

Oxygen Multiservice Gateway

VDSL2/ADSL2+ Multiservice Access Device

User's Guide

*v3.3.0ote
September 2015*



Product and Publication Details

<i>Product Family:</i>	Broadband Access Terminals
<i>Product Name:</i>	Oxygen Multiservice Gateway
<i>Product Type:</i>	SOHO
<i>Publication Type:</i>	User's Guide
<i>Publication Version:</i>	v3.3.0ote
<i>Publication Date:</i>	September 2015
<i>Language:</i>	English

About This Guide

This guide is designed to assist users in using the Oxygen Multiservice Gateway. Information in this document has been carefully checked for accuracy; however, Oxygen Broadband 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 may be specific information regarding unique functionalities of the offered services by your ISP (e.g. a service activation procedure).

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

Declaration of Conformity

Hereby, Oxygen Broadband s.a. declares that this Oxygen Multiservice Gateway 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 Multiservice Gateway. 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

© Oxygen Broadband s.a., 2015. 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 Oxygen Broadband s.a.

All copyright, intellectual and industrial rights in this document and in the technical knowledge it contains are owned by Oxygen Broadband 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 Oxygen Broadband's website: <http://www.oxygenbroadband.com/downloads/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	26
	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 analog or DECT phone	30
	Step 4. Attach the Power Connector	31
	Step 5. 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	50
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	57
Connections	59
Connection	59
ATM Options	60
802.1Q VLAN	60
Modem Options	61
PPP Options	61
IP Options	62
IPv4 Options	63
IPv6 Options	63
IP Routing	64
DSL Line	65
3G/4G Modem	67
Info	68
7 Network Menu	71
Interface Groups	72
VLAN	74
Ethernet	75
Addresses	76
IPv6 Addresses	76
DHCP	78
Static DHCP Options	78
LAN IPv6 Addresses	79
DNS Settings	81
Host Aliases	81
Forced Lookups	82
Static Routes	84

Dynamic Routing	86
Wake On LAN	87
Public IPs	88
8 Wireless Menu	89
Configuration	90
Security	91
WEP Encryption	91
WPA / WPA2 Encryption	92
Wi-Fi Protected Setup (WPS)	92
MAC Filtering	94
Multiple SSIDs	95
Encryption	95
9 Firewall Menu	97
Configuration	98
WAN Connection	98
LAN Interface Groups	99
Port Forward	100
UPnP / NAT-PMP	102
IP Filters	103
Web Filters	106
DMZ Filters	107
Address Mapping	109
10 Voice Menu	111
Phone Lines	112
Restrictions	114
Speed Dials	116
Black List	117
11 Advanced Menu	119
Dynamic DNS	120
Date and Time	121
SSL VPN	122
Client Mode	122
Server Mode	123
GRE Tunnel	126
L2TP Tunnel	127
Client Mode	127
Server Mode	128
IPSec Tunnel	130
QoS Policy	132

Policy Classes	132
IP DSCP Marking	134
VLAN CoS Marking	134
QoS parameters	134
File Sharing	135
Printing	136
12 System Menu	137
Green Operation	138
SNMP	139
Syslog	140
Backup / Restore	141
Backup Configuration	141
Restore Configuration	142
Firmware Upgrade	143
Remote Admin	145
Change Password	146
Device Restart	147
13 Status Menu	149
About	151
System Log	152
Interfaces	154
DSL Line	155
Wireless	156
Phone Lines	157
Call Details	159
ISDN Interfaces	160
Firewall	161
Clients	162
VPN Service	163
Diagnostics	164
Healthcheck	165
Net Statistics	166
IP Network	168
14 Troubleshooting	171
Testing your Setup	172
Troubleshooting Suggestions	173
Diagnosing Problem using IP Utilities	175
Ping	175
nslookup	175

A	Configuring the Internet Settings	177
	Configuring Ethernet PCs	177
	Configuring Wireless PCs	178
	Positioning the Wireless PCs	178
	Wireless PC Cards and Drivers	178
	Configuring PC Access to your Wireless Device	178
B	IP Addresses, Network Masks, and Subnets	181
	IP Addresses	181
	Structure of an IP Address	181
	Network Classes	182
	Subnet Masks	183
C	Voice Supplementary Services	185
	Call Hold	185
	Call Waiting	185
	Call Transfer	185
	3-Party Call	185
D	Network Printing	189
	AppSocket / JetDirect	189
	Internet Printing Protocol (IPP)	190
E	WPA/WPA2 support	193
	Microsoft Windows and WPA/WPA2 support	193
F	Creating an SSL VPN	195
	General Info	195
	How to Configure SSL-VPN	195
	Routed vs Bridged VPN Tunnel	196
	Server Mode	197
	Client Mode	197
	PC Client	198
	Android Device Client	199
G	ISDN Interfaces	203
	ISDN Cable Pinout	203
	ISDN S-bus Termination	203
	Termination Switches	204
H	Glossary	207
	Glossary	207

List of Figures

2.1	Oxygen Multiservice Gateway 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	Home - Initial system view	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 - Internet Quick Configuration	56
6.2	List of ATM PVCs	57
6.3	Config ATM PVC	58
6.4	List of Connections	59
6.5	New Connection - PPPoE	60
6.6	IPv6 Options	63
6.7	DSL Line Parameters	65
6.8	3G/4G Modem	67
6.9	Show Modem Parameters	69
7.1	Interface Groups	73
7.2	VLAN	74
7.3	Ethernet Ports	75
7.4	LAN Addresses	76
7.5	IPv6 Addresses	77
7.6	DHCP Server Configuration	78
7.7	LAN IPv6 Addresses	80
7.8	DNS Settings Configuration	81
7.9	Host Aliases	82
7.10	Forced Lookups	83
7.11	Static Routing	84
7.12	Static Route Edit	84

7.13	Dynamic Routing	86
7.14	Host wake on LAN	87
7.15	Public IP Addresses	88
8.1	Wireless Settings	90
8.2	Wireless Security - WEP	91
8.3	Wireless Security - WPA/WPA2	92
8.4	Wireless MAC Address Filter	94
8.5	Multiple Wireless SSIDs	95
8.6	Wireless Security - Multiple SSIDs	96
9.1	Firewall Configuration	98
9.2	Port Forwarding	100
9.3	New Port Forwarding	101
9.4	UPnP Configuration	102
9.5	IP Filtering	103
9.6	New IP Filter	104
9.7	Web Filtering	106
9.8	Internet-to-DMZ Protocol Filters	108
9.9	NAT Static Address Mapping	109
10.1	Phone Lines	112
10.2	Phone Lines	113
10.3	Call Restrictions	114
10.4	Speed Dials	116
10.5	Black List Numbers	117
11.1	Dynamic DNS	120
11.2	SNTP Client	121
11.3	SSL VPN - Client Mode	122
11.4	SSL VPN - Server Mode	124
11.5	SSL VPN Users	125
11.6	GRE Tunnel	126
11.7	L2TP VPN Tunnel - Client Mode	127
11.8	L2TP/IPSec Tunnel - Server Mode	128
11.9	L2TP PPP Users	129
11.10	IPSec Tunnel	130
11.11	List of QoS Classes	132
11.12	New QoS Priority Class	133
11.13	File Sharing Service	135
11.14	USB Printer Support	136
12.1	Green Operation	138

12.2	SNMP Configuration	139
12.3	Syslog Configuration	140
12.4	Configuration Backup/Restore	141
12.5	Backup Configuration	141
12.6	Restore Configuration	142
12.7	Local Firmware Upgrade	143
12.8	Automatic Firmware Upgrade	144
12.9	Remote Administration	145
12.10	Password Configuration	146
12.11	Device Reboot	147
12.12	Reboot Status	147
13.1	Device Status	151
13.2	System Log	152
13.3	System Log Notification	153
13.4	Ethernet Port Status	154
13.5	DSL Line Information	155
13.6	Wireless Network Information	156
13.7	Voice Calls and Services	157
13.8	Service Codes	158
13.9	Call Records	159
13.10	ISDN Interfaces	160
13.11	Current Firewall Status	161
13.12	Connected Clients	162
13.13	Clients Info	162
13.14	VPN Service Information	163
13.15	Troubleshooting	164
13.16	Healthcheck Information	165
13.17	Network Statistics	166
13.18	Detailed Network Statistics	167
13.19	IP Interface Statistics	167
13.20	IP Network Information	168
13.21	Detailed IP Connection List	169
14.1	Using the Ping Utility	175
14.2	Using the nslookup Utility	176
F.1	Installation in Play	199
F.2	Creation of Profile	199
F.3	Importing File	200
F.4	File Validation	200
F.5	New VPN Profile	200
F.6	Editing VPN Profile	200

F.7	Setting Server Address	200
F.8	Connection Log	200
F.9	Connection Status	200

1

Introduction

Congratulations on becoming the owner of the Oxygen Multiservice Gateway. You will now be able to access the Internet using your high-speed broadband connection supporting data, voice and video services.

This User's Guide will show you how to connect your Oxygen Multiservice Gateway, 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 Multiservice Gateway 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:

- Internal VDSL2/ADSL2+ modem for high-speed Internet access
- 4-port 10/100Base-T Ethernet router to provide Internet connectivity to all computers on your LAN
- 802.11b/g/n WiFi router to provide Internet connectivity to all wireless devices on your LAN (*WiFi-enabled devices only*)
- Voice over IP (VoIP) functionality with analog and/or **ISDN BRI** voice interfaces (*number and type of ports depend on model*)
- USB host interface for connecting external storage devices (USB sticks, hard disks), USB printers and USB 3G/4G dongles (*optional feature*)
- 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 broadband access performance monitoring
- User-friendly configuration program accessed via a web browser
- Automatic configuration service
- Embedded battery for uninterrupted operation (*optional feature*)

Device Requirements

In order to use the Oxygen Multiservice Gateway, you must have the following:

- Broadband service up and running on your 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 (10/100/1000Base-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 Multiservice Gateway.

Using this Document

Notational Conventions

- Acronyms are defined the first time they appear in the text and also in the glossary (**Appendix H** on page 207).
- For brevity, the Oxygen Multiservice Gateway is frequently referred to as "Oxygen" or "CPE" 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 Oxygen Broadband (<http://www.oxygenbroadband.com>) in order to get the most up-to-date information and support for your Oxygen Multiservice Gateway.

2

Getting to Know the Device

Parts Check

Your Oxygen Multiservice Gateway package should arrive containing the following:

- Oxygen Multiservice Gateway
- Vertical stand accessory
- Ethernet cable (Yellow, RJ-45)
- Three standard phone/DSL line cables (Black, RJ-11)
- Power adapter and power cord
- Quick Installation Guide booklet
- DSL filter
- DSL splitter



WARNING

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



Figure 2.1: Oxygen Multiservice Gateway Package Contents

Front Panel

The front panel contains a series of lights, called Light Emitting Diodes (LEDs), that indicate the status of the unit.

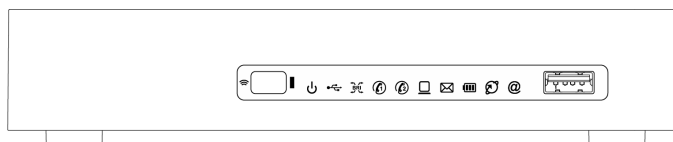


Figure 2.2: Front Panel and LEDs

Examining the front panel from left to right, we can find the LEDs listed in table 2.2. It also contains the WiFi On/Off and WPS activation button (WiFi enabled devices only). Finally it contains a USB host interface for connecting external storage devices (USB sticks, hard disks), USB printers and USB 3G/4G dongles (*optional feature*)

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.

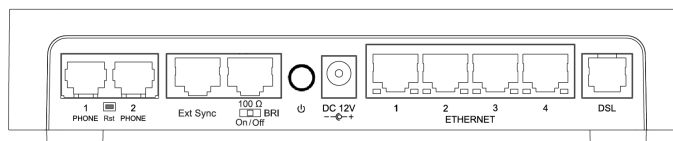


Figure 2.3: Rear Panel Connections

Examining the rear panel from left to right, we can find the ports listed in table 2.3.









Label	Color	Function
Wireless 	Blue	On: Wireless service enabled. <i>(WiFi-enabled devices only)</i>
Power 	Blue/ Purple	Blue: Normal operation. Purple: During boot sequence.
USB 	Blue	On: Active USB port (device detected). <i>(optional feature)</i>
Phone  (1-2)	Blue	On: Voice service successfully initialized for the corresponding phone line. Blinking: Phone in the "Off-Hook" state. <i>(voice-enabled devices only)</i>
ETHERNET 	Blue	On: At least one Ethernet port is active (link detected). Blinking: Traffic on the Ethernet ports.
MWI	Blue	Blinking: New voice message. <i>(optional feature)</i>
Battery 	Blue	On: The device operates on the internal battery. <i>(optional feature)</i>
DSL 	Blue	On: Showtime (successfully connected to the DSL network). Slow Blinking: Handshake (idle - no line detected). Fast Blinking: Training (connection attempt).
Internet 	Blue/ Red	Blue: Successfully connected to the Internet. Blue Blinking: Trying to connect. Red: Connection error (e.g. invalid Username / Password). Blue/ Redcycle: Active 3G/4G-backup connection <i>(optional feature)</i>

Table 2.1: Front panel LEDs



Label	Function
PHONE 1-2	Analog ports for connecting the Telephone devices. (voice-enabled devices only)  WARNING: If you are going to use only one analog phone, connect it to port 1 .
Rst	Reset button. Pressing this pin button for more than 5 seconds restores the factory default configuration on your device.
Ext Sync	ISDN BRI synchronization port. Used for attaching the optional synchronization accessory (not included in the device package), in order to connect and synchronize with another CPE NT device or an ISDN NTU terminal.
BRI	ISDN BRI interface. Used for connecting to your private ISDN PBX, ISDN terminal or to ISDN NT. This port is configurable and operates 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 G on page 203 for details about the pinout of both cables.
I / O	The main switch of the device. Please make sure it is in the "Off" position before starting the installation procedure.
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.
ETHERNET 1-4	Interfaces used to connect the device 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).
DSL	Connects the device to a telephone port in the wall of your home/office or to a splitter for DSL communication.

Table 2.2: Rear panel ports

3

Connecting your Device

This chapter provides basic instructions for connecting the Oxygen Multiservice Gateway to a personal computer or LAN and to the Internet. It is assumed that you have already established a broadband 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 177
- **Configuring Wireless PCs** on page 178 (*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 Multiservice Gateway.

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.

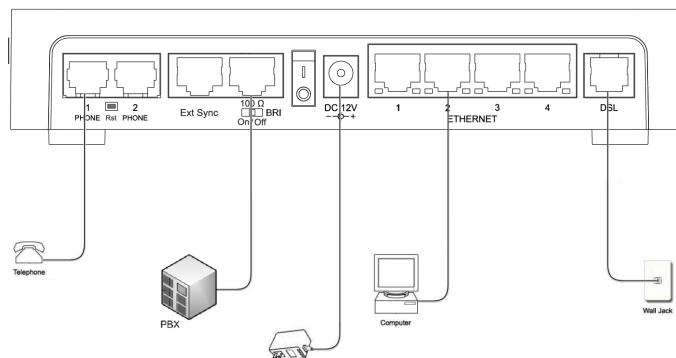


Figure 3.1: Overview of Hardware Connections

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.

Step 2. Connect the Ethernet Cable



Note

If you plan to use a Wireless connection between your PC and the Oxygen Multiservice Gateway (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 analog or DECT phone

Connect your analog telephone-set, DECT base-station, or fax machine to the port(s) labeled **PHONE**.

**WARNING**

*You will not be able to make or receive telephone calls until your Voice-over-IP (VoIP) service has properly been configured. Please refer to Chapter **Voice Menu** on page 111 for more information.*

Step 4. 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 Multiservice Gateway.

**Note**

*During the boot-sequence of the Oxygen Multiservice Gateway, the **Power** LED is Purple (either solid or blinking). The device is ready for operation when the LED is solid Blue.*

Step 5. Configure your PC

You may now have to configure the Internet properties on your Ethernet PC. See **Configuring Ethernet PCs** on page 177, if using a wired Ethernet connection, or **Configuring Wireless PCs** on page 178, if planning to use a wireless one (*WiFi-enabled devices only*).

Next Step

After setting up the Oxygen Multiservice Gateway 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 171), 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 Multiservice Gateway 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 or through WiFi (WiFi enabled devices only).
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://192.168.1.1> in the web address (or location) box, and press **[Enter]** on your keyboard.
4. An access control screen appears. Enter the appropriate username and password.



Note

The default username and password combination is printed on the label to the bottom of your Oxygen Multiservice Gateway. Use these credentials to login to the web interface.

Authentication Required

The server oxygen.lan:80 at OxyGEN Web Interface requires a username and password.

User Name:

Password:

Figure 4.1: Web Configuration Login

5. After successful login, the **Home** page opens, displaying the system view page with an overview of the device.

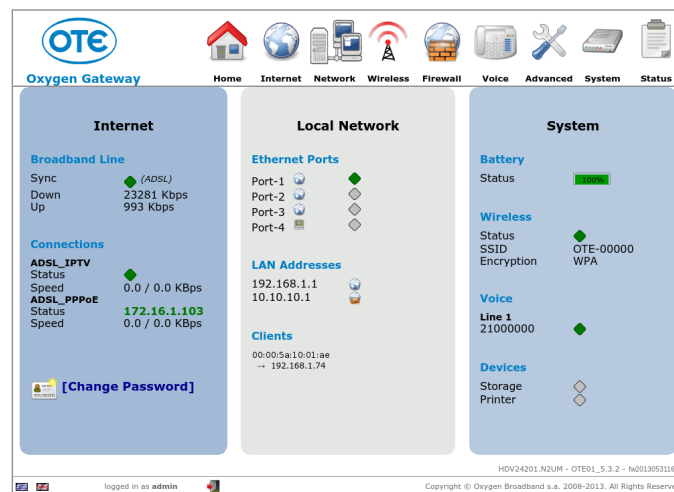


Figure 4.2: Home - Initial system view

Navigating through the Menus

At the top of the screen you can see the main top configuration menu, which displays the company's logo and all the configuration menu categories. This top configuration 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.

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

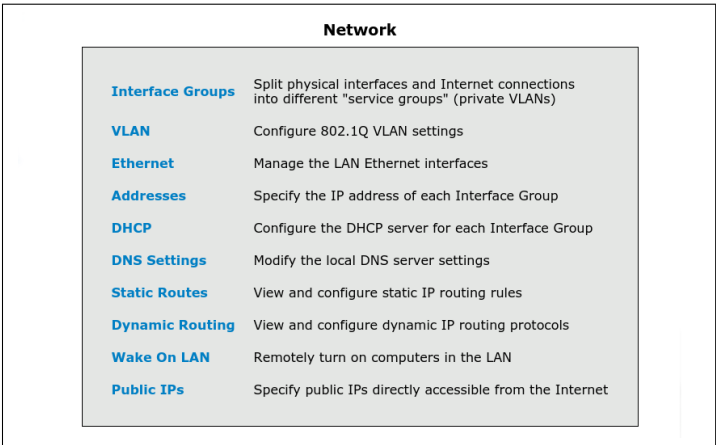


Figure 4.3: Configuration Menu Help Screen

Selection of a sub-menu entry can be performed by clicking on its title (bold 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.

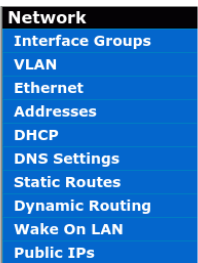



Figure 4.4: Left-side Navigation Menu

Logout

At the bottom of the screen you can always see a field containing Oxygen Broadband'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 Multiservice Gateway by pressing on the icon .

Languages

The Oxygen Multiservice Gateway 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 successful login to the web configuration tool of your device. 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.

Network Section (middle-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 [57](#))
- **Connections** for modifying existing or adding new Internet connections (see page [59](#))
- **DSL Line** for configuring the DSL line settings (see page [65](#))
- **3G/4G Modem** for managing the embedded 3G/4G (*optional feature*) or connected external (USB) dongles (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 [72](#))
- **VLAN** for configuring private VLAN operation (see page [74](#))
- **Ethernet** for modifying the LAN Ethernet interfaces (see page [75](#))
- **Addresses** for specifying the IP address of each Service Group interface (see page [76](#))
- **DHCP** for configuring the DHCP server for each Service Group interface (see page [78](#))
- **DNS Settings** for modifying the local DNS server settings (see page [81](#))
- **Static Routes** for viewing and configuring static IP routing rules (see page [84](#))
- **Dynamic Routing** for configuring dynamic IP routing protocols (see page [86](#))
- **Wake On LAN** for remotely turning on computers on the LAN (see page [87](#))
- **Public IPs** for configuring on the LAN IP addresses, directly accessible from the Internet (see page [88](#))

Wireless Web Page Menu

The **Wireless** menu provides configuration options for the Wireless functionality of the Oxygen Multiservice Gateway (*WiFi-enabled devices only*).

It includes the following sub-menus:

- **Configuration** for activation/deactivation and configuration of the wireless LAN (see page [90](#))
- **Security** for activation and configuration of security on the wireless LAN (see page [91](#))
- **MAC Filtering** for enabling wireless access control based on the MAC address of the WiFi client devices (see page [94](#))
- **Multiple SSIDs** for activating multiple virtual sub-networks on the wireless LAN (see page [95](#))

Firewall Web Page Menu

The **Firewall** menu provides configuration options for the protection of the LAN through the embedded firewall of the Oxygen Multiservice Gateway.

It includes the following sub-menus:

- **Configuration** for configuring the main firewall settings (see page [98](#))
- **Port Forward** for allowing selected incoming connections from the Internet towards the LAN, in order to enable some applications to work behind the firewall (see page [100](#))
- **UPnP / NAT-PMP** for activation/deactivation of automatic firewall port forwarding using the UPnP and/or NAT-PMP protocols (see page [102](#))
- **IP Filters** for precise control of allowed or denied IP connections between the LAN and the Internet (see page [103](#))
- **Web Filters** for denying access to web sites based on a configured list of keywords (see page [106](#))
- **DMZ Filters** for configuring a subnet on the internal network that has its hosts selectively exposed to access from the Internet (see page [107](#))
- **Address Mapping** for configuring the use of different public (WAN) IPs from different LAN hosts using Network Address Translation (NAT) (see page [109](#))

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:

- **Phone Lines** for configuring the external phone lines (see page [112](#))
- **Restrictions** for setting-up the voice dialing restrictions (see page [114](#))
- **Speed Dials** for configuring quick-dialing patterns (see page [116](#))
- **Black List** for configuring black-listed numbers for incoming calls (see page [117](#))

Advanced Web Page Menu

The **Advanced** configuration menu lets you control a series of different advanced services offered by the Oxygen Multiservice Gateway.

It includes the following sub-menus:

- **Dynamic DNS** for configuring the Dynamic DNS application (see page [120](#))
- **Date and Time** for changing date and time protocol settings (see page [121](#))
- **SSL VPN** for setting-up a secure SSL-based VPN connection using OpenVPN (see page [122](#))
- **GRE Tunnel** for setting-up a Generic Routing Encapsulation tunnel (see page [126](#))
- **L2TP Tunnel** for setting-up an L2TP and/or IPSec-based VPN tunnel (see page [127](#))
- **IPSec Tunnel** for setting-up an IPSec VPN tunnel (see page [130](#))
- **QoS Policy** for defining and configuring Quality of Service classes (see page [132](#))
- **File Sharing** for activation/deactivation of file sharing through connected USB storage devices (see page [135](#))
- **Printing** for activation/deactivation of USB printer support (see page [136](#))

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:

- **Green Operation** for enabling/disabling various environmental-friendly "Green" functionality options (see page [138](#))
- **SNMP** for configuration of the Simple Network Management Protocol (see page [139](#))
- **Syslog** for controlling the system logging service (see page [140](#))
- **Backup / Restore** for backing-up the current or restoring a previous configuration of the device (see page [141](#))
- **Firmware Upgrade** for performing a local or remote firmware upgrade (see page [143](#))
- **Remote Admin** for allowing remote access to the device for administration and/or support purposes (see page [145](#))
- **Change Password** for modifying the device administration password (see page [146](#))
- **Device Restart** for restarting the device and optionally erasing the entire configuration (factory defaults) (see page [147](#))

Status Web Page Menu

The **Status** menu lets you view device messages, the runtime 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 [151](#))
- **System Log** for viewing system log entries (see page [152](#))
- **Interfaces** for displaying information for the Ethernet and (*optional*) USB interfaces (see page [154](#))
- **DSL Line** for displaying status and statistics for the DSL broadband connection (see page [155](#))
- **Wireless** for a list of the connected WiFi clients and access points (AP) in range (*WiFi-enabled devices only*) (see page [156](#))
- **Phone Lines** for viewing information about the active voice calls and the status of supplementary services (see page [157](#))
- **Call Details** for viewing duration and history information for voice calls (see page [159](#))
- **ISDN Interfaces** for viewing information about the ISDN interfaces (see page [160](#))
- **Firewall** for displaying the current firewall status (see page [161](#))
- **Clients** for a list of connected clients (see page [162](#))
- **VPN Service** for displaying VPN service information (see page [163](#))
- **Diagnostics** for performing broadband connection and IP diagnostic tests (see page [164](#))
- **Healthcheck** for quickly checking the service operation status of the device (see page [165](#))
- **Net Statistics** for information about the LAN- and WAN-side network traffic (see page [166](#))
- **IP Network** for a list of addresses of IP interfaces, IP routes, DNS servers and active IP connections (see page [168](#))

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.
Add New	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.
Save	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.
Apply	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.
Browse...	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 group of radio buttons, 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 Multiservice Gateway 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: 192.168.1.1
	Subnet mask: 255.255.255.0
DHCP	Enabled, 192.168.1.51 - 100
WAN Connection	Type: PPPoE VLAN: <i>none</i>
NAT / Firewall	Enabled
Wireless	Enabled, SSID: OTE-XXXXX , (XXXXX is different for every device)
	Security: WPA , Key: <i>Different for each device,</i> <i>printed on the label of the device</i> (WiFi-enabled devices only)
Web Configuration	user / password

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.

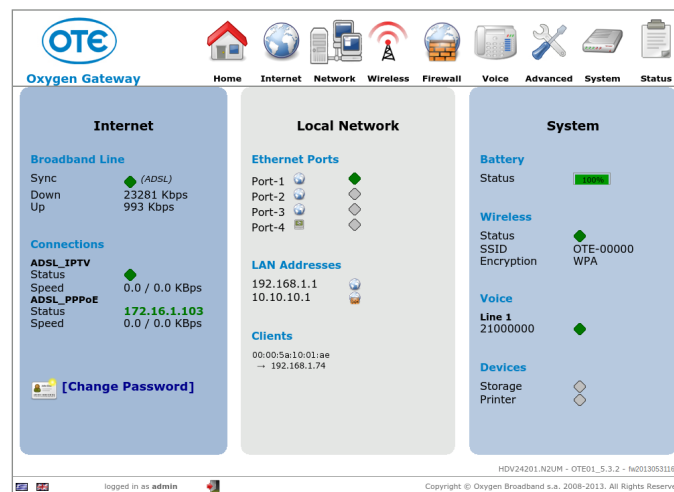


Figure 5.1: System View - Home

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

Internet Section (left-pane)

This section displays Internet-related information about the device.

On the upper side of the section, DSL synchronization status of the device is displayed 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 broadband line status info, 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 Multiservice Gateway. Below the link information, the user can see the private IP addresses assigned to each of the active *Service 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 connected 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

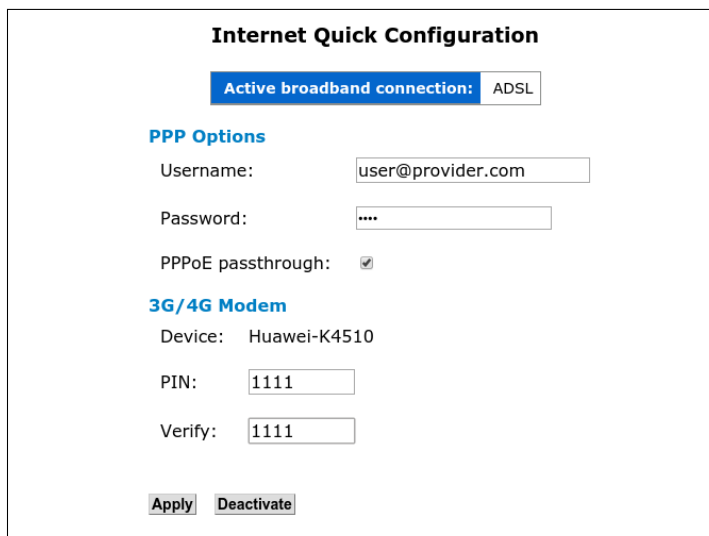
The **Internet** configuration web page menu allows the configuration of ATM PVCs, Internet connections and the DSL or other data modem functionality (*optional feature*). Available configuration options include:

- **Quick Start**
- **ATM PVCs**
- **Connections**
- **DSL Line**
- **3G/4G Modem**

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 the PPP configuration options.



The screenshot displays the 'Internet Quick Configuration' interface. At the top, it indicates the 'Active broadband connection' is 'ADSL'. Below this, the 'PPP Options' section includes fields for 'Username' (filled with 'user@provider.com') and 'Password' (filled with four asterisks), and a checked checkbox for 'PPPoE passthrough'. The '3G/4G Modem' section shows the 'Device' as 'Huawei-K4510', with 'PIN' and 'Verify' fields both containing '1111'. At the bottom, there are 'Apply' and 'Deactivate' buttons.

Figure 6.1: Quick Start - Internet Quick Configuration

This page contains the minimum information required in order to configure the WAN connection supporting the service. Please refer to section **Connections** on page 59 for a detailed description of all parameters.

Enter the appropriate credentials provided by your ISP and click on **Apply**.

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 Multiservice Gateway) 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.



WARNING

ATM PVCs are only relevant for your VDSL Oxygen Multiservice Gateway, only when the device operates in ADSL fallback mode. VDSL operation does not rely on ATM virtual circuits, but on the direct transport of Ethernet frames.

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	RFC 1483 bridged	 
1-PVC_1	8	36	RFC 1483 bridged	 
Add New				

Figure 6.2: 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:

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).

ATM Virtual Circuit 1-PVC_0

PVC
VPI: VCI:

Protocol

for PPPoE, bridged and routed EoA connections

Encapsulation

QoS
Traffic Class:
PCR:
SCR:

Figure 6.3: Config ATM PVC

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**, **PCR** and **SCR** are the ATM QoS traffic class of the connection, the Peak Cell Rate and the Sustained 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 Multiservice Gateway 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.





























Internet Connections					
	Service	Port	Type	Status	Action
ADSL_IPTV		1-PVC_1	Bridged EoA		   
ADSL_PPpOE		1-PVC_0	PPPoE		   
VDSL_IPTV		VDSL	Bridged		   
VDSL_PPpOE		VDSL	PPPoE		   
Add New					

Figure 6.4: 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 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. It should also be noted that connection names cannot contain spaces and selected special characters.
2. **Status** is the status of connection. Available options are *Enabled* and *Disabled*.
3. **Service** is the type of service this connection will support. Available options are *Data*, *Voice* and *Video* (when offered by your ISP).
4. **WAN port** is the type of port this connection will use. Available options are *VDSL*, *ADSL*, *Ethernet (optional feature)*, *L2TP (optional feature)* and *Modem (optional feature)*.
5. **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 screenshot shows a web-based configuration interface titled "New Internet Connection". It is divided into several sections, each with a blue header:

- Connection**: Includes fields for "Name" (my_conn), "Status" (radio buttons for Enabled and Disabled, with Enabled selected), "Service" (Data), "WAN port" (ADSL), and "Type" (PPPoE).
- ATM Options**: Includes "PVC" (8/35), "VPI / VCI" (8 / 35), and "Encapsulation" (LLC).
- 802.1Q VLAN**: Includes a checkbox for "Enabled" (unchecked), "VLAN ID" (empty), and "VLAN CoS" (empty).
- PPP Options**: Includes "Username" (user@provider), "Password" (masked with ****), "Dial On Demand" (checkbox unchecked, with a time field in seconds), and "PPPoE passthrough" (checkbox unchecked).
- IP Options**: Includes "MTU size" (1492).
- Routing**: Includes "Default route" (No).

A "Save" button is located at the bottom left of the form.

Figure 6.5: New Connection - PPPoE

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.

802.1Q VLAN

In case of Ethernet-over-DSL (e.g. PPPoE) or other Ethernet-type 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 an embedded 3G/4G modem or a dongle connected to the USB port of the Oxygen Multiservice Gateway (*optional features*).

1. **Device** is the modem used for this connection, or *ANY MODEM* in order to use the active first modem detected. Refer to section **3G/4G Modem** on page 67 for a description of the configurations steps required in order to define and activate a 3G/4G modem.
2. **Profile** is the set of parameters used in case of a 3G/4G 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/4G modem of the Oxygen Multiservice Gateway 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 3G/4G 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.

PPP Options

These are the PPP authentication parameters required in the case of a PPP connection (e.g. *PPPoE*):

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. **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 Ethernet-over-DSL (e.g. PPPoE) or other Ethernet-type connections.
4. **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 for a defined interval (configured in seconds).

IP Options

In case IPv6 functionality is globally enabled on the Oxygen Multiservice Gateway (please refer to section **IPv6 Addresses** on page 76), the **Operation** drop-down list controls the IPv4 and IPv6 type of operation of the WAN connection. Available options are:

1. **IPv4 only** (i.e. no IPv6 operation)
2. **IPv6 only** (i.e. no IPv4 operation)
3. **IPv4 + Tunnel IPv6**: This category controls the IPv6 over IPv4 tunneling operation, when this option has been selected in the **Operation** drop-down list. In order to configure a tunneling mechanism you need to perform the following steps:
 - **Tunnelbroker.net**: You must first fill in the **Tunnel ID**, then the remote server's IPv4 address into **Server IPv4**, the Local IPv6 address into the **Local IPv6**, then the /64 subnet into **IPv6 subnet** fields, the credentials for the connection in the fields **User ID** and **Password** and, optionally, an address for the tunnel interface **Local Tunnel**.
 - **Sixxs.net**: Configuration of Sixxs tunnel is done following the same steps as in Tunnelbroker tunneling mechanism described above
 - **6to4**: to enable the tunnel for this WAN connection and Service Group interface.
4. **IPv6 + Tunnel IPv4**: This method is a way to support IPv6 operation in the LAN if the ISP access network supports only IPv4 operation. There exist various IPv6 tunneling mechanisms supported by the Oxygen Multiservice Gateway. In order to configure a tunneling mechanism you need to perform the following steps:
 - Select the desired tunneling **Method** i.e. choose **DS-lite**, **MAP-T**
 - Select **Auto** for automatic configuration or **Fixed** for manual configuration from the **Remote server** drop-down list. In the latter case, fill-in the necessary tunnel-specific parameters in order to configure the selected tunnel.
5. **Dual Stack** (simultaneous and independent IPv4 and IPv6 operation).

Under the **IP Options** heading, it is also possible to set the **MTU size** (Maximum Transmission Unit) in bytes of the IP connection interface.

**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.

IPv4 Options

This category provides the IPv4 address configuration required in the case of non-PPP routed connections. Available choices are: automatic configuration through **DHCP client**, 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*.

IPv6 Options

In case IPv6 functionality for the connection is enabled using the **Operation** drop-down list described above, the parameters under this category control the **Method** for acquiring IPv6 addressing information. Available options are:

1. **SLAAC**, which allows for WAN interface to be autoconfigured for an IPv6 prefix through Router Advertisements (R.A.)
2. **Link local only**, where the WAN interface obtains only a link-local IPv6 address
3. **Stateless DHCPv6**, where the WAN connection uses Router Advertisements (R.A.) for its IPv6 address and DHCPv6 for additional IPv6 parameters (e.g. Prefix Delegation), and
4. **Stateful DHCPv6**, where all IPv6 addressing information is obtained through DHCPv6

IP Options
Operation: Dual-Stack ▼
MTU size: 1492
IPv6 Address
Method: Stateless DHCPv6 ▼

Figure 6.6: IPv6 Options

IP Routing

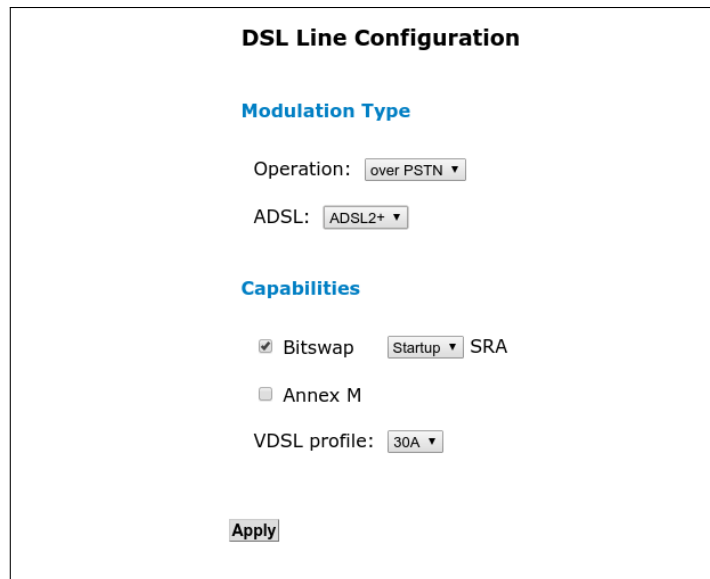
The **Default route** parameter defines if the connection will provide the default route for Internet connectivity. Available options are *Yes*, for a connection offering default route, *Backup*, for a connection acting as a backup in case of failure of the default-route connection, and *No*, for any 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 Multiservice Gateway.



The image shows a web-based configuration interface titled "DSL Line Configuration". It is divided into two main sections: "Modulation Type" and "Capabilities".

Modulation Type

- Operation: over PSTN (dropdown menu)
- ADSL: ADSL2+ (dropdown menu)

Capabilities

- ☒ Bitswap (checked) Startup (dropdown menu) SRA
- ☐ Annex M
- VDSL profile: 30A (dropdown menu)

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

Figure 6.7: DSL Line Parameters

The following parameters can be configured:

- **Operation:** type of the line synchronization operation. Select between *PSTN* and *ISDN* according to the type of the connected line.
- **ADSL:** Select the **ADSL** line type / operation mode.
- **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.
- **VDSL profile:** Select the appropriate VDSL profile from the drop-down list, or *Off* for disabling VDSL mode of operation (only ADSL fallback).
- **Annex M:** a variation of the ADSL technology offering increased upload speed (*if supported by your model of the Oxygen Multiservice Gateway and by the ISP's DSLAM - PSTN connections only*).

**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.

3G/4G Modem

The Oxygen Multiservice Gateway is optionally equipped with an embedded 3G/4G modem. Alternatively, its optional USB host ports can be used for WAN connectivity through external 3G/4G modems. The corresponding detected 3G/4G modem with its current status is displayed in the **3G/4G Modem** configuration option.

The first option available in this page, is the configuration of the **Backup Operation** of the 3G/4G modem. Available options are *Auto* and *Manual*. With *Auto*, backup connectivity to the WAN is activated automatically once the primary Internet connection is detected to be inactive. If, on the other hand, the *Manual* option is selected, the backup connection to the WAN must be manually activated by pressing the **Dial** button.

3G/4G Modem

Backup Operation

Mode: ☐ Auto ☒ Manual

Name	WNC-D18Q1
Status	Ready
IMEI	355855023461146

Action:

Parameters

Modem PIN:

Mode:

APN:*

Init. string:*

Dial string:*

Authentication:

Username:*

Password:*

Modem speed:

(*) Optional

Figure 6.8: 3G/4G Modem



WARNING

The Manual configuration option under the **Backup Operation** parameter is strongly advised for users with a fixed volume mobile data plan, in order to avoid unexpected charges from their 3G/4G Service Provider.

In order to perform a scan for the presence of a connected 3G/4G modem, press **New Scan**. A new scan for connected 3G/4G modems is performed and any connected devices are automatically added to the list of known modems.

The **Status** row field displays the current status of the modem. Available values are *Ready*, *Locked PIN*, *Locked PUK*, *Not detected*.

You can perform 3G/4G modem actions by selecting the appropriate **Action** from the drop-down menu. Depending on the status of the modem, the available actions are:

1. *Configure*, in order to configure the modem parameters,
2. *Disable PIN*, in order to disable PIN control on the SIM,
3. *Change PIN*, in order to modify the SIM PIN value,
4. *Reset*, in order to perform a hard-reset of the modem, and
5. *Unlock*, (visible when the modem has been locked due to use of a wrong PIN value) in order to unlock the modem SIM using the correct **PUK** code.

When configuring the modem, the most usual task is to set the **PIN** of the SIM inserted into the modem. It is also possible to set the following advanced parameters (usually not required to be modified):

1. **Mode**, which is the preferred mobile data communication standard. There are multiple options available depending on the modem, the region and provider configurations. Common options include *Auto* (default and recommended), *LTE / 3G*, *LTE only*, *3G only*, *3G preferred*, *2G only*, *2G preferred* etc.
2. **APN**, **Init. string**, **Dial string**, and PPP **Authentication**, **Username** and **Password** values. These parameters are only used in order to bypass the values configured under the WAN connection settings (please refer to section **Connections** on page 59).
3. **Modem speed** which assigns an internal operation speed limit to the device modem. Required to be modified ONLY for some specific modem types. Please leave to *Default* unless instructed to modify it by your ISP.

Info

By clicking on the **Info** button when available, a page like the following appears:

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

Modem Info	
Manufacturer	GSM
Model	K35
Revision	11.608.11.15.00
IMEI	359574032087703
System Devices	0 / 1
SIM IMSI	202052964839014
Status	Ready
Operator	Operator
Signal	Fair (48%)
Connection Mode	3G
Mode Preference	Auto
Connection Time	4m 6s
Speed (Down/Up)	-
Maximum (Down/Up)	-
Bytes (Down/Up)	7.07 KB / 24.66 KB

Figure 6.9: Show Modem Parameters

7

Network Menu

The **Network** configuration menu handles all the local network IP services provided by the Oxygen Multiservice Gateway. Available configuration options include:

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

Interface Groups

The Oxygen Multiservice Gateway 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. This way WAN connections and LAN interfaces are organized into **Service Groups**. The Oxygen Multiservice Gateway supports two alternative methods for this division of the LAN interfaces into different Service Groups:

1. **Private VLANs**, and
2. **802.1Q VLANs**

With **Private VLANs**, which is the simple solution, each local Ethernet ports is assigned to a single Service Group. This is an internal function of the Oxygen Multiservice Gateway and no requirement is imposed on the clients existing the local Ethernet network.

With **802.1Q VLANs**, on the other hand, it is possible to assign the same Ethernet port to multiple Service Groups, through the use of VLAN tags. As it is clear, this is a more powerful but also more complex approach, as it normally requires advanced configuration also for the clients existing the local Ethernet network.

Selection between **Private VLANs** and **802.1Q VLANs** is performed in the **VLAN** configuration page (see page 74).

Regardless of the VLAN method selected for splitting the local Ethernet ports, their assignment to different broadband Service Groups is performed using the **Interface Groups** web menu.

To this end, this web configuration page provides a list of all LAN ports (when using *Private VLANs*) or defined LAN 802.1Q VLANs (when using *802.1Q VLANs*). Using the corresponding drop-down list of supported **Services**, each **Interface** (physical port or 802.1Q VLAN) 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 Service Groups is presented for information-only purposes and cannot be changed here. It is handled using the **Service** parameter in the **Connections** configuration page (see page 59).*

Additionally the following parameters can be enabled:

1. **IGMP snooping** to activate local snooping of multicast traffic based on LAN *Internet Group Management Protocol* messages.
2. **IGMP proxy** to activate the proxying operation for multicast *IGMP* packets from the LAN towards the WAN.

Interface Groups

Interface	Service
Port-1	Data ▼
Port-2	Data ▼
Port-3	Data ▼
Port-4	Video ▼
WiFi-1	Data ▼
WiFi-2	Data ▼

Connection	Service
ADSL_IPTV	Video
ADSL_PPPOE	Data
VDSL_IPTV	Video
VDSL_PPPOE	Data

IGMP snooping: ☐

IGMP proxy: ☐

Apply

Figure 7.1: Interface Groups

VLAN

VLAN (Virtual Local Area Network) is a technology that allows you to partition one physical network into a set of virtual networks. As described in the previous section **Interface Groups**, VLANs are essential for the support of multiple broadband services over the Local Area Network. The Oxygen Multiservice Gateway supports two alternative methods for this division of the LAN interfaces into different Service Groups: **Private VLANs**, and **802.1Q VLANs**.

Private VLANs is the simpler approach and the default mode of operation for the Oxygen Multiservice Gateway. The **VLAN** configuration page allows the activation and control of the more complex mode **802.1Q VLANs**. In order to activate the use of **802.1Q VLANs** on the Oxygen Multiservice Gateway, you must first select *Enabled* as **802.1Q Status**.

Local Network 802.1Q VLANs

Status

☐ Enabled ☒ Disabled

VLAN ID

Switch native VLAN:

VLAN ID	Port-1	Port-2	Port-3	Port-4	WiFi-1	WiFi-2
<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"/>	<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"/>	<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"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Apply

Figure 7.2: VLAN

The next step is the definition of the list of allowed VLAN-IDs and the assignment of each physical Ethernet port to the defined VLAN-ID. To configure an 802.1Q VLAN:

1. Enter the **VLAN ID**. Valid **VLAN ID** values are between 1 and 4096.
2. Select for each port the type of **VLAN** membership method you want: '---' for no membership, Access for membership without the use of 802.1Q tag, and Tagged for membership with the use of 802.1Q tags.
3. Click **Apply**.

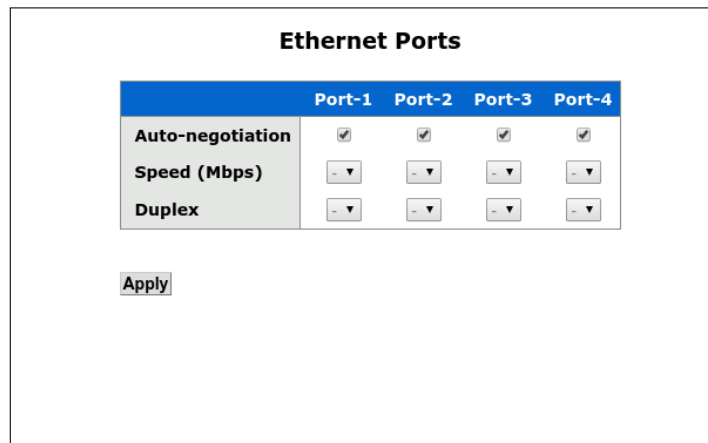


Note

Only one VLAN-ID can be accessed for each port as Access VLAN. If no VLAN-ID has been selected for an Ethernet port, this port is automatically set to belong to the **Switch native VLAN**.

Ethernet

The Oxygen Multiservice Gateway is a full featured device, capable of supporting fast, gigabit and/or optical LAN Ethernet connections (*model dependent*).



	Port-1	Port-2	Port-3	Port-4
Auto-negotiation	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Speed (Mbps)	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Duplex	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Apply

Figure 7.3: Ethernet Ports

This web configuration page provides to the web administrator, the ability to configure Ethernet *Speed* and *Duplex* values. For optional *Combo* interfaces (Optical and Copper with one of the two active), it is also possible to select the preferred priority between *Optical* and *Copper* mode of operation.

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"/>	192.168.1.1	255.255.255.0
Voice	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
Video	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
WiFi-2	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
DMZ	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10.10.10.1	255.255.255.0

Figure 7.4: 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 *192.168.1.1*
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 Multiservice Gateway. This requires the existence of a DHCP Server in the LAN. 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 192.168.1.1.

IPv6 Addresses

Under the **Addresses** configuration menu, it is also possible to enable or disable the global IPv6 operation of the Oxygen Multiservice Gateway. This is performed using the respective radio button that appears under the **Global IPv6 Operation** title. The **Global IPv6 Operation** setting affects the presence of various IPv6-related options in different web pages (e.g. refer to subsection **IPv6 Options** in page 63).

Global IPv6 Operation

☒ Enabled ☐ Disabled

ULA IPv6 Addresses

	Status	Address	Mask
Data	Off	::	64
Voice	Off	::	64
Video	Off	::	64
WIFI-2	Off	::	64
DMZ	Off	::	64

Apply

Figure 7.5: IPv6 Addresses

Apart from the **Global IPv6 Operation** status of the device, in this configuration page, it is also possible to control the assignment of IPv6 **Unique Local Addresses (ULA)** to each Service Interface Group. Through the **Status** drop-down list, you can choose between **Off**, **Fixed** and **Auto** state. When option **Auto** is selected, a ULA address is configured for the respective interface based on a pseudo-random 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, in order to define your 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 Multiservice Gateway allows the automatic network configuration of all LAN devices on each Interface Group.

LAN Addresses

	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

[Static DHCP Options]

Figure 7.6: DHCP Server Configuration

To configure the DHCP Server:

1. Enable/Disable the DHCP server by selecting *On/Off* from the drop-down menu of **DHCP** 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 Options

In addition to the standard DHCP options provided by the DHCP server it is also feasible to set certain DHCP option values. This is attainable using the **Static DHCP Options** page. Following the corresponding

link, a list of already configured options appears. You may delete existing entries by clicking on the icon  of **Action** column.

To add a new static DHCP option select the **Service** group for which the DHCP server will provide the option (*All* for all Service Groups) and the type of **Option**. Enter the corresponding option **Value**. You can optionally enter also the **Vendor** ID if you wish the configured option to be transmitted to hosts. Finally click on **Save**.

LAN IPv6 Addresses

For devices with enabled IPv6 operation, a second menu appears, titled **LAN IPv6 addresses**. Here, you can specify the method for IPv6 address assignment to the LAN hosts. In particular, for each Service Group there is a possibility of different options.

1. *Stateless Address Configuration (SLAAC)*: With this option, Router Advertisements that contain Prefix and LifeTime information are sent to the LAN hosts that belong to the specific Service Group. In parallel, RDNSS is enabled, which means that supporting hosts may obtain DNS server information is also performed through **Router Advertisement** for hosts whose Operating System supports this functionality (e.g. Linux PCs). Parameters related to the **Router Advertisement** operation of the Oxygen Multiservice Gateway can be controlled using the corresponding fields on the bottom of the configuration page. **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.
2. *Stateless DHCPv6*: With this option, LAN hosts obtain their IPv6 address via Router Advertisement. However, the Router Advertisement packets have the so-called Other Configuration Flag set to on. This way, the LAN host is dictated to start a DHCPv6 request and the Oxygen Multiservice Gateway provides it with stateless configuration parameters, such as DNS server, NTP, SIP servers, AFTR server etc. This is the most common mode of IPv6 operation for LAN hosts.
3. *Stateful DHCPv6*: With this option, both address and additional information are transmitted over DHCPv6. Using either of these three IPv6 assignment methods the Oxygen Multiservice Gateway assigns the /64 IPv6 prefix to IPv6-enabled hosts in the LAN. Therefore, in parallel to the method used for IPv6 address assignment, it is essential to also select the source of the assigned IPv6 prefixes. They can be either obtained from the WAN through DHCPv6 Prefix Delegation (please refer to the *Stateless DHCPv6* and *Stateful DHCPv6* options in section **Connections** on page 59) or they can be manually configured. The first option is realized by selecting *Auto* under the **Pool** drop-down list, whereas the latter by selecting *Fixed* and configuring the appropriate **Subnet** and **Lease** time values.

LAN IPv6 Addresses

	Status	Pool	Subnet	Lease
Data	Stateless DHCPv6 ▾	Auto ▾		86400
Voice	Off ▾	Auto ▾		86400
Video	Off ▾	Auto ▾		86400
DMZ	Off ▾	Auto ▾		86400

Router Advertisements

Maximum R.A. interval: (sec)

Valid lifetime: (sec)

Preferred lifetime: (sec)

Figure 7.7: LAN IPv6 Addresses

DNS Settings

The Oxygen Multiservice Gateway 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.

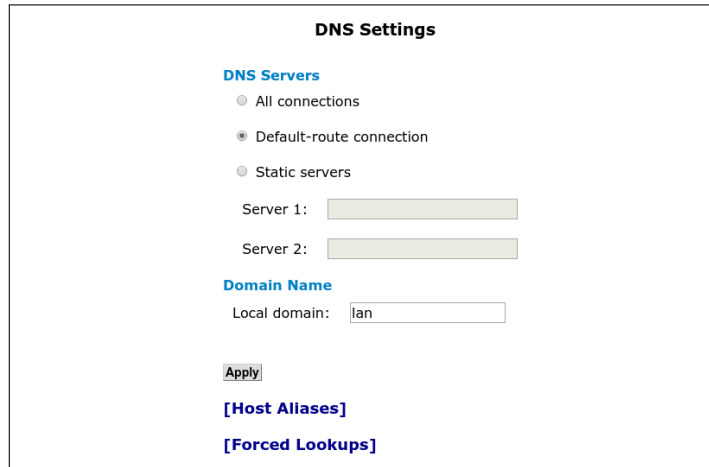


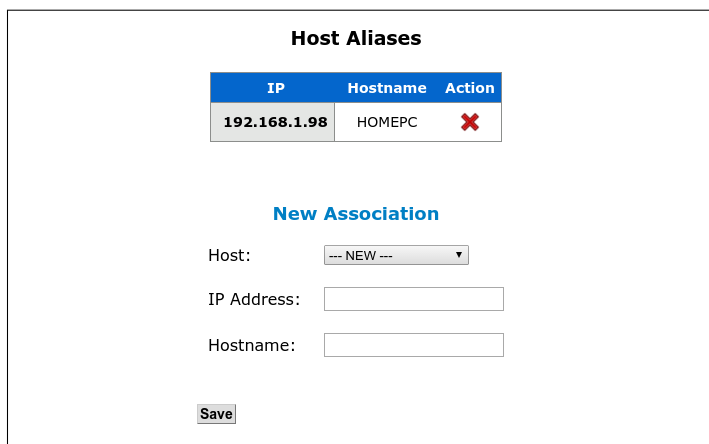
Figure 7.8: DNS Settings Configuration


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 Multiservice Gateway 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:



IP	Hostname	Action
192.168.1.98	HOMEPC	


New Association

Host:

IP Address:


Hostname:

Figure 7.9: Host Aliases

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

Forced Lookups

In the **Forced Domain Lookups** page you can find the usage of the DNS Servers related to certain WAN connections for specific domain names. At the top of the page, a list of the configured bindings is displayed. You can *Delete* entries by clicking on the icon  of **Action** column.

To add a new *forced lookup* entry, select the corresponding **Service / Connection** and enter the **Domain** name to be resolved through the DNS servers of that **Service / Connection**. Finally click on **Save**.

Forced Domain Lookups

Server	Domain	Action
WAN: ADSL_PPPoE	my.domain	✖

New Association

Service / Connection: --- WAN --- ▾

Domain:

Save

Figure 7.10: Forced Lookups

Static Routes

In most cases, for Internet traffic it is adequate to specify the correct **Default Route** WAN connection (please refer to section **Connections** on page 59). Using specific methods (e.g. dynamic routing protocols or DHCP options), it is also possible for the ISP to automatically 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:

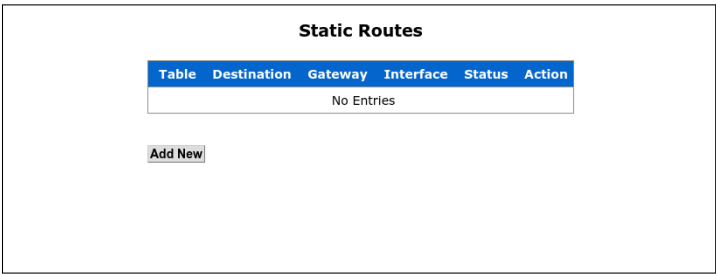




Figure 7.11: Static Routing

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:

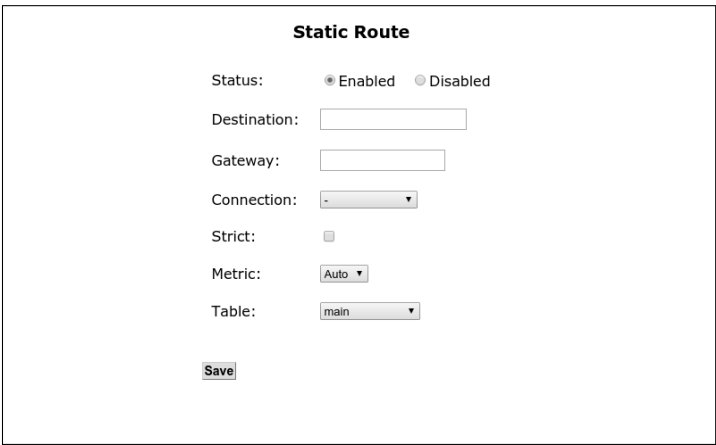


Figure 7.12: Static Route Edit

1. Enter the **Destination** network address and mask (e.g. 192.168.20.0/24).
2. Enter the **Gateway** IP address and/or **Interface/Connection** used for the forwarding of the packets.

3. Optionally enable additional options **Strict**, select a **Metric** value and the routing **Table**.
4. Click **Save**.

**Note**

Network value 0.0.0.0/0 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 Multiservice Gateway.

Dynamic Routing		
Service Stopped		
Status		
<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled		
Active Connections		
Connection	Enabled	Disabled
ADSL_IPTV	<input type="radio"/>	<input checked="" type="radio"/>
ADSL_PPPoE	<input type="radio"/>	<input checked="" type="radio"/>
VDSL_IPTV	<input type="radio"/>	<input checked="" type="radio"/>
VDSL_PPPoE	<input type="radio"/>	<input checked="" type="radio"/>

Apply

Figure 7.13: 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.

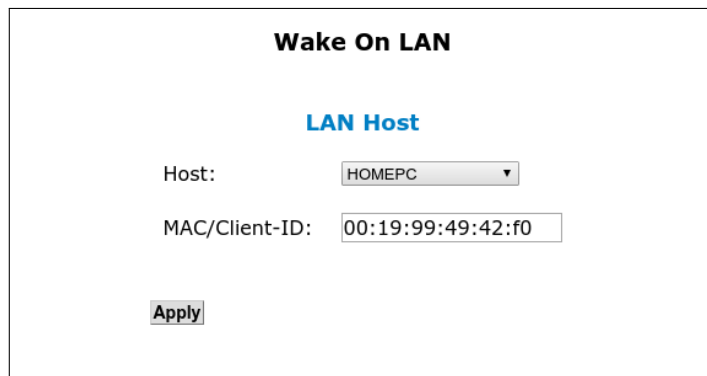


Figure 7.14: Host wake on LAN

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 Multiservice Gateway 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 sections **Addresses** on page 76 and section **DMZ Filters** on page 107). If it is 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 Multiservice Gateway 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.

	Enabled	IP Address	Netmask
Data	<input type="checkbox"/>		
Voice	<input type="checkbox"/>		
Video	<input type="checkbox"/>		
DMZ	<input type="checkbox"/>		

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

Figure 7.15: Public IP Addresses

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

1. Enter the public **IP Address** used for the Oxygen Multiservice Gateway. 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 Multiservice Gateway and will not be translated via NAT.
3. Check the **Enabled** checkbox in order to activate the relevant operation for the specific Interface Group.
4. Click **Apply**.

8

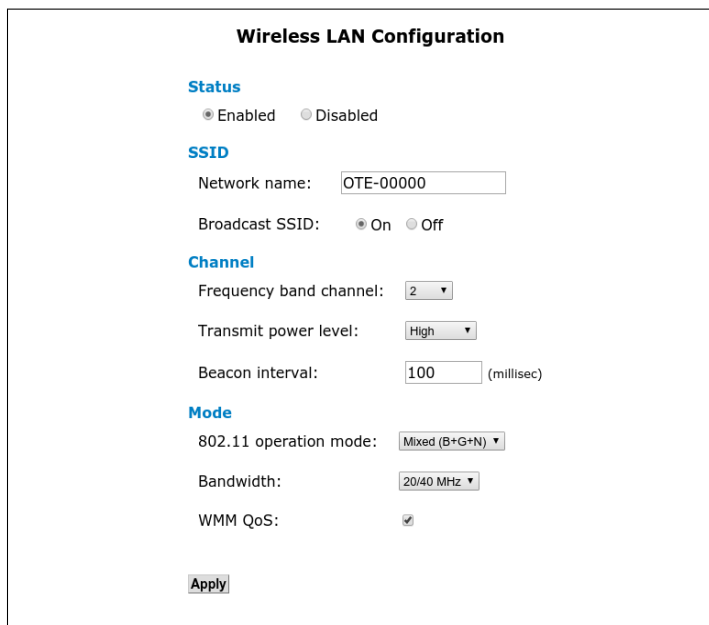
Wireless Menu

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

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

Configuration

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



The image shows a 'Wireless LAN Configuration' form. It is divided into several sections: 'Status' with radio buttons for 'Enabled' (selected) and 'Disabled'; 'SSID' with a text field for 'Network name' containing 'OTE-00000' and radio buttons for 'Broadcast SSID' set to 'On'; 'Channel' with dropdowns for 'Frequency band channel' (set to 2), 'Transmit power level' (set to High), and a text field for 'Beacon interval' (set to 100) with '(millisec)' next to it; 'Mode' with a dropdown for '802.11 operation mode' (set to 'Mixed (B+G+N)'), a dropdown for 'Bandwidth' (set to '20/40 MHz'), and a checked checkbox for 'WMM QoS'. An 'Apply' button is at the bottom left.

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 **Frequency band channel** as *Auto* or specify a specific channel number. When manually selecting channels, choose 1 or 6 or 11 to avoid interference from neighbor channels.
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.

The screenshot shows a web interface titled "Wireless LAN Security". It contains the following fields and options:

- Name (SSID):** OTE-00000
- Mode:** Security mode: WEP (selected from a dropdown menu)
- Authentication:**
 - Mode: 64 bit (selected from a dropdown menu)
 - WEP key: mykey (entered in a text box)
 - 0 characters remaining!
 - Hex: 6D796B6579
- A red warning message: "Warning! The use of WEP with 802.11n operation mode is vulnerable!"
- An "Apply" button at the bottom.

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**.

**Warning**

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/WPA2

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).

Wi-Fi Protected Setup (WPS)

When **WPA2** is the chosen security mode it is possible to enable and use **WPS**. With this mode it is possible to allow clients to connect to the Gateway using the **WPS** button (optionally) or through the web interface.

To enable **WPS** mode:

1. Check the **Enabled** option.
2. Click on **Apply**. Now **WPS** is enabled.

3. Click on **Activate** to allow wireless clients to connect using WPS for a predefined time interval (2 minutes).
4. Connect to the Oxygen Multiservice Gateway according to your WPS-capable wireless device instructions.

**Note**

WPA is the default security policy of the Oxygen Multiservice Gateway. 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 E** on page 193 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 Multiservice Gateway (but not encrypting traffic), is through the **MAC Filtering** sub-menu.

MAC Filtering

Default Policy

☒ Disabled ☐ Allow ☐ Reject

Stored MAC Addresses

1	HOMEPC	00:19:99:49:42:f0
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:

- **Disabled**: every host can connect.
- **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 Multiservice Gateway 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 72). 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. It is also possible to limit the connectivity between clients on the same SSID by checking the **Isolate Clients** option.

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.

Wireless LAN Security

WiFi-1WiFi-2

Name (SSID)
OTE-00000-2

Mode
Security mode: WPA/WPA2 ▼

Authentication
Mode: Personal (PSK-TKIP) ▼
WPA key:

Apply

Figure 8.6: Wireless Security - Multiple SSIDs

9

Firewall Menu

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

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

Configuration

This web configuration page allows the basic configuration of the firewall of the Oxygen Multiservice Gateway.



WARNING

It is strongly recommended NOT to modify the default settings of this configuration page.

Firewall Configuration

Status: Enabled ▼

Port forward: WAN ▼

WAN Connections

Connection	NAT	Ping
ADSL_IPTV	<input checked="" type="checkbox"/>	<input type="checkbox"/>
ADSL_PPpE	<input checked="" type="checkbox"/>	<input type="checkbox"/>
VDSL_IPTV	<input checked="" type="checkbox"/>	<input type="checkbox"/>
VDSL_PPpE	<input checked="" type="checkbox"/>	<input type="checkbox"/>
LAN: DMZ	<input checked="" type="checkbox"/>	<input type="checkbox"/>

LAN Interface Groups

Service	Router Access	WAN Access	Secondary WAN
Data	Standard ▼	<input checked="" type="checkbox"/>	... ▼
Voice	Standard ▼	<input checked="" type="checkbox"/>	... ▼
Video	Standard ▼	<input checked="" type="checkbox"/>	... ▼
DMZ	Minimal ▼	<input checked="" type="checkbox"/>	... ▼

Routing between LAN groups: ☐

Apply

Figure 9.1: Firewall Configuration

Using the **Status** drop-down list it is possible to *Enable* (default and most common option) or *Disable* firewall operation. It is also possible to control via firewall only incoming connections towards the Oxygen Multiservice Gateway, but freely *Forward traffic* between the LAN and the WAN (*Input-only, Allow-Forward*).

WAN Connection

Under the **WAN Connections** table, it is possible to activate or deactivate **NAT** operation for each WAN connection and allow or reject incoming **Ping** connection attempts. In the same table, it is also possible to control if **NAT** operation is going to be active for traffic from the **DMZ** Service towards the WAN (please refer to section **DMZ Filters** on page 107).

LAN Interface Groups

For each **Service** LAN Interface Group, it is possible to control the level of IP access towards the Oxygen Multiservice Gateway and towards the broadband WAN network.

The **Router Access** parameter controls access towards the Oxygen Multiservice Gateway itself. *Standard* allows full access (e.g. access to Web configuration tool), *Minimal* allows communication only for IP address assignment (DHCP) and name resolution (DNS), and finally *Ping-only* for the same traffic like *Minimal* with the addition of Ping ICMP connection requests.

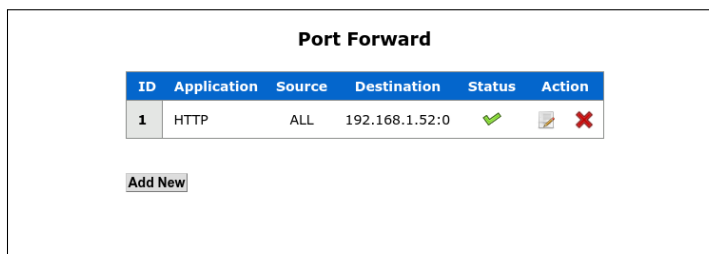
The **WAN Access** checkbox, on the other hand, controls if IP routing is allowed between the LAN Interface Group and the WAN connections belonging to the same Service. Similar to the **WAN Access** checkbox, the **Secondary WAN** drop-down list controls IP routing between the LAN and the WAN. This drop-down list can be used in order to allow routing of IP traffic between the WAN connection belonging to a Service and the LAN hosts belonging to the selected **Secondary WAN** service.



Finally, the **Routing between LAN groups** checkbox can be used in order to allow connectivity between different LAN hosts in different LAN Interface Groups.

Port Forward

The firewall and Network Address Translation (NAT) engine of the Oxygen Multiservice Gateway 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 Multiservice Gateway 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.



ID	Application	Source	Destination	Status	Action
1	HTTP	ALL	192.168.1.52:0	✓	 

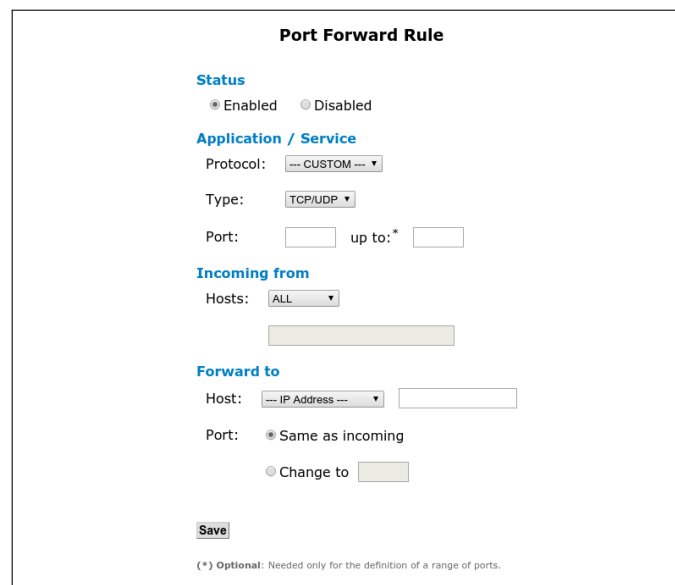
[Add New](#)

Figure 9.2: 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. Make sure **Status** is *Enabled*.
2. 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.
3. 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.
4. 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.
5. 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 181).



Port Forward Rule

Status
☒ Enabled ☐ Disabled

Application / Service
Protocol:
Type:
Port: up to: *

Incoming from
Hosts:

Forward to
Host:
Port: ☒ Same as incoming
☐ Change to

Save

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

Figure 9.3: New Port Forwarding

6. 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 Multiservice Gateway through DHCP, you can select it from the drop-down list and a static DHCP lease will also be automatically added .
7. 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.
8. 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 Multiservice Gateway by transparently applying the required port-forwarding rules. Through these protocols, the PCs on the LAN notify the Oxygen Multiservice Gateway about the need for specific port forwarding rules, and the necessary actions are performed without any user intervention.

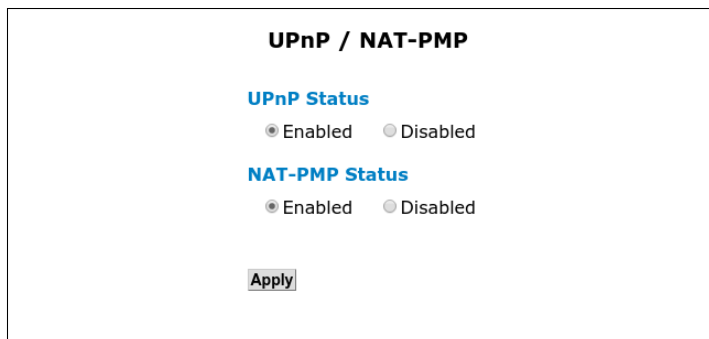
The image shows a configuration window titled "UPnP / NAT-PMP". Inside the window, there are two sections. The first section is "UPnP Status" with two radio buttons: "Enabled" (which is selected) and "Disabled". The second section is "NAT-PMP Status" with two radio buttons: "Enabled" (which is selected) and "Disabled". At the bottom of the window, there is an "Apply" button.

Figure 9.4: 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 161).

IP Filters

The IP filtering service allows the Oxygen Multiservice Gateway to control in a detailed way 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 Multiservice Gateway 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.

IP Filters						
ID	Application		Source	Destination	Filter	Status Action
1	HTTP		LAN: Data 192.168.1.75	WAN: Data		
Add New						

Figure 9.5: 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. Make sure **Status** is *Enabled*.
2. 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.
3. 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:--Service--** for any WAN connection belong to a specific **Service**, **--WAN--** to match all Internet connections or **--LAN--** to match the entire LAN (all Interface Groups).
4. 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

IP Filtering Rule

Status
☒ Enabled ☐ Disabled

Filter
☒ Drop ☐ Reject ☐ Accept
 Silently discard connection attempts.

Source
 Service / Connection: LAN: Data
 Host / Subnet: 192.168.1.75

Destination
 Service / Connection: WAN: Data
 Host / Subnet:

Application / Service
 Direction: Originating
 Protocol: CUSTOM
 Type: TCP/UDP
 Port: up to:

Save

(*) NOTE: Enter the IP address or name of a fixed host, a subnet (xxx.xxx.xxx.xxx/yy) or leave blank for "any-IP".
 (**) NOTE: Options "Source" and "Destination" define unidirectional traffic, "Bidirectional" defines stateless bidirectional traffic and "Originating" defines stateful bidirectional traffic.
 (***) Optional: Needed only for the definition of a range of ports.

Figure 9.6: New IP Filter

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 181).

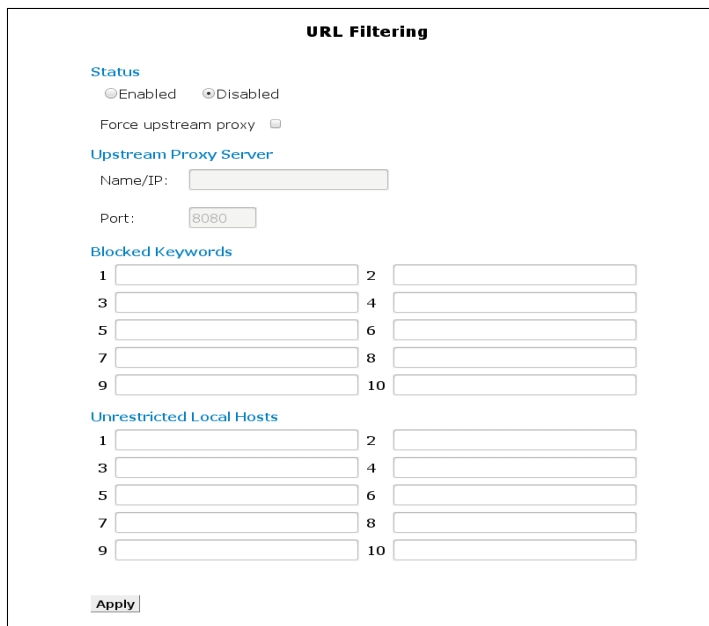
5. Repeat steps 3 to 4 for the selection of the **Destination** of the filtered traffic.
6. Specify the **Application/Service** being filtered by choosing any of the pre-defined applications in the **Protocol** drop-down menu or by choosing *CUSTOM* followed by the protocol **Type** (*TCP*, *UDP* or *Both*) and the **Port** number.
7. Select the **Direction** of IP traffic for which the value applies:
 - **Destination**: IP traffic towards the selected Application/Service as the **Destination** host/network.
 - **Source**: IP traffic from the selected Application/Service from the **Source** host/network.
 - **Bidirectional**: IP traffic either towards the selected Application/Service to the **Destination** host/network or from the selected Application/Service from the **Source** host/network (e.g. **Destination + Source**).
 - **Originating**: IP traffic towards the selected Application/Service on the **Destination** host/network and the response to the this traffic (e.g. **Destination + replies to it**).
8. 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 Multiservice Gateway.

Web Filters

The Oxygen Multiservice Gateway 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 the 'URL Filtering' configuration page. It includes a 'Status' section with 'Enabled' and 'Disabled' radio buttons, and a 'Force upstream proxy' checkbox. Below is the 'Upstream Proxy Server' section with input fields for 'Name/IP' and 'Port' (set to 8080). There are two lists of input fields: 'Blocked Keywords' and 'Unrestricted Local Hosts', each with 10 numbered slots. An 'Apply' button is at the bottom.

Figure 9.7: 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. Optionally specify the IP address for a list of **Unrestricted Local Hosts**, for which the web filtering will not apply.
5. 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 71). From a security point of view, however, the DMZ is treated like a semi-external network, usually using public IP addresses and kept totally separated from the *Data*, *Voice* and *Video* Interface Groups. 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 based on the configuration options (see below).
3. For connections from the DMZ towards the Internet, by default no NAT is applied, since public IP addresses are usually assigned to the DMZ hosts (please refer to section **Configuration** on page 98 for enabling NAT on traffic from the DMZ hosts towards the WAN).
4. Connections from the DMZ towards the LAN Interface Groups are filtered through the firewall.
5. Connections from the LAN Interface Groups towards the DMZ are allowed, but NAT is applied hiding the internal IP addressing scheme.

The **DMZ Filters** sub-menu, first of all controls item 1 of the list above, through the configuration of the list of services that are allowed to pass the firewall from the Internet towards the hosts in the DMZ. From the list of services/protocols displayed, check the ones that should be allowed through the firewall.

Regarding item 2, of the list above, traffic from the DMZ to the Internet is normally only allowed in response to incoming connection requests. Using, however, the **Allow all outgoing connections** checkbox, it is possible to allow any traffic from the DMZ towards the Internet.

Having selected the preferred DMZ operation parameters, 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.*

Demilitarized Zone (DMZ) Protocols

Application	Allowed	Application	Allowed
AUTH	<input type="checkbox"/>	DNS	<input type="checkbox"/>
FTP	<input type="checkbox"/>	HTTP	<input type="checkbox"/>
HTTPS	<input type="checkbox"/>	IMAP2	<input type="checkbox"/>
IMAP3	<input type="checkbox"/>	IMAPS	<input type="checkbox"/>
NNTP	<input type="checkbox"/>	NTP	<input type="checkbox"/>
OpenVPN	<input type="checkbox"/>	POP3	<input type="checkbox"/>
POP3S	<input type="checkbox"/>	SIP	<input type="checkbox"/>
SMTP	<input type="checkbox"/>	SMTP-AUTH	<input type="checkbox"/>
SMTPS	<input type="checkbox"/>	SNMP	<input type="checkbox"/>
SNMP Trap	<input type="checkbox"/>	SSH	<input type="checkbox"/>
Telnet	<input type="checkbox"/>	TFTP	<input type="checkbox"/>
Allow all outgoing connections		<input type="checkbox"/>	

Apply

Figure 9.8: Internet-to-DMZ Protocol Filters

Address Mapping

The Network Address Translation (NAT) service of Oxygen Multiservice Gateway 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)	Firewall	Internal (LAN)
--- IP Address ---	<input checked="" type="checkbox"/>	--- IP Address ---
--- IP Address ---	<input checked="" type="checkbox"/>	--- IP Address ---
--- IP Address ---	<input checked="" type="checkbox"/>	--- IP Address ---
--- IP Address ---	<input checked="" type="checkbox"/>	--- IP Address ---
--- IP Address ---	<input checked="" type="checkbox"/>	--- IP Address ---

Apply

Figure 9.9: NAT Static Address Mapping

In order to configure such a mapping:

1. Enter the **External (WAN)** IP address value. Alternatively, from the drop-down list, you can select a specific WAN connection or a specific Service. In this case, the IP address automatically assigned to the selected WAN connection(s) will be used for the *static address mapping*.
2. Specify the LAN host this mapping rule will apply to. Under the **Internal (LAN)** heading, enter the LAN IP address of the internal server. Note that, if the desired LAN server obtains its IP address from the Oxygen Multiservice Gateway through DHCP, you can select it from the drop-down list.
3. Check the **Firewall** option if IP traffic for the specific mapping should be controlled by the **Firewall** of the Oxygen Multiservice Gateway or if it will be freely forwarded.

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 Multiservice Gateway. You can access the following voice sub-menus:

- ***Phone Lines***
- ***Restrictions***
- ***Speed Dials***
- ***Black List***

Phone Lines

This configuration page allows the control of the phone lines of the Oxygen Multiservice Gateway. The list of phone lines includes 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*).

Phone Lines

Line 1 Line 2 Line 3 Line 4 Line 5 Line 6 Line 7 Line 8 Outgoing

Status: ☒ Enabled ☐ Disabled

Number:

Username:

Password:

Authname:

DTMF:

Force Caller-ID:

Incoming Calls

Significant digits:

Default ☒ ☐ ☒

Apply

Figure 10.1: Phone Lines

For each phone line, select the corresponding tab and configure the relevant parameters.

In the case of **VoIP** service accounts, the line settings first of all require the selection of **Status** and corresponding **Server** from the drop-down list. Subsequently, you must insert the SIP credentials **Number**, **Username**, **Password** and **Authname** and the mode of transport of **DTMF** tones, with available options being *RFC 2833*, *Inband* and *SIP Info* (RFC 2976). Finally it is also possible to configure if the the **Caller-ID** will be transmitted as received from the local voice ports, or if it will be forced to the number of the line (**Force Caller-ID** drop-down list).

Having configured the line settings, the next step is the configuration of the way **Incoming Calls** are handled. The first option is to select the number of right-end digits to be retained for the internal numbering scheme. This is the number of **Significant Digits**. If, for example, this parameter is set to 3, when an incoming call is received for number 2101234500, the called number will be truncated to 500 and afterwards it will be routed to the internal voice interfaces. This is useful, especially in the case of ranges of consecutive numbers, which are usually directly converted to internal numbers through simple transformations. The final step for routing incoming calls, is to select to which internal voice interfaces

the call will be directed to. This is possible using the table of voice interfaces under the **Incoming Calls** section, by selecting every appropriate interface (e.g. FXS ports and/or ISDN-NT interfaces).



Note

The list of available options in the table of the **Incoming Calls** section, depends on the voice interfaces and optional functionality of the Oxygen Multiservice Gateway.

Phone Lines

Line 1 Line 2 Line 3 Line 4 Line 5 Line 6 Line 7 Line 8 Outgoing

Outgoing Calls

	FXS-1	FXS-2	All ISDN NT
1: Line 1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2: Line 2	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
3: Line 3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4: Line 4	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5: Line 5	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6: Line 6	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
7: Line 7	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
8: Line 8	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Internal Only	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Blocked	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Anonymous	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Figure 10.2: Phone Lines

Having performed the above configuration for each available phone line, the final step is the selection of the phone line / number used by each internal voice interface for placing outgoing calls. This is performed using the **Outgoing** tab of this page. When selecting this tab, a table of all available voice interfaces as well as phone lines / numbers appears. By selecting for each voice interface one of the available lines / numbers, the selected line / number is going to be used for outgoing calls. Two additional options are **Internal Only** for allowing only outgoing calls towards other local voice interfaces and **Blocked** for blocking all outgoing calls from the corresponding voice interface. Finally, it is possible to set the corresponding voice interface to **Anonymous**, hiding the Caller-ID in outgoing calls.

Click **Apply** after finishing, to apply changes.

Restrictions

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

Destination	Pattern	Status
Provider	#521*XXXX*XXXXXXXXXX	Allow
Provider	#XX#	Allow
Provider	#XX*	Allow
Provider	*#.	Allow
Provider	*#XX#	Allow
Provider	**XX#.	Allow
Provider	*031*XXXX*XXXX*XXXX	Allow
Provider	*31*	Allow
Provider	*521*XXXXXXXXXX	Allow
Provider	*XX#	Allow
Provider	*XX#.	Allow
Provider	*XX*	Allow
Provider	00XXXXXX.	Allow
Provider	2XXXXXXX	Allow
Provider	5XXXXXX.	Allow
Provider	6XXXXXXX	Allow
Provider	7XXXXXX.	Allow
Provider	807XXXX.	Allow
Provider	8XXXXXXX	Allow
Provider	9XXXXXXX	Allow
Provider	X.	Allow
PIN		

Apply

Figure 10.3: Call Restrictions

Single or whole categories of destination numbers are defined using a flexible pattern syntax. Classification of the destinations into categories is based on patterns, both default and custom. Patterns can consist of digits 0-9, X as a wildcard for any digit, ! as a wildcard for any number of digits, . as a wildcard for any number of digits (at least one) and square brackets defining ranges of digits. Examples of destination patterns are:

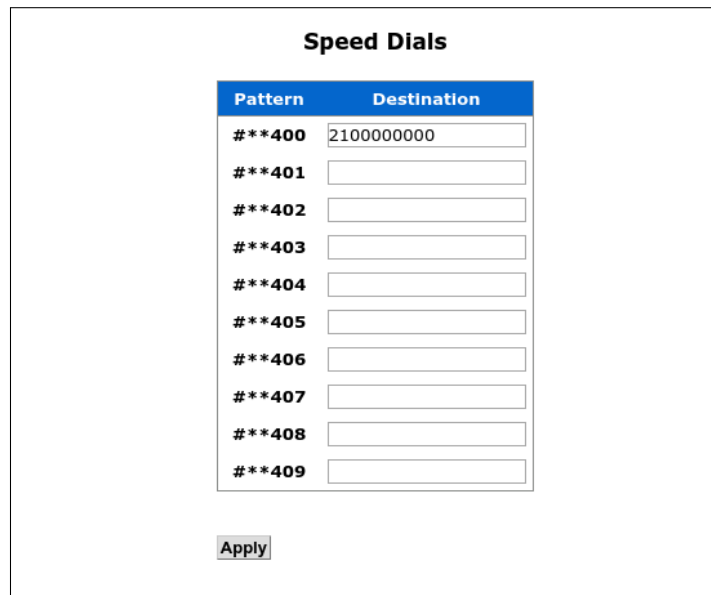
- **100** : the number 100
- **10X** : numbers 100 to 109
- **10!** : any number starting with 10 (including 10)

- **10.** : any number starting with 10 (at least 3 digits)
- **10[0-4]** : numbers 100 to 104

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 Multiservice Gateway. 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	2100000000
***401	
***402	
***403	
***404	
***405	
***406	
***407	
***408	
***409	

Apply

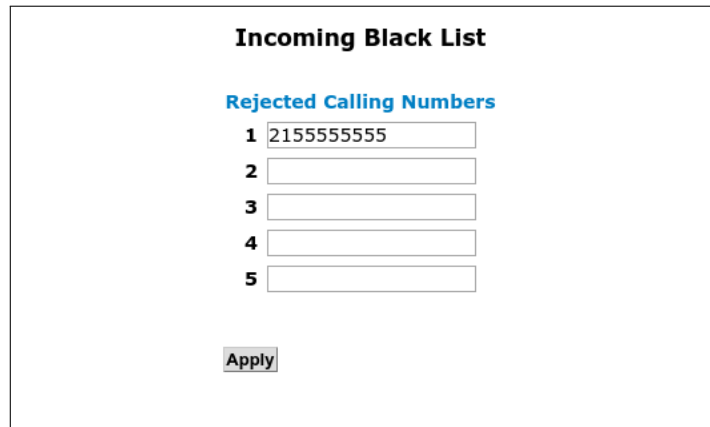
Figure 10.4: Speed Dials

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". Below the title is a heading "Rejected Calling Numbers" in blue. Under this heading, there are five numbered input fields. The first field, labeled "1", contains the number "2155555555". The other four fields, labeled "2", "3", "4", and "5", are empty. At the bottom of the form is a button labeled "Apply".

Figure 10.5: Black List 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

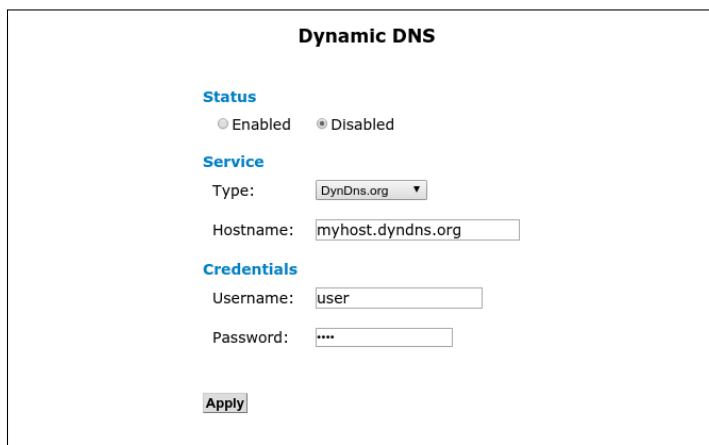
Advanced Menu

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

- ***Dynamic DNS***
- ***Date and Time***
- ***SSL VPN***
- ***GRE Tunnel***
- ***L2TP Tunnel***
- ***IPSec Tunnel***
- ***QoS Policy***
- ***File Sharing***
- ***Printing***

Dynamic DNS

The Dynamic DNS 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 Multiservice Gateway supports different Dynamic DNS service providers.



The screenshot shows a web interface titled "Dynamic DNS". It contains three sections: "Status" with radio buttons for "Enabled" and "Disabled" (where "Disabled" is selected); "Service" with a "Type" dropdown menu set to "DynDns.org" and a "Hostname" text field containing "myhost.dyndns.org"; and "Credentials" with a "Username" text field containing "user" and a "Password" text field with masked characters. An "Apply" button is located at the bottom left of the form.

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**.

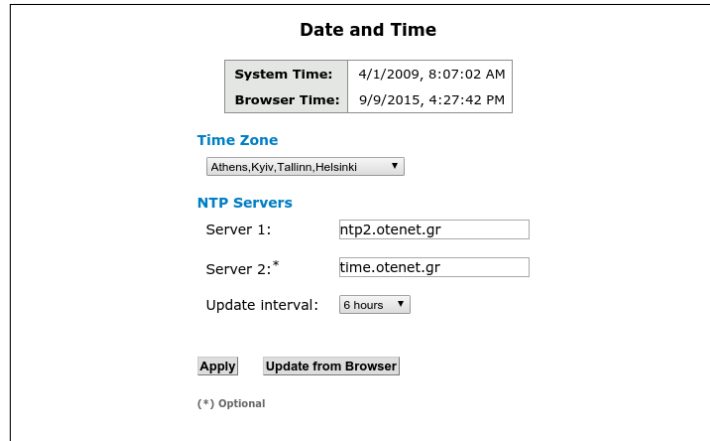


Note

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 Multiservice Gateway.

Date and Time

This sub-menu lets you configure the date and time values of the Oxygen Multiservice Gateway. Usually, this is performed using the embedded Simple Network Time Protocol (SNTP) client which allows the Oxygen Multiservice Gateway to contact a configured Network Time Protocol (NTP) server and obtain the current date and time values.



Date and Time

System Time:	4/1/2009, 8:07:02 AM
Browser Time:	9/9/2015, 4:27:42 PM

Time Zone

Athens, Kyiv, Tallinn, Helsinki ▼

NTP Servers

Server 1:

Server 2: *

Update Interval:

(*) Optional

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. Select the **Update Interval** between two successive update attempts.
5. Click **Apply**.

Alternatively, you may configure the date and time of the Oxygen Multiservice Gateway using the date and time values of your PC provided to the Oxygen Multiservice Gateway via your web browser. You may do so by clicking on **Update from Browser** button.

SSL VPN

This sub-menu lets you configure your Oxygen Multiservice Gateway 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 Multiservice Gateway, 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. At the top, there's a 'Service' button and a 'Disabled' button. Below this, the 'Status' section has radio buttons for 'Enabled' and 'Disabled', with '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 checkbox for 'Enable NAT', and a 'Service' dropdown menu set to 'Data'. There is an 'Apply' button below the 'VPN Tunnel' section. The 'Security' section has 'Current certificates' with 'View Info' and 'Download' buttons, and 'New certificates' with a 'Choose File' button and the text 'No file chosen'. An 'Upload' button is at the bottom of the 'Security' section.

Figure 11.3: 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. *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 F**. Please note that you must make the same selection for both the server and the client.

5. When using *Routed* type, select if **NAT** (Network Address Translation) is going to be enabled for LAN devices for traffic over the SSL VPN tunnel. In other words when *NAT* is enabled, 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 OpenVPN 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, as they are provided by an Oxygen OpenVPN server.

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 providing addressing information to connected clients.

Figure 11.4: 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. Optionally check **Isolate clients** to disable connectivity between the SSL VPN connected clients. Optionally select if logging should be recorded on external storage drive by checking **USB logging**.
7. 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 Multiservice Gateway.


If, on the other hand, you wish to prohibit further access to configured remote users, *Revoke* them

SSL VPN Users

User	Network	Pool	Validity	Action
tester	-	-	Mar 26 2029	 

Add New User

Username:

Validity: 

[\[Manage SSL VPN User Pools\]](#)

Figure 11.5: SSL VPN Users

by clicking on the corresponding icon  of **Action** column, in the list of the configured 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.

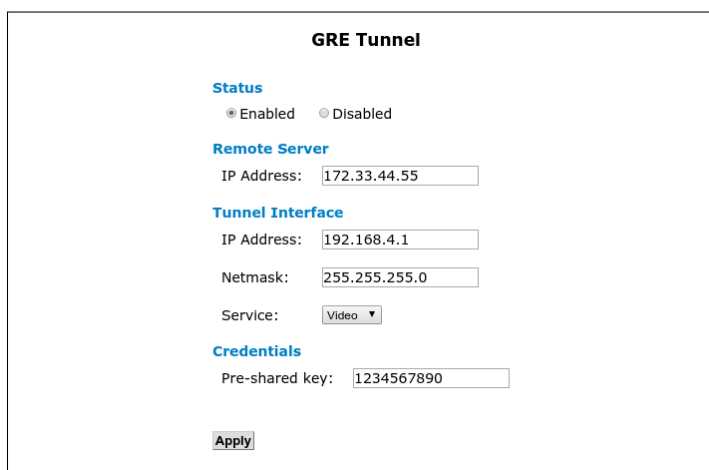


Note

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

GRE Tunnel

This sub-menu lets you configure a Generic Routing Encapsulation (GRE) Tunnel between your Oxygen Multiservice Gateway 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 the 'GRE Tunnel' configuration window. It has a title bar 'GRE Tunnel'. Below it, there are four sections: 'Status' with radio buttons for 'Enabled' (selected) and 'Disabled'; 'Remote Server' with a text field for 'IP Address' containing '172.33.44.55'; 'Tunnel Interface' with text fields for 'IP Address' (192.168.4.1) and 'Netmask' (255.255.255.0), and a dropdown menu for 'Service' set to 'Video'; and 'Credentials' with a text field for 'Pre-shared key' containing '1234567890'. At the bottom left is an 'Apply' button.

Figure 11.6: 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 Server** 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. Select the corresponding **Service** from the drop-down list. The internal firewall will allow forwarding of IP traffic between the **GRE tunnel** and the selected LAN Interface Group.
5. Optionally enter the appropriate numeric **Pre-shared key** value (the remote endpoint must use the same key value).
6. Click **Apply**.

L2TP Tunnel

This sub-menu allows the configuration of an L2TP (Layer-2 Tunneling Protocol) or L2TP/IPSec (Internet Protocol Security) -based VPN tunnel. L2TP tunnels, 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. Your Oxygen Multiservice Gateway can act either as a server or as a client for L2TP or L2TP/IPSec VPN tunnels.

L2TP Tunnel

L2TP	Stopped
IPSec	Stopped

Status

☐ Enabled
 ☒ Disabled

Operation

Type: L2TP ▼

Mode: Client ▼

Remote Server

Host/IP:

Credentials

L2TP Pre-shared key:*

L2TP Username:*

L2TP Password:*

(*) Optional

Apply

Figure 11.7: L2TP VPN Tunnel - Client Mode

To configure the L2TP tunnel, first select *Enabled* as **Status**. Then, use the **Type** drop-down list to select the type of L2TP VPN. Available options are *L2TP* and *L2TP/IPSec* for L2TP-only or L2TP over IPSec operation respectively. Finally, select between *Server* and *Client* **Mode** of operation.

Once the type and mode of operation of L2TP VPN has been selected, the relevant parameters appear on the web configuration page.

Client Mode

The main required parameter for L2TP client operation, is the public **Hostname** or **IP Address** of the **Remote Server**. For tunnel authorization purposes, a **Pre-shared key**, **Username** and **Password** combination must also be supplied (with same values configured on the remote server).

If IPSec is used for the encryption of the L2TP tunnel (*L2TP/IPSec type*), some additional parameters, related to IPSec operation, appear under the **IPSec Options** heading. These include the **NAT-T** checkbox

L2TP Tunnel

Status

L2TP Stopped
IPsec Stopped

Enabled Disabled

Operation

Type: L2TP/IPsec ▼

Mode: Server ▼

IPsec Options

NAT-T: ☐

IKE Phase 1: 3des ▼ md5 ▼ 1024 ▼

IKE Phase 2: 3des ▼ md5 ▼

PFS option: ☐

Aggressive mode: ☒

Key lifetime: * (sec)

VPN Tunnel

Network: 10.8.101.0

Netmask: 255.255.255.0

Service: Data ▼

Credentials

IPsec Pre-shared key:

L2TP Pre-shared key: *

PPP authentication: Inactive ▼

PPP users: Manage

(*) optional

Apply

Figure 11.8: L2TP/IPsec Tunnel - Server Mode

if VPN traffic passes through NAT, **IKE Phase 1** and **IKE Phase 2** algorithms, **PFS option** and **Aggressive mode**. Finally, through **Key lifetime**, it possible to specify the lifetime of the IPsec tunnel key.

Server Mode

In the case of **Server** mode of operation, the main parameters used for the operation of the tunnel are the same like in the client mode. The main difference is that, insted of the **Remote Server** parameter, this time an IP address pool must be configured for the **VPN Tunnel**. This is performed using the **Network** and **Netmask** parameters, whereas **Service** is the LAN service, for which access through the VPN is allowed.

Finally, the list of **PPP Users** along with the **PPP authentication** method must be configured. In order to manage the list of **PPP Users**, press on the **Manage** button.

In order to add a new PPP user, enter the **Username** and corresponding **Password** values and click on **Save**. The user will be added to the list of **PPP Users**. If you want to revoke a user click on its **✗** icon from the **Action** column.

PPP Users

User	Action
No Entries	

Add New User

Username:

Password:

Save

Figure 11.9: L2TP PPP Users

IPSec Tunnel

This sub-menu allows the configuration of an IPSec-based VPN tunnel. IPSec is a protocol suite for securing IP communications by authenticating and encrypting each IP packet of a data stream. IPSec wraps the original packet, encrypts it, adds a new IP header and sends it to the other side of the VPN tunnel. Your Oxygen Multiservice Gateway can act as a client for an IPSec VPN tunnel connecting to an IPSec VPN server or another IPSec VPN client.

IPSec Tunnel

Status

☐ Enabled ☒ Disabled

Options

NAT-T:

☐

IKE Phase 1:

3des

md5

1024

IKE Phase 2:

3des

md5

PFS option:

☐

Aggressive mode:

☒

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"/>

Apply

Figure 11.10: IPSec Tunnel

To configure the IPSec tunnel, first select *Enabled* as **Status** and enter the **IP Address** of the **Remote Server** (or Remote peer).

Parameters related to IPSec operation, appear under the **Options** heading. These include the **NAT-T** checkbox if VPN traffic passes through NAT, **IKE Phase 1** and **IKE Phase 2** algorithms, **PFS option** and **Aggressive mode**. Finally, through **Key lifetime**, it is possible to specify the lifetime of the IPSec tunnel key.

For tunnel authorization purposes, a **Pre-shared key** value must be supplied (with same value configured on the remote server).

Finally, the pairs of **Local** and **Remote Subnets** must be configured. The IPSec VPN tunnel allows

traffic to pass through only if it belongs to one of the defined *Local* and *Remote Subnet* pairs.

QoS Policy

This sub-menu lets you configure the Quality of Service (QoS) policy of the Oxygen Multiservice Gateway. This policy consists of the classification of IP traffic into **Priority Classes**, the **DSCP Marking** of the IP packets and the use of **CoS Marking** on Ethernet frames with 802.1Q VLAN tag.

Policy Classes

With **Policy Classes**, IP traffic is selectively distributed 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 already configured **QoS classes** for IP traffic.

QoS Policy

Priority Classes

Name	Priority	Connection	Action
No Entries			





Add New

IP DSCP Marking

Application	Port	Source	Destination	DSCP	Action
No Entries					



Add New

VLAN CoS Marking

Connection	VLAN ID	Incoming	Outgoing	Action	
VDSL_IPTV	836	-	3		
VDSL_PPPOE	240	-	"5:5 2:4"		

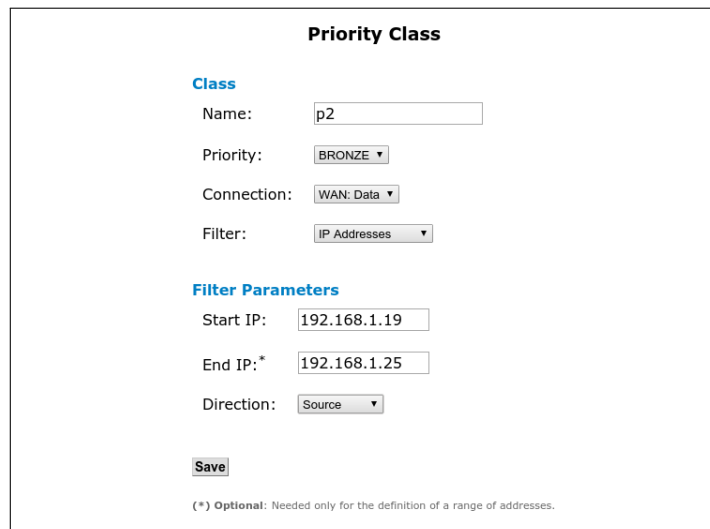
[QoS Parameters]

Figure 11.11: 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:

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 WAN **Connection** from the drop-down list, for which this class applies.



Priority Class

Class

Name:

Priority:

Connection:

Filter:

Filter Parameters

Start IP:

End IP:

Direction:

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

Figure 11.12: New QoS Priority Class

4. Select the desired traffic classification method under the **Filter** parameter. The Oxygen Multiservice Gateway offers the following different methods for the classification of IP Traffic:

- I *DiffServ Value*: Based on the TOS/DSCP value of the IP header of the packets. All packets with a CoS/DSCP value equal to the one configured in the **DSCP** field, will belong to this **Priority Class**.
- II *IP Addresses*: Based on the source or destination IP address of the IP packets. Traffic with IP address belong to the range of IP addresses defined using the **Start IP** and **End IP** parameters, will belong to this **Priority Class**.
- III *Connection Bytes*: Traffic streams with data volume that exceeds the **Begin after** parameter will belong to this **Priority Class**, until they exceed the (optionally defined) **Stop after** parameter.
- IV *Application/LAN service*: Based on the application or service the IP packets belong to. Traffic part of a specific Service of application belong to this **Priority Class**. This application 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.
- V *IP Packet size*: Based on the size of the IP packet being transferred. You have to set a *payload* and optionally a maximum *To* value.

5. Click **Save**.

IP DSCP Marking

Under **IP DSCP Marking**, it is possible to manage the QoS DSCP values for selected streams of IP traffic. To configure a new **DSCP Marking** rule press on **Add new** below the **DSCP Marking** table and the **QoS Marking Rule** page appears:

1. Select the **DSCP** value from the drop-down list.
2. Select the **Source** connection and optionally enter a host IP address or subnet. Leave blank to allow any from the corresponding **Source** port.
3. Similarly configure the **Destination** values.
4. Set the **Application** parameters *Direction*, *Protocol*, *Type* and *Port* range.
5. Click **Save**.

VLAN CoS Marking

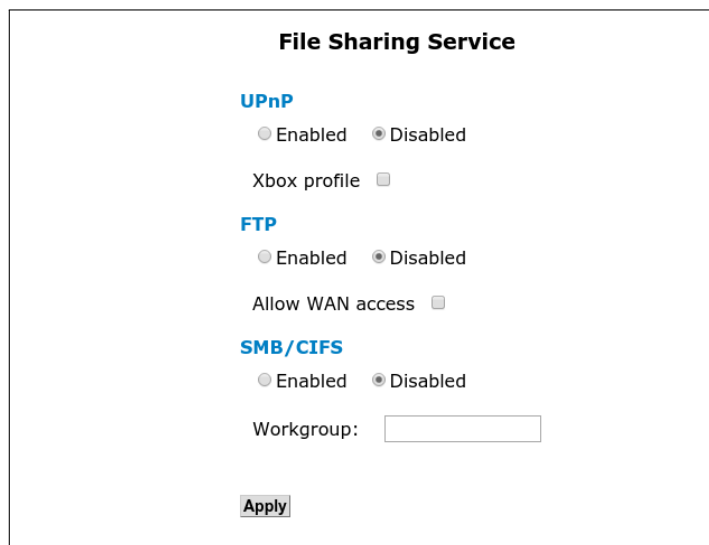
Under **VLAN CoS Marking**, it is possible to set and manage the QoS CoS values (802.1Q priority bits) for managing and outgoing 802.1Q VLAN Ethernet frames.

QoS parameters

Finally, it is also possible to apply a bandwidth limit per interface type. Clicking on **QoS parameters** you are presented with the option to enter bandwidth limitation values for corresponding interfaces. Setting the value to 0 or empty will use the default sync values.

File Sharing

When your Oxygen Multiservice Gateway 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.



File Sharing Service

UPnP

☐ Enabled ☒ Disabled

Xbox profile ☐

FTP

☐ Enabled ☒ Disabled

Allow WAN access ☐

SMB/CIFS

☐ Enabled ☒ Disabled

Workgroup:


Apply

Figure 11.13: File Sharing Service

To this end, 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 optional activation of a special Xbox profile), *FTP* server (with the option to **Allow WAN access**) 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 Multiservice Gateway, 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 Multiservice Gateway 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.

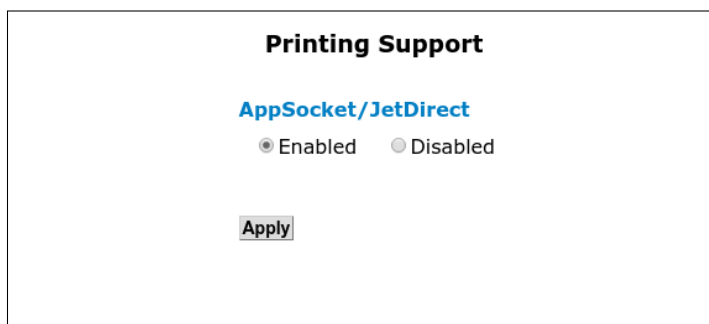


Figure 11.14: USB Printer Support

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 189 for more information about the available options and the configuration process for the LAN PCs.



Note

Note that some USB printers may not be supporting this functionality

12

System Menu

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

- *Green Operation*
- *SNMP*
- *Syslog*
- *Backup / Restore*
- *Firmware Upgrade*
- *Remote Admin*
- *Change Password*
- *Device Restart*

Green Operation

This sub-menu let you configure the operation of the Oxygen Multiservice Gateway, when it is operating in battery mode (*optional feature*).

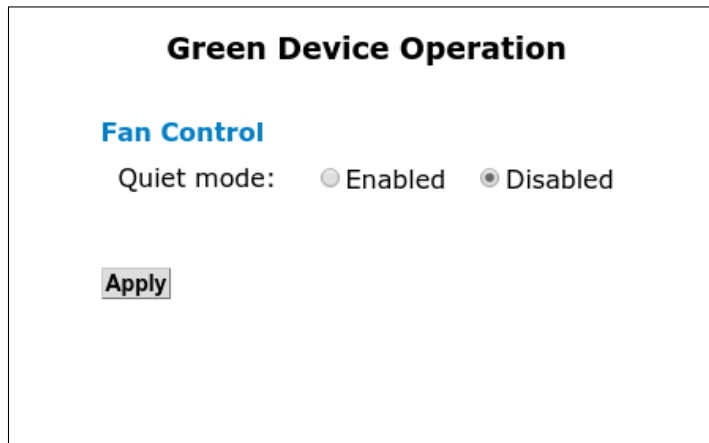


Figure 12.1: Green Operation

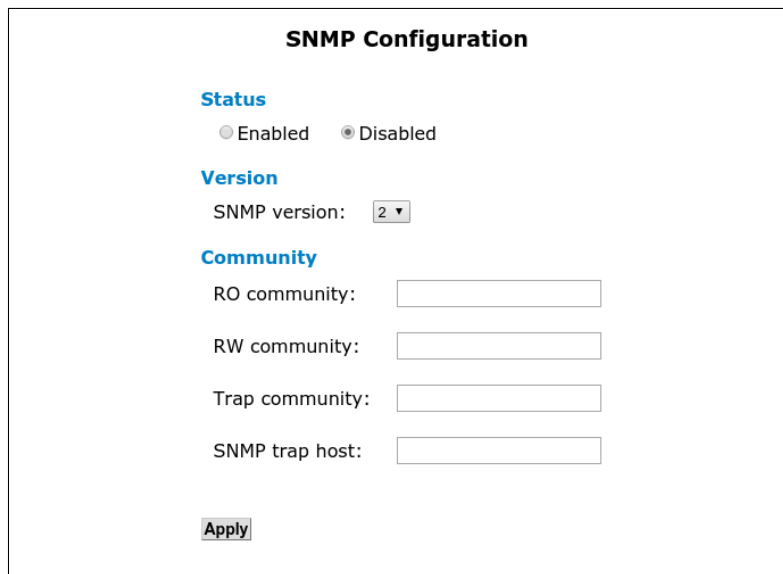
Available options are:

- **Wireless:** select if WiFi operation will be active or automatically disabled when the device operates in battery mode in order to prolong battery operation time (WiFi-enabled devices).
- **On Active Call** select if the number of concurrent calls will be limited to one, in order to prolong battery operation time.

In selected models with internal cooling fan, it is also possible to enable or disable the quiet mode of operation.

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 Multiservice Gateway.



The image shows a web-based configuration form titled "SNMP Configuration". It is organized into four sections: "Status", "Version", "Community", and an "Apply" button at the bottom. The "Status" section has two radio buttons: "Enabled" and "Disabled", with "Disabled" being selected. The "Version" section has a label "SNMP version:" followed by a dropdown menu showing "2". The "Community" section has four labels with corresponding text input fields: "RO community:", "RW community:", "Trap community:", and "SNMP trap host:". The "Apply" button is a small rectangular button at the bottom left of the form.

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**) and Read Write (**RW**) **community** strings.
4. Optionally select a **Trap Community** and **Host**.
5. Click **Apply**.

Syslog

Syslog is the logging service providing information about the operation of the Oxygen Multiservice Gateway.

To configure the Syslog service:

1. Select *Enabled* or *Disabled* under **Status** to enable or disable the service.
2. Select the desired **Log level** from the drop-down list. Only events into the selected above log-levels will be logged.
3. Optionally check **Store in USB** to store the syslog to an external storage drive.
4. Click **Apply**.

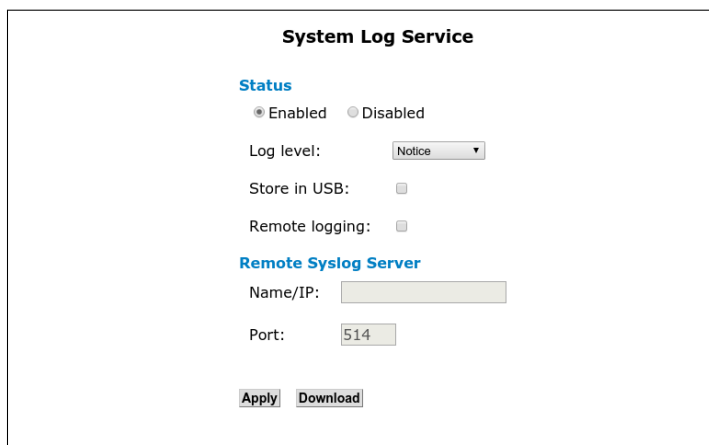


Figure 12.3: Syslog Configuration

Using the Web interface of Oxygen Multiservice Gateway, log messages can be viewed in the **System Log** page of the **Status** configuration menu (see page 152).

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).

To download the current log locally to your device click on **Download**.

Backup / Restore

This sub-menu allows you to save the current configuration of the Oxygen Multiservice Gateway as a backup on a PC, and optionally restore it at a later time.

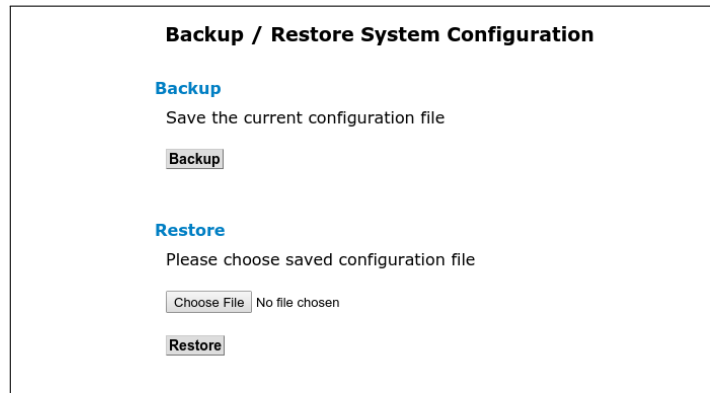


Figure 12.4: Configuration Backup/Restore

Backup Configuration

To save the currently above configuration to a backup file:

1. Click **Backup**.

A message window opens prompting you to save the file:

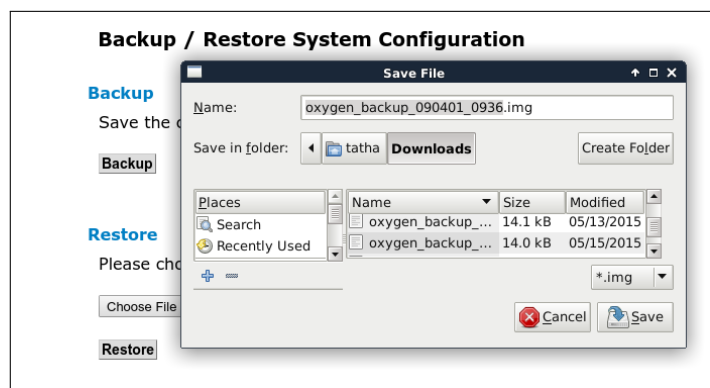
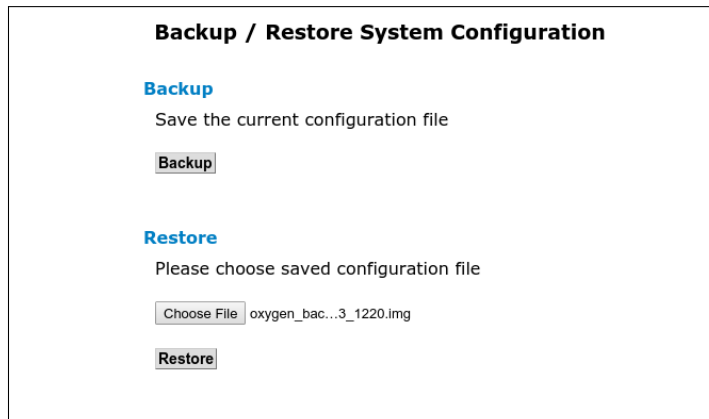


Figure 12.5: Backup Configuration

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

Restore Configuration

To restore a previously saved configuration:



The screenshot shows a dialog box titled "Backup / Restore System Configuration". It has two sections: "Backup" and "Restore". The "Backup" section has the text "Save the current configuration file" and a "Backup" button. The "Restore" section has the text "Please choose saved configuration file", a "Choose File" button, and a text field containing "oxygen_bac...3_1220.img". Below the text field is a "Restore" button.

Figure 12.6: Restore Configuration

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



WARNING

The Oxygen Multiservice Gateway will be automatically restarted after the end of the configuration-restore process.

Firmware Upgrade

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

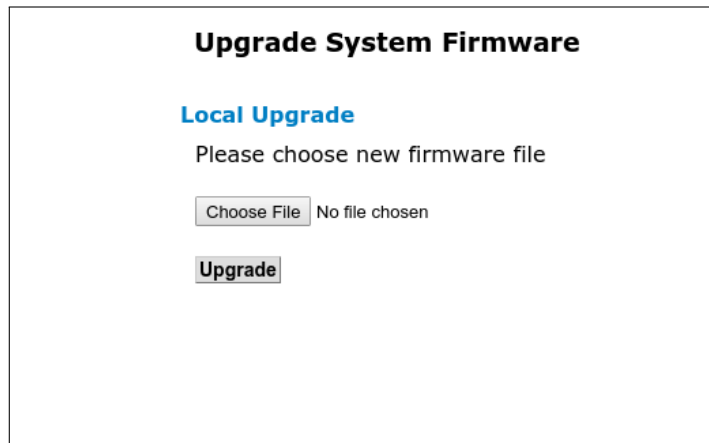


Figure 12.7: Local Firmware Upgrade

To locally upgrade the firmware:

1. Click **Browse** or **Choose File** 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 Multiservice Gateway.

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 the latest firmware release. If a newer compared to the one stored on your device 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 Multiservice Gateway will be automatically restarted after the end of the firmware-upgrade process.

Upgrade System Firmware

Automatic Upgrade

Check for new firmware release

Local Upgrade

Please choose new firmware file

No file chosen

Figure 12.8: Automatic Firmware Upgrade

Remote Admin

This sub-menu controls remote administration access to the Oxygen Multiservice Gateway. This may help the IT support staff of your Service Provider to configure the device remotely.

Remote Administration

Status	Active (telnet-http-https)
Expiration	Never

New Key

Figure 12.9: Remote Administration

Change Password

This sub-menu lets you change the password for the active user profiles of the Oxygen Multiservice Gateway.



Change System Password

Username:

Current password:

New password:

Verify:

Figure 12.10: Password Configuration

To change the password for a user:

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 Multiservice Gateway.

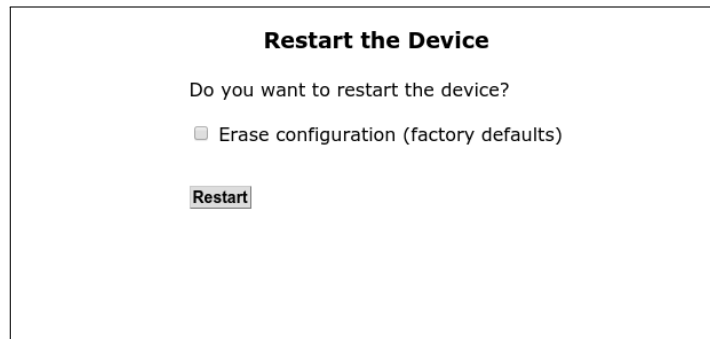


Figure 12.11: Device Reboot

To reboot the Oxygen Multiservice Gateway:

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:

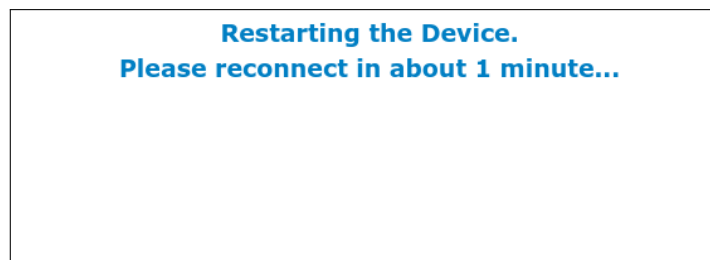


Figure 12.12: Reboot Status

13

Status Menu

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

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

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

About

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

Device Status	
Model	Oxygen Gateway Router
Operating System	Gennet/Linux
Revision	-
Serial	000000000000
MAC Address	001D1CED0018
Uptime	6h 8m 16s
Connected	6h 5m 9s
Firmware Details	
Version	OTE01_5.3.2
Type	HDV24201.N2UM
Build	fw2015080614
DSL Firmware	VTU-R:10.21.0.100IKF7185
Last Upgrade	Successful

Figure 13.1: Device Status

System Log

The **System Log** page provides useful information about the operation of your Oxygen Multiservice Gateway.

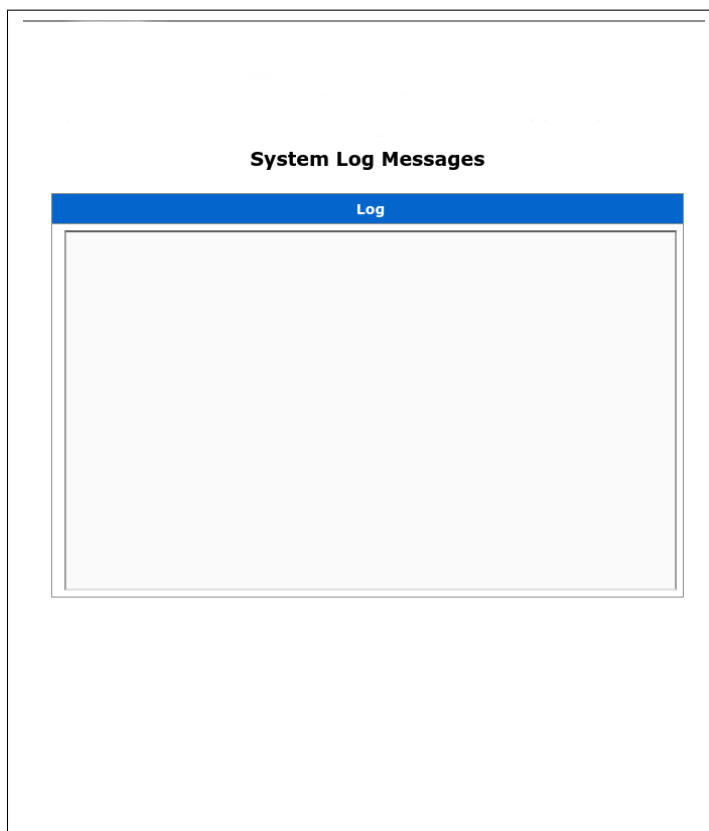


Figure 13.2: System Log

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 140).

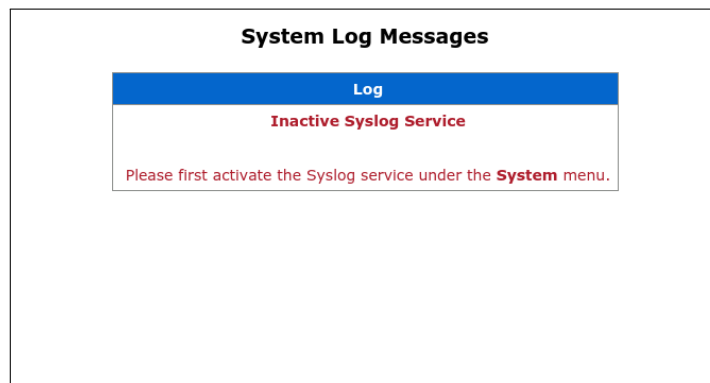





Figure 13.3: System Log Notification

Interfaces

This page displays information about the link, speed and duplex 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.

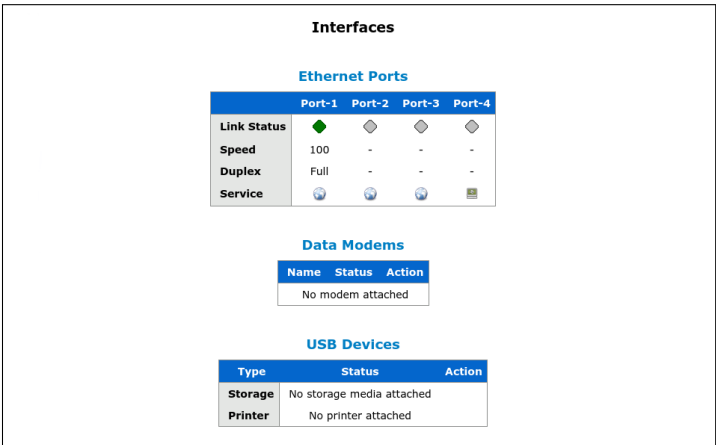






Figure 13.4: Ethernet Port Status

It also shows information about the status of connected **Data Modems** and **USB Devices** (Storage disks or Printers) on the USB Host port (*optional feature*) of the Oxygen Multiservice Gateway.

When a data modem is detected, you can get detailed information about its status by clicking on the *Info* icon  which appears in the **Action** column. When on the other hand, an external storage device is connected, the storage link appears. Follow the  icon 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 Multiservice Gateway 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 Multiservice Gateway.

DSL Line Info		
State	Showtime	
Modulation	ADSL2+	
Type	ANNEX A	
DSLAM	GSPN	
Overall Failures	0	
ATM Cell Drop Count	-	
Received Frames	1,325,068	
Transmitted Frames	1,325,067	
Rate	Receive	Transmit
Bit Rate	24,072,000	997,000
Cell Rate	60,028	2,764
Signal	Local	Remote
Loss of Signal	0	0
Signal to Noise Ratio	6.0 dB	6.50 dB
Line Attenuation	1.9 dB	1.30 dB
Transmit Power	12.2 dBm	0.0 dBm
DSL Errors	Local	Remote
Severe (SEF)	0	0
Corrected (FEC)	391,574	0
Checksum (CRC)	2,634	607,977,544
Header (HEC)	63,121	0
Retrain Clear Counters Clear Logs		

Figure 13.5: 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. Clicking on the **Clear Counters** button resets the DSL line statistics to 0.

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 Multiservice Gateway (*WiFi-enabled devices only*).

Wireless Network				
Connected Clients				
IP Address	Name	MAC Address	Status	Action
No Entries				
Access Points In Range				
SSID	MAC Address	Channel	Encryption	Signal (%)
AGSuite1	00:90:AE:18	1	WPA2/WPA	94
Oxygen-00000	00:1D:1C:F3	5	WPA	94
Random21123	00:1D:1C:FA	11	WPA2	94
Stavros-fax	00:1D:1C:F3	11	Off	93
CYTA5A03	00:1D:1C:F8	6	WPA2	92
Random	22:1D:1C:F8	6	Off	92
Oxygen-Voice-T	42:1D:1C:FA	1	WPA	90
Oxygen-Broadband-T	00:1D:1C:FA	1	WPA	90
fco	A0:F3:C1:C9	2	WPA2/WPA	90
Oxygen-Visit-T	32:1D:1C:FA	1	WPA	89
Amundi_Wi-Fi	0A:18:D6:93	1	WPA2/WPA	24
HP-Print-b7-LaserJet 400 color	10:08:B1:B1	6	Off	24
DIRECT-GSM2020 Series	32:CD:A7:25	1	WPA2	21
OTEd22e10	A4:7E:39:D2	10	WPA	18
Random	9C:97:26:E2	1	WPA2/WPA	18
Life	00:14:C1:45	11	WPA2/WPA	18
conn-x8b0d50	14:60:80:8B	3	WPA	15
Random	38:22:9D:1C	11	WPA2/WPA	15
OTE WiFi Fon	A4:7E:39:D2	10	Off	15
AEGIS ISA	DC:02:8E:5B	6	WPA2/WPA	11

Figure 13.6: 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				
Calling	Called	Peers	Codec	Status
No Entries				
Supplementary Services				
Service	Code	FXS-1	FXS-2	
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 13.7: Voice Calls and Services

To activate for example a supplementary service such as **Call Waiting** you should press *****43#** and in order to deactivate it ****#43#**. In the case of the **Call Forward** supplementary service, when activating the service the target number must also be entered. For example, in order to activate **Call Forward Unconditional (CFU)**:

- press *****21#** on your telephone keypad
- enter the number you want to forward calls to
- then press **#**

The table below lists the specific codes for the most common supplementary 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:

Service	Code
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

Table 13.1: Voice Supplementary Service Codes

**Note**

You can **activate** any other supplementary service using the sequence **##Code#**, **deactivate** using **##Code#** or **check** the current service status using **##Code#**.

Supplementary Service Codes	
Service	Code
Reset all settings	###
Disable all call forwards	##002#
Redial last called number	*3131
Dial last caller	*3232
Speed dial	##4XX
Read speed dial number	*#4XX
Blind transfer	*#9
Attended transfer	**9
Park call	*#72
Park calls on	701-720
Calling Line Identity Restriction (per call)	##31*XXX.
Calling Line Identity Presentation (per call)	##31*XXX.

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

Figure 13.8: Service Codes

Call Details

This page displays information about voice call records.

Call Details

Last Numbers per Line

Incoming	Outgoing
No Entries	

Last 10 Calls

Source	Destination	Start Time	Duration
No Entries			

Figure 13.9: Call Records

Specifically, it displays the total call duration for **Local** (between the local extensions of the Oxygen Multiservice Gateway), **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 Multiservice Gateway;

ISDN Interfaces					
	Mode	Blocked	Link (L1/L2)	Errors	Active
BRI-1	NT-PTMP		/	-	-
Sync port					

Established Channels				
Calling	Called	Status	Direction	B-channel
No Entries				



Figure 13.10: ISDN Interfaces

For each ISDN interface, it is possible to see the **Status**, the **Mode** of operation (*Terminal (TE)* vs *Network (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 **Errors** and **Active** B-channels.

In order to debug the ISDN interfaces select the available **Debug Capture Interface** from the drop-down list and click on the **Start** button. Click on **Stop** to stop the capturing and download the log locally to your device. Use a program like Wireshark (<http://www.wireshark.org/>) in order to open and analyze the file.

Firewall

This page displays a list of the active firewall rules.

Firewall Information					
Statically Forwarded Ports					
	Interface	Port	Source	Destination	Packets
1	PPP: 0	TCP 80	ALL	192.168.1.52 (80)	0
UPnP/NAT-PMP Forwarded Ports					
	Application	Port	Source	Destination	
No Entries					
Filtered IP Traffic					
	Source	Destination	Filter	Packets	
IPv4 filters					
1	LAN: data 192.168.1.75	PPP: 0 TCP 80		0	
2	PPP: 0 TCP 80	LAN: data 192.168.1.75		0	
IPv6 filters					
No Entries					




 Drop
  Reject
  Accept

Figure 13.11: 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 100).
- **UPnP/NAT-PMP Forwarded Ports:** which contains ports forwarded automatically through the corresponding protocols. (see section **UPnP / NAT-PMP** on page 102).
- **Filtered IP Traffic:** which displays the list of IP filtering rules. (see section **IP Filters** on page 103).

Clients

This page provides a list of all clients connected to the Oxygen Multiservice Gateway.




Connected Clients						
Interface	IP	MAC Address	Name	Status	Port	Action
Ethernet	192.168.1.74	00:19:99:49:42:f4	CLIENT PC		Port-1	

Figure 13.12: Connected Clients

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


Information for 192.168.1.74	
IP Address	192.168.1.74
Interface	LAN-2
MAC Address	00:19:99:49:42:f4
DHCP Identifier	-
Ethernet Port	100/Full Duplex
Service	
State	Active

Figure 13.13: Clients Info

VPN Service

This page displays information about the **SSL VPN** and/or the **L2TP** and/or **IPSec** VPN services running on the Oxygen Multiservice Gateway (*optional feature*).

VPN Service

SSL VPN

Service

Running

ID	Name	Tunnel IP	Public IP
No Entries			

L2TP

L2TP

Stopped

IPSec

Stopped

ID	Tunnel IP	Public IP
No Entries		

IPSec

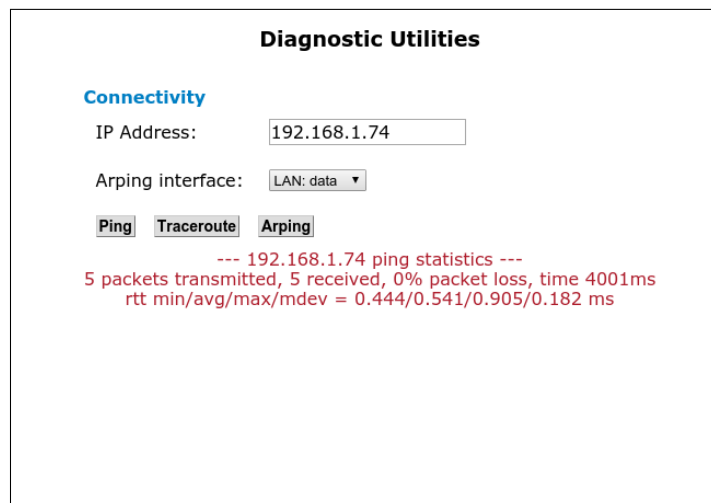
Source	Destination	Status	Bytes
No Entries			

Figure 13.14: VPN Service Information

For each VPN service, the current status of the service as well as details about connected VPN peers is displayed.

Diagnostics

This page provides you with an option to troubleshoot IP connectivity from your Oxygen Multiservice Gateway. You can perform a **Ping** test to check plain end-to-end connectivity, a **Traceroute** test in order to identify also the intervening nodes or **Arping** to check connectivity using ARP request method.



The screenshot shows a web interface titled "Diagnostic Utilities". Under the "Connectivity" section, there is a form with the following fields and controls:

- IP Address:** A text input field containing "192.168.1.74".
- Arping interface:** A dropdown menu showing "LAN: data" with a downward arrow.
- Buttons:** Three buttons labeled "Ping", "Traceroute", and "Arping". The "Ping" button is highlighted.
- Output:** Below the buttons, the following text is displayed in red:

```
--- 192.168.1.74 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4001ms  
rtt min/avg/max/mdev = 0.444/0.541/0.905/0.182 ms
```

Figure 13.15: Troubleshooting

To perform a connectivity test:

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

Healthcheck

This page displays health information about the status and connectivity of the Oxygen Multiservice Gateway.

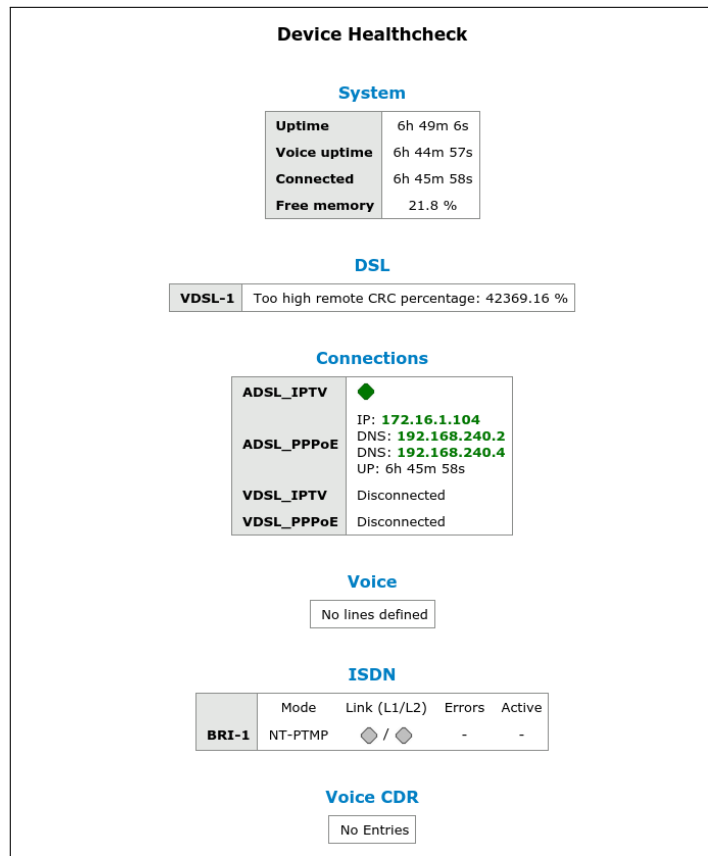


Figure 13.16: Healthcheck Information

Displayed information includes (model and service dependant):

- System uptime and memory status
- Broadband line status
- WAN connection status
- Voice lines status
- ISDN interfaces status (optional features)
- Latest voice calls

Net Statistics

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

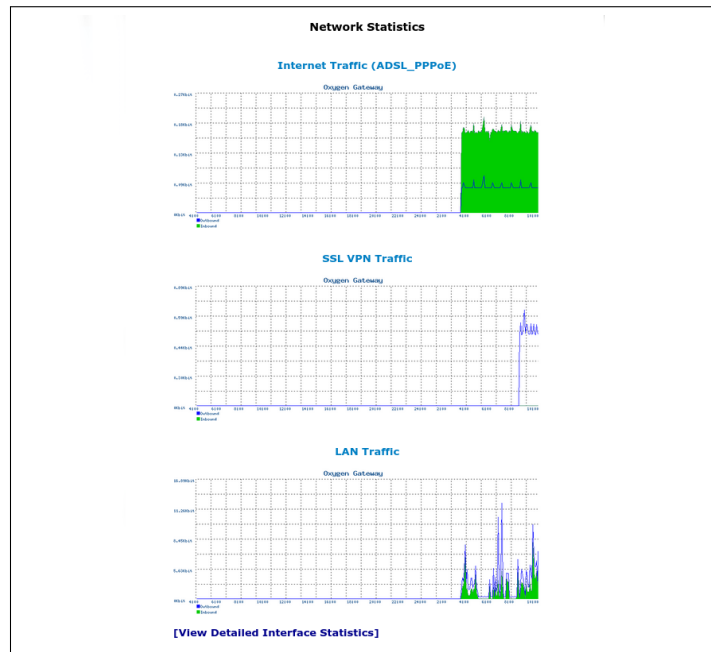


Figure 13.17: Network Statistics

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

Additionally, by clicking on the **View Detailed Interface Statistics** link, a new page appears with a list of all WAN and LAN IP interfaces, their status and RX/TX traffic counters.

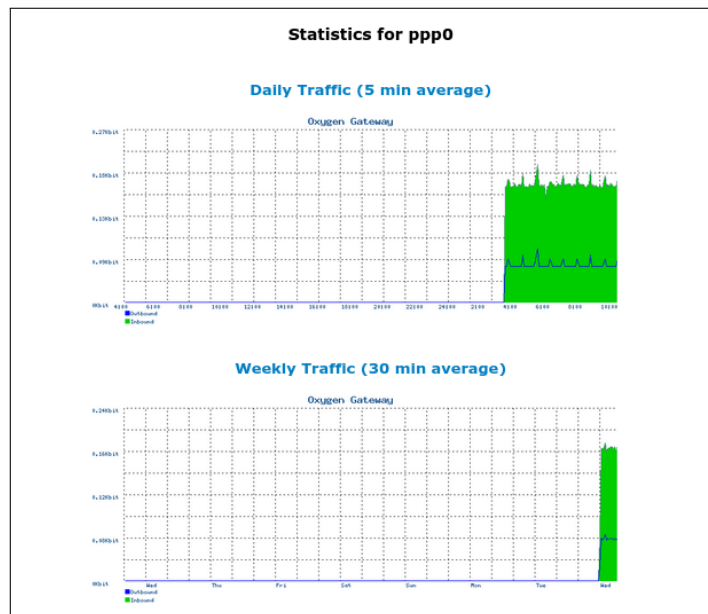


Figure 13.18: Detailed Network Statistics

IP Interface Statistics

Connections

Connection	Status	Uptime	Interface	Packets (Rx/Tx)	Errors (Rx/Tx)
ADSL_IPTV	●	-	PVC: 0-8/36	582 / 12,356	0 / 0
ADSL_PPPE	●	6h 51m 51s	PPP: 0	6,998 / 2,528	0 / 0
VDSL_IPTV	●	-	-	- / -	- / -
VDSL_PPPE	●	-	-	- / -	- / -

Interfaces

Interface	Status	Packets (Rx/Tx)	Errors (Rx/Tx)
LAN: data	●	20,422 / 18,382	0 / 0
LAN: dmz	●	0 / 5	0 / 0
LAN: ssid2	●	0 / 4	0 / 0
LAN: video	●	575 / 4	0 / 0
LAN: voip	●	0 / 5	0 / 0
Switch	●	20,418 / 43,839	0 / 0
ETH: 1	●	0 / 0	0 / 0
ETH: data	●	20,418 / 30,815	0 / 0
ETH: dmz	●	0 / 0	0 / 0
ETH: ssid2	●	0 / 0	0 / 0
ETH: ssid3	●	0 / 0	0 / 0
ETH: ssid4	●	0 / 0	0 / 0
ETH: ssid5	●	0 / 0	0 / 0
ETH: ssid6	●	0 / 0	0 / 0
ETH: ssid7	●	0 / 0	0 / 0
ETH: ssid8	●	0 / 0	0 / 0
ETH: video	●	0 / 13,016	0 / 0
ETH: voip	●	0 / 0	0 / 0
GRE: 0	●	0 / 0	0 / 0
IPv6Tun: 0	●	0 / 0	0 / 0
SSL VPN	●	0 / 4,729	0 / 0
WiFi-1	●	3 / 17,043	0 / 0
WiFi-2	●	0 / 16,941	0 / 0

Figure 13.19: IP Interface Statistics

IP Network

This sub-menu displays the list of active IP Interfaces on the Oxygen Multiservice Gateway, 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			
<div>IPv4 IPv6</div>			
Interfaces			
Interface	IP Address	MAC Address	Status
LAN: data	192.168.1.1/24	00:1d:1c:ed:00:18	●
LAN: dmz	10.10.10.1/24	16:72:ad:47:c1:a0	●
LAN: ssid2	-	02:1d:1c:f3:5b:9a	●
LAN: video	-	00:1d:1c:fd:00:1c	●
LAN: voip	-	7e:29:fd:cf:34:a6	●
Switch	-	00:1d:1c:ed:00:18	●
ETH: 1	-	00:1d:1c:ed:00:19	●
ETH: data	-	00:1d:1c:ed:00:18	●
ETH: dmz	-	00:1d:1c:ed:00:18	●
ETH: ssid2	-	00:1d:1c:ed:00:18	●
ETH: ssid3	-	00:1d:1c:ed:00:18	●
ETH: ssid4	-	00:1d:1c:ed:00:18	●
ETH: ssid5	-	00:1d:1c:ed:00:18	●
ETH: ssid6	-	00:1d:1c:ed:00:18	●
ETH: ssid7	-	00:1d:1c:ed:00:18	●
ETH: ssid8	-	00:1d:1c:ed:00:18	●
ETH: video	-	00:1d:1c:ed:00:18	●
ETH: voip	-	00:1d:1c:ed:00:18	●
WAN-Eth	-	00:1d:1c:ed:00:18	●
GRE: 0	-	-	●
IPv6Tun: 0	-	-	●
PPP: 0	172.16.1.104	-	●
SSL VPN	-	d2:0f:35:17:d5:da	●
PVC: 0-8/35	-	00:1d:1c:ed:00:1c	●
PVC: 0-8/36	-	00:1d:1c:fd:00:1c	●
VDSL: 0	-	00:1d:1c:ed:00:1c	●
WIFI-1	-	00:1d:1c:f3:5b:9a	●
WIFI-2	-	02:1d:1c:f3:5b:9a	●

MAC Address Table			
IP Address	MAC Address	Interface	Status
192.168.1.74	00:19:99:40:42:f4	LAN: data	●

Routing Table		
Network	Gateway	Interface
10.10.10.0/24	-	LAN: dmz
192.168.1.0/24	-	LAN: data
192.168.100.0	-	PPP: 0
192.168.240.0	-	PPP: 0
192.168.240.0/27	-	PPP: 0
192.168.240.1	-	PPP: 0
239.0.0.0/8	-	LAN: data
default	192.168.240.1	PPP: 0

Figure 13.20: 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	Bytes
www	TCP	192.168.1.74:56110	192.168.1.1:80	4040 / 1709
domain	UDP	127.0.0.1:35419	127.0.0.1:53	102 / 102
www	TCP	192.168.1.74:56137	192.168.1.1:80	2188 / 965
www	TCP	192.168.1.74:56114	192.168.1.1:80	2799 / 1219
domain	UDP	127.0.0.1:44512	127.0.0.1:53	51 / 51
www	TCP	192.168.1.74:56144	192.168.1.1:80	742 / 360
www	TCP	192.168.1.74:56109	192.168.1.1:80	4678 / 1954
domain	UDP	127.0.0.1:55737	127.0.0.1:53	51 / 51
domain	UDP	127.0.0.1:41974	127.0.0.1:53	51 / 51
domain	UDP	127.0.0.1:45866	127.0.0.1:53	51 / 51
domain	UDP	127.0.0.1:52365	127.0.0.1:53	51 / 51
domain	UDP	127.0.0.1:50215	127.0.0.1:53	102 / 102
domain	UDP	127.0.0.1:40073	127.0.0.1:53	51 / 51
domain	UDP	127.0.0.1:49889	127.0.0.1:53	51 / 51
domain	UDP	127.0.0.1:49286	127.0.0.1:53	64 / 0
domain	UDP	127.0.0.1:36579	127.0.0.1:53	102 / 102
www	TCP	192.168.1.74:56138	192.168.1.1:80	4642 / 1957
domain	UDP	172.16.1.104:22245	192.168.240.4:53	64 / 64
domain	UDP	127.0.0.1:46568	127.0.0.1:53	51 / 51
www	TCP	192.168.1.74:56143	192.168.1.1:80	742 / 360
domain	UDP	127.0.0.1:40762	127.0.0.1:53	51 / 51
domain	UDP	127.0.0.1:51117	127.0.0.1:53	51 / 51
domain	UDP	127.0.0.1:47935	127.0.0.1:53	51 / 51

Figure 13.21: Detailed IP Connection List

14

Troubleshooting

This chapter suggests solutions for problems you may encounter in installing or using the Oxygen Multiservice Gateway, 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 broadband 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	Purple during the boot sequence. Solid Blue to indicate that the device has finished booting. If this light is not on, check the power cable attachment.
DSL	Blinking Blue when a synchronization attempt is being performed. Solid Blue upon successful synchronization.
Internet	Blinking Blue while trying to connect. Solid Blue when a valid IP address has been assigned to the device by the ISP. Solid Red when an invalid username/password combination is being used.
Ethernet	Solid Blue to indicate active link on the corresponding Ethernet link. Blinking when the device is sending or receiving data from the LAN.
Wireless	Solid Blue 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 Blue 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>	Verify that you are using the power adapter provided with the device and that it is securely connected to the Oxygen Multiservice Gateway and a wall socket/power strip.
<i>DSL LED does not illuminate after phone cable is attached.</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>Ethernet LED does not illuminate after Ethernet cable is attached.</i>	Verify that the Ethernet cable is securely connected to your PC or LAN switch and to the Oxygen Multiservice Gateway. 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.
Internet Access	
<i>My PC cannot access the Internet</i>	<p>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 Multiservice Gateway's LAN IP address (by default 192.168.1.1). 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:</p> <ul style="list-style-type: none"> • Check that the gateway IP address on the computer is Oxygen Multiservice Gateway's LAN IP address (by default 192.168.1.1). If it is not, correct the address or configure the PC to receive IP information automatically through DHCP. • Verify DNS IP of CPE

<i>My LAN PCs cannot display web pages on the Internet.</i>	<ul style="list-style-type: none">• Verify that the DNS server IP address specified on the PC is the IP address of the Oxygen Multiservice Gateway (by default <i>192.168.1.1</i>) then verify with your ISP that the address configured on the Oxygen Multiservice Gateway is correct.• You can use the Ping utility, discussed on page 175, to test connectivity with your ISP's DNS server.
---	--

Web pages

<i>I forgot/lost my username or password.</i>	<p>If you have not changed the password from the default, try using the username and password that is printed on the label on the bottom of the Oxygen Multiservice Gateway. 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>
<i>I cannot access the web pages from my browser.</i>	<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 <i>192.168.1.1</i>). 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, and that Javascript is enabled. 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 Multiservice Gateway.</p>

Diagnosing Problem using IP Utilities

Ping

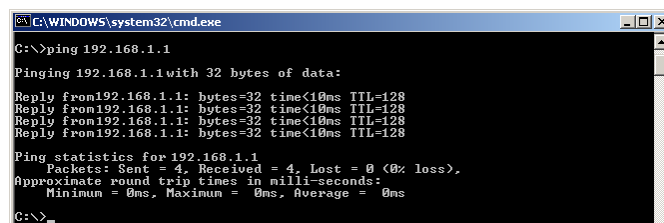
Ping is a command you can use to check whether your PC can recognize other computers on your network and the Internet. A ping command sends a message to the computer you specify. If the computer receives the message, it sends messages in reply. To use it, you must know the IP address of the computer 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 192.168.1.1
```

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 Multiservice Gateway is working (using the preconfigured default LAN IP address 192.168.1.1) 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). You can also specify a host name as ping target (e.g. *ping www.google.com*). This way you test both DNS operation and IP connectivity.

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 your Oxygen Multiservice Gateway which forwards requests to the DNS server of 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:

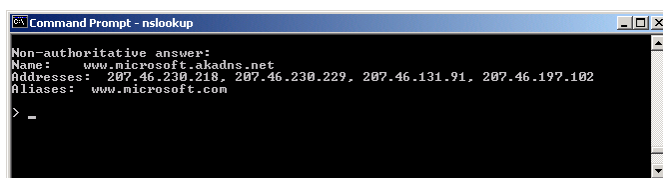


Figure 14.2: Using the nslookup Utility

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 Multiservice Gateway.

Configuring Ethernet PCs

By default, the Oxygen Multiservice Gateway automatically assigns the required Internet settings to your PCs.

- Follow the instructions that correspond to the operating system installed on your PC in order to configure it to accept IP addressing information assigned by the Oxygen Multiservice Gateway (DHCP operation)
- If you want to allow Wireless PCs to access your device, follow the instructions in **Configuring Wireless PCs** on page 178.

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 Multiservice Gateway 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 Multiservice Gateway. By default, the LAN port is assigned the IP address **192.168.1.1**. (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 that correspond to the operating system installed on your PC for static IP address configuration.

**Note**

Your PCs must have IP addresses that place them in the same subnet as the Oxygen Multiservice Gateway's Data LAN port.

Configuring Wireless PCs

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 Multiservice Gateway.
 - ii Configure the SSID, encryption method and channel to match the corresponding values previously configured on the device. (see **Security** on page 91). Default values are shown in Table 4.2 on page 50.
4. Configure TCP/IP setting for the operating system installed on your Wireless enabled PCs using the same procedure described for **Configuring Ethernet PCs** on page 177.

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



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 192.168.1.0. 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**

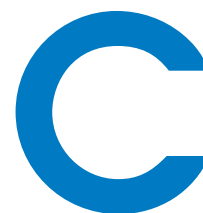
Sometimes a subnet mask does not specify any additional network ID bits, and thus no subnets. Such a mask is called a default subnet mask. These masks are:

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.



Voice Supplementary Services

The voice functionality offered by the Oxygen Broadband Oxygen series of broadband access devices, include a series of **Supplementary Services** like *Call Hold*, *Call Waiting*, *Call Transfer*, *3-Party Call*.

In the following paragraphs you can find instructions of the key sequences used in order to handle these supplementary services.

Call Hold

Call Waiting

Call Transfer

3-Party Call

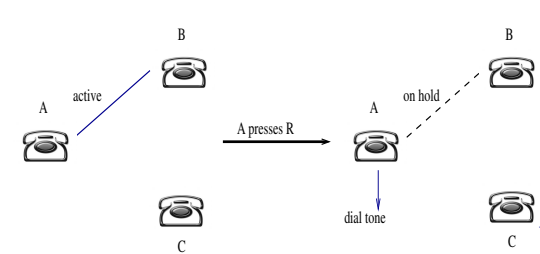
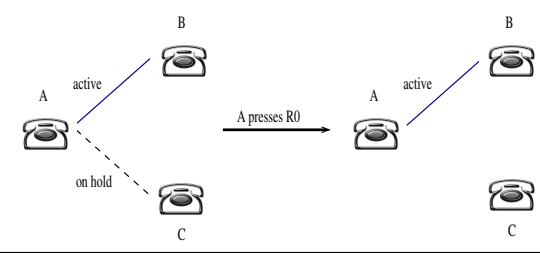
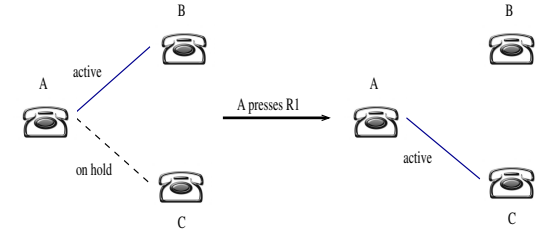
Illustration	Action
 <p>The diagram illustrates the first step of the 'Activate Hold' process. On the left, a telephone labeled 'A' is connected to a telephone labeled 'B' by a solid blue line, with the word 'active' written above the line. A second telephone labeled 'C' is shown below 'B'. An arrow labeled 'A presses R' points to the right. On the right, telephone 'A' is now connected to 'B' by a dashed line, with 'on hold' written above it. A solid blue line now connects 'A' to 'C', with 'dial tone' written below it. Telephone 'C' is also shown below 'B'.</p>	<p>Press the button R, to put an active call on hold and enable a call set up.</p> <p>* a dial tone is generated</p>
 <p>The diagram illustrates the second step. On the left, telephone 'A' is connected to 'B' by a dashed line ('on hold') and to 'C' by a solid blue line ('active'). An arrow labeled 'A presses R0' points to the right. On the right, telephone 'A' is connected to 'B' by a solid blue line ('active'), and telephone 'C' is shown below 'B' without any connection to 'A'.</p>	<p>Press the buttons R and 0, to terminate the call on hold.</p>
 <p>The diagram illustrates the third step. On the left, telephone 'A' is connected to 'B' by a solid blue line ('active') and to 'C' by a dashed line ('on hold'). An arrow labeled 'A presses R1' points to the right. On the right, telephone 'A' is connected to 'C' by a solid blue line ('active'), and telephone 'B' is shown above 'C' without any connection to 'A'.</p>	<p>Press the buttons R and 1, to switch to the call on hold and terminate an active call.</p>

Table C.1: Activate Hold

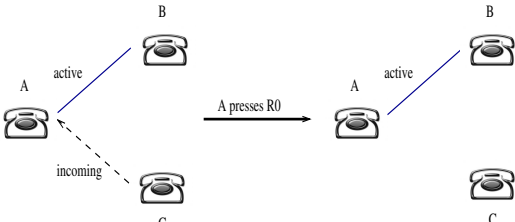
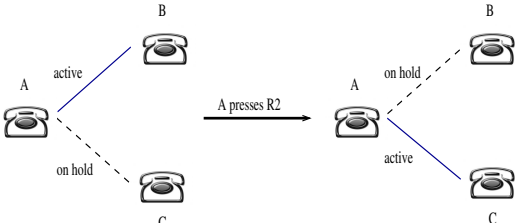
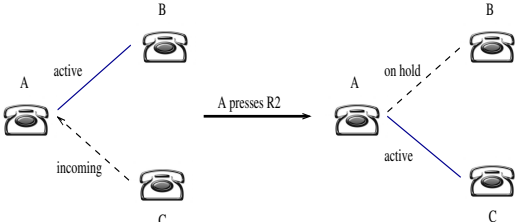
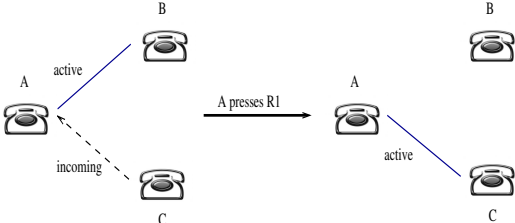
Illustration	Action
 <p>The diagram shows a sequence of two states. In the first state, a telephone labeled 'A' is connected to 'B' via a solid blue line labeled 'active'. A dashed line labeled 'incoming' points from a telephone labeled 'C' to 'A'. An arrow labeled 'A presses R0' points to the second state. In the second state, 'A' is still connected to 'B' via a solid blue line labeled 'active', but the incoming call from 'C' is no longer present.</p>	<p>Press the buttons R and 0, to reject an incoming call.</p>
 <p>The diagram shows a sequence of two states. In the first state, 'A' is connected to 'B' via a solid blue line labeled 'active' and to 'C' via a dashed line labeled 'on hold'. An arrow labeled 'A presses R2' points to the second state. In the second state, 'A' is connected to 'C' via a solid blue line labeled 'active' and to 'B' via a dashed line labeled 'on hold'.</p>	<p>Press the buttons R and 2, to switch between a call on hold and an active call.</p>
 <p>The diagram shows a sequence of two states. In the first state, 'A' is connected to 'B' via a solid blue line labeled 'active' and an incoming call from 'C' is shown with a dashed line labeled 'incoming'. An arrow labeled 'A presses R2' points to the second state. In the second state, 'A' is connected to 'C' via a solid blue line labeled 'active' and the call from 'B' is now shown with a dashed line labeled 'on hold'.</p>	<p>Press the buttons R and 2, to switch between an active call and an incoming call.</p>
 <p>The diagram shows a sequence of two states. In the first state, 'A' is connected to 'B' via a solid blue line labeled 'active' and an incoming call from 'C' is shown with a dashed line labeled 'incoming'. An arrow labeled 'A presses R1' points to the second state. In the second state, 'A' is connected to 'C' via a solid blue line labeled 'active', and the call to 'B' is no longer present.</p>	<p>Press the buttons R and 1, to terminate an active call and switch to an incoming call.</p>

Table C.2: Activate Waiting

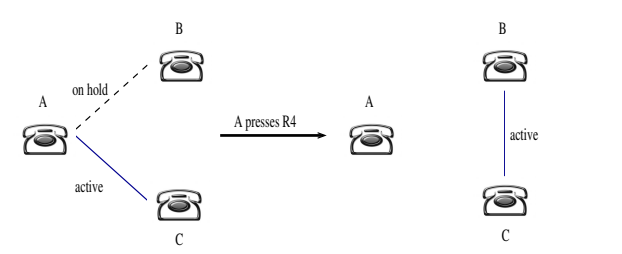
Illustration	Action
	Press the buttons R and 4, to transfer a call.

Table C.3: Activate Transfer

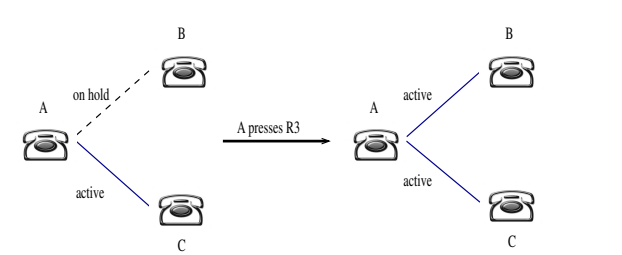
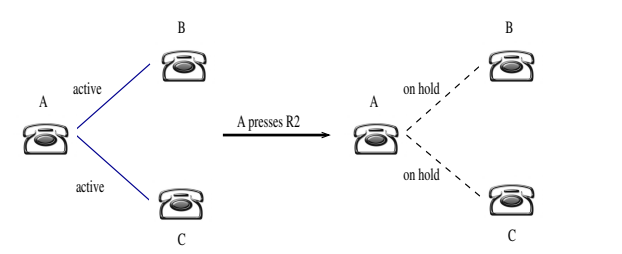
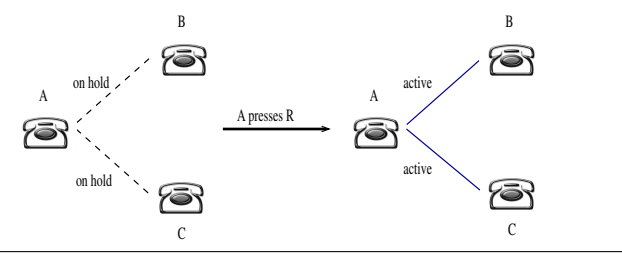
Illustration	Action
	Press the buttons R and 3, to establish a 3-party call.
	Press the buttons R and 2, to put B and C on hold. * during a 3-party call
	Press the button R, to retrieve B and C. * during a 3-party call

Table C.4: Activate 3-Party Call



Network Printing

The Oxygen Multiservice Gateway 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 Multiservice Gateway. 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 **192.168.1.1** 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 Multiservice Gateway, which uses the IPP protocol. This alternative requires the use of local storage space in the Oxygen Multiservice Gateway, 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://192.168.1.1:631/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 Multiservice Gateway.

**Note**

The IP address **192.168.1.1** used in all the configuration examples, is the default LAN IP address of your Oxygen Multiservice Gateway. 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 Multiservice Gateway firmware versions.



WPA/WPA2 support

The Oxygen Multiservice Gateway 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.

Microsoft Windows and WPA/WPA2 support

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

How to Configure SSL-VPN

The Oxygen broadband devices support both **Server** and **Client** modes for the SSL-VPN Tunnel. This means that we can use an Oxygen Multiservice Gateway 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 122). 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 11.3 in page 122).

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 accross 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 substabtially reduced by unnecessary broadcast traffic that should be limited to the high-bandwidth LAN.




WARNING

When using the Oxygen Multiservice Gateway in Bridged Mode, make sure that ONLY one DHCP server is active on both sides of the Layer-2 VPN link.

Server Mode

When Oxygen Multiservice Gateway is configured to run in *Server* mode, the configuration page presented in Figure 11.4 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 11.5 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 Multiservice Gateway.



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 Multiservice Gateway is configured to run in *Client* mode, the following fields appear in the SSL-VPN web configuration page presented in Figure 11.3. 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 Multiservice Gateway are going to appear to the server as if they have the client's VPN 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 Multiservice Gateway acting as the server, this is the zip file

that was generated 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. After successfully uploading the zip file, the last step you may have to perform (unless your SSL VPN server uses the **Dynamic DNS** Service), is to correctly specify the public IP address of the VPN Server in the **Host/IP** field.

PC Client

In order to connect from a PC to an Oxygen Multiservice Gateway 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 edit 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 address of the OpenVPN server and **port** is equal to 1194.

Once the connect.ovpn file contains the correct hostname or IP address 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.

**Note**

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.

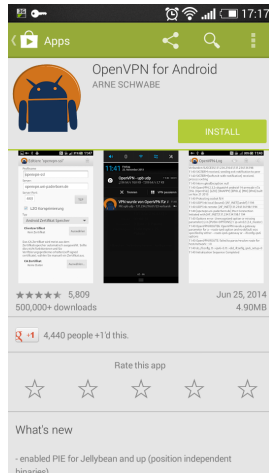


Figure F.1: Installation in Play

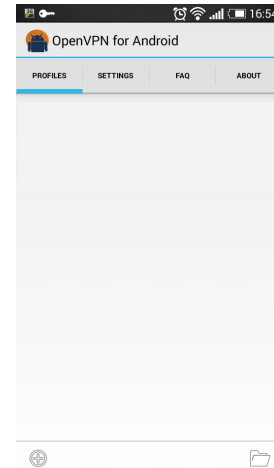


Figure F.2: Creation of Profile

Android Device Client

In order to connect from an Android smartphone or table to an Oxygen Multiservice Gateway configured to run in *Server* mode, you will need to install the **OpenVPN for Android** client, which can be found in **Google Play**.

After installing the **OpenVPN for Android**, the next step is to create an appropriate VPN profile. To this end you must first create a new VPN user on the Oxygen VPN server and then transfer to your Android device all files contained in the the zip archive that was generated by the server upon the user creation (seperate files, not in zip format). After having transfered the appropriate configuration and certificate files to your Android device, start the **OpenVPN for Android** application and press the folder icon on the lower-right corner of the screen.

Next step is to select the appropriate **connect.ovpn** configuration file, which contains all the OpenVPN connection parameters. After selecting it, the configuration file is loaded and verified by the device and, if everything is correct, a new VPN profile is generated.

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 configuraion file already contains the corresponding hostname of the server. Otherwise, you must manually configure the correct **Server Address**. To this end, press the Edit button, select the **Basic** settings menu and finally configure the correct **Server Address**.

Once the profile has been successfully created, you are ready to connect. You can connect by pressing on the profile name. Logging information will appear.

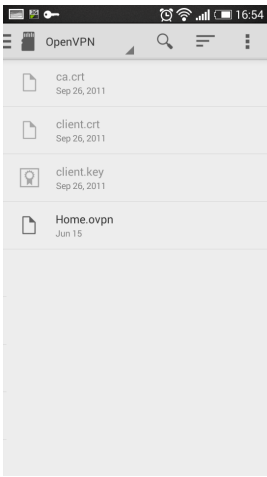


Figure F.3: Importing File

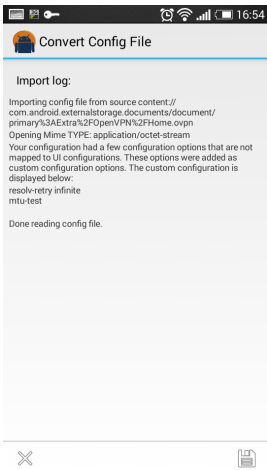


Figure F.4: File Validation

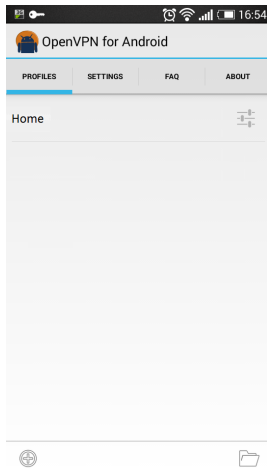


Figure F.5: New VPN Profile

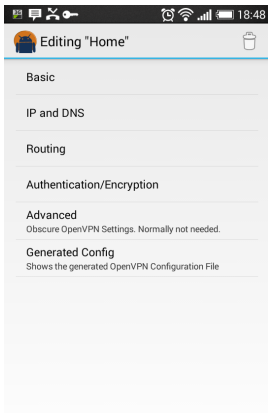


Figure F.6: Editing VPN Profile

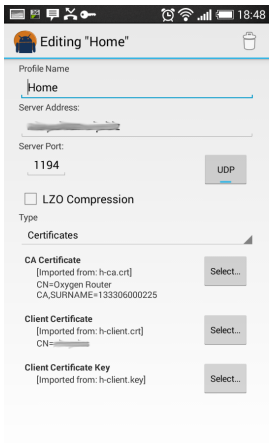


Figure F.7: Setting Server Address

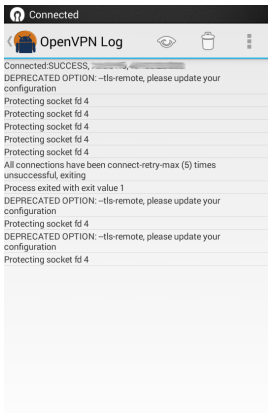


Figure F.8: Connection Log

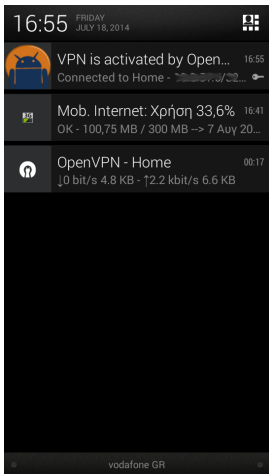


Figure F.9: Connection Status

Once connected, you can see status information on the top menu of your screen.

**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.



ISDN Interfaces

ISDN Cable Pinout

The Oxygen Multiservice Gateway 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 **Terminal (TE)** or **Network (NT)** mode . Terminal 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, Network mode must be selected in order to connect to an ISDN PBX or and ISDN phone 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 of operation. This means that, when a port is configured to operate in Network (NT) mode, a straight-through cable must be used for the connection to the corresponding TE ISDN interface (see tables G.2 and G.4). On the other hand, when a port is configured to operate in Terminal (TE) mode, an ISDN crossover cable is required (see tables G.3 and G.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				

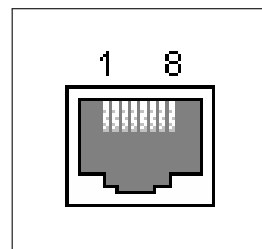


Table G.1: ISDN Interface Signals

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

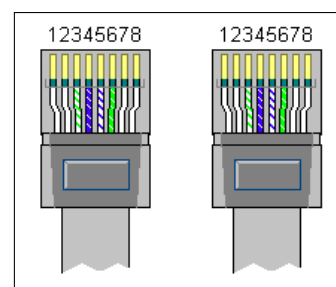


Table G.2: "Straight" ISDN BRI cable

- **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.

Termination Switches

When configured to operate in Network (NT) mode, the Oxygen Multiservice Gateway BRI interface emulates the NT unit, whereas when configured to operate in Terminal (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 Multiservice Gateway has for each BRI interface configurable

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

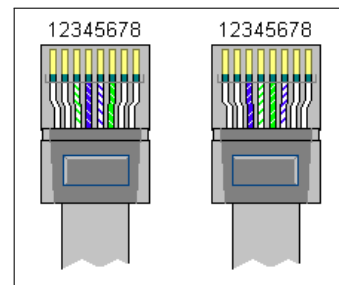


Table G.3: "Cross" ISDN BRI cable

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

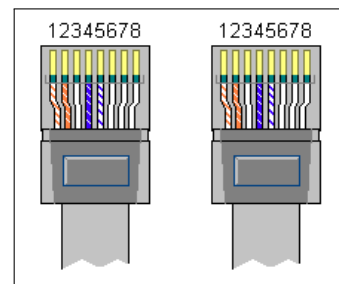


Table G.4: "Straight" ISDN PRI cable

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 Multiservice Gateway model, are located either below the BRI interfaces or at the bottom of the device.

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

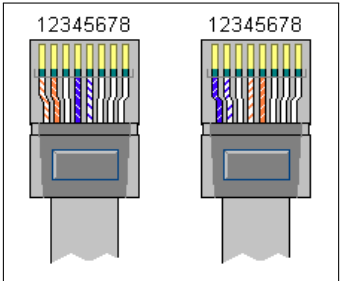


Table G.5: "Cross" ISDN PRI cable

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

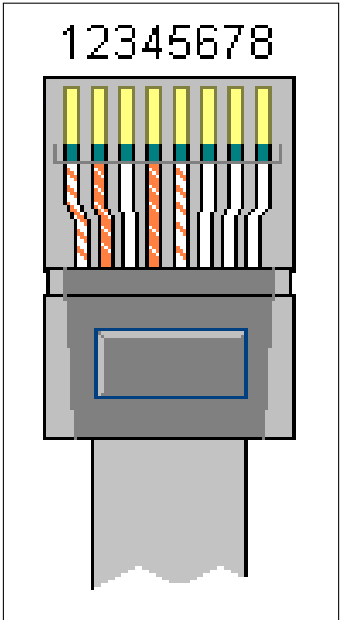


Table G.6: "Loop-back" ISDN PRI connector



Glossary

Glossary

Term	Description
6to4	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.
802.1Q	The standard issued by the IEEE defining VLAN tagging in Ethernet networks. See <i>VLAN</i> .
802.11	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.
10BASE-T	A designation for the type of Ethernet networks with a data rate of 10 Mbps. See <i>Ethernet</i> .
100BASE-T	A designation for the type of Ethernet networks with a data rate of 100 Mbps. See <i>Ethernet</i> .
ACS Server	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.

ADSL	Asymmetric Digital Subscriber Line 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.
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 <i>Dual Stack Lite</i>).
Analog	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. <i>See Digital.</i>
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	Asynchronous Transfer Mode 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	Automatic Medium-Dependent Interface Crossover 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	Bit Error Rate 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. <i>See Bit, IP Address, Network Mask.</i>
Bit	Short for "binary digit", a bit is a number that can have two values, 0 or 1. <i>See Binary.</i>
Bit-swap	Bit-swapping 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	Bits per second
BRAS	Broadband Remote Access Server 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.

Bridged EoA	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 <i>EoA</i> .
Bridging	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 Multiservice Gateway can perform both routing and bridging. See <i>Routing</i> .
Broadband	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.
Broadcast	To send data to all computers on a network.
Broadcast SSID	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 <i>SSID</i> .
CAP	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.
CBR	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.
Cell	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 <i>ATM</i> .
Certificate	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.
Certificate Authority	A certificate authority issues digital certificates and once queried verifies if a certificate presented is genuine or not.
Channel	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.
CIFS	Common Internet File System See <i>SMB/CIFS</i> .

Codec	COder-DECoder 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.
Coding Gain	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.
CPE	Customer Premises Equipment Any equipment provided by the customer at their premises.
CRC	Cyclic Redundancy Check 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.
Crossover Ethernet Cable	A type of Ethernet cable that is used to interconnect two computers by "crossing over" (reversing) their respective PIN contacts.
Crosstalk	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.
Decibel (dB)	A measure of signal intensity. It's a logarithmic unit, so an increase in 3dB is equal to double the original intensity.
DECT	Digital Enhanced Cordless Telecommunications An ETSI standard for digital portable phones (cordless home telephones), commonly used for domestic or corporate purposes.
Default Route	The network route used when no other known route exists for a given IP packet's destination IP address.
DHCP	Dynamic Host Configuration Protocol 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.
DHCP Lease	Dynamic Host Configuration Protocol Lease 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.
DHCP Relay	Dynamic Host Configuration Protocol Relay 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 Multiservice Gateway's interfaces can be configured as a DHCP relay. See <i>DHCP</i> .

DHCP Server	Dynamic Host Configuration Protocol Server A DHCP server is a computer that is responsible for assigning IP addresses to the computers on a LAN. See <i>DHCP</i> .
DHCPv6	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.
Dial Plan	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.
DiffServ	Differentiated Services 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.
Digital	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. See <i>Analog</i> .
DMT	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.
DMZ Host	DeMilitarized Zone Host A host put outside the router firewall, since all incoming connection attempts from the Internet are automatically forwarded to it.
DNS	Domain Name System The DNS maps domain names into IP addresses. DNS information is distributed hierarchically throughout the Internet among computers called DNS servers. For example, www.yahoo.com is the domain name associated with IP address 216.115.108.243. 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 <i>Domain Name</i> .
Domain Name	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. See <i>DNS</i> .
Download	To transfer data in the downstream direction, i.e., from the Internet to the user.
Downstream	Downstream refers to "host to end-user" (receive, download) direction.

DSCP	<p>Differentiated Services Code Point</p> <p>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.</p>
DSL	<p>Digital Subscriber Line</p> <p>A technology that allows both digital data and analog voice signals to travel over existing copper telephone lines.</p>
DSL Modem	<p>Short for MODulator-DEModulator, this hardware device converts ATM cells to Ethernet packets and visa-versa in the use of DSL.</p>
DSLAM	<p>Digital Subscriber Line Access Multiplexer</p> <p>A device which takes a number of ADSL subscriber lines and concentrates these to the core network of the ISP.</p>
DTMF	<p>Dual-Tone MultiFrequency</p> <p>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.</p>
Dual Stack	<p>It is a transition mechanism that allows the coexistence and independence of IPv4 and IPv6 traffic flows in the same device.</p>
Dual Stack Lite	<p>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.</p>
Duplex	<p>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.</p> <p>See <i>Full Duplex</i> and <i>Half Duplex</i>.</p>
Dynamic DNS	<p>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.</p>

Dynamic IP Addressing	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 <i>Static IP Addressing</i> .
Dynamic IP Routing	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 <i>Static IP Routing</i> .
DynDNS	See <i>Dynamic DNS</i> .
EC	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 <i>FDM</i> .
Encapsulation	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.
Encryption Key	The key encrypts data over the WLAN, and only wireless PCs configured with a key that corresponds to the key configured on the Oxygen Multiservice Gateway can send/receive encrypted data.
EoA	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.
Ethernet	The most commonly installed computer network technology, usually using twisted pair wiring. Ethernet data rates are 10 Mbps and 100 Mbps. See also <i>10BASE-T</i> , <i>100BASE-T</i> , <i>Twisted Pair</i> .
EUI-64	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	The process of erasing the current configuration of a CPE and restoring the initial default values for all parameters.

FDM	<p>Frequency Division Multiplexing</p> <p>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.</p> <p>See <i>EC</i>.</p>
Filter	See <i>Microfilter</i> .
Firewall	A security device that controls access from the Internet to a local network.
Firmware	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.
Frame	<p>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).</p> <p>See <i>Packet</i>.</p>
Frequency Band Channel	See <i>Wireless Channel</i> .
FTP	<p>File Transfer Protocol</p> <p>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.</p>
Full Duplex	Refers to the transmission of data in both directions of a wire (or other signal carrier) at the same time. Compare with <i>Half Duplex</i> .
Full LLU	<p>Full Local Loop Unbundling</p> <p>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 <i>Shared LLU</i>.</p> <p>See <i>LLU</i>.</p>
FXO	<p>Foreign Exchange Office</p> <p>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 <i>FXS</i>.</p>
FXS	<p>Foreign Exchange Station</p> <p>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 <i>FXO</i>.</p>
GAP	<p>Generic Access Profile</p> <p>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.</p> <p>See <i>DECT</i>.</p>

Gateway	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.
Gbps	Abbreviation of Gigabits per second, or one billion bits per second. Internet data rates are often expressed in Gbps.
GRE Tunnel	Generic Routing Encapsulation Tunnel A tunneling mechanisms which uses IP as the transport protocol and can be used for carrying many different passenger protocols. <i>See Tunneling.</i>
Half Duplex	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 <i>Full Duplex</i> .
Handshake	An automated process of negotiation that dynamically sets parameters of a communications channel established between two entities before normal communication over the channel begins.
Hex	Hexadecimal 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.
Host	A device (usually a computer) connected to a network.
HTTP	Hyper-Text Transfer Protocol HTTP is the main protocol used to transfer data from web sites so that it can be displayed by web browsers. <i>See Web Browser, Web Site.</i>
Hub	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. <i>See Switch.</i>
IAD	Integrate Access Device A type of CPE that offers high voice and data functionality, mainly over broadband networks.
ICMP	Internet Control Message Protocol An Internet protocol used to report errors and other network-related information. The ping command makes use of ICMP.
IEEE	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.
IGD-UPnP	Internet Gateway Device IGD is a UPnP device profile that allows UPnP aware clients to work properly from behind a NAT. <i>See UPnP.</i>
Inband	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.

Info-tainment	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.
Interface	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.
Interface Group	A group of physical ports in an Ethernet switch belonging to the same Private VLAN. <i>See Private VLAN.</i>
Interleaving	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.
Internet	The global collection of interconnected networks used for both private and business communications.
Intranet	A private, company-internal network that looks like part of the Internet (users access information using web browsers), but is accessible only by employees.
IP	Internet Protocol. <i>See TCP/IP.</i>
IP Address	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. <i>See Domain Name, Network Mask.</i>
IP Filtering	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.
IP Header	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.
IP Video	An encoding mechanism that is used to transmit motion video clips over an IP network (IPTV).
IP Voice	A technology that enables voice traffic to be transmitted over any network that uses IP, including LANs, WANs, and the Internet.
IPoA	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

IPP	<p>Internet Printing Protocol</p> <p>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.</p>
IPSec	<p>Internet Protocol Security</p> <p>A protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream.</p>
IPTV	See <i>IP Video</i> .
IPv6	<p>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 IPv6 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.</p>
ISDN	<p>Integrated Services Digital Network</p> <p>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.</p>
ISP	<p>Internet Service Provider</p> <p>A company that provides Internet access to its customers, usually for a fee.</p>
JavaScript	<p>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.</p>
Jetdirect	See <i>Appsocket / Jetdirect</i> .
Kbps	Kilobits (or thousands of bits) per second. When used in reference to transmission rates, the prefix kilo means exactly one thousand.
L2TP	<p>Layer-2 Tunneling Protocol</p> <p>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.</p>

LAN	<p>Local Area Network</p> <p>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.</p>
Lease	See <i>DHCP Lease</i> .
LED	<p>Light Emitting Diode</p> <p>An electronic light-emitting device. The indicator lights on the front of the Oxygen Multiservice Gateway are LEDs.</p>
Line Card	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.
LLC	<p>Logical Link Control</p> <p>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 <i>VC Mux</i>.</p>
LLU	<p>Local Loop Unbundling</p> <p>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 <i>Full LLU</i>, <i>Shared LLU</i>.</p>
Load Coil	A metallic, doughnut shaped device used on local loops to extend their reach. Load coils severely limit the bandwidth in digital communications.
Local Loop	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.
LPD	<p>Line Printer Daemon</p> <p>A printing method most commonly used in Unix/Linux systems and TCP/IP networks.</p>
MAC address	<p>Media Access Control Address</p> <p>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.</p>
MAC Filtering	An access-control method based on the MAC address of the clients attempting to connect.
Mask	See <i>Network Mask</i> .
Mbps	Abbreviation for Megabits per second, or one million bits per second. Network data rates are often expressed in Mbps.

MER	<p>MAC Encapsulated Routing</p> <p>This term is usually used for routed EoA connections.</p> <p>See <i>EoA</i> and <i>Routed EoA</i>.</p>
Microfilter	<p>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.</p>
Modem	<p>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.</p>
MTU	<p>Maximum Transmission Unit</p> <p>The largest packet size that can be transferred in one physical frame over a link.</p>
Multicast	<p>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.</p>
Multiplexing	<p>Transmitting several messages simultaneously on the same circuit or channel.</p>
MWI	<p>Message Waiting Indication</p> <p>The MWI is a telephony feature informing the user when there are unheard messages in the voice mailbox.</p>
Narrowband	<p>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 <i>Broadband</i> and <i>Wideband</i>.</p>
NAT	<p>Network Address Translation</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>Network Address Translation - Port Mapping Protocol</p> <p>A protocol for automating the process of port forwarding in NAT gateways. Compare with <i>IGD-UPnP</i>.</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 <i>Binary</i>, <i>IP Address</i>, <i>Subnet</i>.</p>
NIC	<p>Network Interface Card</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 <i>Ethernet</i>, <i>RJ-45</i>.</p>
Noise Margin	See <i>SNR Margin</i> .
Nslookup	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.
NTP	<p>Network Time Protocol</p> <p>A complex client/server network protocol that assures accurate synchronization of computer clock times in a network of computers.</p> <p>See <i>SNTP</i>.</p>
Numbering Plan	A scheme of rules used for the partitioning of the telephone numbers into different categories or types of subscribers.
OUI	<p>Organizational Unique Identifier</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>
Outband	<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 <i>RFC 2833</i> and <i>RFC 2976</i>. Compare <i>Inband</i>.</p>
Packet	<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 <i>Frame</i>.</p>
Passthrough	<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>

Password	A secret sequence of characters allowing a user to authenticate himself. User-name / password combinations are required in multi-user systems allowing the user to gain access to a computer system or an online service.
Pattern	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.
PBX	Private Branch Exchange 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.
PCR	Peak Cell Rate The rate of transmitted ATM cells per second that the source device may never exceed.
PIN	Personal Identification Number A secret numeric access code used to authenticate a user.
Ping	Packet Internet (or Inter-Network) Groper A program used to verify whether there is IP connectivity between two networked hosts.
POP	Point of Presence 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).
Port (Physical)	A physical access point to a device such as a computer or router, through which data flows into and out of the device.
Port (TCP/UDP)	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.
Port Forwarding	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.

POTS	<p>Plain Old Telephone Service</p> <p>Basic analog telephone service, present in most homes worldwide, which supports very limited special facilities.</p>
PPP	<p>Point-to-Point Protocol</p> <p>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 Multiservice Gateway uses two forms of PPP called PPPoA and PPPoE. See <i>PPPoA</i>, <i>PPPoE</i>.</p>
PPPoA	<p>Point-to-Point Protocol over ATM</p> <p>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.</p>
PPPoE	<p>Point-to-Point Protocol over Ethernet</p> <p>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 Multiservice Gateway.</p>
Private IP	<p>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 <i>Public IP</i>.</p>
Private VLAN	<p>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.</p>
Protocol	<p>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.</p>
PSK	<p>Pre-Shared Key</p> <p>A shared password which was previously shared between two parties using some other secure communications channel before it needs to be used.</p>
PSTN	<p>Public Switched Telephone Network</p> <p>The circuit-switched telephone network supporting the standard analog telephony service (POTS).</p>
Public IP	<p>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 <i>Private IP</i>.</p>

PVC	<p>Permanent Virtual Circuit</p> <p>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.</p>
QoS	<p>Quality of Service</p> <p>QoS is a scheme that involves a wide of set of standards and mechanisms for ensuring high-quality performance for critical applications.</p>
RDNSS	<p>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.</p>
Registration	<p>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.</p>
Remote	<p>In a physically separate location. For example, an employee away on travel who logs in to the company's intranet is a remote user.</p>
Repeater	<p>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.</p>
RFC 2225 (previously 1577)	<p>"Classical IP and ARP over ATM"</p> <p>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.</p>
RFC 2364	<p>"PPP Over AAL5"</p> <p>This RFC describes the use of ATM Adaptation Layer 5 (AAL5) for framing PPP encapsulated packets. RFC 2364 is the basis behind PPPoA connections.</p>
RFC 2684 (previously 1483)	<p>"Multiprotocol Encapsulation over ATM Adaptation Layer"</p> <p>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.</p>
RFC 2833	<p>"RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals"</p> <p>This RFC describes how to carry DTMF signaling, other tone signals and telephony events outband in RTP packets.</p>

RFC 2976	<p>"The SIP INFO Method"</p> <p>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.</p>
RFC 4193	<p>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.</p>
RFC 5006	See <i>RDNSS</i> .
RIP	<p>Routing Information Protocol</p> <p>The original dynamic IP routing protocol used for the automatic advertisement and configuration of IP routing rules.</p> <p>See <i>Dynamic IP Routing</i>.</p>
RJ-11	<p>Registered Jack Standard-11</p> <p>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.</p>
RJ-45	<p>Registered Jack Standard-45</p> <p>The 8-pin plug used in transmitting data over cable lines. Ethernet cabling usually uses this type of connector.</p>
RO Community	<p>Read-Only Community</p> <p>An SNMP community string granting Read-Only access to the managed network device.</p> <p>See <i>SNMP</i>.</p>
Routed EoA	<p>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.</p> <p>See <i>EoA</i>.</p>
Routing	<p>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.</p>
RW Community	<p>Read-Write Community</p> <p>An SNMP community string granting Read-Write access to the managed network device.</p> <p>See <i>SNMP</i>.</p>

Second SSID	The broadcasting of a second WiFi SSID, allowing the partitioning a single physical access point into two virtual ones. See <i>SSID</i> .
Secondary DNS	A DNS server that can be used if the primary DNS server is not available. See <i>DNS</i> .
Set-top Box	See <i>STB</i> .
Shared LLU	Shared Local Loop Unbundling 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 <i>Full LLU</i> . See <i>LLU</i> .
SIP	Session Initiation Protocol 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.
SIP Domain	Session Initiation Protocol Domain A SIP domain describes a collection of SIP users and endpoints that share a common domain-part in the SIP URI addresses used.
SIP Info	See <i>RFC 2976</i> .
SIP Proxy	Session Initiation Protocol Proxy 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.
Sixxs	An IPv6 tunneling mechanism (see <i>Tunnel Brokers</i>).
SMB/CIFS	Server Message Block / Common Internet File System 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.
SNMP	Simple Network Management Protocol 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.

SNR	<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>
SNR Margin	<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>
SNTP	<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 <i>NTP</i>.</p>
SOHO	<p>Small Office Home Office</p> <p>A category of remote "power" users exhibiting a demand for enhanced functionality over their broadband connection.</p>
Speed Dial	<p>An abbreviated-dialing code that can be used for fast-dialing a pre-configured destination number.</p>
Splitter	<p>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.</p>
SRA	<p>Seamless Rate Adaptation</p> <p>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.</p>
SSH	<p>Secure Shell</p> <p>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.</p>

SSID	<p>Service Set Identifier</p> <p>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.</p> <p>See <i>Broadcast SSID</i>.</p>
SSL VPN	<p>Secure Sockets Layer Virtual Private Network</p> <p>A form of VPN that uses SSL for the encryption of the exchanged information.</p>
Static IP Addressing	<p>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 <i>Dynamic IP Addressing</i>.</p>
Static IP Routing	<p>The use of statically-configured (e.g. manually configured) routing entries in the routing table of a networked device. Compare with <i>Dynamic IP Routing</i>.</p>
STB	<p>Set-top Box</p> <p>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.</p>
Straight Ethernet Cable	<p>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.</p> <p>See <i>Crossover Ethernet Cable</i>.</p>
Subnet	<p>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.</p> <p>See <i>Network Mask</i>.</p>
Subnet mask	<p>A mask that defines a subnet.</p> <p>See <i>Network Mask</i>.</p>
Switch	<p>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.</p>
Synchronization	<p>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 <i>Training</i>.</p>

Syslog	A protocol and the associated service for the control of logging information and the optional transmission of it over the network.
T.38	A standard defined by the ITU, for the reliable outband transport of fax calls over IP networks. Compare with <i>Inband</i> .
TCP	See <i>TCP/IP</i> .
TCP/IP	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.
Telnet	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 <i>SSH</i> .
TFTP	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.
TKIP	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.
TOS	Type of Service 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). See <i>DSCP</i> .
TR-069	A technical specification by the DSL Forum for the remote management of CPEs by a central ACS server. See <i>ACS Server</i> .
Traceroute	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.
Traffic Class	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.
Training	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 <i>Synchronization</i> .

Triggers	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.
Triple-Play	A term usually used for the description of broadband networks supporting Data, Voice and Video services at the same time.
Tunnel Brokers	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 tunnelling 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.
Tunneling	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.
Twisted Pair	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. <i>See 10BASE-T, 100BASE-T, Ethernet.</i>
UBR	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.

UDP	<p>User Datagram Protocol</p> <p>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.</p> <p>See <i>TCP/IP</i>.</p>
ULA	<p>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.</p>
Unicast	<p>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 <i>Broadcast</i> and <i>Multicast</i>.</p>
Unnumbered Interfaces	<p>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 (192.168.1.1). The unnumbered interface is temporary — PPP or DHCP will assign a "real" IP address automatically.</p>
UPnP	<p>Universal Plug and Play</p> <p>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.</p>
Upstream	<p>The direction of data transmission from the user to the Internet.</p>
URL	<p>Uniform Resource Locator</p> <p>An address that specifies the location of a file or a service on the Internet (e.g. http://www.oxygenbroadband.com).</p>
USB	<p>Universal Serial Bus</p> <p>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.</p>
USB Device Port	<p>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.</p>

USB Host Port	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.
Username	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.
V.90 / V.92	International standards for 56K data communications.
VBR	Variable Bit Rate 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.
VC	Virtual Circuit 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. See <i>PVC</i> .
VCI	Virtual Circuit Identifier 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. See <i>PVC</i> .
VCmux	Virtual Circuit Multiplexing 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 <i>LLC</i> .
VDSL	Very High Bit-rate Digital Subscriber Line A DSL technology variation proposed for shorter local loops, which provides 13 - 53Mbps downstream and 1.5 - 2.3Mbps upstream.
VLAN	Virtual Local Access Network 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.
VLAN ID	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. See <i>VLAN</i> .
VoIP	See <i>IP Voice</i> .
VPI	Virtual Path Identifier 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. See <i>VC</i> .

VPN	<p>Virtual Private Network</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>Wide Area Network</p> <p>Any network spread over a large geographical area, such as a country or continent. With respect to the Oxygen Multiservice Gateway, WAN refers to the Internet. Compare with <i>LAN</i>.</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 <i>HTTP</i>, <i>Web Site</i>, <i>WWW</i>.</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 <i>Web Site</i>.</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 <i>HTTP</i>, <i>Web Page</i>.</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 <i>Wireless LAN</i>.</p>

Wireless	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. <i>See Wireless LAN.</i>
Wireless Channel	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.
Wireless LAN	Wireless Local Area Network 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.
WLAN	<i>See Wireless LAN.</i>
WPA / WPA2	Wi-Fi Protected Access 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.
WWW	World Wide Web Also called (the) Web. Collective term for all web sites anywhere in the world that can be accessed via the Internet.
xDSL	Refers to the family of digital subscriber line technologies, such as ADSL, HDSL, IDSL, RADSL, SDSL and VDSL.