

OxyGEN miniOffice

ADSL2+ Broadband Access Device

Administrator's Guide

*v2.3.0gen
May 2012*

GENNET_{S.A.}

Product and Publication Details

<i>Product Family:</i>	Broadband Access Terminals
<i>Product Name:</i>	Gennet OxyGEN <i>miniOffice</i>
<i>Product Type:</i>	SOHO/SME
<i>Publication Type:</i>	Administrator's Guide
<i>Publication Version:</i>	v2.3.0gen
<i>Publication Date:</i>	May 2012
<i>Language:</i>	English

About This Guide

This guide is designed to assist users in using the Gennet OxyGEN *miniOffice*. Information in this document has been carefully checked for accuracy; however, Gennet s.a. assumes no responsibility or liability for any errors or inaccuracies that may appear in this document. Information as well as drawings and specifications contained in this document are subject to change without prior notice.

Further to the above, some screens, icons, messages, and colors of the information shown in your device may be different from the information presented in this manual due to customization decided by your ISP. The same applies to the device default settings, default passwords and the existence or absence of certain menus, sub-menus or options, which again have been decided in accordance with your ISP policies. This manual should be used in conjunction with the Quick Installation Guide supplied as a printed leaflet in the packaging of your device. In the Quick Installation Guide there is specific information regarding unique functionalities of your ISP and the offered service (e.g. a service activation procedure).

Should you have any inquiries, please feel free to contact support@gennetsa.com. For latest product info and features, visit our website at <http://www.gennetsa.com>.

Declaration of Conformity

Hereby, Gennet s.a. declares that this OxyGEN *miniOffice* device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Safety Rules

The most careful attention has been devoted to quality standards in the manufacture of the OxyGEN *miniOffice*. Safety is a major factor in the design of every set. But, safety is your responsibility too. For your safety, be sure to read and follow all the safety rules:

- Do NOT disassemble the device or the power adapter. Opening or removing covers can expose you to hazardous voltage points or other risks. ONLY qualified service personnel can service the devices. Please contact the vendor for further information.
- Use ONLY the designated power adapter for your device. Connect the power adapter to the appropriate supply voltage, that is, 220V/50Hz AC for Europe.
- Do NOT use the device if the power adapter is damaged, as it might cause electrocution. If the power adapter is damaged, remove it carefully from the power outlet and contact the vendor to order a new one.

- Place connecting cables carefully so that no one will step on them or stumble over them. Do NOT allow anything to rest on the power cable and do NOT place the product where someone can step on the power cable.
- Do NOT install or use your device during a thunderstorm. There may be a remote risk of electric shock from lightning.
- Do NOT expose this device to dampness, dust or corrosive liquids. If liquid is spilled, please refer to the proper service personnel.
- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Do NOT push objects of any kind into the device through ventilation slots. Doing so may be dangerous and may result in fire or electric shock.
- Connect ONLY appropriate accessories to the device.
- Make sure to connect the cables to the correct ports, that the connector matches the port and that you have positioned the connector correctly in relation to the port. Do NOT force a connector into a port. If the connector and port don't join with reasonable ease, they probably don't match.
- When removing the connector from the port remove it by pulling on the connector, not the cable. Some types of connectors have a release clip that releases the connection. Failure to release this clip or abruptly pulling on the cord could cause damage to the connector or the device.

Copyright Declarations

© Gennet s.a., 2012. All rights reserved.

This document contains information that is protected by copyright. It is made available to the end users only for their internal use. No part of this document nor any data herein may be published, disclosed, copied, reproduced, redistributed by any form or means, electronically or mechanically, or used for any other purpose whatsoever without the prior written approval of Gennet s.a.

All copyright, intellectual and industrial rights in this document and in the technical knowledge it contains are owned by Gennet s.a. and/or their respective owners. Any rights not expressly granted herein are reserved.

This product includes copyrighted third-party software licensed under the terms of the GNU General Public License (GPL) or the GNU Lesser General Public License (LGPL). Please see the GNU GPL and LGPL for the exact terms and conditions of these licenses. Source code is available upon request (at cost) and may also be available at the Gennet's website: <http://broadband.gennetsa.com/gpl/> for at

least three years from the purchase date of this product. Note that we do not offer ANY support for the distribution and the source code is distributed WITHOUT ANY WARRANTY and is subject to the copyrights of one or more authors.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)

Artwork was made by or based on artwork by Bosky Cinek (<http://boskastrona.ovh.org>) and Tango Desktop Project (<http://tango.freedesktop.org>) and placed under the Creative Commons attribution share-alike License.

Trademarks

All product and corporate names appearing in this document may or not be registered trademarks or copyrights of their respective companies, and are used only for identification or explanation and to the owners' benefit, without intent to infringe.

- Firefox is a registered trademark of the Mozilla Foundation.
- Internet Explorer is a registered trademark of Microsoft Corporation.
- Safari is a registered trademark of Apple Inc.
- Windows is a registered trademark of Microsoft Corporation.
- Google Chrome is a trademark of Google Inc.

Contents

1	Introduction	19
	Features	20
	Device Requirements	21
	Using this Document	22
	Notational Conventions	22
	Typographical Conventions	22
	Special Messages	22
	Getting Support	23
2	Getting to Know the Device	25
	Parts Check	25
	Front Panel	25
	Rear Panel	26
3	Connecting your Device	29
	Connecting the Hardware	29
	Step 1. Connect the DSL Cable and optional Telephone Line	30
	Step 2. Connect the Ethernet Cable	30
	Step 3. Attach the Power Connector	30
	Step 4. Configure your PC	31
	Next Step	31
4	Getting Started with the Web Pages	33
	Accessing the Web Pages	34
	Navigating through the Menus	36
	Logout	37
	Languages	38
	Home Page Menu	39
	Internet Web Page Menu	40
	Network Web Page Menu	41
	Wireless Web Page Menu	42
	Firewall Web Page Menu	43
	Voice Web Page Menu	44

Advanced Web Page Menu	45
System Web Page Menu	46
Status Web Page Menu	47
Commonly used Buttons and Icons	48
Default Device Settings	49
5 Home - System View	51
Internet Section (left-pane)	52
Network Section (middle-pane)	53
System Section (right-pane)	54
6 Internet Menu	55
Quick Start	56
ATM PVCs	58
Connections	60
Connection	60
ATM Options	61
802.1Q VLAN	62
Modem Options	62
IPv6 Options	62
PPP Options	63
IP Options	63
IP Routing	64
DSL Line	65
External Modems	67
Edit	68
Info	68
7 Network Menu	69
Interface Groups	70
Addresses	71
IPv6 Addresses	71
DHCP	73
Static DHCP Leases	73
LAN IPv6 Addresses	74
DNS Settings	76
Host Aliases	76
Static Routes	78
Dynamic Routing	80
Wake On LAN	81
Public IPs	82
8 Wireless Menu	83

Configuration	84
Security	85
WEP Encryption	85
WPA / WPA2 Encryption	86
MAC Filtering	87
Multiple SSIDs	88
Encryption	88
Hotspot	90
9 Firewall Menu	93
Port Forward	94
UPnP / NAT-PMP	96
IP Filters	97
Web Filters	99
DMZ Filters	100
Address Mapping	101
10 Voice Menu	103
Foreword	104
Voice Service	106
External Lines	107
VoIP	107
ISDN	109
VoIP Trunking	110
Local Extensions	111
DECT Station	113
ISDN Interfaces	114
Dial Plan	117
Restrictions	119
Speed Dials	120
Black List	121
11 Advanced Menu	123
Dynamic DNS	124
Date and Time	125
IPv6 Tunnel	126
SSL VPN	128
Client Mode	128
Server Mode	129
GRE Tunnel	132
VPN Tunnel	133
QoS Policy	135

Device Detection	137
Radius Server	139
File Sharing	141
Printing	142
12 System Menu	143
TR-069	144
SNMP	145
Syslog	146
Backup / Restore	147
Backup Configuration	147
Restore Configuration	148
Firmware Upgrade	149
Remote Admin	151
Users	153
Change Password	154
Device Restart	155
13 Status Menu	157
About	159
Battery	160
System Log	161
Interfaces	162
Ethernet Switch	162
USB Devices	162
DSL Line	163
Wireless	164
Phone Lines	165
Call Details	167
ISDN Interfaces	168
Firewall	169
Clients	170
Diagnostics	171
Net Statistics	172
IP Network	173
14 Troubleshooting	175
Testing your Setup	176
Troubleshooting Suggestions	178
Diagnosing Problem using IP Utilities	180
Ping	180
nslookup	180

A	Configuring the Internet Settings	183
	Configuring Ethernet PCs	183
	Before you Begin	183
	Windows Vista PCs	184
	Windows XP PCs	184
	Windows 2000 PCs	184
	Apple Mac OS X PCs	185
	Assigning Static Internet Information to your PCs	185
	Configuring Wireless PCs	186
	Positioning the Wireless PCs	186
	Wireless PC Cards and Drivers	186
	Configuring PC Access to your Wireless Device	186
B	IP Addresses, Network Masks, and Subnets	189
	IP Addresses	189
	Structure of an IP Address	189
	Network Classes	190
	Subnet Masks	191
C	Network Printing	193
	AppSocket / JetDirect	193
	Internet Printing Protocol (IPP)	194
D	Microsoft Windows and WPA/WPA2 support	197
E	Creating an SSL VPN	199
	General Info	199
	How to Configure SSL-VPN	199
	Routed vs Bridged VPN Tunnel	200
	Server Mode	201
	Client Mode	201
	How to Connect from a PC	202
F	ISDN Interfaces	205
	ISDN Cable Pinout	205
	ISDN S-bus Termination	205
G	Glossary	209

List of Figures

2.1	OxyGEN <i>miniOffice</i> Package Contents	26
2.2	Front Panel and LEDs	26
2.3	Rear Panel Connections	26
3.1	Overview of Hardware Connections	30
4.1	Web Configuration Login	34
4.2	Initial System View - Home	35
4.3	Configuration Menu Help Screen	36
4.4	Left-side Navigation Menu	36
5.1	System View - Home	51
6.1	Quick Start - List of Services	56
6.2	Quick Start - Internet Connection	56
6.3	List of ATM PVCs	58
6.4	New ATM PVC	58
6.5	List of Connections	60
6.6	New Connection - PPPoE	61
6.7	IPv6 Options	63
6.8	DSL Line Parameters	65
6.9	List of External Modems	67
6.10	Edit Modem Parameters	68
6.11	Show Modem Information	68
7.1	Interface Groups	70
7.2	LAN Addresses	71
7.3	IPv6 Addresses	72
7.4	DHCP Server Configuration	73
7.5	Static DHCP Leases	74
7.6	LAN IPv6 Addresses	75
7.7	DNS Settings Configuration	76
7.8	Host Aliases	77
7.9	Static Routing	78
7.10	New Static Route	78

7.11	Dynamic Routing	80
7.12	Host wake on LAN	81
7.13	Public IP Addresses	82
8.1	Wireless Settings	84
8.2	Wireless Security - WEP	85
8.3	Wireless Security - WPA	86
8.4	Wireless MAC Address Filter	87
8.5	Multiple Wireless SSIDs	88
8.6	Wireless Security - Multiple SSIDs	89
8.7	Wireless Hotspot	90
9.1	Port Forwarding	94
9.2	New Port Forwarding	95
9.3	UPnP Configuration	96
9.4	IP Filtering	97
9.5	New IP Filter	98
9.6	Web Filtering	99
9.7	Internet-to-DMZ Protocol Filters	100
9.8	NAT Static Address Mapping	101
10.1	Voice External Lines and Local Extensions	104
10.2	Voice Service	106
10.3	Phone Lines	107
10.4	Phone Lines	108
10.5	Voice Trunking Service	110
10.6	List of Extensions	111
10.7	New Local Extension	112
10.8	List of DECT Handsets	113
10.9	ISDN Voice Interfaces	114
10.10	ISDN Interface Parameters	115
10.11	Voice Dialing Plan	118
10.12	Call Restrictions	119
10.13	Speed Dials	120
10.14	Black List of Numbers	121
11.1	Dynamic DNS	124
11.2	SNTP Client	125
11.3	IPv6 Tunnels	126
11.4	SSL VPN - Client Mode	128
11.5	SSL VPN - Server Mode	130
11.6	SSL VPN Users	131
11.7	GRE Tunnel	132

11.8	L2TP VPN Tunnel	133
11.9	IPSec VPN Tunnel	134
11.10	List of QoS Classes	135
11.11	New QoS Priority Class	135
11.12	STB Auto-detection	137
11.13	Radius Usernames	139
11.14	New Radius Username	140
11.15	Radius Subnet Configuration	140
11.16	File Sharing Service	141
11.17	USB Printer Support	142
12.1	TR-069 Configuration	144
12.2	SNMP Configuration	145
12.3	Syslog Configuration	146
12.4	Configuration Backup/Restore	147
12.5	Backup the Configuration	147
12.6	Local Firmware Upgrade	149
12.7	Automatic Firmware Upgrade	150
12.8	Remote Administration	151
12.9	Users' Management	153
12.10	Change Password	154
12.11	Device Reboot	155
12.12	Reboot Status	155
13.1	Device Status	159
13.2	Battery Status	160
13.3	System Log	161
13.4	System Log Notification	161
13.5	Ethernet Port Status	162
13.6	DSL Line Information	163
13.7	Wireless Network Information	164
13.8	Voice Calls and Services	165
13.9	Service Codes	166
13.10	Call Records	167
13.11	ISDN Interfaces	168
13.12	Current Firewall Status	169
13.13	Connected Clients	170
13.14	Troubleshooting	171
13.15	Network Statistics	172
13.16	IP Network Information	173
13.17	Detailed IP Connection List	174
14.1	Using the Ping Utility	180

14.2 Using the nslookup Utility 181

1

Introduction

Congratulations on becoming the owner of the Gennet OxyGEN *miniOffice*. You will now be able to access the Internet using your high-speed DSL connection supporting data, voice and video services.

This Administrator's Guide will show you how to connect your OxyGEN *miniOffice*, and how to customize its configuration to get the most out of your new product.

Features

The list below contains the main features of the OxyGEN *miniOffice* and may be useful to users with knowledge of networking protocols. If you are not an experienced user, the chapters throughout this guide will provide you with enough information to get the most out of your device. The features include:

- Fully flexible WAN access with the option of 2 DSL (VDSL2 and/or ADSL2+) ports and/or a 10/100/1000Base-T port and/or an SFP connector for high-speed Internet access (model dependent)
- Fully flexible LAN access with the option of 4-port 10/100Base-T switch and/or a 10/100/1000Base-T port to provide Internet connectivity to all computers on your LAN
- 802.11b/g/n WiFi router with multiple external antennas to provide Internet connectivity to all wireless devices on your LAN
- Voice over IP (VoIP) functionality with a variable combination of voice interfaces, FXS and/or FXO and/or ISDN BRI or PRI ports (*number and type of ports depend on model*)
- 1 to 2 USB host interfaces for connecting external storage devices (USB sticks, hard disks), USB printers and USB 3G modems
- Embedded IP PBX functionality with support for external IP phones and (*optional*) internal DECT base-station
- Network Address Translation (NAT) and Firewall functions to provide security for your LAN
- Automatic network configuration through DHCP Server and DHCP Client
- IP services including dynamic IP routing and DNS configuration
- IP and DSL performance monitoring
- User-friendly configuration program accessed via a web browser
- Automatic configuration service
- Increased memory and CPU capacities

Device Requirements

In order to use the OxyGEN miniOffice, you must have the following:

- DSL service up and running on your telephone line
- Instructions from your Internet Service Provider (ISP) on what type of Internet access you will be using, and the parameters needed to set up access
- One or more computers, each containing a wired (10/100Base-T) or wireless (802.11b/g or 802.11b/g/n) Ethernet card (*with WiFi-enabled devices only*).
- For system configuration using the embedded web-based configuration tool: Microsoft Internet Explorer version 5.5 or newer, Mozilla Firefox 1.5 or newer, Google Chrome, Apple Safari version 1.2 or newer

**WARNING**

It is essential that JavaScript is enabled on your Web browser in order to be able to use the embedded Web Configuration tool of the OxyGEN miniOffice.

Using this Document

Notational Conventions

- Acronyms are defined the first time they appear in the text and also in the glossary (**Appendix G** on page 209).
- For brevity, the OxyGEN miniOffice is frequently referred to as "OxyGEN" or "the device".
- The term LAN (Local Area Network) refers to a group of Ethernet-connected computers at one site.

Typographical Conventions

- *Italic* text is used for items you select from menus and drop-down lists and the names of sections in this guide.
- **Bold** text is used for names and parameters of the displayed web pages, and to emphasize important points.

Special Messages

This document uses the following icons to draw your attention to specific instructions or explanations.



Note

Provides clarifying or non-essential information on the current topic.



WARNING

Provides messages of high importance, including messages relating to personal safety or system integrity.

Getting Support

Please visit the web site of Gennet (<http://www.gennetsa.com>) in order to get the most up-to-date information and support for your OxyGEN *miniOffice*.

2

Getting to Know the Device

Parts Check

Your OxyGEN *miniOffice* package should arrive containing the following:

- OxyGEN *miniOffice*
- Ethernet cable (Yellow, RJ-45)
- Standard phone/DSL line cable (Black, RJ-11)
- Serial console cable (RJ-45 to DB-9)
- Power adapter and power cord
- Quick Installation Guide booklet
- CD with this guide



WARNING

If for any reason you do not have any of the items listed above, please contact your Service Provider as soon as possible.

Front Panel

The front panel contains a series of lights, called Light Emitting Diodes (LEDs), that indicate the status of the unit. It, optionally, also contains 1 or 2 USB Host interfaces for connecting an external storage device,

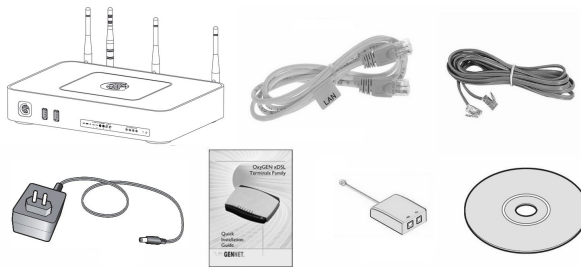


Figure 2.1: OxyGEN miniOffice Package Contents

a USB printer or a USB 3G modem.

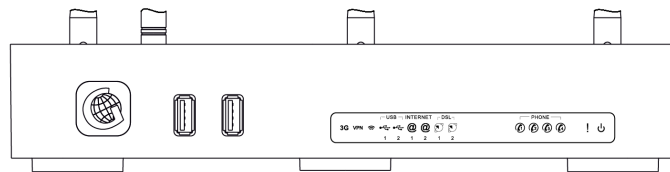


Figure 2.2: Front Panel and LEDs

Examining the front panel from left to right, we can find the ports and LEDs listed in table 2.1.

Rear Panel

The rear panel contains the ports for the device's data, telephony and power connections, the main On/Off switch and a *Restore Defaults* pin button.

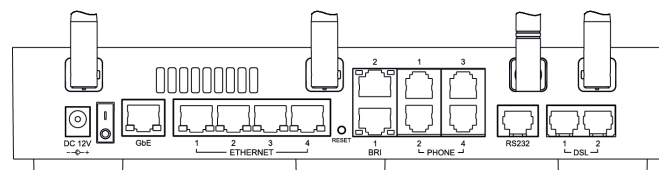


Figure 2.3: Rear Panel Connections

Examining the rear panel from left to right, we can find the ports listed in table 2.2.









Label	Color	Function
USB (1-2)		USB Host interface for connecting external USB devices (e.g. Flash Disk, Printer, Camera). <i>(optional feature)</i>
3G	Green	On: 3G broadband service active. <i>(optional feature)</i>
VPN	Green	On: VPN service active and connected. <i>(optional feature)</i>
Wireless 	Green	On: Wireless service enabled. <i>(WiFi-enabled devices only)</i>
USB  (1-2)	Green	On: Active USB port (device detected). <i>(optional feature)</i>
Internet  (1-2)	Green / Red	Green: Successfully connected to the Internet. Green Blinking: Trying to connect. Red Blinking: Connection error.
DSL  (1-2)	Green	On: Showtime (successfully connected to the DSL network). Slow Blinking: Handshake (idle - no line detected). Fast Blinking: Training (connection attempt).
Phone  (1-4)	Green	Blinking: Phone in the "Off-Hook" state. <i>(voice-enabled devices only)</i>
FXO 	Green	On: Active call through the PSTN network (FXO port). Blinking: New incoming call from the PSTN network. <i>(optional feature)</i>
Alarm 	Red	On: The device is in boot sequence, during a firmware upgrade or has a malfunction / operation error. Off: Normal operation.
Power 	Green	On: Normal operation.

Table 2.1: Front panel ports and LEDs

Label	Function
Reset	Reset button. Pressing this pin button for more than 5 seconds restores the factory default configuration on your device.
DC 12 V	This is where you will connect the power adapter. Please use only the power adapter supplied with your device. ⚠ WARNING: Using a power adapter with a different voltage rating or type will damage your device.
I / O	The main switch of the device. Please make sure it is in the "Off" position before starting the installation procedure.
GbE	10/100/1000 base-T Ethernet interface. This port is Auto-MDIX and therefore for all types of devices you may use a straight Ethernet cable (i.e. no need for a crossover Ethernet cable).
ETHERNET 1-4	10/100 base-T switched Ethernet interfaces. Used for connecting to your LAN's PC, Set-Top Box or external Ethernet switch. These ports are Auto-MDIX and therefore for all types of devices you may use a straight Ethernet cable (i.e. no need for a crossover Ethernet cable).
BRI 1-2	ISDN BRI interfaces. Used for connecting to your private ISDN PBX, ISDN terminal or to the ISDN NT. These ports are configurable and operate either in Network (NT) or in Terminal (TE) mode. When operating in NT mode, a straight ISDN cable is used, whereas when set to operate in TE mode, an ISDN crossover cable is required (Please refer to Appendix F on page 205 for details about the pinout of both cables).
PHONE 1-4	Analog telephony ports (FXS). Used for connecting the Telephone devices. <i>(voice-enabled devices only)</i> ⚠ WARNING: If you are going to use only one analog phone, connect it to port 1 .
RS232	Console port for device management. Connect to your PC using the supplied RJ45-to-DB9 serial cable and manage the device through the Command Line Interface (CLI) application. ➡ Note: Console port settings are 115200, 8N1, no flow-control.
DSL 1-2	DSL ports. Connect the device to telephone ports in the wall of your home/office or to splitters for DSL communication. 3 x External antennas for good wireless 802.11n LAN reception. <i>(WiFi-enabled devices only)</i> 1 x External antenna for good 2G/3G module reception. <i>(optional feature)</i>

Table 2.2: Rear panel ports

3

Connecting your Device

This chapter provides basic instructions for connecting the OxyGEN *miniOffice* to a personal computer or LAN and to the Internet. It is assumed that you have already established a DSL service with your Internet Service Provider (ISP). These instructions provide a basic configuration that should be compatible with your home or small office network setup. Refer to the subsequent chapters for additional configuration instructions.

In addition to configuring the device, you also need to configure the Internet properties of your computer(s). For more details, see sections:

- **Configuring Ethernet PCs** on page 183
- **Configuring Wireless PCs** on page 186 (*WiFi-enabled devices only*)

Connecting the Hardware

This section describes how to connect the device to the power outlet and your personal computer(s) or network.



WARNING

Before you begin, turn the power off for all devices. These include your personal computer(s) and the OxyGEN *miniOffice*.

The diagram below illustrates the hardware connections. The layout of the ports on your device may vary slightly from the layout shown. Refer to the steps that follow for specific instructions.

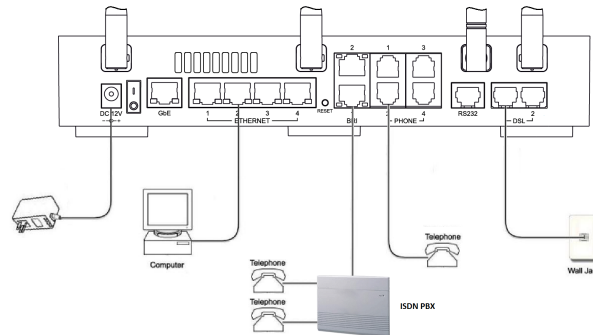


Figure 3.1: Overview of Hardware Connections

Step 1. Connect the DSL Cable and optional Telephone Line

Connect one end of the provided black phone cable to the port labeled **DSL** on the rear panel of the device. Connect the other end to your wall phone port providing the DSL service.

If your device has more than one DSL ports (*optional feature*), these ports are treated completely independently. Use the same procedure for connecting each of them to a separate telephone line providing DSL service.

Step 2. Connect the Ethernet Cable

(If you plan to use a Wireless connection between your PC and the OxyGEN *miniOffice* (*optional feature*), please skip this step and move directly to the next one.) Connect your PC to either one of the Ethernet ports of the device via the supplied yellow Ethernet cable.



Note

All Ethernet ports are Auto-MDIX. Therefore, you can use straight Ethernet cables to connect to either PCs or switches with no need for a crossover Ethernet cable.

Step 3. Attach the Power Connector

Connect the provided AC power adapter to the Power connector on the back of the device and plug the adapter into a wall outlet or power strip. Turn on the OxyGEN *miniOffice*.

**Note**

During the boot-sequence of the OxyGEN miniOffice, the **Alarm LED** is solid Amber. The device is ready for operation when the LED is off.

Step 4. Configure your PC

You may now have to configure the Internet properties on your Ethernet PC. See **Configuring Ethernet PCs** on page 183, if using a wired Ethernet connection, or **Configuring Wireless PCs** on page 186, if planning to use a wireless one (*WiFi-enabled devices only*).

Next Step

After setting up the OxyGEN miniOffice and configuring your PC, you can log on to the device by following the instructions in **Getting Started with the Web Pages** on page 33. Using the Web Configuration tool you will be able to setup all the functionality related to your Internet service.

This guide includes also a chapter called **Troubleshooting** (page 175), which enables you to find solutions to common problems that hinder your device from working properly.

4

Getting Started with the Web Pages

The OxyGEN *miniOffice* includes a web configuration tool that provides an interface to the software installed on the device. It enables you to configure the device settings to meet the needs of your network. You can access it through a web browser on a PC connected to the device.



Note

Some screens, icons, messages, and colors of the information shown in your device may be different from the information presented in this manual, due to the capabilities of the exact model you are using and due to customization decided by your ISP. The same applies to the device default settings, default passwords and the existence or absence of certain menus, sub-menus or options, which again have been decided in accordance with your ISP policies.

Accessing the Web Pages

To access the web pages, you need the following:

1. A laptop or PC connected to the LAN port on the device.
2. A JavaScript enabled web browser installed on the PC. The minimum browser version requirement is Microsoft Internet Explorer version 5.5 or newer, Mozilla Firefox 1.5 or newer, Google Chrome, Apple Safari version 1.2 or newer.
3. Launch your web browser, type <http://oxygen.lan> or <http://192.168.1.254> in the web address (or location) box, and press **[Enter]** on your keyboard.
4. An access control screen appears. Enter the correct username and password.

The default username and password combination is **admin** and **admin** respectively.

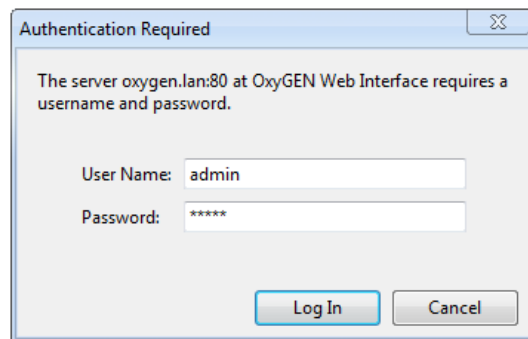


Figure 4.1: Web Configuration Login



Note

OxyGEN miniOffice offers two different levels of administration profiles: simple user mode (default username/password combination is **user/user**), and administrator mode (default username/password combination is **admin/admin**).

5. After successful login, the home page opens displaying the **System View** page with an overview of the device:

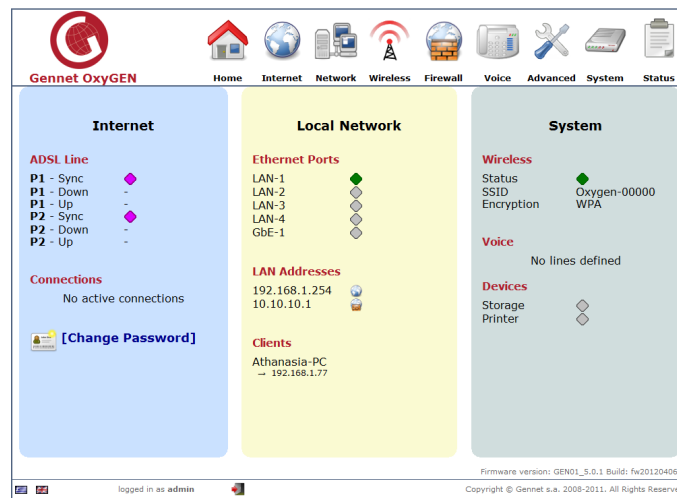


Figure 4.2: Initial System View - Home

Navigating through the Menus

At the top of the screen you can see the main configuration menu, which displays the company's logo and all the configuration menu categories. This menu is constantly visible during the use of the web configuration tool. It comprises the categories described in the following sections, with each menu category (except **Home**) providing different configuration options.



Note

The exact sub-menu entries available under each main menu category may vary depending on the administration mode (i.e. **admin** or **user** account) used for logging into the Web Configuration tool and on the exact firmware version that runs on your OxyGEN miniOffice.

Clicking on the desired menu category icon, leads to a screen with a brief description about the functionality of each sub-menu entry.

Network	
Interface Groups	Split physical interfaces and Internet connections into different "service groups" (private VLANs)
VLAN	Configure 802.1Q VLAN settings
Addresses	Specify the IP address of each Interface Group
DHCP	Configure the DHCP server for each Interface Group
DNS Settings	Modify the local DNS server settings
Static Routes	View and configure static IP routing rules
Wake On LAN	Remotely turn on computers in the LAN
Public IPs	Specify public IPs directly accessible from the Internet


Figure 4.3: Configuration Menu Help Screen

Selection of a sub-menu entry can be performed by clicking on its title (bold red letters) or using the navigation menu on the left side of the screen (see figure 4.4). The latter is always visible, in order to assist further navigation through the different configuration options.

Network
Interface Groups
Addresses
DHCP
DNS Settings
Static Routes

Figure 4.4: Left-side Navigation Menu

Logout

At the bottom of the screen you can always see a field containing Gennet's Copyright notice, the firmware version and the current administration mode (i.e. the username used for login). At any moment you can logout from the web configuration tool of the OxyGEN *miniOffice* by pressing on the icon .

Languages

The OxyGEN *miniOffice* optionally offers localized versions of the web configuration tool. In this case, the flags of the available languages are displayed in the field at the bottom of the screen. At any moment, you can switch language by clicking on the corresponding flag.

Home Page Menu

This is by default the page displayed after login. It provides an overview of the system and is divided into three main sections:

Internet Section (left-pane) - displays Internet-related information about the device.

Internet Section (left-pane) - displays LAN-related information about the device.

System Section (right-pane) - displays information about the Wireless (*WiFi-enabled devices only*), Voice (*voice-enabled devices only*), USB Host (*optional feature*) and other functionality of the device.

Internet Web Page Menu

The **Internet** menu allows the configuration and management of the broadband access connections.

It includes the following sub-menus:

- **Quick Start** for quick configuration of Internet access (see page [56](#))
- **ATM PVCs** for modifying existing or adding new ATM virtual circuits (see page [58](#))
- **Connections** for modifying existing or adding new Internet connections (see page [60](#))
- **DSL Line** for configuring the DSL line settings (see page [65](#))
- **External Modems** for managing the connected external (USB) modems (see page [67](#))

Network Web Page Menu

The **Network** menu provides configuration options for the LAN with the locally connected PCs and other IP-enabled devices.

It includes the following sub-menus:

- **Interface Groups** for splitting the local interfaces into different "service groups" (private VLANs) (see page [70](#))
- **Addresses** for specifying the IP address of each Interface Group (see page [71](#))
- **DHCP** for configuring the DHCP server for each Interface Group (see page [73](#))
- **DNS Settings** for modifying the local DNS server settings (see page [76](#))
- **Static Routes** for viewing and configuring static IP routing rules (see page [78](#))
- **Dynamic Routing** for configuring dynamic IP routing protocols (see page [80](#))
- **Wake On LAN** for remotely turning on computers on the LAN (see page [81](#))
- **Public IPs** for configuring on the LAN public IPs directly accessible from the Internet (see page [82](#))

Wireless Web Page Menu

The **Wireless** menu provides configuration options for the Wireless functionality of the OxyGEN *miniOffice* (*WiFi-enabled devices only*).

It includes the following sub-menus:

- **Configuration** for activation/deactivation and configuration of the wireless LAN (see page [84](#))
- **Security** for activation and configuration of security on the wireless LAN (see page [85](#))
- **MAC Filtering** for enabling wireless access control based on the MAC address of the devices (see page [87](#))
- **Multiple SSIDs** for activating multiple SSIDs on the wireless LAN (see page [88](#))
- **Hotspot** for controlling the captive-portal functionality optionally offered by the OxyGEN *miniOffice* (see page [90](#))

Firewall Web Page Menu

The **Firewall** menu provides configuration options for the protection of the LAN through the embedded firewall of the OxyGEN *miniOffice*.

It includes the following sub-menus:

- **Port Forward** for allowing selected incoming connections from the Internet, in order to enable some applications to work behind the firewall (see page [94](#))
- **UPnP / NAT-PMP** for activation/deactivation of automatic firewall port forwarding using the UPnP and/or NAT-PMP protocols (see page [96](#))
- **IP Filters** for allowing or denying IP connections between the LAN and the Internet (see page [97](#))
- **Web Filters** for allowing or denying access to web sites based on keywords (see page [99](#))
- **DMZ Filters** for configuring a subnet on the internal network that has its hosts selectively exposed to access from the Internet (see page [100](#))
- **Address Mapping** for configuring the use of different public (WAN) IPs from different LAN hosts using Network Address Translation (NAT) (see page [101](#))

Voice Web Page Menu

The **Voice** menu lets you configure the parameters necessary for the provision of the voice service over your broadband connection.

It includes the following sub-menus:

- **Voice Service** for setting-up the main parameters of the VoIP telephony service (see page [106](#))
- **External Lines** for configuring the external phone lines (see page [107](#))
- **VoIP Trunking** for configuring the voice trunking functionality (see page [110](#))
- **Local Extensions** for configuring the local extensions (see page [111](#))
- **DECT Station** for configuring the DECT base station (see page [113](#))
- **ISDN Interfaces** for setting-up the ISDN voice interfaces (*optional feature*) (see page [114](#))
- **Dial Plan** for setting-up the voice dialing patterns (see page [117](#))
- **Restrictions** for setting-up the voice dialing restrictions (see page [119](#))
- **Speed Dials** for configuring quick-dialing patterns (see page [120](#))
- **Black List** for configuring black-listed incoming numbers (see page [121](#))

Advanced Web Page Menu

The **Advanced** configuration menu lets you control a series of different advanced services offered by the OxyGEN miniOffice.

It includes the following sub-menus:

- **Dynamic DNS** for configuring the Dynamic DNS application (see page [124](#))
- **Date and Time** for changing date and time protocol settings (see page [125](#))
- **SSL VPN** for setting-up a secure SSL-based VPN connection using OpenVPN (see page [128](#))
- **GRE Tunnel** for setting-up a Generic Routing Encapsulation tunnel (see page [132](#))
- **VPN Tunnel** for setting-up an L2TP and/or IPSec-based VPN tunnel (see page [133](#))
- **QoS Policy** for defining and configuring Quality of Service classes (see page [135](#))
- **Device Detection** for setting-up a LAN device (e.g. Set-top box (STB) or VoIP phone) auto-detection mechanism (see page [137](#))
- **Radius Server** for configuring the embedded Radius server (see page [139](#))
- **File Sharing** for activation/deactivation of file sharing through connected USB storage devices (see page [141](#))
- **Printing** for activation/deactivation of USB printer support (see page [142](#))

System Web Page Menu

The **System** menu provides system administration utilities such as firmware upgrade, configuration backup & restore, and Syslog service configuration.

It includes the following sub-menus:

- **TR-069** for activation/deactivation and configuration of the TR-069 remote management protocol (see page [144](#))
- **SNMP** for configuration of the Simple Network Management Protocol (see page [145](#))
- **Syslog** for controlling the system logging service (see page [146](#))
- **Backup / Restore** for backing-up the current or restoring a previous configuration of the device (see page [147](#))
- **Firmware Upgrade** for performing a local or remote firmware upgrade (see page [149](#))
- **Remote Admin** for allowing remote access to the device for administration and/or support purposes (see page [151](#))
- **Users** for activation/deactivation of system user accounts (see page [153](#))
- **Change Password** for modifying the device administration password (see page [154](#))
- **Device Restart** for restarting the device and optionally erasing the entire configuration (factory defaults) (see page [155](#))

Status Web Page Menu

The **Status** menu lets you view device messages, the values of device parameters and statistics about local interfaces and Internet connections.

It includes the following sub-menus:

- **About** for displaying general information about the device (see page [159](#))
- **Battery** for displaying information about the embedded battery of the OxyGEN miniOffice (see page [160](#))
- **System Log** for viewing system log entries (see page [161](#))
- **Interfaces** for displaying information for the Ethernet and (*optional*) USB interfaces (see page [162](#))
- **DSL Line** for displaying status and statistics for the DSL broadband connection (see page [163](#))
- **Wireless** for a list of the connected WiFi clients and access points (AP) in range (*WiFi-enabled devices only*) (see page [164](#))
- **Phone Lines** for viewing information about the active voice calls and the status of supplementary services (see page [165](#))
- **Call Details** for viewing total duration and history of voice calls (see page [167](#))
- **ISDN Interfaces** for viewing information about the ISDN interfaces (see page [168](#))
- **Firewall** for displaying the current firewall status (see page [169](#))
- **Clients** for a list of connected clients (see page [170](#))
- **Diagnostics** for performing DSL and IP diagnostic tests (see page [171](#))
- **Net Statistics** for information about the LAN- and WAN-side network traffic (see page [172](#))
- **IP Network** for a list of addresses of IP interfaces, IP routes, DNS servers and active IP connections (see page [173](#))

Commonly used Buttons and Icons

The following buttons and icons are used throughout the web pages:








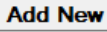


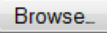
Button	Function
<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	Radio buttons - these appear in many configuration pages. You will be asked to select one radio button from the list of two or more available options. You cannot select more than one radio button at a time.
	This button appears in pages showing lists of configuration items (e.g. Internet connections, Firewall rules). Click on this button to <i>Edit</i> the corresponding entry.
	This button appears in pages showing lists of configuration items (e.g. Internet connections, Firewall rules). Click on this button to <i>Delete</i> the corresponding entry.
	This icon corresponds to the Internet <i>Data</i> service.
	This icon corresponds to the telephony <i>Voice</i> service (if provided by your ISP).
	This icon corresponds to the <i>Video</i> service (if provided by your ISP).
	This icon corresponds to the <i>DMZ</i> service.
	This icon corresponds to the <i>Ethernet WAN</i> service.
	This button appears in pages showing lists of configuration items (e.g. Internet connections, Firewall rules). Click on this button to <i>Add</i> a new entry.
	This button appears in pages related to adding or editing a member of a configuration list (e.g. Internet connection, Firewall rule). Click on this button to <i>Save</i> the entry.
	This button appears in most configuration pages. Click on this button to store and <i>Apply</i> the values of the different parameters appearing in the web page.
	This button appears in pages where a file must be uploaded (e.g. <i>Firmware Upgrade</i>). Click on this button to <i>Browse</i> through your PC and find the desired file.

Table 4.1: Common Buttons and Icons

The following terms are used throughout this guide in association with these buttons:

Click - point the mouse arrow over the button, menu entry or link on the screen and click the left mouse button. This performs an action, such as displaying a new page or performing the action specific to the button on which the left mouse button is clicked.

Select - usually used when describing which radio button to select from a list, or which entry to select from a drop-down list. Point the mouse arrow over the entry and left-click to select it. This does not perform an action - you will also be required to click on a button, menu entry or link in order to proceed.

Default Device Settings

Upon delivery, the OxyGEN *miniOffice* is preconfigured with default settings for use in a typical home or small office network.

The table below lists some of the most important default settings; these and other features are described fully in the subsequent chapters. If you are familiar with network configuration, review these settings to verify that they meet the needs of your network. Follow the instructions to change them if necessary. If you are unfamiliar with these settings, try using the device without modification, or contact your ISP for assistance.

Option	Default Setting
LAN	Hostname: oxygen.lan IP address: 192.168.1.254 Subnet mask: 255.255.255.0
DHCP	Enabled, 192.168.1.51 - 100
WAN Connection	PVC: 8/35 Type: PPPoE Encap.: LLC
NAT / Firewall	Enabled
Wireless	Enabled, SSID: Oxygen-XXXXX, <i>(XXXXX is different for every device)</i> Security: WPA, <i>Key: Different for each device,</i> <i>printed on the label of the device</i> <i>(WiFi-enabled devices only)</i>
Web Configuration	admin / admin user / user

Table 4.2: Default Settings



WARNING

We strongly recommend that you contact your ISP prior to changing the default configuration.

5

Home - System View

The **Home** web page is the default page displayed after login. It provides an overview of the system with the most important status information.

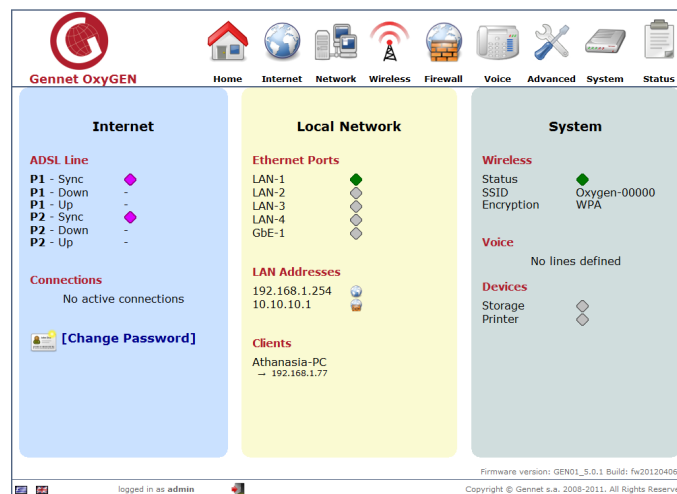


Figure 5.1: System View - Home

The **Home** web page is divided into three main sections:

Internet Section (left-pane)

This section displays Internet-related information about the device. First of all, it displays the DSL synchronization status of the device, according to the following color-codes:







Icon	DSL Status
 Magenta	Handshake (Idle)
 Orange	Training
 Green	Synchronized

Table 5.1: DSL Status Colors

If synchronization has succeeded, the achieved **Downstream** and **Upstream** data rates are also displayed.

Below the DSL sync data, on the same pane, there is also information about the WAN Connections. All configured WAN connections are listed with an indication of their current status (**red icon**: disconnected, **green IP**: connected, **other**: status/error messages).

Network Section (middle-pane)

This section displays information about the Local Area Network and the connected IP devices. On the upper side of the section, there is information about the link status of the Ethernet ports of the OxyGEN *miniOffice*. Below the link information, the user can see the private IP addresses assigned to each of the active *Interface Groups* (private VLANs - one for each service of a multi-service broadband connection). The icons , , and  correspond to the *Data*, *Voice* and *Video* services respectively. Finally, in the bottom part of the section, a list of the local hosts is displayed.

System Section (right-pane)

This section displays information about the Wireless LAN (*WiFi-enabled devices only*), the Voice service (*voice-enabled devices only*) and the devices connected to the USB Host port (*optional feature*). The information presented includes the Status, SSID (Network Name) and Security Mode for the Wireless LAN, the Numbers of the active VoIP connections along with their registration status and finally the status of the USB services.



Internet Menu

The **Internet** configuration web page menu allows the configuration of ATM PVCs, Internet connections and the DSL or other external modem functionality (*optional feature*). Available configuration options include:

- **Quick Start**
- **ATM PVCs**
- **Connections**
- **DSL Line**
- **External Modems**

Quick Start

The **Quick Start** page is the fast and easy way to configure your device for Internet access and any other service provided by your ISP over the broadband connection.

The first thing shown when the **Quick Start** configuration option is selected, is a list of the available service options.

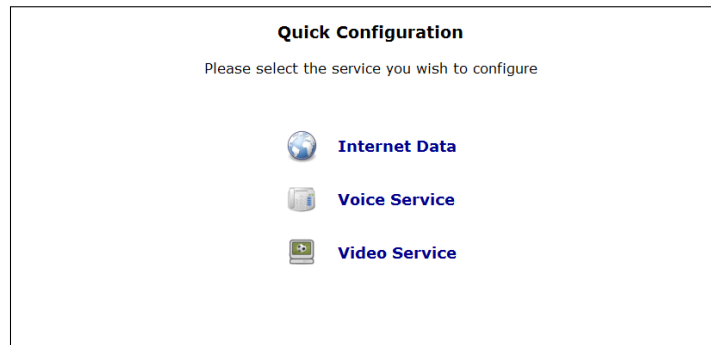


Figure 6.1: Quick Start - List of Services

Click on the desired entry from the list. Following the link will lead you to the corresponding configuration page.

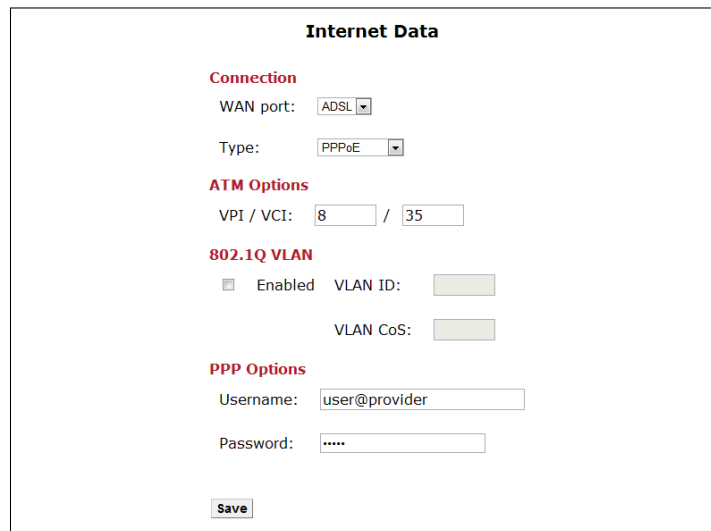
The screenshot shows the "Internet Data" configuration page. It has several sections: "Connection" with "WAN port" set to "ADSL" and "Type" set to "PPPoE"; "ATM Options" with "VPI / VCI" set to "8 / 35"; "802.1Q VLAN" with an unchecked "Enabled" checkbox and empty "VLAN ID" and "VLAN CoS" fields; and "PPP Options" with "Username" set to "user@provider" and "Password" masked with dots. A "Save" button is at the bottom.

Figure 6.2: Quick Start - Internet Connection

This page contains the minimum information required in order to configure the WAN connection supporting the service. Please refer to section **Connections** on page 60 for a detailed description of all parameters.

By clicking the **Save** button, the information entered is stored and the connection is dialed.

Repeat the procedure for all services supported by your ISP.

ATM PVCs

Asynchronous Transfer Mode (ATM) is the underlying technology used for providing IP connectivity over the ADSL broadband connection. Permanent Virtual Circuits (PVC) over the ATM network serve as point-to-point links from the DSL access device (the OxyGEN miniOffice) to the core network of the ISP. WAN ADSL connections are always associated with an ATM PVC. Note that, in certain cases, multiple WAN connections may share the same ATM PVC.

Following the **ATM PVCs** configuration option, a list of the configured PVCs is displayed.

ATM Virtual Circuits				
VPI	VCI	Protocol	Action	
1-PVC_0	8	35	rfc1483br	
1-PVC_1	8	36	rfc1483br	

Figure 6.3: List of ATM PVCs

You can *Edit* and *Delete* configured PVCs by clicking on the icons and respectively of **Action** column.

In order to add a new ATM PVC, press **Add New**. The following screen will appear:

ATM Virtual Circuit 1-PVC_0

DSL Port
Port 1

PVC
VPI: VCI:

Protocol

for PPPoE, bridged and routed EoA connections

Encapsulation

QoS
Traffic Class:

PCR:

SCR:

Figure 6.4: New ATM PVC

These are the basic parameters used to describe the ATM PVC over the ADSL connection:

1. The **DSL Port** drop-down list allows the selection of the DSL interface the new ATM PVC will apply to.
2. **VPI** and **VCI** are the characteristic numbers defining the PVC. Valid VPI and VCI numbers are between 0 and 255 and between 0 and 65535 respectively.
3. **Protocol** defines the type of connection this PVC is going to be used with. Available options are *RFC 1483/2684 bridged* (for PPPoE and EoA connections), *RFC 1483/2684 routed* (for IPoA connections) and *RFC 2364* (for PPPoA connections).
4. **Encapsulation** is the type of service encapsulation used over the ATM connection. Available options are *LLC* (Logical Link Control) and *VCMux* (VC Multiplexing).
5. **Traffic Class** and **PCR** are the ATM QoS traffic class of the connection and the Peak Cell Rate value respectively. Available **Traffic Class** options are *CBR* (Constant Bit Rate), *VBR-rt* (Variable Bit Rate - real time), *VBR-nrt* (Variable Bit Rate - non real time) and *UBR* (Unspecified Bit Rate).

**WARNING**

Please consult your Service Provider about the values that must be used for all the parameters listed above. If the PVCs configured on your OxyGEN miniOffice do not have the same type and VPI/VCI values with the ones used by your Service Provider, no data communication will be possible.

**Note**

The first digit of the name of each ATM PVC refers to the DSL port ID the PVC applies to. For example, 1-PVC_x are PVCs of DSL port 1.

Connections

More detailed handling of the WAN connections, compared to **Quick Start**, can be achieved through the **Connections** configuration option. Entering the sub-menu, the first thing displayed is a list of all configured WAN connections with their current status.

Service	Port	Type	Status	Action
quick_data	1-PVC_0	PPPoE	Active	Edit, Delete, Dial, Disconnect
quick_voice	1-PVC_1	Routed EoA	Active	Edit, Delete, Dial, Disconnect

Add New

Figure 6.5: List of Connections

You can *Edit* and *Delete* configured connections by clicking on the icons and respectively of **Action** column. You can also *Dial* or *Disconnect* any connection by clicking on the icons and respectively of the same column.

In the previous Figure, the connection named *quick_data*, is the one created through the **Quick Start** procedure for the *Data* service.

In order to add a new WAN connection, click **Add New** and the following page will appear. The parameters of this page are explained in detail in the following sub-sections.

Connection

These are the basic parameters used to describe the connection:

1. **Name** is a name used in order to distinguish between the different connections. Note that names must be unique among different connections and that, once configured, they cannot be modified.
2. **Service** is the type of service this connection will support. Available options are *Data*, *Voice* and *Video* (when offered by your ISP).
3. **WAN port** is the type of port this connection will use. Available options are *ADSL*, *Ethernet (optional feature)* and *USB (optional feature)*.

Connection quick_data

Connection

Name:

Status: Enabled Disabled

Service:

WAN port:

Type:

ATM Options

PVC:

VPI / VCI: /

Encapsulation:

802.1Q VLAN

Enabled VLAN ID:

VLAN CoS:

PPP Options

Username:

Password:

MTU size:

PPPoE passthrough:

IP Routing

Default route:

Figure 6.6: New Connection - PPPoE

4. **Type** is the protocol used for connecting to your broadband Service Provider. The available options depend on the selection of the **WAN port** parameter. Please consult your Service Provider about the option that must be selected.

The parameters appearing on the rest of the configuration page, depend mainly on the values of the **WAN port** and **Type** parameters.

ATM Options

These parameters appear only for ADSL connections and define the ATM PVC over which the WAN connection will be performed. From the drop-down list you can select an existing PVC or configure a **NEW** one providing values for the **VPI**, **VCI** and **Encapsulation** parameters.

When multiple DSL ports are present (*optional feature*), the **Px** characters indicate which DSL port this ATM-PVC refers to (e.g. **P1** is port 1).

802.1Q VLAN

In case of *PPPoE* or *EoA* ADSL connections and of any type of VDSL or Ethernet connection, the Ethernet frames can optionally be tagged with a 802.1Q VLAN ID. This way, multiple connections can share the same ATM PVC, VDSL or Ethernet WAN port, separated at the Ethernet level using normal Ethernet VLANs. In order to activate this functionality for the connection, select the **Enabled** checkbox and specify the corresponding **VLAN ID**. Valid **VLAN ID** values are 1 to 4094.

Additionally, all outgoing Ethernet frames through this connection can also be marked with a specific 802.1p Class of Service (CoS) value for Quality of Service on the Ethernet level. Valid **VLAN CoS** values are between 0 and 7.

Modem Options

This provides the parameters required in the case of broadband access through a modem connected to the USB port of the OxyGEN miniOffice (*optional feature*).

1. **External modem** is the USB modem used for this connection, or *ANY MODEM* in order to use the first modem detected. Refer to section **External Modems** on page 67 for a description of the configurations steps required in order to define an external modem.
2. **Profile** is the set of parameters used in case of a USB 3G modem. Pre-defined sets of parameters can be selected, whereas *CUSTOM* allows the user to manually enter the modem-related parameters.
3. **APN** is the Access Point Name used to determine how the 3G modem of the OxyGEN miniOffice communicates via the GSM network to the Service Provider's network.
4. **Init string** is the modem initialization string.
5. **Dial string** is the modem dial string.



WARNING

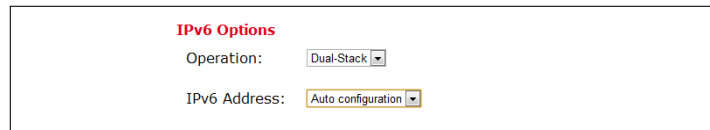
Please refer to your GSM/3G Service Provider in order to find the correct **APN**, **Init string** and **Dial string** values, in case you do not use one of the pre-defined profiles.

IPv6 Options

In case IPv6 functionality is enabled in OxyGEN miniOffice (please refer to section **IPv6 Addresses**), there are the following options:

1. **Operation** may be defined between plain **IPv4**, plain **IPv6** and **Dual Stack**.

2. **IPv6 Address** may be selected between **Auto Configuration**, which allows for WAN interface to be autoconfigured for an IPv6 prefix through the remote server and **Link Local**, where the WAN interface obtains only a link-local IPv6 address.



The screenshot shows a configuration window titled "IPv6 Options". It contains two dropdown menus: "Operation" set to "Dual-Stack" and "IPv6 Address" set to "Auto configuration".

Figure 6.7: IPv6 Options

PPP Options

These are the PPP authentication parameters required in the case of a *PPPoE*, *PPPoA* or *USB PPP* connection:

1. **Username** is the username used for the PPP negotiation with your Service Provider. Please consult your Service Provider about the correct value.
2. **Password** is the password used for the PPP negotiation with your Service Provider. Please consult your Service Provider about the correct value.
3. **MTU size** is the Maximum Transmission Unit (MTU) size in bytes of the PPP connection interface.
4. **PPPoE passthrough** enables or disables the transparent forwarding of PPPoE sessions initiated from a LAN host (e.g. a PC) towards the WAN in case of *RFC 1483/2684 bridged ATM PVCs*, *VDSL* or *Ethernet WAN* connections.
5. **Dial On Demand** enables or disables the "on-demand" functionality of the PPP session, to be automatically activated when there is need for data traffic and deactivated when the connection is idle.



WARNING

Do not modify the default MTU value, unless instructed so by your Service Provider. Invalid MTU values can lead to loss of connectivity or degradation of service.

IP Options

This category provides the IP address configuration required in the case of non-PPP routed connections. Available choices are: automatic configuration through **DHCP**, and **Static IP** address configuration. In the latter case:

1. **IP Address** is the IP address used for the WAN interface.
2. **Netmask** is the corresponding subnet mask.
3. **Gateway** is the default gateway, used only if the **Default route** option described below is either *Yes* or *Backup*.

IP Routing

The **Default route** parameter defines if the connection will provide the default route for Internet connectivity. Available options are *Yes*, for a connection offering default route, *Backup*, for a connection acting as a backup in case of failure of the default-route connection, and *No*, for any plain connection without a default-route gateway.



Note

Only one connection is allowed to provide default route. Usually, this connection will be the one providing Internet Data service.

DSL Line

In this configuration sub-menu, it is possible to modify the different parameters controlling the functionality of the DSL modem embedded into the OxyGEN *miniOffice*.

DSL Line Configuration

Port 1 Port 2

Modulation Type

ADSL2+

Capability

Bitswap SRA

Databoost

EC/FDM Mode

EC

Coding Gain

Auto

Apply

Figure 6.8: DSL Line Parameters

The following parameters can be configured:

- **Bitswap**: swap bits around different frequency channels, in order to adapt to changes of the line conditions without retraining.
- **SRA**: seamless rate adaptation of the DSL data rate as a response to changes of the line conditions in order to avoid dropping a connection.
- **Annex M**: a variation of the ADSL technology offering increased upload speed (*if supported by your model of the OxyGEN miniOffice and by the ISP's DSLAM - PSTN connections only*).
- **Databoost**: a special, proprietary, mode of operation offering higher speeds of connection (*if supported by the ISP's DSLAM*).
- **EC/FDM Mode**: choice between *echo-cancellation* (EC) or *frequency division multiplexing* (FDM) mode of operation.
- **Coding Gain**: the increase in efficiency that the coded signal provides over an uncoded one.

**WARNING**

Do not modify the default DSL configuration values, unless instructed so by your Service Provider. Invalid values can lead to loss of connectivity or degradation of service.

**Note**

When multiple DSL ports are present (optional feature), each DSL port has its own set of parameters. Select between the different DSL ports using the appropriate tab at the top of the page.

External Modems

The optional USB host ports of OxyGEN *miniOffice* can be used for WAN connectivity through the use of external 3G or analog modems. The list of the configured external modems with their current status is displayed in the **External Modems** configuration option.

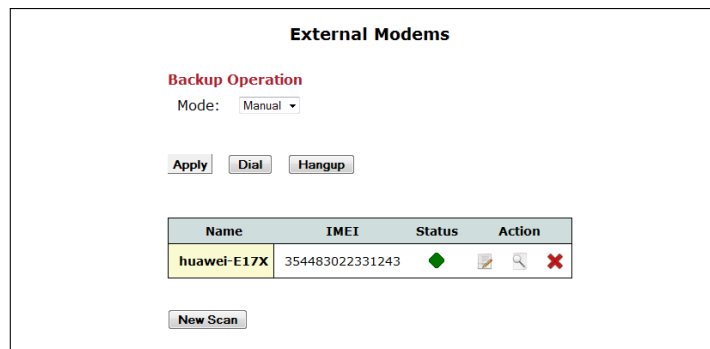


Figure 6.9: List of External Modems

In order to scan for the presence of new, unconfigured USB 3G modems, press **New Scan**. A new scan for connected USB 3G modems is performed and any connected devices are automatically added to the list of known modems.

The **Status** column displays the current status of each external modem, according to the following color-codes:

Icon	Modem Status
	Green Ready
	Orange Locked. Needs PIN
	Red Locked. Needs PUK
	Grey Not detected

Table 6.1: Modem Status Colors

You can *Edit* and *Delete* configured modems by clicking on the icons and respectively of **Action** column. You can also get more information about the status of any modem by clicking on the *Info* icon of the same column.

Edit

By clicking on the *Edit* icon  next to a configured modem, a page like the following appears:

External Data Modem

Status: ◆

IMEI: 354483022331243

Modem PIN:

remove PIN

New PIN:

Verify PIN:

Advanced settings [[show](#)]

Figure 6.10: Edit Modem Parameters

Using this page, the **PIN** of the modem can be configured. It is also possible to disable further use of PIN by the modem using the **remove PIN** checkbox, to enter a **New PIN** value or to enter the **PUK** code in case the modem is locked and PUK-unlocking is required.

Info

By clicking on the *Info* icon  next to a configured modem, a page like the following appears:

Modem Info

Manufacturer	huawei
Model	E17X
Revision	11.304.17.00.00
IMEI	354483022331243
System Devices	0 / 1
Status	Ready
Signal	Excellent (31)
Connection Mode	GSM/GPRS
Connection Time	0 sec
Speed (Down/Up)	0 / 0 kbps
Bytes (Down/Up)	0 / 0

Figure 6.11: Show Modem Information

This page displays detailed information about the modem and its status, including the modem model details, the IMEI of the device, the current status, signal strength, connection and usage details.

7

Network Menu

The **Network** configuration menu handles all the local network IP services provided by the OxyGEN *miniOffice*. Available configuration options include:

- **Interface Groups**
- **Addresses**
- **DHCP**
- **DNS Settings**
- **Static Routes**
- **Dynamic Routing**
- **Wake On LAN**
- **Public IPs**

Interface Groups

The OxyGEN *miniOffice* is a full featured device, capable of supporting more than one service over the broadband access network. In the typical multi-service deployment scenario, it is essential that the local Ethernet interfaces are divided and assigned to the different broadband services using private VLANs. This is what the **Interface Groups** web menu configures: the assignment of local interfaces to the different broadband services.

Interface Groups

Interface	Service
LAN-1	Data
LAN-2	Voice
LAN-3	Video
LAN-4	Data
GbE-1	DMZ
WiFi-1	Data

Connection	Service
quick_data	Data
quick_voice	Voice

IGMP snooping:

IGMP proxy:

Allow LAN routing:

Figure 7.1: Interface Groups

To this end, this web configuration page provides a list of all LAN interfaces and supported services in drop-down lists. Using the corresponding drop-down list, each interface can be assigned to the appropriate service group.



Note

*The configured broadband connections and the service each of them supports, are also presented in this page. However, their membership to Interface Groups cannot be changed here. It is handled using the **Service** parameter in the **Connections** configuration page (see page 60).*

Addresses

Each of the Interface Groups supporting the different services has its own private (LAN) IP address. The **Addresses** configuration menu allows the modification of this IP address for each Interface Group.

IP Addresses				
	Enabled	DHCP Client	IP Address	Netmask
Data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	192.168.1.254	255.255.255.0
Voice	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
Video	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
DMZ	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10.10.10.1	255.255.255.0

Figure 7.2: LAN Addresses

To configure the LAN IP address of a broadband service:

1. Make sure that the **Enabled** checkbox is checked
2. Enter the **IP Address**. For example, enter *192.168.1.254*
3. Enter the **Netmask**. For example, enter *255.255.255.0*
4. Click **Apply**.

Alternatively, you can use a DHCP client for automatic configuration of the LAN IP address of the OxyGEN miniOffice. Enable/Disable the DHCP client by selecting/deselecting the corresponding **DHCP Client** checkbox.



Note

The default LAN IP address for the Data Interface Group is 192.168.1.254.

IPv6 Addresses

In IPv6-enabled products you can enable or disable the IPv6 functionality of the OxyGEN miniOffice by using the respective radio button that appears under IPv6 addresses. Note that enabling the generic IPv6 functionality is necessary in order for subsection **IPv6 Options** to appear in page **62**.

Moreover, through the **Status** drop-down list, you can choose between **Off**, **Fixed** and **Auto** states for each Interface Group. This option refers to the Unique Local Address (ULA) configuration. When option **Auto** is selected, a ULA address is configured for the respective interface based on a pseudo-random

IP Addresses

	Enabled	DHCP Client	IP Address	Netmask
Data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	192.168.1.254	255.255.255.0
Voice	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
Video	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
DMZ	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10.10.10.1	255.255.255.0

IPv6 Addresses

IPv6 functionality: Enabled Disabled

	Status	Address	Mask
Data	Auto	fd11:fedc:271:ed80:21d:1cf:fe0	64
Voice	Off	::	64
Video	Off	fd12:1525:694:9a0:d4ae:d3ff:fe	64
DMZ	Off	fd12:256e:e0f3:8768:54e9:93ff:	64

Figure 7.3: IPv6 Addresses

algorithm that combines NTP time and the so-called EUI-64 identifier according to RFC 4193. Otherwise, you may choose the **Fixed** mode of operation, where the administrator may define their own ULA format by inserting the corresponding entries in the **Address** and **Mask** fields. Finally, you can disable ULA addresses by selecting **Off** option for the respective Interface Group.

DHCP

The embedded DHCP server of the OxyGEN *miniOffice* allows the automatic network configuration of all LAN devices on each Interface Group.

	DHCP	Start IP	End IP	Lease
Data	On	192.168.1.51	192.168.1.100	86400
Voice	Off			86400
Video	Off			86400
DMZ	Off			86400

NOTE: In case of Relay, Start IP is the DHCP server's IP.

Static Options

NTP (42)

NTP (42)

Apply

Figure 7.4: DHCP Server Configuration

To configure the DHCP Server:

1. Enable/Disable the DHCP server by selecting *On/Off* from the drop-down menu of **Status** column. The status of the DHCP server is changed accordingly. A third option is *Relay*, where the local DHCP server is deactivated and all DHCP requests received on the LAN are forwarded to an external DHCP server.
2. Specify the IP Address range by entering the **Start IP** and **End IP** values. In case of *Relay* operation, only the **Start IP** entry field is active and must contain the IP address of the external DHCP server.
3. Configure the validity period of each assigned IP address under the **Lease Time** parameter. The default lease time value is *86400* seconds (1 day).
4. Click **Apply**.



Note

By default the DHCP server is activated only for the Data Interface Group with an address pool from 192.168.1.51 to 192.168.1.100.

Static DHCP Leases

The embedded DHCP server of the OxyGEN *miniOffice* assigns IP settings to every device on each Interface Group using the available addresses from the corresponding address pool in a dynamic way.

In some cases, however (e.g. port forwarding), it is required that a PC or some other network device will always obtain the same IP address. In this case, the DHCP server is required to assign a fixed IP address based on the physical (MAC) address of the device. The **Static DHCP Leases** configuration page enables this functionality. Following the corresponding link, the following page appears:

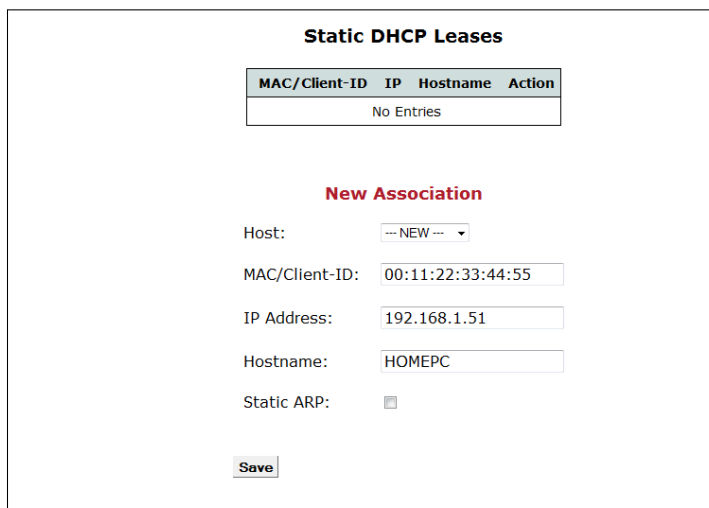


Figure 7.5: Static DHCP Leases

At the top of the page, a list of the configured address reservations is displayed. You can *Delete* configured reservations by clicking on the icon **✖** of **Action** column.

In order to make a new static DHCP lease, fill in the **MAC** address of the device along with the desired **IP Address** and **Hostname** (*optional*) and finally click **Save**. If the host has already got an IP address automatically through the DHCP server, the MAC, IP Address and Hostname values can be automatically filled in, through the **Host** drop-down list.

LAN IPv6 Addresses

For IPv6 enabled products, a second menu appears, entitled **LAN IPv6 addresses**. Here, you can specify the method of IPv6 addressing to the LAN hosts. In particular, for each Interface Group there is a possibility of different options.

1. Stateless Address Configuration (SLAAC) method may be used for LAN addressing. To enable this method, **Router Advertisements (RAs)** must be enabled by selecting option **On** in the corresponding drop-down list. With this option, Router Advertisements that contain Prefix and LifeTime information are sent to the LAN hosts that belong to the specific Interface Group. Moreover, RDNSS option is enabled, which means that supporting hosts may obtain DNS server information as well. If RAs are desirable but RDNSS option is not required, you may choose option **On(no DNS)**. Finally, option **Off** disables router advertisements. Moreover, in the **Router**

Advertisements part of the page, detailed parameters, such as the **Maximum RA interval**, **Valid** and **Preferred Lifetime** may be configured (in seconds). Default values for these parameters are 600 secs, 86400 and 14400 secs respectively.

- Stateless/Stateful **DHCPv6** method may be used. When **DHCPv6** drop-down list is set to **On** and **RA** option is enabled, the Router Advertisement packets have the so-called Other Configuration Flag set to 1. Subsequently, the LAN host is dictated to start a DHCPv6 request and the OxyGEN miniOffice provides it with stateless configuration parameters, such as DNS server, NTP, SIP servers, AFTR server etc. If **DHCPv6** is **On** and **RA** option is **Off**, the Router Advertisement packets have both Managed and Other Configuration Flags set to 1, which means that both prefix information and stateless information are transmitted over DHCPv6. Finally, when **DHCPv6** is enabled, you may choose whether the device will automatically assign the /64 prefixes to the LAN hosts derived from the WAN-side obtained prefix (this may be done by selecting **Auto** from the list) or may be done manually by selecting **Manual** and inserting the desired /64 subnet in the **Subnet** box. Finally, in the **Manual** mode, you may also configure the **Lease** in seconds for each Interface Group.

LAN IPv6 Addresses					
	RA	DHCPv6	Subnet	Lease	
Data	On	On	Auto	fd11:fedc:271:ed80::/64	86400
Voice	On (no DNS)	Off	Auto		86400
Video	Off	On	Auto	fd12:1525:694:9a0::/64	86400
DMZ	Off	Off	Auto		86400

Router Advertisements

Maximum RA interval: (sec)

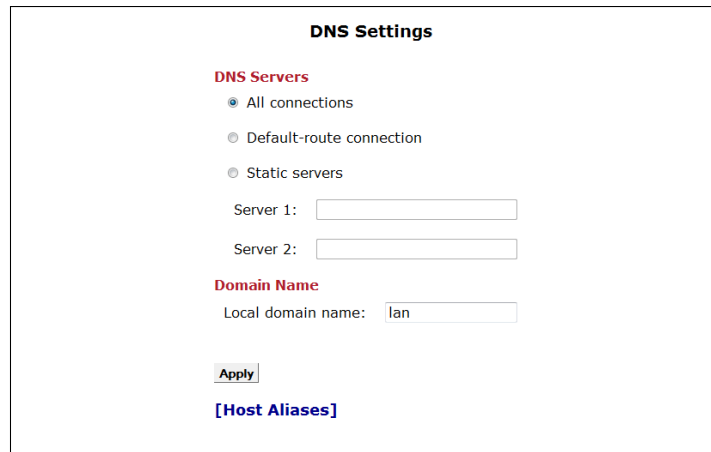
Valid lifetime: (sec)

Preferred lifetime: (sec)

Figure 7.6: LAN IPv6 Addresses

DNS Settings

The OxyGEN *miniOffice* serves as a Domain Name Service (DNS) proxy for all devices on the LAN towards the DNS servers of the ISP. Normally, the IP addresses of the DNS servers are automatically configured for every WAN connection (either through PPP or through DHCP), but in certain cases it may be required to manually configure them.



DNS Settings

DNS Servers

- All connections
- Default-route connection
- Static servers

Server 1:

Server 2:

Domain Name

Local domain name:

[\[Host Aliases\]](#)

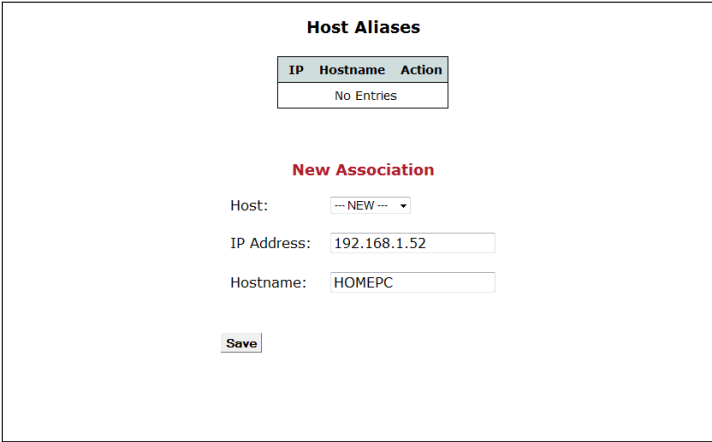
Figure 7.7: DNS Settings Configuration

Using the **DNS Settings** configuration page it is possible to:

1. Select between:
 - simultaneous use of the DNS servers obtained by every WAN connection (**All connections**)
 - use of the DNS servers obtained only by the **Default-route connection**, or
 - manual configuration of the IP addresses of the DNS servers (**Static servers**)
2. In case of manual DNS configuration, provide the IP address of the primary and (*optional*) secondary DNS servers.
3. Specify the LAN **Domain Name**.

Host Aliases

The DNS servers of the ISP configured through the WAN connections are queried by the OxyGEN *miniOffice* for resolving hostnames. In some cases however, it is required that a manual configuration is performed for some hostname-to-IP bindings. The **Host Aliases** configuration page enables this functionality. Following the corresponding link, the following page appears:



Host Aliases

IP	Hostname	Action
No Entries		

New Association

Host:

IP Address:

Hostname:

Figure 7.8: Host Aliases

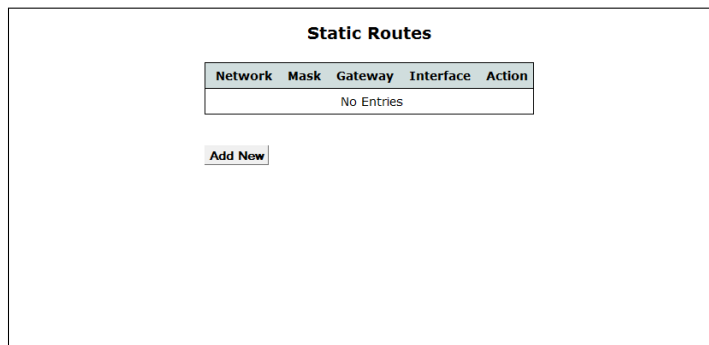
At the top of the page, a list of the configured bindings is displayed. You can *Delete* configured bindings by clicking on the icon **X** of **Action** column.

In order to make a new static DNS alias, fill in the desired **IP Address** and **Hostname** combination and finally click **Save**. If the host has already got an IP address automatically through the DHCP server, the IP Address and Hostname values can be automatically filled in, through the **Host** drop-down list.

Static Routes

The ISP usually provides default-route information through the automatic IP configuration of the WAN connections. Using specific methods (e.g. dynamic routing protocols or DHCP options), it is also possible to apply more detailed routing rules on the device. In certain cases, however, manual configuration of routing entries is required. This functionality is supported through the **Static Routes** configuration page.



Selecting this entry, the following screen appears with a list of the configured static routing entries:



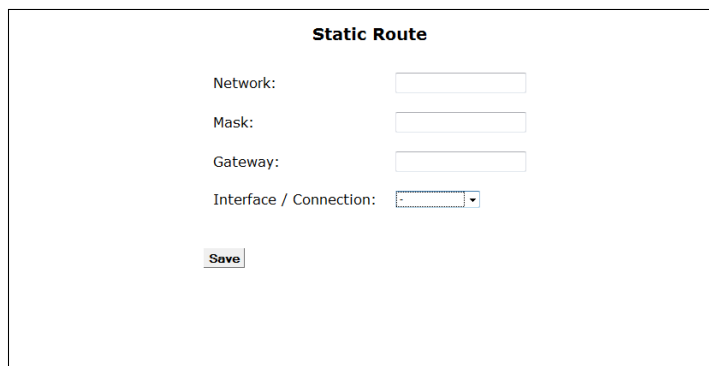
Network	Mask	Gateway	Interface	Action
No Entries				

[Add New](#)

Figure 7.9: Static Routing

You can *Edit* and *Delete* configured route entries by clicking on the icons  and  respectively of **Action** column.

To add a new static routing rule, click **Add New** and the new **Static Route** page opens:



Static Route

Network:

Mask:

Gateway:

Interface / Connection:

[Save](#)

Figure 7.10: New Static Route

1. Enter the destination **Network** address and **Mask**.
2. Enter the **Gateway** IP address and/or **Interface/Connection**, used for the forwarding of the packets.
3. Click **Save**.

**Note**

Network value *0.0.0.0* with a **Mask** *0.0.0.0* corresponds to default route.

**WARNING**

Enter static routing entries with caution! Wrong routing rules can lead to loss of connectivity or degradation of service.

Dynamic Routing

An automatic method of applying routing information on the device, is through the activation of a dynamic routing protocol, such as RIP. When such a routing protocol is offered by the ISP's network, use the **Dynamic Routing** menu entry to activate the corresponding functionality on the OxyGEN miniOffice.

Dynamic Routing

Status

Enabled Disabled

RIP v2

Connection	Enabled	Disabled
quick_data	<input type="radio"/>	<input checked="" type="radio"/>

Apply

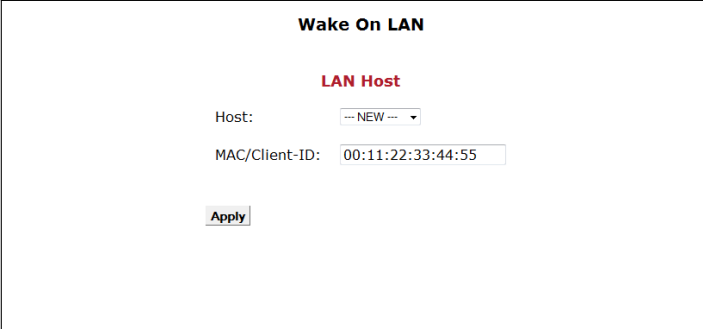
Figure 7.11: Dynamic Routing

In order to activate RIP on all or a single WAN connection:

1. Select the *Enabled* radio button under **Status** for the overall activation of the dynamic routing service.
2. Activate or deactivate the protocol for each individual WAN connection, by clicking on the corresponding *Enabled* or *Disabled* radio button in the table of WAN connections.
3. Click **Apply**.

Wake On LAN

Most modern PCs have a special capability of being automatically activated while in *Off (Standby)* status, when they receive a special Ethernet packet. This capability is called Wake On LAN (WOL) and can be used for the remote activation of PCs or servers without physical access to their *On/Off* switch.



The screenshot shows a window titled "Wake On LAN". Inside, there is a section labeled "LAN Host" in red. Below this, there are two fields: "Host:" with a dropdown menu showing "--- NEW ---" and "MAC/Client-ID:" with a text input field containing "00:11:22:33:44:55". An "Apply" button is located below the fields.

Figure 7.12: Host wake on LAN

In order to activate a host on the LAN using the Wake On LAN service, enter the **MAC** address of the host and click **Apply**. Alternatively, if the host has already been added to the DHCP server's list of static leases, the MAC address can be automatically filled in, through the **Host** drop-down list.



Note

The support of the Wake On LAN service by the PC or server depends on its BIOS and Network Interface Card (NIC) settings.

Public IPs

In the majority of installations, each host in the LAN uses a separate private IP address and accesses the Internet through the automatic transformation by the OxyGEN *miniOffice* between the private and one or more public IP addresses (NAT operation). In some cases, however, it is required to use also public IP addresses in the LAN (usually for Web servers, FTP servers etc.). In order to realize this, one option is to use a separate DMZ (DeMilitarized Zone) Interface Group, totally separated from the other LAN hosts (refer to section **Addresses** on page 71). If it required, however, that the hosts with the public IP addresses coexist in the same Ethernet segment with the other internal hosts using private IP addresses, a second available option is to notify the OxyGEN *miniOffice* about the existence of public IPs in the LAN. This is achieved through the **Public IPs** configuration menu. In this configuration page, a subnet of public IP addresses can be configured for each Interface Group. IP addresses belonging to these subnets will be routed directly (without NAT), and NAT will only be applied to the private IP addresses.

Public IP Addresses

	Enabled	Firewalled	IP Address	Netmask
Data	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>
Voice	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>
Video	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>
WiFi-2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>
DMZ	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>

NOTE: These IP addresses are directly routable from the Internet and are not protected with NAT!

Figure 7.13: Public IP Addresses

Using the corresponding table entries, for each local LAN Interface Group:

1. Enter the public **IP Address** used for the OxyGEN *miniOffice*. This will be used by the device as a secondary IP and it must be configured on each host in the LAN using a public IP as the default gateway.
2. Enter the **Netmask** of the public IP subnet. The value of this parameter together with the corresponding **IP Address** define the subnet of IPs that will not be treated as public by the OxyGEN *miniOffice* and will not be translated via NAT.
3. Select if the subnet of public IPs is going to be protected with firewall or not, using the **Firewalled** checkbox.
4. Check the **Enabled** checkbox in order to activate the relevant operation for the specific Interface Group.
5. Click **Apply**.

8

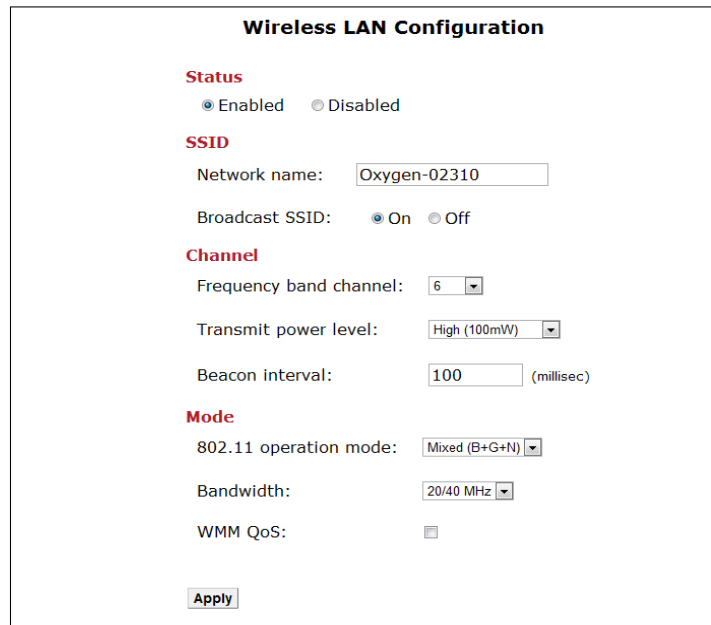
Wireless Menu

The **Wireless** configuration menu handles all the configuration options for the wireless functionality provided by the OxyGEN *miniOffice* (*WiFi-enabled devices only*). Available configuration sub-menus are:

- **Configuration**
- **Security**
- **MAC Filtering**
- **Multiple SSIDs**
- **Hotspot**

Configuration

This page allows the configuration of all the general parameters controlling the operation of your wireless connection:



The screenshot displays the 'Wireless LAN Configuration' interface. It is organized into several sections:

- Status:** Radio buttons for 'Enabled' (selected) and 'Disabled'.
- SSID:** A text input field for 'Network name' containing 'Oxygen-02310'. Below it, radio buttons for 'Broadcast SSID' are set to 'On'.
- Channel:** A dropdown menu for 'Frequency band channel' set to '6'. Below it, a dropdown for 'Transmit power level' is set to 'High (100mW)'. A text input for 'Beacon interval' is set to '100' with '(millisec)' next to it.
- Mode:** A dropdown for '802.11 operation mode' set to 'Mixed (B+G+N)'. Below it, a dropdown for 'Bandwidth' is set to '20/40 MHz'. A checkbox for 'WMM QoS' is currently unchecked.

An 'Apply' button is located at the bottom left of the configuration area.

Figure 8.1: Wireless Settings

To configure the wireless network:

1. *Enable* or *Disable* the wireless network using the corresponding **Status** radio button
2. Assign a wireless **Network name** (SSID)
3. Choose if the SSID value is going to be broadcast and visible (*On*) or hidden (*Off*) using the radio buttons of **Broadcast SSID**
4. Select the used wireless frequency channel as *Auto* or specify a specific channel number
5. Select the required **Transmit power level**
6. Optionally set the **Beacon interval**. The default setting of 100 milliseconds should be ideal for most situations.
7. Select the **Mode** of operation between any combination of the supported 802.11 profiles.
8. Select the desirable **Bandwidth** of operation for the selected **Mode**.
9. Choose whether **WMM** (Wi-Fi Multimedia Extensions) should be enabled or not.

Security

This page allows the modification of the wireless security settings.

Select the desired security option from the drop-down list next to the **Security mode** label. The available security options are: *WEP*, *WPA* and *WPA2*. Entry *Off* leaves your wireless traffic unencrypted.



WARNING

If no encryption is used (Off mode), anyone within the range of the wireless network can potentially capture your Internet traffic and access your home network.

WEP Encryption

Wired Equivalent Privacy (WEP) is a widely used, but deprecated wireless security method because of the deficiencies found in its encryption algorithm.

Wireless LAN Security

Name (SSID)
Oxygen-02310

Mode
Security mode: WEP

Authentication
Mode: 64 bit

WEP key: mykey
0 characters remaining!

Hex: 6D796B6579

Apply

Figure 8.2: Wireless Security - WEP

To activate WEP security mode:

1. Select *WEP* from the **Security mode** drop-down list.
2. Choose between *64-bit* or *128-bit* security key lengths.
3. Enter a security **WEP key** of 5 or 13 ASCII characters respectively.
4. Click **Apply**.

**Note**

WEP keys are some times used in hexadecimal format by wireless PC drivers. For this reason, when the desired ASCII WEP key is entered, its corresponding hexadecimal representation is displayed as well next to the **Hex** label.

Figure 8.3: Wireless Security - WPA

WPA / WPA2 Encryption

The Wi-Fi Protected Access (WPA) encryption method provides superior security compared to WEP. Selecting *WPA* or *WPA2* as the encryption method, the following screen appears:

When using WPA or WPA2, there are two different modes of **Authentication**: *Personal* and *Enterprise*.

Personal is the simpler and most common method. It uses a fixed security **WPA key** (PSK - Pre-Shared Key), 8 to 63 ASCII characters long, shared among the Access-Point and the endpoints (PCs).

Enterprise, on the other hand, is a more complex method. It relies on the use of an external **Radius Server** for authenticating each endpoint that requests WiFi connectivity (802.1X protocol).

**Note**

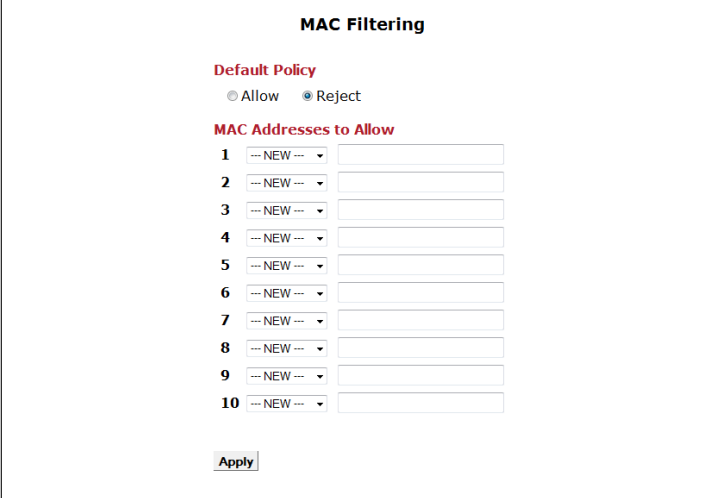
WPA is the default security policy of the OxyGEN miniOffice. The default WPA key is printed on the bottom label of the device.

**WARNING**

Microsoft Windows XP with Service Pack 3 (SP3) and newer Microsoft Windows versions by default support WPA and WPA2. Please refer to **Appendix D** on page 197 for details about WPA and/or WPA2 support on Windows XP SP1 and SP2.

MAC Filtering

Apart from the wireless encryption protocols, another method of limiting wireless access to the OxyGEN miniOffice (but not encrypting traffic), is through the **MAC Filtering** sub-menu.



MAC Filtering

Default Policy

Allow Reject

MAC Addresses to Allow

1	NEW	
2	NEW	
3	NEW	
4	NEW	
5	NEW	
6	NEW	
7	NEW	
8	NEW	
9	NEW	
10	NEW	

Apply

Figure 8.4: Wireless MAC Address Filter

The **Default Policy** radio buttons set which is the default rule for client access:

- **Allow**: every host **except** for the ones with MAC addresses in the list that follows can connect.
- **Reject**: **only** the hosts listed can connect.

After selection of the default policy, add the desired set of **MAC Addresses** in the provided list and click **Apply**.

Multiple SSIDs

This page allows the simultaneous use of the device's wireless network for multiple services. This is realized through the separation of the wireless functionality of the OxyGEN *miniOffice* into multiple virtual, independent sub-networks. Each of these independent sub-networks is identified using a **network name** (SSID) and is treated like a totally different wireless network. For example, each sub-network can have its own encryption method (see next paragraph) or can be assigned to a different *Service / Interface Group* (see page 70). It is also possible to limit the **maximum number of connected clients** and to control the maximum *Down* and *Up* **Bandwidth limit** for each wireless sub-network.

Multiple SSIDs

Number of SSIDs: 2

WiFi-1

Network name: Oxygen-00000

Maximum clients:

WiFi-2

Network name:

Maximum clients:

Bandwidth limit: / Kbps (Down/Up)

Service:

Apply

Figure 8.5: Multiple Wireless SSIDs



Note

When the number of active SSIDs is modified, a device restart is required before the new value is applied (a relevant notification message appears on the web interface).

Encryption

When multiple SSIDs are enabled, each wireless sub-network can use its own encryption method. To this end, select the corresponding **WiFi-x** tab from the list of tabs that appear at the top of the screen in the **Security** page, and configure the encryption method and key just like in the single SSID case.

Finally click **Apply** to activate and save your changes for all wireless sub-networks.



Figure 8.6: Wireless Security - Multiple SSIDs

Hotspot

The wireless operation of OxyGEN *miniOffice* (either in single or in multiple-SSID mode) can also serve as the basis for its operation in Hotspot deployments. In this case, one or more of the configured wireless sub-networks can act as a captive portal that controls access requests from multiple wireless clients. Internet access is provided only to authenticated wireless clients. On the other hand, HTTP requests from unauthenticated clients are redirected to an authentication web server. The authentication server prompts the user of the unauthenticated client for a username and password. These credentials are checked with the aid of an external radius server. If authentication is successful, the state of the client is changed to authenticated and Internet access is granted according to the policy (security, QoS, ...) enforced by the access-control platform.

As mentioned above, the Hotspot functionality relies on 2 additional services, provided externally:

- A web portal to which users are redirected. This portal, or Universal Access Method (UAM) server, provides any mean of access control service such as user login.
- A Radius service for authentication, authorization, accounting (AAA) as well as for enforcing the required access policy for each user account.

The **Hotspot** page contains all the corresponding parameters:

The screenshot shows a web-based configuration interface for a wireless hotspot. The title is "Wireless Hotspot". Under the "Status" section, there are two radio buttons: "Enabled" and "Disabled", with "Disabled" selected. The "Local Interfaces" section includes a "Service" dropdown menu currently set to "Video" and an "Interfaces:" label. The "Radius Server" section has three input fields: "Primary:", "Backup:", and "Secret key:". The "UAM Server" section has two input fields: "URL:" and "Secret key:". An "Apply" button is positioned at the bottom left of the form area.

Figure 8.7: Wireless Hotspot

Using this page, the IP address or hostname of a **Primary** and (optionally) of a **Backup Radius Server** can be configured, along with the common pre-shared password (**Secret key**). Regarding the **UAM Server**, on the other hand, the service is defined by configuring the server's **URL** and the **Secret key** providing authentication and authorization between the Hotspot service of the OxyGEN *miniOffice* and the UAM server.

QoS policy can be applied for each authenticated wireless client using the appropriate bandwidth control attributes from the Radius server. The default bandwidth control attributes are *WISPr-Bandwidth-Max-Down* and *WISPr-Bandwidth-Max-Up* which have been extended with the Gennet *gennet_class* attribute. The former two attributes can be used for assigning the exact download and upload bandwidths in bits per second (*bps*). The latter can be used to assign the authenticated wireless client to one of the pre-defined service classes:

- **gold:** 4096000 / 1024000 bps (Down/Up)
- **silver:** 2048000 / 512000
- **bronze:** 1024000 / 256000
- *other value:* 512000 / 128000

Note that if the OxyGEN miniOffice receives *BOTH* the *WISPr-Bandwidth-Max-Up/Down* and the *gennet_class* attributes, it will honour the *gennet_class* and ignore the *WISPr-Bandwidth-Max-Up/Down* ones.

**Note**

The OxyGEN miniOffice optionally offers also an embedded Radius server. Please refer to section **Radius Server** on page 139 for more information.

9

Firewall Menu

The **Firewall** configuration menu provides all the configuration options related to the embedded firewall of the OxyGEN miniOffice. The following sub-menus are available:

- **Port Forward**
- **UPnP / NAT-PMP**
- **IP Filters**
- **Web Filters**
- **DMZ Filters**
- **Address Mapping**

Port Forward

The firewall and Network Address Translation (NAT) engine of the OxyGEN miniOffice keeps the private network (LAN) protected from external threats. It is frequently required, however, to selectively allow access from the Internet to a host on the local network that runs an application or service. This selective accessibility of a server on the LAN from the WAN is enabled using the **Port Forward** sub-menu. Each forwarding rule tells the OxyGEN miniOffice on which computer a service or application is running. The service or application is defined by its characteristic TCP/UDP port number(s), and whenever traffic is received on the external (public) IP address with this specific port number as destination, this traffic is automatically routed to the specified private IP address.

Selecting the **Port Forward** option, a list of the configured port forwarding rules is displayed.

Application	Connection	Port	Source	Destination	Action
custom	all	TCP 7217	ALL	192.168.1.51	
custom	all	UDP 7217	ALL	192.168.1.51	

Add New

Figure 9.1: Port Forwarding

You can Edit and Delete configured port forwarding rules by clicking on the icons and respectively of **Action** column.

To configure a new port forwarding rule, click **Add New** and the **Port Forward Rule** page opens:

1. Select the **Protocol** that will be forwarded. This can be one of the pre-defined services/applications appearing in the drop-down list or CUSTOM for explicitly defining the forwarded port.
2. In case of CUSTOM protocol selection, specify the **Type** of incoming connection (TCP, UDP or Both) and the corresponding **Port** number (valid ports are 1-65535). Port ranges can also be specified.
3. Specify the Internet **Connection** this new port forwarding rule will apply to. You can select a specific Internet connection or ALL to match all Internet connections.
4. Select if incoming connections from all **Hosts** are going to be forwarded (option ALL) or only connections from a restricted host/network. For a single host, enter its IP address, whereas for a network use the xxx.xxx.xxx.xxx/yy notation (xxx.xxx.xxx.xxx is the network address and yy is the length of the mask in bits - see **Appendix B** on page 189).

Port Forward Rule

Application / Service

Protocol:

Type:

Port: up to: ^{*}

Incoming from

Connection:

Hosts:

Forward to

Host:

Port: Same as incoming

Change to

(*) Optional: Needed only for the definition of a range of ports.

Figure 9.2: New Port Forwarding

5. Under the **Forward to** heading, enter the private (LAN) IP address of the internal server in the **Host** entry field. Note that if the desired local network server obtains its IP address from the OxyGEN miniOffice through DHCP, you can select it from the drop-down list and a static DHCP lease will also be automatically added (see **Static DHCP Leases** on page 73).
6. Specify if the port must be forwarded unchanged (normal situations) or if the port of the internal server is different from the public one. Note that this option is only available if a single port is going to be forwarded and not in the case of a port range.
7. Click **Save** to activate the rule.

UPnP / NAT-PMP

UPnP and NAT-PMP are protocols that enable applications on the LAN to operate automatically through the NAT and Firewall engine of the OxyGEN miniOffice by transparently applying the required port-forwarding rules. Through these protocols, the PCs on the LAN notify the OxyGEN miniOffice about the need for specific port forwarding rules, and the necessary actions are performed without any user intervention.

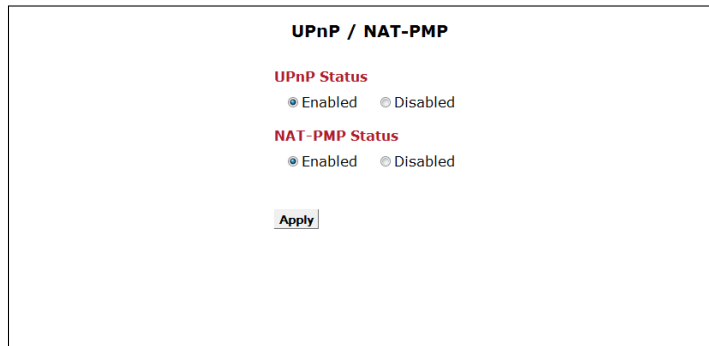


Figure 9.3: UPnP Configuration

To enable or disable the UPnP and/or NAT-PMP protocol service:

1. Select *Enabled* or *Disabled* using the corresponding radio buttons
2. Click **Apply**.



Note

IP forwarding rules automatically applied through UPnP and/or NAT-PMP are listed in the **Firewall** sub-menu of the **Status Menu** (see page 169).

IP Filters

The IP filtering service allows the OxyGEN miniOffice to control connection attempts and IP streams in both the incoming (Internet → LAN) and the outgoing (LAN → Internet) direction. Different services and applications can be allowed or denied based on the source and/or destination IP address.



Note



The default policy of the OxyGEN miniOffice is that all outgoing connections are allowed and all incoming connections denied.

Selecting the **IP Filters** option, a list of the configured IP filtering rules is displayed.

Application	Port	Source	Destination	Filter	Action
No Entries					

[Add New](#)

Figure 9.4: IP Filtering

You can Edit and Delete configured IP filtering rules by clicking on the icons  and  respectively of **Action** column.

To configure a new IP filtering rule, click **Add New** and the **IP Filtering Rule** page opens:

1. Enter the type of filter rule in **Filter** field. Options Drop and Reject both lead to discarded connection attempts. The difference is that with Drop the connection attempt is rejected silently whereas Reject sends an ICMP notification packet. Accept on the other hand, leads to an acceptance of the connection attempt and subsequent IP traffic.
2. Select the **Source** of the filtered traffic: Using the **Service/Connection** drop-down list, select a specific Internet connection or LAN Interface Group (private VLANs), --WAN-- to match all Internet connections or --LAN-- to match the entire LAN (all Interface Groups).
3. Specify if the filtering rule is going to be applied to traffic from any host or only to traffic from a specific **Host** or **Subnet**. In the former case, the relevant input field must be left blank or set to 0.0.0.0/0. For a single host, on the other hand, enter its IP address, whereas for a sub-network use the xxx.xxx.xxx.xxx/yy notation (xxx.xxx.xxx.xxx is the network address and yy is the length of the mask in bits - see **Appendix B** on page 189).

IP Filtering Rule

Filter

Drop
 Reject
 Accept

Silently discard connection attempts.

Source

Service / Connection:

Host / Subnet:*

Destination

Service / Connection:

Host / Subnet:*

Application / Service

Protocol:

Type:

Port: up to:**

(*) NOTE: Enter the IP address or name of a fixed host, a subnet (xxx.xxx.xxx.xxx/xx) or leave blank for "any-IP".

(**) Optional: Needed only for the definition of a range of ports.

Figure 9.5: New IP Filter

4. Repeat steps 2 to 3 for the selection of the **Destination** of the filtered traffic.
5. Specify the **Application/Service** being filtered by choosing any of the pre-defined applications in the **Protocol** drop-down menu or by choosing **CUSTOM** followed by the protocol **Type** (TCP, UDP or Both) and the **Port** number.
6. Click **Save** to activate the rule.

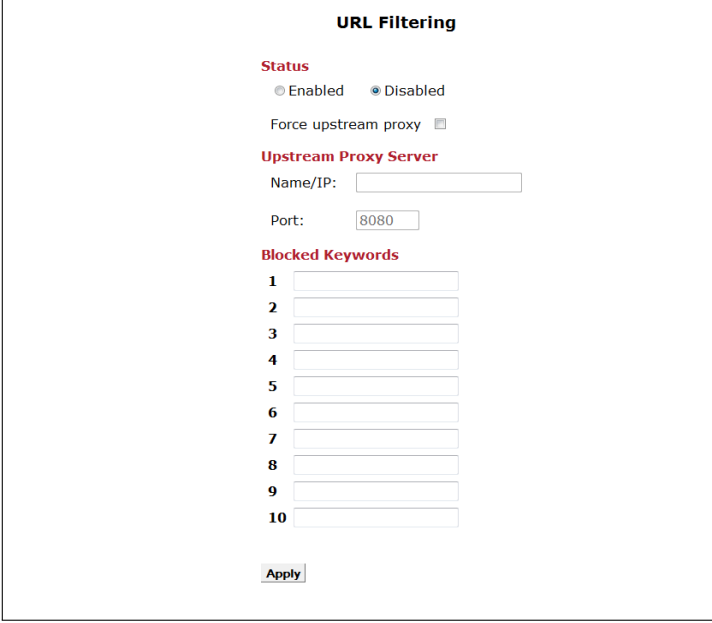


WARNING

Enter IP filtering rules with caution! Wrong IP filtering rules can lead to loss of connectivity, degradation of service and even loss of access to the configuration menu of the OxyGEN miniOffice.

Web Filters

The OxyGEN miniOffice offers also a web filtering, parental control service, that allows the selective rejection of outgoing HTTP requests based on keywords found in the requested URL.



The screenshot shows a web configuration page titled "URL Filtering". It contains the following elements:

- Status:** Two radio buttons, "Enabled" (unselected) and "Disabled" (selected).
- Force upstream proxy:** A checkbox that is currently unchecked.
- Upstream Proxy Server:** A section with two input fields: "Name/IP:" and "Port:". The "Port:" field contains the value "8080".
- Blocked Keywords:** A list of ten numbered input fields (1 through 10) for entering keywords.
- Apply:** A button at the bottom of the form.

Figure 9.6: Web Filtering

After entering the **Web Filters** web configuration page:

1. Enable or Disable the service using the appropriate **Status** radio button.
2. When Enabled, add URL keywords in the **Blocked Keywords** list.
3. Optionally force all web traffic to pass through an external HTTP proxy server. To this end, check the **Force upstream proxy** checkbox, and fill-in the **Name** or **IP** and the **Port** of the proxy server.
4. Click **Apply** to save and activate your settings.

DMZ Filters

A DMZ (DeMilitarized Zone) is a local subnet that can be accessed from the Internet and is usually used to host Web servers, FTP servers etc. Being a local subnet, the Ethernet ports that are part of the DMZ and the IP addressing scheme used for the DMZ subnet are configured, like for every LAN service, using the relevant configuration options of the **Network** configuration menu (see page 69). From a security point of view, however, the DMZ is treated like a semi-external network using public IP addresses and kept totally separated from the Data, Voice and Video private LANs. To be more precise:

1. Connections from the Internet towards the DMZ are filtered through the firewall.
2. Connections from the DMZ towards the Internet are allowed and no NAT is applied.
3. Connections from the DMZ towards the LAN (private VLANs) are filtered through the firewall.
4. Connections from the LAN (private VLANs) towards the DMZ are allowed, but NAT is applied hiding the internal IP addressing scheme.

The **DMZ Filters** sub-menu controls item 1 of the list above, through the configuration of the services that are allowed to pass the firewall from the Internet towards the hosts in the DMZ.

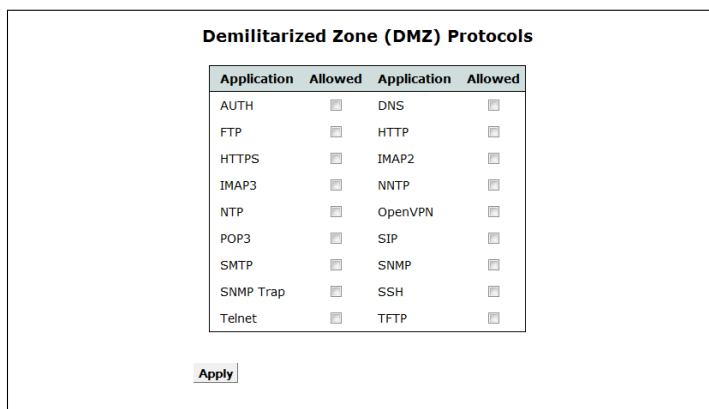


Figure 9.7: Internet-to-DMZ Protocol Filters

From the list of services/protocols displayed, check the ones that should be allowed through the firewall and click **Apply** to activate your settings.



Note

Entries corresponding to all allowed services/applications are automatically added to the list of **IP Filters**, since the **DMZ Filters** functionality can be considered as a special case of IP filtering. The **IP Filters** sub-menu gives the administrator the freedom to configure more complex cases, whereas the **DMZ Filters** configuration page presents, in a simpler form, only Internet → DMZ rules.

Address Mapping

The Network Address Translation (NAT) service of OxyGEN miniOffice allows multiple hosts in the internal LAN to share the same external (public) IP address. While this is adequate for most users, it is sometimes required (normally in business environments), to share more than one external IP addresses. This is the case, for example, when a SOHO/SME has been provided multiple static IP addresses by the ISP and the administrator wants to use one of these IP addresses for the company's Web server, a second for the FTP server, etc.

The **Address Mapping** configuration sub-menu allows the controlled mapping of external IP addresses to LAN hosts.

External (WAN)		Internal (LAN)	
--- IP Address ---		--- IP Address ---	
--- IP Address ---		--- IP Address ---	
--- IP Address ---		--- IP Address ---	
--- IP Address ---		--- IP Address ---	
--- IP Address ---		--- IP Address ---	

Apply

Figure 9.8: NAT Static Address Mapping

In order to configure such a mapping:

1. Enter the **External Address** value
2. Specify the LAN host this mapping rule will apply to. Under the **LAN Address** heading, enter the LAN IP address of the internal server. Note that, if the desired LAN server obtains its IP address from the OxyGEN miniOffice through DHCP, you can select it from the drop-down list.

Repeat the above procedure for all required external IP addresses and corresponding LAN servers, and finally click **Apply** to activate the service.

10

Voice Menu

The **Voice** configuration menu handles all parameters related to the voice operation of the OxyGEN miniOffice. You can access the following voice sub-menus:

- **Voice Service**
- **External Lines**
- **VoIP Trunking**
- **Local Extensions**
- **DECT Station**
- **ISDN Interfaces**
- **Dial Plan**
- **Restrictions**
- **Speed Dials**
- **Black List**

Foreword

Before presenting the different sub-menus with the parameters related to the voice operation of OxyGEN miniOffice, it is important to understand the structure and functionality of the different entities presented.

First we have the **External Lines**. These are the different types of connections to the external telephony network:

- the Voice over IP (VoIP) service accounts of the VoIP-over-broadband service provider
- the FXO port(s) connecting to the public PSTN network (optional feature)
- the ISDN interface(s) configured to operate in TE mode, for connecting to the public ISDN network (optional feature)

An additional special case of External Line is the **VoIP Trunk** connection (optional feature). The difference between the VoIP lines and the VoIP trunk is that the former are normal VoIP client connections registering at the provider's SIP Proxy / Softswitch, whereas the latter is a special point-to-point type of connection, with no registration requirement, used for transparently forwarding incoming VoIP calls from a specific remote server to one or more local voice interfaces or extensions and vice versa.

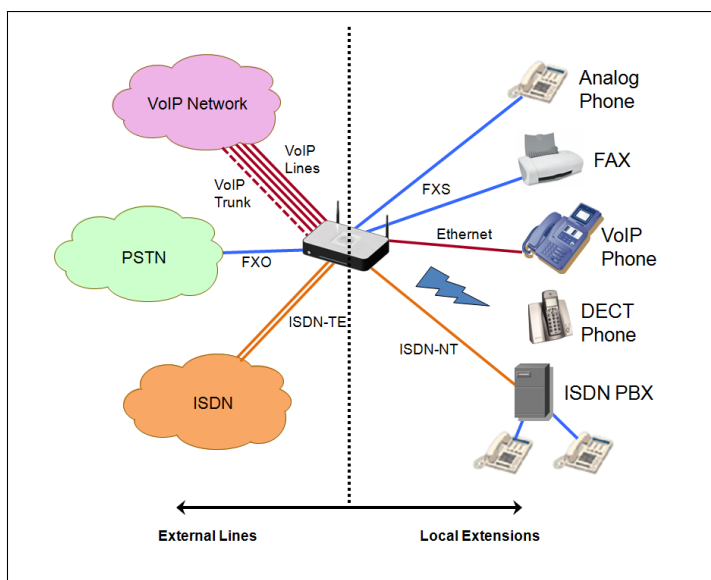


Figure 10.1: Voice External Lines and Local Extensions

On the other hand, we have **Local Extensions**. These are the internal phone numbers and connections of the telephony network. Local Extensions include:

- FXS ports with connected analog phones or FAX machines

- *DECT handsets registered at the embedded DECT basestation of the OxyGEN miniOffice (optional feature)*
- *external VoIP phones connected either through wired Ethernet or through WiFi*
- *ISDN interface(s) configured to operate in NT mode, for connecting to ISDN terminals or user ISDN PBXs (optional feature)*

*For each **External Line** one or more **Local Extensions** can be assigned as targets of incoming calls. This way it is selected which FXS port, DECT handset, or other Local Extension is going to ring when a call is received by the External Line.*

*Likewise, for each **Local Extension**, one of the **External Lines** is selected as the line used for outgoing calls towards the external telephony network.*

Voice Service

This page allows the configuration of the basic Voice over IP (VoIP) settings to enable the **Voice Service** over the broadband connection.

Voice Service

SIP Service

SIP domain:

Proxy Name/IP:

Proxy port:

Registr. interval: (sec)

Append domain to username

Codecs

Preferred codec:

Fax support:

SIP DSCP:

RTP DSCP:

Max calls:

Session Refresh

Mode:

Interval: (sec)

Refresher:

Figure 10.2: Voice Service

To configure the system settings for **Voice Service**:

1. Enter values for the basic SIP parameters such as **SIP domain**, **Proxy Name** or **IP**, **Proxy port** (default: 5060), and **Registration interval** (default: 300).
2. Check if the domain name must be **appended** to the username in outgoing voice-call requests (user@domain@proxy-ip) (depends on the voice Proxy / Softswitch of the ISP).
3. Select the **Preferred codec** and **Fax support** method.
4. Click **Apply**.

External Lines

This configuration page allows the control of the external phone lines of the OxyGEN miniOffice. It includes a list of all types of connections to the telephony network: the Voice over IP (VoIP) service accounts, and, when present, the FXO and External ISDN (TE) interfaces (optional features).

External Phone Lines				
VoIP				
Line	Number	Server	Status	Action
Line 1	2104600001	R	◆	
Line 2	2104600002	R	◆	
Line 3	2104600003	R	◆	
Line 4	2104600004	T	◆	

[FXO Port]

ISDN		
Line	Number	Action
No Entries		

New ISDN

Figure 10.3: Phone Lines

The different types of external phone lines are organized in separate tables. The upper one contains the different VoIP service accounts. These accounts operate as individual clients, registering at the SIP Proxy / Softswitch specified in section **Voice Service** (see page 106).

When the OxyGEN miniOffice is equipped with one or more ISDN voice interfaces (optional features) and at least one of these interfaces has been configured to operate in **External (TE)** mode (refer to section **ISDN Interfaces** on page 114), the list of external lines contains also entries for the ISDN telephony service.

You can Edit the parameters of each phone line by clicking on the corresponding icon of the **Action** column. The page that appears, depends on the type of phone line being configured and contains the relevant settings.

VoIP

In the case of **VoIP** service accounts, the line settings first of all require the selection of whether the line should be **Registered** or **Trunk** (for more details please refer to sections **Voice Service** and **VoIP Trunking** correspondingly). Subsequently, you must insert the SIP credentials **Username**, **Password** and **Authname** and the mode of transport of **DTMF** tones, with available options being RFC 2833, Inband and SIP Info (RFC 2976).

The parameter **Line number** contains the telephony number of the account. Optionally, it is also

External VoIP Line 1

Status
 Enabled Disabled

Parameters
Server: Registered
Username: 2104600003
Password: ****
Authname:
DTMF: RFC 2833
Line number: 2104600003
Consecutive:

Outgoing Calls
Force Caller-ID:

Incoming Calls
Significant digits:
Add prefix:
Route calls to:

List of Extensions	Selected Extensions
FXS-2 FXS-3 FXS-4 All ISDN NT	FXS-1

Target hunting: Linear

Apply

Figure 10.4: Phone Lines

possible to support a whole family of consecutive numbers assigned by the VoIP telephony provider. This family of numbers can be described by specifying the first one (also known as Head Number) in the **Line number** field followed by the range of **Consecutive** numbers (including the **Head Number**). For example, a Line Number 2101234500 and a Consecutive value of 10, correspond to numbers 2101234500-2101234509. Another option is to add a special prefix to the called number, and this is performed using the **Add prefix** parameter.

Another feature is the ability to transform the called number before routing it to local extensions. This is useful, especially in the case of ranges of consecutive numbers, which are usually directly converted to internal numbers through simple transformations. Using the values of the example above, a typical use would be to transform numbers 2101234500-2101234509 to internal numbers (local extensions) 500-509. The number of right-end digits to be retained for the internal numbering scheme is the number of **Significant Digits**, and in the example described above the value would be 3.

The final step in the configuration process of the VoIP phone line is the selection of the local extension(s) to which incoming calls are going to be directed. To this end, all the defined local extensions

(either voice interfaces or local VoIP numbers) are listed in the **List of Extensions** table. Using the arrow-buttons, the desired local extensions can be moved to and back from the **Selected Extensions** table. The result of this procedure is that, whenever an incoming call for the number(s) of this external line is received by the OxyGEN miniOffice, the number is going to be compared with the list of **Local Extensions** and, if no match is found, the **Selected Extensions** are going to ring.

ISDN

In the case of **ISDN** external lines, the first thing to configure is the ISDN mode of operation: **MSN** (Multiple Subscriber Numbers) or **DDI** (Direct Dial In). In both of these modes, multiple numbers can be assigned to the line. The most important functionality difference, however, is that Multiple Subscriber Numbers are different (not necessarily consecutive) numbers over the same, single ISDN line, in a point-to-multipoint mode of operation, whereas with Direct Dial In multiple, consecutive numbers are applied to one or more ISDN lines, but with a point-to-point mode of operation.

Subscription to the MSN and DDI services is mutually exclusive. You have to ask your provider for the mode of operation and the numbers assigned to your external ISDN line(s).

The rest of the configuration parameters are similar to the VoIP account settings: you have to configure a single (in case of MSN) or a whole range of numbers (in case of DDI), for which the incoming calls are going to be handled by the OxyGEN miniOffice, optionally apply any number transformations (Significant digits and Add prefix) and then select the local extension to which the corresponding calls are going to be directed.



Note

The ISDN parameters appear only when at least one ISDN voice interface is configured to operate in **External (TE)** mode. Please refer to section **ISDN Interfaces** on page 114 for a description of the corresponding configuration.



Note

The operation of your external ISDN line in **MSN** or **DDI** mode depends on your ISDN telephony service provider.

VoIP Trunking

As mentioned in sections **Foreword**, **Voice Service** and **External Lines**, the OxyGEN miniOffice can register using multiple VoIP service accounts (external lines) to an external SIP Proxy / Softswitch. Apart from this Client-Proxy mode, the OxyGEN miniOffice offers also a point-to-point "Trunking" mode of operation. Under this mode, all incoming VoIP calls received from a specific remote server are transparently forwarded to one or more local voice interfaces or extensions. The same applies to calls in the reverse direction: calls placed from one or more local voice interfaces or extensions are sent directly to the remote VoIP peer. This point-to-point functionality is supported through the **VoIP Trunking** configuration page.

Selecting this entry, the following screen appears:



VoIP Trunking

VoIP Service

SIP domain:

Peer Name/IP:

Peer port:

Figure 10.5: Voice Trunking Service

Under the **VoIP Service** heading, it is possible to configure the values for the basic SIP parameters, such as **SIP domain**, **Peer Name** or **IP** and **Peer port** (default: 5060).

Local Extensions

The embedded PBX functionality of OxyGEN miniOffice allows each FXS port and, when available, each DECT handset, Internal (NT) ISDN interface and local VoIP phone (optional features) to have its own internal phone number. The **Extensions** sub-menu allows the configuration of these internal phone numbers (local extensions).

Entering the sub-menu, a list of all configured local extensions with their current status is displayed.

Local Extensions

Automatic Provisioning

Enabled Disabled

Extensions: -

External line:

Number	Phone ID	Name	Status	Action
401	FXS-1	-	◆	
402	FXS-2	-	◆	
403	FXS-3	-	◆	
404	FXS-4	-	◆	

Figure 10.6: List of Extensions

You can Edit and Delete configured extensions by clicking on the icons and respectively of **Action** column.

In order to add a new local extension, click **Add New** and the following page appears:

Each local extension is uniquely described by its internal **Number**. No extensions can share the same internal **Number**. After entering the **Number** of the local extension, select its type using the **Port** drop-down menu. Available options are the different local voice interfaces of the OxyGEN miniOffice or **SIP Phone** for an external IP phone. In the latter case, a **MAC Address** value is required in order to uniquely identify the IP phone device (use a dummy/virtual MAC value in case of PC softphones) and the **Credentials (Username and Password)** for the registration of the external VoIP client on the embedded PBX of the OxyGEN miniOffice.

The rest of the parameters, common for each type of local extension, are:

- **Name:** the name assigned to the local extension and transmitted in outgoing calls as the calling name.

Local Voice Extension

Number:

Port:

Model:

MAC Address:

Name:

External line:

Credentials

Username:

Password:

Supplementary Services

Accept DDI external calls

Anonymous Call Rejection

Do Not Disturb

Caller-ID Restriction

SIP keepalive

Call Forward

	Number
All (CFU)	<input type="text"/>
Busy (CFB)	<input type="text"/>
No Answer (CFNA)	<input type="text"/>

Figure 10.7: New Local Extension

- **External line:** the VoIP service account used for external calls originating from the configured local extension (refer to sections **External Lines** on page 107 and **VoIP Trunking** on page 110)

Apart from the main extension parameters, this page allows also the configuration of the status of **Supplementary Services**:

- **Accept DDI external calls:** a checkbox indicating if the configured number is a strictly local extension number or if incoming calls for the specific number should also be accepted on the external voice lines.
- **Anonymous Call Rejection:** a checkbox indicating whether the configured local extension accepts or rejects incoming call attempts without CLIP information (i.e. anonymous calls).
- **Call Waiting:** a checkbox controlling the activation/deactivation of the Call Waiting supplementary service (option available only on local voice interfaces).

DECT Station

The OxyGEN miniOffice is optionally equipped with an embedded DECT base-station. This feature allows the addition of up to 6 DECT handsets, with each of these handsets handled as a totally independent device. This means that each handset has its own local extension number and is independently configured, like any FXS port or optional local VoIP phone, using the **Local Extensions** configuration sub-menu (see page 111).

Before configuring, however, a DECT handset as a local extension, it must first be added to the list of known or "paired" handsets. This is performed using the **DECT Station** configuration sub-menu.

DECT Handsets

Device	Action
1	
2	
3	
4	

Registration Mode

Status: **Inactive**

PIN:

Figure 10.8: List of DECT Handsets

The table on the top of the page lists all configured DECT handsets. You can Delete configured DECT handsets by clicking on the icon **X** of **Action** column.

In order to activate "pairing mode" on the OxyGEN miniOffice, enter the 4-digit **PIN** value and press the **Start** button. The "pairing mode" is deactivated either automatically after 60 seconds or by pressing the **Stop** button.



Note

The embedded DECT base-station of OxyGEN miniOffice is interoperable with handsets conforming to the GAP (Generic Access Profile) protocol.



Note

Please refer to the documentation of your GAP-compatible DECT handset in order to identify the procedure of activating "pairing-mode" on the handset.

ISDN Interfaces

This configuration page allows the control of the optional ISDN voice interfaces of the OxyGEN miniOffice.

Interface	Mode	Type	Action
BRI-1	NT	PTMP	
BRI-2	NT	PTMP	

External (TE)
Interface hunting: Linear

Internal (NT)
Interface hunting: Linear

External line: Internal Only

General
Debug ISDN:

Figure 10.9: ISDN Voice Interfaces

All ISDN interfaces are programmable and can be configured to operate either in **External (TE)** or **Internal (NT)** mode. External mode must be selected in order to connect the interface to an ISDN Network Termination Unit (NT) and the public ISDN network. On the other hand, Internal mode must be selected in order to connect to an ISDN PBX replacing the ISDN Network Termination Unit and the public ISDN network with the broadband VoIP network.



WARNING

Although programmable, you will need a different type of cable for each mode of operation. When operating in **Internal (NT)** mode, use a straight-through cable for the connection, whereas for **External (TE)** mode, an ISDN crossover cable is required. Please refer to **Appendix F** on page 205 for details about the pinout of both cables.

By clicking on the Edit icon next to each ISDN interface, a page like the following appears:

Using this page, it is possible to configure the parameters related to the operation of the specific ISDN interface:

- **Mode** of operation. This parameter controls the operation of the interface either in External (TE) or Internal (NT) mode.
- **Connection type**. This drop-down list allows to select between Point-to-Point (PTP) and Point-to-Multipoint (PTMP) for ISDN DDI and MSN connections respectively.
- **Early media** operation. This checkbox controls if the interface enables transmission and reception of voice stream before the call is connected (e.g. for in-band notifications or tones).

ISDN Voice Interface BRI-1

Mode:

Connection type:

Early media:

Hold L1:

Hold L2:

External line:

Figure 10.10: ISDN Interface Parameters

- **Hold L1** and **Hold L2** functionality. These checkboxes control if the ISDN Layers 1 and 2 respectively are going to be constantly kept activated or if they are going to be dynamically brought up and down. Usually, both checkboxes should be selected for Point-to-Point (PTP) type of connections (ISDN DDI) and unselected for Point-to-Multipoint (PTMP) type of connections (ISDN MSN).
- **External line** for outgoing calls. This drop-down list controls, for Internal (NT) interfaces only, which VoIP service account is used for outgoing external calls (please refer to sections **External Lines** on page 107 and **VoIP Trunking** on page 110).

After selecting the mode and other parameters for each ISDN interface, the last step is to control if all interfaces are going to operate like totally independent interfaces or if they are going to operate in group-mode. In the former case, every ISDN interface is treated as a totally separate entity in all voice-related configuration pages, whereas in the latter all External (TE) interfaces form one group (**ISDN TE**) and all Internal (NT) another (**ISDN NT**) (for example, see the **Route calls to** parameter in section **External Lines** on page 107 or the **Outgoing** and **Fallback** drop-down lists in section **Dial Plan** on page 117).

Selection between these two modes of interface behavior is performed, individually for the External (TE) and the Internal (NT) interfaces, using the **Interface hunting** drop-down list. Value None corresponds to independent interfaces, whereas the other options correspond to grouped operation with different interface hunting modes. Specifically:

- *Linear* distributes voice calls following a linear schedule.
- *Round-Robin* distributes voice calls following a round-robin schedule.
- *Parallel* sends calls simultaneously to all grouped ISDN interfaces.
- *None* treats each ISDN interface separately.

In case of grouped Internal (NT) interfaces, one additional step is the selection of the **External line** for outgoing calls. This drop-down list controls for all ISDN interfaces configured as Internal (NT), which VoIP service account is used for outgoing external calls (please refer to sections **External Lines** on page 107 and **VoIP Trunking** on page 110).

Click **Apply** after finishing, to activate your changes.

**Note**

When the **Internal (NT)** ISDN interfaces are configured to operate in grouped mode, the value of the **External line** parameter for the group overrides the corresponding values selected for each individual interface.

Dial Plan

The **Dial Plan** configuration page allows you to control the routing of voice calls.

Single or whole categories of destination numbers are defined using a flexible pattern syntax, and the full set of patterns defines the numbers that are treated by the OxyGEN miniOffice as valid destinations of voice calls. By default, the country's numbering plan defines the most important of these destination categories/patterns. In addition to these default categories of numbers, a number of **Custom** destination categories (dialing patterns) can also be defined.

In order to define any dial-plan destination category, you must enter the corresponding **Pattern**. Patterns can consist of digits 0-9, X as a wildcard for any digit, ! as a wildcard for any number of digits and square brackets defining ranges of digits. Examples of destination patterns are:

- **100** : the number 100
- **10X** : numbers 100 to 109
- **10!** : any number starting with 10
- **10[0-4]** : numbers 100 to 104

The role of destination patterns is, however, not only to define the full set of valid destinations of voice calls. The classification of numbers into categories can also be used for the selective routing of outgoing calls. The default destination for each outgoing call is the VoIP network. However, in the event that the OxyGEN miniOffice is also equipped with FXO and/or ISDN voice ports (optional features), it is possible to selectively route each category of numbers through the VoIP or PSTN/ISDN network using the corresponding **Outgoing** drop-down list. Additionally, in case of existence of multiple External lines, a **Fallback** outgoing interface can be selected in case of failure of the primary outgoing interface (e.g. FXO fallback in case of VoIP service unavailability).



Note

For security reasons, routing of emergency calls cannot be modified from its factory-default value.

Dial Plan

Destination	Pattern	Outgoing	Fallback
Provider	100	SIP	Disabled
Provider	108	SIP	Disabled
Provider	109	SIP	Disabled
Provider	112	SIP	Disabled
Provider	166	SIP	Disabled
Provider	199	SIP	Disabled
Provider	00XXXXXXXX	SIP	Disabled
Provider	1X.	SIP	Disabled
Provider	2XXXXXXXXXX	SIP	Disabled
Provider	69XXXXXXXXXX	SIP	Disabled
Provider	800XXXXXXXX	SIP	Disabled
Provider	801XXXXXXXX	SIP	Disabled
Provider	901XXXXXXXX	SIP	Disabled
Provider	909XXXXXXXX	SIP	Disabled
Provider	[0-2]XXXXXXXXXX!	SIP	Disabled
Provider	[5-9]XXXXXXXXXX!	SIP	Disabled
Custom		SIP	Disabled
Custom		SIP	Disabled
Custom		SIP	Disabled
FXO Call	**01#	FXO	Disabled

Country code:

International prefix:

Emergency Calls

Number:

SIP domain:

Peer Name/IP:

Peer port:

Username:

Password:

Authname:

Figure 10.11: Voice Dialing Plan

Restrictions

The **Restrictions** configuration page allows you to perform access-control for the different voice-call destinations.

Call Restrictions

Line 1 Line 2 Line 3 Line 4

Destination	Pattern	Status
Provider	100	Allow
Provider	108	Allow
Provider	112	Allow
Provider	166	Allow
Provider	199	Allow
Provider	00XXXXXXXX.	Allow
Provider	1X.	Allow
Provider	2XXXXXXXXXX	Allow
Provider	69XXXXXXXXXX	Allow
Provider	800XXXXXXXX	Allow
Provider	801XXXXXXXX	Allow
Provider	901XXXXXXXX	Allow
Provider	909XXXXXXXX	Allow
Provider	[0-2]XXXXXXXXXX!	Allow
Provider	[5-9]XXXXXXXXXX!	Allow
PIN		<input type="text"/>

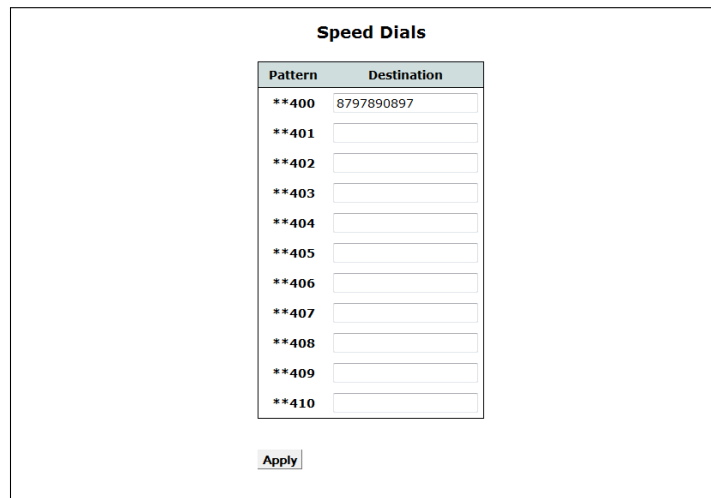
Apply

Figure 10.12: Call Restrictions

Classification of the destinations into categories is based on the same patterns, both default and custom, used in the **Dial Plan** configuration sub-menu (see page 117). For each one of these destination categories, you can Allow, Block or control with a PIN the dialing of the corresponding destination patterns. If the latter choice is made for at least one destination, a 4-digit **PIN** must also be configured, and this PIN must be dialed by the user whenever he tries to call a number that belongs to a PIN-controlled category.

Speed Dials

The **Speed Dials** configuration page allows you to assign destination phone numbers to the list of speed-dialing patterns of the OxyGEN miniOffice. These speed-dialing patterns are short codes which are matched with full telephone numbers and, once dialed, the corresponding destination number is called.



Pattern	Destination
**400	8797890897
**401	
**402	
**403	
**404	
**405	
**406	
**407	
**408	
**409	
**410	

Apply

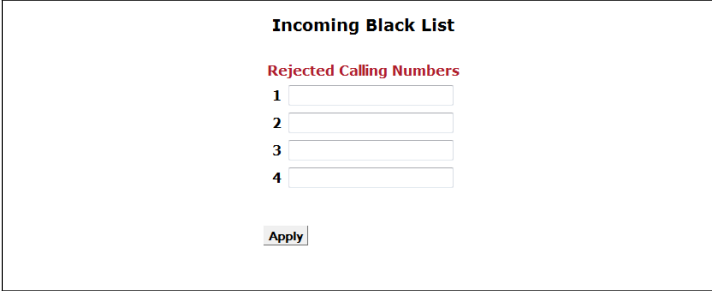
Figure 10.13: Speed Dials

In order to configure the speed-dialing functionality:

1. In the **Destination** fields put the phone numbers you wish to be called when the corresponding speed-dial **Pattern** is dialed.
2. Click **Apply**.

Black List

The **Black List** configuration page allows you to block incoming calls from selected calling numbers.



The screenshot shows a web form titled "Incoming Black List". Under the heading "Rejected Calling Numbers", there are four numbered input fields (1, 2, 3, 4) for entering phone numbers. Below these fields is an "Apply" button.

Figure 10.14: Black List of Numbers

In order to activate this feature, enter the black-listed numbers in the list of input fields under the **Rejected Calling Numbers** heading and click **Apply** to save your settings.

11

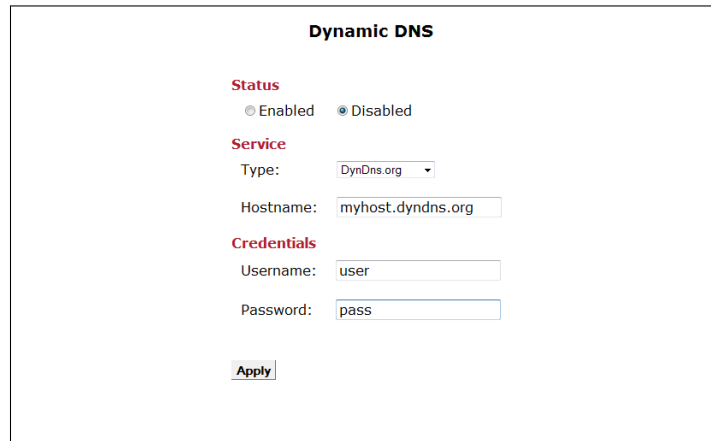
Advanced Menu

The **Advanced** configuration menu allows the configuration of a series of different advanced services offered by the OxyGEN miniOffice. It includes the following sub-menus:

- ***Dynamic DNS***
- ***Date and Time***
- ***IPv6 Tunnel***
- ***SSL VPN***
- ***GRE Tunnel***
- ***VPN Tunnel***
- ***QoS Policy***
- ***Device Detection***
- ***Radius Server***
- ***File Sharing***
- ***Printing***

Dynamic DNS

The Dynamic DNS service (also known as DynDNS service) allows Internet users with dynamic IP address broadband access to register a domain name. This way it is possible to access their home network through a fixed hostname, despite the fact that their IP address changes frequently. The OxyGEN miniOffice supports different Dynamic DNS service providers.



The screenshot shows a web form titled "Dynamic DNS". It has three main sections: "Status", "Service", and "Credentials".

- Status:** Two radio buttons are present: "Enabled" (unselected) and "Disabled" (selected).
- Service:** A "Type:" label is followed by a dropdown menu showing "DynDns.org". Below it is a "Hostname:" label followed by a text input field containing "myhost.dyndns.org".
- Credentials:** A "Username:" label is followed by a text input field containing "user". Below it is a "Password:" label followed by a text input field containing "pass".

At the bottom of the form is an "Apply" button.

Figure 11.1: Dynamic DNS

To enable the Dynamic DNS service:

1. Select **Enabled** as Dynamic DNS **Status**.
2. Specify the Service **Type**, **Hostname**, **Username** and **Password**.
3. Click **Apply**.

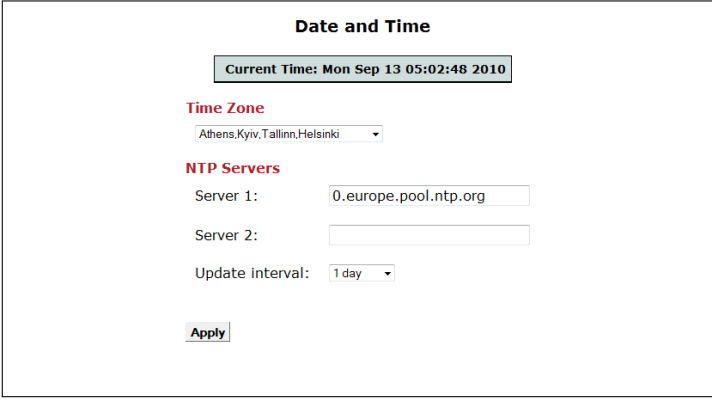


Note

You must first create an account at a Dynamic DNS service provider and configure the corresponding **Hostname**, **Username** and **Password**, before activating the service on the OxyGEN miniOffice.

Date and Time

This sub-menu lets you configure the Simple Network Time Protocol (SNTP) client settings. This client allows the OxyGEN miniOffice to contact a configured Network Time Protocol (NTP) server and obtain the current date and time values.



The screenshot shows a window titled "Date and Time". At the top, it displays "Current Time: Mon Sep 13 05:02:48 2010". Below this, there is a section for "Time Zone" with a dropdown menu currently showing "Athens,Kyiv,Tallinn,Helsinki". Underneath is a section for "NTP Servers" with two input fields: "Server 1:" containing "0.europe.pool.ntp.org" and "Server 2:" which is empty. Below the server fields is an "Update interval:" dropdown menu set to "1 day". At the bottom left of the window is an "Apply" button.

Figure 11.2: SNTP Client

To configure the SNTP client:

1. Select the **Time Zone** from the drop down list.
2. Specify the **NTP Server** hostname or IP address.
3. Optionally set a second **NTP Server** hostname or IP address
4. Optionally select also the **Interval** between two successive update attempts.
5. Click **Apply**.

The OxyGEN miniOffice offers also the possibility of operating as an NTP proxy for all hosts on the LAN. In order to activate this functionality, make sure that the **Local NTP server** checkbox is checked.

IPv6 Tunnel

This menu lets you configure the operation of several IPv6 tunnels for OxyGEN miniOffice. Available choices for tunneling mechanisms are **Dual Stack Lite**, **TunnelBroker.net**, **6to4** and **Sixxs.net**.



Figure 11.3: IPv6 Tunnels

In order to configure a tunneling mechanism you need to perform the following steps:

1. Select **Enabled** in the **Status** radio button.
2. Select the desired tunneling method, i.e. choose **Dual Stack Lite**, **TunnelBroker.net**, **6to4** and **Sixxs.net** from the provided drop-down list.
3. Fill-in the necessary fields in order to configure the selected tunnel.
4. Click **Apply**.

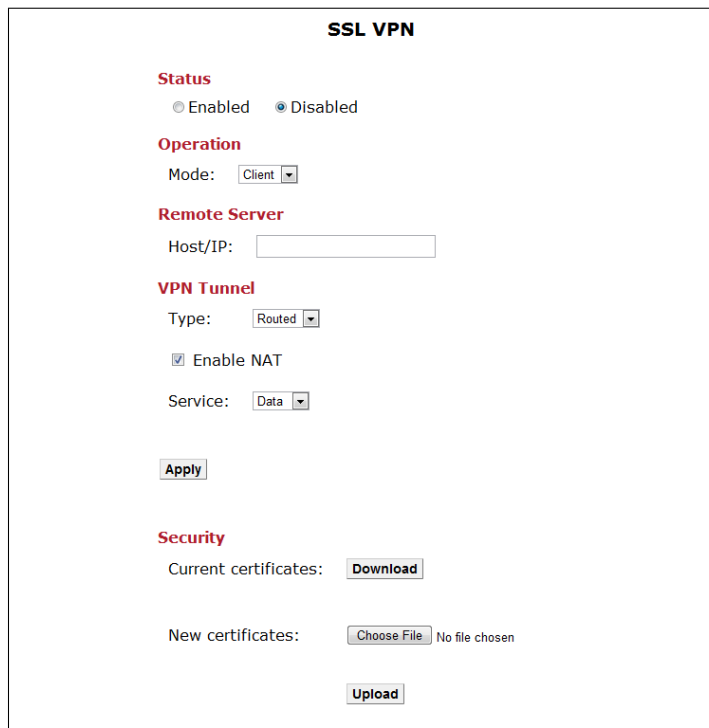
More particularly, detailed instructions for each tunnel are provided below:

1. **Dual Stack Lite:** In **Remote Server** field, you may choose **Fixed** mode, where the remote AFTR server's IPv6 address must be filled in the field **Remote Address**. If, on the other hand, no preconfigured address for the AFTR is desirable, then select **Auto** and leave **Remote Address** box empty. This will enable DHCPv6 AFTR option and obtain the IP from the DHCPv6 server. Optionally, you can assign the local tunnel interface an IPv4 address in the **Local tunnel** field and also enable NAT in the respective check box. Finally, the Interface Group whose packets will be forwarded to the tunnel interface may be selected in **Service** drop-down list.

2. **Tunnelbroker.net**: You must first fill in the **Tunnel ID**, then the remote server's IPv6 address into **Remote Address**, the credentials for the connection in the fields **User ID** and **Password** and, optionally, an address for the tunnel interface **Local Tunnel**.
3. **6to4**: Select the Interface Group for which the tunnel will be enabled through the **Service** drop-down list.
4. **Sixxs.net**: Configuration of Sixxs tunnel is done following the same steps as in Tunnelbroker tunneling mechanism described above.

SSL VPN

This sub-menu lets you configure your OxyGEN miniOffice to act either as a server or as a client for a Secure Sockets Layer (SSL) Virtual Private Network (VPN) tunnel. An SSL VPN is a form of VPN that uses the SSL protocol for ensuring the security of data transmitted over the Internet. In the OxyGEN miniOffice, this functionality is based on the widely used opensource OpenVPN project (<http://openvpn.net/>) and supports both client and server modes of operation.



The screenshot shows the 'SSL VPN' configuration page. It is titled 'SSL VPN' at the top. Under the 'Status' section, there are two radio buttons: 'Enabled' (unselected) and 'Disabled' (selected). The 'Operation' section has a 'Mode' dropdown menu set to 'Client'. The 'Remote Server' section has a 'Host/IP' text input field. The 'VPN Tunnel' section has a 'Type' dropdown menu set to 'Routed', a checked 'Enable NAT' checkbox, and a 'Service' dropdown menu set to 'Data'. There is an 'Apply' button below the 'VPN Tunnel' section. The 'Security' section has a 'Current certificates:' label with a 'Download' button, and a 'New certificates:' label with a 'Choose File' button (showing 'No file chosen') and an 'Upload' button.

Figure 11.4: SSL VPN - Client Mode

Client Mode

To configure your device to act as an SSL VPN client :

1. Select **Enabled** as SSL VPN **Status**.
2. Select **Client** as the **Operation mode** from the drop down list.
3. Specify the hostname or IP address of the SSL server in the **Host/IP** field.
4. Select between **Routed** (Layer-3 / IP) or **Bridged** (Layer-2 / Ethernet) **Type** of VPN tunnel. The former means that the VPN tunnel is a point-to-point IP connection, with IP addresses from a

subnet different than the LAN. Bridged, on the other hand, means that the VPN connection will operate like an Ethernet bridge between the LANs behind both the server and the client. For more detailed information about the advantages and disadvantages of each type, please refer to **Appendix E**.

5. When using Routed type, select if **NAT** (Network Address Translation) is going to be enabled for LAN devices over the configured SSL VPN tunnel. In other words, if the multiple devices in the client's LAN are going to connect to the SSL VPN server using the IP address used by the client for the VPN tunnel.
6. When using Bridged type, select which LAN **Service** (Interface Group) is going to be bridged over the configured SSL VPN tunnel.
7. Click **Apply**.

In order to finish with the secure connection to the SSL VPN server, you will also need to install the corresponding **Certificates**. These certificates must be provided to you by the administrator of the SSL VPN server and can be uploaded by selecting the appropriate file using the **Browse** key and finally by clicking the **Upload** key. The required certificate files and their names are:

- **connect.ovpn**: the client configuration file
- **ca.crt**: the certificate authority (CA) certificate
- **client.crt**: the client certificate
- **client.key**: the client key

It is also possible to install all files in one step, by gathering them in a zip archive.

Server Mode

If, on the other hand, you wish to configure your device to act as an SSL VPN server :

1. Select Enabled as SSL VPN **Status**.
2. Select Server as the **Operation mode** from the drop down list.
3. As in Client mode, select between Routed (Layer-3 / IP) or Bridged (Layer-2 / Ethernet) **Type** of VPN tunnel. Please note that you must make the same selection for both the server and the client.
4. When using Routed type, specify the **Network** and **Netmask** values for the subnet used as an IP address pool for the connected clients.

SSL VPN

Status

Enabled Disabled

Operation

Mode: Server

VPN Tunnel

Type: Routed

Network: 10.8.5.0

Netmask: 255.255.255.0

Service: Data

Isolate clients:

Offer default route:

Apply

Security

SSL VPN users: Manage

Current certificates: Download

New certificates: Choose File No file chosen

Upload

Figure 11.5: SSL VPN - Server Mode

5. When using *Bridged* type, select which LAN **Service** (Interface Group) is going to be bridged over the configured SSL VPN tunnel. The DHCP server settings of this Service are going to be used for the assignment of IP addresses to any DHCP requests from the SSL VPN client.
6. Click **Apply**.

The last step required for the operation of the SSL VPN server, is the definition of remote users and the generation of the corresponding certificates. To this end, click the **Manage** key next to the **SSL VPN users** label. The following screen appears:

In order to add a new remote user, enter the username under the **Add New User** heading and click the **Save** key. The new user is added and a message window opens prompting you to save a zip file. This zip file contains the configuration files and certificates corresponding to the added user. Save the file and give it to the new remote user. It will be needed in order to connect to the SSL VPN server running on your OxyGEN miniOffice.

If, on the other hand, you wish to prohibit further access to configured remote users, Revoke them by clicking on the corresponding icon **✘** of **Action** column in the list of the configured users.



User	Action
No Entries	

[Add New User](#)

Figure 11.6: SSL VPN Users



Note

There is no way of re-generating the certificates corresponding to a configured SSL VPN username. In case you want to do so, the only option is to revoke the username and then add it again.

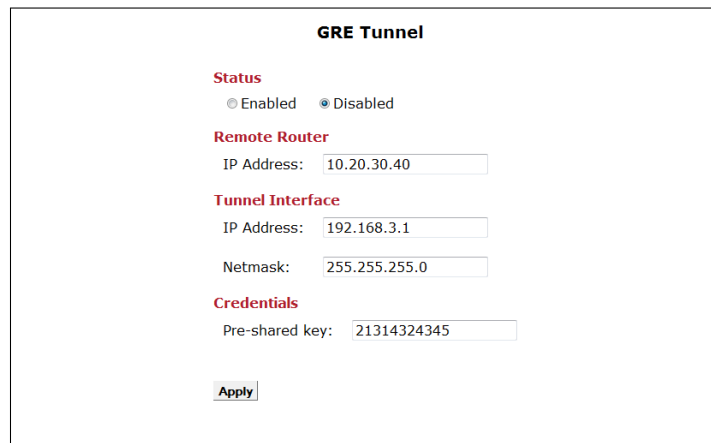


Note

*For more detailed information about the configuration of SSL VPN please refer to **Appendix E**.*

GRE Tunnel

This sub-menu lets you configure a Generic Routing Encapsulation (GRE) Tunnel between your OxyGEN miniOffice and another GRE-capable endpoint. GRE is a tunneling mechanism which uses IP as the transport protocol and can be used for carrying many different passenger protocols.



The screenshot shows a configuration window titled "GRE Tunnel". It contains the following sections and fields:

- Status:** Radio buttons for "Enabled" and "Disabled". The "Disabled" option is selected.
- Remote Router:** A text field for "IP Address" containing the value "10.20.30.40".
- Tunnel Interface:** Two text fields: "IP Address" containing "192.168.3.1" and "Netmask" containing "255.255.255.0".
- Credentials:** A text field for "Pre-shared key" containing the value "21314324345".
- An "Apply" button at the bottom left.

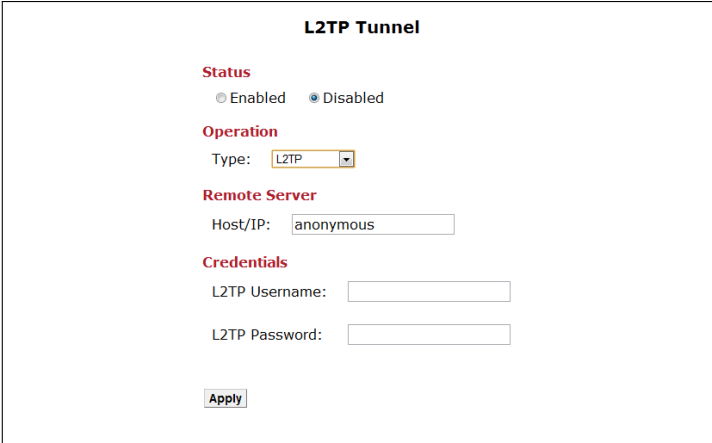
Figure 11.7: GRE Tunnel

To configure the GRE tunnel:

1. Select **Enabled** as GRE Tunnel **Status**.
2. Enter the public IP of the remote endpoint in the **Remote Router** field.
3. Specify the **IP Address** and **Netmask** for the local virtual interface of the GRE tunnel (the remote endpoint must use compatible values).
4. Enter the appropriate **Pre-shared key** value (the remote endpoint must use the same key value).
5. Click **Apply**.

VPN Tunnel

This sub-menu allows the configuration of an L2TP (Layer-2 Tunneling Protocol) and/or IPsec (Internet Protocol Security) -based VPN tunnel. IPsec is a protocol suite for securing IP communications by authenticating and encrypting each IP packet of a data stream. L2TP tunnels, on the other hand, are used for the transport of other protocols (e.g. Point-to-Point Protocol - PPP) inside UDP datagrams (default port 1701). Since, however, L2TP does not provide any encryption or confidentiality by itself, it is frequently combined with an encryption protocol (e.g. IPsec) which is passed within the tunnel to provide privacy.



The screenshot shows a web configuration page titled "L2TP Tunnel". It contains several sections:

- Status:** Two radio buttons, "Enabled" and "Disabled". The "Disabled" button is selected.
- Operation:** A dropdown menu labeled "Type:" with "L2TP" selected.
- Remote Server:** A text input field labeled "Host/IP:" containing the text "anonymous".
- Credentials:** Two text input fields, "L2TP Username:" and "L2TP Password:", both currently empty.
- An "Apply" button at the bottom.

Figure 11.8: L2TP VPN Tunnel

To configure the VPN tunnel, use the **Status/Type** drop-down list to enable and at the same time select the type of VPN. Available options are L2TP only, IPsec only, L2TP/IPsec and Off for disabled VPN service.

Once the type of VPN has been selected, the relevant parameters appear on the web configuration page. In the case of an L2TP-based VPN, these include the public **IP Address** of the remote server, along with the **Subnet** and **Netmask** behind the remote server. For tunnel authorization purposes, a **Username** and **Password** combination must be supplied (with same values configured on the remote server).

If IPsec is enabled on the VPN tunnel, some more parameters appear. The **Remote Server** is configured like in the case of the L2TP tunnel, but now it is also required to provide information about the local subnet: **Subnet** and **Netmask** under the **Local Server** heading. Authorization is in this case based on a **Pre-shared key** (common for both endpoints of the VPN tunnel) and, finally, parameters of the encryption algorithm are specified using the corresponding drop-down lists under the **IPsec Options** heading.

IPSec Tunnel

Status
 Enabled Disabled

Options
NAT-T:
IKE Phase 1:
IKE Phase 2:
Key lifetime: (sec)

Remote Server
IP Address:

Credentials
Pre-shared key:

VPN Tunnel

Local Subnet	Remote Subnet
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

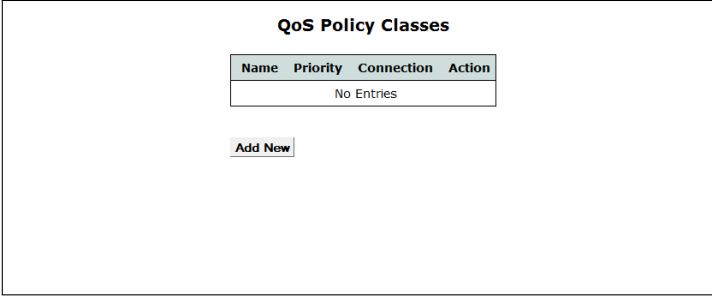
(*) NOTE: Enter the IP address of a fixed host or a subnet (xxx.xxx.xxx/xx).

Figure 11.9: IPSec VPN Tunnel

QoS Policy

This sub-menu lets you configure the Quality of Service (QoS) policy of the OxyGEN miniOffice. This policy consists of the classification of IP traffic into 3 different priority categories: GOLD (high-priority), SILVER (medium-priority) and BRONZE (low-priority). For the realization of this classification scheme, the IP traffic is divided into different classes, with each class representing a different type of traffic (e.g. a different service, an application, traffic from/to a specific host, etc.).



The first thing displayed when selecting the **QoS Policy** link is a list of the configured QoS classes for IP traffic.



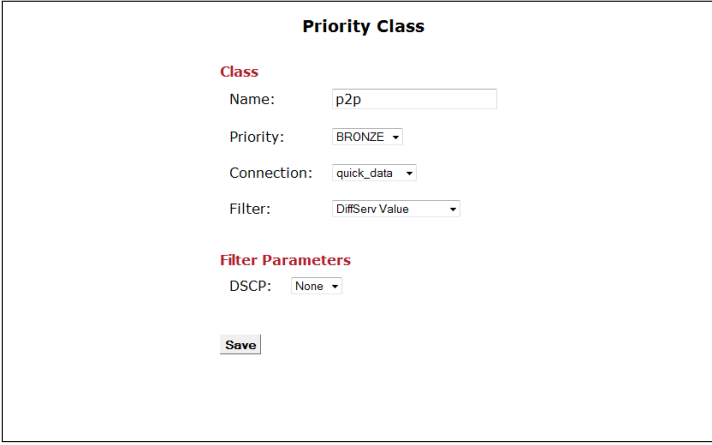
Name	Priority	Connection	Action
No Entries			

[Add New](#)

Figure 11.10: List of QoS Classes

You can Edit and Delete configured QoS classes by clicking on the icons  and  respectively of **Action** column.

To configure a new QoS class, click **Add New** and the **Priority Class** page opens:



Priority Class

Class

Name:

Priority:

Connection:

Filter:

Filter Parameters

DSCP:

[Save](#)

Figure 11.11: New QoS Priority Class

1. Enter the **Name** of the new priority class. This name is going to be used in order to distinguish between the different priority classes. Note that names must be unique among different classes and that once configured, they cannot be modified.

2. Select **GOLD**, **SILVER** or **BRONZE** as the desired **Priority** category.
3. Select the desired traffic classification method under the **Filter** parameter. The OxyGEN miniOffice offers four different methods for the classification of IP Traffic:
 - I **DiffServ Value**: Based on the TOS/DSCP value of the IP header of the packets. The corresponding value is configured in the **DSCP** field.
 - II **IP Addresses**: Based on the source or destination IP address of the IP packets. The range of valid IP addresses is defined using the **Start IP** and **End IP** parameters.
 - III **Connection Bytes**: Based on the amount of data transferred. The low limit is configured using the **Begin after** parameter whereas the optional upper limit using the **Stop after** parameter.
 - IV **Application/Service**: Based on the application or service the IP packets belong to. This can be one of the pre-defined protocols/applications appearing in the drop down list or **CUSTOM** for explicitly defining the characteristics of the service. In the latter case, the **Type** of IP packets (**TCP**, **UDP** or **Both**) and the corresponding **Port** numbers (valid ports are 1-65535) must be configured. Port ranges can also be specified.
4. Click **Save**.

Device Detection

This sub-menu allows the configuration of the automatic Set-Top Box (STB) or VoIP phone detection mechanism supported by the OxyGEN miniOffice. With this provisioning mechanism, whenever a STB is detected on the LAN served by the OxyGEN miniOffice, it is automatically placed on the Video Interface Group and IP traffic to and from this device is treated as video traffic and routed accordingly. Similarly, if a VoIP phone is detected, the corresponding LAN port is placed on the Voice Interface Group and the VoIP phone is optionally provisioned for the embedded IP-PBX of the OxyGEN miniOffice (refer to section **Local Extensions** on page 111).



Note

The STB detection mechanism is an optional feature and depends on the provision of a Video Service by your Service Provider.

Detection of the STB or VoIP phone is based on the DHCP service, and the presence of a device is identified by either of the following two information fields present in the broadcasted DHCP request:

- The MAC address of the device (more specifically the first 3 bytes - the OUI part)
- The Vendor Identifier string

Device Auto-detection

Status
 Enabled Disabled

MAC Address OUI
1 STB
2 STB
3 STB

Vendor Identifier
1 STB
2 STB
3 STB

STB Traffic Separation
Mode: L2 - Split Ports

Figure 11.12: STB Auto-detection

In order to configure the device auto-detection mechanism:

1. Select Enabled as **Status**.
2. Fill in either the **MAC Address OUI** or the **Vendor Identifier** values and the corresponding type of device.

3. For STBs, select the **Traffic Separation** mode. L2 corresponds to layer-2 (Ethernet) separation (Private VLANs) with Data and Video Interface Groups totally separated, whereas L3 corresponds to layer-3 (IP) separation, with IP routing between the Data and Video Interface Groups.
4. Click **Apply**.

**Note**

The detection mechanism relies on the DHCP service. Therefore, if the target device does not obtain its network settings from the embedded DHCP server of the OxyGEN miniOffice, its automatic detection cannot be performed.

Radius Server

Another advanced service offered by the OxyGEN miniOffice, is an embedded Radius server. Radius (Remote Authentication Dial In User Service) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service. Radius serves three functions:

1. to authenticate users or devices before granting them access to a network,
2. to authorize those users or devices for certain network services and
3. to account for usage of those services.

An example use of a Radius server is for the Authentication, Authorization and Accounting of WiFi users in Hotspots (see section **Hotspot** on page 90).

The **Radius Server** sub-menu allows the configuration of usernames and allowed hosts/subnets for the embedded Radius server of OxyGEN miniOffice. When entering the configuration page, a list of all configured usernames is displayed.

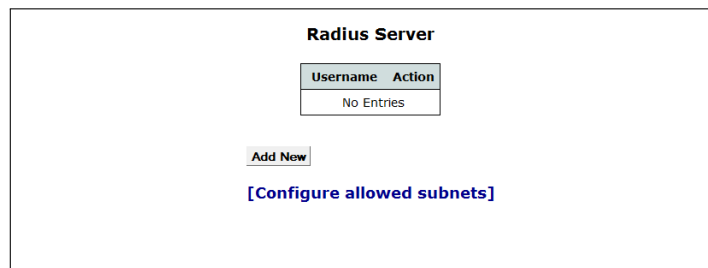




Figure 11.13: Radius Usernames

You can Edit and Delete configured usernames by clicking on the icons  and  respectively of **Action** column.

In order to add a new Radius username, click **Add New** and the **Radius User** page appears.

Using the appropriate entry fields, enter the desired new **Username** and **Password** value. You can also set values to a series of **Attributes** using the provided drop-down lists for Attribute and corresponding entry fields for Value. Finally, click the **Save** key and the new username is added.

Apart from the list of remote usernames, it is also possible to configure the hosts and/or subnets allowed to contact the embedded Radius server of OxyGEN miniOffice. To this end, follow the **Configure Allowed Subnets** link and the **Allowed Subnets** screen appears.

In order to add a new remote host or subnet, enter the IP address of the host or subnet in the **Subnet** entry field. For a single host, enter its IP address, whereas for a subnet use the xxx.xxx.xxx.xxx/yy notation

Radius User

Credentials

Username:

Password:

Attributes

1	Acct-Input-Gigawords	<input type="text"/>
2	Acct-Input-Gigawords	<input type="text"/>
3	Acct-Input-Gigawords	<input type="text"/>
4	Acct-Input-Gigawords	<input type="text"/>
5	Acct-Input-Gigawords	<input type="text"/>
6	Acct-Input-Gigawords	<input type="text"/>
7	Acct-Input-Gigawords	<input type="text"/>
8	Acct-Input-Gigawords	<input type="text"/>
9	Acct-Input-Gigawords	<input type="text"/>

Figure 11.14: New Radius Username

Allowed Subnets

Subnet	Secret	Action
No Entries		

New Subnet

Subnet:

Password:

Figure 11.15: Radius Subnet Configuration

(xxx.xxx.xxx.xxx is the network address and yy is the length of the mask in bits - see **Appendix B** on page 189). Add also a **Password** value, click the **Save** key and the new entry is added.

If, on the other hand, you wish to prohibit further access to a configured remote host/subnet, Revoke them by clicking on the corresponding icon **✖** of **Action** column in the list of allowed subnets.

File Sharing

When your OxyGEN miniOffice is equipped with a USB Host port (optional feature), it is possible to connect an external storage device (USB stick, Hard Disk) to this port. The **File Sharing** sub-menu lets you configure the protocols handling the advertising and sharing of a connected external USB storage device for all computers on the LAN.

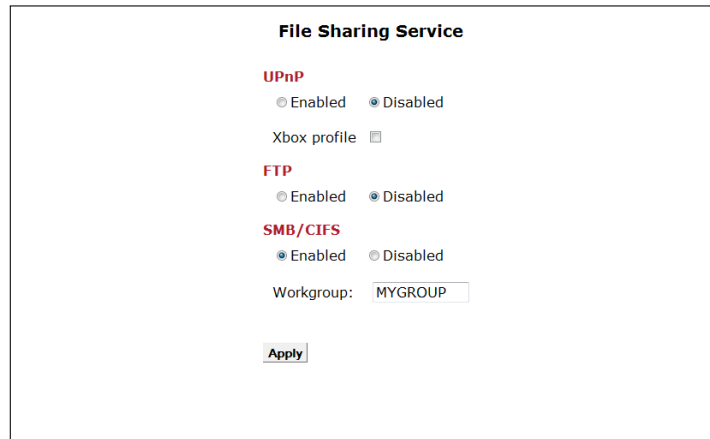



Figure 11.16: File Sharing Service

Select **Enabled** for the file-sharing protocols you wish to activate, and click **Apply** in order to activate and save your selection. Available options are UPnP (with a special Xbox profile), FTP server and SMB/CIFS for Windows PCs. In the latter case, the Windows **Workgroup** value can also be configured.



WARNING

Before unplugging an external storage device from the OxyGEN miniOffice make sure you first **Disconnect** it using the  icon under the **Devices** category of the **Home** page or in the **Interfaces** sub-menu of the **Status** configuration menu. Removal of the device without disconnecting first, may lead to corrupted data on the storage device!

Printing

When your OxyGEN miniOffice is equipped with a USB Host port (optional feature), it is possible to connect a USB printer to this port. The **Printing** sub-menu lets you configure the protocols handling the advertising and sharing of the connected USB printer for all computers on the LAN.



Figure 11.17: USB Printer Support

Select **Enabled** for the printing protocols you wish to activate, and click **Apply** in order to activate and save your selection. Please refer to Appendix **Network Printing** on page 193 for more information about the available options and the configuration process for the LAN PCs.

12

System Menu

The **System** menu allows the configuration and use of the following administrative utilities:

- **TR-069**
- **SNMP**
- **Syslog**
- **Backup / Restore**
- **Firmware Upgrade**
- **Remote Admin**
- **Users**
- **Change Password**
- **Device Restart**

TR-069

The TR-069 protocol is a DSL Forum (<http://www.dslforum.org>) technical specification defining an application layer protocol for remote management of end-user devices, like the OxyGEN miniOffice.

TR-069 Management

Status
 Enabled Disabled

Service
Server URL:
ACS user:
ACS pass:
CPE user:
CPE pass:

Logging
 Enabled Disabled

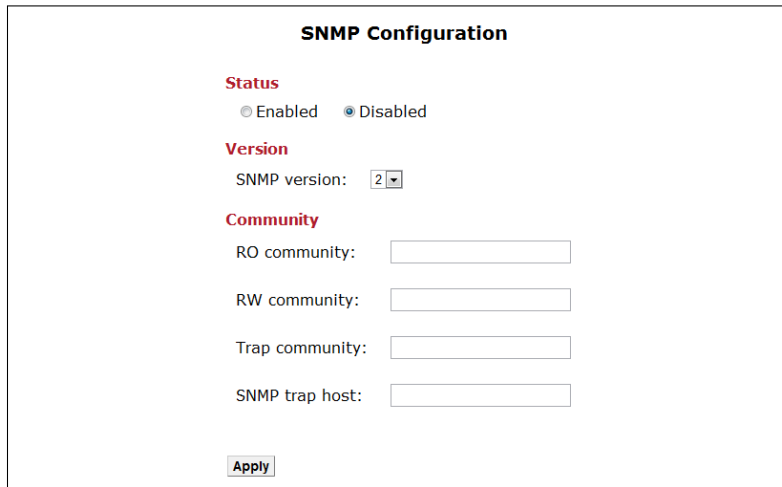
Figure 12.1: TR-069 Configuration

To configure the TR-069 management service:

1. Select **Enabled** or **Disabled** under **Status** to enable or disable the service.
2. Configure in **Server URL** the URL of the Auto Configuration Server (ACS).
3. Configure the **ACS Username** and **Password** for device authentication (optional).
4. Configure the local **CPE Username** and **Password** for ACS-initiated connections to the CPE (optional).
5. Click **Apply**.

SNMP

The Simple Network Management Protocol (SNMP) is a widely used networking management protocol for remote management of all ranges of IP-enabled devices, including end-user devices like the OxyGEN miniOffice.



The image shows a dialog box titled "SNMP Configuration". It contains the following fields and controls:

- Status:** Two radio buttons, "Enabled" and "Disabled". The "Disabled" button is selected.
- Version:** A label "SNMP version:" followed by a dropdown menu showing the value "2".
- Community:** Four text input fields labeled "RO community:", "RW community:", "Trap community:", and "SNMP trap host:".
- Apply:** A button labeled "Apply" at the bottom left.

Figure 12.2: SNMP Configuration

To configure the SNMP management service:

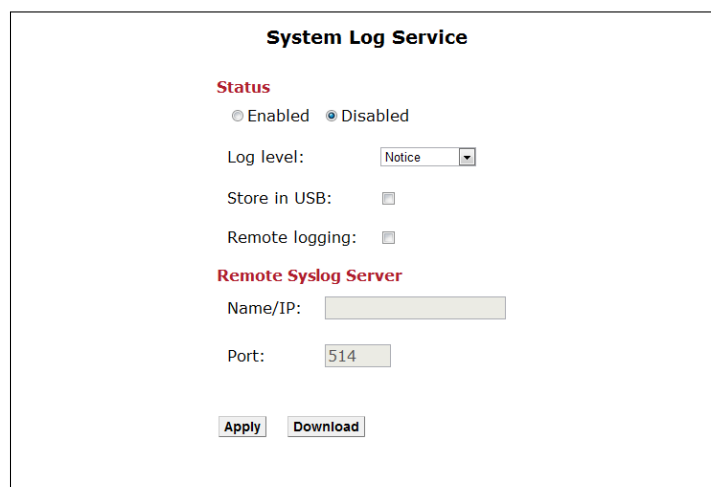
1. Select **Enabled** or **Disabled** under **Status** to enable or disable the service.
2. Select the appropriate **SNMP version**.
3. Enter the Read Only (RO) community string.
4. Click **Apply**.

Syslog

Syslog is the logging service providing information about the operation of the OxyGEN miniOffice.

To configure the Syslog service:

1. Select **Enabled** or **Disabled** under **Status** to enable or disable the service.
2. Click **Apply**.



System Log Service

Status

Enabled Disabled

Log level:

Store in USB:

Remote logging:

Remote Syslog Server

Name/IP:

Port:

Figure 12.3: Syslog Configuration

Using the Web interface of OxyGEN miniOffice, log messages can be viewed in the **System Log** page of the **Status** configuration menu (see page 161).

You can, optionally, also define a remote Syslog server for transmission of the log messages over the network. To this end check the **Remote logging** checkbox and define the remote server's **Name** or **IP** address and the protocol **Port** (default syslog port is 514).

Backup / Restore

This configuration option allows you to save the current configuration of the OxyGEN miniOffice as a backup on a PC, and optionally restore it at a later time.

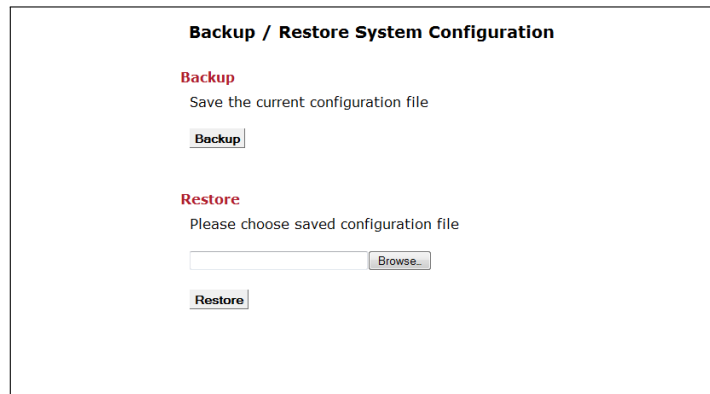


Figure 12.4: Configuration Backup/Restore

Backup Configuration

To save the backup configuration file:

1. Click **Backup**.

A message window opens prompting you to save the file:

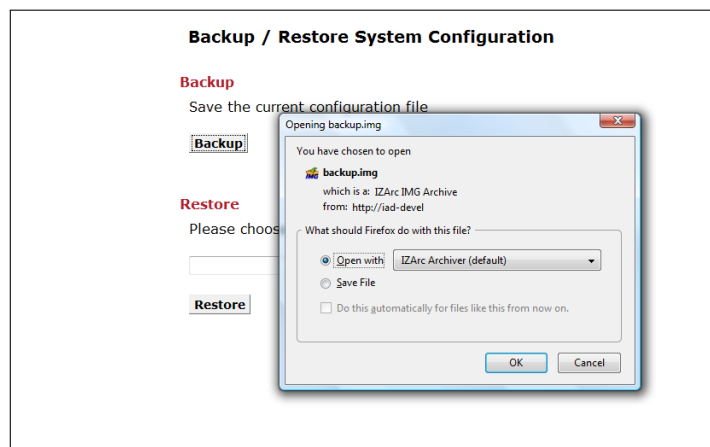


Figure 12.5: Backup the Configuration

2. Click **Save**.
3. Specify the path where the file is to be saved and click **Save**.

Restore Configuration

To restore a previously saved configuration:

1. Click **Browse** to specify the path of the saved configuration file.
2. Click **Restore**.

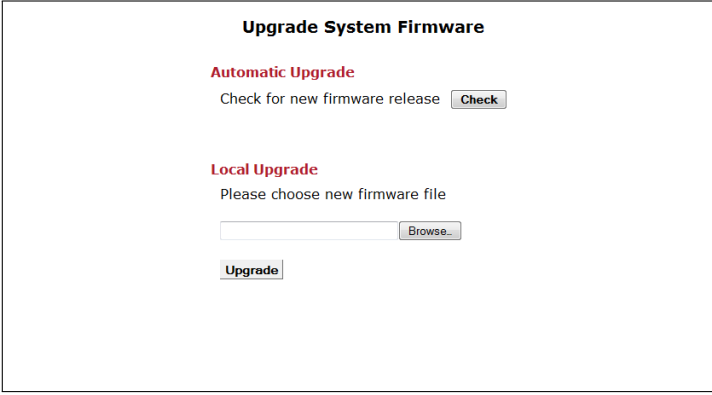


WARNING

The OxyGEN miniOffice will be automatically restarted after the end of the configuration-restore process.

Firmware Upgrade

This page allows you to upgrade the OxyGEN miniOffice to the latest firmware version. This can be performed locally, if you have the new firmware file stored on your PC, or through the Internet, if your ISP has configured a pre-defined server with the latest firmware version.



Upgrade System Firmware

Automatic Upgrade
Check for new firmware release

Local Upgrade
Please choose new firmware file

Figure 12.6: Local Firmware Upgrade

To locally upgrade the firmware:

1. Click **Browse** to specify the path of the firmware file.
2. Click **Upgrade**.



WARNING

Use only the appropriate firmware file for the exact model of your OxyGEN miniOffice.

If, on the other hand, your ISP has configured a web server with the latest firmware version, the **Automatic Upgrade** heading is visible. Click **Check** in order to query the server for a new firmware release. If such a new release is available, a notification message will appear.

Click **Download** in order to download the new firmware file and perform the upgrade.



WARNING

The OxyGEN miniOffice will be automatically restarted after the end of the firmware-upgrade process.

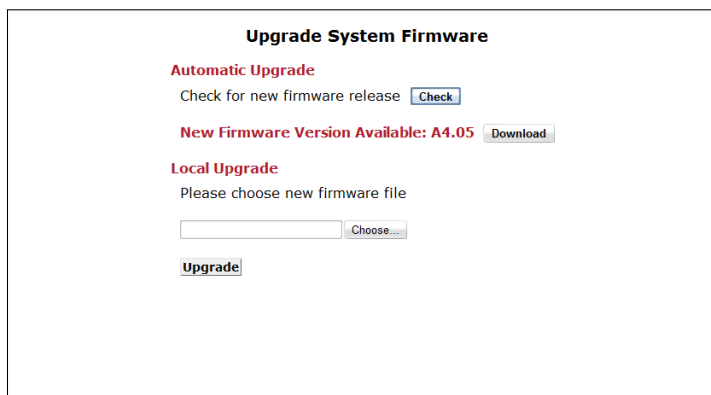
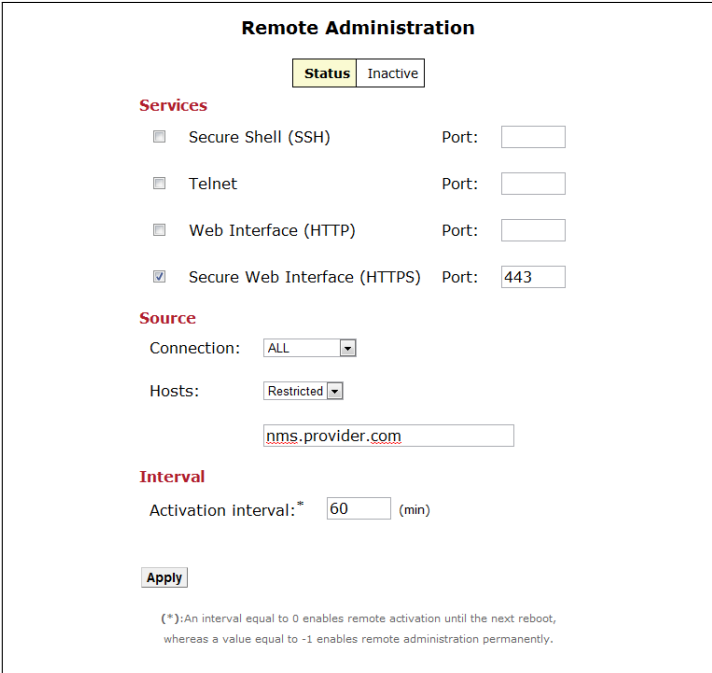


Figure 12.7: Automatic Firmware Upgrade

Remote Admin

This sub-menu controls remote administration access to the OxyGEN miniOffice. This may help the IT support staff of your ISP to configure the device remotely.



Remote Administration

Status Inactive

Services

Secure Shell (SSH) Port:

Telnet Port:

Web Interface (HTTP) Port:

Secure Web Interface (HTTPS) Port:

Source

Connection: ALL

Hosts: Restricted

Interval

Activation interval: 60 (min)

Apply

(*) An interval equal to 0 enables remote activation until the next reboot, whereas a value equal to -1 enables remote administration permanently.

Figure 12.8: Remote Administration

To enable the remote access:

1. Select the remote access services you wish to activate. The available services for remote access are:
 - Secure Shell (SSH)
 - Web Interface (HTTP)
 - Secure Web Interface (HTTPS)
2. For each selected access service optionally specify a port different than the well-known one (e.g. port 8080 instead of 80 for HTTP).
3. Specify **Any** in order to allow incoming connections from any IP address, or restrict remote access for the selected methods for a single **IP** address.
4. Configure the time interval, during which remote access will be enabled (default 10 min). After this interval, remote access will be automatically deactivated.

**Note**

An **Interval** value equal to 0 will keep remote administration activated until the next device restart, whereas a value of -1 will keep it permanently active.

**Note**

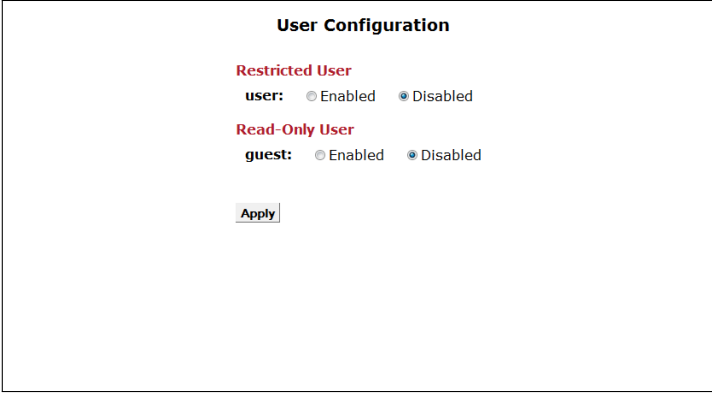
By clicking **New Key**, a password-keyword is generated. This keyword acts as a "seed" for the generation of a temporary local installer account. Further information for this functionality is available upon request.

5. Click **Apply**.

At any moment, you can see the current remote administration status by clicking on the **Support Info** key.

Users

This sub-menu allows you to activate or deactivate the restricted user (username **user**) and the read-only user (username **guest**) profiles of the OxyGEN miniOffice. The former has only access to a pre-configured subset of the available configuration sub-menus and the latter can only view the current device settings without authorization to make modifications.



The screenshot shows a web interface titled "User Configuration". It contains two sections: "Restricted User" and "Read-Only User". Each section has a label and two radio button options: "Enabled" and "Disabled". In the "Restricted User" section, the "user:" label is followed by "Enabled" (unselected) and "Disabled" (selected). In the "Read-Only User" section, the "guest:" label is followed by "Enabled" (unselected) and "Disabled" (selected). Below these sections is an "Apply" button.

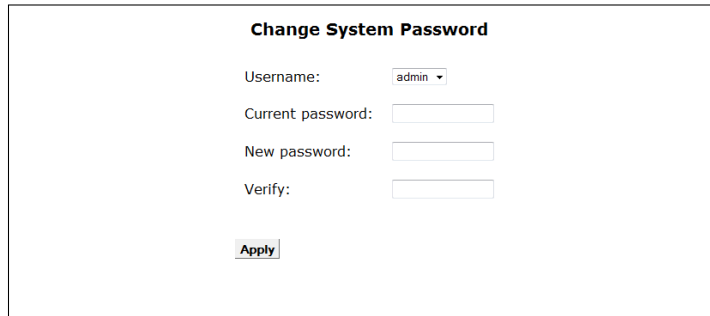
Figure 12.9: Users' Management

To manage the web interface profiles:

1. Select *Enabled* or *Disabled* to change accordingly the status of the corresponding username.
2. Click **Apply**.

Change Password

This sub-menu lets you change the password for the active administration profile.



Change System Password

Username:

Current password:

New password:

Verify:

Figure 12.10: Change Password

To change the password:

1. Enter the **Current password**.
2. Enter the **New password**.
3. Confirm the password by retyping it in the **Verify** field.
4. Click **Apply**.



Note

After changing the password you will have to restart your web browser and login again using the new password value.

Device Restart

This sub-menu lets you reboot the OxyGEN miniOffice. You can reboot it using the following configuration options:

- Current configuration
- Factory defaults configuration

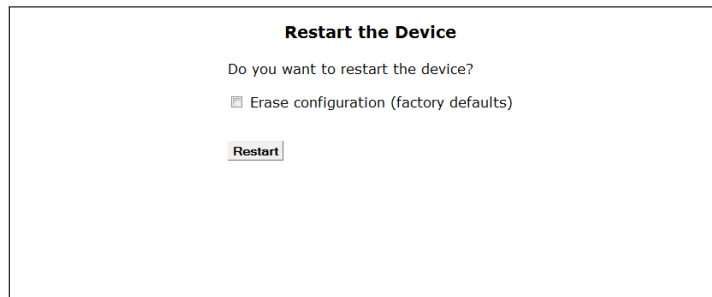


Figure 12.11: Device Reboot

To reboot the OxyGEN miniOffice:

1. Optionally select the **Erase Configuration** checkbox in order to erase the current configuration and restore the factory default one.
2. Click **Restart**.

A message appears displaying the status of the rebooting process:

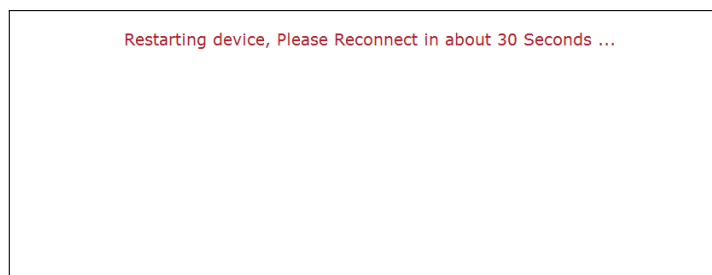


Figure 12.12: Reboot Status

13

Status Menu

The **Status** menu displays device messages and statistics about local interfaces and internet connections. It includes the following sub-menus:

- **About**
- **Battery**
- **System Log**
- **Interfaces**
- **DSL Line**
- **Wireless**
- **Phone Lines**
- **Call Details**
- **ISDN Interfaces**
- **Firewall**
- **Clients**
- **Diagnostics**

- ***Net Statistics***
- ***IP Network***

About

This page displays basic information about the device, including Model Type, Serial Number and Firmware Versions.

Device Status	
Model	Gennet OxyGEN miniOffice
Operating System	Gennet/Linux
DSL Firmware	E.25.57.24 A
Serial	123456789009
MAC Address	00E00C009501
Uptime	17h 7m 41s
Connected	14h 12m 52s
Firmware Details	
Version	GEN01_5.0.1 (Annex A)
Type	OJA25800.N2U
Build	fw2012040613
Last Upgrade	Successful

Figure 13.1: Device Status

Battery

This page provides information about the embedded battery of your OxyGEN miniOffice (optional feature).

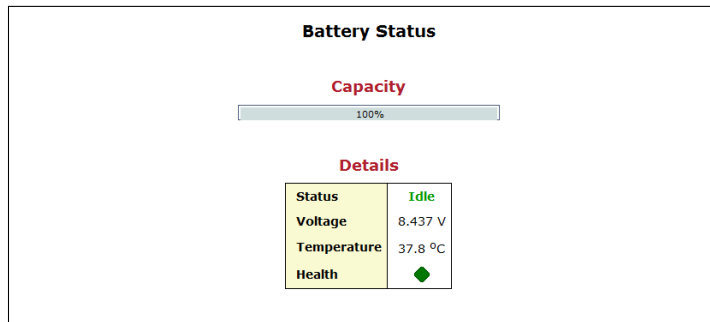


Figure 13.2: Battery Status

The information displayed includes its current **Capacity** and **Status**, the values of **Voltage** and **Temperature** and finally a general battery **Health** indication.

System Log

The **System Log** page provides useful information about the operation of your OxyGEN miniOffice.

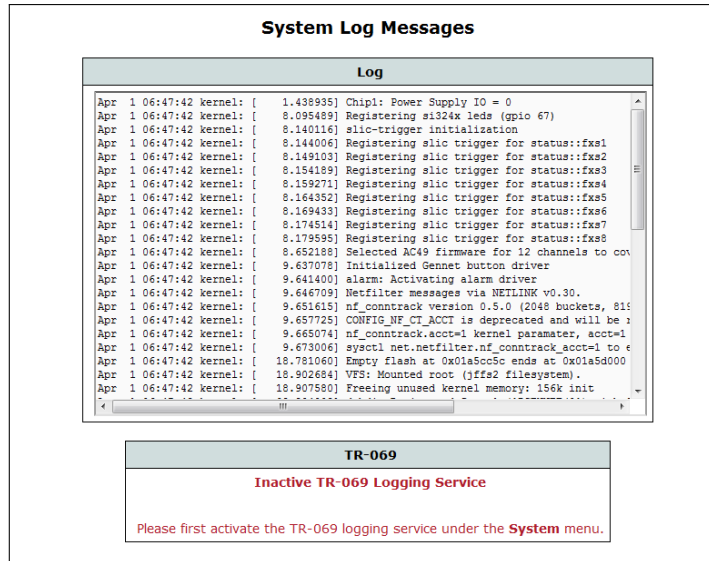


Figure 13.3: System Log

In case the Syslog service has not been activated, an error message appears notifying that you should first activate the logging process (see section **Syslog** on page 146).

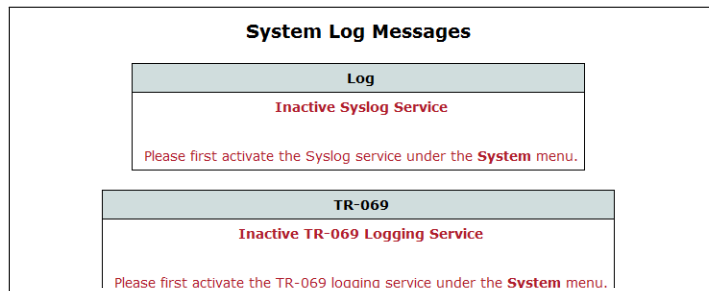















Figure 13.4: System Log Notification

Interfaces

Ethernet Switch

This page displays information about the link and speed status of the LAN Ethernet ports. It also displays the service each port is assigned to (Interface Group), using the icons ,  and  for the Data, Voice and Video services respectively.


Interfaces					
Ethernet Ports					
	LAN-1	LAN-2	LAN-3	LAN-4	GbE-1
Link Status					
Speed	100	-	-	-	-
Duplex	Full	-	-	-	-
Service					

USB Devices		
Type	Status	Action
Storage	No storage media attached	
Printer	No printer attached	
3G Modem	No modem attached	

Figure 13.5: Ethernet Port Status


USB Devices

It also shows information about the status of connected USB devices (Storage disks or Printers) on the USB Host port (optional feature) of the OxyGEN miniOffice.

When an external storage device is connected, the storage link appears. Follow this link in order to browse through the contents of the external storage device. At the same time, the  icon appears in the **Action** column. Use this icon to **Disconnect** the device before physically unplugging it.



WARNING

Before unplugging an external storage device from the OxyGEN miniOffice make sure you first **Disconnect** it using the  icon under the **Devices** category of the **Home** page or in the **Interfaces** sub-menu of the **Status** configuration menu. Removal of the device without disconnecting first, may lead to corrupted data on the storage device!

DSL Line

This page displays basic information about the DSL connection of the OxyGEN miniOffice.

DSL Line Info				
	ADSL-1		ADSL-2	
State	Showtime		HandShake	
Type	AnnexA			
Modulation	ADSL2+		Inactive	
DSLAM	CNXT			
Overall Failures	0		0	
ATM Cell Drop Count	0		0	
Transmitted Frames	201330688		0	
Received Frames	624		0	
Rate	Receive	Transmit	Receive	Transmit
Bit Rate	24,175,300	1,023,200	0	0
Cell Rate	57,017	2,413	0	0
Signal	Local	Remote	Local	Remote
Loss of Signal	0	0	0	0
Signal to Noise Ratio	6.15 dB	15.0 dB	-	-
Line Attenuation	0.5 dB	0.0 dB	-	-
Transmit Power	0.4 dB	8.3 dB	-	-
DSL Errors	Local	Remote	Local	Remote
Severe (SEF)	0	0	0	0
Corrected (FEC)	0	603979776	0	0
Checksum (CRC)	43	0	0	0
Header (HEC)	205	0	0	0

Figure 13.6: DSL Line Information


Available information includes connection status, type of connection, sync rates, signal quality and error counters. Optionally you can also restart the DSL training process by clicking on the **Retrain** button.

Wireless

This page displays a list of the connected wireless clients, as well as a list of the wireless access points in range of the OxyGEN miniOffice (WiFi-enabled devices only).

Wireless Network					
Connected Clients					
Interface	IP	MAC Address	Name	Status	Action
No Entries					
Access Points in Range					
SSID	MAC Address	Channel	Encryption	Signal (%)	
No Entries					

Figure 13.7: Wireless Network Information

By clicking on the Info icon  next to each client entry, you can see more details about the corresponding connected wireless client.

Phone Lines

This page displays information about the active voice calls and the status of basic supplementary services for all phone lines. It also displays the relevant service activation and deactivation codes.

Phone Lines					
Established Channels					
Line	Peer	Codec	On Hold	Direction	Duration
No Entries					
Supplementary Services					
Service	Code	FXS 1	FXS 2	FXS 3	FXS 4
Call Waiting (CW)	43	◆	◆	◆	◆
Anonymous Call Rejection (ACR)	90	◇	◇	◇	◇
Do Not Disturb (DND)	91	◇	◇	◇	◇
Call Forward Unconditional (CFU)	21	◇	◇	◇	◇
Call Forward on Busy (CFB)	67	◇	◇	◇	◇
Call Forward on No Answer (CFNA)	61	◇	◇	◇	◇
Calling Line Identity Restriction (CLIR)	31	◇	◇	◇	◇

NOTE: Activation of a service is performed using the sequence **CODE#, deactivation using *#CODE# and query of the current service status using **#CODE#.

[\[View Other Supplementary Service Codes\]](#)

Figure 13.8: Voice Calls and Services

You can also see the codes for other supported supplementary services, by following the **View Other Supplementary Service Codes** link, which leads to the following page:

Supplementary Service Codes	
Service	Code
Reset all settings	###
Disable all call forwards	#002#
Redial last called number	3131
Dial last caller	3232
Speed dial	*41X
Read speed dial number	#41X
Blind transfer	#9
Attended transfer	*9
Park call	#72
Park calls on	701-720
Calling Line Identity Restriction (per call)	*31*X
Calling Line Identity Presentation (per call)	#31*X
Call Line 1	401
Call Line 2	402
Dial through FXO	

System Operation Codes	
Service	Code
Factory defaults	**880#
Unmount all USB devices	**051#
Turn on wireless	**001#
Turn off wireless	*#001#

Figure 13.9: Service Codes

Call Details

This page displays information about voice call records.

Call Details			
Total Call Duration			
Type	Duration (min:sec)		
Local Calls	0:00		
Incoming Calls	0:00		
Outgoing Calls	0:00		
Last Numbers per Line			
	Incoming	Outgoing	
FXS 1	-	-	
FXS 2	-	-	
FXS 3	-	-	
FXS 4	-	-	
Last 10 Calls			
Source	Destination	Start Time	Duration
No Entries			

Figure 13.10: Call Records

Specifically, it displays the total call duration for **Local** (between the local extensions of the OxyGEN miniOffice), **Incoming** and **Outgoing** calls. It also displays the **Last Incoming** and **Last Outgoing** call for each line and finally a list of the **Last 10** voice calls.

ISDN Interfaces

This page displays information about the status of ISDN interfaces of the OxyGEN miniOffice;

	Mode	Blocked	Link (L1/L2)	Active
BRI-1	TE-PTMP	◆	◆ / ◆	-
BRI-2	NT-PTMP	◆	◆ / ◆	-
Sync port			◆	

Debug Capture

Interface: ▾

Figure 13.11: ISDN Interfaces

For each ISDN interface, it is possible to see the **Status**, the **Mode** of operation (External (TE) vs Internal (NT) and Point-to-Point (PTP) vs Point-to-Multipoint (PTMP)), the **Link** status of ISDN Layers 1 and 2, and finally the number of **Active** B-channels.

Firewall

This page displays a list of the active firewall rules.

Firewall Information					
Statically Forwarded Ports					
Port	Source	Destination	Packets		
1	TCP 7217	ALL (ANY)	192.168.1.51 (7217)	0	
2	UDP 7217	ALL (ANY)	192.168.1.51 (7217)	0	
UPnP/NAT-PMP Forwarded Ports					
Application	Port	Source	Destination		
No Entries					
Filtered IP Traffic					
Port	Interfaces	Source	Destination	Filter	Packets
1	TCP 22	* ⇒ *	192.168.1.88	ALL	0

🗑️ Drop
🚫 Reject
🟢 Accept

Figure 13.12: Current Firewall Status

The rules are divided into three different categories:

- **Statically Forwarded Ports:** which contains all active port forwarding rules (see section **Port Forward** on page 94).
- **UPnP/NAT-PMP Forwarded Ports:** which contains ports forwarded automatically through the corresponding protocols. (see section **UPnP / NAT-PMP** on page 96).
- **Filtered IP Traffic:** which displays the list of IP filtering rules. (see section **IP Filters** on page 97).

Clients

This page provides a list of all clients connected to the OxyGEN miniOffice.




Interface	IP	MAC Address	Name	Status	Action
Ethernet	192.168.1.73	00:00:5a:10:02:60	HOMEPC		

Figure 13.13: Connected Clients

By clicking on the Info icon  next to each client entry, you can see more details about the corresponding connected LAN client.

Diagnostics

This page provides you with an option to troubleshoot IP connectivity from your OxyGEN miniOffice. You can either perform a **Ping** test to check plain end-to-end connectivity or a **Traceroute** test in order to identify also the intervening nodes.

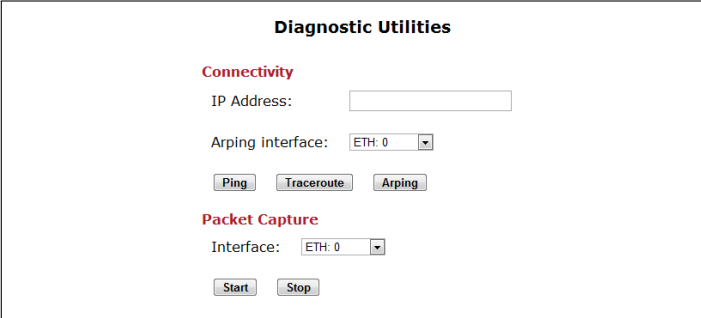


Figure 13.14: Troubleshooting

To perform an IP connectivity test:

1. Enter the IP address of a target endpoint.
2. Click either **Ping** or **Traceroute** in order to perform the corresponding IP connectivity test.

Additionally, it is possible to perform detailed **IP Debugging** through packet capturing (also known as "sniffing") over a specific WAN connection. Using the **Capture interface** drop-down list, select the interface of the desired WAN connection and click **Start capture**. Click **Stop capture** in order to stop the packet capturing process and the capture file will automatically be downloaded to your PC via the Web browser. Use a program like Wireshark (<http://www.wireshark.org/>) in order to open and analyze the file.



Note

There is a limit on the maximum size of the file with the captured data packets equal to 20MB.



Note

When the **Store in USB** checkbox has been checked in the **Syslog** configuration menu (see section **Syslog** on page (see page 146), and a storage device has been attached to the USB interface of the OxyGEN miniOffice, the capture file will be stored in the attached storage device, and the maximum-size limit of 20MB is not applied.

Net Statistics

This page displays traffic graphs of LAN and Internet statistics. **Outbound** and **Inbound** traffic is displayed as separate lines on the corresponding graph, for both local (LAN) and broadband (Internet) traffic.

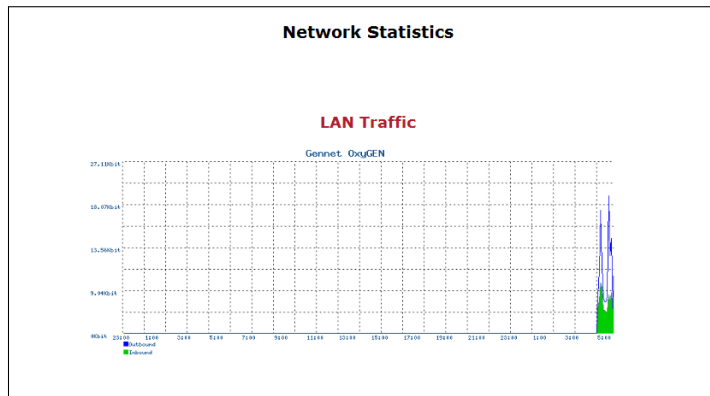


Figure 13.15: Network Statistics

Additionally by clicking on each graph, a new page appears with more detailed information (Daily, Weekly profiles).

IP Network

This sub-menu displays the list of active IP Interfaces on the OxyGEN miniOffice, the IP routing table (including static and dynamic routes) and a list of the active Domain Name Service (DNS) servers. It also displays the relevant timeout values as well as the maximum and current number of active IP connections.

IP Network Information

Interfaces

Interface	IP Address	Mac Address	Status
brs_data	192.168.1.254	00:1D:1C:FF:14:0B	◆
brs_ssid2	10.99.56.1	00:00:00:00:00:00	◆
brs_video	n/a	00:00:00:00:00:00	◆
brs_voip	n/a	00:00:00:00:00:00	◆
brs_wan	n/a	00:00:00:00:00:00	◆
eth0	n/a	00:1D:1C:FF:14:0B	◆
gre0	n/a	n/a	◆
lo	127.0.0.1	n/a	◆
tunl0	n/a	n/a	◆
wlan0	n/a	00:1D:1C:29:A4:C1	◆

Routing Table

Network	Mask	Gateway	Interface
192.168.1.0	255.255.255.0	0.0.0.0	brs_data
10.99.56.0	255.255.255.0	0.0.0.0	brs_ssid2
239.0.0.0	255.0.0.0	0.0.0.0	brs_data

Routing Rules

From	Lookup	Device
No Entries		

Active DNS Servers

Priority	Address	Interface
No Entries		

Connection Tracking

Timeout	Generic	TCP	UDP	UDP stream
	600	7200	30	180
Connections	Maximum	Current	Percentage	
	1984	20	1%	

[\[View Detailed Connection Tracking\]](#)

Figure 13.16: IP Network Information

In order to see a detailed list of the IP connections, you can follow the **View Detailed Connection Tracking** link and a page similar to the following will appear:

Detailed Connection Tracking				
Service	Protocol	Source	Destination	State
www	tcp	192.168.1.73:4524	192.168.1.254:80	TIME_WAIT
www	tcp	192.168.1.73:4532	192.168.1.254:80	TIME_WAIT
www	tcp	192.168.1.73:4534	192.168.1.254:80	CLOSE_WAIT
www	tcp	192.168.1.73:4533	192.168.1.254:80	CLOSE_WAIT
www	tcp	192.168.1.73:4512	192.168.1.254:80	TIME_WAIT
www	tcp	192.168.1.73:4529	192.168.1.254:80	TIME_WAIT
ssh	tcp	192.168.1.73:4185	192.168.1.254:22	ESTABLISHED
www	tcp	192.168.1.73:4538	192.168.1.254:80	ESTABLISHED
www	tcp	192.168.1.73:4531	192.168.1.254:80	CLOSE_WAIT
www	tcp	192.168.1.73:4514	192.168.1.254:80	TIME_WAIT
www	tcp	192.168.1.73:4523	192.168.1.254:80	TIME_WAIT
www	tcp	192.168.1.73:4516	192.168.1.254:80	TIME_WAIT
www	tcp	192.168.1.73:4526	192.168.1.254:80	TIME_WAIT
?	udp	192.168.1.254:3073	239.255.255.250:1900	
www	tcp	192.168.1.73:4525	192.168.1.254:80	TIME_WAIT
www	tcp	192.168.1.73:4522	192.168.1.254:80	TIME_WAIT
www	tcp	192.168.1.73:4539	192.168.1.254:80	ESTABLISHED
www	tcp	192.168.1.73:4537	192.168.1.254:80	ESTABLISHED
www	tcp	192.168.1.73:4515	192.168.1.254:80	TIME_WAIT
www	tcp	192.168.1.73:4513	192.168.1.254:80	TIME_WAIT
www	tcp	192.168.1.73:4521	192.168.1.254:80	TIME_WAIT
www	tcp	192.168.1.73:4511	192.168.1.254:80	TIME_WAIT
www	tcp	192.168.1.73:4530	192.168.1.254:80	TIME_WAIT
domain	udp	127.0.0.1:3186	127.0.0.1:53	

Figure 13.17: Detailed IP Connection List

14

Troubleshooting

This chapter suggests solutions for problems you may encounter in installing or using the OxyGEN miniOffice, and provides instructions for using common IP utilities to diagnose problems.

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

Testing your Setup

Once you have connected your hardware and configured your PCs, any computer on your LAN should be able to use the device's DSL connection to access the Internet. To test the connection, turn on the device, wait for 60 seconds and then verify that the LEDs are illuminated as follows:

LED	Behavior
Power	Solid Green during the boot sequence and during normal operation. If this light is not on, check the power cable attachment.
Alarm	Solid Amber during the boot sequence. Once the boot sequence is finished, the led is off.
DSL	Blinking Green when a synchronization attempt is being performed. Solid Green upon successful synchronization.
Internet	Blinking Red while trying to connect. Solid Green when a valid IP address has been assigned to the device by the ISP. Blinking Green when an invalid username/password combination is being used.
Ethernet	Solid Green to indicate active link on the corresponding Ethernet link. Blinking when the device is sending or receiving data from the LAN.
Wireless	Solid Green to indicate that the Wireless LAN connection is operational. Slow blinking while the wireless operation is being turned on or off. (WiFi-enabled devices only)
USB	Solid Green to indicate that the USB connection is operational.

Table 14.1: LED Indicators


If the LEDs illuminate as expected, test your Internet connection from a LAN computer. To do this, open your web browser, and type the URL of any external website (such as <http://www.yahoo.com>). The device should connect to the site.

If the LEDs do not illuminate as expected, you may need to configure your Internet access settings using the information provided by your ISP. If the LEDs still do not illuminate as expected or the web page is not displayed, follow the Troubleshooting Suggestions presented in the next paragraph or contact your

ISP for assistance.

Troubleshooting Suggestions

Problem	Troubleshooting Suggestion
LEDs	
<i>Power LED does not illuminate after product is turned on.</i>	<i>Verify that you are using the power adapter provided with the device and that it is securely connected to the OxyGEN miniOffice and a wall socket/power strip.</i>
<i>DSL LED does not illuminate after phone cable is attached.</i>	<i>Verify that a standard telephone cable (called an RJ-11 cable) like the one provided is securely connected to the DSL port and your wall phone port. Allow about 60 seconds (depending on the distance between the router and the telephone exchange and on the quality of the telephone line) for the device to negotiate a connection with your ISP.</i>
<i>Ethernet LED does not illuminate after Ethernet cable is attached.</i>	<i>Verify that the Ethernet cable is securely connected to your PC or LAN switch and to the OxyGEN miniOffice. Make sure the PC and/or LAN switch is turned on. Verify that your cable is sufficient for your network requirements. A 100 Mbit/sec network (100-BaseT) should use cables labeled CAT 5. A 10Mbit/sec network may tolerate lower quality cables.</i>
Internet Access	
<i>My PC cannot access the Internet</i>	<p data-bbox="657 1102 1338 1354"><i>Run a health check on your device. Use the Ping utility (discussed in the following section) to check whether your PC can communicate with the OxyGEN miniOffice's LAN IP address (by default 192.168.1.254). If it cannot, check first the Ethernet cabling. The Ethernet LED corresponding to the Ethernet port being used must be lit or blinking. If you statically assigned a private IP address to the computer, (not a registered public address), verify the following:</i></p> <ul data-bbox="706 1354 1338 1627" style="list-style-type: none"> <li data-bbox="706 1354 1338 1512">● <i>Check that the gateway IP address on the computer is OxyGEN miniOffice's LAN IP address (by default 192.168.1.254). If it is not, correct the address or configure the PC to receive IP information automatically through DHCP.</i> <li data-bbox="706 1522 1338 1627">● <i>Verify with your ISP that the DNS server specified for the PC is valid. Correct the address or configure the PC to receive this information automatically.</i>

<p><i>My LAN PCs cannot display web pages on the Internet.</i></p>	<p>Verify that the DNS server IP address specified on the PCs is correct for your ISP, as discussed in the item above. If you specified that the DNS server be assigned dynamically from a server, then verify with your ISP that the address configured on the OxyGEN miniOffice is correct, and then you can use the Ping utility, discussed on page 180, to test connectivity with your ISP's DNS server.</p>
<hr/> <p style="text-align: center;">Web pages</p> <hr/>	
<p><i>I forgot/lost my username or password.</i></p>	<p>If you have not changed the password from the default, try using admin as both the username and password. Otherwise, you can reset the device to the default configuration by pressing the Reset button on the rear panel of the device (see Rear Panel on page 26). Then, type the default username and password shown above.</p> <p> WARNING: Resetting the device removes any custom settings and returns all settings to their default values.</p>
<p><i>I cannot access the web pages from my browser.</i></p>	<p>Use the Ping utility, discussed in the following section, to check whether the PC can communicate with the device's LAN IP address (by default 192.168.1.254). If it cannot, check the Ethernet cabling. Verify that you are using Microsoft Internet Explorer version 5.5 or newer, Mozilla Firefox 1.5 or newer, Google Chrome, Apple Safari version 1.2 or newer. Verify that the PC's IP address is configured as being on the same subnet as the IP address assigned to the LAN port on the OxyGEN miniOffice.</p>

Diagnosing Problem using IP Utilities

Ping

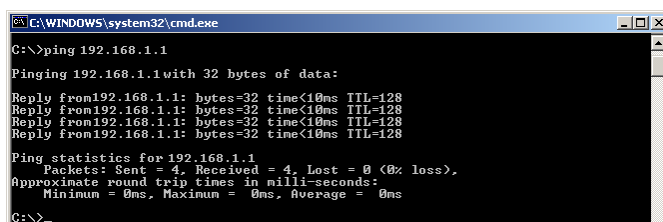
Ping is a command you can use to check whether your PC can recognize other computers on your network and the Internet. A ping command sends a message to the computer you specify. If the computer receives the message, it sends messages in reply. To use it, you must know the IP address of the computer with which you are trying to communicate.

*On Windows-based computers, you can execute a ping command from the Start menu. Click the **Start** button, and then click **Run**. In the **Open** text box, type a statement such as the following:*

```
ping 192.168.1.254
```

*Click **OK**. You can substitute any private IP address on your LAN or a public IP address for an Internet site, if known.*

*If the target computer receives the message, a **Command Prompt** window is displayed:*



```
C:\WINDOWS\system32\cmd.exe
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<10ms TTL=128
Reply from 192.168.1.1: bytes=32 time<10ms TTL=128
Reply from 192.168.1.1: bytes=32 time<10ms TTL=128
Reply from 192.168.1.1: bytes=32 time<10ms TTL=128
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

Figure 14.1: Using the Ping Utility

*If the target computer cannot be located, you will receive the message **Request timed out**.*

Using the ping command, you can test whether the path to the OxyGEN miniOffice is working (using the preconfigured default LAN IP address 192.168.1.254) or another address you assigned.

*You can also test whether access to the Internet is working by typing an external address, such as that for www.yahoo.com (216.115.108.243). If you do not know the IP address of a particular Internet location, you can use the **nslookup** command, as explained in the following section.*

From most other IP-enabled operating systems, you can execute the same command at a command prompt or through a system administration utility.

nslookup

You can use the nslookup command to determine the IP address associated with an Internet site name. You specify the common name, and the nslookup command looks up the name in on your DNS server

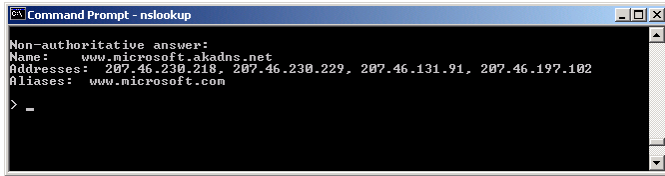
(usually located with your ISP). If that name is not an entry in your ISP's DNS table, the request is then referred to another higher-level server, and so on, until the entry is found. The server then returns the associated IP address.

On Windows-based computers, you can execute the **nslookup** command from the Start menu. Click the **Start** button, and then click **Run**. In the **Open** text box, type the following:

```
nslookup
```

Click **OK**. A **Command Prompt** window is displayed with a bracket prompt (>). At the prompt, type the name of the Internet address that you are interested in, such as **www.microsoft.com**.

The window will display the associate IP address, if known, as shown below:



```
Command Prompt - nslookup
Non-authoritative answer:
Name:    www.microsoft.akadns.net
Addresses: 207.46.230.218, 207.46.230.229, 207.46.131.91, 207.46.197.102
Aliases: www.microsoft.com
>
```

Figure 14.2: Using the nslookup Utility

There may be several addresses associated with an Internet name. This is common for web sites that receive heavy traffic; they use multiple, redundant servers to carry the same information.

To exit from the **nslookup** utility, type **exit** and press **[Enter]** at the command prompt.



Configuring the Internet Settings

This appendix provides instructions for configuring the Internet settings on your computers to work with the OxyGEN miniOffice.

Configuring Ethernet PCs

Before you Begin

By default, the OxyGEN miniOffice automatically assigns the required Internet settings to your PCs. You need to configure the PCs to accept this information when it is assigned.



Note

*In some cases, you may want to assign Internet information manually to some or all of your computers rather than allow the OxyGEN miniOffice to do so. See **Assigning Static Internet Information to your PCs** on page 185 for instructions.*

- *If you have connected your LAN PCs via Ethernet to the OxyGEN miniOffice, follow the instructions that correspond to the operating system installed on your PC:*
 - *Windows Vista PCs on page 184*
 - *Windows XP PCs on page 184*

- *Windows 2000 PCs on page 184*
- *Apple Mac OS X PCs on page 185*

- *If you want to allow Wireless PCs to access your device, follow the instructions in **Configuring Wireless PCs** on page 186.*

Windows Vista PCs

1. *In the Windows task bar, click the Start button, and then click Control Panel.*
2. *Click on the Classic View option on the left side of the screen, and then double-click the Network and Sharing Center icon.*
3. *Click on the Manage Network Connections option on the left side of the screen.*
4. *Right-click on the Local Area connection and select Properties.*
5. *Click the radio button labeled Obtain an IP address automatically. Also click the radio button labeled Obtain a DNS server address automatically.*
6. *Click OK to confirm your changes, and then close the Control Panel.*

Windows XP PCs

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

Windows 2000 PCs

First, check for the IP protocol and, if necessary, install it:

1. *In the Windows task bar, click the Start button, point to Settings, and then click Control Panel.*
2. *Double-click the Network and Dial-up Connections icon.*

3. In the *Network and Dial-up Connections* window, right-click the *Local Area Connection* icon, and then select *Properties*. The *Local Area Connection Properties* dialog box is displayed with a list of currently installed network components. If the list includes *Internet Protocol (TCP/IP)*, then the protocol has already been enabled. Skip to step 10.
4. If *Internet Protocol (TCP/IP)* does not display as an installed component, click *Install*.
5. In the *Select Network Component Type* dialog box, select *Protocol*, and then click *Add*.
6. Select *Internet Protocol (TCP/IP)* in the *Network Protocols* list, and then click *OK*. You may be prompted to install files from your *Windows 2000* installation CD or other media. Follow the instructions to install the files.
7. If prompted, click *OK* to restart your computer with the new settings and repeat steps 1-3. Next, configure the PCs to accept IP information assigned by the *OxyGEN miniOffice*.
8. In the *Local Area Connection Properties* dialog box, select *Internet Protocol (TCP/IP)* and then click *Properties*.
9. In the *Internet Protocol (TCP/IP) Properties* dialog box, click the radio button labeled *Obtain an IP address automatically*. Also click the radio button labeled *Obtain DNS server address automatically*.
10. Click *OK* twice to confirm and save your changes, and then close the *Control Panel*.

Apple Mac OS X PCs

1. Select *Apple* and then *System Preferences*.
2. Click on the *Network* icon.
3. Select the *Ethernet* entry on the left side of the window.
4. Select *Automatic* in the *Location* drop-down list.
5. Select *Using DHCP* in the *Configure* drop-down list.
6. Click *Apply* to confirm your changes.

Assigning Static Internet Information to your PCs

If you are a typical user, you will not need to assign static Internet information to your LAN PCs because your ISP automatically assigns this information for you.

In some cases however, you may want to assign Internet information to some or all of your PCs directly (often called "statically"), rather than allowing the *OxyGEN miniOffice* to assign it. This option may be desirable (but not required) if:

- You have obtained one or more public IP addresses that you want to always associate with specific computers (for example, if you are using a computer as a public web server).
- You maintain different subnets on your LAN (subnets are described in **Appendix B**).

Before you begin, you must have the following information available:

- The IP address and subnet mask of each PC
- The IP address of the default gateway for your LAN. In most cases, this is the address assigned to the LAN port on the OxyGEN miniOffice. By default, the LAN port is assigned the IP address **192.168.1.254**. (You can change this number or another number can be assigned by your ISP.)
- The IP address of your ISP's Domain Name System (DNS) server.

On each PC to which you want to assign static information, follow the instructions on pages 184 through 185 relating only to checking for and/or installing the IP protocol. Once it is installed, continue to follow the instructions for displaying each of the Internet Protocol (TCP/IP) properties. Instead of enabling dynamic assignment of the IP addresses for the computer, DNS server and default gateway, click the radio buttons that enable you to enter the information manually.

**Note**

Your PCs must have IP addresses that place them in the same subnet as the OxyGEN miniOffice's LAN port.

Configuring Wireless PCs

You need to configure the operating system installed on your Wireless enabled PCs using the same procedure described for **Configuring Ethernet PCs** on page 183.

Positioning the Wireless PCs

The wireless network cards used determine the maximum distance between your wireless PCs and your device. Guidelines on positioning the hardware components of your wireless network should be provided by your network card provider.

Wireless PC Cards and Drivers

Each PC on your wireless LAN must be fitted with a wireless access card. You must also install the corresponding driver files for your particular wireless card on your PC. You should receive driver files and instructions on how to install them together with your wireless card.

Configuring PC Access to your Wireless Device

Before you start configuring your Wireless PC, you must ensure that you have:

- *A Wireless access card for each of the PCs*
- *Corresponding wireless access card driver software files*

The configuration steps below will vary depending on both the operating system and wireless card installed on the PC. These steps provide a basic outline, however you should refer to the documentation provided with your wireless access card for specific instructions. To configure Wireless PCs:

- 1. Install the wireless access card.*
- 2. Install the wireless driver software files.*
- 3. Configure the following wireless parameters on each of the wireless PCs:*
 - i Set the adapter to use infrastructure mode. This configures the PCs to access each other and the Internet via the OxyGEN miniOffice.*
 - ii Configure the SSID, encryption method and channel to match the corresponding values previously configured on the device. (see **Security** on page 85). Default values are shown in Table 4.2 on page 49.*

Your wireless network can now communicate with the Internet via the device.

B

IP Addresses, Network Masks, and Subnets

IP Addresses



Note

This section refers only to IP addresses for IPv4 (version 4 of the Internet Protocol). IPv6 addresses are not covered. This section assumes basic knowledge of binary numbers, bits and bytes.

IP addresses, the Internet's version of telephone numbers, are used to identify individual nodes (computers or devices) on the Internet. Every IP address contains four numbers, each from 0 to 255 and separated by dots (periods), e.g. 20.56.0.211. These numbers are called, from left to right, field1, field2, field3, and field4.

This style of writing IP addresses as decimal numbers separated by dots is called dotted decimal notation. The IP address 20.56.0.211 is read "twenty dot fifty-six dot zero dot two-eleven."

Structure of an IP Address

IP addresses have a hierarchical design similar to that of telephone numbers. For example, a 7-digit telephone number starts with a 3-digit prefix that identifies a group of thousands of telephone lines, and ends with four digits that identify one specific line in that group. Similarly, IP addresses contain two kinds of information:

- **Network ID**
Identifies a particular network within the Internet or intranet
- **Host ID**
Identifies a particular computer or device on the network

The first part of every IP address contains the network ID, and the rest of the address contains the host ID. The length of the network ID depends on the network's class (see following section). The table below shows the structure of an IP address.

	Field1	Field2	Field3	Field4
Class A	Network ID	Host ID		
Class B	Network ID		Host ID	
Class C	Network ID			Host ID

Here are some examples of valid IP addresses:

- *Class A: 10.30.6.125 (network = 10, host = 30.6.125)*
- *Class B: 129.88.16.49 (network = 129.88, host = 16.49)*
- *Class C: 192.60.201.11 (network = 192.60.201, host = 11)*

Network Classes

The three commonly used network classes are A, B, and C. (There is also a class D but it has a special use beyond the scope of this discussion.) These classes have different uses and characteristics.

Class A networks are the Internet's largest networks, each with room for over 16 million hosts. Up to 126 of these huge networks can exist, for a total of over 2 billion hosts. Because of their huge size, these networks are used for WANs and by organizations at the infrastructure level of the Internet, such as your ISP.

Class B networks are smaller but still quite large, each able to hold over 65,000 hosts. There can be up to 16,384 class B networks in existence. A class B network might be appropriate for a large organization such as a business or government agency.

Class C networks are the smallest, only able to hold 254 hosts at most, but the total possible number of class C networks exceeds 2 million (2,097,152 to be exact). LANs connected to the Internet are usually class C networks.

Some important notes regarding IP addresses:

- The class can be determined easily from field1:

- field1 = 1-126: Class A
- field1 = 128-191: Class B
- field1 = 192-223: Class C

(field1 values not shown are reserved for special uses)

- A host ID can have any value except all fields set to 0 or all fields set to 255, as those values are reserved for special uses.

Subnet Masks

A mask looks like a regular IP address, but contains a pattern of bits that tells what parts of an IP address are the network ID and what parts are the host ID: bits set to 1 mean "this bit is part of the network ID" and bits set to 0 mean "this bit is part of the host ID".

Subnet masks are used to define subnets (what you get after dividing a network into smaller pieces). A subnet's network ID is created by "borrowing" one or more bits from the host ID portion of the address. The subnet mask identifies these host ID bits.

For example, consider a class C network 192.168.1. To split this into two subnets, you would use the subnet mask:

255.255.255.128

It's easier to see what's happening if we write this in binary form:

11111111. 11111111. 11111111.10000000

As with any class C address, all of the bits in field1 through field3 are part of the network ID, but note how the mask specifies that the first bit in field4 is also included. Since this extra bit has only two values (0 and 1), this means there are two subnets. Each subnet uses the remaining 7 bits in field4 for its host IDs, which range from 1 to 126 hosts (instead of the usual 0 to 255 for a class C address).

Similarly, to split a class C network into four subnets, the mask is:

255.255.255.192 or 11111111.11111111.11111111.11000000

The two extra bits in field4 can have four values (00, 01, 10, 11), so there are four subnets. Each subnet uses the remaining six bits in field4 for its host IDs, ranging from 1 to 62.

**Note**

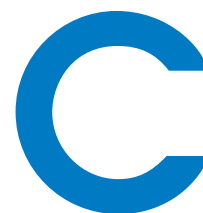
Sometimes a subnet mask does not specify any additional network ID bits, and thus no subnets. Such a mask is called a default subnet mask. These masks are:

Class A:255.0.0.0

Class B:255.255.0.0

Class C:255.255.255.0

These are called default because they are used when a network is initially configured, at which time it has no subnets.



Network Printing

The OxyGEN miniOffice supports alternative ways of network printing through a printer attached to the USB Host port (optional feature). Those, depending on the exact firmware version, are:

- AppSocket/JetDirect
- Internet Printing Protocol (IPP)

The user can configure the printing system using the Web configuration pages, under the **Printing** sub-menu of the **Advanced** configuration menu. Additionally, the current status of a connected printer can be seen in the **Interfaces** page of the **Status** configuration menu.

AppSocket / JetDirect

This is the most efficient way to use the printer. With this method, the PC provides the printing data as soon as they are going to be printed, requiring this way no spooling (and thus no storage space) in the OxyGEN miniOffice. As a consequence, there is no limit on the size of the submitted print jobs.

In order to install the printer in Microsoft Windows:

1. In the Windows task bar, click the Start button, point to Settings, and then click Printers and Faxes.
2. Click Add a Printer. The Add Printer Wizard is activated.

3. *Select the Local Printer option.*
4. *Make sure that the Automatically detect and install my Plug and Play printer option is NOT selected and click Next.*
5. *Select Create a new port and Standard TCP/IP Port as Type of port. Click Next.*
6. *The Add Standard TCP/IP Printer Port Wizard is activated Click Next.*
7. *Enter **192.168.1.254** in the Printer Name or IP Address field, and click Next.*
8. *Select Custom, and click Settings.*
9. *In the Configure Standard TCP/IP Port Monitor window that appears, select the Raw radio button, verify that the Port Number is 9100, and finally click OK.*
10. *Click Finish to exit the Add Standard TCP/IP Printer Port Wizard and continue with the installation process.*
11. *If prompted to install a driver for the printer, select the printer's make and model from the displayed list or click Have disk in order to specify a driver location.*
12. *Finally assign a name to the printer click Next.*
13. *Click Finish to exit the wizard and finish the printer installation process.*

Internet Printing Protocol (IPP)

This method is based on a spooling server, embedded into the OxyGEN miniOffice, which uses the IPP protocol. This alternative requires the use of local storage space in the OxyGEN miniOffice, which naturally imposes an upper limit to the size of submitted print jobs. In normal situations, printing jobs are roughly limited to 40-60 pages.

In order to install the printer in Microsoft Windows:

1. *In the Windows task bar, click the Start button, point to Settings, and then click Printers and Faxes.*
2. *Click Add a Printer. The Add Printer Wizard is activated.*
3. *Select the Network Printer option and click Next.*
4. *Select Connect to a printer on the Internet.*
5. *Enter **http://192.168.1.254:631/classes/Oxygen_Printers** in the URL field, and click Next.*

6. If prompted to install a driver for the printer, select the printer's make and model from the displayed list or click *Have disk* in order to specify a driver location.
7. Finally assign a name to the printer click *Next*.
8. Click *Finish* to exit the wizard and finish the printer installation process.

**WARNING**

It is **STRONGLY** recommended to use the **AppSocket/JetDirect** printing method, since it has no limit on the size of the print-job and will have the least impact on the operation of your OxyGEN miniOffice.

**Note**

The IP address **192.168.1.254** used in all the configuration examples, is the default LAN IP address of your OxyGEN miniOffice. Make sure you modify the value accordingly, if you have manually changed the LAN IP address of your device.

**Note**

Some of the network printing protocols described above may not be available in specific OxyGEN miniOffice firmware versions.



Microsoft Windows and WPA/WPA2 support

The OxyGEN miniOffice supports alternative ways of securing the wireless communication. Those are:

- *Wired Equivalent Privacy (**WEP**): a widely used, but deprecated wireless security method because of the deficiencies found in its encryption algorithm.*
- *Wi-Fi Protected Access (**WPA**): an encryption method that provides superior security compared to WEP. It has been introduced as an intermediate measure to take the place of WEP until the preparation of the full IEEE 802.11i standard and implements the majority of the latter.*
- *Wi-Fi Protected Access 2 (**WPA2**): the encryption method that implements the mandatory elements of the IEEE 802.11i standard and replaced WPA.*

As mentioned, WEP is a legacy security method which has proven to be vulnerable to external attacks and for this reason has been replaced by WPA2, with WPA being an intermediate step during the WEP-to-WPA2 transition. In order to be able to use the WPA2 security algorithm, however, one has to make sure that it is supported by both the Operating System of his PC and the driver of the PC's wireless card. Unfortunately, there are cases of legacy equipment where there is only support for WEP or there is support for the interim WPA and not for the final 802.11i (i.e. WPA2) standard.

In the case of Microsoft Windows, WPA and WPA2 support is offered either by default or through an update according to the following:

- *Windows XP with Service Pack 3 (SP3) and newer (e.g. Windows Vista, Windows 7, Windows Server 2008): WPA and WPA2 are supported by default.*

- *Windows XP SP2: WPA (but not WPA2) is supported by default. In order to add support for WPA2, one has either to upgrade to SP3 or to install the Wireless Client Update for Windows XP with Service Pack 2 from Microsoft (see <http://support.microsoft.com/kb/917021>).*
- *Windows XP SP1: neither WPA nor WPA2 are supported by default. In order to add support for both WPA and WPA2, one has to upgrade to newer SP versions. Alternatively, WPA (but not WPA2) support can be added by installing the Windows XP Support Patch for Wi-Fi Protected Access from Microsoft (see <http://support.microsoft.com/kb/815485>).*

Computers with Windows versions older than Windows XP SP1, do not offer WPA and/or WPA2 support and must be upgraded to newer OS versions in order to do so.



Creating an SSL VPN

General Info

The list of features supported by the Gennet OxyGEN series of broadband access devices, include the creation of a secure, SSL-based **Virtual Private Network (VPN)** connection.

A **VPN** connection is the creation of an encrypted tunnel between two endpoints (e.g. the PC of a remote user and the OxyGEN miniOffice) for the secure and reliable exchange of data. This way, remote users or sites have access to files and networking resources in a central location just as if they were physically present.

An **SSL VPN** is a form of VPN that uses the **SSL (Secure Sockets Layer)** protocol for ensuring the security of data transmitted over the Internet. In contrast to the traditional **IPSec (Internet Protocol Security)** VPN Tunnels, an SSL-VPN does not require the operating system to support the technology. All VPN support is performed in user-space programs without need for specialized VPN drivers or other operating-system level support.

How to Configure SSL-VPN

The OxyGEN SSL-VPN feature is based on the widely used opensource OpenVPN project (<http://openvpn.net/>).

The OxyGEN broadband devices support both **Server** and **Client** modes for the SSL-VPN Tunnel. This means that we can use an OxyGEN miniOffice as server at the central site and different remote users connect to it using their PCs (with software clients) or use another OxyGEN terminal from a remote site.

Configuration of the corresponding parameters is performed using the Web configuration tool, in the **SSL VPN** sub-menu of the **Advanced** menu category (see page 128). The first task to be performed once we enter this configuration page, is to enable the service using the appropriate **Status** radio button and to choose whether the device will operate as a Server or as a Client in the SSL-VPN tunnel using the **Operation mode** drop-down menu (see Figure 11.4 in page 128).

Routed vs Bridged VPN Tunnel

An important selection for the operation of the VPN tunnel, is its type: **Routed** or **Bridged**.

In a Routed VPN tunnel, connection between the server and client is in the IP level. This practically means that they both have their separate and independent LAN subnets, with non-overlapping ranges of IP addresses and these subnets are interconnected through the SSL VPN tunnel. Forwarding of the packets between the different subnets is performed based on the destination IP address.


In a Bridged VPN tunnel, on the other hand, connection between the server and the client is performed in the Ethernet layer. This results in a simpler network topology, where the LAN subnets behind the server and the client operate like a single IP network, with the same range of IP addresses. Just as if they were connected by an Ethernet switch.

The choice between the above two types of tunnels, is not always very easy however. Routed tunnels are the most common choice, since they are more straightforward to configure and troubleshoot. The tricky part in configuring Routed tunnels is how to verify, in certain cases, that all hosts in the LANs behind the server and the client have the proper routing information in order to forward packets through the VPN tunnel. Additionally, when a Routed tunnel is used, only IP packets traverse it. This means that applications and services which rely on non-IP protocols or on IP broadcasts (e.g. Windows "Network Neighborhood"), fail to operate across the tunnel.

Bridged tunnels, on the other hand, are more difficult to handle. Bridged connections are difficult to troubleshoot and the corresponding functionality is even absent in some older versions of the PC Operating Systems. They have the advantage that by bridging the two LANs behind the server and the client they solve the problem of applications depending on IP broadcasts, however, this can also be the source of serious network degradation: since the VPN tunnels operate over a, usually, low bandwidth WAN link, the true capacity of the link can be substantially reduced by unnecessary broadcast traffic that should be limited to the high-bandwidth LAN.

Server Mode

When OxyGEN miniOffice is configured to run in Server mode, the configuration page presented in Figure 11.5 appears. When using a Routed type of tunnel, to configure your device, you must specify the **Network** and **Netmask** values for the subnet used as an IP address pool for the connected clients. Each remote client that connects to the OxyGEN SSL-VPN server will automatically acquire an IP address from this pool. If, on the other hand, you have selected a Bridged type of tunnel, no IP addressing info is required and you must only select which LAN Service is going to be bridged over the SSL VPN tunnel. The DHCP server of the selected Service is also going to be used for providing IP addressing information to any requests received over the tunnel. Once you have entered the correct values, click **Apply** in order to activate your settings.

The final step in order to finish setting up the SSL-VPN server, is to define remote users and generate the corresponding certificates. To this end click the **Manage** key under the **Users** heading. The screen presented in Figure 11.6 appears. The table at the top of the page, displays a list of the configured users. You can Revoke configured users by clicking on the corresponding  icon of **Action** column.

In order to add a new remote user, enter the username under the **Add New User** heading and click the **Save** key. The new user is added and a message window opens prompting you to save a zip file. This zip file contains the certificates corresponding to the added user. Save the file and give it using a secure method (e.g. not via e-mail) to the new remote user. The zip file contains all information needed in order to connect to the SSL-VPN server running on your OxyGEN miniOffice.



Note

There is no way of re-generating the certificates corresponding to a configured SSL VPN username. In case you want to do so, the only option is to revoke the username and then add it again.

Client Mode

When OxyGEN miniOffice is configured to run in Client mode, the following fields appear in the SSL-VPN web configuration page presented in Figure 11.4. The first task is to specify the hostname or IP address of the SSL-VPN server in the **Host/IP** field. When using a Routed type of tunnel, it is also possible to select if **NAT** (Network Address Translation) is going to be used over the tunnel. This way, once the server assigns an IP address to the client, all devices in the LAN behind the client OxyGEN miniOffice are going to appear to the server as if they have the client's tunnel IP address. If, on the other hand, you have selected a Bridged type of tunnel, you must only select which LAN Service is going to be bridged over the SSL VPN tunnel. Once you have entered the correct values, click **Apply** in order to activate your settings.

In order to finish with the secure connection to the SSL-VPN server, you will also need to install the corresponding certificate files. These certificates must be provided to you by the administrator of the SSL-VPN server. In the case of an OxyGEN miniOffice acting as the server, this is the zip file that was

saved once the username was added to the users database. The zip file containing all the appropriate certificate files can be uploaded using the **Browse** key and finally by clicking the **Upload** key.

How to Connect from a PC

In order to connect from a PC to an OxyGEN miniOffice configured to run in Server mode, you will need to install the **OpenVPN client**. To download OpenVPN, go to <http://openvpn.net/download.html>.


For Microsoft Windows 2000 or later versions, a self-installing exe file can be downloaded. It is highly recommended that you install OpenVPN version 2.1 or later, since it includes a GUI that significantly simplifies the OpenVPN operation.

After running the Windows installer, OpenVPN is ready to use. The last thing remaining before being able to connect to the OxyGEN server is to install the corresponding certificate files. To this end, you must unzip the zip file that was generated by the server upon the user creation. The correct path for an installation including the OpenVPN GUI is usually under *Program Files/OpenVPN/config/*. Place all files contained in the zip archive into this directory. The file **connect.ovpn** is the main configuration file containing all the OpenVPN connection parameters.

If your OxyGEN server is using the **Dynamic DNS** service in order to update its dynamic IP address, you are ready to connect since the connect.ovpn file already contains the corresponding hostname of the server. Otherwise, you must manually configure the connect.ovpn file and modify accordingly the line starting with the keyword **remote**. The syntax of the command is

```
remote server port
```

where **server** is the hostname or IP of the OpenVPN server and **port** is equal to 1194.

Once the connect.ovpn file contains the correct hostname or IP of the OpenVPN server, you are ready to connect. You can connect directly from the connect.ovpn file by right-clicking and selecting **Start OpenVPN** on this configuration file. Once running, you can use the **F4** key to exit. Alternatively, if you have installed the GUI, start it. The  icon appears on the taskbar. Right-click on it and select **Connect** in order to start the SSL-VPN connection towards the OxyGEN server. Once connected, the red screens on the GUI icon will turn into green and a notification will appear with the assigned IP address.

Please refer to <http://openvpn.net/> for more detailed information about OpenVPN installation and configuration for Windows-based PCs but also for other operating systems.



WARNING

If you have configured IP static routes on your OxyGEN SSL-VPN server, these routes are automatically going to be passed to every client upon successful connection.

**WARNING**

You must use the same Type (Routed or Bridged) on both ends of the SSL VPN tunnel, or otherwise the two devices will fail to connect.

F

ISDN Interfaces

ISDN Cable Pinout

The OxyGEN miniOffice is optionally equipped with one or more ISDN interfaces (BRI or PRI). These ISDN interfaces are programmable and can be configured to operate either in **External (TE)** or **Internal (NT)** mode (please refer to section **ISDN Interfaces** on page 114 for details). External mode must be selected in order to connect the interface to an ISDN Network Termination Unit (NT) and the public ISDN network. On the other hand, Internal mode must be selected in order to connect to an ISDN PBX replacing the ISDN Network Termination Unit and the public ISDN network with the broadband VoIP network.

Although programmable, you will need a different type of cable for each mode of operation. The default pinout of both BRI and PRI ISDN interfaces corresponds to NT mode operation. This means that, when a port is configured to operate in Internal (NT) mode, a straight-through cable must be used for the connection to the corresponding TE ISDN interface (see tables F.2 and F.4). On the other hand, when a port is configured to operate in External (TE) mode, an ISDN crossover cable is required (see tables F.3 and F.5).

ISDN S-bus Termination

The BRI S-Interface is a 4-wire interface, with separate Transmit and Receive pairs. It can operate in four modes:

Pin	BRI TE	BRI NT	PRI TE	PRI NT
1			Rx+	Tx+
2			Rx-	Tx-
3	Tx+	Rx+		
4	Rx+	Tx+	Tx+	Rx+
5	Rx-	Tx-	Tx-	Rx-
6	Tx-	Rx-		
7				
8				

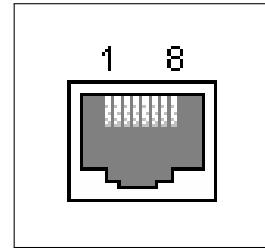


Table F.1: ISDN Interface Signals

Connector 1	Connector 2	Pair
3	3	#1
4	4	#2
5	5	#2
6	6	#1

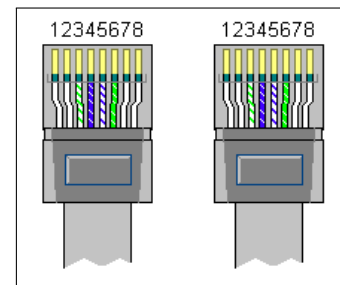


Table F.2: "Straight" ISDN BRI cable

- **Point-to-Point:** allows one TE (Terminal Equipment) device that may be up to 1 km from the NT (Network Termination) unit.
- **Short Passive Bus:** allows connection of up to 8 TE devices in parallel on the S/T bus. Each TE terminal can be connected at any point of the bus within 100 to 200 meters from the NT unit.
- **Extended Passive Bus:** allows connection to 8 TE terminals at distances of up to 500 meters from the NT terminal. All TE devices are situated at the end of the bus, with maximum distance between them 25 - 50 meters.

An ISDN S-bus must be terminated twice, once at the start and once at the end of the bus, with 100-ohm resistors. In the common case that the NT unit is at one end of the bus, the NT will have 100-ohm terminators applied, and the farthest TE terminal device will have 100-ohm terminator.

When configured to operate in NT mode, the OxyGEN miniOffice BRI interface emulates the NT unit, whereas when configured to operate in TE mode, it emulates the TE terminal. In any case, depending on the bus topology, it frequently must be terminated with 100-ohm resistance. To this end, the OxyGEN miniOffice has for each BRI interface configurable switches to apply a 100-ohm termination to the S-Interface signal pairs (**On** position) or not (**Off** position). These switches, depending on the OxyGEN miniOffice model, are located either below the BRI interfaces or at the bottom of the device.

Connector 1	Connector 2	Pair
3	4	#1
4	3	#2
5	6	#2
6	5	#1

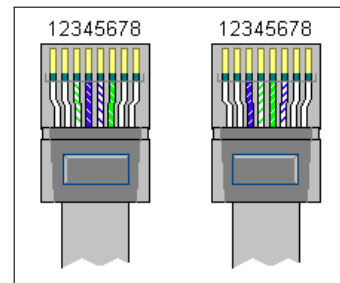


Table F.3: "Cross" ISDN BRI cable

Connector 1	Connector 2	Pair
1	1	#1
2	2	#1
4	4	#2
5	5	#2

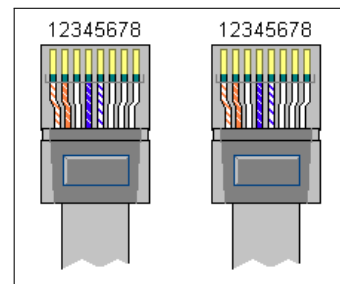


Table F.4: "Straight" ISDN PRI cable

Connector 1	Connector 2	Pair
1	4	#1
2	5	#1
4	1	#2
5	2	#2

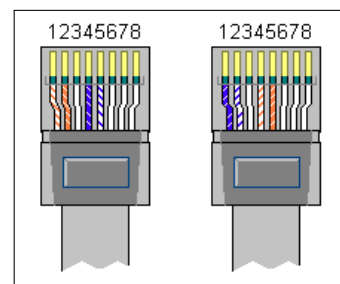


Table F.5: "Cross" ISDN PRI cable

Connector 1	Connector 1	Pair
1	5	#1
2	4	#1

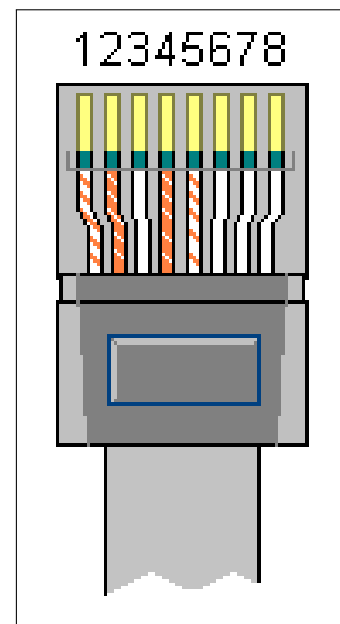


Table F.6: "Loop-back" ISDN PRI connector



Glossary

Term	Description
<i>6to4</i>	<i>It is an IPv6 transition technology. This mechanism allows IPv6 sites to communicate with each other over the IPv4 network without explicit tunnel setup. These sites communicate with native IPv6 domains via relay routers. Using 6 to 4, IPv6 hosts do not require IPv4-compatible IPv6 addresses or configured tunnels. Therefore, IPv6 gains considerable independence of the underlying wide area network and can step over many hops of IPv4 subnets.</i>
<i>802.1Q</i>	<i>The standard issued by the IEEE defining VLAN tagging in Ethernet networks. See VLAN.</i>
<i>802.11</i>	<i>A family of specifications for wireless LANs developed by the IEEE. This is an Ethernet protocol, often called Wi-Fi. The 802.11 family includes many different modulation techniques that use the same basic protocol, the most popular of which are 802.11b, 802.11g, 802.11a and the emerging 802.11n.</i>
<i>10BASE-T</i>	<i>A designation for the type of Ethernet networks with a data rate of 10 Mbps. See Ethernet.</i>
<i>100BASE-T</i>	<i>A designation for the type of Ethernet networks with a data rate of 100 Mbps. See Ethernet.</i>
<i>ACS Server</i>	<i>Auto-Configuration Server The ACS is a server responsible for the configuration of the end-user devices in a broadband network using the TR-069 protocol.</i>

ADSL	<p><i>Asymmetric Digital Subscriber Line</i></p> <p>The most commonly deployed "flavor" of DSL for home users is asymmetrical DSL. The term asymmetrical refers to its unequal data rates for downloading and uploading (the download rate is higher than the upload rate). The asymmetrical rates benefit home users because they typically download much more data from the Internet than they upload. ADSL speeds range from 1.5Mbps to 9Mbps downstream (to the subscriber) and from 16Kbps to 800Kbps upstream, depending on line distance.</p>
ADSL Lite	A lower data rate version of ADSL technology.
ADSL2/ADSL2+	Newer forms of ADSL that add new features and functionality targeted at improving performance and interoperability. Among the changes are improvements in ADSL's data rate, an increase in the distance between the DSLAM and the CPE, dynamic data rate adaptation, better resistance to noise, diagnostics, and a stand-by mode to save power. ADSL2+ rates range up to a maximum theoretical download speed of 24 Mbps.
AFTR	Address Family Transition Router element de-encapsulates the packets sent to it by the CPE and performs network address translation before sending them to the public Internet. The NAT in the AFTR uses the IPv6 address of the client in its NAT mapping table. This means that different clients can use the same private IPv4 addresses, therefore avoiding the need for allocating private IPv4 IP addresses to customers or using multiple NATs (see also Dual Stack Lite).
Analog	<p>An analog signal is a signal that has had its frequency modified in some way, such as by amplifying its strength or varying its frequency, in order to add information to the signal. The voice component in the traditional telephony (POTS) service is an analog signal.</p> <p>See Digital.</p>
Annex A	Annex of the ADSL standards defining xDSL service functioning over POTS lines.
Annex B	Annex of the ADSL standards defining xDSL service functioning over ISDN lines.
Annex L	Annex of the ADSL standards defining xDSL service with increased range of up to 7 kilometers.
Annex M	Annex of the ADSL standards defining xDSL service with upstream bandwidth increased from 1 Mbit/s to 2 Mbit/s.
ARP	Address Resolution Protocol. The protocol used for finding a host's hardware address (MAC address) when only its network layer address (IP address) is known.
APN	Access Point Name. The APN determines how the GSM endpoint communicates via the GSM network to a host site (i.e., how the carrier network passes IP traffic to the host network). An APN determines what IP addresses are assigned to the mobile station, what security methods are used, and how the GSM data network connects to the customer's network.
Appsocket / Jetdirect	An HP protocol for printing over the network.
Asymmetrical	Offering different data rates in the upstream and downstream directions, where upstream is the direction from the end-user to the network, and downstream is the direction from the network to the user.

ATM	<i>Asynchronous Transfer Mode</i> A standard for high-speed transmission of data, text, voice, and video, widely used within the Internet. ATM utilizes virtual channels instead of dedicated circuits to carry data in fixed-length cells (1 cell = 53 bytes) over a broadband network with the corresponding data rates ranging from 45 Mbps to 2.5 Gbps.
Attenuation	The reduction in amplitude and intensity of a signal as a consequence of its transmission over a medium. It is usually measured in decibels (dB) and the greater the distance from the modem to the local telephone exchange, the higher this value is likely to be.
Authentication	The process of verifying a user's identity, such as by prompting for a password.
Auto-MDIX	<i>Automatic Medium-Dependent Interface Crossover</i> A technology that automatically detects the required cable connection type (straight or crossover) and configures the connection appropriately.
Bandwidth	1. The information carrying capacity of a channel. Expressed in hertz (e.g., kHz or MHz) for analog transmission media and in bits per second (e.g. kbps, Mbps) for digital transmission media.
Beacon Interval	The duration between beacon packets. Access Points broadcast Beacons in order to synchronize wireless networks. In a "noisy" environment - one with much interference - decreasing the Beacon Interval may improve network performance. In very remote locations (with few wireless nodes) this value may be increased.
BER	<i>Bit Error Rate</i> BER is the percentage of bits received with errors divided by the total number of bits that have been received over a given time period.
Binary	The "base-two" system of numbers that uses only two digits, 0 and 1, to represent all numbers. In binary, the number 1 is written as 1, 2 as 10, 3 as 11, 4 as 100, etc. Although expressed as decimal numbers for convenience, IP addresses in actual use are binary numbers; e.g., the IP address 209.191.4.240 is 11010001.10111111.00000100.11110000 in binary. See Bit, IP Address, Network Mask.
Bit	Short for "binary digit", a bit is a number that can have two values, 0 or 1. See Binary.
Bit-swap	<i>Bit-swapping</i> is the essential adaptive hand-shaking mechanism used by DMT modems to adapt to line changes (ADSL line noise increases).
Black-list	A list of numbers that are blocked from calling the local phone lines. Whenever, a call originating from these numbers is received, it is automatically rejected.
Bps	<i>Bits per second</i>
BRAS	<i>Broadband Remote Access Server</i> The BRAS sits at the core of an ISP's network, and aggregates user sessions from the access network. Beyond aggregation it is also the injection point for policy management and IP QoS.

<i>Bridged EoA</i>	<i>Bridged EoA connections enable an ADSL CPE to bridge Ethernet frames between the LAN and the WAN just like a normal Ethernet switch, the only difference being that WAN Ethernet frames are encapsulated into AAL5 using RFC 1483/2684 bridging. See EoA.</i>
<i>Bridging</i>	<i>Passing data from your network to your ISP and vice versa using the hardware addresses of the devices at each location. Bridging contrasts with routing which can add more intelligence to data transfers by using network addresses instead. The OxyGEN miniOffice can perform both routing and bridging. See Routing.</i>
<i>Broadband</i>	<i>A telecommunications technology that can send different types of data over the same medium using multiple frequencies, which can be divided into frequency channels. This apparently leads into an increase of the effective rate of transmission, since multiple pieces of data are sent simultaneously. DSL is a broadband technology.</i>
<i>Broadcast</i>	<i>To send data to all computers on a network.</i>
<i>Broadcast SSID</i>	<i>The routinely transmission of the Wi-Fi network name (SSID) into open air by wireless access points and routers. Disabling SSID broadcasts, makes the WiFi network invisible unless a user already knows the SSID value. See SSID.</i>
<i>CAP</i>	<i>Carrier-less Amplitude/Phase In CAP modulation; incoming data modulates a single carrier that is then transmitted down a telephone line. The carrier itself is suppressed before transmission (it contains no information, and can be reconstructed at the receiver), hence the adjective "carrier-less." CAP and DMT are two modulation systems on the market for ADSL.</i>
<i>CBR</i>	<i>Constant Bit Rate A service category defined by the ATM Forum for applications and services which have very stringent cell loss, delay and delay variation requirements.</i>
<i>Cell</i>	<i>The basic unit of information transfer in the ATM network. The cell is comprised of 53 bytes, with five of the bytes making up the header field and the remaining 48 bytes forming the user information field. See ATM.</i>
<i>Certificate</i>	<i>An electronic document which incorporates a digital signature to bind together a public key with an identity. The public key is used to encrypt information and a private key is used to decrypt it.</i>
<i>Certificate Authority</i>	<i>A certificate authority issues digital certificates and once queried verifies if a certificate presented is genuine or not.</i>
<i>Channel</i>	<i>A transmission path between two points. The term channel usually refers to a one-way path, but when paths in the two directions of transmission are always associated, the term channel can refer to this two-way path.</i>
<i>CIFS</i>	<i>Common Internet File System See SMB/CIFS.</i>

Codec	<p><i>COder-DECoder</i></p> <p>A device or program capable of encoding and/or decoding a digital data stream or signal. In VoIP codec represents the encoding method used for the voice stream data.</p>
Coding Gain	<p>The increase in efficiency that a coded signal provides over an uncoded signal. Expressed in decibels (dB), it is the measure in the difference between the SNR levels of the uncoded and coded systems required to reach the same BER levels. An improvement in coding gain can provide the option of achieving the same efficiency over a link with reduced transmission power or bandwidth.</p>
CPE	<p><i>Customer Premises Equipment</i></p> <p>Any equipment provided by the customer at their premises.</p>
CRC	<p><i>Cyclic Redundancy Check</i></p> <p>CRC is a method of checking for errors in data transmitted. Using this technique, the transmitter appends an extra field to every frame of data. This field holds redundant information about the frame that helps the receiver detect errors in the frame.</p>
Crossover Ethernet Cable	<p>A type of Ethernet cable that is used to interconnect two computers by "crossing over" (reversing) their respective PIN contacts.</p>
Crosstalk	<p>Crosstalk is an undesired coupling from one telecommunication circuit or medium to another. It is caused by the electric or magnetic fields of one signal affecting a signal in an adjacent circuit. For example, in a telephone circuit, crosstalk can result in your hearing part of a voice conversation from another circuit.</p>
Decibel (dB)	<p>A measure of signal intensity. It's a logarithmic unit, so an increase in 3dB is equal to double the original intensity.</p>
DECT	<p><i>Digital Enhanced Cordless Telecommunications</i></p> <p>An ETSI standard for digital portable phones (cordless home telephones), commonly used for domestic or corporate purposes.</p>
Default Route	<p>The network route used when no other known route exists for a given IP packet's destination IP address.</p>
DHCP	<p><i>Dynamic Host Configuration Protocol</i></p> <p>DHCP automates address assignment and management. When a computer connects to the LAN, DHCP assigns it an IP address from a shared pool of IP addresses; after a specified time limit, DHCP returns the address to the pool.</p>
DHCP Lease	<p><i>Dynamic Host Configuration Protocol Lease</i></p> <p>The automatic assignment of network settings using the DHCP protocol. Each DHCP lease can be static (permanent) or dynamic. In the latter case, it is characterized by a lease time, which determines the validity period of the lease.</p>
DHCP Relay	<p><i>Dynamic Host Configuration Protocol Relay</i></p> <p>A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the addresses. Each of the OxyGEN miniOffice's interfaces can be configured as a DHCP relay. See DHCP.</p>

<i>DHCP Server</i>	<i>Dynamic Host Configuration Protocol Server</i> A DHCP server is a computer that is responsible for assigning IP addresses to the computers on a LAN. See DHCP.
<i>DHCPv6</i>	<i>DHCPv6 is the version of the Dynamic Host Configuration Protocol (DHCP) for Internet Protocol Version 6 (IPv6) networks. In addition to stateless address autoconfiguration in IPv6, DHCPv6 provides an alternate solution to assign addresses, nameservers and other configuration information in a manner similar to DHCP for IPv4. A notable case is Domain Name System servers used on a network.</i>
<i>Dial Plan</i>	<i>A set of rules defined at a voice endpoint or switch, which controls the exact action that is going to be performed when a number is dialed. The dial plan is usually closely related to the defined numbering plan, controlling the way calls belonging to different categories are going to be routed.</i>
<i>DiffServ</i>	<i>Differentiated Services</i> A QoS model for IP networks. It is based on the TOS byte of the IP header and differentiates the relative priority of each IP packet on a per-hop basis.
<i>Digital</i>	<i>Representation of data, having a form based on discrete values expressed as binary numbers (0's and 1's). The data component in DSL is a digital signal.</i> See Analog.
<i>DMT</i>	<i>Discrete Multi-Tone (DMT) multicarrier modulation uses 256 QAM modulation tones simultaneously to create the ADSL signal. DMT is the basis of ANSI Standard T1.413, and has the support of other world standards bodies. CAP and DMT are two modulation systems for ADSL.</i>
<i>DMZ Host</i>	<i>DeMilitarized Zone Host</i> A host put outside the router firewall, since all incoming connection attempts from the Internet are automatically forwarded to it.
<i>DNS</i>	<i>Domain Name System</i> The DNS maps domain names into IP addresses. DNS information is distributed hierarchically throughout the Internet among computers called DNS servers. For example, <i>www.yahoo.com</i> is the domain name associated with IP address <i>216.115.108.243</i> . When you start to access a web site, a DNS server looks up the requested domain name to find its corresponding IP address. If the DNS server cannot find the IP address, it communicates with higher-level DNS servers to determine the IP address. See Domain Name.
<i>Domain Name</i>	<i>A domain name is a user-friendly name used in place of its associated IP address. Domain names must be unique; their assignment is controlled by the Internet Corporation for Assigned Names and Numbers (ICANN). Domain names are a key element of URLs, which identify a specific file at a web site.</i> See DNS.
<i>Download</i>	<i>To transfer data in the downstream direction, i.e., from the Internet to the user.</i>
<i>Downstream</i>	<i>Downstream refers to "host to end-user" (receive, download) direction.</i>

<i>DSCP</i>	<i>Differentiated Services Code Point</i> A QoS model defined in RFC 2474 which is based on six bits of the TOS byte of the IP header. Each DSCP value specifies a particular per-hop behavior that is applied to the IP packet.
<i>DSL</i>	<i>Digital Subscriber Line</i> A technology that allows both digital data and analog voice signals to travel over existing copper telephone lines.
<i>DSL Modem</i>	<i>Short for MOdulator-DEModulator, this hardware device converts ATM cells to Ethernet packets and visa-versa in the use of DSL.</i>
<i>DSLAM</i>	<i>Digital Subscriber Line Access Multiplexer</i> A device which takes a number of ADSL subscriber lines and concentrates these to the core network of the ISP.
<i>DTMF</i>	<i>Dual-Tone MultiFrequency</i> DTMFs are a series of tones used for telephone signaling over the telephony lines. DTMFs are mainly used as a signaling system used for dialing telephone numbers using a numeric keypad (tone-dialing), instead of using the spinning dial on old telephones (pulse-dialing). They are also used, however, for other signaling applications like the passing of commands to voice-mail systems or to IVRs.
<i>Dual Stack</i>	<i>It is a transition mechanism that allows the coexistence and independence of IPv4 and IPv6 traffic flows in the same device.</i>
<i>Dual Stack Lite</i>	<i>Because of IPv4 address exhaustion, Dual-Stack Lite was designed to let an Internet service provider omit the deployment of any IPv4 address to a CPE. Instead, only global IPv6 addresses are provided. The CPE distributes private IPv4 addresses for the LAN clients, the same as a NAT device. The subnet information is arbitrarily chosen by the customer, identically to the NAT model. However, instead of performing the NAT itself, the CPE encapsulates the IPv4 packet inside an IPv6 packet. The CPE uses its global IPv6 connection to deliver the packet to the ISP's Carrier-grade NAT (CGN), which has a global IPv4 address. The IPv6 packet is decapsulated, restoring the original IPv4 packet. NAT is performed upon the IPv4 packet and is routed to the public IPv4 Internet. The CGN uniquely identifies traffic flows by recording the CPE public IPv6 address, the private IPv4 address, and TCP or UDP port number as a session.</i>
<i>Duplex</i>	<i>The mode of operation of an Ethernet link, determining if data can be transmitted in both directions at the same time or in one direction at a time.</i> <i>See Full Duplex and Half Duplex.</i>
<i>Dynamic DNS</i>	<i>A service allowing the use of domain names in conjunction with dynamic IP addresses. The service relies on notifications from the device bearing the domain name towards a server controlling the Dynamic DNS service, with the current value of the dynamic IP address.</i>

<i>Dynamic IP Addressing</i>	<i>The automatic assignment of network settings to computers or other networked devices. Network settings obtained under a dynamic IP addressing scheme are usually valid for a specific period of time and must be refreshed or reconfigured in order to continue operation of the device. This is the most common policy used by ISPs for their customers and the protocols used are either IPCP (part of PPP) or DHCP. Compare with Static IP Addressing.</i>
<i>Dynamic IP Routing</i>	<i>The use of a special IP routing protocol (e.g. RIP) for the advertisement and the application of routing entries in the routing table of a networked device. Compare with Static IP Routing.</i>
<i>DynDNS</i>	<i>See Dynamic DNS.</i>
<i>EC</i>	<i>Echo Cancellation One of the two ADSL modes of operation (the other is FDM). In the EC mode, two separate bands are allocated in the ADSL frequency spectrum: one to POTS, and one is shared by the Upstream and the Downstream. The Upstream signal overlaps the lower spectrum of the Downstream signals and this overlap is resolved by Echo Cancellation techniques. See FDM.</i>
<i>Encapsulation</i>	<i>In general, encapsulation is the inclusion of one protocol within another one so that the included protocol is not apparent. In ADSL with encapsulation we typically refer to the LLC and VCMux methods used for the transmission of IP packets over the ATM link.</i>
<i>Encryption Key</i>	<i>The key encrypts data over the WLAN, and only wireless PCs configured with a key that corresponds to the key configured on the OxyGEN miniOffice can send/receive encrypted data.</i>
<i>EoA</i>	<i>Ethernet over ATM Ethernet frames are simply encapsulated into the ATM Adaptation Layer 5 (AAL5) using RFC 1483/2684 bridging. In EoA routed connections the device obtains its own IP address on the WAN interface and performs routing between the LAN devices and the Internet, whereas in bridged mode it performs pure Ethernet bridging between the two networks. In the former case, IP address management is either static or dynamic with the use of DHCP session management.</i>
<i>Ethernet</i>	<i>The most commonly installed computer network technology, usually using twisted pair wiring. Ethernet data rates are 10 Mbps and 100 Mbps. See also 10BASE-T, 100BASE-T, Twisted Pair.</i>
<i>EUI-64</i>	<i>It is derived from the interface's 48-bit MAC address. A MAC address 00:1D:1C:06:37:64 is turned into a 64-bit EUI-64 by inserting FF:FE in the middle: 00:1D:1C:FF:FE:06:37:64. To form an IPv6 address, the meaning of the Universal/Local bit (the 7th most significant bit of the EUI-64, starting from 1) is inverted. To create an IPv6 address with the network prefix 2001:db8:1:1::/64 it yields the address 2001:db8:1:1:021d:1cff:fe06:3764 (with the underlined U/L bit inverted to a 1, because the MAC address is universally unique). Factory Defaults</i>

<i>The process of erasing the current configuration of a CPE and restoring the initial default values for all parameters.</i>	
<i>FDM</i>	<i>Frequency Division Multiplexing</i> <i>One of the two ADSL modes of operation (the other is EC). In the FDM mode, three separate bands are allocated in the ADSL frequency spectrum: one to POTS, one to Upstream and one to Downstream.</i> <i>See EC.</i>
<i>Filter</i>	<i>See Microfilter.</i>
<i>Firewall</i>	<i>A security device that controls access from the Internet to a local network.</i>
<i>Firmware</i>	<i>Firmware is the software that is embedded in a hardware device's flash memory and acts as the control center for the device's operation.</i>
<i>Frame</i>	<i>Frames, like packets, are packages of data transmitted on a network. The difference between frames and packets is that the term "frame" is traditionally used for OSI Layer-2 protocols (e.g. Ethernet frames) whereas the term "packet" refers to OSI Layer-3 protocols (e.g. IP packet).</i> <i>See Packet.</i>
<i>Frequency Band Channel</i>	<i>See Wireless Channel.</i>
<i>FTP</i>	<i>File Transfer Protocol</i> <i>A protocol (and the corresponding application) used to transfer files between computers connected to the Internet. Common uses include uploading new or updated files to a web server, and downloading files from a web server.</i>
<i>Full Duplex</i>	<i>Refers to the transmission of data in both directions of a wire (or other signal carrier) at the same time. Compare with Half Duplex.</i>
<i>Full LLU</i>	<i>Full Local Loop Unbundling</i> <i>Full LLU is a form of LLU, where the incumbent operator allows another operator to use the whole spectrum of frequencies of a local telephony loop. This way the other operator can offer over the copper twisted pair both DSL and optionally also traditional telephony (POTS) service. Compare with Shared LLU.</i> <i>See LLU.</i>
<i>FXO</i>	<i>Foreign Exchange Office</i> <i>An analog telephony port that receives the analog line with the voice service. FXO ports are used for connecting to the PSTN through the wall jack or the Phone port of an ADSL splitter. Compare with FXS.</i>
<i>FXS</i>	<i>Foreign Exchange Station</i> <i>An analog telephony port delivering the voice service to the subscriber. FXS ports are used for connecting to devices, like telephones or fax machines. Compare with FXO.</i>

<i>GAP</i>	<p><i>Generic Access Profile</i></p> <p><i>An ETSI standard (EN 300 444) that describes a set of mandatory requirements to allow any conforming DECT base-station to interoperate with any conforming DECT handset at the air interface (i.e. the radio connection) and at the level of procedures to establish, maintain and release telephone calls (Call Control). GAP also mandates procedures for registering handsets to a base-station. See DECT.</i></p>
<i>Gateway</i>	<p><i>A gateway is a computer or network device that allows or controls access to another computer or network. In many cases, the term is used to represent an IP router.</i></p>
<i>Gbps</i>	<p><i>Abbreviation of Gigabits per second, or one billion bits per second. Internet data rates are often expressed in Gbps.</i></p>
<i>GRE Tunnel</i>	<p><i>Generic Routing Encapsulation Tunnel</i></p> <p><i>A tunneling mechanisms which uses IP as the transport protocol and can be used for carrying many different passenger protocols. See Tunneling.</i></p>
<i>Half Duplex</i>	<p><i>Refers to the transmission of data in both directions of a wire (or other signal carrier), but only in one direction at any given moment. Compare with Full Duplex.</i></p>
<i>Handshake</i>	<p><i>An automated process of negotiation that dynamically sets parameters of a communications channel established between two entities before normal communication over the channel begins.</i></p>
<i>Hex</i>	<p><i>Hexadecimal</i></p> <p><i>The representation of numbers in a base-16 format. This is a very common notation in computer science, which is governed by binary encoding of data.</i></p>
<i>Host</i>	<p><i>A device (usually a computer) connected to a network.</i></p>
<i>HTTP</i>	<p><i>Hyper-Text Transfer Protocol</i></p> <p><i>HTTP is the main protocol used to transfer data from web sites so that it can be displayed by web browsers. See Web Browser, Web Site.</i></p>
<i>Hub</i>	<p><i>A hub is a place of convergence where data arrives from one or more directions and is forwarded out in all directions. It connects an Ethernet bridge/router to a group of PCs on a LAN and allows communication to pass between the networked devices. In modern networks Ethernet Hubs are replaced by Switches. See Switch.</i></p>
<i>IAD</i>	<p><i>Integrate Access Device</i></p> <p><i>A type of CPE that offers high voice and data functionality, mainly over broadband networks.</i></p>
<i>ICMP</i>	<p><i>Internet Control Message Protocol</i></p> <p><i>An Internet protocol used to report errors and other network-related information. The ping command makes use of ICMP.</i></p>

<i>IEEE</i>	<i>The Institute of Electrical and Electronics Engineers is a technical professional society that fosters the development of standards that often become national and international standards.</i>
<i>IGD-UPnP</i>	<i>Internet Gateway Device IGD is a UPnP device profile that allows UPnP aware clients to work properly from behind a NAT. See UPnP.</i>
<i>Inband</i>	<i>A method of information transmission as part of the regular data stream. For DTMFs, inband is the transmission of DTMF signals as normal audio tones.</i>
<i>Info-tainment</i>	<i>A combination of traditional elements of video, film, graphics, animation, music, audio, and text for the purposes of providing information and/or entertainment. Often characterized by hyperlinks among the various media.</i>
<i>Interface</i>	<i>An interface is, generally speaking, the common boundary (and at the same time the point of contact) between two different substances. For an ADSL CPE, the term interface is commonly used for the human-machine interaction service (e.g. Web interface). The term is also frequently used, as an alternative to port, to refer to the physical connectors on the device.</i>
<i>Interface Group</i>	<i>A group of physical ports in an Ethernet switch belonging to the same Private VLAN. See Private VLAN.</i>
<i>Interleaving</i>	<i>A form of error correction that can help reduce the number of errors on an ADSL line. It helps to stabilize a line that might otherwise suffer frequent disconnections. One drawback of interleaving is that it introduces latency to the connection.</i>
<i>Internet</i>	<i>The global collection of interconnected networks used for both private and business communications.</i>
<i>Intranet</i>	<i>A private, company-internal network that looks like part of the Internet (users access information using web browsers), but is accessible only by employees.</i>
<i>IP</i>	<i>Internet Protocol. See TCP/IP.</i>
<i>IP Address</i>	<i>Internet Protocol Address The address of a host (computer) on the Internet, consisting of four numbers, each from 0 to 255, separated by periods, e.g., 209.191.4.240. An IP address consists of a network ID that identifies the particular network the host belongs to, and a host ID uniquely identifying the host itself on that network. A network mask is used to separate the network ID and the host ID in the IP address. Because IP addresses are difficult to remember, they usually have an associated domain name that can be specified instead. See Domain Name, Network Mask.</i>
<i>IP Filtering</i>	<i>The process of selective acceptance or selective forwarding of IP packets. Selection criteria can be quite complex, including parameters like the source and/or destination IP address, TCP/UDP ports, etc.</i>

<i>IP Header</i>	<i>A special part in the beginning of each IP packet, which contains important information for the transmission of the packet, like the source and destination IP addresses.</i>
<i>IP Video</i>	<i>An encoding mechanism that is used to transmit motion video clips over an IP network (IPTV).</i>
<i>IP Voice</i>	<i>A technology that enables voice traffic to be transmitted over any network that uses IP, including LANs, WANs, and the Internet.</i>
<i>IPoA</i>	<i>Internet Protocol over ATM In IPoA connections IP packets are transported over ATM use the same type of encapsulation as EoA. What is added is an address resolution function to the ATM PVCs. This is based on the standards RFC 1483/2684 and RFC 1577/2255</i>
<i>IPP</i>	<i>Internet Printing Protocol A protocol allowing printing over IP networks. Based on the HTTP protocol, it allows users to find out about a printer's capabilities, submit print jobs, find out the status of a printer or a print job, or cancel a previously submitted job.</i>
<i>IPSec</i>	<i>Internet Protocol Security A protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream.</i>
<i>IPTV</i>	<i>See IP Video.</i>
<i>IPv6</i>	<i>Internet Protocol version 6 (IPv6) is a set of specifications from the Internet Engineering Task Force (IETF) that is an upgrade of IP version 4 (IPv4). The basics of IPv6 are similar to those of IPv4 – devices can use IPv6 as source and destination addresses to pass packets over a network, and tools like ping work for network testing as they do in IPv4, with some slight variations. However, IPv6 differs than IPv4 in that IP addresses are lengthened from 32 bits to 128 bits. This extension enables a considerable future growth of the Internet and tackles with the issue of the shortage of network addresses. IPv6 also supports auto-configuration to help correct most of the shortcomings in version 4, and it has integrated security and mobility features.</i>
<i>ISDN</i>	<i>Integrated Services Digital Network A WAN oriented data communication service provided by telephone companies. ISDN is unique among WAN services in that it provides access both to the circuit switched public switched telephone network and to packet switched services, such as X.25 and frame relay. ISDN utilizes digital local facilities and provides out-of-band signaling capabilities.</i>
<i>ISP</i>	<i>Internet Service Provider A company that provides Internet access to its customers, usually for a fee.</i>
<i>JavaScript</i>	<i>A scripting language used in many web sites for client-side web development. JavaScript is not a stand-alone language, but rather an add-on to HTML. JavaScript functions are usually embedded in or included from HTML pages and, running locally in a user's browser, can detect user actions, such as individual keystrokes.</i>
<i>Jetdirect</i>	<i>See Appsocket / Jetdirect.</i>

<i>Kbps</i>	<i>Kilobits (or thousands of bits) per second. When used in reference to transmission rates, the prefix kilo means exactly one thousand.</i>
<i>L2TP</i>	<i>Layer-2 Tunneling Protocol A tunneling protocol used to support virtual private networks (VPNs). Used for the transport of other protocols (e.g. Point-to-Point Protocol - PPP) inside UDP datagrams (default port 1701). Since, however, L2TP does not provide any encryption or confidentiality by itself, it is frequently combined with an encryption protocol (e.g. IPSec) which is passed within the tunnel to provide privacy.</i>
<i>LAN</i>	<i>Local Area Network A network limited to a small geographic area, such as a home or small office. Typical characteristics are its small geographical size (typically measured in meters), privately owned, high-speed (usually measured in megabits per second), and low error rate (typically 1 bit in a trillion). Compare with WAN.</i>
<i>Lease</i>	<i>See DHCP Lease.</i>
<i>LED</i>	<i>Light Emitting Diode An electronic light-emitting device. The indicator lights on the front of the OxyGEN miniOffice are LEDs.</i>
<i>Line Card</i>	<i>A line card is a circuit pack which sends signals from the Central Office to equipment used on the customer's premises. These signals provide the intelligence needed to make terminal equipment work.</i>
<i>LLC</i>	<i>Logical Link Control LLC is an ATM multiplexing method that allows multiple protocols to be carried over a single VC by incorporating more information in the packet header. Note that both ends of the connection must be set to the same multiplexing method. If they are not the same, the system will discard all incoming packets that do not match the configured multiplexing method. Compare with VCMux.</i>
<i>LLU</i>	<i>Local Loop Unbundling LLU is the process where the incumbent operators make their local telephone network (the copper cables that run from customers premises to the telephone exchange) available to other companies. ISPs then put their own equipment into the local telephone exchanges and that equipment links the customers directly to the ISP's servers, handling nothing else except traffic to and from the ISP. See Full LLU, Shared LLU.</i>
<i>Load Coil</i>	<i>A metallic, doughnut shaped device used on local loops to extend their reach. Load coils severely limit the bandwidth in digital communications.</i>
<i>Local Loop</i>	<i>The local loop is a 2-wire non-loaded copper wire pair with no bridged taps. The local loop is terminated at the customer's premises on a standard network interface which is supplied by either the customer or a vendor.</i>
<i>LPD</i>	<i>Line Printer Daemon A printing method most commonly used in Unix/Linux systems and TCP/IP networks.</i>

<i>MAC address</i>	<p><i>Media Access Control Address</i></p> <p><i>The permanent hardware address of a device, assigned by its manufacturer. MAC addresses are expressed as six pairs of hex characters, with each pair separated by colons. For example; XX:XX:XX:XX:XX:XX.</i></p>
<i>MAC Filtering</i>	<p><i>An access-control method based on the MAC address of the clients attempting to connect.</i></p>
<i>Mask</i>	<p><i>See Network Mask.</i></p>
<i>Mbps</i>	<p><i>Abbreviation for Megabits per second, or one million bits per second. Network data rates are often expressed in Mbps.</i></p>
<i>MER</i>	<p><i>MAC Encapsulated Routing</i></p> <p><i>This term is usually used for routed EoA connections.</i></p> <p><i>See EoA and Routed EoA.</i></p>
<i>Microfilter</i>	<p><i>A low-pass filters that allows only the voice service signal to pass. Microfilters are installed between each analog device (typically telephones, fax machines, etc) and the phone jack in order to filter out any DSL signal noise from the voice service, protecting at the same time the DSL signal from being contaminated by any signal noise from the voice service. This way, both voice and DSL signal can share the common inside wiring.</i></p>
<i>Modem</i>	<p><i>Originally short for MOulator/DEModulator, modem has become common usage. An electronic device that modulates an analog carrier, enabling digital information to be sent over analog transmission facilities.</i></p>
<i>MTU</i>	<p><i>Maximum Transmission Unit</i></p> <p><i>The largest packet size that can be transferred in one physical frame over a link.</i></p>
<i>Multicast</i>	<p><i>The delivery of IP packets to a group of destinations simultaneously. Multicast IP streams of information are characterized by special multicast IP addresses and participation of a host in a multicast group is controlled using the IGMP protocol. A typical use of multicast IP is the IPTV service, where multiple subscribers receive the same video content at the same time. Compare with Broadcast and Unicast.</i></p>
<i>Multiplexing</i>	<p><i>Transmitting several messages simultaneously on the same circuit or channel.</i></p>
<i>MWI</i>	<p><i>Message Waiting Indication</i></p> <p><i>The MWI is a telephony feature informing the user when there are unheard messages in the voice mailbox.</i></p>
<i>Narrowband</i>	<p><i>Traditionally, a channel with bandwidth less than or equal to one voice-grade line. With advances in network technology, narrowband has come to be associated with any channel operating at less than T1 (1.544Mbps) or E1 (2.048Mbps). Contrast with Broadband and Wideband.</i></p>

NAT	<p><i>Network Address Translation</i></p> <p>A service performed by many routers that translates your network's publicly known IP address into a private IP address for each computer on your LAN. Only your router and your LAN know these addresses; the outside world sees only the public IP address when talking to a computer on your LAN. This way, many computers at the LAN can share the same public IP address. Additionally, the LAN devices have one additional level of protection from the Internet, since their real IP address remains "hidden" behind the NAT service.</p>
NAT-PMP	<p><i>Network Address Translation - Port Mapping Protocol</i></p> <p>A protocol for automating the process of port forwarding in NAT gateways. Compare with IGD-UPnP.</p>
Network	<p>A group of computers that are connected together, allowing them to communicate with each other and share resources, such as software, files, etc. A network can be small, such as a LAN, or very large, such as the Internet.</p>
Network Mask	<p>A network mask is a sequence of bits applied to an IP address to separate between the network-part and the host-part of the address. Applying the network mask to the IP address leads to the network ID, with bits set to 1 meaning "select this bit" while bits set to 0 meaning "ignore this bit." For example, if the network mask 255.255.255.0 is applied to the IP address 100.10.50.1, the network ID is 100.10.50, and the host ID is 1.</p> <p>See Binary, IP Address, Subnet.</p>
NIC	<p><i>Network Interface Card</i></p> <p>An adapter card that plugs into your computer and provides the physical interface to your network cabling. For Ethernet NICs this is typically an RJ-45 connector.</p> <p>See Ethernet, RJ-45.</p>
Noise Margin	<p>See SNR Margin.</p>
Nslookup	<p>An application that queries the assigned DNS server(s) and thus allows the user to find out the IP address that corresponds to a hostname.</p>
NTP	<p><i>Network Time Protocol</i></p> <p>A complex client/server network protocol that assures accurate synchronization of computer clock times in a network of computers.</p> <p>See SNTP.</p>
Numbering Plan	<p>A scheme of rules used for the partitioning of the telephone numbers into different categories or types of subscribers.</p>
OUI	<p><i>Organizational Unique Identifier</i></p> <p>A 3-byte long unique identifier assigned by the IEEE to vendors of network-connected devices. The 3 first bytes of the MAC address of each device are the OUI of the manufacturer of the device, whereas the remaining 3 bytes are the device's unique serial number, assigned to the device by the manufacturer.</p>

<i>Outband</i>	<p>A method of information transmission out of the regular data stream as a separate asynchronous message. For DTMFs, outband is the transmission of DTMF signals as special RTP or SIP signals.</p> <p>See RFC 2833 and RFC 2976. Compare Inband.</p>
<i>Packet</i>	<p>Data transmitted on a network consists of packages called packets. Each packet contains a payload (the data), plus overhead information such as where it came from (source address) and where it should go (destination address). Packets typically refer to OSI Layer-3 protocols (e.g. IP packets), in contrast to frames, which refer to OSI Layer-2 protocols (e.g. Ethernet frame).</p> <p>See Frame.</p>
<i>Passthrough</i>	<p>Passthrough means the transparent forwarding of a protocol or a service without differentiation from the other types of traffic. Used in any kind of broadband CPE mainly for PPPoE or VPN sessions and in IADs for fax transmission. In PPPoE or VPN passthrough mode, PPPoE or VPN sessions originating from PCs on the LAN are not distinguished from ordinary data traffic, whereas in fax pass-through mode, gateways do not distinguish a fax call from an ordinary voice call.</p>
<i>Password</i>	<p>A secret sequence of characters allowing a user to authenticate himself. Username / password combinations are required in multi-user systems allowing the user to gain access to a computer system or an online service.</p>
<i>Pattern</i>	<p>Patterns are strings of digits and special characters that match one or a whole range of dialed telephony numbers. For example, 1XXX signifies 1000 through 1999. The X in 1XXX signifies a single digit, a placeholder or wildcard. In general, a pattern matches the dialed number for outgoing calls, optionally performs digit manipulation, and points to the appropriate destination for call routing.</p>
<i>PBX</i>	<p>Private Branch Exchange</p> <p>A PBX is a private telephone switch that provides voice switching (including a full set of switching features) for an office or campus. PBXs often use proprietary digital-line protocols, although some are analog-based.</p>
<i>PCR</i>	<p>Peak Cell Rate</p> <p>The rate of transmitted ATM cells per second that the source device may never exceed.</p>
<i>PIN</i>	<p>Personal Identification Number</p> <p>A secret numeric access code used to authenticate a user.</p>
<i>Ping</i>	<p>Packet Internet (or Inter-Network) Groper</p> <p>A program used to verify whether there is IP connectivity between two networked hosts.</p>
<i>POP</i>	<p>Point of Presence</p> <p>The point within a Local Access and Transport Area (LATA) at which the Interexchange Carrier (IEC) establishes itself. The POP provides the IEC with LATA access and enables the Local Exchange Carrier (LEC) to access inter-LATA services. Also, the consolidation point in a local calling area where traffic is routed to an Internet Service Provider (ISP).</p>

<i>Port (Physical)</i>	<i>A physical access point to a device such as a computer or router, through which data flows into and out of the device.</i>
<i>Port (TCP/UDP)</i>	<i>A TCP or UDP port or port number is an application-specific or process-specific 16-bit long field in the TCP or UDP Transport Layer protocols of the Internet Protocol Suite. Each packet header will specify both a source and a destination port with port values ranging from 1 to 65535. Applications implementing common services will normally listen on specific, well know port numbers (usually below 1023) which have been defined by convention for use with the given protocol (e.g. an HTTP server listens on TCP port 80). On the other hand, the client end of the connection will typically use a varying, high port number.</i>
<i>Port Forwarding</i>	<i>Port Forwarding is the technique of taking packets destined for a specific TCP or UDP port and IP address, and forwarding them to a different port and/or IP address. This is done transparently, meaning that network clients can not see that Port Forwarding is being done. They connect to a port on a device when in reality the packets are being redirected elsewhere. Port forwarding is a common functionality offered by NAT-capable routers in order to allow an outside computer to connect to a computer in a private LAN.</i>
<i>POTS</i>	<i>Plain Old Telephone Service Basic analog telephone service, present in most homes worldwide, which supports very limited special facilities.</i>
<i>PPP</i>	<i>Point-to-Point Protocol A protocol for serial data transmission that is used to carry IP (and other protocol) data between your ISP and your computer. The WAN interface on the OxyGEN miniOffice uses two forms of PPP called PPPoA and PPPoE. See PPPoA, PPPoE.</i>
<i>PPPoA</i>	<i>Point-to-Point Protocol over ATM One of the two types of PPP interfaces you can define for a Virtual Circuit (VC), the other type being PPPoE. You can define only one PPPoA interface per VC.</i>
<i>PPPoE</i>	<i>Point-to-Point Protocol over Ethernet One of the two types of PPP interfaces you can define for a Virtual Circuit (VC), the other type being PPPoA. You can define one or more PPPoE interfaces per VC or you can even run a PPPoE client on your personal computer and let it "passthrough" the OxyGEN miniOffice.</i>
<i>Private IP</i>	<i>An IP address that can NOT be accessed from the Internet and has only local significance. Private IP addresses are commonly used in home networks and intranets in general. By using these private IP addresses for local networks, the number of public IP addresses needed for devices decreases a lot. In order to enable these devices to access the Internet, the Network Address Translation service comes into play. The multiple hosts on the LAN share a few, or even one, public IP address and a NAT device performs the necessary address translations. Compare with Public IP.</i>

<i>Private VLAN</i>	<i>Private VLANs allow the separation of physical ports in an Ethernet switch to different groups. Two ports belonging to different Private VLANs cannot communicate with each other but can access another network (e.g. the broadband access) through the "uplink" port.</i>
<i>Protocol</i>	<i>A set of rules governing the transmission of data. In order for a data transmission to work, both ends of the connection have to follow the rules of the protocol.</i>
<i>PSK</i>	<i>Pre-Shared Key A shared password which was previously shared between two parties using some other secure communications channel before it needs to be used.</i>
<i>PSTN</i>	<i>Public Switched Telephone Network The circuit-switched telephone network supporting the standard analog telephony service (POTS).</i>
<i>Public IP</i>	<i>An IP address that can be accessed from the Internet. Administration of public IP addresses, so that two devices connected to the public network don't use the same IP address or that two networks don't have the same network address, is done by IANA (Internet Assigned Numbers Authority). IANA makes sure to provide unique IP network addresses to Internet Service Providers (ISPs) and keeps track of their usage. Users are assigned IP addresses by ISPs. Compare with Private IP.</i>
<i>PVC</i>	<i>Permanent Virtual Circuit A point-to-point circuit from the Customer Premise Equipment (CPE) to either their Internet Service Provider (ISP) or Enterprise Network. Over the ATM network (used in ADSL access networks) each PVC circuit is primarily identified by a VPI and VCI pair of values.</i>
<i>QoS</i>	<i>Quality of Service QoS is a scheme that involves a wide of set of standards and mechanisms for ensuring high-quality performance for critical applications.</i>
<i>RDNSS</i>	<i>Recursive DNS server option gives the possibility to assign a server which provides a recursive DNS resolution service for translating domain names into IP addresses through the Router Advertisements packets.</i>
<i>Registration</i>	<i>The periodic communication process between a SIP endpoint and a SIP proxy. Using this procedure, the endpoint notifies the proxy about its existence and authenticates itself in order to be able to place and receive calls.</i>
<i>Remote</i>	<i>In a physically separate location. For example, an employee away on travel who logs in to the company's intranet is a remote user.</i>
<i>Repeater</i>	<i>In telecommunication networks, a repeater is a device that receives a signal on an electromagnetic or optical transmission medium, amplifies the signal, and then retransmits it along the next leg of the medium. Repeaters overcome the attenuation caused by free-space electromagnetic-field divergence or cable loss. A series of repeaters make possible the extension of a signal over a distance. In addition to strengthening the signal, repeaters also remove the "noise" or unwanted aspects of the signal.</i>

RFC 2225 (previously 1577)	<p><i>"Classical IP and ARP over ATM"</i></p> <p><i>This RFC classical IP and ARP in an ATM network environment, considering only the application of ATM as a direct replacement for the "wires" and local LAN segments connecting IP end-stations and routers operating in the "classical" LAN-based paradigm.</i></p>
RFC 2364	<p><i>"PPP Over AAL5"</i></p> <p><i>This RFC describes the use of ATM Adaptation Layer 5 (AAL5) for framing PPP encapsulated packets. RFC 2364 is the basis behind PPPoA connections.</i></p>
RFC 2684 (previously 1483)	<p><i>"Multiprotocol Encapsulation over ATM Adaptation Layer"</i></p> <p><i>This RFC describes two encapsulations methods for carrying network interconnect traffic over ATM Adaptation Layer 5 (AAL5). RFC 2684 Routed encapsulation operates at the IP layer and will route only IP packets. RFC 2684 Bridged encapsulation, on the other hand, can handle non-IP packets and routes all types of packets including IPX and NetBEUI by operating at the MAC layer. RFC 2684 is the basis behind PPPoE and EoA connections.</i></p>
RFC 2833	<p><i>"RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals"</i></p> <p><i>This RFC describes how to carry DTMF signaling, other tone signals and telephony events outband in RTP packets.</i></p>
RFC 2976	<p><i>"The SIP INFO Method"</i></p> <p><i>This RFC adds the INFO method to the SIP protocol. The intent of the INFO method is to allow for the carrying of session related control information that is generated during a session. One example of such session control information is outband carrying DTMF digits generated during a SIP session.</i></p>
RFC 4193	<p><i>This document defines ULA IPv6 addresses. Among other issues, it describes a pseudo-random algorithm that routers may use in order to generate ULA addresses and is described by the following steps. 1) Obtain the current time of day in 64-bit NTP format. 2) Obtain an EUI-64 identifier from the system running this algorithm. If an EUI-64 does not exist, one can be created from a 48-bit MAC address. If an EUI-64 cannot be obtained or created, a suitably unique identifier, local to the node, should be used (e.g., system serial number). 3) Concatenate the time of day with the system-specific identifier in order to create a key. 4) Compute an SHA-1 digest on the key; the resulting value is 160 bits. 5) Use the least significant 40 bits as the Global ID. 6) Concatenate FC00::/7, the L bit set to 1, and the 40-bit Global ID to create a Local IPv6 address prefix.</i></p>
RFC 5006	<p><i>See RDNSS.</i></p>
RIP	<p><i>Routing Information Protocol</i></p> <p><i>The original dynamic IP routing protocol used for the automatic advertisement and configuration of IP routing rules.</i></p> <p><i>See Dynamic IP Routing.</i></p>
RJ-11	<p><i>Registered Jack Standard-11</i></p> <p><i>The standard plug used to connect telephones, fax machines, modems, etc. to a telephone port. It is a 6-pin connector usually containing four wires.</i></p>

<i>RJ-45</i>	<i>Registered Jack Standard-45</i> <i>The 8-pin plug used in transmitting data over cable lines. Ethernet cabling usually uses this type of connector.</i>
<i>RO Community</i>	<i>Read-Only Community</i> <i>An SNMP community string granting Read-Only access to the managed network device.</i> <i>See SNMP.</i>
<i>Routed EoA</i>	<i>Routed EoA connections enable an ADSL CPE to route IP packets between the LAN and the WAN just like a normal Ethernet router, the only difference being that WAN Ethernet frames are encapsulated into AAL5 using RFC 1483/2684 bridging.</i> <i>See EoA.</i>
<i>Routing</i>	<i>Forwarding data between your network and the Internet on the most efficient route, based on the data's destination IP address and current network conditions. A device that performs routing is called a router.</i>
<i>RW Community</i>	<i>Read-Write Community</i> <i>An SNMP community string granting Read-Write access to the managed network device.</i> <i>See SNMP.</i>
<i>Second SSID</i>	<i>The broadcasting of a second WiFi SSID, allowing the partitioning a single physical access point into two virtual ones.</i> <i>See SSID.</i>
<i>Secondary DNS</i>	<i>A DNS server that can be used if the primary DNS server is not available.</i> <i>See DNS.</i>
<i>Set-top Box</i>	<i>See STB.</i>
<i>Shared LLU</i>	<i>Shared Local Loop Unbundling</i> <i>Shared LLU is a form of LLU, where the incumbent operator retains the use of the lower POTS frequencies in a local telephony loop and makes the higher DSL frequencies available to another ISP. This way the ISP can offer the DSL service over the copper twisted pair, and at the same time the incumbent operator can still offer traditional telephony service over the same line. Compare with Full LLU.</i> <i>See LLU.</i>
<i>SIP</i>	<i>Session Initiation Protocol</i> <i>SIP is a signaling protocol, defined by IETF in RFC 3261, which is used for establishing multimedia sessions, like voice, video, and data conferencing, over IP networks.</i>
<i>SIP Domain</i>	<i>Session Initiation Protocol Domain</i> <i>A SIP domain describes a collection of SIP users and endpoints that share a common domain-part in the SIP URI addresses used.</i>
<i>SIP Info</i>	<i>See RFC 2976.</i>

<i>SIP Proxy</i>	<p><i>Session Initiation Protocol Proxy</i></p> <p>A SIP proxy is the key element of a SIP voice over IP deployment. It is the component that handles the setup of SIP calls in the network, in a similar fashion to the role PBXs and Voice Switches had in traditional telephony deployments.</p>
<i>Sixxs</i>	<p>An IPv6 tunneling mechanism (see Tunnel Brokers).</p>
<i>SMB/CIFS</i>	<p>Server Message Block / Common Internet File System</p> <p>CIFS/SMB is the network protocol used by all variants of Microsoft Windows to access and share files and printers over a network. The protocol is also supported by all recent Macintosh operating systems, and Unix/Linux variations.</p>
<i>SNMP</i>	<p>Simple Network Management Protocol</p> <p>SNMP is network management protocol widely used within TCP/IP networks. It allows a network management server to get statistics and parameter values from another computer or networking devices across the intranet or even the Internet. It also allows the modification of the parameter values. Access from the managed end-points is controlled using simple password-like character strings, called the community strings. Usually, each managed end-point has two different community strings, one with Read-Only access privileges and one with Read-Write.</p>
<i>SNR</i>	<p>Signal to Noise Ratio</p> <p>SNR is the ratio between the signal (meaningful information) and background noise power. Usually measured in decibels (dB), the higher this ratio, the better the quality of the connection link. During the initialization of ADSL modems, the SNR is measured to determine the maximum data rate that can be supported over the modem-to-DSLAM ADSL link maintaining a standard BER. At the DSLAM, the ISP configures three SNR values: a) minimum, b) target, and c) maximum SNR. The target SNR must be achieved to get ADSL sync. Power levels will be increased if SNR drops below the minimum and decreased if it's above the maximum. If the SNR drops below the minimum and the modem can't increase power levels then ADSL will drop.</p>
<i>SNR Margin</i>	<p>SNR Margin (or Noise Margin) is a measure of the difference between the current SNR value and the SNR that is required to keep a reliable service at the connection speed. If the current SNR is very close to the minimum required SNR, it is very probable to suffer intermittent connection faults, or slowdowns. A high margin, on the other hand, ensures that bursts of interference don't cause constant disconnections.</p>
<i>SNTP</i>	<p>Simple Network Time Protocol</p> <p>STNP is a simplified version of NTP, lacking some of the complicated internal algorithms that are not needed for all types of servers.</p> <p>See NTP.</p>
<i>SOHO</i>	<p>Small Office Home Office</p> <p>A category of remote "power" users exhibiting a demand for enhanced functionality over their broadband connection.</p>

<i>Speed Dial</i>	<i>An abbreviated-dialing code that can be used for fast-dialing a pre-configured destination number.</i>
<i>Splitter</i>	<i>A device that separates signal components based on their frequency content. In ADSL networks, splitters separate the high frequency (ADSL) and low frequency (POTS or ISDN) signals at both the end user and central office end points.</i>
<i>SRA</i>	<i>Seamless Rate Adaptation A feature supported by many ADSL modems and DSLAMs that involves dynamic data transfer-rate changes to accommodate for temporary noise conditions on the line thus preventing dropped connections.</i>
<i>SSH</i>	<i>Secure Shell An interactive, character-based program, used to access a remote computer. It is like an enhancement of Telnet, offering encryption of the exchanged data packets.</i>
<i>SSID</i>	<i>Service Set Identifier The name of a wireless network. SSID is an alphanumeric key set by the wireless network administrator in order to differentiate one WLAN from another. Additionally, if SSID broadcasting is disabled, it leads into an increase of the WiFi network security, since wireless devices on a WLAN must employ the same SSID in order to communicate with each other. See Broadcast SSID.</i>
<i>SSL VPN</i>	<i>Secure Sockets Layer Virtual Private Network A form of VPN that uses SSL for the encryption of the exchanged information.</i>
<i>Static IP Addressing</i>	<i>The use of statically-assigned (i.e. permanent) IP addresses to computers or other networked devices. Static IP addressing is usually performed using manual configuration methods. Compare with Dynamic IP Addressing.</i>
<i>Static IP Routing</i>	<i>The use of statically-configured (e.g. manually configured) routing entries in the routing table of a networked device. Compare with Dynamic IP Routing.</i>
<i>STB</i>	<i>Set-top Box A device that connects to a television and transforms video content supplied from an external source, into a signal appropriate to be displayed on the television screen. In broadband triple-play network, the source of the video content is a streamer which encodes the video content and sends it over IP packets. The STB receives the packets, decodes the video data and finally exports the video signal to a connected television.</i>
<i>Straight Ethernet Cable</i>	<i>The most usual type of Ethernet cable wired in a "straight" 1-to-1 configuration (contact 1 to 1, 2 to 2, etc). A straight Ethernet cable is used to connect personal computers with network switches and hubs, but is inappropriate for directly connecting two personal computers. In the latter case a crossover Ethernet cable must be used. See Crossover Ethernet Cable.</i>

<i>Subnet</i>	<i>A subnet is a portion of a network. The subnet is distinguished from the larger network by a subnet mask that selects some of the computers of the network and excludes all others. The subnet's computers remain physically connected to the rest of the parent network, but they are treated as though they were on a separate network. See Network Mask.</i>
<i>Subnet mask</i>	<i>A mask that defines a subnet. See Network Mask.</i>
<i>Switch</i>	<i>A device that can establish communication channels between end-users. A voice circuit switch provides dedicated voice paths to communicating entities; a store and forward switch shares paths on a statistically multiplexed basis. An Ethernet switch performs the same operation for Ethernet connections.</i>
<i>Synchronization</i>	<i>The state after the initial negotiation period (training), when two modems have succeeded in finding a common set of parameters for the establishment of a communications channel and normal communication over the channel is possible. Compare with Training.</i>
<i>Syslog</i>	<i>A protocol and the associated service for the control of logging information and the optional transmission of it over the network.</i>
<i>T.38</i>	<i>A standard defined by the ITU, for the reliable outband transport of fax calls over IP networks. Compare with Inband.</i>
<i>TCP</i>	<i>See TCP/IP.</i>
<i>TCP/IP</i>	<i>Transmission Control Protocol/Internet Protocol The basic protocols used on the Internet. TCP is responsible for dividing data up into packets for delivery and reassembling them at the destination, while IP is responsible for delivering the packets from source to destination. When TCP and IP are bundled with higher-level applications such as HTTP, FTP, Telnet, etc., TCP/IP refers to this whole suite of protocols.</i>
<i>Telnet</i>	<i>An interactive, character-based program used to access a remote computer. While HTTP (the web protocol) and FTP only allow you to download files from a remote computer, Telnet allows you to log into and use a computer from a remote location. Compare with SSH.</i>
<i>TFTP</i>	<i>Trivial File Transfer Protocol A protocol for file transfers, TFTP is easier to use than File Transfer Protocol (FTP) but not as capable or secure.</i>
<i>TKIP</i>	<i>Temporal Key Integrity Protocol TKIP provides WPA with a data encryption function. It ensures that a unique master key is generated for each packet, supports message integrity and sequencing rules and supports re-keying mechanisms.</i>

<i>TOS</i>	<p><i>Type of Service</i></p> <p><i>A 1-byte long field in the header of IP packets for the indication of the desired QoS level. Initially, only 3 bits were used out of the whole byte for the traffic management purposes (IP Precedence bits) whereas modern models take 6 bits into account (DSCP).</i></p> <p><i>See DSCP.</i></p>
<i>TR-069</i>	<p><i>A technical specification by the DSL Forum for the remote management of CPEs by a central ACS server.</i></p> <p><i>See ACS Server.</i></p>
<i>Traceroute</i>	<p><i>A program, which (like Ping) can be used to verify whether there is IP connectivity between two networked hosts, but also reveals all the IP routing hops in-between.</i></p>
<i>Traffic Class</i>	<p><i>A traffic class is a collection of QoS mechanisms and parameters aiming to provide a defined level of service to IP packets in the traffic class.</i></p>
<i>Training</i>	<p><i>The initial negotiation period, when two modems have succeeded contacting each other and are negotiating in finding a common set of parameters (e.g. symbol, data rate) for the establishment of a communications channel. Compare with Synchronization.</i></p>
<i>Triggers</i>	<p><i>Triggers are used to deal with application protocols that create separate sessions. Some applications, such as NetMeeting, open secondary connections during normal operations, for example, a connection to a server is established using one port, but data transfers are performed on a separate connection. A trigger tells the device to expect these secondary sessions and how to handle them. Once you set a trigger, the embedded IP address of each incoming packet is replaced by the correct host address so that NAT can translate packets to the correct destination. You can specify whether you want to carry out address replacement, and if so, whether to replace addresses on TCP packets only, UDP packets only, or both.</i></p>
<i>Triple-Play</i>	<p><i>A term usually used for the description of broadband networks supporting Data, Voice and Video services at the same time.</i></p>
<i>Tunnel Brokers</i>	<p><i>In networking, tunnelling implies enabling new networking functions while still preserving the underlying network as is. There may be several reasons why a network needs tunnelling, for example, to carry a payload over an incompatible delivery network. IPv6 tunneling enables IPv6 hosts and routers to connect with other IPv6 hosts and routers over the existing IPv4 Internet. The main purpose of IPv6 tunneling is to deploy IPv6 as well as maintain compatibility with large existing base of IPv4 hosts and routers. IPv6 tunneling encapsulates IPv6 datagrams within IPv4 packets. The encapsulated packets travel across an IPv4 Internet until they reach their destination host or router. The IPv6-aware host or router decapsulates the IPv6 datagrams, forwarding them as needed.</i></p>

<i>Tunneling</i>	<i>Tunneling provides a mechanism to transport packets of one protocol kind within another protocol. The protocol that is carried is called the passenger protocol, and the protocol that is used for carrying the passenger protocol is called the transport protocol. The tunnels behave as virtual point-to-point links that have two endpoints identified by the tunnel source and tunnel destination addresses at each endpoint.</i>
<i>Twisted Pair</i>	<i>The ordinary copper telephone wiring used by telephone companies. It contains one or more wire pairs twisted together to reduce inductance and noise. Each telephone line uses one pair. In homes, it is most often installed with two pairs. For Ethernet LANs, a higher grade called Category 3 (CAT 3) is used for 10BASE-T networks, and an even higher grade called Category 5 (CAT 5) is used for 100BASE-T networks. See 10BASE-T, 100BASE-T, Ethernet.</i>
<i>UBR</i>	<i>Unspecified Bit Rate A service category defined by the ATM Forum primarily for data applications. This service has no guaranteed quality of service associated with it. However, the QOS for the UBR service is engineered to meet certain (target) objectives.</i>
<i>UDP</i>	<i>User Datagram Protocol Along with TCP and IP, the three protocols that mainly govern the operation of the Internet. UDP, like TCP, is responsible for dividing data up into packets for delivery and reassembling them at the destination. However, it is considered an unreliable transmission protocol, since (unlike TCP) it does not guarantee successful reception of the data through the deployment of a retransmission mechanism. See TCP/IP.</i>
<i>ULA</i>	<i>A unique local address (ULA) is an IPv6 address in the block fc00::/7, defined in RFC 4193. It is the IPv6 equivalent of the IPv4 private address. Unique local addresses are available for use in private networks, e.g. inside a single site or organization and are not routable in the global IPv6 Internet.</i>
<i>Unicast</i>	<i>The point-to-point transmission of IP packets. Contrary to broadcasting and multicasting, a unicast IP stream is sent to a single final destination. Compare with Broadcast and Multicast.</i>
<i>Unnumbered Interfaces</i>	<i>An unnumbered interface is an IP interface that does not have a local subnet associated with it. Instead, it uses a router-id that serves as the source and destination address of packets sent to and from the router. Unlike the IP address of a normal interface, the router-id of an unnumbered interface is allowed to be the same as the IP address of another interface. For example, the WAN unnumbered interface of your device uses the same IP address of the LAN interface (192.168.1.254). The unnumbered interface is temporary --- PPP or DHCP will assign a "real" IP address automatically.</i>

UPnP	<p><i>Universal Plug and Play</i></p> <p><i>UPnP is a networking architecture that provides peer-to-peer network connectivity among networking equipment, software and peripherals, particularly within the home. UPnP builds on Internet standards and technologies, such as TCP/IP, HTTP, and XML. It defines and publishes UPnP device control protocols, like the Internet Gateway Device (IGD) used for NAT traversal. One inherent disadvantage of UPnP is that it lacks authentication mechanisms, and usually it is assumed that local systems and their users are completely trustworthy.</i></p>
Upstream	<i>The direction of data transmission from the user to the Internet.</i>
URL	<p><i>Uniform Resource Locator</i></p> <p><i>An address that specifies the location of a file or a service on the Internet (e.g. http://www.gennetsa.com).</i></p>
USB	<p><i>Universal Serial Bus</i></p> <p><i>A connection port on a computer that is universally compatible with many types of devices, such as, printers, speakers, mouse, etc. USB 1.1 can support speeds of up to 12Mbps whereas the newer USB 2.0 can support speeds of up to 480Mbps.</i></p>
USB Device Port	<i>A term used for referring to Type-B Female USB ports. Peripheral devices (e.g. printers, USB sticks, etc) usually have a USB device port in order to connect to PCs.</i>
USB Host Port	<i>A term used for referring to Type-A Female USB ports. A USB host port is used for connecting peripheral devices (e.g. printers, USB sticks, etc). PCs are equipped with multiple USB host ports.</i>
Username	<i>A sequence of characters used to uniquely identify a user. Usernames, often in combination with passwords, are required in multi-user systems allowing the user to gain access to a computer system or an online service.</i>
V.90 / V.92	<i>International standards for 56K data communications.</i>
VBR	<p><i>Variable Bit Rate</i></p> <p><i>A service category defined by the ATM Forum for applications and services which have less stringent cell loss, delay and delay variation requirements than the applications which use the CBR service.</i></p>
VC	<p><i>Virtual Circuit</i></p> <p><i>A point-to-point circuit. Depending on whether they remain constant over time or are dynamically set-up, VCs in ATM networks are divided into two categories: Permanent (PVC) and Switched (SVC), with the former being the usual case for the CPE-to-DSLAM connection in ADSL deployments.</i></p> <p><i>See PVC.</i></p>
VCI	<p><i>Virtual Circuit Identifier</i></p> <p><i>Together with the Virtual Path Identifier (VPI), the VCI uniquely identifies a PVC. Your ISP will tell you the VCI for each PVC they provide.</i></p> <p><i>See PVC.</i></p>

VCMux	<p><i>Virtual Circuit Multiplexing</i></p> <p>VCMux is an ATM multiplexing method that allows only one protocol to be carried per PVC. Note that both ends of the connection must be set to the same multiplexing method. If they are not the same, the system will discard all incoming packets that do not match the configured multiplexing method. Compare with LLC.</p>
VDSL	<p><i>Very High Bit-rate Digital Subscriber Line</i></p> <p>A DSL technology variation proposed for shorter local loops, which provides 13 - 53Mbps downstream and 1.5 - 2.3Mbps upstream.</p>
VLAN	<p><i>Virtual Local Access Network</i></p> <p>A group of devices on different physical LAN segments which can communicate with each other as if they were all on the same physical LAN segment. For Ethernet networks, VLANs are defined using the 802.1Q standard.</p>
VLAN ID	<p>A 12-bit field specifying the 802.1Q VLAN to which an Ethernet frame belongs. Valid values are 1 up to 4094. VLAN ID 1 is often reserved for management purposes.</p> <p>See VLAN.</p>
VoIP	See IP Voice.
VPI	<p><i>Virtual Path Identifier</i></p> <p>Together with the Virtual Circuit Identifier (VCI), the VPI uniquely identifies a VC. Your ISP will tell you the VPI for each VC they provide.</p> <p>See VC.</p>
VPN	<p><i>Virtual Private Network</i></p> <p>A VPN is a private network that makes use of a public network (such as the Internet), while maintaining security and privacy through encryption and security procedures. Common VPN protocols are IPSec, L2TP and SSL.</p>
WAN	<p><i>Wide Area Network</i></p> <p>Any network spread over a large geographical area, such as a country or continent. With respect to the OxyGEN miniOffice, WAN refers to the Internet. Compare with LAN.</p>
Web Browser	<p>A software program that uses Hyper-Text Transfer Protocol (HTTP) to download information from (and upload to) web sites, and displays the information, which may consist of text, graphic images, audio, or video, to the user. Web browsers use Hyper-Text Transfer Protocol (HTTP). Popular web browsers include Mozilla Firefox, Microsoft Internet Explorer, Google Chrome and Apple Safari.</p> <p>See HTTP, Web Site, WWW.</p>
Web Filtering	<p>The process of selective acceptance in downloading of Web pages. Selection criteria can be quite complex, ranging from the existence of certain keywords in the requested URL to the examination of the exact contents of the Web page.</p>

Web Page	<p>A web site file typically containing text, graphics and hyperlinks (cross-references) to the other pages on that web site, as well as to pages on other web sites. When a user accesses a web site, the first page that is displayed is called the home page.</p> <p>See Web Site.</p>
Web Site	<p>A computer on the Internet that distributes information to (and gets information from) remote users through web browsers using the HTTP protocol. A web site typically consists of web pages that contain text, graphics, and hyperlinks.</p> <p>See HTTP, Web Page.</p>
WEP	<p>Wired Equivalent Privacy</p> <p>WEP encrypts data over WLANs. Data is encrypted into blocks of either 64 bits length or 128 bits length. The encrypted data can only be sent and received by users with access to a private network key. Each PC on your wireless network must be manually configured with the same key as your device in order to allow wireless encrypted data transmissions. Eavesdroppers cannot access your network if they do not know your private key. WEP is considered to be a low security option.</p>
Wideband	<p>Variously defined. The term wideband is often used to describe a digital transmission facility operating at speeds in excess of 1.544Mbps. It is also used in the analog domain to describe a channel with a large bandwidth (e.g., "the CATV industry offers a collection of wideband channels")</p>
WiFi	<p>Wireless Fidelity</p> <p>A term usually used for 802.11 based Wireless LANs.</p> <p>See Wireless LAN.</p>
Wireless	<p>Wireless is a term used to describe telecommunications in which electromagnetic waves (rather than some form of wire) carry the signal over part or the entire communication path.</p> <p>See Wireless LAN.</p>
Wireless Channel	<p>The 802.11 WiFi standards divide the available frequency bands into channels, with a certain degree of overlap between neighboring channels. Not every wireless channel is available for use in every part of the world, since availability of channels is regulated by each country.</p>
Wireless LAN	<p>Wireless Local Area Network</p> <p>A WLAN is a type of LAN in which users connect through a wireless (radio) connection. The IEEE 802.11 standard specifies the technologies for wireless LANs.</p>
WLAN	<p>See Wireless LAN.</p>

WPA / WPA2	<p><i>Wi-Fi Protected Access</i></p> <p><i>WPA is an initiative by the IEEE and Wi-Fi Alliance to address the security limitations of WEP. WPA provides a stronger data encryption method, called Temporal Key Integrity Protocol (TKIP). It runs in a special, easy-to-set-up home mode called Pre-Shared Key (PSK) that allows you to manually enter a pass phrase on all the devices in your wireless network. WPA data encryption is based on a WPA master key. The master key is derived from the pass phrase and the network name (SSID) of the device.</i></p>
WWW	<p><i>World Wide Web</i></p> <p><i>Also called (the) Web. Collective term for all web sites anywhere in the world that can be accessed via the Internet.</i></p>
xDSL	<p><i>Refers to the family of digital subscriber line technologies, such as ADSL, HDSL, IDSL, RADSL, SDSL and VDSL.</i></p>