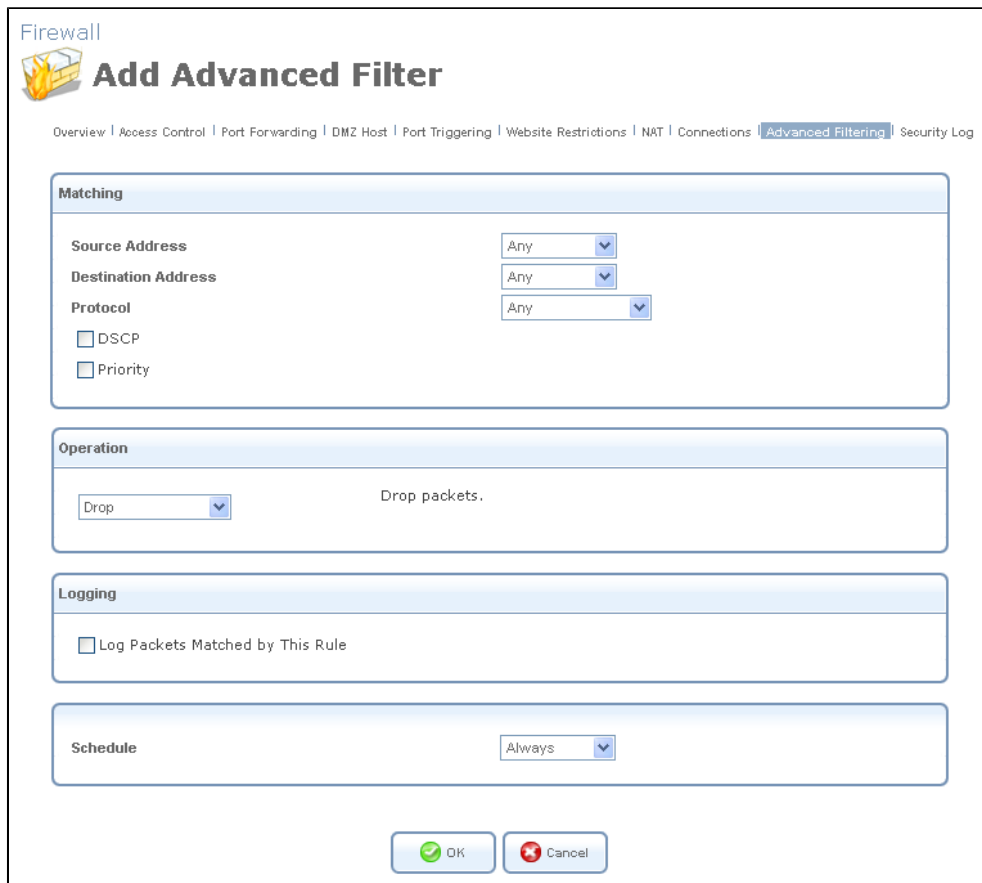


Figure 7.141. Add Advanced Filter

The 'Matching' and 'Operation' sections of this screen define the operation to be executed when matching conditions apply.

Matching Use this section to define characteristics of the packets matching the rule.

- **Source Address** The source address of packets sent or received by OpenRG. Use this drop-down menu to specify the computer or group of computers on which you would like to apply the rule. Select an address or a name from the list to apply the rule on the corresponding host, or 'Any' to apply the rule on any host trying to send data. If you would like to add a new address, select the 'User Defined' option in the drop-down menu. This will commence a sequence that will add a new **Network Object**, representing the new host. Refer to [Section 8.9.2](#) in order to learn how to do so.
- **Destination Address** The destination address of packets sent or received by OpenRG. This address can be configured in the same manner as the source address. For example, use this drop-down menu to specify an IP address of a remote application server (such as a security server), which requires that the incoming packets have a specific IP address (e.g., one of those defined in your NAT IP address pool).
- **Protocol** You may also specify a traffic protocol. Selecting the 'Show All Services' option from the drop-down menu expands 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. Refer to [Section 8.9.2](#) in order to learn how to do so.

- **DSCP** Select this check box to display two DSCP fields, which enable you to specify a hexadecimal DSCP value and its mask assigned to the packets matching the priority rule. For more information, refer to [Section 7.4.5](#).
- **Priority** Select this check box to display a drop-down menu, in which you can select a priority level assigned to the packets matching the priority rule. For more information, refer to [Section 7.4.3](#).
- **Length** Select this check box if you would like to specify the length of packets, or the length of their data portion.

Operation Define what action the rule will take, by selecting one of the following radio buttons:

- **Drop** Deny access to packets that match the source and destination IP addresses and service ports defined above.
- **Reject** Deny access to packets that match the criteria defined, and send an ICMP error or a TCP reset to the origination peer.
- **Accept Connection** Allow access to packets that match the criteria defined. The data transfer session will be handled using Stateful Packet Inspection (SPI), meaning that other packets matching this rule will be automatically allowed access.
- **Accept Packet** Allow access to packets that match the criteria defined. The data transfer session will not be handled using SPI, meaning that other packets matching this rule will not be automatically allowed access. This can be useful, for example, when creating rules that allow broadcasting.

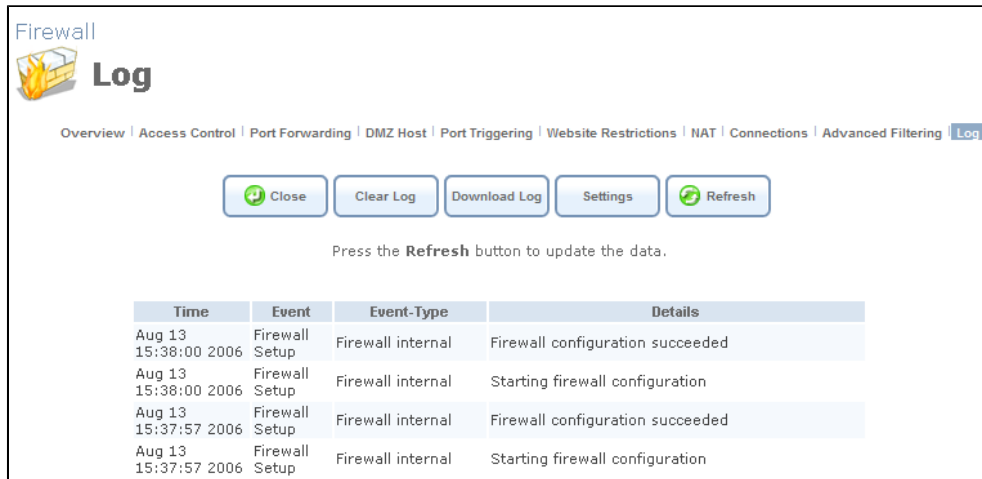
Logging Monitor the rule.

- **Log Packets Matched by This Rule** Select this check box to log the first packet from a connection that was matched by this rule.

Schedule 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. To learn how to configure scheduler rules, refer to [Section 8.9.3](#).

7.3.10. Viewing the Firewall Log

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



Time	Event	Event-Type	Details
Aug 13 15:38:00 2006	Firewall Setup	Firewall internal	Firewall configuration succeeded
Aug 13 15:38:00 2006	Firewall Setup	Firewall internal	Starting firewall configuration
Aug 13 15:37:57 2006	Firewall Setup	Firewall internal	Firewall configuration succeeded
Aug 13 15:37:57 2006	Firewall Setup	Firewall internal	Starting firewall configuration

Figure 7.142. Firewall Log

The log's columns are:

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. Use the buttons at the top of the page to:

Close Close the 'Log' screen and return to OpenRG's home page.

Clear Log Clear all currently displayed log messages.

Download Log Download the log as a Comma Separated Value (CSV) file, named **firewall.csv**.

Settings View or change the security log settings (explanation follows).

Refresh Refresh the screen to display the latest updated log messages.

To view or change the security log settings:

1. Click the 'Settings' button that appears at the top of the 'Firewall Log' screen. The 'Log Settings' screen appears.

The screenshot shows the 'Log Settings' interface for a firewall. It features a breadcrumb trail at the top: Overview | Access Control | Port Forwarding | DMZ Host | Port Triggering | Website Restrictions | NAT | Connections | Advanced Filtering | Log. The settings are grouped into four main sections:

- Accepted Events:**
 - Accepted Incoming Connections
 - Accepted Outgoing Connections
- Blocked Events:**
 - All Blocked Connection Attempts
 - Winnuke
 - Defragmentation Error
 - Blocked Fragments
 - Syn Flood
 - Echo Chargen
 - Multicast/Broadcast
 - Spoofed Connection
 - Packet Illegal Options
 - UDP Flood
 - ICMP Replay
 - ICMP Redirect
 - ICMP Multicast
 - ICMP Flood
- Other Events:**
 - Remote Administration Attempts
 - Connection States
- Log Buffer:**
 - Prevent Log Overrun

At the bottom of the screen, there are three buttons: OK (with a green checkmark), Apply (with a green plus sign), and Cancel (with a red minus sign).

Figure 7.143. Log Settings

2. Select the types of activities for which you would like to have a log message generated:

- Accepted Events

Accepted Incoming Connections Write a log message for each successful attempt to establish an inbound connection to the home network.

Accepted Outgoing Connections Write a log message for each successful attempt to establish an outgoing connection to the public network.

- Blocked Events

All Blocked Connection Attempts Write a log message for each blocked attempt to establish an inbound connection to the home network or vice versa. You can enable logging of blocked packets of specific types by disabling this option, and enabling some of the more specific options below it.

Specific Events Specify the blocked events that should be monitored. Use this to monitor specific event such as SynFlood. A log message will be generated if either the corresponding check box is checked, or the "All Blocked Connection Attempts" check box is checked.

- Other Events

Remote Administration Attempts Write a log message for each remote administration connection attempt, whether successful or not.

Connection States Provide extra information about every change in a connection opened by the firewall. Use this option to track connection handling by the firewall and Application Level Gateways (ALGs).

- Log Buffer

Prevent Log Overrun Select this check box in order to stop logging firewall activities when the memory allocated for the log fills up.

3. Click 'OK' to save the settings.

7.3.10.1. The Firewall Event Types

The following are the available event types that can be recorded in the firewall log:

1. Firewall internal – an accompanying explanation from the firewall internal mechanism will be added in case this event-type is recorded.
2. Firewall status changed – the firewall changed status from up to down or the other way around, as specified in the event type description.
3. STP packet – an STP packet has been accepted/rejected.
4. Illegal packet options – the options field in the packet's header is either illegal or forbidden.
5. Fragmented packet – a fragment has been rejected.
6. WinNuke protection – a WinNuke attack has been blocked.
7. ICMP replay – an ICMP replay message has been blocked.
8. ICMP redirect protection – an ICMP redirected message has been blocked.
9. Packet invalid in connection – a packet has been blocked, being on an invalid connection.
10. ICMP protection – a broadcast ICMP message has been blocked.

11. Broadcast/Multicast protection – a packet with a broadcast/multicast source IP has been blocked.
12. Spoofing protection – a packet from the WAN with a source IP of the LAN has been blocked.
13. DMZ network packet – a packet from a demilitarized zone network has been blocked.
14. Trusted device – a packet from a trusted device has been accepted.
15. Default policy – a packet has been accepted/blocked according to the default policy.
16. Remote administration – a packet designated for OpenRG management has been accepted/blocked.
17. Access control – a packet has been accepted/blocked according to an access control rule.
18. Parental control – a packet has been blocked according to a parental control rule.
19. NAT out failed – NAT failed for this packet.
20. DHCP request – OpenRG sent a DHCP request (depends on the distribution).
21. DHCP response – OpenRG received a DHCP response (depends on the distribution).
22. DHCP relay agent – a DHCP relay packet has been received (depends on the distribution).
23. IGMP packet – an IGMP packet has been accepted.
24. Multicast IGMP connection – a multicast packet has been accepted.
25. RIP packet – a RIP packet has been accepted.
26. PPTP connection – a packet inquiring whether OpenRG is ready to receive a PPTP connection has been accepted.
27. Kerberos key management 1293 – security related, for future use.
28. Kerberos 88 – for future use.
29. AUTH:113 request – an outbound packet for AUTH protocol has been accepted (for maximum security level).
30. Packet-Cable – for future use.
31. IPV6 over IPV4 – an IPV6 over IPV4 packet has been accepted.
32. ARP – an ARP packet has been accepted.
33. PPP Discover – a PPP discover packet has been accepted.

34. PPP Session – a PPP session packet has been accepted.
35. 802.1Q – a 802.1Q (VLAN) packet has been accepted.
36. Outbound Auth1X – an outbound Auth1X packet has been accepted.
37. IP Version 6 – an IPv6 packet has been accepted.
38. OpenRG initiated traffic – all traffic that OpenRG initiates is recorded.
39. Maximum security enabled service – a packet has been accepted because it belongs to a permitted service in the maximum security level.
40. SynCookies Protection – a SynCookies packet has been blocked.
41. ICMP Flood Protection – a packet has been blocked, stopping an ICMP flood.
42. UDP Flood Protection – a packet has been blocked, stopping a UDP flood.
43. Service – a packet has been accepted because of a certain service, as specified in the event type.
44. Advanced Filter Rule – a packet has been accepted/blocked because of an advanced filter rule.
45. Fragmented packet, header too small – a packet has been blocked because after the defragmentation, the header was too small.
46. Fragmented packet, header too big – a packet has been blocked because after the defragmentation, the header was too big.
47. Fragmented packet, drop all – not used.
48. Fragmented packet, bad align – a packet has been blocked because after the defragmentation, the packet was badly aligned.
49. Fragmented packet, packet too big – a packet has been blocked because after the defragmentation, the packet was too big.
50. Fragmented packet, packet exceeds – a packet has been blocked because defragmentation found more fragments than allowed.
51. Fragmented packet, no memory – a fragmented packet has been blocked because there was no memory for fragments.
52. Fragmented packet, overlapped – a packet has been blocked because after the defragmentation, there were overlapping fragments.
53. Defragmentation failed – the fragment has been stored in memory and blocked until all fragments arrived and defragmentation could be performed.

54. Connection opened – usually a debug message regarding a connection.
55. Wildcard connection opened – usually a debug message regarding a connection.
56. Wildcard connection hooked – usually debug message regarding connection.
57. Connection closed – usually a debug message regarding a connection.
58. Echo/Chargen/Quote/Snork protection – a packet has been blocked, protecting from Echo/Chargen/Quote/Snork.
59. First packet in connection is not a SYN packet – a packet has been blocked because of a TCP connection that had started without a SYN packet.
60. Error: No memory – a message notifying that a new connection has not been established because of lack of memory.
61. NAT Error : Connection pool is full – a message notifying that a connection has not been created because the connection pool is full.
62. NAT Error: No free NAT IP – a message notifying that there is no free NAT IP, therefore NAT has failed.
63. NAT Error: Conflict Mapping already exists – a message notifying that there is a conflict since the NAT mapping already exists, therefore NAT has failed.
64. Malformed packet: Failed parsing – a packet has been blocked because it is malformed.
65. Passive attack on ftp-server: Client attempted to open Server ports – a packet has been blocked because of an unauthorized attempt to open a server port.
66. FTP port request to 3rd party is forbidden (Possible bounce attack) – a packet has been blocked because of an unauthorized FTP port request.
67. Firewall Rules were changed – the firewall rule set has been modified.
68. User authentication – a message during login time, including both successful and failed authentication.
69. First packet is Invalid – first packet in connection failed to pass firewall or NAT.

7.3.11. Applying Corporate-Grade Security

The following set of instructions is designed to assist you in applying corporate-grade security standards to your network. When implementing these instructions, it is important to execute the configuration steps in the exact order they are presented. To apply corporate-grade firewall security standards perform the following:

- Do not allow non-administrative services access to the LAN:

1. Open a Telnet session from a LAN host that is connected to OpenRG.
2. Telnet to OpenRG at address 192.168.1.1.
3. Log into OpenRG as an administrator (the default username is "admin" and the password is "admin").
4. After logging on, issue the following command at the prompt:

```
OpenRG> conf set fw/protect/allow_rg_remote_administration_only 1
OpenRG> conf reconf 1
OpenRG> exit
```

- Configure OpenRG to permit only HTTPS as means of remote administration:
 1. Click the 'Management' menu item under 'System'.
 2. Click the 'Remote Administration' link.
 3. Enable the following check boxes:
 - Using Primary HTTPS Port (443)
 - Using Secondary HTTPS Port (8443)

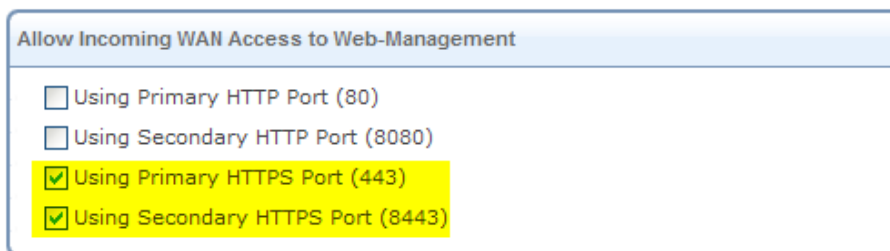


Figure 7.144. Enabling Secure Remote Administration

4. Disable all other check boxes.
 5. Click 'OK' to save the settings.
- Apply firewall protection on the LAN:
 1. Click the 'Network Connections' menu item under 'System'.
 2. Click the 'LAN Ethernet' connection link.
 3. Click the 'Advanced' button.
 4. Enable the 'Internet Connection Firewall' check box.



Figure 7.145. Apply Firewall Protection

5. Click 'OK' to save the settings.

At this point you have set your firewall to corporate-grade security. If you wish to allow additional LAN services, or other outbound services, refer to [Section 7.3.9](#) to learn how to do so.

7.3.11.1. Enabling Secure Local Administration

You can connect directly to OpenRG in order to perform local administration tasks. To do so, it is necessary to establish a PPP over Serial (PPPoS) connection between the administration host and OpenRG, by performing the following:

1. Connect a serial cable between the administration host and the gateway.
2. Run a PPP client on the administration host (depicted in the following sections).
3. After the PPP connection is established, OpenRG can be accessed via HTTP/HTTPS over this connection.
4. Reset the gateway when you are done.

To perform local administration you need a computer with:

- A serial connection
- Windows 2000/XP or Linux operating system

7.3.11.1.1. Running a PPP Client on Linux

To run a PPP client on a Linux host, perform the following:

```
pppd <SERIAL_DEV_NAME> <BAUD> noauth user <USERNAME> local nobsdcomp nodeflate
```

SERIAL_DEV_NAME The name of the serial device on the Linux machine, e.g. /dev/ttyS1.

BAUD The required baud rate

USERNAME The name of a user of OpenRG with Administrator Privileges. Make sure that a proper secret is defined in either /etc/ppp/chap-secrets or /etc/ppp/pap-secrets on the Linux machine.

7.3.11.1.2. Running a PPP Client on Windows XP

To run a PPP client on Windows XP, perform the following:

1. Install a NULL Modem Driver:
 - a. Click the 'Phone and Modem Options' icon on the Control Panel.
 - b. Select the Modems tab, and click the 'Add' button.
 - c. Mark the 'Don't detect my modem; I will select it from a list' check-box, and click 'Next'.

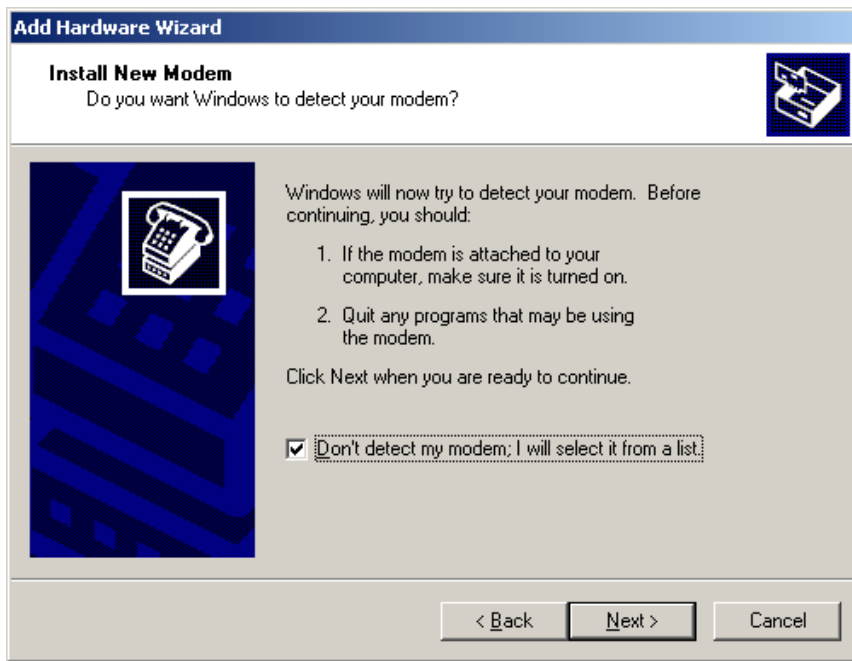


Figure 7.146. Installing the NULL Modem Driver

- d. From 'Standard Modem Types' select 'Communications cable between two computers', and click 'Next'.

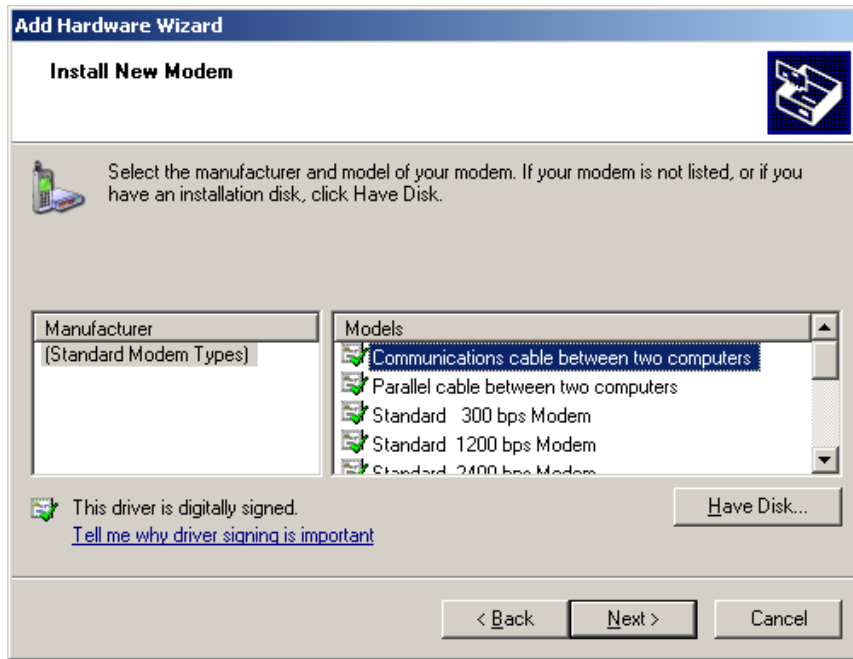


Figure 7.147. Select Modem Type

- e. Select 'All ports', and click 'Next'.

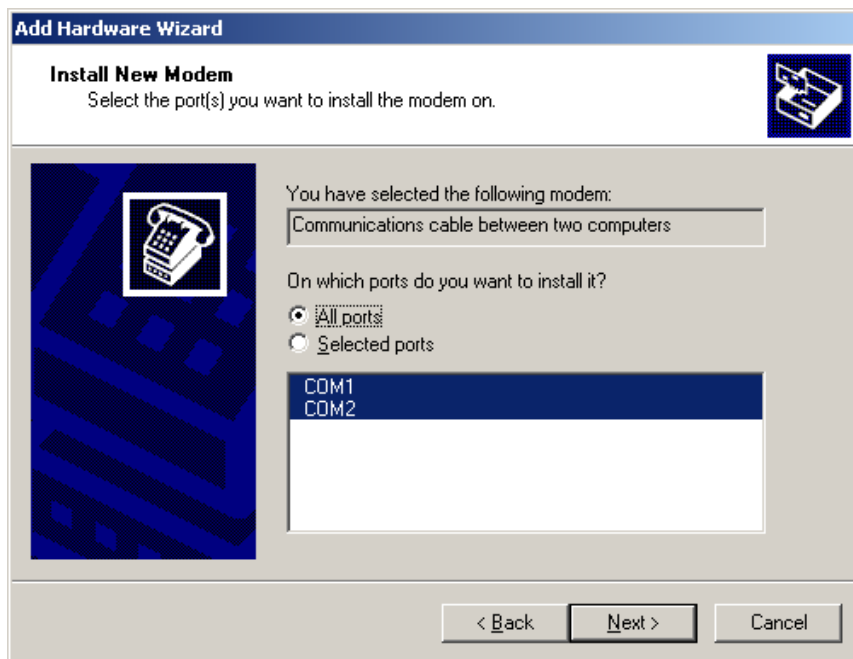


Figure 7.148. Select Ports

2. Create a new direct connection:

- a. Click the 'Network Connections' icon from 'Network and Internet Connections' on the Control Panel.

- b. Select 'Create a new connection' button, and click 'Next'.
 - c. Select 'Set up an advanced connection' and click 'Next'.
 - d. Select 'Connect directly to another computer' and click 'Next'.
 - e. Select 'Guest' and click 'Next'.
 - f. Enter a name for the connection and click 'Next'.
 - g. From the drop-down menu, select the serial device that is connected to OpenRG, and click 'Next'.
 - h. Click 'Finish'.
3. Edit the created connection:
- a. Right-click the newly created connection and select 'Properties'.
 - b. From the 'Networking' tab, select PPP from the drop-down menu.
 - c. Click the 'Settings' button, and clear all of the check boxes.
 - d. Click 'OK'.
 - e. Click the 'General' tab, and from the drop-down menu select the COM port you are using.
 - f. Click 'Configure'.
 - g. In the 'Modem Configuration' screen, select 115200 as the Maximum speed from the drop-down menu.
 - h. Make sure all of the check box options are not selected.
 - i. Click 'OK' twice.
4. Connect to OpenRG:
- a. Double click the newly created connection.
 - b. Enter a name of a user with Administrator privileges.
 - c. Enter the password for the user.
 - d. Click 'Connect'.

7.3.11.1.3. Running a PPP Client on Windows 2000

To run a PPP client on Windows 2000, perform the following:

1. Install a NULL Modem Driver:
 - a. Click the 'Phone and Modem Options' icon on the Control Panel.
 - b. Select the Modems tab, and click the 'Add' button.
 - c. Mark the 'Don't detect my modem; I will select it from a list' check box, and click 'Next'.

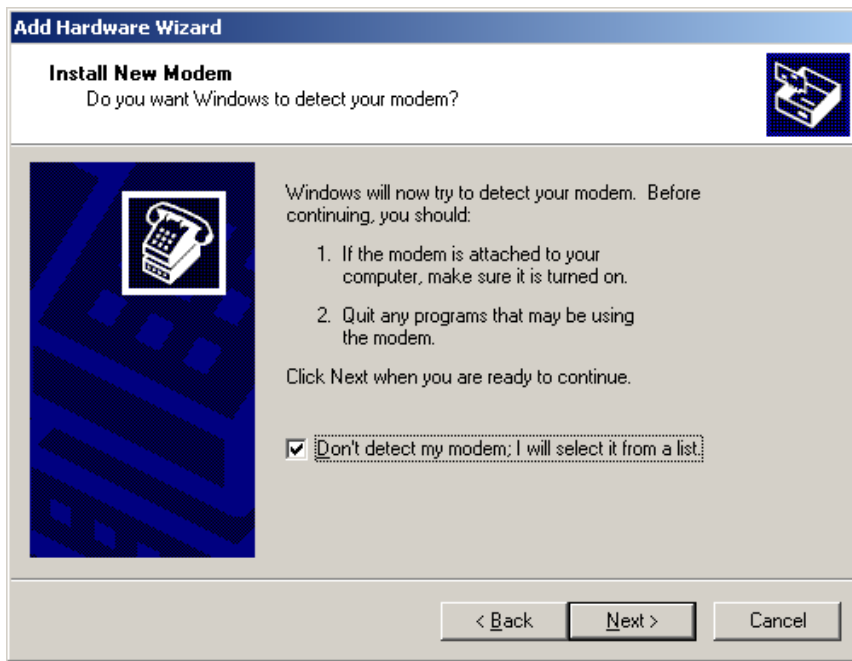


Figure 7.149. Installing a Modem Driver

- d. From 'Standard Modem Types' select 'Communications cable between two computers', and click 'Next'.

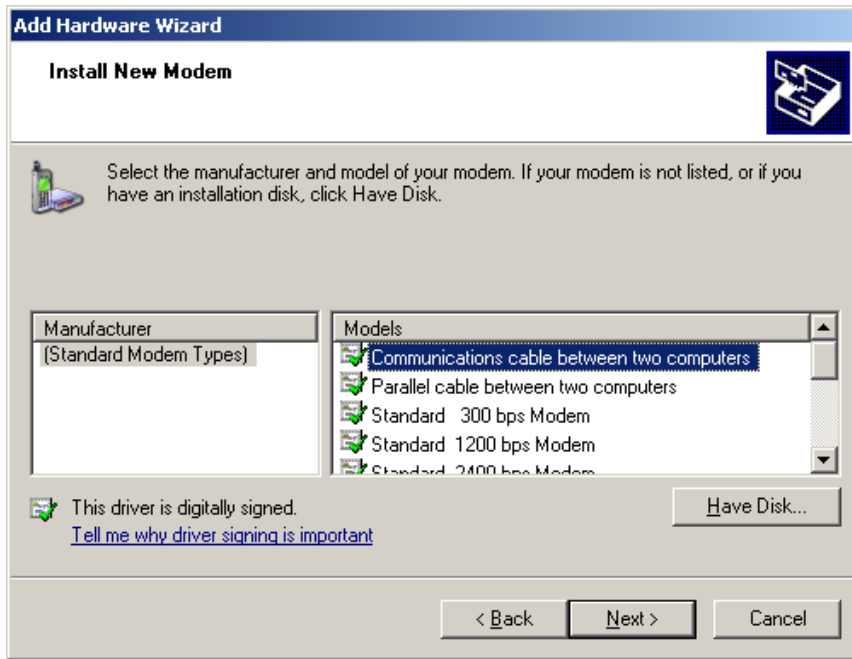


Figure 7.150. Select Modem Type

- e. Select 'All ports', and click 'Next'.

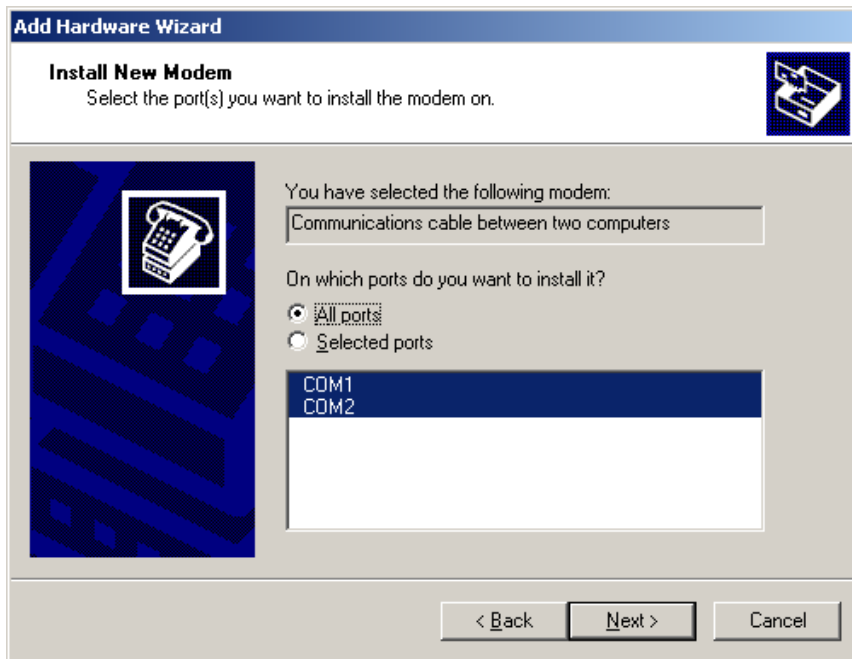


Figure 7.151. Select Ports

2. Create a new direct connection:

- a. Click the 'Network Connections' icon from 'Network and Internet Connections' on the Control Panel.

- b. Select 'Create a new connection' button, and click 'Next'.
 - c. Select 'Connect directly to another computer' and click 'Next'.
 - d. Select 'Guest' and click 'Next'.
 - e. From the drop-down menu, select the serial device that is connected to OpenRG, and click 'Next'.
 - f. Select the 'Only for myself' radio button and click 'Next'.
 - g. Enter a name for the connection and click 'Finish'.
3. Edit the created connection:
- a. Right-click the newly created connection and select 'Properties'.
 - b. From the 'Networking' tab, select PPP from the drop-down menu.
 - c. Click the 'Settings' button, and clear all of the check boxes.
 - d. Click 'OK'.
 - e. Click the 'General' tab, and from the drop-down menu select the COM port you are using.
 - f. Click the 'Configure' button.
 - g. In the 'Modem Configuration' screen, select 115200 as the Maximum speed from the drop-down menu.
 - h. Make sure all of the check box options are not selected.
 - i. Click 'OK' twice.
4. Connect to OpenRG:
- a. Double-click the newly created connection.
 - b. Enter a name of a user with Administrator privileges.
 - c. Enter the password for the user.
 - d. Click 'Connect'.

7.4. Quality of Service

Network-based applications and traffic are growing at a high rate, producing an ever-increasing demand for bandwidth and network capacity. For obvious reasons, bandwidth and capacity cannot be expanded infinitely, requiring that bandwidth-demanding services be delivered over existing infrastructure, without incurring additional, expansive investments.

The next logical means of ensuring optimal use of existing resources are Quality of Service (QoS) mechanisms for congestion management and avoidance. Quality of Service refers to the capability of a network device to provide better service to selected network traffic. This is achieved by shaping the traffic and processing higher priority traffic before lower priority traffic.

As Quality of Service is dependent on the "weakest link in the chain", failure of but a single component along the data path to assure priority packet transmission 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.

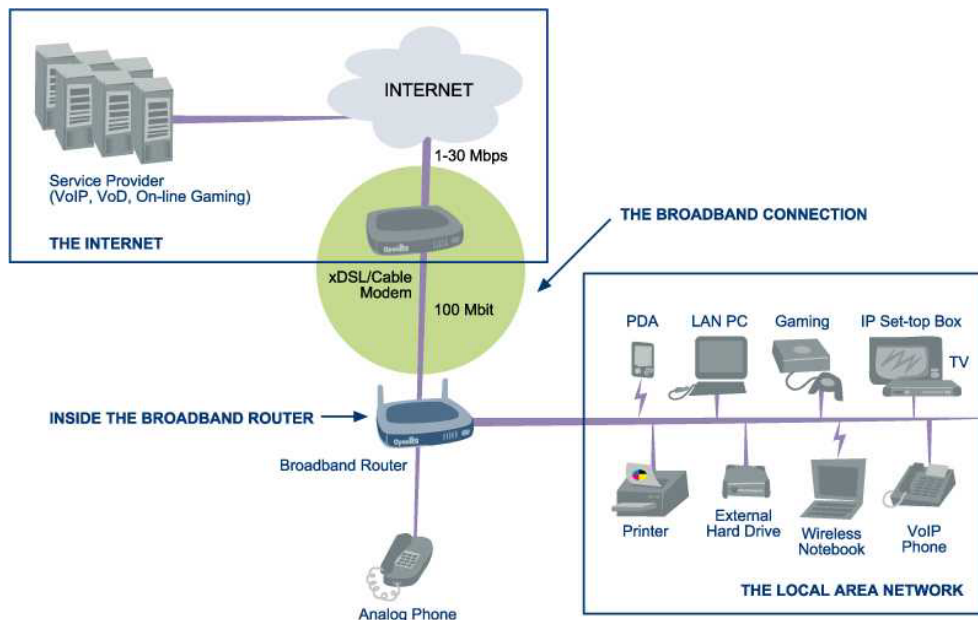


Figure 7.152. End-to-end QoS Challenge Areas

The following are the potential bottleneck areas that need to be taken into consideration when implementing an end-to-end QoS-enabled service.

- **The Local Area Network** LANs have finite bandwidth, and are typically limited to 100 Mbps. When given the chance, some applications will consume all available network bandwidth. In business networks, a large number of network-attached devices can lead to congestion. The need for QoS mechanisms is more apparent in wireless LANs (802.11a/b/g), where bandwidth is even more limited (typically no more than 20 Mbps on 802.11g networks).
- **The Broadband Router** All network traffic passes through and is processed by the broadband router. It is therefore a natural focal point for QoS implementation. Lack of sufficient buffer space, memory or processing power, and poor integration among system

components can result in highly undesirable real-time service performance. The only way to assure high quality of service is the use of proper and tightly-integrated router operating system software and applications, which can most effectively handle multiple real-time services simultaneously.

- **The Broadband Connection** Typically the most significant bottleneck of the network, this is where the high speed LAN meets limited broadband bandwidth. Special QoS mechanisms must be built into routers to ensure that this sudden drop in connectivity speed is taken into account when prioritizing and transmitting real-time service-related data packets.
- **The Internet** Internet routers typically have a limited amount of memory and bandwidth available to them, so that congestions may easily occur when links are over-utilized, and routers attempt to queue packets and schedule them for retransmission. One must also consider the fact that while Internet backbone routers take some prioritization into account when making routing decisions, all data packets are treated equally under congested conditions.

The following figure depicts OpenRG's QoS role and architecture in a network. Many of the terms it contains will become familiar as you read on.

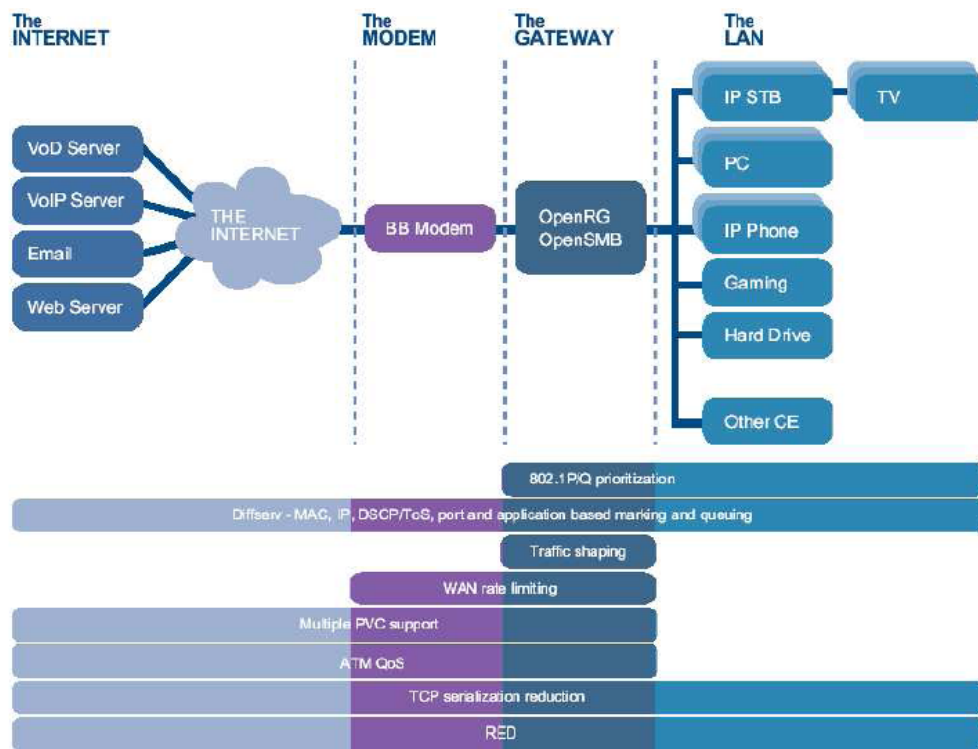


Figure 7.153. OpenRG's QoS Architecture

7.4.1. Overview

The 'General' screen 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, described later.



Note: Selecting a QoS profile will cause all previous QoS configuration settings to be **permanently lost**.

Click the QoS tab under 'Services'. The 'General' screen appears with the 'Overview' link being selected.

Figure 7.154. General

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

- **Tx Bandwidth** This parameter defines the gateway's outbound transmission rate. Enter your Tx bandwidth in Kbits per second.
- **Rx Bandwidth** This parameter defines the gateway's Internet traffic reception rate. Enter your Rx bandwidth in Kbits per second.



Note: By default, these parameters are set to 0 Kbps, which means that the bandwidth has not been limited on OpenRG. Entering inaccurate Tx/Rx values will cause incorrect behavior of the QoS module. It is important to set these values as accurately as possible.

If you wish to restore the default bandwidth settings, select 'Unlimited' from the drop-down menu, and click 'Apply'. Note that you can also set the desired bandwidth on the WAN (or any other) device in the 'Traffic Shaping' screen (to learn how to do so, refer to [Section 7.4.4.2](#)).

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 profile, however the device is limited by the requested bandwidth, if specified.
- **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.

7.4.2. Internet Connection Utilization

The 'Internet Connection Utilization' screen provides application level usage information of your Internet connection's bandwidth. You can view what application on which LAN computer is using how much bandwidth, at any given time. This information is provided in both application and computer views.

7.4.2.1. Application View

By default, the information is presented in "By Application" view. The screen refreshes constantly. You can stop its refreshing by using the 'Auto Refresh Off' button at the bottom of the screen.

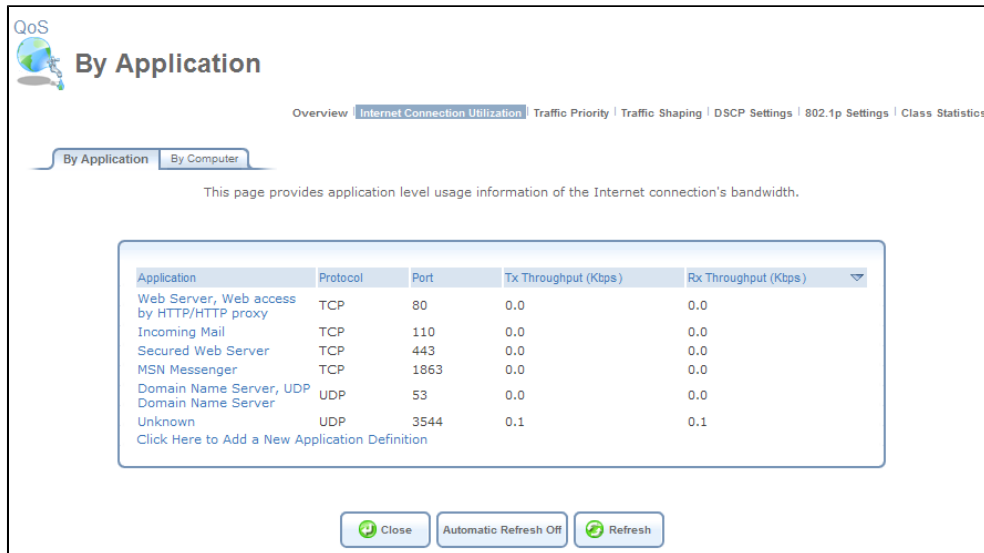


Figure 7.155. Internet Connection Utilization by Application

The table displays the following information fields. Note that you can sort the table according to these fields (ascending or descending), by clicking the fields' names.

Application The type of application using the bandwidth.

Protocol The application's network protocol.

Port The port through which traffic is transferred.

Tx Throughput The transmission bit rate in kilo-bits per second.

Rx Throughput The reception bit rate in kilo-bits per second.

OpenRG does not recognize all possible applications running on LAN computers, and marks such an application as "Unknown" (see [Figure 7.155](#)). You can define an unknown application by clicking the 'Click Here to Add a New Application Definition' link at the bottom of the table. The 'Protocols' screen appears, in which you can define the application by adding it as a new service entry. To learn more about adding protocols, refer to [Section 8.9.1](#).

Furthermore, you can click each application's name to view its details, particularly which LAN computer is running it.

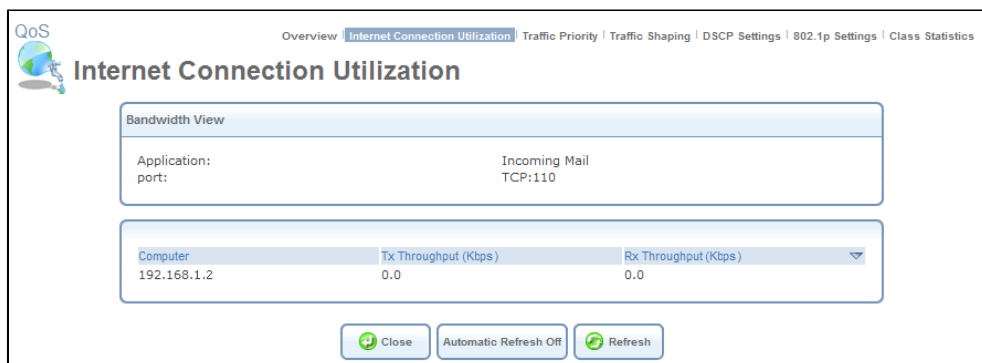


Figure 7.156. A Specific Application

In this example, the application "Incoming Mail" is running on computer 192.168.1.2, using TCP protocol on port 110. This screen provides a combined application and computer view, and enables you to select the general traffic priorities for that computer.

7.4.2.2. Computer View

The "By Computer" tab presents a table displaying the sum of bandwidth used by each LAN computer. The fields displayed are the computer's IP address and the Tx and Rx throughput.

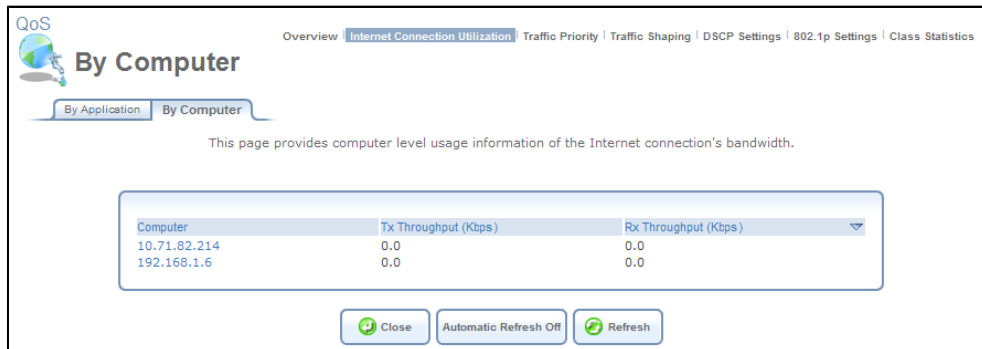


Figure 7.157. Internet Connection Utilization by Computer

Click a computer's IP address to view the bandwidth-consuming applications running on that computer.

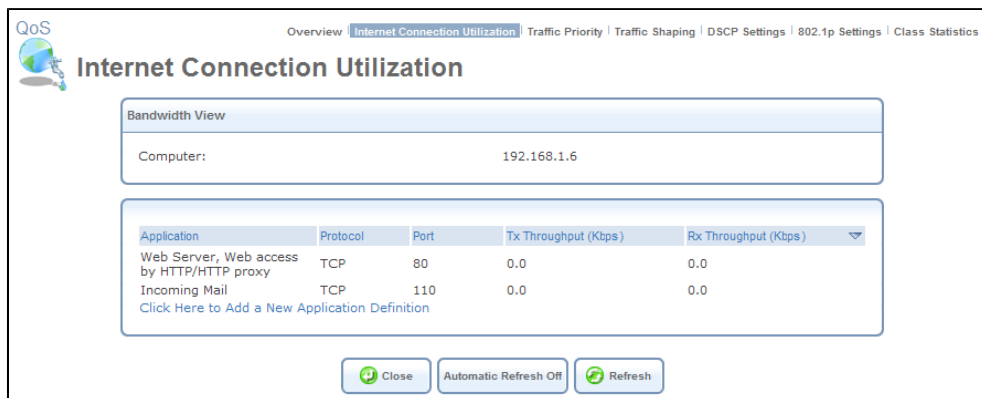


Figure 7.158. A Specific Computer

In this example, computer 192.168.1.6 is running the applications "Web Server" and "Incoming Mail". This screen provides a combined computer and application view, by displaying a computer-specific application table. This table also enables you to define an unknown application (as described in the previous section).

7.4.3. 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

OpenRG supports two priority marking methods for packet prioritization:

- DSCP (refer to [Section 7.4.5](#)).
- 802.1p Priority (refer to [Section 7.4.6](#)).

The matching of packets by rules is connection-based, known as Stateful Packet Inspection (SPI), using the same connection-tracking mechanism used by OpenRG's firewall. 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). This feature applies to all applications that have ALG in the firewall, such as:

- SIP
- MSN Messenger/Windows Messenger
- TFTP
- FTP
- MGCP
- H.323
- Port Triggering applications (refer to [Section 7.3.5](#))
- PPTP

- IPSec

To set traffic priority rules:

1. Under the 'QoS' menu item, click 'Traffic Priority'. The 'Traffic Priority' screen appears (see [Figure 7.159](#)). 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.

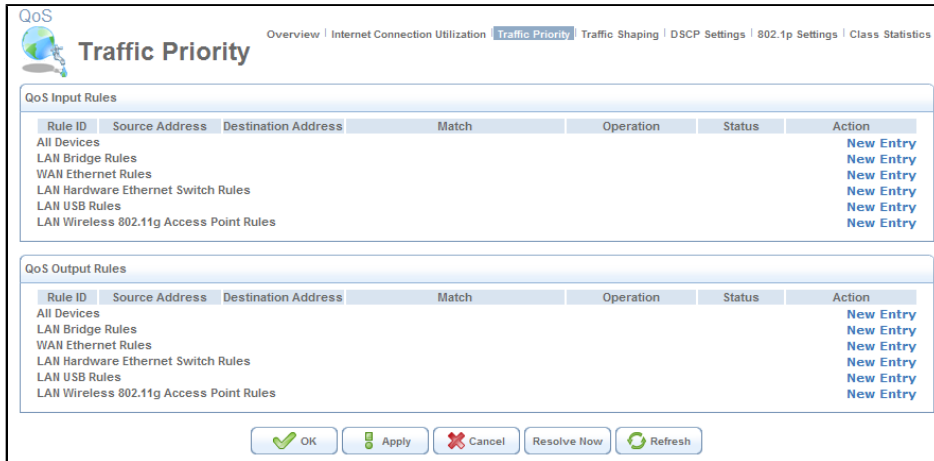


Figure 7.159. Traffic Priority

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 appears.



Figure 7.160. Add Traffic Priority Rule

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 characteristics of the packets matching the rule.

- **Source Address** The source address of packets sent or received by OpenRG. Use this drop-down menu to specify the computer or group of computers on which you would like to apply the rule. Select an address or a name from the list to apply the rule on the corresponding host, or 'Any' to apply the rule on any host trying to send data. If you would like to add a new address, select the 'User Defined' option in the drop-down menu. This will commence a sequence that will add a new **Network Object**, representing the new host. Refer to [Section 8.9.2](#) in order to learn how to do so.
- **Destination Address** The destination address of packets sent or received by OpenRG. This address can be configured in the same manner as the source address. For example, use this drop-down menu to specify an IP address of a remote application server (such as a security server), which requires that the incoming packets have a specific IP address (e.g., one of those defined in your NAT IP address pool).
- **Protocol** You may also specify a traffic protocol. Selecting the 'Show All Services' option from the drop-down menu expands 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. Refer to [Section 8.9.2](#) in order to learn how to do so.

Using a protocol requires observing the relationship between a client and a server, in order to distinguish between the source and destination ports. For example, let's assume you have an FTP server in your LAN, serving clients inquiring from the WAN. You want to apply a QoS rule on incoming packets from any port on the WAN (clients) trying to access FTP port 21 (your server), and the same for outgoing packets from port 21 trying to access any port on the WAN. Therefore, you must set the following Traffic Priority rules:

- In the 'Matching' section of 'QoS Input Rules', select 'FTP' from the 'Protocol' drop-down menu. The 'TCP Any -> 21' setting appears under 'Ports'.
- Define a priority in the 'Operation' section.
- Click 'OK' to save the settings.
- Define a QoS output rule in the same way as the input rule.
- **DSCP** Select this check box to display two DSCP fields, which enable you to specify a hexadecimal DSCP value and its mask assigned to the packets matching the priority rule. For more information, refer to [Section 7.4.5](#).
- **Priority** Select this check box to display a drop-down menu, in which you can select a priority level assigned to the packets matching the priority rule.

- **Device** Select this check box to display a drop-down menu, in which you can select a network device on which the packet-rule matching will be performed. This option is relevant in case you have previously selected the 'All Devices' option in the 'Traffic Priority' screen (see [Figure 7.159](#)).
- **Length** Select this check box if you would like to specify the length of packets, or the length of their data portion.

Operation Perform the following operation/s on packets that match the priority rule.

- **Set DSCP** Select this check box if you would like to change the DSCP value on packets matching the rule, prior to routing them further. The screen refreshes (see [Figure 7.161](#)), enabling you to enter the hexadecimal DSCP value in its respective field that appears.

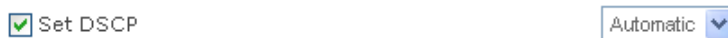


Figure 7.161. Set DSCP Rule

- **Set Priority** Select this check box if you would like to change a priority of the packets matching the rule. The screen refreshes (see [Figure 7.162](#)), enabling you to select between one of eight priority levels, zero being the lowest and seven the highest. Each priority level is assigned a default queue number, where Queue 0 has the lowest priority. OpenRG's QoS supports up to eight queues.



Figure 7.162. Set Priority with Queuing

The matching between a priority level and a queue number can be edited in the '802.1p Settings' screen (for more information, refer to [Section 7.4.6](#)).



- **Apply QoS on** Select whether to apply QoS on a connection or just the first packet. When applying on a connection, the data transfer session will be handled using Stateful Packet Inspection (SPI). This means that other packets matching this rule will be automatically allowed to access, and the same QoS scheme will be applied to them.

Logging Monitor the rule.

- **Log Packets Matched by This Rule** Select this check box to log the first packet from a connection that was matched by this rule.

Schedule 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. To learn how to configure scheduler rules, refer to [Section 8.9.3](#).

3. Click 'OK' to save the settings.

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  action icon and  action icon .








Input Rule Sets						
Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
Initial Rules						
<input checked="" type="checkbox"/> 0	192.168.71.20	Any		Drop	Active	  
<input checked="" type="checkbox"/> 1	192.168.71.25	Any		Drop	Active	  
New Entry						

Figure 7.163. Move Up and Move Down Action Icons

7.4.4. 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.

7.4.4.1. Traffic Classes

The bandwidth of a device can be divided in order to reserve constant portions of bandwidth to predefined traffic types. Such a portion is known as a Traffic Class. When not used by its predefined traffic type, or owner (for example VoIP), the bandwidth will be available to all other traffic. However when needed, the entire class is reserved solely for its owner.

Moreover, you can limit the maximum bandwidth that a class can use even if the entire bandwidth is available. When a shaping class is first defined for a specific traffic type, two shaping classes are created. The second class is the 'Default Class', which is responsible for all the packets that *do not* match the defined shaping class, or any other classes that may be defined on the device. You can also define **wildcard** devices, such as all WAN devices. This can be viewed in the 'Class Statistics' screen (see [Figure 7.177](#)).

7.4.4.2. Device Traffic Shaping

This section describes the different Traffic Shaping screens and terms, and presents the feature's configuration logic.

1. Click 'Traffic Shaping' under the QoS tab in the 'Services' screen. The 'Traffic Shaping' screen appears.

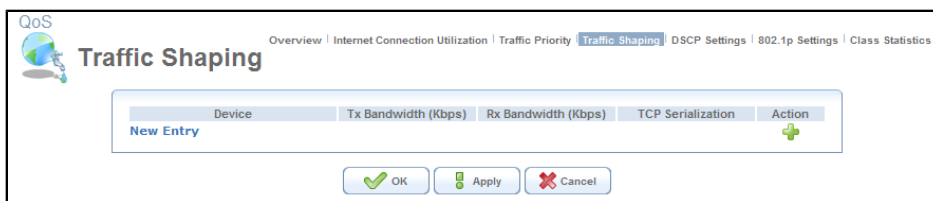


Figure 7.164. Traffic Shaping

2. Click the 'New Entry' link. The 'Add Device Traffic Shaping' screen appears (see [Figure 7.165](#)).
3. Select the device for which you would like to shape the traffic. The drop-down menu includes all your gateway's devices, and you can select either a specific device for which to shape the traffic, or 'Any Device' to add a traffic shaping class to all devices. In this example, select the WAN Ethernet option.

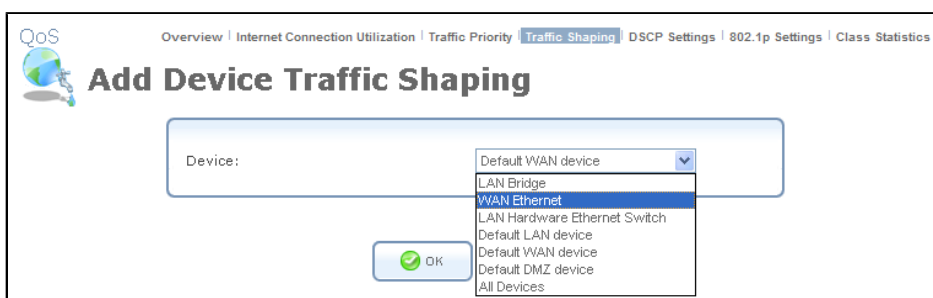


Figure 7.165. Add Device Traffic Shaping



If you would like to configure OpenRG's LAN traffic transmission/reception rate, select the relevant LAN device. If you would like to apply the settings on all LAN devices, select the 'Default LAN Device' entry.

4. Click 'OK'. The 'Edit Device Traffic Shaping' screen appears.

QoS Overview | Internet Connection Utilization | Traffic Priority | **Traffic Shaping** | DSCP Settings | 802.1p Settings | Class Statistics

Edit Device Traffic Shaping

Device: WAN Ethernet

Tx Traffic Shaping

Tx Bandwidth: Specify 97656 Kbps
 TCP Serialization: Disabled
 Queue Policy: Class Based

Class ID	Name	Priority	Bandwidth		Status	Action
			Reserved	Maximum		
default	default	4	0 Kbps	Unlimited	Active	

Rx Traffic Policing

Rx Bandwidth: Specify 97656 Kbps

Class ID	Name	Bandwidth		Status	Action
		Reserved	Maximum		
New Entry					

OK Apply Cancel

Figure 7.166. Edit Device Traffic Shaping

7.4.4.3. Tx Traffic Shaping

The bandwidth of a device can be divided in order to reserve constant portions of bandwidth to predefined traffic types. Such a portion is known as a Shaping Class. When not used by its predefined traffic type, or owner (for example VoIP), the class will be available to all other traffic. However when needed, the entire class is reserved solely for its owner. Moreover, you can limit the maximum bandwidth that a class can use even if the entire bandwidth is available.

Configure the following fields:

Tx Bandwidth This parameter limits the gateway's bandwidth transmission rate. The purpose is to limit the bandwidth of the WAN device to that of the weakest outbound link, for instance, the DSL speed provided by the ISP. This forces OpenRG to be the network bottleneck, where sophisticated QoS prioritization can be performed. If the device's bandwidth is not limited correctly, the bottleneck will be in an unknown router or modem on the network path, rendering OpenRG's QoS useless.

TCP Serialization You can enable TCP Serialization in its drop-down menu, either for active voice calls only or for all traffic. The screen will refresh, adding a 'Maximum Delay' field (see Figure 7.167). This function allows you to define the maximal allowed transmission time frame (in milliseconds) of a single packet. Any packet that requires a longer time to be transmitted, will be fragmented to smaller sections. This avoids transmission of large, bursty packets that may cause delay or jitter for real-time traffic such as VoIP. If you insert a delay value in milliseconds, the delay in number of bytes will be automatically updated on refresh.

TCP Serialization: Enabled

Maximum Delay: 0 ms (0 bytes)

Figure 7.167. TCP Serialization – Maximum Delay

Queue Policy Tx traffic queueing can be based on a shaping class (see the following explanations) or on the pre-defined priority levels (refer to [Section 7.4.3](#)). Note that when it is based on a shaping class, the class's bandwidth requirements will be met regardless of the priority, and only excess bandwidth will be given to traffic with a higher priority. However, when unlimited bandwidth is selected for the Tx traffic, the queue policy can only be based on the pre-defined priority levels.

To define a Tx Traffic Shaping Class:

1. Click the 'New Entry' link in the 'Tx Traffic Shaping' section of the 'Edit Device Traffic Shaping' screen (see [Figure 7.166](#)). The 'Add Shaping Class' screen appears.

Figure 7.168. Add Shaping Class


2. Name the new class and click 'OK' to save the settings, e.g. Class A.
3. Back in the 'Edit Device Traffic Shaping' screen, click the class name to edit the shaping class. Alternatively, click its  action icon. The 'Edit Shaping Class' screen appears.

Figure 7.169. Edit Shaping Class

Configure the following fields:

Name The name of the class.

Class Priority The class can be granted one of eight priority levels, zero being the highest and seven the lowest (note the obversion when compared to the rules priority levels). This level sets the priority of a class in comparison to other classes on the device.

Bandwidth The reserved transmission bandwidth in kilo-bits per second. You can limit the maximum allowed bandwidth by selecting the 'Specify' option in the drop-down menu. The screen will refresh, adding another Kbits/s field.

Bandwidth: Reserved Maximum Kbps

Figure 7.170. Specify Maximum Bandwidth

Policy The class policy determines the policy of routing packets inside the class. Select one of the four options:

- **Priority** Priority queuing utilizes multiple queues, so that traffic is distributed among queues based on priority. This priority is defined according to packet's priority, which can be defined explicitly, by a DSCP value (refer to [Section 7.4.5](#)), or by a 802.1p value (refer to [Section 7.4.6](#)).
- **FIFO** The "First In, First Out" priority queue. This queue ignores any previously-marked priority that packets may have.
- **Fairness** The fairness algorithm ensures no starvation by granting all packets a certain level of priority.
- **RED** The Random Early Detection algorithm utilizes statistical methods to drop packets in a "probabilistic" way before queues overflow. Dropping packets in this way slows a source down enough to keep the queue steady and reduces the number of packets that would be lost when a queue overflows and a host is transmitting at a high rate.
- **WRR** Weighted Round Robin utilizes a process scheduling function that prioritizes traffic according to the pre-defined 'Weight' parameter of a traffic's class. This level of prioritizing provides more flexibility in distributing bandwidth between traffic types, by defining additional classes within a parent class.

Schedule By default, the class will always be active. However, you can configure scheduler rules in order to define time segments during which the class may be active. To learn how to configure scheduler rules, refer to [Section 8.9.3](#).

7.4.4.4. Rx Traffic Policing

Configure the following fields:

Rx Bandwidth This parameter limits the device's bandwidth reception rate. In this example, the purpose is to limit the bandwidth that the WAN device can receive from the ISP.

Queue Policy Similar to Tx traffic, Rx traffic queueing can be based on a shaping class or on strict priority (unless unlimited bandwidth is selected). By default, however, the queue policy is set to Policer, which is a relatively simple method of bandwidth control. With the policer option, you can dedicate a portion of the bandwidth to a certain traffic type. This portion will always remain available to its traffic type, even when not in use. This is a simpler method, as priority is not used at all.

When selecting a class based queue policy, you must define an Rx Traffic Policy Class, which is identical to defining a Tx Traffic Shaping Class, described earlier. However if you select the policer as your queue policy, defining a policing class is even simpler, as it lacks the priority setup.

To define an Rx Traffic Policy Class:

1. Click the 'New Entry' link in the 'Rx Traffic Policing' section of the 'Edit Device Traffic Shaping' screen (see [Figure 7.166](#)). The 'Add Policing Class' screen appears.

Figure 7.171. Add Policing Class


2. Name the new class and click 'OK' to save the settings, e.g. Class B.
3. Back in the 'Edit Device Traffic Shaping' screen, click the class name to edit the shaping class. Alternatively, click its  action icon. The 'Edit Policing Class' screen appears.

Figure 7.172. Edit Policing Class

Configure the following fields:

Name The name of the class.

Bandwidth The reserved reception bandwidth in kilo-bits per second. You can limit the maximum allowed bandwidth by selecting the 'Specify' option in the combo box. The screen refreshes, adding yet another Kbps field.

Bandwidth: Reserved Maximum Kbps

Figure 7.173. Specify Maximum Bandwidth

Schedule By default, the class will always be active. However, you can configure scheduler rules in order to define time segments during which the class may be active. To learn how to configure scheduler rules, refer to [Section 8.9.3](#).

7.4.5. Differentiated Services Code Point Settings

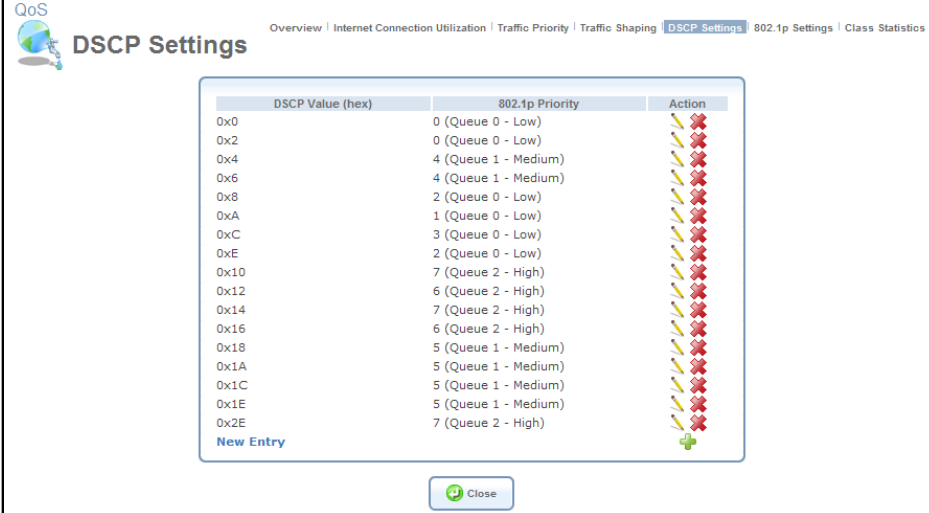
In order to understand what is *Differentiated Services Code Point* (DSCP), one must first be familiarized with the *Differentiated Services* model. Differentiated Services (Diffserv) is a Class of Service (CoS) model that enhances best-effort Internet services by differentiating traffic by users, service 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. OpenRG provides a table of predefined DSCP values, which are mapped to 802.1p priority marking method (refer to [Section 7.4.6](#)).

You can edit or delete any of the existing DSCP setting, as well as add new entries.

1. Under the QoS menu item, click 'DSCP Settings'. The following screen appears.




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

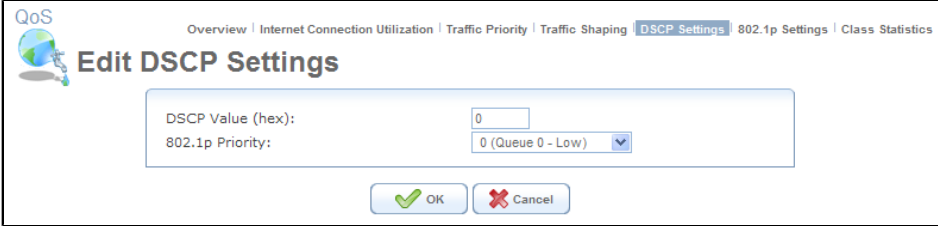
New Entry

Close

Figure 7.174. DSCP--Traffic Priority Matching

Each DSCP value is assigned a default queue number as a part of its 802.1p priority settings. OpenRG's QoS supports up to eight queues, where Queue 0 has the lowest priority.

2. To edit an existing entry, click its  action icon. To add a new entry, click the 'New Entry' link. In both cases, the 'Edit DSCP Settings' screen appears.



QoS Edit DSCP Settings

DSCP Value (hex):

802.1p Priority:

Figure 7.175. Edit DSCP Settings

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 drop-down menu (each priority level is mapped to low/medium/high priority).

4. Click 'OK' to save the settings.

Note that the DSCP value overriding the priority of incoming packets with an unassigned value (priority 0, assumed to be a no-priority-set) is "0x0".

7.4.6. 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 (0-7), where level 7 is the highest one. In addition, OpenRG maps these eight levels to priority queues, where Queue 0 has the lowest priority.

OpenRG's QoS supports up to eight queues. By default, the higher the level and queue values, the more priority they receive. Therefore, the more critical the traffic is, the higher priority level and queue number it should receive. To change the mapping between a priority value and a queue value, perform the following:

1. Under the 'QoS' menu item, click '802.1p Settings'. The following screen appears.

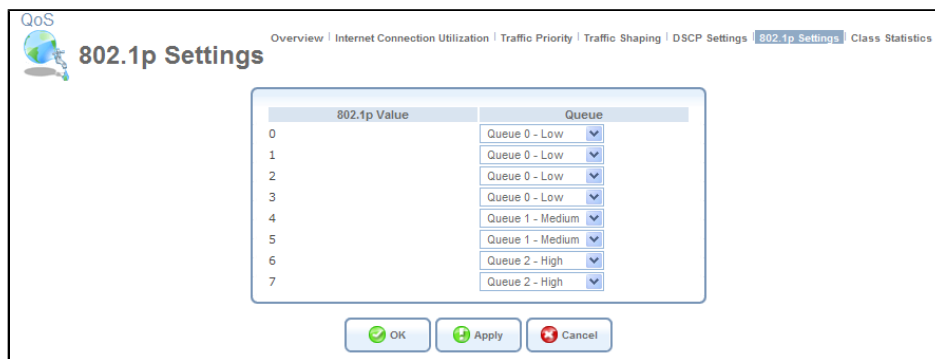


Figure 7.176. Traffic Queuing in 802.1p Settings

2. From the corresponding drop-down menu, select a desired value.
3. Click 'OK' to save the settings.

7.4.7. Class Statistics

OpenRG 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 menu item. The following screen appears.

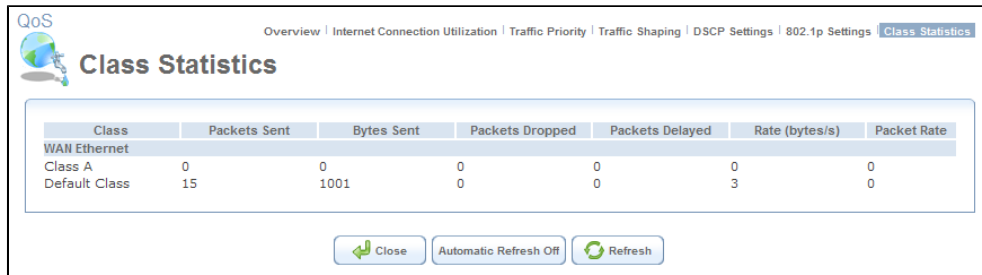


Figure 7.177. Class Statistics

Note that class statistics will only be available after defining at least one class (otherwise the screen will not present any information).

7.4.8. Voice QoS Scenario

In order to gain a better understanding of the Quality of Service concept, the following section presents a scenario where the WAN bandwidth is shaped to provide priority to a voice stream. When shared by a Voice over IP (VoIP) conversation and a file transfer, the bandwidth will normally be exploited by the file transfer, reducing the quality of the conversation or even causing it to disconnect. With QoS, the VoIP conversation, which is a real-time session, receives the priority it requires, maintaining a high level of voice quality.

7.4.8.1. Hardware Requirements

- A gateway running OpenRG
- Two IP phones
- A LAN computer running an FTP client, containing a large file (100MB)
- A WAN computer running an FTP server

7.4.8.2. Physical Setup

1. Connect an IP phone and the LAN computer to OpenRG's LAN ports.
2. Connect OpenRG's WAN port to your network. The second IP phone and the WAN computer should be available on the WAN.

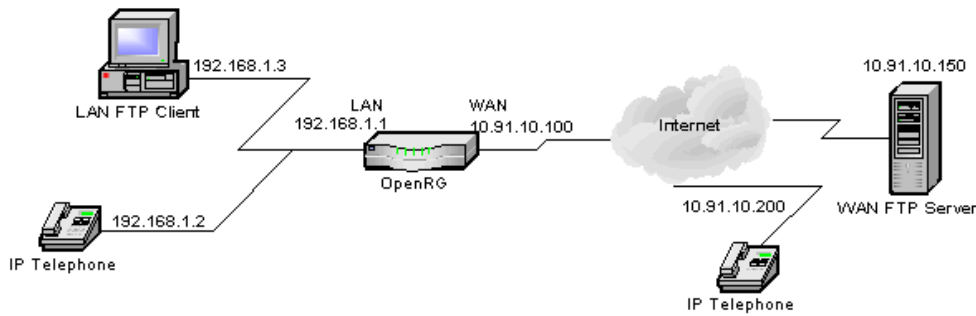


Figure 7.178. Physical Setup

7.4.8.3. Scenario Configuration

1. Configure OpenRG and all other devices with the static IPs described in [Figure 7.178](#).
2. Define a global service for the VoIP stream over a SIP protocol:

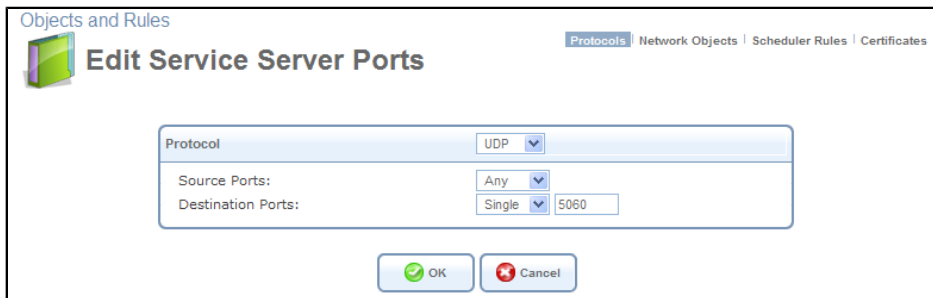


Figure 7.180. Edit Service Server Ports

- a. In OpenRG's WBM, click the 'Protocols' icon in the 'Advanced' screen, and then click the 'New Entry' link. The 'Edit Service' screen appears (see [Figure 7.179](#)).
- b. Enter "SIP" as the service name. You may also add a description for the service.

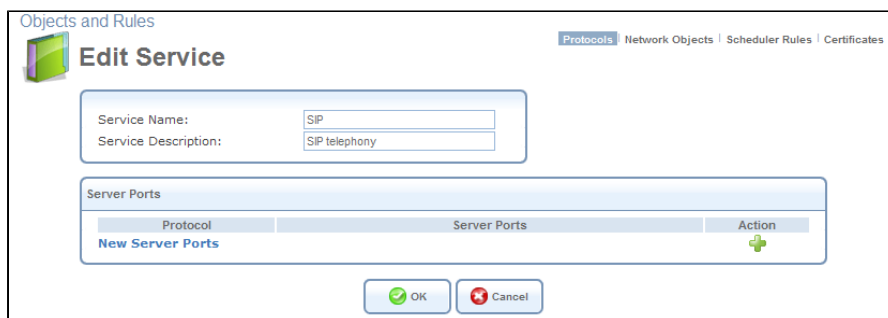


Figure 7.179. Edit Service

- c. Click the 'New Server Ports' link. The 'Edit Service Server Ports' screen appears (see [Figure 7.180](#)).
- d. From the drop-down menu, select the UDP protocol. The screen will refresh.
- e. Verify that "Any" is selected from the 'Source Ports' drop-down menu.

- f. From the 'Destination Ports' drop-down menu, select "Single". The screen will refresh again.
 - g. Enter 5060 as the single destination port.
 - h. Click 'OK' to save the settings.
3. Limit the bandwidth of OpenRG's WAN device:
- a. Under the 'QoS' menu item, click 'Traffic Shaping'. The following screen appears.

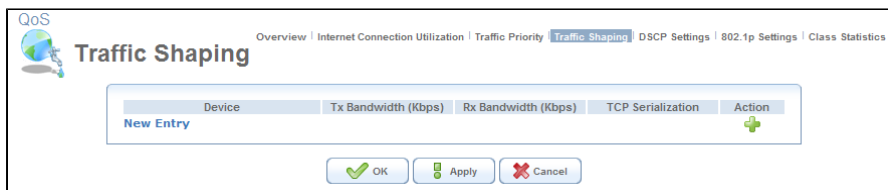


Figure 7.181. Traffic Shaping

- b. Click the 'New Entry' link, and select 'All Devices' from the drop-down menu.

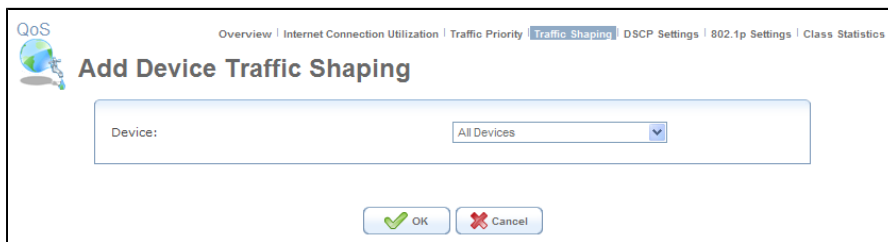


Figure 7.182. Add Device Traffic Shaping

- c. Click 'OK'. The 'Edit Device Traffic Shaping' screen appears.

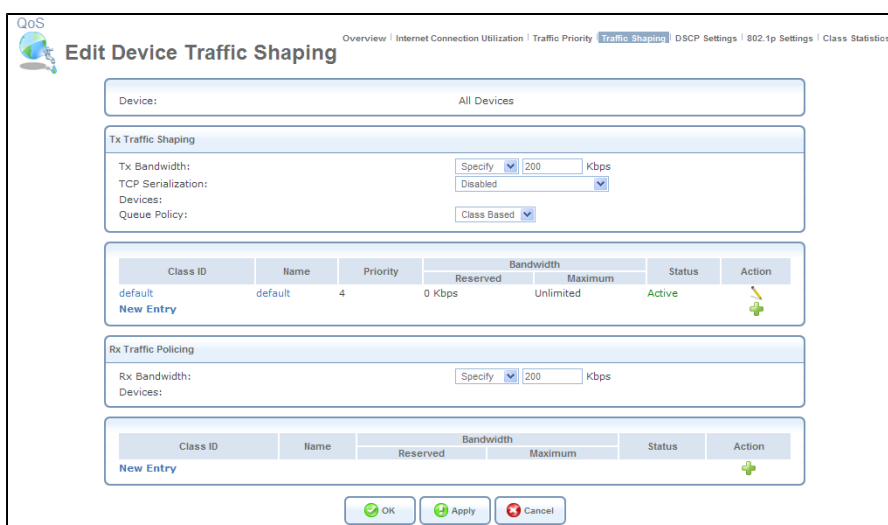


Figure 7.183. Edit Device Traffic Shaping

- d. In the Tx Bandwidth drop-down menu, select 'Specify', and enter 200 Kbps in the field that appears.
 - e. In the Rx Bandwidth drop-down menu, select 'Specify', and enter 200 Kbps in the field that appears.
 - f. Verify that TCP Serialization is disabled.
4. Configure a QoS class for the Tx and Rx VoIP streams. Perform this procedure twice: once for Tx Traffic Shaping and once for Rx Traffic Policing.
- a. Click the 'New Entry' link in the Tx/Rx traffic shaping section of the 'Edit Device Traffic Shaping' screen. The 'Add Class' screen appears (see [Figure 7.184](#)).
 - b. Name the new class "VoIP Tx/Rx", and click 'OK' to save the settings.

The screenshot shows a web interface titled 'Add Shaping Class'. At the top, there are navigation links: Overview, Internet Connection Utilization, Traffic Priority, Traffic Shaping (highlighted), DSCP Settings, 802.1p Settings, and Class Statistics. Below the title is a text input field labeled 'Name:' containing the text 'VoIP Tx'. At the bottom of the dialog are two buttons: 'OK' with a green checkmark icon and 'Cancel' with a red X icon.

Figure 7.184. Add Shaping Class

- c. Uncheck the entry in the Class ID column to disable the class at this point (see [Figure 7.185](#)).

The screenshot displays two configuration panels. The top panel is 'Tx Traffic Shaping' with settings: Tx Bandwidth: Specify 200 Kbps, TCP Serialization: Disabled, Devices: (empty), Queue Policy: Class Based. Below it is a table:

Class ID	Name	Priority	Bandwidth		Status	Action
			Reserved	Maximum		
<input type="checkbox"/> 1	VoIP Tx	0	0 Kbps	Unlimited	Active	
<input checked="" type="checkbox"/> default	default	4	0 Kbps	Unlimited	Active	

The bottom panel is 'Rx Traffic Policing' with settings: Rx Bandwidth: Specify 200 Kbps, Devices: (empty). Below it is a table:

Class ID	Name	Priority	Bandwidth		Status	Action
			Reserved	Maximum		
<input type="checkbox"/> 0	VoIP Rx	0	0 Kbps	Unlimited	Active	

At the bottom of the Rx Traffic Policing section are three buttons: 'OK', 'Apply', and 'Cancel'.

Figure 7.185. Shaping Classes – Uncheck the Class ID

- d. Click the class name to edit the shaping class. Alternatively, click its action icon. The 'Edit Class' screen appears (see [Figure 7.186](#)).
- e. Enter 100 Kbps in the Reserved Tx/Rx Bandwidth field.
- f. Leave all other fields at their default values.

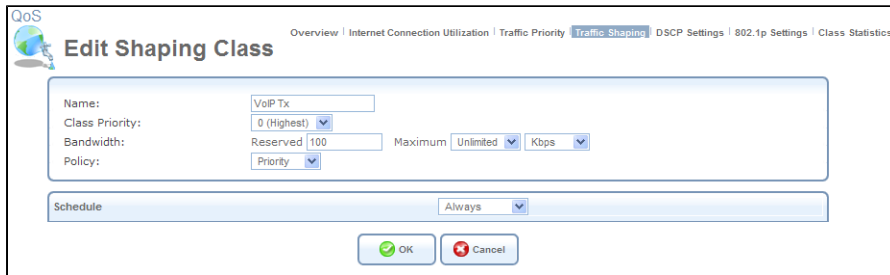


Figure 7.186. Edit Shaping Class

- g. Click 'OK' to save the settings.
 - h. Click 'OK' once more in the 'Edit Device Traffic Shaping' screen to save all settings.
5. Define and associate class rules:
- a. Click 'Traffic Priority' under the 'QoS' tab in the 'Services' screen. The 'Traffic Priority' screen appears.

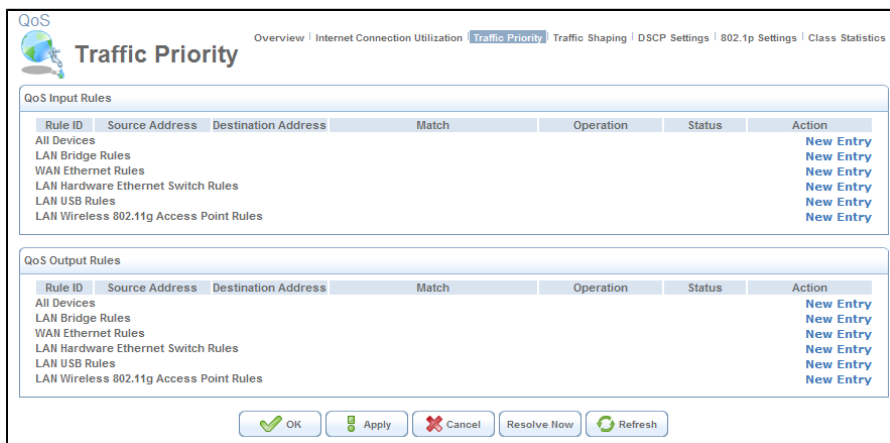


Figure 7.187. Traffic Priority

- b. Click the 'New Entry' link of the 'WAN Ethernet Rules' under the 'QoS Output Rules' section. The 'Add Traffic Priority Rule' screen appears.

QoS Overview | Internet Connection Utilization | **Traffic Priority** | Traffic Shaping | DSCP Settings | 802.1p Settings | Class Statistics

Add Traffic Priority Rule

Matching

Source Address: Any

Destination Address: Any

Protocol: Any

DSCP
 Priority
 Length

Operation

Set DSCP
 Set Priority
 Set Rx Class Name
 Set Tx Class Name

Apply QoS on: Connection

Logging

Log Packets Matched by This Rule

Schedule

Always

OK Cancel

Figure 7.188. Add Traffic Priority Rule

- c. In the 'Matching' section, select 'Show All Services' from the 'Protocol' drop-down menu, and then select "SIP". The screen will refresh displaying the protocol parameters (see [Figure 7.189](#)).
- d. In the 'Operation' section, check the 'Set Rx/Tx Class Name' check boxes, and select 'VoIP Rx/Tx' from the drop-down menus that appear.

Matching

Source Address: Any

Destination Address: Any

Name	Ports	Action
SIP	UDP Any -> 5060	✖
Add...		

DSCP
 Priority

Operation

Set DSCP
 Set Priority
 Set Rx Class Name: VoIP Rx
 Set Tx Class Name: VoIP Tx

Apply QoS on: Connection

Figure 7.189. Add Traffic Priority Rule – SIP Protocol

- e. Leave all other fields at their default values, and click 'OK' to save the settings.

7.4.8.3.1. Implementing the WRR Class Policy in VoIP's QoS

The WRR class policy enables you to fine-tune your Tx traffic priority settings. For instance, in a scenario where you utilize more than one VoIP protocol (for example, SIP and H.323), you can further prioritize VoIP's Tx traffic. In the following example, the SIP protocol is given preference over H.323. Therefore, you may assign 70% of the VoIP bandwidth to the SIP-based traffic, and 30% to the H.323-based traffic. To enable the WRR class policy, perform the following:

1. In the 'Edit Device Traffic Shaping' screen (see [Figure 7.185](#)), click the 'VoIP Tx' link. The 'Edit Shaping Class' screen appears (see [Figure 7.186](#)).
2. From the 'Policy' drop-down menu, select the WRR option. The screen refreshes, and a new section called 'Subclasses' is added.

Figure 7.190. Subclasses Section in Edit Shaping Class


3. In the 'Subclasses' section, click either the 'New Entry' link or the  action icon. The 'Add Shaping Class' screen appears.

Figure 7.191. Add Shaping Class

This time, the screen contains two fields: 'Name' and 'Weight'.

4. In the 'Name' field, enter 'SIP' for the name of a VoIP's subclass assigned to the SIP-based traffic.
5. In the 'Weight' field, enter a numeric value that correlates with the amount of bandwidth you want to grant to the subclass. In the current example, the subclass is granted 70% of VoIP's Tx traffic. Therefore, enter 7 in the 'Weight' field.



Note: The class weight range is between 1 and 10000.

6. Click 'OK' to save the settings.

Repeat the same procedure for creating the H.323 subclass of VoIP. However, in the 'Weight' field enter **3** that corresponds to 30% of the VoIP bandwidth you want to assign to the H.323 subclass.



Note: When you activate the WRR class policy, it is not mandatory to define an Rx shaping class and its priority rules.

Once the subclasses are created, define the priority rules for the subclasses, as follows:

1. Click 'Traffic Priority' under the 'QoS' tab in the 'Services' screen. The 'Traffic Priority' screen appears (see [Figure 7.187](#)).
2. Click the 'New Entry' link of the 'WAN Ethernet Rules' under the 'QoS Output Rules' section. The 'Add Traffic Priority Rule' screen appears (see [Figure 7.188](#)).
3. In the 'Matching' section, select 'Show All Services' in the 'Protocol' drop-down menu, and then select 'SIP'. The screen refreshes displaying the protocol parameters.



Note: You can also define the 'SIP' protocol manually, as described in [Section 7.4.8.3](#).

4. In the 'Operation' section, check the 'Set Tx Class Name' check box, and select 'SIP' in the drop-down menu that appears.

The screenshot shows a configuration window with two main sections: 'Matching' and 'Operation'.

Matching Section:

- Source Address: Any
- Destination Address: Any
- Protocol: A table with columns 'Name', 'Ports', and 'Action'.

Name	Ports	Action
SIP	UDP Any -> 5060	✘
Add...		
- Below the table are three checkboxes: DSCP, Priority, and Length, all of which are unchecked.

Operation Section:

- Set DSCP:
- Set Priority:
- Set Rx Class Name: (with a red 'x' icon next to it)
- Set Tx Class Name:
- Apply QoS on: Connection
- On the right side, there is a message: "No RX class names available" with a dropdown menu showing "SIP".

Figure 7.192. Add Traffic Priority Rule # SIP Protocol

5. Leave all other fields at their default values, and click 'OK' to save the settings.

Repeat the same procedure for defining a priority rule for the H.323 subclass. The only difference is that you should select the 'H.323 Call Signaling' value for the protocol settings, and 'H.323' for the Tx class name.

7.4.8.4. Running the Scenario

1. Initiate a direct call (using the SIP protocol) from one IP phone to the other. For VoIP configuration, refer to [Section 7.6](#). Verify that the conversation can be conducted clearly and adequately.
2. Initiate an FTP file upload from the LAN computer to the WAN computer. This can be done using the Windows command line. Use the **hash** command to utilize the pound sign process indicator before starting the file transfer. As soon as the upload commences, your ability to transmit voice will be lost—the WAN party will not be able to hear you. The upload, on the other hand, will be proceeding rapidly, taking up all of your transmit bandwidth (see [Figure 7.193](#)).

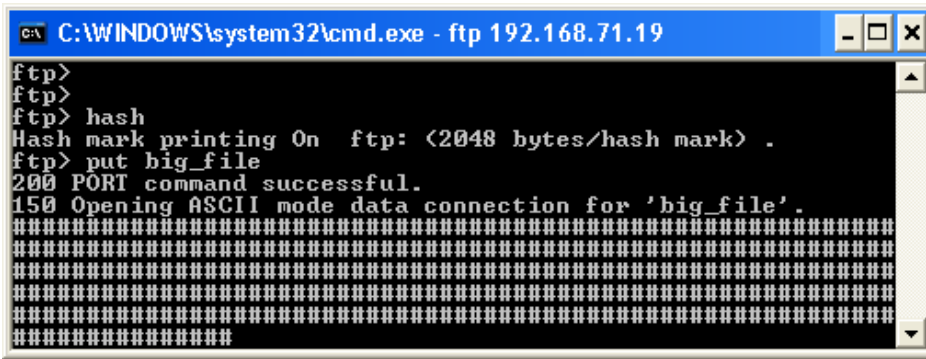


Figure 7.193. FTP Process

3. Activate QoS to restore the voice transmission:

- a. Under the 'QoS' menu item, click 'Traffic Shaping'. The 'Traffic Shaping' screen appears.

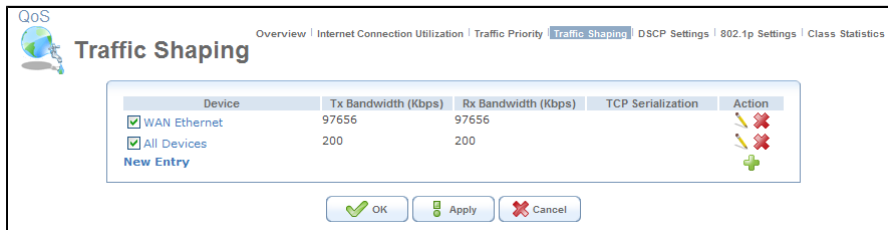


Figure 7.194. Traffic Shaping

- b. Click the Device name, in this case 'All devices', and check both entries in the Class ID column to enable the classes (see [Figure 7.195](#)).

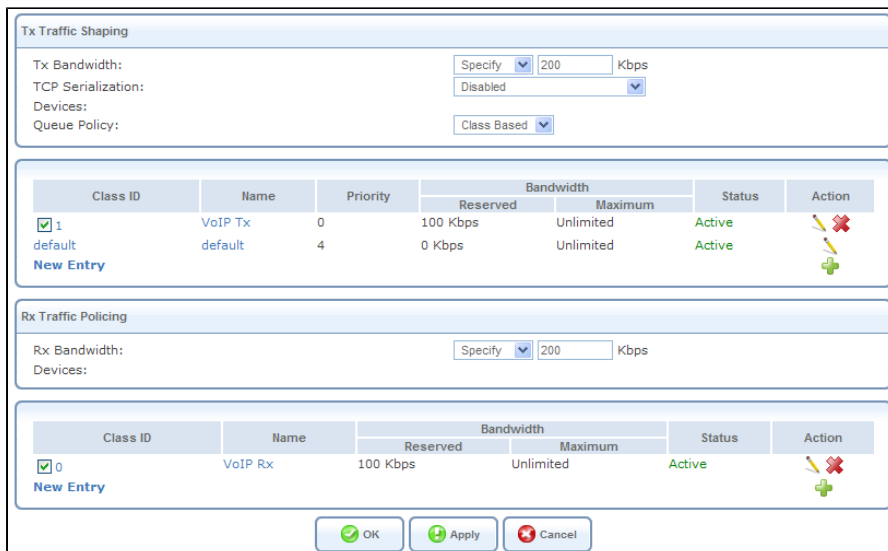


Figure 7.195. Shaping Classes – Check the Class ID

- c. Click 'OK' to save the settings.

The transmission capability will be restored, as most of the bandwidth will now be reserved for the VoIP stream. The file upload rate, on the other hand, will obviously slow down.



Note: Some IP phones and ATA devices are preconfigured to send DSCP-marked data. OpenRG will handle such data with QoS priority, even if a QoS class is not configured for the VoIP stream. To run the above scenario successfully, you must first disable DSCP marking on such devices.

7.4.9. IPTV QoS Scenario

This section presents a scenario in which the WAN bandwidth is shaped to provide priority to a media broadcast (for example, an IPTV stream). When your bandwidth is shared between a media stream and data transfer, a greater portion of it will normally be used by the data transfer, reducing the quality of the media broadcast or even disrupting it. With the help of OpenRG's Traffic Shaping feature, the media stream receives the priority it requires, thereby maintaining its quality. This scenario is based on the following real-life case.

Assume that you have a 100 Mbps Ethernet LAN with a 100 Mbps WAN interface router. The router communicates with the ISP network via a modem that has a 2Mbps bandwidth, and does not have a QoS module. When OpenRG's Traffic Shaping feature is disabled, the router sends traffic to the modem as fast as it is received from the LAN host. This typical configuration makes the modem a bottleneck. However, if you enable Traffic Shaping on the router, it will limit the router's bandwidth, artificially forcing it to be the bottleneck. This configuration creates a regulated traffic queue that enables the router to accept uneven and bursty flows of packets and transmit them in a steady, predictable stream.

7.4.9.1. Simulating Limited Bandwidth and IPTV Setup

As a first step, simulate limited bandwidth by reducing OpenRG's Rx/Tx bandwidth in the following way:

1. Under the 'Services' tab, click 'QoS'. The following screen appears.

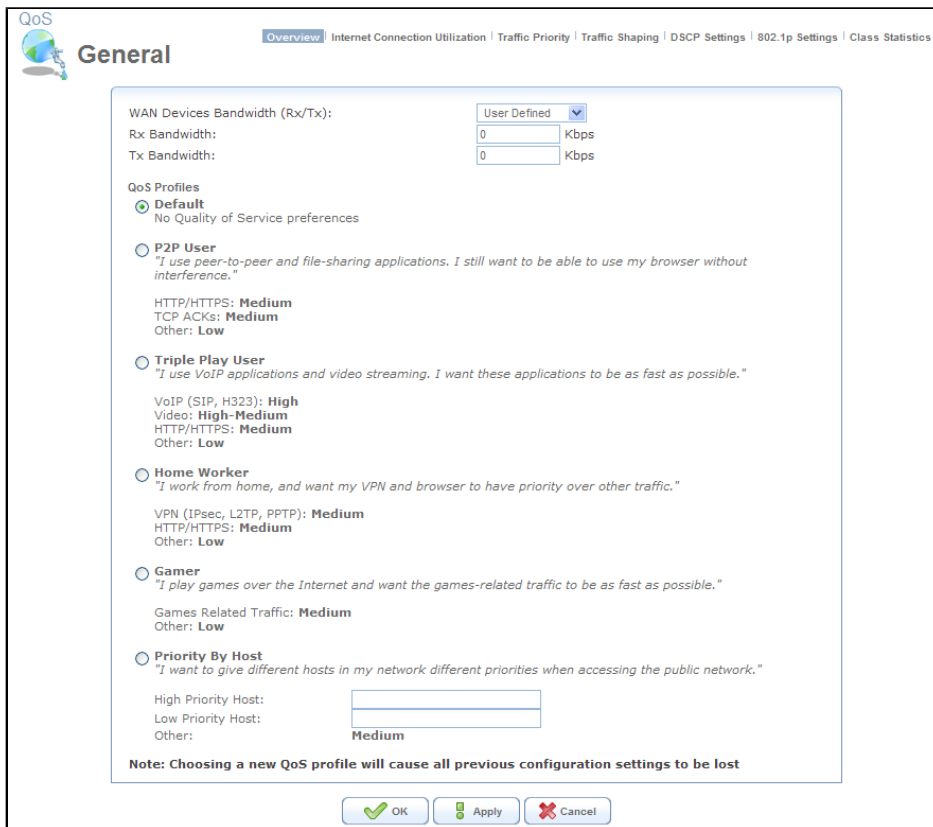


Figure 7.196. General

2. From the 'WAN Devices Bandwidth(Rx/Tx)' drop-down menu, select 5000/256 Kbps.
3. Click 'OK' to save the settings.

To simulate an IPTV setup, use the *Video LAN Client* (VLC) application. VLC supports both Client and Server modes. In its server mode, VLC can be used on a WAN host as the broadcaster, which sends a video stream to a multicast group. In its client mode, VLC can be used as a media player on a LAN host. VLC uses a multicast IP address range between 224.0.0.0 – 239.255.255.255. It can be installed both on Linux and Windows computers. You can download VLC from <http://www.videolan.org/vlc/download-windows.html>.

To configure the VLC server, perform the following:

1. In VLC's 'File' menu, select 'Wizard'. The following screen appears.



Figure 7.197. Streaming/Transcoding Wizard

2. Select the 'Stream to Network' radio button and click 'Next'. The 'Input' screen appears.

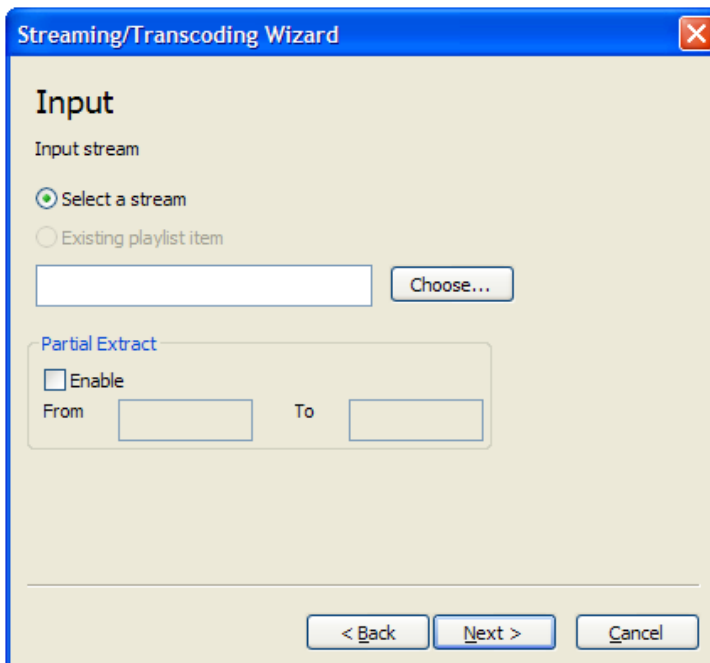


Figure 7.198. Input

3. Verify that the 'Select a stream' radio button is selected, and click 'Choose'. The following dialog box appears.

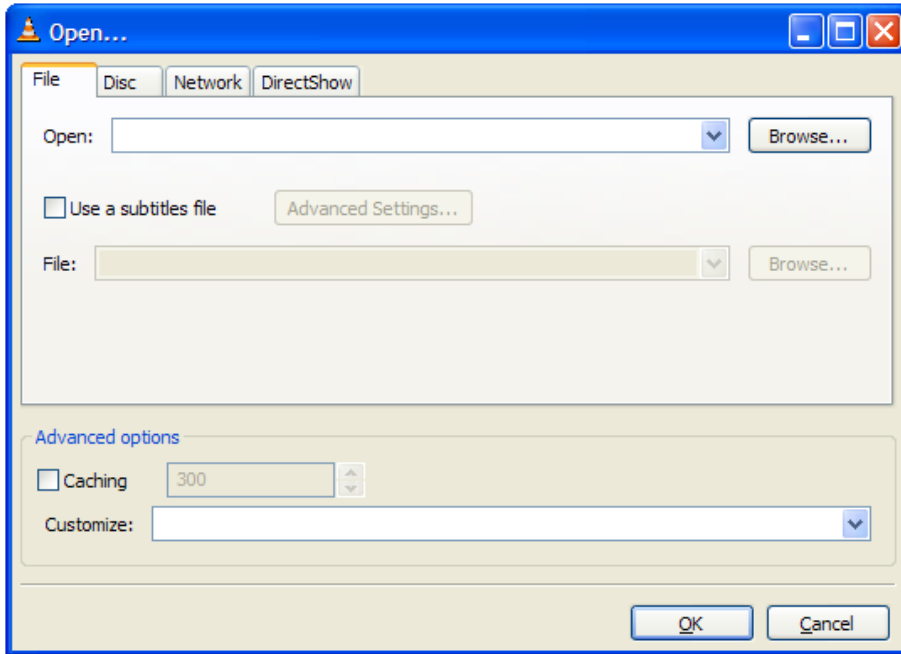


Figure 7.199. File Selection Dialog Box

4. Click 'Browse', and select the video file you would like to stream.
5. Click 'OK', and then 'Next'. The 'Streaming' screen appears.

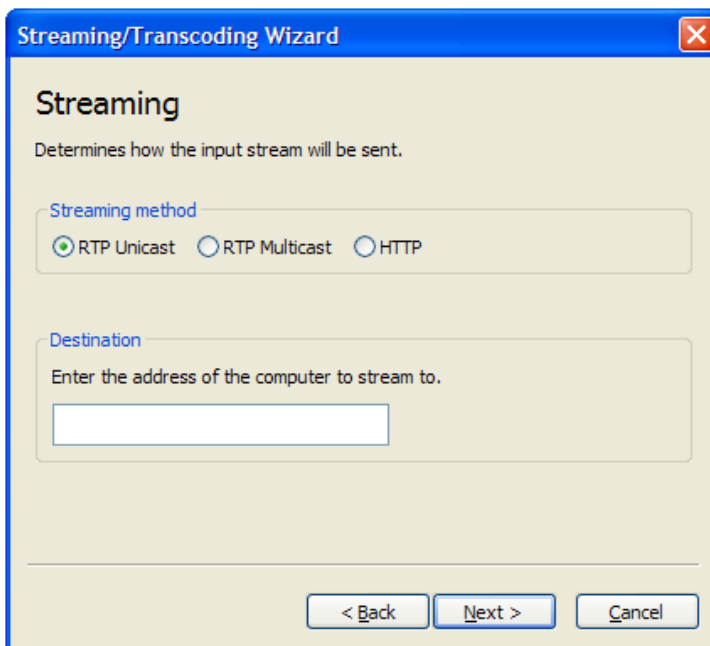


Figure 7.200. Streaming

6. Under 'Streaming method', select 'RTP Multicast'.
7. In the 'Destination' field, enter the multicast group IP address (between 224.0.0.22 – 224.0.0.102).

- Click 'Next'. The 'Encapsulation format' screen appears.

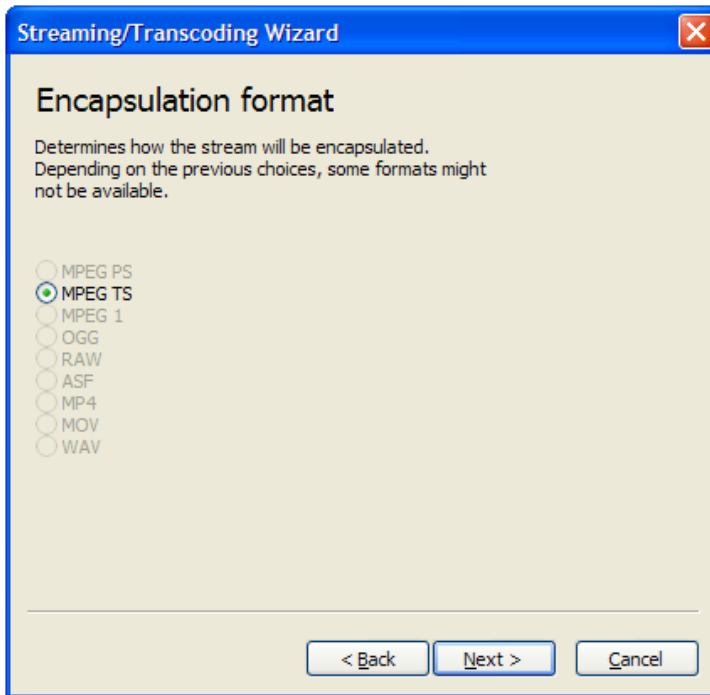


Figure 7.201. Encapsulation format

- Verify that the 'MPEG TS' radio button is selected, and click 'Next'. The 'Additional streaming options' screen appears.

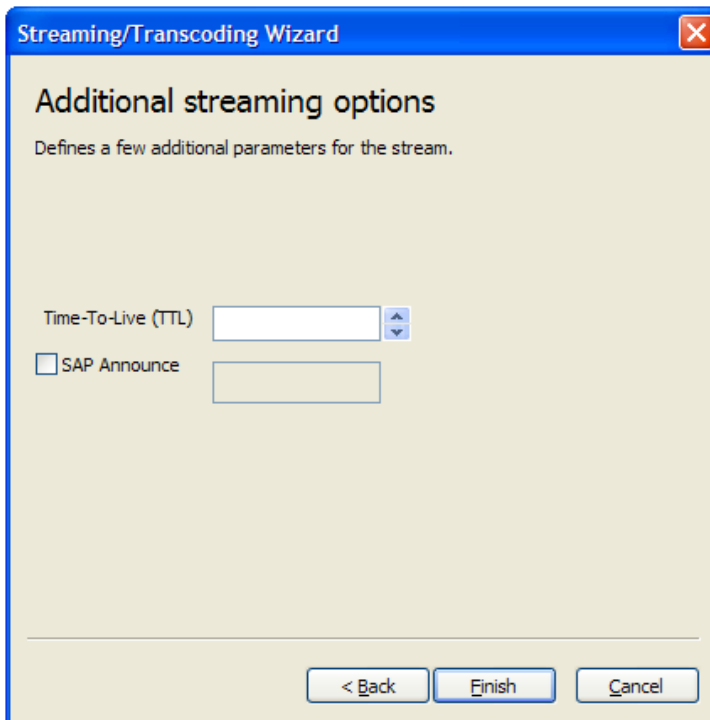


Figure 7.202. Additional streaming options

- Set the 'Time-To-Live (TTL)' parameter to be greater than five (depends on the number of network hops).

11. Click 'Finish' to exit the wizard.

To configure the VLC client, perform the following:

1. From the 'File' menu, select 'Open Network Stream'. The following screen appears.

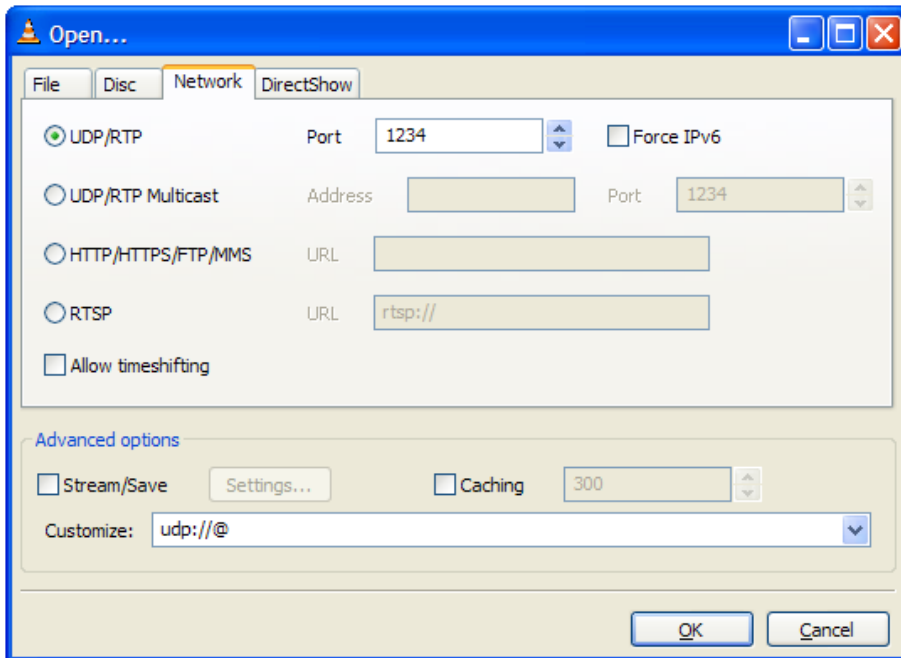


Figure 7.203. Network

2. Select the 'UDP/RTP Multicast' radio button, and enter the multicast group address (as defined in the VLC server) in the 'Address' text box that opens.
3. Click 'OK' to save the settings.

While watching the video on the LAN PC, load the network by downloading a large file from the WAN using FTP. Run the FTP's **hash** command to visualize the file download speed. The video and sound stream quality will noticeably degrade.

7.4.9.2. Using QoS for Improving the Streaming Quality

To improve the media stream quality, perform the following:

1. Designate a protocol and a specific port number for the media stream:
 - a. In OpenRG's WBM, click the 'Advanced' tab and select 'Protocols'. The 'Protocols' screen appears.

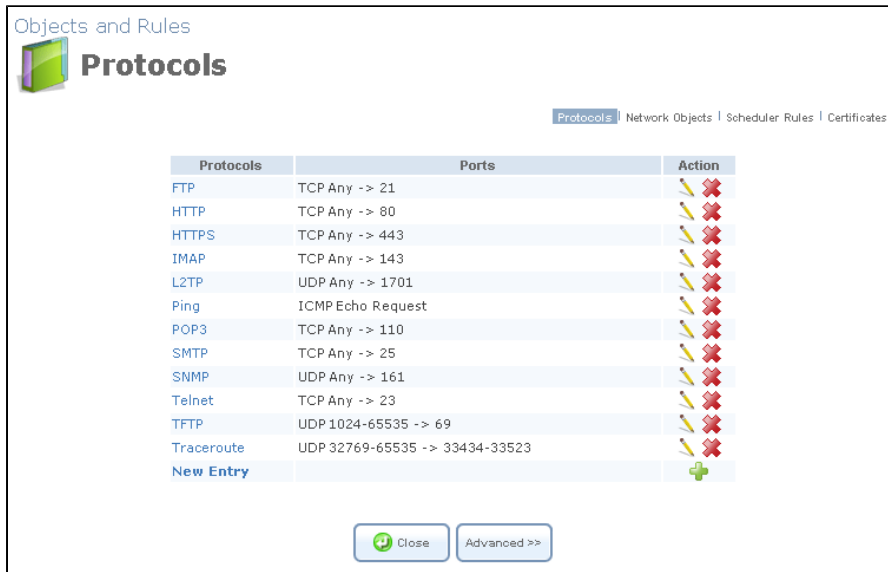


Figure 7.204. Protocols

This screen displays a list of preset and user-defined applications and common port settings. You may add new protocols to support new applications or edit existing ones according to your needs. For more information, refer to [Section 8.9.1](#).

- b. Click the 'New Entry' link. The 'Edit Service' screen appears.

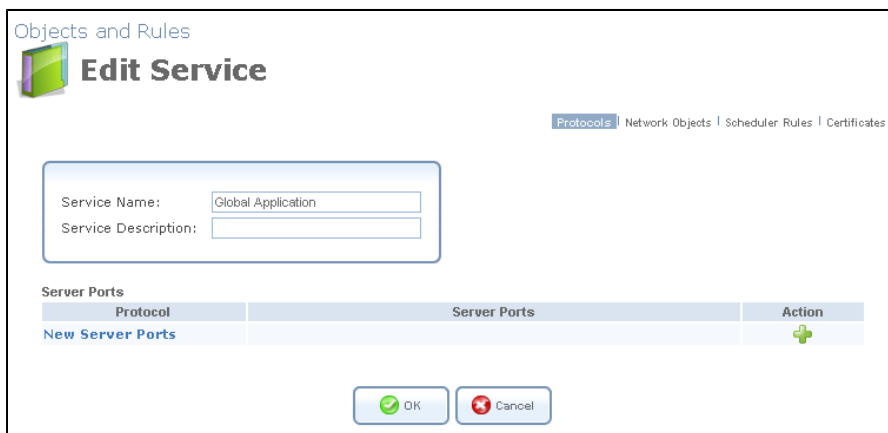


Figure 7.205. Edit Service

- c. Change the default service name to 'IPTV', and click the 'New Server Ports' link. The 'Edit Service Server Ports' screen appears.

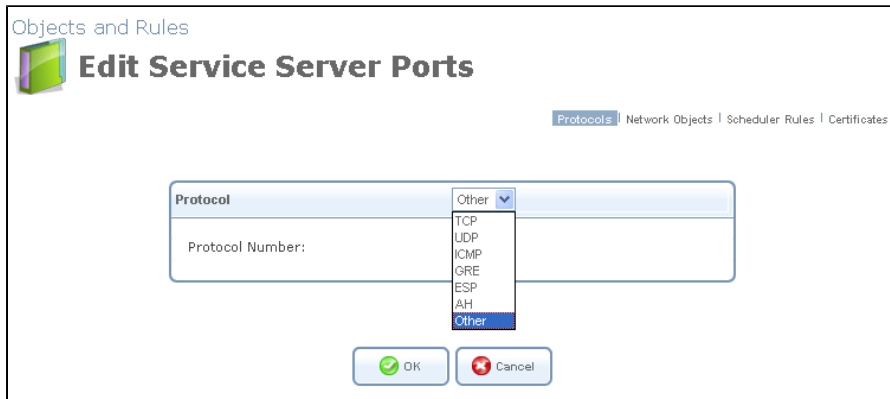


Figure 7.206. Edit Service Server Ports

- d. From the 'Protocol' drop-down menu, select 'UDP'. The screen refreshes, changing to the following.

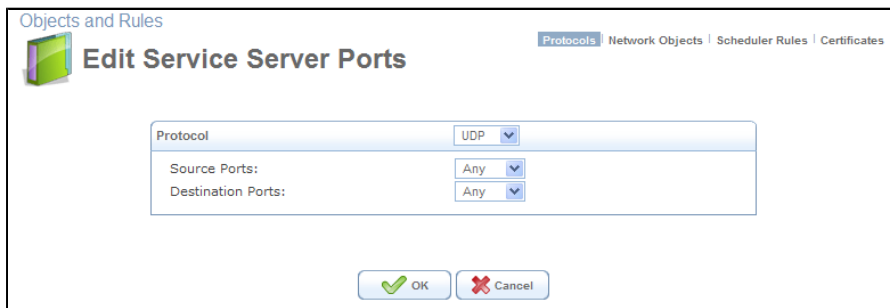


Figure 7.207. Edit Service Server Ports – UDP

- e. From the 'Source Ports' drop-down menu, select 'Any'.
 - f. From the 'Destination Ports' drop-down menu, select 'Single' and enter port 1234 (the default port to which VLC sends the media stream).
 - g. Click 'OK' to save the settings.
2. Create a traffic shaping class ID:
- a. Under the 'Services' tab, click the 'QoS' menu item and select 'Traffic Shaping'. The 'Traffic Shaping' screen appears, displaying the bandwidth you have set on the default WAN device.

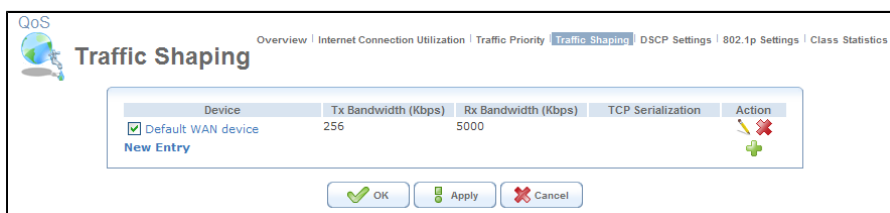


Figure 7.208. Traffic Shaping


- b. Click the 'Default WAN device' link or its  action icon . The 'Edit Device Traffic Shaping' screen appears.

Figure 7.209. Edit Device Traffic Shaping

- c. Under 'Class ID', click the 'New Entry' link. The 'Add Policing Class' screen appears.

Figure 7.210. Add Policing Class

- d. Change the default class name to 'IPTV', and click 'OK'. The 'Edit Device Traffic Shaping' screen appears with the IPTV class entry displayed in the 'Rx Traffic Policing' section.

Figure 7.211. Edit Device Traffic Shaping – IPTV Class

- e. Click the 'IPTV' link or its  action icon . The 'Edit Policing Class' screen appears.

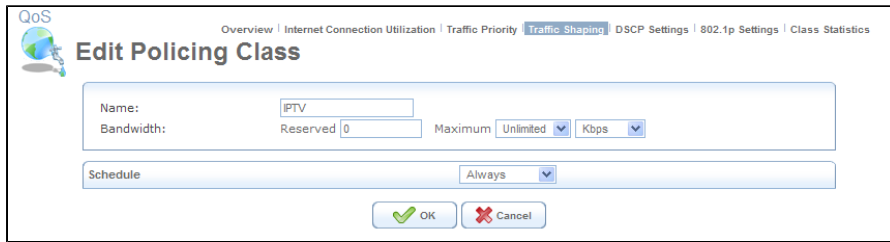


Figure 7.212. Edit Policing Class – IPTV

- f. In the 'Reserved' field of the 'Bandwidth' parameter, enter 3000 and click 'OK'. You will be redirected back to the 'Edit Device Traffic Shaping' screen (see [Figure 7.211](#)). The bandwidth reserved for the IPTV will be displayed in its respective field.
3. As the last step, define a priority rule for the incoming traffic:
- a. Under the 'QoS' menu item, click 'Traffic Priority'. The corresponding screen appears.

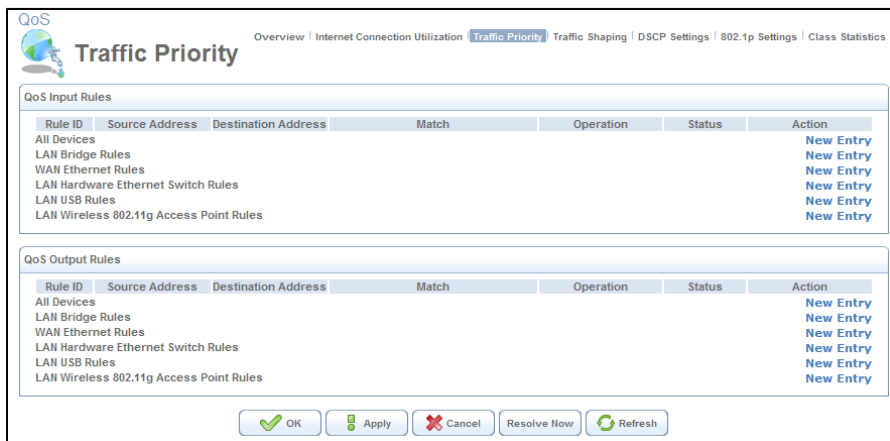


Figure 7.213. Traffic Priority

- b. In the 'QoS Input Rules' section, click the 'New Entry' link of the 'WAN Ethernet Rules' item. The 'Add Traffic Priority Rule' screen appears.

Figure 7.214. Add Traffic Priority Rule

- c. From the 'Protocol' drop-down menu, select 'IPTV' (if it is not displayed, select 'Show All Services'). The screen refreshes, displaying the IPTV protocol entry.

Name	Ports	Action
IPTV	UDP Any -> 1234	✘

Figure 7.215. Add Traffic Priority Rule – IPTV Protocol

- d. Under 'Operation', select the 'Set Rx Class Name' check box. The screen refreshes, displaying the IPTV Rx class.

Figure 7.216. Add Traffic Priority Rule – IPTV Rx Class

- e. Click 'OK' to save the settings.

Restart the video stream on the LAN while downloading a large file from the WAN using FTP. You will notice that the video stream has no disruptions, while the file download speed slows down slightly.

7.5. Media Sharing

OpenRG's Media Sharing solution enables you to share and stream media files from a storage device connected to OpenRG. You can access the shared media files with either a network-aware Consumer Electronic (CE) device, as described in [Section 2.4.4](#), or from a LAN PC with an installed media rendering software. Both methods utilize a Universal Plug and Play (UPnP) media renderer (for more information on UPnP, refer to [Section 8.7.1](#)).

7.5.1. Configuring the Media Sharing Service

Configure OpenRG's media sharing service by clicking its tab in WBM's 'Services' screen. The 'Media Sharing' screen appears.

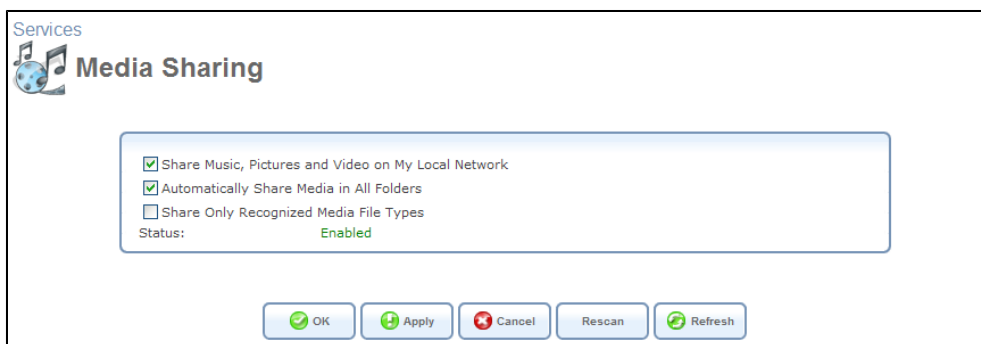


Figure 7.217. Media Sharing

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. To disable automatic sharing and manually share a specific partition or folder, perform the following:

1. Deselect the 'Automatically Share Media in All Folders' check box and click 'Apply'. The screen refreshes.

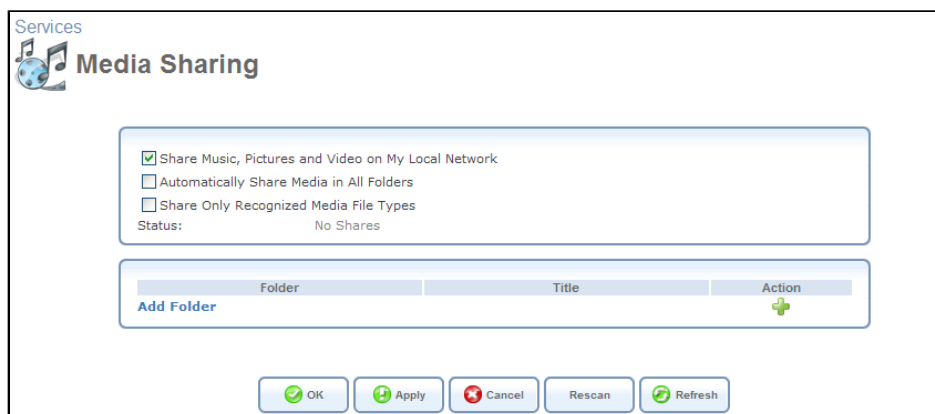


Figure 7.218. Manual Folder Sharing Mode

The 'Status' field changes to 'No Shares', and a new section appears, enabling you to create and manage a list of manually shared partitions and their folders.



2. Click the 'Add Folder' link, or the  action icon . The 'Folder Settings' screen appears.



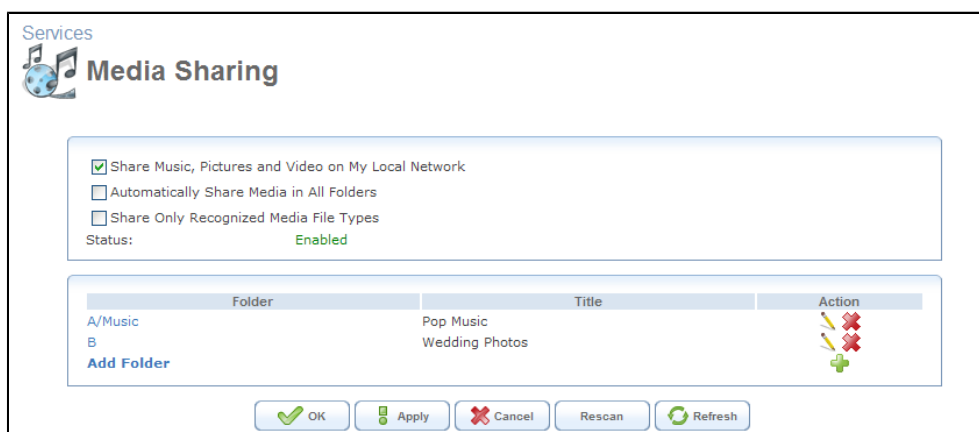
Figure 7.219. Folder Settings

3. In the 'Folder' field, enter the exact path (for example, **A/Music**, where 'A' is a partition's letter, and 'Music' is a folder on this partition).

 Note: The partition's letter cannot be changed. OpenRG automatically assigns a letter to a partition, once the storage device is connected. For more information, refer to [Section 6.4](#).

4. In the 'Title' field, enter a descriptive title for the folder (for example, 'Pop Music'). Note that entering this information is mandatory.
5. Click 'OK' to save the settings.

The 'Media Sharing' screen appears, displaying the shared partition. If necessary, repeat the same procedure to share additional partitions and their folders.









Folder	Title	Action
A/Music	Pop Music	 
B	Wedding Photos	 

Figure 7.220. Manually Shared Partitions

At any time, you can edit the partition or folder sharing settings by clicking its  action icon . In addition, you can remove a partition or a folder from the shares list by clicking its  action icon .



Note: In case of changing the sharing settings, click the 'Rescan' button in the WBM's 'Media Sharing' screen before trying to access the shared media remotely. Clicking the 'Rescan' button updates the media database with the current shared media content and its path. The more disk space the media files occupy, the longer the scanning process may take.

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

- Audio: MP3, OGG, WAV, and WMA.
- Video: MPEG, MPG, MPE, ASF, AVI, DIVX, WMV, MOV, and QT.
- Graphics: JPEG, JPG, JPE, GIF, PNG, TIFF, TIF, and BMP.

Once a storage device is connected, OpenRG automatically scans it for media files. In addition, OpenRG adds the **MEDIASRV.DB** file to all the writable partitions it identifies. This is an index file that the media server uses to access the files on the disk.



Note: Unless OpenRG is based on the Freescale platform, an NTFS partition cannot be used for media sharing because it is only *readable*. OpenRG does not scan an NTFS partition for the presence of media files.

When adding or removing a file via OpenRG's file server, the media database is updated automatically. However, if other file management utilities are used (for example, FTP) to add or remove a file, you should click the 'Rescan' button to update the database with the changes. Otherwise, OpenRG will update the database during its periodic scanning of the shared media, which is performed every 24 hours.

7.5.2. Accessing the Shared Media from a LAN Computer

In [Section 2.4.4](#), you learned how to view and stream your media files on your TV set. In addition, you can access your media content from any LAN PC on which a media rendering client application is installed. One of such applications is **Nero Home™**. The following example utilizes Nero Home to demonstrate how to access the shared media via a LAN PC. After installing Nero Home, perform the following:

1. Launch the Nero Home application. Nero Home's main screen appears.



Figure 7.221. Nero Home Main Screen

2. Click the 'MediaHome Network' link. The 'MediaHome Network' screen appears, displaying the available media servers.

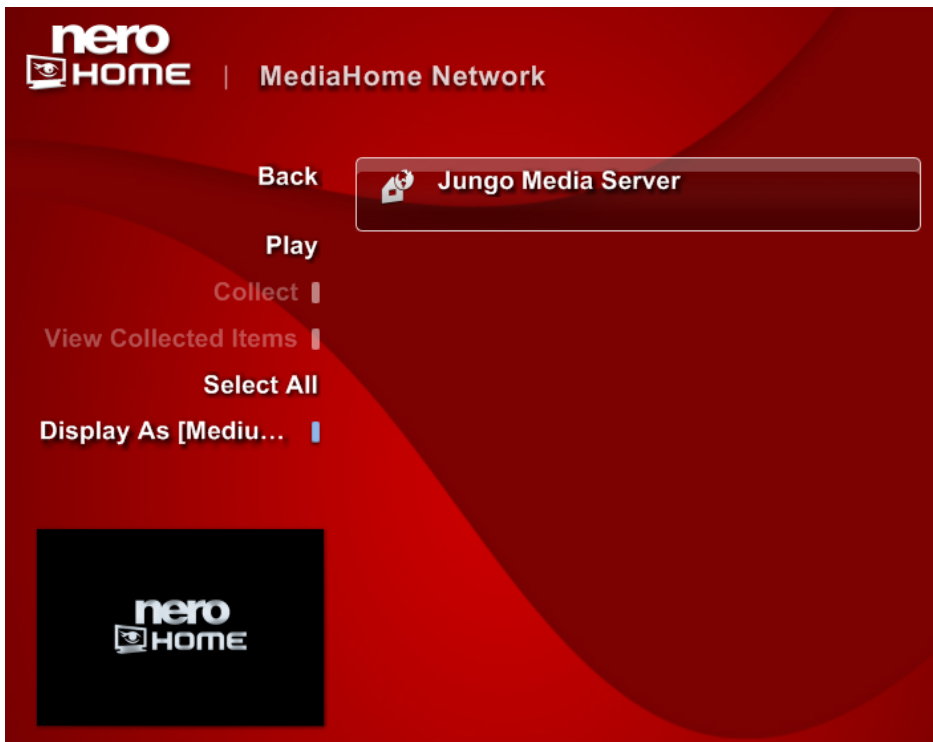


Figure 7.222. MediaHome Network

As evident, reception of OpenRG's media server broadcast by the Nero Home application is automatic, requiring no further configuration.

3. Click the 'Jungo Media Server' button. The path letters of the OpenRG shares containing your disk content appear.



Figure 7.223. Jungo Media Server

4. Select a share. The share's content is displayed.

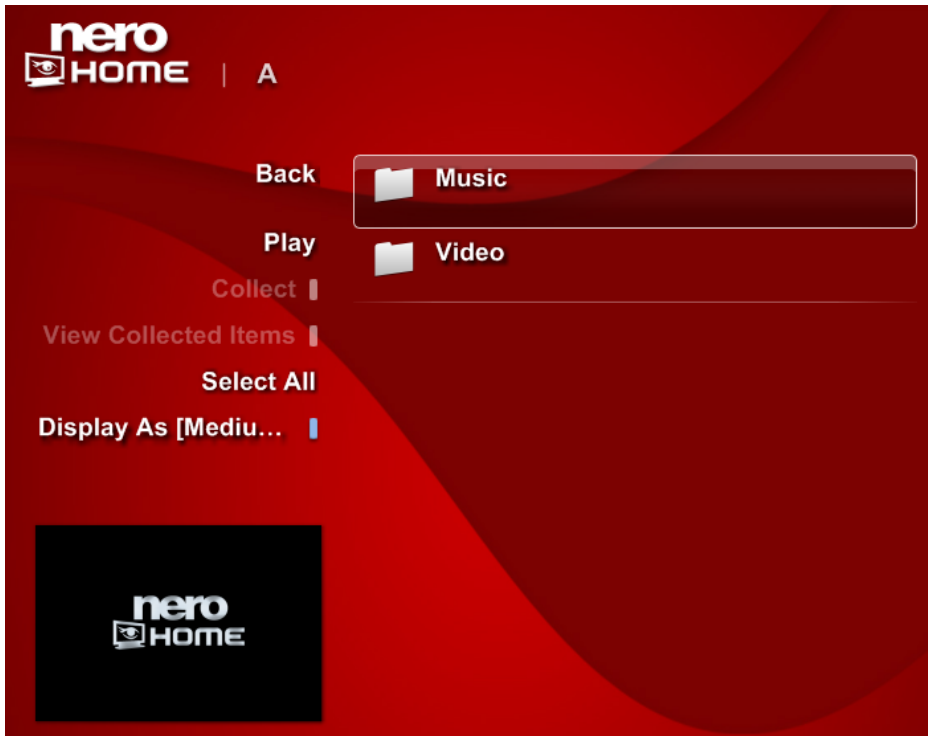



Figure 7.224. Media Folders on a Share

 Note: Nero Home displays the same directory hierarchies as on the storage device.

5. Select a folder, for example "Music". The folder's content is displayed.

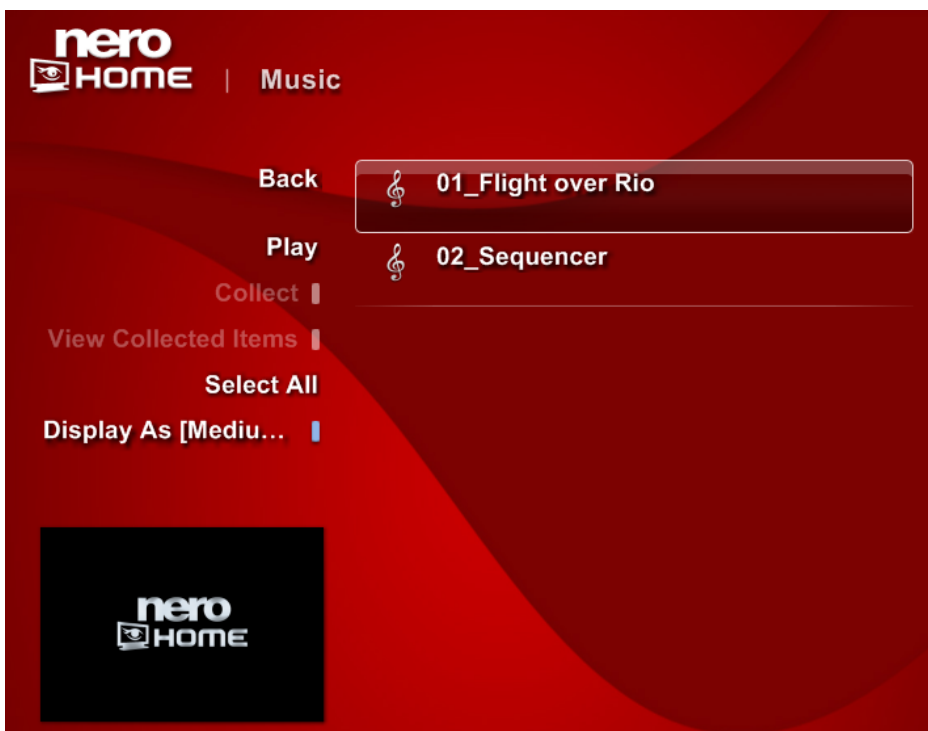


Figure 7.225. Media Files in the Shared Folder

6. Click 'Play' to open the file in a media player.

If you have chosen to manually share specific partitions or folders (automatic sharing mode is disabled), the 'Jungo Media Server' screen displays only the titles of the folders that you had specified.

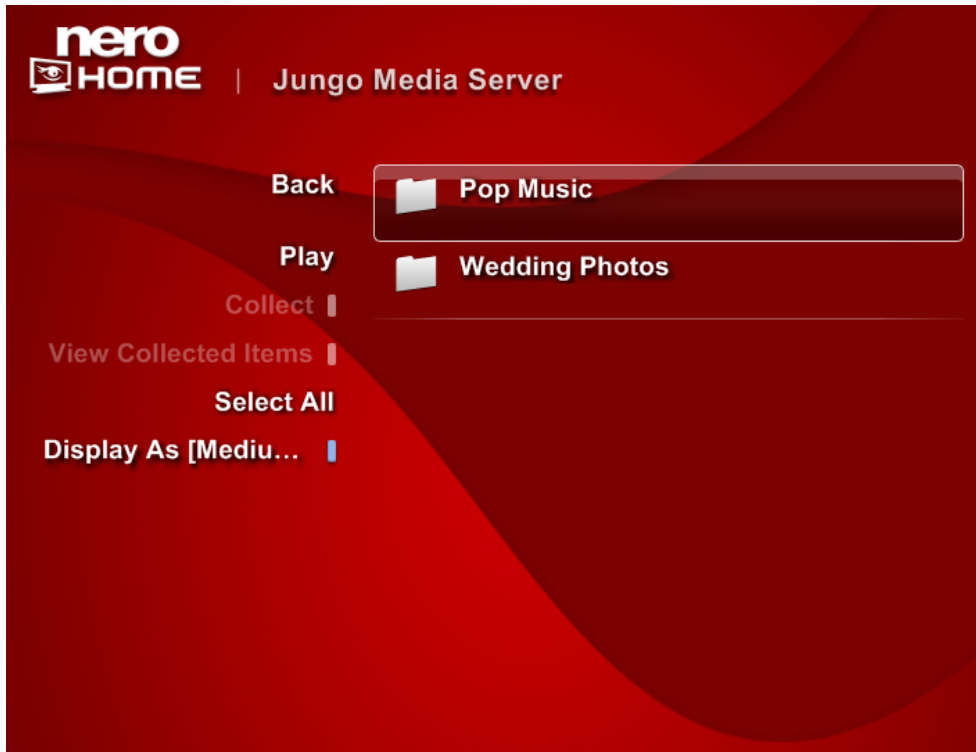


Figure 7.226. Manually Shared Folders

For more information about Nero Home operation, refer to the Nero Home Manual.

7.6. Voice

OpenRG's Analog Telephone Adapter (ATA) Voice solution enables you to connect multiple phones over a single broadband connection, providing the benefits and quality of digital Voice Over IP (VoIP). This solution enables you to place and receive calls over the Internet using a standard telephone set connected to OpenRG.

This section assumes that you have already connected your telephone equipment to the gateway, as described in [Section 2.4.1](#).




Note: OpenRG's voice functionality is based on the Asterisk VoIP stack.



Note: Some of the documented WBM features may appear slightly different or may not be available on certain platforms.

7.6.1. Configuring Your Telephone Line Services

Before using your telephone, configure the services available on its line according to your preference. In the 'Line Settings' screen under the 'Voice' menu item, click the line's  action icon. In the 'Services' section, select the services you would like to activate.

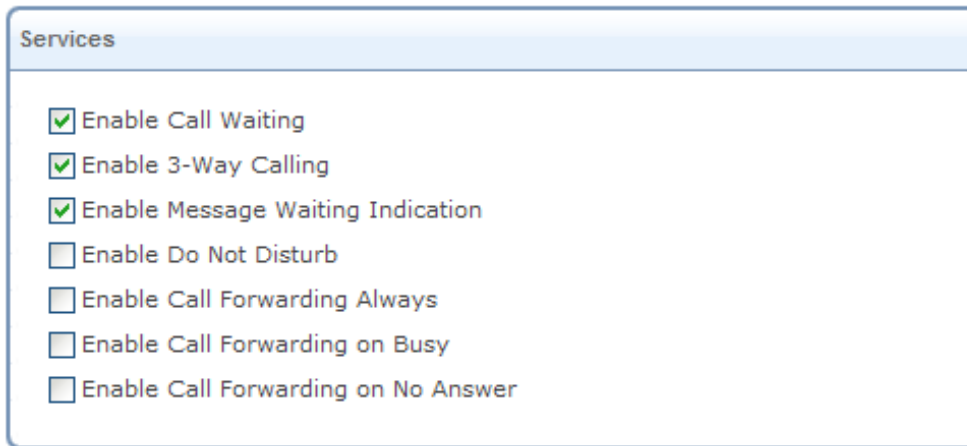


Figure 7.227. Line Settings – Services

Enable Call Waiting Select this check box to enable the Call Waiting feature.

Enable 3-Way Calling Select this check box to allow all forms of three-way conversations. When this option is disabled you will not be able to place a call on hold, transfer a call or engage in a call conference.

Enable Message Waiting Indication Select this check box to play a special tone whenever you receive a voice message.

Enable Do Not Disturb Select this check box to prevent calls from reaching your line. The caller will hear a busy tone. This feature can also be enabled or disabled by dialing *78 or *79 respectively.

Enable Call Forwarding Always Select this check box to forward incoming calls to another telephone number. The screen refreshes, displaying a field for entering the alternate number.



Figure 7.228. Enable Call Forwarding Always

Enable Call Forwarding on Busy Select this check box to forward incoming calls to another telephone number when the line is busy. The screen refreshes, displaying a field for entering the alternate number.

Enable Call Forwarding on Busy

Forward Calls to:

Figure 7.229. Enable Call Forwarding on Busy

Enable Call Forwarding on No Answer Select this check box to forward incoming calls to another telephone number if the call is not answered within a specific timeframe. The screen refreshes, displaying a field for entering the alternate number, and a field for determining the timeframe to ring before the call is forwarded.

Enable Call Forwarding on No Answer

Forward Calls to:

Time to Ring Before Forwarding Call: seconds

Figure 7.230. Enable Call Forwarding on No Answer

7.6.2. Operating Your Telephone

Following are several guidelines that will help you perform basic telephone operations.

- **Placing a Call**

1. Pick up the handset on the phone.
2. Dial the remote party's number or a pre-configured speed dial number. To have the call sent out immediately, you may dial '#'.

- **Answering a Waiting Call**

When the Call Waiting feature is enabled, you may receive a call while engaged in another call. When such call arrives, you will hear a call waiting tone.

1. To answer a waiting call, press 'Flash'.
2. 'Flash' may be used to switch back and forth between calls.

- **Blind Transfer**

To transfer an existing call (B) to a third party (C) without consultation, perform the following:

1. Press 'Flash'. Party B will now be placed on hold, and you will hear a dial tone.
2. Dial *98. You should hear three short beeps followed by a dial tone.
3. Dial party C's number. You should hear a high toned beep followed by two low toned beeps, followed by a dial tone. B is now initiating a call to C. You may now dial a new call or hang up the phone.

- **Call Transfer With Consultation**

To transfer an existing call (B) to a third party (C), perform the following:

1. Press 'Flash' on the phone. Party B will now be placed on hold, and you will hear a dial tone.
2. Dial party C's number or a pre-configured speed dial number followed by '#' (you can engage in conversation).
3. To complete the transfer, place the phone's handset on-hook.

- **3-Way Conference**

To extend an existing call (B) into a 3-way conference by bringing in an additional party (C), perform the following:

1. Press 'Flash' on the phone. Party B will now be placed on hold and you will hear a dial tone.
2. Dial party C's number or a pre-configured speed dial number followed by '#' (you can engage in conversation).
3. Press 'Flash' to join both C and B to a single conference.
4. When you place the phone's handset on-hook, party B and party C will remain in conversation.

7.6.3. Configuring and Using Speed Dial

You can assign speed dial numbers to parties that you call frequently. Speed dial entries can be configured according to three types of destinations:

- **Proxy speed dial entry** This entry is intended for calling users that have an account with your telephone service provider.

1. Click the 'Speed Dial' link under the 'Voice' menu item. The 'Speed Dial' screen appears.

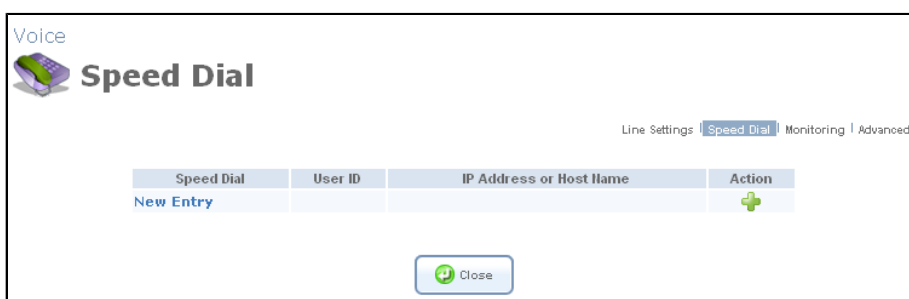


Figure 7.231. Speed Dial

2. Click the 'New Entry' link to add a new speed dial entry. The 'Speed Dial Settings' screen appears.

Voicemail **Speed Dial Settings**

Line Settings | **Speed Dial** | Monitoring | Advanced

Speed Dial:

Destination:

User ID:

Figure 7.232. Speed Dial – via Proxy

3. Enter the following parameters:

Speed Dial A shortcut number that you will dial to call this party.

Destination The entry's destination, in this case a proxy.

User ID Specify the remote party's user ID (most commonly the telephone number).

4. Click 'OK' to save the settings.

- **Local line speed dial entry** This entry is intended for calling the other lines in your home network (local lines connected to your gateway).

1. In the 'Speed Dial' screen (see [Figure 7.231](#)), click 'New Entry' and select the 'Local Line' option from the drop-down menu. The screen refreshes.

Voicemail **Speed Dial Settings**

Line Settings | **Speed Dial** | Monitoring | Advanced

Speed Dial:

Destination:

Line:

Figure 7.233. Speed Dial - Local Line

2. Enter the following parameters:

Speed Dial A shortcut number that you will dial to call this party.

Destination The entry's destination, in this case a local line.

Line The drop-down menu displays your pre-defined local lines. Select a destination line.

3. Click 'OK' to save the settings.

- **Direct call speed dial entry** This entry is intended for calling any telephone number over the Internet.

1. In the 'Speed Dial' screen (see [Figure 7.231](#)), click 'New Entry' and select the 'Direct Call' option from the drop-down menu. The screen refreshes.

Figure 7.234. Speed Dial – Direct Call

2. Enter the following parameters:

Speed Dial A shortcut number that 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 (most commonly the telephone number).

IP Address or Host Name Specify the IP address or host name of the remote party's SIP client.

3. Click 'OK' to save the settings.

7.6.4. Sending a Fax

You can send and receive faxes over an OpenRG telephone line. Simply connect a fax machine to an active FXS telephone port on the gateway, and send the fax as you would from any other telephone.



Note: This feature is currently available on the Broadcom 96358 platform only.


Although you can send and receive faxes with the default settings, OpenRG enables you to configure the fax transmission method and codec. In the 'Line Settings' screen under the 'Voice' menu item, click the line's  action icon. In the 'Fax Transmission' section, configure the following options.

Figure 7.235. Line Settings – Fax Transmission


Fax Transmission Method The method used to switch to a codec that supports transmission of fax messages. Select a method from the drop-down menu:

- **None** Selecting this option deactivates this feature. The codec agreed upon by both sides of the conversation (refer to [Section 7.6.8.6](#)), which does not necessarily support fax transmission, will not change. Therefore fax transmission may fail.
- **T.38 Auto** Fax tones will be converted into T.38 packets and then transmitted. This digital mode is the most reliable fax transmission method.
- **Pass-Through Auto** A conversation will begin with the codec agreed upon by both sides. If fax tones become present, OpenRG will switch to the codec selected in the next drop-down menu, which supports fax transmission.
- **Pass-Through Force** Select this option to ensure that OpenRG begins all conversations with the fax-supporting codec selected in the next drop-down menu.

Fax Pass-Through Codec This option is only visible if a Pass-Through method is selected. Select either the u-Law or A-Law codec supporting fax transmission.

7.6.5. Customizing Your Phone Service with a Numbering Plan

A numbering plan is a set of preconfigured shortcut numbers that when dialed, perform preset actions. The caller can dynamically activate or deactivate certain actions, using the telephone keypad. For example, the caller can activate call forwarding by dialing a prefix and the number to which to forward the call.

In the 'Line Settings' screen under the 'Voice' menu item, click the line's  action icon. In the 'Numbering Plan' section, configure the following options.

Numbering Plan

Minimum Number of Digits:

Maximum Number of Digits:

Inter-Digit Timer: milliseconds

Prefixes


















Prefix Range	Maximum Number of Digits	Facility Action	Action
*72	40	Activate Call Forwarding Always	 
*73	3	Deactivate Call Forwarding Always	 
*78	40	Activate Do Not Disturb	 
*79	3	Deactivate Do Not Disturb	 
*90	40	Activate Call Forwarding on Busy	 
*91	3	Deactivate Call Forwarding on Busy	 
*92	40	Activate Call Forwarding on No Answer	 
*93	3	Deactivate Call Forwarding on No Answer	 
New Entry			

Figure 7.236. Line Settings – Numbering Plan

Minimum Number of Digits The minimum number of digits that must be dialed in order for OpenRG to send out the call.

Maximum Number of Digits The maximum number of digits that can be dialed in order for OpenRG to send out the call.

Inter-Digit Timer Specifies the duration (in milliseconds) of allowed inactivity between dialed digits. If the limit is exceeded, the dialing process times out and a warning tone is played. When you work with a proxy or gatekeeper, the number you have dialed before the dialing process has timed out is sent to the proxy/gatekeeper as the user ID to be called. This is useful for calling a remote party without creating a speed dial entry (assuming the remote party is registered with the proxy/gatekeeper).

The 'Prefixes' table displays the configured actions, containing the following parameters.

- **Prefix Range** The digits, or range of digits, constituting the prefix that activates the action. Note that a range is limited to ten digits, as only the last digit can be changed. For example, *72, 1800, 1800-1809, etc.
- **Maximum Number of Digits** The maximum number of digits that can be dialed when activating this action (including the prefix range).
- **Facility Action** The action that will be activated.

You can edit or delete the prefix entries defined in the table, using the action icons. To add a new entry, perform the following:

1. Click the 'New Entry' link. The 'Edit Prefix' screen appears.

Figure 7.237. Edit Prefix

2. Enter a prefix range.
3. Determine the minimum and maximum number of digits to be dialed when activating a rule.
4. Enter the number of digits to remove from the dialed number. This is useful for removing unwanted dialed numbers, such as the digit 9 for external access.
5. Select the facility action to perform. Among activating and deactivating the "Call Forwarding" and "Do Not Disturb" features described earlier, a new "VoIP Call" action is available. Use this action to override the generic numbering plan rules. For example, if you limit callers to dial 3-digit numbers only (by setting the generic maximum number of digits to 3), but would like to enable them to dial 1-800 numbers, enter "1800" as the prefix range, and specify the maximum number of digits that 1-800 numbers may have.
6. Click 'OK' to save the settings.

7.6.6. Using Distinctive Ring

If your gateway's Digital Signal Processing (DSP) module supports the Distinctive Ring service (available on some SIP servers), you can enrich your telephone line functionality by:

- Creating additional numbers for your line, and assigning a distinctive ring pattern to each of them. This is useful, for example, if you want to distinguish between incoming calls.
- Assigning a distinctive ring pattern to the incoming calls, by matching the caller ID to a specific ring tone. By doing so, you can recognize the caller's identity before answering the call.



Note: The availability of the service implementations depends on the SIP service provider.

To activate the Distinctive Ring service, you must first create a SIP account on a server that supports this feature. Examples of such SIP servers are Broadsoft (<http://www.broadsoft.com>)

and Broadvoice (<http://www.broadvoice.com>). After registering and configuring your SIP account, enter the SIP account settings and the proxy parameters in OpenRG's 'Line Settings' screen, as described in [Section 2.4.1.2](#).


7.6.7. Ensuring Constant Connectivity with Failover

Normally, telephones connected to the FXS ports are provided with lines by a SIP service over the Internet. If your gateway includes an *FXO* port, you can connect it to your telephone wall outlet (PSTN). Selecting the 'Enable PSTN Failover' option will switch phones to the FXO port in case Internet connection is lost, ensuring you always have telephone connectivity.



Note: This feature is currently available only on the Broadcom 96358 platform.

You can both send and receive PSTN phone calls via FXO. When a call arrives from PSTN, all telephones connected to the FXS ports will ring simultaneously, unless the 'Do Not Disturb' feature is enabled on some of them. When using an FXS line on which call waiting is enabled, you will hear a call waiting tone whenever a call arrives from PSTN.

Connect your gateway's FXO port to the telephone wall outlet. In the 'Line Settings' screen under the 'Voice' menu item, click the line's  action icon . In the 'PSTN Failover' section, configure the following option.

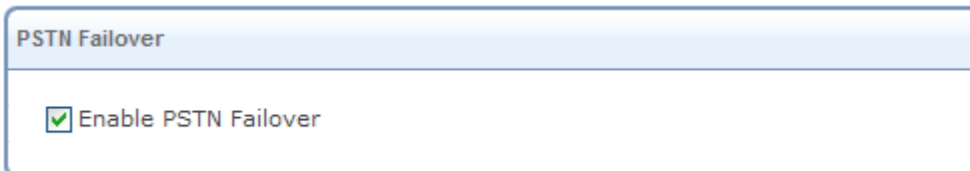



Figure 7.238. Line Settings – PSTN Failover

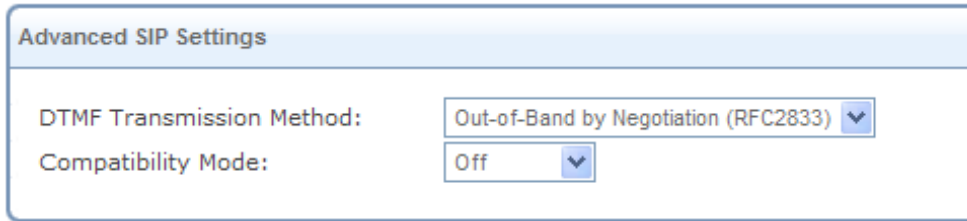
Enable PSTN Failover Select this check box to enable this feature.

7.6.8. Advanced Telephony Options

This section provides advanced options intended for a technician or a system administrator.

7.6.8.1. Determining DTMF Tones

DTMFs are the tones generated by your telephone's keypad, which are used by different telephone servers (for example, for selecting an option from a menu). If required, you can change the transmission method of these tones. In the 'Line Settings' screen under the 'Voice' menu item, click the line's  action icon . In the 'Advanced SIP Settings' section, configure the following options.



The image shows a screenshot of a web interface titled "Advanced SIP Settings". It contains two configuration items: "DTMF Transmission Method" with a dropdown menu currently showing "Out-of-Band by Negotiation (RFC2833)", and "Compatibility Mode" with a dropdown menu currently showing "Off".

Figure 7.239. Line Settings – Advanced SIP Settings

DTMF Transmission Method Select a transmission method from the drop-down menu:

- **Inband** The DTMF keypad tones are sent within the voice stream.
- **Out-of-Band Always (RFC2833)** The DTMF keypad tones are represented by the keypad number and are sent as separate packets. This is a more reliable transmission method.
- **Q.931 Keypad** The DTMF keypad tones are sent using Q.931 messages.
- **H.245 Alphanumeric** The DTMF keypad tones are sent using an H.245 alphanumeric Information Element (IE).
- **H.245 Signal** The DTMF keypad tones are sent using an H.245 signal IE.
- **Out-of-Band by Negotiation (RFC2833)** This method allows negotiation with the remote party. DTMF tones will be sent either in-band or out-of-band, depending on the remote party's preference.
- **SIP INFO** A special SIP message that includes the DTMF event description.

Compatibility Mode If you are using Broadsoft as your SIP provider, select its mode from this drop-down menu. Otherwise, leave as "Off".

7.6.8.2. Monitoring Your Lines

You can monitor the status of your telephone lines in one convenient place—the 'Monitoring' screen. Access this screen by clicking the 'Monitoring' link under the 'Voice' menu item.

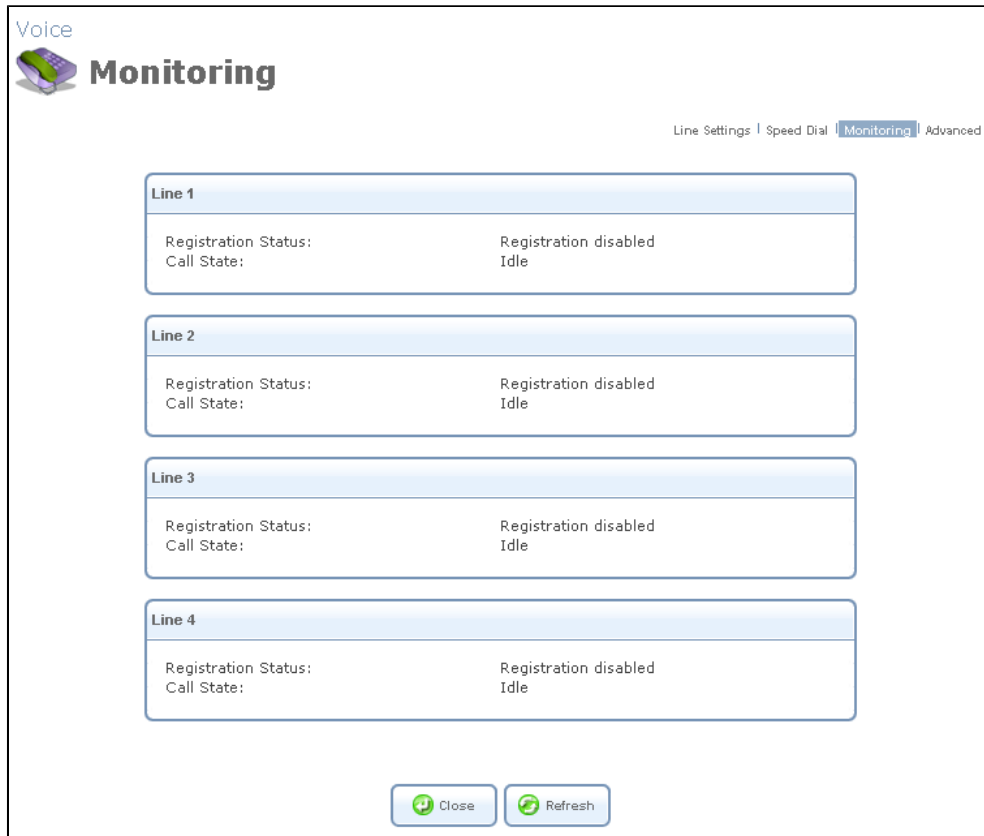


Figure 7.240. Monitoring

This screen displays all available lines and information on their statuses in real-time. These statuses include:

Registration Status Indicates whether the line is registered with a telephony service.

Call State The current state of the line—either "Idle" or "In call".

When a call is in progress, additional call statistics appear, such as the number of packets sent/received/lost, interarrival jitter, and more.

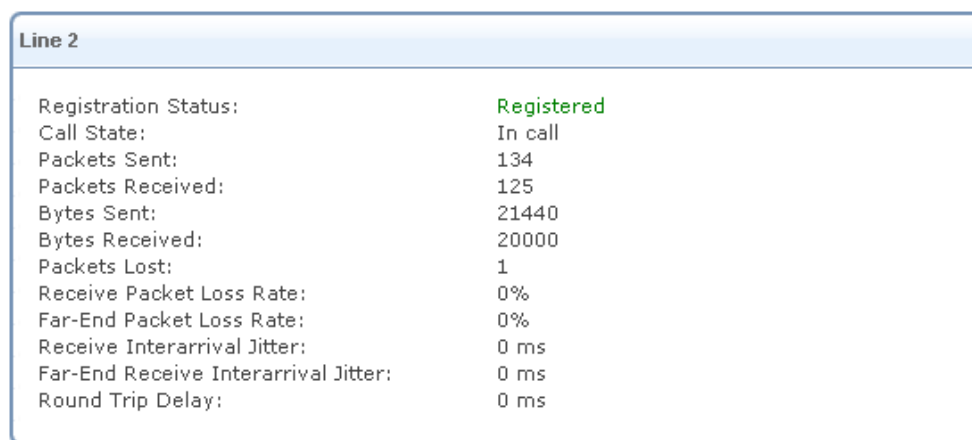


Figure 7.241. Call Statistics

7.6.8.3. Changing the Signaling Protocol

The signaling protocols available with OpenRG are Session Initiation Protocol (SIP), H.323, and Radvision's MGCP. To change your signaling protocol according to your telephone service provider, click the 'Advanced' link under the 'Voice' menu item. In the 'Signaling Protocol' section, select a protocol in the drop-down menu. A different subset of parameters will become visible with each signaling protocol choice. To apply the protocol change you must click 'Apply' (at the bottom of the 'Advanced' screen).

7.6.8.3.1. SIP

The screenshot shows a configuration window titled "Signaling Protocol". It contains the following fields and options:

- Signaling Protocol:** A dropdown menu set to "SIP".
- Local SIP Port:** A text input field containing "5060".
- Use Strict SIP Message Checking:** A checked checkbox.

Figure 7.242. SIP Signaling Protocol

Local SIP Port The port on OpenRG that listens to SIP requests from the proxy. By default, port 5060 is used for SIP signaling of phones connected to the gateway. A common problem occurs when using a SIP agent on the LAN (for example, an IP phone). A SIP agent requires port forwarding configuration (refer to [Section 7.3.3](#)), which uses the same port—5060. This multiple use of the port causes failure of either or both services. Therefore, when configuring port forwarding for a SIP agent, you must change OpenRG's SIP port value (for example, to 5062). Note that the calling party must be made aware of this value when initiating a direct call (not using a proxy).

Use Strict SIP Message Checking By default, OpenRG uses strict SIP message checking, which includes checking of tags in headers, international character conversions in URIs, and multiline formatted headers. There are cases in which this option should be disabled to ensure interoperability with certain service providers or third party user agents (SIP endpoints).

7.6.8.3.2. H.323

The screenshot shows a configuration window titled "Signaling Protocol". It contains the following fields and options:

- Signaling Protocol:** A dropdown menu set to "H.323".
- DTMF Transmission Method:** A dropdown menu set to "Out-of-Band Always (RFC2833)".
- Register with a Gatekeeper:** A checked checkbox.
- Gatekeeper Address:** Four text input fields, each containing "0".
- Gatekeeper Port:** A text input field containing "1719".
- Use Fast Start:** An unchecked checkbox.
- Local H.323 Port:** A text input field containing "1720".

Figure 7.243. H.323 Signaling Protocol

DTMF Transmission Method Select a DTMF transmission method. For more information, refer to [Section 7.6.8.1](#).

Register with a Gatekeeper Register the user with a gatekeeper, allowing other parties to call the user through the gatekeeper. When this item is checked, the following fields become visible:

Gatekeeper Address The IP address or name of the primary gatekeeper.

Gatekeeper Port The port on which the primary gatekeeper is listening for connections.

Specify Gatekeeper ID Select whether a gatekeeper ID should be used for the primary H.323 gatekeeper.

Gatekeeper ID The identifier for the primary H.323 gatekeeper.

Registration Time to Live Specify the valid duration of the H.323 gatekeeper registration in seconds.

Use Alternate Gatekeeper Select this check-box to configure an alternate gatekeeper for redundancy. When this item is checked, the following fields become visible:

Alternate Gatekeeper Address The IP address or name of the alternate gatekeeper.

Alternate Gatekeeper Port The port on which the alternate gatekeeper is listening for connections.

Use Fast Start The fast start connection method can result in quicker connection establishment, depending on the remote party's settings. Note that Microsoft NetMeeting does not support this option, so in order to interoperate with Microsoft NetMeeting, you should disable the feature.

Use H.245 Tunneling Indicates whether H.245 packets should be encapsulated within H.225 packets.

Local H.323 Port Specify the port number to use for H.323 signaling.

The Asterisk protocol has several limitations:

1. When a gatekeeper is configured, all calls are routed through it. This has the following effect on the speed-dials:
 - Destination type "Proxy" works normally – the call is sent to the gatekeeper.
 - Destination type "Local line" – the call will succeed, however it will not be a local call. It will be routed through the gatekeeper, and will go on normally since all of the local lines are registered with this gatekeeper.
 - Destination type "Direct Call" – speed dials of this type become disabled. This will be indicated in the speed dial table. For direct call speed dials, the "IP Address or Host Name" column will include, in addition to the address, the following red remark: "Disabled in H.323 gatekeeper mode".

- When a gatekeeper is not configured, the only way to make a non-local call is to define a "direct call" speed dial, stating the destination's IP address (or host name). Speed dials of type "Proxy" are meaningless.

7.6.8.3.3. MGCP

Signaling Protocol

Signaling Protocol:

Send DTMF Out-Of-Band

Media Gateway Controller Address: ...

Media Gateway Controller Port:

Media Gateway Port:

Use OpenRG's IP Address as Domain Name

Figure 7.244. MGCP Signaling Protocol

Send DTMF Out-of-Band Select this option to use out-of-band DTMF transmission method (for more information, refer to [Section 7.6.8.1](#)).

Media Gateway Controller Address The IP address of the MGC (MGCP server), in dotted number notation.

Media Gateway Controller Port The port MGC uses to listen for connections.

Media Gateway Port The port the gateway uses for MGCP connections.

Use OpenRG's IP Address as Domain Name OpenRG's IP address will be used as the domain name for identification. Unselect this check box when provided with a domain name from the MGCP service provider. The screen will refresh, adding the following field.

Media Gateway Domain Name Enter the domain name provided by the MGCP service provider.

7.6.8.4. Changing the Reserved RTP Port Range

The voice stream is transmitted in Real Time Protocol (RTP) packets, which require a range of open ports. If the default ports are required for another application, you can enter a different start port, thus creating a new range. To change the start port, configure the following option in the 'RTP' section.

RTP

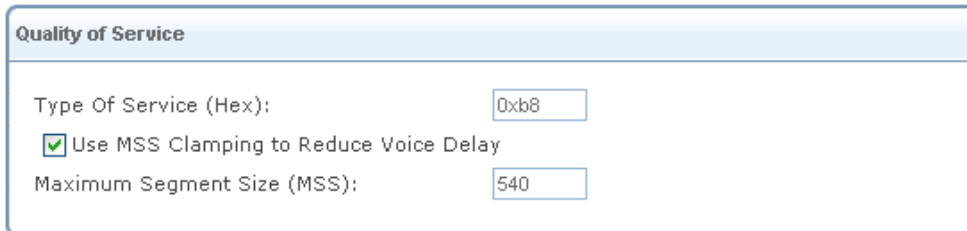
Local RTP Port Range - Contiguous Series of 16 Ports Starting From:

Figure 7.245. Advanced – RTP

Local RTP Port Range The range of ports reserved for Real Time Protocol (RTP) voice transport.

7.6.8.5. Configuring Quality of Service Parameters

Quality of Service (QoS) is aimed at improving the quality of voice traffic. To configure the QoS parameters, click the 'Advanced' link under the 'Voice' menu item. In the 'Quality of Service' section, configure the following options.



Quality of Service	
Type Of Service (Hex):	<input type="text" value="0xb8"/>
<input checked="" type="checkbox"/> Use MSS Clamping to Reduce Voice Delay	
Maximum Segment Size (MSS):	<input type="text" value="540"/>

Figure 7.246. Advanced – 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 OpenRG. 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.

Use MSS Clamping to Reduce Voice Delay When using Maximum Segment Size (MSS) Clamping, TCP streams routed via OpenRG when a voice call is active, will have a smaller segment size. This will cause RTP to receive better priority, and will help prevent high voice jitter that is caused by slow upstream transmission rate, which is common with most WAN connections (DSL, DOCSIS, etc.). When checking this option, the 'Maximum Segment Size (MSS)' field appears, where you can change the maximal segment size.

7.6.8.6. Selecting Audio Codecs

Audio 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.

To select the audio codecs, click the 'Advanced' link under the 'Voice' menu item. In the 'Codecs' section, configure the following options.

Codecs	
Supported Codecs	Packetization Time (milliseconds)
<input checked="" type="checkbox"/> G.711, 64kbps, u-Law	20 ▼
<input checked="" type="checkbox"/> G.711, 64kbps, A-Law	20 ▼
<input checked="" type="checkbox"/> G.729, 8kbps	20 ▼
<input checked="" type="checkbox"/> G.726-32, 32kbps	20 ▼
<input checked="" type="checkbox"/> G.723, 5.3/6.3kbps	30 ▼
<input checked="" type="checkbox"/> G.722, 64kbps	10 ▼

Figure 7.247. Advanced – Codecs

Supported Codecs In order to make a call, at least one codec must be enabled. Moreover, all codecs may be enabled for best performance. When you start a call to a remote party, your available codecs are compared against the remote party's, to determine which codec will be used. The priority by which the codecs are compared is according to the descending order of their list, depicted in [Figure 7.247](#). If there is no codec that both parties have made available, the call attempt will fail. Note that if more than one codec is common to both parties, you cannot force which of the common codecs that were found will be used by the remote party's client. If you do wish to force the use of a specific codec, leave only that codec checked.

Packetization Time The Packetization Time is the length of the digital voice segment that each packet holds. The default is 20 millisecond packets. Selecting 10 millisecond packets enhances the voice quality, as less information is lost due to packet loss, but doubles the load on the network traffic.

7.6.8.7. Improving Voice Reception with Echo Cancellation

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



Note: This feature is currently available on the following platforms: Intel IXP425, Broadcom BCM96358, and on platforms with the VINETIC chipset.

To improve voice reception with echo cancellation, click the 'Advanced' link under the 'Voice' item menu. In the 'Echo Cancellation' section, configure the following options.


Figure 7.248. Advanced – Echo Cancellation

Enabled Select or deselect this check box to enable or disable this feature.

Tail Length Defines the length of the elapsed time frame used for calculating the extrapolation of the echo cancellation. A long tail improves the echo cancellation, but increases the load on the Digital Signal Processor (DSP).

Non-Linear Process (NLP) Determines the type of calculation that is used for removing the echo effect. You can set this feature to Normal, High or Off. Using high NLP improves the echo cancellation, but increases the load on the DSP.

Delay Compensation A time delay compensating the echo cancellation.

 Note: On some platforms, the feature's graphic interface may differ from the one presented in the above figure.

7.6.8.8. Saving Bandwidth with Silence Suppression

Silence suppression enables optimization when no speech is detected. With this feature enabled, OpenRG is able to detect the absence of audio and conserve bandwidth by preventing the transmission of "silent packets" over the network.

To save bandwidth with silence suppression, click the 'Advanced' link under the 'Voice' item menu. In the 'Silence Suppression' section, configure the following options.

Figure 7.249. Advanced – Silence Suppression

Enable Silence Suppression Select this check box to enable this feature.

Enable Comfort Noise Select this option to play a soft "comfort" noise if the other side is performing silence suppression, in order to signal your caller that the conversation is still active.

7.6.8.9. Avoiding Voice Distortion with Jitter Buffer

A Jitter Buffer is a shared data area where voice packets can be collected, stored, and sent to the voice processor in evenly spaced intervals. Variations in packet arrival time, called "jitter", can occur because of network congestion, timing drift, or route changes. The jitter buffer intentionally delays the arriving packets so that the end user experiences a clear connection with very little voice distortion.

To avoid voice distortion with jitter buffer, click the 'Advanced' link under the 'Voice' item menu. In the 'Jitter Buffer' section, configure the following options.

Figure 7.250. Advanced – Jitter Buffer

Type The type of the jitter buffer. Can be either adaptive or fixed. In case of adaptive jitter buffer, the following fields are visible:

Adapt According to Determines whether the jitter buffer size depends on the packet length or on the estimated network jitter.

Scaling Factor The size of the jitter buffer is Scaling Factor multiplied by packet length or by estimated network jitter (depending on the value of the previous field).

Local Adaptation The jitter buffer modifies its size during silence gaps. This way the change in delay is not noticed by the listener. This parameter determines when to perform this adaptation. The options are:

Off Regard as silence packets only those packets that the far end has marked as such.

On Regard as silence packets both the packets that the far end detected, and the packets that were locally detected as speech gaps.

On with sample interpolation No silence is needed. The adaptation is performed gradually through interpolation, so the listener does not notice the jitter buffer change in size. Notice that for this mode, modem or fax transmission could be distorted. This feature should only be used in the case of voice transmission.

Initial Size The initial size of the jitter buffer (in milliseconds).

Maximum Size The maximum size of the jitter buffer (in milliseconds).

Minimum Size The minimum size of the jitter buffer (in milliseconds).

7.6.8.10. Changing the FXS Ports Settings

The 'FXS Ports' section in the 'Advanced' screen contains advanced electronic settings for the FXS (analog) ports, which should only be modified by an experienced administrator or technician.

FXS Ports	
Ringing Voltage:	70 Vpk
Ringing Frequency:	25 Hz
Ringing Waveform:	Sinusoid
On-Hook Voltage:	48 V
Off-Hook Current:	26 mA
Two-Wire Impedance:	600 ohm
Transmit Gain:	0 dB
Receive Gain:	0 dB

Figure 7.251. Advanced – FXS Ports

Ringing Voltage The ringing voltage in volts.

Ringing Frequency The ringing frequency in hertz.

Ringing Waveform The ringing waveform – sinusoid or trapezoid.

On-Hook Voltage The voltage of an idle handset in volts.

Off-Hook Current Limit The current of an active handset in milli-amperes.

Two-Wire Impedance Select the voice band impedance in ohms, synthesized by the SLIC.

Transmit Gain The transmit gain in decibels.

Receive Gain The receive gain in decibels.

7.7. IP-PBX

OpenRG's Internet Protocol – Private Branch Exchange (IP-PBX) solution provides a private telephone switching system that allows telephone extensions to connect to each other as well as to the outside world.

In most cases, a PBX is an independent piece of equipment residing in an enterprise. Your gateway, however, includes such a PBX, saving you the need to purchase and install an independent PBX. Among the invaluable features of the PBX are its ability to switch calls between users in a network form, as well as share a specific number of external phone lines saving the added cost of designating an external phone line for each user.

OpenRG's PBX manages both Plain Old Telephone Service (POTS) and Voice over IP (VoIP) devices, utilizing VoIP lines to connect them to telephony service providers (proxies). Devices within OpenRG's PBX can freely communicate with each other, thus creating a cost-effective telephony environment.

This section assumes that you have already connected your telephone equipment to the gateway, as described in [Section 2.4.1](#).



Note: In order for all of OpenRG's PBX features to function properly, a partitioned storage device, formatted with EXT2/3 (recommended) or FAT32, must be available on your gateway. Such a device can be a USB disk-on-key or hard drive. Also note that when restoring defaults, all PBX-related data will be deleted from this storage device. This data includes voice mail messages and greetings, auto-attendant greetings and music on-hold files.

Click the 'IP-PBX' menu item under the 'Services' tab. The main PBX screen appears, displaying the various links used to configure your gateway's telephone exchange system, the first being the 'Extensions' screen.

The screenshot shows the 'IP-PBX' interface with the 'Extensions' tab selected. The 'Analog Extensions' table lists extensions 100 through 107, each with a pencil icon in the 'Action' column. The 'VoIP Extensions' table has a 'New VoIP Extension' link and a plus icon in the 'Action' column. At the bottom, there are 'Close' and 'Refresh' buttons.

Figure 7.252. PBX Main Screen

Physical FXS telephone ports (if available on your gateway) are preconfigured with extension numbers by default, in the 'Analog Extensions' section of this screen. For these ports, OpenRG merely serves as an Analog Telephone Adaptor (ATA) device. In addition to these ports, you can add any number of IP telephones to your LAN (connecting them to the LAN ports, using a hub if necessary), and configure them in the 'VoIP Extensions' section.



Note: Some of the documented WBM features may appear slightly different or may not be available on certain platforms.

7.7.1. Configuring Your Analog Extensions

To view and edit an analog port's default extension, as well as other settings, click the extension number (or its action icon). The 'Edit Extension' screen appears.

Figure 7.253. Edit Extension

Configure the following parameters:

Extension Number Specify the extension number.

Last Name, First Name Specify a full name for the extension's user.

Enable Call Waiting Select this check box to enable the Call Waiting feature.

Enable 3-Way Calling Select this check box to allow all forms of three-way conversations. When this option is disabled you will not be able to place a call on hold, transfer a call or engage in a call conference.

Enable Message Waiting Indication Select this check box to play a special tone whenever you receive a voice message.

Enable Do Not Disturb Select this check box to prevent calls from reaching your extension. The caller will be forwarded to your voice mail. This feature can also be enabled or disabled by dialing *78 or *79 respectively.

Enable Call Forwarding Always Select this check box to forward incoming calls to another telephone number. The screen refreshes, displaying a field for entering the alternate number.

Enable Call Forwarding Always
Forward Calls to:

Figure 7.254. Enable Call Forwarding Always

Enable Call Forwarding on Busy Select this check box to forward incoming calls to another telephone number when the line is busy. The screen refreshes, displaying a field for entering the alternate number.

Enable Call Forwarding on Busy

Forward Calls to:

Figure 7.255. Enable Call Forwarding on Busy

Enable Call Forwarding on No Answer Select this check box to forward incoming calls to another telephone number if the call is not answered within a specific timeframe. The screen refreshes, displaying a field for entering the alternate number, and a field for determining the timeframe to ring before the call is forwarded.

Enable Call Forwarding on No Answer

Forward Calls to:

Time to Ring Before Forwarding Call: seconds

Figure 7.256. Enable Call Forwarding on No Answer

Enable Voice Mail Enable the voice mail feature. To learn how to use this feature, refer to [Section 7.7.9](#).

7.7.2. Operating Your Telephone

Following are several guidelines that will help you perform basic telephone operations.

- **Placing a Call**

1. Pick up the handset on the phone.
2. Dial the remote party's number (for an external call, begin with **9** and dial '#' to have the call sent out immediately).

- **Answering a Waiting Call**

When the Call Waiting feature is enabled, you may receive a call while engaged in another call. When such call arrives, you will hear a call waiting tone.

1. To answer a waiting call, press 'Flash'.
2. 'Flash' may be used to switch back and forth between calls.

- **Blind Transfer**

To transfer an existing call (B) to a third party (C) without consultation, perform the following:

1. Press 'Flash'. Party B will now be placed on hold, and you will hear a dial tone.
2. Dial party C's number (for an external call, begin with **9** and dial '#' to have the call sent out immediately).
3. To complete the transfer, place the phone's handset on-hook. B is now initiating a call to C.

- **Call Transfer With Consultation**

To transfer an existing call (B) to a third party (C), perform the following:

1. Press 'Flash' on the phone. Party B will now be placed on hold, and you will hear a dial tone.
2. Dial party C's number (for an external call, begin with **9** and dial '#' to have the call sent out immediately). You can engage in conversation.
3. To complete the transfer, place the phone's handset on-hook.

- **3-Way Conference**

To extend an existing call (B) into a 3-way conference by bringing in an additional party (C), perform the following:

1. Press 'Flash' on the phone. Party B will now be placed on hold and you will hear a dial tone.
2. Dial party C's number (for an external call, begin with **9** and dial '#' to have the call sent out immediately). You can engage in conversation.
3. Press 'Flash' to join both C and B to a single conference.
4. When you place the phone's handset on-hook, party B and party C will remain in conversation.

7.7.3. Connecting VoIP Telephones

Connect a VoIP telephone to an available LAN socket on your gateway. Once connected, you will have to configure the telephone and then add a VoIP extension for it in OpenRG. When done, the status of the extension should change to "Registered".

VoIP Extensions					
Extension	Last Name	First Name	Type	Status	Action
222	Smith	John	SIP	Registered	 
New VoIP Extension					

Figure 7.257. VoIP Extensions

OpenRG supports both SIP and MGCP VoIP devices. You must be aware of your type of device and configure it accordingly.

7.7.3.1. Configuring Your VoIP Telephone

Configure the telephone with the following settings. Refer to the device's documentation if necessary.

- **SIP Device** – Configure the SIP service provider with OpenRG's IP address (192.168.1.1), and the device's SIP user ID with an extension number of your choice.

- **MGCP Device** – Configure the device's media gateway controller field with OpenRG's IP address (192.168.1.1). In addition, if the device's user ID is configurable, verify that it is set to "aaln/1". Note that if the device has multiple lines, their user ID should be "aaln/1", "aaln/2", and so forth.

7.7.3.2. Adding a VoIP Extension

To add a VoIP extension for the IP telephone, click the 'New VoIP Extension' link in the 'Extensions' screen (see [Figure 7.252](#)). The 'Edit Extension' screen appears.

The screenshot shows the 'Edit Extension' web interface for an IP-PBX. The page title is 'Edit Extension' and it includes a navigation menu with options: Extensions, External Lines, Auto Attendant, Incoming Calls, Outgoing Calls, Music On-Hold, Hunt Groups, and Advanced. The main form is divided into several sections:

- Basic Information:** Fields for Extension Number (108), Last Name, and First Name. A dropdown menu for VoIP Device Type is set to SIP, with MGCP also visible in the list.
- Calling Features:** A section with four unchecked checkboxes: Enable Do Not Disturb, Enable Call Forwarding Always, Enable Call Forwarding on Busy, and Enable Call Forwarding on No Answer.
- Voice Mail:** A section with a checked checkbox for 'Enable Voice Mail' and a password field containing seven asterisks.
- Advanced SIP Settings:** A section with two unchecked checkboxes: 'Require Authentication' and 'Optimize RTP Path Using re-INVITE'.

At the bottom of the form are two buttons: 'OK' (with a green checkmark icon) and 'Cancel' (with a red X icon).

Figure 7.258. Edit Extension – SIP

Configure the following parameters, common to both device types (SIP/MGCP):

Extension Number Specify the extension number, as pre-configured in the device's settings.

Last Name, First Name Specify a full name for the extension's user.

VoIP Device Type Select your device type, SIP or MGCP. The screen refreshes accordingly, and the different parameters are described later in this section.

Enable Do Not Disturb Select this check box to prevent calls from reaching your extension. The caller will be forwarded to your voice mail. This feature can also be enabled or disabled by dialing *78 or *79 respectively.

Enable Call Forwarding Always Select this check box to forward incoming calls to another telephone number. The screen refreshes, displaying a field for entering the alternate number.

Enable Call Forwarding Always
Forward Calls to:

Figure 7.259. Enable Call Forwarding Always

Enable Call Forwarding on Busy Select this check box to forward incoming calls to another telephone number when the line is busy. The screen refreshes, displaying a field for entering the alternate number.

Enable Call Forwarding on Busy
Forward Calls to:

Figure 7.260. Enable Call Forwarding on Busy

Enable Call Forwarding on No Answer Select this check box to forward incoming calls to another telephone number if the call is not answered within a specific timeframe. The screen refreshes, displaying a field for entering the alternate number, and a field for determining the timeframe to ring before the call is forwarded.

Enable Call Forwarding on No Answer
Forward Calls to:
Time to Ring Before Forwarding Call: seconds

Figure 7.261. Enable Call Forwarding on No Answer

Enable Voice Mail Enable the voice mail feature. To learn how to use this feature, refer to [Section 7.7.9](#).

7.7.3.2.1. SIP Device Parameters

By default, the 'VoIP Device Type' drop-down menu option is set to SIP. In addition to the general parameters described above, configure the following SIP-specific parameters in the 'Advanced SIP Settings' section.

Require Authentication Select this check box to secure your telephony network. By default, SIP devices register with OpenRG as their proxy (you must configure the device's proxy field with OpenRG's IP address), by identifying themselves with extension numbers, pre-configured on both the devices and on OpenRG. When selecting the 'Require Authentication' option, OpenRG will not accept mere extension number identification, but will require additional authentication data, in the form of a user name and password. This protects your telephony network from, for example, a malicious wireless intruder disguising himself as one of your office extensions, and making free phone calls at your expense. When this option is selected, the screen refreshes, providing username and password fields.

Advanced SIP Settings

Require Authentication

Authentication User Name:

Authentication Password:

Optimize RTP Path Using re-INVITE

Figure 7.262. SIP Settings

- **Authentication User Name** The user name used for SIP device authentication. Note that this user name must first be configured on the SIP device.
- **Authentication Password** The password used for SIP device authentication. Note that this password must first be configured on the SIP device.

Optimize RTP Path Using re-INVITE Select this option if you would like OpenRG to attempt letting the telephony LAN device and the SIP proxy exchange Real Time Protocol (RTP) traffic (the audio stream) directly, which is more efficient. Note that in order for this feature to work, it must also be enabled for the VoIP line through which the call is routed (refer to **Optimize RTP Path Using re-INVITE**).



OpenRG also supports features such as Call Waiting, 3-way Calling, and Message Waiting Indication. However, on a SIP device these features are controlled from the telephone, and therefore non-configurable on OpenRG.

7.7.3.2.2. MGCP Device Parameters

Selecting the MGCP option in the 'VoIP Device Type' drop-down menu refreshes the screen.

IP-PBX Edit Extension

Extensions | External Lines | Auto Attendant | Incoming Calls | Outgoing Calls | Music On-Hold | Hunt Groups | Advanced

Extension Number:

Last Name:

First Name:

VoIP Device Type:

Calling Features

Enable Call Waiting

Enable 3-Way Calling

Enable Do Not Disturb

Enable Call Forwarding Always

Enable Call Forwarding on Busy

Enable Call Forwarding on No Answer

Voice Mail

Enable Voice Mail

Password:

MGCP Settings

Media Gateway Host Name or Address:

Figure 7.263. Edit Extension – MGCP

In addition to the general parameters described above, configure the following MGCP-specific parameters.

Enable Call Waiting Select this check box to enable the Call Waiting feature.

Enable 3-Way Calling Select this check box to allow all forms of three-way conversations. When this option is disabled you will not be able to place a call on hold, transfer a call or engage in a call conference.

Media Gateway Host Name or Address Specify the telephony device's name or IP address. If the device is connected to OpenRG's LAN, it is recommended to override its dynamic IP address assignment, by pre-configuring it with a static IP address outside OpenRG's range of dynamically-assigned IP addresses. This will avoid its address from changing (in which case you would have to re-enter the new address in this field.)

7.7.4. Opening Telephony Service Accounts

To connect your PBX to the outside world, it is necessary that you obtain a telephony service account, for example a SIP account, as you have already done in [Section 2.4.1](#). This example simulates two separate SIP accounts—one for office use and one for home use. Therefore, open an additional SIP account, either with "FWD" or with another provider of your choice.

In addition to SIP, OpenRG supports the H.323 protocol, which you can obtain as your type of telephony service.

7.7.5. Defining VoIP Lines

After creating telephony accounts and obtaining the necessary details, configure respective VoIP lines, as follows:

1. Click the 'External Lines' link in the PBX main screen (see [Figure 7.252](#)). The 'External Lines' screen appears.

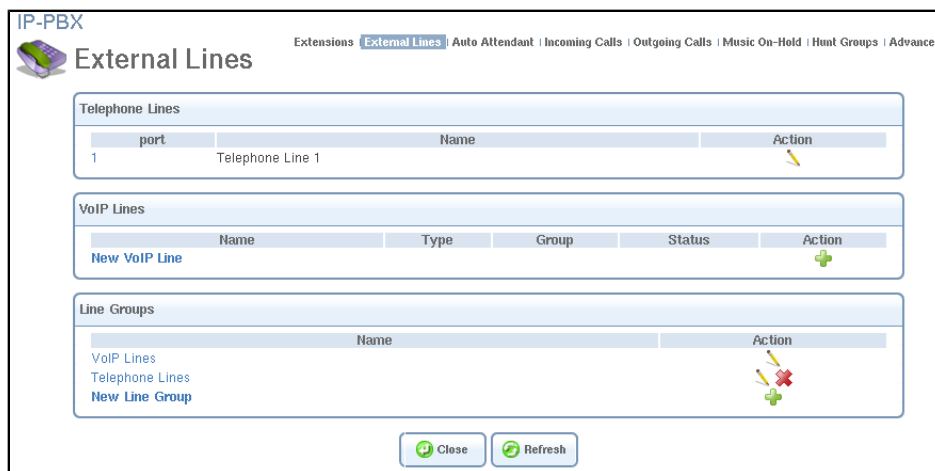


Figure 7.264. External Lines

2. Click the 'New VoIP Line' link. The 'Edit Line' screen appears.

The screenshot shows the 'Edit Line' configuration page in IP-PBX. The page is titled 'Edit Line' and has a navigation bar with links: Extensions, External Lines, Auto Attendant, Incoming Calls, Outgoing Calls, Music On-Hold, Hunt Groups, and Advanced. The main content area is divided into several sections:

- Name:** VoIP Line 0
- Type:** SIP
- Limit Number of Simultaneous Calls
- Line Group:** VoIP Lines
- SIP Account:**
 - User Name:
 - Authentication User Name:
 - Authentication Password:
- SIP Proxy:**
 - Host Name or Address:
 - Port: 5060
 - Register with Proxy
 - Register Expires: 3600 seconds
 - Use Proxy Address as User Agent Domain
- Outbound Proxy:**
 - Use Outbound Proxy
- Advanced SIP Settings:**
 - DTMF Transmission Method: Out-of-Band by Negotiation (RFC2833)
 - Compatibility Mode: Off
 - Optimize RTP Path Using re-INVITE

At the bottom of the form are 'OK' and 'Cancel' buttons.

Figure 7.265. Edit Line

3. Configure the following parameters, common to both account types (SIP/H.323). Then, configure the account-specific parameters, as described in the following respective sections.

Name The name of the VoIP line. For example, type "Office" as the name for this VoIP line, as it will simulate your office line.

Type Select the type of VoIP line according to your type of telephony service subscription—SIP or H.323. Their different settings are depicted in the following sections.

Limit Number of Simultaneous Calls You can control the maximum number of simultaneous calls performed from OpenRG through the VoIP line. This is useful, for example, if your telephony account has a call limit. When selecting this option, the screen refreshes, providing a field for entering the maximum number.

The screenshot shows a close-up of the 'Limit Number of Simultaneous Calls' configuration section. The 'Limit Number of Simultaneous Calls' checkbox is checked. The 'Maximum Number of Simultaneous Calls' field is set to 2. The 'Name' field is 'VoIP Line 0', the 'Type' is 'SIP', and the 'Line Group' is 'VoIP Lines'.

Figure 7.266. Limit Number of Simultaneous Calls

Line Group A group of VoIP lines to which this line belongs. When multiple line groups are defined, use the drop-down menu to select a group to which this VoIP line will belong. To define line groups, refer to [Section 7.7.5.3](#).

7.7.5.1. SIP Account

By default, the 'Type' drop-down menu option is set to SIP. In addition to the general parameters described above, configure the following SIP-specific parameters.

SIP Account	
User Name:	<input type="text"/>
Authentication User Name:	<input type="text"/>
Authentication Password:	<input type="text"/>

Figure 7.267. Edit Line – SIP Account

User Name Enter your SIP account ID.

Authentication User Name/Password The login name and password used for authentication with the proxy.

SIP Proxy	
Host Name or Address:	<input type="text"/>
Port:	<input type="text" value="5060"/>
<input checked="" type="checkbox"/> Register with Proxy	
Register Expires:	<input type="text" value="3600"/> seconds
<input checked="" type="checkbox"/> Use Proxy Address as User Agent Domain	

Figure 7.268. Edit Line – SIP Proxy

Host Name or Address Enter the IP address or host name that you received when registering your SIP account. Your free account's host name should be "fwd.pulver.com" (this may vary; you should check your registration e-mail).

Port The port that this proxy is listening on.

Register with Proxy Select this option to register with the proxy, allowing other parties to call OpenRG through it. When this item is checked, the following field becomes visible:

Register Expires The number of seconds between registration renewals.

Use Proxy Address as User Agent Domain Select this option to use the set proxy or its IP address as a domain name specified in outgoing SIP messages. When this option is unchecked, the 'User Agent Domain' field appears. Use this field for setting another proxy address as a user agent domain.

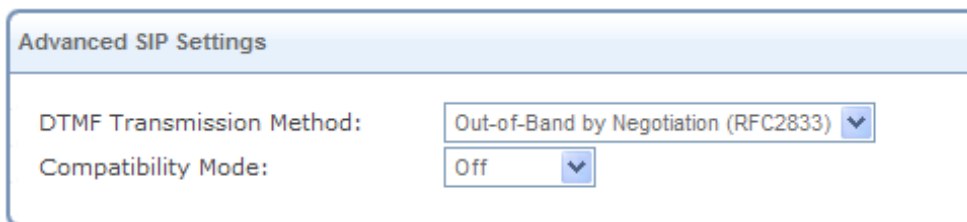
Outbound Proxy	
<input checked="" type="checkbox"/> Use Outbound Proxy	
Host Name or Address:	<input type="text" value="fwdnat.pulver.com"/>
Port:	<input type="text" value="5082"/>

Figure 7.269. Edit Line – Outbound Proxy

Use Outbound Proxy Some network service providers require the use of an outbound proxy. This is an additional proxy, through which all outgoing calls are directed. In some cases, the outbound proxy is placed alongside the firewall and is the only way to let SIP traffic pass from the internal network to the Internet. The free world-wide dialing service is an example of a service provider that requires the use of an outbound proxy. When this option is checked, the following fields become visible.

Host Name or Address Enter the outbound proxy's IP address or host name that you received when registering your SIP account in the 'Host Name or Address' field. Your free account's outbound proxy's name should be "fwdnat.pulver.com" (this may vary; you should check your registration e-mail).

Port The port on which the outbound proxy is listening. Set this field to 5082 (this may also vary).



The image shows a screenshot of a software interface titled "Advanced SIP Settings". It contains two rows of settings, each with a label and a dropdown menu. The first row is "DTMF Transmission Method:" with a dropdown menu showing "Out-of-Band by Negotiation (RFC2833)". The second row is "Compatibility Mode:" with a dropdown menu showing "Off".

Figure 7.270. Edit Line – Advanced SIP Settings

DTMF Transmission Method Select a transmission method from the drop-down menu:

- **Inband** The DTMF keypad tones are sent within the voice stream.
- **Out-of-Band Always (RFC2833)** The DTMF keypad tones are represented by the keypad number and are sent as separate packets. This is a more reliable transmission method.
- **Q.931 Keypad** The DTMF keypad tones are sent using Q.931 messages.
- **H.245 Alphanumeric** The DTMF keypad tones are sent using an H.245 alphanumeric Information Element (IE).
- **H.245 Signal** The DTMF keypad tones are sent using an H.245 signal IE.
- **Out-of-Band by Negotiation (RFC2833)** This method allows negotiation with the remote party. DTMF tones will be sent either in-band or out-of-band, depending on the remote party's preference.
- **SIP INFO** A special SIP message that includes the DTMF event description.

Compatibility Mode If you are using Broadsoft as your SIP provider, select its mode from this drop-down menu. Otherwise, leave as "Off".

Optimize RTP Path Using re-INVITE Select this option if you would like OpenRG to let the SIP proxy and a telephony LAN device exchange Real Time Protocol (RTP) traffic (the audio stream) directly, which is more efficient.

Verify that the status of the new VoIP line changes to "Registered". Your SIP-based "Office" line is now ready to be used. In the same manner as described above, define another VoIP line named "Home", which will simulate your home line. You may define VoIP lines for as many SIP proxy accounts as you have, designating each account for a different purpose.

VoIP Lines					
Name	Type	Group	Status	Action	
Office	SIP	VoIP Lines	Registered		
Home	SIP	VoIP Lines	Registered		
New VoIP Line					

Figure 7.271. VoIP Lines



Note: The 'Telephone Lines' section is currently available on the Broadcom BCM96358 platform only. This section displays an analog (PSTN) line connected via the gateway's Foreign Exchange Office (FXO) port. You can both make and receive phone calls through this line. This is especially useful in case of Internet connectivity problem, when VoIP lines are unavailable.

7.7.5.2. H.323 Account

If you have obtained an H.323 telephony account, select the "H.323" option in the 'Type' drop-down menu of the 'Edit Line' screen (see [Figure 7.265](#)). The screen refreshes.

The screenshot shows the 'Edit Line' configuration screen for an H.323 account. The 'Name' field is set to 'VoIP Line 0'. The 'Type' dropdown menu is set to 'H.323'. The 'Limit Number of Simultaneous Calls' checkbox is checked, and the 'Maximum Number of Simultaneous Calls' is set to 2. The 'Line Group' dropdown menu is set to 'VoIP Lines'. Below these fields is the 'H.323 Account' section, which includes an 'E.164 Alias (Phone Number)' field. At the bottom of the screen are 'OK' and 'Cancel' buttons.

Figure 7.272. Edit Line – H.323

In addition to the general parameters you have already configured above, configure the following H.323-specific parameter.

E.164 Alias (Phone Number) Enter your H.323 account phone number.

7.7.5.3. Grouping Your VoIP Lines

By default, the PBX is pre-configured with one editable, non-removable VoIP line group, to which all created lines will automatically be added. If you would like to distribute your VoIP lines between several groups, simply define additional ones. Click the 'New Line Group'. The 'Edit Line Group' screen appears.

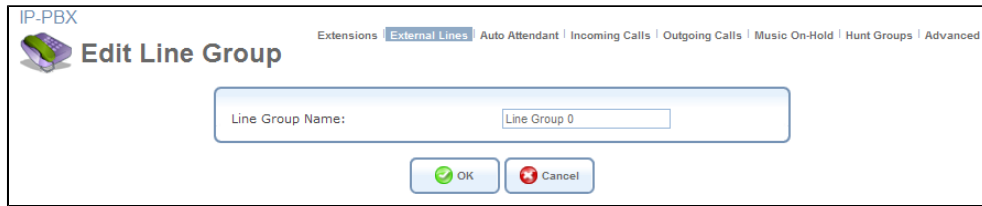


Figure 7.273. Edit Line Group

Enter a name for the new group, and click 'OK' to save your settings. New and existing VoIP lines can now be assigned to each line group, by selecting the group in the 'Line Group' drop-down menu of the 'Edit Line' screen (see [Figure 7.265](#)).

7.7.6. Creating Auto Attendants

OpenRG's PBX includes an auto attendant feature, allowing you to intelligently handle incoming calls, by providing callers the ability to route their calls to relevant parties using the telephone's keypad. You can customize a menu of multiple auto attendants according to your office structure or any other preference. By default, the PBX is pre-configured with one editable, non-removable auto attendant named 'Main Auto Attendant'.

This section depicts an example where the default 'Main' auto attendant is used for an office. Optional auto attendants describe the office location, and inform of the office working hours (an off-hours message). You will first create the optional auto attendants, and then edit the 'Main' attendant with reference to an optional attendant.

1. Create an "Office Directions" auto attendant:
 - a. Click the 'Auto Attendant' link in the PBX main screen (see [Figure 7.252](#)). The following screen appears.

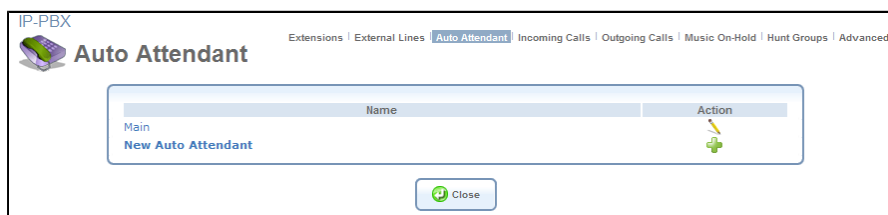


Figure 7.274. Auto Attendant

- b. Click the 'New Auto Attendant' link. The 'Edit Auto Attendant' screen appears.

IP-PBX
 Extensions | External Lines | **Auto Attendant** | Incoming Calls | Outgoing Calls | Music On-Hold | Hunt Groups | Advanced

Edit Auto Attendant

Name:

Greeting:

Status:

Key	Action
0	None
1	None
2	None
3	None
4	None
5	None
6	None
7	None
8	None
9	None
#	None
*	None
No Selection	Replay Greeting

Settings

Time to Wait for a Selection: seconds

Figure 7.275. Edit Auto Attendant

- c. Configure the following parameters:

Name The name of the auto attendant. Type "Office Directions" as the name for this auto attendant.

Greeting The greeting callers will hear when dialing to OpenRG. In order to use OpenRG's default greeting or record your own, you must first connect an external storage device to your gateway. To record your preferred message, click the 'Edit Greeting' button. The 'Auto Attendant Greeting' screen appears.

IP-PBX
 Extensions | External Lines | **Auto Attendant** | Incoming Calls | Outgoing Calls | Music On-Hold | Hunt Groups | Advanced

Auto Attendant Greeting

Record Instructions

Step 1 Select the extension you are using:

Step 2 Pick up the extension handset and dial *51. At the tone, record your greeting.

Step 3 To playback the greeting, dial *52.

Step 4 If you wish to re-record your greeting, repeat steps 1 through 3.

Figure 7.276. Auto Attendant Greeting

Follow the instructions in this screen to record the message directing to your office location. Note that in **Step 1** you must select the extension through which you are recording the message. **Important:** When done, press the 'Close' button.

Menu Options Use this section to configure an action for each keypad button press. This includes the pound and star keys, as well as an action for when no button is pressed. Note that at any time, the caller can dial and be routed to any extension number. The actions that can be defined for every keypad button are:

- **None** No action will be performed.

- **Transfer to Extension** Transfer the call to a specific extension. When defining this action, the screen refreshes, displaying a drop-down menu with all currently available extensions.

Menu Options		
Key	Action	
0	Transfer to Extension	100
1	None	100
2	None	101
3	None	102
		103

Figure 7.277. Menu Options – Transfer to Extension

- **Play Another Auto Attendant** Transfer to a different auto attendant. This action will only be available when more than one attendant exists. When defining this action, the screen refreshes, displaying a drop-down menu with all other available auto attendants. For example:

Menu Options		
Key	Action	
0	Play Another Auto Attendant	Support Auto Attendant
1	None	Support Auto Attendant
2	None	Sales Auto Attendant

Figure 7.278. Menu Options – Play Auto Attendant

- **Replay Greeting** The greeting message will be replayed.

In the 'No Selection' drop-down menu, select "Play Another Auto Attendant". If the caller does select an action, at the end of the attendant's playback the only other auto attendant available at this time ('Main') will be played. Click 'OK' to save the settings.

Time to Wait for a Selection Specify the timeframe that the system will wait for the caller to select an action. After this timeframe, the action defined in the 'No Selection' menu option will occur.

2. Create a "Working Hours" auto attendant:

Follow the above procedure to create yet another auto attendant, informing the caller of your office working hours. This auto attendant will be played in the timeframe which you will later on define as non-business hours.

Important: Skip **Step 6** – the auto attendant will be replayed until the call is terminated.

3. Edit the 'Main' auto attendant as your main office attendant:

- Click the 'Main' auto attendant link. The 'Edit Auto Attendant' screen appears (see [Figure 7.275](#)).
- Type "Office" as the name for this auto attendant.

- c. Select 'Play Another Auto Attendant' for the **5** key (for example). The screen refreshes, displaying an additional combo box.

5	Play Another Auto Attendant	Office Directions
6	None	Office Directions Working Hours
7	None	

Figure 7.279. Menu Options – Play Auto Attendant

- d. Select the 'Office Directions' auto attendant.
- e. Press the 'Edit Greeting' button to record your main office message. This message should include the following directives:
- Inform the caller that he/she may dial an extension number at any time to be transferred to that extension.
 - Inform the caller that he/she may press the **5** key to listen to directions on how to get to the office.
- f. Click 'OK' to save the settings.

Your auto attendants are now ready to be used.

Name	Action
Office	
Office Directions	 
Working Hours	 
New Auto Attendant	

Figure 7.280. Newly Created Auto Attendants

7.7.7. Handling Incoming Calls

OpenRG can receive calls from the telephony proxies associated with its VoIP lines. Such calls will automatically be routed to the PBX through their respective lines. The PBX features an incoming call handling mechanism, enabling you to control your incoming calls per VoIP line, in both day and night modes. This is useful for handling business hours and off-hours calls differently. Since this feature is configured per VoIP line, you must first define one (refer to [Section 7.7.5](#)) in order to set its incoming call policy.

After you have created auto attendants, click the 'Incoming Calls' link in the PBX main screen (see [Figure 7.252](#)).

External Line	Day Mode	Night Mode	Action
Analog Telephone Line	Play Auto Attendant "Main"	Play Auto Attendant "Main"	
Office	Play Auto Attendant "Main"	Play Auto Attendant "Main"	
Home	Play Auto Attendant "Main"	Play Auto Attendant "Main"	

Day Mode Schedule

Days of Week: Monday - Friday

Hours Range: 08 :00 - 17 :00

OK Apply Cancel

Figure 7.281. Incoming Calls

As you can learn from this screen, by default VoIP accounts are configured to play the 'Main Auto Attendant', both day and night, Monday through Friday. Configuring this feature consists of two stages—defining incoming call handling for day and night modes, and scheduling the day mode (which automatically sets the night mode to the rest of the week cycle).

1. Define incoming call handling for day and night modes:
 - a. In the 'Incoming Call Handling' section, click the 'Office' VoIP line (or its action icon). The 'Edit Incoming Call Handling' screen appears.

External Line: Office

Day Mode

When a Call Comes in: Play Auto Attendant Office

Night Mode

When a Call Comes in: Play Auto Attendant Working Hours

OK Cancel

Figure 7.282. Edit Incoming Call Handling

- b. Configure the actions that will occur when a call arrives. The following instructions apply to both day and night modes, which are set in the same manner.

Play Auto Attendant When this option is selected in the first drop-down menu, the second one displays a list of your available auto attendants.

Day Mode

When a Call Comes in: Play Auto Attendant Office

- Office
- Office Directions
- Working Hours

Figure 7.283. Play Auto Attendant

Select to play the "Office" auto attendant in day mode, and the "Working Hours" auto attendant in night mode. Click 'OK' to save the settings.

Transfer to Extension When this option is selected, the screen refreshes. The second drop-down menu displays a list of your available extensions, to which you can choose to route the call. Additionally, a check box appears.

Play Auto-Attendant If Busy or Unanswered Select this option if you would like to play an auto attendant in case the extension is busy or if the call is unanswered. The screen refreshes again, enabling you to select the auto attendant to be played.

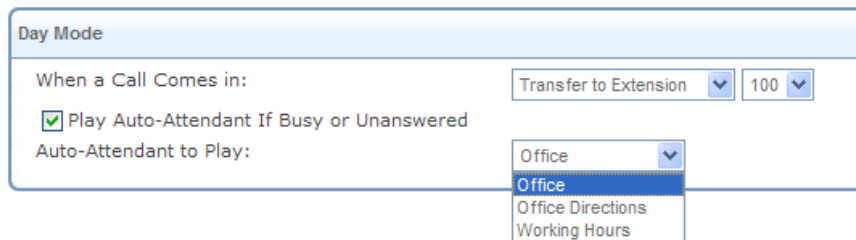



Figure 7.284. Transfer to Extension

- c. Back in the 'Incoming Calls' screen, click the 'Home' VoIP line (or its  action icon), and configure to transfer incoming calls to extension **100** in both day and night modes. Click 'OK' to save the settings.

2. Scheduling the day mode:

The 'Day Mode Schedule' section of the 'Incoming Calls' screen (see [Figure 7.281](#)) enables you to divide a week cycle into two time segments, during which incoming calls can be handled differently. Only one segment must be configured (the "day" mode), as the rest of the time in the week cycle will be referred to as the second segment (the "night" mode). Determine the day mode time segment:

Days of Week Select from which day through which day will be included in this mode.

Hours Range Enter from what hour to what hour of every day will be included in this mode.

Your incoming call handling plan should be as follows:




Incoming Call Handling			
External Line	Day Mode	Night Mode	Action
Analog Telephone Line	Play Auto Attendant "Main"	Play Auto Attendant "Main"	
Office	Play Auto Attendant "Office"	Play Auto Attendant "Working Hours"	
Home	Transfer to Extension 100	Transfer to Extension 100	

Figure 7.285. Incoming Call Handling

- When a call arrives through the office VoIP line in business hours, the main "Office" attendant will be played, prompting the user to dial any extension number or to press **5** for instructions on how to get to the office. To experience this, you can use the home extension to dial "9" and then your office VoIP line number.

- When a call arrives through the office VoIP line in off-hours, the "Working Hours" attendant will be played, informing the caller of your business hours.
- When a call arrives through the home VoIP line, it will automatically be transferred to extension **100**. To experience this, you can use the office extension to dial "9" and then your home VoIP line number.

7.7.8. Handling Outgoing Calls

OpenRG's PBX provides a sophisticated mechanism for handling outgoing calls, by utilizing a *Dial Plan*. A dial plan is a set of rules you can determine in order to route outgoing calls through specific VoIP lines. Each dial plan rule is referred to as a "dial plan entry", which you can add, edit or remove.

The dial plan mechanism enables you to manipulate the number dialed by the caller, by adding or omitting digits. This can be used for various purposes, such as reaching an external line, replacing telephony proxies' dialing codes, and even defining speed dial shortcuts. To define a new dial plan entry, click the 'New Dial Plan Entry' link. The 'Edit Dial Plan Entry' screen appears (see [Figure 7.287](#)).

Click the 'Outgoing Calls' link in the PBX main screen (see [Figure 7.252](#)). The following screen appears.

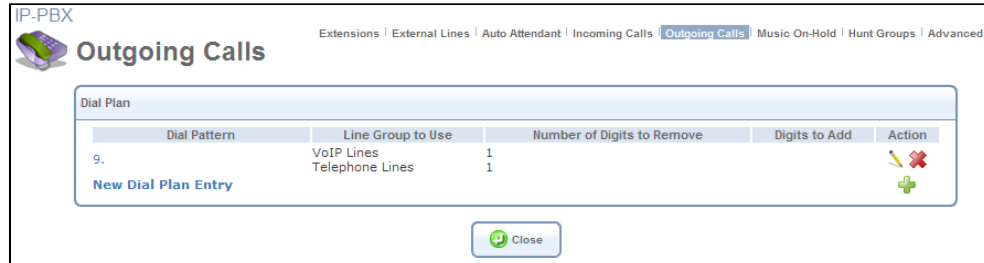


Figure 7.286. Outgoing Calls

As you can learn from this screen, the dial plan contains a default entry, which provides the option to press "9" for an external line. To view the entry's settings, click its action icon. The 'Edit Dial Plan Entry' screen appears.

Figure 7.287. Edit Dial Plan Entry

This screen is divided into two main sections, 'Dial Pattern' and 'Main Route'. When a caller from any extension dials a number that matches the dial pattern, the PBX will attempt to route the call according to the defined route conditions. According to the default dial plan entry above, when a caller dials "9", the call will be routed to an external line through the default 'VoIP Lines' group, and the dialed "9" digit will be omitted. The caller will then be able to place an external call by simply dialing the desired telephone number.

As you have obtained an FWD SIP account in previous examples, you may want to use the dial plan to overcome an FWD limitation. As a rule, FWD requires dialing " * " (asterisk) as a prefix to 1-800 numbers. Failure to do so will result in an FWD voice message explaining this requirement. To override this limitation, add the following entry to the dial plan.

1. In the 'Outgoing Calls' screen (see [Figure 7.286](#)) click the 'New Dial Plan Entry' link. The 'Edit Dial Plan Entry' screen appears.
2. Enter "91800XXXXXXXX" as the dial pattern. This pattern represents every possible 1-800 number, dialed after "9" (for an external call), and complies with the specified pattern syntax.

Figure 7.288. Dial Pattern

3. In the 'Main Route' section, configure the following:

Line Group to Use Select the line group through which you would like to route the call. In this example, select "VoIP Lines".

Remove Digits From the Beginning of the Dialed Number Select this option to ignore one or more of the digits specified in the dial pattern before dialing the telephone number. When this option is selected, the screen refreshes, adding the following field:

Number of Digits to Remove Verify that the value of this field is 1.

The screenshot shows a configuration window titled 'Main Route'. It contains the following elements:

- 'Line Group to Use:' dropdown menu set to 'VoIP Lines'.
- Checked checkbox: 'Remove Digits From the Beginning of the Dialed Number'.
- Text input field: 'Number of Digits to Remove:' with the value '1'.
- Unchecked checkbox: 'Add Digits to the Beginning of the Dialed Number'.
- Unchecked checkbox: 'If All Lines in Group Are in Use or Unavailable, Use Alternate Route 1'.

Figure 7.289. Number of Digits to Remove

Add Digits to the Beginning of the Dialed Number Select this option to add digits before dialing the telephone number. When this option is selected, the screen refreshes, adding the following field:

Digits to Add Enter an " * " (asterisk) as the digit to be added.

The screenshot shows the same 'Main Route' configuration window. In addition to the options in Figure 7.289, it now includes:

- Checked checkbox: 'Add Digits to the Beginning of the Dialed Number'.
- Text input field: 'Digits to Add:' with the value '*'.

Figure 7.290. Digits to Add

If All Lines in Group Are in Use or Unavailable, Use Alternate Route 1 Select this option to provide an alternate route for the dialed call, in case all lines in the specified line group are in use (this step is not mandatory for the current example). When this option is selected, the screen refreshes, adding the following section:

Alternate Route 1 This section is identical to the 'Main Route' section above, enabling you to select a different set of parameters, thus expanding a call's routing options. You can further select the alternate route option, to create Alternate Route 2, and so on.



Note: On the Broadcom BCM96358 platform, this screen section is enabled by default, and the 'Telephone Lines' group (analog lines) is selected. This is useful if the Internet connection is down, in which case all the VoIP lines are unavailable. In such a case, a dialed external call will be routed by default to the analog (PSTN) line via an FXO port.

Main Route

Line Group to Use: VoIP Lines ▼

Remove Digits From the Beginning of the Dialed Number

Add Digits to the Beginning of the Dialed Number

If All Lines in Group Are in Use or Unavailable, Use Alternate Route 1

Alternate Route 1

Line Group to Use: Telephone Lines ▼

Remove Digits From the Beginning of the Dialed Number

Number of Digits to Remove: 1

Add Digits to the Beginning of the Dialed Number

If All Lines in Group Are in Use or Unavailable, Use Alternate Route 2

Figure 7.291. Alternate Route 1

4. Click 'OK' to save the settings.

The dial plan entry is added to the 'Outgoing Calls' screen, and is applied on all VoIP lines in the line group selected (in this case, the default 'VoIP Lines' group).

Dial Plan				
Dial Pattern	Line Group to Use	Number of Digits to Remove	Digits to Add	Action
91800XXXXXX	VoIP Lines	1	*	
9.	VoIP Lines	1		
New Dial Plan Entry				

Figure 7.292. Dial Plan

Calls dialed from OpenRG to 1-800 numbers will now be automatically converted into the format required by FWD, concealing its limitation and simplifying telephony operability.

7.7.9. Using the Voice Mail

The voice mail feature is an interactive attendant application, enabling you to listen to your messages and configure various voice mail options.

7.7.9.1. Accessing the Voice Mail

Every extension features its own voice mailbox. The PBX will indicate that you have messages by commencing the dial tone with a stutter when you pick up the handset. To access an extension's voice mail application, perform the following:

1. Pick up the handset, and dial ***1234**. An attendant will ask for a password.
2. Dial your password. The default password is **0000#**.

As soon as you enter the voice mail application, the attendant will inform you whether you have any messages, and prompt you to press different keys for various mail options. Navigate through these options to perform all voice mail operations.

7.7.9.2. Voice Mail Operations

Following are the available voice mail operations and their corresponding keys. Sub-options are marked with bullets.

1 – New/old messages

- **4** – Play previous message
- **5** – Repeat current message
- **6** – Play next message
- **7** – Delete current message
- **8** – Forward message to another mailbox
- **9** – Save message in a folder
- ***** – Help; during message playback: rewind
- **#** – Exit; during message playback: fast-forward

2 – Change folders

3 – Advanced options

- **1** – Send reply
- **2** – Call back
- **3** – Envelope
- **4** – Outgoing call
- **5** – Leave message
- ***** – Return to main menu

0 – Mailbox options

- **1** – Record your "unavailable" message
- **2** – Record your "busy" message
- **3** – Record your name
- **4** – Change your password
- ***** – Return to the main menu

* – Help

– Exit

7.7.10. Adding On-Hold Music Files

While callers are placed on hold, they will hear background music playing. In order to use OpenRG's default music or upload your own music files, you must first connect an external storage device to your board. To upload an on-hold music file, perform the following:

1. Click the 'Music On-Hold' link in the PBX main screen (see [Figure 7.252](#)). The following screen appears.

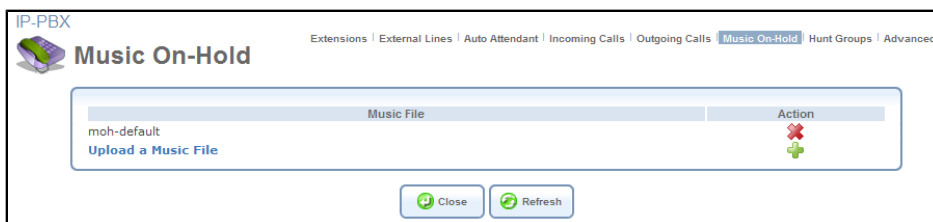


Figure 7.293. Music On-Hold

2. Click the 'Upload a Music File' link. The following screen appears.

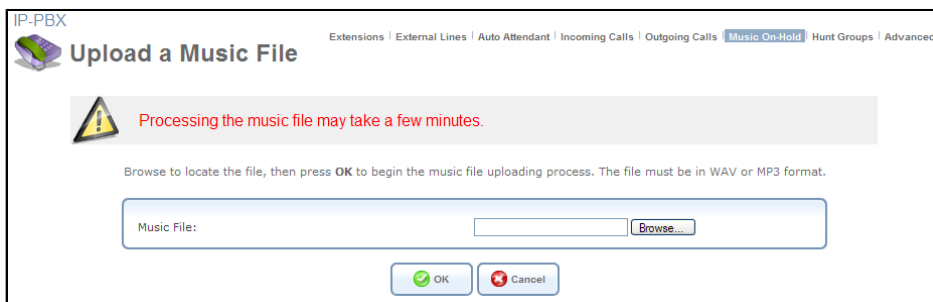


Figure 7.294. Browse For a Music File

3. Click the 'Browse' button to open a browsing window on your computer and select the WAV or MP3 format file to upload.
4. Click 'OK' to begin the upload. Note that this may take several minutes, depending on the size of your file(s).

7.7.11. Automating Call Distribution with Hunt Groups

Your PBX features *Hunt Groups* for automating distribution of incoming calls to two or more extensions. This allows you to set up groups of operators in order to handle different types of inquiries. For example, you may distribute calls to a **sales hunt group** and a **support hunt group**. Moreover, you can control the distribution of calls within a hunt group in a particular order if an extension is busy or unavailable.

Since hunt groups are groups of extensions, once defined they become optional call recipients. The option "Transfer to Hunt Group" will be added as a menu option in the 'Edit Auto Attendant' screen (see [Figure 7.295](#)) and in the 'Edit Incoming Call Handling' screen (see [Figure 7.296](#)).

Menu Options

Key	Action
0	None
1	None
2	Transfer to Extension Play Another Auto Attendant Replay Greeting
3	Transfer to Hunt Group

Figure 7.295. Edit Auto Attendant

Figure 7.296. Edit Incoming Call Handling

To define a hunt group, click the 'Hunt Groups' link in the PBX main screen (see [Figure 7.252](#)). The following screen appears.

Figure 7.297. Hunt Groups

Click the 'New Hunt Group' link. The following screen appears.



Figure 7.298. Edit Hunt Group

Name The name of the hunt group.

Ring Mode Select whether to ring all extensions at once when a call arrives, where the first operator to answer will accept the call, or to ring one extension at a time in an orderly fashion. Selecting the second choice will refresh the screen.

Figure 7.299. Hunt Group Ring Mode

Time to Ring Each Extension Enter the timeframe in which the call will ring on each extension before being routed to the next.

Extensions to Ring Select the extensions that will participate in this hunt group. The drop-down menu will display all of your available extensions. Note that this step is mandatory, otherwise the hunt group is empty. If you had chosen to ring one extension at a time as your ring mode, by default the ring will be routed between the extensions in their order of appearance in this table. When adding multiple extensions, the  action icon and  action icon appear, allowing you to easily change the order of the extensions. If you had chosen simultaneous rings, the order of extensions is not relevant.












Extensions to Ring	
Extension	Action
100	 
101	  
102	  
103	 
<input type="text" value="Add Extension..."/> 	

Figure 7.300. Extensions to Ring

Ring Order The ringing cycle order, used to determine the cycle's starting point, or which extension will ring first. This field appears only if you had chosen to ring one extension at a time as your ring mode. In this mode, the extensions will ring one after the other in a cyclic manner, according to their order in the 'Extensions to Ring' table. Select the ring order algorithm to be used:

- Round Robin – The extensions take orderly turns at being the first extension to ring. The order of the turns is the same order defined for the ringing cycle.
- Least Recent – The first extension to ring is the one that has been idle for the longest time.
- Random – The first extension to ring will be chosen randomly.

The screenshot shows a configuration window titled 'Advanced'. It contains the following settings:

- Ring Order:** A dropdown menu with 'Round Robin' selected and expanded to show options: 'Round Robin', 'Least Recent', and 'Random'.
- Make Estimated Hold Time Announcements:** A checkbox that is currently unchecked.
- Estimated Hold Time Announcement Interval:** A text input field containing '00' followed by 'seconds'.
- Make Wait Announcements:** A dropdown menu with 'Periodically' selected.
- Wait Announcement Interval:** A text input field containing '60' followed by 'seconds'.

Figure 7.301. Ring Order

Make Estimated Hold Time Announcements Hold time announcements include messages asking the callers to hold, as well as informing the callers of their number in the queue of calls. These messages are played in addition to the on-hold music played in the background. Select whether to play these messages periodically, once, or not at all.

Estimated Hold Time Announcement Interval Enter the number of seconds before the hold time announcements will be repeated. Note that if you had chosen to play the announcements once or not at all, this field will not be visible.

Make Wait Announcements Wait announcements are messages asking the caller to hold. Select whether to play this message periodically or not at all.

Wait Announcement Interval Enter the number of seconds before the wait announcement will be repeated. Note that if you had chosen not to play the announcement at all, this field will not be visible.



Note: When an external caller is transferred to a relevant hunt group without dialing a specific hunt group's extension, the calling features of the reached extension (such as call waiting, call forwarding, etc.) are not activated. This is done in order to automatically transfer the call to the next hunt group's extension, if the previously called extension does not answer. In contrast, when a specific hunt group's extension is requested, its calling features are activated, and the call is not transferred further within the hunt group when the dialed extension does not answer.

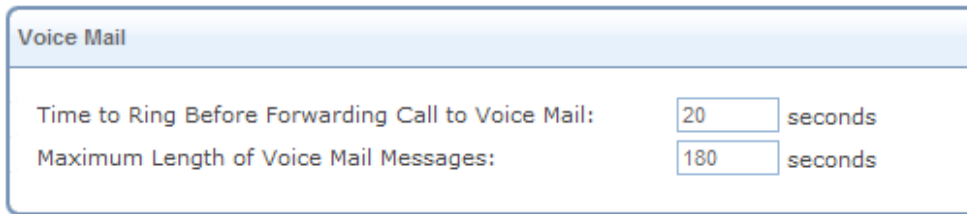
7.7.12. Advanced Telephony Options

The 'Advanced' screen enables configuration of advanced settings. Some of these settings are platform-specific, and therefore may not be available with your gateway's software.



Note: OpenRG's PBX utilizes the **G.711 u-LAW** codec for relaying voice data. This codec cannot be changed or disabled from the WBM.

7.7.12.1. Configuring Voice Mail Attributes



Time to Ring Before Forwarding Call to Voice Mail:	<input type="text" value="20"/>	seconds
Maximum Length of Voice Mail Messages:	<input type="text" value="180"/>	seconds

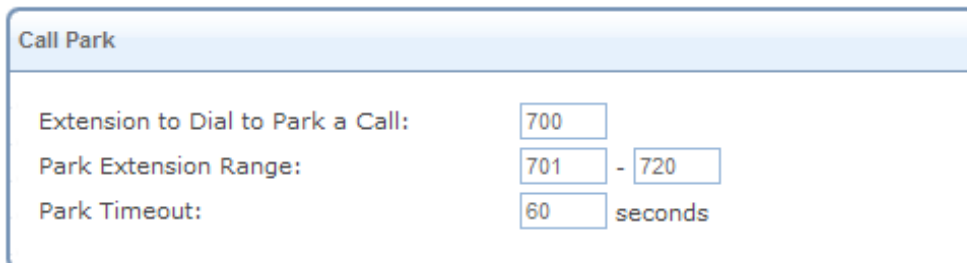
Figure 7.302. Advanced – Voice Mail

Time to Ring Before Forwarding Call to Voice Mail The timeframe in seconds until the call will be forwarded to the voice mail.

Maximum Length of Voice Mail Messages The maximal length in seconds of a message that can be recorded.

7.7.12.2. Switching Extensions with Call Park

Call parking allows you to put a call on hold at one extension and continue the conversation from any other extension on your PBX.



Extension to Dial to Park a Call:	<input type="text" value="700"/>
Park Extension Range:	<input type="text" value="701"/> - <input type="text" value="720"/>
Park Timeout:	<input type="text" value="60"/> seconds

Figure 7.303. Advanced – Call Park

Extension to Dial to Park a Call The extension number that must be dialed in order to park the call. When dialing this number, a voice recording will say a parking extension number that you must dial from any other extension on the PBX in order to resume the parked call.

Park Extension Range The range of parking extension numbers that are available for the system to provide a caller parking a call.

Park Timeout The duration (in seconds) for which the call is parked. During this timeframe, the call can be picked up from any extension on the PBX by dialing the parking extension number provided. After this timeframe, the extension from which the call was parked will ring to resume the call.

7.7.12.3. Setting the SIP Port

Figure 7.304. Advanced – SIP

Local SIP Port The port on OpenRG that listens to SIP requests from the proxy. By default, port 5060 is used for SIP signaling of phones connected to the gateway. A common problem occurs when using a SIP agent on the LAN (for example, an IP phone). A SIP agent requires port forwarding configuration (refer to [Section 7.3.3](#)), which uses the same port—5060. This multiple use of the port causes failure of either or both services. Therefore, when configuring port forwarding for a SIP agent, you must change OpenRG's SIP port value (for example, to 5062). Note that the calling party must be made aware of this value when initiating a direct call (not using a proxy).

7.7.12.4. Configuring H.323 Parameters

Figure 7.305. Advanced – H.323

Register with a Gatekeeper Register the user with a gatekeeper, allowing other parties to call the user through the gatekeeper. When this item is checked, the following fields become visible:

Gatekeeper Address The IP address or name of the primary gatekeeper.

Gatekeeper Port The port on which the primary gatekeeper is listening for connections.

Specify Gatekeeper ID Select whether a gatekeeper ID should be used for the primary H.323 gatekeeper.

Gatekeeper ID The identifier for the primary H.323 gatekeeper.

Registration Time to Live Specify the valid duration of the H.323 gatekeeper registration in seconds.

Use Alternate Gatekeeper Select this check-box to configure an alternate gatekeeper for redundancy. When this item is checked, the following fields become visible:

Alternate Gatekeeper Address The IP address or name of the alternate gatekeeper.

Alternate Gatekeeper Port The port on which the alternate gatekeeper is listening for connections.

Use Fast Start The fast start connection method can result in quicker connection establishment, depending on the remote party's settings. Note that Microsoft NetMeeting does not support this option, so in order to interoperate with Microsoft NetMeeting, you should disable the feature.

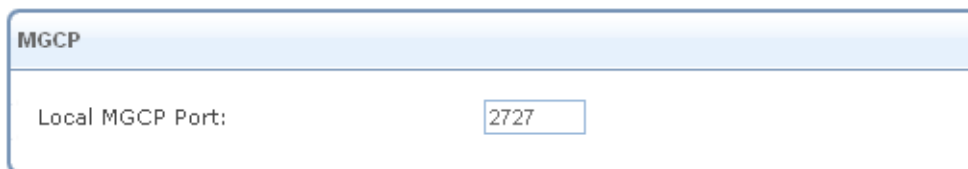
Use H.245 Tunneling Indicates whether H.245 packets should be encapsulated within H.225 packets.

Local H.323 Port Specify the port number to use for H.323 signaling.

DTMF Transmission Method DTMFs are the tones generated by your telephone's keypad.

- **Inband** The DTMF keypad tones are sent within the voice stream.
- **Out-of-Band Always (RFC2833)** The DTMF keypad tones are represented by the keypad number and are sent as separate packets. This is a more reliable transmission method.
- **Q.931 Keypad** The DTMF keypad tones are sent using Q.931 messages.
- **H.245 Alphanumeric** The DTMF keypad tones are sent using an H.245 alphanumeric Information Element (IE).
- **H.245 Signal** The DTMF keypad tones are sent using an H.245 signal IE.

7.7.12.5. Setting the MGCP Port



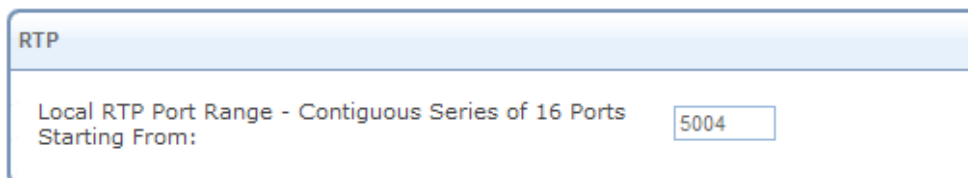
The screenshot shows a configuration window titled "MGCP". Inside the window, there is a label "Local MGCP Port:" followed by a text input field containing the number "2727".

Figure 7.306. Advanced – MGCP

Local MGCP Port The port OpenRG uses for MGCP connections.

7.7.12.6. Changing the Reserved RTP Port Range

The voice stream is transmitted in Real Time Protocol (RTP) packets, which require a range of open ports. If the default ports are required for another application, you can enter a different start port, thus creating a new range. To change the start port, configure the following option in the 'RTP' section.



The screenshot shows a configuration window titled "RTP". Inside the window, there is a label "Local RTP Port Range - Contiguous Series of 16 Ports Starting From:" followed by a text input field containing the number "5004".

Figure 7.307. Advanced – RTP

Local RTP Port Range The range of ports reserved for Real Time Protocol (RTP) voice transport.

7.7.12.7. Configuring Quality of Service Parameters

Quality of Service (QoS) is aimed at improving the quality of voice traffic. To configure the QoS parameters, click the 'Advanced' link under the 'Voice' menu item. In the 'Quality of Service' section, configure the following options.

Figure 7.308. Advanced – 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 OpenRG. 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.

Use MSS Clamping to Reduce Voice Delay When using Maximum Segment Size (MSS) Clamping, TCP streams routed via OpenRG when a voice call is active, will have a smaller segment size. This will cause RTP to receive better priority, and will help prevent high voice jitter that is caused by slow upstream transmission rate, which is common with most WAN connections (DSL, DOCSIS, etc.). When checking this option, the 'Maximum Segment Size (MSS)' field appears, where you can change the maximal segment size.

7.7.12.8. Configuring Dial Codes for Call Features

The 'Feature Codes' section enables you to view and customize activation codes for various call forwarding features.

Feature	Code
<input checked="" type="checkbox"/> Set Call Forwarding Always Destination Number	*56
<input checked="" type="checkbox"/> Activate Call Forwarding Always	*72
<input checked="" type="checkbox"/> Deactivate Call Forwarding Always	*73
<input checked="" type="checkbox"/> Set Call Forwarding on Busy Destination Number	*40
<input checked="" type="checkbox"/> Activate Call Forwarding on Busy	*90
<input checked="" type="checkbox"/> Deactivate Call Forwarding on Busy	*91
<input checked="" type="checkbox"/> Set Call Forwarding on No Answer Destination Number	*42
<input checked="" type="checkbox"/> Activate Call Forwarding on No Answer	*92
<input checked="" type="checkbox"/> Deactivate Call Forwarding on No Answer	*93
<input checked="" type="checkbox"/> Activate Do Not Disturb	*78
<input checked="" type="checkbox"/> Deactivate Do Not Disturb	*79

Figure 7.309. Feature Codes

Set Call Forwarding Always Destination Number Enables you to set an alternate destination number for all incoming calls, by entering <extension number># after the feature's code (*56 by default). For example, to set extension 300 as a destination number, dial *56300#. You will hear a voice confirmation for setting a destination number.

Activate Call Forwarding Always Forwards all incoming calls to a predefined extension. If you have not dialed a destination number when configuring the previous setting, a voice message will notify you accordingly. In this case, set a destination number as described earlier, prior to enabling the 'Activate Call Forwarding Always' feature. After dialing the code (*72 by default), you will hear a voice confirmation for the feature's activation.

Deactivate Call Forwarding Always Deactivates the 'Call Forwarding Always' feature. After dialing the code (*73 by default), you will hear a voice confirmation for 'Call Forwarding Always' deactivation.

Set Call Forwarding on Busy Destination Number Enables you to set an alternate destination for incoming calls, which are directed to a busy extension. After dialing the code (*40 by default), enter an extension number followed by "#". After dialing this sequence, you will hear a voice confirmation for setting the destination number.

Activate Call Forwarding on Busy Redirects a caller to an alternate extension, whenever the original target extension is busy. If you have not dialed a destination number when configuring the previous setting, a voice message will notify you accordingly. In this case, set a destination number as described earlier, prior to enabling the 'Call Forwarding on Busy' feature. After dialing the code (*90 by default), you will hear a voice confirmation for the feature's activation. Note that this feature is relevant only if the 'Call Forwarding Always' feature is deactivated.

Deactivate Call Forwarding on Busy Deactivates the 'Call Forwarding on Busy' feature. After dialing the feature's code (*91 by default), you will hear a voice confirmation for 'Call Forwarding on Busy' deactivation.

Set Call Forwarding on No Answer Destination Number Enables you to set an alternate destination number for incoming calls directed to an extension, which does not answer within a specific timeframe (by default, 20 seconds). Dial a destination number as described earlier, after the feature's code (*42 by default). You will hear a voice confirmation for setting the destination number.

Activate Call Forwarding on No Answer Redirects a caller to a alternate extension, whenever the original target extension does not answer within a specific timeframe. If you have not dialed a destination number when configuring the previous setting, a voice message will notify you accordingly. In this case, set a destination number as described earlier, prior to enabling the 'Call Forwarding on No Answer' feature. After dialing the code (*92 by default), you will hear a voice confirmation for the feature's activation. Note that this feature is relevant only if the 'Call Forwarding Always' feature is deactivated.

Deactivate Call Forwarding on No Answer Deactivates the 'Call Forwarding on No Answer' feature. After dialing the feature's code (*93 by default), you will hear a voice confirmation for 'Call Forwarding on No Answer' deactivation.

Activate Do Not Disturb Prevents calls from reaching a target extension. The caller will be forwarded to the extension's voice mail. After dialing the feature's code (*78 by default), you will hear a voice confirmation for the feature's activation.

Deactivate Do Not Disturb Cancels redirection of callers to the voice mail, and makes the target extension available for incoming calls. After dialing the feature's code (*79 by default), you will hear a voice confirmation for the feature's deactivation.



Note: You can forward calls to external numbers by including an appropriate prefix. For example, if the prefix for external calls is '9', then by dialing *5691800555555#, you can forward calls to 1-800-555-555.

If either 'Call Forwarding Always' or 'Do Not Disturb' is activated, you will hear a stutter dial tone when picking up a phone connected to an analog extension.

7.7.12.9. Improving Voice Reception with Echo Cancellation

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



Note: This feature is currently available on the following platforms: Intel IXP425, Broadcom BCM96358, and on platforms with the VINETIC chipset.

To improve voice reception with echo cancellation, click the 'Advanced' link under the 'Voice' item menu. In the 'Echo Cancellation' section, configure the following options.

The screenshot shows the 'Echo Cancellation' configuration window. It has a title bar 'Echo Cancellation' and a light blue background. There are four settings listed:

- Enabled
- Tail Length: x 2ms
- Non-Linear Process: (dropdown arrow)
- Delay Compensation: x 0.125ms

Figure 7.310. Advanced – Echo Cancellation

Enabled Select or deselect this check box to enable or disable this feature.

Tail Length Defines the length of the elapsed time frame used for calculating the extrapolation of the echo cancellation. A long tail improves the echo cancellation, but increases the load on the Digital Signal Processor (DSP).

Non-Linear Process (NLP) Determines the type of calculation that is used for removing the echo effect. You can set this feature to Normal, High or Off. Using high NLP improves the echo cancellation, but increases the load on the DSP.

Delay Compensation A time delay compensating the echo cancellation.



Note: On some platforms, the feature's graphic interface may differ from the one presented in the above figure.

7.7.12.10. Saving Bandwidth with Silence Suppression

Silence suppression enables optimization when no speech is detected. With this feature enabled, OpenRG is able to detect the absence of audio and conserve bandwidth by preventing the transmission of "silent packets" over the network.

To save bandwidth with silence suppression, click the 'Advanced' link under the 'Voice' item menu. In the 'Silence Suppression' section, configure the following options.

A screenshot of a web-based configuration panel titled "Silence Suppression". The panel has a light blue header with the title. Below the header, there are two checkboxes, both of which are currently unchecked. The first checkbox is labeled "Enable Silence Suppression" and the second is labeled "Enable Comfort Noise".

Silence Suppression	
<input type="checkbox"/>	Enable Silence Suppression
<input type="checkbox"/>	Enable Comfort Noise

Figure 7.311. Advanced – Silence Suppression

Enable Silence Suppression Select this check box to enable this feature.

Enable Comfort Noise Select this option to play a soft "comfort" noise if the other side is performing silence suppression, in order to signal your caller that the conversation is still active.

7.7.12.11. Avoiding Voice Distortion with Jitter Buffer

A Jitter Buffer is a shared data area where voice packets can be collected, stored, and sent to the voice processor in evenly spaced intervals. Variations in packet arrival time, called "jitter", can occur because of network congestion, timing drift, or route changes. The jitter buffer intentionally delays the arriving packets so that the end user experiences a clear connection with very little voice distortion.

To avoid voice distortion with jitter buffer, click the 'Advanced' link under the 'Voice' item menu. In the 'Jitter Buffer' section, configure the following options.

Jitter Buffer

Type: Adaptive ▾

Initial Size: 16 milliseconds

Minimum Size: 0 milliseconds

Maximum Size: 200 milliseconds

Adaptation Period: 10000 milliseconds

Figure 7.312. Advanced – Jitter Buffer

Type The type of the jitter buffer. Can be either adaptive or fixed. In case of adaptive jitter buffer, the following fields are visible:

Adapt According to Determines whether the jitter buffer size depends on the packet length or on the estimated network jitter.

Scaling Factor The size of the jitter buffer is Scaling Factor multiplied by packet length or by estimated network jitter (depending on the value of the previous field).

Local Adaptation The jitter buffer modifies its size during silence gaps. This way the change in delay is not noticed by the listener. This parameter determines when to perform this adaptation. The options are:

Off Regard as silence packets only those packets that the far end has marked as such.

On Regard as silence packets both the packets that the far end detected, and the packets that were locally detected as speech gaps.

On with sample interpolation No silence is needed. The adaptation is performed gradually through interpolation, so the listener does not notice the jitter buffer change in size. Notice that for this mode, modem or fax transmission could be distorted. This feature should only be used in the case of voice transmission.

Initial Size The initial size of the jitter buffer (in milliseconds).

Maximum Size The maximum size of the jitter buffer (in milliseconds).

Minimum Size The minimum size of the jitter buffer (in milliseconds).

7.7.12.12. Changing the FXS Ports Settings

The 'FXS Ports' section in the 'Advanced' screen contains advanced electronic settings for the FXS (analog) ports, which should only be modified by an experienced administrator or technician.

Ringing Voltage:	70	vpk
Ringing Frequency:	25	Hz
Ringing Waveform:	Sinusoid	
On-Hook Voltage:	48	v
Off-Hook Current:	26	mA
Two-Wire Impedance:	600 ohm	
Transmit Gain:	0	dB
Receive Gain:	0	dB

Figure 7.313. Advanced – FXS Ports

Ringing Voltage The ringing voltage in volts.

Ringing Frequency The ringing frequency in hertz.

Ringing Waveform The ringing waveform – sinusoid or trapezoid.

On-Hook Voltage The voltage of an idle handset in volts.

Off-Hook Current Limit The current of an active handset in milli-amperes.

Two-Wire Impedance Select the voice band impedance in ohms, synthesized by the SLIC.

Transmit Gain The transmit gain in decibels.

Receive Gain The receive gain in decibels.

7.7.12.13. Configuring On Hook Caller ID Generation

The following settings determine the method by which the caller identity is generated while the handset is on-hook—the telephone is not in use.

Transmission Phase:	After the First Ring
Modulation Type:	Bell 202
FSK Amplitude:	-13 dBm0
Alerting Info:	Not Required

Figure 7.314. Advanced – On Hook Caller ID Generation

Transmission Phase Select when to display the caller ID—either before or after the first ring.

Modulation Type Select the modulation type—Bell 202 or ITU V.23.

FSK Amplitude Enter the Frequency Shift Keying amplitude.

Alerting Info Select DT-AS if alerting information is required. Otherwise, leave as "Not Required".

7.7.12.14. Configuring Off Hook Caller ID Generation

The following settings determine the method by which the caller identity is generated while the handset is off-hook—a conversation is active.

The screenshot shows a configuration window titled "Off Hook Caller ID Generation". It contains three rows of settings:

- Modulation Type:** A dropdown menu with "Bell 202" selected.
- FSK Amplitude:** A text input field containing "-13" followed by "dBm0".
- Alerting Info:** A dropdown menu with "DT-AS" selected.

Figure 7.315. Advanced – Off Hook Caller ID Generation

Modulation Type Select the modulation type—Bell 202 or ITU V.23.

FSK Amplitude Enter the Frequency Shift Keying amplitude.

Alerting Info Select DT-AS if alerting information is required. Otherwise, leave as "Not Required".

7.7.12.15. Setting the Flash Button Timeout

The PBX distinguishes between pressing the hook and "Flash" button by the length of time that the Flash button is pressed. If it is pressed for longer than this timeframe, pressing Flash becomes equivalent to pressing the hook (phone hang-up).

The screenshot shows a configuration window titled "Hook Flash". It contains one row of settings:

- Maximum Hook Flash Time:** A dropdown menu with "850" selected, followed by "milliseconds".

Figure 7.316. Advanced – Hook Flash

Maximum Hook Flash Time Select the maximum timeframe (between 250 and 850 milliseconds) after which pressing the Flash button hangs up the call.

7.8. Parental Control

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?"

OpenRG's 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.

OpenRG's 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

7.8.1. Overview

OpenRG's 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 OpenRG's 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.

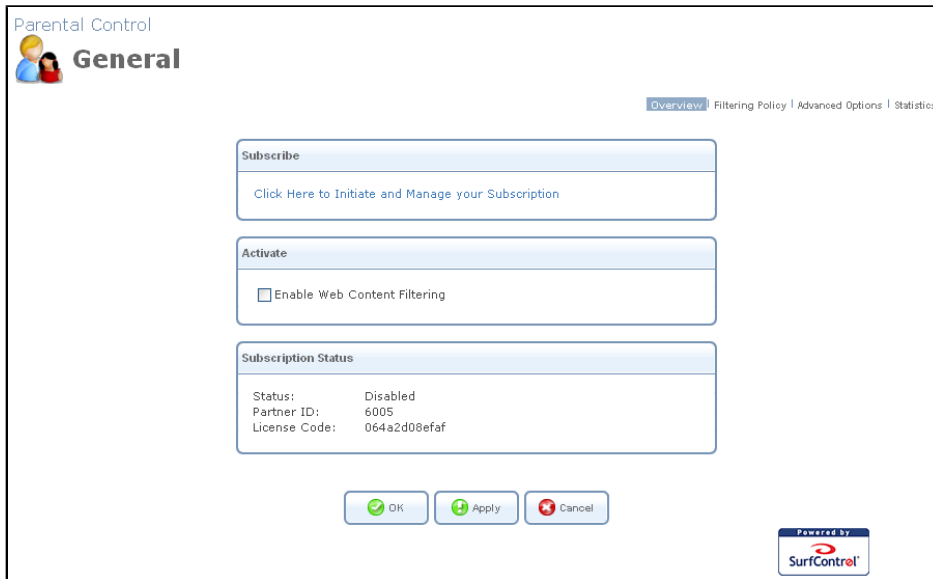


Figure 7.317. General

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 OpenRG's 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.

7.8.2. Filtering Policy

7.8.2.1. Creating a Filtering Policy

A filtering policy defines which sites will be blocked based on their category. OpenRG 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 (see [Figure 7.318](#)). 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. The 'Filtering Policy' screen appears.

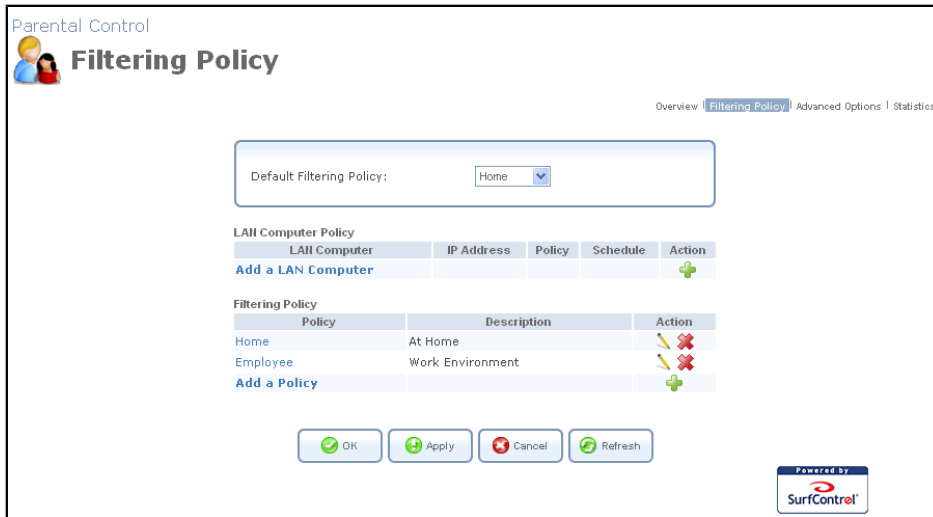


Figure 7.318. Filtering Policy

2. Click the 'Add a policy' link. The following screen appears.

Figure 7.319. Creating a Filtering Policy

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.

7.8.2.2. Applying the Filtering Policy

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 (see [Figure 7.318](#)), 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. The 'LAN Computer Policy' screen appears.

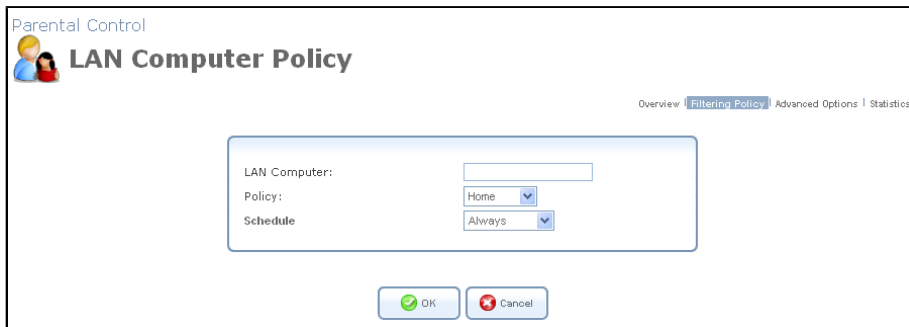


Figure 7.320. LAN Computer Policy

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. To learn how to configure scheduler rules, refer to [Section 8.9.3](#).
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.

7.8.3. Advanced Options

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

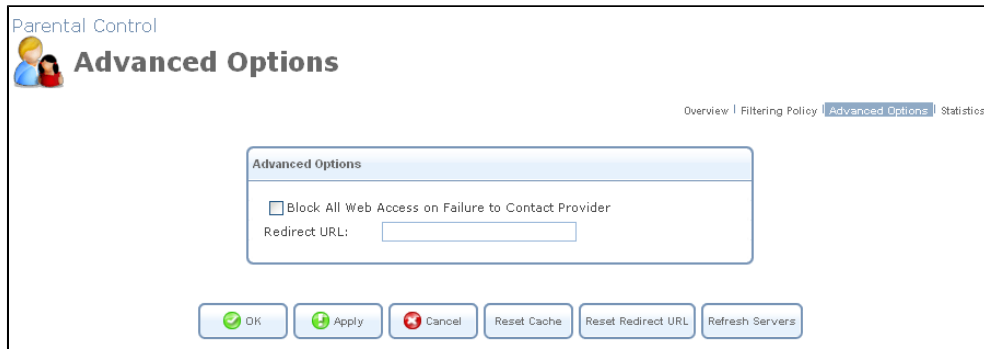


Figure 7.321. Advanced Options

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 (see [Figure 7.322](#)), 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.

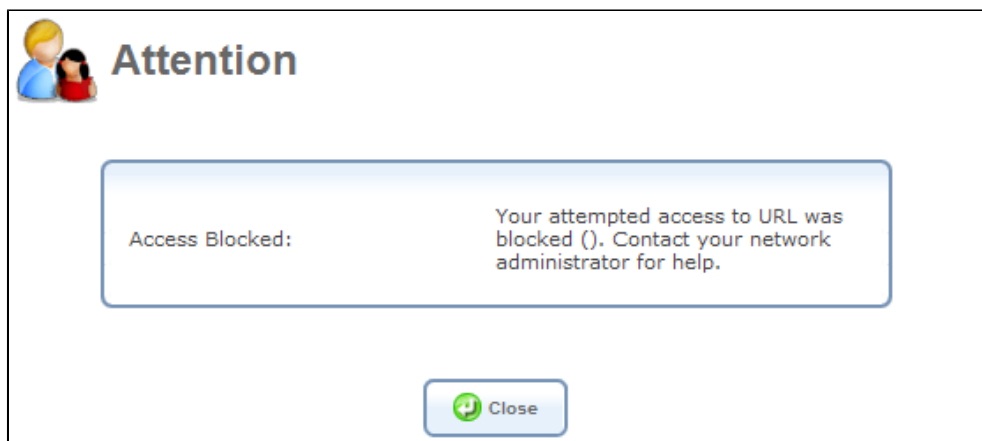


Figure 7.322. Blocked Access

7.8.4. Statistics

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

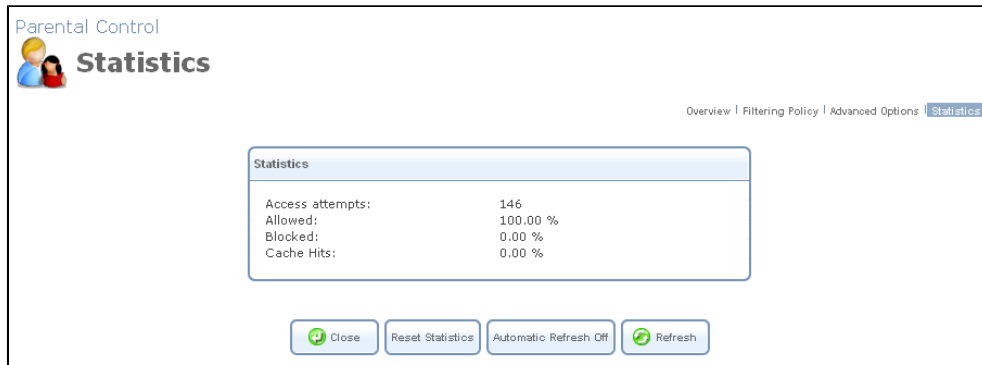



Figure 7.323. Statistics

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

 Note: When Parental Control is enabled, HTTP services cannot be blocked by the 'Security Access Control' feature (refer to [Section 7.3.2](#)).

7.9. Email Filtering

Email filtering is the processing of electronic mail according to specified criteria, and is most commonly used as Anti-Virus and Anti-Spam. OpenRG enables you to utilize an email filtering subscription on your gateway to control your email traffic and protect your network from malicious electronic messages. Every email message sent to your gateway will first be verified by your email filtering server and handled according to your preferences. This feature greatly reduces potential harm to your network by eliminating sending and receiving unsolicited emails and computer viruses.

7.9.1. Overview

The 'Overview' screen enables you to activate and use email filtering.

7.9.1.1. Activating Email Filtering

The first step in setting up email filtering on your network is obtaining a subscription from an email filtering service provider. Currently, OpenRG is provided with a connection to a demo server, for demonstration purposes.

1. Under the 'Services' tab, click the 'Email Filtering' menu item. The service's 'General' screen appears.

The screenshot shows the 'Email Filtering' configuration interface. The 'General' tab is active, displaying options to subscribe, set a user name, and activate the service. The subscription status is currently 'Disabled'.

Figure 7.324. General

2. In the 'Subscribe' section, click the 'Click Here to Initiate and Manage your Subscription' link. The email filtering service provider's site will be displayed in a new browser window.
3. Follow the instructions on the site and subscribe for a free trial. You should receive a user name. The user name for OpenRG's demo server is "openrg".

To activate the email filtering subscription on your gateway, perform the following:

1. Under the 'Services' tab, click the 'Email Filtering' menu item. The service's 'General' screen appears (see [Figure 7.324](#)).
2. In the 'User Name' section, enter the user name provided by your email filtering service provider. In this case, enter "openrg".
3. In the 'Activate' section, select the 'Enable Email Filtering' check box, and click 'Apply'. The screen refreshes, displaying additional 'POP3 Server Status' and 'SMTP Server Status' sections (see [Figure 7.325](#)). These sections list information on your incoming and outgoing mail servers, respectively. The 'Server Host' entry displays the IP address of the email filtering server. Note that the 'Status' entries (as well as the subscription status) should all indicate "OK". If this is not the case, click the 'Refresh' button. Wait a few seconds and repeat this step.

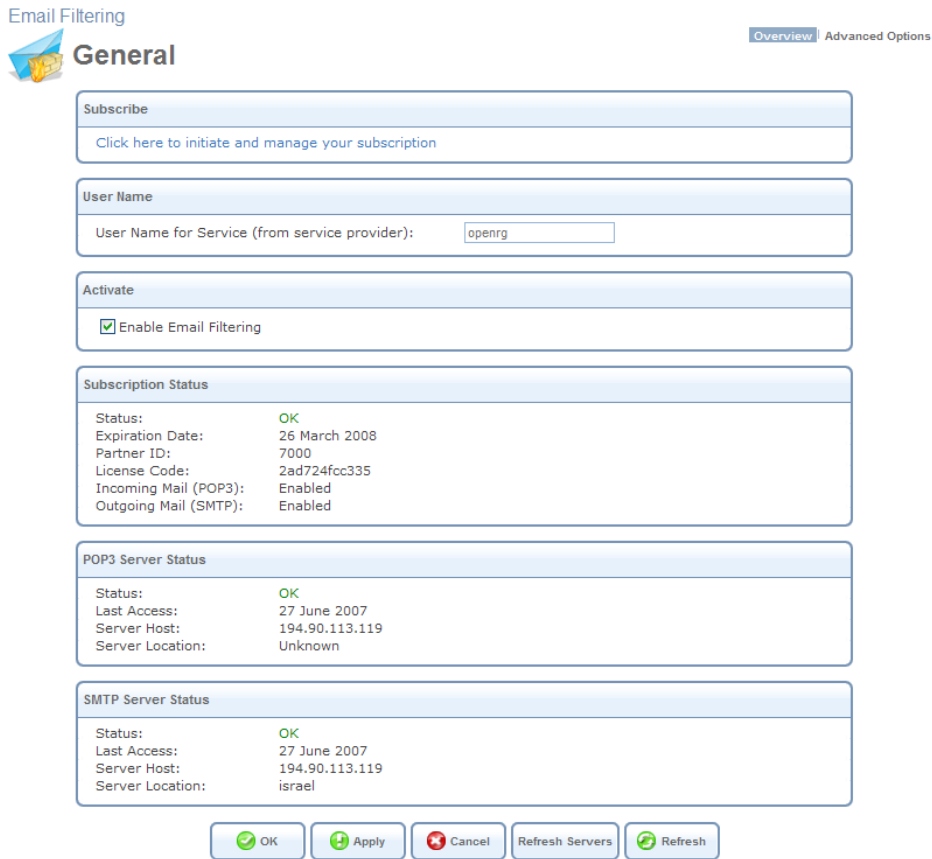


Figure 7.325. Email Filtering – Activated

7.9.1.2. Using Email Filtering

Perform the following email filtering test:

1. Send an email from a WAN computer to a computer in OpenRG's LAN running a PC-based mail client such as Outlook™ or Eudora™. Write the word "sexx" in the subject line of the message.
2. Check for the received message on the LAN computer. The message should arrive with the following subject: "*** Detected as Spam by POP3 spam keywords*** sexx".

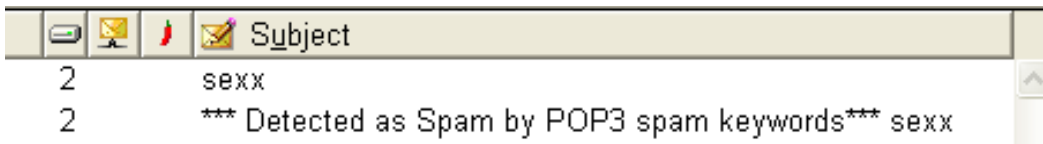


Figure 7.326. LAN Computer Inbox

This is how the email filtering service is configured to handle spam of this sort. However, you may choose how to handle spam and other types of email messages by configuring your email filtering account.

- Repeat the steps above, only this time deactivate email filtering by deselecting the 'Enable Email Filtering' check-box (see [Figure 7.325](#)). The message should arrive exactly as sent, as no filtering had been performed.

7.9.2. Advanced Options

The 'Advanced Options' screen contains additional configuration parameters for incoming and outgoing mail.

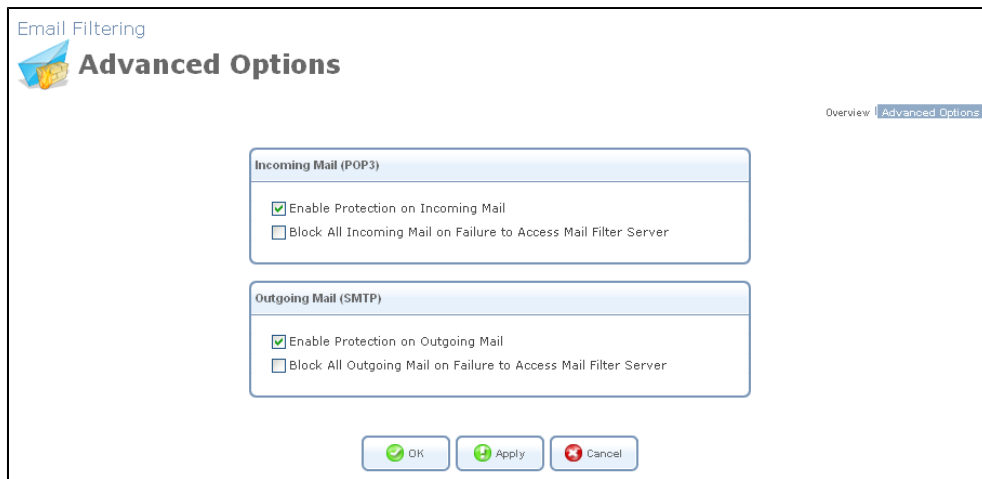


Figure 7.327. Advanced Options

- Incoming Mail (POP3)

Enable Protection on Incoming Mail Email filtering rules will be applied on incoming mail.

Block All Incoming Mail on Failure to Access Mail Filter Server Select this option if you would like to block all incoming mail messages in case email filtering cannot be performed.

- Outgoing Mail (SMTP)

Enable Protection on Outgoing Mail Email filtering rules will be applied on outgoing mail. This option is enabled by default.

Block All Outgoing Mail on Failure to Access Mail Filter Server Select this option if you would like to block all outgoing mail messages in case email filtering cannot be performed.

7.10. Virtual Private Network

7.10.1. Internet Protocol Security

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.

7.10.1.1. Technical Specifications

- Security architecture for the Internet Protocol
- IP Security Document Roadmap
- Connection type: Tunnel, Transport
- Use of Internet Security Association and Key Management Protocol (ISAKMP) in main and aggressive modes
- Key management: Manual, Automatic (Internet Key Exchange)
- NAT Traversal Negotiation for resolution of NATed tunnel endpoint scenarios
- Dead Peer Detection for tunnel disconnection in case the remote endpoint ceases to operate
- Gateway authentication: X.509, RSA signatures and pre-shared secret key
- IP protocols: ESP, AH
- Encryption: AES, 3DES, DES, NULL, HW encryption integration (platform dependent)

- Authentication: MD5, SHA-1
- IP Payload compression
- Interoperability: VPNC Certified IPSec, Windows 2000, Windows NT, FreeS/WAN, FreeBSD, Checkpoint Firewall-1, Safenet SoftRemote, NetScreen, SSH Sentinel

7.10.1.2. IPSec Settings

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.

The screenshot shows the 'Internet Protocol Security (IPSec)' configuration interface. At the top left, there is a 'VPN' logo and the title 'Internet Protocol Security (IPSec)'. A breadcrumb trail at the top right reads 'IPSec > SSL-VPN > PPTP Server > L2TP Server'. The main content area is divided into three sections:

- Block Unauthorized IP:** This section has a checked 'Enabled' checkbox. Below it are two input fields: 'Maximum Number of Authentication Failures' with the value '5' and 'Block Period (in seconds):' with the value '60'.
- Anti-Replay:** This section has a checked 'Enable Anti-Replay Protection' checkbox.
- Connections:** This section contains a table with the following data:

Name	Status	Action
VPN IPSec	Waiting for Connection	[Edit] [Delete]

At the bottom of the screen, there are five buttons: 'OK', 'Apply', 'Cancel', 'Settings', and 'Log Settings'.

Figure 7.328. Internet Protocol Security (IPSec)

This screen enables you to configure the following settings:

Block Unauthorized IP Select the 'Enabled' check box to block unauthorized IP packets to OpenRG. 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 OpenRG 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. To learn how to create an IPSec connection, refer to [Section 8.4.15](#).

7.10.1.2.1. Public Key Management

The 'Settings' button in the 'Internet Protocol Security (IPSec)' screen enables you to manage OpenRG's public keys.

1. Click the 'Settings' button (see [Figure 7.328](#)) to view OpenRG's public key. If necessary, you can copy the public key from the screen that appears.

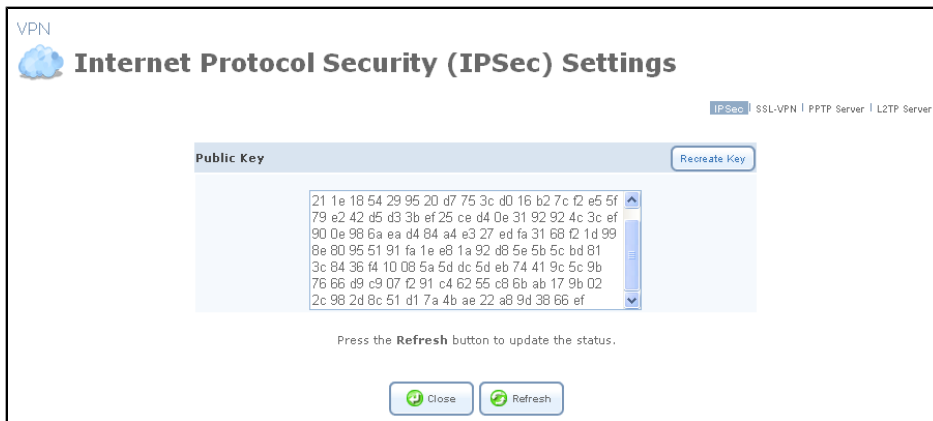


Figure 7.329. Internet Protocol Security (IPSec) Settings

2. Click the 'Recreate Key' button to recreate the public key, or the 'Refresh' button to refresh the key displayed in this screen.

7.10.1.2.2. Log Settings

The IPSec Log can be used to identify and analyze the history of the IPSec package commands, attempts to create connections, etc. The IPSec activity, as well as that of other OpenRG modules, are displayed together in this view.

1. Click the 'Log Settings' button. The 'IPSec Log Settings' screen appears (see [Figure 7.330](#)).
2. Select the check boxes relevant to the information you would like the IPSec log to record.
3. Click 'OK' to save the settings.

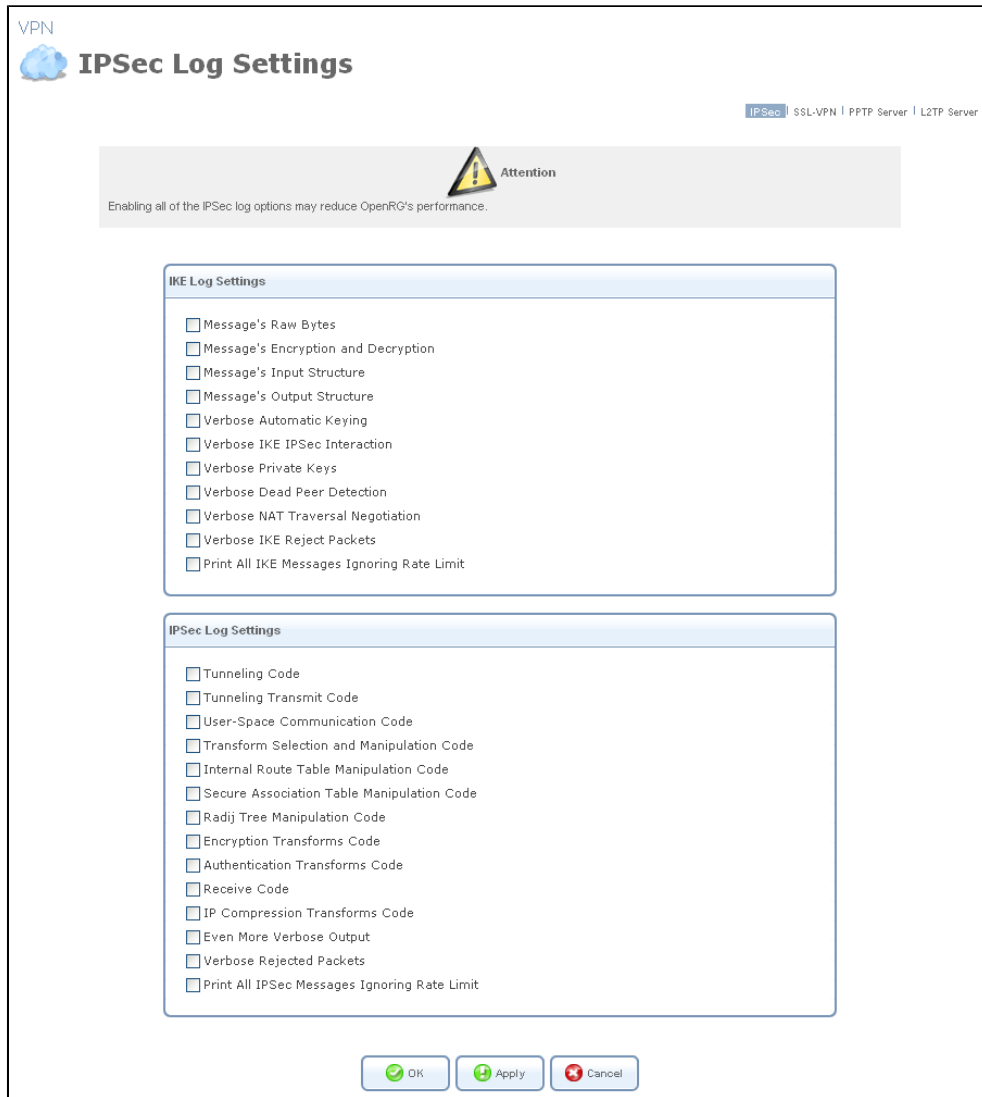



Figure 7.330. IPSec Log Settings

7.10.1.3. IPSec Connection Settings

The IPSec connections are displayed under the 'Connections' section of the 'Internet Protocol Security (IPSec)' screen (see [Figure 7.328](#)), in addition to the general 'Network Connections' screen (refer to [Section 8.4](#)). To configure an IPSec connection settings, perform the following:

1. Click the connection's  action icon . The 'VPN IPSec Properties' screen appears, displaying the 'General' sub-tab.

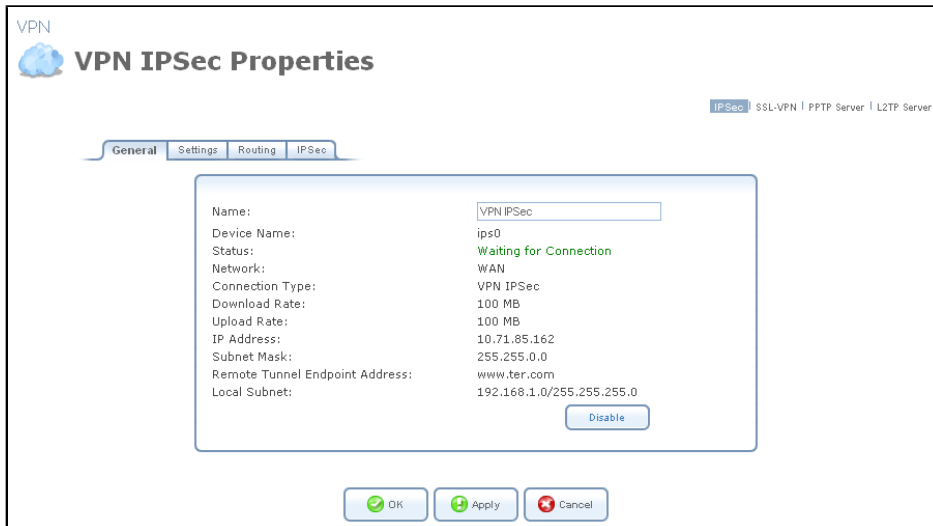


Figure 7.331. VPN IPSec Properties – General

2. Click the 'Settings' sub-tab, and configure the following settings:



Figure 7.332. VPN IPSec Properties – Settings

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, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to [Section 8.9.3](#).

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to [Section 8.4.2](#).

3. Click the 'Routing' sub-tab, and define the connection's routing rules. To learn how to create routing rules, refer to [Section 8.6.1](#).

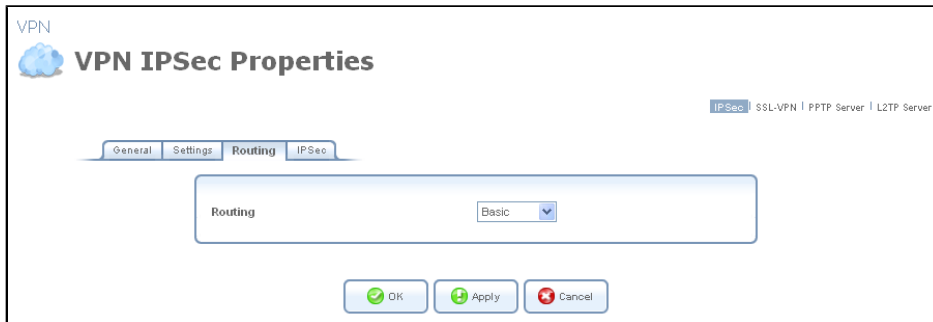


Figure 7.333. VPN IPsec Properties – Routing

4. Click the 'IPsec' sub-tab, and configure the following settings.

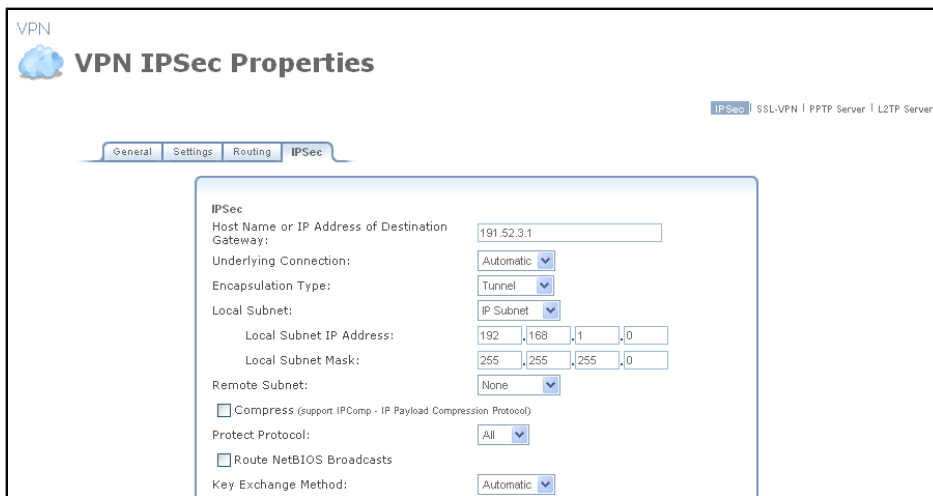


Figure 7.334. VPN IPsec Properties – IPsec

Host Name or IP Address of Destination Gateway The IP address of your IPsec peer. If your connection is an IPsec Server, this field will display "Any Remote Gateway".

Underlying Connection In a single WAN scenario, the underlying connection parameter will be set to "Automatic" (non-configurable). However, if you have multiple WAN devices, a drop-down menu will appear (see [Figure 7.332](#)), enabling you to choose the underlying WAN device. The IPsec connection will only use your chosen device, unless failover is enabled. In this case, the failed-to device will be used instead (assuming its route rules consent), until the chosen device is up again. Note that if you select "Automatic", there will be no attempt to return to the original device from the failed-to device. For more information about failover, refer to [Section 8.6.1.3.3](#).

Encapsulation Type Select between 'Tunneling' or 'Transport' encapsulation. 'Transport' encapsulation is performed between two gateways (no subnets), and therefore needs no explicit configuration. 'Tunneling' requires that you configure the following parameters:

- **Local Subnet** Define your local endpoint, by selecting one of the following options:

IP Subnet (default) Enter OpenRG's Local Subnet IP Address and Local Subnet Mask.

IP Range Enter the 'From' and 'To' IP addresses, forming the endpoints range of the local subnet(s).

IP Address Enter the Local IP Address to define the endpoint as a single host.

None Select this option if you do not want to define a local endpoint. The endpoint will be set to the gateway.

- **Remote Subnet** This section is identical to the 'Local Subnet' section above, but is for defining the remote endpoint.

Compress (Support IPComp protocol) Select this check box to compress packets during encapsulation with the IP Payload Compression protocol. Please note that this reduces performance (and is therefore unchecked by default).

Protect Protocol Select the protocols to protect with IPSec: All, TCP, UDP, ICMP or GRE. When selecting TCP or UDP, additional source port and destination port drop-down menus will appear, enabling you to select 'All' or to specify 'Single' ports in order to define the protection of specific packets. For example, in order to protect L2TP packets, select UDP and specify 1701 as both single source and single destination ports.

Route NetBIOS Broadcasts Select this option to allow NetBIOS packets through the IPSec tunnel, which otherwise would not meet the routing conditions specified.

Key Exchange Method The IPSec key exchange method can be 'Automatic' (the default) or 'Manual'. Selecting one of these options will alter the rest of the screen.

1. Automatic key exchange settings:

Key Exchange Method:	Automatic
<input checked="" type="checkbox"/> Auto Reconnect	
<input checked="" type="checkbox"/> Enable Dead Peer Detection	
DPD Delay in Seconds:	60
DPD Timeout in Seconds:	120
IPSec Automatic Phase 1	
Mode:	Main Mode
Negotiation Attempts:	3
Life Time in Seconds (1-28800):	3600
Rekey Margin (start negotiation prior to expiration: 1-540):	540
Rekey Fuzz Percent (can be more than 100 Percent: 1-200):	100
Peer Authentication:	IPSec Shared Secret
IPSec Shared Secret:	qwewqwe
Encryption Algorithm	
<input type="checkbox"/> DES-CBC	
<input checked="" type="checkbox"/> 3DES-CBC	
<input type="checkbox"/> AES128-CBC	
<input type="checkbox"/> AES192-CBC	
<input type="checkbox"/> AES256-CBC	
Hash Algorithm	
<input checked="" type="checkbox"/> Allow Peers to Use MD5	
<input checked="" type="checkbox"/> Allow Peers to Use SHA1	
Group Description Attribute	
<input type="checkbox"/> DH Group 1	
<input checked="" type="checkbox"/> DH Group 2	
<input checked="" type="checkbox"/> DH Group 5	
IPSec Automatic Phase 2	
Life Time in Seconds (1-86400):	28800
<input checked="" type="checkbox"/> Use Perfect Forward Secrecy (PFS)	
Group Description Attribute	
<input checked="" type="radio"/> Same group as phase 1	
<input type="radio"/> DH Group 1	
<input type="radio"/> DH Group 2	
<input type="radio"/> DH Group 5	
Encryption Algorithm	
<input checked="" type="checkbox"/> Allow AH Protocol (no encryption)	
<input type="checkbox"/> Allow ESP Protocol with Null-Encryption (no encryption)	
<input type="checkbox"/> Allow ESP Protocol with DES-CBC Encryption	
<input checked="" type="checkbox"/> Allow ESP Protocol with 3DES-CBC Encryption	
<input type="checkbox"/> Allow ESP Protocol with AES-CBC 128-bit Encryption	
<input type="checkbox"/> Allow ESP Protocol with AES-CBC 192-bit Encryption	
<input type="checkbox"/> Allow ESP Protocol with AES-CBC 256-bit Encryption	
Authentication Algorithm (for ESP protocol)	
<input checked="" type="checkbox"/> Allow Peers to Use MD5	
<input checked="" type="checkbox"/> Allow Peers to Use SHA1	
Hash Algorithm (for AH protocol)	
<input checked="" type="checkbox"/> Allow Peers to Use MD5	
<input checked="" type="checkbox"/> Allow Peers to Use SHA1	

Figure 7.335. Automatic Key Exchange Settings

Auto Reconnect The IPsec connection will reconnect automatically if disconnected for any reason.

Enable Dead Peer Detection OpenRG will detect whether the tunnel endpoint has ceased to operate, in which case will terminate the connection. Note that this feature will be functional only if the other tunnel endpoint supports it. This is determined during the negotiation phase of the two endpoints.

- **DPD Delay in Seconds** The timeframe in which no traffic has passed through the tunnel. After this timeframe, OpenRG will send a packet to test the tunnel endpoint, expecting a reply.

- **DPD Timeout in Seconds** The timeframe OpenRG will wait for the test reply, after which it will terminate the connection.

IPSec Automatic Phase 1 – Peer Authentication

- **Mode** Select the IPSec mode – either 'Main Mode' or 'Aggressive Mode'. Main mode is a secured but slower mode, which presents negotiable propositions according to the authentication algorithms that you select in the check boxes. Aggressive Mode is faster but less secured. When selecting this mode, the algorithm check boxes are replaced by radio buttons, presenting strict propositions according to your selections.
- **Negotiation attempts** Select the number of negotiation attempts to be performed in the automatic key exchange method. If all attempts fail, OpenRG will wait for a negotiation request.
- **Life Time in Seconds** The timeframe in which the peer authentication will be valid.
- **Rekey Margin** Specifies how long before connection expiry should attempts to negotiate a replacement begin. It is similar to that of the key life time and is given as an integer denoting seconds.
- **Rekey Fuzz Percent** Specifies the maximum percentage by which Rekey Margin should be randomly increased to randomize re-keying intervals.
- **Peer Authentication** Select the method by which OpenRG will authenticate your IPSec peer.
 - **IPSec Shared Secret** – Enter the IPSec shared secret.
 - **RSA Signature** – Enter the peer's RSA signature (based on OpenRG's public key), as described in [Section 7.10.1.5.3](#).
 - **Certificate** – If a certificate exists on OpenRG, it will appear when you select this option. Enter the certificate's local ID and peer ID. To learn how to add certificates to OpenRG, refer to [Section 8.9.4](#).
- **Encryption Algorithm** Select the encryption algorithms that OpenRG will attempt to use when negotiating with the IPSec peer.
- **Hash Algorithm** Select the hash algorithms that OpenRG will attempt to use when negotiating with the IPSec peer.
- **Group Description Attribute** Select the Diffie-Hellman (DH) group description(s). Diffie-Hellman is a public-key cryptography scheme that allows two parties to establish a shared secret over an insecure communications channel.

IPSec Automatic Phase 2 – Key Definition

- **Life Time in Seconds** The length of time before a security association automatically performs renegotiation.
- **Use Perfect Forward Secrecy (PFS)** Select whether Perfect Forward Secrecy of keys is required on the connection's keying channel (with PFS, penetration of the key-exchange protocol does not compromise keys negotiated earlier). Deselecting this option will hide the next parameter.

Group Description Attribute Select whether to use the same group chosen in phase 1, or reselect specific groups.

- **Encryption Algorithm** Select the encryption algorithms that OpenRG will attempt to use when negotiating with the IPSec peer.
- **Authentication Algorithm (for ESP protocol)** Select the authentication algorithms that OpenRG will attempt to use when negotiating with the IPSec peer.
- **Hash Algorithm (for AH protocol)** Select the hash algorithms that OpenRG will attempt to use when negotiating with the IPSec peer.

2. Manual key definition:

Key Exchange Method: Manual

IPSec Manual

Security Parameter Index (SPI): (HEX, 100 - FFFFFFFF)

Local:

Remote:

Use Different Encryption Keys

IPSec Protocol: ESP

Encryption Algorithm: 3DES-CBC

Key:

Authentication Algorithm: SHA1

Key:

Figure 7.336. Manual Key Definition

Security Parameter Index (SPI): (HEX, 100 - FFFFFFFF) A 32 bit value that together with an IP address and a security protocol, uniquely identifies a particular security association. The local and remote values must be coordinated with their respective values on the IPSec peer.

Use Different Encryption Keys Selecting this option allows you to define both local and remote algorithm keys when defining the IPSec protocol (in the next section).

IPSec Protocol Select between the ESP and AH IPSec protocols. The screen will refresh accordingly:

- **ESP** – Select the encryption and authentication algorithms, and enter the algorithm keys in hexadecimal representation.
- **AH** – Select the hash algorithm, and enter the algorithm key in hexadecimal representation.

5. Click 'OK' to save the settings.

7.10.1.4. IPSec Gateway-to-Host Connection Scenario

In order to create an IPSec connection between OpenRG and a Windows host, you need to configure both the gateway and the host. This section describes both OpenRG's configuration and a Windows XP client configuration.

7.10.1.4.1. Configuring IPSec on OpenRG

1. Under the 'System' tab, click the 'Network Connections' menu item. The 'Network Connections' screen appears.

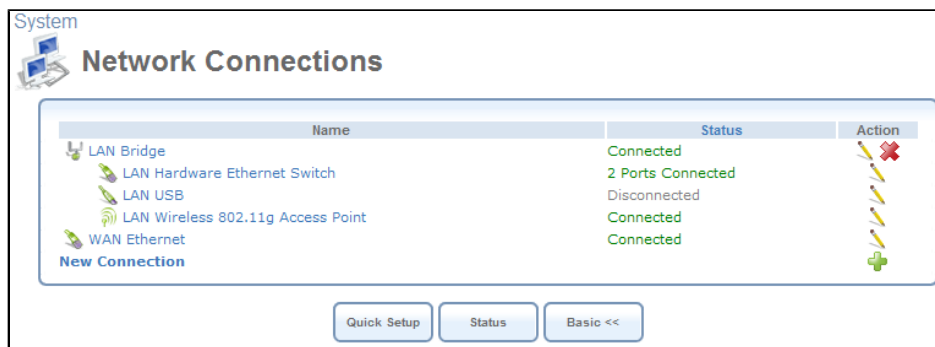


Figure 7.337. Network Connections

2. Click the 'New Connection' link. The 'Connection Wizard' screen appears.

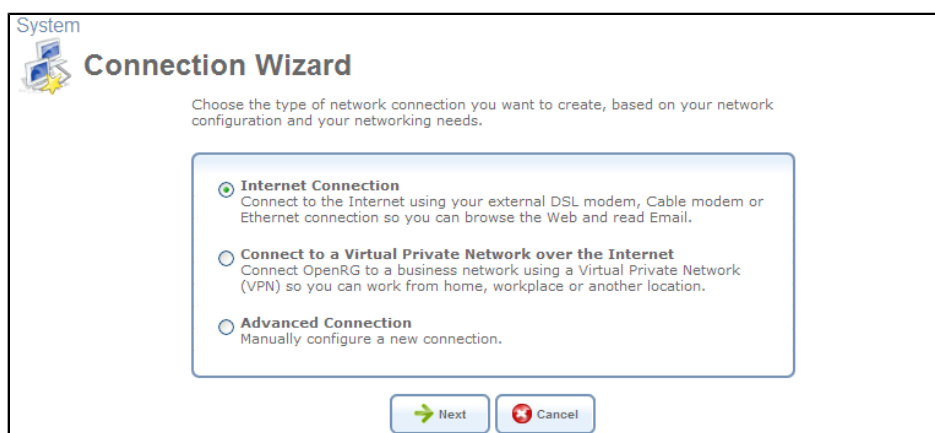


Figure 7.338. Connection Wizard

3. Select the 'Connect to a Virtual Private Network over the Internet' radio button and click 'Next'. The 'Connect to a Virtual Private Network over the Internet' screen appears.

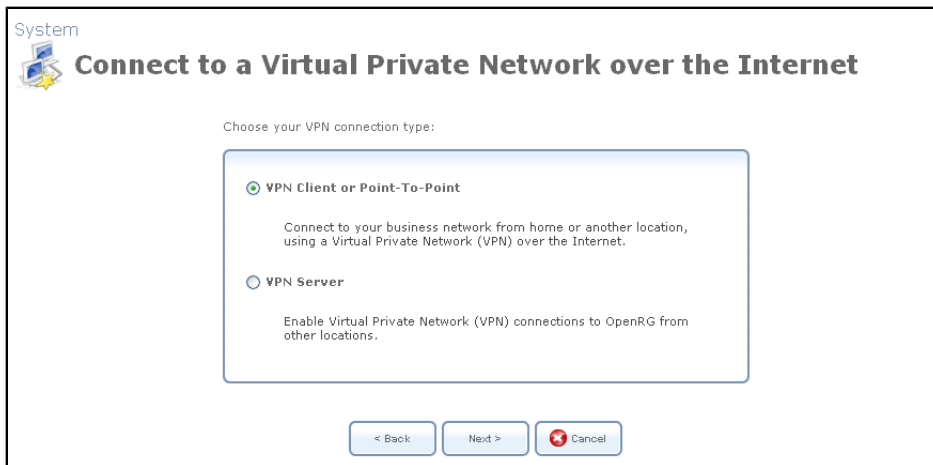


Figure 7.339. Connect to a Virtual Private Network over the Internet

4. Select the 'VPN Client or Point-To-Point' radio button and click 'Next'. The 'VPN Client or Point-To-Point' screen appears.

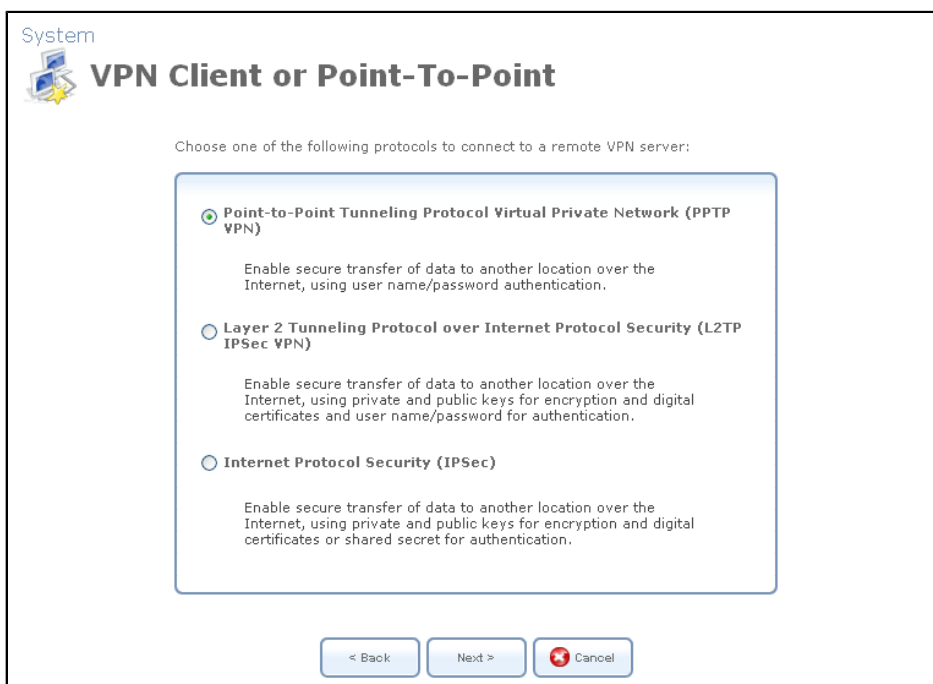


Figure 7.340. VPN Client or Point-To-Point

5. Select the 'Internet Protocol Security (IPSec)' radio button and click 'Next'. The 'Internet Protocol Security (IPSec)' screen appears.

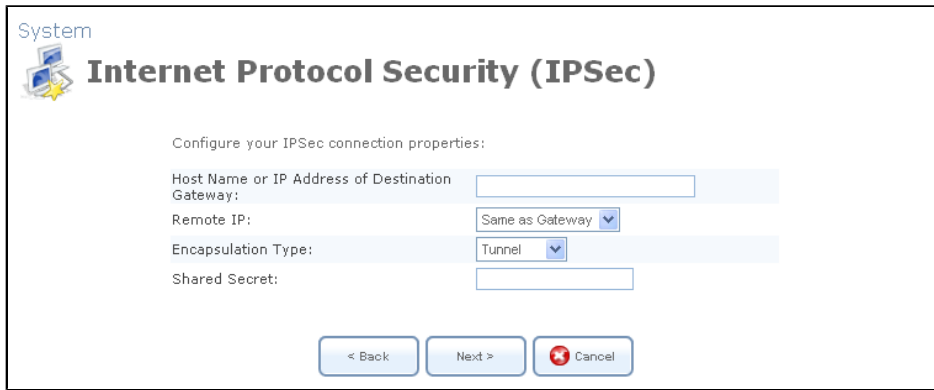


Figure 7.341. Internet Protocol Security (IPSec)

6. Specify the following parameters:

Host Name or IP Address of Destination Gateway Specify 22.23.24.25

Remote IP Select "Same as Gateway".

Encapsulation Type Select "Tunnel".

Shared Secret Enter "hr5x".

7. Click 'Next'. The 'Connection Summary' screen appears.

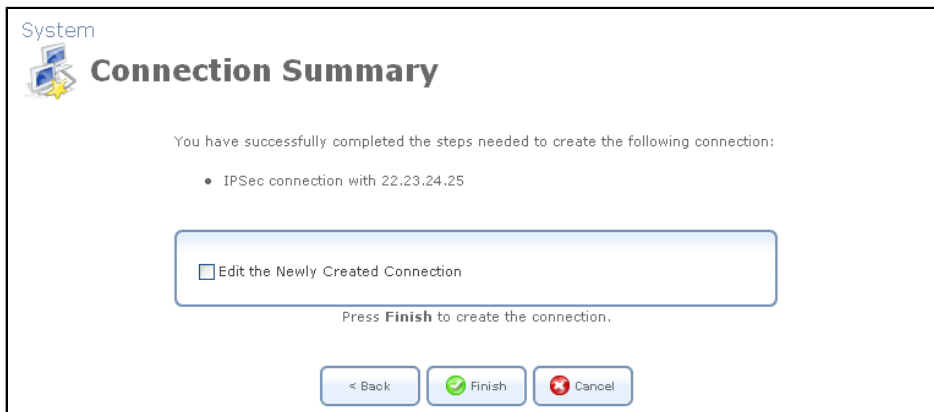


Figure 7.342. Connection Summary

8. Click 'Finish'. The 'Network Connections' screen displays the newly created IPSec connection.

Name	Status	Action
LAN Bridge	Connected	
LAN Hardware Ethernet Switch	2 Ports Connected	
LAN USB	Disconnected	
LAN Wireless 802.11g Access Point	Device missing	
WAN Ethernet	Connected	
VPN IPSec	Waiting for Connection	
New Connection		

Figure 7.343. New VPN IPSec Connection

7.10.1.4.2. Configuring IPSec on the Windows Host

The following IP addresses are needed for the host configuration:

- Windows IP address – referred to as <windows_ip>.
- OpenRG WAN IP address – referred to as <openrg_wan_ip>.
- OpenRG LAN Subnet address – referred to as <openrg_lan_subnet>.

The configuration sequence:

1. Creating the IPSec Policy:

- a. Click the Start button and select Run. Type "secpol.msc" and click 'OK'. The 'Local Security Settings' window appears.

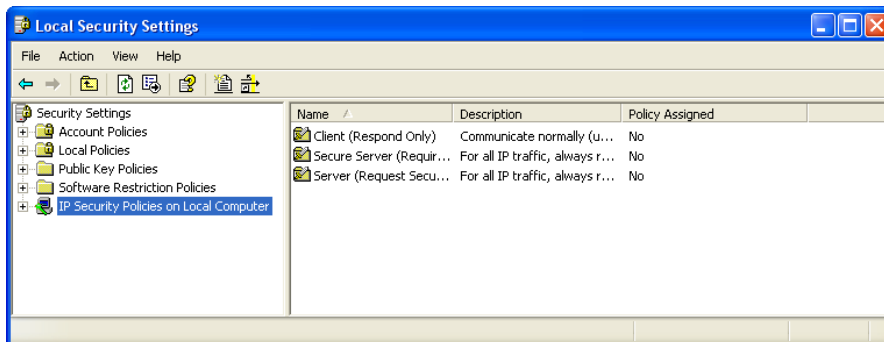


Figure 7.344. Local Security Settings

- b. Right-click the 'IP Security Policies on Local Computer' and choose 'Create IP Security Policy...'. The IP Security Policy Wizard appears.

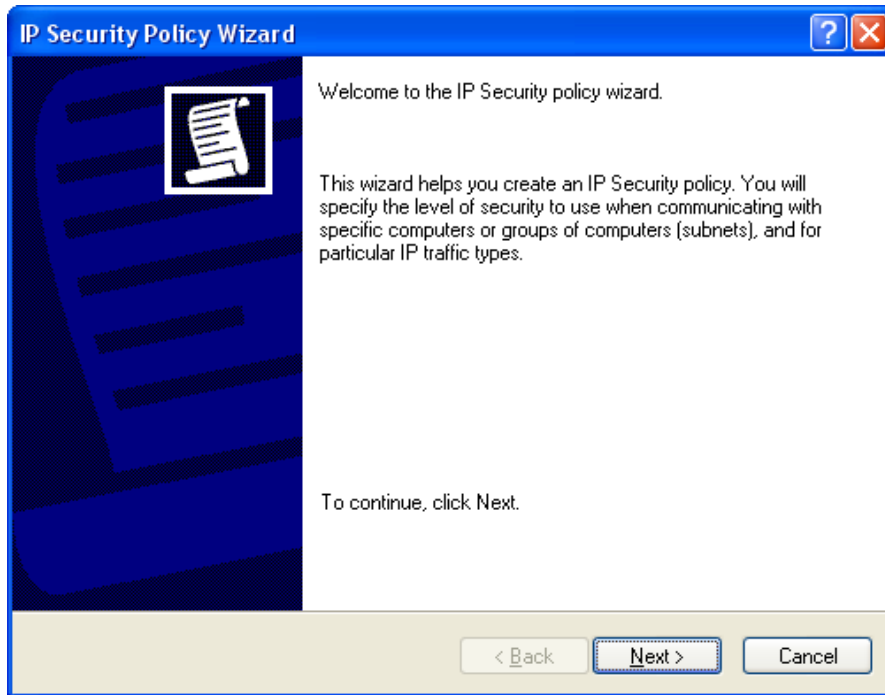


Figure 7.345. IP Security Policy Wizard

- c. Click 'Next' and type a name for your policy, for example "OpenRG Connection".

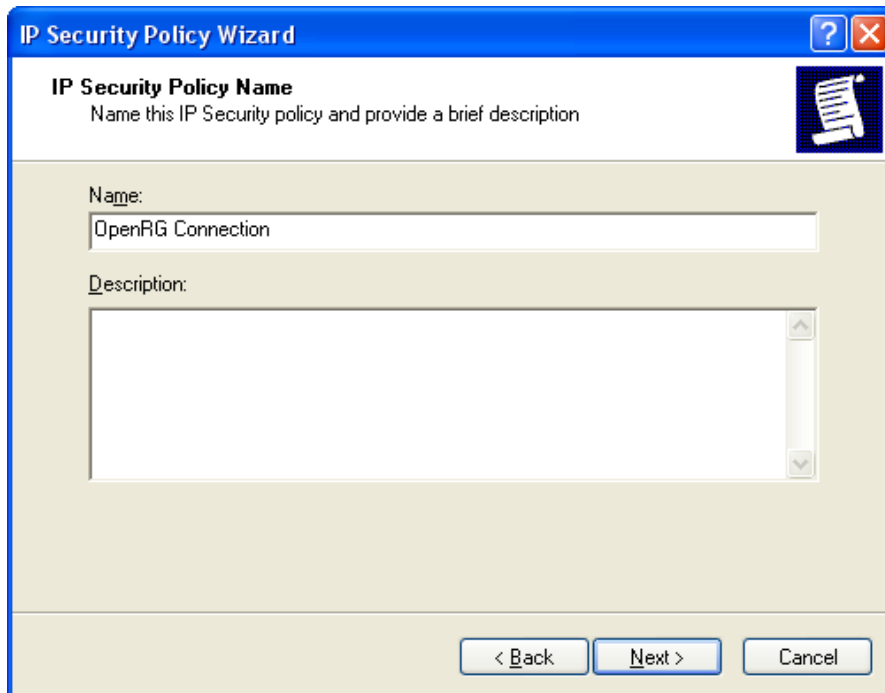


Figure 7.346. IP Security Policy Name

- d. Click 'Next'. The 'Requests for Secure Communication' screen appears.

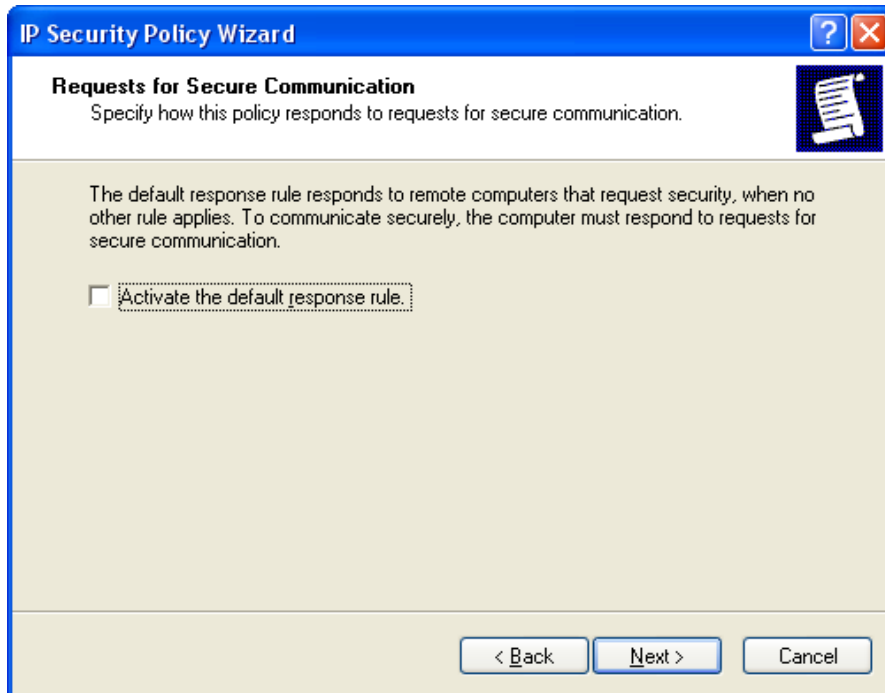


Figure 7.347. Requests for Secure Communication

- e. Deselect the 'Activate the default response rule' check box, and click 'Next'. The 'Completing the IP Security Policy Wizard' screen appears.

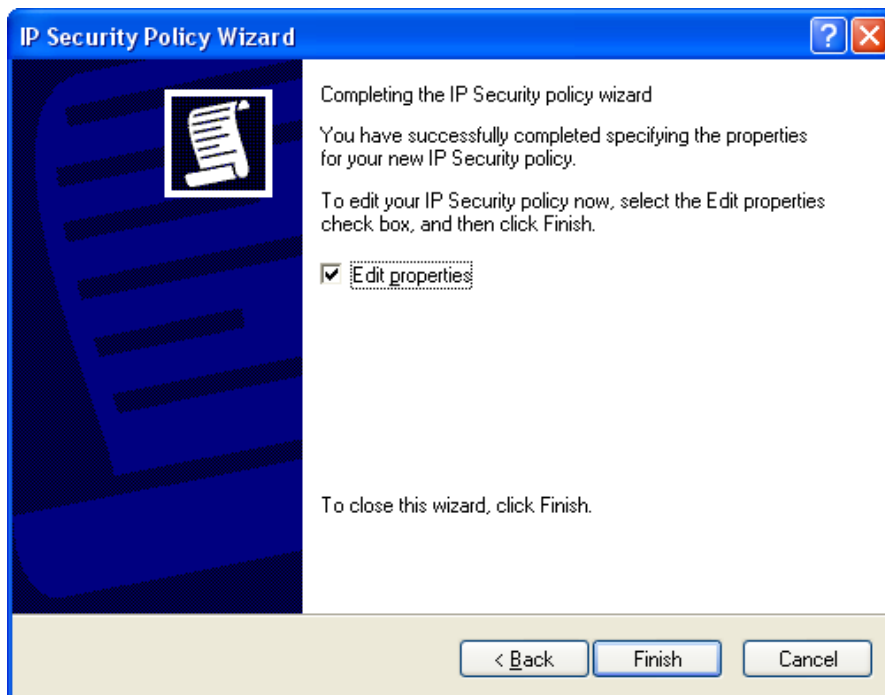


Figure 7.348. Completing the IP Security Policy Wizard

- f. Make sure that the 'Edit Properties' check box is selected, and click 'Finish'. The 'OpenRG Connection Properties' window appears.

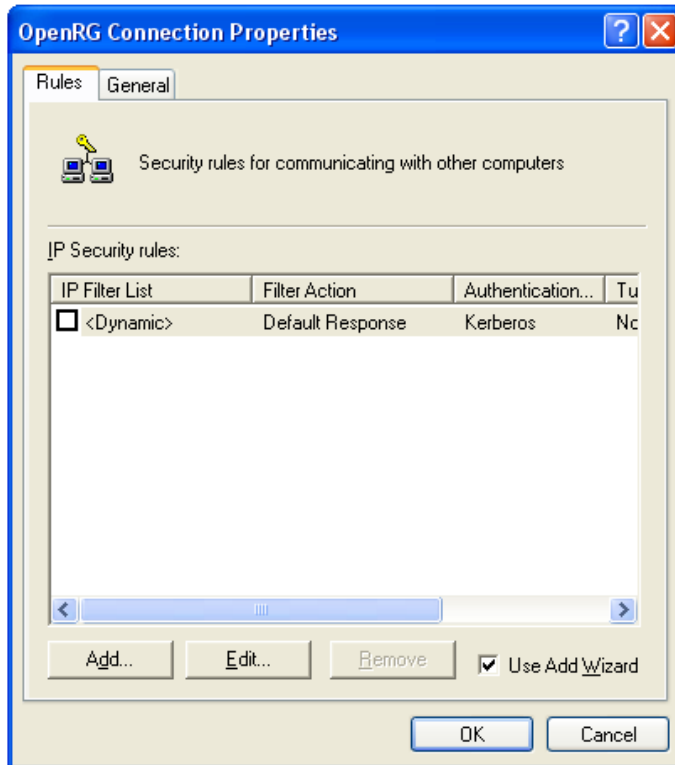


Figure 7.349. OpenRG Connection Properties

- g. Click 'OK'.
2. Building Filter List 1 – Windows XP to OpenRG:
 - a. In the 'Local Security Settings' window, right-click the new 'OpenRG Connection' policy, created in the previous step, and select Properties. The Properties window appears (see [Figure 7.349](#)).
 - b. Deselect the 'Use Add Wizard' check box and click the 'Add' button to create a new IP Security rule. The 'New Rule Properties' window appears.

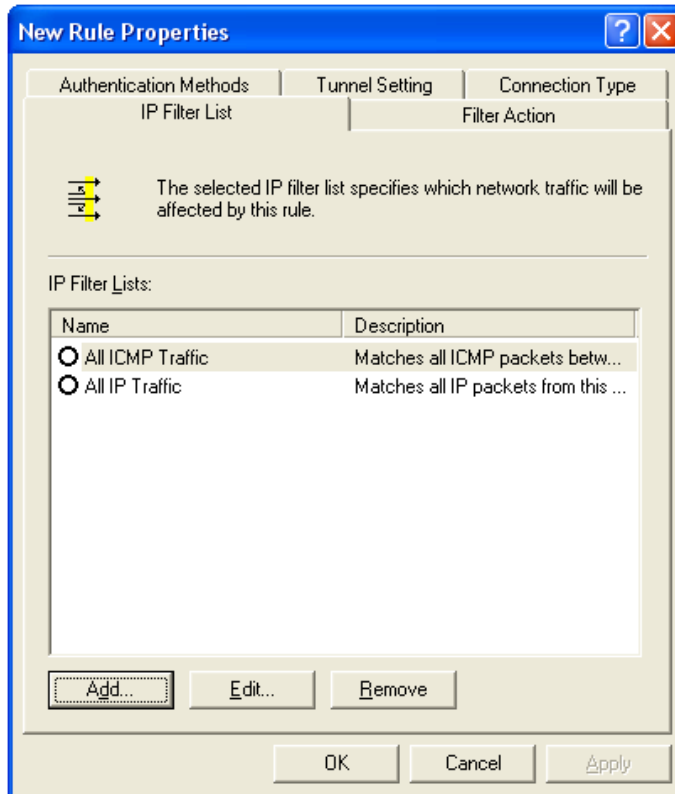


Figure 7.350. New Rule Properties

- c. Under the IP Filter List tab, click the 'Add' button. The 'IP Filter List' window appears.

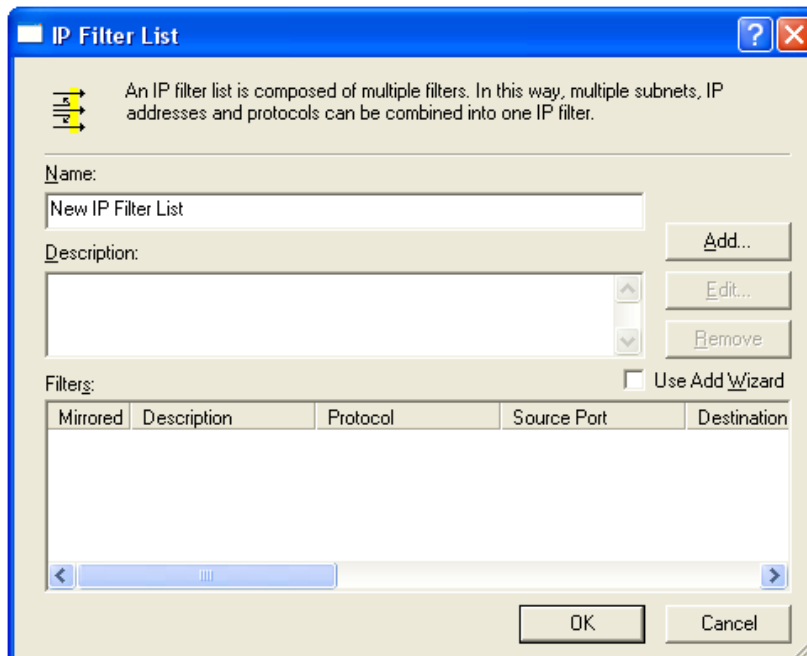


Figure 7.351. IP Filter List

- d. Enter the name "Windows XP to OpenRG" for the filter list, and deselect the 'Use Add Wizard' check box. Then, click the 'Add' button. The 'Filter Properties' window appears.

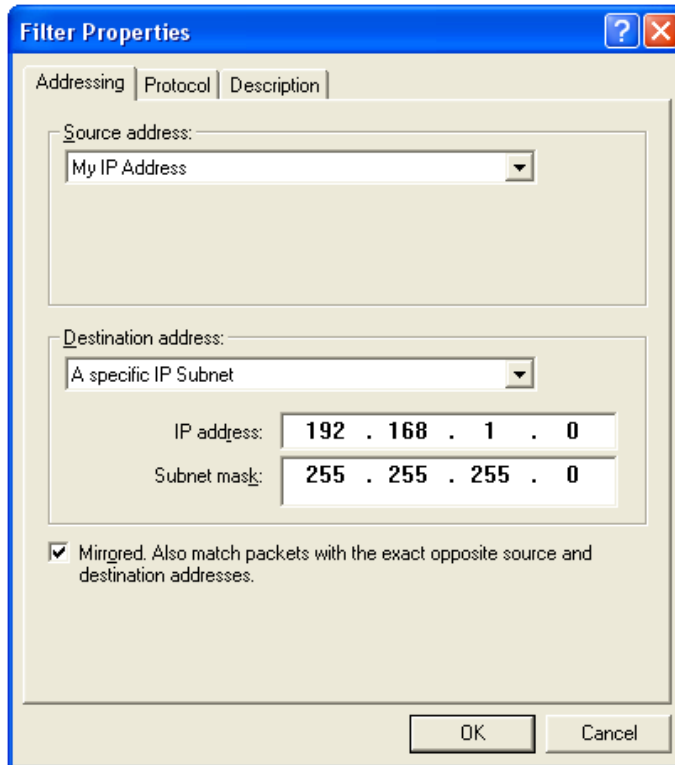


Figure 7.352. Filter Properties

- e. In the 'Source address' drop-down menu, select 'My IP Address'.
 - f. In the 'Destination address' drop-down menu, select 'A Specific IP Subnet'. In the 'IP Address' field, enter the LAN Subnet (<openrg_lan_subnet>), and in the 'Subnet mask' field enter 255.255.255.0.
 - g. Click the 'Description' tab if you would like to enter a description for your filter.
 - h. Click the 'OK' button. Click 'OK' again in the 'IP Filter List' window to save the settings.
3. Building Filter List 2 – OpenRG to Windows XP:
- a. Under the IP Filter List tab of the 'New Rule Properties' window, click the 'Add' button. The 'IP Filter List' window appears (see [Figure 7.351](#)).
 - b. Enter the name "OpenRG to Windows XP" for the filter list, deselect the 'Use Add Wizard' check box, and click the 'Add' button. The 'Filter Properties' window appears.

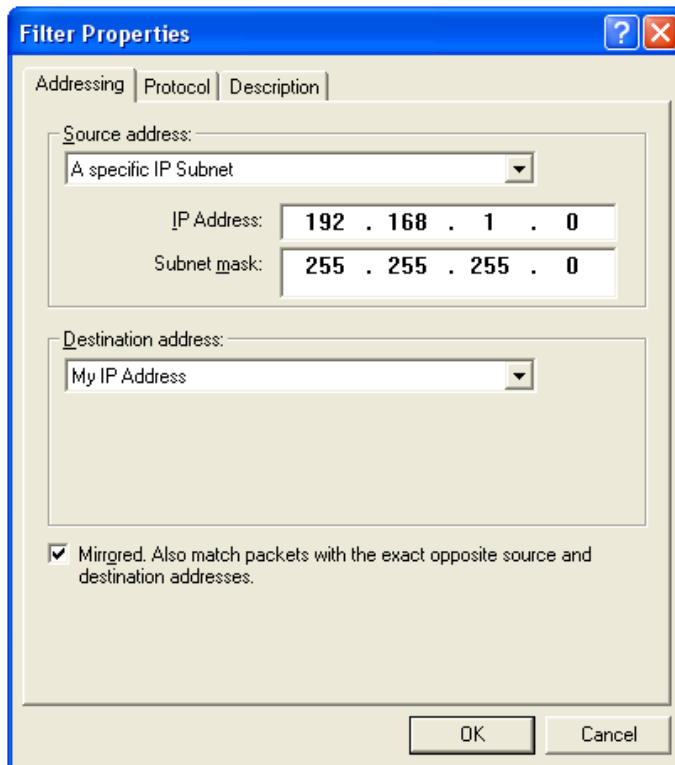


Figure 7.353. Filter Properties

- c. In the 'Source address' drop-down menu, select 'A Specific IP Subnet'. In the 'IP Address' field enter the LAN Subnet (<openrg_lan_subnet>), and in the 'Subnet mask' field enter 255.255.255.0.
 - d. In the 'Destination address' drop-down menu, select 'My IP Address'.
 - e. Click the 'Description' tab if you would like to enter a description for your filter.
 - f. Click the 'OK' button. Click 'OK' again in the 'IP Filter List' window to save the settings.
4. Configuring Individual Rule of Tunnel 1 (Windows XP to OpenRG):
 - a. Under the 'IP Filter List' tab of the 'New Rule Properties' window, select the 'Windows XP to OpenRG' radio button.

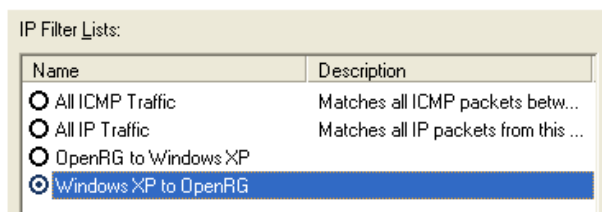


Figure 7.354. IP Filter List

- b. Click the 'Filter Action' tab.

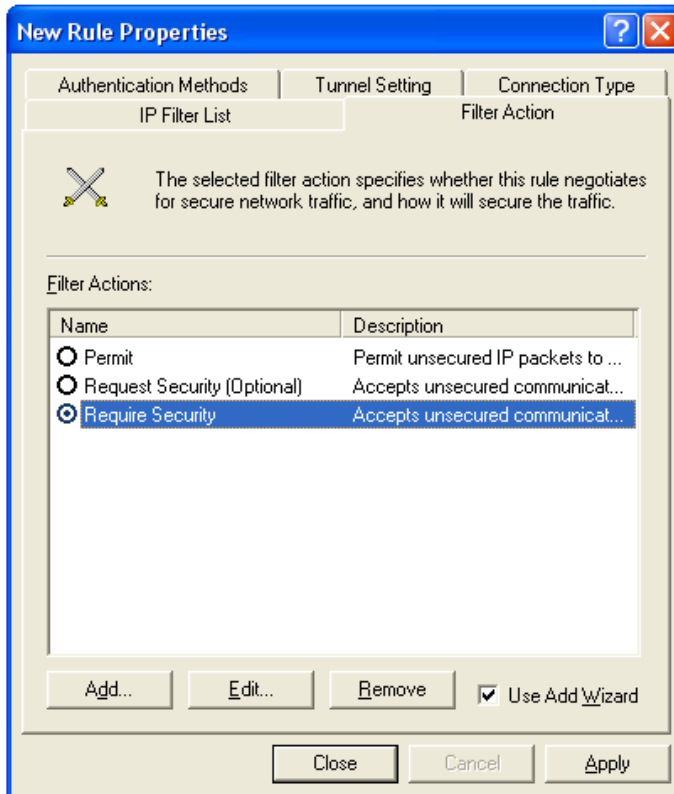


Figure 7.355. Filter Action

- c. Select the 'Require Security' radio button, and click the 'Edit' button. The 'Require Security Properties' window appears.

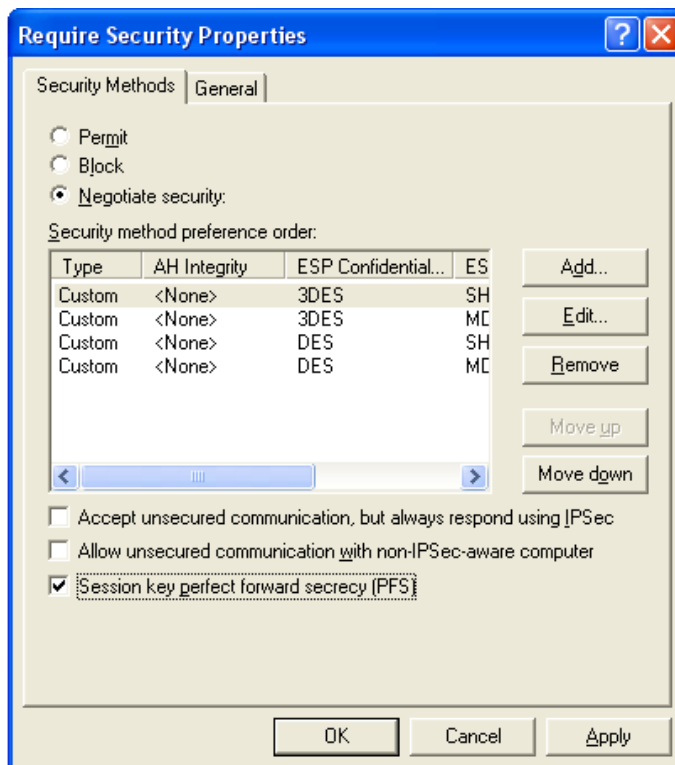


Figure 7.356. Require Security Properties

- d. Verify that the 'Negotiate security' option is enabled, and deselect the 'Accept unsecured communication, but always respond using IPsec' check box. Select the 'Session key Perfect Forward Secrecy (PFS)' (the PFS option must be enabled on OpenRG), and click the OK button.
- e. Under the 'Authentication Methods' tab, click the Edit button. The 'Edit Authentication Method Properties' window appears.

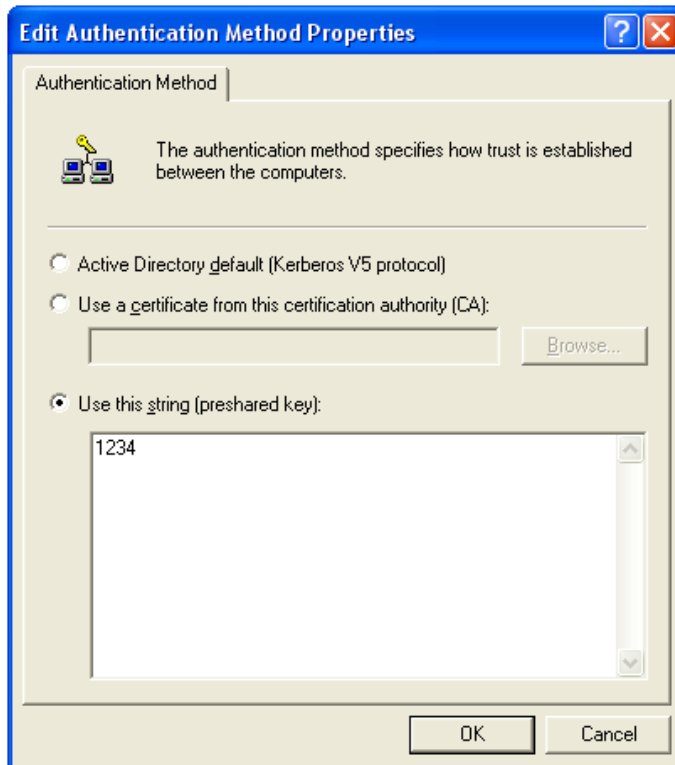


Figure 7.357. Edit Authentication Method Properties

- f. Select the 'Use this string (preshared key)' radio button, and enter a string that will be used as the key (for example, 1234). Click the 'OK' button.
- g. Under the 'Tunnel Setting' tab, select the 'The tunnel endpoint is specified by this IP Address' radio button, and enter <openrg_wan_ip>.

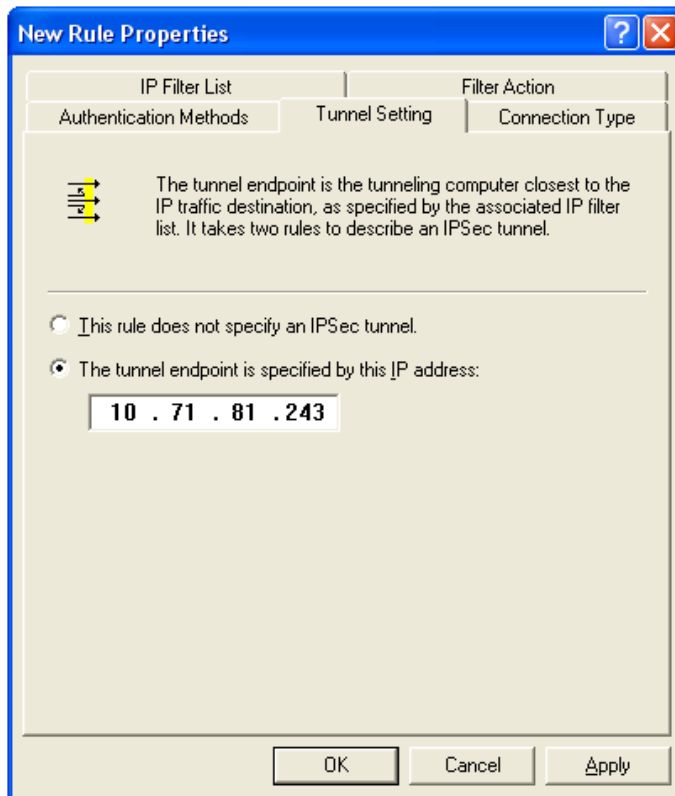


Figure 7.358. Tunnel Setting

- h. Under the 'Connection Type' tab, verify that 'All network connections' is selected.
 - i. Click the 'Apply' button and then click the 'OK' button to save this rule.
5. Configuring Individual Rule of Tunnel 2 (OpenRG to Windows XP):
- a. Under the 'IP Filter List' tab of the 'New Rule Properties' window, select the 'OpenRG to Windows XP' radio button.

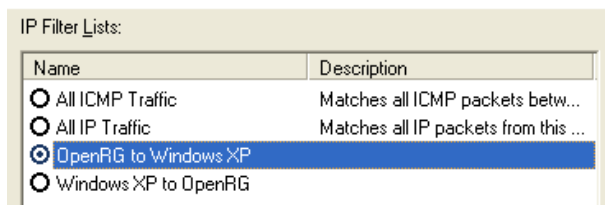


Figure 7.359. IP Filter List

- b. Click the 'Filter Action' tab (see [Figure 7.355](#)).
- c. Select the 'Require Security' radio button, and click the 'Edit' button. The 'Require Security Properties' window appears (see [Figure 7.356](#)).
- d. Verify that the 'Negotiate security' option is enabled, and deselect the 'Accept unsecured communication, but always respond using IPSec' check box. Select the

'Session key Perfect Forward Secrecy (PFS)' (the PFS option must be enabled on OpenRG), and click the OK button.

- e. Under the 'Authentication Methods' tab, click the Edit button. The 'Edit Authentication Method Properties' window appears (see [Figure 7.357](#)).
- f. Select the 'Use this string (preshared key)' radio button, and enter a string that will be used as the key (for example, 1234). Click the 'OK' button.
- g. Under the 'Tunnel Setting' tab, select the 'The tunnel endpoint is specified by this IP Address' radio button, and enter <windows_ip>.

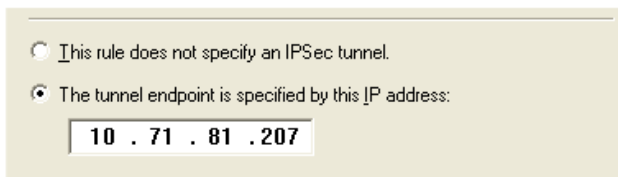


Figure 7.360. Tunnel Setting

- h. Under the 'Connection Type' tab, verify that 'All network connections' is selected.
- i. Click the 'Apply' button and then click the 'OK' button to save this rule.
- j. Back on the 'OpenRG Connection Properties' window, note that the two new rules have been added to the 'IP Security rules' list.

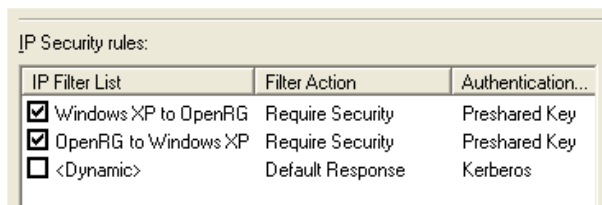


Figure 7.361. OpenRG Connection Properties

Click 'Close' to go back to the 'Local Security Settings' window (see [Figure 7.344](#)).

- 6. Assigning the New IPSec Policy: In the 'Local Security Settings' window, right-click the 'OpenRG Connection' policy, and select 'Assign'. A small green arrow will appear on the policy's folder icon and its status under the 'Policy Assigned' column will change to 'Yes'.

Name	Description	Policy Assigned
Client (Respond Only)	Communicate normally (u...	No
OpenRG Connection		Yes
Secure Server (Requir...	For all IP traffic, always r...	No
Server (Request Secu...	For all IP traffic, always r...	No

Figure 7.362. Local Security Settings

7.10.1.5. IPSec Gateway-to-Gateway Connection Scenario

Establishing an IPSec tunnel between Gateways A and B creates a transparent and secure network for clients from subnets A and B, who can communicate with each other as if they were inside the same network.

This section describes how to create a gateway to gateway IPSec tunnel with the following authentication methods:

- **Pre-shared Secret** – Developed by the VPN Consortium (VPNC). OpenRG's VPN feature is VPNC certified.
- **RSA Signature** – A method using an RSA signature that is based on OpenRG's public key.
- **Peer Authentication of Certificates** – A method using a Certificate Authority (CA).

This section describes the network configuration of both gateways, followed by the IPSec tunnel setup methods. The configurations of both gateways are identical, except for their IP addresses and the use of these addresses when creating the tunnel—the default gateway address of each gateway should be the WAN IP address of the other gateway.



Note: This section describes the configuration of Gateway A only. The same configuration must be performed on Gateway B, with the exceptions that appear in the note admonitions.

The following figure describes the IPSec tunnel setup, and contains all the IP addresses involved. Use it as a reference when configuring your gateways.

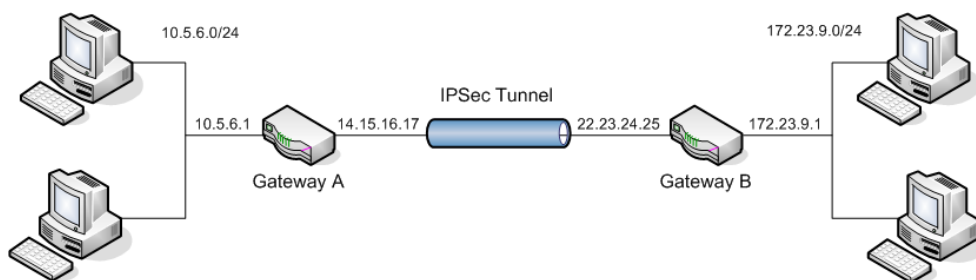


Figure 7.363. Configuration Diagram

7.10.1.5.1. Network Configuration

Before you can set up an IPSec connection, you must configure both of the gateways' LAN and WAN interface settings. This example contains specific IP addresses, which you can either use or substitute with your own.

- LAN Interface Settings

1. Under the 'System' tab, click the 'Network Connections' menu item. The 'Network Connections' screen appears.

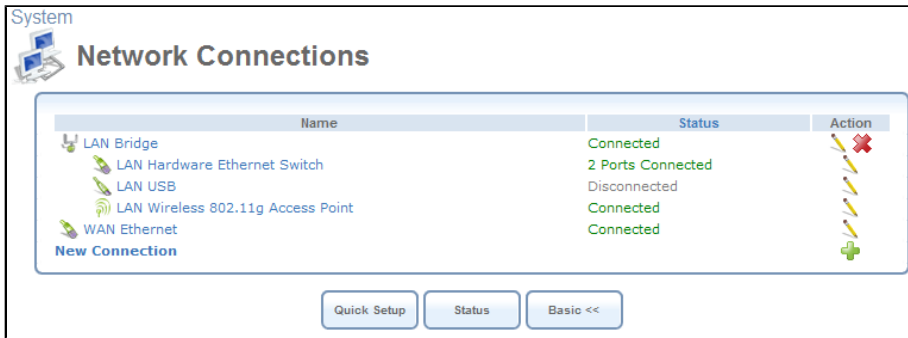


Figure 7.364. Network Connections

2. If your LAN Ethernet connection is bridged, click the 'LAN Bridge' link (as depicted in this example). Otherwise, click the 'LAN Ethernet' link (or the 'LAN Hardware Ethernet Switch' link, depending on your platform). The 'LAN Bridge Properties' screen appears.

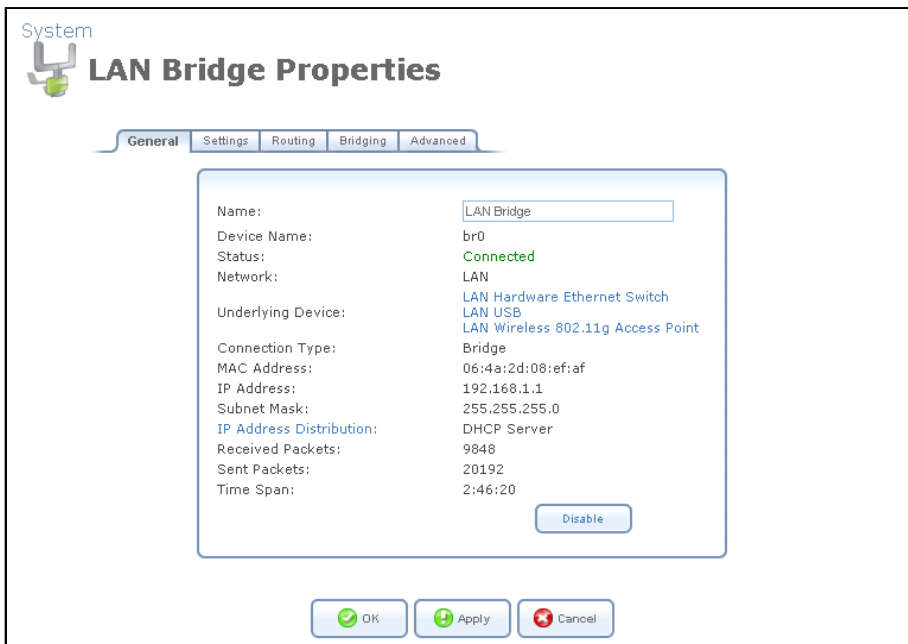


Figure 7.365. LAN Bridge Properties – General

3. Press the 'Settings' tab, and configure the following settings:

Internet Protocol	Use the Following IP Address <input type="button" value="v"/>
IP Address:	<input type="text" value="10"/> . <input type="text" value="5"/> . <input type="text" value="6"/> . <input type="text" value="1"/>
Subnet Mask:	<input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/>
DNS Server	
Primary DNS Server:	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
Secondary DNS Server:	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
IP Address Distribution	DHCP Server <input type="button" value="v"/>
Start IP Address:	<input type="text" value="10"/> . <input type="text" value="5"/> . <input type="text" value="6"/> . <input type="text" value="1"/>
End IP Address:	<input type="text" value="10"/> . <input type="text" value="5"/> . <input type="text" value="6"/> . <input type="text" value="254"/>
Subnet Mask:	<input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/>

Figure 7.366. LAN Bridge Properties – Settings

Internet Protocol Select "Use the Following IP Address"

IP Address Specify 10.5.6.1

Subnet Mask Specify 255.255.255.0

IP Address Distribution Select "DHCP Server"

Start IP Address Specify 10.5.6.1

End IP Address Specify 10.5.6.254

Subnet Mask Specify 255.255.255.0



Note: When configuring Gateway B, the IP address should be 172.23.9.1, according to the example depicted here.

4. Click 'OK' to save the settings.

- WAN Interface Settings

1. Under the 'System' tab, click the 'Network Connections' menu item. The 'Network Connections' screen appears.

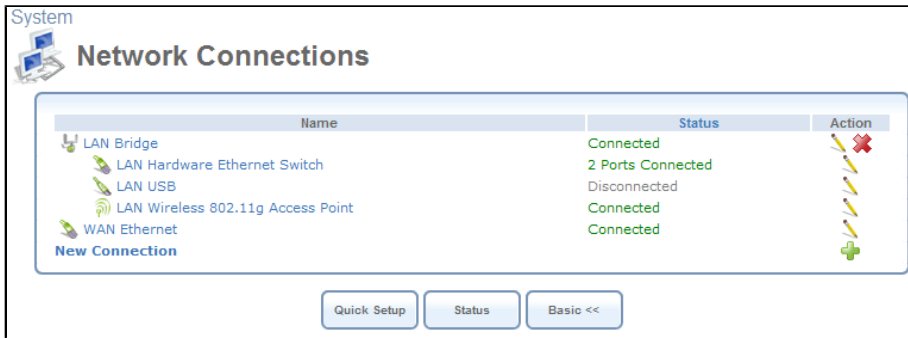


Figure 7.367. Network Connections

2. Click the 'WAN Ethernet' link, the 'WAN Ethernet Properties' screen appears.

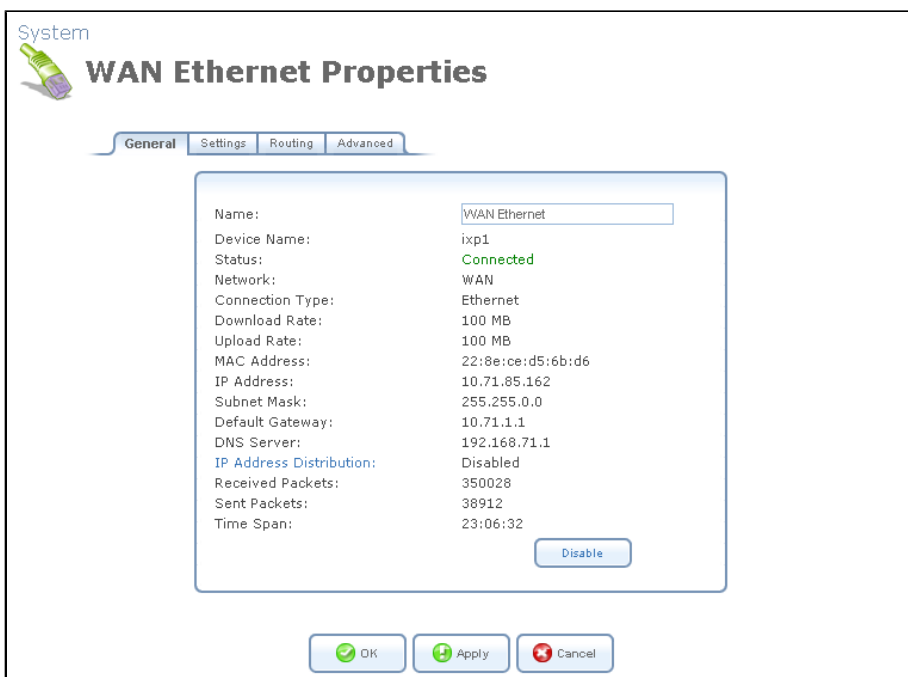


Figure 7.368. WAN Ethernet Properties – General

3. Press the 'Settings' tab, and configure the following settings:

Internet Protocol	Use the Following IP Address ▾
IP Address:	14 . 15 . 16 . 17
Subnet Mask:	255 . 0 . 0 . 0
Default Gateway:	14 . 15 . 16 . 1

Figure 7.369. WAN Ethernet Properties – Settings

Internet Protocol Select "Use the Following IP Address"

IP Address Specify 14.15.16.17

Subnet Mask Specify the appropriate subnet mask, i.e 255.0.0.0

Default Gateway Specify the appropriate Default Gateway in order to enable IP routing, i.e 14.15.16.1



Note: When configuring Gateway B, the IP address should be 22.23.24.25, and the default gateway 22.23.24.1, according to the example depicted here.

4. Click 'OK' to save the settings.

7.10.1.5.2. Gateway-to-Gateway with Pre-shared Secrets

A typical gateway-to-gateway VPN uses a pre-shared secret for authentication. Gateway A connects its internal LAN 10.5.6.0/24 to the Internet. Gateway A's LAN interface has the address 10.5.6.1, and its WAN (Internet) interface has the address 14.15.16.17. Gateway B connects the internal LAN 172.23.9.0/24 to the Internet. Gateway B's WAN (Internet) interface has the address 22.23.24.25. The Internet Key Exchange (IKE) Phase 1 parameters used are:

- Main mode
- 3DES (Triple DES)
- SHA-1
- MODP group 2 (1024 bits)
- Pre-shared secret of "hr5x"
- SA lifetime of 28800 seconds (eight hours) with no Kbytes re-keying

The IKE Phase 2 parameters used are:

- 3DES (Triple DES)
- SHA-1
- ESP tunnel mode
- MODP group 2 (1024 bits)
- Perfect forward secrecy for re-keying
- SA lifetime of 3600 seconds (one hour) with no Kbytes re-keying
- Selectors for all IP protocols, all ports, between 10.5.6.0/24 and 172.23.9.0/24, using IPv4 subnets

To set up Gateway A for this scenario, follow these steps:

1. Under the 'System' tab, click the 'Network Connections' menu item. The 'Network Connections' screen appears.

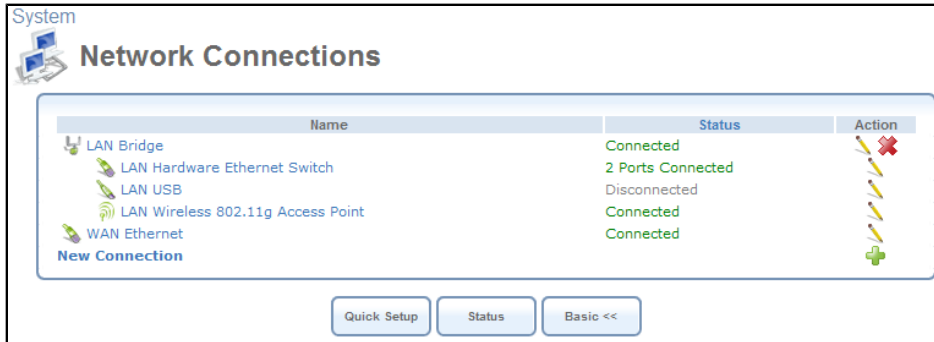


Figure 7.370. Network Connections

2. Click the 'New Connection' link. The 'Connection Wizard' screen appears.

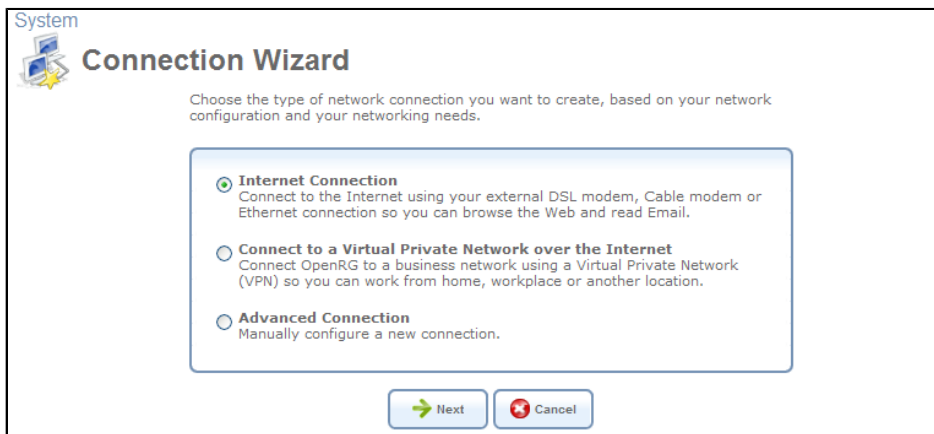


Figure 7.371. Connection Wizard

3. Select the 'Connect to a Virtual Private Network over the Internet' radio button and click 'Next'. The 'Connect to a Virtual Private Network over the Internet' screen appears.

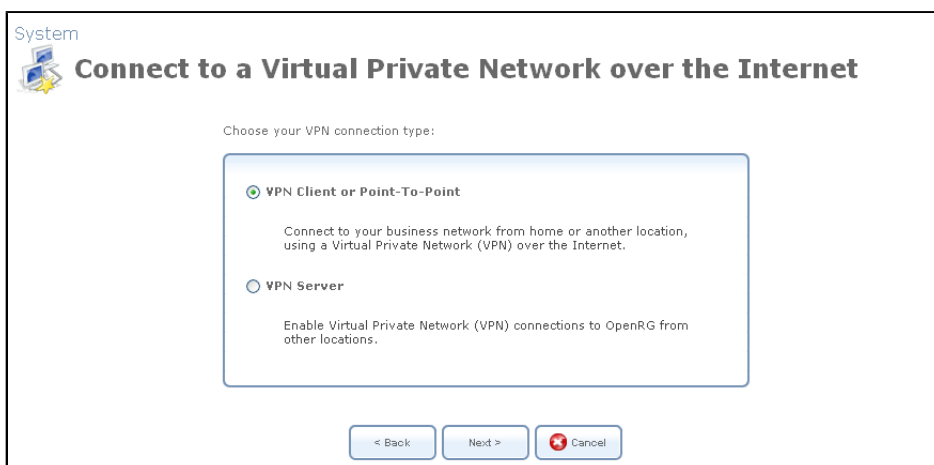


Figure 7.372. Connect to a Virtual Private Network over the Internet

- Select the 'VPN Client or Point-To-Point' radio button and click 'Next'. The 'VPN Client or Point-To-Point' screen appears.

Figure 7.373. VPN Client or Point-To-Point

- Select the 'Internet Protocol Security (IPSec)' radio button and click 'Next'. The 'Internet Protocol Security (IPSec)' screen appears.

Figure 7.374. Internet Protocol Security (IPSec)

- Specify the following parameters, as depicted in [Figure 7.375](#).

Host Name or IP Address of Destination Gateway Specify 22.23.24.25

Remote IP Select "IP Subnet"

Remote Subnet IP Address Specify 172.23.9.0

Remote Subnet Mask Specify 255.255.255.0

Shared Secret Specify "hr5x"

Configure your IPsec connection properties:

Host Name or IP Address of Destination Gateway:	<input type="text" value="22.23.24.25"/>
Remote IP:	<input type="text" value="IP Subnet"/>
Remote Subnet IP Address:	<input type="text" value="172"/> . <input type="text" value="23"/> . <input type="text" value="9"/> . <input type="text" value="0"/>
Remote Subnet Mask:	<input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/>
Shared Secret:	<input type="text" value="hr5x"/>

Figure 7.375. Internet Protocol Security (IPSec)



Note: When configuring Gateway B, the IP Address of Destination Gateway should be 14.15.16.17, and the Remote Subnet IP Address should be 10.5.6.0, according to the example depicted here.

- Click 'Next', the 'Connection Summary' screen appears.

System

Connection Summary

You have successfully completed the steps needed to create the following connection:

- IPSec connection with 22.23.24.25

Edit the Newly Created Connection

Press **Finish** to create the connection.

< Back
Finish
Cancel

Figure 7.376. Connection Summary

- Select the 'Edit the Newly Created Connection' check box, and click 'Finish'. The 'VPN IPsec Properties' screen appears, displaying the 'General' tab.

VPN

VPN IPsec Properties

IPsec | SSL-VPN | PPTP Server | L2TP Server

General
Settings
Routing
IPsec

Name:	<input type="text" value="VPN IPsec"/>
Device Name:	ips0
Status:	Waiting for Connection
Network:	WAN
Connection Type:	VPN IPsec
Download Rate:	100 MB
Upload Rate:	100 MB
IP Address:	10.71.85.162
Subnet Mask:	255.255.0.0
Remote Tunnel Endpoint Address:	www.ter.com
Local Subnet:	192.168.1.0/255.255.255.0

OK
Apply
Cancel

Figure 7.377. VPN IPsec Properties – General

9. Click the 'IPSec' tab, and configure the following settings:

- Deselect the 'Compress' check box.
- Under 'Hash Algorithm', deselect the 'Allow Peers to Use MD5' check box.
- Under 'Group Description Attribute', deselect the 'DH Group 5 (1536 bit)' check box.
- Under 'Encryption Algorithm', deselect the 'Allow AH Protocol (No Encryption)' check box.

10. Click 'OK' to save the settings.

Perform the same procedure on Gateway B with its respective parameters. When done, the IPSec connection's status should change to "Connected".








Name	Status	Action
LAN Bridge	Connected	 
LAN Hardware Ethernet Switch	2 Ports Connected	
LAN USB	Disconnected	
LAN Wireless 802.11g Access Point	Device missing	
WAN Ethernet	Connected	
VPN IPSec	Connected	 
New Connection		

Figure 7.378. Connected VPN IPSec Connection

7.10.1.5.3. Gateway-to-Gateway with an RSA Signature

The RSA signature, which is part of the RSA encryption mechanism, is an additional method available on OpenRG for providing peer authentication in a VPN IPSec connection. The RSA signature can be created in OpenRG on the basis of its public key. When using this method, the two gateways must be configured with each other's RSA signature, as further explained in this section.

To enable the gateway-to-gateway VPN IPSec connection using the RSA signature, perform the following:

1. Create a VPN IPSec connection on each gateway as described in [Section 7.10.1.5.2](#).
2. In OpenRG A, go to the 'Advanced' screen, and click the 'IPSec' icon. The 'Internet Protocol Security (IPSec)' screen appears.



Figure 7.379. Internet Protocol Security (IPSec)

3. Click the 'Settings' button. The 'Internet Protocol Security (IPSec) Settings' screen appears, displaying OpenRG's public key.

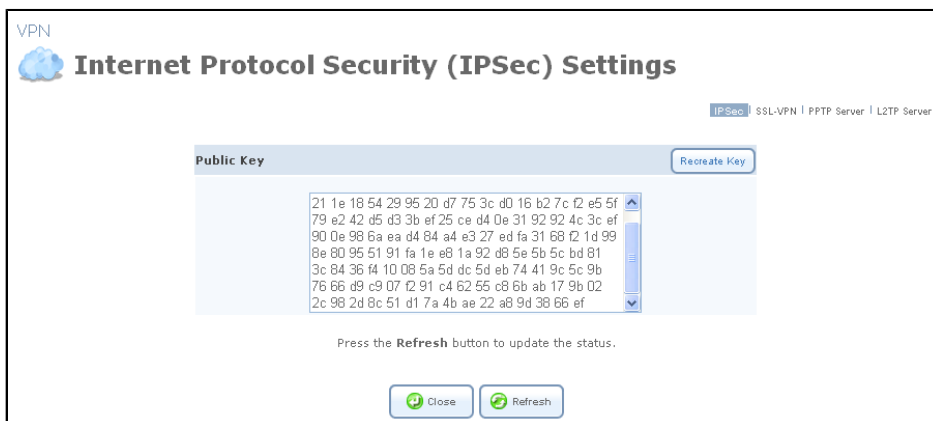



Figure 7.380. Internet Protocol Security (IPSec) Settings

4. Copy the public key and paste it into a text editor.
5. Remove all spaces from the public key so that it will appear as one string.
6. In OpenRG **B**, click the 'VPN' menu item under the 'Services' tab. The 'Internet Protocol Security (IPSec)' screen appears, displaying the VPN IPSec connection you have created (see [Figure 7.379](#)).
7. Click the connection's  action icon, and select the 'IPSec' sub-tab of the 'VPN IPSec Properties' screen that appears (see [Figure 7.377](#)).
8. From the 'Peer Authentication' drop-down menu, select the 'RSA Signature' option. The screen refreshes, displaying the 'RSA Signature' text field.
9. In the text field, type **0x** and paste the public key string from the text editor.

10. Repeat the same procedure for configuring OpenRG **A** with the RSA signature of OpenRG **B**. When done, the IPsec connection's status on both gateways should change to 'Connected'.

7.10.1.5.4. Gateway-to-Gateway with Certificate-based Peer Authentication

An additional authentication method for a gateway-to-gateway VPN is peer authentication of certificates. Authentication is performed when each gateway presents a certificate, signed by a mutually agreed upon Certificate Authority (CA), to the other gateway.

For testing purposes, Linux provides a mechanism for creating self-signed certificates, thus eliminating the need to acquire them from the CA. This section provides a description for this procedure, after which you will be able to use these certificates for authentication of the gateway-to-gateway VPN connection.

To create a self-signed certificate, perform the following:

1. Running as root, install the OpenSSL Debian package:

```
# apt-get install openssl
```

2. Switch back to a regular user, and create a directory for the certificates:

```
$ cd ~  
$ mkdir cert_create  
$ cd cert_create/
```

3. Use the Linux 'CA.sh' utility. Note that only the required fields are listed below. For the rest, you may simply press Enter.

```
$ /usr/lib/ssl/misc/CA.sh -newca  
Enter PEM pass phrase: <enter a password>  
Common Name: <enter your CA name>  
Enter pass phrase for ./demoCA/private/./cakey.pem: <enter a password>
```

For more information about this script, run 'man CA.pl' (CA.pl and CA.sh are the same).

4. Copy the certificates from the **/demoCA** directory under which they were created, providing them with your CA name.

```
$ cp demoCA/cacert.pem <your CA name>_cacert.pem  
$ cp demoCA/careq.pem <your CA name>_careq.pem
```

5. Load the new certificates to both gateways:
 - a. Browse to the 'Advanced' tab and click the 'Certificates' icon.
 - b. Select the 'CA's' sub-tab and click 'Upload Certificate'. The 'Load CA's Certificate' screen appears.
 - c. Browse for the location of the certificate, which is **~/cert_create/<your CA name>_cacert.pem**, and click 'Upload'.

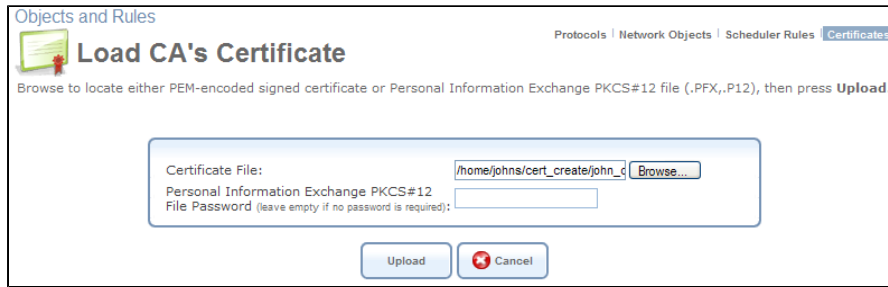


Figure 7.381. Load CA's Certificate

6. Generate a certificate request from both gateways:
 - a. Browse to the 'Advanced' tab and click the 'Certificates' icon.
 - b. In the 'OpenRG's Local' sub-tab, click 'Create Certificate Request'. The 'Create X509 Request' screen appears.
 - c. In the 'Certificate Name' field, enter "OpenRG-1" (and "OpenRG-2" on the other gateway, respectively).

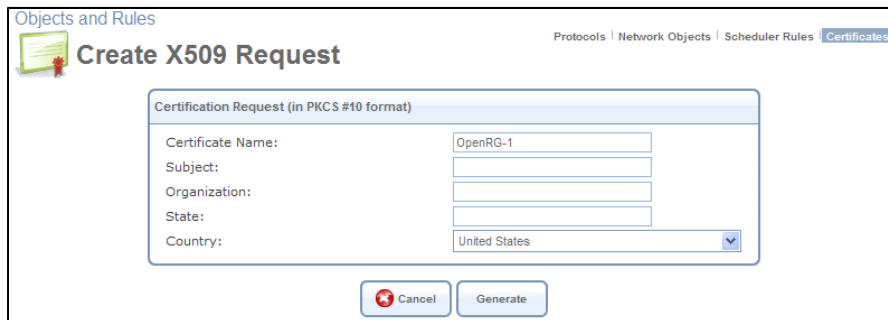


Figure 7.382. Create X509 Request

- d. Click 'Generate' and then 'Refresh'. The 'New X509 Request' screen appears.

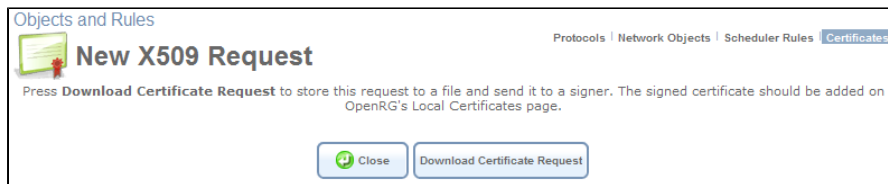



Figure 7.383. New X509 Request

- e. Click 'Download Certificate Request', and save the file under `~/cert_create/OpenRG-1/2_OpenRG.csr`.

 Note: Do not delete the empty certificate that now appears under the 'OpenRG's Local' sub-tab, as this is the request itself. If you delete it, the certificate will not be accepted by OpenRG.

7. Sign the certificate request using the 'CA.sh' script on both gateways:

```

$ mv <OpenRG-1>.csr newreq.pem
$ /usr/lib/ssl/misc/CA.sh -sign
  Enter pass phrase for ./demoCA/private/akey.pem: <enter a password>
  Sign the certificate? [y/n]: <choose y>
  1 out of 1 certificate requests certified, commit? [y/n] <choose y>
$ mv newcert.pem <OpenRG-1>_newcert.pem
$ mv newreq.pem <OpenRG-1>_newreq.pem

<Repeat the above for OpenRG-2>

```

8. Load the certificates to both gateways:

- a. Browse to the 'Advanced' tab and click the 'Certificates' icon.
- b. In the 'OpenRG's Local' sub-tab, click 'Upload Certificate'. The 'Load OpenRG's Local Certificate' screen appears.
- c. Browse to the location of the certificate, which is `~/cert_create/<OpenRG-1/2>_newcert.pem`, and click 'Upload'.

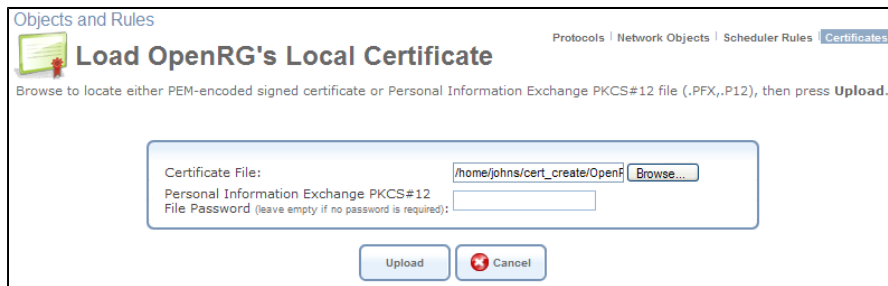


Figure 7.384. Load OpenRG's Local Certificate

To authenticate the VPN connection with the created certificates, perform the following:

1. Click the 'VPN IPsec' link in the 'Network Connections' screen, and then click the 'IPsec' sub-tab.
2. In the 'IPsec Automatic Phase 1' section, in the 'Peer Authentication' drop-down menu, select "Certificate". The screen refreshes, providing additional settings.

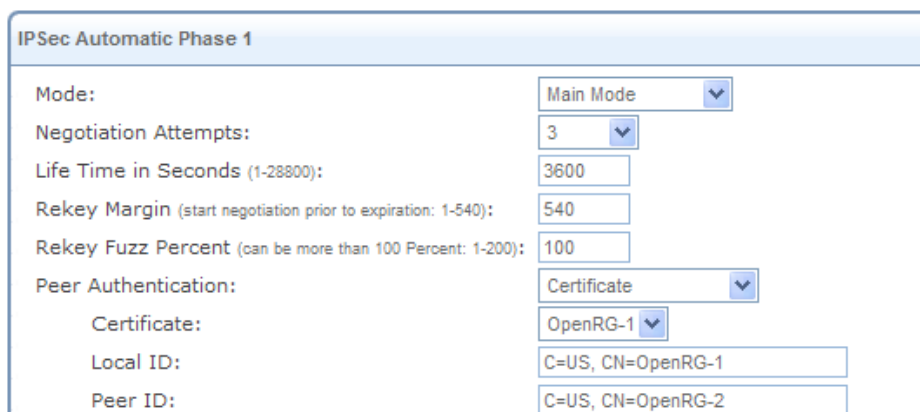


Figure 7.385. VPN IPsec Properties

3. In the 'Certificate' drop-down menu, select Gateway A's newly added certificate.

4. In the 'Local ID' field, enter Gateway A's certificate details. You can copy these details from the 'Certificates' screen under the 'Advanced' tab. Click the certificate and copy the details from the subject field, for example "C=US, CN=OpenRG-1".
5. In the 'Peer ID' field, enter Gateway B's certificate details, for example "C=US, CN=OpenRG-2".
6. Click 'OK' to save the settings.

Perform the same procedure on Gateway B with its respective parameters. When done, the IPsec connection's status should change to "Connected".














Name	Status	Action
LAN Bridge	Connected	 
LAN Hardware Ethernet Switch	2 Ports Connected	 
LAN USB	Disconnected	 
LAN Wireless 802.11g Access Point	Device missing	 
WAN Ethernet	Connected	 
VPN IPsec	Connected	 
New Connection		

Figure 7.386. Connected VPN IPsec Connection

7.10.2. Secure Socket Layer 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 OpenRG 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 OpenRG will be routed to the "SSL VPN Portal". This portal will present them each with their list of applications.

 Note: The only requirement for the client computer is the availability of Java Runtime Environment (JRE), which is mandatory for using this feature. Use the "Click here" link at the bottom of the SSL VPN portal screen to install this environment, or visit <http://www.sun.com>.

7.10.2.1. Using SSL VPN – the Remote Desktop Example

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

7.10.2.1.1. Creating a Global Shortcut

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. The 'SSL VPN' screen appears.

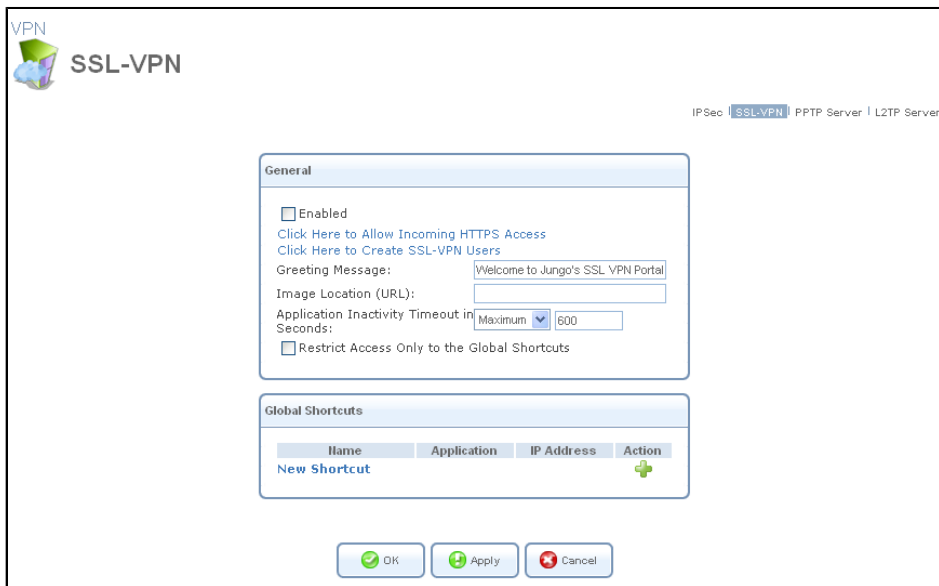


Figure 7.387. SSL VPN

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

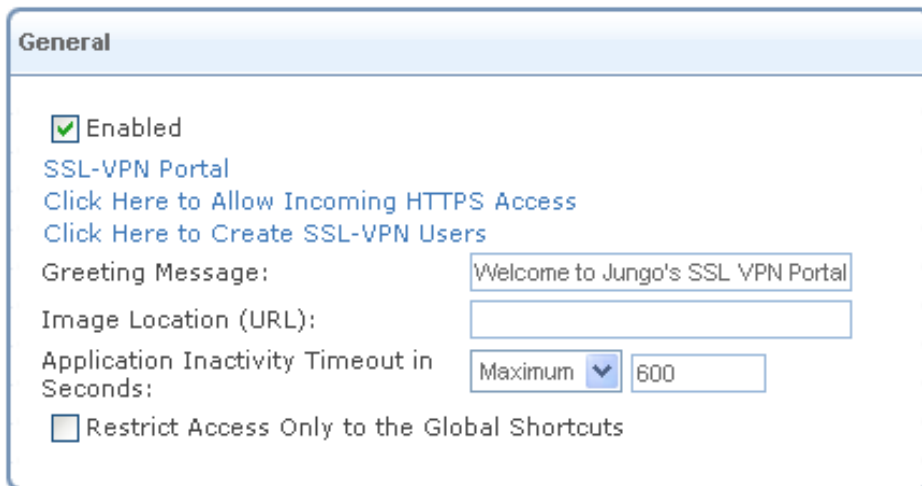


Figure 7.388. Enabled SSL VPN

This link opens the SSL-VPN portal that remote users will access when browsing to OpenRG, as described in [Section 7.10.2.3](#).

3. Click the 'Click Here to Allow Incoming HTTPS Access' link. The 'Remote Administration' screen appears (for more information, refer to [Section 8.7.3](#)). In the 'Allow Incoming WAN Access to Web-Management' section, select both HTTPS port 443 and 8443, and click 'OK'.

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)

Figure 7.389. Remote Administration Ports

- 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. Refer to [Section 8.3](#) to learn how to define and configure users. You can specify a group of users in the same manner.

System **Users**

Full Name	User Name	Permissions	Action
Administrator	admin	Administrator Permissions Wireless Permissions	
John Smith	john	Remote Access by SSL-VPN Microsoft File and Printer Sharing Access Remote Access by SSL-VPN	
New User			

Name	Description	Members	Action
Users		John Smith	
New Group			

Close

Figure 7.390. New User

Click 'Close' when done.

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

VPN **Shortcut Wizard** IPSec | **SSL-VPN** | PPTP Server | L2TP Server

Choose the host to connect to:

From a List
Select a host from a list of known hosts (DHCP leases).

Manual Selection
Manually enter the IP address of the host.

Figure 7.391. New Shortcut

- Choose whether to select a host from a given list, comprised of DHCP leases that are known to OpenRG, 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'.

Figure 7.392. Choose Host from List

The next wizard screen appears, either with the IP address of a selected host, or without an IP address for manual selection.

Figure 7.393. Select and Configure an Application

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

Figure 7.394. RDP Parameters

- In this screen, perform the following:

- a. Enter a name for the shortcut.
- b. Enter the IP address of the LAN computer on which the RDP will be performed.
- c. 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.
- d. 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.
- e. Select the size of the screen in which the remote desktop application will be displayed.

Click 'Next'. The 'Shortcut Summary' screen appears.

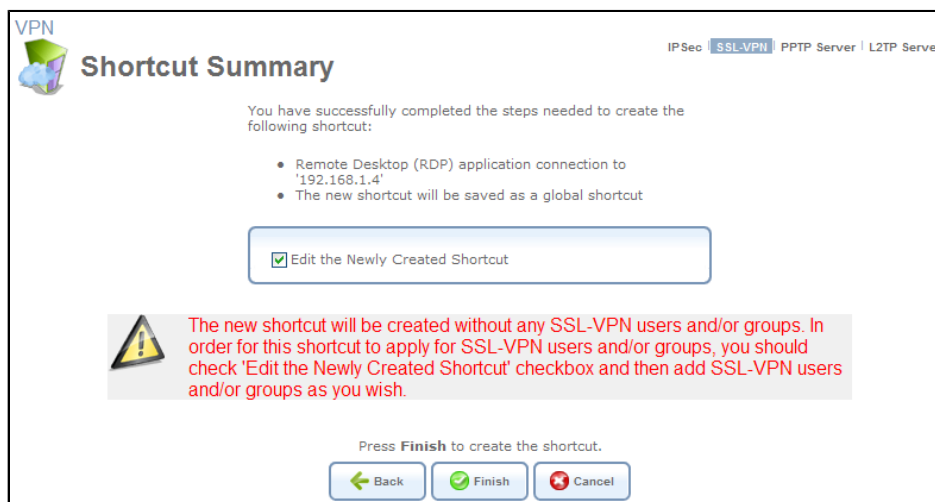


Figure 7.395. Shortcut Summary

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.

Figure 7.396. Edit Shortcut

- 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.

Figure 7.397. User

- Click 'OK'. The new user is added to the 'Users' section in the 'Edit Shortcut' screen.

Name	Action
John Smith	
New User	

Figure 7.398. Associated User

- 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.

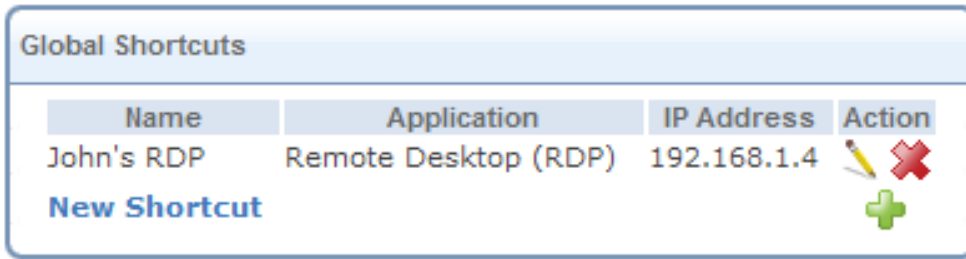


Figure 7.399. Global Shortcuts

7.10.2.1.2. Launching the Application

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

1. Browse to OpenRG from a remote computer by typing **https://<OpenRG's Internet address>** (OpenRG's 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.

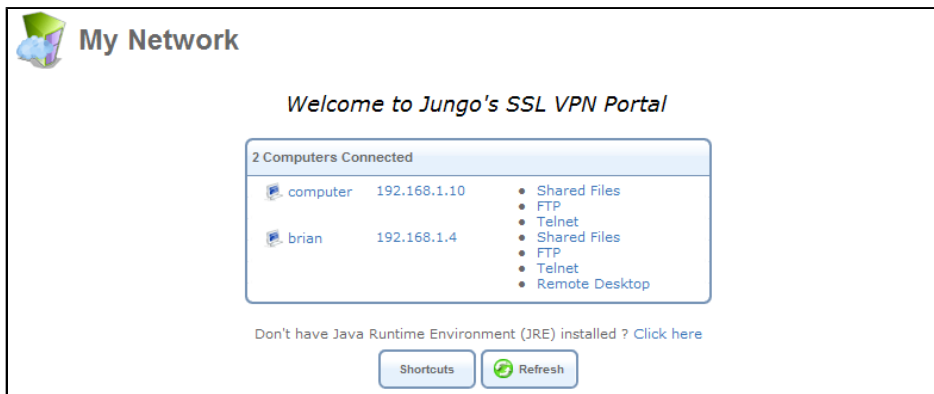


Figure 7.400. SSL VPN Portal

3. Click the 'Shortcuts' button. The 'Shortcuts' screen appears, displaying shortcuts to the available applications.

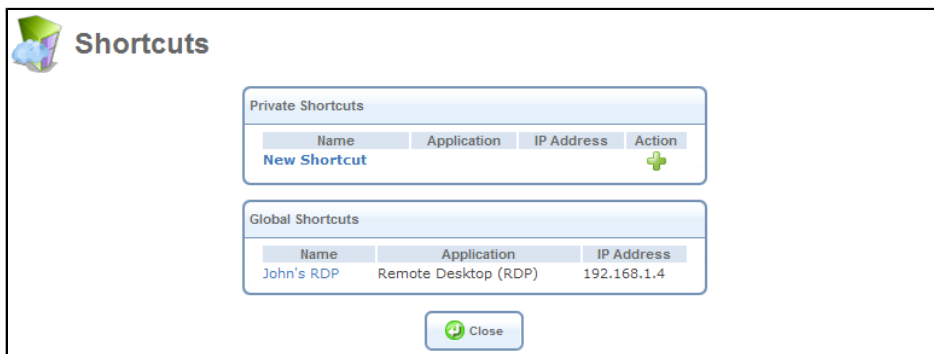


Figure 7.401. Shortcuts

4. 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.

7.10.2.2. Using Other Applications over SSL VPN

OpenRG provides the following popular applications that remote users can use to access the home network in order to perform various tasks. To set up an application, follow the remote desktop example described in the previous section. The only difference between the setups of the applications is in the parameters defined in the 'Shortcut Wizard' screen, as described in the following sections.

7.10.2.2.1. Web-based CIFS

This option enables the remote user to share files with a computer inside OpenRG's LAN using Jungo's Web-based Common Internet File System (Web-based CIFS). File sharing is performed from within the WBM, which displays the LAN computer's file system, and enables a vast set of actions described later in this section. In addition, this method does not require installing JRE, since no third-party software is used. In the 'Shortcut Wizard' screen, configure the following parameters.

Figure 7.402. Web-based CIFS Parameters

Name Enter a name for this shortcut.

IP Address Enter the IP address of the LAN computer on which to perform the application.

Specify Login Information If the LAN computer requires a login, specify the following parameters to auto-login when launching the application:

User Name The user name with which to login.

Password The password with which to login.

Share Specify the name of the share directory on which to perform the application.

Show Hidden Files Select this check box to allow showing of hidden files.

Once you configure a shortcut to Web-based CIFS and associate it with a user (or group), you can use the application when logged into the SSL VPN portal as that user, by clicking the shortcut link that appears in the 'Shortcuts' screen.

Global Shortcuts		
Name	Application	IP Address
My WB CIFS	Web Based CIFS	192.168.1.4

Figure 7.403. Shortcut to Web-based CIFS

If you had not specified a share directory name when configuring the shortcut, the link will lead you to the base directory of the host with the specified IP address.

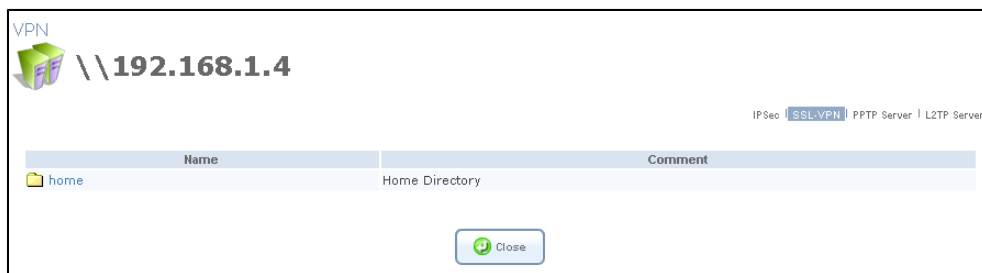


Figure 7.404. Web-based CIFS Host

If you had specified a share directory name when configuring the shortcut (in this example —"home"), the link will lead you to the share directory on the specified host.



Figure 7.405. Web-based CIFS Share

The directory content is displayed, with the file name, size, last modification and actions you may perform on the file. You can browse the directory contents and sort the columns according to the file name, size or modification date. The action icons for each file and directory allow you to perform the following:

- Download



Note: Directories are downloaded as tarball archives (in ***.tar** format).

- Rename

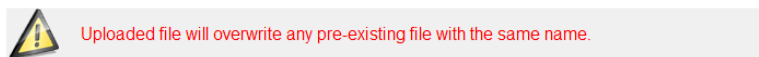
- Copy to Clipboard
- Remove

You can perform additional actions using the drop-down menu.



Figure 7.406. Web-based CIFS Actions


- **Upload a File** Select this option to upload a file to the share. The screen refreshes.



The form contains a dropdown menu labeled 'Upload a File', an empty text input field, a 'Browse...' button, and an 'Upload' button.

Figure 7.407. Upload a File

Enter the location of the file to upload, or click the 'Browse' button to browse for the file. Click the 'Upload' button to upload the file.

- **Upload a Directory** You can also upload an entire directory of files, by performing the following:
 1. Create a tarball archive out of the target directory.
 2. Enter the location of the archive, or click the 'Browse' button to browse to its location.
 3. Click the 'Upload' button to upload the archive.
- **Create a new Directory** You can create a new directory by simply typing its name and clicking the 'Go' button.
- **Paste from Clipboard** This option appears only after using the 'Copy to Clipboard' option ( action icon) to copy a directory or file from one directory to another.

7.10.2.2.2. CIFS

This option enables the remote user to share files with a computer inside OpenRG's LAN using the Common Internet File System (CIFS). The protocol allows to manipulate files on a network

computer just as if they were on the remote computer. Operations such as read, write, create, delete, and rename are all supported. In the 'Shortcut Wizard' screen, configure the following parameters.

Figure 7.408. CIFS Parameters

Name Enter a name for this shortcut.

IP Address Enter the IP address of the LAN computer on which to perform the application.

Specify Login Information If the LAN computer requires a login, specify the following parameters to auto-login when launching the application:

User Name The user name with which to login.

Password The password with which to login.

Initial Directory Specify the root directory on which to perform the application. For example, A/, C:\Program Files, etc.

Once you configure a shortcut to CIFS and associate it with a user (or group), you can use the application when logged into the SSL VPN portal as that user, by clicking the shortcut link that appears in the 'Shortcuts' screen.

Global Shortcuts		
Name	Application	IP Address
My CIFS	CIFS	192.168.1.4

Figure 7.409. Shortcut to CIFS

7.10.2.2.3. VNC

This option enables the remote user to connect and control a computer inside OpenRG's LAN using the Virtual Network Connection (VNC) application (similar to RDP). In the 'Shortcut Wizard' screen, configure the following parameters.

Application: VNC

Name:

IP Address: 0.0.0.0

Override Default Port

Specify Login Information

Password:

Figure 7.410. VNC Parameters

Name Enter a name for this shortcut.

IP Address Enter the IP address of the LAN computer on which to perform the application.

Override Default Port Select this 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.

Specify Login Information If the LAN computer requires a login, specify the following parameter to auto-login when launching the application:

Password The password with which to login.

Once you configure a shortcut to VNC and associate it with a user (or group), you can use the application when logged into the SSL VPN portal as that user, by clicking the shortcut link that appears in the 'Shortcuts' screen.

Global Shortcuts		
Name	Application	IP Address
My VNC	VNC	192.168.1.4

Figure 7.411. Shortcut to VNC

7.10.2.2.4. FTP

This option enables the remote user to transfer files between the remote computer and a computer inside OpenRG's LAN using the File Transfer Protocol (FTP) application. Note that an FTP server must be installed on the LAN computer. In the 'Shortcut Wizard' screen, configure the following parameters.

Figure 7.412. FTP Parameters

Name Enter a name for this shortcut.

IP Address Enter the IP address of the LAN computer on which to perform the application.

Override Default Port Select this 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.

Specify Login Information If the LAN computer requires a login, specify the following parameters to auto-login when launching the application:

User Name The user name with which to login.

Password The password with which to login.

Initial Directory Specify the root directory on which to perform the application. For example, A/, C:\Program Files, etc.

List Command Select the FTP command that determines the list of files and their properties available for FTP. You should only change this option if the LAN computer does not support the default "LIST" command.

Once you configure a shortcut to FTP and associate it with a user (or group), you can use the application when logged into the SSL VPN portal as that user, by clicking the shortcut link that appears in the 'Shortcuts' screen.

Global Shortcuts		
Name	Application	IP Address
My FTP	FTP	192.168.1.4

Figure 7.413. Shortcut to FTP

7.10.2.2.5. Telnet

This option enables the user to connect and perform tasks on a computer inside OpenRG's LAN with the Telnet application. In the 'Shortcut Wizard' screen, configure the following parameters.

Application:

Name:

IP Address: ...

Figure 7.414. Telnet Parameters

Name Enter a name for this shortcut.

IP Address Enter the IP address of the LAN computer on which to perform the application.

Once you configure a shortcut to Telnet and associate it with a user (or group), you can use the application when logged into the SSL VPN portal as that user, by clicking the shortcut link that appears in the 'Shortcuts' screen.

Name	Application	IP Address
My Telnet	Telnet	192.168.1.4

Figure 7.415. Shortcut to Telnet

7.10.2.3. Accessing and Using the SSL VPN Portal

The SSL VPN portal is accessible from within OpenRG for administration purposes, by clicking the 'SSL-VPN Portal' link in the 'SSL-VPN' screen (see [Figure 7.387](#)).

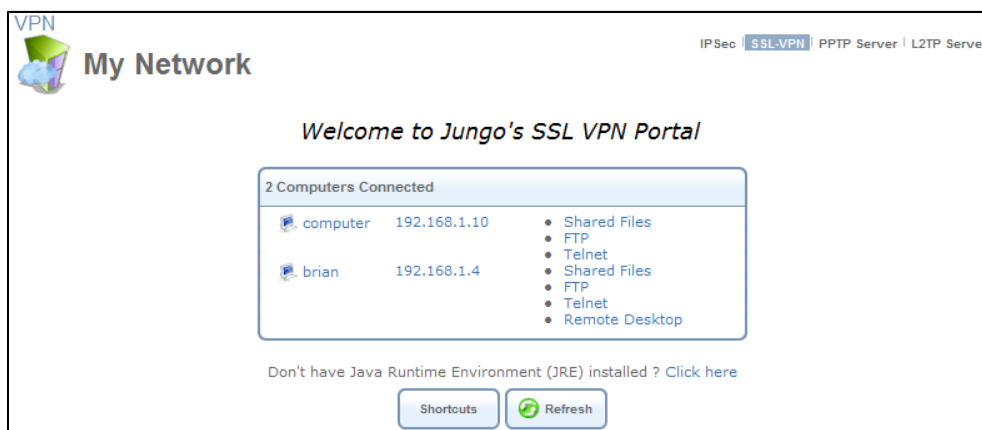


Figure 7.416. SSL VPN Portal Viewed from OpenRG

However, its purpose is to serve as an administrative portal for remote users who log into OpenRG from the Internet via HTTPS. To log in as a remote user, browse to OpenRG from a remote computer by typing **https://<OpenRG's Internet address>** (OpenRG's Internet address can be found under the 'Internet Connection' tab). For example, **https://10.71.86.21**. You will be required to provide the login details of the remote user with which you would like to connect.

The initial SSL VPN screen refreshes as OpenRG detects the open ports of each host, displaying links to applications (services) associated with these ports. This auto-detection utility is available in addition to the global shortcuts mechanism.

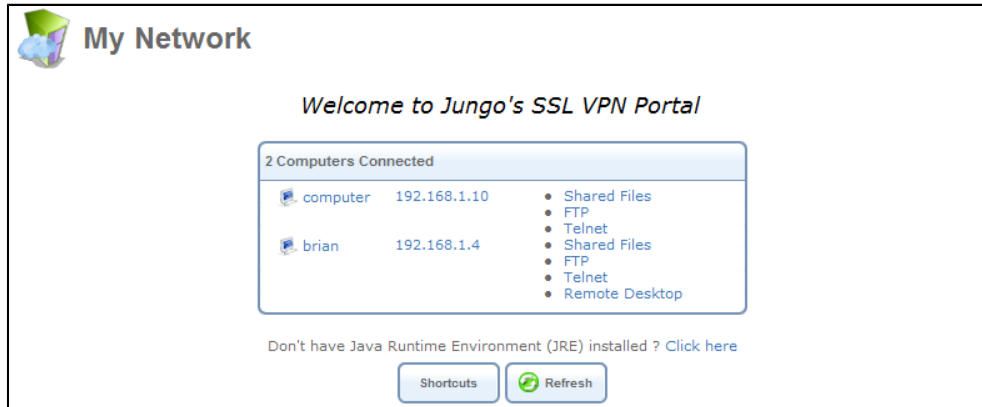


Figure 7.417. SSL VPN Portal Viewed from the Internet

Click a host name or IP address to view its information.

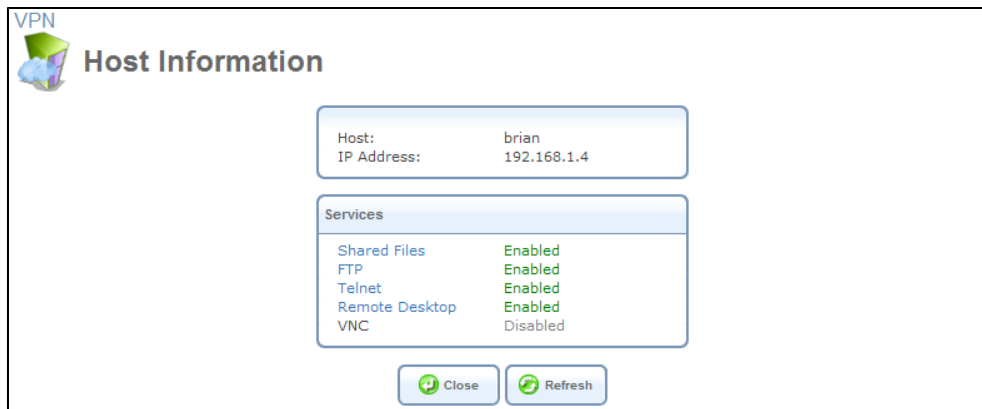



Figure 7.418. Host Information

When clicking an application link in the 'Services' section, OpenRG will attempt to use the login details of the logged-in user (in case the application requires a username and password).

 **Note:** All available applications require the Java Runtime Environment (JRE) to be available on the remote computer. Use the "Click here" link at the bottom of the SSL VPN portal screen to install this environment.

Click 'Close' to return to the SSL VPN portal.

Global shortcuts are predefined with all the necessary parameters (including login details where required) to ensure a reliable application launch. Click the 'Shortcuts' button to view the available global shortcuts.

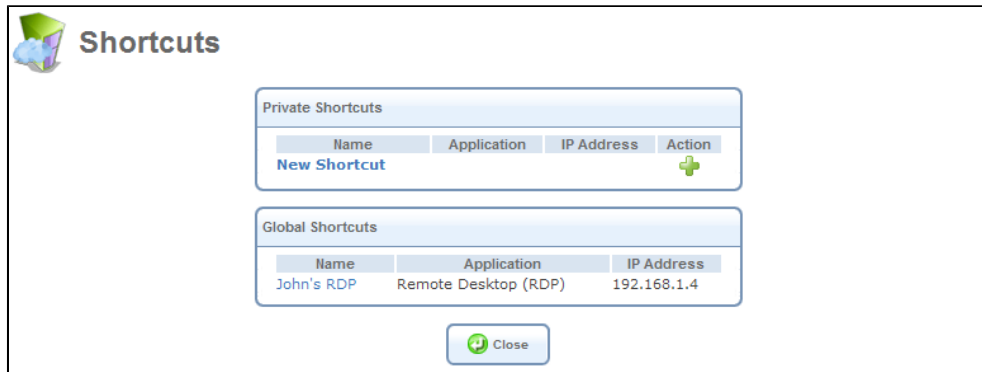


Figure 7.419. Shortcuts

7.10.2.3.1. Creating a Private Shortcut

In addition to the global shortcuts, each user can use the SSL-VPN portal to configure private shortcuts, displayed only for him when logged in. To add a new private shortcut, perform the following:

1. In the 'Private Shortcuts' section of the 'Shortcuts' screen, click the 'New Shortcut' link. The 'Shortcut Wizard' screen appears. This process is identical to the addition of a global shortcut.
2. After configuring the application parameters, click 'Next'. The following wizard screen appears.

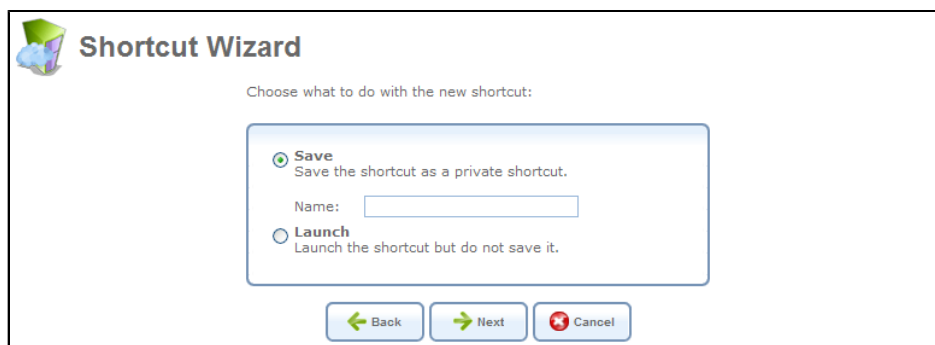


Figure 7.420. Save or Launch

3. You can either save the private shortcut or launch it without saving. Select a radio button and click 'Next'. The 'Shortcut Summary' screen appears.

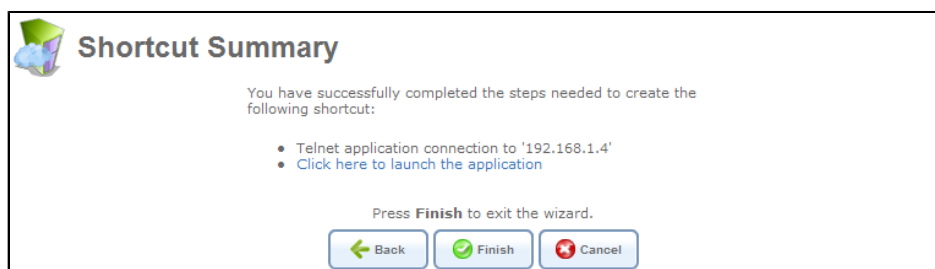


Figure 7.421. Launch

- If you chose "Launch", click the provided link. Otherwise, click 'Finish'. The new shortcut is added to the 'Private Shortcuts' section of the 'Shortcuts' screen, and will be available exclusively for this user when connecting to the SSL VPN portal.

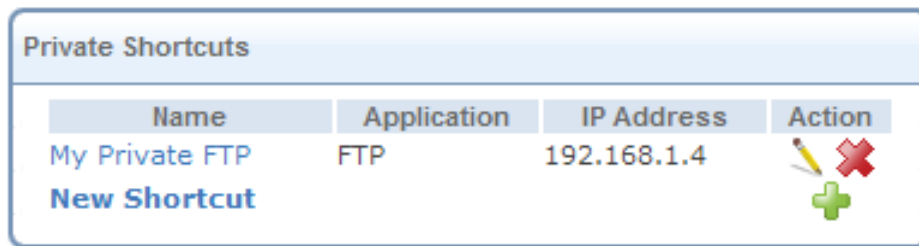


Figure 7.422. Private Shortcuts

7.10.2.3.2. Customizing the SSL VPN Portal

You can customize the look and the behavior of the SSL VPN portal from the 'SSL VPN' screen.

General

Enabled

SSL-VPN Portal
[Click Here to Allow Incoming HTTPS Access](#)
[Click Here to Create SSL-VPN Users](#)

Greeting Message:

Image Location (URL):

Application Inactivity Timeout in Seconds:

Restrict Access Only to the Global Shortcuts

Figure 7.423. SSL VPN

Greeting Message Enter the greeting message that will appear at the top of the SSL VPN portal screen.

Image Location (URL) Enter the URL of an image you would like to display at the top-left of the portal screen (instead of the default image).

Application Inactivity Timeout in Seconds The timeframe of application idleness in seconds, after which the application disconnects. The user will have to use the shortcut to reactivate the application. Enter zero if you would like to un-limit this timeframe.

Restrict Access Only to the Global Shortcuts When checked, only the global shortcuts will appear and be accessible.

7.10.2.3.3. Viewing Jungo.net File Sharing Invitations

The 'Global Shortcuts' section enables you to view file sharing invitations that you send to remote users from Jungo.net (refer to [Section 7.11.2.3](#)). Whenever an invitation is sent, its log appears in the 'Global Shortcuts' section.












Global Shortcuts			
Name	Application	IP Address	Action
invite_45	Web Based CIFS	127.0.0.1	 
invite_46	Web Based CIFS	127.0.0.1	 
invite_47	Web Based CIFS	127.0.0.1	 
invite_48	Web Based CIFS	127.0.0.1	 
New Shortcut			

Figure 7.424. Remote File Access Invitations Log

For a detailed view of an invitation, click its  action icon . To remove an invitation from a list, click its  action icon . This will also cancel the invitation. If you removed an invitation by mistake, you can recover it by clicking the 'Reconfigure My Settings' button in the Jungo.net portal's 'Account' screen. The Jungo.net portal will reconfigure your gateway, and the removed invitation will reappear in the list. For more information, refer to the Jungo.net User Manual.

7.10.3. Point-to-Point Tunneling Protocol Server

OpenRG can act as a Point-to-Point Tunneling Protocol Server (PPTP Server), accepting PPTP client connection requests.

7.10.3.1. Configuring the PPTP Server

Access this feature either from its link in the 'VPN' tab under the 'Services' screen, or by clicking the 'PPTP Server' icon in the 'Advanced' screen. The 'Point-to-Point Tunneling Protocol Server (PPTP Server)' screen appears:

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

IPSec | SSL-VPN | **PPTP Server** | L2TP 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 .245

Connections

Name	Status	Action

OK Apply Cancel Advanced >>

Figure 7.425. Point-to-Point Tunneling Protocol Server (PPTP Server)

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. Refer to [Section 8.3](#) to learn how to define and configure users.

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.

7.10.3.2. Advanced PPTP Server Settings

To configure advanced PPTP server settings press the 'Advanced' button on the PPTP screen (see [Figure 7.425](#)). The screen expands, offering additional settings:

Figure 7.426. Advanced PPTP Server Parameters

Maximum Idle Time to Disconnect in Seconds Specify the amount of idle time (during which no data is sent or received) that should elapse before the gateway disconnects a PPTP connection.

Authentication Required Select whether PPTP will use authentication.

Allowed Authentication Algorithms Select the algorithms the server may use when authenticating its clients.

Encryption Required Select whether PPTP will use encryption.

Allowed Encryption Algorithms Select the algorithms the server may use when encrypting data.

MPPE Encryption Mode Select the Microsoft Point-to-Point Encryption mode: stateless or stateful.

Please note that the server settings must be in tune with the client settings, described in [Section 8.4.13](#).

7.10.4. Layer 2 Tunneling Protocol Server

OpenRG can act as a Layer 2 Tunneling Protocol Server (L2TP Server), accepting L2TP client connection requests.

7.10.4.1. Configuring the L2TP Server

Access this feature either from the 'VPN' menu item under the 'Services' tab, or by clicking the 'L2TP Server' icon in the 'Advanced' screen. The 'Layer 2 Tunneling Protocol Server (L2TP Server)' screen appears.

The screenshot shows the configuration interface for the L2TP Server. It includes a 'Server' section with two checkboxes: 'Enabled' and 'Protect L2TP Connection by IPSec'. Below this is the 'Remote Address Range' section, which contains two rows of IP address fields: 'Start IP Address' (192.168.1.235) and 'End IP Address' (192.168.1.244). At the bottom, there is a 'Connections' table with columns for 'Name', 'Status', and 'Action'. Below the table are four buttons: 'OK', 'Apply', 'Cancel', and 'Advanced >>'.

Figure 7.427. Layer 2 Tunneling Protocol Server (L2TP Server)

This screen enables you to configure the following connection settings:

Enabled Select or deselect this check box to enable or disable this feature.

Note that selecting 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. Refer to [Section 8.3](#) to learn how to define and configure users.

Protect L2TP Connection by IPSec By default, the L2TP connection is not protected by the IP Security (IPSec) protocol. Select 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.

7.10.4.2. Advanced L2TP Server Settings

To configure advanced L2TP server settings, click the 'Advanced' button in the L2TP Server screen (see [Figure 7.427](#)). The screen expands, offering additional settings.

VPN
Layer 2 Tunneling Protocol Server (L2TP Server)

IPSec | SSL-VPN | PPTP Server | L2TP Server

Server

Enabled
[Click Here to Create VPN Users](#)
 Protect L2TP Connection by IPsec
 L2TP Shared Secret (optional):

Max Idle Time to Disconnect in Seconds:

Authentication Required

Allowed Authentication Algorithms:

PAP
 CHAP
 MS-CHAP
 MS-CHAP v2

Encryption Required

Allowed Encryption Algorithms:

MPPE-40
 MPPE-128

MPPE Encryption Mode:

Remote Address Range

Start IP Address: . . .

End IP Address: . . .

Connections

Name	Status	Action

OK Apply Cancel Basic <<

Figure 7.428. Advanced L2TP Server Parameters

L2TP Shared Secret (optional) Use this optional field to define a shared secret for the L2TP connection, for added security.

Maximum Idle Time to Disconnect in Seconds Specify the amount of idle time (during which no data is sent or received) that should elapse before the gateway disconnects the L2TP connection.

Authentication Required Select whether L2TP will use authentication.

Allowed Authentication Algorithms Select the algorithms the server may use when authenticating its clients.

Encryption Required Select whether L2TP will use encryption.

Allowed Encryption Algorithms Select the algorithms the server may use when encrypting data.

MPPE Encryption Mode Select the Microsoft Point-to-Point Encryption mode: stateless or stateful.

7.10.4.3. Configuring an L2TP over IPSec VPN Client

If you wish to connect to OpenRG's L2TP server (with the default IPSec configuration) using the Windows IPSec client, configure your host's L2TP connection with the following:

- Your login credentials (for more information, refer to [Section 8.3](#))
- The L2TP server's IPSec shared secret (for more information, refer to [Section 7.10.4.1](#)).
- The L2TP server's IP address (OpenRG's WAN address)

In case you wish to use a third-party IPSec client (for example, Netscreen) with your L2TP connection, configure the client with the following parameters. Note that these parameters match the gateway's default IPSec VPN connection parameters.

Remote Party's Identity

- **ID Type** Select 'IP Address', and specify OpenRG's WAN IP address.
- **Protocol** Select UDP.
- **Port** Select L2TP 1701.

My Identity

- **ID Type** Select 'IP Address'.
- **Port** Select L2TP 1701.

Security Policy Select the 'Main' mode.

Phrase 1 Negotiation Mode

- Select 'IPSec Shared Secret' as the peer authentication method, and enter the shared secret defined in the L2TP server's IPSec VPN settings.
- Define the encryption algorithm—by default, OpenRG supports the 3DES-CBC algorithm.
- Define the hash algorithm—OpenRG supports both the MD5 and SHA1 algorithms.
- Define the Key group—by default, OpenRG supports Diffie-Hellman (DH) Group 2 and Group 5.

Phrase 2 Negotiation Mode

- Enable the 'Encapsulation Protocol' option.
- Define the encryption and hash algorithms exactly as in Phase 1.
- Set the encapsulation method to 'Transport'.

7.11. Storage

7.11.1. FTP Server

OpenRG can operate as a File Transfer Protocol (FTP) server, allowing users and guests to access its internal disks, to easily (but securely) exchange files. OpenRG's 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, for example, to let guests download a certain file.

7.11.1.1. User Access FTP

To configure an FTP user, perform the following:

1. Click the 'Users' icon in the 'Advanced' screen of the management console. The 'Users' screen appears.

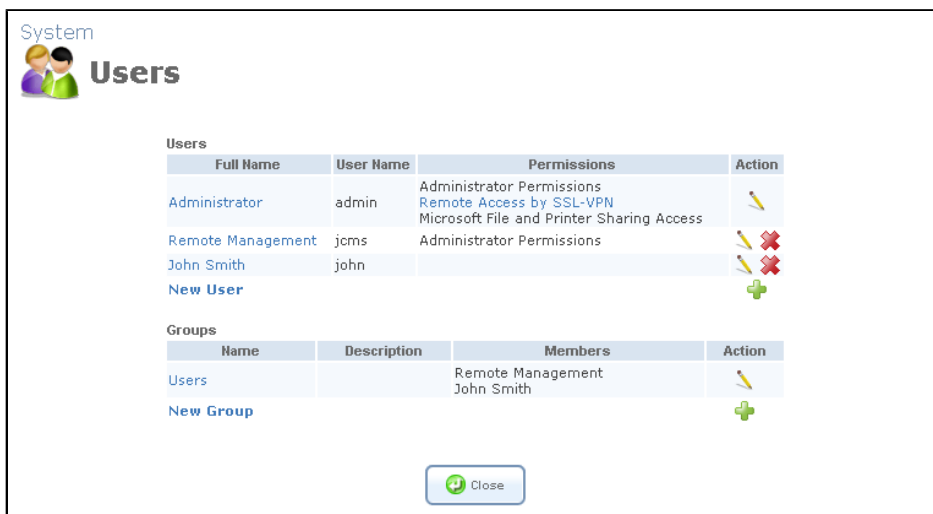


Figure 7.429. Users

2. Click the edit icon of the user for which you would like to grant FTP access. The 'User Settings' screen appears.

System User Settings

General

Full Name: John Smith

User Name (case sensitive): john

New Password:

Retype New Password:

Primary Group: Users

Permissions:

- Administrator Permissions
- Remote Access by SSL-VPN
- Mail Server Access
- Microsoft File and Printer Sharing Access
- FTP Server Access
- Internet Printer Access
- Remote Access by VPN

Disk Management

Enable User Home Directory

Figure 7.430. User Settings

3. In this screen, perform the following:
 1. In the Permissions section, check the 'FTP Server Access' check box, to grant this permission.
 2. Check the 'Enable User Home Directory' check box. This feature creates a home directory for the user.
4. Click 'OK' to save the settings.
5. Access the FTP Server settings either from the 'Storage' tab under the 'Services' screen, or by clicking the 'FTP Server' icon in the 'Advanced' screen. The 'FTP server' screen appears. Check the 'Enabled' check box to view the full FTP screen.

Storage FTP Server

FTP Server | File Server | WINS Server | Web Server | Mail Server | Backup and Restore

Enabled

Allow WAN Access

Idle Timeout: 300 Seconds

Clients: Unlimited

User's Directory: Home Directory

Welcome Message:

OK Apply Cancel Anonymous

Figure 7.431. Enabled FTP Server

6. In this screen, perform the following:
 1. Check the 'Allow WAN Access' check box if you wish to allow registered users to use the FTP from the WAN.
 2. Enter the maximum number of seconds that a user may spend between FTP commands before the session times out, in the 'Idle Timeout' field. This setting is global for all users, both registered and guests.
 3. Choose the maximum number of users that can use the FTP simultaneously. You can choose between "Unlimited" and "Maximum" in the 'Clients' combo box. When choosing 'Maximum', a second field appears allowing you to enter the number of users. This setting is also global.
 4. In the 'User's Directory' combo box, choose 'Home Directory' to allow registered users to access their home directories. Alternatively choose 'Common Directory'. A second field will appear in which you should specify a common directory relative to '<User Data>/'. All registered users will be able to access this directory only.
 5. Enter a welcome message that will be displayed for all users after logging in (optional).
7. Click 'OK' to save the settings.

7.11.1.2. Anonymous Access FTP

To configure an anonymous or guest FTP user, perform the following:

1. Click the 'Anonymous' button at the bottom of the 'FTP Server' screen (see [Figure 7.431](#)). The 'Anonymous Access' screen will appear (see [Figure 7.432](#)).
2. Check the 'Allow LAN/WAN Access' check boxes to allow guests FTP access to the LAN or the WAN, or both. A second field appears labeled 'LAN/WAN Root Directory'. The default directory is { home/ftp }, which is OpenRG's pre-configured directory with guest permissions and the usernames "ftp" and "anonymous" (any passwords will be accepted).



Figure 7.432. Anonymous Access

3. Click 'OK' to save the settings.



Note: The FTP Server assumes that any path or directory that you enter during the configuration exists. Each file in the directory should have the correct permissions for the relevant user. Files in the anonymous directories should have the relevant permissions for the built-in 'ftp' user.

7.11.2. File Server

OpenRG 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 OpenRG's disk management (refer to [Section 6.4](#)).

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 appears.

Storage

File Server

File Server | WINS Server | FTP Server | Web Server | Mail Server | Backup and Restore

Enabled
 NetBIOS Workgroup: HOME
 Automatically Share All Partitions
 Allow Guest Access: Read/Write

Name	Path	Comment	Action
share1	A	Kingston DataTraveler 2.0 (Rev: PMAP)	+

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

OK Apply Cancel Refresh

Figure 7.433. File Server

Enabled Select or deselect this check box to enable or disable this feature.

NetBIOS Workgroup OpenRG's workgroup name that will be displayed in the Windows network map of LAN hosts.

Automatically Share All Partitions A partitioned storage device connected to OpenRG is automatically displayed and shared by all LAN computers. This feature is enabled by default.

Allow Guest Access From the drop-down menu, select a permission level, according to which the LAN users will access the share:

Read/Write Every LAN user can read and write the shared files without authentication.

Read Only Every LAN user can only read the shared files.

Disabled LAN users must authenticate themselves, in order to access the share. They will be able to use the share according to their permissions defined in OpenRG's 'User Settings' screen.

File Server Shares Define file shares on your disk partitions, as depicted in the following sections.

7.11.2.1. Automatic File Sharing

By default, all partitions are automatically shared and displayed. **Figure 7.433** depicts such a scenario, where a share entry (with a default name "share1") appears in the 'File Server Shares' section as soon as a partitioned and formatted storage device is connected to your gateway. If you wish to share specific directories or partitions, perform the following:

1. Deselect the 'Automatically Share All Partitions' option and click 'Apply'. The list of all automatically shared partitions disappears.

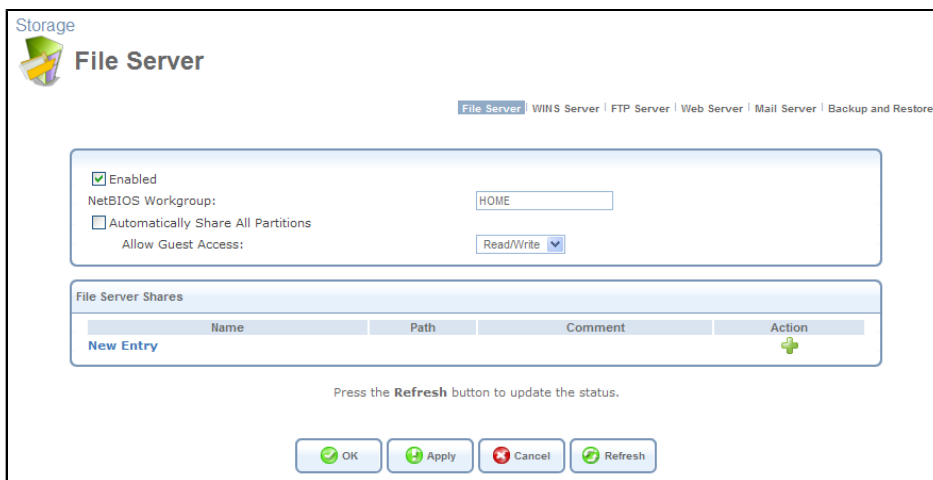


Figure 7.434. Disabled Automatic Partition Sharing

2. Click the 'New Entry' link to define a new share. The 'File Server Share Settings' screen appears.

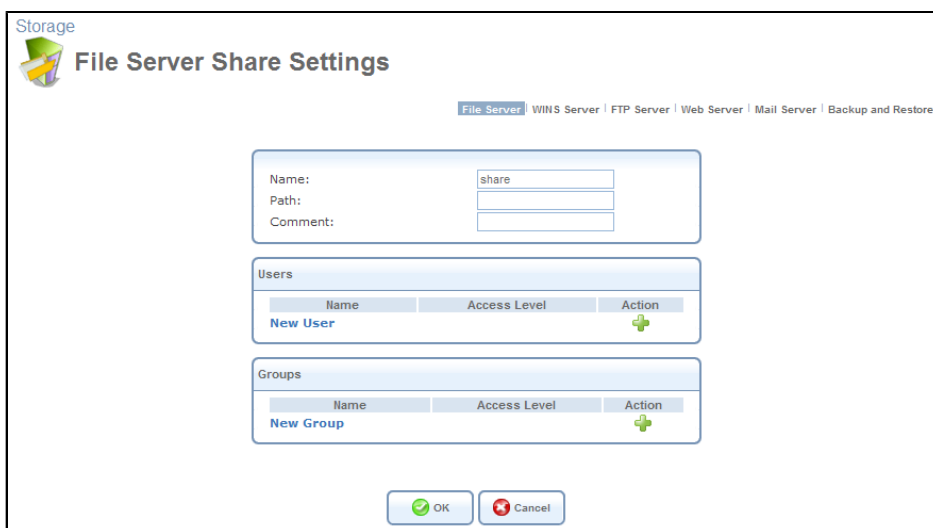



Figure 7.435. File Server Share Settings

3. Enter the share's name, path, and (optionally) comment.

 Note: The default name "share" can be changed to another one. The share's name is not case sensitive. Even if entered in upper-case letters, the name will be displayed in lower case, after saving the setting.

4. Associate a user or group of users with the share, to grant them access to the shared files. To learn how to do so, refer to [Section 7.11.2.2](#).
5. Click 'OK' to save the settings. The 'File Server' screen appears, displaying the share (see [Figure 7.433](#)).

Click the share's name to view its content. The screen refreshes as the share is accessed.

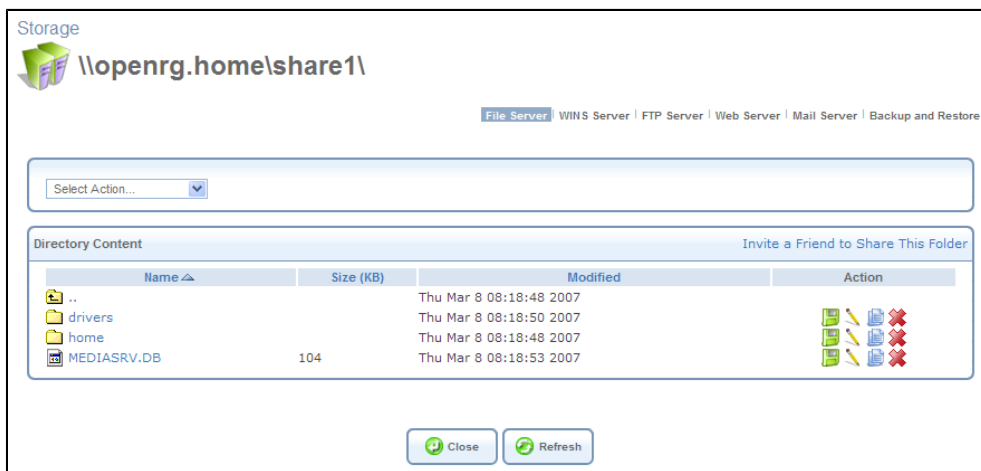


Figure 7.436. File Server Share

This screen enables you to both modify and view the content of your file share. In the upper section of this screen, you can modify your file share by adding files or directories to it. Use the drop-down menu to select an action.

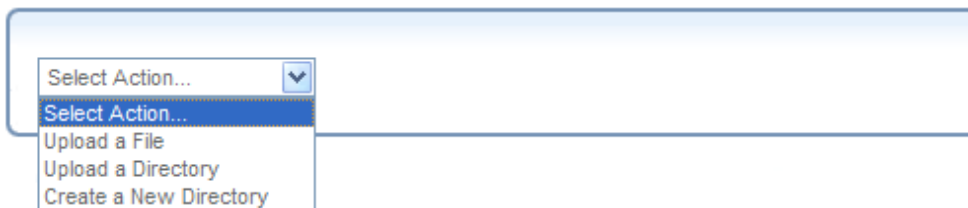


Figure 7.437. File Share Actions

- **Upload a File** Select this option to upload a file to the share. The screen refreshes.



 Uploaded file will overwrite any pre-existing file with the same name.

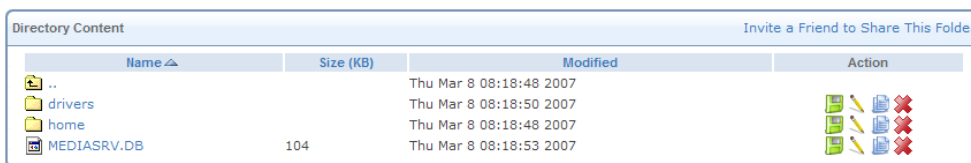


Figure 7.438. Upload a File

Enter the location of the file to upload, or click the 'Browse' button to browse for the file. Click the 'Upload' button to upload the file.

- **Upload a Directory** You can also upload an entire directory of files, by performing the following:
 1. Create a tarball archive out of the target directory.
 2. Enter the location of the archive, or click the 'Browse' button to browse to its location.
 3. Click the 'Upload' button to upload the archive.
- **Create a new Directory** You can create a new directory by simply typing its name and clicking the 'Go' button.
- **Paste from Clipboard** This option appears only after using the 'Copy to Clipboard' option ( action icon) to copy a directory or file from one directory to another.

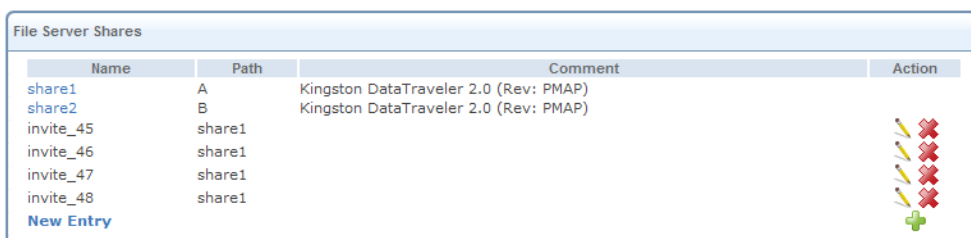
The lower section of the screen displays your share's content. You can click the different directory names to access them, or you can download, rename, copy or remove the directories using the standard action icons.



Name	Size (KB)	Modified	Action
..		Thu Mar 8 08:18:48 2007	
drivers		Thu Mar 8 08:18:50 2007	
home		Thu Mar 8 08:18:48 2007	
MEDIASRV.DB	104	Thu Mar 8 08:18:53 2007	



Figure 7.439. File Share Content

If your gateway is connected to the Jungo.net portal (refer to [Section 7.2](#)), the **Invite a Friend to Share This Folder** link appears in the right corner of this section. This link enables you to invite remote users to access your shares over the Internet (refer to [Section 7.11.2.3](#)). Whenever an invitation is sent, its log appears in the 'File Server Shares' section of the screen.



Name	Path	Comment	Action
share1	A	Kingston DataTraveler 2.0 (Rev: PMAP)	
share2	B	Kingston DataTraveler 2.0 (Rev: PMAP)	
invite_45	share1		
invite_46	share1		
invite_47	share1		
invite_48	share1		
New Entry			

Figure 7.440. Remote File Access Invitations

For a detailed view of an invitation, click its  action icon . To remove an invitation from a list, click its  action icon . This will also cancel the invitation. If you removed an invitation by mistake, you can recover it by clicking the 'Reconfigure My Settings' button in the Jungo.net portal's 'Account' screen. The Jungo.net portal will reconfigure your gateway, and the removed invitation will reappear in the list. For more information, refer to the Jungo.net User Manual.

7.11.2.2. Microsoft File Sharing

You can disable the automatic file sharing feature by unchecking the 'Automatically share all partitions' check box (see [Figure 7.433](#)), and manually define file shares using the 'Microsoft File Sharing Protocol' on OpenRG's partitioned storage device. First, enable Microsoft File Sharing for each user:

1. Click the 'Users' icon in the 'Advanced' screen of the management console. The 'Users' screen appears.

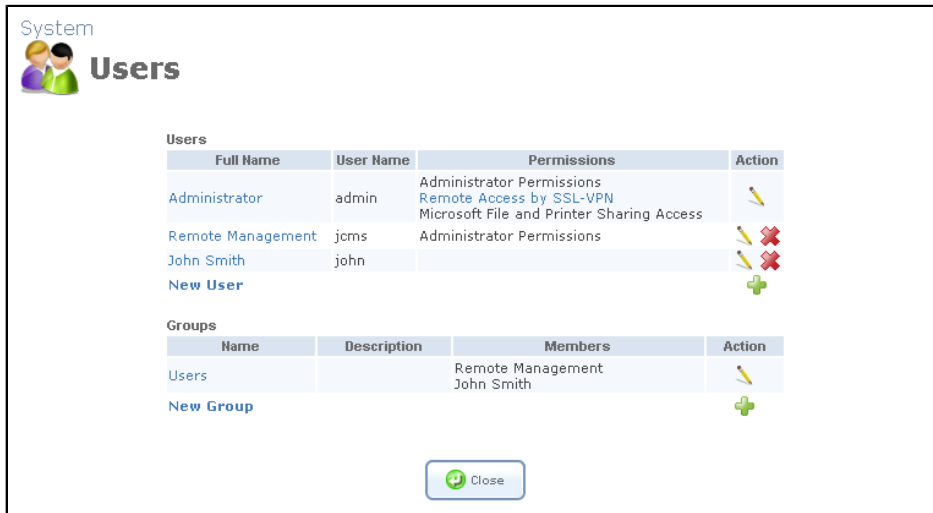


Figure 7.441. Users

2. Click the name of the user for whom you wish to enable file sharing.
3. In the 'User Settings' screen that appears, check the "Microsoft File and Printer Sharing Access" check box in the 'Permissions' section.

System
User Settings

General

Full Name: John Smith
User Name (case sensitive): john
New Password: *****
Retype New Password: *****
Primary Group: Users

Permissions:

- Administrator Permissions
- Remote Access by SSL-VPN
- Mail Server Access
- Microsoft File and Printer Sharing Access
- FTP Server Access
- Internet Printer Access
- Remote Access by VPN

Disk Management

Enable User Home Directory

Mail Box

Enabled

Quota: Maximum 30 MB
Aliases:

E-Mail Notification

[Click Here to Configure Notification Mail Server](#)

Notification Address:

System Notify Level: None

Security Notify Level: None

OK Cancel

Figure 7.442. User Settings

4. Click 'OK' to save the settings.

Next, define file shares:

1. Click the 'File Server' icon in the 'Advanced' screen of the management console.
2. Click the 'New Entry' link in the 'File Server Shares' section. The 'File Server Share Settings' screen appears.

Storage

File Server Share Settings

FTP Server | **File Server** | WINS Server | Web Server | Mail Server | Backup and Restore

Name:

Path:

Comment:

Users

Name	Access Level	Action
John Smith	Read/Write	
New User		


Groups

Name	Access Level	Action
New Group		

Figure 7.443. File Server Share Settings

3. In this screen:

- a. Enter a name for the share in the 'Name' field.
- b. Enter a valid partition path (e.g. A, B/my_documents) in the 'Path' field.

 Note: If a drive's sub directory does not exist yet, you will have to create it as soon as the share is defined and accessible.

- c. You may add a comment in the 'Comment' field.
- d. In the 'Users' section, click the 'New User' link to allow a user to use the share.
- e. In the 'User' screen that appears (see [Figure 7.444](#)), choose the user and the allowed access level in the combo boxes, and click 'OK'.

Storage

User

FTP Server | **File Server** | WINS Server | Web Server | Mail Server | Backup and Restore

Name:

Access Level:

Figure 7.444. User Access Settings

You can also allow a group of users to use the share, in the same manner, in the 'Groups' section.

4. Click 'OK' to save the settings. The 'File Server' screen reappears, displaying the new share in the 'File Server Shares' section.




File Server Shares				
Name	Path	Comment	Action	
file://openrg/my_share	A	An example share		
New Entry				

Figure 7.445. File Server Shares Section

You can now access the file share.

However, note that access to a file share is different for FAT32, NTFS, and EXT2/3 formatted partitions. FAT32 has no restrictions—any user can access any share for both reading and writing. However, the data stored on NTFS partitions is only readable (unless OpenRG is based on the Conexant Solos or Freescale platforms).

In addition, shares defined on EXT2/3 partitions are only readable to non-administrator users (even with writing permissions), with the following exceptions:

- The user will be able to write to the share's root directory (e.g. A\, my_share\).
- The user will be able to write to his/her home directory, if such had been created for that user, by enabling the 'Enable User Home Directory' option in the 'User Settings' screen (see [Figure 7.442](#)).

Moreover, to create new directories that will be writable for users, you must be logged in as a user, not an administrator. Any directories created by an administrator will only be writable to the administrator.

To access the new share from OpenRG, perform the following:

1. Click the share's link under the 'Name' column in the 'File Server Shares' section (see [Figure 7.445](#)).



Note: If the share is not available, for example if the disk has been removed, the link will not be clickable and appear as plain text.

A Windows login dialog box appears.

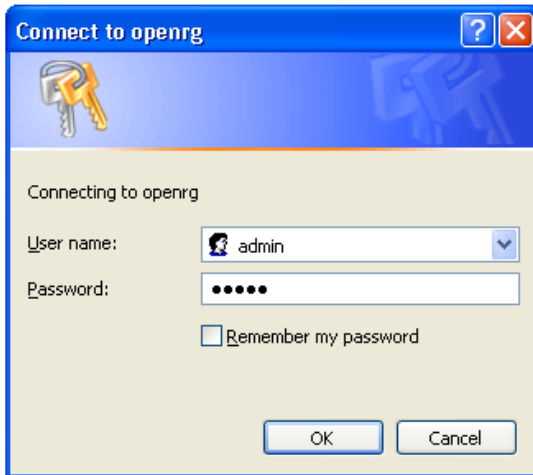


Figure 7.446. Login Dialog

2. Enter your OpenRG username and password to login (non administrator users must have file access permission in order to access the share). The share opens in a new window.

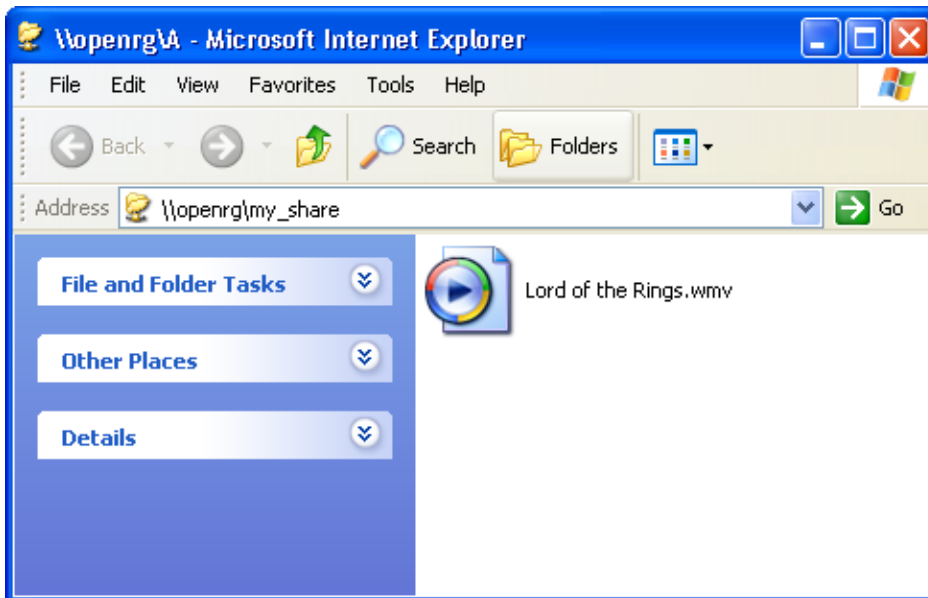


Figure 7.447. File Share

Once logged into a share, Windows remembers your username and password, and automatically re-logs with the same user. To logout and re-login with a different user (for example, to switch between an administrator and a user), either logout and re-login to Windows, or type the following command in the command line: `'net use /del *'`.

Users with appropriate permissions can access file shares from any PC on the LAN using the following standard methods:

- From OpenRG's Web-based management as described above.
- Browsing to the share itself by simply typing its path (for example, `openrg\A`) in a browser address line or in the command line.

- Mapping the share using Window's 'Map Network Drive' utility.

All of the methods above will require an initial username and password login, as described above. The share content will be displayed in a new window. If the share is the partition configured to serve as the system storage area, it will contain automatically-generated system folders. Otherwise, it will either be empty or contain pre-loaded files.

All of the methods above require an initial username and password login, as described above. The share content is displayed in a new window. If the share is the partition configured to hold the system and user data, it will contain automatically-generated system folders. Otherwise, it will either be empty or contain pre-loaded files.

7.11.2.3. Inviting Remote Users to Use File Shares

Once you have created file shares on your gateway's storage device, you can grant access to the content of these shares (or specific directories within them) to friends over the Internet. OpenRG utilizes the Jungo.net system to enable you to invite friends to view your files. This is done by sending invitation emails, allowing recipients access to your file shares. Before you can invite friends to access your file shares, verify the following:

- A storage device is connected to your gateway
- File shares are defined and contain directories you wish to share
- Your gateway is connected to Jungo.net (to learn how to create a Jungo.net account, refer to [Section 7.2](#)).

To invite a friend to access your file shares, perform the following:

1. In the 'File Server' screen (see [Figure 7.433](#)), click the share's name. The screen refreshes as the share is accessed.



Figure 7.448. File Server Share

2. If you would like to share a specific directory, click its name to access it. Otherwise, click the 'Invite a friend to share this folder' link, to share the entire file server share. A new browser window opens.

The screenshot shows a web-based invitation form. It contains the following fields and values:

- From Email Address:** jsmith@jungo.com
- To Email Address:** my_friend@cnn.com
- Subject:** Please share my data: A
- Share Name:** A
- Message:** Hi,
I would like to share my data with you: A
Please click the URL below to access it.
Regards,
- Expiry Date:** Jan 27 2007
- Number Of Visits:** 0 (Zero for unlimited number of visits)

At the bottom of the form are two buttons: "Invite" and "Cancel".

Figure 7.449. Invitation Form

In this form, verify the pre-filled details or enter new ones:

From Email Address Your email address.

To Email Address The email address of the person you would like to invite to access your file share content.

Subject A subject for the message.

Share Name The name of the share/directory to which access is granted (e.g. A, A/home).

Message You may write a textual message to your recipient.

Expiry Date Select a date on which access to the file share will be terminated (the default is one month).

Number Of Visits Specify the number of allowed visits to the share. Leave as zero for unlimited visits.

3. Click the 'Invite' button. The message is sent, and the following status screen appears.

Invite Date	Share Name	To Email Address	Subject	Expiry Date	Number Of Visits	Action
27-Dec-06 17:20:13	A	my_friend@cnn.com	Please share my data: A	27-Jan-07	Unlimited	

Figure 7.450. Invitation Status

Back in the 'File Server' screen, the invitation is displayed in the file server shares section. Note that clicking its link, even as an administrator, results in an "Access Denied" message, as only the intended recipient has the necessary permissions to access the share.

Name	Path	Comment	Action
A	A	Generic USB Flash Disk (Rev: 0.00)	
invite_304	A		
New Entry			

Figure 7.451. File Server Shares

Let's take a look at this from your friend's point of view: Your recipient will receive the following email message.

To: my_friend@cnn.com
 From: jsmith@jungo.com
 Subject: Please share my data: A

Hi,
 I would like to share my data with you: A
 Please click the URL below to access it.
 Regards,

URL: <http://10.71.83.222/invite.cgi?id=304&ipc=59B36FC7FFFFFFFF>

Figure 7.452. Invitation Message

Clicking the link in this message opens a new browser window.

JUNGO OpenRG

Language: EN English Welcome invite_304_my_friend_cnn.com | Home | Help | Logout

Shortcuts

Welcome to Jungo's SSL VPN Portal

Global Shortcuts		
Name	Application	IP Address
invite_304	Web Based CIFS	127.0.0.1

Don't have Java Runtime Environment (JRE) installed? [Click here](#)

Figure 7.453. Shortcut to Share

To access the file share, the recipient must click the shortcut name, in this example "invite_304". The screen refreshes as the share is accessed.

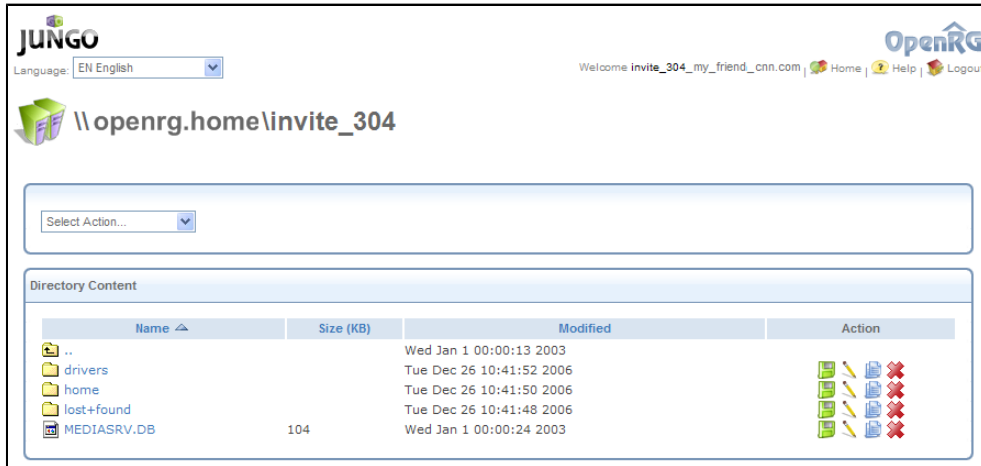


Figure 7.454. Remote File Server Share

7.11.2.4. Access Control Lists

The Windows operating system boasts an extensive file permission scheme. When you right-click a file and choose Properties, you can see under the Security tab (see [Figure 7.455](#)) that file permissions can be defined for any number of users and groups. Each user and group may be allowed or denied several levels of access, ranging from Full Control to Read only.

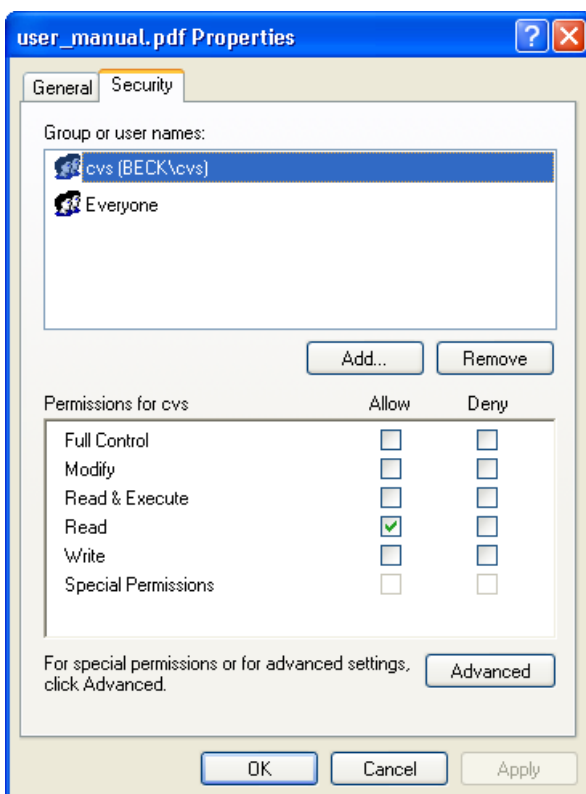


Figure 7.455. File Properties

Linux, on the other hand, has a very limited file permissions scheme, offering the basic Read (r), Write (w) and Execute (x) permissions to the file owner and his group only. Access Control Lists (ACLs) are an extension of the common Linux permission scheme. ACLs allow granting the aforementioned permissions not only to the file owner and his group, but to any number of users and groups. The need for ACLs in OpenRG is mainly to support permissions defined by a Windows client connected to the file server. This connection is done via the 'Microsoft File and Printer Sharing Protocol', which is supported on OpenRG and allows interoperability between Linux/Unix servers and Windows-based clients. The basic user and group file permissions in Windows are: Full control, Modify, Read and Execute, Read, and Write. Each permission can be allowed or denied. Linux supports Read, Write and Execute only, and does not support the Allow/Deny mechanism. When you modify a file's permissions on a Windows client, OpenRG uses a "best effort" algorithm to translate the ACLs to Linux r/w/x bits, making the file compatible with Linux clients.

7.11.2.4.1. Viewing and Modifying ACLs

This section explains how to view and modify file ACLs on a Windows client connected to OpenRG's file server. To view a file's ACLs:

1. Click the file share link in the 'File Server Shares' section (see [Figure 7.445](#)) of the 'File Server' screen to open the file share (login with a valid user for the share if a login prompt appears).
2. Create a file on the share.
3. Right-click the file and choose "Properties".
4. Click the Security tab to view the file ACLs (see [Figure 7.455](#)). If you do not have a Security tab:
 1. Open "My Computer" and choose Tools and then Folder Options.
 2. Under the View tab, uncheck the "Use simple file sharing (Recommended)" check box.

Under the Security tab you can view the permissions of the file owner, the owner's group and the group "Everyone", for all other users. If you have more users (or groups) defined on OpenRG, you can add them to the file's ACL and grant them permissions. To modify a file's ACLs:

1. Click the 'Add' button in the Security tab window to view the users and groups list.
2. In the 'Select Users or Groups' window that appears (see [Figure 7.456](#)), press the 'Advanced' button.

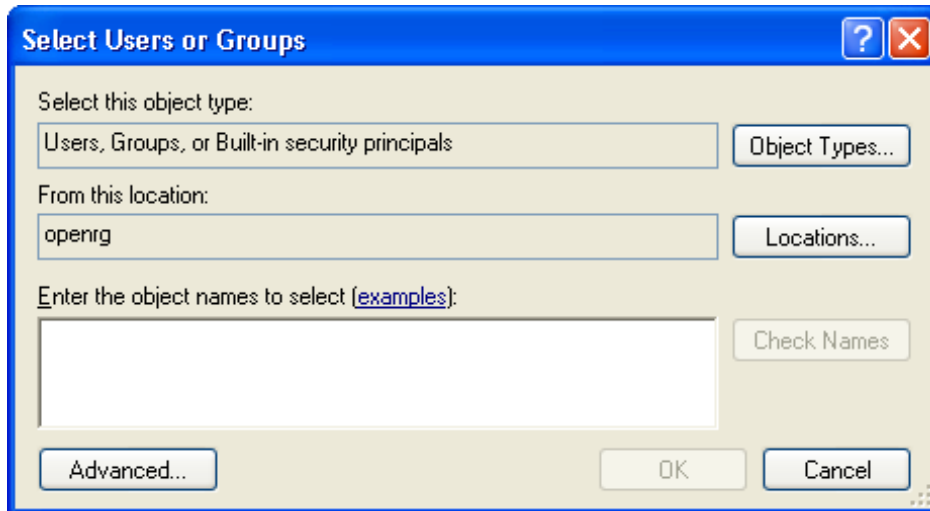


Figure 7.456. Select Users or Groups

3. In the advanced window (see [Figure 7.457](#)) press the 'Find Now' button.
4. A login prompt will appear. Log in with the same share user ¹. A list of both OpenRG users and system default users will be displayed.

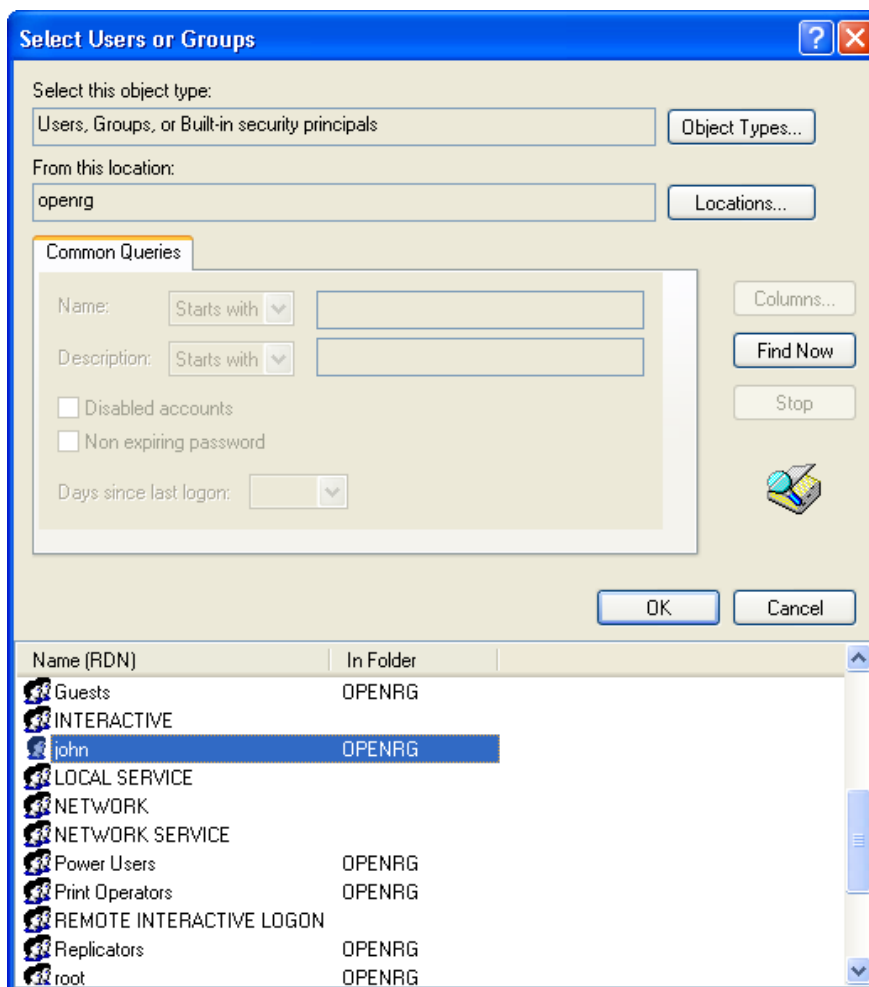


Figure 7.457. Users or Groups List

5. Select an OpenRG user from the list and click 'OK'. Click 'OK' again in the initial 'Select Users or Groups' window to save the settings. The selected user will be added to the groups and users list on the Security tab, with the default ACLs.
6. Check or uncheck the different permissions to allow or deny the user of the permissions.
7. Click 'OK' to save the settings.

In the same manner, you can remove a user or a group using the 'Remove' button in the Security window.

7.11.2.5. Using the File Server with Mac

In order to connect to OpenRG's file server with a Mac computer, perform the following:

1. On your Mac computer connected to OpenRG, click "Connect to Server" from the "Go" menu. The 'Connect to Server' screen appears.



Figure 7.458. Connect to Server

2. In the server address field, enter **smb://192.168.1.1** , and click the 'Connect' button. A new window appears, displaying the available file shares.



Figure 7.459. Connect to Server

3. Select the share to which you would like to connect. If prompted, enter a valid username and password, and click 'OK'. When a connection is established, the share content appears.



Figure 7.460. Connect to Server

7.11.3. WINS Server

OpenRG 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 OpenRG's DHCP (refer to [Section 7.13.2](#)). The WINS database is automatically updated with its NetBIOS name and the assigned IP address. OpenRG'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. To configure OpenRG's WINS server settings, perform the following:

1. Access the WINS Server settings either from its link in the 'Storage' tab under the 'Services' screen, or by clicking the 'WINS Server' icon in the 'Advanced' screen. The 'WINS Server' screen will appear (see [Figure 7.461](#)). By default, OpenRG's WINS server is disabled.

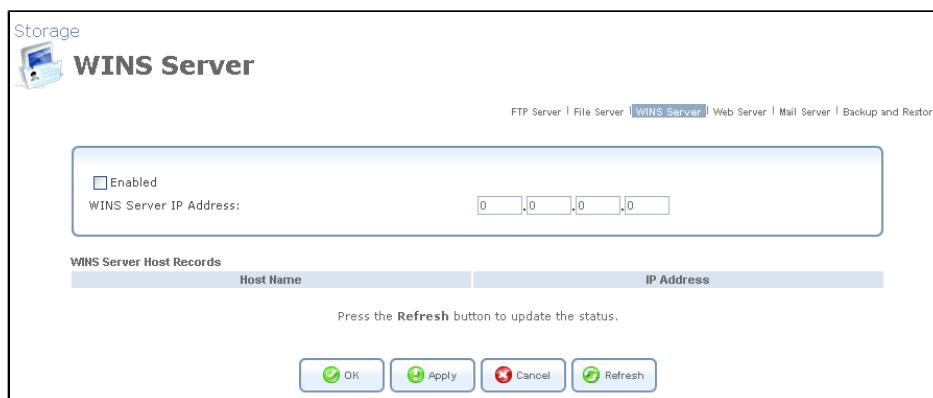


Figure 7.461. WINS Server

2. If you would like to use an external WINS server, enter its IP address and click 'OK'.
3. If you would like to use OpenRG's WINS server, select the 'Enabled' check-box. The screen will refresh, omitting the IP address field (see [Figure 7.462](#)).

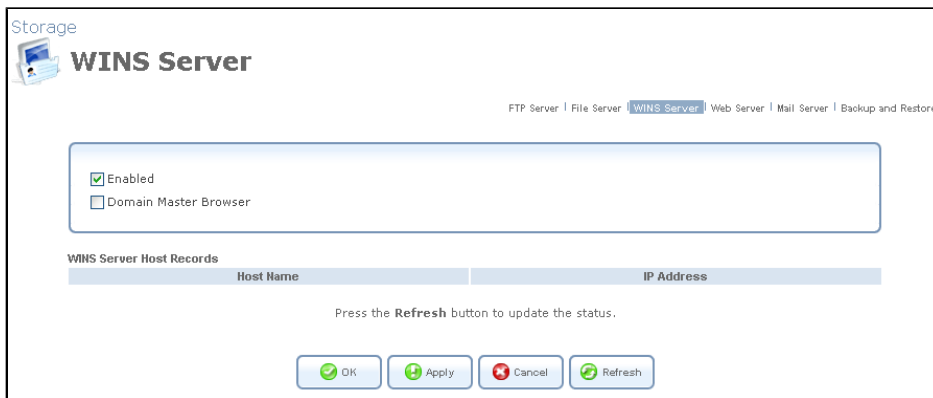


Figure 7.462. WINS Server

4. Select the 'Domain Master Browser' check box if you would like OpenRG to act as a domain master in the Windows NetBIOS protocol.
5. Click 'OK' to save the settings.

Hosts connected to the LAN will register their names and IP addresses with either the specified remote WINS server or with OpenRG's WINS server, depending on the configuration above. In both cases, the registered hosts will be added to the 'WINS Server Host Records' table in this screen.

7.11.4. Web Server

OpenRG 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 OpenRG, 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.

There are several preliminary actions that you must take before configuring your Web server on OpenRG:

1. Register a domain name and map it to OpenRG's WAN IP (refer to [Section 7.12](#)).
2. Connect a storage device (such as a hard drive) to OpenRG and configure its file server (refer to [Section 7.11.2](#)).
3. Verify that the System Storage Area is configured, as described in [Section 6.4.2](#).

4. Create your Web files, and upload them to a folder on the file server.



Note: It is important that you name the Web site's homepage **index.html** or **index.htm**, and upload it to the file server.

Access the Web server settings either from its link under the 'Storage' menu item of the 'Services' tab, or by clicking the 'Web Server' icon in the 'Advanced' screen. The 'Web Server' screen appears.

The screenshot shows the 'Web Server' configuration interface. At the top, there's a breadcrumb trail: 'Storage > FTP Server | File Server | WINS Server | **Web Server** | Mail Server | Backup and Restore'. The main configuration area includes:

- Enabled
- WAN Access
- Log Requests
- HTTP Port:
- HTTPS Port:
- Data Location: A/
- User Private Web Page
 - Enabled
 - Data Location: A/home/USER/

Below this is a 'Virtual Hosts' table with columns: Name, Aliases, Data Location, and Action. A 'New Entry' link with a green plus icon is at the bottom left of the table. At the bottom of the screen are three buttons: 'OK', 'Apply', and 'Cancel'.

Figure 7.463. Web Server

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.



Note: The default HTTP and HTTPS ports may be used by another service. In this case, reconfigure either this service or the Web server with unoccupied port numbers. For example, as the WBM by default uses HTTP port 80, it will disconnect after activating the Web server. To access it again, either change the Web server's default HTTP port, or browse to the WBM with an alternative port—for example, **http://192.168.1.1:82**.

The following sections describe how to configure OpenRG's Web server capabilities, including hosting user-private Web pages and multiple independent Web sites.

7.11.4.1. Setting Up Your Web Site on OpenRG

1. In the 'Data Location' field of the 'Web Server' screen, enter the file system path of the OpenRG folder containing your Web site's content.

Data Location: A/

Figure 7.464. Data Location Field

2. Click 'OK' to save the settings.

7.11.4.2. Hosting User Private Web Pages

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 OpenRG.

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 8.3.1](#)).
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.

User Private Web Page
 Enabled
 Data Location: A/home/USER/

Figure 7.465. User Private Web Page

4. Click 'OK' to save the settings.

7.11.4.3. Setting Up Virtual Hosts on OpenRG

You can configure any number of additional Web sites on the OpenRG 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 OpenRG's 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 (see [Figure 7.463](#)). The 'Virtual Host' screen appears.

Storage
Virtual Host

FTP Server | File Server | WINS Server | **Web Server** | Mail Server | Backup and Restore

Server Name:
 Data Location:

Aliases

Name	Action
New Entry	

Figure 7.466. Virtual Host

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 OpenRG 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. The 'Virtual Host Aliases' screen appears.

Storage
Virtual Host Aliases

FTP Server | File Server | WINS Server | **Web Server** | Mail Server | Backup and Restore

Alias:

Figure 7.467. Virtual Host Aliases

5. Type an alias URL in the 'Alias' field, and click 'OK'. The new alias appears under the 'Aliases' section (see [Figure 7.466](#)).
6. Click 'OK' to save the settings. Your site's URL and alias are added to the 'Virtual Hosts' section of the Web server screen.

Virtual Hosts

Name	Aliases	Data Location	Action
www.mysite.com	www.myalias.com	mysite/public_html	
New Entry			

Figure 7.468. New Virtual Host

7. Click 'OK' to save the settings.

7.11.5. Mail Server

OpenRG can operate as a mail server, serving both users on the LAN and the WAN. Users can access their mailboxes both as a home-based service, when working within the network, or as a web-based service, when working remotely.



Note: In order for this feature to operate properly, a system storage area must be created on OpenRG's storage device. For more information, refer to [Section 6.4.2](#).

7.11.5.1. Mail Server Configuration

Before configuring your mail server, you must register a domain name and map its A field (default server) or MX field (mail server) to OpenRG's WAN IP address. This can easily be done using the Dynamic DNS feature (refer to [Section 7.12](#)). To configure your mail server:

1. Access the Mail Server settings either from its link in the 'Storage' tab under the 'Services' screen, or by clicking the 'Mail Server' icon in the 'Advanced' screen. The 'Mail Server' screen appears.



Figure 7.469. Mail Server

2. Enable the mail server by checking the 'Enabled' check box. The full mail server screen appears.

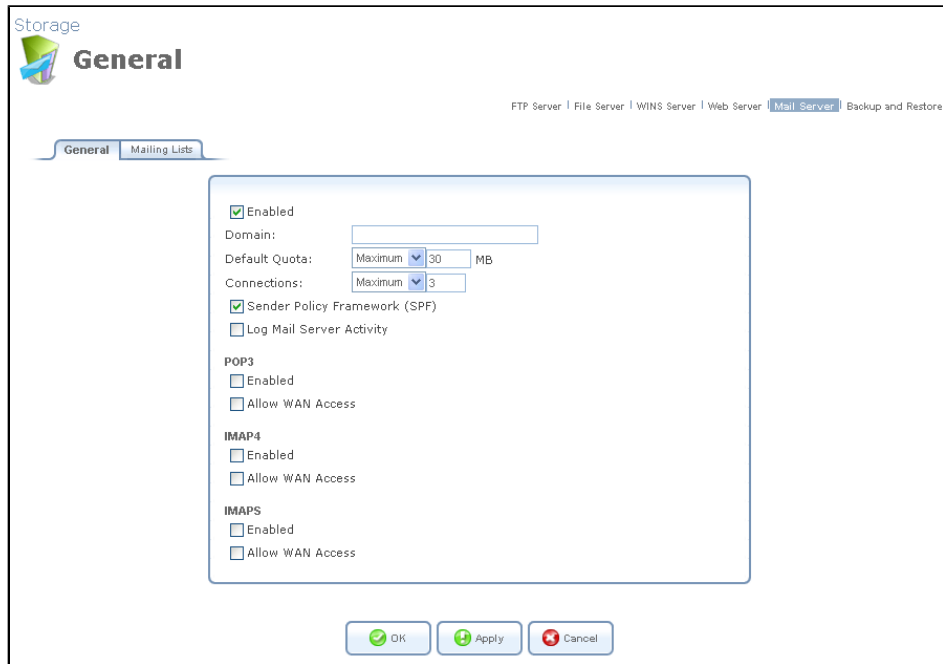


Figure 7.470. Enabled Mail Server

3. Enter the registered domain name in the 'Domain' field.
4. Choose the default Inbox quota for each new mailbox in the 'Quota' section.
5. Choose the maximum number of simultaneous connections allowed to the mail server. It is recommended that this value be left at the default of three.
6. Check the Sender Policy Framework (SPF) check box to allow mail filtering (recommended).
7. Check the 'Log Messages' check box to log the senders and receivers of all the sent, received and rejected messages in the system log. It is recommended that this option remains unchecked.
8. The next three sections should be configured according to your required mail retrieval protocols. You can enable POP3, IMAP4 and IMAPS, and choose whether to allow each with WAN access, by checking the relevant check boxes.
9. Click 'OK' to save the settings.

7.11.5.2. Mailbox Configuration

To configure a mailbox:

1. Click the 'Users' icon in the 'Advanced' screen of the WBM. The 'Users' screen appears:

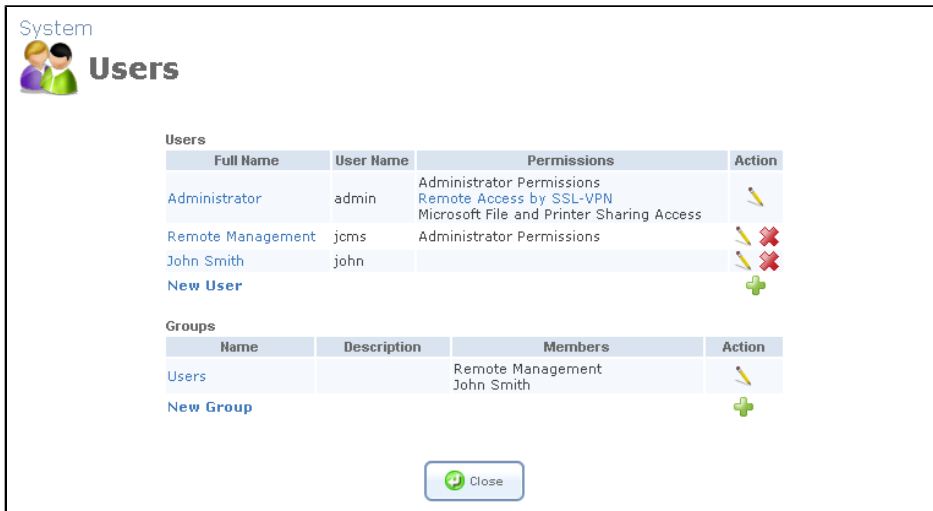


Figure 7.471. Users

2. Click the action icon of the user for which you would like to create a mailbox. The 'User Settings' screen appears:

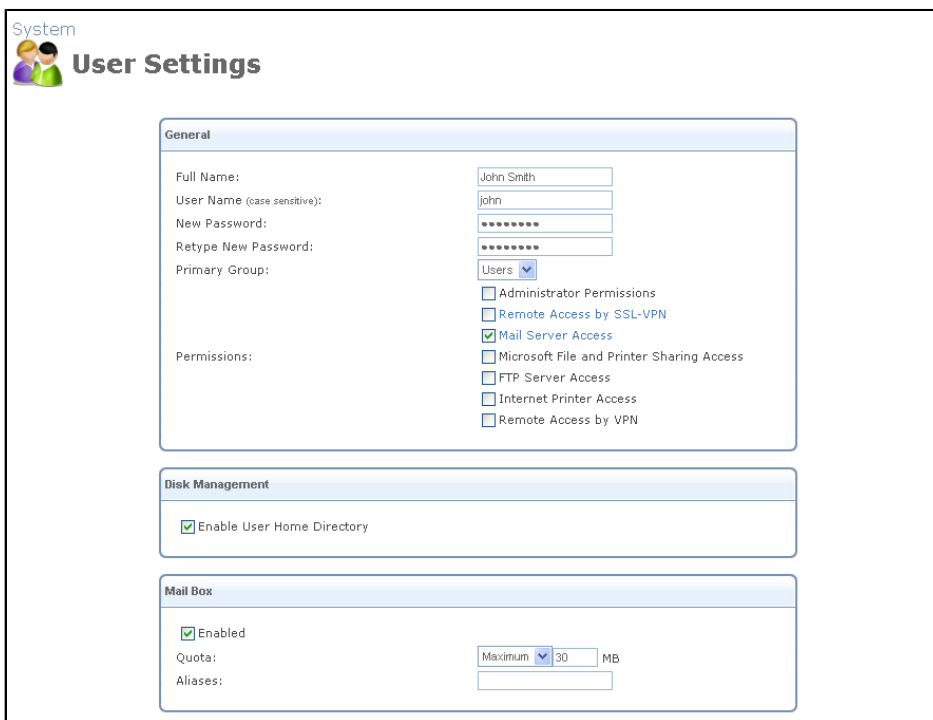


Figure 7.472. User Settings

3. In this screen, perform the following:
 1. Check the 'Enable User Home Directory' check box. This feature creates a home directory for the user.
 2. In the Permissions section, check the 'Mail Server Access' check box, to grant this permission.


3. Enable the mailbox by checking the 'Enabled' check box in the 'Mail Box' section.
4. Click 'OK' to save the settings.

The user's email address will be <username>@<domain name> where <username> is the OpenRG username of the user, and <domain name> is the domain name configured for the mail server.

7.11.5.3. Additional Features

7.11.5.3.1. Email Aliases

You may add any number of aliases to an email address. Emails sent to an alias address will be rerouted to the main address. To configure email aliases:

1. Click the 'Users' icon in the 'Advanced' screen of the WBM. The 'Users' screen appears.
2. Click the  action icon of the user for which you would like to add aliases.
3. In the 'User Settings' screen that appears (see [Figure 7.473](#)), enter the aliases (usernames only) as a comma-separated list in the 'Aliases' field of the 'Mail Box' section.



Mail Box

Enabled

Quota: Maximum MB

Aliases:

Figure 7.473. Mail Box Aliases

4. Click 'OK' to save the settings.

7.11.5.3.2. Mailing Lists

You may configure mailing lists to easily send mass emails. To configure mailing lists: [Figure 7.476](#)




Mailing Lists		
Name	Description	Action
<input checked="" type="checkbox"/> mail_list	A mailing list example	 
New Entry		

Figure 7.476. New Mailing List

1. Click the 'Mail Server' icon in the 'Advanced' screen of the WBM. The 'Mail Server' screen appears (see [Figure 7.470](#)).
2. Click the 'Mailing Lists' tab. The 'Mailing Lists' screen appears.

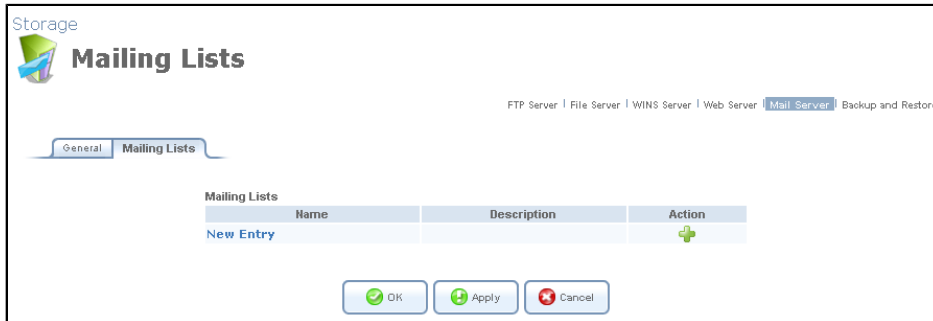


Figure 7.474. Mailing Lists

3. Click the 'New Entry' link to add a new mailing list. The 'Mailing Lists' screen appears.

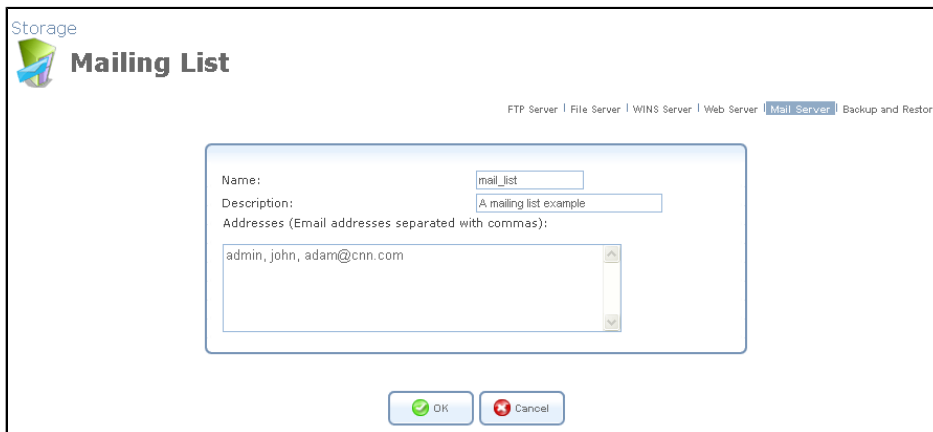


Figure 7.475. Mailing Lists

4. Enter a name and description for the mailing list in their respective fields. In the 'Addresses' field, enter a comma-separated list of the email addresses that you would like to include in the mailing list. Adding local addresses requires entering the usernames only, while adding external addresses requires entering the full email addresses.
5. Click 'OK' to save the settings.

7.11.5.4. Email Client Configuration

OpenRG email clients can access their mailboxes both from within the LAN and remotely over the internet.

7.11.5.4.1. LAN Email Clients

LAN email clients should configure the following:

- The incoming and outgoing mail servers should be configured with OpenRG's LAN IP (192.168.1.1) or LAN domain name (openrg.home).
- The outgoing mail server (SMTP) does not require authentication from the LAN.
- The incoming mail server (POP3, IMAP4 or IMAPS) requires authentication of the user's username and password.

7.11.5.4.2. WAN Email Clients

WAN email clients should configure the following:

- The incoming and outgoing mail servers should be configured with OpenRG's WAN IP or WAN domain name.
- The outgoing mail server requires authentication of the user's username and password.
- The incoming mail server (POP3, IMAP4 or IMAPS) must be enabled for OpenRG's WAN, and requires authentication of the user's username and password.

7.11.6. Backup and Restore

OpenRG's backup facility allows backing up data, stored in the system storage area, to external USB disks. 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 (refer to [Section 7.11.2](#)).
- The file server must be consisted of at least two disks.

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

7.11.6.1. Backing Up Your Data

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 appears:

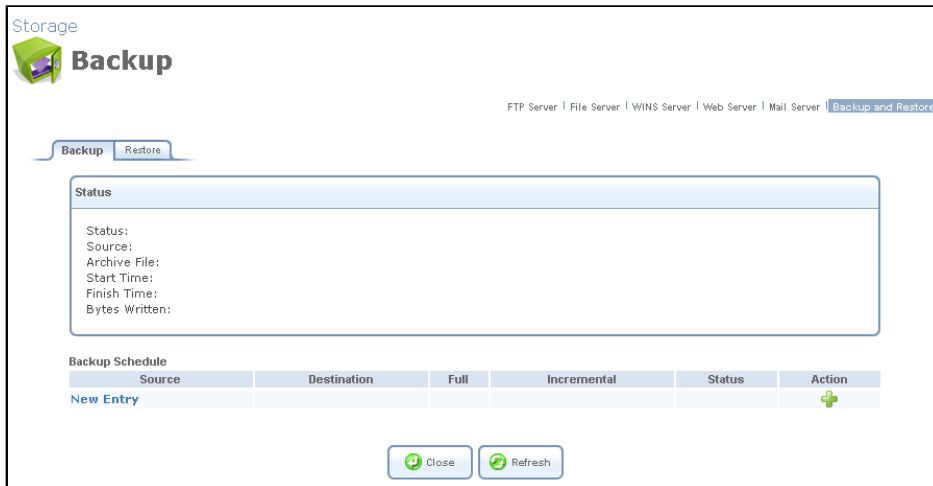


Figure 7.477. Backup and Restore

2. Click the 'New Entry' link in the 'Backup Schedule' section.
3. In the 'Edit Backup' screen that appears (see [Figure 7.478](#)), configure the following parameters:
 1. Type the source to backup. For example, { A/homes }.
 2. Type the destination of the backup files. For example, { B/backups }. It is recommended that the destination be an external storage device.
 3. 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.



Note: Do not schedule a monthly backup on the 31st, as backups will not run on months with 30 days.

Storage

Edit Backup

FTP Server | File Server | WINS Server | Web Server | Mail Server | **Backup and Restore**

Source:

Destination:

Full Backup

Last Backup:

Location:

Schedule: Monthly on day 1 of every month at 12:00

Incremental Backup

Last Backup:

Location:

Schedule: Weekly every Sunday at 12:00

OK Cancel Backup Now

Figure 7.478. Edit Backup

7.11.6.2. Restoring Your Data

To restore your data:

1. Press the 'Backup and Restore' icon in the 'Advanced' screen of the WBM. The 'Backup and Restore' screen appears (see [Figure 7.477](#)).
2. Press the 'Restore' tab.
3. In the 'Restore' screen that appears (see [Figure 7.479](#)), configure the following parameters:
 1. Type the source to restore in the 'Source Archive' field. For example, { A/homes }.
 2. 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 appears 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.
 3. 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 appears 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 7.479. Edit Restore

7.12. Personal Domain Name (Dynamic DNS)

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.

7.12.1. Opening a Dynamic DNS Account

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.com/account/create.html>. When applying for an account, you will need to specify a user name and password. Please have them readily available when customizing OpenRG's DDNS support.

7.12.2. Using Dynamic DNS

Use the DDNS feature to define different static host names for each of your WAN connections. Moreover, you can define more than one static host name for each WAN connection, by simply repeating the following procedure for the same connection.

1. Access this feature either from the 'Advanced' tab under the 'Services' screen, or by clicking its icon in the 'Advanced' screen. The 'Dynamic DNS' connections screen appears (see [Figure 7.480](#)). This screen displays a table that will present the different connections and their DDNS aliases.

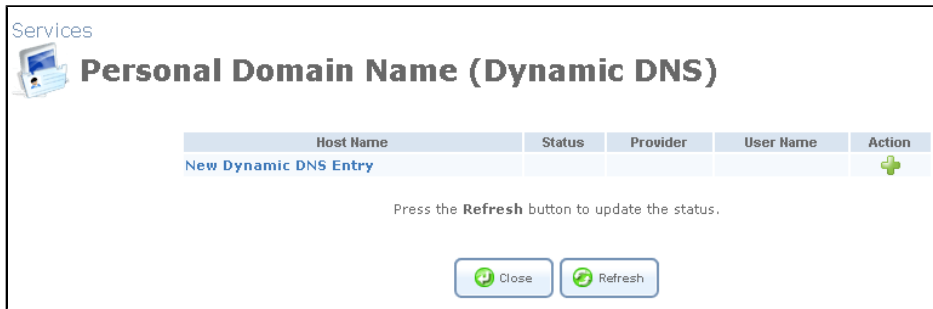


Figure 7.480. Dynamic DNS

2. Click the 'New Dynamic DNS Entry' link to add a new DDNS entry. The 'Dynamic DNS' screen appears:

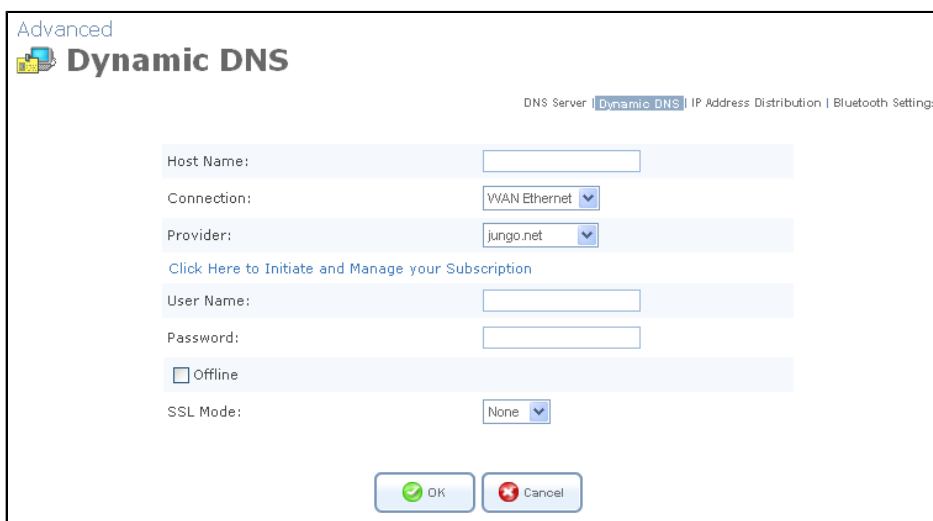


Figure 7.481. Dynamic DNS

3. Specify the DDNS parameters:

Host Name Enter your full DDNS domain name.

Connection Select the connection to which you would like to couple the DDNS service. The DDNS service will only use the chosen device, unless *failover* is enabled. In this case, the failed-to device will be used instead (assuming its route rules consent), until the chosen device is up again. For more information on failover, refer to [Section 8.6.1.3.3](#).

Provider Select your DDNS service provider. The screen will refresh, displaying the parameters required by each provider. The provider depicted herein is **dyndns**, which includes all available parameters.

Click Here to Initiate and Manage your Subscription Clicking this link will open the selected provider's account creation Web page. For example, when `dyndns.org` is selected, the following page will open: <http://www.dyndns.com/account/>.

User Name Enter your DDNS user name.

Password Enter your DDNS password.

Wildcard Select this check-box to enable use of special links such as `http://www.<your host>.dyndns.com`.

Mail Exchanger Enter your mail exchange server address, to redirect all e-mails arriving at your DDNS address to your mail server.

Backup MX Select this check-box to designate the mail exchange server to be a backup server.

Offline If you wish to temporarily take your site offline (prevent traffic from reaching your DDNS domain name), check this box to enable redirection of DNS requests to an alternative URL, predefined in your DDNS account. The availability of this feature depends on your account's level and type of service.

SSL Mode With OpenRG versions that support Secure Socket Layer (SSL), secured DDNS services are accessed using HTTPS. Upon connection, OpenRG validates the DDNS server's certificate. Use this entry to choose the certificate's validation method.

None Do not validate the server's certificate.

Chain Validate the entire certificate chain. When selecting this option, the screen will refresh (see [Figure 7.482](#)), displaying an additional combo box for selecting whether to validate the certificate's expiration time. Choose 'Ignore' or 'Check' respectively. If the certificate has expired, the connection will terminate immediately.



Figure 7.482. SSL Mode

Direct Insure that the server's certificate is directly signed by the root certificate. This option also provides the 'Validate Time' combo box for validation of the certificate's expiration time, as described above.

7.13. Advanced

7.13.1. 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 subnets within the LAN simultaneously.
- Automatically appends a domain name to unqualified names.
- Allows new domain names to be added to the database using OpenRG'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.

7.13.1.1. Viewing and Modifying the DNS Table

- To view the list of computers stored in the DNS table:
 1. Access this feature either from the 'Advanced' tab under the 'Services' screen, or by clicking its icon in the 'Advanced' screen. The DNS table will be displayed (see [Figure 7.483](#)).

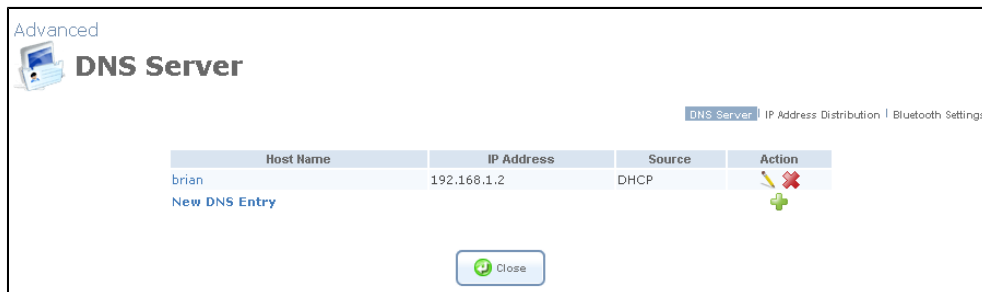


Figure 7.483. DNS Table

- To add a new entry to the list:
 1. Click the 'New DNS Entry' button. The 'DNS Entry' screen will appear (see [Figure 7.484](#)).
 2. Enter the computer's host name and IP address.
 3. Click 'OK' to save the settings.

Figure 7.484. Add or Edit a DNS Entry

- To edit the host name or IP address of an entry:
 1. Click the 'Edit' button that appears in the Action column. The 'DNS Entry' screen appears (see [Figure 7.484](#)).
 2. If the host was manually added to the DNS Table then you may modify its host name and/or IP address, otherwise you may only modify its host name.
 3. Click 'OK' to save the settings.
- To remove a host from the DNS table:
 1. Click the 'Delete' button that appears in the Action column. The entry will be removed from the table.

7.13.2. 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. OpenRG'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 OpenRG
- 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, OpenRG can act as a DHCP relay, escalating DHCP responsibilities to a WAN DHCP server. In this case, OpenRG will act merely as a router, while its LAN hosts will receive their IP addresses from a DHCP server on the WAN. With OpenRG's optional Zero Configuration Technology feature, the IP Auto Detection method detects statically-defined IP addresses in addition to OpenRG'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. For more information regarding this option, please refer to [Chapter 10](#).

7.13.2.1. DHCP Server Settings

To view a summary of the services currently being provided by the DHCP server, either use its link in the 'Advanced' tab under the 'Services' screen, or click the 'IP Address Distribution' icon in the 'Advanced' screen. The 'IP Address Distribution' screen appears:

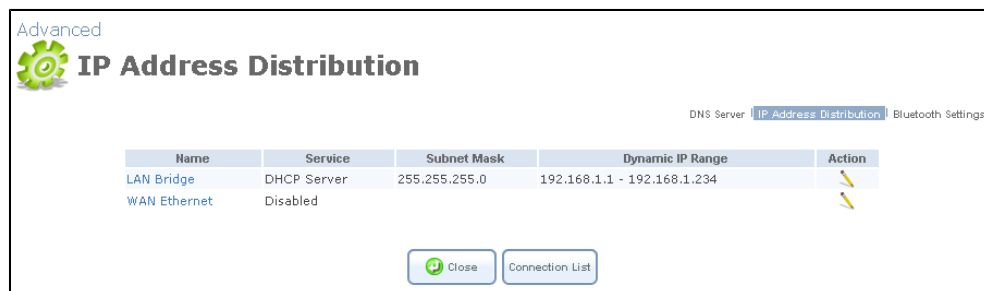


Figure 7.485. IP Address Distribution



Note: If a device is listed as 'Disabled' in the 'Service' column, then DHCP services are not being provided to hosts connected to the network through that device. This means that the gateway will not assign IP addresses to these computers, which is useful if you wish to work with static IP addresses only.

To edit the DHCP server settings for a device:

1. Click the device's action icon . The DHCP settings for this device appears:

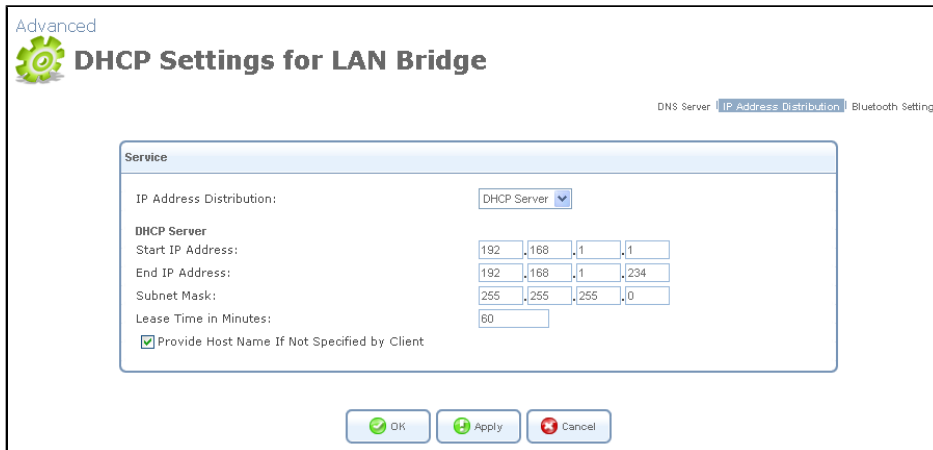


Figure 7.486. DHCP Settings for LAN Bridge

2. Select the DHCP service:

Disabled Disable the DHCP server for this device.

DHCP Server Enable the DHCP server for this device.

DHCP Relay Set this device to act as a DHCP relay (refer to [Section 7.13.2.2](#)).

3. Assuming you have chosen DHCP Server, complete the following fields:

1. **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 255.255.0.0.

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 local 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 a host name to it.

2. Click 'OK' to save the settings.

7.13.2.2. DHCP Relay Settings

To configure a device as a DHCP relay, perform the following steps:

1. Select the 'DHCP Relay' option in the 'IP Address Distribution' combo-box under the Service section (see [Figure 7.486](#)). The screen will refresh (see [Figure 7.487](#)).

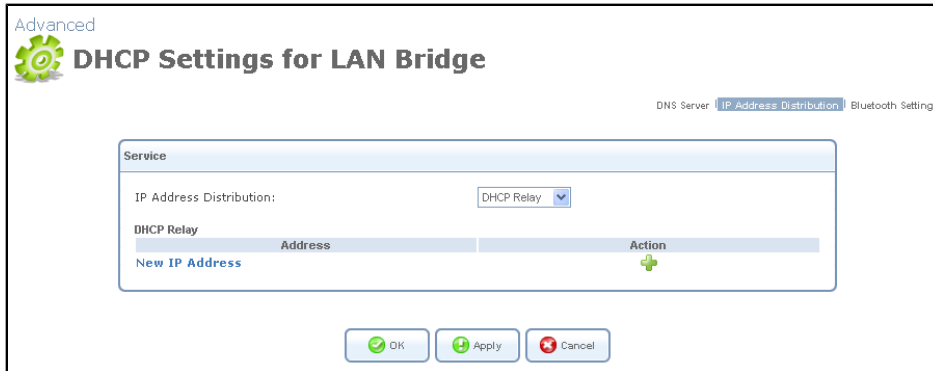


Figure 7.487. DHCP Settings for LAN Bridge

2. Click the 'New IP Address' link. The 'DHCP Relay Server Address' screen appears:

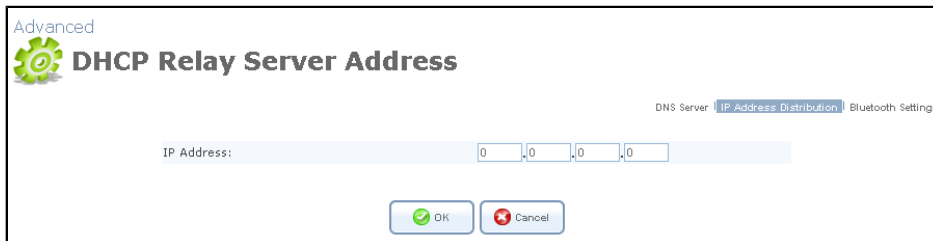


Figure 7.488. DHCP Relay Server Address

3. Specify the IP address of the DHCP server.
4. Click 'OK' to save the settings.
5. Click 'OK' once more in the 'DHCP Settings' screen.
6. Click the 'Network Connections' tab in the 'System' screen. The 'Network Connections' screen appears (see [Figure 8.12](#)).
7. Click the 'WAN Ethernet' link. The 'WAN Ethernet Properties' screen appears (see [Figure 8.123](#)).
8. In the 'Routing' section, select 'Advanced' from the combo-box. The screen will refresh (see [Figure 7.489](#)).

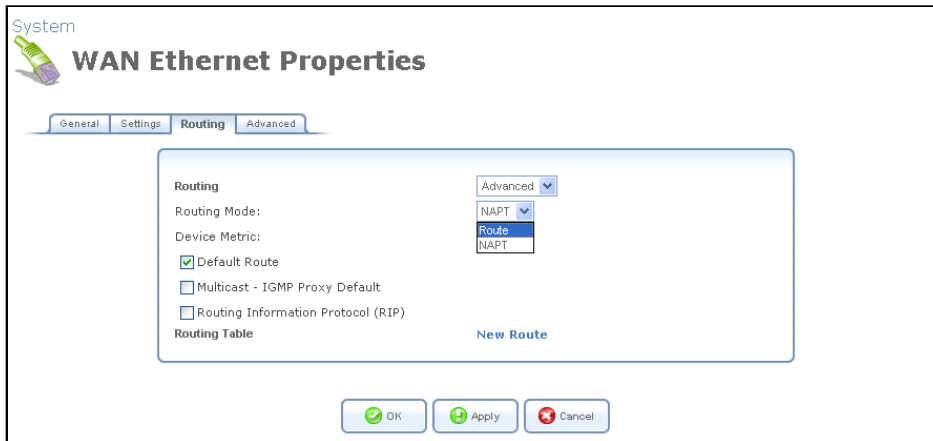


Figure 7.489. Configure WAN Ethernet -- Routing

9. In the 'Routing Mode' combo-box, select "Route". This will change OpenRG's WAN to work in routing mode, which is necessary in order for DHCP relaying to function properly.
10. Click 'OK' to save the settings.

7.13.2.3. DHCP Connections

To view a list of computers currently recognized by the DHCP server, press the 'Connection List' button that appears at the bottom of the 'IP Address Distribution' screen (see [Figure 7.485](#)). The 'DHCP Connections' screen appears:

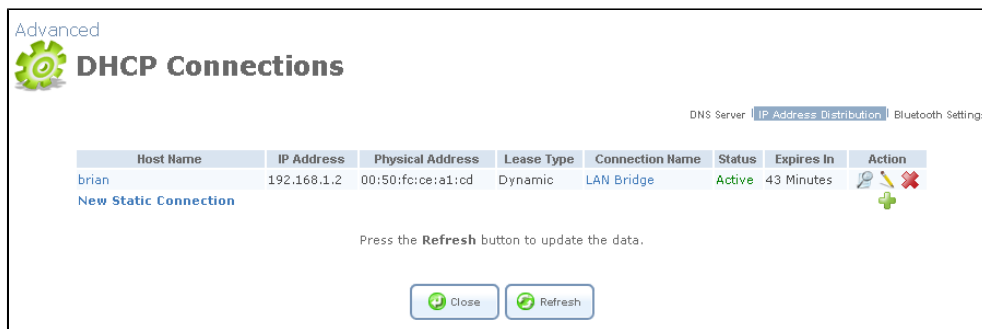


Figure 7.490. DHCP Connections

To define a new connection with a fixed IP address:

1. Click the 'New Static Connection' link. The 'DHCP Connection Settings' screen appears:

Figure 7.491. DHCP Connection Settings

2. Enter a host name for this connection.
3. Enter the fixed IP address that you would like to have assigned to the computer.
4. Enter the MAC address of the computer's network card.



Note: A device's fixed IP address is actually assigned to the specific network card's (NIC) MAC address installed on the LAN computer. If you replace this network card then you must update the device's entry in the DHCP Connections list with the new network card's MAC address.

5. Click 'OK' to save the settings.

The 'DHCP Connections' screen will reappear (see [Figure 7.492](#)), displaying the defined static connection. This connection can be edited or deleted using the standard action icons.

Host Name	IP Address	Physical Address	Lease Type	Connection Name	Status	Expires In	Action
brian	192.168.1.2	00:50:fc:ce:a1:cd	Dynamic	LAN Bridge	Active	37 Minutes	
John_Smith	192.168.1.3	00:50:fc:a5:e0:bb	Static	LAN Bridge	Active		
New Static Connection							

Figure 7.492. DHCP Connections

7.13.3. Bluetooth Settings

Yet another method to connect to OpenRG's LAN is by Bluetooth, an open specification for wireless, short-range transmission between PCs, mobile phones and other portable devices. When connected to OpenRG via Bluetooth, users can benefit from standard network connectivity, limited only by the capabilities of their connected devices. OpenRG utilizes the Bluetooth Network Encapsulation Protocol (BNEP), used by the Bluetooth Personal Area Network (PAN) profile. This layer encapsulates packets from various networking protocols,

which are transported directly over the Logical Link Control and Adaptation Protocol (L2CAP) layer.



Hardware Note: Platforms that do not feature an integrated Bluetooth chip, require a Linux-supported Bluetooth dongle, which can be connected to the gateway either by USB or PCI.

As soon as a Bluetooth dongle is connected, OpenRG can be found and connected to by Bluetooth devices. To configure OpenRG's Bluetooth settings, perform the following steps:

1. Access the Bluetooth settings either from its link in the 'Advanced' tab under the 'Services' screen, or by clicking the 'Bluetooth Settings' icon in the 'Advanced' screen. The 'Bluetooth Settings' screen appears. Select the 'Enabled' check box to enable this feature.

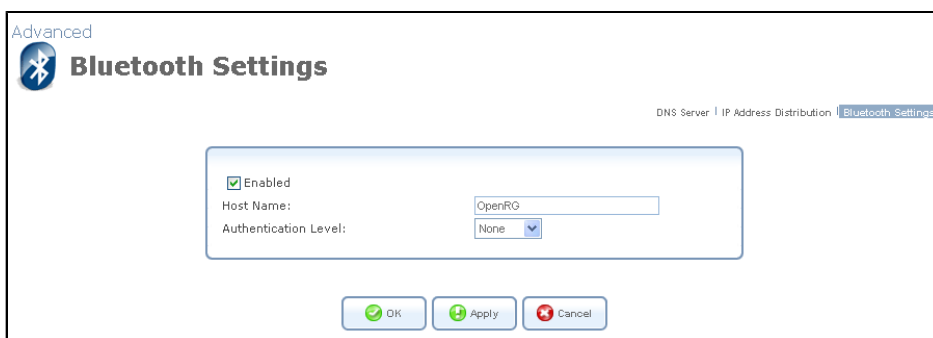


Figure 7.493. Bluetooth Settings

Enabled Select this check-box to enable Bluetooth connections to OpenRG.

Host Name OpenRG's identification name in the PAN. You can change the default to any string.

Authentication Level Select the level of authentication to be performed upon a connection request:

None Connect without authentication.

Enabled Enable authentication using a pin number, which will have to be provided by the device wishing to connect.

Encrypt Enable and encrypt the authentication method.

PIN Enter a value for the authentication/encryption key if you selected the 'Enabled' or 'Encrypted' options above.

2. Click 'OK' to save the settings.

The new Bluetooth connection will be added to the network connections list under the LAN bridge, and will be configurable like any other connection.

7.13.4. RADIUS Server

A Remote Authentication Dial-in User Service (RADIUS) server is most commonly a "third party" server, used for authentication of wireless clients who wish to connect to an access point. The wireless client contacts an access point (a RADIUS client), which in turn communicates with the RADIUS server. The RADIUS server performs the authentication by verifying the client's credentials, to determine whether the device is authorized to connect to the access point's LAN. If the RADIUS server accepts the client, it responds by exchanging data with the access point, including security keys for subsequent encrypted sessions. OpenRG can act both as a RADIUS client and a server, and can be used for the authentication of any clients—wireless or wired.

This enables a scenario of multiple gateways acting as RADIUS clients, connected to a "master" gateway that acts as a RADIUS server. Such a scenario can be useful in an enterprise consisting of multiple divisions.

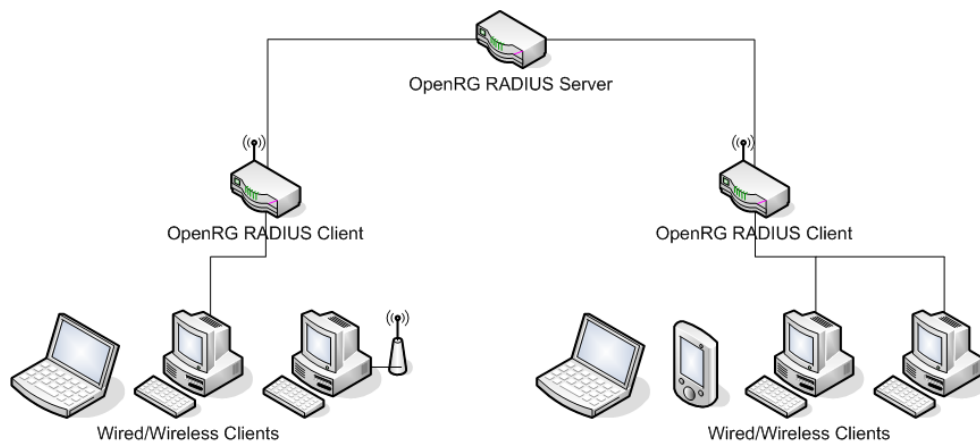


Figure 7.494. RADIUS Server Scenario

7.13.4.1. RADIUS Server Configuration

OpenRG as a RADIUS client is described in the LAN Wireless section of this manual (section [Section 8.4.7](#)). To configure OpenRG as a RADIUS server, perform the following:

1. Access the RADIUS Server settings either from the link in the 'Advanced' tab under the 'Services' screen, or by clicking the 'RADIUS Server' icon in the 'Advanced' screen. The 'RADIUS Server' screen appears.

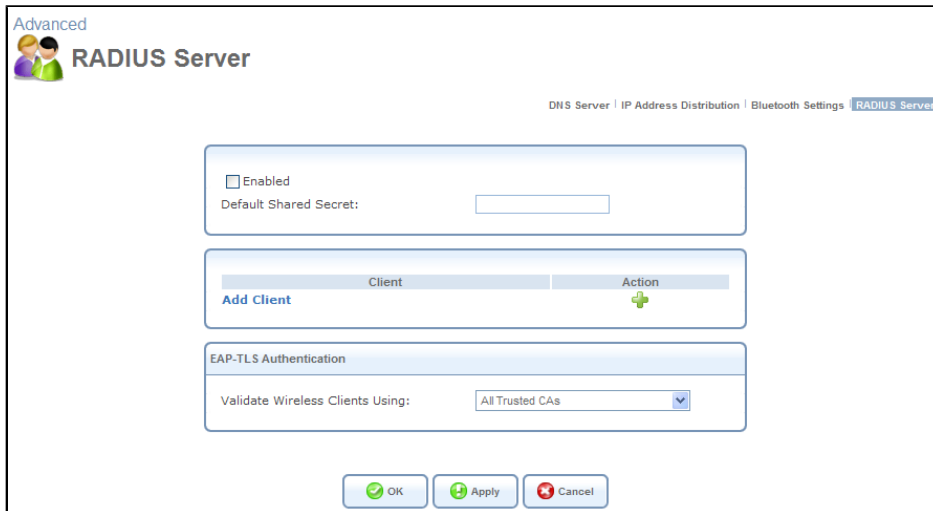


Figure 7.495. RADIUS Server

2. Check the 'Enabled' check box to enable this feature.
3. If you would like to set a shared secret that any RADIUS client can provide when requesting authentication, specify a 'Default Shared Secret'.
4. You can also set specific shared secrets for known clients by clicking 'Add Client'. The 'Add RADIUS Client' screen appears.

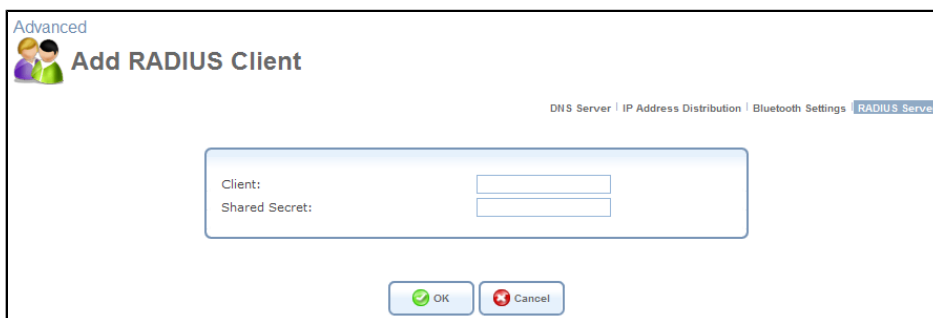


Figure 7.496. Add RADIUS Client

5. Enter the client's IP address and a shared secret value, and click 'OK'. You are routed back to the 'RADIUS Server' screen, which now displays the newly added client.



Figure 7.497. Newly Added Client

7.13.4.2. RADIUS Authentication Algorithms

OpenRG's RADIUS server utility uses six different authentication algorithms. These are:

- PAP
- CHAP
- MSCHAP
- MSCHAP v2
- EAP PEAP MSCHAP v2
- EAP TLS

While the first four use only username and password combinations for authentication, the EAP-PEAP algorithm utilizes the server's certificate for authentication, and EAP TLS authenticates both the client and server with certificates (for more information about certificates, refer to [Section 8.9.4](#)). When a request is received from a client, a negotiation begins in which certificates are passed between the client and server, resolving in either acceptance or rejection. In the 'EAP-TLS Authentication' section of the 'RADIUS Server' screen, you can select the certificate by which to validate wireless clients. Select "All Trusted CAs" to validate a client with any of OpenRG's trusted certificates, or choose a specific certificate from the list.

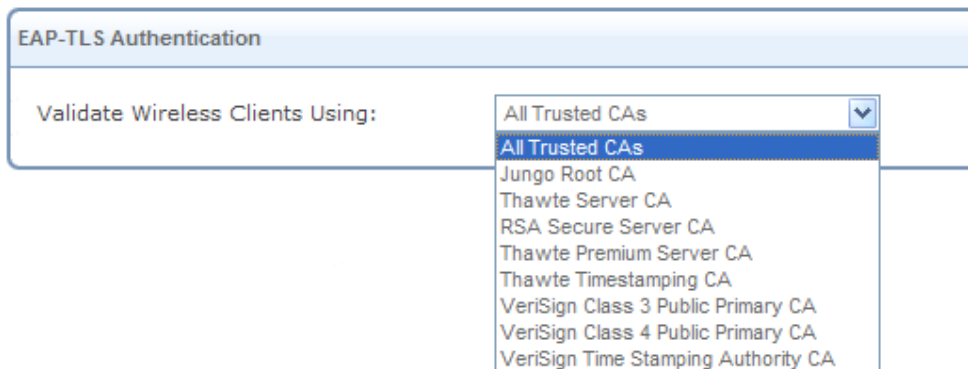


Figure 7.498. EAP-TLS Authentication

7.13.4.3. Connecting Windows Clients with RADIUS Authentication

This section describes the methods for connecting a wireless Windows™ client to a RADIUS client gateway, served by a RADIUS server gateway. There are two methods; one uses the EAP PEAP MSCHAP v2 authentication algorithm and the other uses the EAP TLS algorithm. The following must be configured:

- An OpenRG gateway serving as a RADIUS server
- An OpenRG gateway serving as a RADIUS client
- A Windows computer serving as a wireless client

Configure the OpenRG RADIUS server as described earlier (refer to [Section 7.13.4.1](#) [441]). Next, configure the OpenRG RADIUS client as follows:

1. Access the LAN Wireless network connection settings from the 'Network Connections' link in the 'System' screen, and select the 'Wireless' tab.

The screenshot shows the 'LAN Wireless 802.11g Access Point Properties' window with the 'Wireless' tab active. The configuration includes:

- Wireless Network (SSID):** john_smith
- SSID Broadcast:**
- 802.11 Mode:** 802.11b/g Mixed
- Channel:** 11 - 2.462GHz (FCC)
- Network Authentication:** Open System Authentication
- MAC Filtering Mode:** Disable
- MAC Filtering Table:** Empty table with columns for MAC Address and Action.
- Security:** 802.1X WEP
- RADIUS Server:**
 - Server IP: 192.168.1.1
 - Server Port: 1812
 - Shared Secret: *****
- Advanced Settings:**
 - Transmission Rate: Auto
 - CTS Protection Mode: None
 - Beacon Interval: 100 ms
 - DTIM Interval: 1 ms
 - Fragmentation Threshold: 2346
 - RTS Threshold: 2347

Figure 7.499. LAN Wireless Settings

You may change your wireless network's name (SSID) from the default "openrg" to something more personal (in this example, "john_smith").

2. In the 'Security' section, select either 802.1X WEP or WPA. If you selected WPA, select 802.1X as the authentication method.
3. In the 'RADIUS Server' section, enter the IP address and shared secret of the gateway serving as a RADIUS server (192.168.1.1), in their respective fields.
4. Click 'OK' to save the settings.

The configuration of the wireless client differs a little between the two algorithms. Start the configuration by performing the following:

1. Access the Windows 'Network Connections' utility and double-click the wireless network connection icon. The 'Wireless Network Connection' window displays the wireless networks in range.

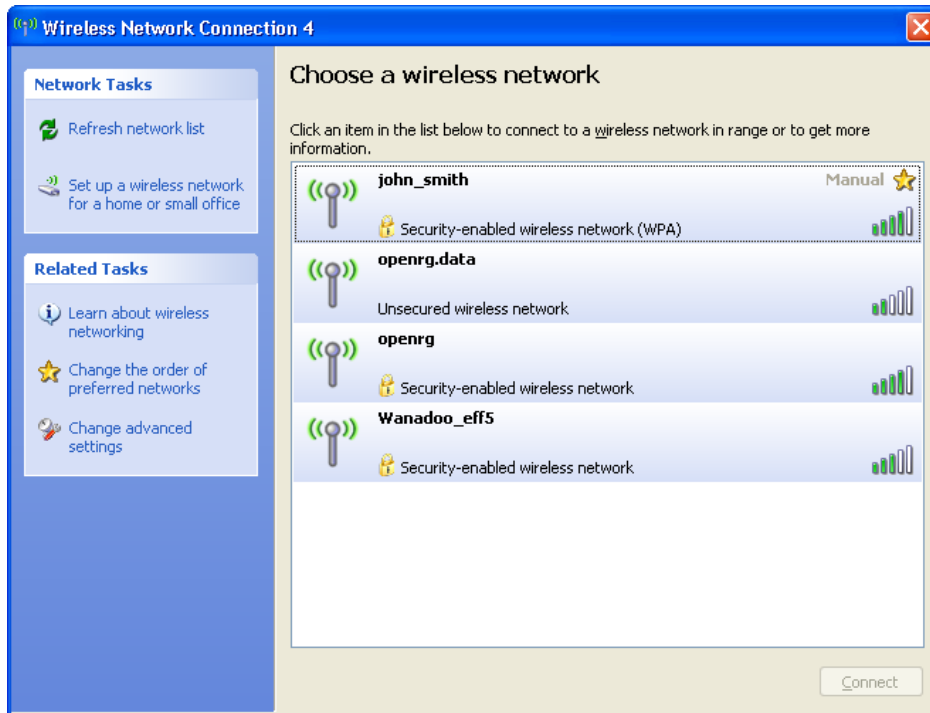


Figure 7.500. Wireless Network Connection Window

2. Click your wireless network entry and then click the 'Change advanced settings' link at the bottom of the side-bar (under "Related Tasks"). The 'Wireless Network Connection Properties' window appears. Click its 'Wireless Networks' tab.

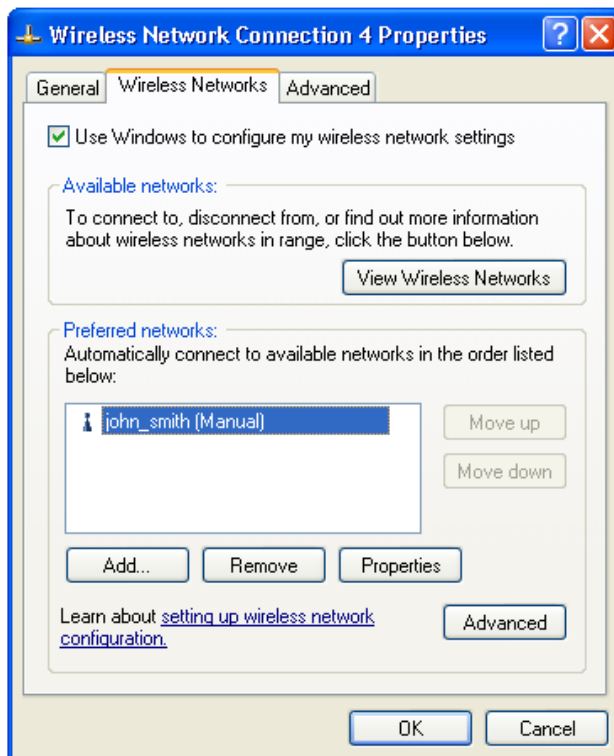


Figure 7.501. Wireless Network Connection Properties Window

- Click your wireless network entry and then click 'Properties'. The connection's properties window appears.

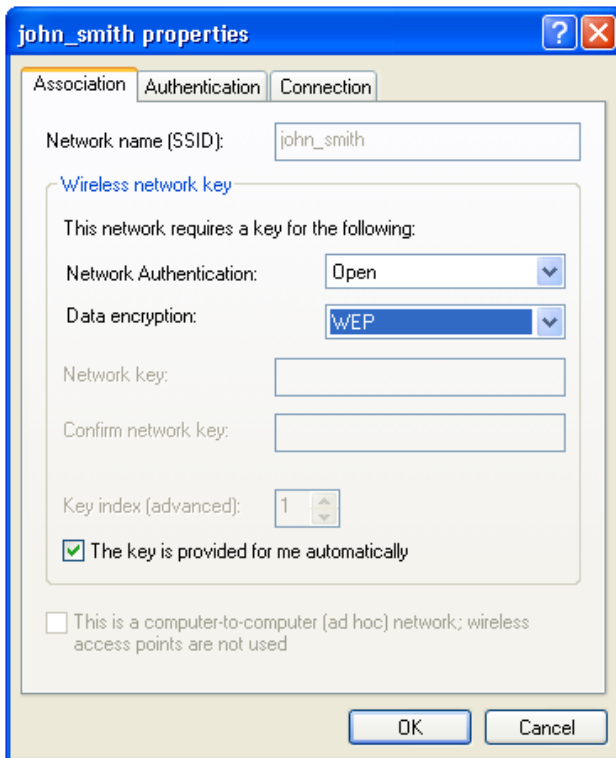


Figure 7.502. Connection Properties Window

- Verify that your chosen data encryption method is selected. For example, if you had configured the wireless connection (in the RADIUS client) with 802.1X WEP, the 'Data encryption' drop-down menu should display "WEP".
- Verify that "The key is provided for me automatically" check box is selected.
- Click the 'Authentication' tab. Verify that the 'Enable IEEE 802.1x' check box is selected.

The procedure now changes according to the algorithm you wish to use.

- With the **EAP PEAP MSCHAP v2** algorithm, negotiation is performed using a server's certificate and a client's user name and password.

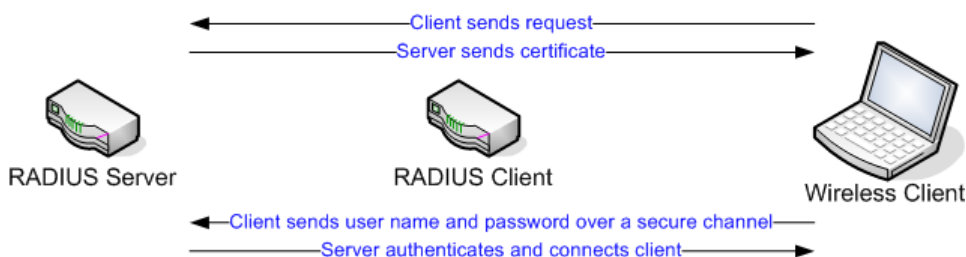


Figure 7.503. Negotiation with the EAP PEAP MSCHAP v2 Algorithm

To use this algorithm, perform the following. For the EAP TLS algorithm, refer to diagram 'Negotiations with the EAP TLS Algorithm'.

1. In the 'Authentication' tab, select the 'Protected EAP (PEAP)' option.

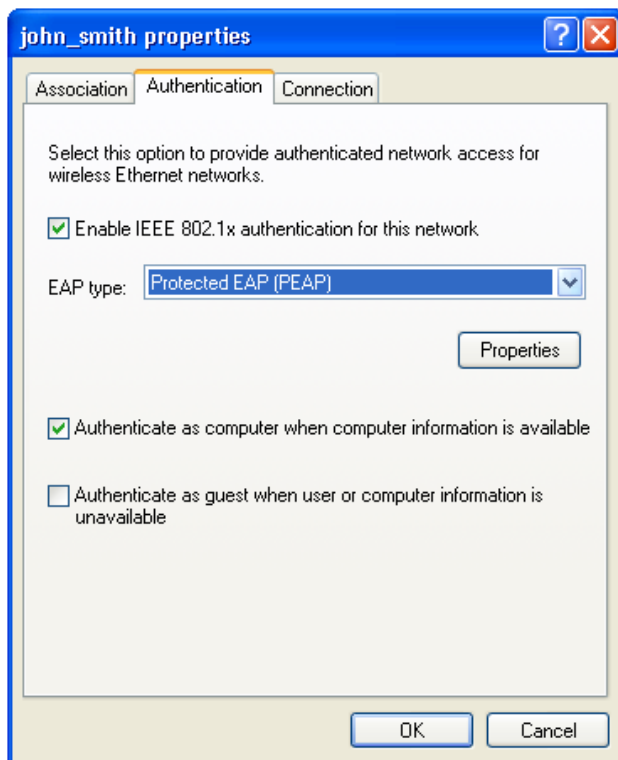


Figure 7.504. Connection Properties Window – EAP PEAP Algorithm

2. Click 'Properties'. The 'Protected EAP Properties' window appears.

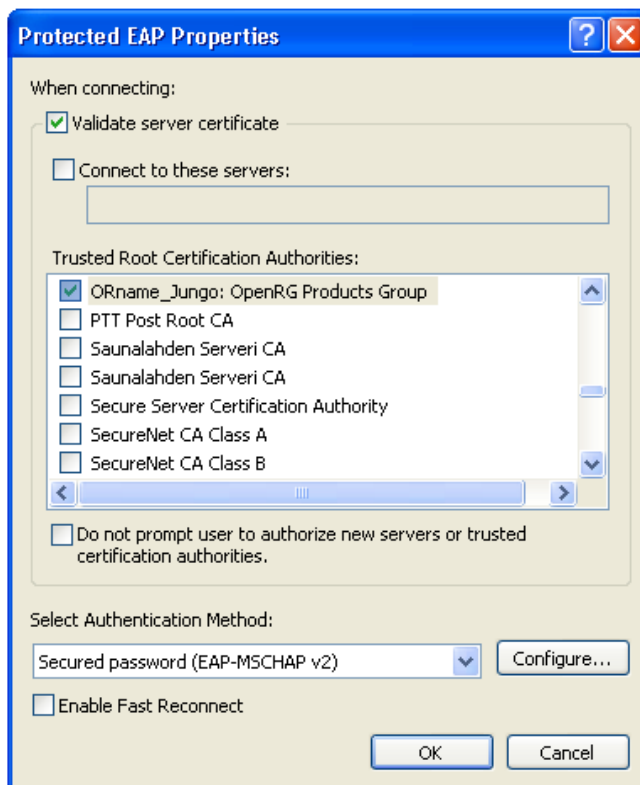


Figure 7.505. Protected EAP Properties

3. Verify that the 'Validate server certificate' check box is selected.
4. Next, you must select a Certificate Authority (CA) by which Windows will verify the RADIUS server. In order for OpenRG's CA to appear in the 'Trusted Root Certification Authorities' list as depicted in [Figure 7.505](#), you must first load the certificate information from the OpenRG RADIUS server to Windows. Perform the following:
 - a. In the OpenRG RADIUS server WBM, click the 'Certificates' icon in the 'Advanced' screen. The 'Certificates' screen appears, displaying OpenRG's default certificate under the 'OpenRG's Local' tab.

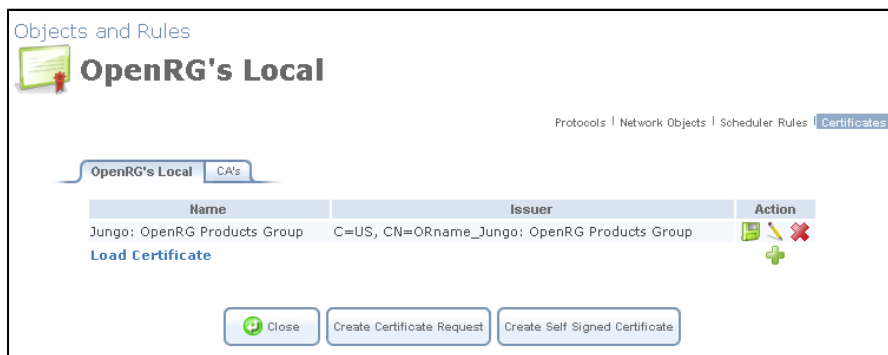



Figure 7.506. Certificates

- b. Click the  action icon of the certificate entry, and select 'Open' in the download dialogue window. The 'Certificate' window appears.

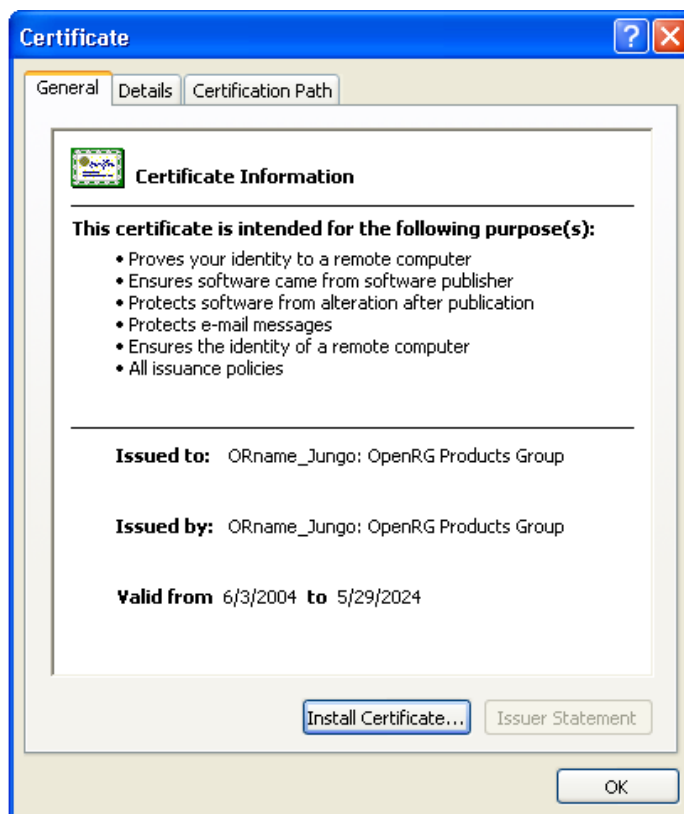


Figure 7.507. Certificate

- c. Click 'Install Certificate...'. The 'Certificate Import Wizard' commences. Click 'Next', and select the 'Place all certificates in the following store' option. Click 'Browse' to select the 'Trusted Root Certification Authorities' certificate store.

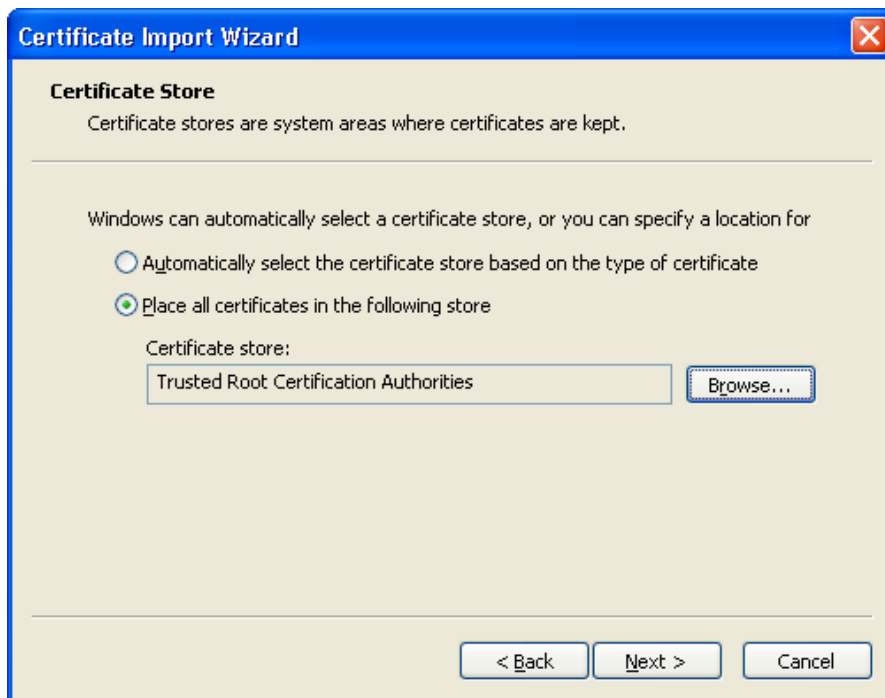


Figure 7.508. Certificate Import Wizard

- d. Complete the wizard (click 'Next' and then 'Finish').
5. Back in the 'Protected EAP Properties' window (see [Figure 7.505](#)), select the OpenRG CA in the 'Trusted Root Certification Authorities' list.
6. Verify that the "Secured password (EAP-MSCHAP v2)" option is selected in the 'Select Authentication Method' drop-down list, and click 'Configure...'.
7. Uncheck the 'Automatically use my Windows logon name and password' option in the dialogue window, and click 'OK'.



Figure 7.509. EAP MSCHAPv2 Properties

8. Click 'OK' on all open configuration windows.

To connect to the wireless network, click your wireless network entry in the 'Wireless Network Connection' window (see [Figure 7.500](#)), and then click 'Connect'. The following message bubble appears.

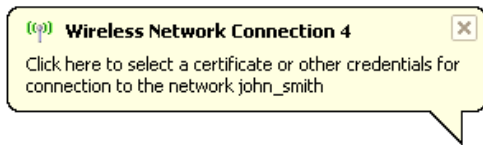


Figure 7.510. Wireless Network Connection Message

Click the bubble. The 'Enter Credentials' window appears.

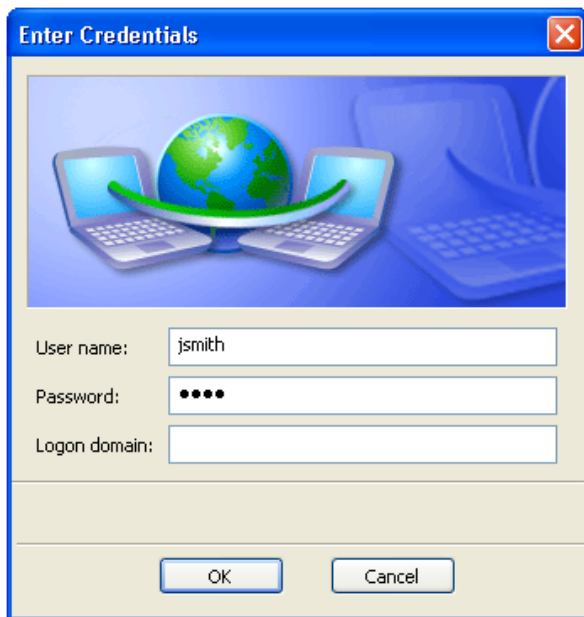


Figure 7.511. Enter Credentials

Enter a user name and password of a user with administrative permissions, predefined in the OpenRG RADIUS server users' list (leave the 'Logon domain' field empty). The wireless connection is now authenticated and established.

- With the **EAP TLS** algorithm, negotiation is performed using both server and client certificates.

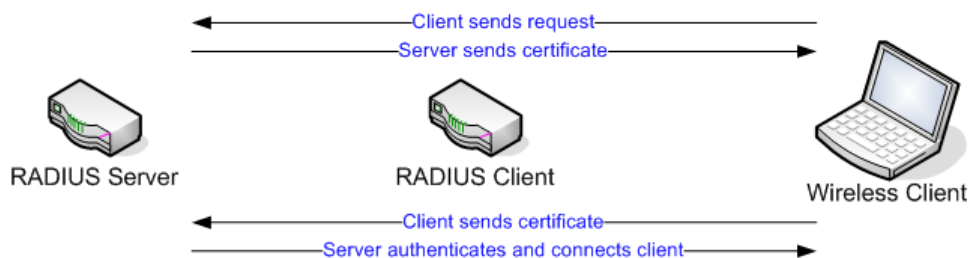


Figure 7.512. Negotiation with the EAP TLS Algorithm

To use this algorithm, perform the following.

1. In the 'Authentication' tab, select the 'Smart Card or other Certificate' option.

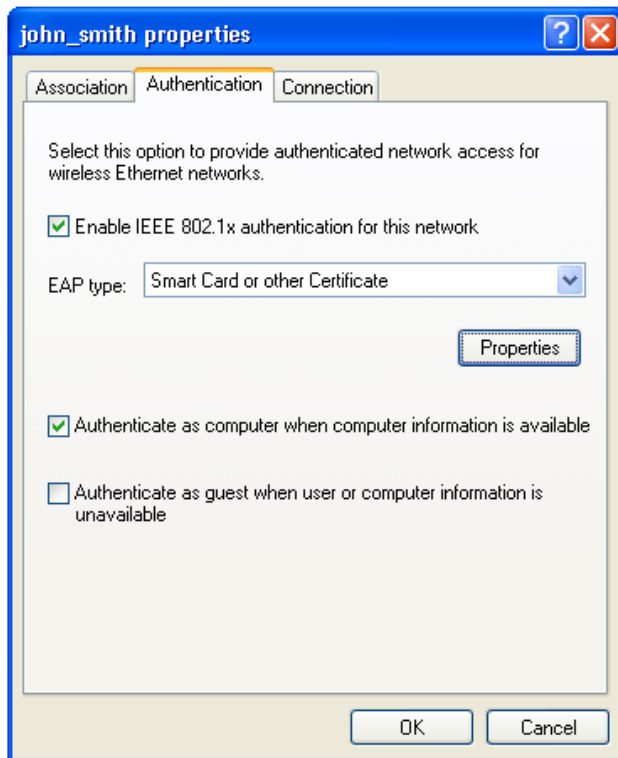


Figure 7.513. Connection Properties Window – EAP TLS Algorithm

2. Click 'Properties'. The 'Smart Card or other Certificate Properties' window appears.

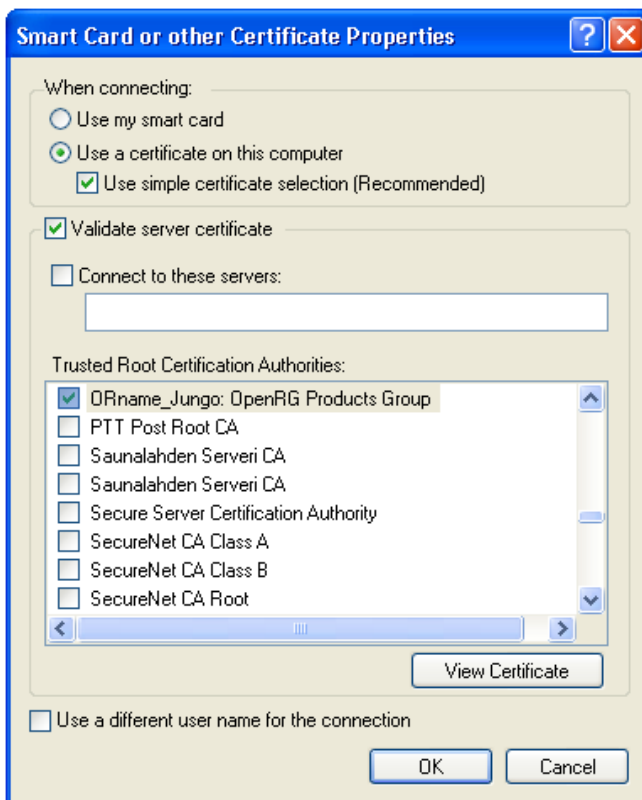


Figure 7.514. Smart Card or other Certificate Properties

3. Verify that the 'Validate server certificate' check box is selected.
4. Verify that the 'Connect to these servers' check box is not selected.
5. Next, you must select a Certificate Authority (CA) by which Windows will verify the RADIUS server. In order for OpenRG's CA to appear in the 'Trusted Root Certification Authorities' list as depicted in [Figure 7.514](#), you must first load the certificate information from the OpenRG RADIUS server to Windows. This procedure is identical to the one described in the EAP PEAP MSCHAP v2 configuration above.
6. Select the OpenRG CA in the 'Trusted Root Certification Authorities' list.
7. Click 'OK' on all open configuration windows.

Since EAP TLS uses certificates for verification of both the server and the client, an additional certificate and private key must be made available for verification of the Windows client. These are commonly available in a **.p12** file, which can be obtained from a certificate authority such as Verisign™, and should be placed on the Windows client. A certificate that authorizes these two must then be saved on the RADIUS server. After obtaining the **.p12** file, save it on the Windows client and perform the following:

1. Load the **.p12** file.
 - a. Double-click the .p12 file. The 'Certificate Import Wizard' commences.
 - b. Click 'Next', and enter the private key's password.
 - c. Click 'Next', and select the 'Place all certificates in the following store' option. Click 'Browse' to select the 'Personal' certificate store.

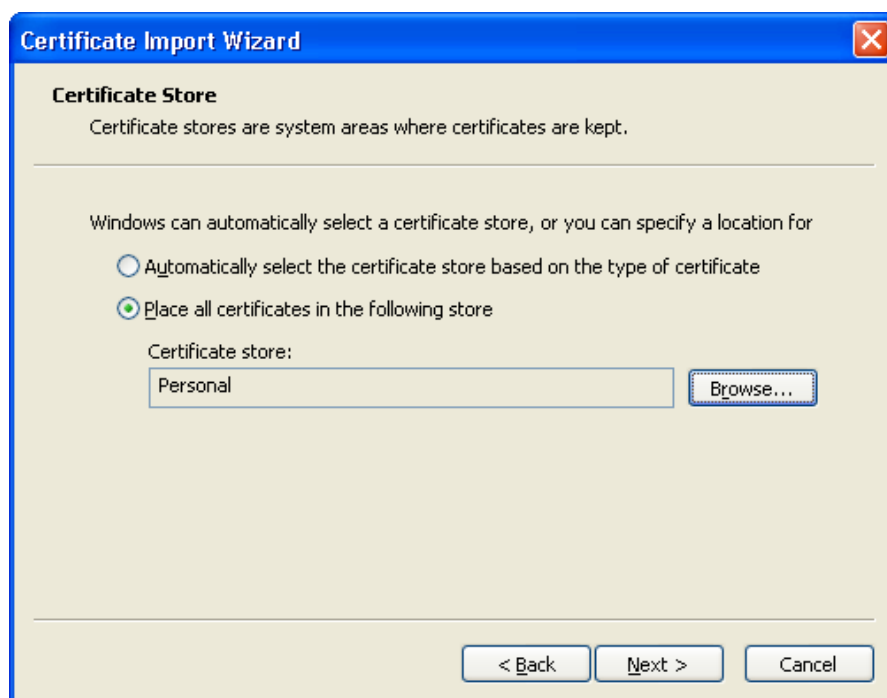


Figure 7.515. Certificate Import Wizard

- d. Complete the wizard.
2. Load the authorization certificate to the RADIUS server. Note that either this certificate, or "All Trusted CAs", should be selected in the 'EAP-TLS Authentication' section of the 'RADIUS Server' screen, as described in [Section 7.13.4.2](#) [442].
- a. In the OpenRG RADIUS server WBM, click the 'Certificates' icon in the 'Advanced' screen. The 'Certificates' screen appears. Click the 'CA's' tab.

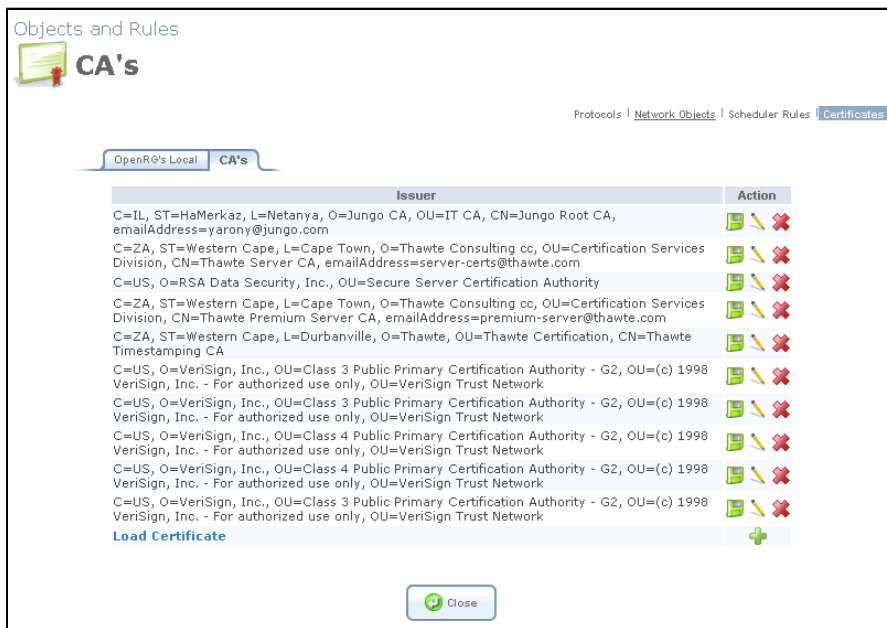


Figure 7.516. CA's

- b. Click 'Load Certificate' and then 'Browse' to locate the certificate file.

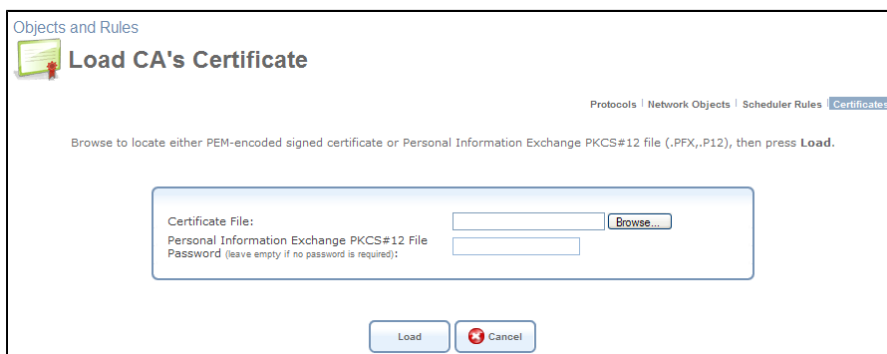


Figure 7.517. Load CA's Certificate

- c. Click 'Load'. The certificate is added to the list in the 'CA's' screen.

To connect to the wireless network, click your wireless network entry in the 'Wireless Network Connection' window (see [Figure 7.500](#)), and then click 'Connect'. A confirmation screen appears, informing of the RADIUS server's certificate. Accept the certificate to establish the connection.

8

System

8.1. Overview

The 'Overview' screen (see [Figure 8.1](#)) presents a summary of OpenRG's system status indication. This includes various details such as version number, release date and type of platform .

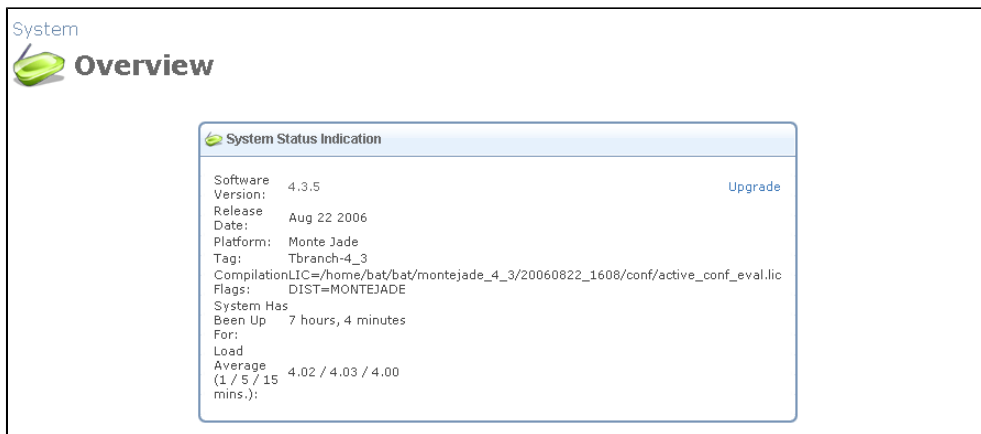


Figure 8.1. System Monitoring Overview

8.2. Settings

8.2.1. Overview

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

Settings
Overview | Date and Time

System Settings

System

OpenRG's Hostname:

Local Domain:

OpenRG Management Console

Automatic Refresh of System Monitoring Web Pages

Warn User Before Configuration Changes

Session Lifetime: Seconds

User Interface Theme:

Management Application Ports

Primary HTTP Management Port:

Secondary HTTP Management Port:

Primary HTTPS Management Port:

Secondary HTTPS Management Port:

Primary Telnet Port:

Secondary Telnet Port:

Secure Telnet over SSL Port:

Jungo.net Port:

Jungo.net SSL Port:

Management Application SSL Authentication Options

Primary HTTPS Management Client Authentication:

Secondary HTTPS Management Client Authentication:

Secure Telnet over SSL Client Authentication:

System Logging

System Log Buffer Size: KB

Remote System Notify Level:

Persistent System Log

Security Logging

Security Log Buffer Size: KB

Remote Security Notify Level:

Persistent Security Log

Outgoing Mail Server

Server:

From Email Address:

Port:

Server Requires Authentication

Swap

Enabled

Status:

Swap Size: MB

HTTP Interception

Intercept HTTP Traffic for Assisting with Internet Connectivity Problems

Monitor Connectivity to the Internet Service Provider

Host Information

Enable Auto Detection of Host Services

Figure 8.2. System Settings

System Configure general system parameters.

- **OpenRG'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.

OpenRG 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.
- **User Interface Theme** You can select an alternative GUI theme from the list provided.

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 port



Note: You can selectively enable these management application ports in the 'Remote Administration' screen (for more information, refer to [Section 8.7.3](#)).

Management Application SSL Authentication Options Configure the remote client authentication settings, for each of the following OpenRG management options:

- Primary HTTPS Management Client Authentication
- Secondary HTTPS Management Client Authentication
- Secure Telnet over SSL Client Authentication

The applied authentication settings can be either of the following:

- **None** The client is not authenticated during the SSL connection. Therefore, the client does not need to have a certificate recognized by OpenRG, which can be used for authentication (for more information about certificates, refer to [Section 8.9.4](#)). This is the default setting for all of the mentioned management options.

- **Required** The client is required to have a valid certificate, which is used instead of the regular login procedure. If the client does not have such a certificate, the connection is terminated.
- **Optional** If the client has a valid certificate, it may be used for authentication instead of the regular login procedure. This means that in case of the HTTPS management session, the user, having a valid certificate, directly accesses the 'Network Map' screen of OpenRG's WBM.

In case of the secure Telnet connection, the user, having a valid certificate, directly accesses OpenRG's CLI prompt. To learn how to establish a secure Telnet connection to OpenRG, refer to [Section 8.7.3](#). Note that the 'Common Name' (**CN**) parameter in the **Subject** field of a client's certificate should contain an existing username, to which administrative permissions are assigned.

System Logging Configure system logging parameters. You can view the system log in the 'System Log' screen under 'Monitor' (refer to [Section 8.5.3](#)).

- **System Log Buffer Size** Set the size of the system log buffer in Kilobytes.
- **Remote System Notify Level** By default, the 'None' option is selected, which means that OpenRG will not send notifications to a remote host. To activate the feature, select one of the following notification types:
 - Error
 - Warning
 - Information

The screen refreshes, displaying the 'Remote System Host IP Address' field.

Remote System Host IP Address: ...

Figure 8.3. Remote System Host IP Address

Enter the remote host's IP address and click 'Apply'.



Note: If you would like to view OpenRG's system logs on a LAN host, you must first install and run the syslog server.

- **Persistent System Log** Select this check box to save the system log to the Flash---the gateway's permanent memory. This will prevent the system log from being erased when the gateway reboots. Note that by default, this check box is deselected.

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
 - Information
- **Persistent Security Log** Select this check box to save the security log to the Flash. This will prevent the security log from being erased when the gateway reboots. Note that by default, this check box is deselected.



Note: Do not leave the persistent logging feature enabled permanently, as continuous writing of the log files to the Flash reduces gateway's performance.

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 This feature enables you to free a portion of the RAM by creating a swap file on the storage device connected to OpenRG. This is especially useful for platforms with a small RAM. To activate this feature:

1. Verify that a storage device is connected to OpenRG.
2. Select the 'Enabled' check box.
3. In the 'Swap Size' field, enter a swap file size in megabytes.
4. Click 'Apply'. A swap file is created on the storage device, and the feature's status changes to 'Ready'.

HTTP Interception

- **Intercept HTTP Traffic for Assisting with Internet Connectivity Problems** If the WAN device is physically disconnected or cannot obtain an up and running status (even

if an Internet connection exists), OpenRG will display an attention screen providing troubleshooting options (these options are displayed with distributions containing the "Support Cost Reduction (SCR)" feature; otherwise an explanation of the connection's status is provided).

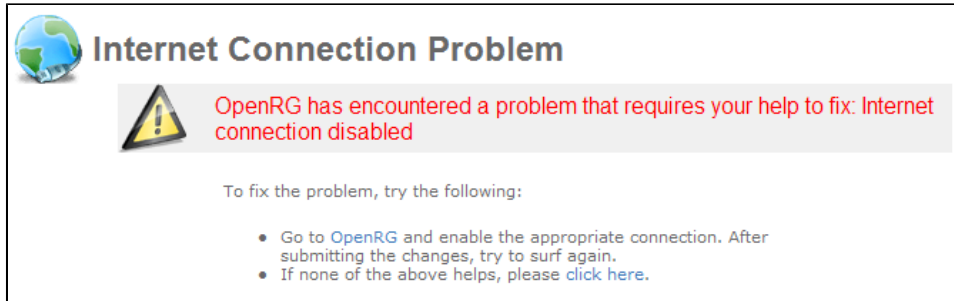


Figure 8.4. Internet Connection Problem

This screen is displayed instead of the browser's standard 'The page cannot be displayed' page. For more information, refer to [Section 2.3.3](#).

- **Monitor Connectivity to the Internet Service Provider** The WAN device can be up and running even if no Internet connection is available (for example, when a static IP address is defined). Select this check box to have OpenRG perform periodic Internet connectivity checks and display the attention screen if the connection becomes unavailable.

Host Information OpenRG can auto-detect its LAN hosts' properties, available services, traffic statistics, and connections (for more information refer to [Section 6.1](#)). To enable this feature, select its check box.

8.2.2. Date and Time

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

1. Click the 'Date and Time' icon in the 'Advanced' screen of the WBM. The 'Date and Time' settings screen appears.

Settings
Date and Time

Overview | Date and Time

Localization

Local Time: Sep 10, 2006 15:42:41
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 Sync Now

Time Server	Action
ntp.jungo.com	
New Entry	

Status: Got time update from server, Last Update: Sun Sep 10 08:28:00 2006

Press the Refresh button to update the status.

OK Apply Cancel Clock Set Refresh

Figure 8.5. Date and Time Settings

2. Select the local time zone from the drop-down menu. If you wish to manually define or correct your local time zone, select the 'Other' option from the drop-down menu. The 'GMT Offset' field appears, in which you can enter your local time's offset from the Greenwich Mean Time (GMT).

OpenRG can automatically detect the daylight saving (summer time) settings for a large number of time zones, according to its internal time zone database. However, there are time zones for which the daylight saving time has not been specified in the database, as it may vary occasionally. In case your local daylight saving information has not been detected in the database, the following fields will be displayed, enabling you to specify your time zone's daylight saving settings:

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, proceed as follows:
 - Select the 'Enabled' check box under the 'Automatic Time Update' section.

- Select the protocol to be used to perform the time update by selecting either the 'Time of Day' or 'Network Time Protocol' radio button.
- In the 'Update Every' field, specify the frequency of performing the update.
- By default, OpenRG is configured with Jungo's NTP server for testing purposes only. You can define another time server address by clicking the 'New Entry' link at the bottom of the 'Automatic Time Update' section. You can find a list of time server addresses sorted by region at <http://www.pool.ntp.org>.

In addition, OpenRG can function as a Simple Network Time Protocol (SNTP) server, enabling you to automatically update the time settings of your computers from a single but reliable source. By default, OpenRG's SNTP server is enabled. To synchronize time between the SNTP server and a PC connected to the gateway, perform the following:

1. In the 'Automatic Time Update' section of the 'Date and Time' screen (see [Figure 8.5](#)), click the 'Network Time Protocol (NTP)' radio button.
2. Click 'OK' to save the settings.
3. On a PC connected to the gateway, perform the following:

 Note: The following explanations are based on the Windows XP user interface.

1. In Control Panel, double-click the 'Date and Time' icon. The 'Date and Time Properties' window appears.

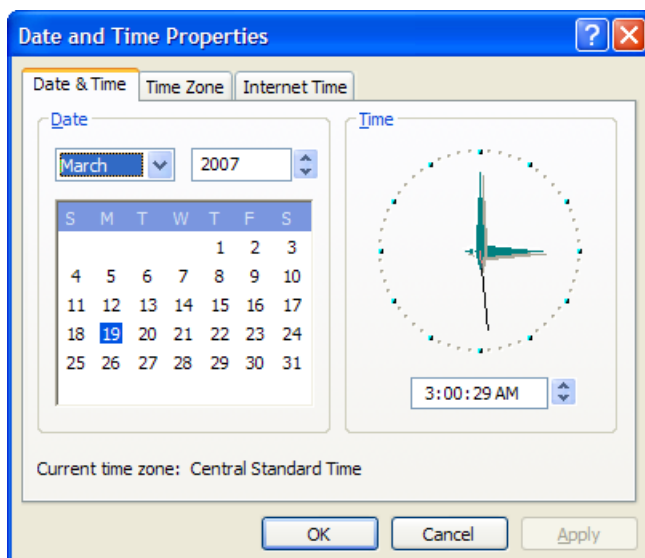


Figure 8.6. Windows – Date and Time Properties

2. Click the 'Internet Time' tab. The window changes to the following.

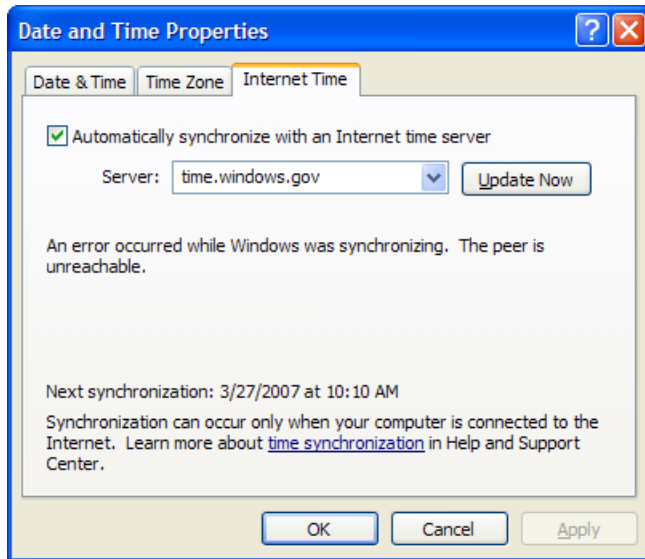


Figure 8.7. Windows – Internet Time Screen

3. In the 'Server' field, enter OpenRG's LAN IP address (The default one is 192.168.1.1).
4. Click 'Update Now'. Windows will synchronize with OpenRG's SNTP server. In addition, Windows will perform a periodical synchronization with the SNTP server.
5. Click 'OK' to save the settings.

8.3. Users

The 'Users' screen lists the currently defined users and provides a link to add new users. You may also group users according to your preferences. This screen can also be accessed by clicking the 'Users' icon in the 'Advanced' screen. The "Administrator" is a default user provided by the system.

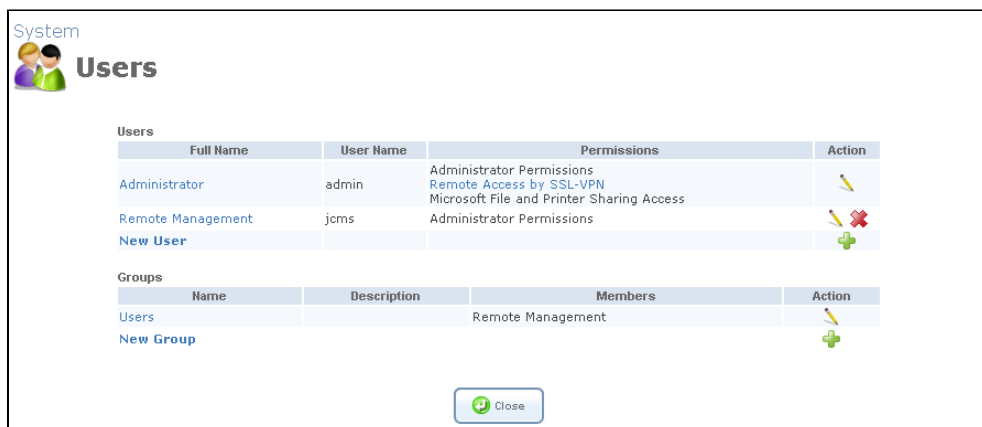


Figure 8.8. Users

8.3.1. User Settings

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

Figure 8.9. User Settings

8.3.1.1. General

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 the system settings via the Web-based management or Telnet.
- **Remote Access by SSL-VPN** Grants remote access to OpenRG using the SSL-VPN protocol.
- **Mail Server Access** Grants the permission to use OpenRG's mail server. When selecting this option, you must also enable the user's home directory and mailbox in the following sections.
- **Microsoft File and Printer Sharing Access** Grants the permission to use shared files and printers.
- **FTP Server Access** Grants the permission to use OpenRG's FTP server.
- **Internet Printer Access** Grants the permission to use an Internet Printing Protocol (IPP) printer.
- **Remote Access by VPN** Grants remote access to OpenRG using the VPN protocol.

8.3.1.2. Disk Management

Enable User Home Directory By default, this option is selected. When activated, it creates a directory for the user in the 'Home' directory of the system storage area. This directory is necessary when using various applications, such as the mail server. For more information, refer to [Section 6.4.2](#).

8.3.1.3. Mail Box

Enabled Select or deselect this check box to enable or disable this feature.

Quota Limit the user's mail box quota by entering the number of megabytes, or select "Unlimited" from the drop-down menu.

Aliases You may enter nicknames (separated by commas or spaces) for the user's email address.

8.3.1.4. E-Mail Notification

You can use email notification to receive indications of system events for a predefined severity classification. The available types of events are 'System' or 'Security' events. The available severity of events are 'Error', 'Warning' and 'Information'.

If the 'Information' level is selected, the user will receive notification of the 'Information', 'Warning' and 'Error' events. If the 'Warning' level is selected, the user will receive notification of the 'Warning' and 'Error' events etc.

To configure email notification for a specific user:

- Make sure you have configured an outgoing mail server in 'System Settings'. A click on the 'Configure Mail Server' link will display the 'System Settings' screen where you can configure the outgoing mail server.
- Enter the user's email address in the 'Address' field of the 'Email' section.
- Select the 'System' and 'Security' notification levels in the 'System Notify Level' and 'Security Notify Level' drop-down menu respectively.

8.3.2. Group Settings

You may assemble your defined users into different groups, based on different criteria—for example, home users versus office users. By default, new users will be added to the default group "Users". To add a new group, click the 'New Group' link. The 'Group Settings' screen appears.

The screenshot shows a 'Group Settings' dialog box. At the top left, there is a 'System' label and a small icon of two people. The main title is 'Group Settings'. The dialog contains two input fields: 'Name:' with the text 'Group' and 'Description:'. Below these is a section titled 'Group Members' with two checkboxes: 'Administrator' and 'Remote Management'. At the bottom are 'OK' and 'Cancel' buttons.

Figure 8.10. Group Settings

Name Enter a name for the group of users.

Description You may also enter a short description for the group.

Group Members Select the users that will belong to this group. All users defined are presented in this section. A user can belong to more than one group.

8.4. Network Connections

OpenRG 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. When clicking the 'Network Connections' menu item under 'System', the following screen appears.

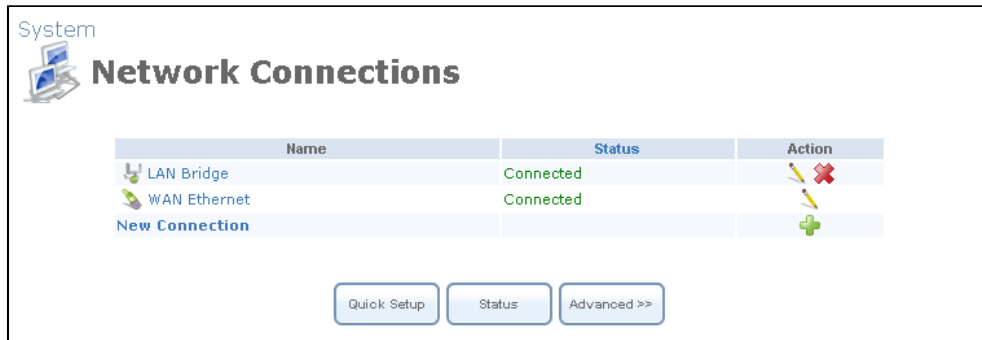


Figure 8.11. Network Connections – Basic

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

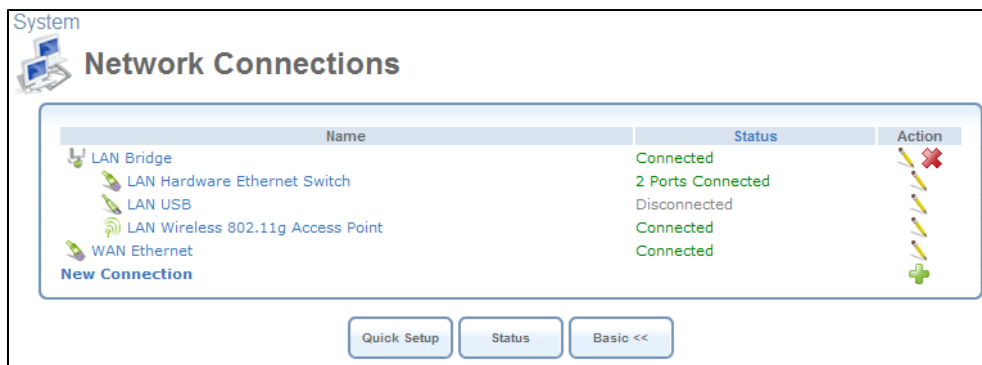



Figure 8.12. Network Connections – Advanced

This chapter describes the different network connections available with OpenRG in their order of appearance in the 'Network Connections' screen (see [Figure 8.12](#)), as well as the connection types that you can create using the Connection Wizard (for more information, refer to [Section 8.4.1](#)).

 Note: Some of the connections described herein may not be available with certain versions.

OpenRG's default network connections are:

- LAN – Creating a home/SOHO network
 - LAN Bridge (refer to [Section 8.4.3](#)).
 - LAN Ethernet (refer to [Section 8.4.4](#)).
 - LAN Hardware Ethernet Switch (refer to [Section 8.4.5](#)).
 - LAN USB (refer to [Section 8.4.6](#)).
 - LAN Wireless 802.11g Access Point (refer to [Section 8.4.7](#)).
- WAN – Internet Connection

- WAN Ethernet (refer to [Section 8.4.8](#)).

The logical network connections available with OpenRG are:

- WAN – Internet Connection
 - Point-to-Point Protocol over Ethernet (refer to [Section 8.4.9](#)).
 - Ethernet Connection (refer to [Section 8.4.10](#)).
 - Point-to-Point Tunneling Protocol (refer to [Section 8.4.13](#)).
 - Layer 2 Tunneling Protocol (refer to [Section 8.4.11](#)).
 - Dynamic Host Configuration Protocol (refer to [Section 8.4.17](#)).
 - Manual IP Address Configuration (refer to [Section 8.4.18](#)).
 - Determine Protocol Type Automatically (refer to [Section 8.4.19](#)).
 - Point-to-Point Protocol over ATM (refer to [Section 8.4.20](#)).
 - Ethernet over ATM (refer to [Section 8.4.21](#)).
 - Classical IP over ATM (refer to [Section 8.4.22](#)).
 - WAN-LAN Bridge (refer to [Section 8.4.23](#)).
- Virtual Private Network over the Internet
 - Layer 2 Tunneling Protocol over Internet Protocol Security (refer to [Section 8.4.11](#)).
 - Layer 2 Tunneling Protocol Server (refer to [Section 8.4.12](#)).
 - Point-to-Point Tunneling Protocol Virtual Private Network (refer to [Section 8.4.13](#)).
 - Point-to-Point Tunneling Protocol Server (refer to [Section 8.4.14](#)).
 - Internet Protocol Security (refer to [Section 8.4.15](#)).
 - Internet Protocol Security Server (refer to [Section 8.4.16](#)).
- Advanced Connections
 - Network Bridging (refer to [Section 8.4.3](#) and [Section 8.4.23](#)).
 - VLAN Interface (refer to [Section 8.4.24](#)).
 - Routed IP over ATM (refer to [Section 8.4.25](#)).

- Internet Protocol over Internet Protocol (refer to [Section 8.4.26](#)).
- General Routing Encapsulation (refer to [Section 8.4.27](#)).

8.4.1. The Connection Wizard

The logical network connections can be easily created using the Connection Wizard. This wizard is consisted of a series of Web-based management screens, intuitively structured to gather all the information needed to create a logical connection.

8.4.1.1. Ethernet Gateway

In order to create a connection on an Ethernet gateway using the wizard, click the 'New Connection' link in the Network Connections screen. The 'Connection Wizard' screen will appear (see [Figure 8.13](#)).

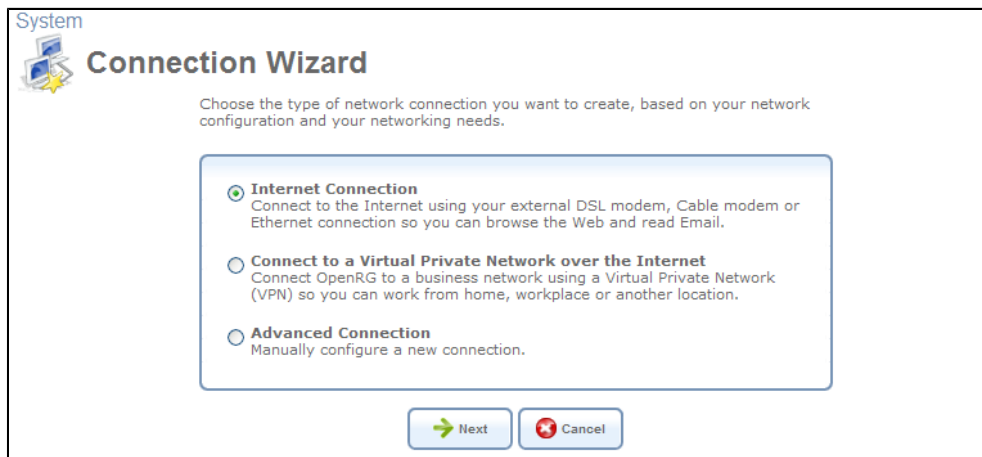


Figure 8.13. Connection Wizard

This screen presents you with the main connection types. Each option that you choose will lead you to further options in a tree-like formation, adding more information with each step and narrowing down the parameters towards the desired network connection.

- Internet Connection Selecting this option will take you to the 'Internet Connection' screen (see [Figure 8.14](#)). This section of the wizard will help you set up your Internet connection, in one of the various methods available.

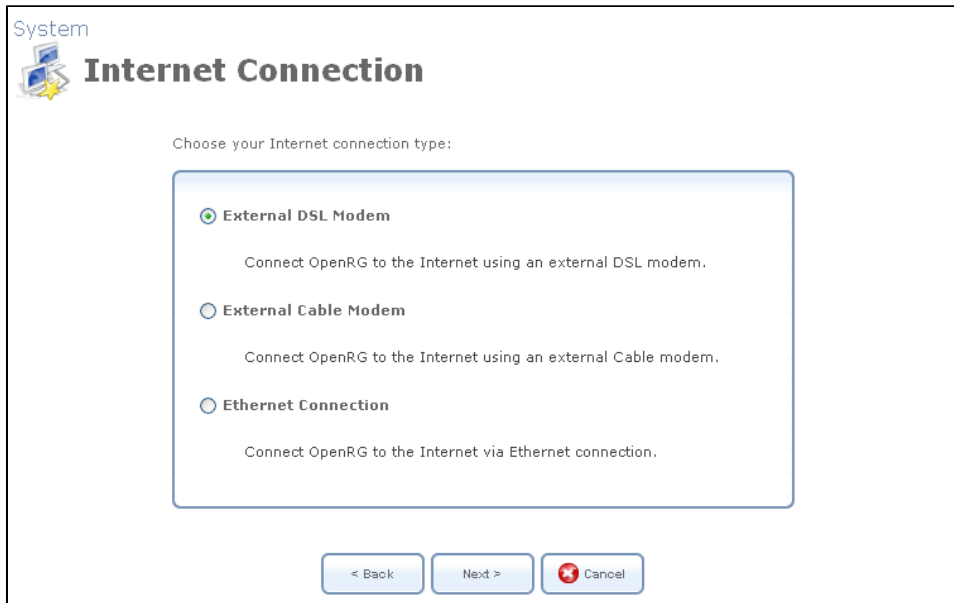


Figure 8.14. Internet Connection Wizard Screen

The tree formation of this section of the wizard is depicted in [Figure 8.15](#), where rectangles represent the steps/screens to be taken and ellipses represent the connections.

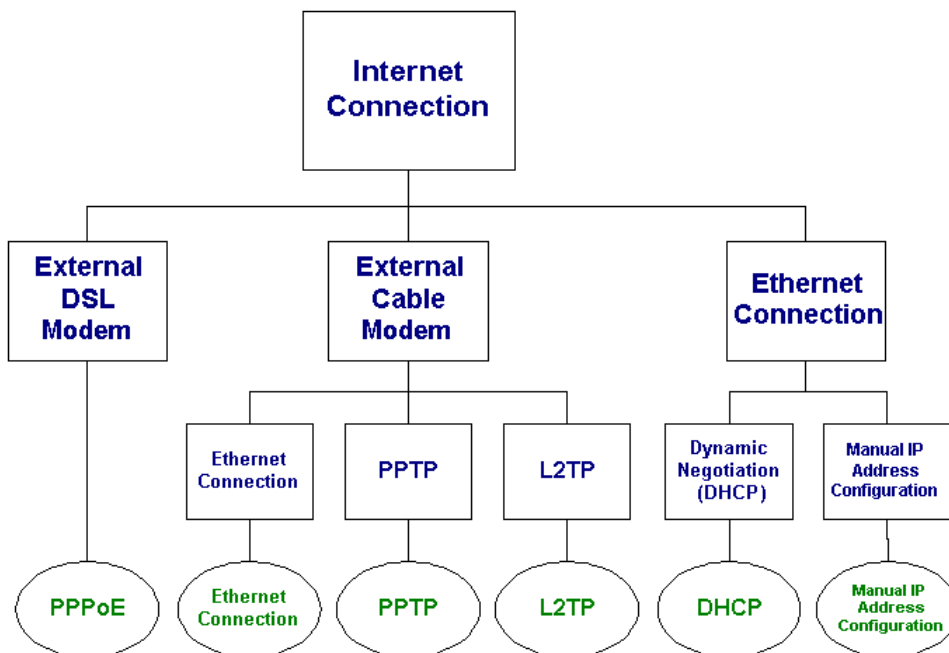


Figure 8.15. Internet Connection Wizard Tree

- Connect to a Virtual Private Network over the Internet Selecting this option will take you to the 'Connect to a Virtual Private Network over the Internet' screen (see [Figure 8.16](#)). This section will help you connect OpenRG to a business network using a Virtual Private Network (VPN) so you can work from home, your workplace or another location.

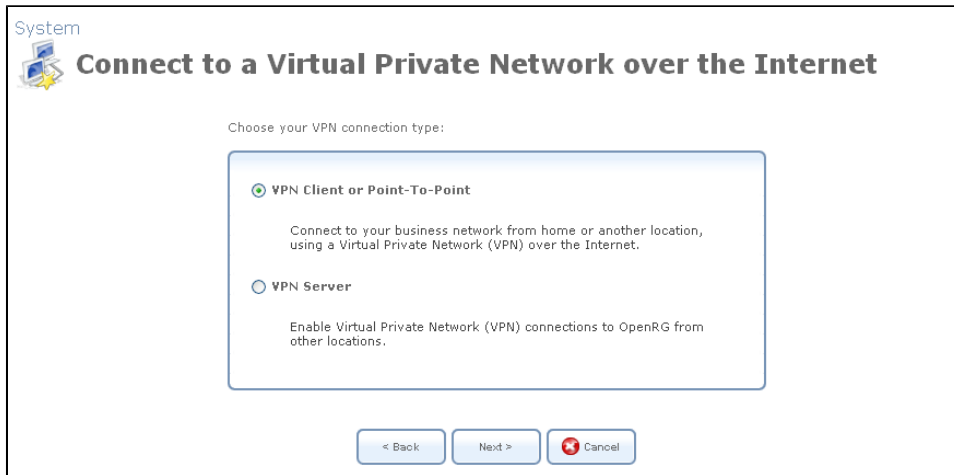


Figure 8.16. VPN Wizard Screen

The tree formation of this section is depicted in [Figure 8.17](#).

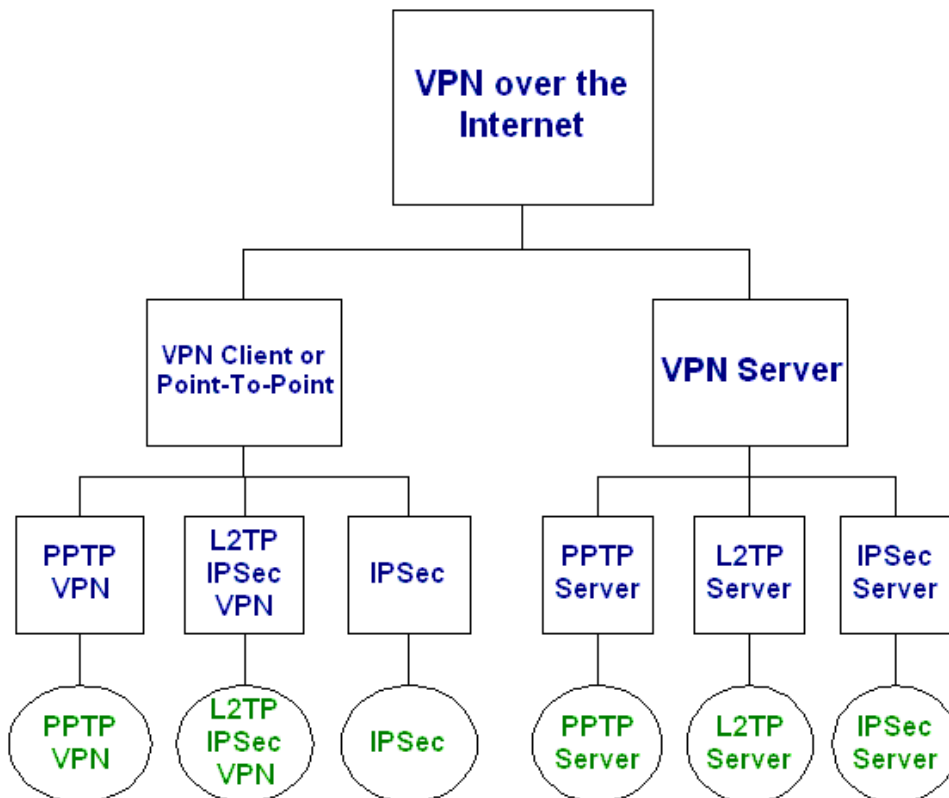


Figure 8.17. VPN Wizard Tree

- Advanced Connection Selecting this option will take you to the 'Advanced Connection' screen (see [Figure 8.18](#)). This section is a central starting point for all the aforementioned logical network connections. In addition, it provides the sequence for creating the Network Bridge and VLAN Interface connections.

System

Advanced Connection

Choose your connection type:

- Point-to-Point Protocol over Ethernet (PPPoE)**
Connect to the Internet using a PPP tunnel over the Ethernet protocol.
- Network Bridging**
Connect separate network interfaces to form one seamless LAN.
- VLAN Interface**
Connect to an external virtual network.
- Point-to-Point Tunneling Protocol (PPTP)**
Connect to the Internet using a PPTP connection.
- Point-to-Point Tunneling Protocol Virtual Private Network (PPTP VPN)**
Enable secure transfer of data to another location over the Internet, using user name/password authentication.
- Point-to-Point Tunneling Protocol Server (PPTP Server)**
Enable Virtual Private Network (VPN) connections to your home network from other locations.
- Layer 2 Tunneling Protocol (L2TP)**
Connect to the Internet using an L2TP connection.
- Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP IPsec VPN)**
Enable secure transfer of data to another location over the Internet, using private and public keys for encryption and digital certificates and user name/password for authentication.
- Layer 2 Tunneling Protocol Server (L2TP Server)**
Enable Virtual Private Network (VPN) connections to your home network from other locations.
- Internet Protocol Security (IPsec)**
Enable secure transfer of data to another location over the Internet, using private and public keys for encryption and digital certificates or shared secret for authentication.
- Internet Protocol Security Server (IPsec Server)**
Enable secure connections to OpenRG from other locations, using private and public keys for encryption and digital certificates or shared secret for authentication.
- Internet Protocol over Internet Protocol (IPIP)**
Enable transfer of data to another location over the Internet, using a non-encrypted virtual private network.
- General Routing Encapsulation (GRE)**
Enable transfer of data to another location over the Internet, using a non-encrypted virtual private network.

< Back Next > Cancel

Figure 8.18. Advanced Connection Wizard Screen

The tree formation of this section is depicted in [Figure 8.19](#).

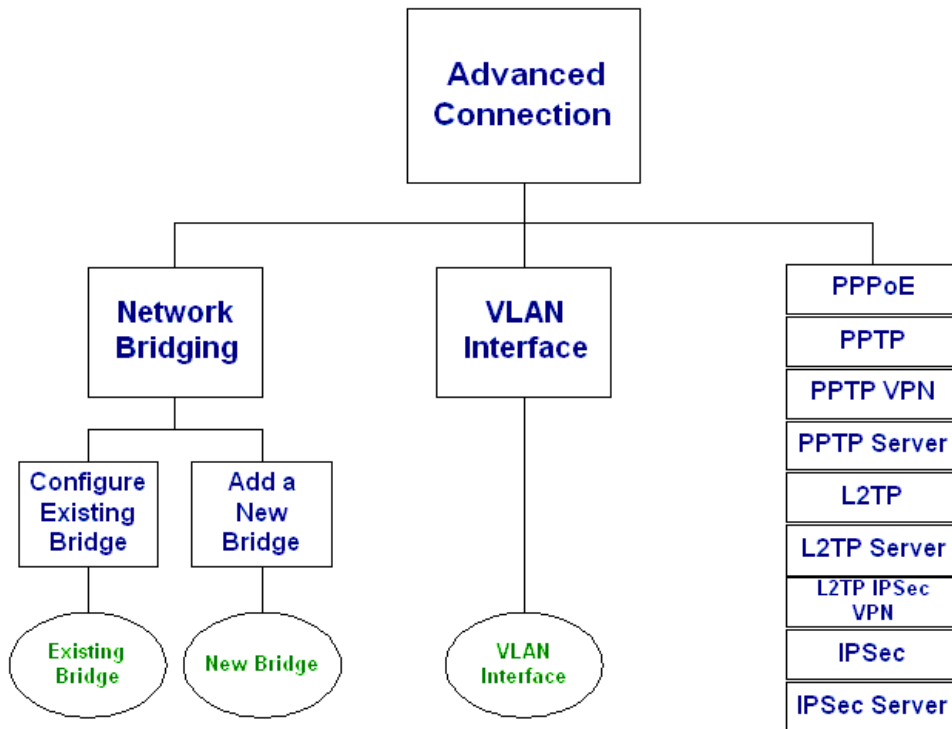


Figure 8.19. Advanced Connection Wizard Tree

Each logical connection described later in this chapter will include the "route" needed to be taken through the Connection Wizard in order for the connection to be created.

8.4.1.2. DSL Gateway

In case you are running a DSL gateway, the connection wizard will be slightly different. Click the 'New Connection' link in the Network Connections screen. The 'Connection Wizard' screen will appear (see [Figure 8.20](#)).

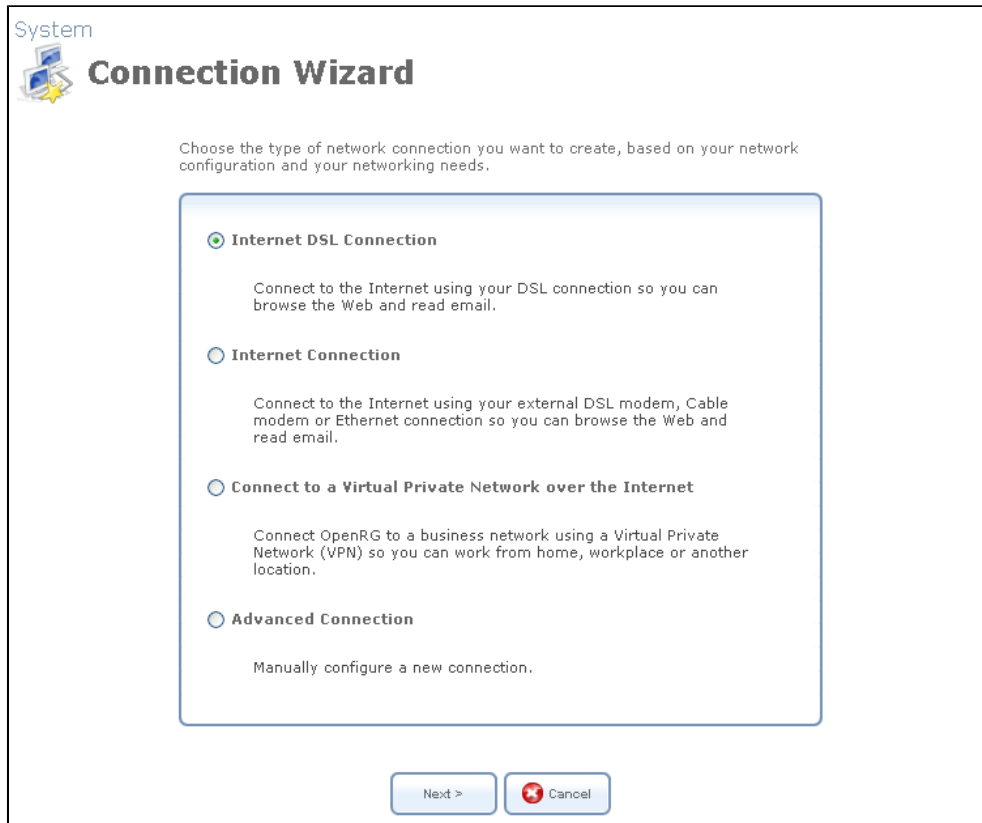


Figure 8.20. DSL Connection Wizard

- **Internet DSL Connection** Selecting this option will take you to the 'Internet DSL Connection' screen (see [Figure 8.21](#)). This section of the wizard will help you set up your DSL Internet connection, in one of the various methods available.

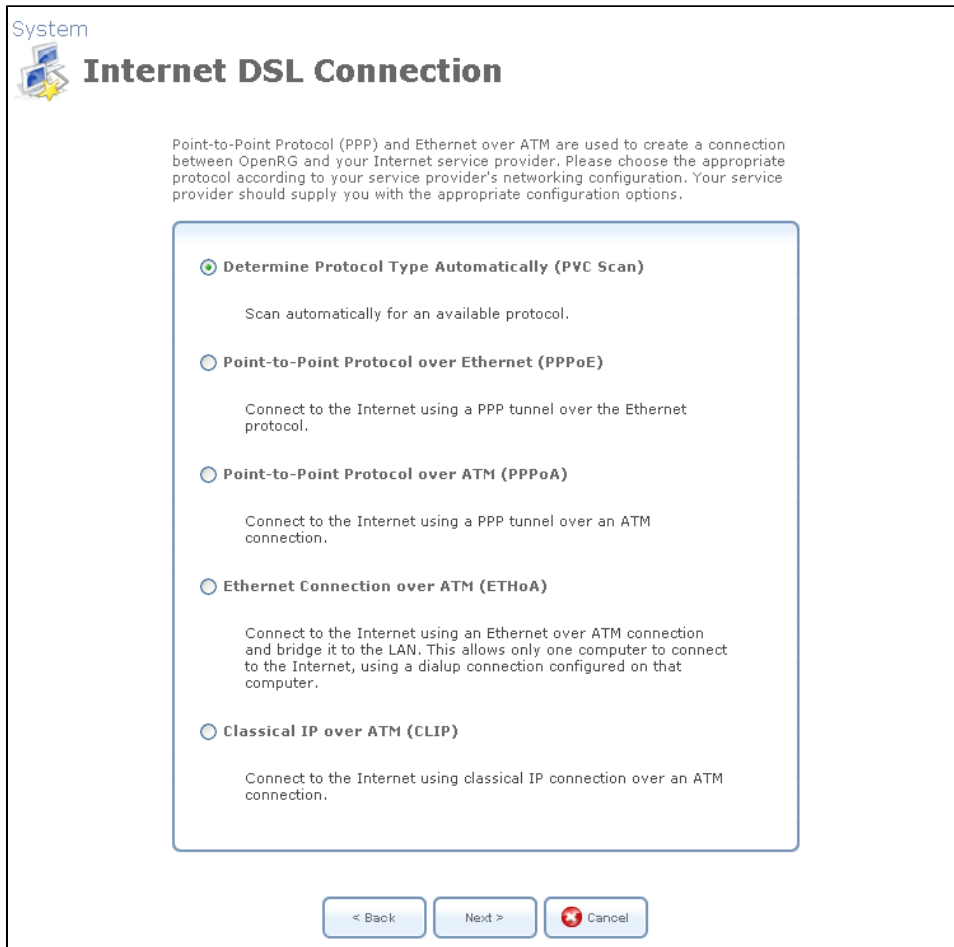


Figure 8.21. Internet DSL Connection Wizard Screen

The tree formation of this section of the wizard is depicted in [Figure 8.22](#), where rectangles represent the steps/screens to be taken and ellipses represent the connections.

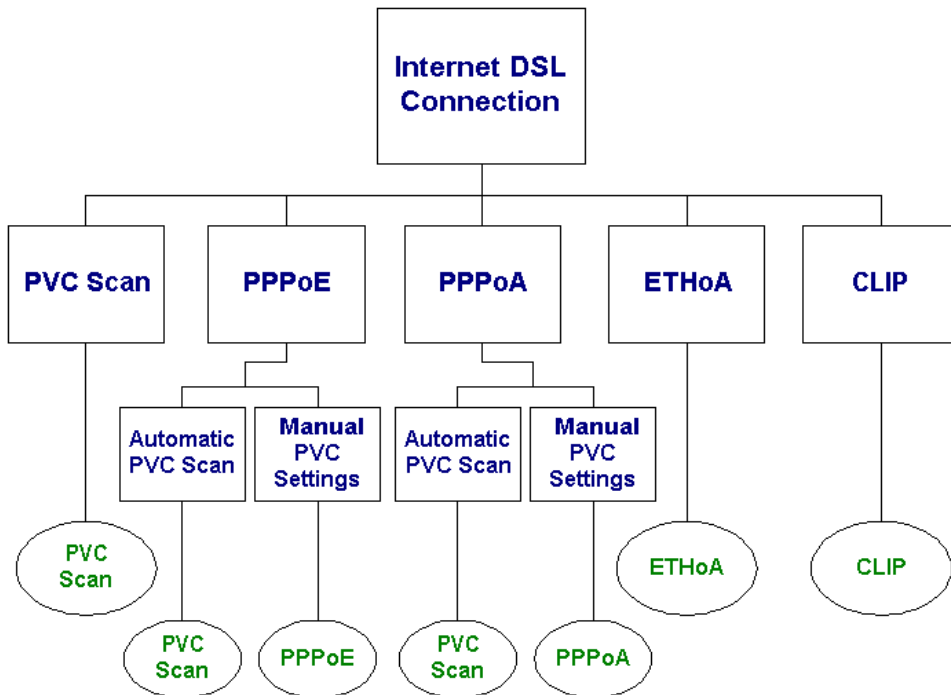


Figure 8.22. Internet DSL Connection Wizard Tree

- Internet Connection Selecting this option will take you to the 'Internet Connection' screen (see [Figure 8.14](#)). This section of the wizard is identical to the one of the Ethernet gateway, described in [Section 8.4.1.1](#).
- Connect to a Virtual Private Network over the Internet Selecting this option will take you to the 'Connect to a Virtual Private Network over the Internet' screen (see [Figure 8.23](#)). This section will help you connect OpenRG to a business network using a Virtual Private Network (VPN) so you can work from home, your workplace or another location.

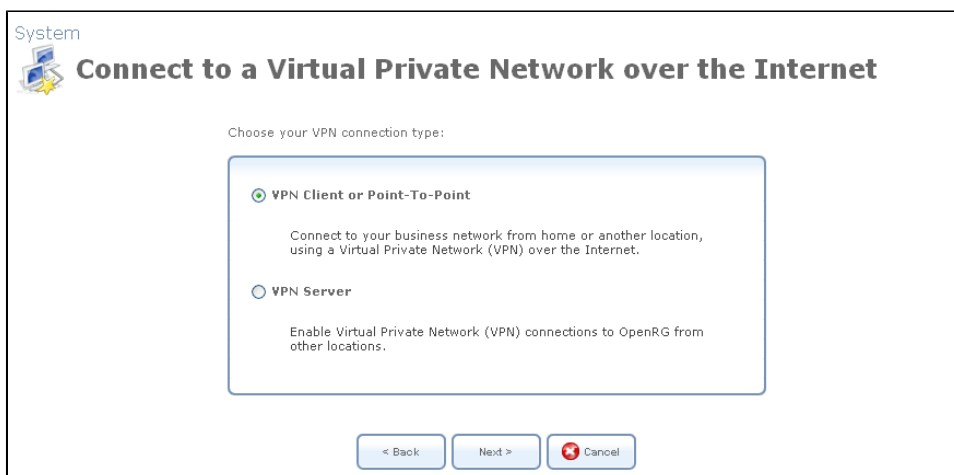


Figure 8.23. VPN Wizard Screen

The tree formation of this section is depicted in [Figure 8.24](#).

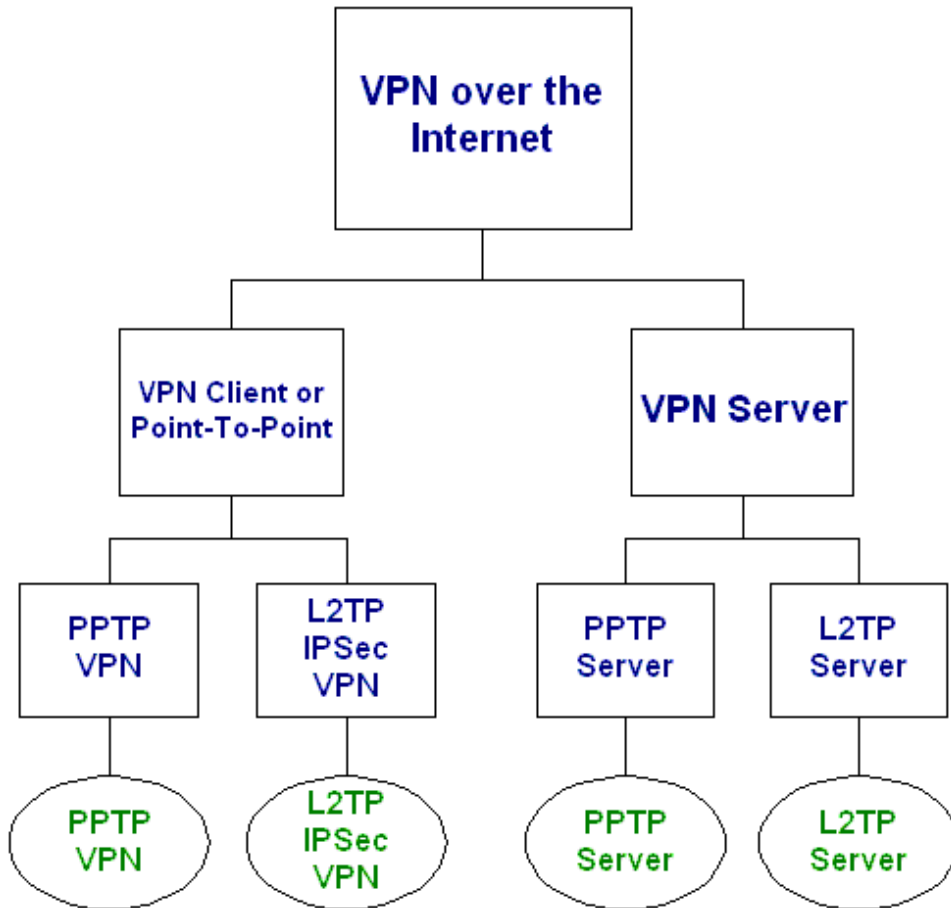


Figure 8.24. VPN Wizard Tree

- Advanced Connection Selecting this option will take you to the 'Advanced Connection' screen (see [Figure 8.25](#)). This section is a central starting point for all the DSL connections, and includes extra connections such as Routed IP over ATM (IPoA), Network Bridge and VLAN Interface.

System

Advanced Connection

Choose your connection type:

- Point-to-Point Protocol over Ethernet (PPPoE)**
Connect to the Internet using a PPP tunnel over the Ethernet protocol.
- Point-to-Point Protocol over ATM (PPPoA)**
Connect to the Internet using a PPP tunnel over an ATM connection.
- Routed IP over ATM (IPoA)**
Connect to the Internet using Routed IP protocol over an ATM connection.
- Ethernet Connection over ATM (ETHoA)**
Connect to the Internet using Ethernet protocol over an ATM connection.
- Classical IP over ATM (CLIP)**
Connect to the Internet using classical IP connection over an ATM connection.
- Network Bridging**
Connect separate network interfaces to form one seamless LAN.
- VLAN Interface**
Connect to an external virtual network.
- Point-to-Point Tunneling Protocol (PPTP)**
Connect to the Internet using a PPTP connection.
- Point-to-Point Tunneling Protocol Virtual Private Network (PPTP VPN)**
Enable secure transfer of data to another location over the Internet, using user name/password authentication.
- Point-to-Point Tunneling Protocol Server (PPTP Server)**
Enable Virtual Private Network (VPN) connections to your home network from other locations.
- Layer 2 Tunneling Protocol (L2TP)**
Connect to the Internet using an L2TP connection.
- Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP IPsec VPN)**
Enable secure transfer of data to another location over the Internet, using private and public keys for encryption and digital certificates and user name/password for authentication.
- Layer 2 Tunneling Protocol Server (L2TP Server)**
Enable Virtual Private Network (VPN) connections to your home network from other locations.
- Internet Protocol Security (IPsec)**
Enable secure transfer of data to another location over the Internet, using private and public keys for encryption and digital certificates or shared secret for authentication.
- Internet Protocol Security Server (IPsec Server)**
Enable secure connections to OpenRG from other locations, using private and public keys for encryption and digital certificates or shared secret for authentication.

< Back Next > Cancel

Figure 8.25. Advanced DSL Connection Wizard Screen

The tree formation of this section is depicted in [Figure 8.26](#).

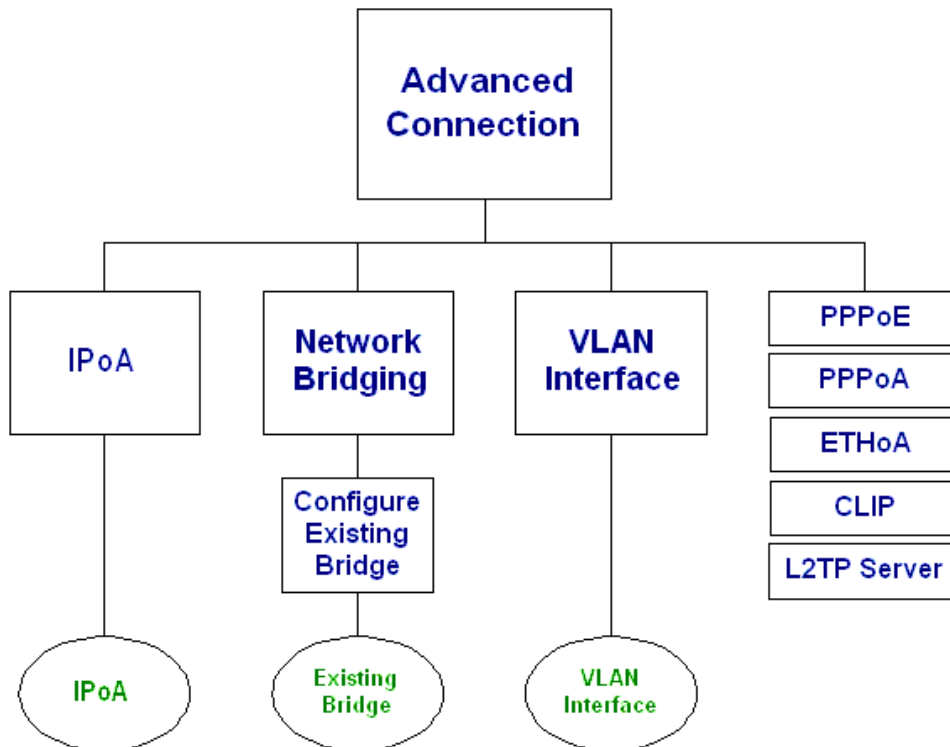


Figure 8.26. Advanced DSL Connection Wizard Tree

Each logical connection described later in this chapter will include the "route" needed to be taken through the Connection Wizard in order for the connection to be created.

8.4.2. Network Types

Every network connection in OpenRG can be configured as one of three types: WAN, LAN or DMZ. This provides high flexibility and increased functionality. For example, you may define that a LAN ethernet connection on OpenRG will operate as a WAN network. This means that all hosts in this LAN will be referred to as WAN computers, both by computers outside OpenRG and by OpenRG itself. WAN and firewall rules may be applied, such as on any other WAN network. Another example, is that a network connection can be defined as a DMZ (Demilitarized) network. Although the network is physically inside OpenRG, it will function as an unsecured, independent network, for which OpenRG merely acts as a router. One of these three network types is defined in each connection's configuration screen, in the 'Network' combo-box, as depicted in the following sections.

8.4.2.1. DMZ Network

When defining a network connection as a DMZ network, you must also:

- Remove the connection from under a bridge, if that is the case.

- Change the connection's routing mode to "Route", in the 'Routing' section of the configuration screen.
- Add a routing rule on your external gateway (which may be with your ISP) informing of the DMZ network behind OpenRG.

8.4.3. 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.

8.4.3.1. Creation with the Connection Wizard

To configure an existing bridge or create a new one, perform the following:

1. In the 'Network Connections' screen under 'System' (see [Figure 8.12](#)), click the 'New Connection' link. The 'Connection Wizard' screen appears (see [Figure 8.13](#)).
2. Select the 'Advanced Connection' radio button and click 'Next'. The 'Advanced Connection' screen appears (see [Figure 8.18](#)).
3. Select the 'Network Bridging' radio button and click 'Next'. The 'Bridge Options' screen appears.

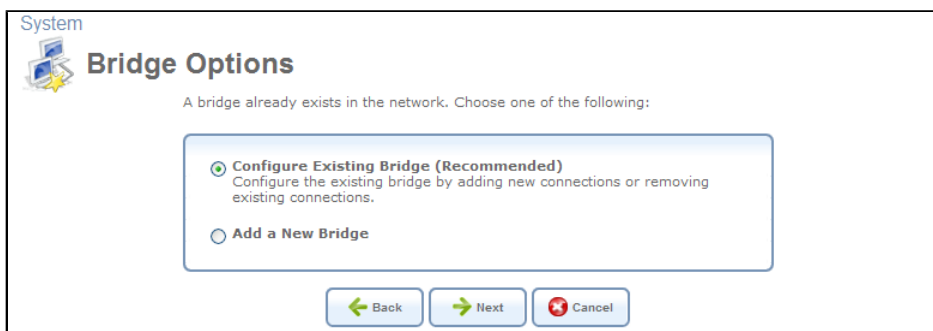


Figure 8.27. Bridge Options

4. Select whether to configure an existing bridge (this option will only appear if a bridge exists) or to add a new one:
 - a. **Configure Existing Bridge** Select this option and click 'Next'. The 'Network Bridging' screen appears allowing you to add new connections or remove existing ones, by selecting or deselecting their respective check boxes. For example, check the WAN check box to create a LAN-WAN bridge.

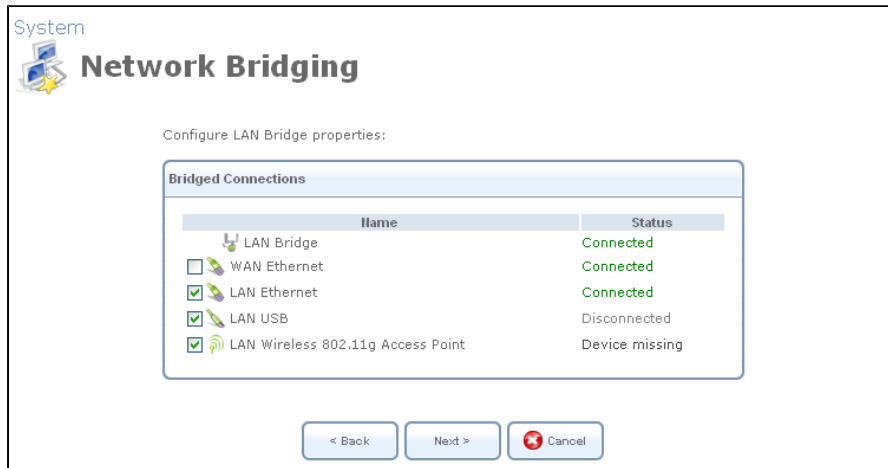


Figure 8.28. Network Bridging – Configure Existing Bridge

- b. **Add a New Bridge** Select this option and click 'Next'. A different 'Network Bridging' screen appears allowing you to add a bridge over the unbridged connections, by selecting their respective check boxes.

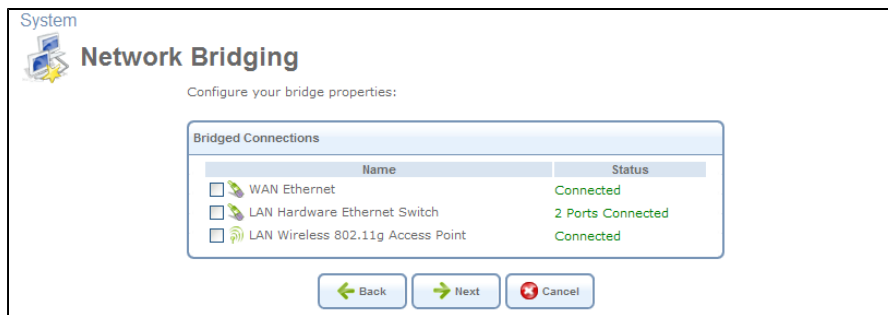


Figure 8.29. Network Bridging – Add a New Bridge

5. Click 'Next'. The 'Connection Summary' screen appears, corresponding to your changes.

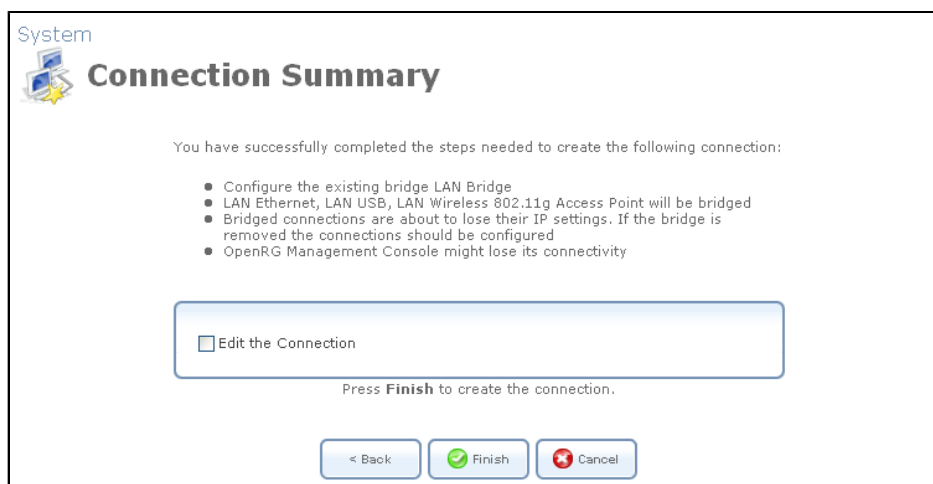


Figure 8.30. Connection Summary – Configure Existing Bridge

6. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.
7. Click 'Finish' to save the settings. The new bridge will be added to the network connections list, and it will be configurable like any other bridge.



Note: Creating a WAN-LAN bridge disables OpenRG's DHCP server. This means that LAN hosts may only receive an IP address from a DHCP server on the WAN. If you configure a host with a static IP address from an alias subnet of the bridge (192.168.1.X), you will be able to access OpenRG but not the WAN, as NAT is not performed in the WAN-LAN bridge mode.

8.4.3.2. General

To view and edit the LAN bridge connection settings, click the 'LAN Bridge' link in the 'Network Connections' screen (see [Figure 8.12](#)). The 'LAN Bridge Properties' screen appears (see [Figure 8.31](#)), 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.

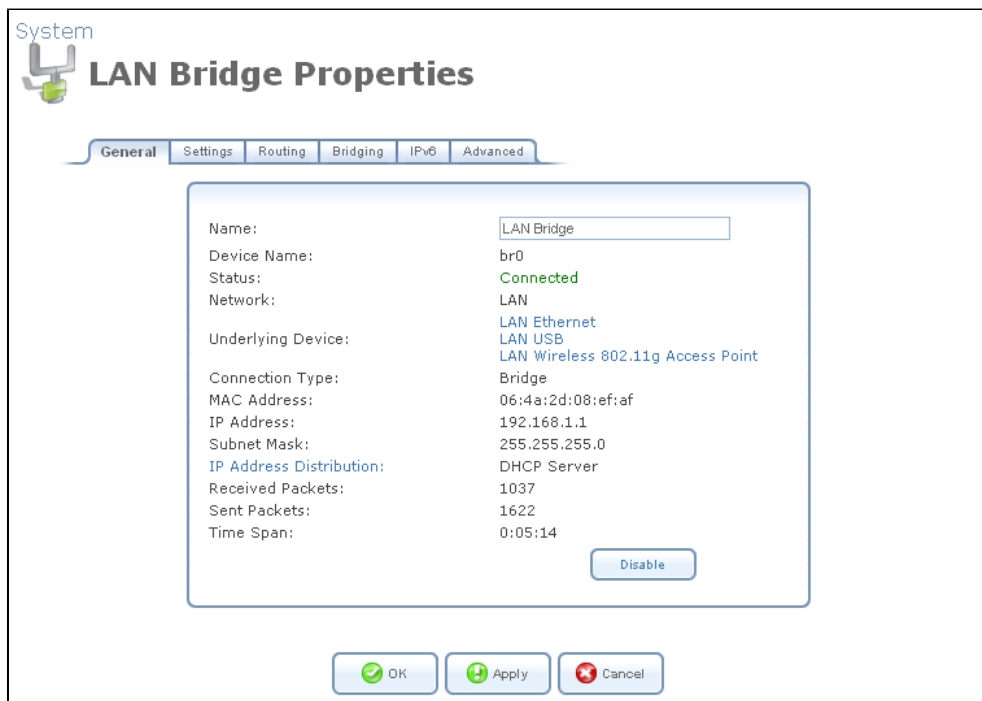


Figure 8.31. LAN Bridge Properties

8.4.3.3. 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.

Device Name:	ra0
Status:	Connected
Schedule:	Always
Network:	LAN
Connection Type:	Wireless 802.11g Access Point
Physical Address:	00:10:60:64:29:1e
MTU:	Automatic 1500

Figure 8.32. General

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, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to [Section 8.9.3](#).

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to [Section 8.4.2](#).

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' drop-down menu:

- No IP Address
- Obtain an IP Address Automatically
- Use the Following IP Address

Note that the screen will refresh to display relevant configuration settings according to your choice.

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.

Internet Protocol No IP Address ▼

Figure 8.33. Internet Protocol – No IP Address

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 click 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.

Internet Protocol Obtain an IP Address Automatically ▼

Override Subnet Mask: 0 . 0 . 0 . 0

Figure 8.34. Internet Protocol Settings – Automatic IP

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.

Internet Protocol Use the Following IP Address ▼

IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255 . 255 . 255 . 0

Figure 8.35. Internet Protocol – Static IP

DNS Server Domain Name System (DNS) 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. To configure the connection to automatically obtain a DNS server address, select 'Obtain DNS Server Address Automatically' from the 'DNS Server' drop down menu.

DNS Server Obtain DNS Server Address Automatically ▼

Figure 8.36. DNS Server – Automatic IP

To manually configure DNS server addresses, select 'Use the Following DNS Server Addresses' from the 'DNS Server' drop down menu (see figure 'DNS Server -- Static IP'). Specify up to two different DNS server address, one primary, another secondary.

DNS Server Use the Following DNS Server Addresses ▼

Primary DNS Server: 0 . 0 . 0 . 0

Secondary DNS Server: 0 . 0 . 0 . 0

Figure 8.37. DNS Server – Static IP

To learn more about this feature, refer to [Section 7.13.1](#).

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. For a comprehensive description of this feature, please refer to [Section 7.13.2](#) . Select one of the following options from the 'IP Address Distribution' combo-box:

- DHCP Server

1. **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 255.255.0.0.

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 local 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 a host name to it.

2. Click 'OK' to save the settings.

- **IP Address Distribution**

	DHCP Server ▼			
Start IP Address:	192	.168	.1	.1
End IP Address:	192	.168	.1	.234
Subnet Mask:	255	.255	.255	.0
Lease Time in Minutes:	60			
<input checked="" type="checkbox"/> Provide Host Name If Not Specified by Client				

Figure 8.38. IP Address Distribution -- DHCP Server

- **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 OpenRG's WAN to work in routing mode. For more information, refer to [Section 7.13.2.2](#) .

1. After selecting 'DHCP Relay' from the drop down menu, a 'New IP Address' link will appear:

IP Address Distribution

DHCP Relay

New IP Address

Figure 8.39. IP Address Distribution - DHCP Relay

Click the 'New IP Address' link. The 'DHCP Relay Server Address' screen will appear:

Figure 8.40. DHCP Relay Server Address

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.

IP Address Distribution

Disabled

Figure 8.41. IP Address Distribution - Disable DHCP

8.4.3.4. 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.

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.

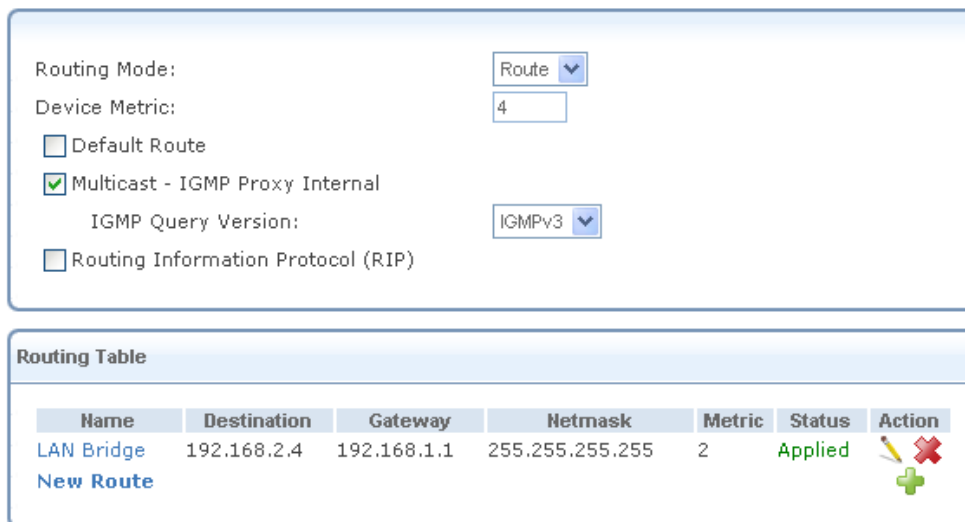
Routing Information Protocol (RIP) Select this check box to enable the Routing Information Protocol (RIP). RIP determines a route based on the smallest hop count between source and destination. When RIP is enabled, select the following:

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

Multicast – IGMP Proxy Internal / Default OpenRG serves as an IGMP proxy, issuing IGMP host messages on behalf of its LAN hosts. This check box is enabled on LAN connections by default, meaning that if a LAN multicast server is available, other LAN hosts asking to join multicast groups (by sending IGMP requests) will be able to join its multicast group. However, this check box is disabled on the WAN connection by default, meaning that LAN hosts will not be able to join multicast groups of WAN multicast servers. When creating a WAN-LAN bridge, this check box must also be deselected.

IGMP Query Version OpenRG supports all three versions of IGMP. Select the version you would like to use. Note that this drop-down menu appears for LAN connections only.

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.



Routing Mode:

Device Metric:

Default Route

Multicast - IGMP Proxy Internal

IGMP Query Version:

Routing Information Protocol (RIP)


Name	Destination	Gateway	Netmask	Metric	Status	Action
LAN Bridge	192.168.2.4	192.168.1.1	255.255.255.255	2	Applied	

[New Route](#)

Figure 8.42. Advanced Routing Properties

To learn more about this feature, refer to [Section 8.6.1](#).

8.4.3.5. Bridging

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



Note: If you would like to logically partition your Ethernet-based network, you can set up a VLAN bridge as described in [Section 8.4.24.7](#).

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.

Name	VLANs	Status	STP	Action
LAN Bridge	Disabled	Connected		
<input checked="" type="checkbox"/> WAN Ethernet	Disabled	Connected	<input type="checkbox"/>	
<input checked="" type="checkbox"/> LAN Ethernet	Disabled	Connected	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> LAN Wireless 802.11g Access Point	Disabled	Device Missing	<input checked="" type="checkbox"/>	

Source MAC Filter	Destination Bridge	Action
New Entry		

Bridge Hardware Acceleration	<input type="checkbox"/> Enabled
------------------------------	----------------------------------

Figure 8.43. LAN Bridge Settings

Bridge Filter This section is used for creating a traffic filtering rule on the bridge, in order to enable direct packet flow between the WAN and the LAN. Such an example is when setting up a hybrid bridging mode (refer to [Section 8.4.23.2](#)).

Bridge Hardware Acceleration Select this check box to utilize the **Fastpath** algorithm for enhancing packet flow through the bridge. Note that this feature must be supported and enabled on the bridge's underlying devices in order to work properly.

8.4.3.6. IPv6

Click on the 'New Unicast Address' link to add an IPv6 unicast address. To learn more about configuring IPv6 settings, refer to [Section 8.6.2](#).




IPv6		
Link Local Address:	fe80::44a:2dff:fe08:efaf / 10	
6to4 Address:	2002:a47:519d:1:44a:2dff:fe08:efaf / 64	
Unicast Addresses		
Address	Use MAC Address for Interface ID	Action
fec0::44a:2dff:fe08:efaf / 64	Yes	 
New Unicast Address		

Figure 8.44. IPv6 Settings

8.4.3.7. 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. To learn more about your gateway's security features, refer to [Section 7.3](#).

Internet Connection Firewall	<input type="checkbox"/> Enabled
------------------------------	----------------------------------

Figure 8.45. Internet Connection Firewall

- **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 and the http://openrg.home.

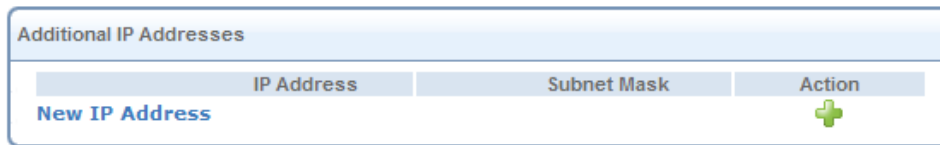


Figure 8.46. Additional IP Addresses

8.4.4. LAN Ethernet

A LAN Ethernet connection connects computers to OpenRG using Ethernet cables, either directly or via network hubs and switches.

8.4.4.1. General

To view and edit the LAN Ethernet connection settings, click the 'LAN Ethernet' link in the 'Network Connections' screen (see [Figure 8.12](#)). The 'LAN Ethernet Properties' screen will appear (see [Figure 8.47](#)), 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.

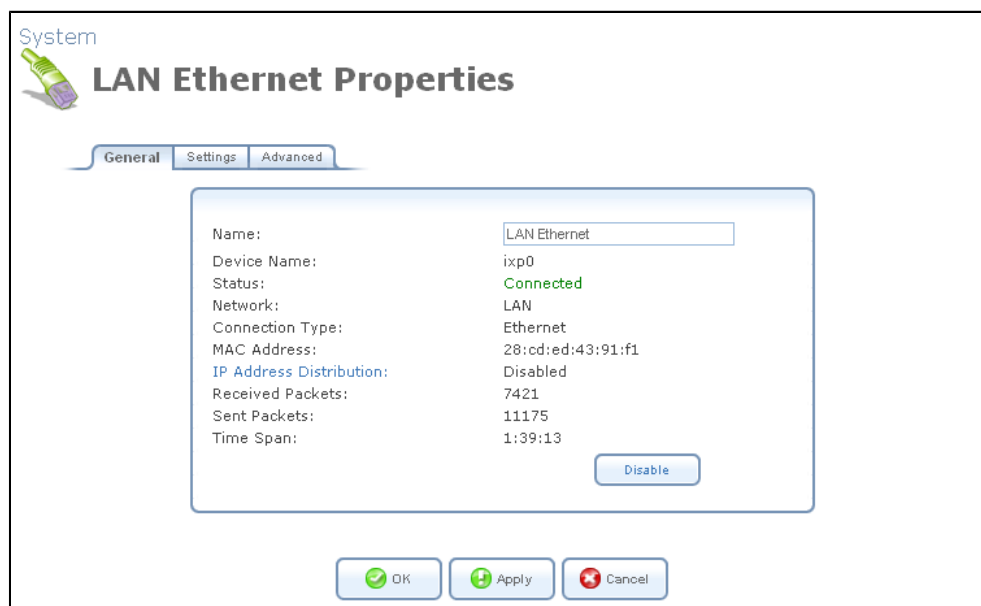


Figure 8.47. LAN Ethernet Properties

8.4.4.2. 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 8.48. General

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, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to [Section 8.9.3](#).

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to [Section 8.4.2](#).

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.

8.4.4.3. 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. To learn more about your gateway's security features, refer to [Section 7.3](#).

Figure 8.49. Internet Connection Firewall

Internet Connection Fastpath Select this check box to utilize the *Fastpath* algorithm for enhancing packet flow, resulting in faster communication between the LAN and the WAN. By default, this feature is enabled.

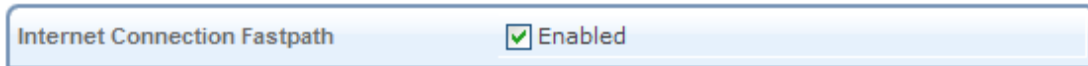


Figure 8.50. Internet Connection Fastpath

- **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 and the `http://openrg.home`.

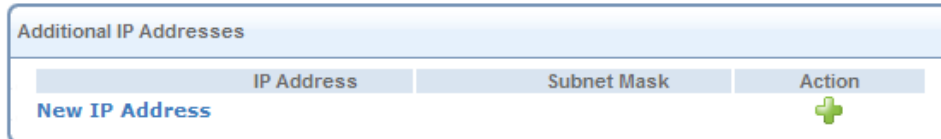


Figure 8.51. Additional IP Addresses

8.4.5. LAN Hardware Ethernet Switch

The LAN Hardware Ethernet Switch interface represents all of OpenRG's ports.

8.4.5.1. General

To view and edit the LAN Hardware Ethernet Switch connection settings, click the 'LAN Hardware Ethernet Switch' link in the 'Network Connections' screen (see [Figure 8.12](#)). The 'LAN Hardware Ethernet Switch Properties' screen appears (see [Figure 8.52](#)), 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.

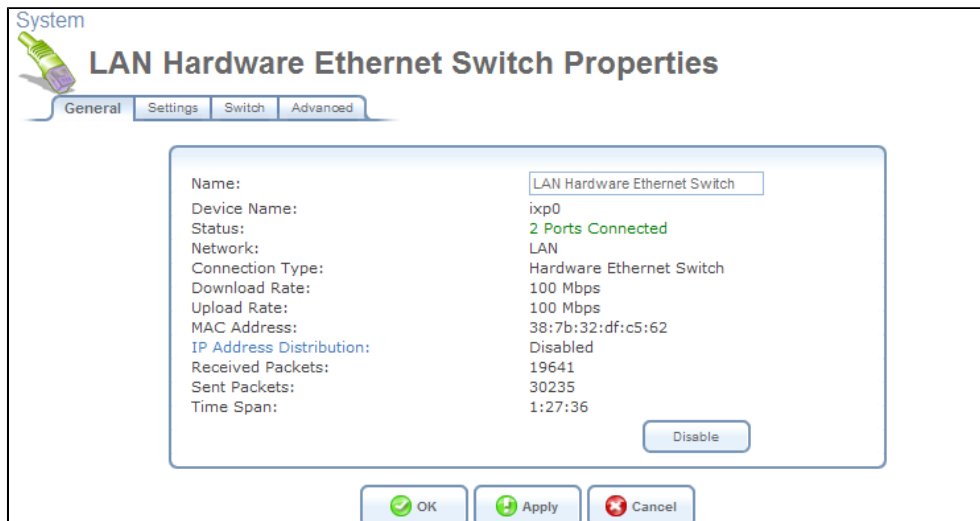


Figure 8.52. LAN Hardware Ethernet Switch Properties

8.4.5.2. Settings

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.

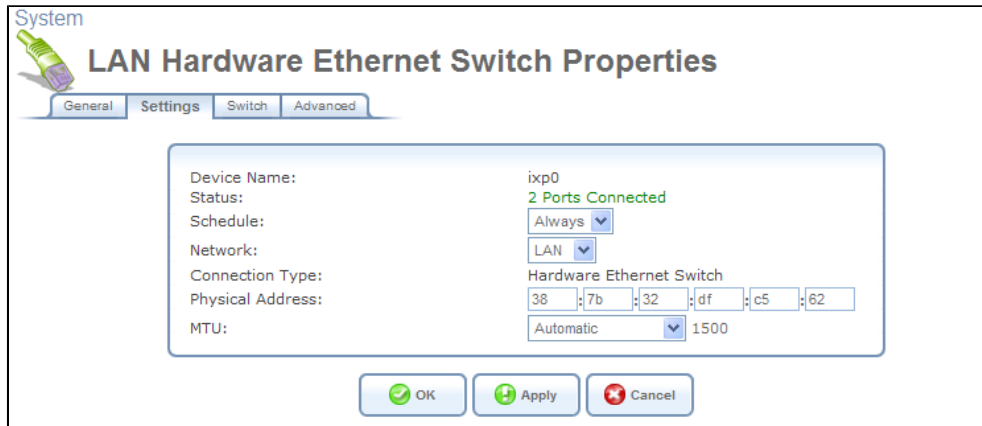


Figure 8.53. Settings

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, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to [Section 8.9.3](#).

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to [Section 8.4.2](#).

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.

8.4.5.3. Switch

This section displays the hardware switch ports properties. The switch ports are physical sockets on the board, to which different cables connect. The table in this screen is consisted of a list of all available ports, their status, and the VLANs of which they are members. Untagged packets (packets with no VLAN tag) that arrive in a port, will be tagged with the VLAN number that appears under the Port VLAN Identifier (PVID) column.

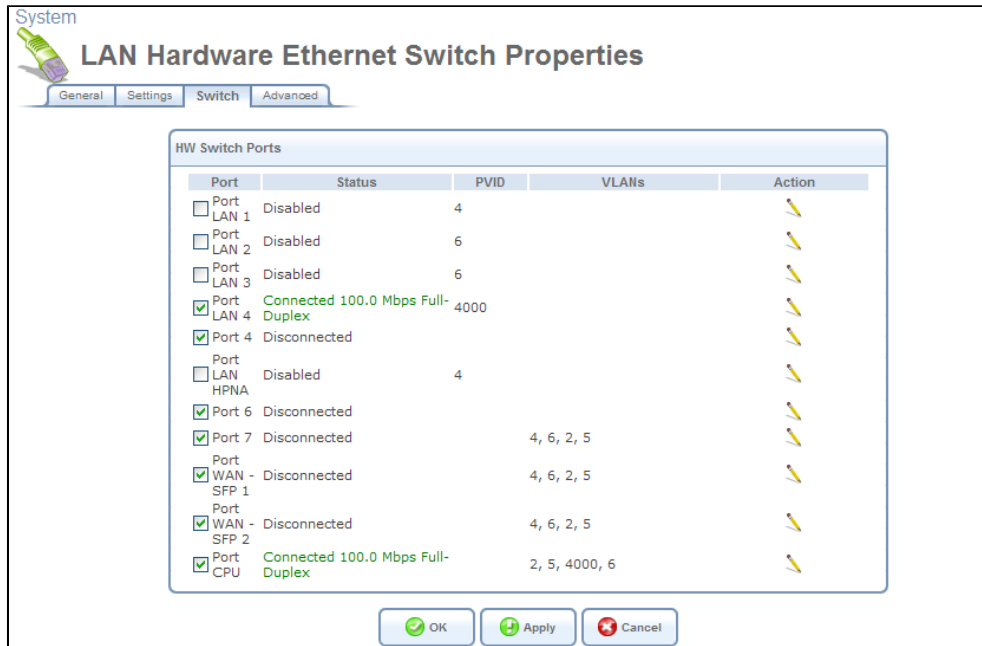


Figure 8.54. Switch

You can edit the configuration of each port. For example, click a connected port's action icon. The 'Port LAN Settings' screen appears.

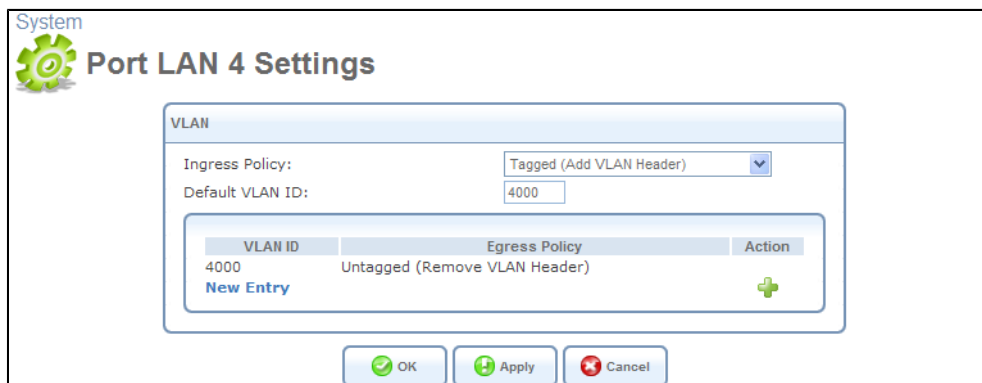


Figure 8.55. Port LAN Settings

Ingress Policy Select whether or not to tag incoming packets with the port's VLAN header. When the 'Tagged (Add VLAN Header)' option is selected, additional fields appear.

Default VLAN ID The port's VLAN identifier. You may add additional identifiers to the VLAN by clicking 'New Entry'.

8.4.5.4. 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. To learn more about your gateway's security features, refer to [Section 7.3](#).

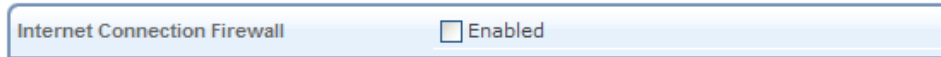


Figure 8.56. Internet Connection Firewall

Internet Connection Fastpath Select this check box to utilize the *Fastpath* algorithm for enhancing packet flow, resulting in faster communication between the LAN and the WAN. By default, this feature is enabled.

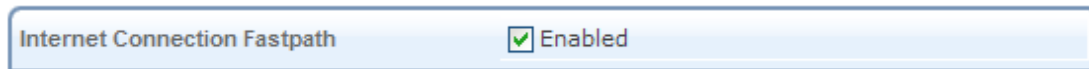


Figure 8.57. Internet Connection Fastpath

- **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 and the <http://openrg.home>.

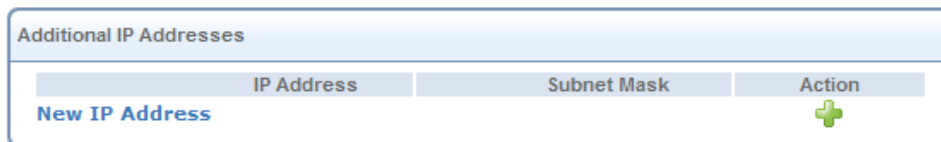


Figure 8.58. Additional IP Addresses

8.4.6. LAN USB

The LAN USB connection allows you to connect a Windows PC to OpenRG using a USB cable. Connect your gateway's USB slave port to a master port on the PC.

8.4.6.1. General

To view and edit the LAN USB connection settings, click the 'LAN USB' link in the 'Network Connections' screen (see [Figure 8.12](#)). The 'LAN USB Properties' screen will appear (see [Figure 8.59](#)), 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 8.59. LAN USB Properties

8.4.6.2. 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.

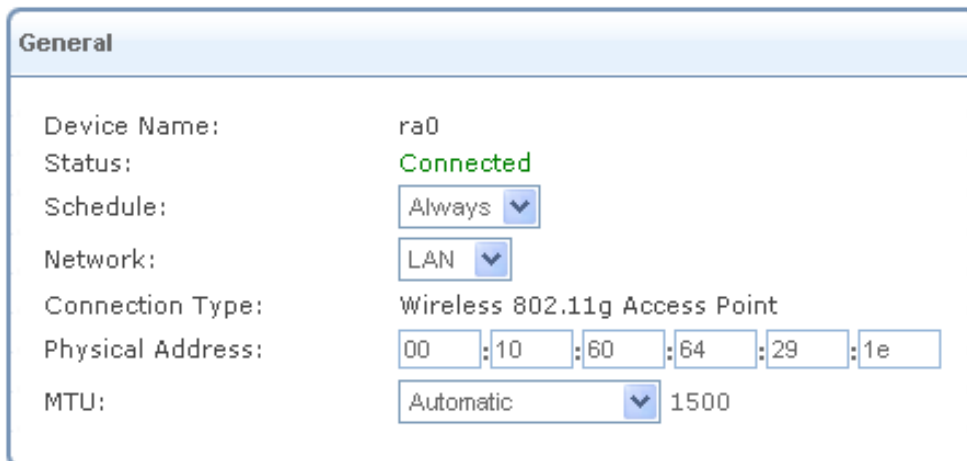


Figure 8.60. General

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, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to [Section 8.9.3](#).

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to [Section 8.4.2](#).

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.

8.4.6.3. 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. To learn more about your gateway's security features, refer to [Section 7.3](#).

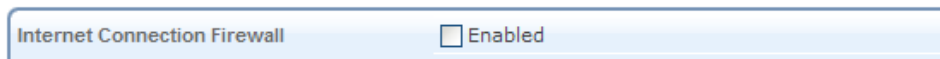


Figure 8.61. Internet Connection Firewall

- **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 and the http://openrg.home.

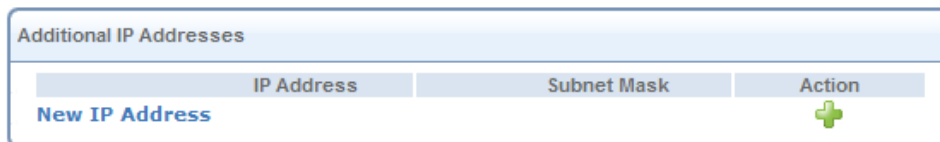


Figure 8.62. Additional IP Addresses

8.4.7. LAN Wireless

OpenRG for wireless gateways provides broadband customer premise equipment (CPE) manufacturers with a complete software solution for developing feature-rich CPE with wireless connectivity over the 802.11 **a**, **b**, **d** and **g** standards. The solution is vertically integrated and includes an operating system, communication protocols, routing, advanced wireless and broadband networking security, remote management and home networking applications.

OpenRG 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 OpenRG Firewall and VPN applications. In addition, OpenRG's built-in authentication server enables home/SOHO users to define authorized wireless users without the need for an external RADIUS server.

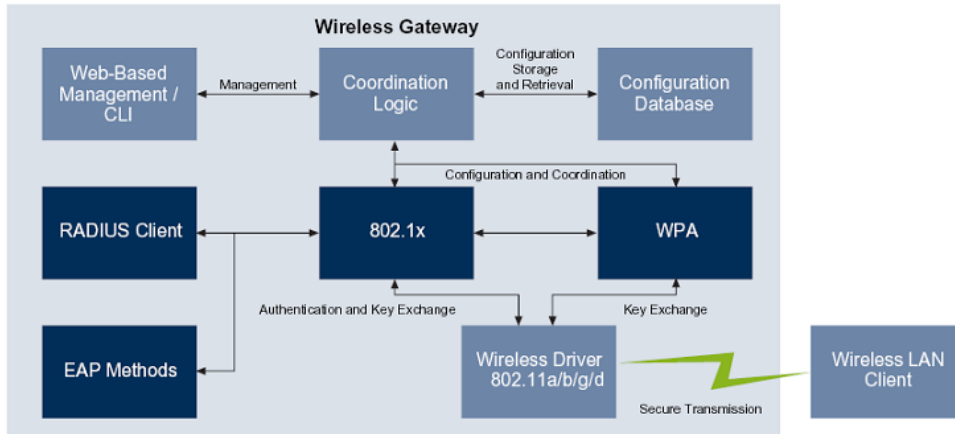


Figure 8.63. OpenRG for Wireless Gateways Authentication and Encryption Components

This section begins with basic instructions to quickly and easily configure your network, and continues with advanced settings options.

8.4.7.1. Supported Wireless Extension Cards

OpenRG currently supports the following wireless extension cards:

- Airgo AGN-100
- Ralink RT-2560
- Ralink RT-2561
- Ralink RT-2661
- Ralink RT-2860 (supported on Ikanos and Infineon platforms only)

OpenRG installed on the Freescale MPC8349ITX platform supports the following Atheros wireless cards:

- Atheros AR2413
- Atheros AR2417
- Atheros AR5413

In addition, OpenRG supports Broadcom's built-in wireless chipset on the following platforms:

- Broadcom BCM96358
- ASUS 6020VI

Note that not all of the wireless features depicted in this section may be available with your version. OpenRG incorporates a wireless card auto-detection mechanism. When booting,

OpenRG checks whether a wireless extension card is available. If so, it verifies the make and model of the card and only loads its supported wireless features. OpenRG will display a "Wireless" section in the 'Quick Setup' management screen. If your gateway includes a supported wireless module, yet you do not see this section, you will need to load a firmware version with wireless support in order to perform this evaluation.

8.4.7.2. Enabling Your Wireless Network

Although basic wireless configuration is performed by the installation wizard (refer to [Section 2.3.2](#)), this section will familiarize you with OpenRG's wireless configuration. Note that in order to connect a wireless PC to the gateway, you must also configure the PC as described in [Section 2.2](#).



Note: Connect the defined wireless card to your development board before booting. Booting without the wireless card may cause the image to halt.

1. Click the 'LAN Wireless 802.11g Access Point' link in the 'Network Connections' screen (see [Figure 8.12](#)). The 'LAN Wireless 802.11g Access Point Properties' screen appears.



Figure 8.64. LAN Wireless 802.11g Access Point Properties – Disabled

2. Press the 'Enable' button to activate the wireless connection (this button is displayed only if a wireless card is available on the gateway). The screen will refresh, and the connection status will change to "Connected".
3. Click the 'Wireless' sub-tab.
4. In the 'SSID' field, you may change the broadcasted name of your wireless network from the default "openrg" to a more unique name.

Wireless Network (SSID):

SSID Broadcast

802.11 Mode:

Channel: (FCC)

Channel Width Mode:

Network Authentication:

MAC Filtering Mode:

Figure 8.65. Wireless Access Point

5. Click 'OK' to save the settings.

A comprehensive description of all of the wireless connection settings in the screen above is described later in this chapter.

You can now use OpenRG's wireless network from the configured PC. Currently only HTTP authentication protects the wireless network from unauthorized users. Consider securing the wireless network using other methods as described in [Section 8.4.7.5](#).

8.4.7.3. Passing Web Authentication

Once OpenRG is running, prior to wireless authentication and encryption, the Web authentication feature protects your wireless network from unauthorized wireless clients. When wireless clients attempt to connect to OpenRG's WAN, they are prompted to enter a user name and password (see [Figure 8.66](#)). Note that all other attempts to use the wireless network prior to the authentication will fail (Telnet, FTP, ping).

Login

Attention

- Your attempt to browse to <http://www.cnn.com> failed because Web authentication is needed.

Language:

User Name:

Password:

[Forgot your password?](#)

Figure 8.66. Web Authentication

Enter your user name and password and click 'OK'. Once authentication has been performed, you may proceed to use OpenRG's wireless network from the configured PC.

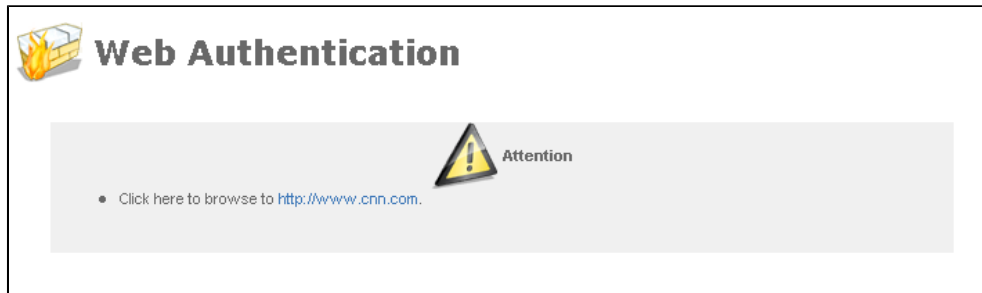
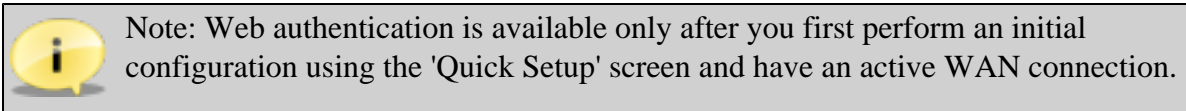


Figure 8.67. Web Authentication – Enabled Browsing



8.4.7.4. Retrieving a Forgotten Password

When attempting to connect to the Internet via OpenRG's wireless access point, you are prompted to enter a username and password. In case you have forgotten your password, click the 'Forgot Your Password?' link that appears in the 'Web Authentication' screen (see [Figure 8.66](#)). The 'Forgotten Password for Wireless Network' screen appears, providing numerous possible courses of action aimed at helping you login.

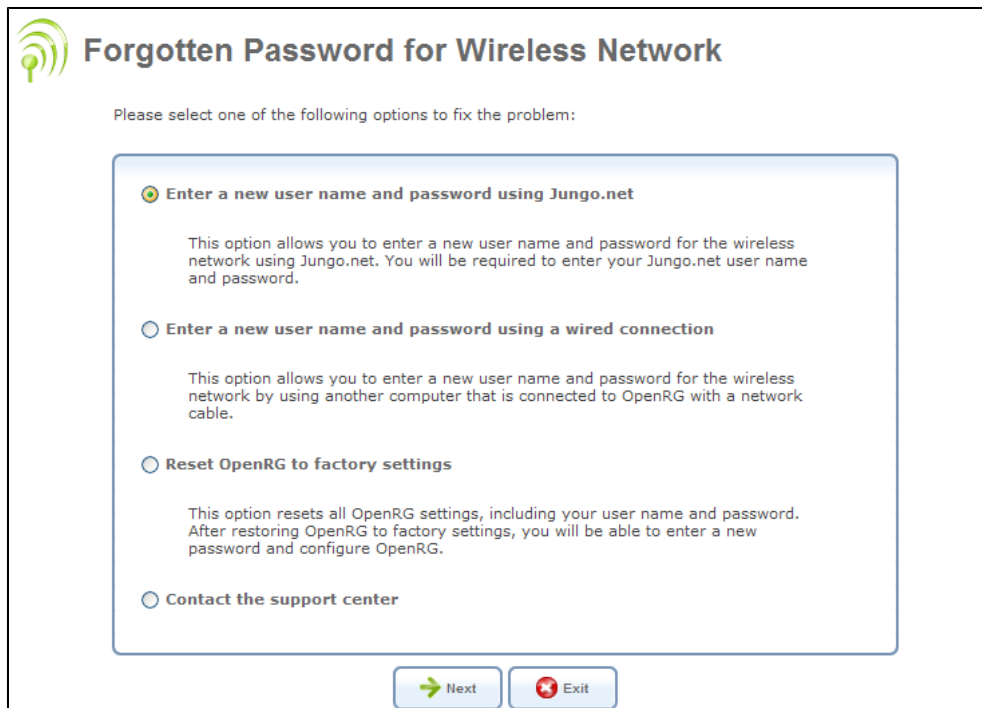


Figure 8.68. Forgotten Password for Wireless Network

- **Enter a new user name and password using Jungo.net** This option appears only when OpenRG is connected to Jungo.net. It enables you to enter a new user name and password for the wireless network using Jungo.net.

1. To use this option, select its radio button and click 'Next'. The Jungo.net login screen appears.

The screenshot shows the Jungo.net login page. On the left, under the heading "What is Jungo.net?", there are several service tiles: Personal Domain Name (Dynamic DNS), Web Server, E-Mail Filtering, Anti-Virus, NationZone, Remote File Access/Sharing, Web Content Filtering, Video Surveillance, Anti-Virus NAC, and IP-PBX. Each tile includes a brief description and a "Learn More..." link. On the right, there is a login form with fields for "User Name:" and "Password:", a "Forgot your password?" link, a checkbox for "Remember me on this computer", and an "OK" button. Below the form, there is a "Not a Jungo.net user?" link and a "Sign Up" button.

Figure 8.69. Jungo.net Login

2. Enter OpenRG's Jungo.net user name and password, and click 'OK'. The 'Wireless LAN User' screen appears.

The screenshot shows the Jungo.net account creation page. The top left has the "JUNGO" logo and a language dropdown set to "EN English". The top right says "JUNGO.net" and "Welcome jsmith | Support | Account | Logout". Below the logo is a navigation menu with "Home", "Personal Domain Name", "Remote File Access", "Web Server", "Web Content Filtering", "E-Mail Filtering", and "NationZone". The main content area is titled "Account" and "Wireless LAN User". It includes links for "Overview", "Settings", and "Transactions". A message states: "You can now create a new user, with which you can login to OpenRG's wireless network, instead of the forgotten one." Below this is a form with fields for "User Name:" (containing "wireless_johns"), "Password:" (masked with "*****"), and "Retype Password:" (masked with "*****"). There are "Go" and "Cancel" buttons at the bottom of the form.

Figure 8.70. Wireless LAN User

3. Create a new wireless client by entering a user name and password, and click 'Go'. The screen refreshes as the user is created, until the 'New User Created' screen appears.

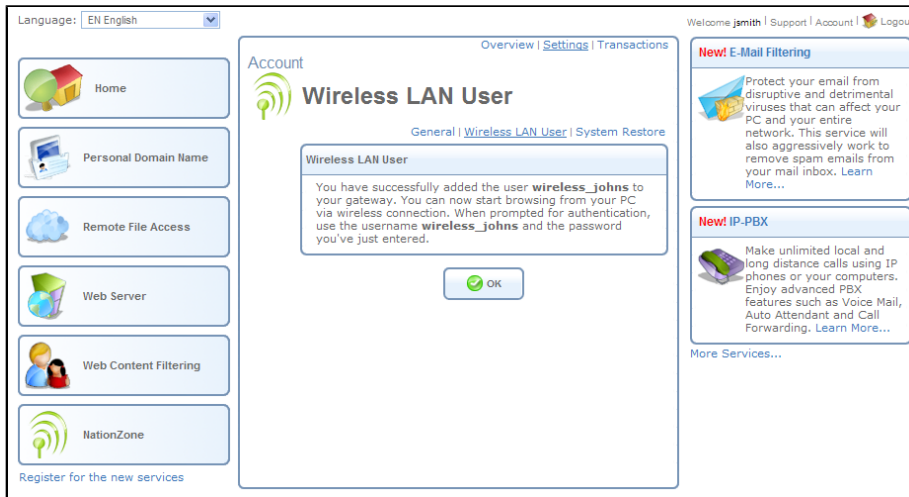


Figure 8.71. New User Created

4. Click 'Finish'. OpenRG's login screen appears. You can now login with the new wireless client details.

- **Enter a new user name and password using a wired connection** This option allows you to enter a new user name and password for the wireless network by using another computer that is physically connected to OpenRG. To use this option, select its radio button and click 'Next'. The next screen contains a detailed description of the steps you must follow in order to create a new user name and password for the wireless network.



Figure 8.72. Enter a New User Name and Password Using a Wired Connection

- **Reset OpenRG to factory settings** This option resets OpenRG's settings, including your user name and password. To use this option, select its radio button and click 'Next'. The next screen contains a detailed description of the steps you must follow in order to reset OpenRG to its factory settings.

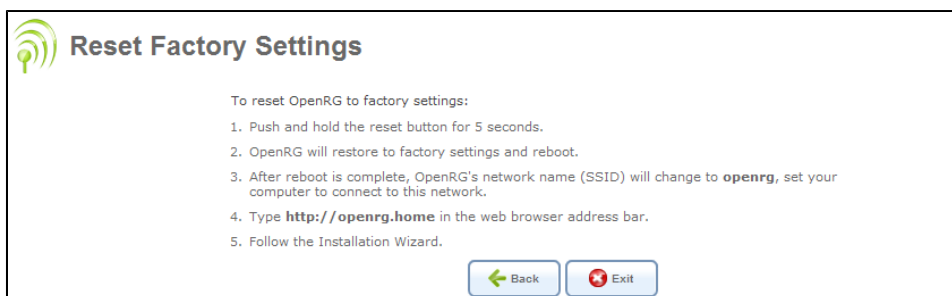


Figure 8.73. Reset Factory Settings

- **Contact the support center** If all previous methods have not been helpful, select this radio button and click 'Next'. The next screen contains instructions for calling the support center, and displays your gateway's identification required when opening a support call.

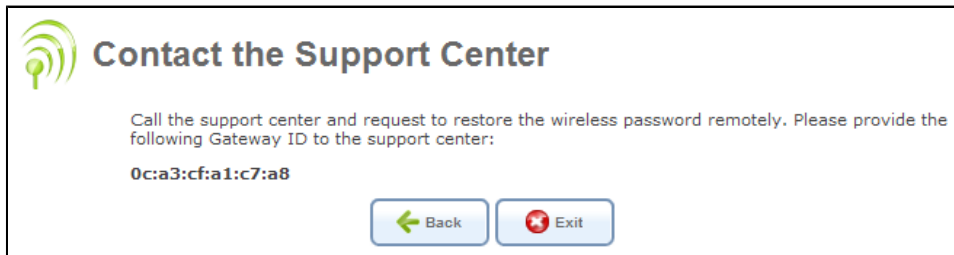


Figure 8.74. Contact the Support Center

8.4.7.5. Securing Your Wireless Network

OpenRG's wireless network is ready for operation with its default values. The following section describes how to secure your wireless connection using the **Wi-Fi Protected Access** (WPA) security protocol. The Wi-Fi Alliance created the WPA security protocol as a data encryption method for 802.11 wireless local area networks (WLANs). WPA is an industry-supported, pre-standard version of 802.11i utilizing the Temporal Key Integrity Protocol (TKIP), which fixes the problems of Wired Equivalent Privacy (WEP), including the use of dynamic keys.

8.4.7.5.1. Securing with WPA

1. Click the 'LAN Wireless 802.11g Access Point' link in the 'Network Connections' screen. The 'LAN Wireless 802.11g Access Point Properties' screen appears:



Figure 8.75. LAN Wireless 802.11g Access Point Properties – Enabled

2. Click the 'Wireless' tab.

3. Enable the 'Wireless Security' feature by selecting its 'Enabled' check box. The screen will refresh, displaying the wireless security options (see [Figure 8.76](#)).
4. From the 'Stations Security Type' drop-down menu, select "WPA".
5. Verify that the selected authentication method is "Pre-Shared Key".
6. In the 'Pre-Shared Key' text field, enter at least 8 characters. Verify that "ASCII" is selected in the associated drop-down menu.

Security

Stations Security Type: WPA

Authentication Method: Pre-Shared Key

Pre-Shared Key: ASCII

Encryption Algorithm: TKIP

Group Key Update Interval: 900 Seconds

Figure 8.76. WPA Wireless Security Parameters

7. Click 'OK'. The following 'Attention' screen will appear warning you that OpenRG might require reloading.

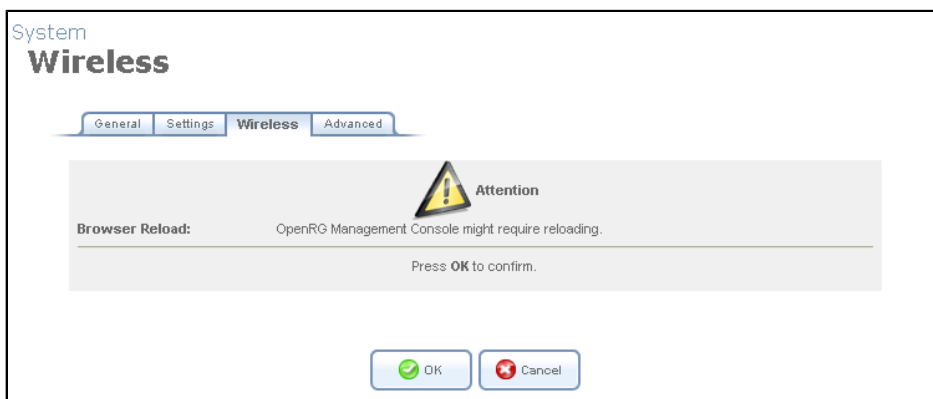


Figure 8.77. Browser Reload Warning

8. Click 'OK' to save the settings.

8.4.7.5.2. Connecting a Wireless Windows Client

If your PC has wireless capabilities, Windows will automatically recognize this and create a wireless connection for you. You can view this connection in the 'Network Connections' window.



Note: The following description and images are in accordance with Microsoft Windows XP, Version 2002, running Service Pack 2.

1. From the Windows Control Panel, open the 'Network Connections' window.



Figure 8.78. Network Connections

2. Double-click the wireless connection icon. The 'Wireless Network Connection' screen appears, displaying OpenRG's wireless connection. Note that the connection is defined as "Security-enabled wireless network (WPA)".

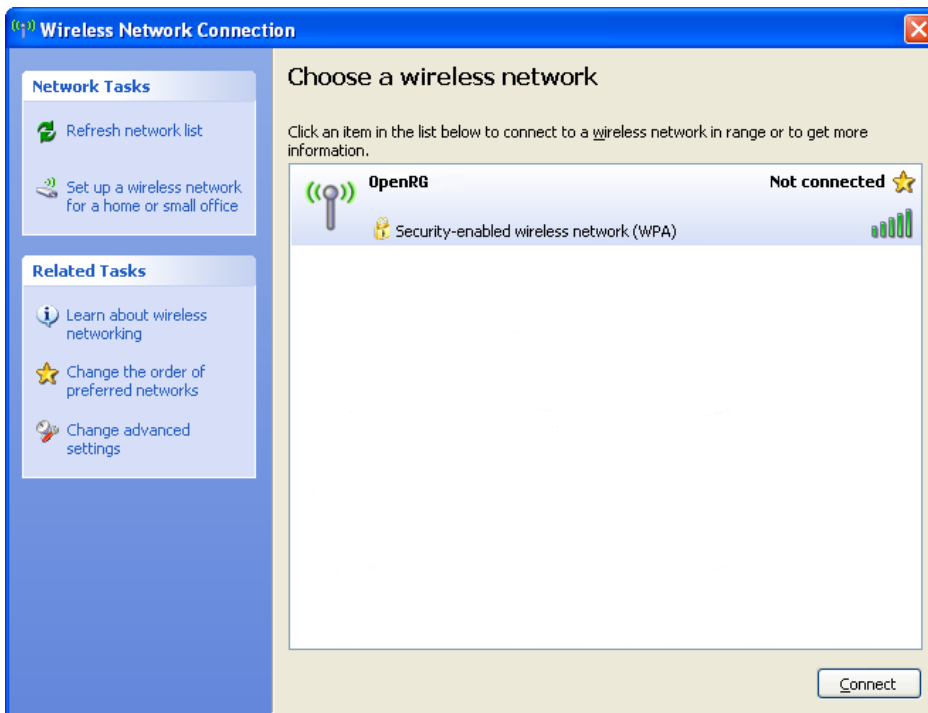


Figure 8.79. Available Wireless Connections

- Click the connection once to mark it, and then click the 'Connect' button at the bottom of the screen. The following login window appears, asking for a 'Network Key', which is the pre-shared key you have configured.



Figure 8.80. Wireless Network Connection Login

- Enter the pre-shared key in both fields and click the 'Connect' button. After the connection is established, its status will change to 'Connected'.

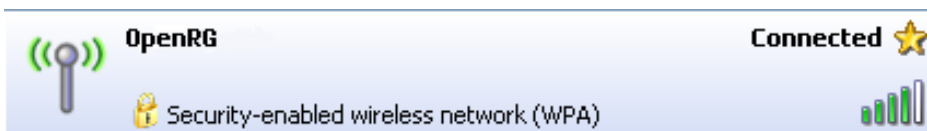


Figure 8.81. Connected Wireless Network

An icon will appear in the notification area, announcing the successful initiation of the wireless connection.

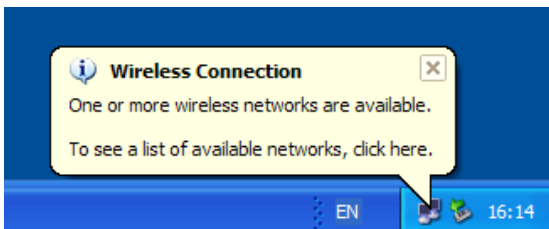


Figure 8.82. Wireless Connection Information

- Test the connection by disabling all other connections in the Windows 'Network Connections' screen above and browsing the Internet.

Should the login window above not appear and the connection attempt fail, configure the wireless connection manually:

- Click the connection once to mark it, and then click the 'Change advanced settings' link in the 'Related Tasks' box on the left part of the window (see [Figure 8.79](#)). The 'Wireless Network Connection Properties' window appears.

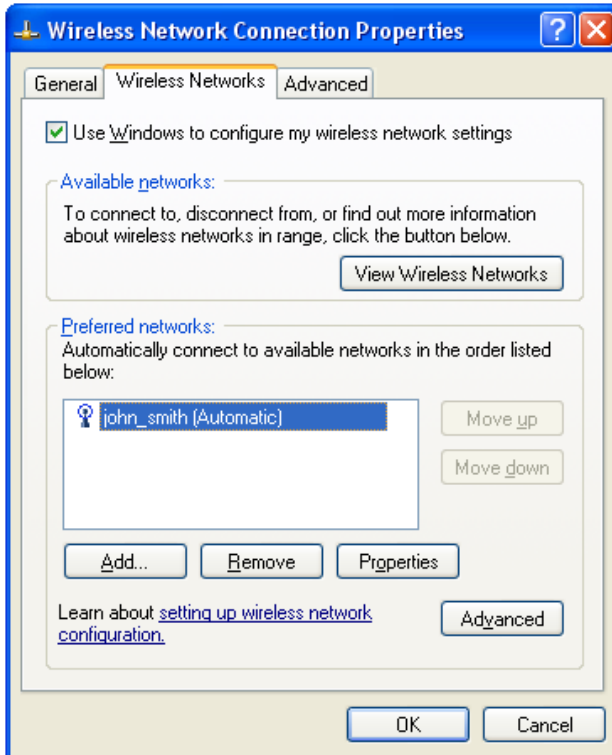


Figure 8.83. Wireless Network Connection Properties

2. Select the 'Wireless Networks' tab (see [Figure 8.83](#)).
3. Click your connection to highlight it, and click the 'Properties' button. Your connection's properties window appears.

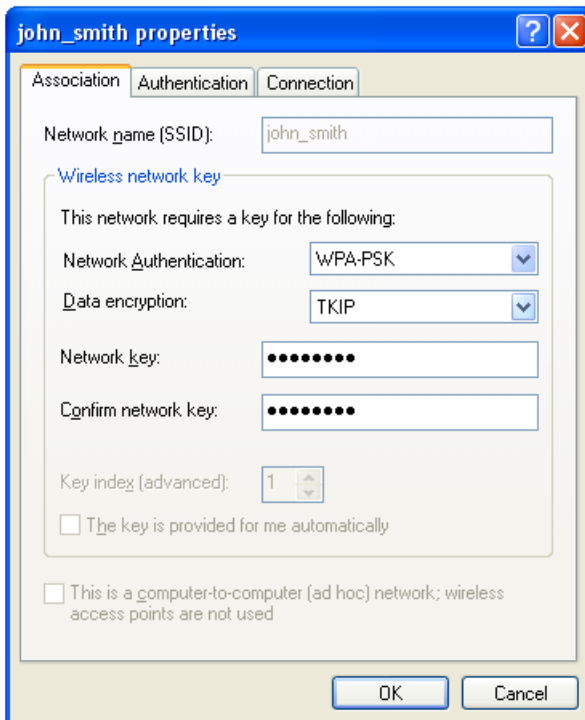


Figure 8.84. Connection Properties Configuration

- a. From the 'Network Authentication' drop-down menu, select "WPA-PSK".
 - b. From the 'Data Encryption' drop-down menu, select "TKIP".
 - c. Enter your pre-shared key in both the 'Network key' and the 'Confirm network key' fields.
4. Click 'OK' in both windows to save the settings.
 5. When attempting to connect to the wireless network, the login window will appear, pre-filled with the pre-shared key. Click the 'Connect' button to connect.

Since your network is now secured, only users that know the pre-shared key will be able to connect. The WPA security protocol is similar to securing network access using a password.

8.4.7.6. Configuring General Wireless Parameters

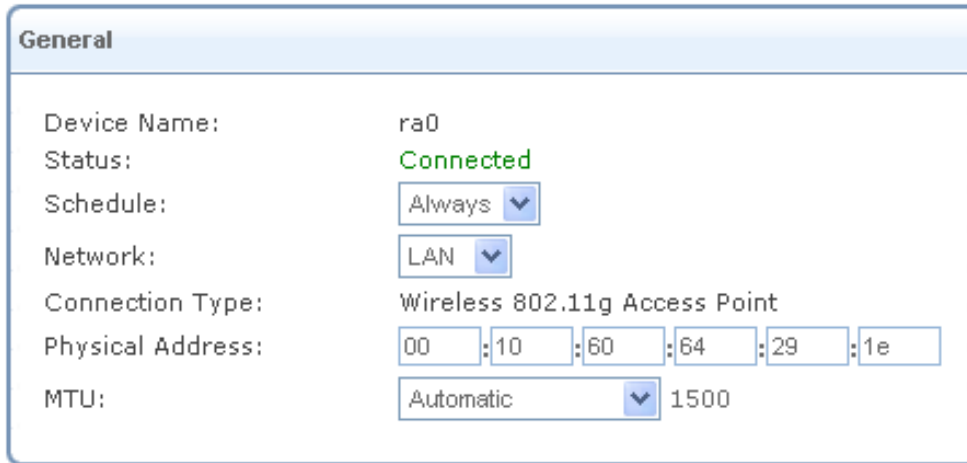
The 'LAN Wireless 802.11g Access Point Properties' screen displays a detailed summary of the wireless connection's parameters, under the 'General' sub-tab.



Figure 8.85. LAN Wireless 802.11g Access Point Properties – Enabled

Use the 'Settings' sub-tab to edit these parameters.

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.



General	
Device Name:	ra0
Status:	Connected
Schedule:	Always
Network:	LAN
Connection Type:	Wireless 802.11g Access Point
Physical Address:	00:10:60:64:29:1e
MTU:	Automatic 1500

Figure 8.86. General

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, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to [Section 8.9.3](#).

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to [Section 8.4.2](#).

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.

8.4.7.7. Defining Advanced Wireless Access Point Settings

The 'Wireless' and 'Advanced' sub-tabs enable you to perform advanced configuration of your wireless access point.

8.4.7.7.1. Wireless Network

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

The screenshot shows a configuration window for a wireless access point. It contains the following settings:

- Wireless Network (SSID): openrg
- SSID Broadcast
- 802.11 Mode: 802.11ng
- Channel: Automatic (FCC)
- Channel Width Mode: 20 MHz only
- Network Authentication: Open System Authentication
- MAC Filtering Mode: Disable

Figure 8.87. Wireless Access Point

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 your client's wireless card: 802.11g, 802.11b or in mixed mode. When using a 802.11ng card, this appears as a single option, as it supports all previous standards.

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. For example, in the U.S.A. the Regulatory Authority is the FCC (Federal Communications Commission).

Channel Width Mode This option appears on platforms supporting 802.11n only. Select the MHz width of the wireless channel, depending on your selected communication standard. For b and g, select either "20 MHz only" or "20/40 MHz (dynamic)". For 802.11n any mode may be selected.

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 drop-down menu, 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.

8.4.7.7.2. MAC Filtering Table

Use this section to define advanced wireless access point settings. Click 'New MAC Address' to define filtering of MAC addresses. The 'MAC Filtering Settings' screen appears.

Figure 8.88. MAC Filtering Settings

Enter the MAC address to be filtered and click 'OK' button. A MAC address list appears, upon which the selected filtering action (allow/deny) will be performed.




MAC Filtering Table	
MAC Address	Action
a0:b0:c0:d0:e0:f0	 
New MAC Address	

Figure 8.89. MAC Filtering Table

8.4.7.7.3. Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) is a method for simplifying the security setup and management of wireless networks. This feature is available on OpenRG, but is disabled by default. By enabling it, you can control the setup of your wireless security, which is defined in the following 'Security' section of the screen (refer to [Section 8.4.7.7.4](#)). Note that WPS only supports the WPA security protocol, therefore when enabling this feature, all other types of protocols are disabled (and are no longer available in the 'Security' section drop-down menu).

To enable WPS, click the 'Enabled' check box. The screen refreshes.

Figure 8.90. Wi-Fi Protected Setup

Create Key automatically You can either enter a security key manually, or have it generated automatically. Select your preference using the provided check box, and click 'Apply'. The screen refreshes.

The screenshot shows the WPS configuration interface. At the top, 'WPS' is checked as 'Enabled'. Below this, 'Create Key automatically' is also checked. The 'Status' is 'Ready'. The 'Protected Setup Method' is set to 'Push Button'. A 'Go' button is visible. Below the WPS section is the 'Security' section, which is set to 'WPA and WPA2'. The 'Authentication Method' is 'Pre-Shared Key'. The 'Pre-Shared Key' field contains the hexadecimal value '3effffffff164f67ffff1877ffff52ff2' and is set to 'Hex'. The 'Encryption Algorithm' is 'AES'. The 'Group Key Update Interval' is checked and set to '900' seconds.

Figure 8.91. Enabled WPS

If you had chosen automatic key generation, a pre-shared key (of hexadecimal value) has been generated, and appears in the 'Security' section. You can enter/change the value at anytime by typing a different one in the field, as well as change the type of the value to ASCII using the provided drop-down menu.

Status Indicates the WPS status. "Ready" means that the system is ready to negotiate with incoming wireless clients, or "enrollees".

Protected Setup Method OpenRG supports two setup methods, "Push Button" and "Pin Code". These are the methods used by wireless clients when seeking an access point. With "Push Button", the enrollment is initiated by either a physical button on the wireless device or through its software. With "Pin Code", the screen refreshes to provide a pin code field:

The screenshot shows the WPS configuration interface with the 'Protected Setup Method' changed to 'Pin Code'. The 'Go' button is still present. The 'Pin Code' field is now empty. The 'Status' remains 'Ready'. The 'Security' section remains unchanged from the previous screenshot.

Figure 8.92. Protected Setup Method – Pin Code

In this field, you must enter the eight digit pin number, provided by the wireless client's software. When attempting to connect a wireless client to OpenRG, you must be aware of its setup method. After initiating the enrollment procedure from the client, select the same setup method from this drop-down menu and click 'Go'. A connection attempt based on the pre-shared key will be initiated between the two devices, which will time out after two minutes if no connection is established. If a connection is established, the 'Status' field will change to reflect that.

The screenshot shows a WPS configuration window. At the top, 'WPS' is labeled with a checked box and the word 'Enabled'. Below this, there is a checked box for 'Create Key automatically'. The 'Status:' field displays 'Enrollee registration successfully completed' in green text. The 'Protected Setup Method:' is set to 'Push Button' in a dropdown menu. A 'Go' button is located at the bottom right of the configuration area.

Figure 8.93. Successful Enrollee Registration

8.4.7.7.4. Security

Use this section to configure your wireless security settings. Select the type of security protocol in the 'Stations Security Type' drop-down menu. The screen refreshes, presenting each protocol's configuration respectively.

- **None** Selecting this option disables security on your wireless connection.

The screenshot shows a 'Security' configuration window. The 'Stations Security Type:' is set to 'None' in a dropdown menu.

Figure 8.94. Disabled Wireless Security

- **WPA** WPA is a data encryption method for 802.11 wireless LANs (refer to [Section 8.4.7.5](#)).

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 drop-down menu provided.

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

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

Inter Client Privacy Select the check box to prevent communication between the wireless network clients using the same access point. Clients will not be able to view and access each other's shared directories.

The screenshot shows a configuration window titled "Security" with the following fields:

- Stations Security Type: WPA (dropdown menu)
- Authentication Method: Pre-Shared Key (dropdown menu)
- Pre-Shared Key: [empty text box] ASCII (dropdown menu)
- Encryption Algorithm: TKIP (dropdown menu)
- Group Key Update Interval: 900 Seconds

Figure 8.95. WPA Wireless Security Parameters

- **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 drop-down menu provided.

Pre Authentication When selecting the 802.1x authentication method, these two entries appear (see [Figure 8.96](#)). Select this option to enable OpenRG to accept RADIUS authentication requests from computers connected to other access points. This enables roaming from one wireless network to another.

PMK Cache Period The number of minutes before deletion (and renewal) of the Pairwise Master Key used for authentication.

The screenshot shows a configuration window with the following fields:

- Authentication Method: 802.1x (dropdown menu)
- Pre Authentication
- PMK Cache Period: 10 Minutes

Figure 8.96. 802.1x Authentication Method

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

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

Inter Client Privacy Select the check box to prevent communication between the wireless network clients using the same access point. Clients will not be able to view and access each other's shared directories.

Wireless Security Enabled

Stations Security Type: WPA2

Authentication Method: Pre-Shared Key

Pre-Shared Key: ASCII

Encryption Algorithm: AES

Group Key Update Interval: 900 Seconds

Inter Client Privacy

Figure 8.97. WPA2 Wireless Security Parameters

- **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 drop-down menu provided.

Pre Authentication When selecting the 802.1x authentication method, these two entries appear (see [Figure 8.98](#)). Select this option to enable OpenRG to accept RADIUS authentication requests from computers connected to other access points. This enables roaming from one wireless network to another.

PMK Cache Period The number of minutes before deletion (and renewal) of the Pairwise Master Key used for authentication.

Authentication Method: 802.1x

Pre Authentication

PMK Cache Period: 10 Minutes

Figure 8.98. 802.1x Authentication Method

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

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

Inter Client Privacy Select the check box to prevent communication between the wireless network clients using the same access point. Clients will not be able to view and access each other's shared directories.

Wireless Security	<input checked="" type="checkbox"/> Enabled
Stations Security Type:	WPA and WPA2 ▾
Authentication Method:	Pre-Shared Key ▾
Pre-Shared Key:	<input type="text"/> ASCII ▾
Encryption Algorithm:	TKIP and AES ▾
<input checked="" type="checkbox"/> Group Key Update Interval:	900 Seconds
<input type="checkbox"/> Inter Client Privacy	

Figure 8.99. WPA and WPA2 Wireless Security Parameters

- **802.1x WEP** 802.1x WEP is a data encryption method utilizing an automatically defined key for wireless clients that use 802.1x for authentication and WEP for encryption.

Inter Client Privacy Select the check box to prevent communication between the wireless network clients using the same access point. Clients will not be able to view and access each other's shared directories.

RADIUS Server Configure the RADIUS Server parameters (for more information, refer to [Section 7.13.4](#)).

- **Server IP** Enter the RADIUS server's IP address.
- **Server Port** Enter the RADIUS server's port.
- **Shared Secret** Enter your shared secret.

Security	
Stations Security Type:	802.1X WEP ▾
RADIUS Server	
Server IP:	<input type="text"/> 0 <input type="text"/> . <input type="text"/> 0 <input type="text"/> . <input type="text"/> 0 <input type="text"/> . <input type="text"/> 0
Server Port:	<input type="text"/> 1812
Shared Secret:	<input type="text"/>

Figure 8.100. 802.1x WEP Wireless Security Parameters

- **Non-802.1x WEP** Non-802.1x WEP is a data encryption method utilizing a statically defined key for wireless clients that do not use 802.1x for authentication, but use WEP for encryption. You may define up to four keys but use only one at a time. Note that the static key must be defined in the wireless Windows client as well.

Inter Client Privacy Select the check box to prevent communication between the wireless network clients using the same access point. Clients will not be able to view and access each other's shared directories.

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: ASCII or HEX.

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

Active	Encryption Key	Entry Method	Key Length
<input checked="" type="radio"/> 1	<input type="text"/>	ASCII	40 bit
<input type="radio"/> 2	<input type="text"/>	ASCII	40 bit
<input type="radio"/> 3	<input type="text"/>	ASCII	40 bit
<input type="radio"/> 4	<input type="text"/>	ASCII	40 bit

Figure 8.101. Non-802.1x WEP Wireless Security Parameters

The encryption key must be defined in the wireless Windows client as well. This is done in the Connection Properties Configuration window (to learn how to reach this window, refer to [Section 8.4.7.5.2](#) [503]).

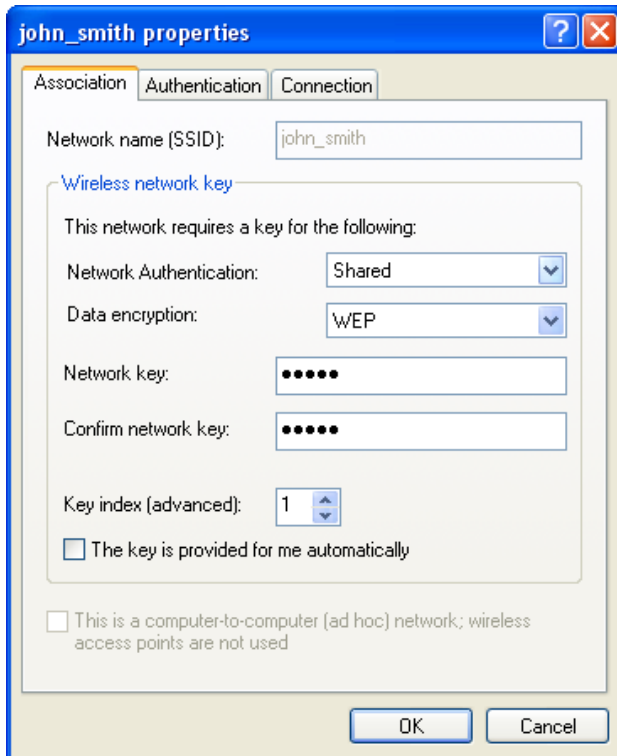


Figure 8.102. Connection Properties Configuration

1. In the 'Network Authentication' drop-down menu, select "Shared".
 2. In the 'Data Encryption' drop-down menu, select "WEP".
 3. Enter your encryption key in both the 'Network key' and the 'Confirm network key' fields.
- **Authentication Only** When selecting this option, wireless clients attempting to connect to the wireless connection will receive OpenRG's main login screen, along with the following attention message:

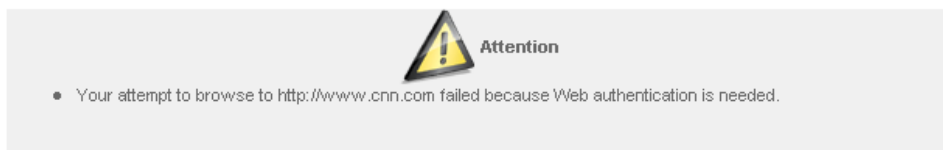


Figure 8.103. Web Authentication Needed

By logging into the WBM, clients authenticate themselves and are then able to use the connection. OpenRG keeps record of authenticated clients. To clear this list, click the 'Clean Mac List' button. Clients will have to re-authenticate themselves in order to use the wireless connection.

Security

Stations Security Type: Authentication Only

Authentication Method: Web Authentication

Clean Mac List

Figure 8.104. Authentication Only Wireless Security Parameters

8.4.7.7.5. Wireless WDS

OpenRG supports Wireless Distribution System (WDS), which enables wireless bridging of access points within its range. Virtual access points are used to interact with OpenRG's WDS peers, granting LAN users access to remote wireless networks.



Note: Different wireless cards support a different number of virtual access points. The scenarios depicted herein refer to the **Ralink RT-2561** wireless card, supporting up to four virtual wireless access points.

Select the 'Enabled' check-box. The screen refreshes.

Wireless WDS Enabled

Mode: Restricted

Encryption Algorithm: WEP

WDS List

New WDS

Figure 8.105. Wireless WDS

Mode OpenRG's WDS can function in one of the following modes:

- **Restricted** – WDS peers must be registered with OpenRG (by MAC addresses).
- **Bridge** – OpenRG will function as a wireless bridge, merely forwarding traffic between access points, and will not respond to wireless requests. The WDS peers must be manually stated and wireless stations will not be able to connect to OpenRG.
- **Repeater** – OpenRG will act as a repeater, interconnecting between access points. WDS peers can be determined by the user ('Restricted' mode) or auto-detected ('Lazy' mode).
- **Lazy** – Automatic detection of WDS peers: when a LAN user searches for a network, OpenRG will attempt to connect to WDS devices in its vicinity.

Encryption Algorithm When wireless security is enabled (refer to [Section 8.4.7.7.4](#)), this drop-down menu will display the encryption algorithms available for encrypting the communication between access points.

To add a WDS device, perform the following:

1. Click the 'New WDS' link, and press 'Apply'. If an 'Attention' screen appears, press 'OK'. The screen will refresh (see [Figure 8.106](#)). A new virtual device appears in the WDS list, with the initial status of disabled.

Wireless WDS Enabled

Mode:

Encryption Algorithm:

WDS List





Device	MAC Address	Status	Action
LAN Wireless 802.11g WDS	00:00:00:00:00:00	Device missing	 
New WDS			

Figure 8.106. Wireless WDS – New WDS

Note that devices added to the WDS list before the WDS feature is enabled in the main device appears as missing.

2. Click the new device's  action icon . The 'LAN Wireless 802.11g WDS Properties' screen appears (see [Figure 8.107](#)).

System

 **LAN Wireless 802.11g WDS Properties**

General Settings Wireless Advanced

Name:

Device Name: ra20

Status: Device missing

Network: LAN

Underlying Device: LAN Wireless 802.11g Access Point

Connection Type: Wireless 802.11g WDS

Download Rate: 54 MB

Upload Rate: 54 MB

IP Address Distribution: Disabled

Figure 8.107. LAN Wireless 802.11g WDS Properties

3. Click the Wireless tab, and enter the MAC address of the WDS peer with which this virtual access point is to interact, in the 'Other AP' section.

Wireless Access Point

MAC Filtering Mode:

MAC Filtering Settings [New MAC Address](#)

Wireless WDS

Other AP: : : : : :

Figure 8.108. LAN Wireless 802.11g WDS Properties – Wireless Tab

4. Click 'OK'. The 'Network Connections' screen appears, displaying the new virtual 'LAN Wireless 802.11g WDS' connection.

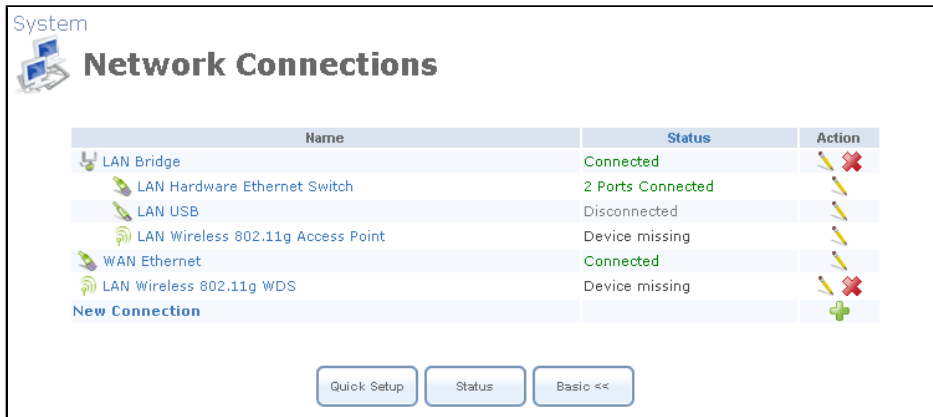



Figure 8.109. Network Connections

- Click the virtual connection's  action icon. The 'LAN Wireless 802.11g WDS Properties' screen reappears.

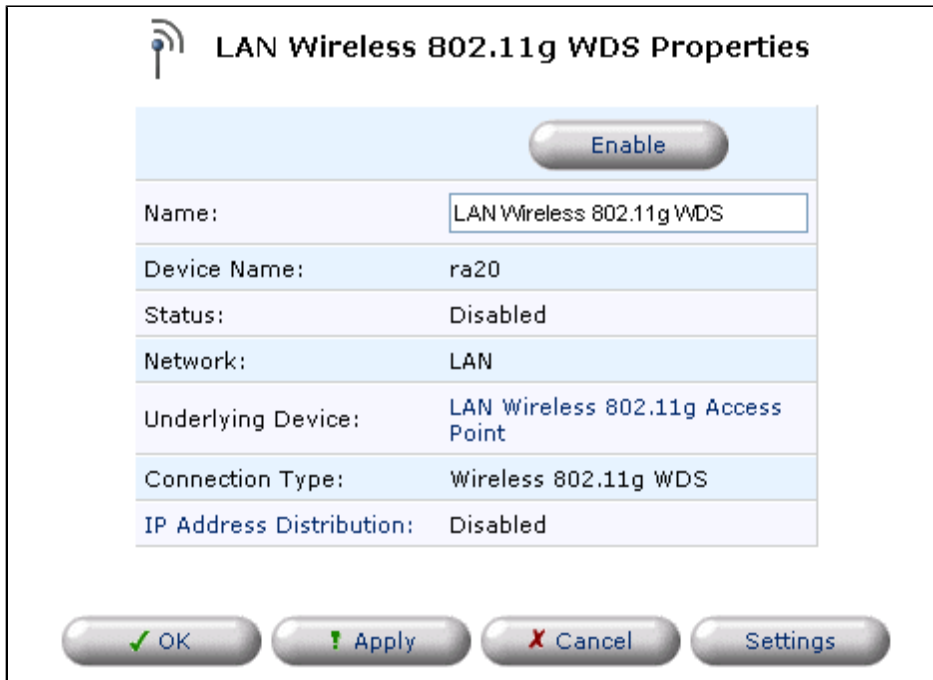


Figure 8.110. LAN Wireless 802.11g WDS Properties

- Press the 'Enable' button. The virtual connection is now enabled. Go back to the physical wireless connection configuration screen to view its details.




Wireless WDS		<input checked="" type="checkbox"/> Enabled	
Mode:		Restricted ▾	
Encryption Algorithm:		None ▾	
WDS List			
Device	MAC Address	Status	Action
LAN Wireless 802.11g WDS	00:00:00:00:00:20	Connected	 
New WDS			

Figure 8.111. Wireless WDS

If the WDS peer also operates in 'Restricted' mode, it should similarly be configured with OpenRG's MAC address in order for both access points to communicate.

8.4.7.7.6. Wireless QoS (WMM)

Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance certification, based on the IEEE 802.11e draft standard. It 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 (when working in 802.11n mode, this check box is not available as WMM is already enabled). The screen refreshes.

Wireless QoS (WMM)	<input checked="" type="checkbox"/> Enabled
Ack Policy (Per Access Category):	
Background:	Normal ▾
Best Effort:	Normal ▾
Video:	Normal ▾
Voice:	Normal ▾

Figure 8.112. Wireless QoS (WMM)

Background, Best Effort, Video and Voice are access categories for packet prioritization. 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 drop-down menu 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.

8.4.7.7.7. Transmission Properties

Use this section to define the wireless transmission settings.

Transmission Rate:	Auto
Transmit Power:	100 %
CTS Protection Mode:	None
CTS Protection Type:	cts-only
Frame Burst - Max Number:	3
Frame Burst - Burst Time:	2
Beacon Interval:	100 ms
DTIM Interval:	1 ms
Fragmentation Threshold:	2346
RTS Threshold:	2346

Figure 8.113. Transmission Properties

Transmission Rate The transmission rate is set according to the speed of your wireless connection. Select the transmission rate from the drop-down menu, or select 'Auto' to have OpenRG automatically use the fastest possible data transmission rate (the only option when using 802.11g). Note that if your wireless connection is weak or unstable, it is best to select a low transmission rate.

Transmit Power The percentage of maximum transmission power.

CTS Protection Mode CTS Protection Mode boosts your gateway's ability to intercept 802.11g and 802.11b transmissions. Conversely, CTS Protection Mode decreases performance. Leave this feature disabled unless you encounter severe communication difficulties between the gateway and 802.11g products. If enabling, select "Always". Select "Auto" to have OpenRG automatically decide whether or not to use this feature.

CTS Protection Type Select the type of CTS protection—cts-only or rts-cts.

Frame Burst This feature (also known as *packet bursting*) increases the speed of a 802.11g-based wireless network by unwrapping short packets and rebundling them into a larger one.



Note: This feature is only supported by the Atheros wireless cards.

- **Frame Burst – Max Number** At any given time, only one wireless client can communicate with the access point. Therefore, clients, competing for air time, transmit data in frame bursts. Use this field to determine the maximum number of frames that OpenRG will allow clients to transmit in a single frame burst.
- **Frame Burst – Burst Time** The maximum length of a frame burst. Limit the time of a frame burst to avoid large frames from taking communication precedence.

Beacon Interval A beacon is a packet broadcast by OpenRG to synchronize the wireless network. The Beacon Interval value indicates how often the beacon is sent.

DTIM Interval The Delivery Traffic Indication Message (DTIM) is a countdown value that informs wireless clients of the next opportunity to receive multicast and broadcast messages. This value ranges between 1 and 16384.

Fragmentation Threshold Packets that are larger than this threshold are fragmented into multiple packets. Try to increase the fragmentation threshold if you encounter high packet error rates. Do not set the threshold too low, since this can result in reduced networking performance.

RTS Threshold OpenRG sends Request to Send (RTS) packets to the wireless client in order to negotiate the dispatching of data. The wireless client responds with a Clear to Send (CTS) packet, signaling that transmission can commence. In case packets are smaller than the preset threshold, the RTS/CTS mechanism is not active. If you encounter inconsistent data flow, try a minor reduction of the RTS threshold size.

8.4.7.7.8. Virtual Access Points

You can set up multiple virtual wireless LANs on OpenRG, limited only to the number supported by your wireless card. Such virtual wireless LANs are referred to as "Virtual APs" (virtual access points).



Note: Different wireless cards support a different number of virtual access points. The scenarios depicted herein refer to the **Ralink RT-2561** wireless card, supporting up to four virtual wireless access points.

The 'Virtual APs' section appears under the 'Wireless' sub-tab of the 'LAN Wireless 802.11g Access Point Properties' screen, and displays OpenRG's physical wireless access point, on top of which virtual connections may be created.

Virtual APs					
Name	BSSID	SSID	Status	Action	
LAN Wireless 802.11g Access Point	00:03:7f:0b:a5:a7	openrg	Connected		
New Virtual AP					

Figure 8.114. Virtual APs

To create a virtual connection, click the 'New Virtual AP' link. The screen refreshes, displaying the new virtual connection.

Virtual APs					
Name	BSSID	SSID	Status	Action	
LAN Wireless 802.11g Access Point	00:03:7f:0b:a5:a7	openrg	Connected		
LAN Wireless 802.11g Access Point - Virtual AP	06:03:7f:0b:a5:a7	openrg	Connected		
New Virtual AP					

Figure 8.115. New Virtual Access Point

The new connection will also be added to the network connections list, and will be configurable like any other connection.

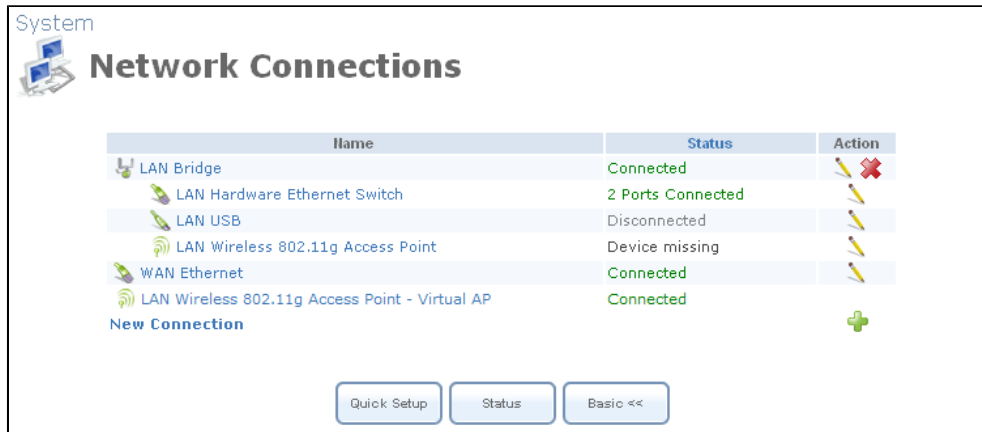



Figure 8.116. Network Connections

You can edit the new virtual access point's properties by clicking its  action icon. The 'LAN Wireless 802.11g Access Point - Virtual AP Properties' screen appears. For example, change the connection's default name by changing the SSID value in the 'Wireless' sub-tab.

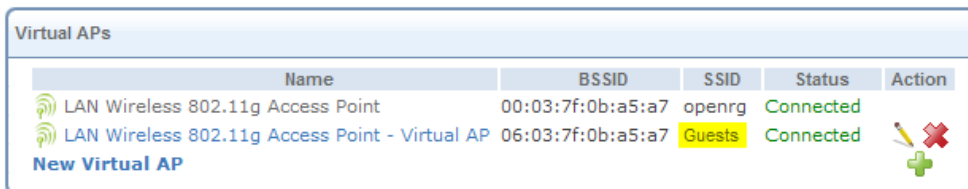


Figure 8.117. LAN Wireless 802.11g Access Point – Virtual AP Properties

A usage example for this virtual connection is to dedicate it for guest access. Through this connection, guests will be able to access the WAN, but they will be denied access to other wireless LANs provided by OpenRG. To do so, perform the following:

1. Set a firewall rule that blocks access to all other OpenRG LANs.

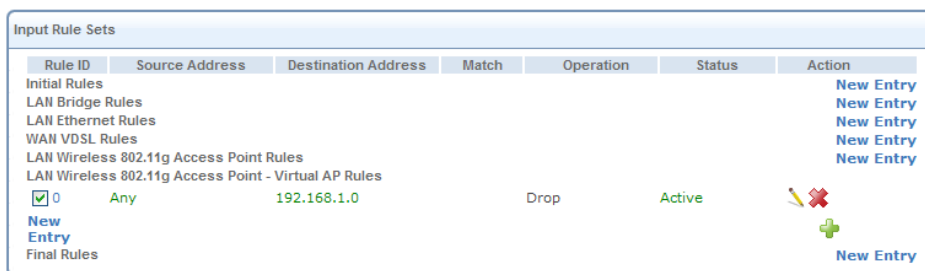


Figure 8.118. Firewall Rule

To learn how to do so, refer to [Section 7.3.9](#).

2. Back in the virtual connection's 'LAN Wireless 802.11g Access Point - Virtual AP Properties' screen:
 - a. In the 'Internet Protocol' section under the 'Settings' sub-tab, enter an IP address for the connection by selecting 'Use the Following IP Address'.

Internet Protocol		Use the Following IP Address			
IP Address:		192	.168	.5	.1
Subnet Mask:		255	.255	.255	.0

Figure 8.119. Internet Protocol

- b. In the 'IP Address Distribution' section, select 'DHCP Server' and enter the IP range from which IP addresses will be granted to wireless guests.

IP Address Distribution		DHCP Server			
Start IP Address:		192	.168	.5	.2
End IP Address:		192	.168	.5	.20
Subnet Mask:		255	.255	.255	.0
WINS Server:		0	.0	.0	.0
Lease Time in Minutes:		60			
<input checked="" type="checkbox"/> Provide Host Name If Not Specified by Client					

Figure 8.120. IP Address Distribution

- c. Click 'OK' to save the settings.

After going through this procedure, you have secured all of your wireless connections. A guest will only be able to connect to the "Guests" wireless LAN, from which only the WAN access will be granted.

8.4.7.7.9. Advanced

Use the 'Advanced' sub-tab to configure the following parameters.

- **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. To learn more about your gateway's security features, refer to [Section 7.3](#).

Internet Connection Firewall	
	<input type="checkbox"/> Enabled

Figure 8.121. Internet Connection Firewall

- **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 and the <http://openrg.home>.


Additional IP Addresses		
IP Address	Subnet Mask	Action
New IP Address		

Figure 8.122. Additional IP Addresses

8.4.8. WAN Ethernet

The WAN Ethernet connection can connect OpenRG to another network either directly or via an external modem. The Connection Wizard provides three methods to quickly configure this connection, described later in this chapter:

1. Ethernet Connection (refer to [Section 8.4.10](#)).
2. Dynamic Host Configuration Protocol (refer to [Section 8.4.17](#)).
3. Manual IP Address Configuration (refer to [Section 8.4.18](#)).

8.4.8.1. General

To view and edit the WAN Ethernet connection settings, click the 'WAN Ethernet' link in the 'Network Connections' screen (see [Figure 8.12](#)). The 'WAN Ethernet Properties' screen will appear (see [Figure 8.123](#)), 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.

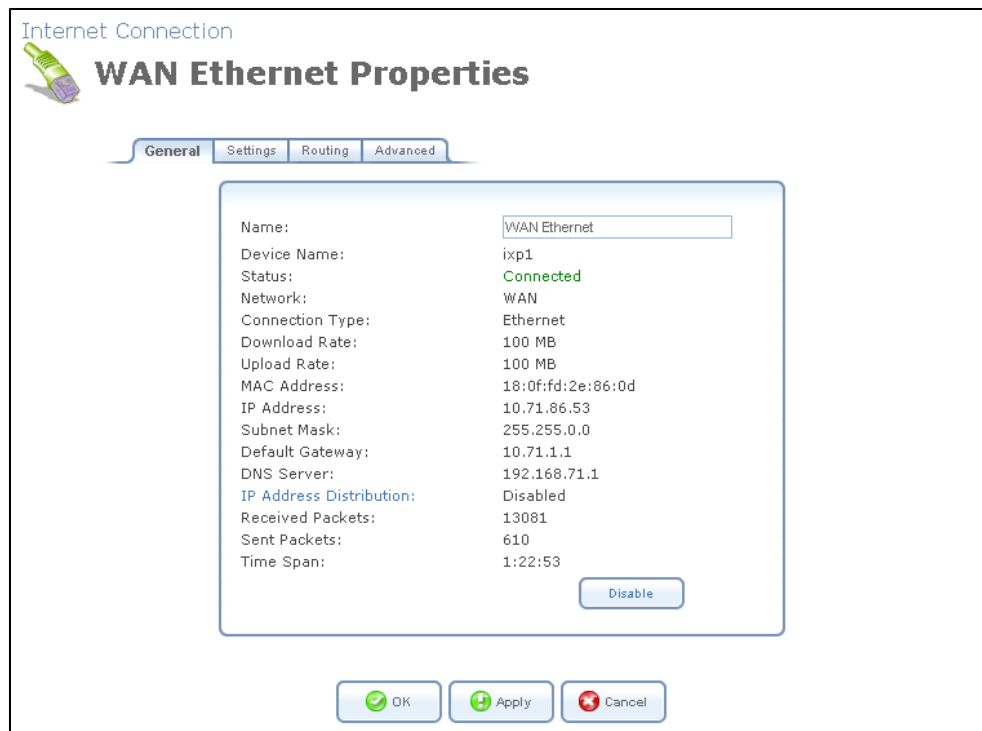


Figure 8.123. WAN Ethernet Properties

8.4.8.2. 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.

General	
Device Name:	ixp1
Status:	Connected
Schedule:	Always ▾
Network:	WAN ▾
Connection Type:	Ethernet
Physical Address:	28 : cd : ed : 43 : 91 : f2
	<input type="button" value="Clone My MAC Address"/>
MTU:	Automatic ▾ 1500

Figure 8.124. General

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, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to [Section 8.9.3](#).

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to [Section 8.4.2](#).

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

Clone My MAC Address Press this button to copy your PC's current MAC address to the board.

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' drop-down menu:

- No IP Address
- Obtain an IP Address Automatically
- Use the Following IP Address

Note that the screen will refresh to display relevant configuration settings according to your choice.

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.



Internet Protocol: No IP Address

Figure 8.125. Internet Protocol – No IP Address

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 click 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.

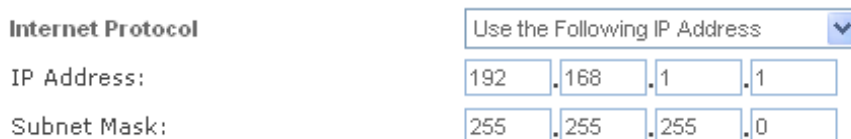


Internet Protocol: Obtain an IP Address Automatically

Override Subnet Mask: 0 . 0 . 0 . 0

Figure 8.126. Internet Protocol Settings – Automatic IP

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.



Internet Protocol: Use the Following IP Address

IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255 . 255 . 255 . 0

Figure 8.127. Internet Protocol – Static IP

DNS Server Domain Name System (DNS) 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. To configure the connection to automatically obtain a DNS server address, select 'Obtain DNS Server Address Automatically' from the 'DNS Server' drop down menu.



DNS Server: Obtain DNS Server Address Automatically

Figure 8.128. DNS Server – Automatic IP

To manually configure DNS server addresses, select 'Use the Following DNS Server Addresses' from the 'DNS Server' drop down menu (see figure 'DNS Server -- Static IP'). Specify up to two different DNS server address, one primary, another secondary.


DNS Server	Use the Following DNS Server Addresses 
Primary DNS Server:	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
Secondary DNS Server:	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>

Figure 8.129. DNS Server – Static IP

To learn more about this feature, refer to [Section 7.13.1](#).

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. For a comprehensive description of this feature, please refer to [Section 7.13.2](#). Select one of the following options from the 'IP Address Distribution' combo-box:

- DHCP Server

1. **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 255.255.0.0.

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 local 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 a host name to it.

2. Click 'OK' to save the settings.


- **IP Address Distribution**  DHCP Server
| Start IP Address: | . . . |
| End IP Address: | . . . |
| Subnet Mask: | . . . |
| Lease Time in Minutes: | |
| Provide Host Name If Not Specified by Client | |

Figure 8.130. IP Address Distribution -- DHCP Server

- **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 OpenRG's WAN to work in routing mode. For more information, refer to [Section 7.13.2.2](#).

1. After selecting 'DHCP Relay' from the drop down menu, a 'New IP Address' link will appear:



Figure 8.131. IP Address Distribution - DHCP Relay

Click the 'New IP Address' link. The 'DHCP Relay Server Address' screen will appear:

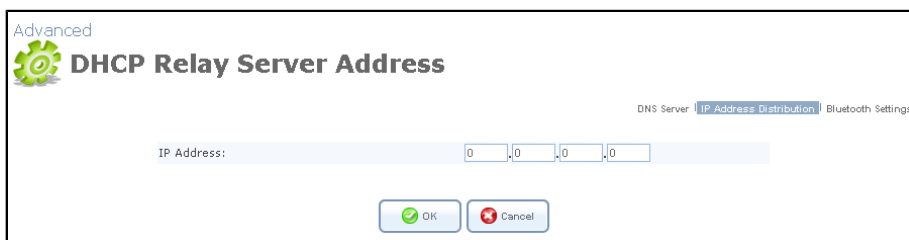


Figure 8.132. DHCP Relay Server Address

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.



Figure 8.133. IP Address Distribution - Disable DHCP

8.4.8.3. 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.

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.

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'.

Multicast – IGMP Proxy Internal / Default OpenRG serves as an IGMP proxy, issuing IGMP host messages on behalf of its LAN hosts. This check box is enabled on LAN connections by default, meaning that if a LAN multicast server is available, other LAN hosts asking to join multicast groups (by sending IGMP requests) will be able to join its multicast group. However, this check box is disabled on the WAN connection by default, meaning that LAN hosts will not be able to join multicast groups of WAN multicast servers. When creating a WAN-LAN bridge, this check box must also be deselected.

IGMP Query Version OpenRG supports all three versions of IGMP. Select the version you would like to use. Note that this drop-down menu appears for LAN connections only.

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.

Routing Mode:

Device Metric:

Default Route

Multicast - IGMP Proxy Internal

IGMP Query Version:

Routing Information Protocol (RIP)

Name	Destination	Gateway	Netmask	Metric	Status	Action
LAN Bridge	192.168.2.4	192.168.1.1	255.255.255.255	2	Applied	
New Route						

Figure 8.134. Advanced Routing Properties

To learn more about this feature, refer to [Section 8.6.1](#).

8.4.8.4. IPv6

Click on the 'New Unicast Address' link to add an IPv6 unicast address. To learn more about configuring IPv6 settings, refer to [Section 8.6.2](#).

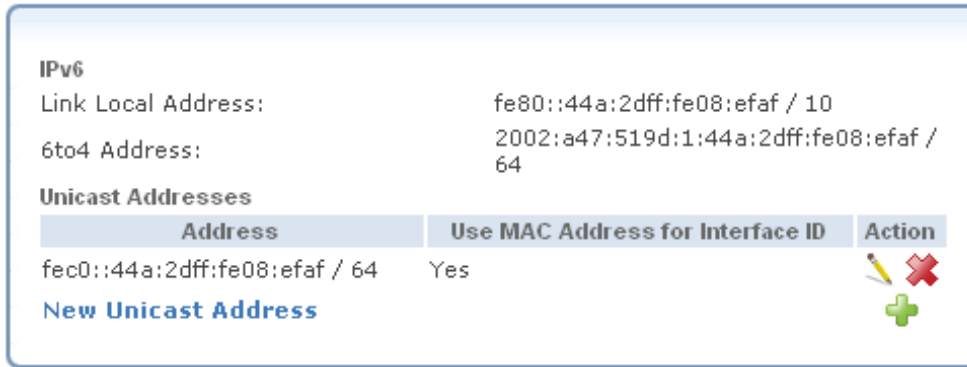


Figure 8.135. IPv6 Settings

8.4.8.5. 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. To learn more about your gateway's security features, refer to [Section 7.3](#).

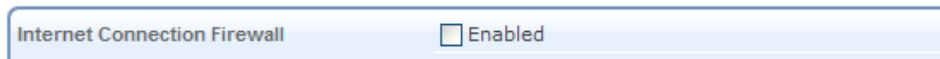


Figure 8.136. Internet Connection Firewall

Internet Connection Fastpath Select this check box to utilize the *Fastpath* algorithm for enhancing packet flow, resulting in faster communication between the LAN and the WAN. By default, this feature is enabled.

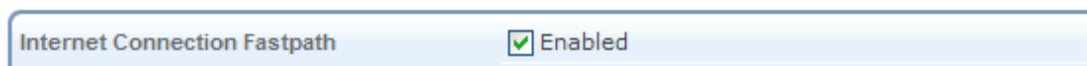


Figure 8.137. Internet Connection Fastpath

- **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 and the <http://openrg.home>.

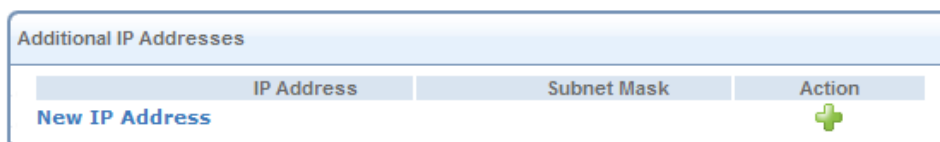


Figure 8.138. Additional IP Addresses

8.4.9. Point-to-Point Protocol over Ethernet (PPPoE)

Point-to-Point Protocol over Ethernet (PPPoE) relies on two widely accepted standards, PPP and Ethernet. PPPoE enables your home network PCs that communicate on an Ethernet network to exchange information with PCs on the Internet. PPPoE supports the protocol layers and authentication widely used in PPP and enables a point-to-point connection to be established in the normally multipoint architecture of Ethernet. A discovery process in PPPoE determines the Ethernet MAC address of the remote device in order to establish a session.

8.4.9.1. Creation with the Connection Wizard

To create a new PPPoE connection, perform the following:

1. Click the 'New Connection' link in the 'Network Connections' screen (see [Figure 8.12](#)). The 'Connection Wizard' screen appears (see [Figure 8.13](#)).
2. Select the 'Internet Connection' radio button and click 'Next'. The 'Internet Connection' screen appears (see [Figure 8.14](#)).
3. Select the 'External DSL Modem' radio button and click 'Next'. The 'Point-to-Point Protocol over Ethernet' screen appears.



System

Point-to-Point Protocol over Ethernet (PPPoE)

Configure your PPPoE connection properties:

Login User Name (case sensitive): john_smith

Login Password: ****

< Back Next > Cancel

Figure 8.139. Point-to-Point Protocol over Ethernet

4. Enter the username and password provided by your Internet Service Provider (ISP), and click 'Next'. The 'Connection Summary' screen appears.



Figure 8.140. Connection Summary

5. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.
6. Click 'Finish' to save the settings.

The new PPPoE connection will be added to the network connections list, and will be configurable like any other connection.



Note: If your WAN connection is set to PPPoE when there is no PPPoE server available, and a DHCP server is available instead, the device status will show: "In Progress – DHCP server found, consider configuring your WAN connection to Automatic". If you select this option, refer to [Section 4.4.1.2](#).

8.4.9.2. General

To view and edit the PPPoE connection settings, click the 'WAN PPPoE' link in the 'Network Connections' screen (see [Figure 8.12](#)). The 'WAN PPPoE Properties' screen will appear (see [Figure 8.141](#)), 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.

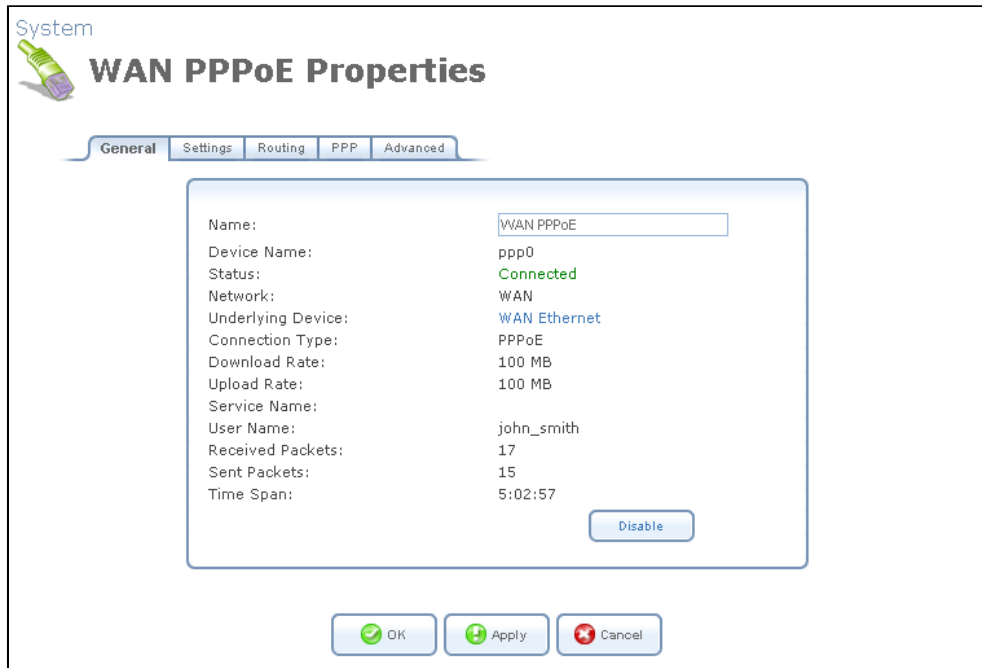


Figure 8.141. WAN PPPoE Properties

8.4.9.3. Settings

General This section displays the connection's general parameters.



Figure 8.142. General PPPoE Settings

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, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to [Section 8.9.3](#).

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to [Section 8.4.2](#).

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.

Underlying Connection Specify the underlying connection above which the protocol will be initiated.

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

- Unnumbered
- Obtain an IP Address Automatically
- Use the Following IP Address

Please note that the screen will refresh to display relevant configuration settings according to your choice.

Unnumbered Select this option to assign a predefined LAN address as OpenRG's WAN address. This is useful when OpenRG operates in routing mode. Before selecting this option, configure the 'Internet Protocol' of your LAN device (or bridge, in case the LAN device is under a bridge) to use a permanent (static) IP address from the range of IP addresses provided by your ISP (instead of 192.168.1.1).

Internet Protocol

Figure 8.143. Internet Protocol – Unnumbered

Obtain an IP Address Automatically Your connection is configured by default to obtain an IP automatically. You should change this configuration in case your service provider requires it. 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.

Internet Protocol

Override Subnet Mask:

Figure 8.144. Internet Protocol – Automatic IP

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.

Internet Protocol

IP Address:

Subnet Mask:

Figure 8.145. Internet Protocol – Static IP

DNS Server Domain Name System (DNS) 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. To configure the connection to automatically obtain a DNS server address, select 'Obtain DNS Server Address Automatically' from the 'DNS Server' drop down menu.



Figure 8.146. DNS Server – Automatic IP

To manually configure DNS server addresses, select 'Use the Following DNS Server Addresses' from the 'DNS Server' drop down menu (see figure 'DNS Server -- Static IP'). Specify up to two different DNS server address, one primary, another secondary.



Figure 8.147. DNS Server – Static IP

To learn more about this feature, refer to [Section 7.13.1](#).

8.4.9.4. 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.

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.

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'.

Multicast – IGMP Proxy Internal / Default OpenRG serves as an IGMP proxy, issuing IGMP host messages on behalf of its LAN hosts. This check box is enabled on LAN connections by default, meaning that if a LAN multicast server is available, other LAN hosts asking to join multicast groups (by sending IGMP requests) will be able to join its multicast group. However, this check box is disabled on the WAN connection by default, meaning that LAN hosts will not be able to join multicast groups of WAN multicast servers. When creating a WAN-LAN bridge, this check box must also be deselected.

IGMP Query Version OpenRG supports all three versions of IGMP. Select the version you would like to use. Note that this drop-down menu appears for LAN connections only.

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.

Routing Mode: ▼

Device Metric:

Default Route

Multicast - IGMP Proxy Internal

IGMP Query Version: ▼

Routing Information Protocol (RIP)

Name	Destination	Gateway	Netmask	Metric	Status	Action
LAN Bridge	192.168.2.4	192.168.1.1	255.255.255.255	2	Applied	
New Route						

Figure 8.148. Advanced Routing Properties

To learn more about this feature, refer to [Section 8.6.1](#).

8.4.9.5. PPP

Point-to-Point Protocol (PPP) is the most popular method for transporting packets between the user and the Internet service provider. PPP supports authentication protocols such as PAP and CHAP, as well as other compression and encryption protocols.

Service Name Specify the networking peer's service name, if provided by your ISP.

PPP-on-Demand Use PPP on demand to initiate the point-to-point protocol session only when packets are actually sent over the Internet.

Time Between Reconnect Attempts Specify the duration between PPP reconnected attempts, as provided by your ISP.

PPP

Service Name (should be filled only if specified by provider):

On Demand (will attempt to connect only when packets are sent)

Time Between Reconnect Attempts: Seconds

Figure 8.149. PPP Configuration

PPP Authentication Point-to-Point Protocol (PPP) currently supports four authentication protocols: Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and Microsoft CHAP version 1 and 2. This section allows you to select the authentication protocols your gateway may use when negotiating with a PPTP server. Select all the protocols if no information is available about the server's authentication protocols. Note that encryption is performed only if 'Microsoft CHAP', 'Microsoft CHAP version 2', or both are selected.

PPP Authentication

Login User Name (case sensitive):

Login Password:

Support Unencrypted Password (PAP)

Support Challenge Handshake Authentication (CHAP)

Support Microsoft CHAP (MS-CHAP)

Support Microsoft CHAP Version 2 (MS-CHAP v2)

Figure 8.150. PPP Authentication

Login User Name As agreed with ISP.

Login Password As agreed with ISP.

Support Unencrypted Password (PAP) Password Authentication Protocol (PAP) is a simple, plain-text authentication scheme. The user name and password are requested by your networking peer in plain-text. PAP, however, is not a secure authentication protocol. Man-in-the-middle attacks can easily determine the remote access client's password. PAP offers no protection against replay attacks, remote client impersonation, or remote server impersonation.

Support Challenge Handshake Authentication (CHAP) The Challenge Handshake Authentication Protocol (CHAP) is a challenge-response authentication protocol that uses MD5 to hash the response to a challenge. CHAP protects against replay attacks by using an arbitrary challenge string per authentication attempt.

Support Microsoft CHAP Select this check box if you are communicating with a peer that uses Microsoft CHAP authentication protocol.

Support Microsoft CHAP Version 2 Select this check box if you are communicating with a peer that uses Microsoft CHAP Version 2 authentication protocol.

PPP Encryption PPP supports encryption facilities to secure the data across the network connection. A wide variety of encryption methods may be negotiated, although typically

only one method is used in each direction of the link. This section allows you to select the encryption methods your gateway may use when negotiating with a PPTP server. Select all the methods if no information is available about the server's encryption methods. Please note that PPP encryption can only be used with MS-CHAP or MS-CHAP-V2 authentication protocols.

PPP Encryption

- Require Encryption (Disconnect If Server Declines)
- Support Encryption (40 Bit Keys)
- Support Maximum Strength Encryption (128 Bit Keys)

Figure 8.151. PPP Encryption

Require Encryption Select this check box to ensure that the PPP connection is encrypted.

Support Encryption (40 Bit Keys) Select this check box if your peer supports 40 bit encryption keys.

Support Maximum Strength Encryption (128 Bit Keys) Select this check box if your peer supports 128 bit encryption keys.

PPP Compression The PPP Compression Control Protocol (CCP) is responsible for configuring, enabling, and disabling data compression algorithms on both ends of the point-to-point link. It is also used to signal a failure of the compression/ decompression mechanism in a reliable manner.

PPP Compression

BSD:

Deflate:

Figure 8.152. PPP Compression

For each compression algorithm, select one of the following from the drop down menu:

Reject Reject PPP connections with peers that use the compression algorithm.

Allow Allow PPP connections with peers that use the compression algorithm.

Require Ensure a connection with a peer is using the compression algorithm.

8.4.9.6. 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. To learn more about your gateway's security features, refer to [Section 7.3](#).

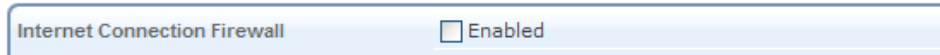


Figure 8.153. Internet Connection Firewall

Internet Connection Fastpath Select this check box to utilize the *Fastpath* algorithm for enhancing packet flow, resulting in faster communication between the LAN and the WAN. By default, this feature is enabled.

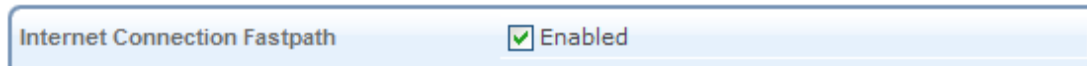


Figure 8.154. Internet Connection Fastpath

8.4.10. Ethernet Connection

The Ethernet connection wizard utility is one of the three methods used to configure the physical WAN Ethernet connection, described in [Section 8.4.8](#). It is the most basic method, intended for connections that do not require user name and password in order to connect to the Internet. To configure a new Ethernet connection, perform the following:

1. Click the 'New Connection' link in the 'Network Connections' screen (see [Figure 8.12](#)). The 'Connection Wizard' screen appears (see [Figure 8.13](#)).
2. Select the 'Internet Connection' radio button and click 'Next'. The 'Internet Connection' screen appears (see [Figure 8.14](#)).
3. Select the 'External Cable Modem' radio button and click 'Next'. The 'Internet Cable Modem Connection' screen appears.

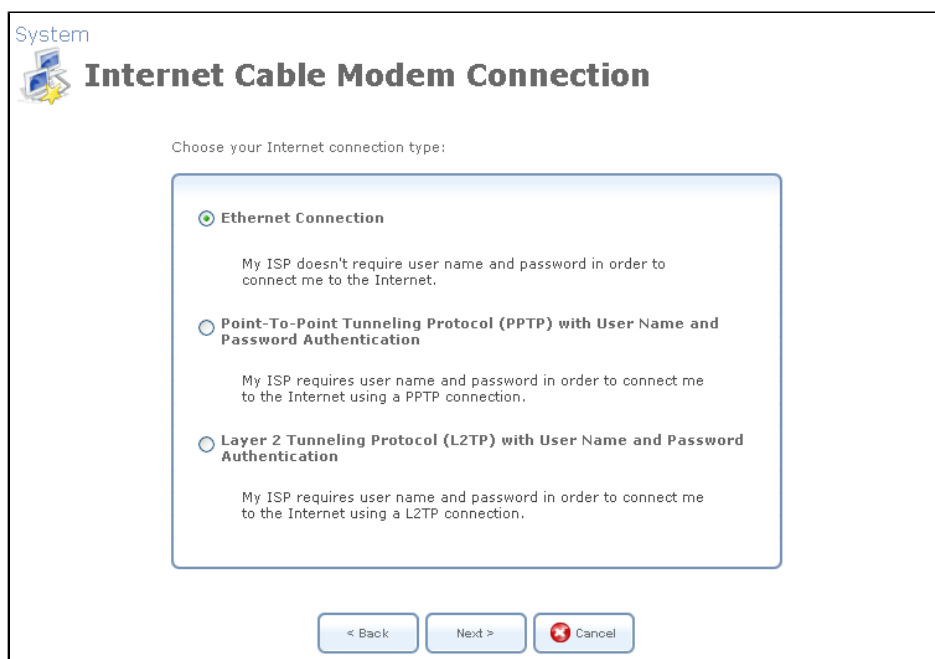


Figure 8.155. Internet Cable Modem Connection

4. Select the 'Ethernet Connection' radio button and click 'Next'. The 'Connection Summary' screen appears.

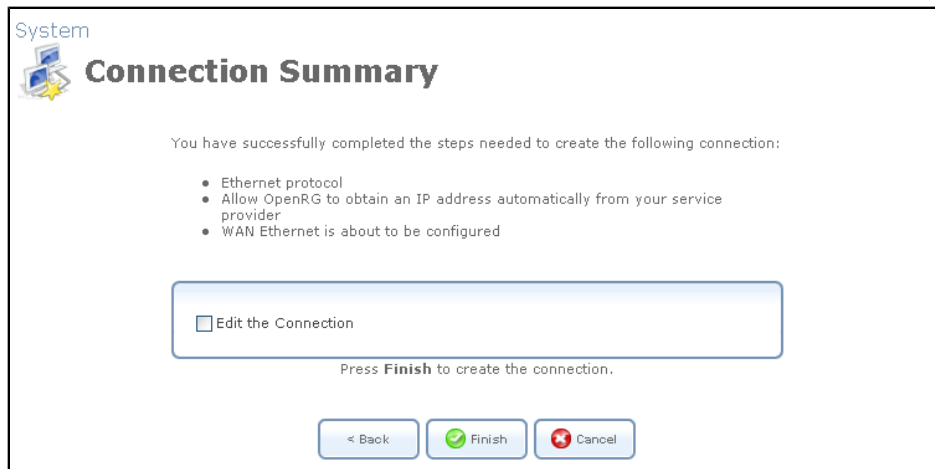


Figure 8.156. Connection Summary

5. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.
6. Click 'Finish' to save the settings.

The WAN Ethernet connection will be configured accordingly. Refer to [Section 8.4.8](#) to learn how to view and edit the connection's settings.

8.4.11. Layer 2 Tunneling Protocol (L2TP)

Layer 2 Tunneling Protocol (L2TP) is an extension to the PPP protocol, enabling your gateway to create VPN connections. Derived from Microsoft's Point-to-Point Tunneling Protocol (PPTP) and Cisco's Layer 2 Forwarding (L2F) technology, L2TP encapsulates PPP frames into IP packets either at the remote user's PC or at an ISP that has an L2TP Remote Access Concentrator (LAC). The LAC transmits the L2TP packets over the network to the L2TP Network Server (LNS) at the corporate side. With OpenRG, L2TP is targeted at serving two purposes:

1. Connecting OpenRG to the Internet when it is used as a cable modem, or when using an external cable modem. Such a connection is established using user name and password authentication.
2. Connecting OpenRG to a remote network using a Virtual Private Network (VPN) tunnel over the Internet. This enables secure transfer of data to another location over the Internet, using private and public keys for encryption and digital certificates, and user name and password for authentication.

8.4.11.1. Creating an L2TP connection with the Connection Wizard

To create a new L2TP connection, perform the following:

1. Click the 'New Connection' link in the 'Network Connections' screen (see [Figure 8.12](#)). The 'Connection Wizard' screen appears (see [Figure 8.13](#)).
2. Select the 'Internet Connection' radio button and click 'Next'. The 'Internet Connection' screen appears (see [Figure 8.14](#)).
3. Select the 'External Cable Modem' radio button (this option is for both internal and external cable modems) and click 'Next'. The 'Internet Cable Modem Connection' screen appears.

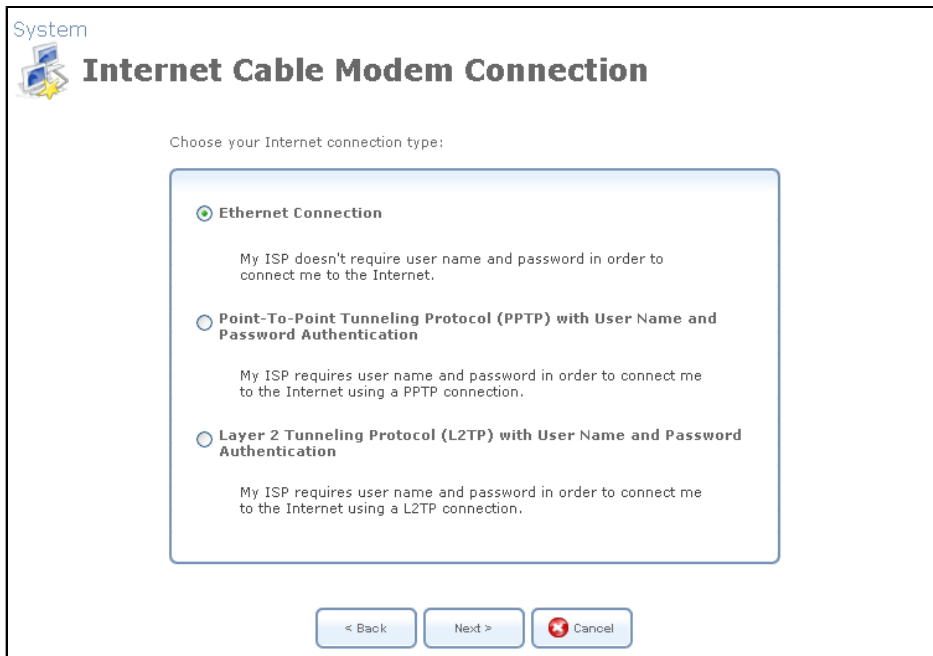


Figure 8.157. Internet Cable Modem Connection

4. Select the 'Layer 2 Tunneling Protocol (L2TP) with the 'User Name and Password Authentication' radio button and click 'Next'. The 'Layer 2 Tunneling Protocol (L2TP)' screen appears.

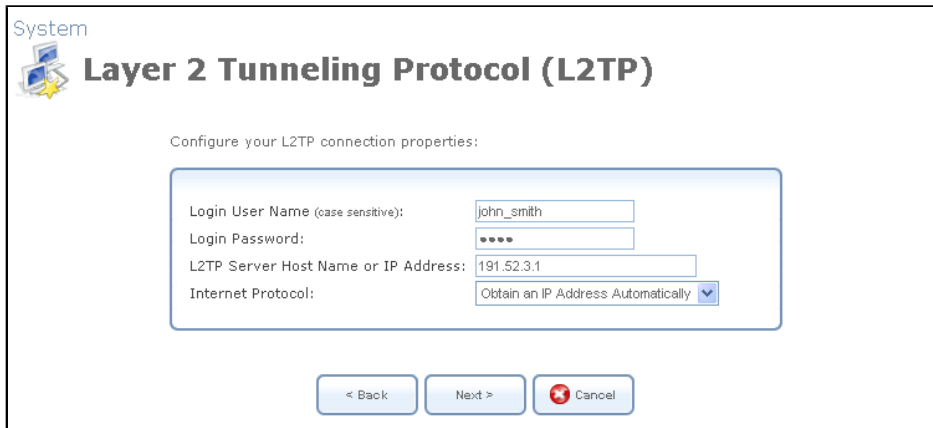


Figure 8.158. Layer 2 Tunneling Protocol (L2TP)

5. Enter the username and password provided by your Internet Service Provider (ISP).
6. Enter the L2TP server host name or IP address provided by your ISP.
7. Select whether to obtain an IP address automatically or specify one. This option is described in great detail in [Internet Protocol](#).
8. Click Next. The 'Connection Summary' screen appears.




Figure 8.159. Connection Summary

9. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.
10. Click 'Finish' to save the settings.

The new L2TP connection will be added to the network connections list, and will be configurable like any other connection.

8.4.11.2. Creating an L2TP IPsec VPN connection with the Connection Wizard

To create a new L2TP IPsec VPN connection, perform the following steps:

1. Click the 'New Connection' link in the 'Network Connections' screen (see [Figure 8.12](#)). The 'Connection Wizard' screen appears (see [Figure 8.13](#)).
2. Select the 'Connect to a Virtual Private Network over the Internet' radio button and click 'Next'. The 'Connect to a Virtual Private Network over the Internet' screen appears (see figure 'Connect to a Virtual Private Network over the Internet').
3. Select the 'VPN Client or Point-To-Point' radio button and click 'Next'. The 'VPN Client or Point-To-Point' screen appears.

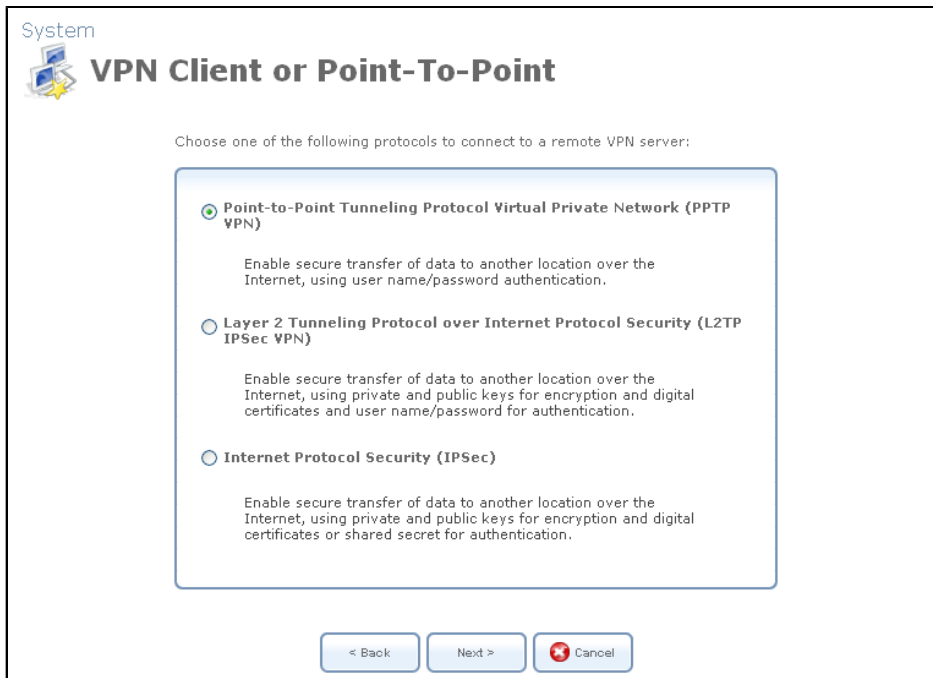


Figure 8.160. VPN Client or Point-To-Point

4. Select the 'Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP IPsec VPN)' radio button and click 'Next'. The 'Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP IPsec VPN)' screen appears.



System

Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP IPsec VPN)

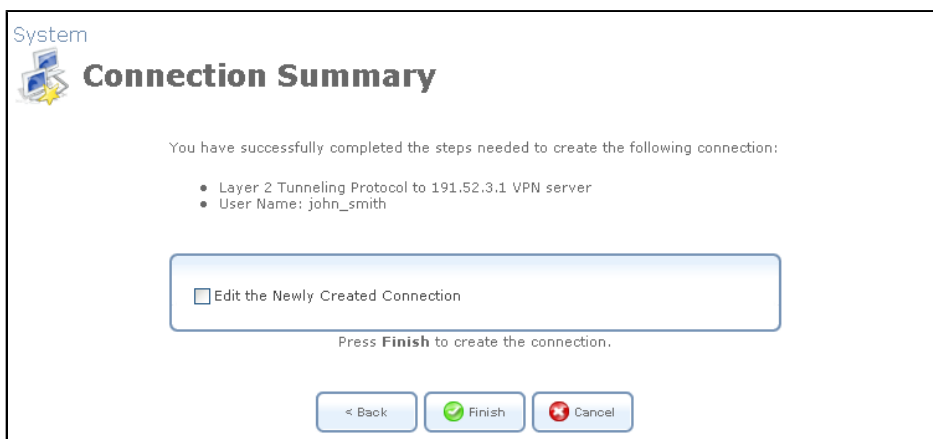
Configure your L2TP VPN connection properties:

Login User Name (case sensitive):	john_smith
Login Password:	••••
IPsec Shared Secret:	••••••••
Remote Tunnel Endpoint Address:	191.52.3.1

< Back Next > Cancel

Figure 8.161. Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP IPsec VPN)

5. Enter the username and password provided by the administrator of the network you are trying to access.
6. Enter the IPsec shared secret, which is the encryption key jointly decided upon with the network you are trying to access.
7. Enter the remote tunnel endpoint address. This would be the IP address or domain name of the remote network computer, which serves as the tunnel's endpoint.
8. Click 'Next'. The 'Connection Summary' screen appears.



System

Connection Summary

You have successfully completed the steps needed to create the following connection:

- Layer 2 Tunneling Protocol to 191.52.3.1 VPN server
- User Name: john_smith

Edit the Newly Created Connection

Press **Finish** to create the connection.

< Back Finish Cancel

Figure 8.162. Connection Summary

9. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.
10. Click 'Finish' to save the settings.

The new L2TP IPsec VPN connection will be added to the network connections list, and will be configurable like any other connection.

8.4.11.3. General

To view and edit the L2TP connection settings, click the 'L2TP' link in the 'Network Connections' screen (see [Figure 8.12](#)). The 'L2TP Properties' screen appears (see [Figure 8.163](#)), 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 8.163. L2TP Properties

8.4.11.4. Settings

General This section displays the connection's general parameters.

General	
Device Name:	ppp300
Status:	Connected
Schedule:	Always ▼
Network:	WAN ▼
Connection Type:	L2TP
MTU:	Automatic ▼ 1456
Underlying Connection:	VPN IPSec

Figure 8.164. General L2TP Settings

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, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to [Section 8.9.3](#).

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to [Section 8.4.2](#).

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' drop-down menu:

- Obtain an IP Address Automatically
- Use the Following IP Address

Note that the screen refreshes to display relevant configuration settings according to your choice.

Obtain an IP Address Automatically Your connection is configured by default to obtain an IP automatically. You should change this configuration in case your service provider requires it. 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.

The screenshot shows the 'Internet Protocol' configuration window. The 'Internet Protocol' dropdown menu is set to 'Obtain an IP Address Automatically'. Below it, there is a checkbox labeled 'Override Subnet Mask' which is currently unchecked. To the right of the checkbox are four input boxes for the subnet mask, each containing the number '0'.

Figure 8.165. Internet Protocol – Automatic IP

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.

The screenshot shows the 'Internet Protocol' configuration window. The 'Internet Protocol' dropdown menu is set to 'Use the Following IP Address'. Below it, there are two rows of input boxes. The first row is labeled 'IP Address:' and contains four boxes with the values '192', '168', '1', and '1'. The second row is labeled 'Subnet Mask:' and contains four boxes with the values '255', '255', '255', and '0'.

Figure 8.166. Internet Protocol – Static IP

DNS Server Domain Name System (DNS) 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. To configure the connection to automatically obtain a DNS server address, select 'Obtain DNS Server Address Automatically' from the 'DNS Server' drop down menu.

The screenshot shows the 'DNS Server' configuration window. The 'DNS Server' dropdown menu is set to 'Obtain DNS Server Address Automatically'.

Figure 8.167. DNS Server – Automatic IP

To manually configure DNS server addresses, select 'Use the Following DNS Server Addresses' from the 'DNS Server' drop down menu (see figure 'DNS Server -- Static IP'). Specify up to two different DNS server address, one primary, another secondary.

DNS Server	Use the Following DNS Server Addresses ▾
Primary DNS Server:	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
Secondary DNS Server:	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>

Figure 8.168. DNS Server – Static IP

To learn more about this feature, refer to [Section 7.13.1](#).

8.4.11.5. 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.

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.

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'.

Multicast – IGMP Proxy Internal / Default OpenRG serves as an IGMP proxy, issuing IGMP host messages on behalf of its LAN hosts. This check box is enabled on LAN connections by default, meaning that if a LAN multicast server is available, other LAN hosts asking to join multicast groups (by sending IGMP requests) will be able to join its multicast group. However, this check box is disabled on the WAN connection by default, meaning that LAN hosts will not be able to join multicast groups of WAN multicast servers. When creating a WAN-LAN bridge, this check box must also be deselected.

IGMP Query Version OpenRG supports all three versions of IGMP. Select the version you would like to use. Note that this drop-down menu appears for LAN connections only.

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.

Routing Mode:

Device Metric:

Default Route

Multicast - IGMP Proxy Internal

IGMP Query Version:

Routing Information Protocol (RIP)

Name	Destination	Gateway	Netmask	Metric	Status	Action
LAN Bridge	192.168.2.4	192.168.1.1	255.255.255.255	2	Applied	
New Route						

Figure 8.169. Advanced Routing Properties

To learn more about this feature, refer to [Section 8.6.1](#).

8.4.11.6. PPP

PPP Point-to-Point Protocol (PPP) is the most popular method for transporting packets between the user and the Internet service provider. PPP supports authentication protocols such as PAP and CHAP, as well as other compression and encryption protocols.

PPP-on-Demand Use PPP on demand to initiate the point-to-point protocol session only when packets are actually sent over the Internet.

Time Between Reconnect Attempts Specify the duration between PPP reconnected attempts, as provided by your ISP.

PPP

On Demand (will attempt to connect only when packets are sent)

Time Between Reconnect Attempts: Seconds

Figure 8.170. PPP Configuration

PPP Authentication Point-to-Point Protocol (PPP) currently supports four authentication protocols: Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and Microsoft CHAP version 1 and 2. This section allows you to select the authentication protocols your gateway may use when negotiating with a PPTP server. Select all the protocols if no information is available about the server's authentication protocols. Note that encryption is performed only if 'Microsoft CHAP', 'Microsoft CHAP version 2', or both are selected.

PPP Authentication

Login User Name (case sensitive):

Login Password:

Support Unencrypted Password (PAP)

Support Challenge Handshake Authentication (CHAP)

Support Microsoft CHAP (MS-CHAP)

Support Microsoft CHAP Version 2 (MS-CHAP v2)

Figure 8.171. PPP Authentication

Login User Name As agreed with ISP.

Login Password As agreed with ISP.

Support Unencrypted Password (PAP) Password Authentication Protocol (PAP) is a simple, plain-text authentication scheme. The user name and password are requested by your networking peer in plain-text. PAP, however, is not a secure authentication protocol. Man-in-the-middle attacks can easily determine the remote access client's password. PAP offers no protection against replay attacks, remote client impersonation, or remote server impersonation.

Support Challenge Handshake Authentication (CHAP) The Challenge Handshake Authentication Protocol (CHAP) is a challenge-response authentication protocol that uses MD5 to hash the response to a challenge. CHAP protects against replay attacks by using an arbitrary challenge string per authentication attempt.

Support Microsoft CHAP Select this check box if you are communicating with a peer that uses Microsoft CHAP authentication protocol.

Support Microsoft CHAP Version 2 Select this check box if you are communicating with a peer that uses Microsoft CHAP Version 2 authentication protocol.

PPP Encryption PPP supports encryption facilities to secure the data across the network connection. A wide variety of encryption methods may be negotiated, although typically only one method is used in each direction of the link. This section allows you to select the encryption methods your gateway may use when negotiating with a PPTP server. Select all the methods if no information is available about the server's encryption methods. Please note that PPP encryption can only be used with MS-CHAP or MS-CHAP-V2 authentication protocols.

PPP Encryption

Require Encryption (Disconnect If Server Declines)

Support Encryption (40 Bit Keys)

Support Maximum Strength Encryption (128 Bit Keys)

Figure 8.172. PPP Encryption

Require Encryption Select this check box to ensure that the PPP connection is encrypted.

Support Encryption (40 Bit Keys) Select this check box if your peer supports 40 bit encryption keys.

Support Maximum Strength Encryption (128 Bit Keys) Select this check box if your peer supports 128 bit encryption keys.

8.4.11.7. L2TP

L2TP Define your ISP's server parameters.

- **L2TP Server Host Name or IP Address** Enter the connection's host name or IP address obtained from your ISP.
- **Shared Secret** Enter the shared secret value obtained from your ISP.

The screenshot shows a window titled "System" with a sub-header "L2TP VPN Properties". Below the title bar are tabs for "General", "Settings", "Routing", "PPP", "L2TP", and "Advanced". The "L2TP" tab is selected. Inside the dialog, there is a section labeled "L2TP" containing two input fields: "L2TP Server Host Name or IP Address" with the value "191.52.3.1" and "Shared Secret" with a masked value of ".....". At the bottom of the dialog are three buttons: "OK" (with a green checkmark), "Apply" (with a green plus sign), and "Cancel" (with a red X).

Figure 8.173. L2TP Configuration

8.4.11.8. 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. To learn more about your gateway's security features, refer to [Section 7.3](#).

The screenshot shows a single checkbox labeled "Internet Connection Firewall" with the text "Enabled" to its right. The checkbox is currently unchecked.

Figure 8.174. Internet Connection Firewall

8.4.12. Layer 2 Tunneling Protocol Server (L2TP Server)

OpenRG can act as a Layer 2 Tunneling Protocol Server (L2TP Server), accepting L2TP client connection requests.

Creation with the Connection Wizard

To create a new L2TP Server, perform the following:

1. Click the 'New Connection' link in the 'Network Connections' screen (see [Figure 8.12](#)). The 'Connection Wizard' screen appears (see [Figure 8.13](#)).
2. Select the 'Connect to a Virtual Private Network over the Internet' radio button and click 'Next'. The 'Connect to a Virtual Private Network over the Internet' screen appears (see figure 'Connect to a Virtual Private Network over the Internet').
3. Select the 'VPN Server' radio button and click 'Next'. The 'VPN Server' screen appears.

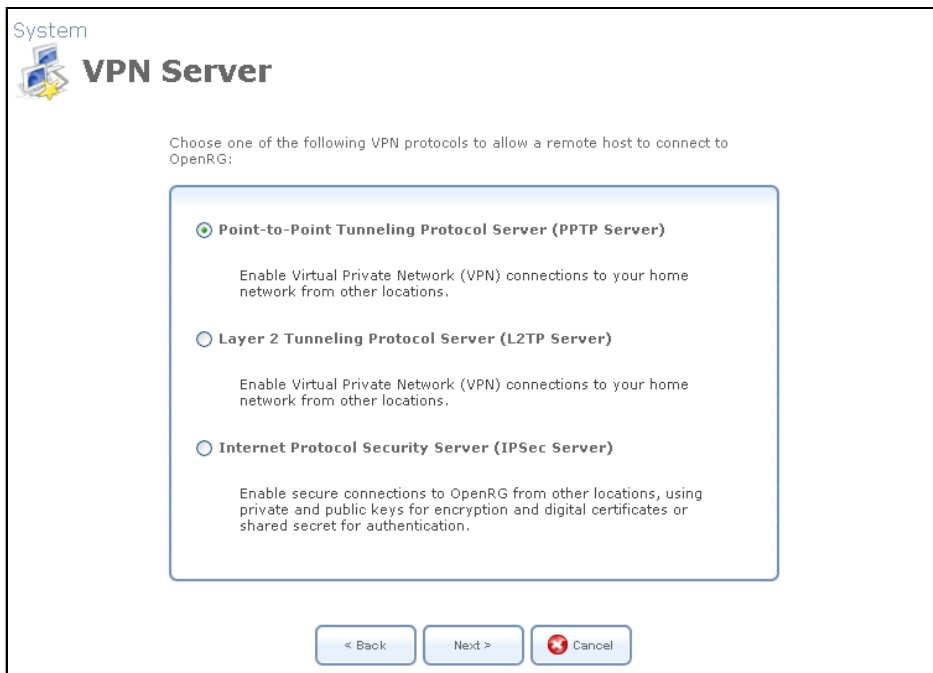


Figure 8.175. VPN Server

4. Select the 'Layer 2 Tunneling Protocol Server (L2TP Server)' radio button and click Next. The 'Layer 2 Tunneling Protocol (L2TP)' screen appears.

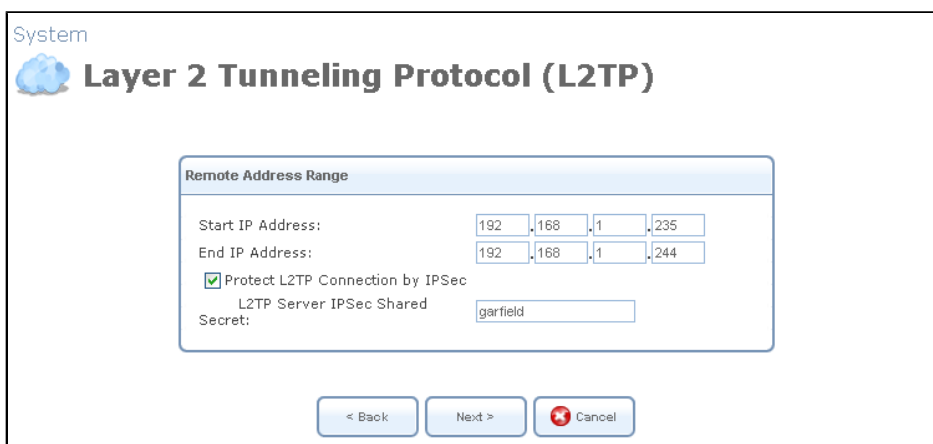


Figure 8.176. Layer 2 Tunneling Protocol (L2TP)

5. In this screen, perform the following:
 - a. Specify the address range that OpenRG will reserve for remote users. You may use the default values as depicted in [Figure 8.176](#).
 - b. By default, the L2TP connection is protected by the IP Security (IPSec) protocol (the option is checked). However, if you wish to keep this setting, you must provide a string that will serve as the 'L2TP Server IPSec Shared Secret'. Alternatively, uncheck this option to disable L2TP protection by IPSec.
6. Click Next. The 'Connection Summary' screen appears (see [Figure 8.177](#)). Note the attention message alerting that there are no users with VPN permissions.

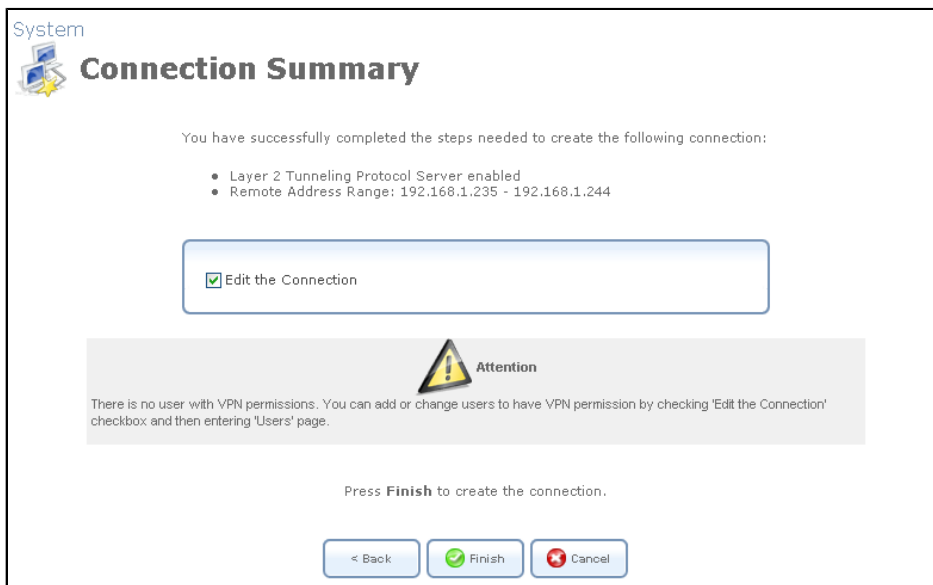


Figure 8.177. Connection Summary

7. Check the 'Edit the Connection' check box and click 'Finish'. The 'Layer 2 Tunneling Protocol Server (L2TP Server)' screen appears.

Figure 8.178. Advanced L2TP Server Parameters

8. Click the 'Click Here to Create VPN Users' link to define remote users that will be granted access to your home network. Refer to [Section 8.3](#) to learn how to define and configure users.
9. Click 'OK' to save the settings.

The new L2TP Server will be added to the network connections list, and will be configurable like any connection. Unlike other connections, it is also accessible via the OpenRG's 'Advanced' screen. Note that the connection wizard automatically creates a default IPsec connection in order to protect the L2TP connection. To learn more, refer to [Section 7.10.4](#).

To learn how to configure your L2TP and IPsec clients in order to connect to the L2TP server, refer to [Section 7.10.4.3](#).

8.4.13. Point-to-Point Tunneling Protocol (PPTP)

Point-to-Point Tunneling Protocol (PPTP) is a protocol developed by Microsoft targeted at creating VPN connections over the Internet. This enables remote users to access the gateway via any ISP that supports PPTP on its servers. PPTP encapsulates network traffic, encrypts content using Microsoft's Point-to-Point Encryption (MPPE) protocol that is based on RC4,

and routes using the generic routing encapsulation (GRE) protocol. With OpenRG, PPTP is targeted at serving two purposes:

1. Connecting OpenRG to the Internet when it is used as a cable modem, or when using an external cable modem. Such a connection is established using user name and password authentication.
2. Connecting OpenRG to a remote network using a Virtual Private Network (VPN) tunnel over the Internet. This enables secure transfer of data to another location over the Internet, using user name and password authentication.

8.4.13.1. Creating a PPTP connection with the Connection Wizard

To create a new PPTP connection, perform the following steps:

1. Click the 'New Connection' link in the 'Network Connections' screen (see [Figure 8.12](#)). The 'Connection Wizard' screen appears (see [Figure 8.13](#)).
2. Select the 'Internet Connection' radio button and click 'Next'. The 'Internet Connection' screen appears (see [Figure 8.14](#)).
3. Select the External Cable Modem radio button (this option is for both internal and external cable modems) and click Next. The 'Internet Cable Modem Connection' screen appears.

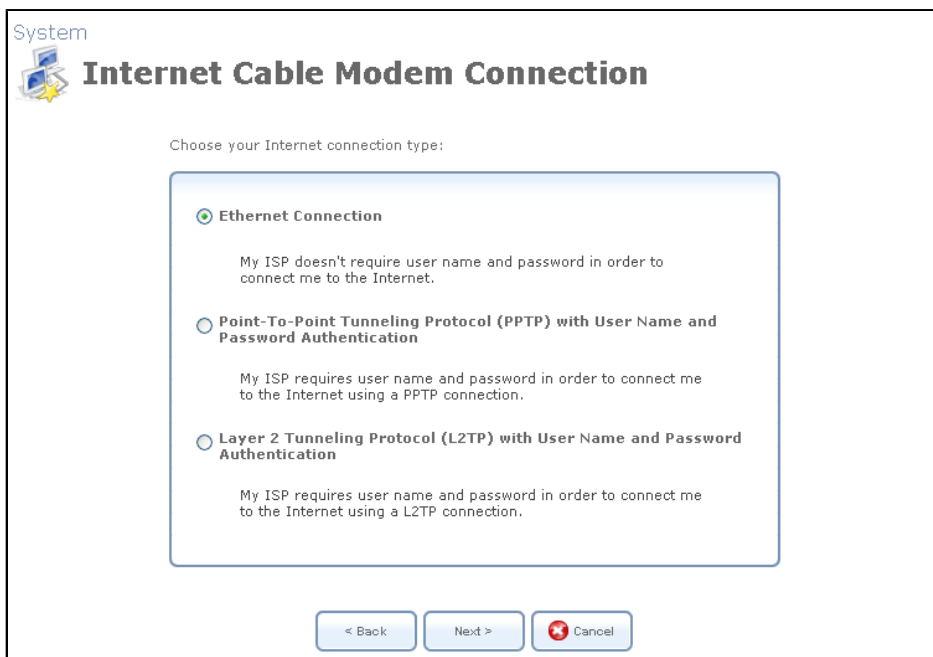


Figure 8.179. Internet Cable Modem Connection

4. Select the 'Point-To-Point Tunneling Protocol (PPTP) with User Name and Password Authentication' radio button and click Next. The 'Point-to-Point Tunneling Protocol (PPTP)' screen appears.

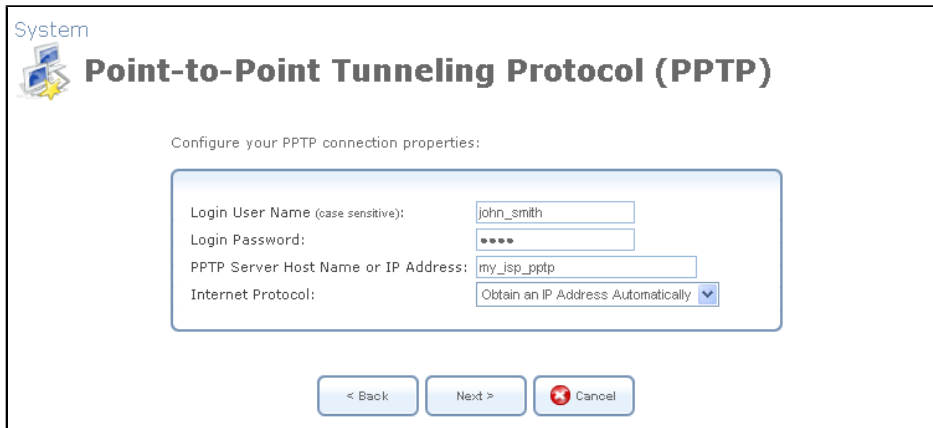


Figure 8.180. Point-to-Point Tunneling Protocol

5. Enter the username and password provided by your Internet Service Provider (ISP).
6. Enter the PPTP server host name or IP address provided by your ISP.
7. Select whether to obtain an IP address automatically or specify one. This option is described in great detail in **Internet Protocol** of this chapter.
8. Click 'Next'. The 'Connection Summary' screen appears.



Figure 8.181. Connection Summary

9. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.
10. Click Finish to save the settings.

The new PPTP connection is added to the network connections list, and is configurable like any other connection.

8.4.13.2. Creating a PPTP VPN connection with the Connection Wizard

To create a new PPTP VPN connection, perform the following steps:

1. Click the 'New Connection' link in the 'Network Connections' screen (see [Figure 8.12](#)). The 'Connection Wizard' screen appears (see [Figure 8.13](#)).
2. Select the 'Connect to a Virtual Private Network over the Internet' radio button and click 'Next'. The 'Connect to a Virtual Private Network over the Internet' screen appears (see figure 'Connect to a Virtual Private Network over the Internet').
3. Select the 'VPN Client or Point-To-Point' radio button and click Next. The 'VPN Client or Point-To-Point' screen appears.

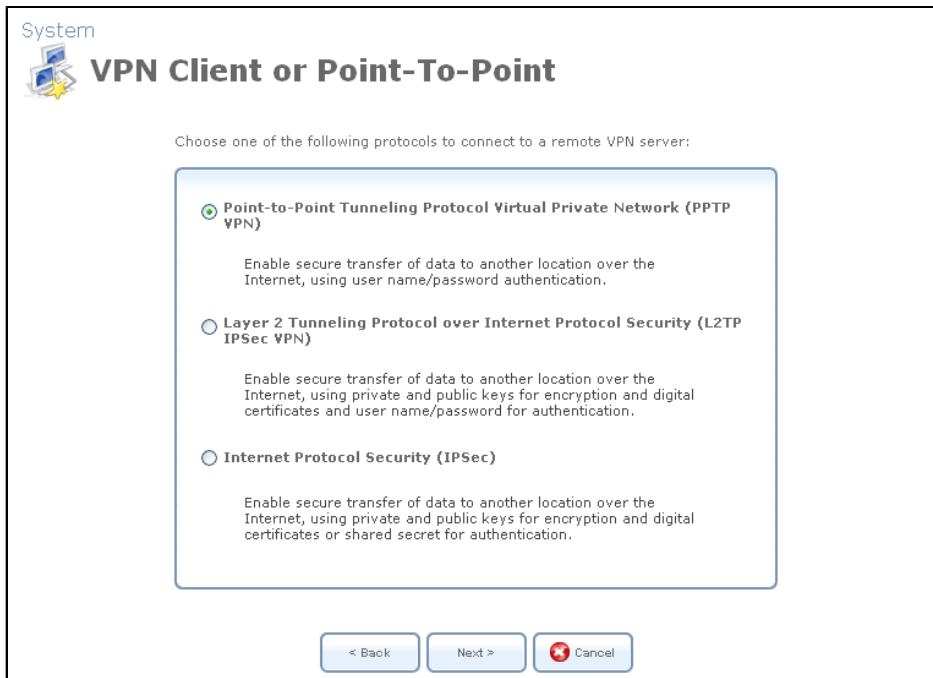


Figure 8.182. VPN Client or Point-To-Point

4. Select the 'Point-to-Point Tunneling Protocol Virtual Private Network (PPTP VPN)' radio button and click Next. The 'Point-to-Point Tunneling Protocol Virtual Private Network (PPTP VPN)' screen appears.

Figure 8.183. Point-to-Point Tunneling Protocol Virtual Private Network (PPTP VPN)

5. Enter the username and password provided by the administrator of the network you are trying to access.
6. Enter the remote tunnel endpoint address. This would be the IP address or domain name of the remote network computer, which serves as the tunnel's endpoint.
7. Click 'Next'. The 'Connection Summary' screen appear.

Figure 8.184. Connection Summary

8. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.
9. Click 'Finish' to save the settings.

The new PPTP VPN connection is added to the network connections list, and is configurable like any other connection.

8.4.13.3. General

To view and edit the PPTP connection settings, click the 'PPTP' link in the 'Network Connections' screen (see [Figure 8.12](#)). The 'PPTP Properties' screen appears (see [Figure 8.185](#)), 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 8.185. PPTP Properties

8.4.13.4. Settings

General This section displays the connection's general parameters.



Figure 8.186. General PPTP Settings

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, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to [Section 8.9.3](#).

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to [Section 8.4.2](#).

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' drop-down menu:

- Obtain an IP Address Automatically
- Use the Following IP Address

Note that the screen refreshes to display relevant configuration settings according to your choice.

Obtain an IP Address Automatically Your connection is configured by default to obtain an IP automatically. You should change this configuration in case your service provider requires it. 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.

The screenshot shows the 'Internet Protocol' section. A dropdown menu is set to 'Obtain an IP Address Automatically'. Below it, there is a checkbox labeled 'Override Subnet Mask:' which is unchecked. To the right of the checkbox are four input fields for the subnet mask, each containing the number '0'.

Figure 8.187. Internet Protocol – Automatic IP

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.

The screenshot shows the 'Internet Protocol' section. A dropdown menu is set to 'Use the Following IP Address'. Below it, there are two rows of input fields. The first row is labeled 'IP Address:' and contains four fields with the values '192', '168', '1', and '1'. The second row is labeled 'Subnet Mask:' and contains four fields with the values '255', '255', '255', and '0'.

Figure 8.188. Internet Protocol – Static IP

DNS Server Domain Name System (DNS) 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. To configure the connection to automatically obtain a DNS server address, select 'Obtain DNS Server Address Automatically' from the 'DNS Server' drop down menu.

The screenshot shows the 'DNS Server' section. A dropdown menu is set to 'Obtain DNS Server Address Automatically'.

Figure 8.189. DNS Server – Automatic IP

To manually configure DNS server addresses, select 'Use the Following DNS Server Addresses' from the 'DNS Server' drop down menu (see figure 'DNS Server -- Static IP'). Specify up to two different DNS server address, one primary, another secondary.

The screenshot shows the 'DNS Server' section. A dropdown menu is set to 'Use the Following DNS Server Addresses'. Below it, there are two rows of input fields. The first row is labeled 'Primary DNS Server:' and contains four fields with the values '0', '0', '0', and '0'. The second row is labeled 'Secondary DNS Server:' and contains four fields with the values '0', '0', '0', and '0'.

Figure 8.190. DNS Server – Static IP

To learn more about this feature, refer to [Section 7.13.1](#).

8.4.13.5. 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.

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.

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'.

Multicast – IGMP Proxy Internal / Default OpenRG serves as an IGMP proxy, issuing IGMP host messages on behalf of its LAN hosts. This check box is enabled on LAN connections by default, meaning that if a LAN multicast server is available, other LAN hosts asking to join multicast groups (by sending IGMP requests) will be able to join its multicast group. However, this check box is disabled on the WAN connection by default, meaning that LAN hosts will not be able to join multicast groups of WAN multicast servers. When creating a WAN-LAN bridge, this check box must also be deselected.

IGMP Query Version OpenRG supports all three versions of IGMP. Select the version you would like to use. Note that this drop-down menu appears for LAN connections only.

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.

Routing Mode: Route ▾

Device Metric:

Default Route

Multicast - IGMP Proxy Internal

IGMP Query Version: IGMPv3 ▾

Routing Information Protocol (RIP)

Routing Table

Name	Destination	Gateway	Netmask	Metric	Status	Action
LAN Bridge	192.168.2.4	192.168.1.1	255.255.255.255	2	Applied	✖
New Route						+

Figure 8.191. Advanced Routing Properties

To learn more about this feature, refer to [Section 8.6.1](#).

8.4.13.6. PPP

PPP Point-to-Point Protocol (PPP) is the most popular method for transporting packets between the user and the Internet service provider. PPP supports authentication protocols such as PAP and CHAP, as well as other compression and encryption protocols.

PPP-on-Demand Use PPP on demand to initiate the point-to-point protocol session only when packets are actually sent over the Internet.

Time Between Reconnect Attempts Specify the duration between PPP reconnected attempts, as provided by your ISP.

PPP

On Demand (will attempt to connect only when packets are sent)

Time Between Reconnect Attempts: Seconds

Figure 8.192. PPP Configuration

PPP Authentication Point-to-Point Protocol (PPP) currently supports four authentication protocols: Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and Microsoft CHAP version 1 and 2. This section allows you to select the authentication protocols your gateway may use when negotiating with a PPTP server. Select all the protocols if no information is available about the server's authentication protocols. Note that encryption is performed only if 'Microsoft CHAP', 'Microsoft CHAP version 2', or both are selected.

PPP Authentication

Login User Name (case sensitive):

Login Password:

Support Unencrypted Password (PAP)

Support Challenge Handshake Authentication (CHAP)

Support Microsoft CHAP (MS-CHAP)

Support Microsoft CHAP Version 2 (MS-CHAP v2)

Figure 8.193. PPP Authentication

Login User Name As agreed with ISP.

Login Password As agreed with ISP.

Support Unencrypted Password (PAP) Password Authentication Protocol (PAP) is a simple, plain-text authentication scheme. The user name and password are requested by your networking peer in plain-text. PAP, however, is not a secure authentication protocol. Man-in-the-middle attacks can easily determine the remote access client's password. PAP offers no protection against replay attacks, remote client impersonation, or remote server impersonation.

Support Challenge Handshake Authentication (CHAP) The Challenge Handshake Authentication Protocol (CHAP) is a challenge-response authentication protocol that uses MD5 to hash the response to a challenge. CHAP protects against replay attacks by using an arbitrary challenge string per authentication attempt.

Support Microsoft CHAP Select this check box if you are communicating with a peer that uses Microsoft CHAP authentication protocol.

Support Microsoft CHAP Version 2 Select this check box if you are communicating with a peer that uses Microsoft CHAP Version 2 authentication protocol.

PPP Encryption PPP supports encryption facilities to secure the data across the network connection. A wide variety of encryption methods may be negotiated, although typically only one method is used in each direction of the link. This section allows you to select the encryption methods your gateway may use when negotiating with a PPTP server. Select all the methods if no information is available about the server's encryption methods. Please note that PPP encryption can only be used with MS-CHAP or MS-CHAP-V2 authentication protocols.

PPP Encryption

Require Encryption (Disconnect If Server Declines)

Support Encryption (40 Bit Keys)

Support Maximum Strength Encryption (128 Bit Keys)

Figure 8.194. PPP Encryption

Require Encryption Select this check box to ensure that the PPP connection is encrypted.

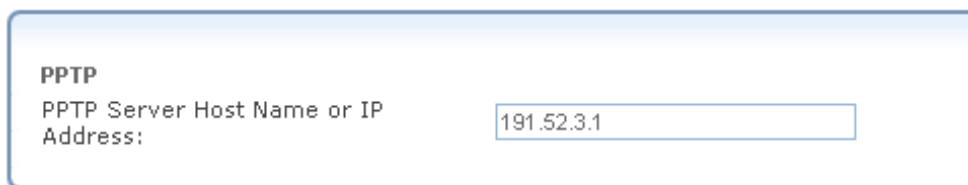
Support Encryption (40 Bit Keys) Select this check box if your peer supports 40 bit encryption keys.

Support Maximum Strength Encryption (128 Bit Keys) Select this check box if your peer supports 128 bit encryption keys.

8.4.13.7. PPTP

PPTP Define your ISP's server parameters.

PPTP Server Host Name or IP Address Enter the connection's host name or IP address obtained from your ISP.

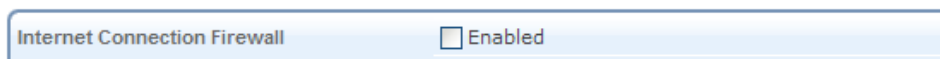


The image shows a configuration window titled "PPTP". Inside the window, there is a label "PPTP Server Host Name or IP Address:" followed by a text input field containing the IP address "191.52.3.1".

Figure 8.195. PPTP Configuration

8.4.13.8. 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. To learn more about your gateway's security features, refer to [Section 7.3](#).



The image shows a control element for "Internet Connection Firewall" with an unchecked checkbox labeled "Enabled".

Figure 8.196. Internet Connection Firewall

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

OpenRG can act as a Point-to-Point Tunneling Protocol Server (PPTP Server), accepting PPTP client connection requests.

Creation with the Connection Wizard

To create a new PPTP Server, perform the following:

1. Click the 'New Connection' link in the 'Network Connections' screen (see [Figure 8.12](#)). The 'Connection Wizard' screen appears (see [Figure 8.13](#)).

2. Select the 'Connect to a Virtual Private Network over the Internet' radio button and click 'Next'. The 'Connect to a Virtual Private Network over the Internet' screen appears (see figure 'Connect to a Virtual Private Network over the Internet').
3. Select the 'VPN Server' radio button and click 'Next'. The 'VPN Server' screen appears.

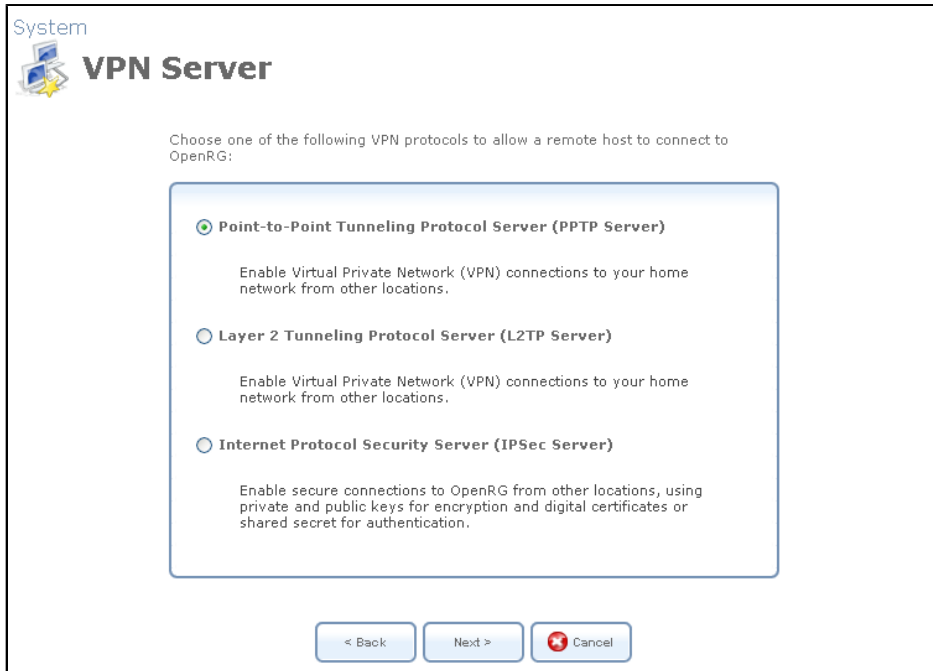


Figure 8.197. VPN Server

4. Select the 'Point-to-Point Tunneling Protocol Server (PPTP Server)' radio button and click 'Next'. The 'Point-to-Point Tunneling Protocol (PPTP)' screen appears.

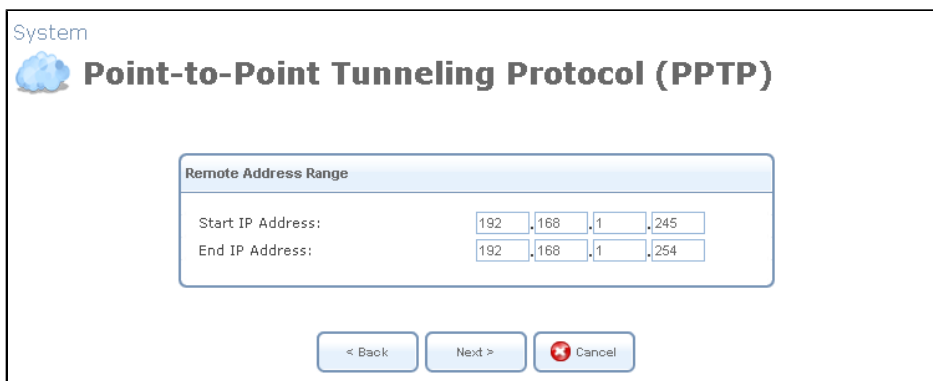


Figure 8.198. Point-to-Point Tunneling Protocol (PPTP)

5. Specify the address range that OpenRG will reserve for remote users. You may use the default values as depicted in [Figure 8.198](#).
6. Click 'Next'. The 'Connection Summary' screen appears (see [Figure 8.199](#)). Note the attention message alerting that there are no users with VPN permissions.

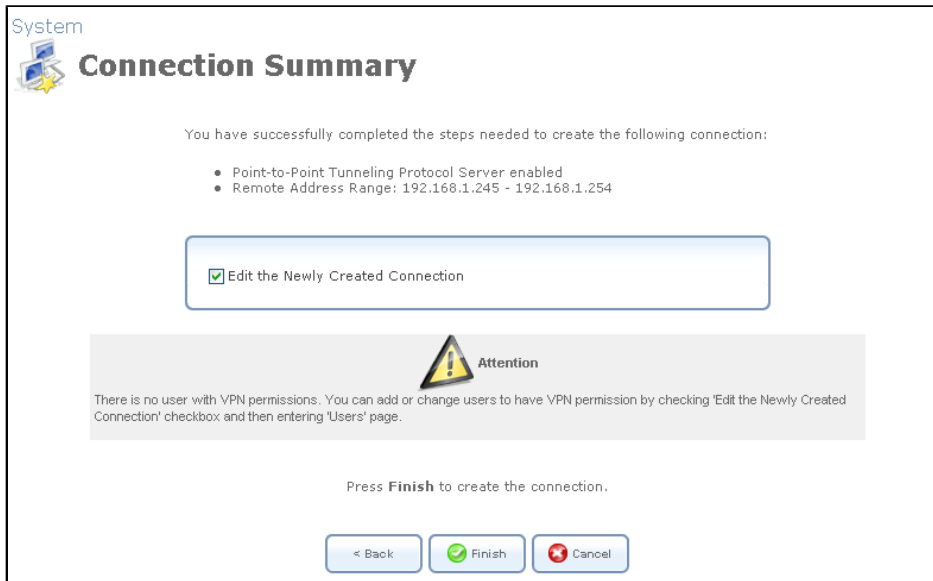


Figure 8.199. Connection Summary

7. Check the 'Edit the Newly Created Connection' check box and click 'Finish'. The 'Point-to-Point Tunneling Protocol Server (PPTP Server)' screen appears.

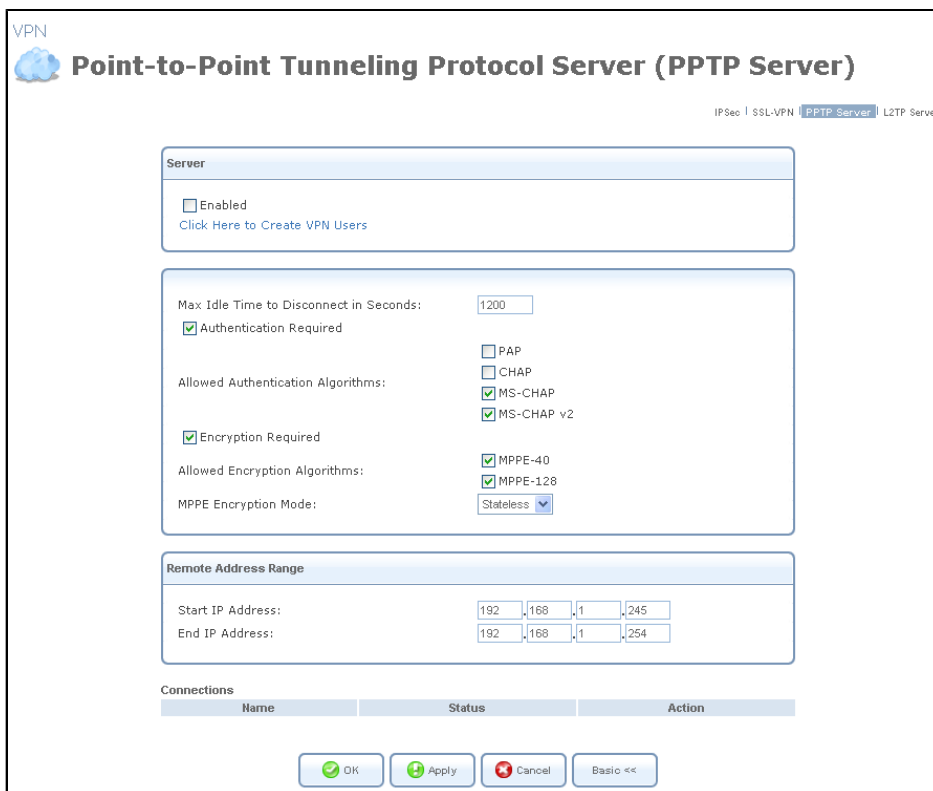


Figure 8.200. Advanced PPTP Server Parameters

8. Click the 'Click Here to Create VPN Users' link to define remote users that will be granted access to your home network. Refer to [Section 8.3](#) to learn how to define and configure users.

9. Click 'OK' to save the settings.

The new PPTP Server will be added to the network connections list, and will be configurable like any connection. Unlike other connections, it is also accessible via the OpenRG's 'Advanced' screen. To learn more about the configuration of a PPTP server, refer to [Section 7.10.3](#).

8.4.15. Internet Protocol Security (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.

Creation with the Connection Wizard

To create a new IPSec connection, perform the following:

1. Click the 'New Connection' link in the 'Network Connections' screen (see [Figure 8.12](#)). The 'Connection Wizard' screen appears (see [Figure 8.13](#)).
2. Select the 'Connect to a Virtual Private Network over the Internet' radio button and click 'Next'. The 'Connect to a Virtual Private Network over the Internet' screen appears (see figure 'Connect to a Virtual Private Network over the Internet').
3. Select the 'VPN Client or Point-To-Point' radio button and click 'Next'. The 'VPN Client or Point-To-Point' screen appears.

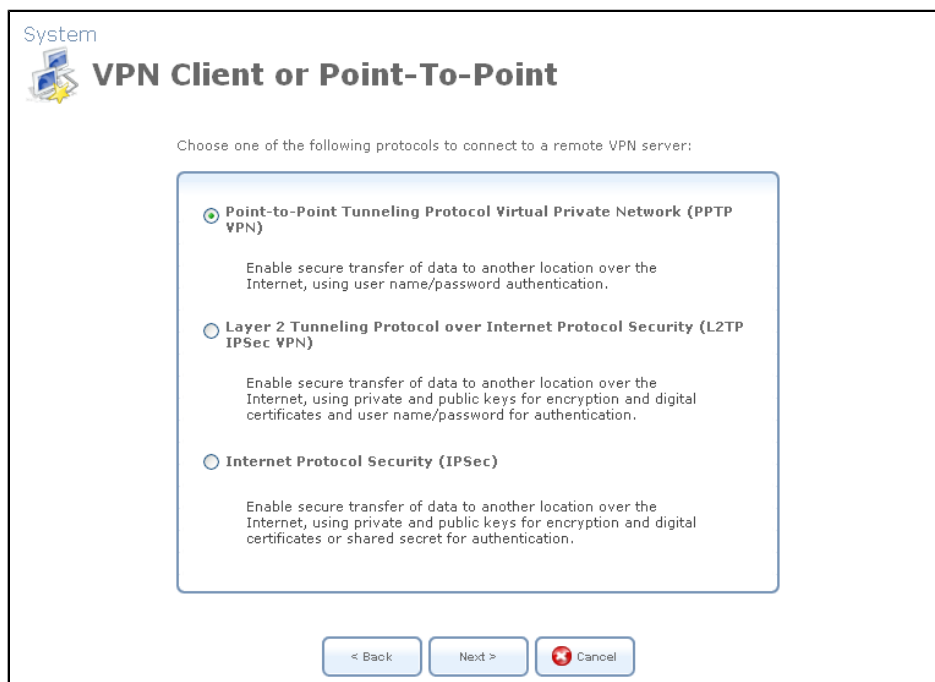


Figure 8.201. VPN Client or Point-To-Point

4. Select the 'Internet Protocol Security (IPSec)' radio button and click 'Next'. The 'Internet Protocol Security (IPSec)' screen appears.



System

Internet Protocol Security (IPSec)

Configure your IPSec connection properties:

Host Name or IP Address of Destination Gateway:

Remote IP:

Encapsulation Type:

Shared Secret:

< Back Next > Cancel

Figure 8.202. Internet Protocol Security (IPSec)

5. Enter the host or IP address of the destination gateway.
6. Select the method for specifying the remote IP address, which serves as the tunnel's endpoint. Use "Same as Gateway" when connecting your LAN to a remote *gateway*. When connecting your LAN to a remote *network* (a group of computers beyond a gateway), use one of the remaining three options. Also, use the *transport* encapsulation type in a gateway-to-gateway scenario only. Upon selection of an option, the screen will refresh providing you with the appropriate fields for entering the data.
 - a. **Same as Gateway** – the default option that uses the gateway IP entered above. When selecting this option, you must also select the encapsulation type, tunnel or transport, from its drop-down menu.
 - b. **IP Address** – a 'Remote IP Address' field appears. Specify the IP address.
 - c. **IP Subnet** – 'Remote Subnet IP Address' and 'Remote Subnet Mask' fields appear. Specify these parameters.
 - d. **IP Range** – 'From IP Address' and 'To IP Address' fields will appear. Specify the IP range.
7. Enter the IPSec shared secret, which is the encryption key jointly decided upon with the network you are trying to access.
8. Click 'Next'. The 'Connection Summary' screen appears.

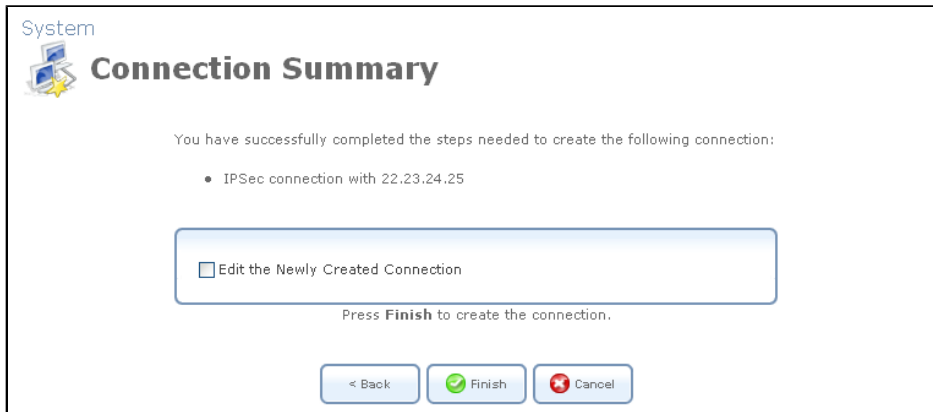


Figure 8.203. Connection Summary

9. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.
10. Click 'Finish' to save the settings.

The new IPSec connection will be added to the network connections list, and will be configurable like any connection. Unlike other connections, it is also accessible via the OpenRG's 'Advanced' screen. To learn more about the configuration of an IPSec connection, refer to [Section 7.10.1](#).

8.4.16. Internet Protocol Security Server (IPSec Server)

Creation with the Connection Wizard

To create a new IPSec Server, perform the following steps:

1. Click the 'New Connection' link in the 'Network Connections' screen (see [Figure 8.12](#)). The 'Connection Wizard' screen appears (see [Figure 8.13](#)).
2. Select the 'Connect to a Virtual Private Network over the Internet' radio button and click 'Next'. The 'Connect to a Virtual Private Network over the Internet' screen appears (see figure 'Connect to a Virtual Private Network over the Internet').
3. Select the 'VPN Server' radio button and click 'Next'. The 'VPN Server' screen appears.

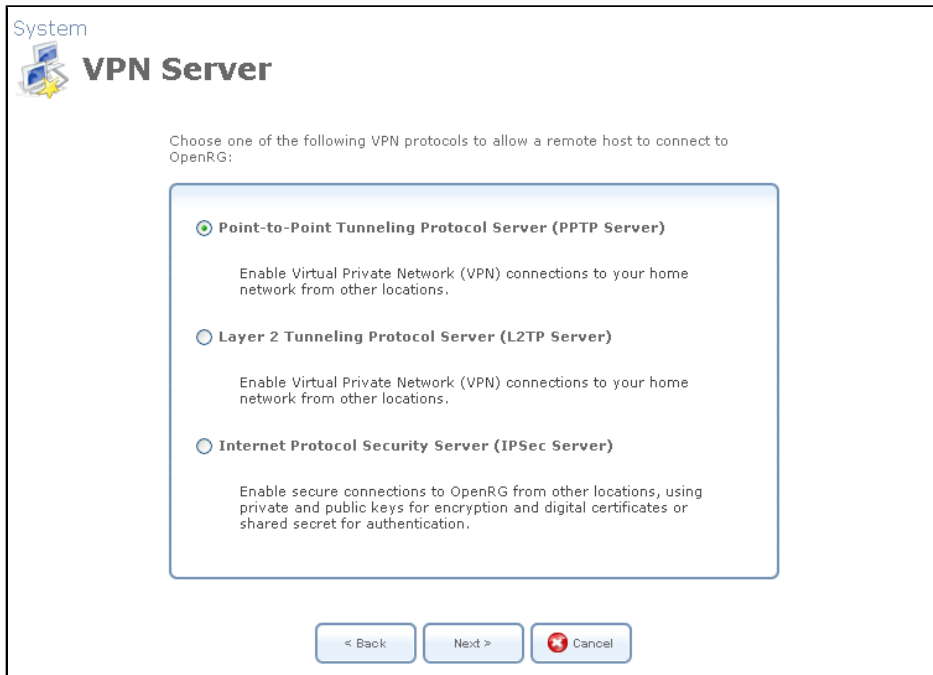


Figure 8.204. VPN Server

4. Select the 'Internet Protocol Security Server (IPSec Server)' radio button and click 'Next'. The 'Internet Protocol Security Server (IPSec Server)' screen appears.



Figure 8.205. Internet Protocol Security Server (IPSec Server)

5. Enter the IPSec shared secret, which is the encryption key jointly decided upon with the network you are trying to access.
6. Click 'Next'. The 'Connection Summary' screen appears.



Figure 8.206. Connection Summary

7. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.

8. Click 'Finish' to save the settings.

The new IPSec Server will be added to the network connections list, and will be configurable like any other connection. To learn more about the configuration of an IPSec server, refer to [Section 7.10.1](#).

8.4.17. Dynamic Host Configuration Protocol (DHCP)

The Dynamic Host Configuration Protocol (DHCP) connection wizard utility is one of the three methods used to configure the physical WAN Ethernet connection, described in [Section 8.4.8](#). It is a dynamic negotiation method, where the client obtains an IP address automatically from the service provider when connecting to the Internet.

To configure a new DHCP connection, perform the following:

1. Click the 'New Connection' link in the 'Network Connections' screen (see [Figure 8.12](#)). The 'Connection Wizard' screen appears (see [Figure 8.13](#)).
2. Select the 'Internet Connection' radio button and click 'Next'. The 'Internet Connection' screen appears (see [Figure 8.14](#)).
3. Select the 'Ethernet Connection' radio button and click 'Next'. The 'Ethernet Connection' screen appears.

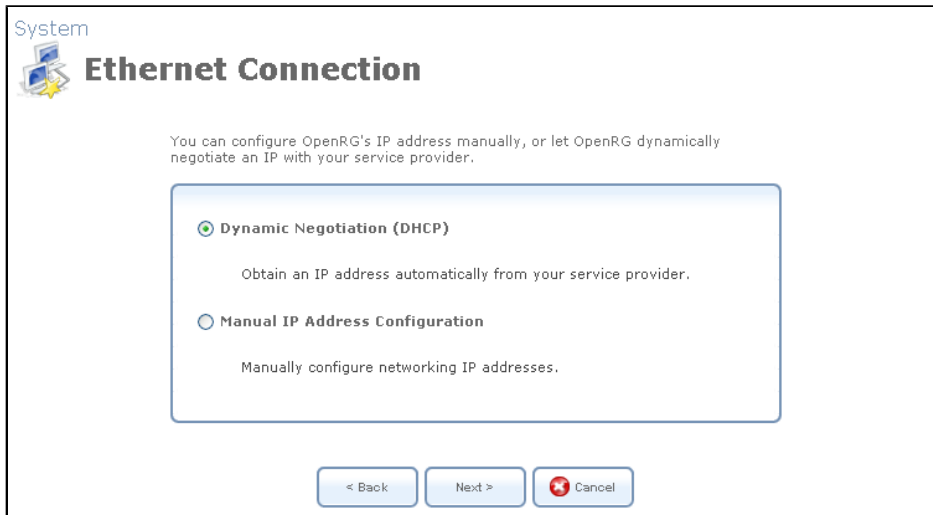


Figure 8.207. Ethernet Connection

4. Select the 'Dynamic Negotiation (DHCP)' radio button and click 'Next'. The 'Connection Summary' screen appears.

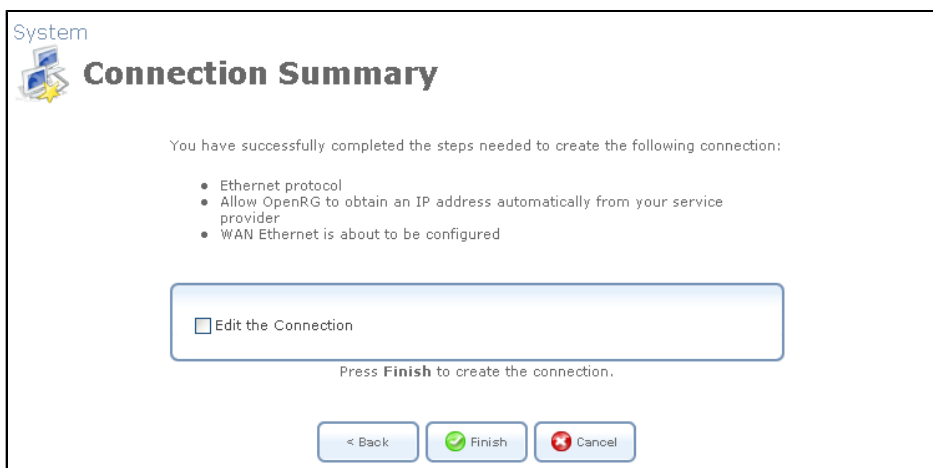



Figure 8.208. Connection Summary

5. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.
6. Click 'Finish' to save the settings.

The WAN Ethernet connection will be configured to obtain an IP address using a DHCP. Refer to [Section 8.4.8](#) to learn how to view and edit the connection's settings.

 Note: If your WAN connection is set to DHCP when there is no DHCP server available, and a PPPoE server is available instead, the device status will show: "Waiting for DHCP Lease – PPPoE server found, consider configuring your WAN connection to PPPoE". If you select this option, refer to [Section 8.4.9](#).

8.4.18. Manual IP Address Configuration

The Manual IP Address Configuration connection wizard utility is one of the three methods used to configure the physical WAN Ethernet connection, described in [Section 8.4.8](#). It is used to manually configure the networking IP addresses when connecting to the Internet.

To manually configure the IP addresses, perform the following:

1. Click the 'New Connection' link in the 'Network Connections' screen (see [Figure 8.12](#)). The 'Connection Wizard' screen appears (see [Figure 8.13](#)).
2. Select the 'Internet Connection' radio button and click 'Next'. The 'Internet Connection' screen appears (see [Figure 8.14](#)).
3. Select the 'Ethernet Connection' radio button and click 'Next'. The 'Ethernet Connection' screen appears.

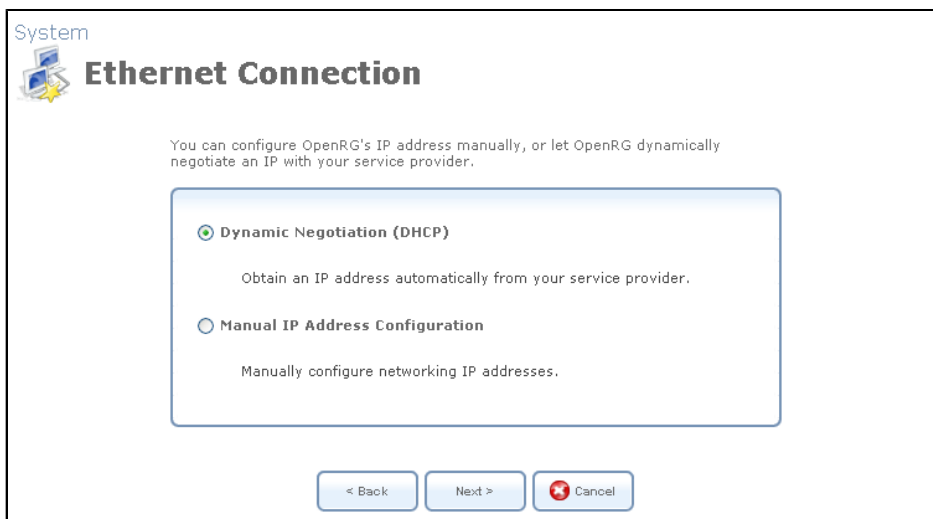


Figure 8.209. Ethernet Connection

4. Select the 'Manual IP Address Configuration' radio button and click 'Next'. The 'Manual IP Address Configuration' screen appears.

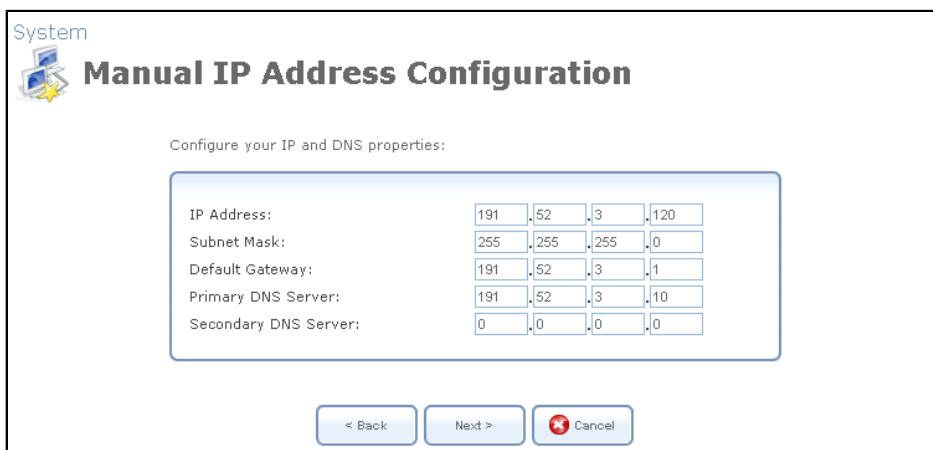


Figure 8.210. Manual IP Address Configuration

5. Enter the IP address, subnet mask, default gateway, and DNS server addresses in their respective fields. These values should either be provided to you by your ISP or configured by your system administrator.
6. Click 'Next'. The 'Connection Summary' screen appears.

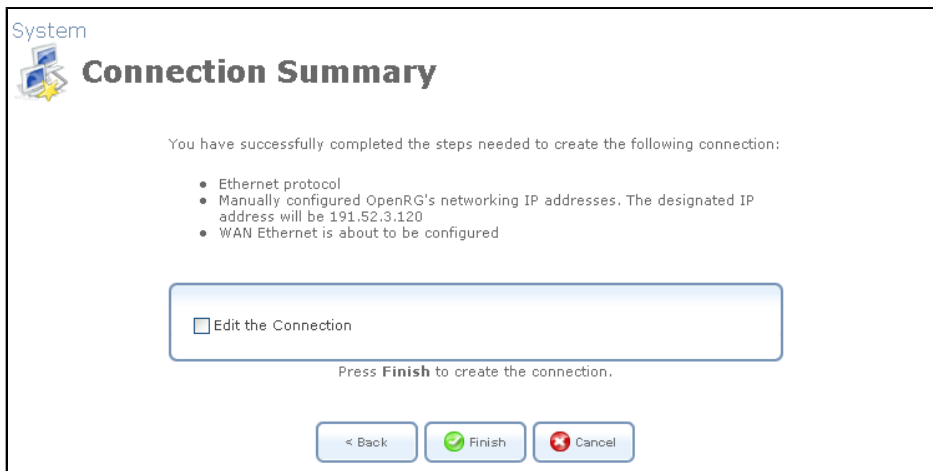


Figure 8.211. Connection Summary

7. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.
8. Click 'Finish' to save the settings.

The WAN Ethernet connection will be configured with the new settings. Refer to [Section 8.4.8](#) to learn how to view and edit the connection's settings.

8.4.19. Determine Protocol Type Automatically

The Determine Protocol Type Automatically (PVC Scan) connection wizard utility, available with the DSL gateway, allows you to automatically scan for a VPI/VCI pair, necessary when connecting with DSL. In case such a pair is not found, your service provider should supply you with one. To automatically scan for a VPI/VCI pair, perform the following:

1. Click the 'New Connection' link in the 'Network Connections' screen (see [Figure 8.12](#)). The 'Connection Wizard' screen appears (see [Figure 8.20](#)).
2. Select the 'Internet DSL Connection' radio button and click 'Next'. The 'Internet DSL Connection' screen appears (see [Figure 8.21](#)).
3. Select the 'Determine Protocol Type Automatically (PVC Scan)' radio button and click 'Next'. The scan will begin, refreshing the screen every few seconds to display the progress.

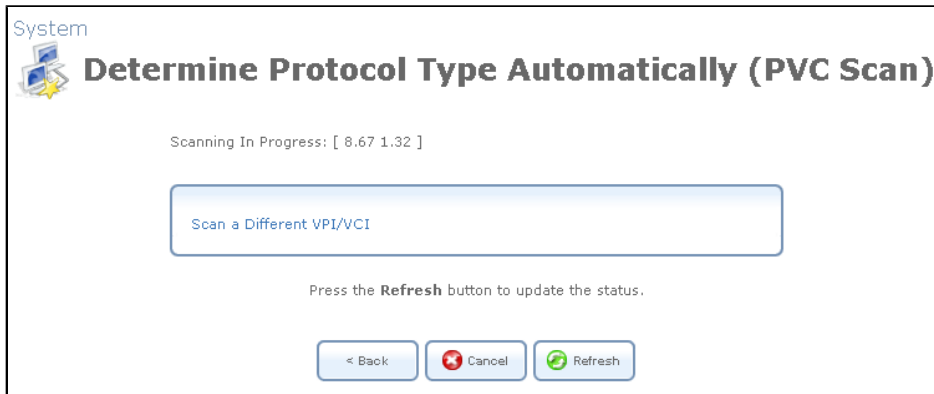
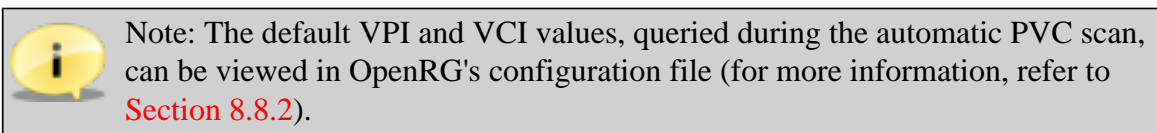


Figure 8.212. Determine Protocol Type Automatically (PVC Scan)

When the scan completes, a message indicating success or failure will be posted.



4. If the scan had failed, the screen will present the following options:

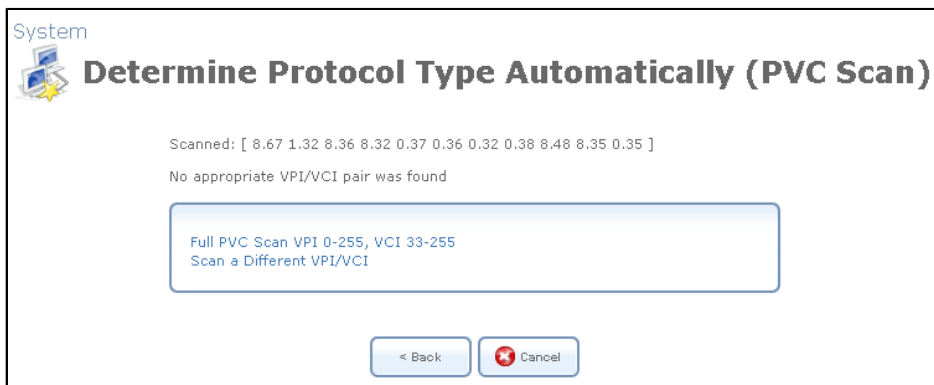


Figure 8.213. PVC Scan – No Pair was Found

- "Full PVC Scan VPI 0-255, VCI 33-255" – click this link to initiate a longer, more thorough scan, between VPI 0-255 and VCI 33-255.
- "Scan a Different VPI/VCI" – click this link to scan for specific VPI/VCI pair. The 'Scan User Defined VPI/VCI' screen appears (see [Figure 8.214](#)). Enter the VPI/VCI pair you wish to scan and click 'OK'.

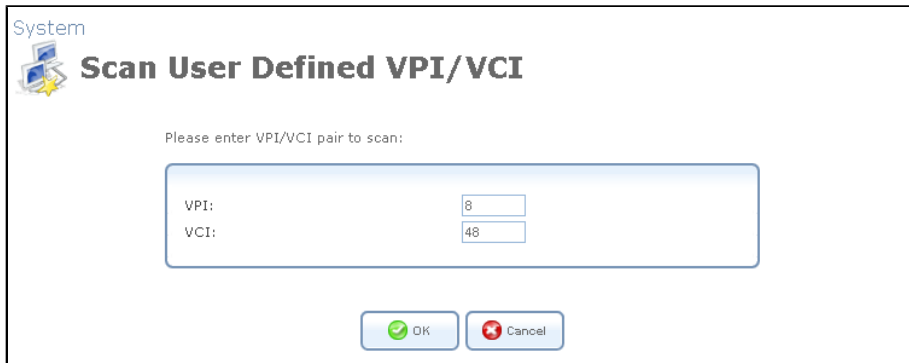


Figure 8.214. Scan User Defined VPI/VCI

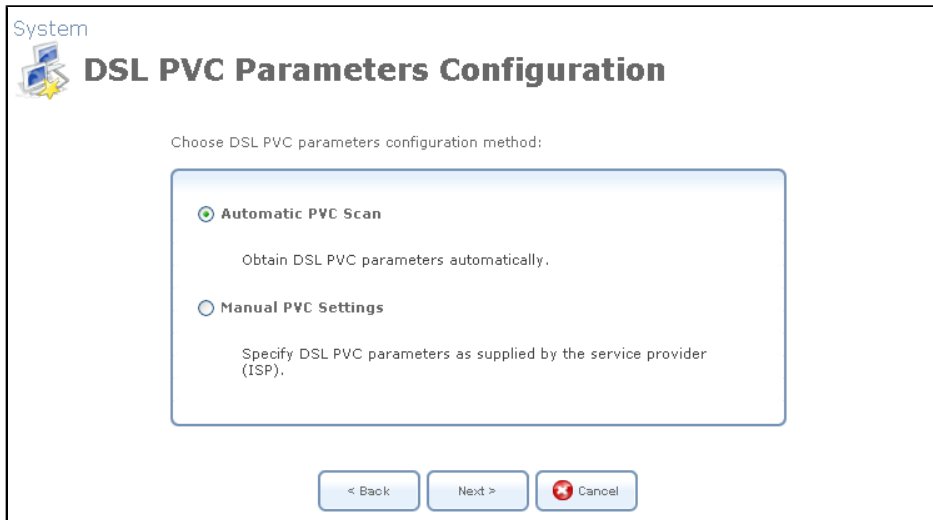
8.4.20. Point-to-Point Protocol over ATM (PPPoA)

Point-to-Point Protocol over ATM (PPPoA) is a standard for incorporating the popular PPP protocol into a DSL connection that uses ATM as its networking protocol. From the PC, IP packets travel over an Ethernet connection to the gateway, which encapsulates the PPP protocol to the IP packets and transports them to the service provider's DSLAM over ATM.

8.4.20.1. Creation with the Connection Wizard

To create a new PPPoA connection, perform the following:

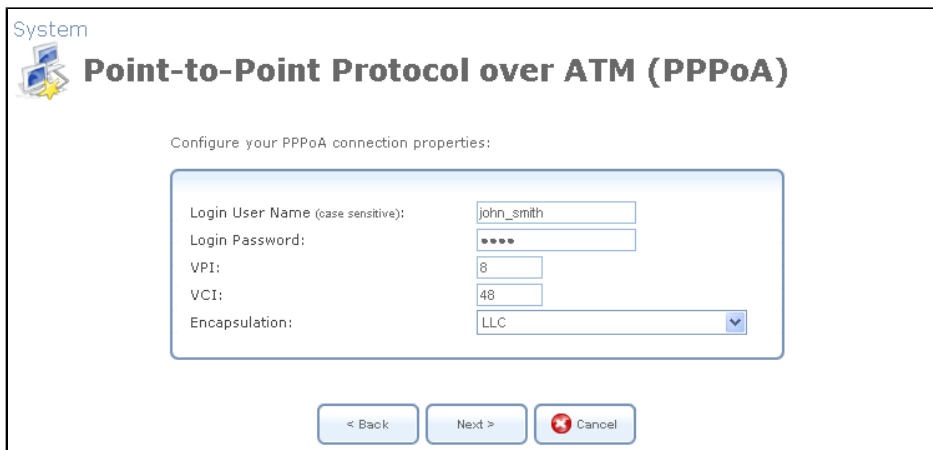
1. Click the 'New Connection' link in the 'Network Connections' screen (see [Figure 8.12](#)). The 'Connection Wizard' screen appears (see [Figure 8.20](#)).
2. Select the 'Internet DSL Connection' radio button and click 'Next'. The 'Internet DSL Connection' screen appears (see [Figure 8.21](#)).
3. Select the 'Point-to-Point Protocol over ATM (PPPoA)' radio button and click 'Next'. The 'DSL PVC Parameters Configuration' screen appears.



The screenshot shows a web interface titled 'DSL PVC Parameters Configuration'. At the top left, there is a 'System' logo and a small icon of a computer and a star. The main heading is 'DSL PVC Parameters Configuration'. Below the heading, the text reads 'Choose DSL PVC parameters configuration method:'. There are two radio button options: 'Automatic PVC Scan' (which is selected) and 'Manual PVC Settings'. Under 'Automatic PVC Scan', the text says 'Obtain DSL PVC parameters automatically.'. Under 'Manual PVC Settings', the text says 'Specify DSL PVC parameters as supplied by the service provider (ISP)'. At the bottom of the form, there are three buttons: '< Back', 'Next >', and 'Cancel'.


Figure 8.215. DSL PVC Parameters Configuration

4. If you wish to obtain the DSL PVC parameters automatically, check the 'Automatic PVC Scan' radio button and click 'Next'. Refer to [Section 8.4.19](#) for more information. Otherwise, check the 'Manual PVC Settings' radio button and click 'Next'. The 'Point-to-Point Protocol over ATM (PPPoA)' screen appears.



The screenshot shows a web interface titled 'Point-to-Point Protocol over ATM (PPPoA)'. At the top left, there is a 'System' logo and a small icon of a computer and a star. The main heading is 'Point-to-Point Protocol over ATM (PPPoA)'. Below the heading, the text reads 'Configure your PPPoA connection properties:'. There is a form with the following fields: 'Login User Name (case sensitive):' with the value 'john_smith', 'Login Password:' with four dots, 'VPI:' with the value '8', 'VCI:' with the value '48', and 'Encapsulation:' with a dropdown menu showing 'LLC'. At the bottom of the form, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Figure 8.216. Point-to-Point Protocol over ATM

 Note: The default VPI and VCI values, queried during the automatic PVC scan, can be viewed in OpenRG's configuration file (for more information, refer to [Section 8.8.2](#)).

5. Enter your username and password, which should be provided to you by your Internet Service Provider (ISP). If you chose a manual PVC scan in the previous step, you will be required to enter the following parameters as well:
 - The VPI and VCI pair of identifiers.
 - The encapsulation method: LLC, VCMux, or VCMux HDLC.
6. Click 'Next'. The 'Connection Summary' screen appears.

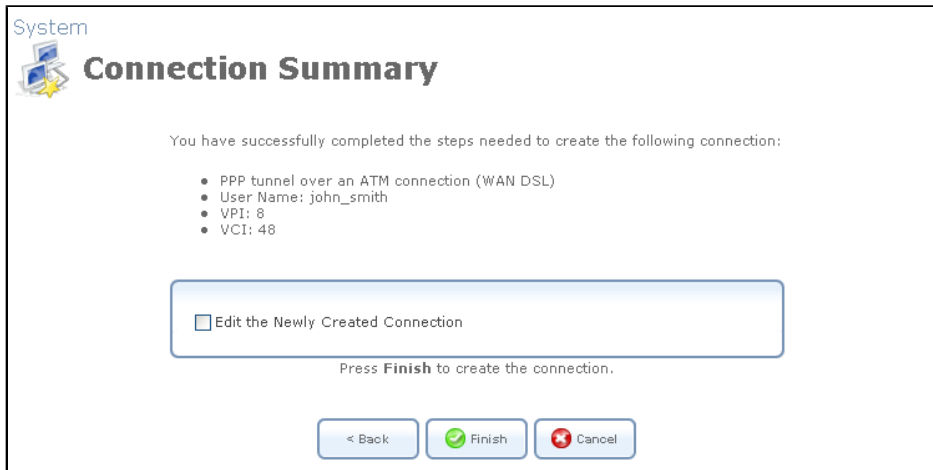


Figure 8.217. Connection Summary

7. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.
8. Click 'Finish' to save the settings.

The new PPPoA connection will be added to the network connections list, and will be configurable like any other connection.

8.4.20.2. General

To view and edit the PPPoA connection settings, click the 'WAN PPPoA' link in the 'Network Connections' screen (see [Figure 8.12](#)). The 'WAN PPPoA Properties' screen appears (see [Figure 8.218](#)), 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.

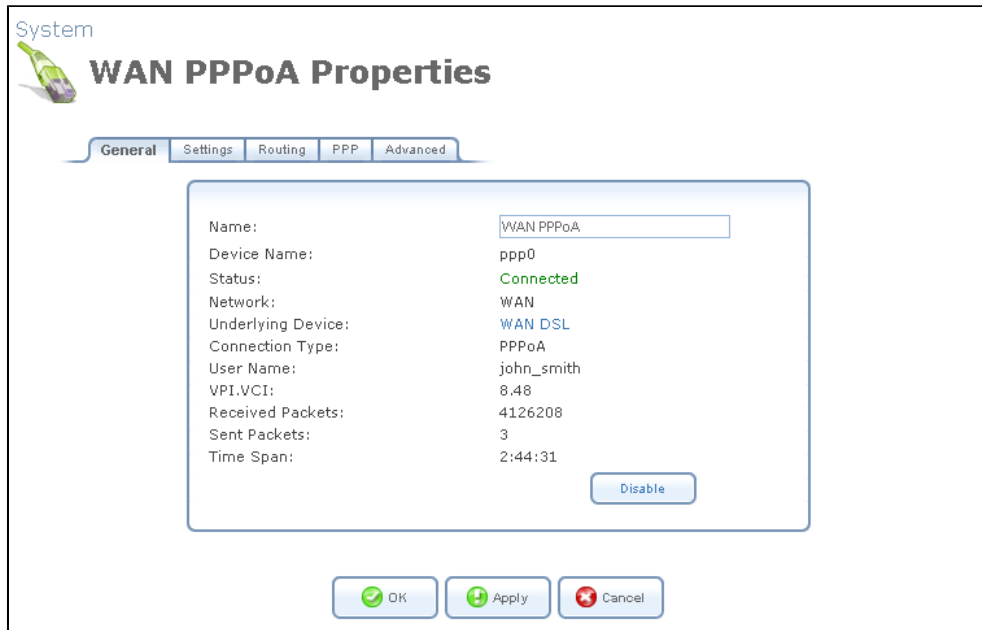


Figure 8.218. WAN PPPoA Properties

8.4.20.3. Settings

General This section displays the connection's general parameters.

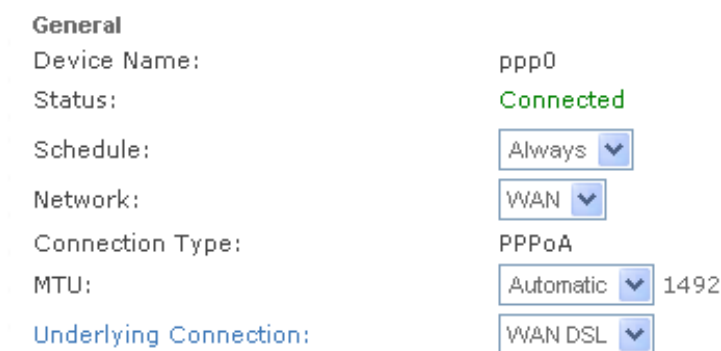


Figure 8.219. General PPPoA Settings

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, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to [Section 8.9.3](#).

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to [Section 8.4.2](#).

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.

Underlying Connection Specify the underlying connection above which the protocol will be initiated.

ATM

Asynchronous Transfer Mode (ATM) is a network technology based on transferring data in cells or packets of a fixed size. The cell used with ATM is relatively small compared to units used with other technologies. The small, constant cell size allows the transmission of video, audio, and computer data, assuring that no single type of data consumes the connection. ATM addressing consists of two identifiers that identify the virtual path (VPI) and the virtual connection (VCI). A virtual path consists of multiple virtual channels to the same endpoint. The 'Encapsulation' for connection should be set to either 'LLC' or 'VCMux'. You should configure these parameters according to the information provided by your ISP.

ATM	<input type="checkbox"/> Automatic PVC Scan
VPI:	<input type="text" value="8"/>
VCI:	<input type="text" value="48"/>
Encapsulation:	<input type="text" value="LLC"/>

Figure 8.220. ATM Settings

Internet Protocol Select one of the following Internet protocol options from the 'Internet Protocol' drop-down menu:

- Obtain an IP Address Automatically
- Use the Following IP Address

Note that the screen refreshes to display relevant configuration settings according to your choice.

Obtain an IP Address Automatically Your connection is configured by default to obtain an IP automatically. You should change this configuration in case your service provider requires it. 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.

Internet Protocol	<input type="text" value="Obtain an IP Address Automatically"/>
<input type="checkbox"/> Override Subnet Mask:	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>

Figure 8.221. Internet Protocol – Automatic IP

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.

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

Figure 8.222. Internet Protocol – Static IP

DNS Server Domain Name System (DNS) 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. To configure the connection to automatically obtain a DNS server address, select 'Obtain DNS Server Address Automatically' from the 'DNS Server' drop down menu.

DNS Server	Obtain DNS Server Address Automatically ▾
-------------------	---

Figure 8.223. DNS Server – Automatic IP

To manually configure DNS server addresses, select 'Use the Following DNS Server Addresses' from the 'DNS Server' drop down menu (see figure 'DNS Server -- Static IP'). Specify up to two different DNS server address, one primary, another secondary.

DNS Server	Use the Following DNS Server Addresses ▾
Primary DNS Server:	0 . 0 . 0 . 0
Secondary DNS Server:	0 . 0 . 0 . 0

Figure 8.224. DNS Server – Static IP

To learn more about this feature, refer to [Section 7.13.1](#).

8.4.20.4. 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.

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.

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'.

Multicast – IGMP Proxy Internal / Default OpenRG serves as an IGMP proxy, issuing IGMP host messages on behalf of its LAN hosts. This check box is enabled on LAN connections by default, meaning that if a LAN multicast server is available, other LAN hosts asking to join multicast groups (by sending IGMP requests) will be able to join its multicast group. However, this check box is disabled on the WAN connection by default, meaning that LAN hosts will not be able to join multicast groups of WAN multicast servers. When creating a WAN-LAN bridge, this check box must also be deselected.

IGMP Query Version OpenRG supports all three versions of IGMP. Select the version you would like to use. Note that this drop-down menu appears for LAN connections only.

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.

Routing Mode:

Device Metric:

Default Route

Multicast - IGMP Proxy Internal

IGMP Query Version:

Routing Information Protocol (RIP)

Name	Destination	Gateway	Netmask	Metric	Status	Action
LAN Bridge	192.168.2.4	192.168.1.1	255.255.255.255	2	Applied	
New Route						

Figure 8.225. Advanced Routing Properties

To learn more about this feature, refer to [Section 8.6.1](#).

8.4.20.5. PPP

PPP Point-to-Point Protocol (PPP) is the most popular method for transporting packets between the user and the Internet service provider. PPP supports authentication protocols such as PAP and CHAP, as well as other compression and encryption protocols.

PPP-on-Demand Use PPP on demand to initiate the point-to-point protocol session only when packets are actually sent over the Internet.

Time Between Reconnect Attempts Specify the duration between PPP reconnected attempts, as provided by your ISP.

PPP

On Demand (will attempt to connect only when packets are sent)

Time Between Reconnect Attempts: Seconds

Figure 8.226. PPP Configuration

PPP Authentication Point-to-Point Protocol (PPP) currently supports four authentication protocols: Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and Microsoft CHAP version 1 and 2. This section allows you to select the authentication protocols your gateway may use when negotiating with a PPTP server. Select all the protocols if no information is available about the server's authentication protocols. Note that encryption is performed only if 'Microsoft CHAP', 'Microsoft CHAP version 2', or both are selected.

PPP Authentication

Login User Name (case sensitive):

Login Password:

- Support Unencrypted Password (PAP)
- Support Challenge Handshake Authentication (CHAP)
- Support Microsoft CHAP (MS-CHAP)
- Support Microsoft CHAP Version 2 (MS-CHAP v2)

Figure 8.227. PPP Authentication

Login User Name As agreed with ISP.

Login Password As agreed with ISP.

Support Unencrypted Password (PAP) Password Authentication Protocol (PAP) is a simple, plain-text authentication scheme. The user name and password are requested by your networking peer in plain-text. PAP, however, is not a secure authentication protocol. Man-in-the-middle attacks can easily determine the remote access client's password. PAP offers no protection against replay attacks, remote client impersonation, or remote server impersonation.

Support Challenge Handshake Authentication (CHAP) The Challenge Handshake Authentication Protocol (CHAP) is a challenge-response authentication protocol that uses MD5 to hash the response to a challenge. CHAP protects against replay attacks by using an arbitrary challenge string per authentication attempt.

Support Microsoft CHAP Select this check box if you are communicating with a peer that uses Microsoft CHAP authentication protocol.

Support Microsoft CHAP Version 2 Select this check box if you are communicating with a peer that uses Microsoft CHAP Version 2 authentication protocol.

PPP Encryption PPP supports encryption facilities to secure the data across the network connection. A wide variety of encryption methods may be negotiated, although typically only one method is used in each direction of the link. This section allows you to select the encryption methods your gateway may use when negotiating with a PPTP server. Select all the methods if no information is available about the server's encryption methods. Please note that PPP encryption can only be used with MS-CHAP or MS-CHAP-V2 authentication protocols.

PPP Encryption

- Require Encryption (Disconnect If Server Declines)
- Support Encryption (40 Bit Keys)
- Support Maximum Strength Encryption (128 Bit Keys)

Figure 8.228. PPP Encryption

Require Encryption Select this check box to ensure that the PPP connection is encrypted.

Support Encryption (40 Bit Keys) Select this check box if your peer supports 40 bit encryption keys.

Support Maximum Strength Encryption (128 Bit Keys) Select this check box if your peer supports 128 bit encryption keys.

PPP Compression The PPP Compression Control Protocol (CCP) is responsible for configuring, enabling, and disabling data compression algorithms on both ends of the point-to-point link. It is also used to signal a failure of the compression/ decompression mechanism in a reliable manner.

PPP Compression

BSD:

Deflate:

Figure 8.229. PPP Compression

For each compression algorithm, select one of the following from the drop down menu:

Reject Reject PPP connections with peers that use the compression algorithm.

Allow Allow PPP connections with peers that use the compression algorithm.

Require Ensure a connection with a peer is using the compression algorithm.

8.4.20.6. 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. To learn more about your gateway's security features, refer to [Section 7.3](#).

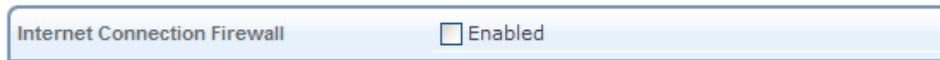


Figure 8.230. Internet Connection Firewall

8.4.21. Ethernet over ATM (ETHoA)

The Ethernet over ATM (ETHoA) connection allows transport of Ethernet frames on DSL connections.

8.4.21.1. Creation with the Connection Wizard

When creating an ETHoA connection via the 'Internet DSL Connection' section, it is bridged to the LAN. You must configure a dialup connection on the LAN computer with your ISP's user name and password. To create a new ETHoA connection, perform the following:

1. Click the 'New Connection' link in the 'Network Connections' screen (see [Figure 8.12](#)). The 'Connection Wizard' screen appears (see [Figure 8.20](#)).
2. Select the 'Internet DSL Connection' radio button and click 'Next'. The 'Internet DSL Connection' screen appears (see [Figure 8.21](#)).
3. Select the 'Ethernet Connection over ATM (ETHoA)' radio button and click 'Next'. The 'Ethernet Connection over ATM (ETHoA)' screen appears.

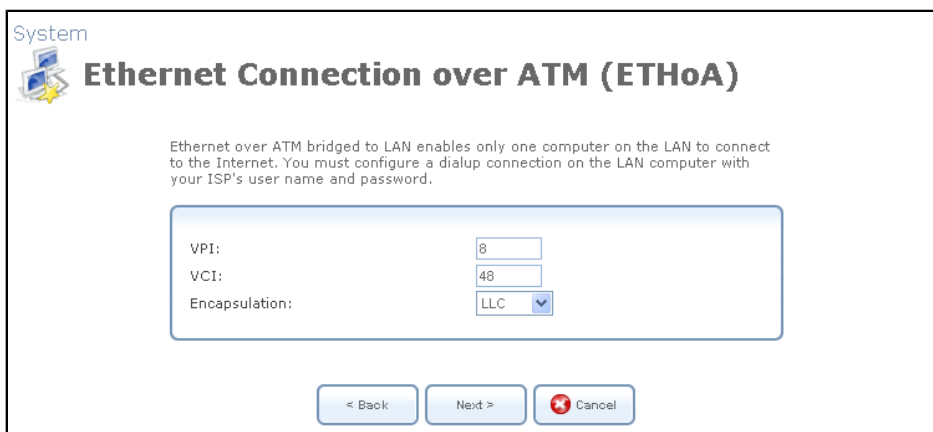


Figure 8.231. Ethernet Connection over ATM

4. Enter the following information, which should be provided to you by your Internet Service Provider (ISP):
 - The VPI and VCI pair of identifiers.
 - The encapsulation method: LLC or VCMux.

5. Click 'Next'. The 'Connection Summary' screen appears.

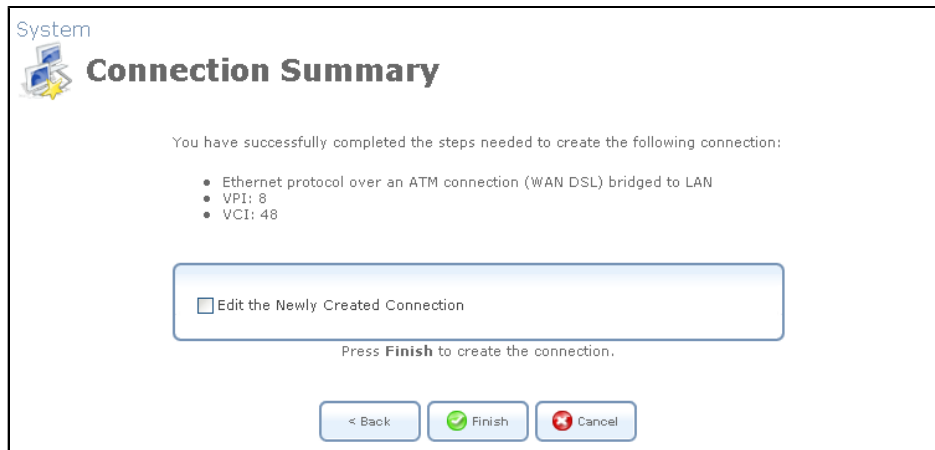


Figure 8.232. Connection Summary

6. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.
7. Click 'Finish' to save the settings.

The new ETHoA connection will be added to the network connections list, and will be configurable like any other connection.

8.4.21.2. General

To view and edit the ETHoA connection settings, click the 'WAN ETHoA' link in the 'Network Connections' screen (see [Figure 8.12](#)). The 'WAN ETHoA Properties' screen appears (see [Figure 8.233](#)), 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 8.233. WAN ETHoA Properties

8.4.21.3. Settings

General This section displays the connection's general parameters.

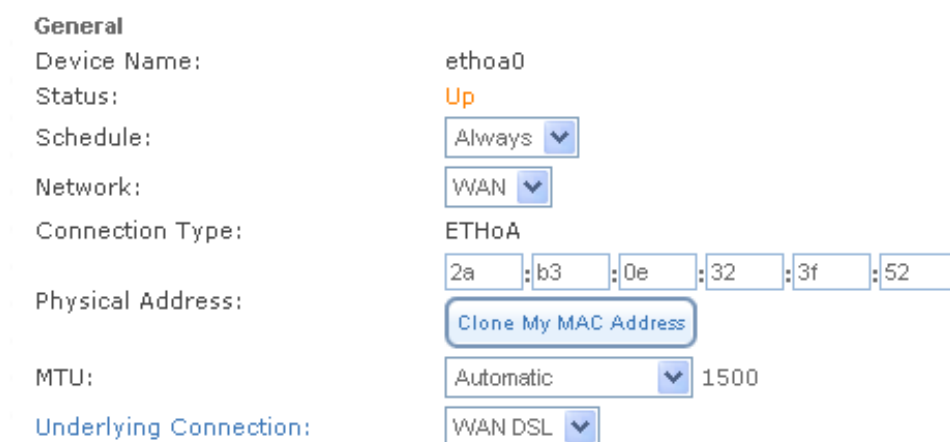


Figure 8.234. General ETHoA Settings

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, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to [Section 8.9.3](#).

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to [Section 8.4.2](#).

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

Clone My MAC Address Press this button to copy your PC's current MAC address to the board.

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.

Underlying Connection Specify the underlying connection above which the protocol will be initiated.

ATM

Asynchronous Transfer Mode (ATM) is a network technology based on transferring data in cells or packets of a fixed size. The cell used with ATM is relatively small compared to units used with other technologies. The small, constant cell size allows the transmission of video, audio, and computer data, assuring that no single type of data consumes the connection. ATM addressing consists of two identifiers that identify the virtual path (VPI) and the virtual connection (VCI). A virtual path consists of multiple virtual channels to the same endpoint. The 'Encapsulation' for connection should be set to either 'LLC' or 'VCMux'. You should configure these parameters according to the information provided by your ISP.

ATM	<input type="checkbox"/> Automatic PVC Scan
VPI:	<input type="text" value="8"/>
VCI:	<input type="text" value="48"/>
Encapsulation:	<input type="text" value="LLC"/>

Figure 8.235. ATM Settings

Internet Protocol Select one of the following Internet protocol options from the 'Internet Protocol' drop-down menu:

- No IP Address
- Obtain an IP Address Automatically
- Use the Following IP Address

Note that the screen will refresh to display relevant configuration settings according to your choice.

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.

Internet Protocol	<input type="text" value="No IP Address"/>
--------------------------	--

Figure 8.236. Internet Protocol – No IP Address

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 click 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.

The screenshot shows the 'Internet Protocol' settings. A dropdown menu is set to 'Obtain an IP Address Automatically'. Below it, there is a checkbox labeled 'Override Subnet Mask' which is unchecked. To the right of the checkbox are four input fields for the subnet mask, each containing the number '0'.

Figure 8.237. Internet Protocol Settings – Automatic IP

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.

The screenshot shows the 'Internet Protocol' settings. A dropdown menu is set to 'Use the Following IP Address'. Below it, there are two rows of input fields. The first row is labeled 'IP Address:' and contains four fields with the values '192', '168', '1', and '1'. The second row is labeled 'Subnet Mask:' and contains four fields with the values '255', '255', '255', and '0'.

Figure 8.238. Internet Protocol – Static IP

8.4.21.4. 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. To learn more about your gateway's security features, refer to [Section 7.3](#).

The screenshot shows a single control element for the 'Internet Connection Firewall'. It consists of a label 'Internet Connection Firewall' followed by a checkbox labeled 'Enabled', which is currently unchecked.

Figure 8.239. Internet Connection Firewall

- **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 and the <http://openrg.home>.

The screenshot shows a table titled 'Additional IP Addresses'. The table has three columns: 'IP Address', 'Subnet Mask', and 'Action'. Below the table header, there is a single row with the text 'New IP Address' in the 'IP Address' column and a green plus sign icon in the 'Action' column.

Figure 8.240. Additional IP Addresses

8.4.22. Classical IP over ATM (CLIP)

Classical IP (CLIP) is a standard for transmitting IP traffic in an ATM network. IP protocols contain IP addresses that have to be converted into ATM addresses, and Classical IP performs this conversion, as long as the destination is within the same subnet. Classical IP does not support routing between networks. The Classical IP-enabled driver in the end station sends out an ARP request to a Classical IP-enabled ARP server, which returns the ATM address.

8.4.22.1. Creation with the Connection Wizard

To create a new CLIP connection, perform the following steps:

1. Click the 'New Connection' link in the 'Network Connections' screen (see [Figure 8.12](#)). The 'Connection Wizard' screen appears (see [Figure 8.20](#)).
2. Select the 'Internet DSL Connection' radio button and click 'Next'. The 'Internet DSL Connection' screen appears (see [Figure 8.21](#)).
3. Select the 'Classical IP over ATM (CLIP)' radio button and click 'Next'. The 'Classical IP over ATM (CLIP)' screen appears.

IP Address:	210	150	3	12
Subnet Mask:	255	255	255	0
Default Gateway:	210	150	3	254
Primary DNS Server:	210	150	3	252
Secondary DNS Server:	0	0	0	0
VPI:	8			
VCI:	48			

Figure 8.241. Classical IP over ATM

4. Enter the following information, which should be provided to you by your Internet Service Provider (ISP):
 - IP Address
 - Subnet Mask
 - Default Gateway
 - Primary DNS Server
 - Secondary DNS Server

- The VPI and VCI pair of identifiers

5. Click Next. The 'Connection Summary' screen appears.

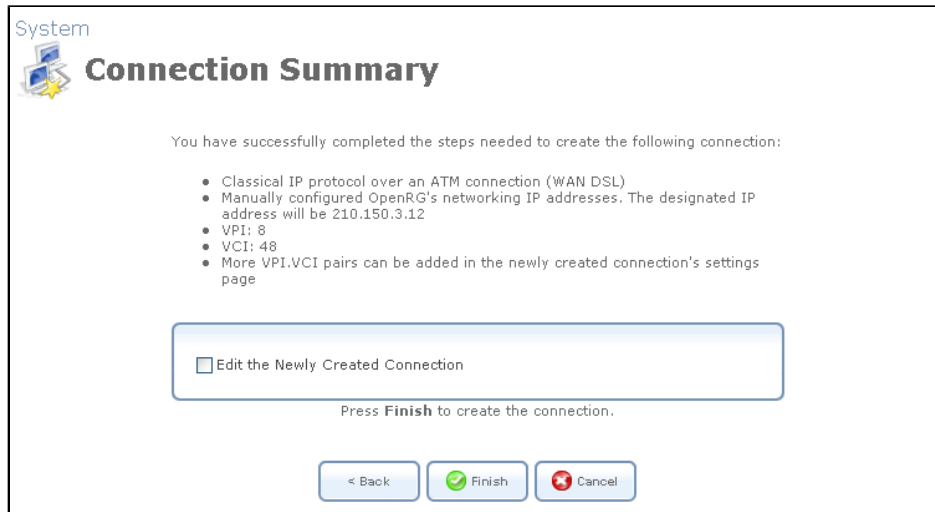


Figure 8.242. Connection Summary

6. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.

7. Click 'Finish' to save the settings.

The new CLIP connection will be added to the network connections list, and will be configurable like any other connection.

8.4.22.2. General

To view and edit the CLIP connection settings, click the 'WAN Classical IP over ATM' link in the 'Network Connections' screen (see [Figure 8.12](#)). The 'WAN Classical IP over ATM Properties' screen appears (see [Figure 8.243](#)), 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.

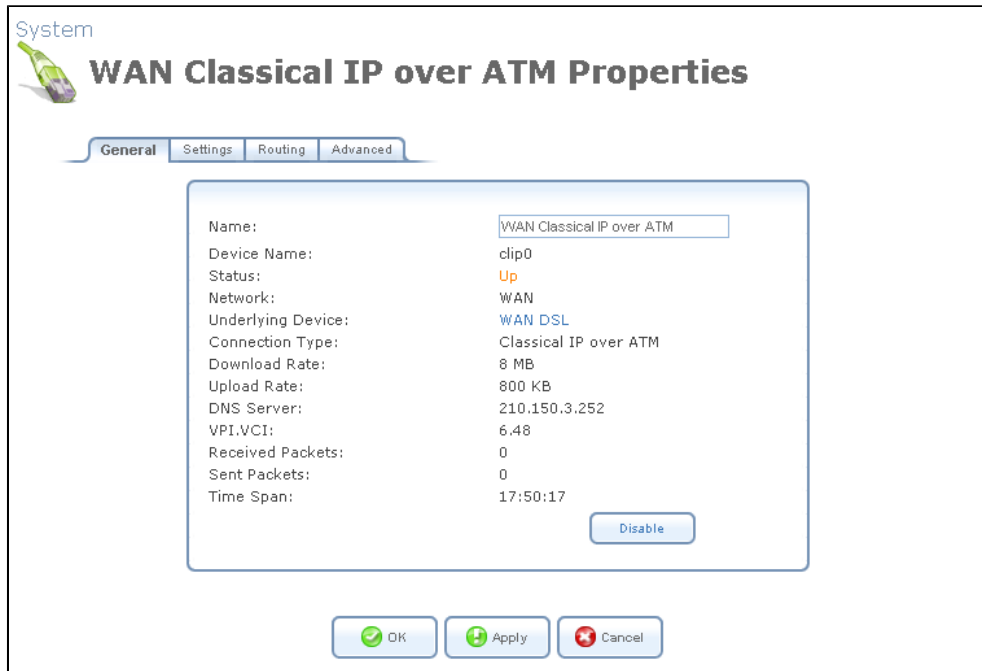


Figure 8.243. WAN Classical IP over ATM Properties

8.4.22.3. Settings

General This section displays the connection's general parameters.

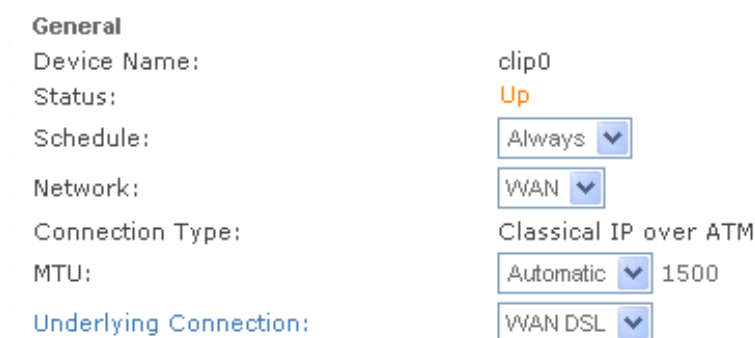


Figure 8.244. General CLIP Settings

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, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to [Section 8.9.3](#).

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to [Section 8.4.2](#).

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.

Underlying Connection Specify the underlying connection above which the protocol will be initiated.

VPI.VCI ATM addressing consists of two identifiers that identify the virtual path (VPI) and the virtual connection (VCI). A virtual path consists of multiple virtual channels to the same endpoint. The 'Encapsulation' for connection should be set to either 'LLC' or 'VCMux'. You should configure these parameters according to the information provided by your ISP.


VPI.VCI	Action
8.48	 
New VPI.VCI	

Figure 8.245. VPI.VCI

To change VPI/VCI connection parameters, perform the following:

1. Click the 'New VPI.VCI' link, the 'VPI.VCI Settings' screen appears (see [Figure 8.246](#)).
2. Specify the VPI and VCI pair of identifiers according to the information provided by your ISP.

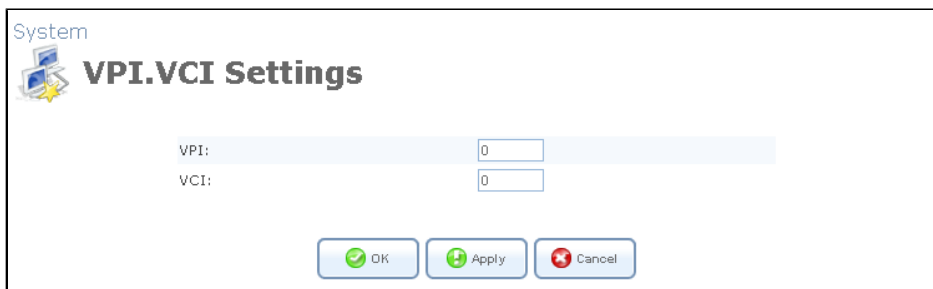


Figure 8.246. VPI.VCI Settings

3. Click 'OK' to save the settings.

Internet Protocol This connection always uses a specified IP address. Your service provider should provide you with this IP address, subnet mask, the default gateway and DNS server.


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

Figure 8.247. Internet Protocol Settings - Static IP

DNS Server Domain Name System (DNS) 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. To configure the connection to automatically obtain a DNS server address, select 'Obtain DNS Server Address Automatically' from the 'DNS Server' drop down menu.

DNS Server

Obtain DNS Server Address Automatically ▼

Figure 8.248. DNS Server – Automatic IP

To manually configure DNS server addresses, select 'Use the Following DNS Server Addresses' from the 'DNS Server' drop down menu (see figure 'DNS Server -- Static IP'). Specify up to two different DNS server address, one primary, another secondary.

DNS Server

Use the Following DNS Server Addresses ▼

Primary DNS Server:

0 . 0 . 0 . 0

Secondary DNS Server:

0 . 0 . 0 . 0

Figure 8.249. DNS Server – Static IP

To learn more about this feature, refer to [Section 7.13.1](#).

8.4.22.4. 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.

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.

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'.

Multicast – IGMP Proxy Internal / Default OpenRG serves as an IGMP proxy, issuing IGMP host messages on behalf of its LAN hosts. This check box is enabled on LAN connections by default, meaning that if a LAN multicast server is available, other LAN hosts asking to join multicast groups (by sending IGMP requests) will be able to join its multicast group. However, this check box is disabled on the WAN connection by default, meaning that

LAN hosts will not be able to join multicast groups of WAN multicast servers. When creating a WAN-LAN bridge, this check box must also be deselected.

IGMP Query Version OpenRG supports all three versions of IGMP. Select the version you would like to use. Note that this drop-down menu appears for LAN connections only.

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.

Routing Mode:

Device Metric:

Default Route

Multicast - IGMP Proxy Internal

IGMP Query Version:

Routing Information Protocol (RIP)

Routing Table

Name	Destination	Gateway	Netmask	Metric	Status	Action
LAN Bridge	192.168.2.4	192.168.1.1	255.255.255.255	2	Applied	
New Route						

Figure 8.250. Advanced Routing Properties

To learn more about this feature, refer to [Section 8.6.1](#).

8.4.22.5. 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. To learn more about your gateway's security features, refer to [Section 7.3](#).

Internet Connection Firewall Enabled

Figure 8.251. Internet Connection Firewall

8.4.23. WAN-LAN Bridge

A WAN-LAN bridge is a bridge over WAN and LAN devices. This way computers on the OpenRG LAN side can get IP addresses that are known on the WAN side.

8.4.23.1. Creation with the Connection Wizard

To configure an existing bridge or create a new one, perform the following:

1. In the 'Network Connections' screen under 'System' (see [Figure 8.12](#)), click the 'New Connection' link. The 'Connection Wizard' screen appears (see [Figure 8.13](#)).
2. Select the 'Advanced Connection' radio button and click 'Next'. The 'Advanced Connection' screen appears (see [Figure 8.18](#)).
3. Select the 'Network Bridging' radio button and click 'Next'. The 'Bridge Options' screen appears.

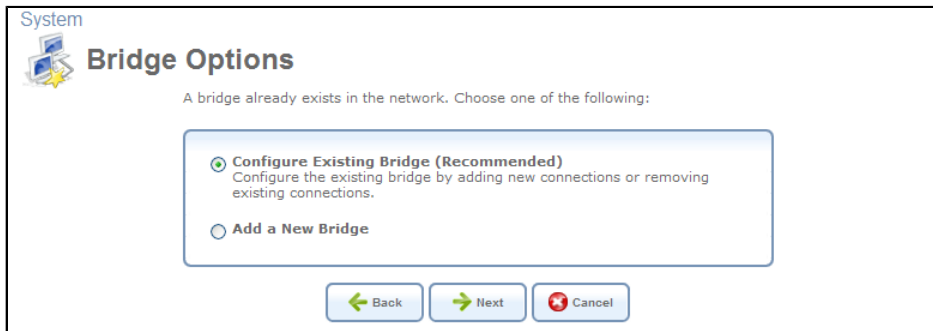


Figure 8.252. Bridge Options

4. Select whether to configure an existing bridge (this option will only appear if a bridge exists) or to add a new one:
 - a. **Configure Existing Bridge** Select this option and click 'Next'. The 'Network Bridging' screen appears allowing you to add new connections or remove existing ones, by selecting or deselecting their respective check boxes. For example, check the WAN check box to create a LAN-WAN bridge.

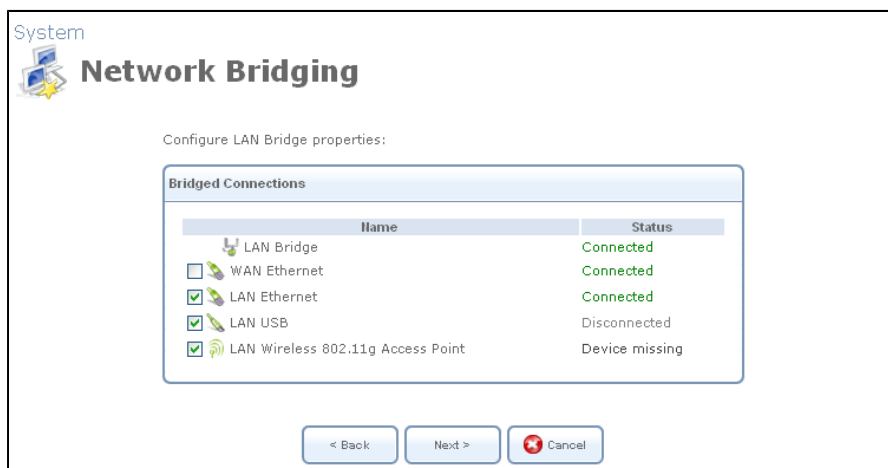


Figure 8.253. Network Bridging – Configure Existing Bridge

- b. **Add a New Bridge** Select this option and click 'Next'. A different 'Network Bridging' screen appears allowing you to add a bridge over the unbridged connections, by selecting their respective check boxes.

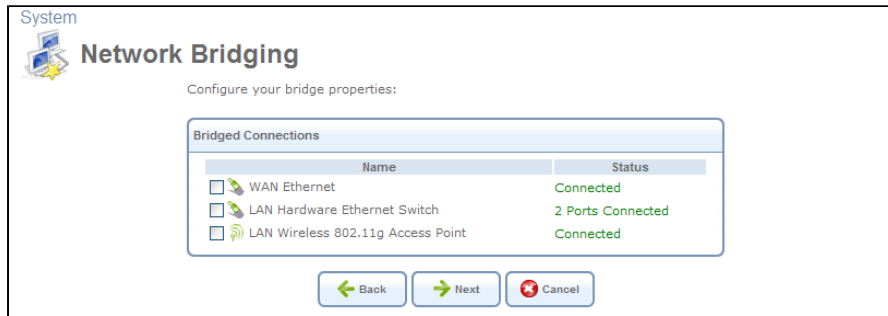


Figure 8.254. Network Bridging – Add a New Bridge

5. Click 'Next'. The 'Connection Summary' screen appears, corresponding to your changes.

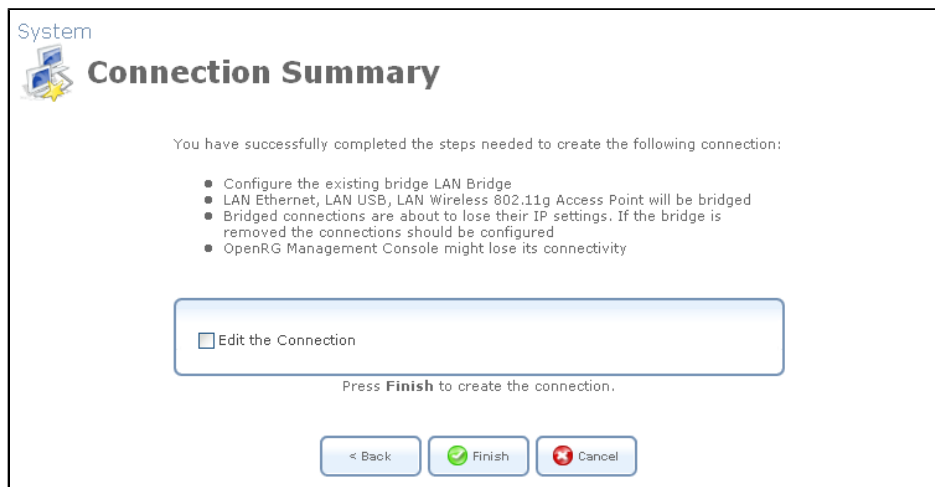


Figure 8.255. Connection Summary – Configure Existing Bridge

6. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.
7. Click 'Finish' to save the settings. The new bridge will be added to the network connections list, and it will be configurable like any other bridge.



Note: Creating a WAN-LAN bridge disables OpenRG's DHCP server. This means that LAN hosts may only receive an IP address from a DHCP server on the WAN. If you configure a host with a static IP address from an alias subnet of the bridge (192.168.1.X), you will be able to access OpenRG but not the WAN, as NAT is not performed in the WAN-LAN bridge mode.

After creating a WAN-LAN bridge, you must also disable the IGMP Proxy on this connection. To do so, perform the following:

1. In the 'Network Connections' screen under 'System', click the 'LAN Bridge' link. The 'LAN Bridge Properties' screen appears.

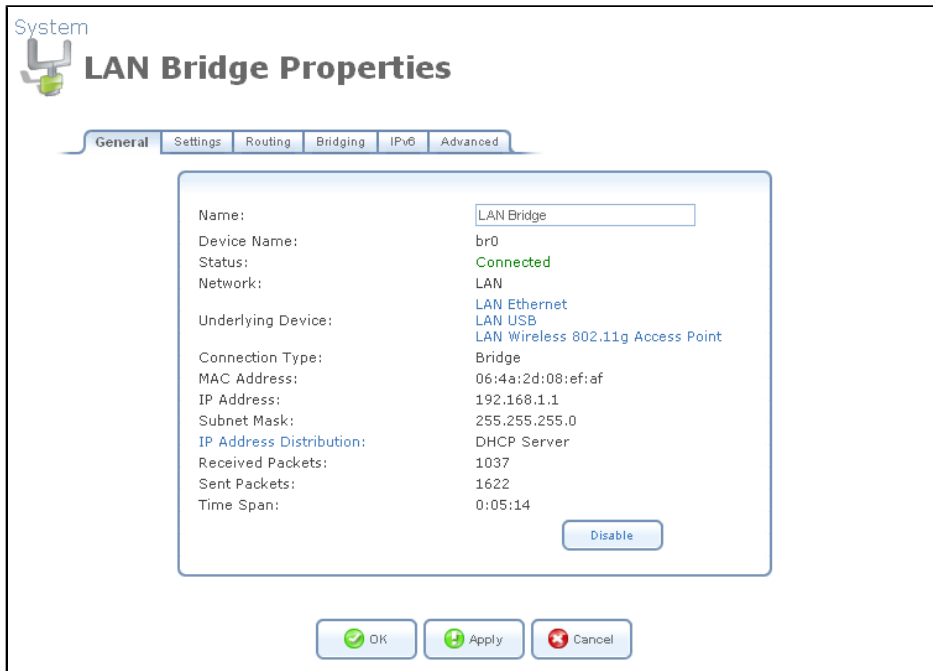


Figure 8.256. LAN Bridge Properties

2. Select the 'Routing' sub-tab, and disable the 'Multicast - IGMP Proxy Default' option (to learn more about this option, refer to [Section 8.4.23.5](#)).
3. Click 'OK' to save the settings.

8.4.23.2. Setting up a Hybrid Bridging Mode

OpenRG enables you to bridge certain bandwidth-consuming and traffic-sensitive LAN hosts, such as IPTV Set Top Boxes, directly to the WAN. Such a network connection scheme does not interfere with OpenRG's routing mode, in which all traffic usually passes through the NAT, and is checked by the firewall. These two modes can work simultaneously, if you have two bridges under OpenRG's LAN network device:

LAN bridge Receives its IP address from OpenRG's DHCP server. The traffic passing through the LAN on its way to the WAN is inspected by OpenRG's firewall, and assigned a public address by the NAT.

WAN-LAN bridge Receives its IP address from the WAN DHCP server, thereby enabling direct communication with the WAN.

OpenRG based on Linux 2.6 supports direct communication between devices placed under the two bridges. For example, if you connect your IPTV Set Top Box with a Personal Video Recorder (PVR) to OpenRG's WAN-LAN bridge, you will be able to access the content recorded on the PVR from any home computer connected to OpenRG's LAN.

This network configuration is called *Hybrid Bridging*. OpenRG detects LAN hosts that should be bridged to the WAN according to their MAC address or a specific DHCP option (either **Vendor Class ID**, **Client ID** or **User Class ID**). Once detected, these LAN hosts are placed

under the WAN-LAN bridge, which you must add and configure for the hybrid bridging mode beforehand.

To add the WAN-LAN bridge, follow the Connection Wizard steps described in [Section 8.4.23.1](#). In the final step, check the 'Edit the Newly Created Connection' check box, and click 'Finish'. The 'Bridge Properties' screen appears.

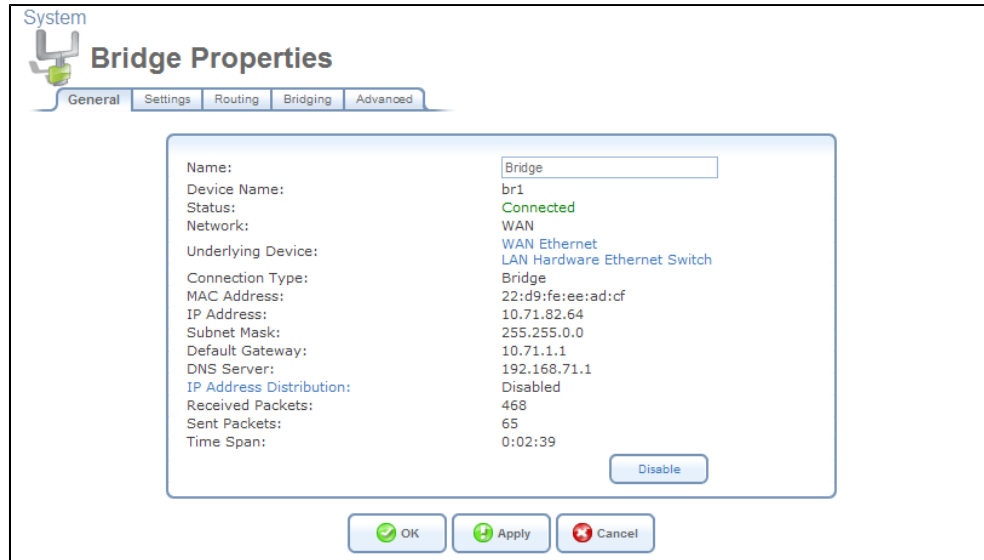


Figure 8.257. Bridge Properties

To configure the WAN-LAN bridge for the hybrid bridging mode, perform the following:

1. In the 'Bridge Properties' screen, click the 'Routing' tab. The following screen appears.

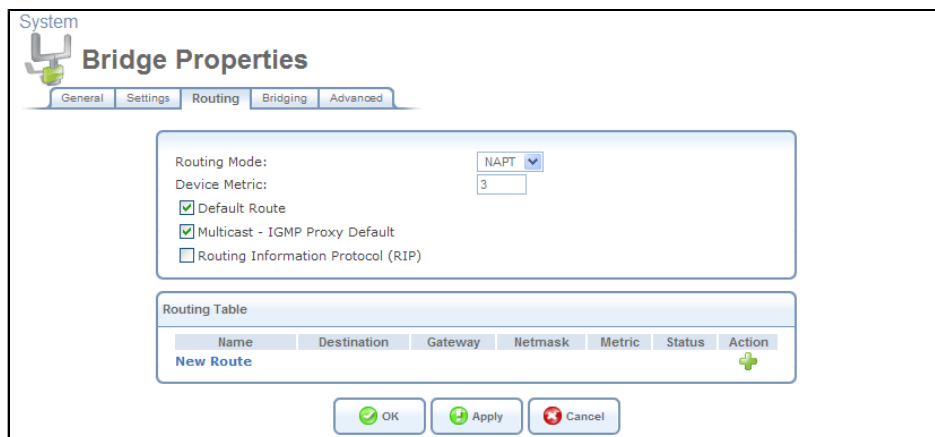


Figure 8.258. WAN-LAN Bridge Routing Settings

2. From the 'Routing Mode' drop-down menu, select 'Route' and click 'Apply'. The following warning screen appears.

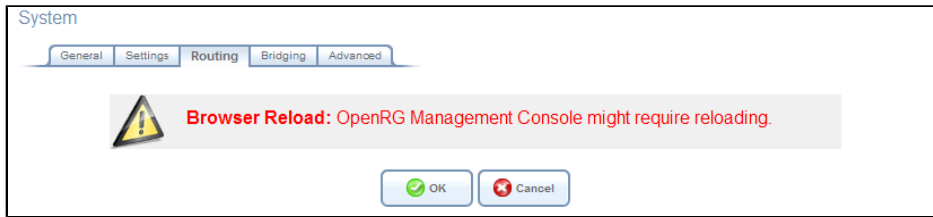


Figure 8.259. Browser Reload Warning Message

3. Click 'OK'. The page refreshes while saving the new settings, and returns to the previous screen.
4. Click the 'Bridging' tab. The following screen appears.

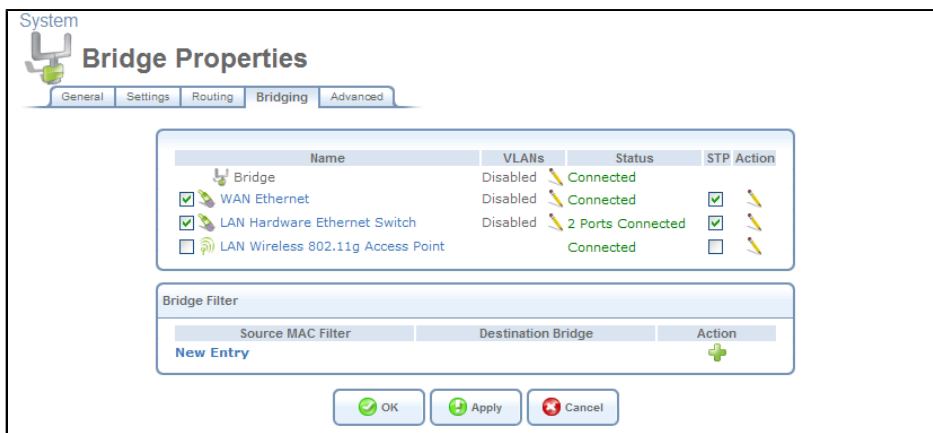


Figure 8.260. WAN-LAN Bridging Settings

5. In the 'Bridge Filter' section, click the 'New Entry' link. The following screen appears.

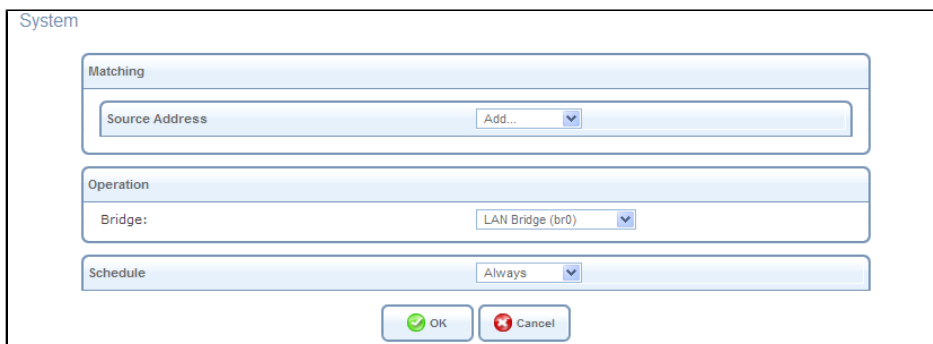


Figure 8.261. Bridge Filter Settings

6. From the drop-down menu in the 'Operation' section, select the WAN-LAN bridge. If not renamed, its default entry appears as "Bridge (br1)".
7. From the 'Source Address' drop-down menu, select 'User Defined'. The 'Edit Network Object' screen appears.

Figure 8.262. Edit Network Object

8. Click the 'New Entry' link. The 'Edit Item' screen appears.

Figure 8.263. Edit Item – MAC Address

This screen enables you to create a traffic filtering rule, which enables direct packet flow between the WAN and the LAN host that will be placed under the WAN-LAN bridge. This filtering rule can be based on either a LAN host's MAC address or one of its DHCP options mentioned earlier.

9. If you wish to base this rule on the MAC address, and enter the MAC address and the MAC mask in their respective fields. Otherwise, perform the following:
- From the 'Network Object Type' drop-down menu, select 'DHCP Option'. The screen refreshes, changing to the following.

Figure 8.264. Edit Item – DHCP Options

- From the designated drop-down menu, select one of the DHCP options. The field
 - Enter a relevant value for the DHCP option (should be supplied by a service provider).
10. Click 'OK' to save the settings.

8.4.23.3. General

To view and edit the WAN-LAN bridge connection settings, click the 'Bridge' link in the 'Network Connections' screen (see [Figure 8.12](#)). The 'Bridge Properties' screen appears (see [Figure 8.265](#)), 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.

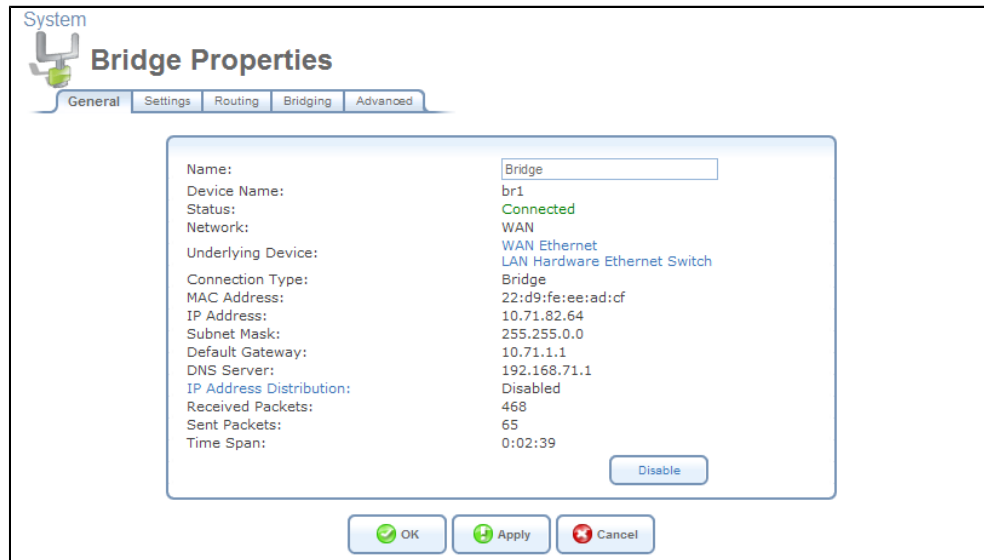


Figure 8.265. Bridge Properties

8.4.23.4. Settings

General This section displays the connection's general parameters.

General	
Device Name:	br0
Status:	Connected
Schedule:	Always ▾
Network:	LAN ▾
Connection Type:	Bridge
Physical Address:	06 : 4a : 2d : 08 : ef : af
MTU:	Automatic ▾ 1500

Figure 8.266. General Bridge Settings

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, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to [Section 8.9.3](#).

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to [Section 8.4.2](#).

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

Clone My MAC Address Press this button to copy your PC's current MAC address to the board.

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' drop-down menu:

- No IP Address
- Obtain an IP Address Automatically
- Use the Following IP Address

Note that the screen will refresh to display relevant configuration settings according to your choice.

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.

Internet Protocol ▼

Figure 8.267. Internet Protocol – No IP Address

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 click 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.

Internet Protocol ▼
 Override Subnet Mask:

Figure 8.268. Internet Protocol Settings – Automatic IP

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.

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

Figure 8.269. Internet Protocol – Static IP

DNS Server Domain Name System (DNS) 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. To configure the connection to automatically obtain a DNS server address, select 'Obtain DNS Server Address Automatically' from the 'DNS Server' drop down menu.

DNS Server	Obtain DNS Server Address Automatically ▾
-------------------	---

Figure 8.270. DNS Server – Automatic IP

To manually configure DNS server addresses, select 'Use the Following DNS Server Addresses' from the 'DNS Server' drop down menu (see figure 'DNS Server -- Static IP'). Specify up to two different DNS server address, one primary, another secondary.

DNS Server	Use the Following DNS Server Addresses ▾
Primary DNS Server:	0 . 0 . 0 . 0
Secondary DNS Server:	0 . 0 . 0 . 0

Figure 8.271. DNS Server – Static IP

To learn more about this feature, refer to [Section 7.13.1](#).

IP Address Distribution In general, the 'IP Address Distribution' section enables you to configure the DHCP server parameters. However, in the WAN-LAN bridge configuration, the DHCP server must be disabled.

8.4.23.5. 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.

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.

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'.

Multicast – IGMP Proxy Internal / Default OpenRG serves as an IGMP proxy, issuing IGMP host messages on behalf of its LAN hosts. This check box is enabled on LAN connections by default, meaning that if a LAN multicast server is available, other LAN hosts asking to join multicast groups (by sending IGMP requests) will be able to join its multicast group. However, this check box is disabled on the WAN connection by default, meaning that LAN hosts will not be able to join multicast groups of WAN multicast servers. When creating a WAN-LAN bridge, this check box must also be deselected.

IGMP Query Version OpenRG supports all three versions of IGMP. Select the version you would like to use. Note that this drop-down menu appears for LAN connections only.

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.

Routing Mode:

Device Metric:

Default Route

Multicast - IGMP Proxy Internal

IGMP Query Version:

Routing Information Protocol (RIP)

Routing Table

Name	Destination	Gateway	Netmask	Metric	Status	Action
LAN Bridge	192.168.2.4	192.168.1.1	255.255.255.255	2	Applied	
New Route						

Figure 8.272. Advanced Routing Properties

To learn more about this feature, refer to [Section 8.6.1](#).

8.4.23.6. Bridging

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



Note: If you would like to logically partition your Ethernet-based network, you can set up a VLAN bridge as described in [Section 8.4.24.7](#).

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.

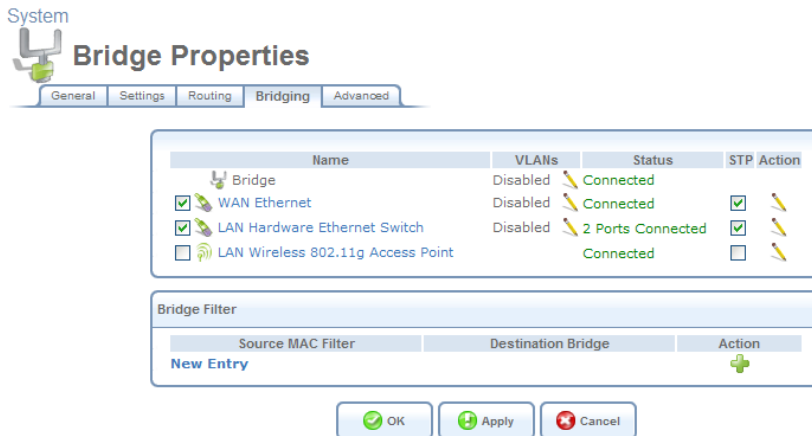


Figure 8.273. Bridge Settings

8.4.23.7. IPv6

Click on the 'New Unicast Address' link to add an IPv6 unicast address. To learn more about configuring IPv6 settings, refer to [Section 8.6.2](#).

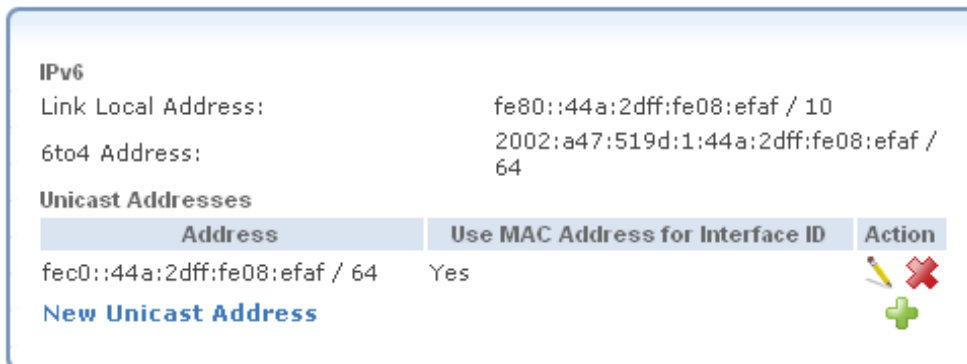


Figure 8.274. IPv6 Settings

8.4.23.8. 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. To learn more about your gateway's security features, refer to [Section 7.3](#).

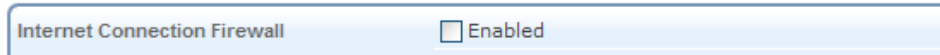


Figure 8.275. Internet Connection Firewall

- **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 and the <http://openrg.home>.

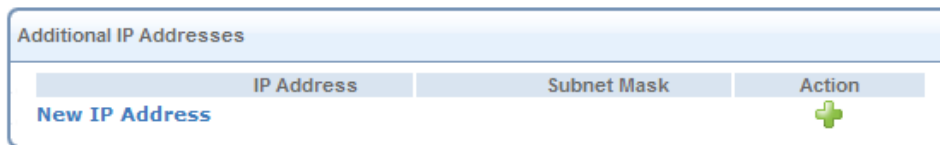


Figure 8.276. Additional IP Addresses

8.4.24. Virtual LAN Interface (VLAN)

A virtual LAN interface enables you to group workstations together into one broadcast domain, even if they are not located on the same LAN segment. OpenRG allows you to create virtual Ethernet-based networks according to the IEEE 802.1Q standard. If you would like your VLANs to communicate with the same network node without communicating with each other, use OpenRG's VLAN bridging capability as described in [Section 8.4.24.7](#).

8.4.24.1. Creation with the Connection Wizard

To create a new VLAN interface, perform the following steps:

1. In the 'Network Connections' screen under 'System' (see [Figure 8.12](#)), click the 'New Connection' link. The 'Connection Wizard' screen appears (see [Figure 8.13](#)).
2. Select the 'Advanced Connection' radio button and click 'Next'. The 'Advanced Connection' screen appears (see [Figure 8.18](#)).
3. Select the 'VLAN Interface' radio button and click 'Next'. The 'VLAN Interface' screen appears.

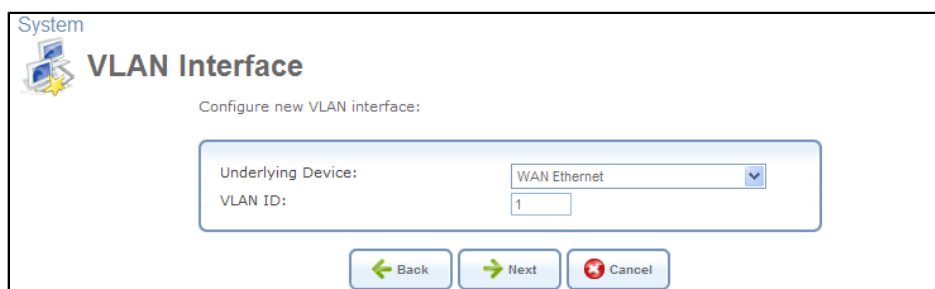


Figure 8.277. VLAN Interface



Note: By default, all of the gateway's physical LAN devices are enslaved by OpenRG's LAN bridge. A VLAN cannot be created over an enslaved network device. Therefore, remove a device from the bridge prior to creating a VLAN over it. To learn how to do so, refer to [Section 8.4.3.1](#).

4. Select the underlying device for this interface. The drop-down menu will display OpenRG's Ethernet connections.
5. Enter a value that will serve as the VLAN ID, and click 'Next'. If you choose to create the VLAN over the LAN bridge, the following screen appears.

System
VLAN Interface
 Select ports to participate in this VLAN and traffic tagging:

Tagging
 Traffic on this VLAN is: Untagged

VLAN Ports
 Selection:

Port	PVID	VLANs
<input type="checkbox"/> LAN Hardware Ethernet Switch		Disabled
<input type="checkbox"/> LAN USB		Disabled
<input type="checkbox"/> LAN Wireless 802.11g Access Point		Disabled

Figure 8.278. VLAN over LAN Bridge

Tagging This feature enables you to select whether to add a *tag header* (a 32-bit label serving as a VLAN ID) to the frames transferred over the VLAN. When the 'Untagged' option is selected, the VLAN is determined based on other information, such as the ID of a port on which the data arrived (PVID). Select the relevant setting from the designated drop-down menu. If the created virtual network is intended for VLAN-unaware hosts, it is recommended that you select the 'Untagged' option.

VLAN Ports You can select the LAN bridge ports on which you would like to enable the VLAN. To enable the VLAN on a specific device port, select its check box. You can also select or deselect all of the ports by clicking the corresponding buttons.

6. After setting the VLAN parameters, click 'Next'. The 'Connection Summary' screen appears.

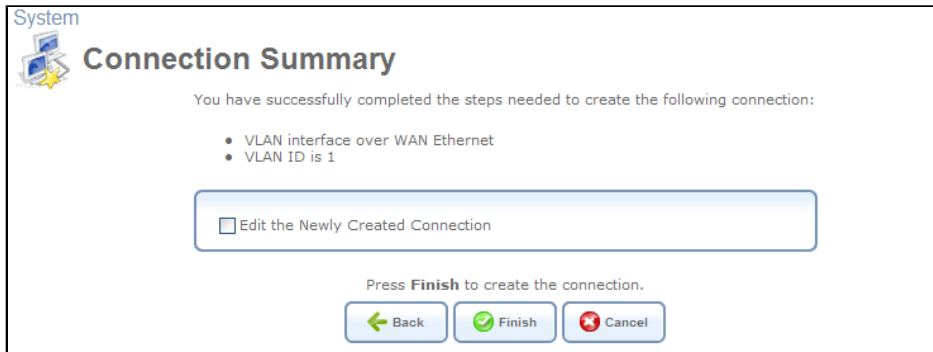


Figure 8.279. Connection Summary

7. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.
8. Click 'Finish' to save the settings.

The new VLAN interface will be added to the network connections list, and will be configurable like any other connection.

8.4.24.2. General

To view and edit the VLAN interface settings, click its link. For example, click the 'WAN Ethernet 2' link in the 'Network Connections' screen. The 'WAN Ethernet 2 Properties' screen appears (see [Figure 8.280](#)), displaying a detailed summary of the connection's parameters, under the 'General' sub-tab. These parameters can be edited in the rest of the screen's tabs, as described in the following sections.

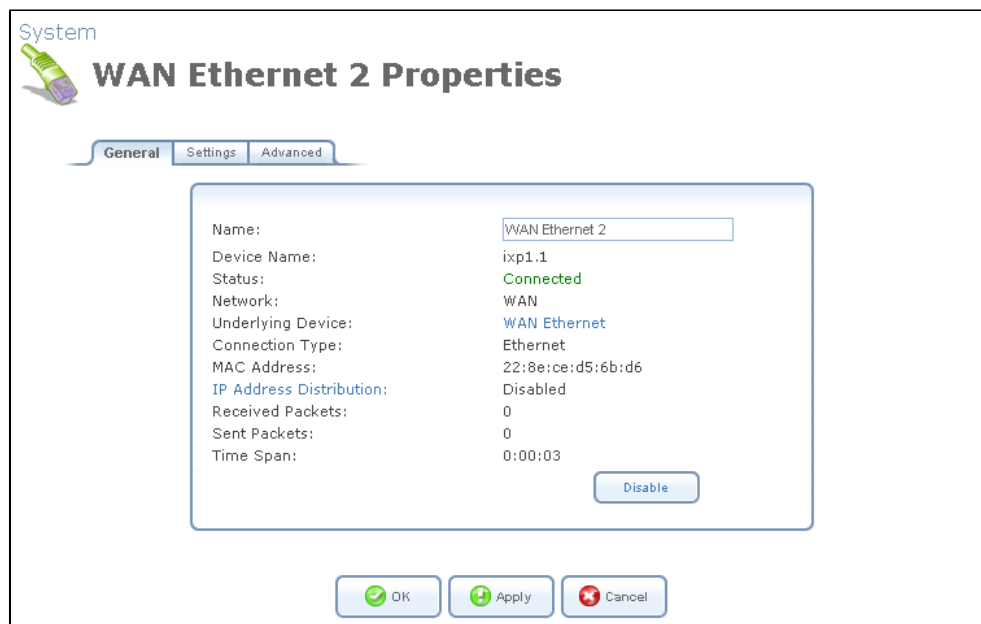


Figure 8.280. WAN Ethernet 2 Properties

8.4.24.3. Settings

General This section displays the connection's general parameters.

General	
Device Name:	ixp1.1
Status:	Connected
Schedule:	Always ▼
Network:	WAN ▼
Connection Type:	Ethernet
Physical Address:	22:8e:ce:d5:6b:d6
MTU:	Automatic ▼ 1500
Underlying Connection:	WAN Ethernet

Figure 8.281. General VLAN Interface Settings

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, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to [Section 8.9.3](#).

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to [Section 8.4.2](#).

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.

Underlying Connection The Ethernet device over which the connection is implemented.

Internet Protocol Select one of the following Internet protocol options from the 'Internet Protocol' drop-down menu:

- No IP Address
- Obtain an IP Address Automatically
- Use the Following IP Address

Note that the screen will refresh to display relevant configuration settings according to your choice.

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.

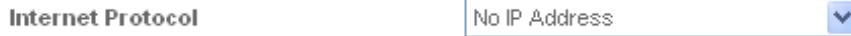


Figure 8.282. Internet Protocol – No IP Address

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 click 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.



Figure 8.283. Internet Protocol Settings – Automatic IP

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.



Figure 8.284. Internet Protocol – Static IP

8.4.24.4. 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. To learn more about your gateway's security features, refer to [Section 7.3](#).

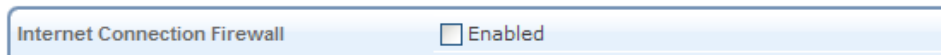


Figure 8.285. Internet Connection Firewall

Internet Connection Fastpath Select this check box to utilize the *Fastpath* algorithm for enhancing packet flow, resulting in faster communication between the LAN and the WAN. By default, this feature is enabled.

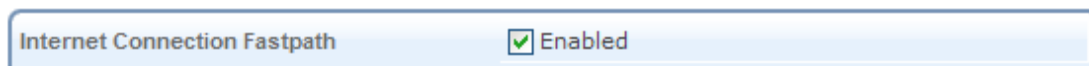


Figure 8.286. Internet Connection Fastpath

- **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 and the http://openrg.home.


Additional IP Addresses		
IP Address	Subnet Mask	Action
New IP Address		

Figure 8.287. Additional IP Addresses

8.4.24.5. DSCP Remark According to 802.1p CoS

When creating a VLAN interface over a LAN connection, it is possible to determine the IP header's Differentiated Services Code Point (DSCP) priority value according to the VLAN header's 802.1p Class of Service (CoS) tag. The DSCP value can then be used for Quality of Service (Qos) traffic prioritization. For more information, refer to [Section 7.4](#).

DSCP Remark According to 802.1p CoS	<input type="checkbox"/> Enabled
-------------------------------------	----------------------------------

Figure 8.288. DSCP Remark According to 802.1p CoS

1. Select the 'Enabled' check-box. The screen refreshes, displaying the following table.



802.1p CoS	DSCP	Action
New DSCP Remark		

Figure 8.289. DSCP Remarks Table

2. Click the 'New DSCP Remark' link. The following screen appears.

System  **DSCP Remark According to 802.1p CoS**

802.1p CoS:

DSCP: (Hex)

Figure 8.290. DSCP Remark Entry Settings

3. Enter the 802.1p CoS and DSCP values to be associated, and click 'OK'. The new pair of values will appear in the table.
4. Click 'OK' to save the settings.

8.4.24.6. VLAN Use Case

The following example demonstrates the advantages of a VLAN interface through practical setup and performance measurements. The VLAN interface in this example is used to grant prioritization to specific traffic, providing a basic level of Quality of Service (refer to [Section 7.4](#)).

8.4.24.6.1. Hardware Requirements

This use case requires the following:

- A development board
- Two equal Linux LAN hosts holding two identical 100MB files
- A 10 Mbps switch (optional)
- A WAN host serving as an FTP server

8.4.24.6.2. Physical Setup

Since this example requires overloading the WAN, the WAN network segment bandwidth must be less than the LAN's. This can be achieved, for example, by either connecting OpenRG's WAN to a 10 Mbps switch, or by forcing the FTP server's WAN interface to 10 Mbps.

1. Connect the two LAN hosts to the development board's LAN ports.
2. Connect the board's WAN port to the 10 Mbps switch, and the switch to the WAN.

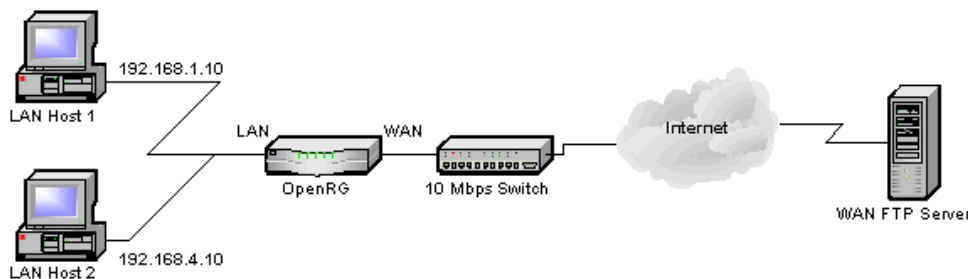



Figure 8.291. Physical Setup

8.4.24.6.3. OpenRG Configuration

To configure the VLAN interface, perform the following steps:

1. In the 'Network Connections' screen, delete the LAN bridge (if one exists) by clicking its  action icon. Click 'OK' in the attention screen to confirm the deletion. The LAN Ethernet that was enslaved to the bridge will automatically be configured with the IP address 192.168.1.1, and serve as the DHCP server for this subnet.

2. Create a VLAN interface over the LAN Ethernet, using the Advanced utility of the connection wizard. The underlying device should be LAN Ethernet (or LAN Hardware Ethernet Switch, depending on your platform). Set the VLAN ID to 100.

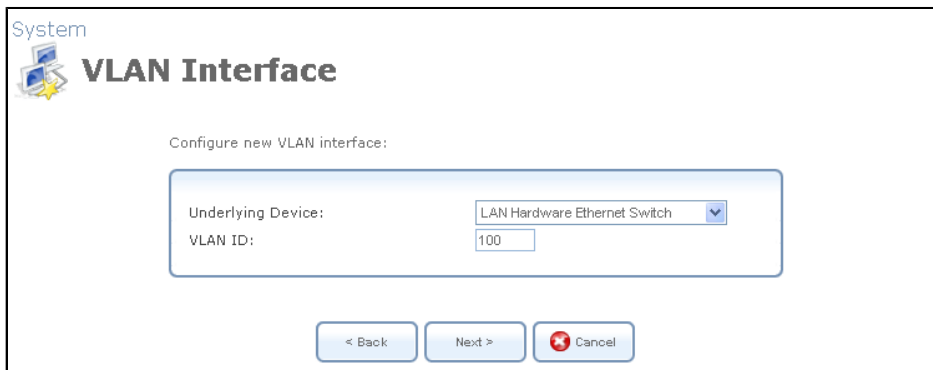


Figure 8.292. VLAN Interface Configuration

3. In the 'Connection Summary' screen, check the 'Edit the Newly Created Connection' check box and click Finish. The 'LAN Ethernet Properties' screen appears:

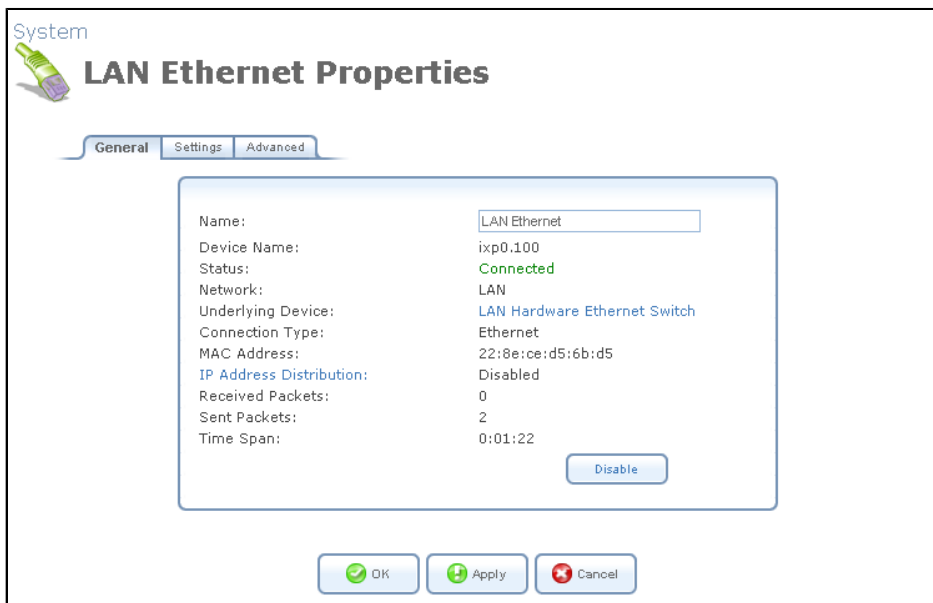


Figure 8.293. LAN Ethernet Properties

4. Click the Settings tab, and in the Internet Protocol section, select "Use the Following IP Address" from the drop-down menu. The screen refreshes (see [Figure 8.294](#)).
5. Enter 192.168.4.1 as the IP address and 255.255.255.0 as the subnet mask.

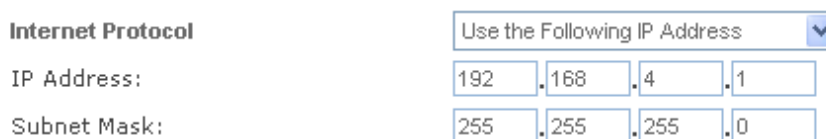


Figure 8.294. Internet Protocol

6. In the IP Address Distribution section, select "DHCP Server" from the drop-down menu. The screen refreshes (see [Figure 8.295](#)).
7. Enter 192.168.4.2 as the start IP address and 192.168.4.254 as the end IP address. Enter 255.255.255.0 as the subnet mask. Leave all other fields at their defaults.

IP Address Distribution

DHCP Server ▼

Start IP Address: 192 . 168 . 4 . 2

End IP Address: 192 . 168 . 4 . 254

Subnet Mask: 255 . 255 . 255 . 0

Lease Time in Minutes: 60

Provide Host Name If Not Specified by Client

Figure 8.295. IP Address Distribution

8. Click the Advanced tab, and verify that the Internet Connection Firewall is disabled.

Internet Connection Firewall Enabled

Additional IP Addresses [New IP Address](#)

Figure 8.296. Internet Connection Firewall

9. Click 'OK' to save the settings.

8.4.24.6.4. Host 1 Configuration

This computer will act as an ordinary LAN host connected to OpenRG with no special settings. After connecting the computer to the gateway, use the following command (in the Linux shell command line) to obtain an IP address from OpenRG:

```
# pump -i eth0
```

Verify that the obtained IP address is in OpenRG's default subnet (192.168.1.x) using this command:

```
# ifconfig eth0
```

8.4.24.6.5. Host 2 Configuration

This computer will act as a VLAN-capable host connected to OpenRG. Use the following command to create the VLAN interface (verify that the `vconfig` utility is installed on this host's Linux operating system):

```
# vconfig add eth0 100
```

After connecting the computer to the gateway, use the following command (in the Linux shell command line) to obtain an IP address from OpenRG:

```
# pump -i eth0.100
```

Verify that the obtained IP address is in OpenRG's VLAN subnet (192.168.4.x) using this command:

```
# ifconfig eth0.100
```

8.4.24.6.6. Running the Scenario

1. Open an FTP connection from both hosts to the WAN FTP server. Use an FTP client that displays throughput rates.
2. Initiate an FTP **upload** of the 100MB files from both hosts to the server simultaneously. Observe that the throughput rates on both hosts are similar - approximately half of the forced WAN bandwidth (5MB each).
3. Configure the VLAN interface of Host 2 to add priority to VLAN frames, using the following command:

```
# vconfig set_egress_map eth0.100 0 7
```

4. Repeat the FTP upload test and observe that the throughput rate of Host 2 increases significantly at the expense of Host 1.

8.4.24.7. VLAN Bridge Use Case

OpenRG enables you to partition an Ethernet-based network by creating segregated virtual networks. Such network topology can be effectively used, for example, in the following real-life situation.

A company's workstations are connected to the same physical network, and all of them receive an IP from the same DHCP server. However, all of the R&D department workstations need to be connected to a separate file server, to which the rest of the company's workstations do not have access. At the same time, the R&D workstations should not have access to the file server that belongs, for example, to the Marketing department.

To create such a network topology, you can set up a *VLAN bridge* and connect all the workstations to it in the manner depicted in the following figure.

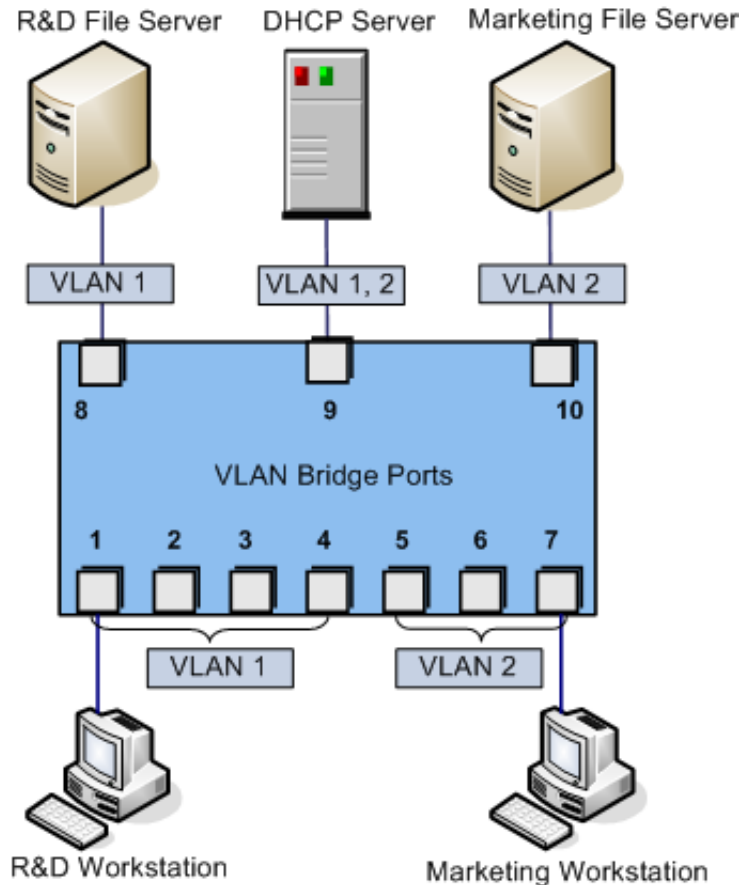


Figure 8.297. VLAN Bridge

The DHCP server is configured to handle both VLANs, and can distinct between requests sent from the R&D workstations and requests from the Marketing workstations.

The advantage of this method of network management is that any workstation can be moved from network to network without a need for any physical (wiring) modification. The only thing a system administrator has to do is to reconfigure the VLAN bridge by changing the default VLAN ID for a certain port.



Note: The following procedure is appropriate only for platforms with LAN hardware switch ports that support PVID.

To set up a VLAN bridge on OpenRG, perform the following:

1. In the 'Network Connections' screen under 'System' (see [Figure 8.12](#)), click the 'New Connection' link. The 'Connection Wizard' screen appears (see [Figure 8.13](#)).
2. Select the 'Advanced Connection' radio button and click 'Next'. The 'Advanced Connection' screen appears (see [Figure 8.18](#)).
3. Select 'Network Bridging' and click 'Next'. The 'Bridge Options' screen appears.

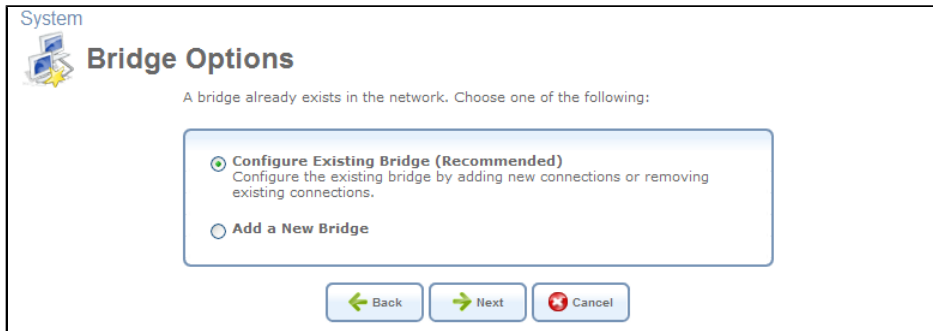


Figure 8.298. Bridge Options

4. Select the 'Configure Existing Bridge' option and click 'Next'. The 'Network Bridging' screen appears.

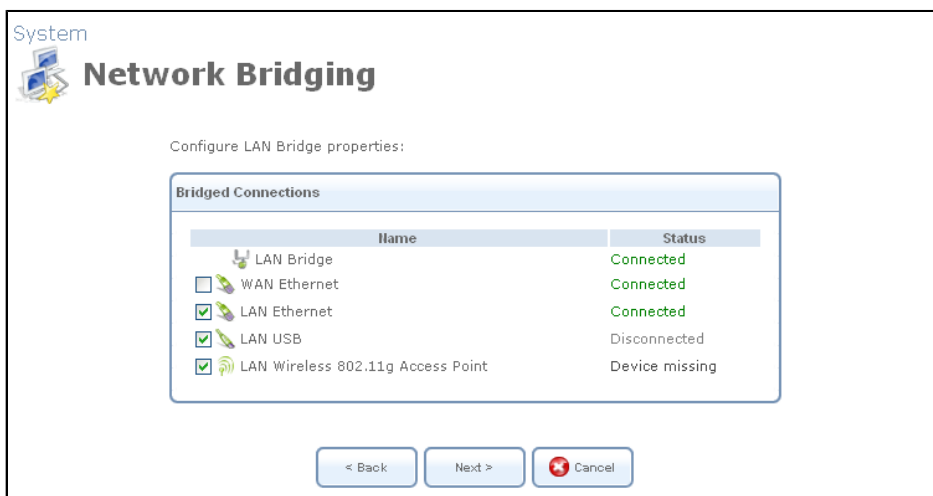


Figure 8.299. Network Bridging – Configure Existing Bridge

5. Select the 'WAN Ethernet' check box and click 'Next'. A LAN-WAN bridge is created, and the 'Connection Summary' screen appears, corresponding to your changes.

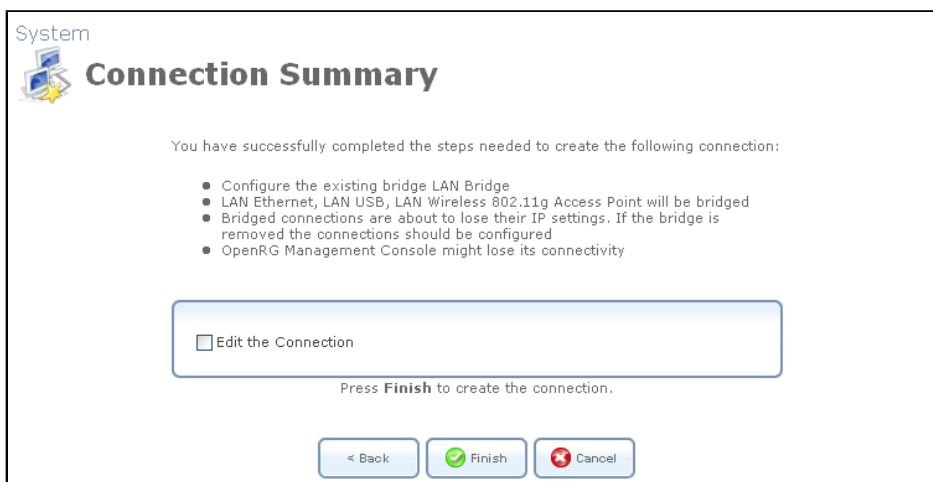


Figure 8.300. Connection Summary – Configure Existing Bridge

6. Click 'Finish' to save the settings.

7. Back in the 'Network Connections' screen, click the 'LAN Bridge' link, and select 'Bridging'. The following screen appears.

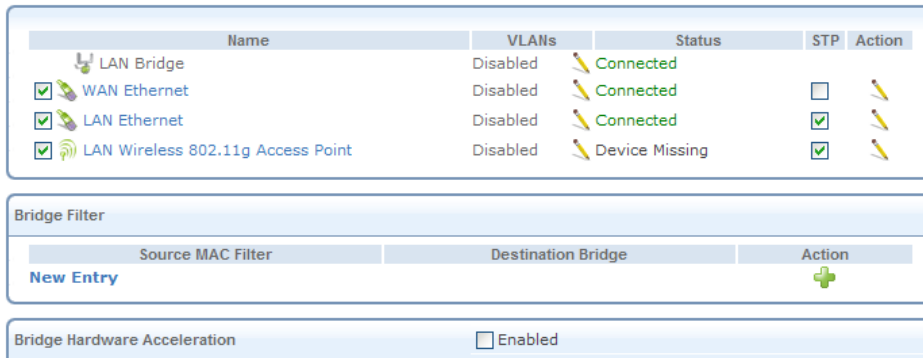


Figure 8.301. LAN Bridge Properties – Bridging

8. Under the 'VLANs' column, click the  action icon of the WAN Ethernet connection. The connection's 'VLAN Settings' screen appears.

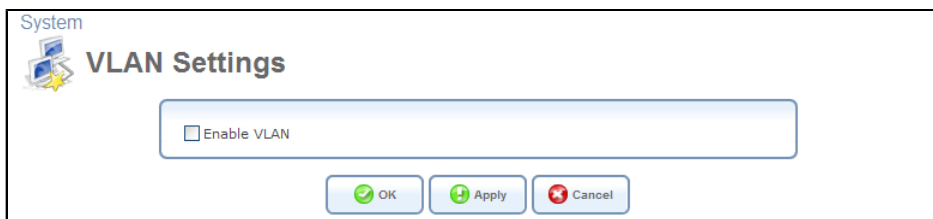


Figure 8.302. VLAN Settings

9. Select the 'Enable VLAN' check box, and click 'Apply'. The screen refreshes, adding the 'VLAN IDs' section.

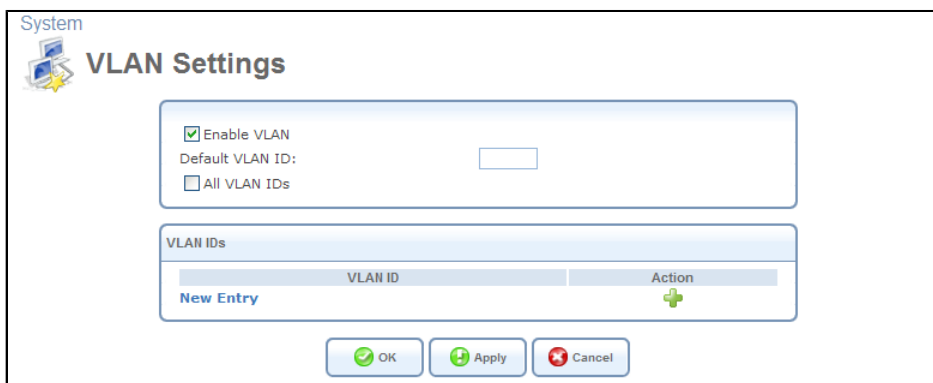


Figure 8.303. VLAN Settings – Add VLAN ID

10. Define **VLAN 1** and then **VLAN 2** by going through the following steps:
- Click the 'New Entry' link. The 'VLAN ID Settings' screen appears.

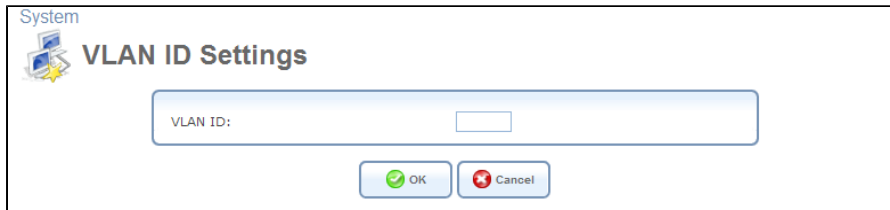


Figure 8.304. VLAN ID Settings

- b. In the 'VLAN ID' field, enter a number that will serve as a VLAN ID (in this example, 1 and 2).
- c. Click 'OK' to save settings. The defined VLAN entries appear in the 'VLAN Settings' screen.

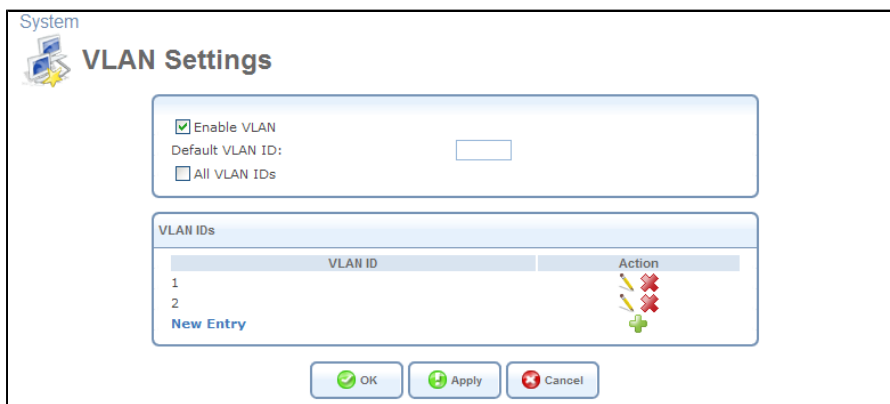



Figure 8.305. VLAN Settings – Added VLANs

- d. Click 'OK'. You are redirected back to the 'Bridging' section of the 'LAN Bridge Properties' screen (see [Figure 8.301](#)).
11. Under the 'VLANs' column, click the  action icon of the LAN Hardware Ethernet Switch connection. The connection's 'VLAN Settings' screen appears (see [Figure 8.302](#)).
 12. Define the two VLAN IDs on the LAN Hardware Ethernet Switch connection exactly as on the WAN Ethernet one.
 13. Configure each of the involved switch ports with a specific VLAN ID:
 - a. In the 'Network Connections' screen, click the 'LAN Hardware Ethernet Switch' link, and select 'Switch'. The following screen appears.

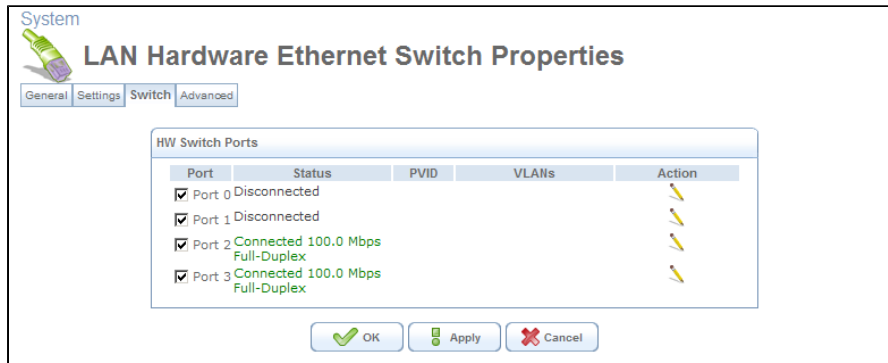


Figure 8.306. LAN Hardware Ethernet Switch Properties – Switch

- b. Click the action icon that corresponds to the port you would like to configure. The 'Port Settings' screen appears.

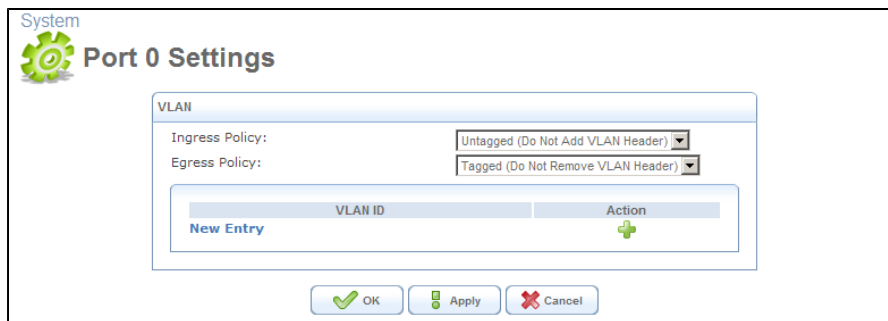


Figure 8.307. Port Settings

- c. From the 'Ingress Policy' drop-down menu, select the 'Tagged' option. The screen refreshes, displaying the 'Default VLAN ID' field (see [Figure 8.308](#)).
- d. Enter an ID of the VLAN that will be created on the port. The incoming (ingress) frames will be marked with this ID.
- e. From the 'Egress Policy' drop-down menu, select the 'Untagged' option.

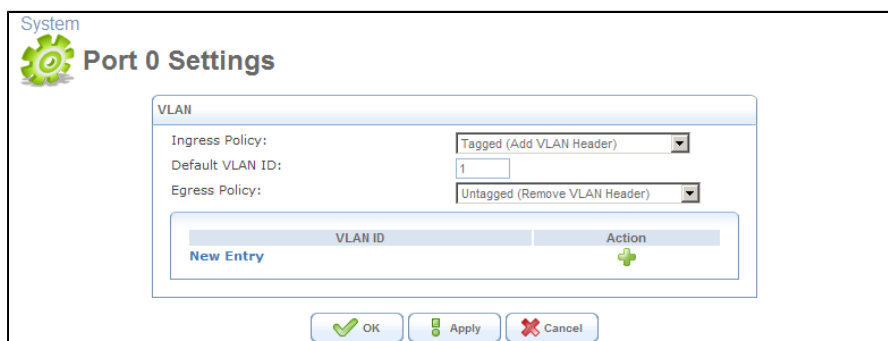


Figure 8.308. Port Settings – VLAN

- f. Click 'OK' to save the settings. OpenRG will request browser reloading.

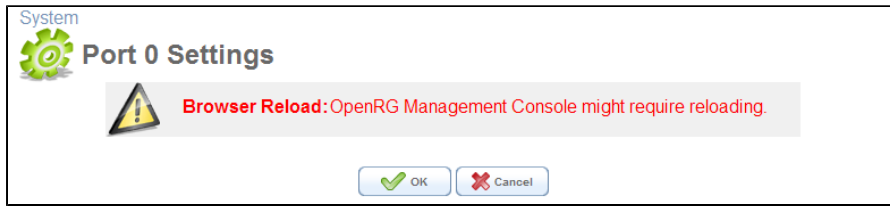


Figure 8.309. Port Settings – Browser Reloading

- g. Click 'OK' to proceed. After the 'Port Settings' screen is back, the default VLAN ID appears in the dedicated VLAN ID entries table.

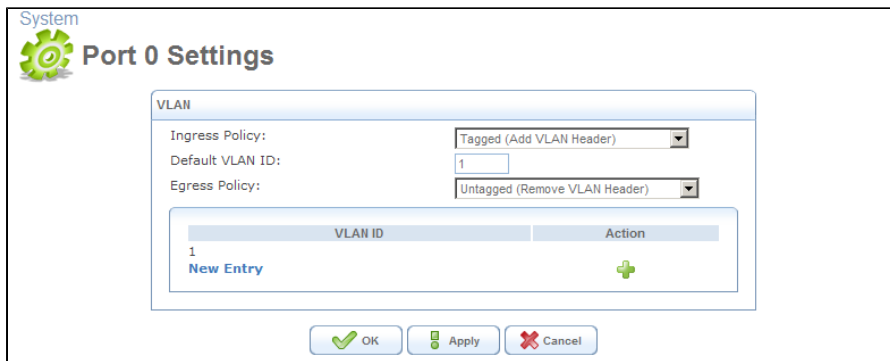


Figure 8.310. Port Settings – Default VLAN ID

- h. Click 'OK'. You are redirected back to the 'LAN Hardware Ethernet Switch Properties' screen, in which the configured port's VLAN ID is displayed.

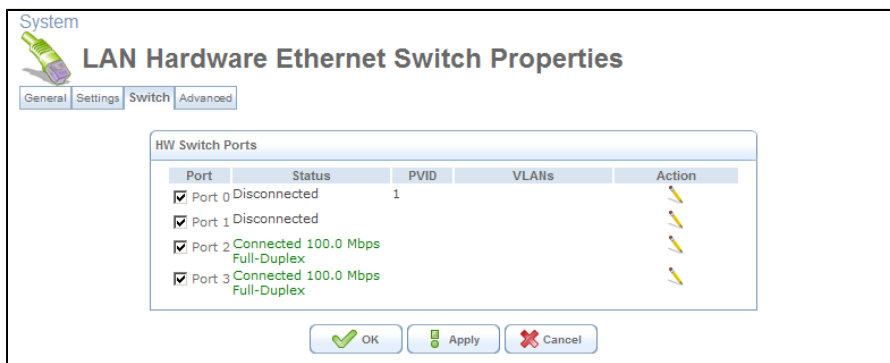


Figure 8.311. Port Settings – Default VLAN ID

- i. Perform the same procedure on each of the ports you will be using.

14. Verify that IP forwarding is disabled on your DHCP server.

To verify that there is no communication between the two VLANs, perform the following test:

1. Connect two hosts to the ports that belong to different VLANs. Each of the hosts will be assigned an IP with a different subnet by the DHCP server.
2. Ping each host from another one. If you have successfully performed the aforementioned procedure, the ping test will fail. This means that the traffic of each VLAN is segregated.

8.4.24.8. Port-based VLAN Tagging

A LAN device can obtain a VLAN tag (identifier) from its LAN switch port settings. This section describes several configuration options in order to achieve port-based VLAN tagging on OpenRG.

This example may suit a scenario where three hosts and a SIP telephone are connected to the gateway. Each of these LAN devices must be assigned with a different VLAN ID and priority when it communicates through the WAN. The following are the assumptions regarding the current network topology and setup:

- A LAN bridge connects the Ethernet switch and WLAN interfaces.
- The WAN connection is DHCP/Ethernet.
- Two VLAN IDs will be used: one for traffic received on port 3 on the LAN Ethernet switch (connected to the IP phone), and the other for all other traffic, generated by the hosts connected to the other Ethernet switch ports and through the WLAN interface. This example can be extended to support more VLAN subnets.

8.4.24.8.1. Option A: Bridge Mode

In this option VLAN interfaces are not configured. All LAN traffic is bridged to the WAN, with different VLAN IDs depending on the receiving LAN Ethernet switch port. You must simply adjust the LAN Ethernet switch port settings for each port, so that it tags received packets with a VLAN ID. You must connect the WAN Ethernet device to the bridge, and configure the bridge to receive and transmit tagged traffic on the Ethernet WAN device.

Based on the Rx port, you can add VLAN IDs on outgoing packets. To mark the packets received on each of the LAN switch ports with different VLAN ID, perform the following:

1. In the WBM, click the 'Device' menu item under the 'Local Network' tab. The 'Device' screen appears.

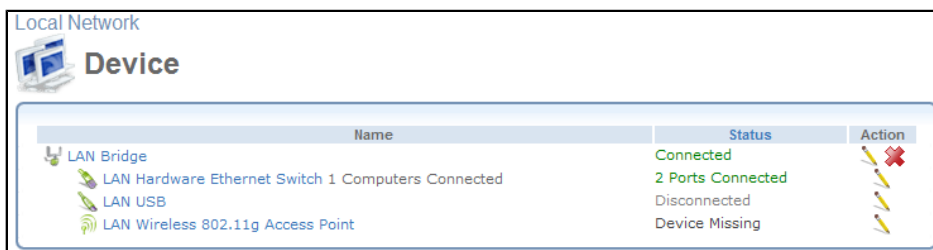



Figure 8.312. Local Network Device View

2. Click the 'LAN Hardware Ethernet Switch' link (or its  action icon).
3. In the 'LAN Hardware Ethernet Switch Properties' screen, click the 'Switch' sub-tab.

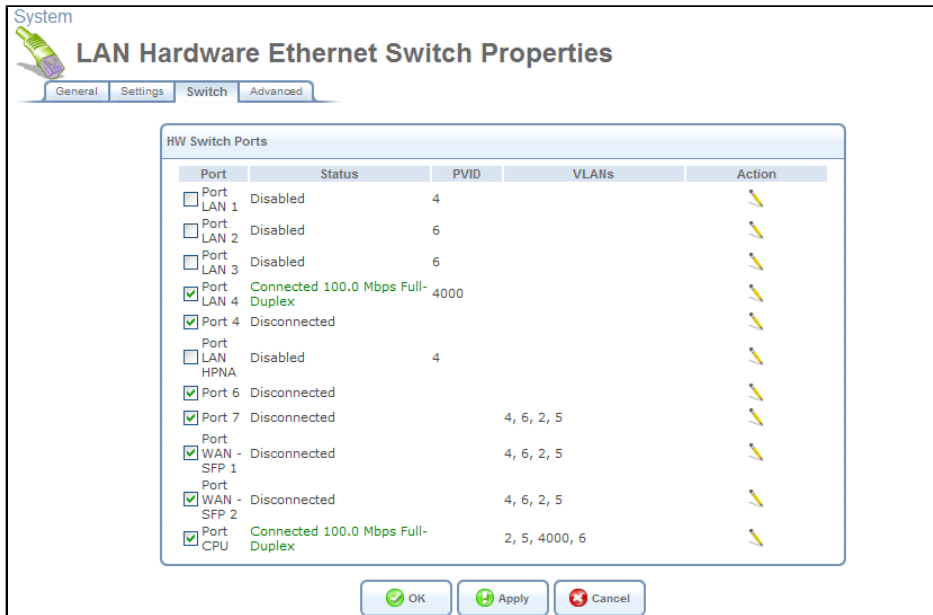


Figure 8.313. Switch

- Click a port's action icon . The 'Port LAN Settings' screen appears.

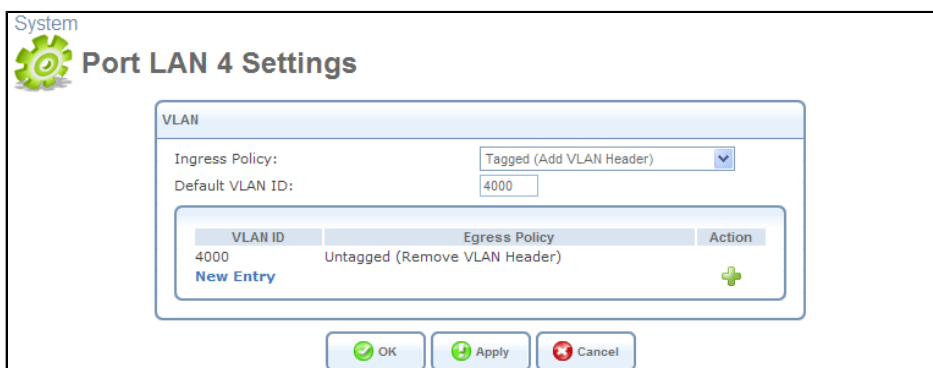


Figure 8.314. Port LAN Settings

- In the 'Ingress Policy' drop-down menu, select 'Tagged (Add VLAN Header)'.
- Under the 'VLAN ID' column, click 'New Entry' in order to add identifiers to the VLAN.

8.4.24.8.2. Option B: Mixed Bridge/Route Mode

In this option, you will configure two VLAN interfaces over the WAN Ethernet device, and one VLAN interface over the LAN bridge. The LAN VLAN interface is used to distinguish the traffic on switch port 3 from the traffic on other switch ports and WLAN interface. Traffic is bridged from the LAN VLAN interface to the first WAN VLAN interface. All other traffic is routed to the second WAN VLAN interface. To set the 802.1p value of the packets according to the receiving interface, you must configure a QoS packet priority output rule on each WAN VLAN interface.

Configure the LAN VLAN interface:

1. In the WBM, click the 'Network Connections' menu item under the 'System' tab, and then click the 'New Connection' link. The Connection Wizard commences.



Figure 8.315. Connection Wizard

2. Select 'Advanced Connection' and click 'Next'.
3. Select 'VLAN Interface' and click 'Next'.

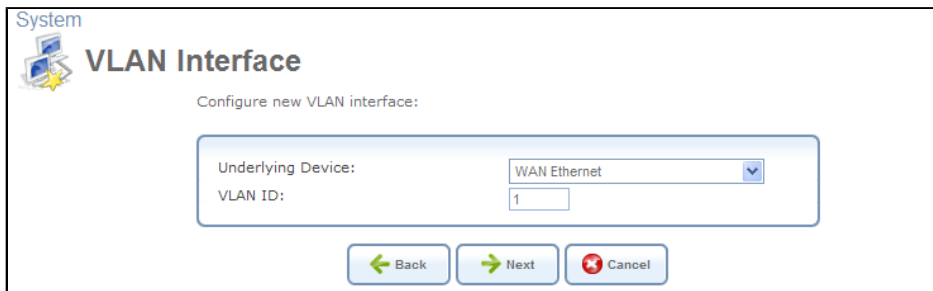


Figure 8.316. VLAN Interface

4. Select 'LAN Bridge' as the underlying device, and provide a VLAN ID. Click 'Next'.

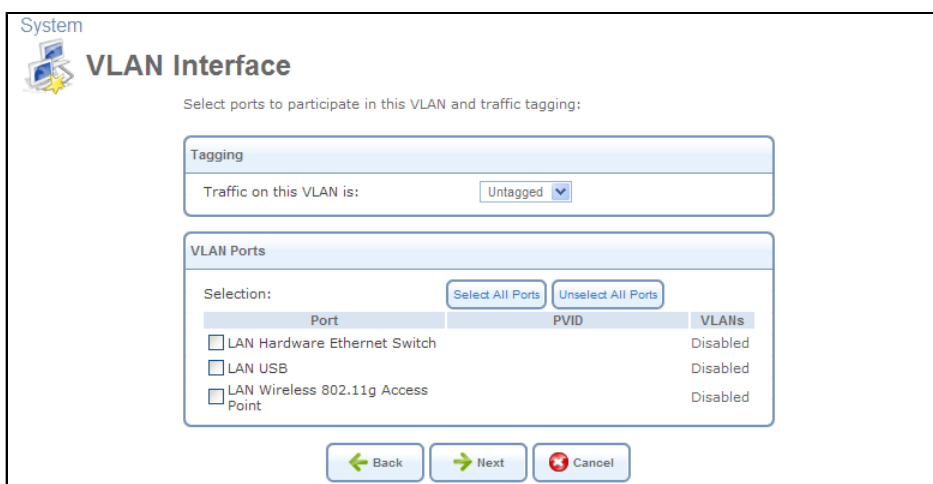


Figure 8.317. VLAN over LAN Bridge

5. In the 'Tagging' section, select 'Tagged'. In the 'VLAN Ports' section, check 'LAN Hardware Ethernet Switch' and port 3. Click 'Next' and then 'Finish'.

The newly created LAN VLAN interface has no IP address. Its traffic will be bridged to the WAN VLAN. The IP devices connected to the LAN Ethernet switch port 3 are assumed to have a public IP address.

Configure the WAN VLAN interface:

1. Follow the instructions above, but in the 'VLAN Interface' screen, select 'WAN Ethernet' as the underlying device and provide a VLAN ID. Click 'Next'. The 'Connection Summary' screen appears.

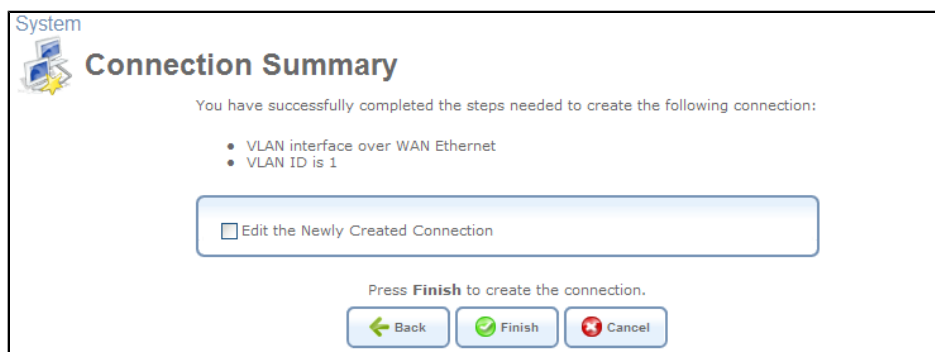


Figure 8.318. Connection Summary

2. Select the 'Edit the Newly Created Connection' check box and click 'Finish'.
3. In the 'WAN Ethernet VLAN Properties' screen, click the 'Routing' sub-tab and deselect the 'Default Route' field.

8.4.24.8.3. Option C: DSCP-based Routing

In this option, traffic from LAN is routed (and NATed) to the WAN rather than bridged. You must configure two VLAN interfaces over the WAN Ethernet device, and one VLAN interface over the LAN bridge. You will use the QoS rules to set the DSCP value on the packets arriving on the LAN VLAN interface. The routing decision will be based on the DSCP value, using DSCP-based static route rules. Traffic from the LAN VLAN will be routed to the first WAN VLAN, and use the second WAN VLAN as default route. DSCP values are translated into 802.1p priority by the QoS module.

8.4.25. Routed IP over ATM (IPoA)

Routed IP over ATM (IPoA) is a standard for transmitting IP traffic in an ATM network.

8.4.25.1. Creation with the Connection Wizard

To create a new IPoA connection, perform the following steps:

1. Click the New Connection link in the 'Network Connections' screen (see [Figure 8.12](#)). The 'Connection Wizard' screen will appear (see [Figure 8.20](#)).

2. Select the Advanced Connection radio button and click Next. The 'Advanced Connection' screen will appear (see [Figure 8.25](#)).
3. Select the Routed IP over ATM (IPoA) radio button and click Next. The 'Routed IP over ATM (IPoA)' screen will appear (see [Figure 8.319](#)).

System
Routed IP over ATM (IPoA)

Configure your IPoA connection properties:

IP Address:	210	150	3	12
Subnet Mask:	255	255	255	0
Default Gateway:	210	150	3	254
Primary DNS Server:	210	150	3	252
Secondary DNS Server:	0	0	0	0
VPI:	8			
VCI:	48			
Encapsulation:	LLC			

< Back Next > Cancel

Figure 8.319. Routed IP over ATM

4. Enter the following information, which should be provided to you by your Internet Service Provider (ISP):
 - IP Address
 - Subnet Mask
 - Default Gateway
 - Primary DNS Server
 - Secondary DNS Server
 - The VPI and VCI pair of identifiers
 - The encapsulation method: LLC or VCMux
5. Click Next. The 'Connection Summary' screen will appear (see [Figure 8.320](#)).

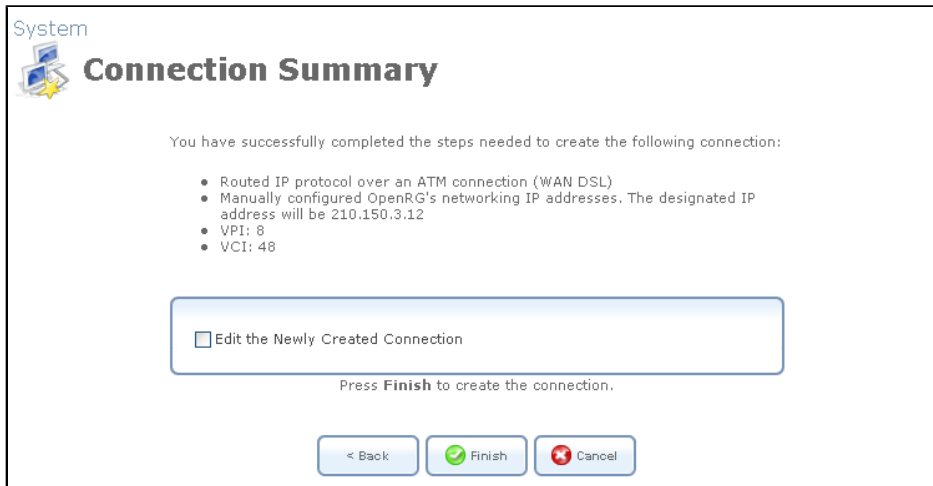


Figure 8.320. Connection Summary

6. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.
7. Click Finish to save the settings.

The new IPoA connection will be added to the network connections list, and will be configurable like any other connection.

8.4.25.2. General

To view and edit the IPoA connection settings, click the 'WAN IPoA' link in the 'Network Connections' screen (see [Figure 8.12](#)). The 'Routed IP over ATM Properties' screen will appear (see [Figure 8.321](#)), 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.

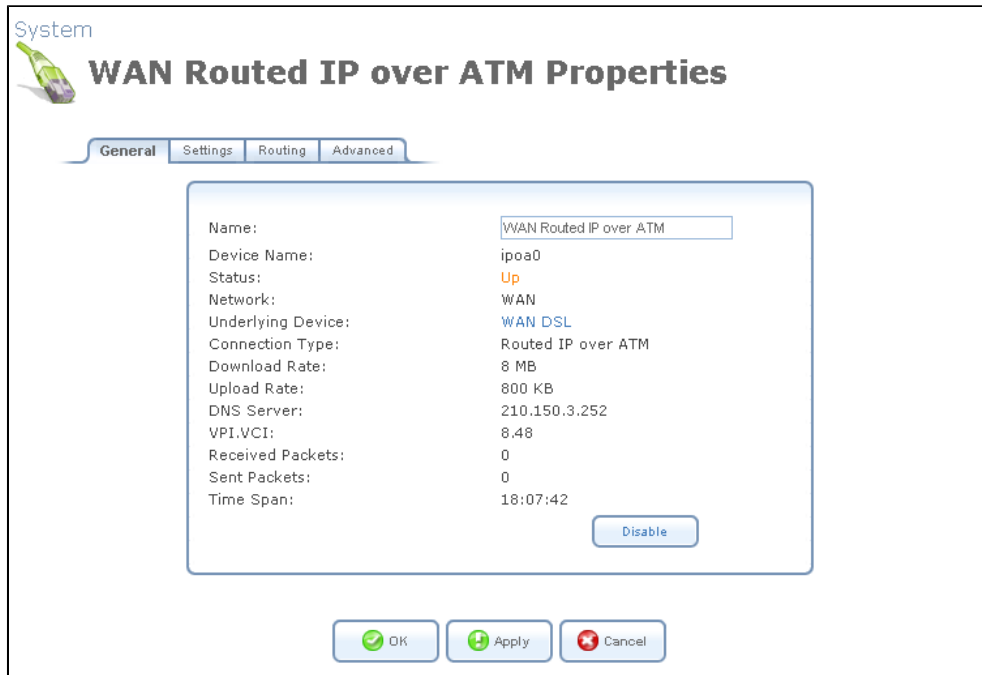


Figure 8.321. Routed IP over ATM Properties

8.4.25.3. Settings

General This section displays the connection's general parameters.



Figure 8.322. General IPoA Settings

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, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to [Section 8.9.3](#).

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to [Section 8.4.2](#).

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.

Underlying Connection Specify the underlying connection above which the protocol will be initiated.

ATM

Asynchronous Transfer Mode (ATM) is a network technology based on transferring data in cells or packets of a fixed size. The cell used with ATM is relatively small compared to units used with other technologies. The small, constant cell size allows the transmission of video, audio, and computer data, assuring that no single type of data consumes the connection. ATM addressing consists of two identifiers that identify the virtual path (VPI) and the virtual connection (VCI). A virtual path consists of multiple virtual channels to the same endpoint. The 'Encapsulation' for connection should be set to either 'LLC' or 'VCMux'. You should configure these parameters according to the information provided by your ISP.

ATM	<input type="checkbox"/> Automatic PVC Scan
VPI:	<input type="text" value="8"/>
VCI:	<input type="text" value="48"/>
Encapsulation:	<input type="text" value="LLC"/>

Figure 8.323. ATM Settings

Internet Protocol This connection always uses a specified IP address. Your service provider should provide you with this IP address, subnet mask, the default gateway and DNS server.

Internet Protocol	<input type="text" value="Use the Following IP Address"/>
IP Address:	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="1"/>
Subnet Mask:	<input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/>

Figure 8.324. Internet Protocol Settings - Static IP

8.4.25.4. 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.

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.

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'.

Multicast – IGMP Proxy Internal / Default OpenRG serves as an IGMP proxy, issuing IGMP host messages on behalf of its LAN hosts. This check box is enabled on LAN connections by default, meaning that if a LAN multicast server is available, other LAN hosts asking to join multicast groups (by sending IGMP requests) will be able to join its multicast group. However, this check box is disabled on the WAN connection by default, meaning that LAN hosts will not be able to join multicast groups of WAN multicast servers. When creating a WAN-LAN bridge, this check box must also be deselected.

IGMP Query Version OpenRG supports all three versions of IGMP. Select the version you would like to use. Note that this drop-down menu appears for LAN connections only.

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.

Routing Mode:

Device Metric:

Default Route

Multicast - IGMP Proxy Internal

IGMP Query Version:

Routing Information Protocol (RIP)

Name	Destination	Gateway	Netmask	Metric	Status	Action
LAN Bridge	192.168.2.4	192.168.1.1	255.255.255.255	2	Applied	

[New Route](#)

Figure 8.325. Advanced Routing Properties

To learn more about this feature, refer to [Section 8.6.1](#).

8.4.25.5. 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. To learn more about your gateway's security features, refer to [Section 7.3](#).



Figure 8.326. Internet Connection Firewall

8.4.26. Internet Protocol over Internet Protocol (IPIP)

OpenRG allows you to create an IPIP tunnel to another router, by encapsulating IP packets in IP. This tunnel can be managed as any other network connection. Supported by many routers, this protocol enables using multiple network schemes. Note, however, that IPIP tunnels are not secured.

8.4.26.1. Creation with the Connection Wizard

To create a new IPIP tunnel, perform the following:

1. In the 'Network Connections' screen under 'System' (see [Figure 8.12](#)), click the 'New Connection' link. The 'Connection Wizard' screen appears (see [Figure 8.13](#)).
2. Select the 'Advanced Connection' radio button and click 'Next'. The 'Advanced Connection' screen appears (see [Figure 8.18](#)).
3. Select the 'Internet Protocol over Internet Protocol (IPIP)' radio button and click 'Next'. The 'Internet Protocol over Internet Protocol (IPIP)' screen appears.

Figure 8.327. Internet Protocol over Internet Protocol (IPIP)

4. Enter the tunnel's remote endpoint IP address.
5. Enter the local IP address for the interface.
6. Enter the IP address and subnet mask of the remote network that will be accessed via the tunnel, and click 'Next'. The 'Connection Summary' screen appears.

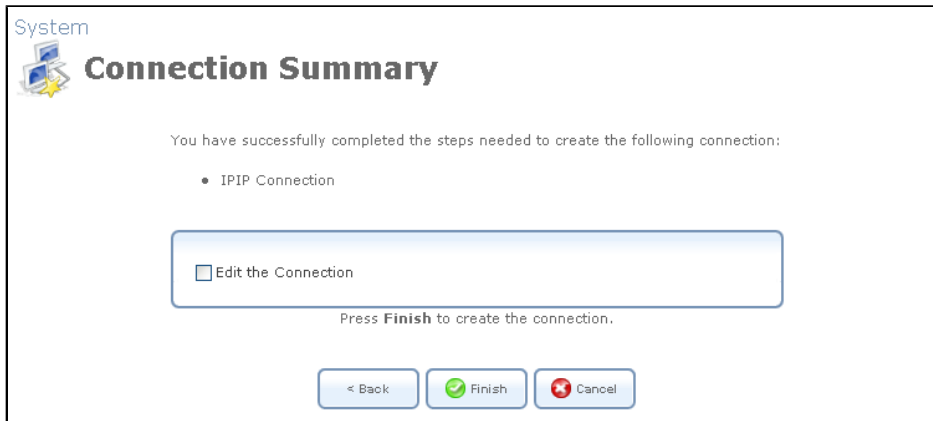


Figure 8.328. Connection Summary

7. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.

8. Click 'Finish' to save the settings.

The new IPIP tunnel will be added to the network connections list, and will be configurable like any other connection.

8.4.26.2. General

To view and edit the IPIP connection settings, click the 'WAN IPIP' link in the 'Network Connections' screen (see [Figure 8.12](#)). The 'WAN IPIP Properties' screen will appear (see [Figure 8.329](#)), 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.

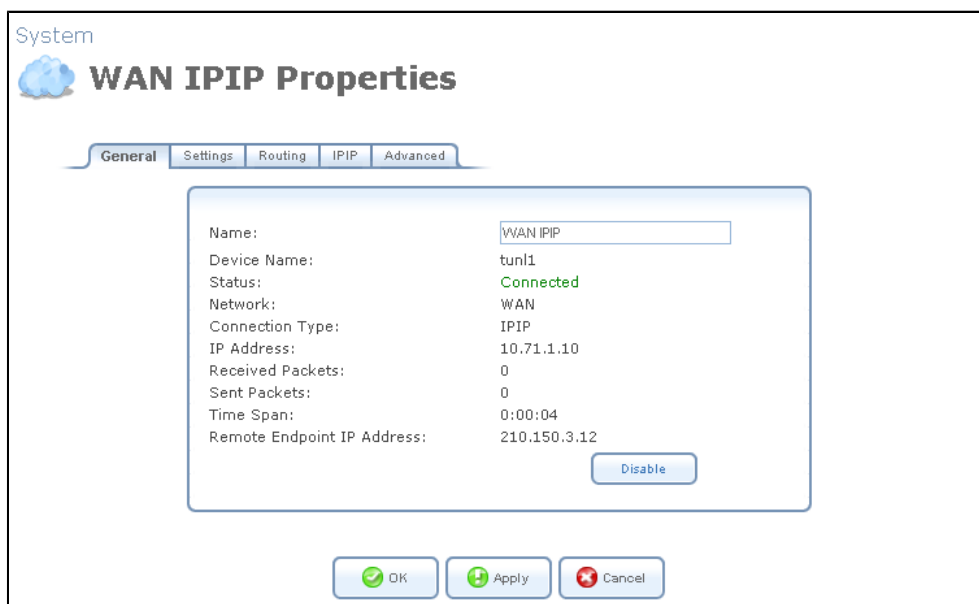


Figure 8.329. WAN IPIP Properties

8.4.26.3. Settings

General This section displays the connection's general parameters.

The screenshot shows a configuration window titled 'General' with the following settings:

- Device Name: tun1
- Status: Connected
- Schedule: Always
- Network: WAN
- Connection Type: IPIP
- MTU: Automatic 1480
- Internet Protocol:
 - IP Address: 10.71.1.10

Figure 8.330. General WAN IPIP Settings

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, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to [Section 8.9.3](#).

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to [Section 8.4.2](#).

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 The local IP address for the interface.

8.4.26.4. 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.

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.

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'.

Multicast – IGMP Proxy Internal / Default OpenRG serves as an IGMP proxy, issuing IGMP host messages on behalf of its LAN hosts. This check box is enabled on LAN connections by default, meaning that if a LAN multicast server is available, other LAN hosts asking to join multicast groups (by sending IGMP requests) will be able to join its multicast group. However, this check box is disabled on the WAN connection by default, meaning that LAN hosts will not be able to join multicast groups of WAN multicast servers. When creating a WAN-LAN bridge, this check box must also be deselected.

IGMP Query Version OpenRG supports all three versions of IGMP. Select the version you would like to use. Note that this drop-down menu appears for LAN connections only.

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.

Routing Mode:

Device Metric:

Default Route

Multicast - IGMP Proxy Internal

IGMP Query Version:

Routing Information Protocol (RIP)

Name	Destination	Gateway	Netmask	Metric	Status	Action
LAN Bridge	192.168.2.4	192.168.1.1	255.255.255.255	2	Applied	
New Route						

Figure 8.331. Advanced Routing Properties

To learn more about this feature, refer to [Section 8.6.1](#).

8.4.26.5. IPIP

The tunnel's remote endpoint IP address.

Figure 8.332. IPIP

8.4.26.6. 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. To learn more about your gateway's security features, refer to [Section 7.3](#).

Figure 8.333. Internet Connection Firewall

8.4.27. General Routing Encapsulation (GRE)

OpenRG allows you to create a GRE tunnel in order to transport multicast traffic and IPv6, in addition to other existing tunneling capabilities (e.g. IPIP, L2TP, PPTP).

8.4.27.1. Creation with the Connection Wizard

To create a new GRE tunnel, perform the following:

1. In the 'Network Connections' screen under 'System' (see [Figure 8.12](#)), click the 'New Connection' link. The 'Connection Wizard' screen appears (see [Figure 8.13](#)).
2. Select the 'Advanced Connection' radio button and click 'Next'. The 'Advanced Connection' screen appears (see [Figure 8.18](#)).
3. Select the 'General Routing Encapsulation (GRE)' radio button and click 'Next'. The 'General Routing Encapsulation (GRE)' screen appears.

Figure 8.334. General Routing Encapsulation (GRE)

4. Enter the tunnel's remote endpoint IP address.
5. Enter the local IP address of the gateway's GRE interface.
6. Enter the IP address and subnet mask of the remote network that will be accessed via the tunnel, and click 'Next'. The 'Connection Summary' screen appears.

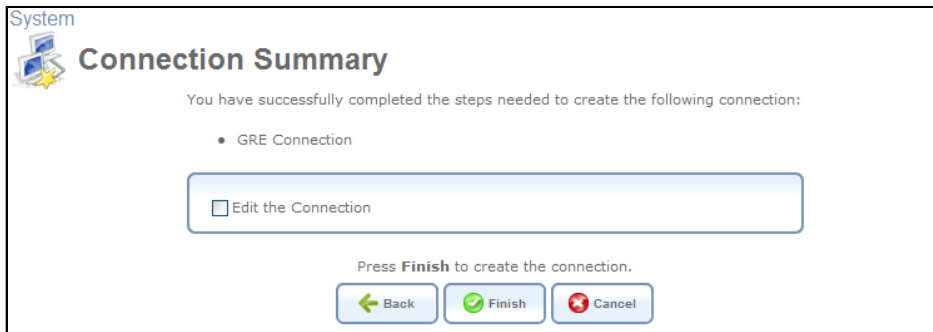


Figure 8.335. Connection Summary

7. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.
8. Click 'Finish' to save the settings.

The new GRE tunnel will be added to the network connections list, and will be configurable like any other connection.

8.4.27.2. General

To view and edit the GRE connection settings, click the 'WAN GRE' link in the 'Network Connections' screen (see [Figure 8.12](#)). The 'WAN GRE Properties' screen appears (see [Figure 8.336](#)), 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 8.336. WAN GRE Properties

8.4.27.3. Settings

General This section displays the connection's general parameters.

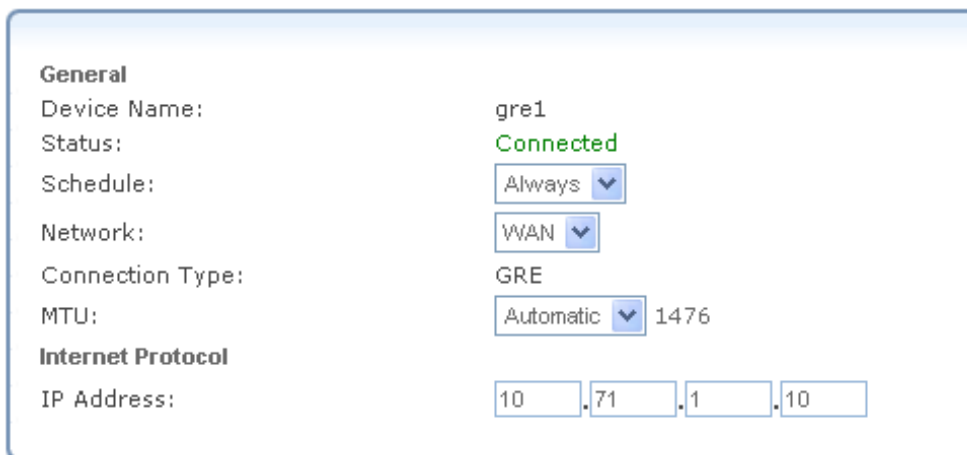


Figure 8.337. General WAN GRE Settings

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, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to [Section 8.9.3](#).

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to [Section 8.4.2](#).

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 The local IP address for the interface.

8.4.27.4. 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.

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.

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'.

Multicast – IGMP Proxy Internal / Default OpenRG serves as an IGMP proxy, issuing IGMP host messages on behalf of its LAN hosts. This check box is enabled on LAN connections by default, meaning that if a LAN multicast server is available, other LAN hosts asking to join multicast groups (by sending IGMP requests) will be able to join its multicast group. However, this check box is disabled on the WAN connection by default, meaning that LAN hosts will not be able to join multicast groups of WAN multicast servers. When creating a WAN-LAN bridge, this check box must also be deselected.

IGMP Query Version OpenRG supports all three versions of IGMP. Select the version you would like to use. Note that this drop-down menu appears for LAN connections only.

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.

Routing Mode:

Device Metric:

Default Route

Multicast - IGMP Proxy Internal

IGMP Query Version:

Routing Information Protocol (RIP)

Routing Table

Name	Destination	Gateway	Netmask	Metric	Status	Action
LAN Bridge	192.168.2.4	192.168.1.1	255.255.255.255	2	Applied	
New Route						

Figure 8.338. Advanced Routing Properties

To learn more about this feature, refer to [Section 8.6.1](#).

8.4.27.5. GRE

The tunnel's remote endpoint IP address.

GRE

Remote Endpoint IP Address:

Figure 8.339. GRE

8.4.27.6. 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. To learn more about your gateway's security features, refer to [Section 7.3](#).

Internet Connection Firewall Enabled

Figure 8.340. Internet Connection Firewall

8.4.27.7. GRE Use Case

The following example demonstrates usage of a GRE interface, to communicate between two hosts that are each in a different LAN, behind separate gateways.



A GRE tunnel is an unsecured (unencrypted) tunnel. Safety measures must be taken when setting up such a tunnel.

8.4.27.7.1. Hardware Requirements

This use case requires the following:

- Two development boards
- Two LAN hosts
- A WAN host serving as an DHCP server

8.4.27.7.2. Physical Setup

1. Connect each LAN host to a LAN port on a different development board.
2. Connect both boards' WAN ports to the WAN, where a DHCP server is available.

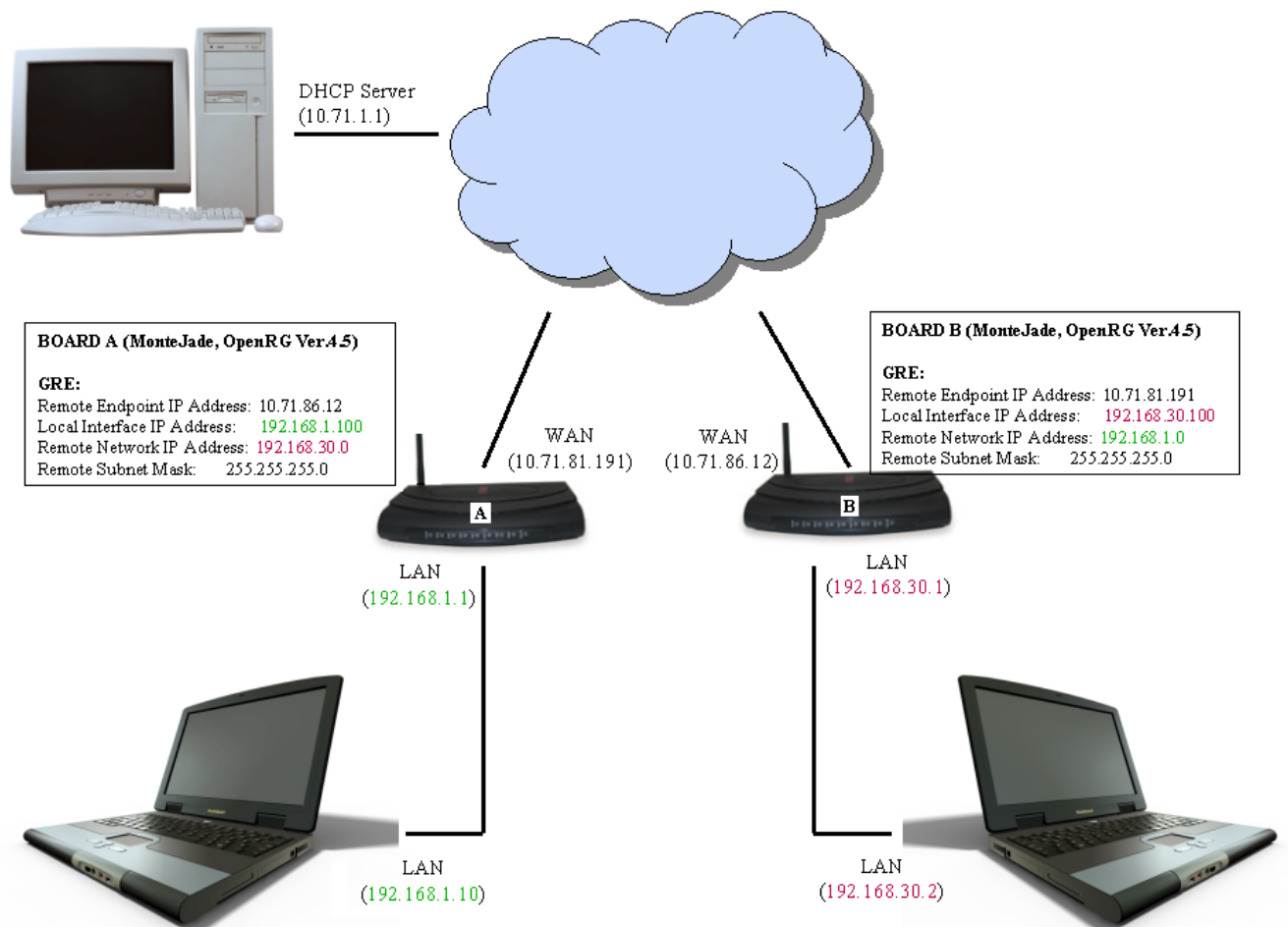


Figure 8.341. Physical Setup

8.4.27.7.3. OpenRG A Configuration

In this example, board A's WAN IP address is 10.71.81.191. In order to create a tunnel, each board must be made aware of the other's WAN IP address (the information must be exchanged).

Create a new GRE tunnel, by performing the following:

1. In the 'Network Connections' screen under 'System' (see [Figure 8.12](#)), click the 'New Connection' link. The 'Connection Wizard' screen appears (see [Figure 8.13](#)).
2. Select the 'Advanced Connection' radio button and click 'Next'. The 'Advanced Connection' screen appears (see [Figure 8.18](#)).
3. Select the 'General Routing Encapsulation (GRE)' radio button and click 'Next'. The 'General Routing Encapsulation (GRE)' screen appears.

Field	Value
Remote Endpoint IP Address:	10 . 71 . 86 . 12
Local Interface IP Address:	192 . 168 . 1 . 100
Remote Network IP Address:	192 . 168 . 30 . 0
Remote Subnet Mask:	255 . 255 . 255 . 0

Figure 8.342. General Routing Encapsulation (GRE)

4. Enter 10.71.86.12 as the tunnel's remote endpoint IP address.
5. Enter 192.168.1.100 as the local IP address of this gateway's GRE interface.
6. Enter 192.168.30.0 as the IP address of the remote network that will be accessed via the tunnel, and 255.255.255.0 as the subnet mask. Click 'Next'.
7. In the 'Connection Summary' screen, select the 'Edit the Connection' check box, and click 'Finish'. The 'WAN GRE Properties' screen appears (see [Figure 8.336](#)).
8. Click the 'Advanced' sub-tab, and deselect the 'Internet Connection Firewall' check box.
9. Click 'OK' to save the settings.

8.4.27.7.4. OpenRG B Configuration

In this example, board B's WAN IP address is 10.71.86.12. In addition, this board's LAN IP address must be different from that of board A (which has the default 192.168.1.1). In this case it is 192.168.30.1.

Create a new GRE tunnel, by performing the following:

1. In the 'Network Connections' screen under 'System' (see [Figure 8.12](#)), click the 'New Connection' link. The 'Connection Wizard' screen appears (see [Figure 8.13](#)).
2. Select the 'Advanced Connection' radio button and click 'Next'. The 'Advanced Connection' screen appears (see [Figure 8.18](#)).
3. Select the 'General Routing Encapsulation (GRE)' radio button and click 'Next'. The 'General Routing Encapsulation (GRE)' screen appears.

Field	1	2	3	4
Remote Endpoint IP Address:	10	71	81	191
Local Interface IP Address:	192	168	30	100
Remote Network IP Address:	192	168	1	0
Remote Subnet Mask:	255	255	255	0

Figure 8.343. General Routing Encapsulation (GRE)

4. Enter 10.71.81.191 as the tunnel's remote endpoint IP address.
5. Enter 192.168.30.100 as the local IP address of this gateway's GRE interface.
6. Enter 192.168.1.0 as the IP address of the remote network that will be accessed via the tunnel, and 255.255.255.0 as the subnet mask. Click 'Next'.
7. In the 'Connection Summary' screen, select the 'Edit the Connection' check box, and click 'Finish'. The 'WAN GRE Properties' screen appears (see [Figure 8.336](#)).
8. Click the 'Advanced' sub-tab, and deselect the 'Internet Connection Firewall' check box.
9. Click 'OK' to save the settings.

8.4.27.7.5. Running the Scenario

After verifying that each host had properly received an IP address in the subnet of its respective gateway, send a ping from host A (192.168.1.10) to host B (192.168.30.2). If the GRE connection is successful, host B should reply.

8.5. Monitor

8.5.1. Network

The Monitoring screen displays a table summarizing the monitored connection data (see [Figure 8.344](#)). OpenRG 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).

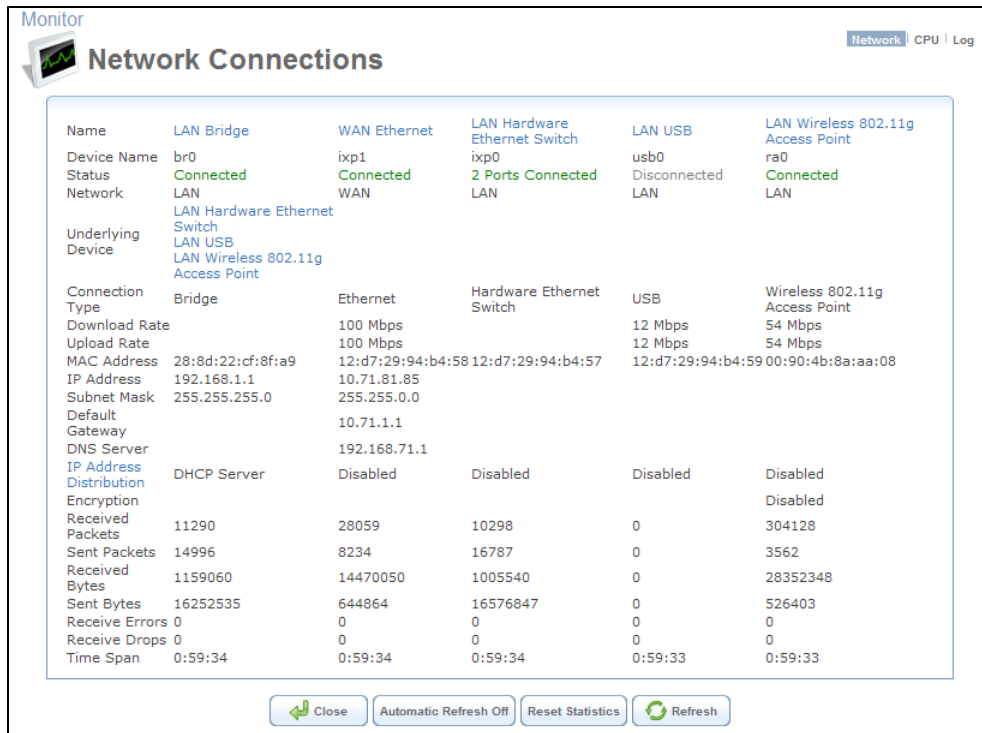


Figure 8.344. Monitoring Connections

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

8.5.2. CPU

The 'CPU' screen (see [Figure 8.345](#)) displays the following system parameters:

- **System Has Been Up For** The amount of time that has passed since the system was last started.
- **Load Average (1 / 5 / 15 mins.)** The average number of processes that are either in a runnable or uninterruptible state. A process in the runnable state is either using the CPU or waiting to use the CPU. A process in the uninterruptible state is waiting for I/O access, e.g. waiting for the disk. The averages are taken over the three time intervals. The meaning of the load average value varies according to the number of CPUs in the system. This means for example, that a load average of 1 on a single-CPU system means that the CPU was loaded all the time, while on a 4-CPU system this means that the CPU was idle 75% of the time.
- **Processes** A list of processes currently running on OpenRG, and their virtual memory usage. The amount of memory granted for each process is presented with the help of the following parameters:
 - **Total Virtual Memory (VmData)** The amount of memory currently utilized by the running process.

- **Heap size (VmSize)** The total amount of memory allocated for the running process.

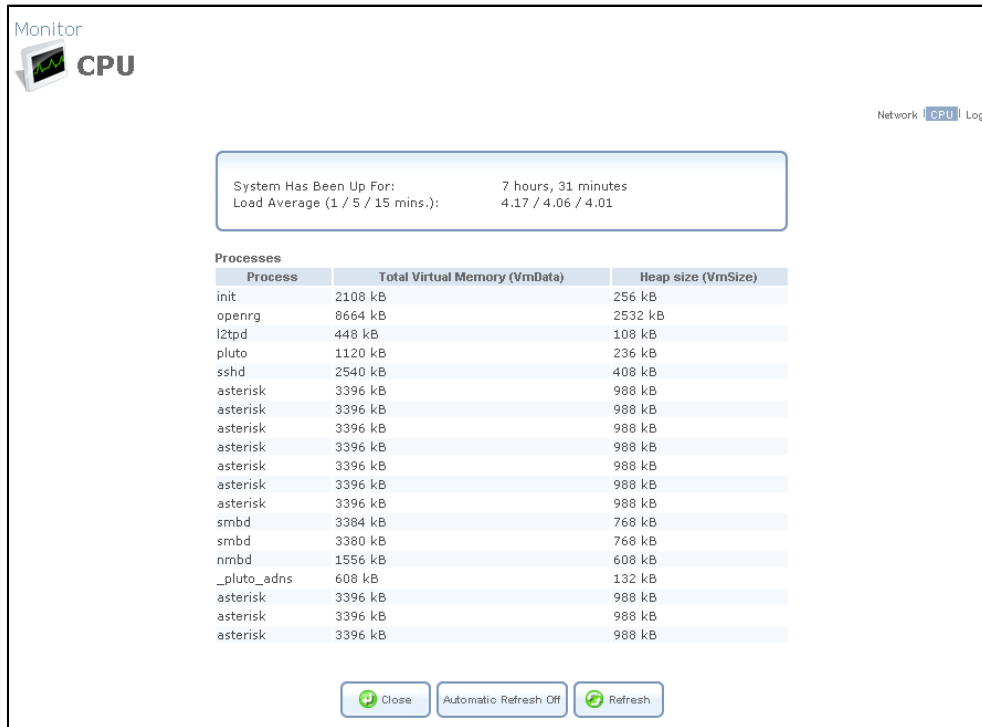


Figure 8.345. CPU Monitoring



Note: Some processes have several child processes. The child processes may be displayed under the same name as the parent one, and use the same memory address space.

The screen is automatically refreshed by default, though you may change this by clicking 'Automatic Refresh Off'.

8.5.3. Log

The 'System Log' screen (see [Figure 8.346](#)) displays a list of recent activities that has taken place on OpenRG.

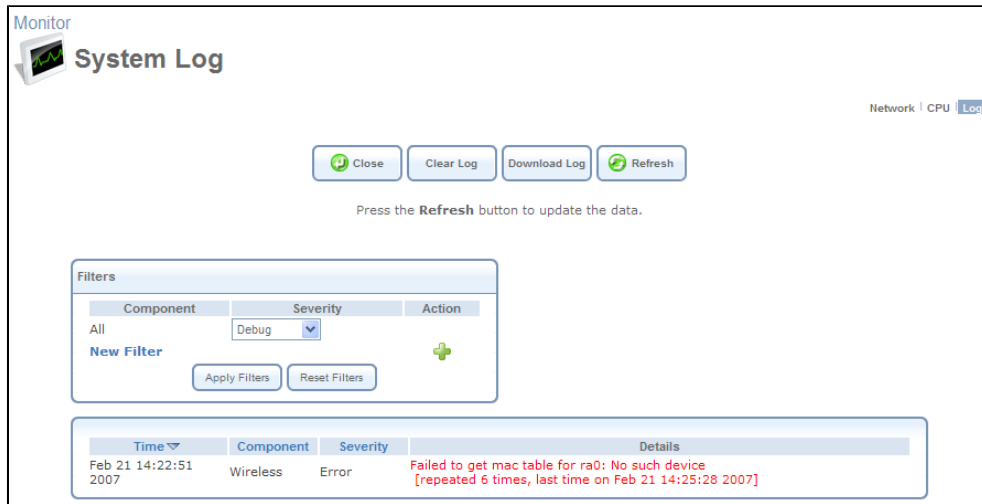


Figure 8.346. System Log


Use the buttons at the top of the page to:

Close Close the 'Log' screen and return to OpenRG's home page.

Clear Log Clear all currently displayed log messages.

Download Log Download the log as a Comma Separated Value (CSV) file, named `openrg_log.csv`.

Refresh Refresh the screen to display the latest updated log messages.

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 OpenRG. By default, the screen displays log messages with 'debug' severity level and higher, for all components (see default filter in [Figure 8.346](#)). You may change the severity level for this filter. To add a new filter, click the 'New Filter' link or its corresponding  action icon. The screen refreshes.

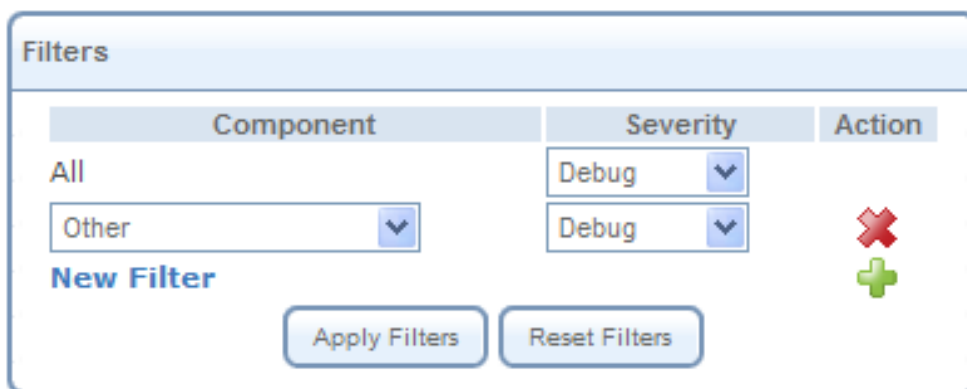



Figure 8.347. System Log Filters

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.



Note: Clicking "Reset Filters" deletes all the defined filters without a warning.

Note that if you would like to view OpenRG's system log in your host's command prompt, you must install and run the syslog server. Then, configure OpenRG with your host's IP address as described in [Section 8.2](#).

8.6. Routing

8.6.1. Overview

Access OpenRG's routing settings by clicking the 'Routing' menu item under the 'System' tab, or by clicking the 'Routing' icon in the 'Advanced' screen. The 'Routing' screen appears in its basic view.

The screenshot shows the 'Routing' configuration page. At the top, there are tabs for 'General', 'IPv6', 'BGP and OSPF', and 'PPPoE Relay'. The 'General' tab is selected. Below the tabs is a 'Routing Table' with a header row containing 'Name', 'Destination', 'Gateway', 'Netmask', 'Metric', 'Status', and 'Action'. A 'New Route' button with a green plus icon is located to the right of the table. Below the table are three sections: 'Routing Information Protocol (RIP)' with an 'Enabled' checkbox and options for 'Poison Reverse' and 'Do not Advertise Direct Connected Routes'; 'Internet Group Management Protocol (IGMP)' with an 'Enabled' checkbox and options for 'IGMP Fast Leave' and 'IGMP Multicast to Unicast'; and 'Domain Routing (add route entry according to interface from which DNS record is received)' with an 'Enabled' checkbox. At the bottom of the page are four buttons: 'OK', 'Apply', 'Cancel', and 'Advanced >>'.

Figure 8.348. Routing – Basic View

To view the advanced routing settings, click the 'Advanced' button.

Routing

General | [IPv6](#) | [BGP and OSPF](#) | [PPPoE Relay](#)

Routing Table

Name	Destination	Gateway	Netmask	Metric	Status	Action
New Route +						

Default Routes

Device	Metric	Status	Action
WAN Ethernet	3	Connected	✎ ✖

Load Balancing

Enabled

DSCP-Based Policy Routing

Route all traffic with matching DSCP values to the chosen devices.
Warning: If the chosen device is marked as a default route, other traffic may also be routed to it.

DSCP	Device	Action
New Route +		

Failover

Enabled

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 (add route entry according to interface from which DNS record is received)

Enabled

Hardware Acceleration

Use Hardware Acceleration When Possible

✔ OK
➕ Apply
✖ Cancel
Basic <<

Figure 8.349. Routing – Advanced View

8.6.1.1. Routing Table

You can add, edit and delete routing rules from the routing table in the manner described in [Section 3.4](#). Note that this table only displays routing rules that you define manually using the WBM, and does not display dynamic rules applied by OpenRG's network connection interfaces, such as IPSec, OSPF, RIP, etc..

To add a routing rule, click the 'New Route' link or the + action icon . The 'Route Settings' screen appears.

Routing
Route Settings

General | IPv6 | BGP and OSPF | PPPoE Relay

Name: LAN Bridge

Destination: 0.0.0.0

Netmask: 255.255.255.255

Gateway: 0.0.0.0

Metric: 0

OK Cancel

Figure 8.350. Route Settings

When adding a routing rule, specify the following:

Name Select the network device.


Destination Enter 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 a route's preference. 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 the order of appearance.

8.6.1.2. Default Routes

OpenRG's default route devices are displayed in the 'Default Routes' section of the 'Routing' screen. You can change the route preference by clicking an entry's  action icon and changing the metric value. If you wish to add an additional (logical) default route device, you must first define a new WAN device that has an IP address.

For example:

1. Define a new PPTP VPN connection over your WAN (to learn how to do so, refer to [Section 8.4.13.2](#)). The 'New Default Route' link appears in the 'Default Routes' section of the 'Routing' screen.




Default Routes				
Device	Metric	Status	Action	
WAN Ethernet	3	Connected		
New Default Route				

Figure 8.351. Default Routes

2. Click the 'New Default Route' link in the 'Default Routes' section. The 'Default Route Settings' screen appears, displaying the new WAN device.

Figure 8.352. Default Route Settings


3. Enter a value for the metric route preference.
4. Click 'OK' to save the settings.

Although multiple devices may be configured as default routes, only one will serve as the default route—the one with the lowest metric value, or, if metric values are identical, the first in order. Defining a single default route is especially important in conjunction with the DSCP-based policy routing (refer to [Section 8.6.1.3.2](#)).

8.6.1.3. Multiple WAN Devices

OpenRG supports platforms with multiple physical WAN devices, which can be used for traffic load balancing, failover, and various routing policies. The multiple WAN features may also be used to define multiple logical devices (e.g. PPTP VPN, PPPoE) on boards with a single WAN device.

- **Load balancing** means that you may choose to balance the traffic load between the two WAN devices (refer to [Section 8.6.1.3.1](#)).
- **DSCP-based policy routing** means that you may specify that all traffic matching a certain DSCP value will be routed to a chosen device (refer to [Section 8.6.1.3.2](#)).
- **Failover** means that traffic will be routed to an active WAN device in case its current WAN device fails, ensuring connectivity (refer to [Section 8.6.1.3.3](#)).

 Note: DSCP-based policy routing takes precedence over load balancing. In addition, if WAN failover occurs, it will take place on the remaining non-DSCP directed traffic only.

8.6.1.3.1. Load Balancing

Load balancing provides the ability to use the bandwidth of two parallel WAN devices for distributing traffic. Load balancing uses the IP pairs technique, in which traffic between a

pair of source and destination IP addresses is routed to the same WAN device for a certain timeframe. A router load balancing on a per-destination basis uses the parallel routes in a round-robin fashion, and forwards an entire destination-based flow in each pass.



Note: Only default route devices (refer to [Section 8.6.1.2](#)) can participate in load balancing.

To enable load balancing between multiple WAN devices, perform the following:

1. Select the 'Enabled' check box in the 'Routing' screen (see [Figure 8.349](#)). The screen refreshes, displaying the load balancing table.

Load Balancing

Enabled

Device	Weight	Action
<input type="checkbox"/> WAN Ethernet	1	
<input type="checkbox"/> WAN Ethernet 2	1	

Figure 8.353. Load Balancing

2. Select the devices on which load balancing will be performed by selecting their respective check boxes.
3. You may also control the weight of each device in the balancing procedure, which determines the ratio of IP pairs provided to each device:
 - a. Click the action icon of the device. The 'Edit Weight of Device' screen appears.

Routing

Edit Weight of Device

General | IPv6 | BGP and OSPF | PPPoE Relay

Device: WAN Ethernet

Weight: 1

OK Cancel

Figure 8.354. Edit Weight of Device

- b. Enter the numeric ratio that will represent the weight of the device.
 - c. Click 'OK' to save the settings.
4. Click 'OK' to save the settings.

8.6.1.3.2. DSCP-Based Policy Routing

DSCP-based policy routing provides the ability to send specific traffic out of a specific WAN device. This is useful for routing different types of data to different WAN devices. It is also

useful if you would like to segregate the voice traffic from the data traffic over two lower-cost broadband circuits in an effort to have better voice quality.

To add a DSCP-based policy route, perform the following:

1. Click the 'New Route' link. The 'Add a DSCP-Based Route to a Device' screen appears.

The screenshot shows a web-based configuration interface for adding a DSCP-based route. At the top left, there is a 'Routing' logo. The main heading is 'Add a DSCP-Based Route to a Device'. Below the heading, there are tabs for 'General', 'IPv6', 'BGP and OSPF', and 'PPPoE Relay'. The 'General' tab is active. In the center, there is a form with two fields: 'Device' with a dropdown menu showing 'WAN Ethernet' and 'DSCP' with a text input field containing '24'. At the bottom of the form, there are two buttons: 'OK' (with a green checkmark) and 'Cancel' (with a red X).

Figure 8.355. Adding a DSCP-Based Route to a Device

2. Select the network device from the drop-down menu.
3. Specify the DSCP value. All traffic matching this DSCP value will be routed to the chosen device.
4. Click 'OK' to save the settings.

You can mark certain traffic with DSCP values of your choice, as explained in [Section 8.4.24.5](#)). The DSCP-based policy routing ensures that specified traffic is routed via a certain WAN device, but if this WAN device is defined as the default route, other traffic may also be routed through it. If you want your device to be dedicated to transmitting only traffic matching the DSCP value you specified, you must deselect the default route check box for that device.

DSCP-based policy routing takes precedence over load balancing, so if most of the traffic falls under the DSCP-based policy routing rules, it will be forwarded accordingly, regardless of the load balancing. Load balancing, in this case, will be a best-effort load balancing, and will balance the remaining traffic not directed by the DSCP-based policy routing rules.

8.6.1.3.3. Failover

Failover is the transfer of operation from a failed device to a similar, reserved device to ensure uninterrupted data flow and operability. OpenRG supports WAN failover on multiple WAN platforms.

WAN failover takes place when a WAN device fails due to disconnection or an unsuccessful DNS test. This means that if the WAN Ethernet 1 device fails, its routing rules are removed, and all traffic will now be routed through WAN Ethernet 2 according to its routing scheme, until WAN Ethernet 1 resumes its connectivity. It is recommended to use this feature in conjunction with default route rules defined on both devices.

OpenRG supports the following types of failover:

- **Full Link Redundancy** Two or more active WAN devices, usually with equal speed, must be configured. During normal operation, traffic is routed through them according to route rules, or load balancing. If one of the devices fails, the next one will take its place.
- **Rollover Connection** During uptime, a rollover device is kept inactive. This is usually a slow link, for example, a dialup. When all other failover devices lose connectivity, the rollover device will become active automatically, and may keep the same IP as the main device. This allows to use a slow connection as a backup to the main fast connection. When a failed device regains connectivity, the rollover device will become inactive again. Note that if dialup is done by demand, activating the backup device may take a noticeable amount of time.

The failover process consists of three phases:

1. **Detection** – performed using a DNS test.
2. **Action** – when a DNS test fails, the failover process simply removes the route records of the failed connection. This enables you to reach the desired failover behavior by configuring OpenRG's routing rules correctly.
3. **Recover** – during failover, tests continue to run on the failed connection. When a test succeeds, the connection will recover its route records.

Failover scenarios:

- **Inbound Failover** A common problem occurs when a connection fails, and its IP is no longer accessible. This is referred to as Inbound Failover, and is resolved by informing the other party to use a different IP, using Dynamic DNS.
- **IPSec** (Also, refer to [Section 7.10.1.3](#)) When an IPSec underlying connection loses connectivity or fails connectivity tests, the following scenarios are possible:
 1. In case an IPSec template is available, traffic will be received from all WAN devices.
 2. In case an IPSec connection is defined, and:
 - a. No underlying connection is configured—the IPSec connection will disconnect and attempt to reconnect while choosing the underlying connection according to existing route rules.
 - b. An underlying connection is configured—the behavior will be similar, with the exception that the chosen underlying connection may only be a failover connection to the configured underlying connection. If you wish to force IPSec to use the configured underlying connection without failover, do not configure the underlying connection as a failover connection.
 3. At the recover stage, if:

- a. No underlying connection is configured—OpenRG assumes that the WAN connection used as the underlying connection is unimportant. Hence, the IPSec connection will not disconnect from its current device.
- b. An underlying connection is configured—the IPSec connection will always try to go back to its configured underlying device. It will disconnect, and return to the recovered WAN connection.

To enable failover between multiple WAN devices, perform the following:

1. Select the 'Enabled' check box in the 'Routing' screen (see [Figure 8.349](#)). The screen refreshes, displaying the failover table.

Failover

Enabled

Device	Status	Connectivity Check	Rollover Connection	Action
Add Device				

Figure 8.356. Failover

2. Click the 'Add Device' link to add a failover device. The 'Add Failover Device' screen appears.

Routing

Add Failover Device

General | IPv6 | BGP and OSPF | PPPoE Relay

Device:

Rollover Connection

Use DNS Lookup to Check Connectivity

DNS Lookup Host:

Figure 8.357. Add Failover Device

Device Select the WAN device you would like to configure as failover.

Rollover Connection Select this check box to configure the WAN device as a rollover connection type of failover.

Use DNS Lookup to Check Connectivity Select this check box to enable a periodic connectivity check using a DNS query.

DNS Lookup Host If you selected the previous check box, enter the URL that the periodic check will query.

3. Click 'OK' to save the settings.

In order to clarify the use of failover, following are failover use-cases that depict actual uses of this feature. These use-cases assume that you are running a multiple WAN platform with at least two WAN devices.

- **Redundancy** In the 'Routing' screen (see [Figure 8.349](#)), perform the following steps:
 1. In the 'Default Routes' section, define WAN Ethernet (WAN 1) as a default route with metric 3.

The screenshot shows the 'Default Route Settings' dialog box in the Routing section. The 'Device' field is set to 'WAN Ethernet' and the 'Metric' field is set to '3'. The dialog has 'OK' and 'Cancel' buttons at the bottom.

Figure 8.358. WAN 1 Default Route Settings

2. Similarly, define WAN Ethernet 2 (WAN 2) as a default route with metric 5.

The screenshot shows the 'Default Route Settings' dialog box in the Routing section. The 'Device' field is set to 'WAN Ethernet 2' and the 'Metric' field is set to '5'. The dialog has 'OK' and 'Cancel' buttons at the bottom.

Figure 8.359. WAN 2 Default Route Settings

3. In the 'Routing Table' section, click the 'New Route' link to define a route rule for WAN 2, with destination 192.168.71.0, netmask 255.255.255.0, and gateway 192.168.71.1.

The screenshot shows the 'Route Settings' dialog box in the Routing section. The 'Name' is set to 'WAN Ethernet 2'. The 'Destination' is '192.168.71.0', 'Netmask' is '255.255.255.0', 'Gateway' is '192.168.71.1', and 'Metric' is '0'. The dialog has 'OK' and 'Cancel' buttons at the bottom.

Figure 8.360. WAN 2 Route Rule

- In the 'Failover' section, add both devices to the failover table, defining them with DNS connectivity checks set to <http://www.google.com>.

Figure 8.361. Add Failover Device

- Click 'OK' to save the settings.

When both connections are active, the default route will be WAN 1, while WAN 2 will be used merely for access to destination 192.168.71.0. If WAN 1 fails, its route records will be deleted, and WAN 2 will become the default route, handling all traffic.

- Full Link Redundancy with Load Balancing** This use-case is similar to the previous one, but with load balancing between the default routes.

- Define all settings according to the previous use-case.
- In the 'Load Balancing' section, select the check boxes of both WAN 1 and WAN 2.

Load Balancing

Enabled

Device	Weight	Action
<input checked="" type="checkbox"/> WAN Ethernet	1	
<input checked="" type="checkbox"/> WAN Ethernet 2	1	

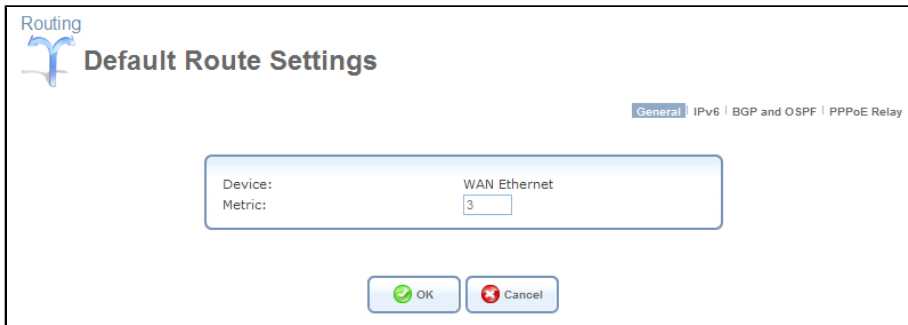
Figure 8.362. Load Balancing

- Click 'OK' to save the settings.

When both connections are active, both will share the traffic, except for traffic to 192.168.71.0, which will only be redirected to WAN 2. If one of the devices fails, the other will instantly take responsibility over all traffic.

- Rollover**

- In the 'Default Routes' section, click the 'New Default Route' link to define WAN 1 as a default route with metric 3.



Routing
Default Route Settings

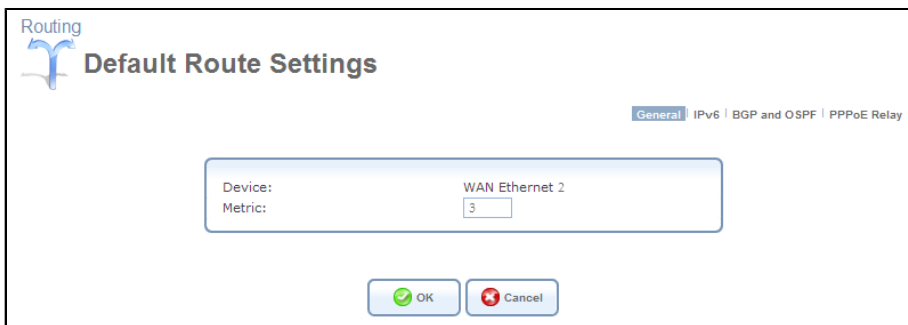
General | IPv6 | BGP and OSPF | PPPoE Relay

Device: WAN Ethernet
Metric: 3

OK Cancel

Figure 8.363. WAN 1 Default Route Settings

2. Similarly, define WAN 2 as a default route with metric 3.



Routing
Default Route Settings

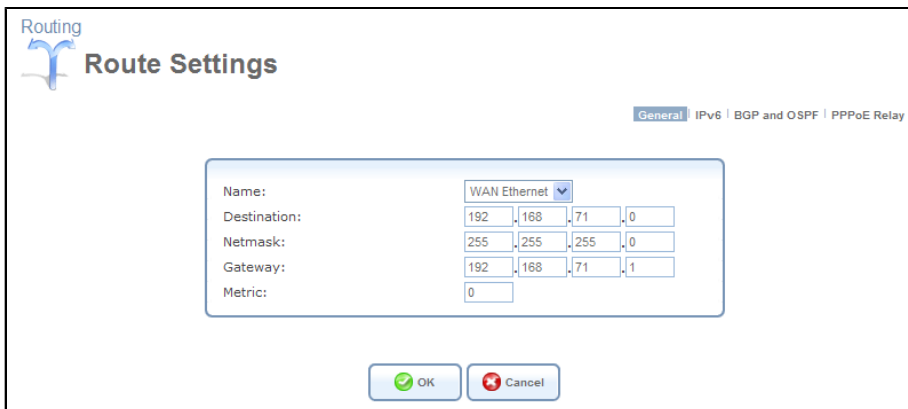
General | IPv6 | BGP and OSPF | PPPoE Relay

Device: WAN Ethernet 2
Metric: 3

OK Cancel

Figure 8.364. WAN 2 Default Route Settings

3. In the 'Routing Table' section, click the 'New Route' link to define a route rule for WAN 1, with destination 192.168.71.0, netmask 255.255.255.0, and gateway 192.168.71.1.



Routing
Route Settings

General | IPv6 | BGP and OSPF | PPPoE Relay

Name: WAN Ethernet

Destination: 192.168.71.0
Netmask: 255.255.255.0
Gateway: 192.168.71.1
Metric: 0

OK Cancel

Figure 8.365. WAN 1 Route Rule

4. In the 'Failover' section, add WAN 1 to the failover table, defining it with a DNS connectivity check set to <http://www.google.com>.

Routing **Add Failover Device**

General | IPv6 | BGP and OSPF | PPPoE Relay

Device: WAN Ethernet

Rollover Connection

Use DNS Lookup to Check Connectivity

DNS Lookup Host: www.google.com

OK Cancel

Figure 8.366. WAN 1 Failover Settings

- Similarly, add WAN 2, defining it as a rollover connection.

Routing **Add Failover Device**

General | IPv6 | BGP and OSPF | PPPoE Relay

Device: WAN Ethernet 2

Rollover Connection

Use DNS Lookup to Check Connectivity

DNS Lookup Host:

OK Cancel

Figure 8.367. WAN 2 Failover Settings

- Click 'OK' to save the settings.

Regularly, only WAN 1 will be active, handling all traffic, while WAN 2 is dormant. If WAN 1 fails, WAN 2 will become active. In case WAN 2 is a dialup device, it will start a dialup session with the ISP. After establishing a connection, it will become the default route, since its default route record is the only one remaining active. Should WAN 1 become active again, WAN 2 will recognize that it is no longer needed, and will shut down.

8.6.1.4. 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.

- **Poison Reverse** OpenRG will advertise acquired route information with a high metric, in order for other routers to disregard it.
- **Do not Advertise Direct Connected Routes** OpenRG will not advertise the route information to the same subnet device from which it was obtained.

Internet Group Management Protocol (IGMP) OpenRG provides support for the IGMP multicasting. When a host sends out a request to join a multicast group, OpenRG will listen and intercept the group's traffic, forwarding it to the subscribed host. OpenRG keeps record of subscribed hosts. When a host requests to cancel its subscription, OpenRG queries for other subscribers and stops forwarding the multicast group's traffic after a short timeout.

- **Enable IGMP Fast Leave** If a host is the only subscriber, OpenRG will stop forwarding traffic to it immediately upon request (there will be no query delay).
- **IGMP Multicast to Unicast** Enables OpenRG to convert the incoming multicast data stream into unicast format, in order to route it to the specific LAN host that had requested the data. In this way, OpenRG will prevent flooding the rest of the LAN hosts with irrelevant multicast traffic.

Domain Routing When OpenRG'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.

8.6.1.5. Hardware Acceleration

The Hardware Acceleration feature utilizes the **Fastpath** algorithm, which enhances packet flow, resulting in faster communication between the LAN and the WAN (excluding the wireless connection). By default, this feature is enabled.

8.6.2. IPv6

At the current stage of the IP network technology, an IPv4 WAN has no inherent support of Internet Protocol version 6 (IPv6). As a result, two IPv6 hosts cannot communicate with each other directly, if they are located at two separate IPv6 LANs interconnected by an IPv4 WAN (either the global Internet or a corporate WAN).

The easiest way to solve this problem is to establish a special network mechanism, called *IPv6-over-IPv4 Tunneling*. This mechanism encapsulates IPv6 packets into IPv4 packets, in order to transmit them via an IPv4 WAN to the target IPv6 host. OpenRG successfully implements the IPv6 technology.

The following scenario demonstrates how to establish communication between two IPv6 hosts via OpenRG. Each host belongs to a separate IPv6 network. The two networks are interconnected by an IPv4 WAN. For convenience, let's call the two machines Host **A** and Host **B**. In the same fashion, let's call the two gateways, connected to the host machines, OpenRG **A** and OpenRG **B** respectively.

The following diagram outlines this scenario.

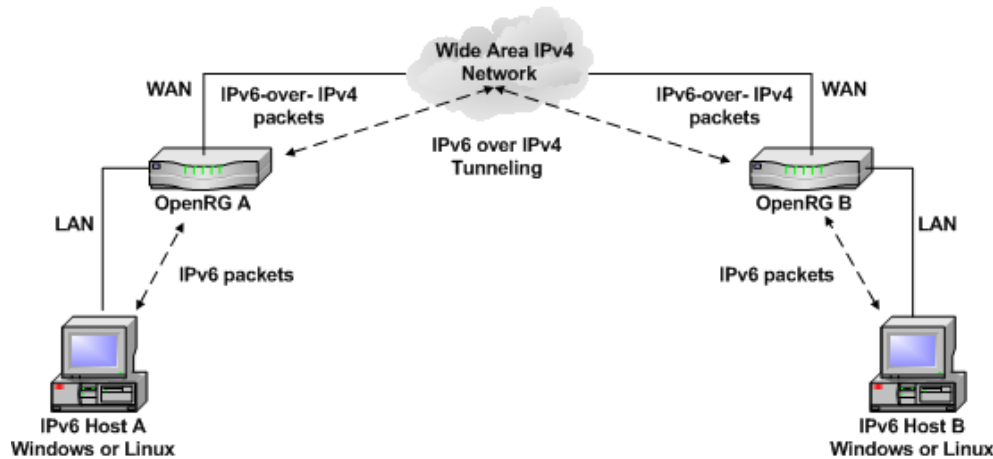


Figure 8.368. IPv6-over-IPv4 Tunneling via OpenRG

There are several variations of the IPv6 network setup, depending on the operating system installed on the host machines. OpenRG's IPv6 feature enables you to establish an IPv6 network between:

- Linux hosts
- Windows hosts
- Linux and Windows hosts



Note: The following instructions should be followed at both ends of the IPv6-over-IPv4 tunnel, otherwise the packets will travel only in a single direction.

After connecting the IPv6 hosts to their gateways at both locations, perform the following:

1. Configure the gateways to support the IPv6-over-IPv4 tunneling.
2. Configure the IPv6 hosts according to the parameters defined in their gateways.

The following sections describe each of these steps.

8.6.2.1. Setting up the IPv6-over-IPv4 Tunneling in OpenRG

This setup procedure consists of the following steps:

- Enabling the IPv6 feature
 - Adding a new LAN subnet to the LAN bridge and configuring its settings
 - Configuring the IPv6-over-IPv4 tunnel settings
1. Verify that the IPv6 feature is enabled in each of the gateways, by performing the following:

- a. Click the 'IPv6' icon in the 'Advanced' screen of the WBM. If the feature is disabled, the following screen appears.

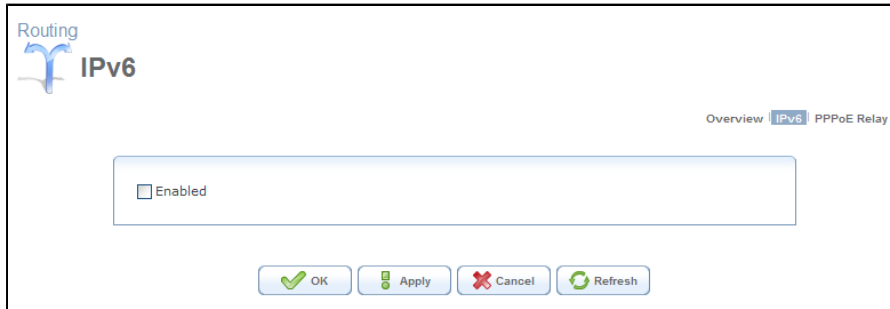


Figure 8.369. Disabled IPv6

- b. Select the 'Enabled' check box. The screen refreshes, changing to the following.

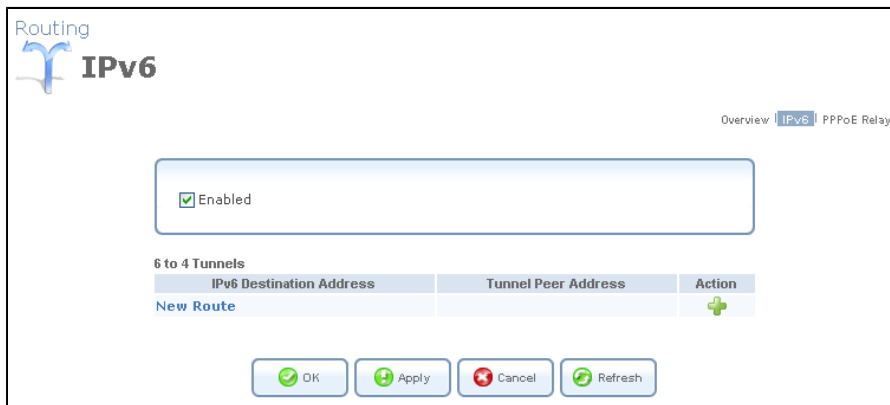


Figure 8.370. Enabled IPv6

- c. Click 'Apply' to save the settings.
2. Add a new LAN subnet to the LAN bridge by performing the following:
- a. In the WBM, click the 'System' tab, and then click the 'Network Connections' menu item. The 'Network Connections' screen appears.

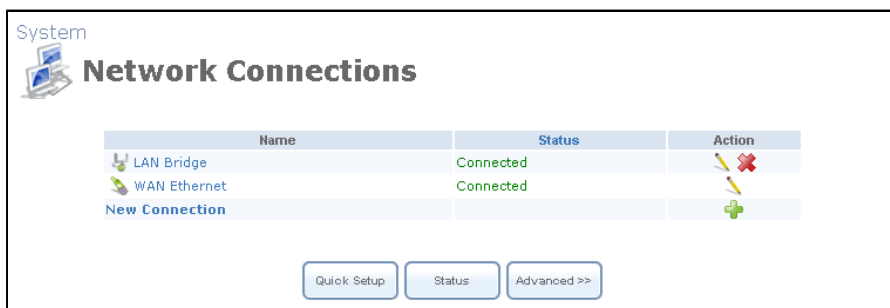


Figure 8.371. Network Connections

- b. Click the 'LAN Bridge' link. The 'LAN Bridge Properties' screen appears.

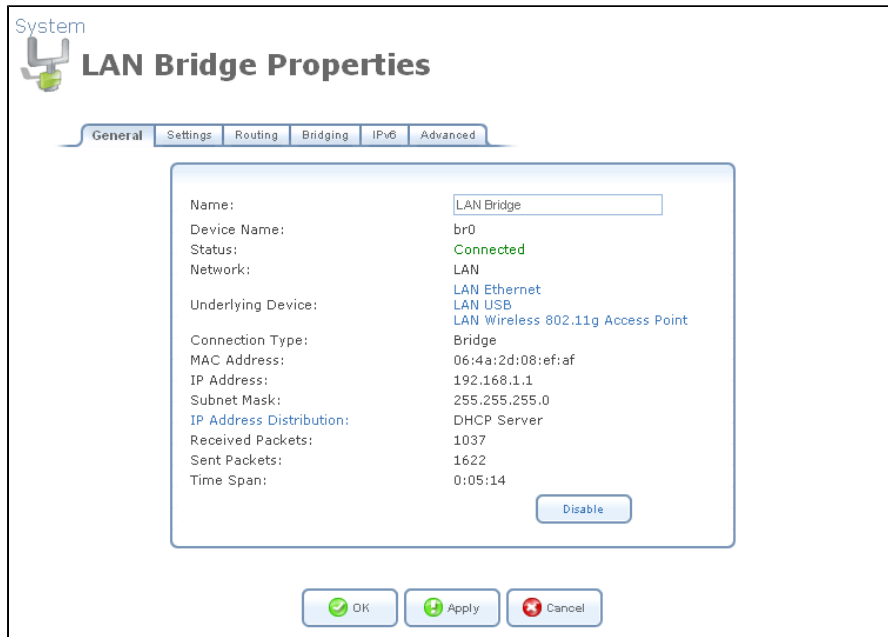


Figure 8.372. LAN Bridge Properties

- c. Click the 'IPv6' link. The IPv6 settings screen appears.

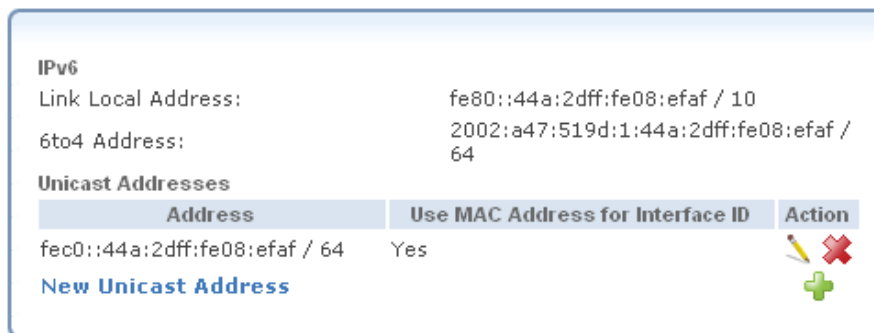


Figure 8.373. IPv6 Settings

- d. Click the 'New Unicast Address' link. Alternatively, click its  action icon. The 'IPv6 Unicast Address' screen appears.

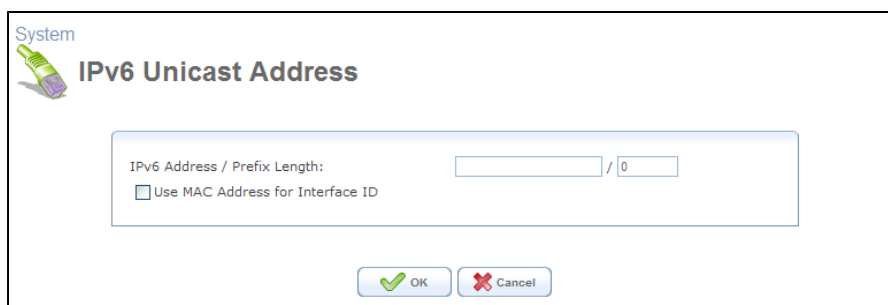


Figure 8.374. IPv6 Unicast Address Parameters

- e. In the 'IPv6 Address/Prefix Length' field, enter the IPv6 address of the new LAN subnet and its prefix length. For example, assign the following IPv6 address to the LAN subnet of OpenRG A: `fec0::100:aaaa:bbbb:cccc:dddd/64`

The `fec0` part shows that this is a *Site-Local* address (an IPv6 address within a LAN). The `100` part is the ID number of the subnet. The next four parts (represented with letters) are unrestricted, unless they are generated from the gateway's MAC address. The `64` part is the prefix length.



Note: The 'IPv6 Unicast Address' screen contains the 'Use MAC Address for Interface ID' option. If it is enabled, OpenRG generates the lower 64 bits of the IPv6 address from its MAC address.

- f. Click 'OK' to save the setting, and to return to the 'LAN Bridge Properties' screen.
- g. Verify that the new subnet has received the unicast address.

In the same way as described above, define a new subnet in OpenRG

B. For example, assign the following IPv6 address to this subnet:

`fec0::200:aaaa:bbbb:cccc:dddd/64`

3. Configure the IPv6-over-IPv4 tunnel in **each of the gateways**. For example, to configure the tunnel in OpenRG A, perform the following:
- a. In the 'IPv6' settings screen (see [Figure 8.370](#)), click the 'New Route' link to specify the IPv6-over-IPv4 tunnel parameters. The 'Set IPv6 Tunnel' screen appears.

Figure 8.375. IPv6 Tunnel Parameters

- b. In the 'IPv6 Destination Address/Prefix Length' field, specify the IPv6 address of the OpenRG B LAN subnet.
- c. In the 'Tunnel Peer IP Address' fields, enter the WAN IP of OpenRG B.
- d. Click 'OK' to save the settings.

In the same fashion, configure OpenRG B.

8.6.2.2. Setting up the IPv6 Network Connection on a Linux Host

This setup procedure consists of the following steps:

- Adding IPv6 support, if not yet enabled
- Adding the new LAN subnet defined in OpenRG
- Creating an IPv6 routing rule

1. Verify that the Linux host supports IPv6, by performing the following:

- a. Open a shell and switch to the root user, by entering the `su` command.
- b. Enter the following command:

```
lsmmod | grep ipv6
```

If the command returns no result, it means that IPv6 support is disabled. To enable IPv6 support, enter the following command as the root user:

```
insmod ipv6
```

2. Add the IPv6 address defined in the new LAN subnet to the host's network settings. For example, assign the IPv6 address of the OpenRG **A** LAN subnet to the Host **A** network device. To do so, run the following command as the root user:

```
ip -6 addr add fec0::100:1111:2222:3333:4444/64 dev <Host A LAN connection label>
```



Note: To check the network connection label in Linux, run the `ifconfig` command.

If Host **B** runs Linux too, follow the procedure described above. In this case, however, you must specify the IPv6 address defined in the OpenRG **B** LAN subnet, and enter the network connection label of the Host **B** machine.

3. Add a routing rule directing the host's outgoing IPv6 packets to OpenRG, which will route them to the destination. For example, to add this routing rule to the network settings of Host **A**, run the following command as the root user:

```
ip -6 route add fec0::200:1111:2222:3333:4444/64 via fec0::100:aaaa:bbbb:cccc:dddd  
dev <Host A LAN connection label>
```

If Host **B** runs Linux too, go to its shell and run the following command as the root user:

```
ip -6 route add fec0:0:0:100:1111:2222:3333:4444/64 via fec0::200:aaaa:bbbb:cccc:dddd  
dev <Host B LAN connection label>
```

To test the connection, ping through the IPv6-over-IPv4 tunnel.

- In Linux Host **A** run:

```
ping6 -I <LAN connection label> fec0::200:1111:2222:3333:4444
```

- In Linux Host **B** run:


```
ping6 -I <LAN connection label> fec0::100:1111:2222:3333:4444
```

The following are additional commands for testing the IPv6 connection:

- To show the IPv6 routing table, enter:

```
ip -6 route
```

- To show the network device's IPv6 address, enter:

```
ip -6 addr
```

If the second host runs Windows, refer to [Section 8.6.2.3](#) for explanations about configuring a Windows host.

8.6.2.3. Setting up the IPv6 Network Connection on a Windows Host

This setup procedure consists of three steps:

- Adding IPv6 support, if not yet enabled
- Adding the new LAN subnet defined in OpenRG
- Creating an IPv6 routing rule



Note: The following description is based on the GUI of Windows XP. For information about installing IPv6 on other Windows versions, visit the Microsoft Web site.

1. Verify that the host running Windows supports IPv6, by performing the following:
 - a. In 'Control Panel', double-click the 'Network Connections' icon. The 'Network Connections' window appears.
 - b. In the 'Network Connections' window, right-click the network connection label (the default label is 'Local Area Connection') and select 'Properties'. The following window appears.

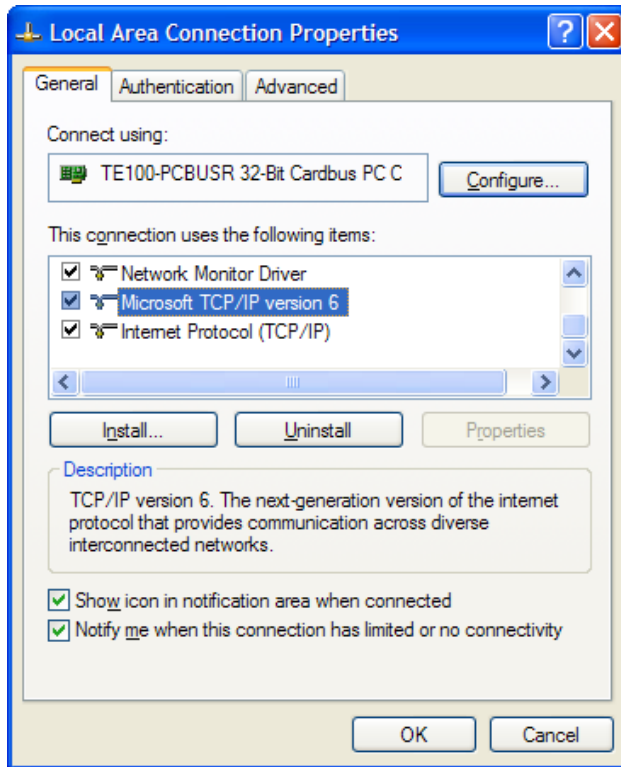


Figure 8.376. Network Connection Properties

- c. Ensure that the 'General' tab is selected, and check if the list of connection options contains the following item: 'Microsoft TCP/IP version 6'. If the list contains this item (IPv6 is installed), verify that its check box is selected and proceed to the next step. Otherwise, install IPv6:

- i. In the 'Start' menu, select 'Run'. The 'Run' window appears.
- ii. In the 'Open' field, enter `cmd` and click 'OK'. The command prompt window appears.
- iii. In the command prompt window, enter the following command:

```
ipv6 install
```

The command initiates the Microsoft TCP/IP version 6 installation. This is an automatic process.

2. Add the IPv6 address of the new LAN subnet to the host's network settings. For example, assign the IPv6 address of the OpenRG A LAN subnet to the Host A network device, by performing the following:

- a. In the command prompt window, run the following command:

```
netsh
```

Netsh is a command-line scripting utility that enables you to modify your computer network configuration.

- b. In the `netsh` context, run the following command:

```
interface ipv6
```

- c. In the `interface ipv6` context, run the following command:

```
add "<Host A LAN connection label>" fec0::100:1111:2222:3333:4444
```



Note: The default LAN connection label in Windows is 'Local Area Connection'.

- d. Enter the following command:

```
add route fec0::100:aaaa:bbbb:cccc:dddd/64 "<Host A LAN connection label>"
```

If Host **B** runs Windows too, follow the procedure described above, with the only difference that you must specify the IPv6 address of the OpenRG **B** LAN subnet.

3. Add a routing rule directing the host's outgoing IPv6 packets to OpenRG, which will route them to the destination. For example, to add this routing rule to the network settings of Host **A**, run the following command in the 'interface ipv6' context:

```
add route fec0::200:1111:2222:3333:4444/64 interface=<Host A LAN connection label>  
nexthop=fec0::100:aaaa:bbbb:cccc:dddd
```

If Host **B** runs Windows too, run the following command in the 'interface ipv6' context:

```
add route fec0::100:1111:2222:3333:4444/64 interface=<Host B LAN connection label>  
nexthop=fec0::200:aaaa:bbbb:cccc:dddd
```

To ping through the IPv6-over-IPv4 tunnel, run the following command:

```
ping6 fec0::200:1111:2222:3333:4444/64
```

If the second host runs Linux, refer to [Section 8.6.2.2](#) for explanations about configuring a Linux host.

8.6.3. BGP and OSPF

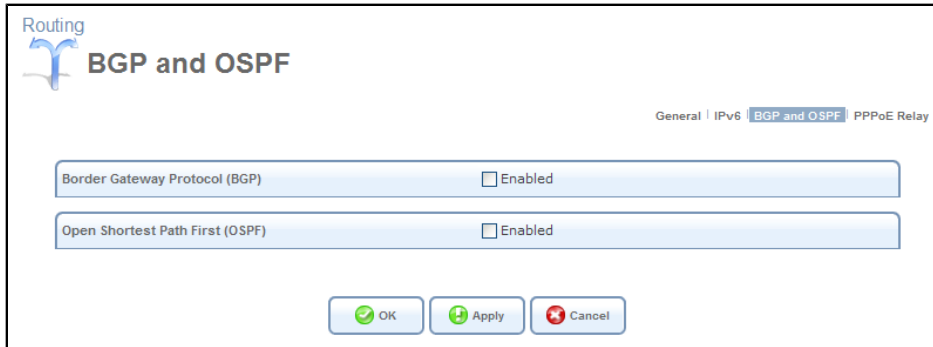
The 'BGP and OSPF' feature is an implementation of two routing protocols used to deliver up-to-date routing information to a network or a group of networks, called *Autonomous System*.

Border Gateway Protocol (BGP) The main routing protocol of the Internet. It is used to distribute routing information among Autonomous Systems (for more information, refer to the protocol's RFC at <http://www.ietf.org/rfc/rfc1771.txt>).

Open Shortest Path First Protocol (OSPF) An Interior Gateway Protocol (IGP) used to distribute routing information within a single Autonomous System (for more information, refer to the protocol's RFC at <http://www.ietf.org/rfc/rfc2328.txt>).


The feature's routing engine is based on the *Quagga* GNU routing software package. By using the BGP and OSPF protocols, this routing engine enables OpenRG to exchange routing information with other routers within and outside an Autonomous System. To enable this feature, perform the following:

1. In the 'Routing' screen, click the 'BGP and OSPF' link. The 'BGP and OSPF' screen appears.

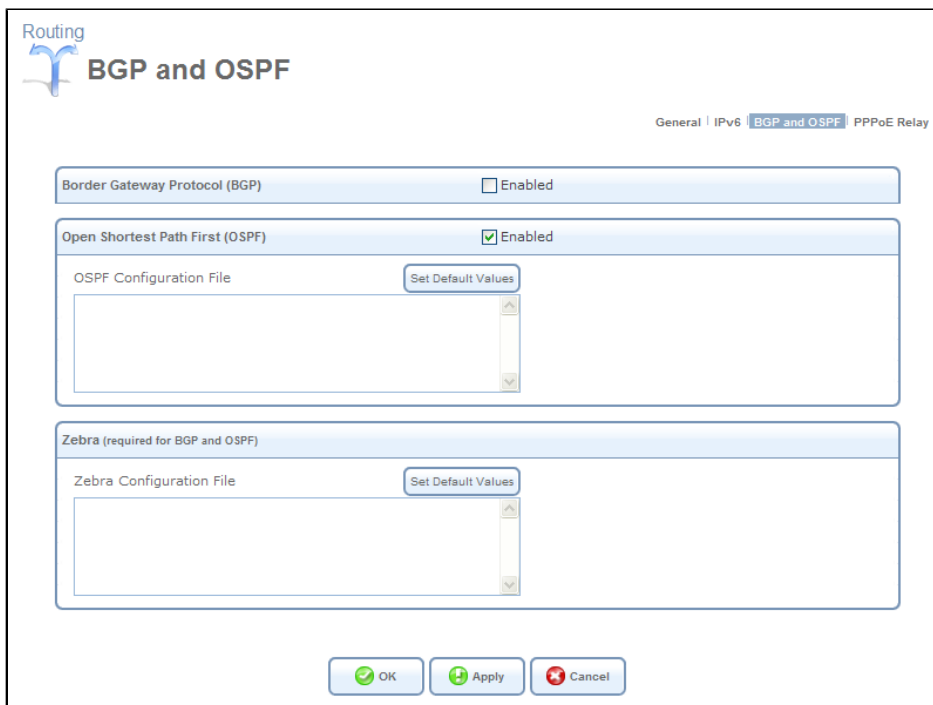


The screenshot shows the 'BGP and OSPF' configuration page. At the top, there is a 'Routing' logo and the title 'BGP and OSPF'. Below the title, there are two tabs: 'General' and 'BGP and OSPF'. The 'BGP and OSPF' tab is selected. There are two main sections: 'Border Gateway Protocol (BGP)' and 'Open Shortest Path First (OSPF)'. Each section has an 'Enabled' checkbox, which is currently unchecked. At the bottom, there are three buttons: 'OK', 'Apply', and 'Cancel'.

Figure 8.377. BGP and OSPF

 Note: Depending on its purpose of use, OpenRG may support both of the protocols or only one of them.

2. Select the 'Enabled' check box of the supported protocol(s). For example, enable OSPF. The screen refreshes, changing to the following.



The screenshot shows the 'BGP and OSPF' configuration page after OSPF has been enabled. The 'Enabled' checkbox for 'Open Shortest Path First (OSPF)' is now checked. Below the 'OSPF' section, there is a 'Zebra (required for BGP and OSPF)' section. Both sections have a 'Set Default Values' button and a text area for configuration files. At the bottom, there are three buttons: 'OK', 'Apply', and 'Cancel'.

Figure 8.378. Enabled OSPF

To activate the routing engine, you need to create a configuration file for the protocol daemon, and also for *Zebra*. *Zebra* is Quagga's IP routing management daemon, which provides kernel routing table updates, interface lookups, and redistribution of routes between the routing protocols.



Note: To view examples of the configuration files, browse to <http://www.quagga.net/docs/quagga.pdf>.

3. Enter the configuration files into their respective code fields. Alternatively, click the 'Set Default Values' button to the right of each code field. The default values, displayed in a field are the following:

- **BGP :**

!router bgp <AS number> The exclamation mark is Quagga's comment character. The `router bgp` string is a command that activates the BGP daemon. The exclamation mark emphasizes that the command must be followed by an exact Autonomous System's ID number.

log syslog A command that instructs the daemon to send its log messages to the system log.

- **OSPF :**

router ospf A command that activates the OSPF daemon.

log syslog See the explanation under BGP.

- **Zebra**

interface ixp1 Instructs the daemon to query and update routing information via a specific WAN device. It is important that you change the default `ixp1` value to your WAN device name.

log syslog See the explanation under BGP.

4. Click 'OK' to save the settings.

If the OSPF daemon is activated, OpenRG starts sending the 'Hello' packets to other routers to create adjacencies. After determining the shortest path to each of the neighboring routers, Zebra updates the routing table according to the network changes. If the BGP daemon is activated, OpenRG starts to advertise routes it uses to other BGP-enabled network devices located in the neighboring Autonomous System(s). The BGP protocol uses TCP as its transport protocol. Therefore, OpenRG first establishes a TCP connection to routers with which it will communicate. *KeepAlive* messages are sent periodically to ensure the liveness of the connection. When a change in the routing table occurs, OpenRG advertises an *Update* message to its peers. This update message adds a new route or removes the unfeasible one from their routing table.

8.6.4. PPPoE Relay

PPPoE Relay enables OpenRG to relay packets on PPPoE connections, while keeping its designated functionality for any additional connections. The PPPoE Relay screen (see [Figure 8.379](#)) displays a check-box that enables PPPoE Relay.



Figure 8.379. PPPoE Relay

8.7. Management

8.7.1. Universal Plug and Play

Universal Plug-and-Play is a networking architecture that provides compatibility among networking equipment, software and peripherals. UPnP OpenRG™-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. This technology leverages existing standards and technologies, including TCP/IP, HTTP 1.1 and XML, facilitating the incorporation of Universal Plug-and-Play capabilities into a wide range of networked products for the home.

Universal Plug-and-Play technologies are rapidly adopted and integrated into widely-used consumer products such as Windows XP. Therefore, it is critical that today's Residential Gateways be UPnP-compliant. Your gateway is at the forefront of this development, offering a complete software platform for UPnP devices. This means that any UPnP-enabled *control point* (client) can dynamically join the network, obtain an IP address and exchange information about its capabilities and those of other computers on the network. They can subsequently communicate with each other directly, thereby further enabling peer-to-peer networking. And this all happens automatically, providing a truly zero-configuration network.

8.7.1.1. UPnP on OpenRG

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.

- To add a UPnP-enabled computer to the home network:

1. Connect the PC to the gateway.
 2. The PC will automatically be recognized and added to the home network. OpenRG will be added to 'My Network Places' as the Internet Gateway Device and will allow configuration via a standard Windows interface.
 3. A message appears in the notification area of the Taskbar notifying that the PC has been added to the network.
- To access the WBM directly from Windows:
 1. Open the 'My Network Places' window by double-clicking its desktop icon.

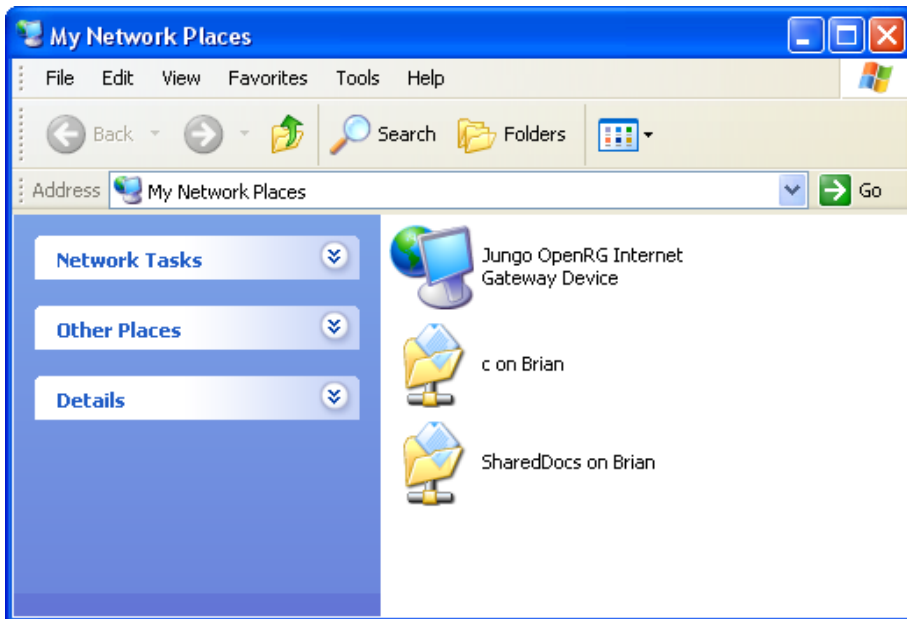


Figure 8.380. My Network Places

2. Double-click the 'Internet Gateway Device' icon. The WBM login screen appears in a browser window. This method is similar to opening a browser window and typing in '192.168.1.1'.
- To monitor the status of the connection between OpenRG and the Internet:
 1. Open the 'Network Connections' control panel.
 2. Double-click 'Internet Connection' icon. The 'Internet Connection Status' window appears.

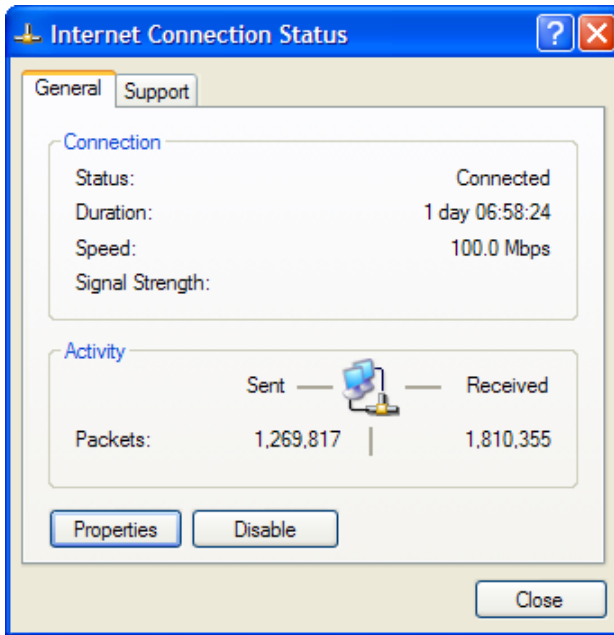


Figure 8.381. Internet Connection Status

You may also make services provided by computers in the home network available to computers on the Internet. For example, you may designate a PC in your home network to act as a Web server, allowing computers on the Internet to request pages from it. Or a game that you want to play over the Internet may require that specific ports be opened to allow communication between your PC and other players. Refer to [Section 7.3.3](#) for more information.

- To make local services available to computers on the Internet:
 1. Open the 'Network Connections' control panel.
 2. Right-click 'Internet Connection' and choose 'Properties'. The 'Internet Connection Properties' window appears.

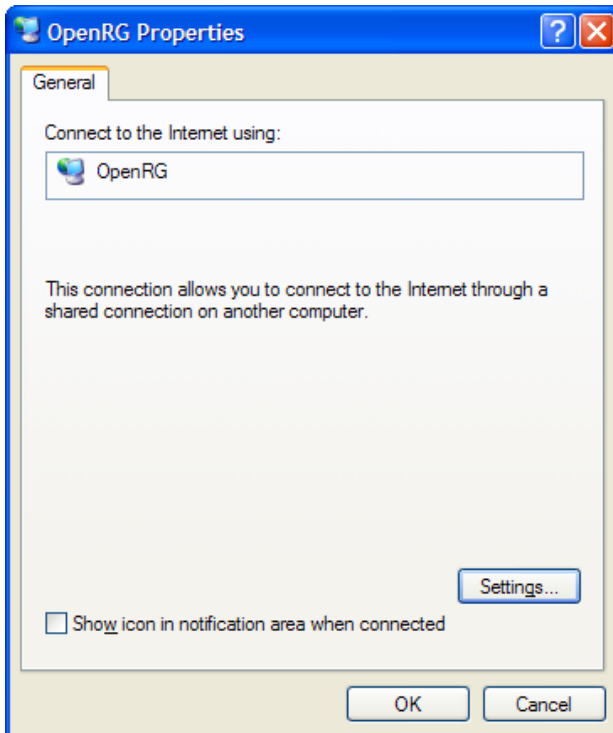


Figure 8.382. Internet Connection Properties

3. Click the 'Settings' button. The 'Advanced Settings' window appears.

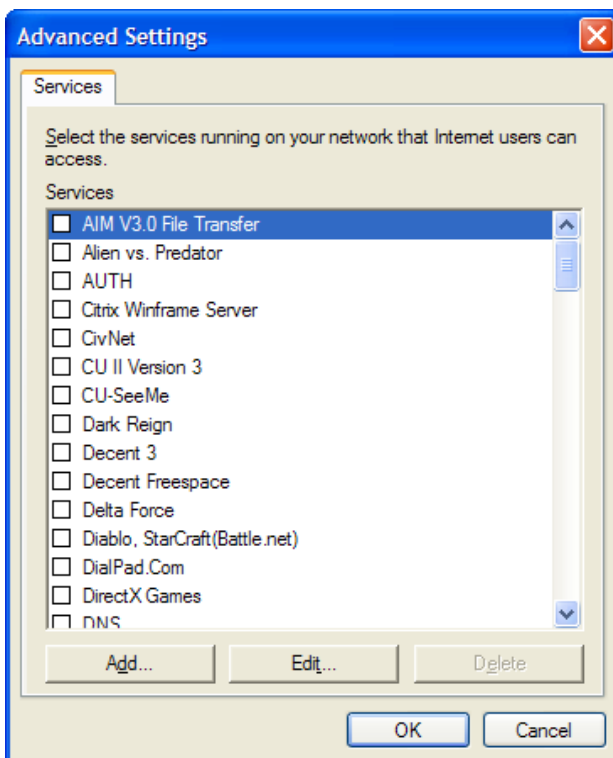


Figure 8.383. Advanced Settings

4. Select a local service that you would like to make available to computers on the Internet. The 'Service Settings' window will automatically appear.

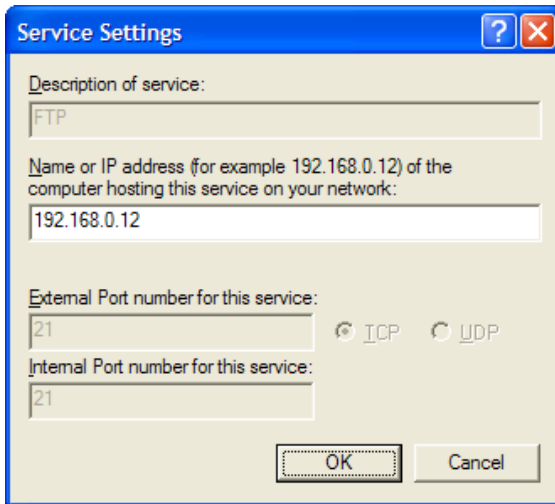


Figure 8.384. Service Settings: Edit Service

5. Enter the local IP address of the computer that provides this service and click 'OK'.
 6. Select other services as desired, and repeat the previous step for each.
 7. Click 'OK' to save the settings.
- To add a local service that is not listed in the 'Advanced Settings' window:
 1. Follow steps 1-3 above.
 2. Click the 'Add...' button. The 'Service Settings' window appears.

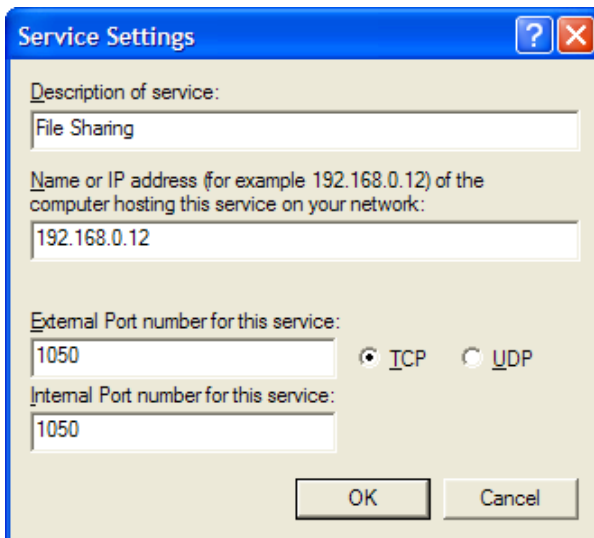


Figure 8.385. Service Settings: Add Service

3. Complete the fields as indicated in the window.
4. Click 'OK' to close the window and return to the 'Advanced Settings' window. The service will be selected.

5. Click 'OK' to save the settings.

8.7.1.2. UPnP Configuration

The UPnP feature is enabled by default. Access its settings either from the 'Management' tab under the 'System' screen, or by clicking the 'Universal Plug and Play' icon in the 'Advanced' screen. The 'Universal Plug and Play' settings screen appears.

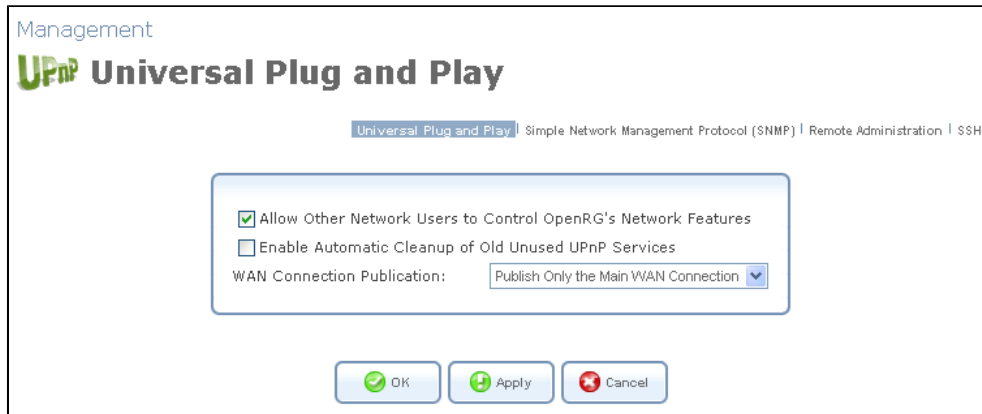


Figure 8.386. Universal Plug and Play

Allow Other Network Users to Control OpenRG's Network Features Select this checkbox to enable the UPnP feature. This will enable you to define local services on any of the LAN hosts, and to make the services available to computers on the Internet, as described in [Section 8.7.1.1](#).

Enable Automatic Cleanup of Old Unused UPnP Services When this feature is enabled, OpenRG periodically checks the availability of the LAN hosts that have been configured to provide the local services. In case the DHCP lease granted to such a host has expired and the host does not appear in the ARP table, OpenRG removes the port forwarding rule created for the corresponding local service (for more information about port forwarding, refer to [Section 7.3.3](#)).

WAN Connection Publication By default, OpenRG will publish only its main WAN connection, which will be controllable by UPnP entities. However, you may select the 'Publish All WAN Connections' option if you wish to grant UPnP control over all of OpenRG's WAN connections.

8.7.2. Simple Network Management Protocol

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

Management

Simple Network Management Protocol (SNMP)

Universal Plug and Play | Simple Network Management Protocol (SNMP) | Remote Administration | SSH

Enabled

Allow Incoming WAN Access to SNMP

Read-Only Community Name:

Read-Write Community Name:

Trusted Peer:

SNMP Traps

Enabled

Figure 8.387. SNMP Management

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 OpenRG's SNMP over the Internet.

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

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

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. OpenRG 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.

SNMP Traps

Enabled

Version:

Destination: ...

Community:

Figure 8.388. SNMP Traps

- **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.

8.7.2.1. Defining an SNMPv3 User Account

Simple Network Management Protocol version 3 (SNMPv3) enables you to perform certain management and monitoring operations on OpenRG outside its WBM. Information is exchanged between a management station and OpenRG's SNMP agent in the form of an SNMP message. The advantage of the third version of SNMP over the previous versions is that it provides user authentication, privacy, and access control.

SNMPv3 specifies a User Security Model (USM) that defines the need to create an SNMP user account, in order to secure the information exchange between the management station and the SNMP agent. The following example demonstrates how to define an SNMPv3 user account in OpenRG. Let's assume that you want to add a new SNMPv3 user called "admin". For this purpose, perform the following steps:

1. Add the SNMPv3 user account to the USM table.
2. Associate the user with a new or an existing group.
3. Associate the group with specific views.
4. Create the group views.

Step 1 is performed from OpenRG's CLI. Steps 2–4 are performed from a Linux shell, as in the following example.

1. Add the new user (admin) to the USM table, by running the following `conf set` commands from OpenRG's CLI:

```
OpenRG> conf set /snmp/mibs/usm_mib/usmuser_table/13.128.0.42.47.128.242.184.29.85.234.15
.79.65.5.97.100.109.105.110/name admin

OpenRG> conf set /snmp/mibs/usm_mib/usmuser_table/13.128.0.42.47.128.242.184.29.85.234.15
.79.65.5.97.100.109.105.110/security_name admin

OpenRG> conf set /snmp/mibs/usm_mib/usmuser_table/13.128.0.42.47.128.242.184.29.85.234.15
.79.65.5.97.100.109.105.110/public ""

OpenRG> conf set /snmp/mibs/usm_mib/usmuser_table/13.128.0.42.47.128.242.184.29.85.234.15
.79.65.5.97.100.109.105.110/auth_protocol 1.3.6.1.6.3.10.1.1.1

OpenRG> conf set /snmp/mibs/usm_mib/usmuser_table/13.128.0.42.47.128.242.184.29.85.234.15
.79.65.5.97.100.109.105.110/priv_protocol 1.3.6.1.6.3.10.1.2.1

OpenRG> conf set /snmp/mibs/usm_mib/usmuser_table/13.128.0.42.47.128.242.184.29.85.234.15
.79.65.5.97.100.109.105.110/storage_type 3

OpenRG> conf set /snmp/mibs/usm_mib/usmuser_table/13.128.0.42.47.128.242.184.29.85.234.15
.79.65.5.97.100.109.105.110/row_status 1

OpenRG> conf set /snmp/mibs/usm_mib/usmuser_table/13.128.0.42.47.128.242.184.29.85.234.15
.79.65.5.97.100.109.105.110/clone_from 0.0

OpenRG> conf set /snmp/mibs/usm_mib/usmuser_table/13.128.0.42.47.128.242.184.29.85.234.15
.79.65.5.97.100.109.105.110/engine_id <ENGINE_ID>
```

The sub-OID 13.128.0.42.47.128.242.184.29.85.234.15.79.65 stands for the engine ID (with length of 13 octets). The decimal values of each engine ID are permanent. The sub-OID 5.97.100.109.105.110 stands for "admin" (5 octets, according to the word length). The decimal values of the user name appear as defined in the ASCII table.

The <ENGINE_ID> parameter should be taken from the engine ID in the output of the following command:

```
OpenRG> conf print /snmp/persist_conf
```



Note: You should copy the engine ID without the "0x" prefix.

After the commands specified above are issued, the authentication protocol is set to `usmNoAuthProtocol` (which has OID 1.3.6.1.6.3.10.1.1), and the privacy protocol is set to `usmNoPrivProtocol` (which has OID 1.3.6.1.6.3.10.1.2.1).

- Associate the user with a group. The associated group can be either a new group or an existing group. For example, to add a new group called "admin_group" and associate it with the user "admin", run the following SNMP SET commands from a Linux shell:

```
$ snmpset -v2c -c private <OpenRG's IP address> vacmSecurityToGroupStatus.3.5.97.100.109.105.110 i createAndWait
$ snmpset -v2c -c private <OpenRG's IP address> vacmGroupName.3.5.97.100.109.105.110 s admin_group
$ snmpset -v2c -c private <OpenRG's IP address> vacmSecurityToGroupStorageType.3.5.97.100.109.105.110 i nonVolatile
$ snmpset -v2c -c private <OpenRG's IP address> vacmSecurityToGroupStatus.3.5.97.100.109.105.110 i active
```

The sub-OID 5.97.100.109.105.110 stands for "admin" (with length of 5 octets). These commands populate `vacmSecurityToGroupTable` with a new group called "admin_group".

- Associate between the group and its views. For example, suppose you want to associate "admin_group" with a view called "admin_view" for reading, writing and notifications, with security level of `noAuthNoPriv`. You can do this by running the following SNMP SET commands from a Linux shell:

```
$ snmpset -v2c -c private <OpenRG's IP address> vacmAccessStatus.11.97.100.109.105.110.95.103.114.111.117.112.0.3.1 i createAndWait
$ snmpset -v2c -c private <OpenRG's IP address> vacmAccessContextMatch.11.97.100.109.105.110.95.103.114.111.117.112.0.3.1 i exact
$ snmpset -v2c -c private <OpenRG's IP address> vacmAccessReadViewName.11.97.100.109.105.110.95.103.114.111.117.112.0.3.1 s admin_view
$ snmpset -v2c -c private <OpenRG's IP address> vacmAccessWriteViewName.11.97.100.109.105.110.95.103.114.111.117.112.0.3.1 s admin_view
$ snmpset -v2c -c private <OpenRG's IP address> vacmAccessNotifyViewName.11.97.100.109.105.110.95.103.114.111.117.112.0.3.1 s admin_view
$ snmpset -v2c -c private <OpenRG's IP address> vacmAccessStorageType.11.97.100.109.105.110.95.103.114.111.117.112.0.3.1 i nonVolatile
$ snmpset -v2c -c private <OpenRG's IP address> vacmAccessStatus.11.97.100.109.105.110.95.103.114.111.117.112.0.3.1 i active
```

The sub-OID 11.97.100.109.105.110.95.103.114.111.117.112 stands for "admin_group" (with length of 11 octets).

4. Create the needed views. For example, suppose you want to define "admin_view" as a view that includes all the 1.3 subtree. You can do this by running the following SNMP SET commands:

```
$ snmpset -v2c -c private <OpenRG's IP address> vacmViewTreeFamilyStatus.10.97.100.109.105.110.95.118.105.101.119.2.1.3 i createAndWait  
  
$ snmpset -v2c -c private <OpenRG's IP address> vacmViewTreeFamilyType.10.97.100.109.105.110.95.118.105.101.119.2.1.3 i included  
  
$ snmpset -v2c -c private <OpenRG's IP address> vacmViewTreeFamilyStorageType.10.97.100.109.105.110.95.118.105.101.119.2.1.3 i nonVolatile  
  
$ snmpset -v2c -c private <OpenRG's IP address> vacmViewTreeFamilyStatus.10.97.100.109.105.110.95.118.105.101.119.2.1.3 i active
```

The sub-OID 10.97.100.109.105.110.95.118.105.101.119 stands for "admin_view".

After completing these steps, you will have an SNMPv3 user account defined in OpenRG. The following is a sample SNMPv3 query issued to OpenRG's SNMP agent:

```
$ snmpwalk -v 3 -u admin -l noAuthNoPriv 192.168.1.1
```

8.7.3. Remote Administration


It is possible to access and control OpenRG 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 OpenRG 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 OpenRG's remote administration options, click the 'Management' menu item under the 'System' tab, or the 'Remote Administration' icon in the 'Advanced' screen. The 'Remote Administration' screen appears.

Management

Remote Administration

Universal Plug and Play | Simple Network Management Protocol (SNMP) | Remote Administration | SSH

 **Attention**
 Allowing remote administration to OpenRG 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:
 Connection Request Port:

TR-064

Enabled

Jungo.net (Jnet)

Enabled
 Jungo.net ACS URL:
 Jungo.net Home Page:

Additional Jnet Ports

Allow Jnet Commands From Remote Upgrade Server
 Remote Upgrade Server URL: <http://update.jungo.com/openrg-4.3.5-MONTEJADE.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

Figure 8.389. Remote Administration



Note: The following management application ports can be configured in the 'System Settings' screen (for more information, refer to [Section 8.2](#)). If you change the default port of a management application, you will have to specify the new port in OpenRG's address when trying to remotely connect to it: **http://<OpenRG's address>:<port>**.

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

Allow Incoming 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).

Allow Incoming Access to the 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.



Note: Web Management, Telnet and SSH may be used to modify settings of the firewall or disable it. The user may also change local IP addresses and other settings, making it difficult or impossible to access the gateway from the home network. Therefore, remote access to Telnet or HTTP services **should be blocked** and should only be permitted when it is absolutely necessary.

Allow SNMP Control and Diagnostic Requests Used to allow Simple Network Management Protocol (SNMP) requests to remotely configure and monitor OpenRG. For more information, refer to [Section 8.7.2](#).

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.

Jungo.net (Jnet) Jungo's proprietary protocol that is used for gateway management from a remote or LAN machine.

- **Enabled** Selecting this check box enables remote management of the gateway via the Jnet protocol.
- **Jungo.net ACS URL** The URL of the Jungo.net Auto-Configuration Server (JACS).
- **Jungo.net Home Page** The URL of the Jungo.net portal.

Additional Jnet Ports This section enables you to set gateway ports for receiving remote management commands over the Jnet and Jnet-SSL protocols.

- **Allow Jnet Commands From Remote Upgrade Server** When this check box is selected, OpenRG allows execution of CLI commands sent from the firmware upgrade server during OpenRG's connection to it (either scheduled or user-initiated). Clicking the 'Remote Upgrade Server URL' link, located under this check box, redirects you to the 'Firmware Upgrade' screen, where you can configure the upgrade settings (for more information, refer to [Section 8.8.5](#)).
- **Enable Incoming Jnet Requests to Port 7020** When this check box is selected, OpenRG listens on port 7020 (by default), waiting for CLI commands sent to it from a LAN machine over the Jnet protocol.
- **Allow Incoming WAN Access to Jnet** When this option is selected, OpenRG listens on the WAN port, waiting for CLI commands sent to it from a remote machine over the Jnet protocol.
- **Enable Incoming Jnet-SSL Requests to Port 7021** When this check box is selected, OpenRG listens on port 7021 (by default), waiting for CLI commands sent to it from a LAN machine over the Jnet protocol secured by the SSL.
- **Allow Incoming WAN Access to Jnet** When this option is selected, OpenRG listens on the WAN port, waiting for CLI commands sent to it from a remote machine over the Jnet protocol secured by the SSL.

To allow remote access to OpenRG's administrative 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 WBM, if port forwarding is configured to use port 80, select port 8080 to avoid conflicts.
2. Click 'OK' to save the settings.

Encrypted remote administration over the Web, which is performed using a secure SSL connection, requires an SSL certificate. When accessing OpenRG for the first time using encrypted remote administration, you will encounter a warning message generated by your browser regarding certificate authentication. This is due to the fact that OpenRG's SSL certificate is self-generated. When encountering this message under these circumstances, ignore it and continue.

It should be noted that even though this message appears, the self-generated certificate is safe, and provides you with a secure SSL connection. It is also possible to assign a user-defined certificate to OpenRG. To learn about certificates, refer to [Section 8.9.4](#).

If you wish to securely administrate OpenRG via its CLI, establish a Telnet over SSL connection to the gateway by performing the following:

1. In OpenRG's 'Remote Administration' screen, select the 'Using Secure Telnet over SSL Port' check box (see [Figure 8.389](#)). By default, the secure Telnet over SSL port is 992. You can change the port number in the 'System Settings' screen, as described in [Section 8.2](#).
2. Verify that the Telnet SSL client is installed on your machine.
3. Connect to OpenRG via Telnet SSL. For example, if you are using a Linux host, enter the following command in a shell:

```
$ telnet-ssl -z ssl 192.168.1.1 992
```

Unless you have a digital certificate recognized by OpenRG, you will be requested to enter OpenRG's username and password.



Note: If OpenRG's 'Telnet over SSL Client Authentication' option is set to 'Required' (refer to [Section 8.2](#)), it is important that the CN field of the certificate contain the name of the OpenRG user, which has administrator rights. Otherwise, OpenRG will deny access to its CLI.

8.7.4. Secure Shell

Secure Shell (SSH) is a protocol that provides encrypted connections to remote hosts or servers. OpenRG 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. To learn more, please refer to [Section 8.7.3](#). Access this feature either from its link in the 'Management' tab under the 'System' screen, or by clicking its icon in the 'Advanced' screen. The 'SSH' screen appears:

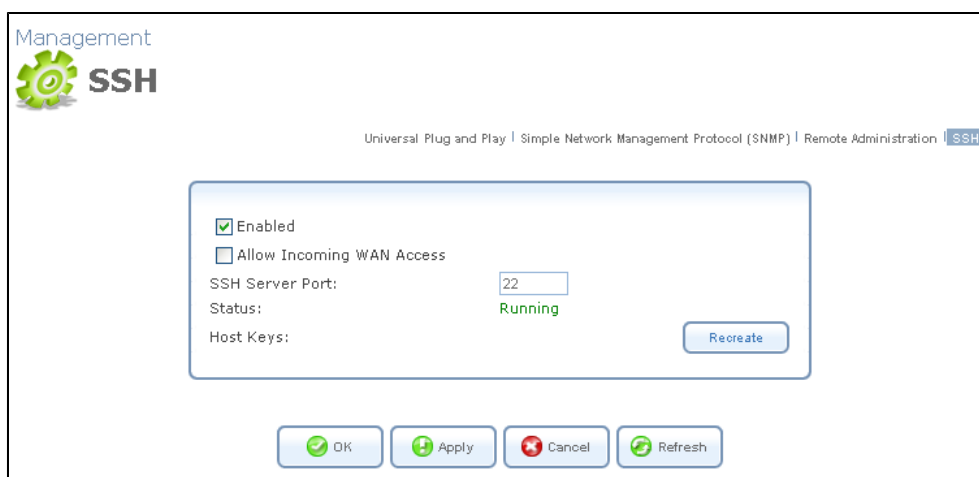


Figure 8.390. Secure Shell

Enabled Select or deselect this check box to enable or disable this feature.

Allow Incoming WAN Access Check this box to open the SSH service to WAN clients.

SSH Server Port Specify the port that will be used for SSH traffic.

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 OpenRG 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 OpenRG's configuration file.

8.8. Maintenance

8.8.1. About OpenRG

The 'About OpenRG' screen (see [Figure 8.391](#)) presents various details about OpenRG's software version, such as version number, type of platform and list of features. In addition, it displays Jungo's contact information.

Maintenance

About [About OpenRG](#) | [Configuration File](#) | [Reboot](#) | [Restore Defaults](#) | [OpenRG Firmware Upgrade](#) | [MAC Cloning](#) | [Diagnostics](#)

This product includes modules based on BSD, GPL and LGPL source code. Click [here](#) to receive the GPL and LGPL source code, and to view the BSD credits.

Software Version:	4.5.5	Upgrade
Release Date:	Aug 22 2006	
Platform:	Monte Jade	
Tag:	Tbranch-4_3	
Compilation Flags:	LIC=/home/bat/bat/montejade_4_3/20060822_1608/conf/active_conf_eval.lic DIST=MONTEJADE	
Hardware Version:	111	
Hardware Serial Number:	222	
Supported Features:	NetFilter Linux Firewall, WBM Evaluation License Agreement, Internet Protocol Security, Intel DSR support, PPTP Server, L2TP Server, PPP Over Ethernet, PPP Over Serial, IPv6, PPTP Client, L2TP Client, ICMP ALG, Port trigger (TFTP ALG, FTP/FTPS ALG, QuickTime/RealAudio/RealPlayer (RTSP) ALG, 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 interfaces management, PPPoE Relay, IGMP Proxy, Jungo Firewall, Remote Upgrade from LAN, NAT, Secure HTTP (SSL), Permanent Storage, RIP V1/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, Mail filter, URL Keyword Filtering, SurfControl, 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, USB RNDIS, File Server, SSH, RAID, Print Server, Microsoft Shared Printing, Internet Printing, Voice Over IP, SIP Signalling, MGCP Call Agent, Remote Update Management, Remote Management Server, Event Logging, WINS Server, FTP Server, Mail Server, Web Server, File System Backup and Restore, OpenRG QOS support, 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, Bluetooth support, Kaffe support	

Contact Jungo Software Technologies:

Web site: <http://www.jungo.com>
E-mail: sales_rg@jungo.com

USA:
Phone: (408) 423-9540
Fax: (408) 423-9539

Europe:
Phone: +972-9-8859365
Fax: +972-9-8859366

Asia Pacific:
Phone: +886-2-8780-8000 ext. 1104
Fax: +886-2-8725-7804

[Close](#)

Figure 8.391. About OpenRG

The line at the top of the screen relates to OpenRG's GNU General Public License (GPL) compatibility, and provides a link to the licensing acknowledgement and source code offering page in Jungo's web site. For more information, refer to [Chapter 13](#).

8.8.2. Configuration File

OpenRG enables you to view, save and load its configuration file in order to backup and restore your current configuration.

1. Access this feature either from the 'Maintenance' tab under the 'System' screen, or by clicking its icon in the 'Advanced' screen. The 'Configuration File' screen appears (see [Figure 8.392](#)), displaying the complete contents of OpenRG's configuration file.

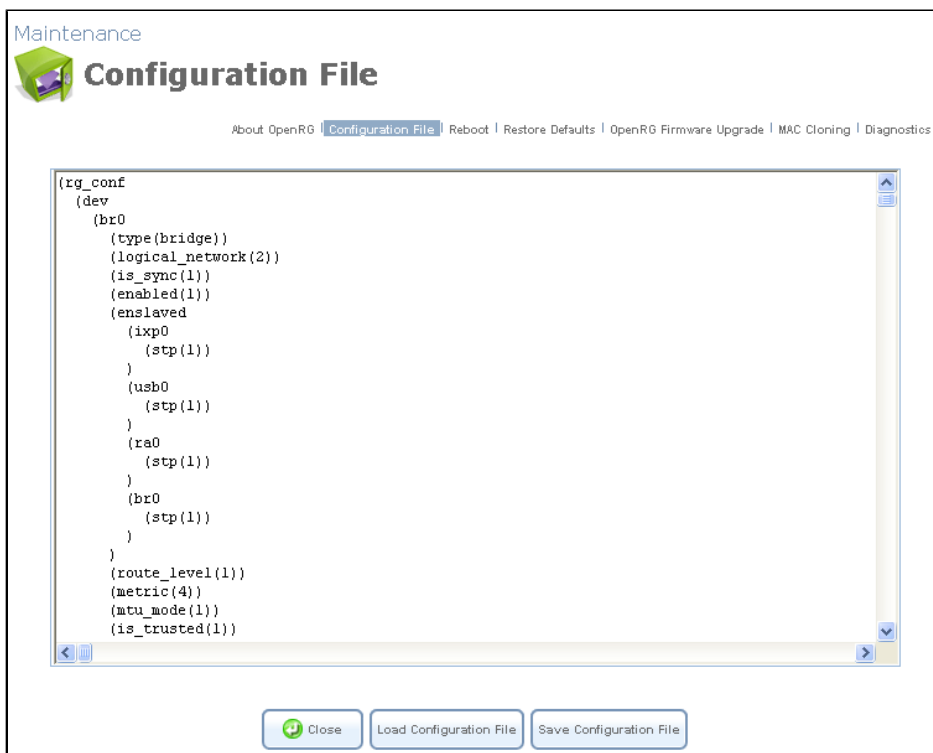


Figure 8.392. Configuration File

2. Press the 'Load Configuration File' button to restore your configuration from a file and restart OpenRG.
3. Press the 'Save Configuration File' button to backup your current configuration to a file.



Note: Upon reboot, OpenRG restores the settings from its configuration file. However, if reboot attempts fail three times consecutively, OpenRG will reset the configuration file by restoring factory defaults before attempting to reboot.

8.8.3. Reboot

To reboot OpenRG:

1. Access this feature either from the 'Maintenance' tab under the 'System' screen, or by clicking its icon in the 'Advanced' screen. The 'Reboot' screen appears:

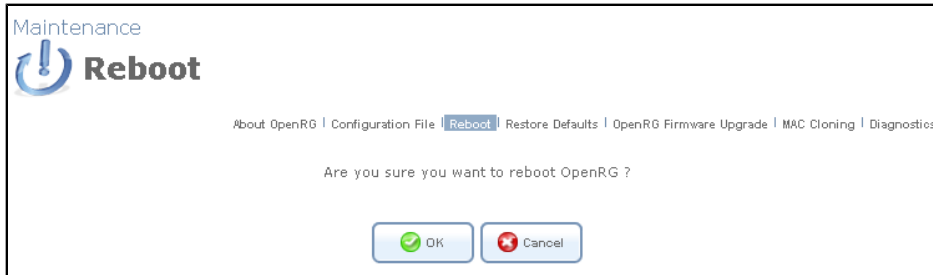


Figure 8.393. Reboot

2. Press 'OK' to reboot OpenRG. This may take up to one minute.

To re-enter the WBM after restarting the gateway, press the browser's 'Refresh' button.

8.8.4. Restore Defaults

Restoring OpenRG's factory default settings removes all of the configuration changes made to OpenRG. This is useful, 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. Access this feature either from the 'Maintenance' tab under the 'System' screen, or by clicking its icon in the 'Advanced' screen. The 'Restore Defaults' screen appears:

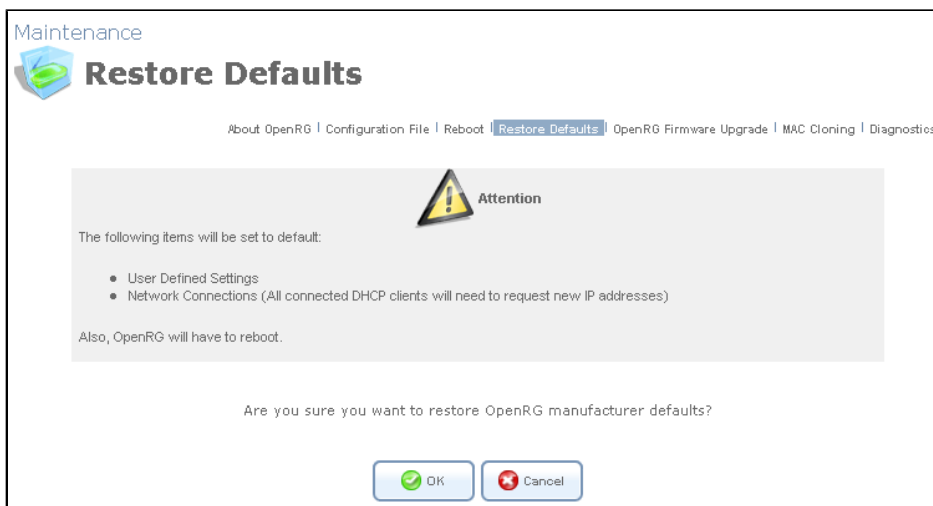


Figure 8.394. Restore Defaults

2. Press 'OK' to restore OpenRG's factory default settings.



Note: All WBM settings and parameters, not only those in the Advanced section, will be restored to their default values. This includes the administrator password; a user-specified password will no longer be valid.

8.8.5. OpenRG Firmware Upgrade

OpenRG 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.

Following are instructions for each of these methods.

8.8.5.1. Upgrading From a Local Computer

To upgrade OpenRG's software image using a locally available **.rmt** file:

1. Access this feature either from the 'Maintenance' tab under the 'System' screen, or by clicking its icon in the 'Advanced' screen. The 'OpenRG Firmware Upgrade' screen appears.

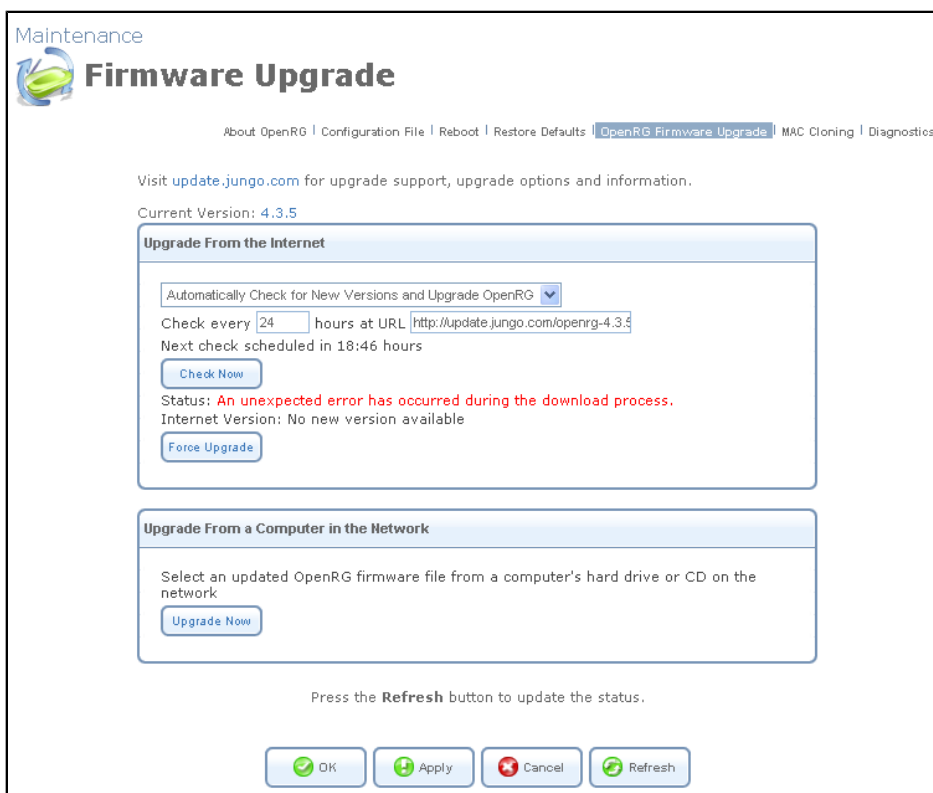



Figure 8.395. OpenRG Firmware Upgrade

2. In the 'Upgrade From a Computer in the Network' section, click the 'Upgrade Now' button. The 'Upgrade From a Computer in the Network' screen appears.



Figure 8.396. Upgrade From a Computer in the Network

3. Enter the path of the software image file, or click the 'Browse' button to browse for the file on your PC, and click 'OK'.

 Note: You can only use files with an '**rmt**' extension when performing the firmware upgrade procedure.

The file will start loading from your PC to the gateway. When loading is completed, the following confirmation screen appears, asking if you would like to upgrade to the new version:

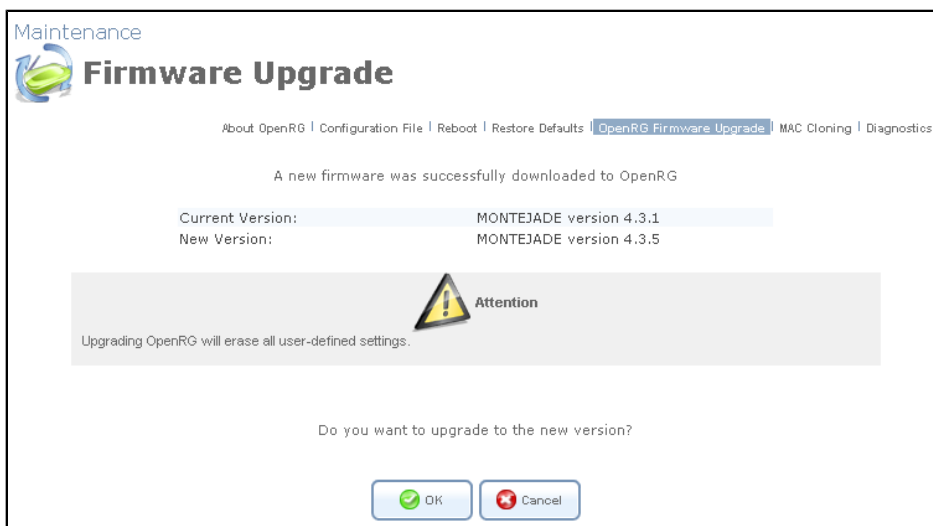


Figure 8.397. Confirm Upgrade

4. Click 'OK' to confirm. When the upgrade process ends, OpenRG automatically reboots, and the login screen of the updated image is displayed. The new software maintains your custom configurations and settings.

8.8.5.2. Upgrading From the Internet

The **Remote Upgrade** mechanism enables you to keep your software image up-to-date, by performing routine daily ¹ checks for newer software versions, as well as letting you perform manual checks. To view the automatic check utility's settings and the last check result, click the 'OpenRG Firmware Upgrade' icon in the 'Advanced' screen. The 'OpenRG Firmware Upgrade' screen will appear (see [Figure 8.395](#)). 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 between the 'Check Now' and 'Force Upgrade' buttons, indicating whether a new version is available or not.

- If a new version is available:
 1. Click the 'Force Upgrade' button. A download process will begin. When downloading is completed, a confirmation screen will appear (see [Figure 8.397](#)), asking whether you wish to upgrade to the new version.
 2. 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, OpenRG will automatically reboot. The new software version will run, maintaining your custom configurations and settings.

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

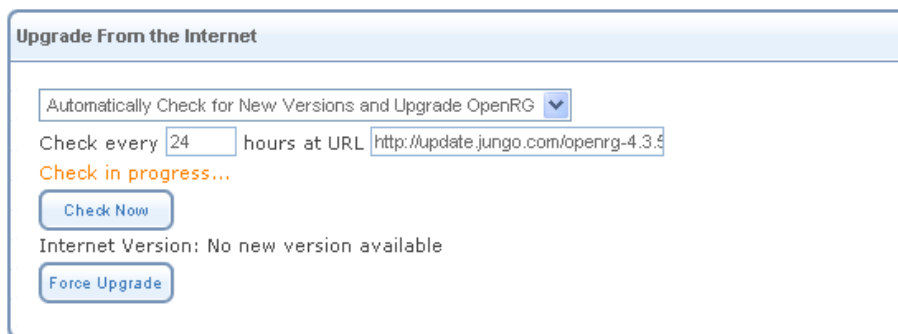


Figure 8.398. Remote Update Check

2. Click the 'Refresh' button until the check is completed and the result is displayed.

8.8.6. 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

¹ The gateway must be connected to the Internet in order to communicate with the Remote Upgrade server. Systems that store the time internally will attempt to connect and check for an update every 24 hours; systems that lack a BIOS battery will check each time the system restarts and at 24-hour intervals thereafter.

may ask you to supply the MAC address of your PC, external modem, or both. When replacing an external modem with OpenRG, you can simplify the installation process by copying the MAC address of your existing PC to OpenRG. In such a case, you do not need to delay the setup process by informing your service provider of newly installed equipment. To use MAC cloning:

1. Access this feature either from the 'Maintenance' tab under the 'System' screen, or by clicking its icon in the 'Advanced' screen. The 'MAC Cloning' screen appears:



The screenshot shows the 'Maintenance' menu with 'MAC Cloning' selected. The 'MAC Cloning' screen has a breadcrumb trail: 'About OpenRG | Configuration File | Reboot | Restore Defaults | OpenRG Firmware Upgrade | MAC Cloning | Diagnostics'. The main content area is titled 'Set MAC of Device:' and 'WAN Ethernet'. It contains a form with the following fields and buttons:

- 'Set MAC of Device:' label
- 'WAN Ethernet' label
- Input fields for MAC address: '22', ':8e', ':ce', ':d5', ':6b', ':d6'
- 'To Physical Address:' label
- 'Clone My MAC Address' button
- 'OK' button (with a green checkmark icon)
- 'Apply' button (with a green plus icon)
- 'Cancel' button (with a red minus icon)

Figure 8.399. MAC Cloning Settings

2. Enter the physical MAC address to be cloned.
3. Press the 'Clone My MAC Address' button.

8.8.7. 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.



Note: The test tools described in this section are platform-dependent, and therefore may not all be available at once.

Access this feature either from the 'Diagnostics' link under the 'Maintenance' menu item, or by clicking its icon in the 'Advanced' screen. The 'Diagnostics' screen appears:

The screenshot shows the 'Maintenance - Diagnostics' interface. At the top, there is a navigation bar with links: 'About OpenRG', 'Configuration File', 'Reboot', 'Restore Defaults', 'OpenRG Firmware Upgrade', 'MAC Cloning', and 'Diagnostics'. Below this, there are five main sections, each with a 'Go' button:

- Ping (ICMP Echo):** Includes fields for 'Destination:', 'Number of pings:' (set to 4), and 'Status:'.
- ARP:** Includes a field for 'Destination:' (IP address format: 0.0.0.0) and 'Status:'.
- Traceroute:** Includes a field for 'Destination:' and 'Status:'.
- PVC Scan:** Includes a 'Status:' field.
- OAM Ping:** Includes a 'Type:' dropdown menu (set to 'F4 End-to-End'), and input fields for 'VPI:' (0), 'VCI:' (4), 'Count:' (0), and 'Status:'.

At the bottom of the page, there is a note: 'Press the Refresh button to update the status.' and two buttons: 'Close' and 'Refresh'.

Figure 8.400. Maintenance – Diagnostics

8.8.7.1. Diagnosing Network Connectivity

To diagnose network connectivity, perform the following:

1. Under the 'Ping' section, enter the IP address or URL to be tested in the 'Destination' field.
2. Enter the number of pings you would like to run.
3. Click 'Go'.
4. In a few moments, diagnostic statistics will be displayed. If no new information is displayed, click 'Refresh'.

8.8.7.2. Performing an ARP Test

The Address Resolution Protocol (ARP) test is used to query the physical address (MAC) of a host. To run the test, perform the following:

1. In the 'Destination' field, enter an IP address of the target host.
2. Click 'Go'.
3. In a few moments, diagnostic statistics will be displayed. If no new information is displayed, click 'Refresh'.

8.8.7.3. Performing a Traceroute Test

To run a traceroute test, perform the following:

1. Under the 'Traceroute' section, enter the IP address or URL to be tested in the 'Destination' field.
2. Click 'Go'. The traceroute test commences, constantly refreshing the screen.
3. To stop the test and view the results, click 'Cancel'.

8.8.7.4. Performing a PVC Scan Test

To run a *Permanent Virtual Circuit* (PVC) scan, perform the following:

1. In the 'PVC Scan' section, click 'Go'.
2. In a few moments, diagnostic statistics will be displayed. If no new information is displayed, click 'Refresh'.

8.8.7.5. Performing an OAM Ping Test

The *Operation And Maintenance* (OAM) ping test is available only on gateways with the ADSL module. This test checks the status of a Virtual Channel (VC) of the Asynchronous Transfer Mode (ATM) connection to the remote Network Access Concentrator (NAC). Each of the ATM's virtual channels has an address that consists of a Virtual Path Indicator (VPI) and Virtual Channel Indicator (VCI). The OAM ping test sends a request, either a VP loopback (F4) or a VC loopback (F5), and receives a reply from the NAC at the other end of the ATM connection.

To run an OAM ping, perform the following:

1. Under the 'OAM Ping' section, select the type of OAM ping to run:
 - F4 End-to-End
 - F4 Segment
 - F5 End-to-End
 - F5 Segment

2. In the 'VPI' field, enter the channel's VPI value.
3. When checking the VC loopback (F5): in the VCI field, enter the channel's VCI value.
4. In the 'Count' field, enter a number of the ping packets sent to the destination address.
5. Click 'Go'.
6. In a few moments, diagnostic statistics will be displayed. If no new information is displayed, click 'Refresh'.

8.9. Objects and Rules

8.9.1. 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, access this feature either from the 'Objects and Rules' tab under the 'System' screen, or by clicking its icon in the 'Advanced' screen. The 'Protocols' screen appears:

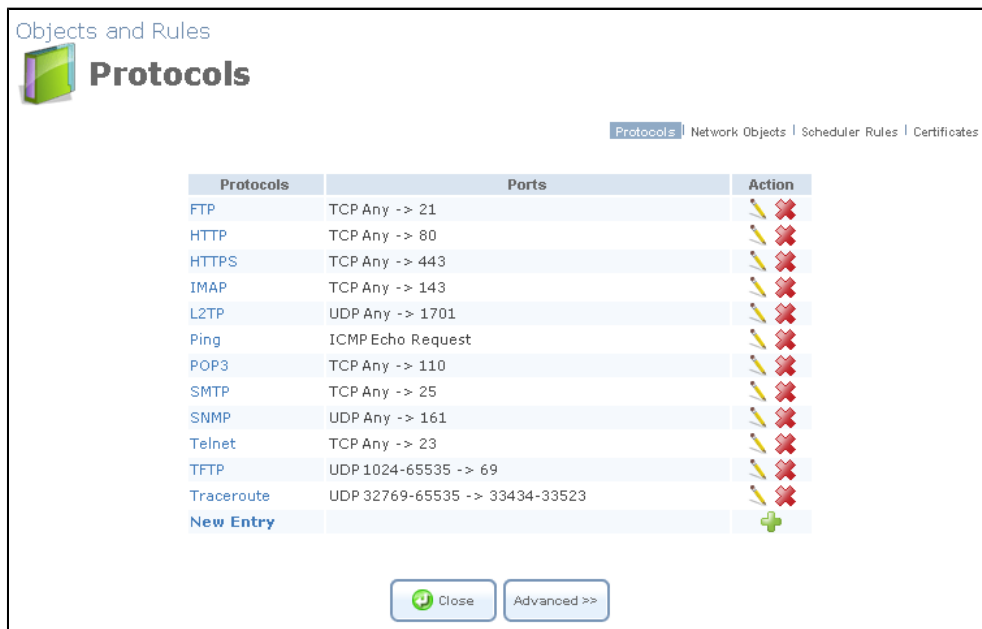


Figure 8.401. Protocols

Click the 'Advanced' button at the bottom of this screen for the full list of protocols supported by OpenRG.

Objects and Rules

Protocols Protocols | Network Objects | Scheduler Rules | Certificates

Protocols	Ports	Action
AIM Talk	TCP Any -> 4099	
AIM V3.0	TCP Any -> 5190	
America's Army	TCP Any -> 14200	
	Any -> 20025-20048	
	UDP Any -> 1716-1718	
	Any -> 8777	
	Any -> 27900	
Battlecom	TCP Any -> 2300-2400	
	Any -> 47624	
	UDP Any -> 2300-2400	
	Any -> 47624	
Battlefield series	TCP Any -> 4711	
	Any -> 18060	
	Any -> 23000-23009	
Blizzard Battlenet	TCP Any -> 4000	
	Any -> 6112	
	UDP Any -> 6112	
Civilization 4	TCP Any -> 6667	
	Any -> 2033	
	UDP Any -> 2300-2400	
	Any -> 13139	
Command and Conquer 3	UDP Any -> 8088-65535	
DHCP ALG	UDP 67-68 -> 67	
DialPad.Com	TCP Any -> 7175	
	Any -> 8680	
	Any -> 8686	
DirectX Games	TCP Any -> 47624-47625	
	Any -> 2300-2400	
	Any -> 28800-28912	
	UDP Any -> 47624-47625	
	Any -> 2300-2400	
DNS	TCP 53 -> 53	
	1024-65535 -> 53	
	UDP 53 -> 53	
	1024-65535 -> 53	
DNS ALG	UDP Any -> 53	
Freetel	UDP Any -> 21300-21303	
FTP	TCP Any -> 21	
FW1VPN	TCP Any -> 259	
Gnutella Server	TCP Any -> 6346	
MSN Messenger	TCP Any -> 1863	
NeverWinter Nights series	UDP Any -> 5120-5300	
	Any -> 6500	
	Any -> 6667	
	Any -> 27900	
	Any -> 28900	
Nintendo Wii	TCP Any -> 28910	
	Any -> 29900-29901	
	Any -> 29920	
NNTP	TCP Any -> 119	
PCAnywhere	TCP Any -> 5631-5632	
	UDP Any -> 5631-5632	
Ping	ICMP Echo Request	
Play-Station2	TCP Any -> 10070-10080	
	UDP Any -> 10070	
Play-Station3	TCP Any -> 5223	
	UDP Any -> 3478-3479	
	Any -> 3658	
X Windows	TCP Any -> 6000-6100	
XBox, Xbox 360	TCP Any -> 3074	
	UDP Any -> 88	
	Any -> 3074	
New Entry		

Figure 8.402. Protocols — Advanced Mode

Note that toggling this view between 'Basic' and 'Advanced' is reflected throughout the WBM wherever the protocols list is displayed, and can be set back with 'Show All Services' and 'Show Basic Services', respectively. To define a protocol:

1. Click the 'New Entry' link in the 'Protocols' screen. The 'Edit Service' screen appears:

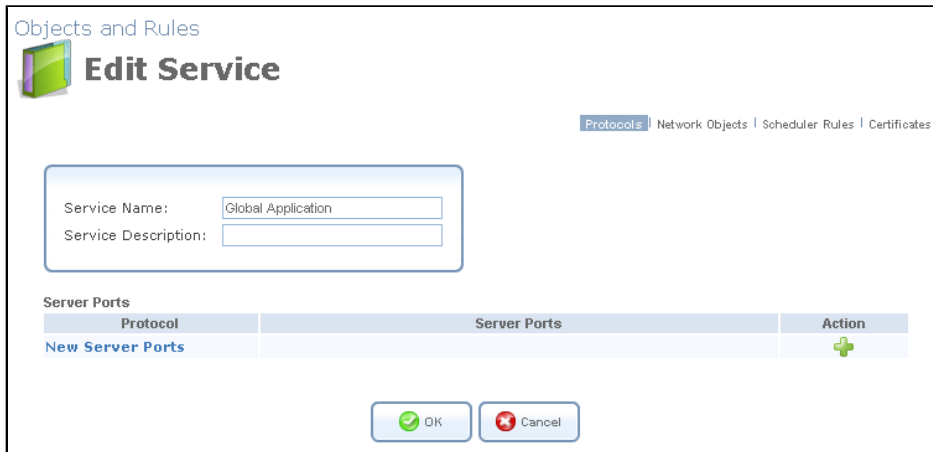


Figure 8.403. Edit Service

2. Name the service in the 'Service Name' field, and click the 'New Server Ports' link. The 'Edit Service Server Ports' screen appears (see [Figure 8.404](#)). 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.

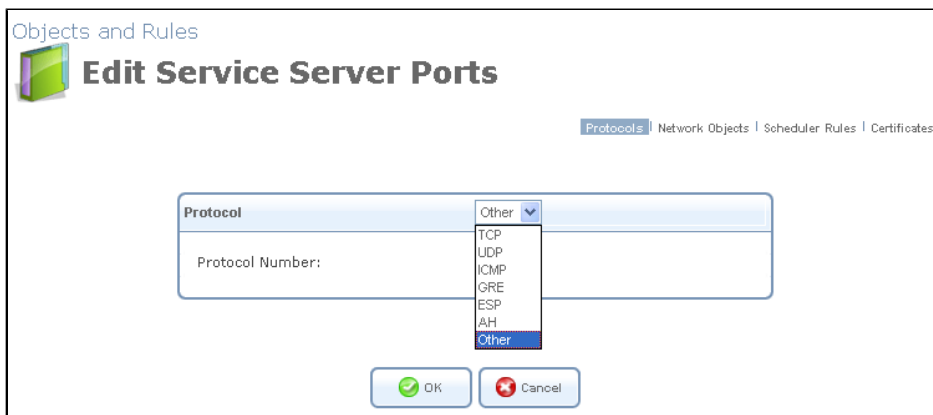


Figure 8.404. Edit Service Server Ports

3. Select a protocol and enter the relevant information.
4. Click 'OK' to save the settings.

8.9.2. Network Objects

Network Objects is a method used to abstractly define a set of LAN hosts, according to specific criteria, such as MAC address, IP address, or host name. Defining such a group can assist when configuring system rules. For example, network objects can be used when configuring OpenRG'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.

It is also possible to define network objects according to MAC addresses, making rule application more persistent against network configuration settings. Moreover, OpenRG supports several DHCP options—60, 61, and 77, enabling the gateway to apply security and QoS rules on a network object according to its unique vendor, client, or user class ID, respectively. For example, a Dell OpenRG™ IP telephone can be identified and applied with specific QoS priority rules.

To define a network object:

1. Access this feature either from the 'Objects and Rules' tab under the 'System' screen, or by clicking its icon in the 'Advanced' screen. The 'Network Objects' screen appears.

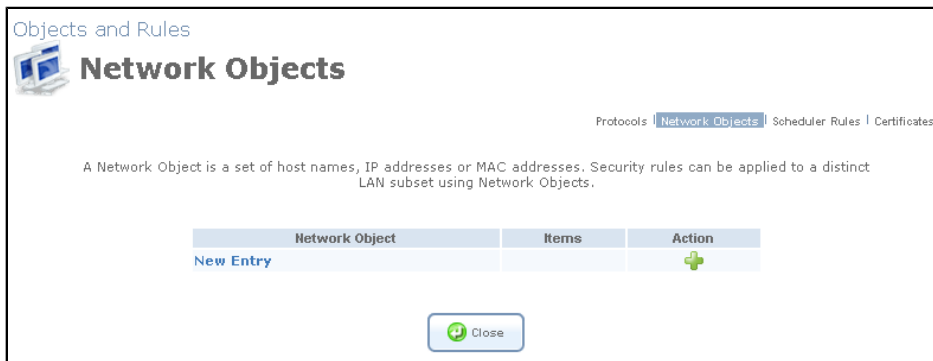


Figure 8.405. Network Objects

2. Click the 'New Entry' link, the 'Edit Network Object' screen appears.

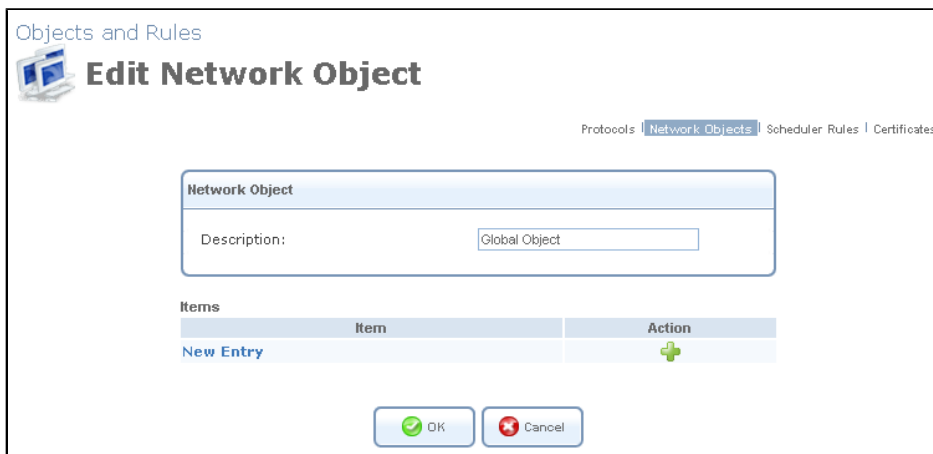


Figure 8.406. Edit Network Object

3. Name the network object in the Description field, and click New Entry to create it. The 'Edit Item' screen appears.

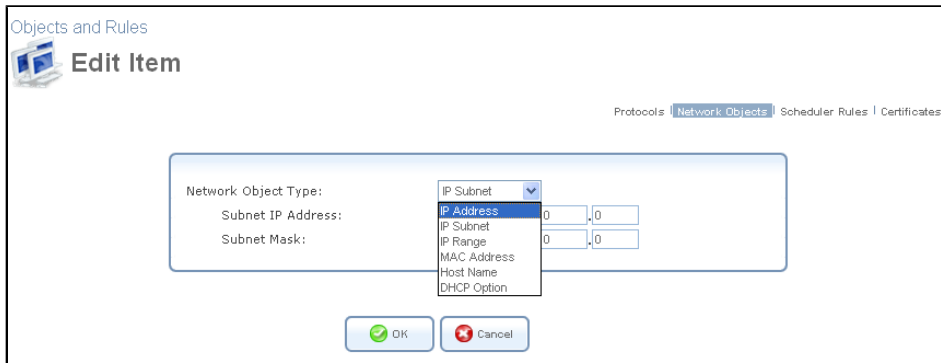


Figure 8.407. Edit Item

When selecting a method from the drop-down menu, the screen refreshes, presenting the respective fields for entering the relevant information. The group definition can be according to one of the following methods:

IP Address Enter an IP address common to the group.

IP Subnet Enter a subnet IP address and a subnet mask.

IP Range Enter first and last IP addresses in the range.

MAC Address Enter a MAC address and mask.

Host Name Enter a host name common to the group.

DHCP Option Enter either a vendor class ID (option 60), client ID (option 61), or user class ID (option 77), supplied by your service provider. Note that DHCP clients must also be configured with one of those IDs, in order to be associated with this network object.

4. Select a method and enter the source address accordingly.
5. Click 'OK' to save the settings.

8.9.3. 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. Access this feature either from the 'Objects and Rules' menu item under the 'System' tab, or by clicking its icon in the 'Advanced' screen. The 'Scheduler Rules' screen appears.



Figure 8.408. Scheduler Rules

2. Click the 'New Entry' link. The 'Edit Scheduler Rule' screen appears.

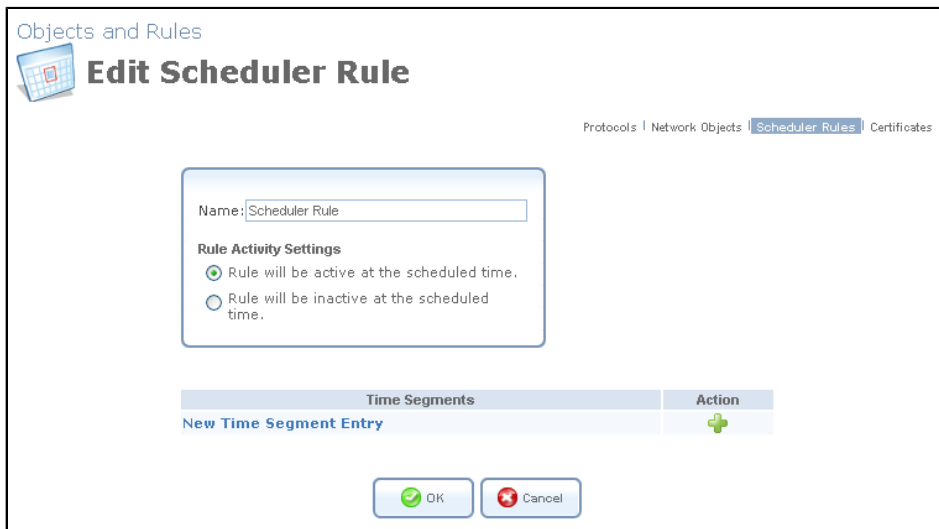


Figure 8.409. Edit Scheduler Rule

3. Specify a name for the rule in the 'Name' field.
4. Click the 'New Time Segment Entry' link to define the time segment to which the rule will apply. The 'Time Segment Edit' screen appears.

Objects and Rules

Edit Time Segment

Protocols | Network Objects | Scheduler Rules | Certificates

Days of Week

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Sunday

Hours Range

Start Time	End Time	Action
New Hours Range Entry		+

Figure 8.410. Time Segment Edit

- a. Select the day(s) of the week, on which the rule will be activated or deactivated.
- b. Click the 'New Hours Range Entry' to narrow the time segment to a specific hour range. The 'Edit Hour Range' screen appears.

Objects and Rules

Edit Hour Range

Protocols | Network Objects | Scheduler Rules | Certificates

Start Time: :

End Time: :

Figure 8.411. Edit Hour Range

- c. Enter the desired start and end time values.



Note: The defined start and end time will be applied to all days of the week you have selected. In addition, if you choose the hour range 21:00-08:00, for example, the rule will be activated on the selected day, and deactivated the next day at 8 o'clock in the morning.

5. Click 'OK' to save the settings. The 'Edit Scheduler Rule' screen appears with the defined time segment.
6. Specify if the rule will be active/inactive during the designated time period, by selecting the appropriate 'Rule Activity Settings' radio button.

7. Click 'OK' to return to the 'Scheduler Rules' screen.

8.9.4. Certificates

8.9.4.1. Overview

Public-key cryptography uses a pair of keys: a public key and a corresponding private key. These keys can play opposite roles, either encrypting or decrypting data. Your public key is made known to the world, while your private key is kept secret. The public and private keys are mathematically associated; however it is computationally infeasible to deduce the private key from the public key. Anyone who has the public key can encrypt information that can only be decrypted with the matching private key. Similarly, the person with the private key can encrypt information that can only be decrypted with the matching public key. Technically, both public and private keys are large numbers that work with cryptographic algorithms to produce encrypted material. The primary benefit of public-key cryptography is that it allows people who have no preexisting security arrangement to authenticate each other and exchange messages securely. OpenRG makes use of public-key cryptography to encrypt and authenticate keys for the encryption of Wireless and VPN data communication, the Web Based Management (WBM) utility, and secured telnet.

8.9.4.1.1. Digital Certificates

When working with public-key cryptography, you should be careful and make sure that you are using the correct person's public key. Man-in-the-middle attacks pose a potential threat, where an ill-intending 3rd party posts a phony key with the name and user ID of an intended recipient. Data transfer that is intercepted by the owner of the counterfeit key can fall in the wrong hands. Digital certificates provide a means for establishing whether a public key truly belongs to the supposed owner. It is a digital form of credential. It has information on it that identifies you, and an authorized statement to the effect that someone else has confirmed your identity. Digital certificates are used to foil attempts by an ill-intending party to use an unauthorized public key. A digital certificate consists of the following:

A public key

Certificate information The "identity" of the user, such as name, user ID and so on.

Digital signatures A statement stating that the information enclosed in the certificate has been vouched for by a Certificate Authority (CA).

Binding this information together, a certificate is a public key with identification forms attached, coupled with a stamp of approval by a trusted party.

8.9.4.1.2. X.509 Certificate Format

OpenRG supports X.509 certificates that comply with the ITU-T X.509 international standard. An X.509 certificate is a collection of a standard set of fields containing information about a user or device and their corresponding public key. The X.509 standard defines what

information goes into the certificate, and describes how to encode it (the data format). All X.509 certificates have the following data:

The certificate holder's public key the public key of the certificate holder, together with an algorithm identifier that specifies which cryptosystem the key belongs to and any associated key parameters.

The serial number of the certificate the entity (application or person) that created the certificate is responsible for assigning it a unique serial number to distinguish it from other certificates it issues. This information is used in numerous ways; for example when a certificate is revoked, its serial number is placed on a Certificate Revocation List (CRL).

The certificate holder's unique identifier this name is intended to be unique across the Internet. A DN consists of multiple subsections and may look something like this: CN=John Smith, EMAIL=openrg@jungo.com, OU=R&D, O=Jungo, C=US (These refer to the subject's Common Name, Organizational Unit, Organization, and Country.)

The certificate's validity period the certificate's start date/time and expiration date/time; indicates when the certificate will expire.

The unique name of the certificate issuer the unique name of the entity that signed the certificate. This is normally a CA. Using the certificate implies trusting the entity that signed this certificate. (Note that in some cases, such as root or top-level CA certificates, the issuer signs its own certificate.)

The digital signature of the issuer the signature using the private key of the entity that issued the certificate.

The signature algorithm identifier identifies the algorithm used by the CA to sign the certificate.

8.9.4.2. OpenRG Certificate Stores

OpenRG maintains two certificate stores:

1. **OpenRG Local Store** This store contains a list of approved certificates that are used to identify OpenRG to its clients. The list also includes certificate requests that are pending a CA's endorsement. You can obtain certificates for OpenRG 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.

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

8.9.4.2.1. Requesting an X509 Certificate

To obtain an X509 certificate, you must ask a CA to issue you one. You provide your public key, proof that you possess the corresponding private key, and some specific information about yourself. You then digitally sign the information and send the whole package -- the certificate request -- to the CA. The CA then performs some due diligence in verifying that the information you provided is correct and, if so, generates the certificate and returns it. You might think of an X509 certificate as looking like a standard paper certificate with a public key taped to it. It has your name and some information about you on it, plus the signature of the person who issued it to you.

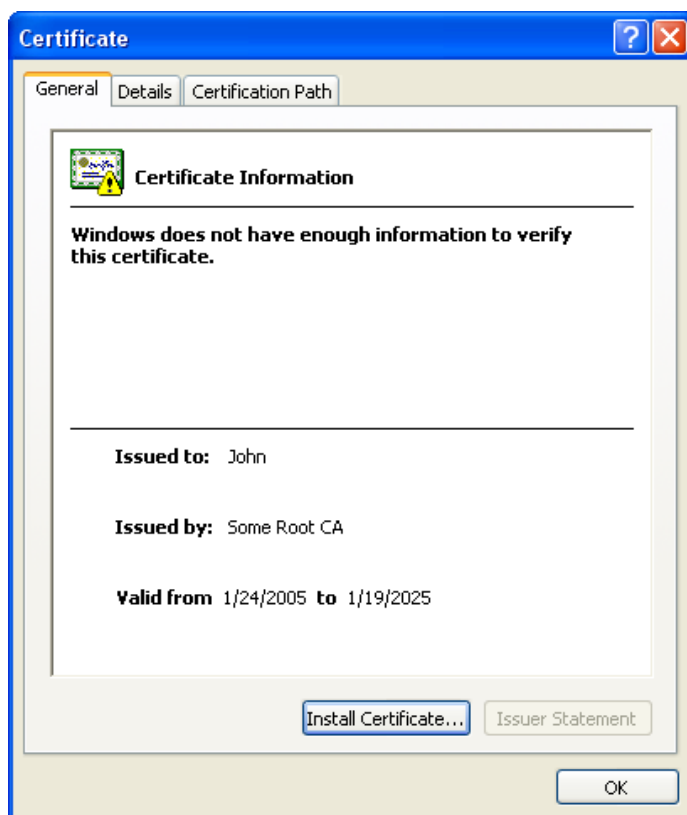


Figure 8.419. Certificate Window



Figure 8.420. Certificate Details

1. Access this feature either from the 'Objects and Rules' tab under the 'System' screen, or by clicking its icon in the 'Advanced' screen. The 'Certificates' screen appears.

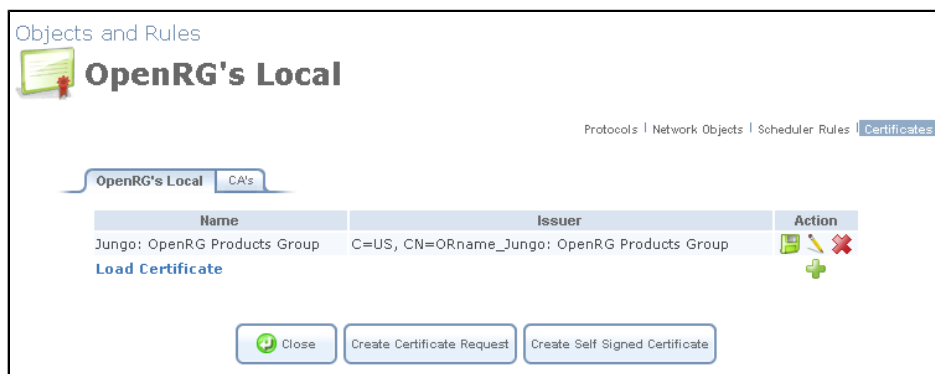


Figure 8.412. Certificate Management

2. Click the 'Create Certificate Request' button. The 'Create X509 Request' screen appears:

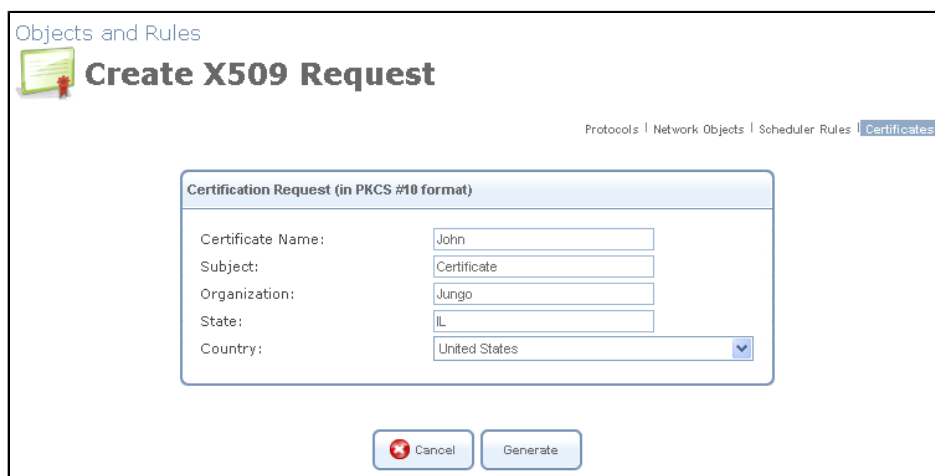


Figure 8.413. Create X509 Request

3. Enter the following certification request parameters:

- Certificate Name
 - Subject
 - Organization
 - State
 - Country
4. Click the 'Generate' button. A screen appears, stating that the certification request is being generated (see [Figure 8.414](#)).

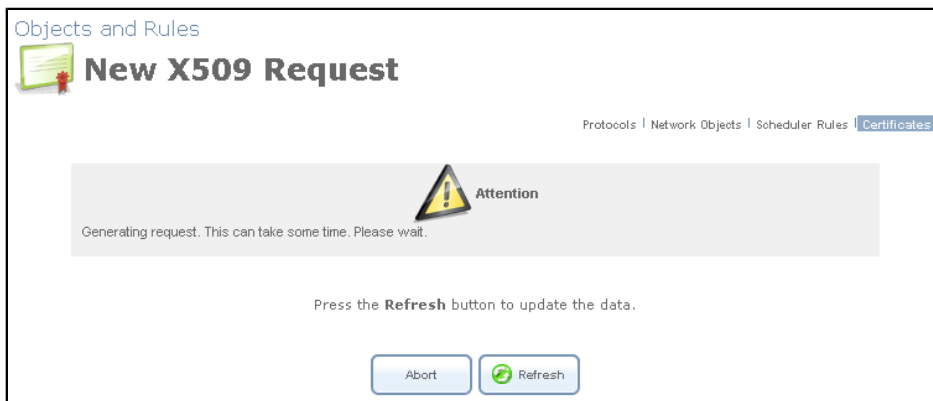


Figure 8.414. Generating a Request

5. After a short while, press the 'Refresh' button, until the 'Save Certificate Request' screen appears.

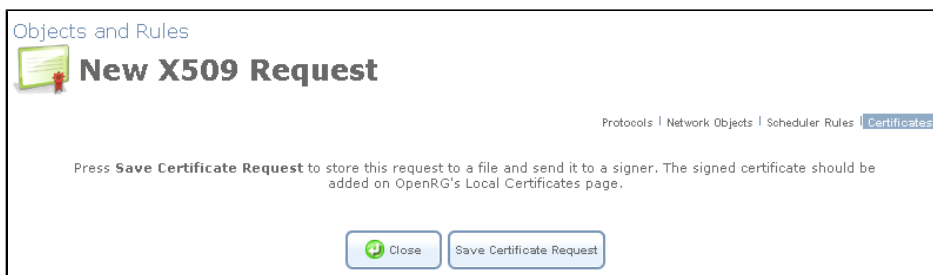



Figure 8.415. Save Certificate Request

6. Click the 'Save Certificate Request' button and save the request to a file.
7. Click the 'Close' button. The main certificate management screen reappears, listing your certificate as "Unsigned". In this state, the request file may be opened at any time by pressing the  action icon and then 'Open' in the dialogue box (Windows only).

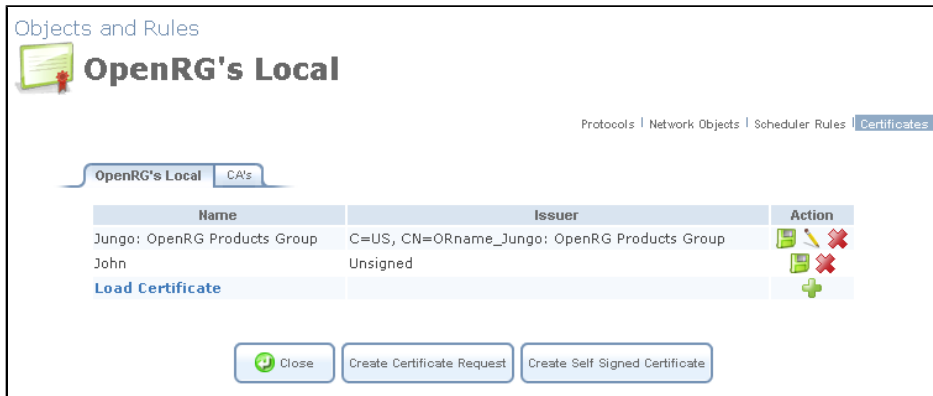


Figure 8.416. Unsigned Certification Request

- After receiving a reply from the CA in form of a '.pem' file, click the 'Load Certificate' link. The 'Load OpenRG's Local Certificate' screen appears.

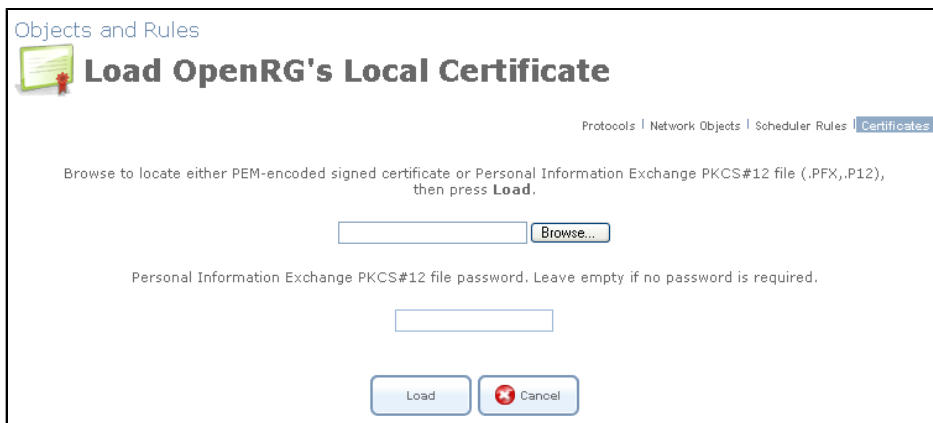


Figure 8.417. Load Certificate

- Use the Browse button to browse to the signed certificate '.pem' file. Leave the password entry empty and press "Load" to load the signed certificate. The certificate management screen appears, displaying the certificate name and issuer (see [Figure 8.418](#)).

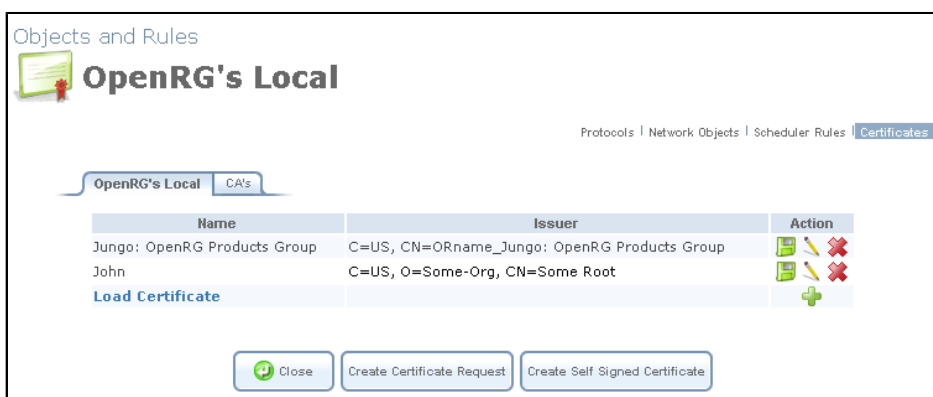


Figure 8.418. Loaded Certificate

10. Click the Save button and then 'Open' in the dialogue box to view the 'Certificate' window (Windows only) (see [Figure 8.419](#)). Alternatively, click 'Save' in the dialogue box to save the certificate to a file.
11. You can also click the edit action icon to view the 'Certificate Details' screen (see [Figure 8.420](#)).

8.9.4.2.2. Creating a Self-Signed Certificate

A default self-signed certificate is included in OpenRG (see [Figure 7.506](#)), in order to enable certificate demanding services such as HTTPS. Note that if deleted, this certificate is restored when OpenRG's Restore Defaults operation is run (refer to [Section 8.8.4](#)). To create a self-signed certificate:

1. Access this feature either from the 'Objects and Rules' tab under the 'System' screen, or by clicking its icon in the 'Advanced' screen. The 'Certificates' screen appears.

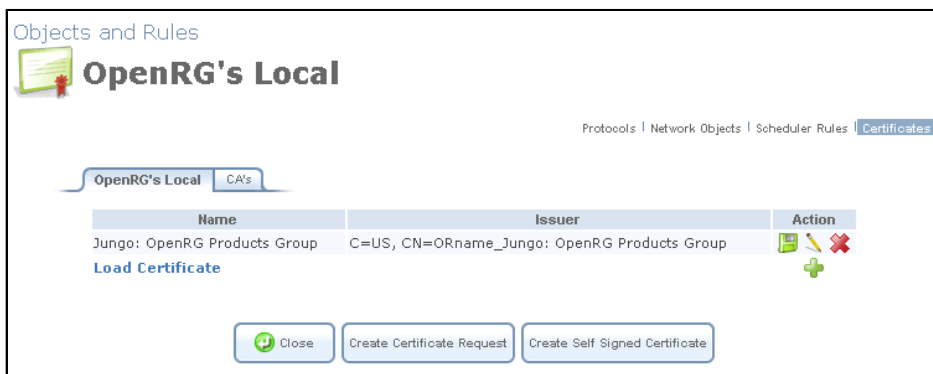


Figure 8.421. Certificate Management

2. Click the 'Create Self Signed Certificate' button. The 'Create Self Signed X509 Certificate' screen appears.

Certificate Name:

Subject:

Organization:

State:

Country:

Figure 8.422. Create Self Signed X509 Certificate

3. Enter the following certification request parameters:

- Certificate Name

- Subject
 - Organization
 - State
 - Country
4. Click the 'Generate' button. A screen appears, stating that the certificate is being generated (see [Figure 8.423](#)).

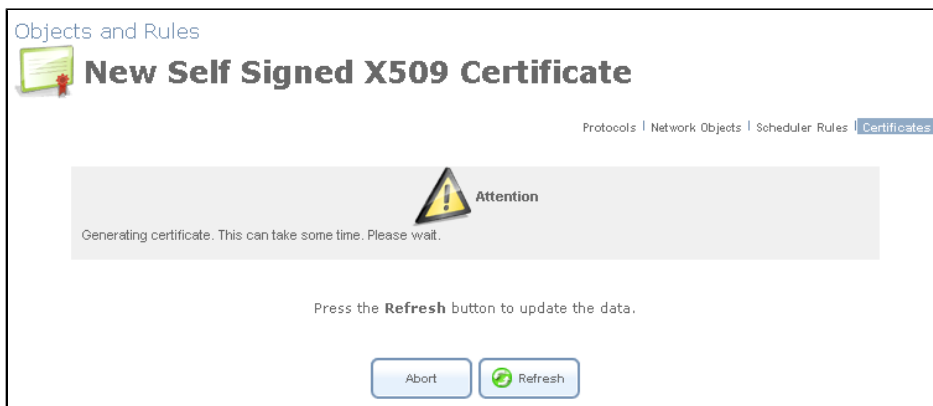


Figure 8.423. Generating Certificate

5. After a short while, press the 'Refresh' button, until the 'Certificate Details' screen appears.

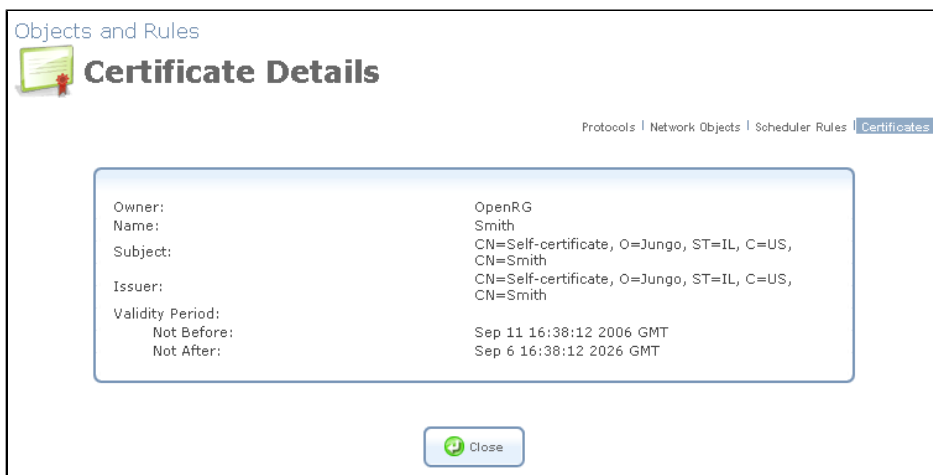


Figure 8.424. Certificate Details

6. Click the 'Close' button. The main certificate management screen reappears, displaying the certificate name and issuer (see [Figure 8.425](#)).



Figure 8.425. Loaded Certificate

7. Click the Save button and then 'Open' in the dialogue box to view the 'Certificate' window (Windows only) (see [Figure 8.419](#)). Alternatively, click 'Save' in the dialogue box to save the certificate to a file.
8. You can also click the edit action icon to view the 'Certificate Details' screen (see [Figure 8.420](#)).

8.9.4.2.3. Loading a PKCS#12 Format Certificate

You can load certificates in PKCS#12 format (usually stored in .p12 files) to OpenRG's certificate store. You must first obtain the '.p12' file, containing the private and public keys and optional CA certificates.

1. Access this feature either from the 'Objects and Rules' tab under the 'System' screen, or by clicking its icon in the 'Advanced' screen. The 'Certificates' screen appears.

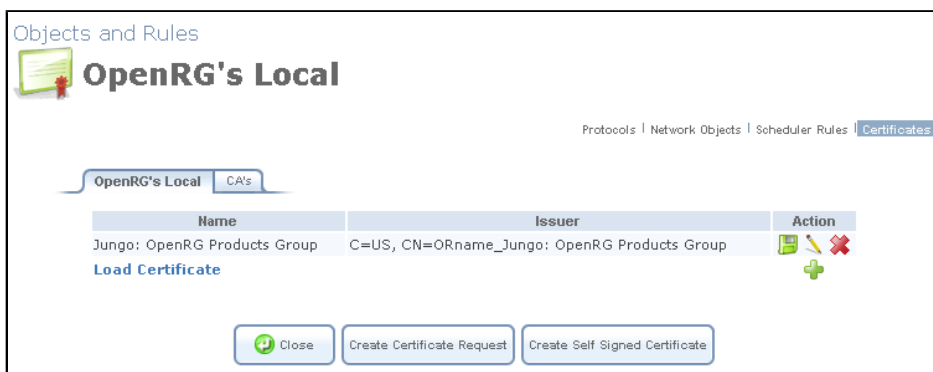


Figure 8.426. Certificate Management

2. Click the 'Load Certificate' link. The 'Load OpenRG's Local Certificate' screen appears:

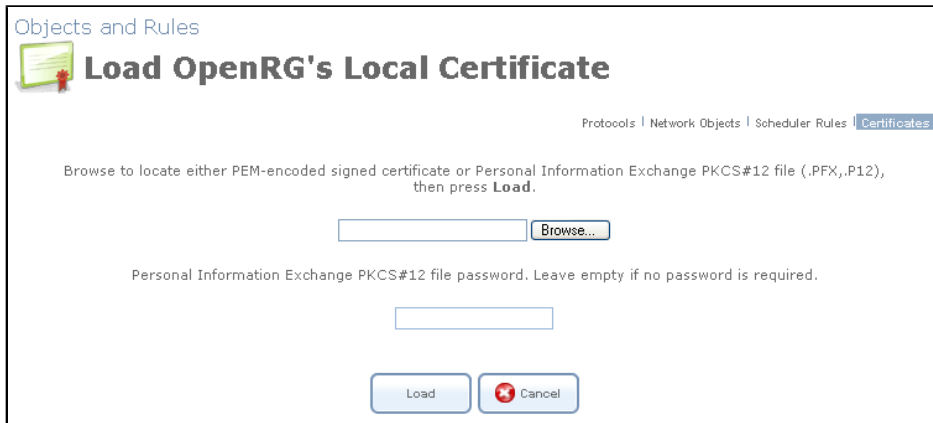


Figure 8.427. Load Certificate

- Use the Browse button to browse to the '.p12' file. If the private key is encrypted using a password, type it in the password entry (otherwise leave the entry empty) and press "Load" to load the certificate. The certificate management screen appears, displaying the certificate name and issuer (see [Figure 8.428](#)). If the '.p12' file contained any CA certificates, they will be displayed in the CA store (click the 'CA's' tab to view the CA certificates).

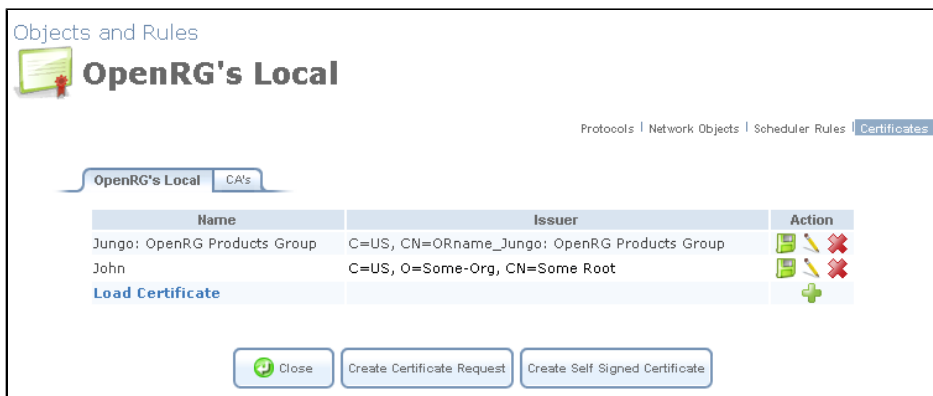


Figure 8.428. Loaded Certificate

- Click the Save button and then 'Open' in the dialog box to view the 'Certificate' window (Windows only) (see [Figure 8.419](#)). Alternatively, click 'Save' in the dialog box to save the certificate to a file.
- You can also click the edit action icon to view the 'Certificate Details' screen (see [Figure 8.420](#)).

8.9.4.2.4. Loading a CA's Certificate

Before you can load a CA's certificate, you must obtain a signed certificate '.pem' or '.p12' file.

- Access this feature either from the 'Objects and Rules' tab under the 'System' screen, or by clicking its icon in the 'Advanced' screen. The 'Certificates' screen appears.

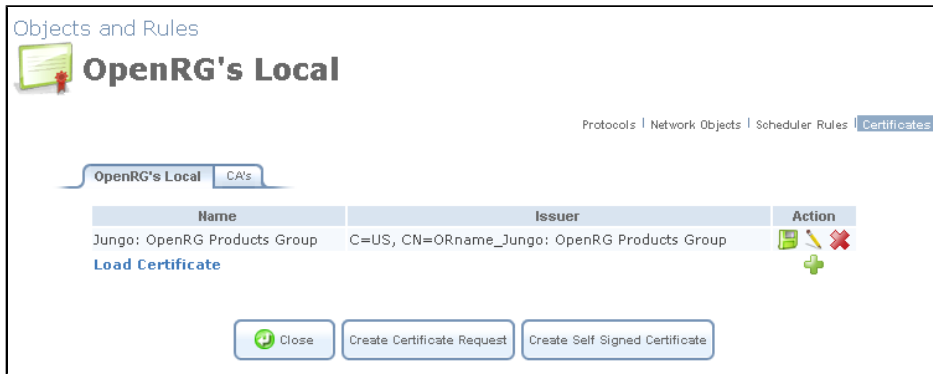


Figure 8.429. Certificate Management

2. Click the 'CA's' certificates tab. The 'CA Certificates' screen appears (see [Figure 8.430](#)). This screen displays a list of certificates.

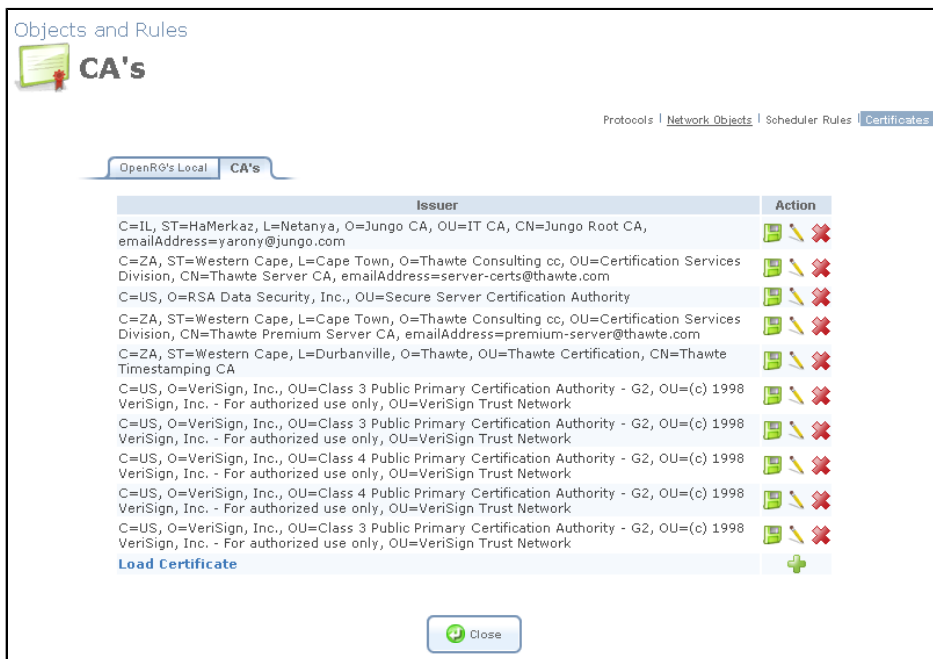


Figure 8.430. CA's Certificates

3. Click the 'Load Certificate' link. The 'Load CA's Certificate' screen appears.

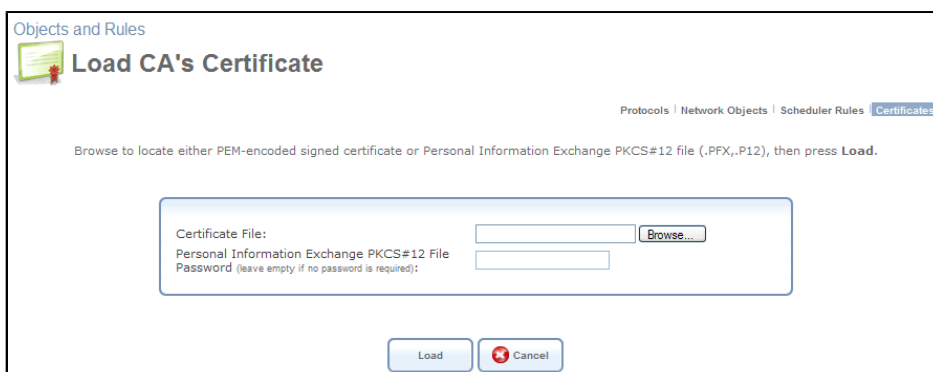


Figure 8.431. Load CA's Certificate

4. Use the Browse button to browse to the '.pem' or '.p12' file. Leave the password entry empty and press "Load" to load the certificate. The CA Certificates screen reappears (see [Figure 8.430](#)), displaying the trusted certificate authority at the bottom of the list.
5. Click the Save button and then 'Open' in the dialogue box to view the 'Certificate' window (Windows only) (see [Figure 8.419](#)). Alternatively, click 'Save' in the dialogue box to save the certificate to a file.
6. You can also click the edit action icon to view the 'Certificate Details' screen (see [Figure 8.420](#)).

9

Advanced

This section of the Web-based Management offers shortcuts to OpenRG's more advanced features. The different icons redirect to their respective screens, described throughout this manual. Please note that changes to advanced settings may adversely affect the operation of OpenRG and your home network, and should be made with caution.

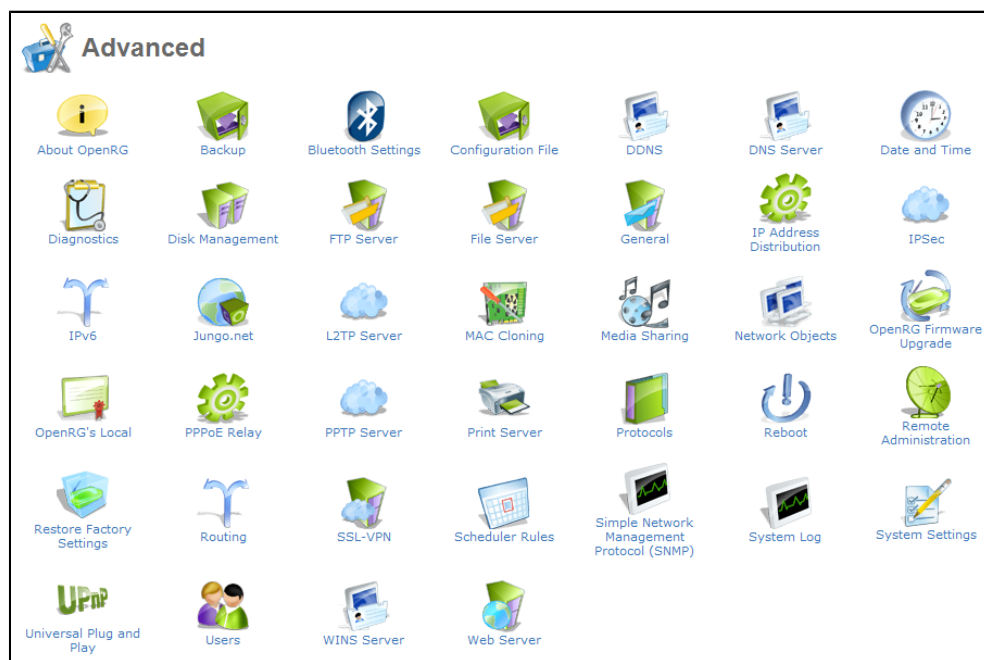


Figure 9.1. Advanced

This screen enables you to configure the following features:



About OpenRG – View various details about OpenRG's software version, such as version number, type of platform and list of features. This icon redirects to the 'Maintenance' tab under 'System' (refer to [Section 8.8.1](#)).



Backup and Restore – Backup user and system data. This icon redirects to the 'Storage' tab under 'Services' (refer to [Section 7.11.6](#)).



Bluetooth Settings – Allow devices to connect to OpenRG's LAN via Bluetooth. This icon redirects to the 'Advanced' tab under 'Services' (refer to [Section 7.13.3](#)).



Certificates – Manage digital certificates. This icon redirects to the 'Objects and Rules' tab under 'System' (refer to [Section 8.9.4](#)).



Configuration File – View, save and load the configuration file. This icon redirects to the 'Maintenance' tab under 'System' (refer to [Section 8.8.2](#)).



DNS Server – View and modify the DNS hosts table. This icon redirects to the 'Advanced' tab under 'Services' (refer to [Section 7.13.1](#)).



Date and Time – Set the local date and time. This icon redirects to the 'Settings' tab under 'System' (refer to [Section 8.2.2](#)).



Diagnostics – Perform networking diagnostics. This icon redirects to the 'Maintenance' tab under 'System' (refer to [Section 8.8.7](#)).



Disk Management – Manage different disks connected to your gateway. This icon redirects to the 'Shared Storage' tab under 'Local Network' (refer to [Section 6.4](#)).



FTP Server – Provide file exchanging capabilities. This icon redirects to the 'Storage' tab under 'Services' (refer to [Section 7.11.1](#)).



File Server – Turn your gateway into a file server. This icon redirects to the 'Storage' tab under 'Services' (refer to [Section 7.11.2](#)).



IP Address Distribution – Modify the behavior of the DHCP server for each LAN device and view a list of DHCP clients in the local network. This icon redirects to the 'Advanced' tab under 'Services' (refer to [Section 7.13.2](#)).



IPSec – Configure Internet protocol security parameters. This icon redirects to the 'VPN' tab under 'Services' (refer to [Section 7.10.1](#)).



IPv6 – Configure IPv6-over-IPv4 tunneling. This icon redirects to the 'Routing' tab under 'System' (refer to [Section 8.6.2](#)).



Jungo.net – use Jungo.net services. This icon redirects to the 'Jungo.net' tab under 'Services' (refer to [Section 7.2](#)).



L2TP Server – Configure Layer 2 tunneling protocol parameters. This icon redirects to the 'VPN' tab under 'Services' (refer to [Section 7.10.4](#)).



MAC Cloning – Clone your PC's MAC address. This icon redirects to the 'Maintenance' tab under 'System' (refer to [Section 8.8.6](#)).



Mail Server – Provide mail services for LAN and WAN users. This icon redirects to the 'Storage' tab under 'Services' (refer to [Section 7.11.5](#)).



Media Sharing – Share and stream media files saved on a storage device connected to OpenRG. This icon redirects to the 'Media Sharing' tab under 'Services' (refer to [Section 7.5](#)).



Network Objects – Define groups of LAN devices for system rules. This icon redirects to the 'Objects and Rules' tab under 'System' (refer to [Section 8.9.2](#)).



OpenRG Firmware Upgrade – Upgrade OpenRG's software image. This icon redirects to the 'Maintenance' tab under 'System' (refer to [Section 8.8.5](#)).



PPPoE Relay – Enable PPPoE relay on OpenRG. This icon redirects to the 'Routing' tab under 'System' (refer to [Section 8.6.4](#)).



PPTP Server – Configure point-to-point tunneling protocol parameters. This icon redirects to the 'VPN' tab under 'Services' (refer to [Section 7.10.3](#)).



Personal Domain Name (Dynamic DNS) – Alias a dynamic IP address to a static hostname. This icon redirects to the 'DDNS' tab under 'Services' (refer to [Section 7.12](#)).



Print Server – Share a LAN printer. This icon redirects to the 'Shared Printer' tab under 'Local Network' (refer to [Section 6.5](#)).



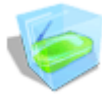
Protocols – View and edit OpenRG's list of supported protocols. This icon redirects to the 'Objects and Rules' tab under 'System' (refer to [Section 8.9.1](#)).



Reboot – Reboot OpenRG. This icon redirects to the 'Maintenance' tab under 'System' (refer to [Section 8.8.3](#)).



Remote Administration – Configure remote administration privileges. This icon redirects to the 'Management' tab under 'System' (refer to [Section 8.7.3](#)).



Restore Defaults – Restore default factory settings. This icon redirects to the 'Maintenance' tab under 'System' (refer to [Section 8.8.4](#)).



Routing – Manage routing policies. This icon redirects to the 'Routing' tab under 'System' (refer to [Section 8.6.1](#)).



SSL VPN – Create a zero-configuration remote connection to OpenRG. This icon redirects to the 'SSL-VPN' tab under 'Services' (refer to [Section 7.10.2](#)).



Scheduler Rules – Define time segments for system rules. This icon redirects to the 'Objects and Rules' tab under 'System' (refer to [Section 8.9.3](#)).



Simple Network
Management
Protocol (SNMP)

SNMP Protocol – Configure OpenRG's SNMP agent. This icon redirects to the 'Management' tab under 'System' (refer to [Section 8.7.2](#)).



System Log

System Log – View, download or clear the system activities log. This icon redirects to the 'Monitor' tab under 'System' (refer to [Section 8.5.3](#)).



System Settings – Modify administrator settings, including OpenRG's hostname. This icon redirects to the 'Settings' tab under 'System' (refer to [Section 8.2](#)).



Universal Plug and Play – Configure UPnP parameters. This icon redirects to the 'Management' tab under 'System' (refer to [Section 8.7.1](#)).



Users – Configure OpenRG's users and their permissions. This icon redirects to the 'Users' tab under 'System' (refer to [Section 8.3](#)).



WINS Server – Register host names and IP addresses of WINS clients. This icon redirects to the 'Storage' tab under 'Services' (refer to [Section 7.11.3](#)).



Web Server – Host a Web site on your gateway. This icon redirects to the 'Storage' tab under 'Services' (refer to [Section 7.11.4](#)).



RADIUS Server – Authenticate wireless clients with a RADIUS server (refer to [Section 7.13.4](#)).

Part III. Additional Features

Table of Contents

10. Zero Configuration Technology	719
10.1. IP Auto-detection	719
10.2. Automatic Configuration for Non-Plug-and-Play Networks	720
10.3. Network Map Builder	720

10

Zero Configuration Technology

Zero Configuration Technology is a communication architecture that automates different procedures on OpenRG, omitting the need for complex user configuration. This technology is an extension of OpenRG's Universal Plug-and-Play support for seamless compatibility between networking equipment, software and peripherals (refer to [Section 8.7.1](#)). OpenRG's zero configuration technology consists mainly of the following technologies:

- IP auto-detection
- Automatic configuration for non-Plug-and-Play networks
- Network map builder

10.1. IP Auto-detection

This module enables the gateway to identify manually pre-configured static IP devices, in addition to its DHCP clients. The DHCP server dynamically assigns IP addresses to DHCP clients that are connected to the network, from a pool of IP addresses. By automatically doing so, it eliminates the home user's need to configure the LAN PC with a complicated IP address, accompanied with additional settings such as network mask and default gateway. However, many users still use manually pre-configured static IP addresses, and generally gateways do not have information regarding such static IP addresses used by the different LAN PCs. The IP auto-detection method detects and learns all the IP addresses on the LAN, and integrates the collected information with the available 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. OpenRG's IP auto detection achieves a complete coverage of the network IP addresses. The gateway sends a set of requests on the network periodically, and collects the replies. Unknown IP addresses are added to the DHCP list and excluded from the pool of addresses for allocation.

10.2. Automatic Configuration for Non-Plug-and-Play Networks

The automatic configuration for non-Plug-and-Play networks enables any device on the LAN to immediately connect to the WAN, regardless of its current configuration. Computers in your network may carry preset configurations of non-plug-and-play networks. For example, mobile PCs that are statically configured to work in the office but not at home. In order to connect to a residential gateway at home, these computers must be reconfigured. A standard residential gateway is unable to establish data connection with such device, unless the user adjusts the computer configuration to meet the gateway's pre-configured parameters. OpenRG's automatic configuration technology is capable of understanding the non-Plug-and-Play network topology, and adjusts itself according to the learned parameters. That is, instead of the user having to reconfigure the computer, OpenRG auto-configures the relevant parameters, enabling the computer to connect to the network and to the Web.

10.3. Network Map Builder

The network map builder provides an up to date accurate graphical representation of the LAN network, displaying the devices currently connected to the gateway and their parameters. While the standard network map displays devices with a DHCP lease from OpenRG, with zero configuration technology devices with statically-defined IP addresses are also displayed. The network map builder relies on existing modules, such as the DHCP and the IP auto detection, as well as its own information collectors to assemble the network information. All information is validated and displayed in the network map. The network map builder actively sends various messages to discover which network objects are currently active on the network. Comparing the replies to its list of IP addresses or host names, OpenRG is updated with information on the network view. This data is then validated and translated to a user friendly, graphic map. For more information about the network map, refer to [Section 4.2](#).

Part IV. Appendix

Table of Contents

11. List of Acronyms	723
12. Glossary	725
13. Licensing Acknowledgement and Source Code Offering	735
14. Contact Jungo	736

11

List of Acronyms

ALG	Application-Level Gateway
API	Application Programming Interface
CPE	Customer Premise Equipment
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
DOCSIS	Data Over Cable Service Interface Specification
DSL	Digital Subscriber Line
FTP	File Transfer Protocol
HomePNA	Home Phoneline Network Alliance
HTTP	HyperText Transport Protocol
IAD	Integrated Access Device
ICMP	Internet Control Message Protocol
IGMP	Internet Group Multicast Protocol
IP	Internet Protocol
IPSec	IP Security
LAN	Local Area Network
MAC	Media Access Control
MTU	Maximum Transmission Unit
NAPT	Network Address Port Translation
OAM	Operations and Maintenance
OEM	Original Equipment Manufacturer

PDA	Personal Digital Assistant
POP3	Post Office Protocol 3
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
RG	Residential Gateway
RIP	Routing Information Protocol
SNMP	Simple Network Management Protocol
SPI	Stateful Packet Inspection
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
URL	Universal Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network
WAN	Wide Area Network

12

Glossary

PAP Password Authentication Protocol, the most basic form of authentication, in which a user's name and password are transmitted over a network and compared to a table of name-password pairs. Typically, the passwords stored in the table are encrypted. The Basic Authentication feature built into the HTTP protocol uses PAP.

CHAP Challenge Handshake Authentication Protocol, a type of authentication in which the authentication agent (typically a network server) sends the client program a random value that is used only once and an ID value. The sender and peer must share a predefined secret.

Authentication The process of identifying an individual, usually based on a username and password. In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

Encryption The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.

MPPE Microsoft Point to Point Encryption (MPPE) is a means of representing Point to Point Protocol (PPP) packets in an encrypted form.

Broadcast Broadcasting sends a message to everyone on the network whereas multicasting sends a message to a select list of recipients.

Multicast To transmit a single message to a select group of recipients. A simple example of multicasting is sending an e-mail message to a mailing list. Teleconferencing and videoconferencing also use multicasting, but require more robust protocols and networks.

PPTP Point-to-Point Tunneling Protocol, a technology for creating Virtual Private Networks (VPNs). Because the Internet is essentially an open network, the Point-to-Point Tunneling

Protocol (PPTP) is used to ensure that messages transmitted from one VPN node to another are secure. With PPTP, users can dial in to their corporate network via the Internet.

PPTP IP Security, a set of protocols developed to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks (VPNs).

VPN A Virtual Private Network (VPN) is a private Network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling Protocol and security procedures.

100Base-T Also known as "Fast Ethernet," an Ethernet cable standard with a data transfer rate of up to 100 Mbps.

10Base-T An older Ethernet cable standard with a data transfer rate of up to 10 Mbps.

802.11, 802.11b A family of IEEE (Institute of Electrical and Electronics Engineers)-defined specifications for wireless networks. Includes the 802.11b standard, which supports high-speed (up to 11 Mbps) wireless data transmission.

802.3 The IEEE (Institute of Electrical and Electronics Engineers - defined specification that describes the characteristics of Ethernet (wired) connections.

Access point A device that exchanges data between computers on a network. An access point typically does not have any Firewall or NAT capabilities.

Ad hoc network A solely wireless computer-to-computer network. Unlike an infrastructure network, an ad hoc network does not include a gateway router.

Adapter Also known as a "network interface card" (NIC). An expansion card or other device used to provide network access to a computer, printer, or other device.

Administrator A person responsible for planning, configuring, and managing the day-to-day operation of a computer network. The duties of an administrator include installing new workstations and other devices, adding and removing individuals from the list of authorized users, archiving files, overseeing password protection and other security measures, monitoring usage of shared resources, and handling malfunctioning equipment.

Bandwidth The amount of information, or size of file, that can be sent through a network connection at one time. A connection with more bandwidth can transfer information more quickly.

Bridge A device that forwards packets of information from one segment of a network to another. A bridge forwards only those packets necessary for communication between the segments.

Broadband connection A high-speed connection, typically 256 Kbps or faster. Broadband services include cable modems and DSL.

Broadband modem A device that enables a broadband connection to access the Internet. The two most common types of broadband modems are cable modems, which rely on cable

television infrastructure, and DSL modems, which rely on telephone lines operating at DSL speeds.

Bus A set of hardware lines used for data transfer among the components of a computer system. A bus essentially allows different parts of the system to share data. For example, a bus connects the disk-drive controller, memory, and input/output ports to the microprocessor.

Cable modem A device that enables a broadband connection to access the Internet. Cable modems rely on cable television infrastructure, in other words, the data travels on the same lines as you cable television.

CAT 5 cable Abbreviation for "Category 5 cable." A type of Ethernet cable that has a maximum data rate of 100 Mbps.

Channel A path or link through which information passes between two devices.

Client Any computer or program that connects to, or requests the services of, another computer or program on a network. For a local area network or the Internet, a client is a computer that uses shared network resources provided by a server.

Client/server network A network of two or more computers that rely on a central server to mediate the connections or provide additional system resources. This dependence on a server differentiating a client/server network from a peer-to-peer network.

Computer name A name that uniquely identifies a computer on the network so that all its shared resources can be accessed by other computers on the network. One computer name cannot be the same as any other computer or domain name on the network.

Crossover cable A type of cable that facilitates network communications. A crossover cable is a cable that is used to interconnect two computers by "crossing over" (reversing) their respective pin contacts.

DHCP Acronym for 'Dynamic Host Configuration Protocol'. A TCP/IP protocol that automatically assigns temporary IP addresses to computers on a local area network (LAN). OpenRG supports the use of DHCP. You can use DHCP to share one Internet connection with multiple computers on a network.

Dial-up connection An Internet connection of limited duration that uses a public telephone network rather than a dedicated circuit or some other type of private network.

DMZ Acronym for 'demilitarized zone'. A collection of devices and subnets placed between a private network and the Internet to help protect the private network from unauthorized Internet users.

DNS Acronym for 'Domain Name System'. A data query service chiefly used on the Internet for translating host names into Internet addresses. The DNS database maps DNS domain names to IP addresses, so that users can locate computers and services through user-friendly names.

Domain In a networked computer environment, a collection of computers that share a common domain database and security policy. A domain is administered as a unit with common rules and procedures, and each domain has a unique name.

Domain name An address of a network connection that identifies the owner of that address in a hierarchical format: server.organization.type. For example, <http://www.whitehouse.gov> identifies the Web server at the WhiteHouse, which is part of the U.S. government.

Drive An area of storage that is formatted with a file system and has a drive letter. The storage can be a floppy disk (which is often represented by drive A), a hard disk (usually drive C), a CD-ROM (usually drive D), or another type of disk. You can view the contents of a drive by clicking the drive's icon in Windows Explorer or My Computer. Drive C (also known as the hard disk), contains the computer's operating system and the programs that have been installed on the computer. It also has the capacity to store many of the files and folders that you create.

Driver Within a networking context, a device that mediates communication between a computer and a network adapter installed on that computer.

DSL Acronym for 'Digital Subscriber Line'. A constant, high-speed digital connection to the Internet that uses standard copper telephone wires.

DSL modem A device that enables a broadband connection to access the Internet. DSL modems rely on telephone lines that operate at DSL speeds.

Duplex A mode of connection. Full-duplex transmission allows for the simultaneous transfer of information between the sender and the receiver. Half-duplex transmission allows for the transfer of information in only one direction at a time.

Dynamic IP address The IP address assigned (using the DHCP protocol) to a device that requires it. A dynamic IP address can also be assigned to a gateway or router by an ISP.

Edge computer The computer on a network that connects the network to the Internet. Other devices on the network connect to this computer. The computer running the most current, reliable operating system is the best choice to designate as the edge computer.

Ethernet A networking standard that uses cables to provide network access. Ethernet is the most widely-installed technology to connect computers together.

Ethernet cable A type of cable that facilitates network communications. An Ethernet cable comes in a couple of flavors. there is twisted pair, and coax Ethernet cables. Each of these allow data to travel at 10Mbit per second.

Firewall A security system that helps protect a network from external threats, such as hacker attacks, originating outside the network. A hardware Firewall is a connection routing device that has specific data checking settings and that helps protect all of the devices connected to it.

Firmware Software information stored in nonvolatile memory on a device.

Flash memory A type of memory that does not lose data when power is removed from it. Flash memory is commonly used as a supplement to or replacement for hard disks in portable computers. In this context, flash memory either is built in to the unit or, more commonly, is available as a PC Card that can be plugged in to a PCMCIA slot.

FTP Acronym for 'File Transfer Protocol'. The standard Internet protocol for downloading, or transferring, files from one computer to another.

Gateway A device that acts as a central point for networked devices, receives transmitted messages, and forwards them. OpenRG can link many computers on a single network, and can share an encrypted Internet connection with wired and wireless devices.

Gateway address The IP address you use when you make a connection outside your immediate network.

Hexadecimal A numbering system that uses 16 rather than 10 as the base for representing numbers. It is therefore referred to as a base-16 numbering system. The hexadecimal system uses the digits 0 through 9 and the letters A through F (uppercase or lowercase) to represent the decimal numbers 0 through 15. For example, the hexadecimal letter D represents the decimal number 13. One hexadecimal digit is equivalent to 4 bits, and 1 byte can be expressed by two hexadecimal digits.

HomePNA An industry standard that ensures that through existing telephone lines and a registered jack, computer users on a home network can share resources (such as an Internet connection, files, and printers) without interfering with regular telephone service. HomePNA currently offers data transmission speeds of up to 10 Mbps.

HomeRF An industry standard that combines 802.11b and portable phone standards for home networking. It uses frequency hopping (switching of radio frequencies within a given bandwidth to reduce the risk of unauthorized signal interception). HomeRF offers data transmission speeds of up to 1.6 Mbps at distances of up to 150 feet.

Host name The DNS name of a device on a network, used to simplify the process of locating computers on a network.

Hub A device that has multiple ports and that serves as a central connection point for communication lines from all devices on a network. When data arrives at one port, it is copied to the other ports.

IEEE Acronym for 'Institute of Electrical and Electronics Engineers'. A society of engineering and electronics professionals that develops standards for the electrical, electronics, computer engineering, and science-related industries. The IEEE (Eye-triple-E) is a non-profit, technical professional association of more than 377,000 individual members in 150 countries. The full name is the Institute of Electrical and Electronics Engineers, Inc., although the organization is most popularly known and referred to by the letters I-E-E-E.

Infrastructure network A network configuration in which wireless devices connect to a wireless access point (such as OpenRG) instead of connecting to each other directly.

Internet domain In a networked computer environment, a collection of computers that share a common domain database and security policy. A domain is administered as a unit with common rules and procedures, and each domain has a unique name.

Intranet A network within an organization that uses Internet technologies (such as Web browser for viewing information) and protocols (such as TCP/IP), but is available only to certain people, such as employees of a company. Also called a private network. Some intranets offer access to the Internet, but such connections are directed through a Firewall.

IP Acronym for 'Internet Protocol'. The protocol within TCP/IP that is used to send data between computers over the Internet. More specifically, this protocol governs the routing of data messages, which are transmitted in smaller components called packets.

IP address Acronym for 'Internet Protocol' address. IP is the protocol within TCP/IP that is used to send data between computers over the Internet. An IP address is an assigned number used to identify a computer that is connected to a network through TCP/IP. An IP address consists of four numbers (each of which can be no greater than 255) separated by periods, such as 192.168.1.1.

ISO/OSI reference model Abbreviation for "International Organization for Standardization Open Systems Interconnection" reference model. An architecture that standardizes levels of service and types of interaction for computers that exchange information through a communications network. The ISO/OSI reference model separates computer-to-computer communications into seven protocol layers, or levels; each builds on and relies on the standards contained in the levels below it. The lowest of the seven layers deals solely with hardware links; the highest deals with software interactions at the program level. It is a fundamental blueprint designed to help guide the creation of hardware and software for networks.

ISP Acronym for 'Internet service provider'. A company that provides individuals or companies access to the Internet.

Kbps Abbreviation of 'kilobits per second'. Data transfer speed, as through a modem or on a network, measured in multiples of 1,000 bits per second.

LAN Acronym for 'local area network'. A group of computers and other devices dispersed over a relatively limited area (for example, a building) and connected by a communications link that enables any device to interact with any other on the network.

MAC address Abbreviation for 'media access control' address. The address that is used for communication between network adapters on the same subnet. Each network adapter is manufactured with its own unique MAC address.

MAC layer Abbreviation for 'media access control' layer. The lower of two sub layers that make up the data-link layer in the ISO/OSI reference model. The MAC layer manages access to the physical network, so a protocol like Ethernet works at this layer.

mapping A process that allows one computer to communicate with a resource located on another computer on the network. For example, if you want to access a folder that resides on another computer, you "map to" that folder, as long as the computer that holds the folder has been configured to share it.

Mbps Abbreviation of 'megabits per second'. A unit of bandwidth measurement that defines the speed at which information can be transferred through a network or Ethernet cable. One megabyte is roughly equivalent to eight megabits.

Modem A device that transmits and receives information between computers.

NAT Acronym for 'network address translation'. The process of converting between IP addresses used within a private network and Internet IP addresses. NAT enables all of the computers on a network to share one IP address.

Network A collection of two or more computers that are connected to each other through wired or wireless means. These computers can share access to the Internet and the use of files, printers, and other equipment.

Network adapter Also known as a 'network interface card' (NIC). An expansion card or other device used to provide network access to a computer, printer, or other device.

Network name The single name of a grouping of computers that are linked together to form a network.

Network printer A printer that is not connected directly to a computer, but is instead connected directly to a network through a wired or wireless connection.

Packet A unit of information transmitted as a whole from one device to another on a network.

PC Card A peripheral device that adds memory, mass storage, modem capability, or other networking services to portable computers.

PCI Acronym for 'Peripheral Component Interconnect'. A specific bus type designed to be used with devices that have high bandwidth requirements.

PCI card A card designed to fit into a PCI expansion slot in a personal computer. PCI cards provide additional functionality; for example, two types of PCI cards are video adapters and network interface cards. See PCI.

PCI expansion slot A connection socket designed to accommodate PCI cards.

PCMCIA Acronym for 'Personal Computer Memory Card International Association'. A nonprofit organization of manufacturers and vendors formed to promote a common technical standard for PC Card-based peripherals and the slot designed to hold them, primarily on portable computers and intelligent electronic devices.

Peer-to-peer network A network of two or more computers that communicate without using a central server. This lack of reliance on a server differentiates a peer-to-peer network from a client/server network.

PING A protocol for testing whether a particular computer is connected to the Internet by sending a packet to the computer's IP address and waiting for a response.

Plug and Play A set of specifications that allows a computer to automatically detect and configure various peripheral devices, such as monitors, modems, and printers.

Port A physical connection through which data is transferred between a computer and other devices (such as a monitor, modem, or printer), a network, or another computer. Also, a software channel for network communications.

PPPoE Acronym for 'Point-to-Point Protocol over Ethernet'. A specification for connecting users on an Ethernet network to the Internet by using a broadband connection (typically through a DSL modem).

Profile A computer-based record that contains an individual network's software settings and identification information.

Protocol A set of rules that computers use to communicate with each other over a network.

Resource Any type of hardware (such as a modem or printer) or software (such as an application, file, or game) that users can share on a network.

Restore factory defaults The term used to describe the process of erasing your base station's current settings to restore factory settings. You accomplish this by pressing the Reset button and holding it for five or more seconds. Note that this is different from resetting the base station.

RJ-11 connector An attachment used to join a telephone line to a device such as a modem or the external telephone lines.

RJ-45 connector An attachment found on the ends of all Ethernet cables that connects Ethernet (wired) cables to other devices and computers

Server A computer that provides shared resources, such as storage space or processing power, to network users.

Shared folder A folder (on a computer) that has been made available for other people to use on a network.

Shared printer A printer (connected to a computer) that has been made available for other people to use on a network.

Sharing To make the resources associated with one computer available to users of other computers on a network.

SNTP Acronym for 'Simple Network Time Protocol'. A protocol that enables client computers to synchronize their clocks with a time server over the Internet.

SSID Acronym for 'Service Set Identifier', also known as a "wireless network name." An SSID value uniquely identifies your network and is case sensitive.

Static IP address A permanent Internet address of a computer (assigned by an ISP).

Straight-through cable A type of cable that facilitates network communications. An Ethernet cable comes in a couple of flavors. There is twisted pair, and coax Ethernet cables. Each of these allow data to travel at 10Mbit per second. Unlike the Crossover cable, straight-through cable has the same order of pin contacts on each end-plug of the cable.

Subnet A distinct network that forms part of a larger computer network. Subnets are connected through routers and can use a shared network address to connect to the Internet.

Subnet mask Typically, a subnet may represent all the machines at one geographic location, in one building, or on the same local area network (LAN). Having an organization's network divided into subnets allows it to be connected to the Internet with a single shared network

address. Similar in form to an IP address and typically provided by an ISP. An example of a subnet mask value is 255.255.0.0.

Switch A central device that functions similarly to a hub, forwarding packets to specific ports rather than broadcasting every packet to every port. A switch is more efficient when used on a high-volume network.

Switched network A communications network that uses switching to establish a connection between parties.

Switching A communications method that uses temporary rather than permanent connections to establish a link or to route information between two parties. In computer networks, message switching and packet switching allow any two parties to exchange information. Messages are routed (switched) through intermediary stations that together serve to connect the sender and the receiver.

TCP/IP Acronym for 'Transmission Control Protocol/Internet Protocol'. A networking protocol that allows computers to communicate across interconnected networks and the Internet. Every computer on the Internet communicates by using TCP/IP.

Throughput The data transfer rate of a network, measured as the number of kilobytes per second transmitted.

USB Acronym for 'universal serial bus'. USB (Universal Serial Bus) is a plug-and-play interface between a computer and add-on devices (such as audio players, joysticks, keyboards, telephones, scanners, and printers). With USB, a new device can be added to your computer without having to add an adapter card or even having to turn the computer off.

USB adapter A device that connects to a USB port.

USB connector The plug end of the USB cable that is connected to a USB port. It is about half an inch wide, rectangular and somewhat flat.

USB port A rectangular slot in a computer into which a USB connector is inserted.

UTP Acronym for 'unshielded twisted pair'. A cable that contains one or more twisted pairs of wires without additional shielding. It's more flexible and takes less space than a shielded twisted pair (STP) cable, but has less bandwidth.

Virtual server One of multiple Web sites running on the same server, each with a unique domain name and IP address.

WAN Acronym for 'wide area network'. A geographically widespread network that might include many linked local area networks.

Wi-Fi A term commonly used to mean the wireless 802.11b standard.

Wireless Refers to technology that connects computers without the use of wires and cables. Wireless devices use radio transmission to connect computers on a network to one another. Radio signals can be transmitted through walls, ceilings, and floors, so you can connect

computers that are in different rooms in the house without physically attaching them to one another.

Wireless access point A device that exchanges data between wireless computers or between wireless computers and wired computers on a network.

Wireless network name The single name of a grouping of computers that are linked together to form a network.

Wireless security A wireless network encryption mechanism that helps to protect data transmitted over wireless networks.

WLAN Acronym for "wireless local area network." A network that exclusively relies on wireless technology for device connections.

13

Licensing Acknowledgement and Source Code Offering

The OpenRG/OpenSMB product may contain code that is subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), and BSD (BSDS) license. The [OpenRG/OpenSMB Open Source and GNU Public Licenses](#) page contains:

- With respect to GPL/LGPL: the code package names, license types and locations for the license files, and
- With respect to BSD (BSDS): the code package names with the license texts.

To receive the source code of the GPL/LGPL packages, refer to http://www.jungo.com/openrg/download_gpl.html.

14

Contact Jungo

For additional support, please contact Jungo Software Technologies Ltd.:

Web site: <http://www.jungo.com>
E-mail: Sales: openrg@jungo.com
 Support: rg_support@jungo.com

Jungo Headquarters
3031 Tisch Way
San Jose, CA 95128
U.S.A
Tel. +1 (408) 423 9540
 +1 (877) 514 0537
Fax. +1 (877) 514 0538

EMEA
One Heathrow Blvd.
286 Bath Road
West Drayton
Middlesex UB7 0DQ
United Kingdom
Tel. +44 (20) 8476 8481
Fax. +44 (20) 8476 8482

Asia Pacific
P.O.Box 118-757 Taipei
Taipei City 10599
Taiwan (R.O.C)
Tel. +886 (9) 1938 2709

R&D Center
1 Hamachshev Street
Netanya 42504
Israel
Tel. +972 (74) 721 2121
Fax. +972 (74) 721 2122